Authentication and Authorization

A Public Key Infrastructure for Authentication

The Grid Security Infrastructure (GSI) is based on asymmetric cryptography used in a "Public Key Infrastructure" (PKI). Asymmetric cryptography allows users to communicate securely without the need for a prior confidential channel to exchange encryption key. Exploiting features of a specific class of mathematical challenges that are easy to create but virtually impossible to solve (like factorizing large prime numbers), end-entities generate a complementary set of keys: a "private key" that will be kept secret and a "public key", that is broadcast to the world. Data encrypted with the public key can only be deciphered with the private key (and vice versa). Thus data confidentiality, message integrity and non-repudiation can be achieved between two halves of the key pair.

A PKI is used to uniquely bind an identifier to a specific public key together in a "certificate". The identifier can represent any entity: a human being, a host on the Internet or a Grid service. Anyone wanting to communicate to another entity on the Grid can obtain their certificate and use the public key contained in it to send messages that can only be read by the original owner – who has knowledge of the private key needed to decipher the message. But the sender must first be sure that the intended recipient is indeed the holder of this private key. Therefore a trusted third party digitally signs the certificate: the Certification Authority (CA). The CA certifies with its signature that the identifier contained in the certificate is a truthful representation of the identity that possesses the associated private key. The CA's digital signature is again based on public-key cryptography.

In TB1 a limited set of Certification Authorities is considered trustworthy by all participating entities: system administrators, end-users and Grid services. This trust is based on a detailed Certificate Policy and a Certification Practice Statement (CP, CPS) that describes, *e.g.*, the way the user is authenticated and what precautions are taken against compromise of the CA. Virtually all CA's accepted in TB1 have drafted such a CP/CPS or have elaborated on their procedures in the WP6 CA Coordination Group (CACG). Each CA covers one country or a small group of countries (in case of the Nordic countries). In this way reliable user authentication can occur face-to-face. This is essential in order to convey trust in the certificates.

The CACG makes binding recommendations to the TB1 administrators on which CA's to trust for user authentication. In TB1 11 CA's have been included: CERN, Czech Republic (CESNET), France (CNRS), Ireland (TCD), UK (GridPP), Italy (INFN), Portugal (LIP), Netherlands (NIKHEF), Nordic Countries (NBI), Russia (Moscow Universities), and Spain (IFAE).

The distributed CA model has been validated using cross-domain submission of jobs on the Grid in May 2001.

Authorization and Virtual Organizations

In the Grid Security Infrastructure, authorization decisions are made at the local resource level. Entities authenticate themselves using their certificate and the ability to use their private key. Pre-existing GSI solutions subsequently relied on a static list of certificate subject names to authorize users. In TB1 this was extended with support for hierarchical directory-based user lists ("Virtual Organization", VO support). An LDAP-based directory service retains a list of users (certificate subject names) that are part of a VO, managed by a representative of the community. This list of users is further divided into groups, managed by one or more group administrators. Test bed sites periodically retrieve a list of users from this

directory and configure access to their resource according to a local policy file. Since the user subject name in used as a key in the authorization list, individual subject names can be in only one Virtual Organization.

Tools developed by the WP6 Authorization Working Group are available on the test bed to support this VO mechanism. Graphical interfaces are available to assist VO managers and group administrators in assigning users to VO's and specific groups. Resource providers can avail of a tool to periodically retrieve new user list and verify these list for compliance with the Usage Guidelines.

The EDG Usage Guidelines were established to allow users on the test bed to register for access just once. The Usage Guidelines describe a basic code of ethics to be adhered to when using the test bed. Users that accepted the Usage Guidelines do not need to subscribe to the Acceptable Use Policy (AUP) of each of the participating sites individually. However, users will still be subject to local site regulations and relevant legislation at every resource they access on the test bed. In the event of a security incident, the rules of the site concerned and the legislation of the State(s) concerned shall be applied.

Users can sign the Usage Guidelines using a secure electronic message exchange, and they are authenticated with their existing identity certificate. The acceptance of the Guidelines in this transaction is recorded in a validation directory.

On the test bed there are six major user communities, assembled in the application work packages: four for WP8, one for WP9 and one for WP10. Directory services have been configured for each of these communities. The Usage Guidelines validation directory is queried to ensure that only users that have agreed to the EDG Usage Guidelines will be allowed access to the TB1 facilities. The complete system is not functional on the test bed.

Local authorization and control

Once a resource provider has authorized a user task to run on the local system, this task is subject to local operating system limitations. It is therefore required that each individual entity on the grid is assigned a unique local identity. In case of a large number of users and resources, a complete mesh will not be established. To take advantage of this reduction in complexity, and to reduce the workload on local test bed administrators in the creation of new accounts, an account-leasing scheme was designed and implemented in the test bed. On first entry into a test bed site, new users are given a temporary "leased" identity. This leased identity is valid as long as the task will last, and need not be freed afterwards. If the lease still exists when the user re-enters the site, the same account will again be assigned to this user. This "gridmapdir" mechanism has been successfully deployed on TB1.