Security and Trust in an Industrial Grid Project

In usual Grid security infrastructures based on personal Grid certificates, it is possible for users (i.e., employees), to first copy data (or software) to a Grid resource using their personal certificate and then copy this from another security domain to some other place. In the D-Grid project AeroGrid, which provides a Grid infrastructure and client tools for an industrial application from the aerospace domain, the industrial partner is a large turbine manufacturer with high demands on security. It is an important requirement that employees are not able to copy any data outside the security domain of the company. Within the project, a security policy for solving this problem has been defined. The basic strategy for a solution is as follows: The policies and the administrators of the company must forbid and enforce that employees can take the private key that belongs to the Grid certificate with them outside the company. Then the Grid certificate would be not usable for accessing data stored on some Grid resources. For the implementation of this strategy, a company-internal Grid Certificate Authority is deployed and a policy for handling certificates and private key is defined. A second industrial requirement is reliability of data arising from complex processes. To have a reliable documentation of the individual steps performed in engineering calculations, it's important to trace all processing steps, i.e. the complete Provenance of the process that led's to a certain result. Within the project, a Service-Oriented Provenance architecture for recording Provenance information (such as user interactions in the graphical user interface or execution of numerical codes) has been provided. This talk presents the security and the Provenance infrastructure of the AeroGrid project as well as details on the implementation and deployment of the security solution.

Primary authors : Mr. SCHREIBER, Andreas (German Aerospace Center (DLR))