Contribution ID: **163** Type: **not specified**

EMI Common Authentication Library

Tuesday, 27 March 2012 12:00 (30 minutes)

Description of the Work

The work on the common authentication library started by designing the API, which was finished several months ago. The API underwent detailed reviews performed by a group of experts who evaluated the API from the standpoint of usability and security. The library mains at two goals. First, it provides a common way how a client and server can easily establish a mutualy authenticated connection and communicate over that. It also provides functions for applications that need to perform operations with the credentials, especially proxy certificates. The API provided covers C, C++ and Java.

After finalizing the API, a product team has been established, which will provide the implementations of the API. The implementations of all the three language bindings will be provided as part of EMI-2 and will be handed out to the EMI product teams for integration with their products.

The talk will describe the main principles of the API and present code snippets showing particular functions of the API.

Conclusions

The EMI common authentication library will be delivered in EMI-2 and be available for EMI product teams. The talk will describe the library emphasizing how the API can be integrated with the applications.

Impact

The EMI common authentication library will provide a single API that is small and do not require many dependencies, which makes it easier to integrate with applications. It covers the main functions needed by EMI components that could utilize the library instead of their current code for handling security functions. Such a move will decrease the maintaince cost of the components and ensure better compatibility.

An attempt has also been made to keep the API independent of particular SSL implementations, which would allow us to switch to another underlying SSL library if needed. The abstraction of the API would also ease the transition to completely different authtentication schema if such a request emerges in the future.

Overview (For the conference guide)

The EMI components utilize the PKI with the SSL/TLS protocol suite for authentication of users and other services they interact with. For historic reasons, most components implement the authentication functions independently on each other, which yields code with similar functionality being implemented
at various places again and again. For the same reasons there is no “profile”defining details of SSL handshake or verification of certificates, etc. Also the grid specifics, such as processing of X.509 certificate and handling of CA policies, are not implemented in a common way. Such an arrangement makes it harder to add new features and also maintain the code basis.

EMI has decided to design and implement a common authentication library that implements the main functions necessary to establish an authenticated connection and exchange messages that are sufficiently protected.

Primary authors: KONSTANTINOV, Aleksandr (University of Oslo); KOURIL, Daniel (CESNET); BENEDYCZAK, Krzysztof (UWAR); MARCEL, Poul (CESNET); ŠUSTR, Zdenek (CESNET)

Presenter: KOURIL, Daniel (CESNET)

Session Classification: Information Systems: ARC/GLUE2, EMI Registry (EMIR) and Authentication Library