Contribution ID: **8** Type: **not specified**

Signing (and encrypted) message handling and implications for admins.

Monday, May 2, 2011 2:00 PM (30 minutes)

In grid computing we use an X509 PKI security infrastructure. This infrastructure is used to enable secure connections between hosts to deliver payload. This often leads to scalability and reliability issues. This talk presents the alternative approach of signing messages for asynchronous handling, allowing authentication of the payload rather than the connection.

The implications of this approach will be illustrated showing how service interdependency can be reduced, and clustering simplified. AMQP (RabbitMQ) will be used as a transport mechanism in this talk to illustrate these concepts. Both the openssl command line and a python library can be used to authenticate signed messages making scalable secure authentication between sites resources practical for administrators.

Summary

How authentication of signing (and encrypted) message handling makes life easier.

Primary author: SYNGE, Owen (DESY (HH))

Presenter: SYNGE, Owen (DESY (HH))

Session Classification: Networking & Security

Track Classification: Security & Networking