Design and Implementation of a Management Service for Digital Certificates

With the TUM Secure E-Mail project, we have the goal to improve security and confidentiality of e-mail communication at TUM. The vision is to equip all students, researchers and administrative staff with digital S/MIME and OpenPGP certificates to enable authenticated, integrity protected and confidential communication between internal and external communication partners.

One of the main challenges within this project is to generate and distribute these certificates and to allow users to perform management tasks like renewing, updating and revoking certificates.

The goal of this thesis is to present the design and realization of a modular and extensible certificate management service to issue, manage and publish S/MIME and OpenPGP certificates. This service has to integrate with existing IT services like authentication services, manage and forward certificate requests and publish certificate information to key servers and directory services.

- Create a flexible and extensible design for a certification service
- Develop and realize required processes for issuing and managing certificates
- Focus on integration with existing IT services
- Implement and test your idea with a strong focus on security

- Passion and a good portion of curiosity
- You are aware of things like OpenPGP, S/MIME and X.509
- You did some coding before and you liked it
- You like to create and realize software architectures
- You are allergic against a lack of security

Matthias Wachs  (wachs@net.in.tum.de)
http://go.tum.de/080020