Enabling OpenPGP in Multi-Device Environments

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.

To be able to use OpenPGP for secure e-mail communication on multiple devices, the information of a user’s OpenPGP installation has to be synchronized between the user’s devices. Existing synchronization approaches only consider the key synchronization, but to use OpenPGP in a convenient way for unexperienced users, additional information including available public keys and trust information has to be exchanged between the devices.

The goal of this thesis is to develop a synchronization mechanism with a special focus on the requirements of OpenPGP to be used on multiple devices. This mechanism will synchronize all information required by OpenPGP between different devices in a secure and consistent way and will be used within the TUM Secure E-Mail project.

- Analyze requirements and processes
- Create and propose an architecture for the synchronization
- Implement and test your idea with a strong focus on usability and security

Your Expertise
- Passion and a good portion of curiosity
- You are aware OpenPGP exists
- You did some coding before and you liked it
- You like to create and realize software architectures

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