SkyTrust - Emulate Adv. Crypto

What's it about?
Crypto methods like attribute-based / identity-based encryption could play an important role in current applications. However, the current libraries are cumbersome to use in productive systems (prototypes, compatibility). Thus, the main idea of this project is to emulate such methods via the SkyTrust system and the intelligent use of authentication systems.

Goals:
- Emulate ID/Attribute-based encryption in SkyTrust
- Use authentication for the emulation

Interests:
- Cloud security
- Protocols
- Cryptography
- Work on a project with real-world impact (Project SkyTrust) AND do applied research

Impact:
- Secure cloud services
- Very important for Europe
- Flexible use of cryptography
- Enables simple encryption applications

Contact: peter.teufl@iaik.tugraz.at