SkyTrust - OpenSSL Engine

What's it about?
We want to integrate SkyTrust into existing web servers. This would allow to store key material for HTTPS servers on external SkyTrust servers while the web server instance itself is only capable of using these keys. Thus, even attacks like heartbleed cannot extract the key material. Examples for such web servers could be NGINX or Apache.

Goals:
- Create OpenSSL engine for SkyTrust

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

Impact:
- Enable web servers to use the flexible SkyTrust system
- Remove the need to locally install HSMs etc.
- Increase security and keep it usable

Contact: peter.teufl@iaik.tugraz.at