Contribution ID: **31** Type: **Presentation**

Is "zero-knowledge" privacy achievable in the distributed cloud? An in-depth analysis of encryption architecture of Cubbit's sync&share service.

Cubbit is a hybrid distributed cloud where a central "coordinator" server organizes the resources of a "swarm" of peer-to-peer interacting devices to offer performant and encrypted cloud services. One of Cubbit's core principles is "privacy by design", meaning that no third party, including the coordinator server, can access the content of the users' files.

The usual paradigm of encrypted cloud solutions is to securely store the encryption keys on the server to facilitate operations such as file sharing and synchronization on different devices. However, this solution allows the cloud provider to potentially access the user's data, thus not guaranteeing total privacy. Implementing a performant sync&share service where the provider itself is unable to access the contents of the files poses several technological as well as architectural challenges.

Here we will present the encryption architecture implemented by Cubbit to allow performant and seamless sync&share while at the same time guaranteeing zero-knowledge privacy. We will focus on key management protocols as well as upload, download, and file-share procedures.

Primary authors: Mr MOSCHETTINI, Marco (Cubbit); Mr PACCOIA, Alessio (Cubbit); Dr POSANI, Lorenzo (Cubbit)

Presenter: Mr MOSCHETTINI, Marco (Cubbit)

Session Classification: Sync/share Technology&Research

Track Classification: Synchronization/Sharing Technology & Research