SHOWCASE

Project name: Sealed Cloud

Description: Sealed Cloud was developed by a consortium consisting of Uniscon, Fraunhofer and Securenet.

In 2011, Sealed Cloud won the German Federal Ministry for Economic Affairs and Energy's Trusted Cloud competition among 117 contestants. Hence, the basic technology is improved continuously for application in German industry.

The purpose is to make Sealed Cloud infrastructure available for other applications. Sealed Cloud is a technically sealed data center that protects applications against spies, externally AND internally.

Normally, data is always processed in data centers (application servers) in unencrypted form. That's risky, since data center providers themselves and external spies can access data. Sealed Cloud fills this security hole technically.

Metadata reveals who was connected with whom, when, how often, and how long online. It reveals business strategies, personal information, and relationships. Which is why privacy advocates advise users to protect their metadata, as well. With Sealed Cloud, metadata is inaccessible.

Sealed Cloud's technical measures cover four categories:

- Perimeter Security: Business-network-to-Internet transition is secured via SSL encryption (with a key length of 2048 bit).

- Encryption & Key Management: With a key length of 256 bit, every single dataset in the database is encrypted pursuant to Advanced Encryption Standard (AES). Only the respectively authorized party can access the key. The system itself has no key.

- Data Clean-up: Should anyone, whether authorized or not, attempt to access the application servers, all unencrypted data is deleted instantly. Server access (e.g. for maintenance purposes) is only granted thereafter.

- Distribution of Power: A set of technical measures enforces the distribution of power among the various parties concerned.