Boxcryptor: “For maximum confidentiality”

With Boxcryptor it is possible to regulate access to the information reliably and thoroughly by means of encryption. The tool itself is not a storage system but a layer on top of an existing storage, it supports various forms of storage (local, network and Cloud) and is available for multiple platforms. The operation of Boxcryptor (the encryption/decryption process), once configured, is completely transparent to the user.

Boxcryptor works with file and folder oriented storage systems (not suitable for databases) and is meant for situations where confidentiality of the data is critical and regular security is not sufficient. Sharing of the data is possible if the underlying storage system also supports sharing. With the help of group management, the owner fully determines who gets access to the encrypted data.

**License and recovery**
The UU uses the Enterprise license from Boxcryptor because it offers the possibility for central administration and group management. The licenses are (for the time being) funded by ITS. To prevent data loss for the UU, one centrally secured master key can be used in emergency situations to access encrypted data. Assessment of a request to this effect lies with the CISO (Corporate Information Security Officer) of the UU and the owner of the data.

**Request**
Almost every security measure provides overhead and increases complexity. That is why Boxcryptor should only be used if really necessary. This may be because the data demands a very high level of confidentiality or, for example, if the external supplier of data sets strict requirements with regard to access of the data.

Requests for the use of Boxcryptor can be submitted to the ICT service desk, after which the LISM (Local Information Security Manager) of the faculty contacts the applicant to discuss whether and how Boxcryptor can be used best. For each storage location, a group owner is designated who can add and/or delete users after creating the folder.

**Introduction and demonstration**
Wrong use of Boxcryptor can give a false sense of security, so a brief introduction for all users is necessary. Not because it is complicated, but because the principle of encryption and the right route to the data must be perfectly clear to the user. This can be requested via the LISM.

**Confidentiality versus availability**
Boxcryptor only guarantees confidentiality. The availability of the data is determined by the agreements on the underlying storage system (think, for example, of the back-up cycle and accessibility). Please include requirements of availability in the choice of the storage system for the confidential data.