Sicherheit

Zur Erhöhung der Sicherheit im Bereich Datenlaufwerke bieten sich digitale, elektronische Signaturen und die Verschlüsselung von Dateien an.

Um diese nutzen zu können wird ein digitales Nutzerzertifikat benötigt. Bei der Erstellung wird ein digitales Schlüsselpaar erzeugt, welches durch eine Zertifizierungsstelle bestätigt wird. Dieses Schlüsselpaar besteht aus 2 Teilen, dem privaten und dem öffentlichen Schlüssel:

- Privater Schlüssel: Dieser ist passwortgeschützt und verbleibt immer im Besitz des Benutzers
- Öffentlicher Schlüssel: Dieser wird vom Kommunikationspartner benötigt und muss diesem in irgendeiner Weise bekannt gemacht werden.

Signieren

Prinzip: Mit Hilfe Ihres privaten Schlüssels signieren Sie Ihre Dateien. Der Kommunikationspartner kann dann mit Hilfe Ihres öffentlichen Schlüssels prüfen, ob / dass die Dateien unverändert vorliegen.

Verschlüsseln

Prinzip: Mit Hilfe des öffentlichen Schlüssels des Kommunikationspartners verschlüsseln Sie Ihre Dateien. Der Kommunikationspartner kann mit Hilfe seines privaten Schlüssels die Dateien dann entschlüsseln. Sie müssen also zur Verschlüsselung zunächst den öffentlichen Schlüssel des Kommunikationspartners besitzen.

Voraussetzungen

Eine grundsätzliche Voraussetzung zur Nutzung ist die korrekte Einbindung der Zertifizierungsstellen in ihr verwendetes Betriebssystem und ein gültiges digitales Nutzerzertifikat. Konfigurieren Sie dann die entsprechende Anwendungssoftware:

Pages in this namespace:

K

- Kleopatra

From:
https://hrz-wiki.jade-hs.de/ - **HRZ-Wiki**

Permanent link:
https://hrz-wiki.jade-hs.de/de/tp/datadrives/security/start

Last update: **2022/09/30 09:33**