niversity Computer Centre, in cooperation with the DFN, offers a Public Key Infrastructure (PKI) which enables the following services:

- **User certificates**:
  - Signing and encryption of files and documents
  - Signing and encryption of emails
- **Group certificates**:
  - Signing and encryption of emails
- **Server certificates**:
  - Bug-proof network connections via SSL/TLSTLS

In the architecture of a PKI, there are one or more digital certificate authorities (CAs) that issue digital certificates. These certification authorities must be known to the operating system or/and the software used so that a check of the validity of a digital certificate can be carried out.

- In the first step, it must therefore be checked whether these certification authorities are already present in the operating system / in the software to be used.
- The second step is then to apply for and use the digital certificate.

You can find more information on the website of the DFN-PKI.

Certification authorities

The control and, if necessary, integration of the certification authorities into the operating system / the software used is described in the subitem Certification authorities.

User certificates

University members - with the exception of students - can use the DFN-PKI to receive digital user certificates according to the X.509 standard. The application is described in the subitem User certificates.

Server Certificates

University members - with the exception of students - can also receive digital server certificates according to the X.509 standard with the help of the DFN-PKI. The application is described in the subitem server certificates.