openHPI – Confidential Communication in the Internet

Security Goals

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

The Internet is a Global Open Communication Networks

The Internet is an "**open**" **communication network**

- Everyone can use the Internet by connecting own devices to the Internet via an **Internet Service Provider – ISP** or a **mobile provider**
- With access to the Internet everyone can request any kind of information/data from the **WWW**
- **Data are transferred** over the Internet **in plain text** if the sender has not taken additional security arrangements

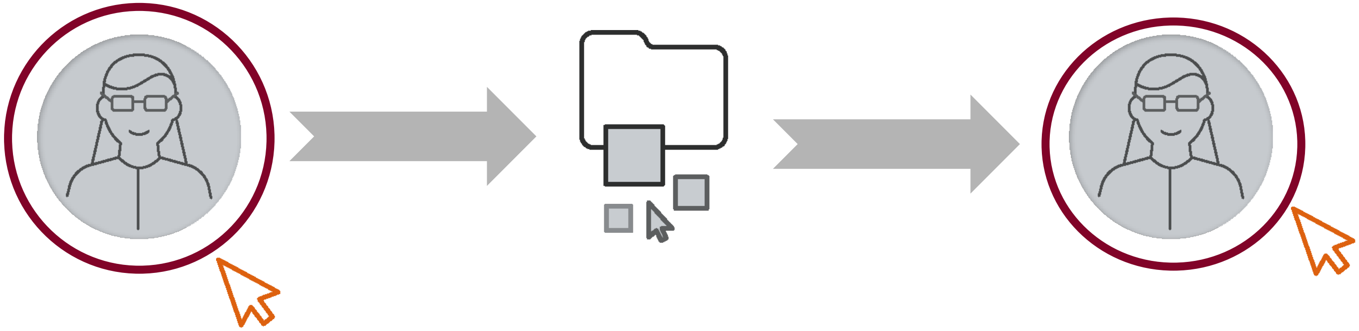
Security Requirements in Open Communication Networks

For the **safe use of the Internet**, the following security objectives must be guaranteed:

- **Integrity of the identity** of the sender,
- **Integrity** of the received information,
- **Confidentiality** of transmitted information, and
- **Legal enforceability** of internet communication
- ...

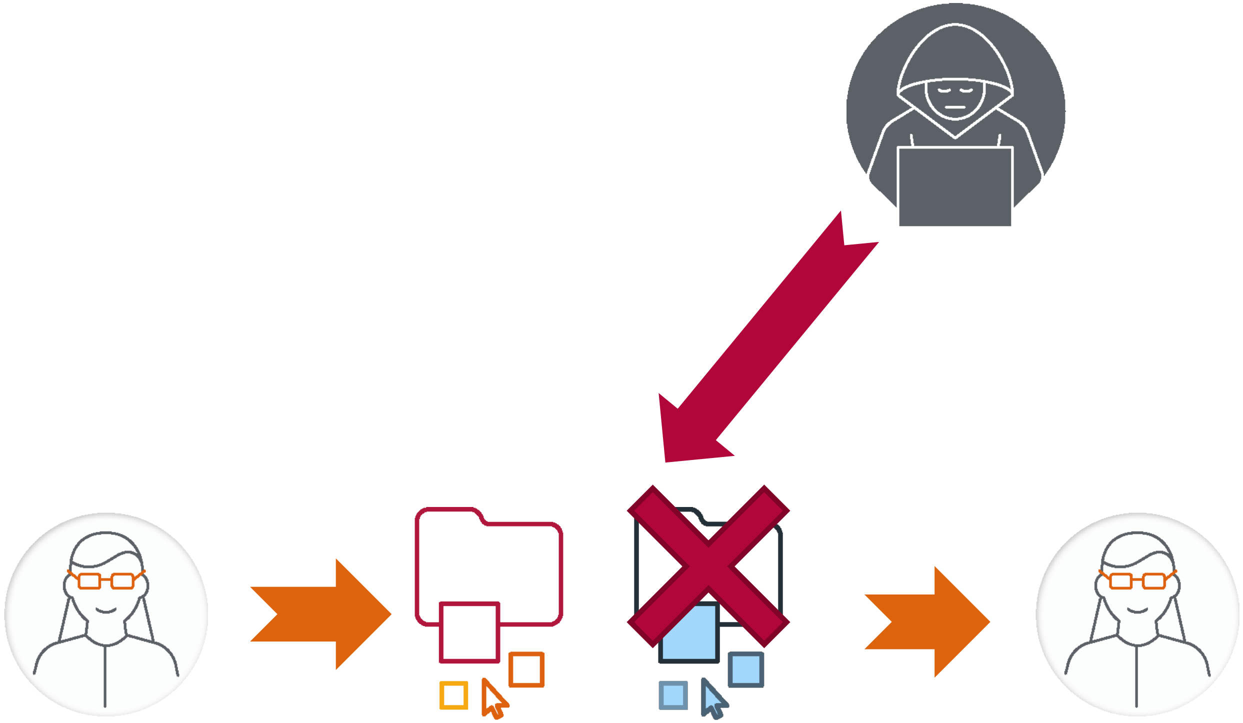
Security Goals
Identity

- Users should be able to confirm the **identity** of their communication partner



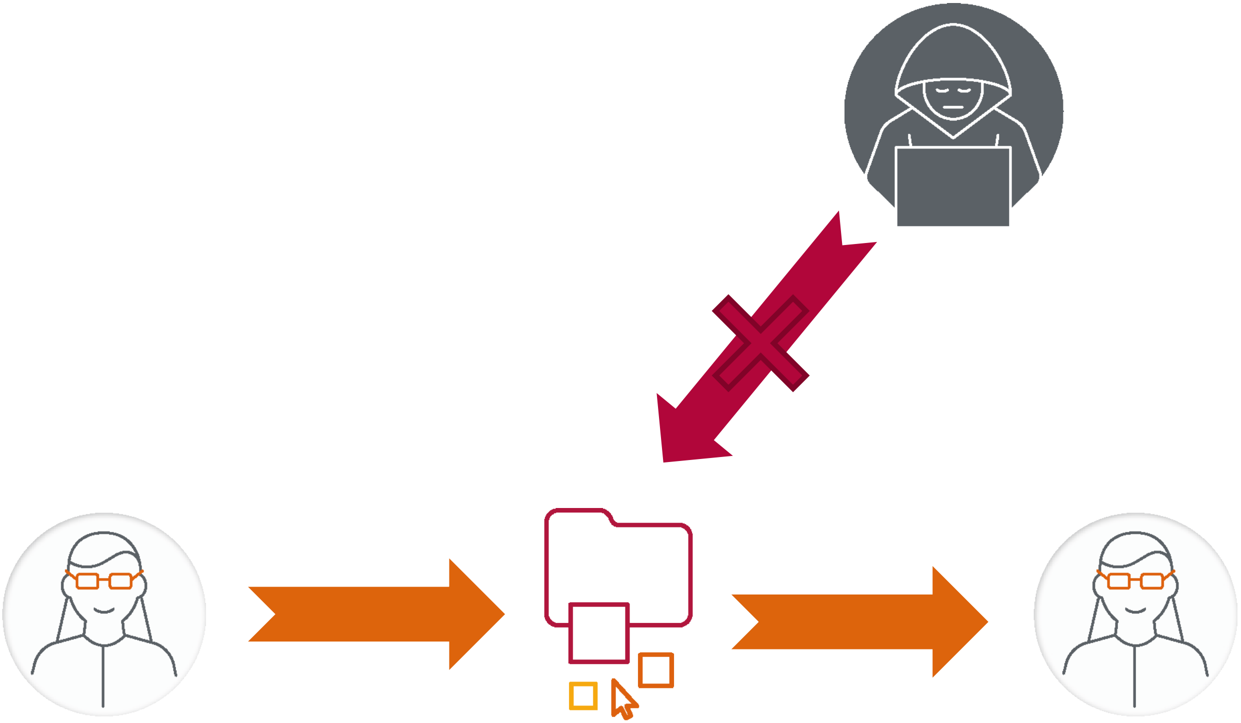
Security Goals
Integrity

- Information must not be changed (unnoticed) without authorization



Security Goals
Confidentiality

- Information must be kept secret from unauthorized parties



Security Goals
Commitment / Legal Binding

- Exchanged information should be legally binding