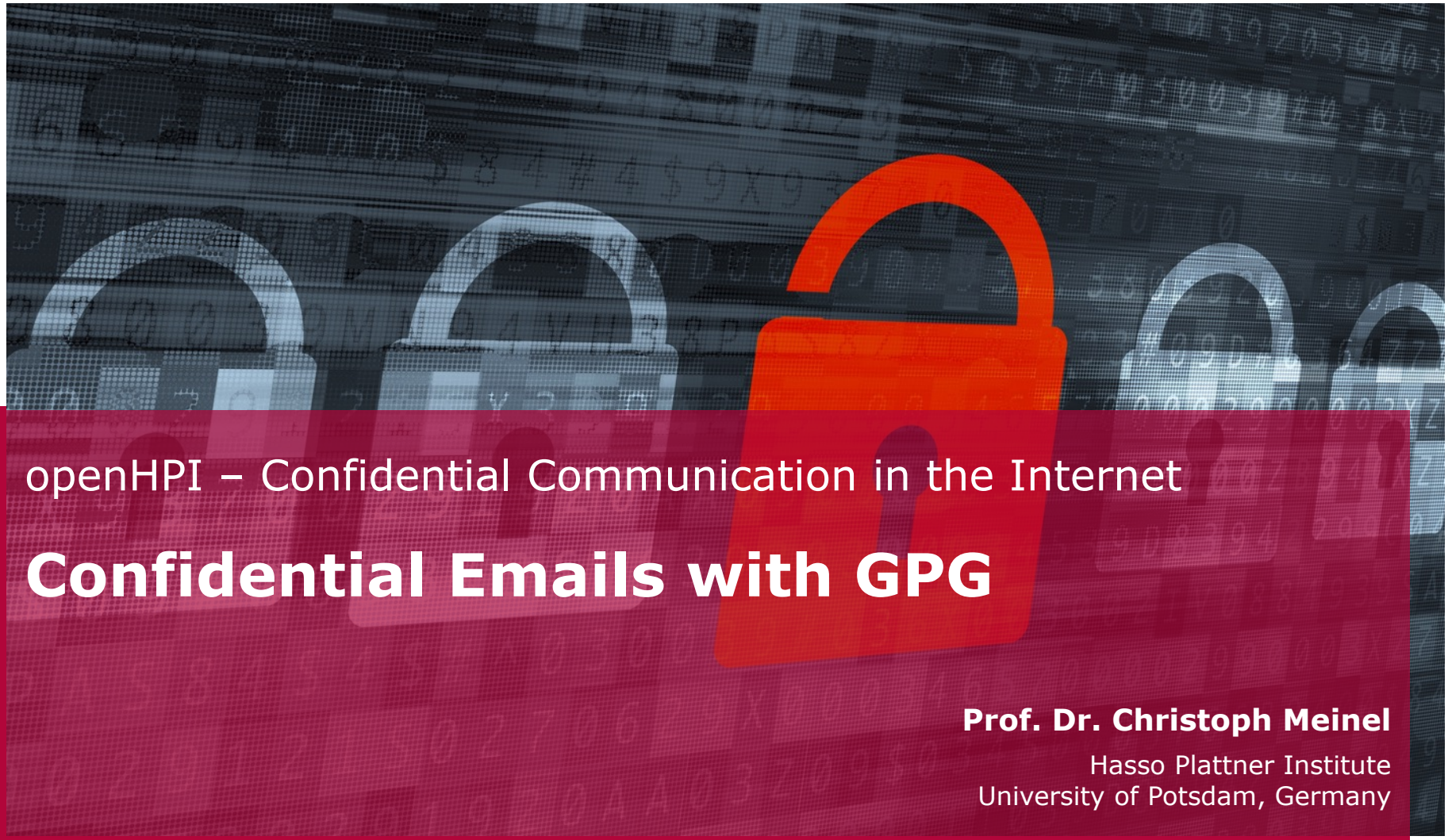

openHPI – Confidential Communication in the Internet

Confidential Emails with GPG

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Confidential Email Communication: **GPG – GNU Privacy Guard**

Confidential email communication:

- Apply encryption and digital signatures
- Works only when both communication partners are engaged

Popular tool: GNU Privacy Guard

- Provides functionality for
  - Encryption and digital signing

GPG is a freely available software

- Freely available variant of the commercial **PGP** (**Pretty Good Privacy**)
- Relies only on freely available (i.e. patent-free) technologies and crypto algorithms
- Implements the **OpenPGP standard** and is therefore PGP-compatible

Confidential Email Communication: **Functionality of GPG**

GPG offers support in the execution of almost all tasks related to encryptions and digital signatures, including

- **Key generation** – creation of a key pair of private and public keys
- **Key provisioning** – storing public keys on the user's system and making them available for various applications, e.g. for email
- **Key distribution** – provision and distribution of public keys via a "key server"
- **Encryption of** files and emails
- **Signature** – creation of digital signatures, e.g. for emails
- **Verification of signatures** - verification of signed data

Confidential Email Communication: **Use of GPG**

GPG is available for **Linux**, **Windows** and **Mac OS X**

... but is not so easy to operate in its basic version

GPG complete packages with graphic interfaces

- Various projects compile installation packages with programs that make the use of GPG much easier
- Installation packages consist of: GNU Privacy Guard, installation program, certificate manager and plugins for email programs and file manager
  - Windows: **GPG4win** (https://www.gpg4win.de)
  - Mac OS X: **GPG Suite** (https://gpgtools.org)
  - Cross platform for Mozilla Thunderbird (plugin): **enigmail** (https://www.enigmail.net)

Confidential Email Communication: **GPG in Practice**

Announcement: openHPI workshop on" Secure Email"

- „Sicher per Email kommunizieren – Mitleser unerwünscht" (German)
- 2-week practical workshop
- **Course contents**:
  - Introduction to GPG and S/MIME
  - Installation of GPG packages
  - Key generation and exchange
  - Encryption & decryption of e-mails
  - Use of digital signatures

- Course has run in 2019, but remains open for self-paced study https://open.hpi.de/courses/email2019