PGP Schlüsselverteilung

Inhalt

- VVV
- Warum
- Verfahren
  - OPENPGPDANE
  - WKS
  - Sonstige
  - HKP
  - priv HKP
  - Fragen & Ideen

Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

PGP- und S/MIME-Schlüssel

Projektpartner

- Mailbox.org (Berlin)
- Frauenhofer SIT (Darmstadt)
- Kassel

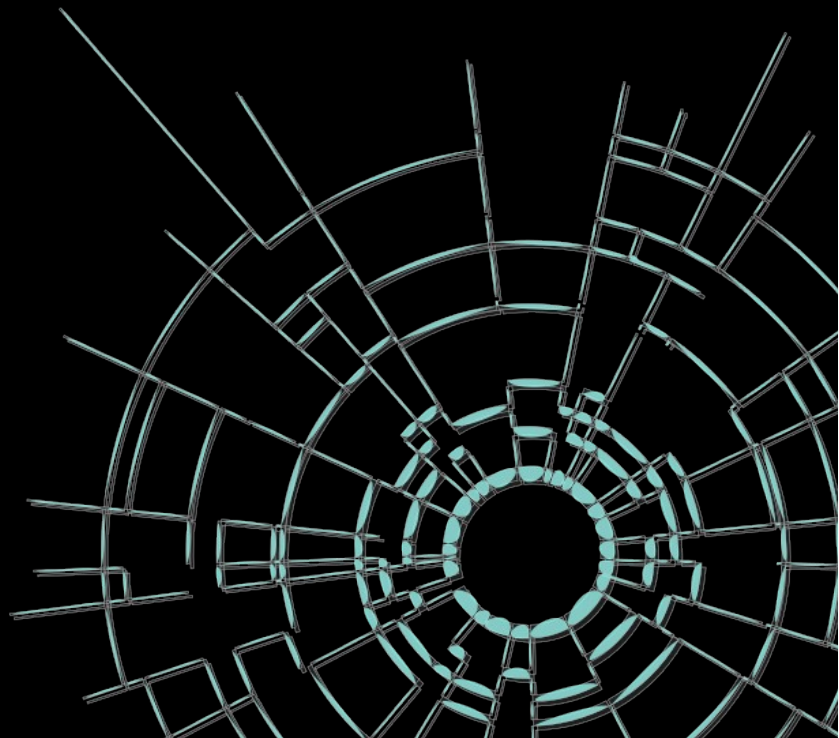
  Projektgruppe verfassungsverträgliche

  Technikgestaltung (Darmstadt)
- Design Research Lab

  Universität der Künste Berlin
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Warum ?

- PGP heute
  - schwer vermittelbar
  - aufwendig nutzbar
- morgen
  - Key mittels Mailadresse ermitteln
- pefi@lavabit.com



Verfahren: OPENPGPDANE

- DNSSEC signierte DNS-RR
- Keine Verschlüsselung
- UDP (EDNS) → FW o. Reflektionsangriffe
- https://tools.ietf.org/id/draft-ietf-dane-openpgpkey-12.txt

Software	DNSSEC	EDNS	OPENPGPKEY	Dyn. Zone	OS
Bind9	OK	OK	OK	OK	ISC license
PowerDNS	OK	OK	~~Nein~~ **OK**	OK	GPL v2
Unbound	OK	OK	Nein	Nein	BSD license

gpg –auto-key-locate dane --search-keys pefi@noname.lan

dig @ns.noname.lan type61 \
e1d5a43ceecf6feefad2b5acd13ced4c50921ece2f6eff3580b757ac._openpgpkey.noname.lan

Verfahren: WKS

- 32 octets of case(in)sensitive Z-Base-32-localpart
- Upload über SMTP
- KeyFormat (amored ASCII vs binary)
- kein DNSSEC/DANE oder Certpinning
- Spam, Postfach voll
- Policy mit Schlüsselgrößen

gpg --auto-key-locate wkd –locate-keys Joe.Doe@noname.lan

https://noname.lan/.well-known/openpgpkey/hu/iy9q119eutrkn8s1mk4r39qejnbu3n5q

https://noname.lan/.well-known/openpgpkey/submission-address

https://tools.ietf.org/html/draft-koch-openpgp-webkey-service-02

Verfahren: Sonstige

- pretty Easy privacy

  https://prettyeasyprivacy.com/

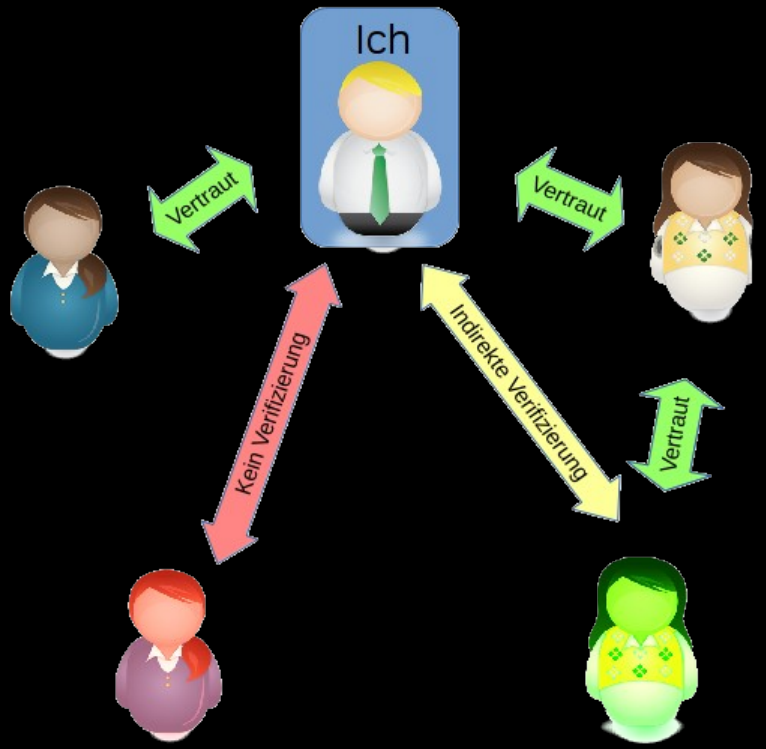
- Public Key Association

  http://www.g10code.de/docs/pka-intro.de.pdf

- Certificate Transparency

  https://www.certificate-transparency.org

Verfahren: HKP



- HTTP Keyserver Protocol
- WOT, KeyID, Fingerprint
- SKS (DB + Ptree ca. 13GB)
- HKP nur Draft (2003)
- Privatsphäre
- OnionBalance hkp://jirk5u4osbsr34t5.onion

gpg --keyserver pgp.mailbox.org --search-keys pefi@noname.lan

pgp.mailbox.org/pks/lookup?op=index&options=mr&search=pefi@noname.lan
pgp.mailbox.org/pks/lookup?op=get&options=mr&search=0x778....102

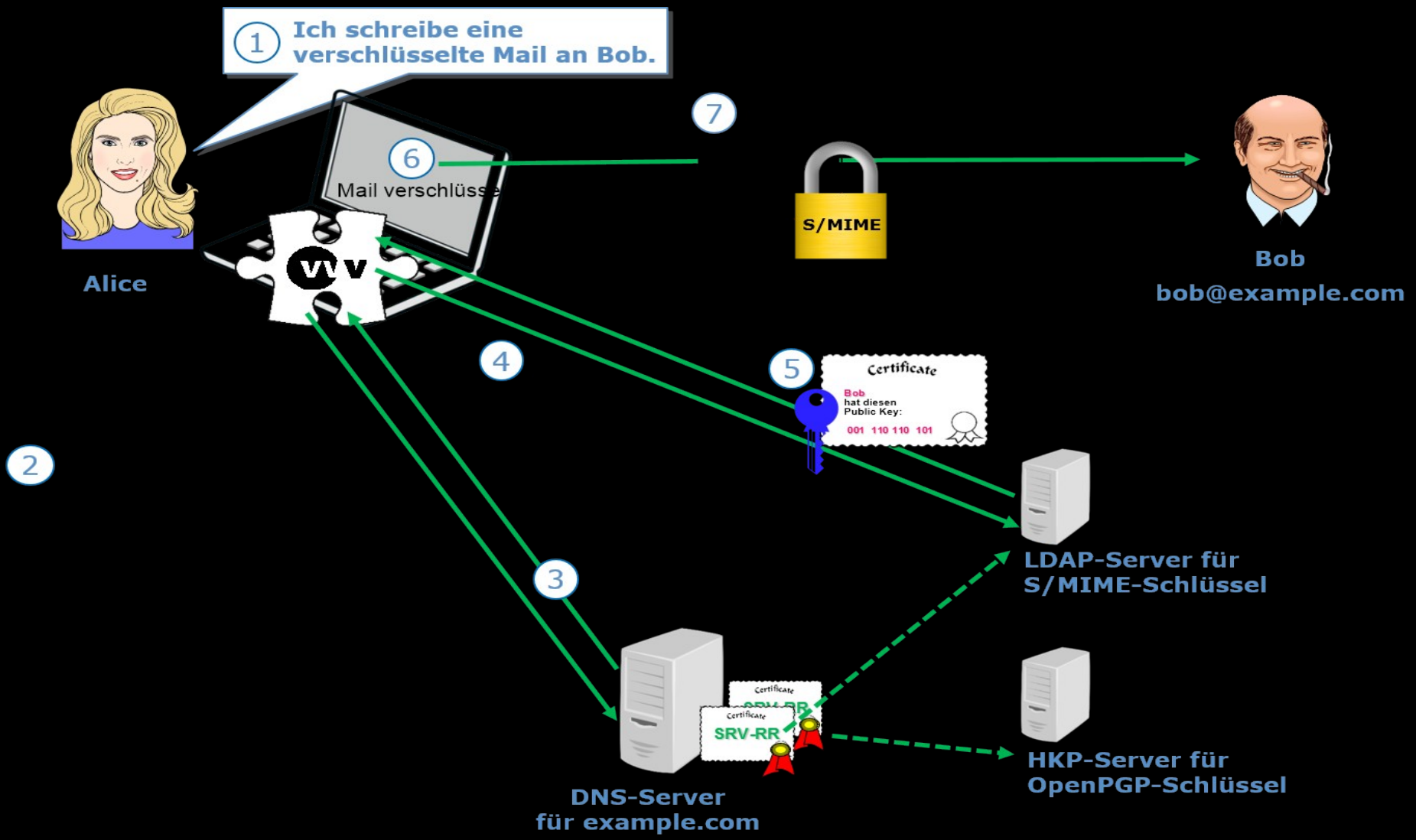
Verfahren: priv. HKP

- Erw. mit DNSSEC/DANE sowie TLS (HKPS)
- DNS-SRV-RR: Schlüsselserver/port

```
_pgpkey-https._tcp.maildomain.net  3600  IN  SRV  0  0  443  hkp.maildomain.net
```

- Providerverantwortung

Verfahren: priv. HKP



Fragen & Ideen:

- Schlüssel bereinigen, zurückrufen, cashen
- Verschiedene Verfahren
- DNSSEC (Keyrollover, Verifikation)

- WKS to HKP Proxy

Danke für die Aufmerksamkeit auf eine angeregte Diskusion

pefi@mailbox.org
33A8 D5A4 E368 1F75 40F0
AD07 ECF3 2C72 A892 1011