# SMILLA - automatic S/MIME encryption

sys4.de

# What is the problem?

# Email security is hard

PGP

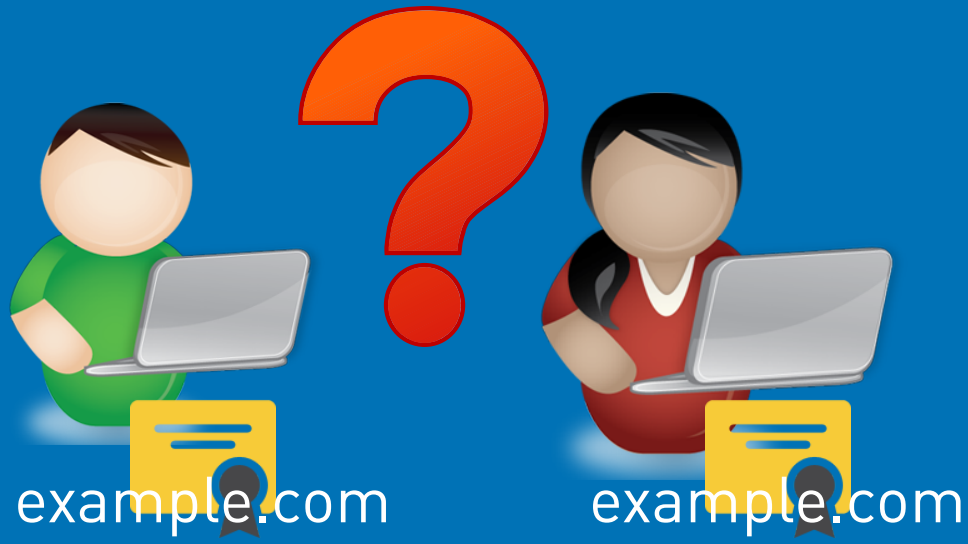
- Key generation
- Key publication (key-server)
- Key rollover/updates
- Key revocation

S/MIME

- Generating/Requesting a certificate
- Trust in Certification Authorities
- Distribution of certificate(s)
- No policy channel
- Revocation is complicated

# BrOken CA Model

- **Any CA** may issue certificates for **any domain**
- **CAs have been compromised** in the past
- CAs have issued wrong or **unauthorized certificates**



# DANE to the rescue

- DANE - DNS-based Authentication of Named Entities
- Allows the use of **self-signed certificates** (certificates without in-certificate trust-chain)
  - The trust chain used in the DNSSEC trust chain
- DANE enables **opportunistic** encryption
- Encryption **without** manual intervention

# SMIME with DANE

# SMIMEA Resource Record

- Authenticates email certificates (x509 ) for S/MIME
- Store hash or certificate in DNSSEC secured domain
- Hashed email localpart
- Allows for self-signed certificates
- Removing the RR revokes a certificate

# SMILLA

- Uses MILTER (Mail Filter) API for Postfix and Sendmail
- Aimed at mail provider and organizations that operate their own email infrastructure
- Looks for x509 certs in SMIMEA records
- Once a record is found, un-encrypted mail will be encrypted
  - SMIMEA record must be DNSSEC secured
  - Mail must not already be encrypted (via S/MIME or PGP)
  - Transparent for the user – “it just happened”

# SMILLA Use Cases

- Encrypt Outbound Mail
  - Mail is encrypted before sent out to the Internet
  - Secures the transport all the way to the recipient
- Encrypt Inbound Mail
  - Mail is encrypted on reception
  - Secures email on storage (for example on a “cloud” server)

# DANE S/MIME

Alice

Mail-
Server Alice

DNS(SEC)
resolver

bob@example.com

Mail-
Server Bob

(1) Bob published
SMIMEA record
in DNS

authoritative
DNS for
example.com

# DANE S/MIME

Alice

(2) Alice sends
an email to Bob
They have never
exchanged certificates
or keys

Mail-
Server Alice

bob@example.com

Mail-
Server Bob

DNS(SEC)
resolver

authoritative
DNS for
example.com

# DANE S/MIME

Alice

bob@example.com

Mail-
Server Alice

Mail-
Server Bob

(3) Mail server sees that the mail is un-encrypted, asks smilla to look for an S/MIME certificate in DNS

DNS(SEC)
resolver

authoritative
DNS for
example.com

# DANE S/MIME

Alice

bob@example.com

Mail-
Server Bob

Mail-
Server Alice

(4) smilla requests the SMIMEA Record for Bob's mail address

DNS(SEC)
resolver

authoritative
DNS for
example.com

# DANE S/MIME

Alice

bob@example.com

Mail-
Server Bob

Mail-
Server Alice

(5) DNSSEC signed response
Is validated inside the
DNS resolver

DNS(SEC)
resolver



authoritative
DNS for
example.com

# DANE S/MIME

Alice

(6) smilla encrypts the mail using the x509 S/MIME certificate from DNS

Mail-
Server Alice

Mail-
Server Bob

bob@example.com

DNS(SEC)
resolver

authoritative
DNS for
example.com

# DANE S/MIME

Alice

Mail-
Server Alice

DNS(SEC)
resolver

(7) Bob decrypts the mail using his private key

bob@example.com

Mail-
Server Bob

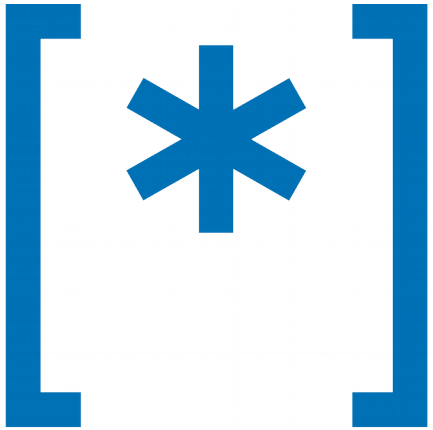
authoritative
DNS for
example.com

# Future work: autoencrypt-milter

- Merge with Paul Wouters “openpgpkey-milter”
- SMIMEA and OPENPGPKEY aware MILTER
- Transparent for users
- In- and outbound encryption
- To be released as Open Source as soon as RFCs become standard at https://github.com/sys4/

# Takeaway

- Mail users care about security – but they fear wrangling with encryption
- DANE lowers the barrier for email encryption
- Opportunistic “end-to-end” encryption
- SMILLA is open source – installation is easy – one-time-cost



We do ASCII

sys4.de

https://sys4.de/download/smilla-en.pdf