cryptoVision
an atos company

PGP und S/MIME gemeinsam verarbeiten: Ein Praxisbericht

Dr. Matthias Edelhoff,
cryptovision

© Atos

Atos

Agenda

01. S/MIME und PGP

02. Das Projekt

03. Fazit und Ausblick

Atos

01. S/MIME und PGP

E-Mail-Sicherheit

Seit den Neunziger-Jahren in Verwendung

Nur etwa jede tausendste E-Mail ist verschlüsselt oder signiert

Nur 12,6 Prozent der beruflichen Nutzer verschlüsseln ihre Mails „oft“

Nur sehr wenige private Nutzer verschlüsseln/ signieren ihre Mails

E-Mail-Sicherheit ist seit 90ern keine Erfolgs-geschichte

Atos

Benutzerfreundlichkeit als Herausforderung

Leichte Beeinträchtigungen unumgänglich

Nutzer muss mit Schlüsseln, Zertifikaten usw. umgehen können

Geeignete Infrastruktur oft nicht vorhanden (z. B. Schlüssel auch auf Smartphone verfügbar)

Zwei inkompatible Standards (und viele proprietäre Formate): S/MIME und PGP

Nutzern ist kaum zu vermitteln, dass es zwei Standards gibt

Entstehungsgeschichte von S/MIME und PGP

S/MIME

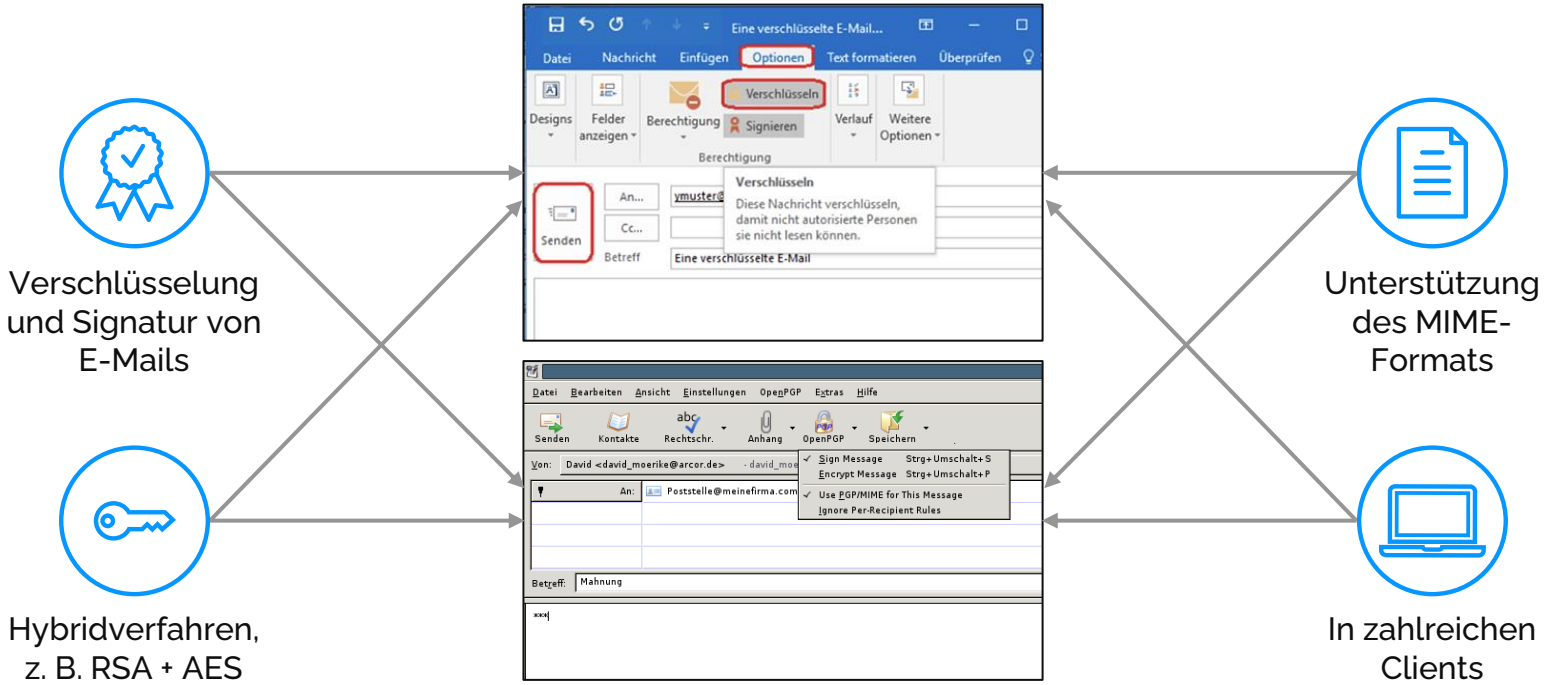
Entwicklung der Firma RSA
Ursprüngliches Ziel: Schutz von E-Mails in Industrie
Nutzung von Zertifikaten als Idealfall
Vertrauen in Zentralinstanz notwendig

PGP

Entwicklung von Phil Zimmermann
Ursprüngliches Ziel: Schutz des Einzelnen vor dem Staat
Misstraute zentralen Instanzen
Verstieß gegen US-Exportgesetze
Verwendete viele proprietäre Formate
Missachtete RSA-Patent

Atos

Gemeinsamkeiten zwischen S/MIME und PGP



Aufbau einer Nachricht

S/MIME

```
Content-Type: application/pkcs7-mime; name=smime.p7m;
      smime-type=enveloped-data
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

MIIBHgYJKoZIhvcNAQcDoIIBDzCCAQsCAQAxgcAwgb0CAQAwJjASMRAwDgYDVQQDEw
dDYXJsUlNBAhBGNGvHgABWvBHTbi7NXXHQMA0GCSqGSIb3DQEBAQUABIGAC3EN5nGI
iJi2lsGPcP2iJ97a4e8kbKQz36zg6Z2i0yx6zYC4mZ7mX7FBs3IWg+f6KgCLx3M1eC
bWx8+MDFbbpXadCDgO8/nUkUNYeNxJtuzubGgzoyEd8Ch4H/dd9gdzTd+taTEgS0ip
dSJuNnkVY4/M652jKKHRLFf02hosdR8wQwYJKoZIhvcNAQcBMBQGCCqGSIb3DQMHBA
gtaMXpRwZRNYAgDsiSf8Z9P43LrY4OxUk660cu1lXeCSFOSOpOJ7FuVyU=
```

PGP

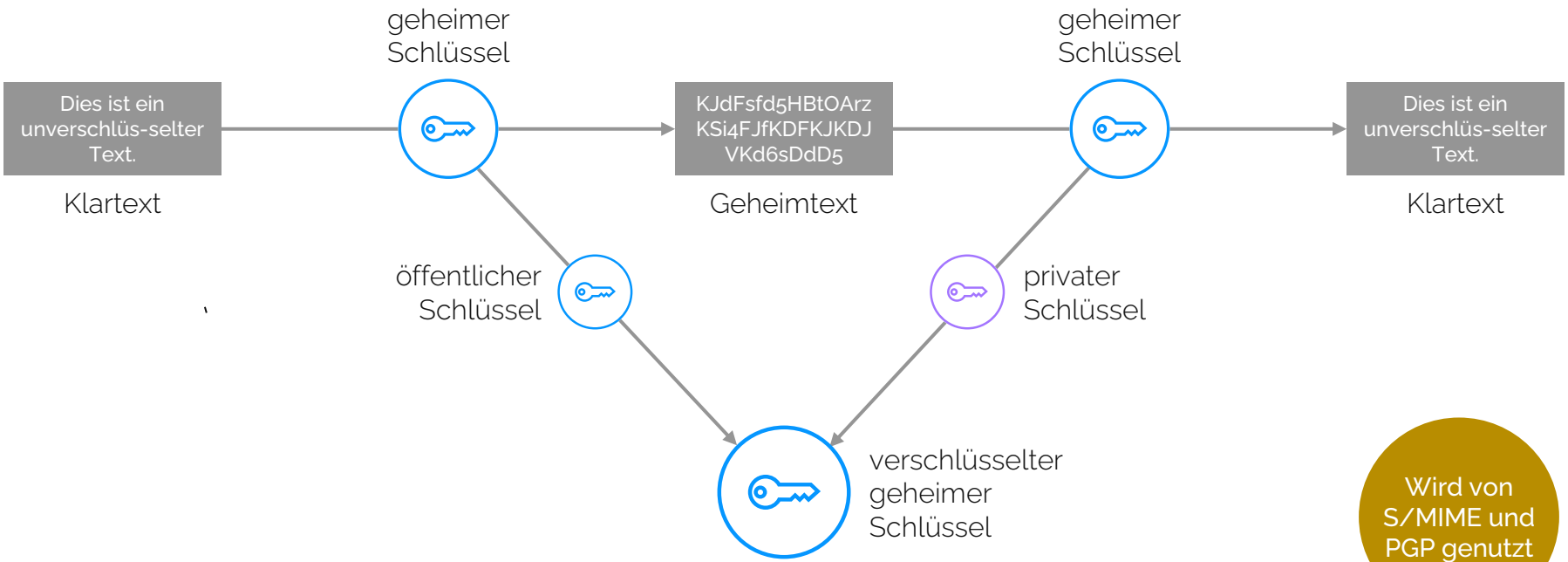
```
Content-Type: multipart/encrypted; boundary=foo;
         protocol="application/pgp-encrypted"

--foo
Content-Type: application/pgp-encrypted

Version: 1

--foo
Content-Type: application/octet-stream

 -----BEGIN PGP MESSAGE-----
Version: 2.6.2

hIwDY32hYGCE8MkBA/wOu7d45aUxF4Q0RKJprD3v5Z9K1YcRJ2fve87lMlDlx4Oj
eW4GDdBfLbJE7VUpp13N19GL8e/AqbyyjHH4aS0YoTk10QQ9nnRvjY8nZL3MPXSZ
g9VGQxFeGqzykzmykU6A26MSMexR4ApeeON6xzZWfo+0yOqAq6lb46wsvldZ96YA
AABH78hyX7YX4uT1tNCWEIIBoqqvCeIMpp7UQ2IzBrXg6GtukS8NxbukLeamqVW3
1yt21DYOjuLzcMNe/JNsD9vDVCvOOG3OCi8=
=zzaA
-----END PGP MESSAGE-----
```

Ähnlicher Aufbau, aber nicht kompatibel

Atos

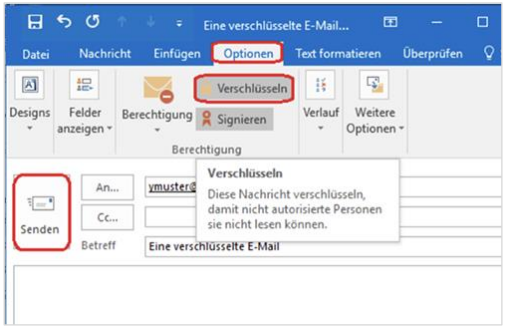
Gleiche Kryptoverfahren

Beispiel: Hybrid-Verfahren



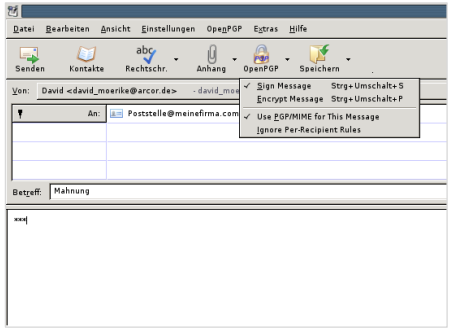
Wird von S/MIME und PGP genutzt

Unterschiede zwischen S/MIME und PGP



S/MIME

- Hierarchisches Vertrauensmodell (Chain of Trust)
- Nutzt mehrere andere Krypto-Standards
- X.509-Zertifikate
- LDAP-Server
- Sperrlisten, OCSP-Sperrprüfung



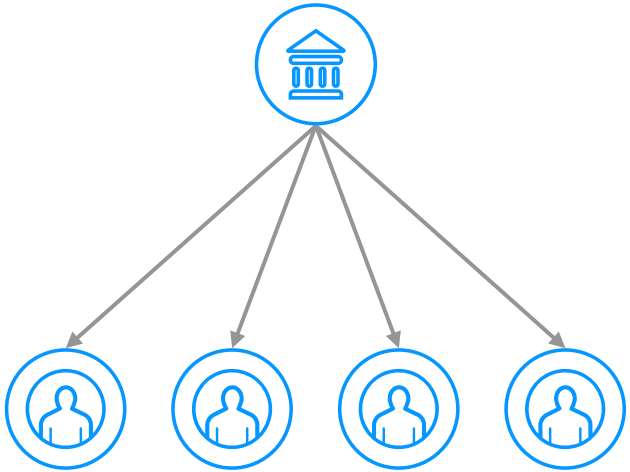
PGP

- Netzartiges Vertrauensmodell (Web of Trust)
- Nutzt hauptsächlich PGP-spezifische Formate
- PGP-Zertifikate
- Schlüssel-Server (wegen Sicherheitslücken in Verruf geraten)
- Keine zentrale Sperrprüfung

Die Vertrauensmodelle von S/MIME und PGP

Chain of Trust (S/MIME)

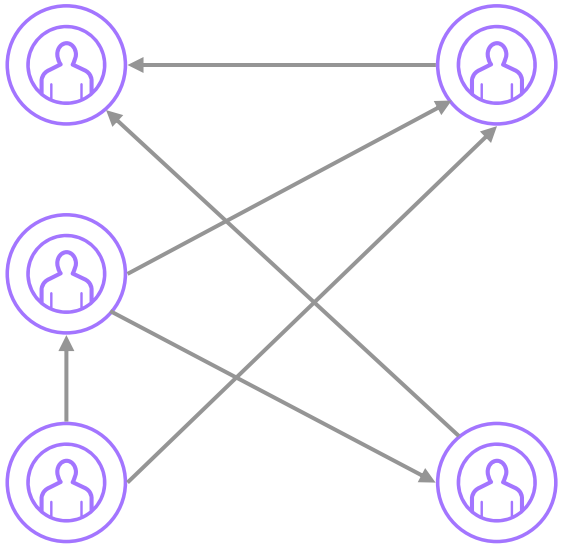
Zertifizierungsstelle



Anwender

Beide Formate unterstützen auch den Schlüsselaustausch ohne Zertifizierung (Direct Trust)

Web of Trust (PGP)



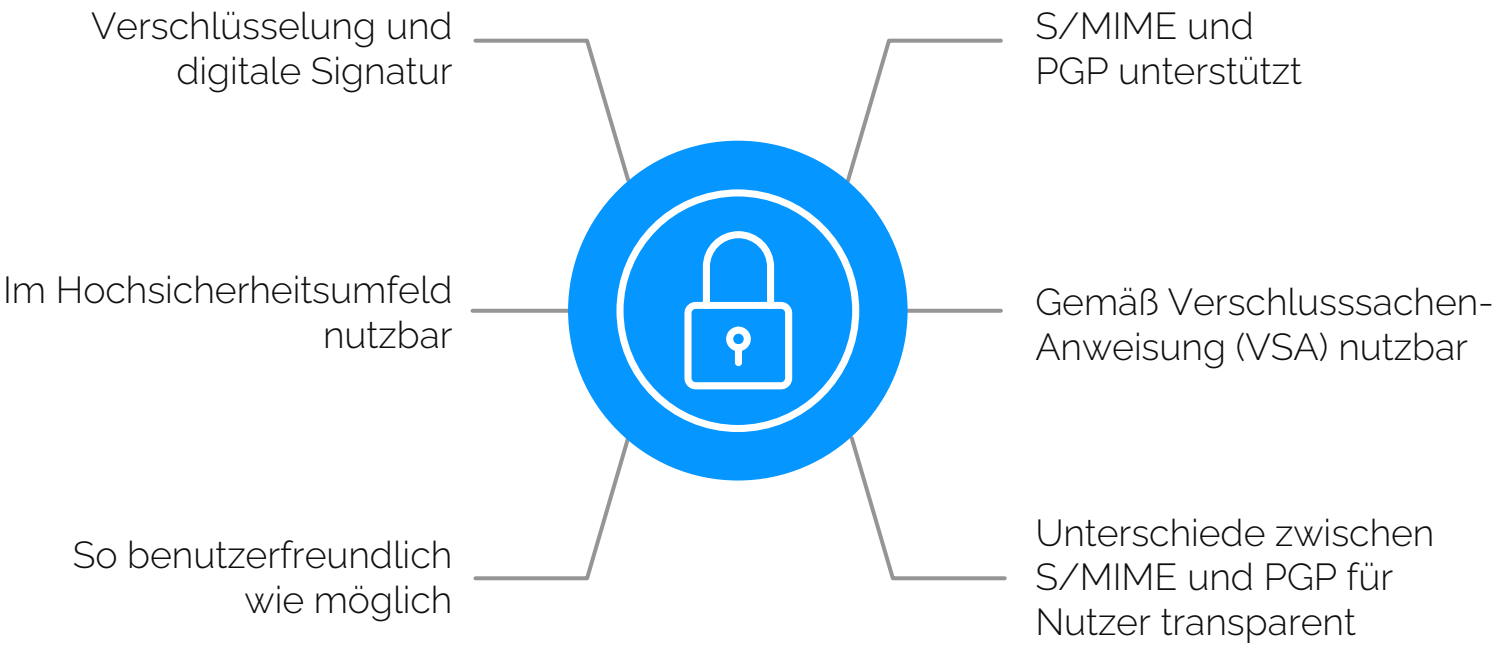
Anwender

Atos

02. Das Projekt

Das Projekt

Entwicklung eines E-Mail-Security-Clients für Outlook und Notes



Usability bei S/MIME- und PGP-Unterstützung

Überblick

Einheitliche Benutzeroberfläche für beide Formate

Automatisierte Formatwahl

Gemeinsamer Schlüsselspeicher (Datei oder Smartcard) für beide Formate

Einheitliche Prozesse (Enrollment, Schlüsselwechsel, …) für beide Formate

Atos

Wie das Format ausgewählt wird

Es wird nicht dem Nutzer überlassen

Alle Informationen für Entscheidung nutzen:

- vorhandene öffentliche Schlüssel der Empfänger
- Gültigkeit der Zertifikate
- Präferenzen der Empfänger
- unterstützten Algorithmen
- konfigurierbare Präferenzen
- Passwort-verschlüsselung als Fall-back

Nur in Ausnahmefällen wird Anwender gefragt

insbesondere bei mehreren Empfängern und seltener Kommunikation

Usability bei S/MIME- und PGP-Unterstützung

Details

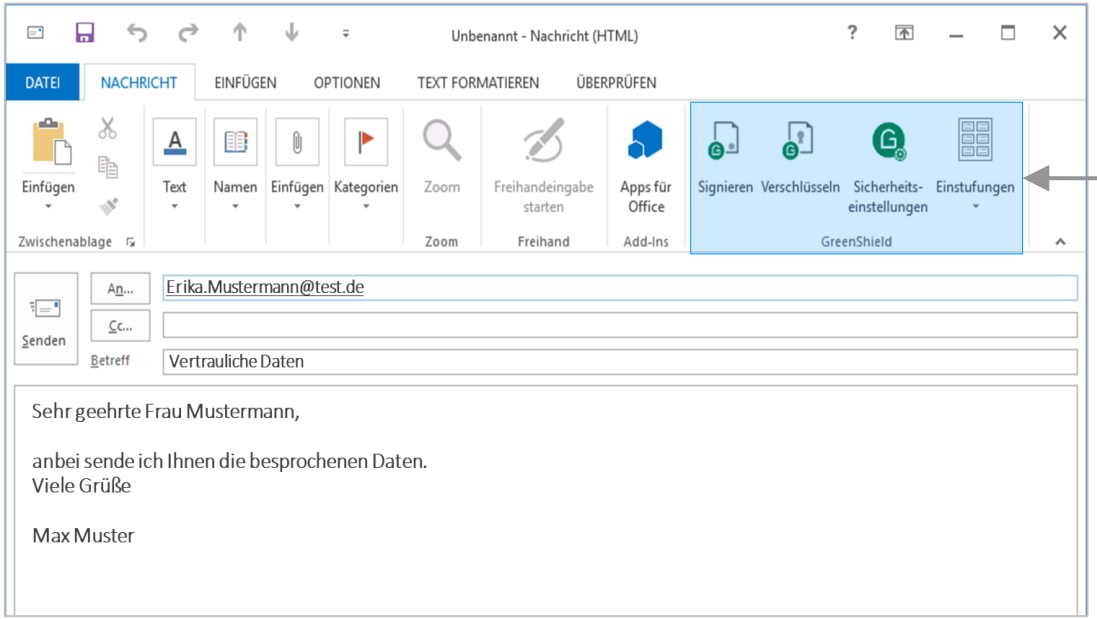
Vergleichbare Warn-, Fehler-, und Erfolgsmeldungen

Direkter Schlüsselausta usch einheitlich

Schlüssel-Sperrung in jeweils üblicher Form

Sperrlisten und OCSP für X.509-Zertifikate

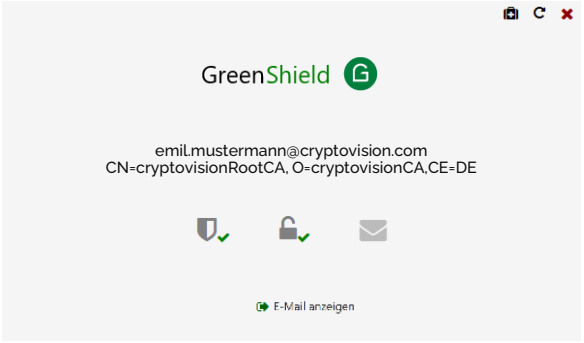
Das Resultat: GreenShield Mail



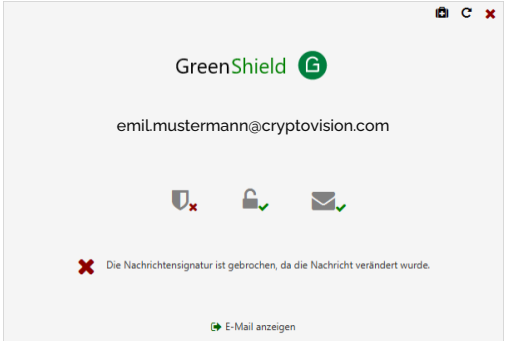
GreenShield Mail
Benutzerfreundliche
E-Mail-Verschlüsselung
mit S/MIME und PGP

Verifizierung von Signaturen

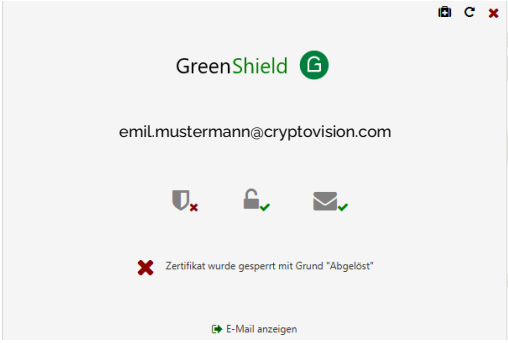
Korrekt

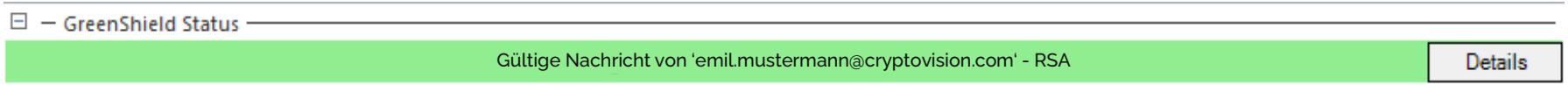


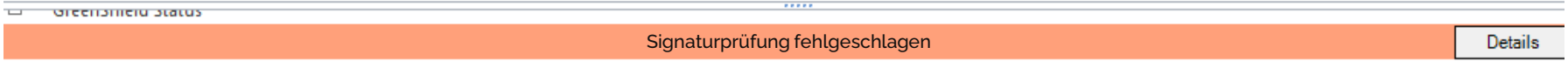
E-Mail wurde verändert



Zertifikat wurde abgelöst



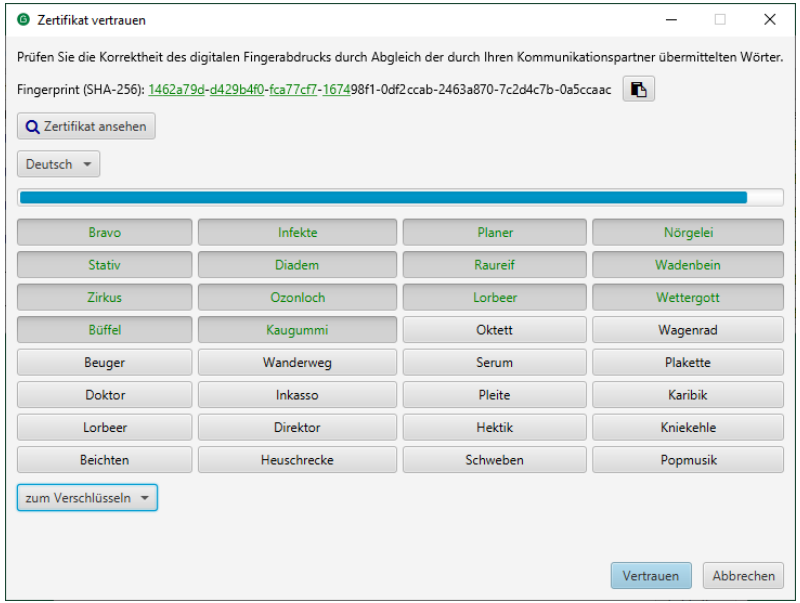




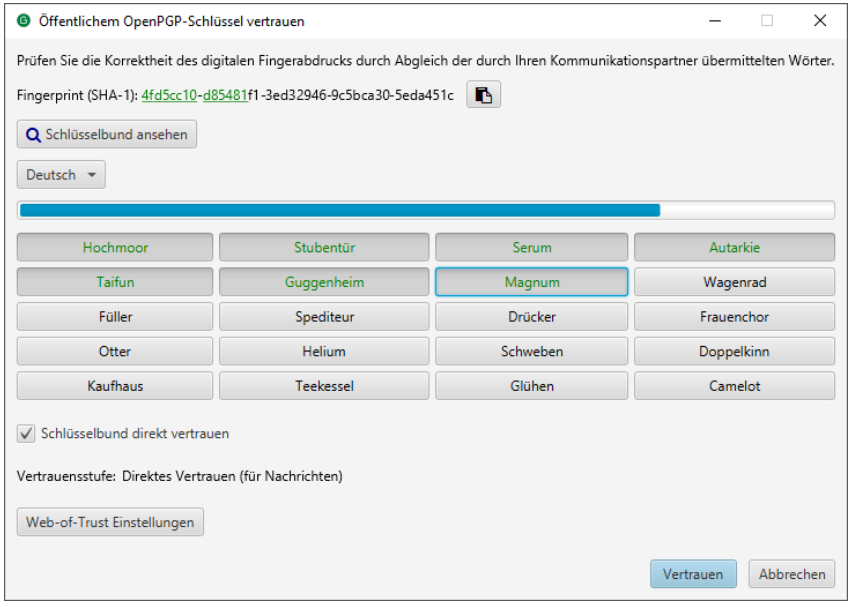
Direct Trust

Verifizierung der öffentlichen Schlüssel über benutzerfreundlich dargestellte Hashwerte:

S/MIME

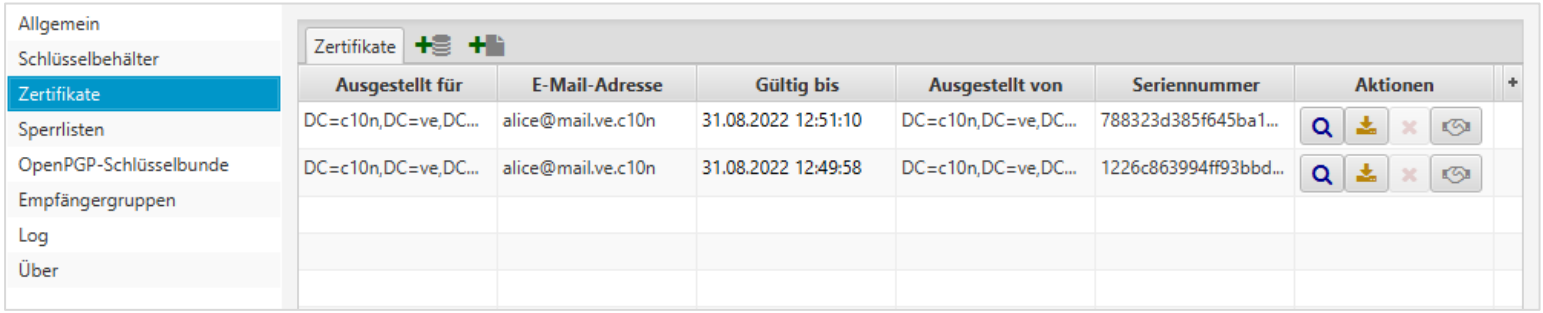


PGP

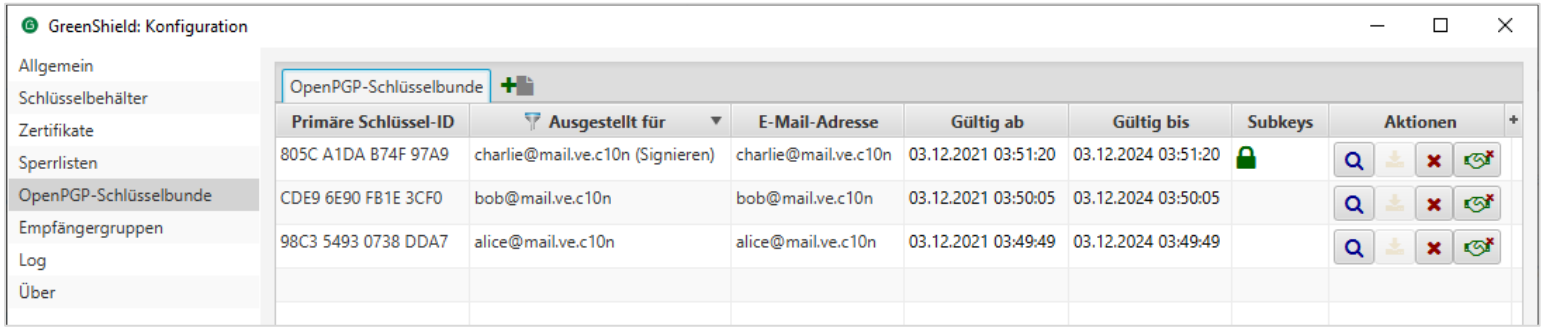


Schlüsselauswahl

S/MIME



PGP



Usability bei S/MIME- und PGP-Unterstützung

Details

Beide Vertrauensmodelle umsetzbar

Schlüssel-Import und -Nutzung (privat und öffentlich) für beide Formate

Unterstützung desselben Schlüssels für beide Formate

Einheitliche Krypto-Algorithmen, falls möglich

Synthetisierung von Zertifikaten

Aus S/MIME-Zertifikat wird PGP-Zertifikat, und umgekehrt

Ablauf einer PGP-Synthetisierung

Voraussetzung: Anwender hat Zugriff auf privaten X.509-Schlüssel

Client will Empfänger PGP-Schlüssel schicken, hat jedoch keinen

Client extrahiert öffentlichen Schlüssel aus X.509-Zertifikat

Client signiert öffentlichen Schlüssel im PGP-Format

Client schickt signierten PGP-Schlüssel an Empfänger

Fehlende Smartcard-Unterstützung von PGP wird umgangen

Auch X.509-Synthetisierung ist möglich, aber seltener

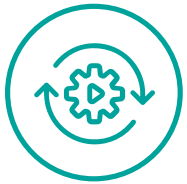
Atos

Was nicht umgesetzt werden konnte

Direkte Smartcard-Unterstützung von PGP ist unzureichend

Krypto-Algorithmen von PGP sind veraltet*

PGP-Server wird nicht unterstützt wegen aufgetretener DoS-Angriffe**



Aktuelle Sperrprüfung mit PGP de facto nicht möglich

* Standard wird derzeit aktualisiert
** Neuentwicklung ist im Gange

Atos

03. Fazit

Fazit

S/MIME und PGP in einer Software

Unterstützung beider Formate erhöht Benutzerfreundlichkeit

Benutzeroberfläche muss Unterschiede verbergen

Automatische Formatwahl notwendig

Komplexität steigt durch zwei Formate deutlich

Prozesse müssen beide Formate bedienen

Smartcard-Unterstützung, Server-Nutzung und Sperrprüfung bei PGP schwer umsetzbar

Benutzer-freundliche Unterstützung von S/MIME und PGP ist möglich

Atos

cryptoVision
an atos company

Danke für Ihre Aufmerksamkeit

www.cryptovision.com

cv cryptovision GmbH |
Munscheidstr. 14 | 45886 Gelsenkirchen

Atos is a registered trademark of Atos SE. November 2021. © Copyright 2021, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.

© Atos

Atos