

# PGP und S/MIME gemeinsam verarbeiten: Ein Praxisbericht

Dr. Matthias Edelhoff,  
cryptovision



# Agenda

01. S/MIME und PGP

02. Das Projekt

03. Fazit und Ausblick

## 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 goern keine Erfolgsgeschichte

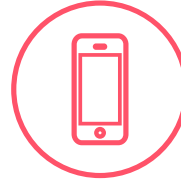
# Benutzerfreundlichkeit als Herausforderung



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

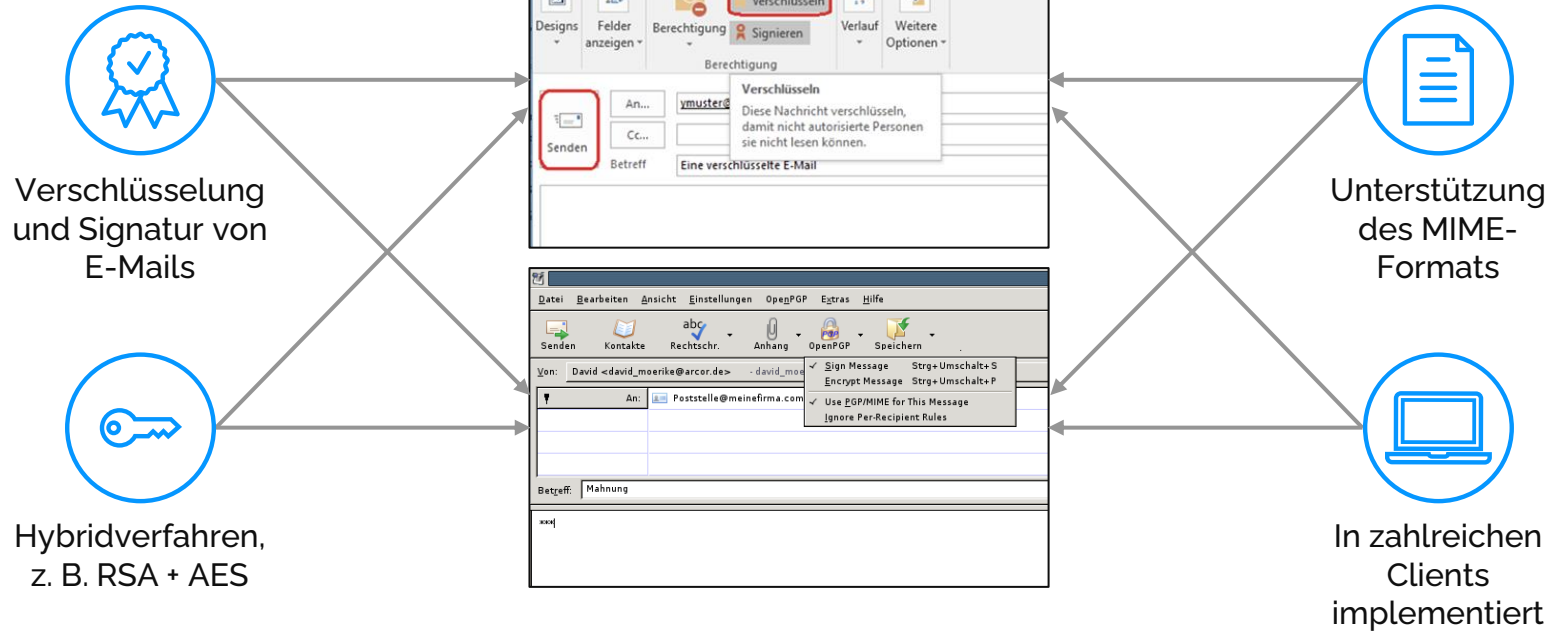
Misstraute zentralen Instanzen

Verstieß gegen US-Exportgesetze

Verwendete viele proprietäre Formate

Missachtete RSA-Patent

# 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
```

```
MIIBHgYJKoZIhvcNAQcDoIIBDzCCAQsCAQAxcAwgb0CAQAwJjASMRawDgYDVQQDEW  
dDYXJsU1NBahBGNGvHgABWvBHThi7NXXHQMA0GCSqGSIb3DQEBAQUABIGAC3EN5nGI  
iJi2lsGPcP2iJ97a4e8kbKQz36zg6Z2i0yx6zYC4mZ7mX7FBs3IWg+f6KgCLx3M1eC  
bWx8+MDFbbpXadCDgO8/nUkUNYENxJtuzubGgzoyEd8Ch4H/dd9gdzTd+taTEgS0ip  
dSJUNnkVY4/M652jKKHRLfF02hosdR8wQwYJKoZIhvcNAQcBMBQGCGCCqGSIb3DQMHBA  
gtaMXpRwZRNyAgDsIsf8Z9P43LrY40xUk660cu1lXeCSFOSOpOJ7FuVyU=
```

## 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
```

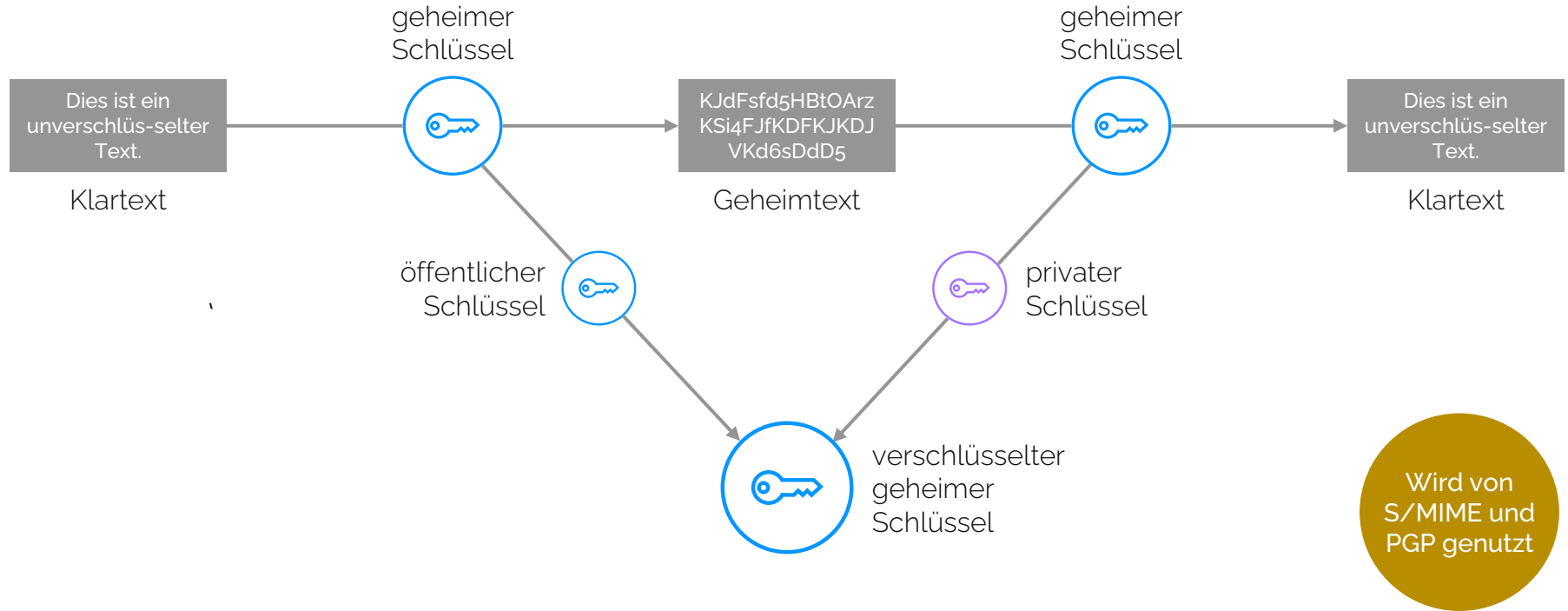
```
hIwDY32hYGCE8MkBA/wOu7d45aUxF4Q0RKJprD3v5Z9K1YcRJ2fve87lM1Dlx4Oj  
eW4GDdBfLbJE7VUpp13N19GL8e/AqbyyJHH4aS0YoTk10QQ9nnRvjY8nZL3MPXSZ  
g9VGQxFeGqzykzmykU6A26MSMexR4ApeeON6xzZWfo+0yOqAq6lb46wsvldZ96YA  
AABH78hyX7YX4uT1tNCWEIIBoqqvCeIMpp7UQ2IzBrXg6GtuskS8NxbukLeamqVW3  
1yt21DY0juLzcMNe/JNsD9vDVCvOOG3OCi8=  
=zzaA  
-----END PGP MESSAGE-----
```

Ähnlicher  
Aufbau,  
aber nicht  
kompatibel

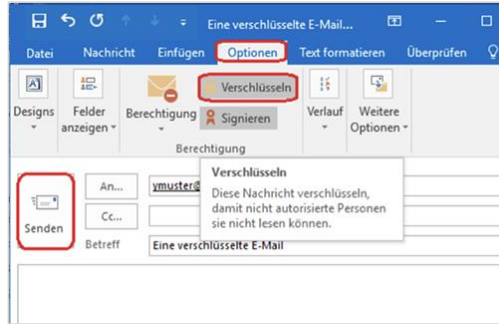


# Gleiche Kryptoverfahren

## Beispiel: Hybrid-Verfahren

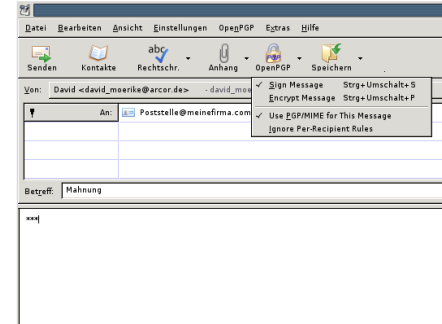


# Unterschiede zwischen S/MIME und PGP



## S/MIME

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



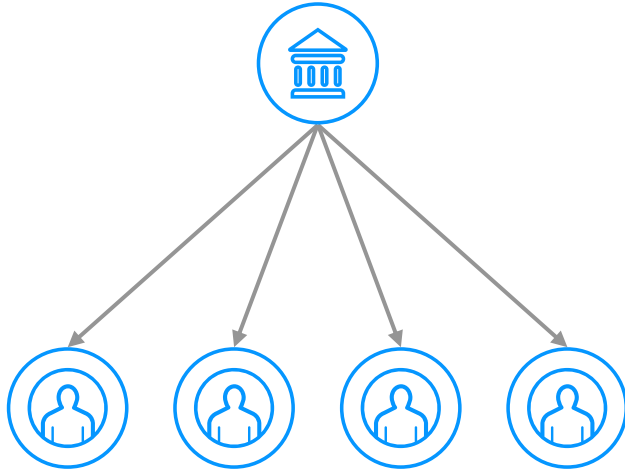
## PGP

- 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)

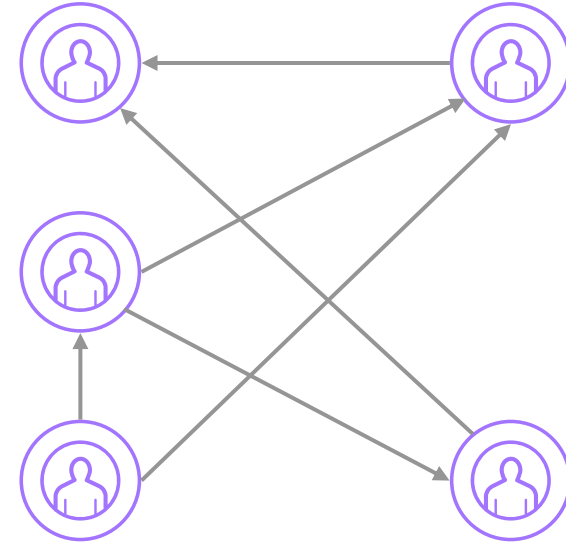
Zertifizierungsstelle



Anwender

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

## Web of Trust (PGP)



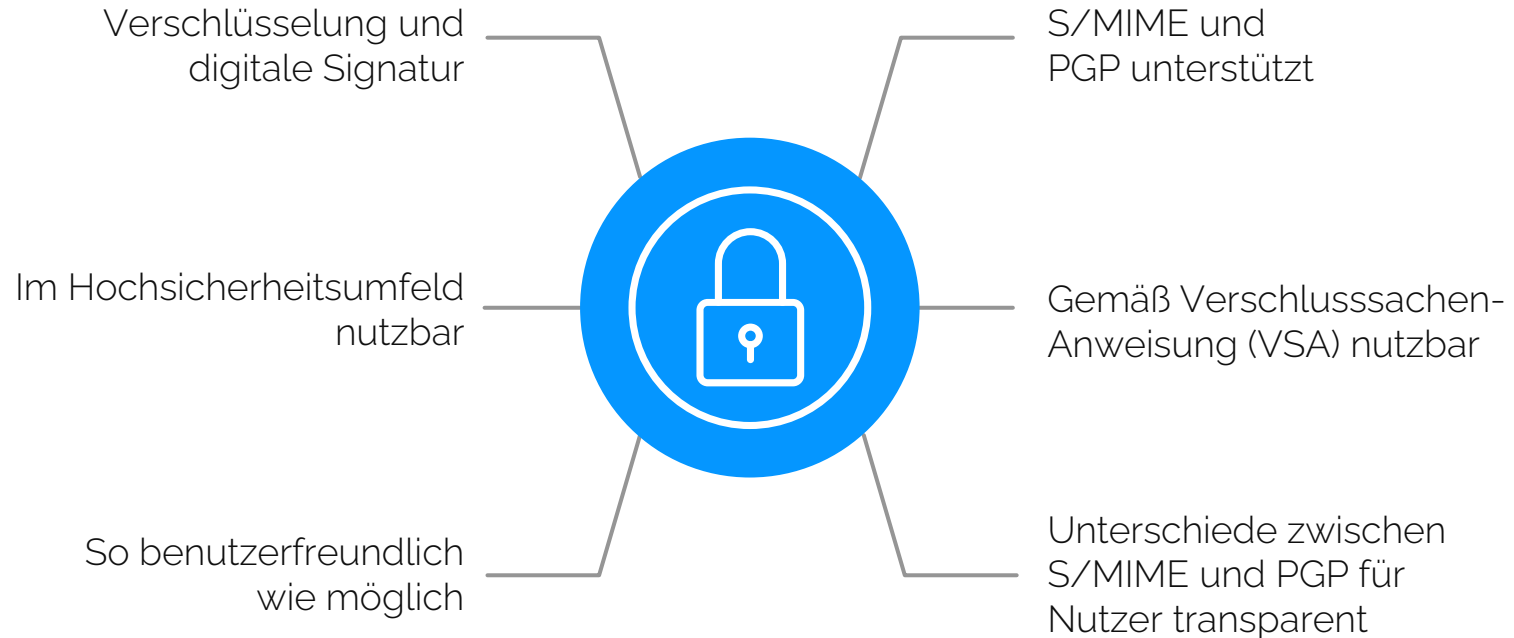
Anwender

## 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

# 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

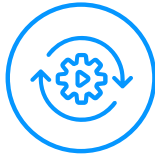
**Nur in Ausnahmefällen wird Anwender gefragt**  
insbesondere bei mehreren Empfängern und  
seltener Kommunikation

# Usability bei S/MIME- und PGP-Unterstützung

## Details



Vergleichbare  
Warn-, Fehler-, und  
Erfolgsmeldungen



Schlüssel-Sperrung in  
jeweils üblicher Form



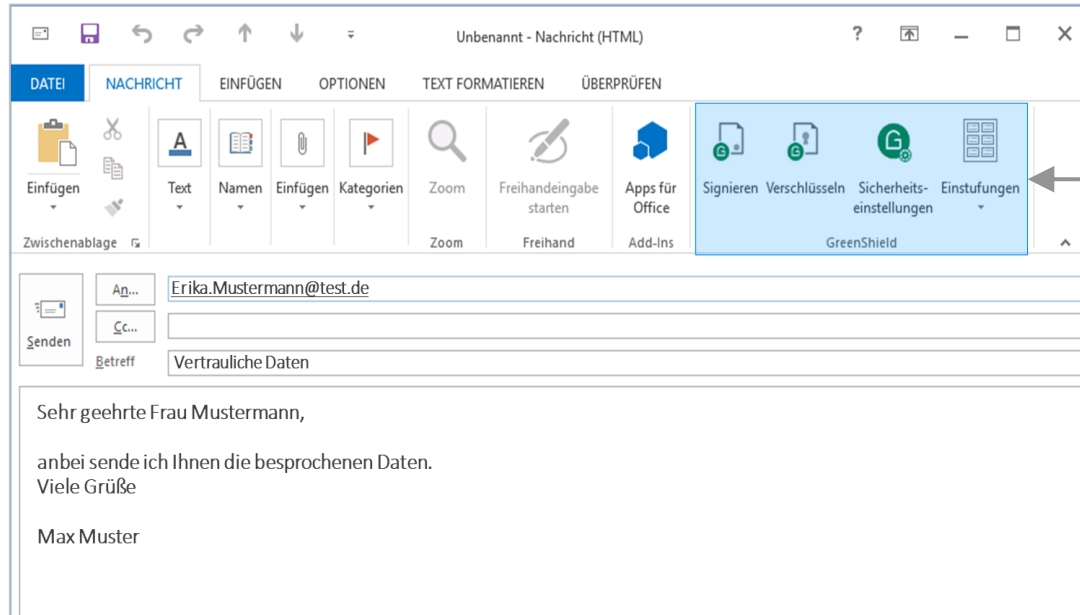
Direkter  
Schlüsselaustausch  
einheitlich



Sperrlisten und OCSP  
für X.509-Zertifikate



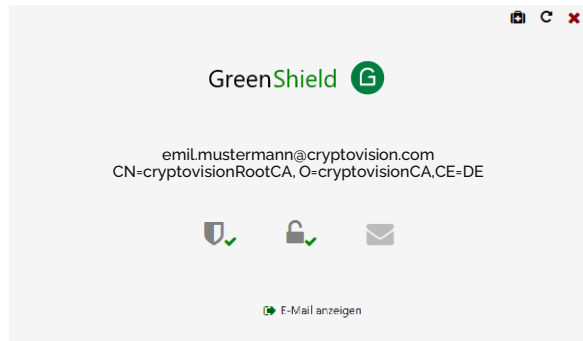
# Das Resultat: GreenShield Mail



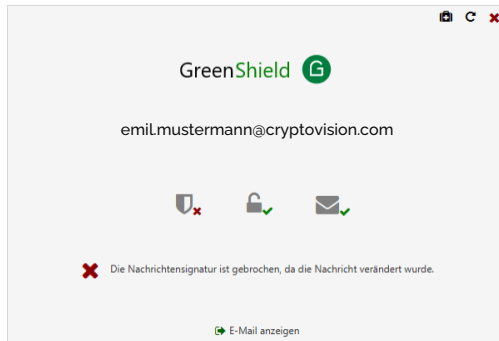
**GreenShield Mail**  
Benutzerfreundliche  
E-Mail-Verschlüsselung  
mit S/MIME und PGP

# Verifizierung von Signaturen

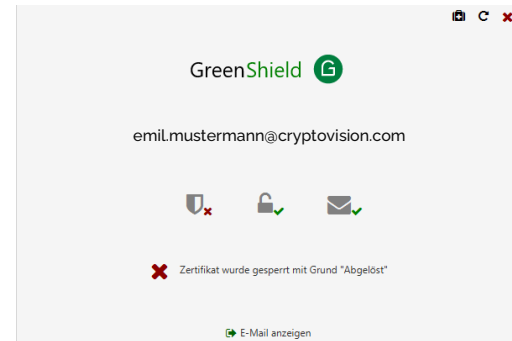
## Korrekt



## E-Mail wurde verändert



## Zertifikat wurde abgelöst



### GreenShield Status

Gültige Nachricht von 'emil.mustermann@cryptovision.com' - RSA

Details

### GreenShield Status

Signaturprüfung fehlgeschlagen

Details

# Direct Trust

Verifizierung der öffentlichen Schlüssel über benutzerfreundlich dargestellte Hashwerte:

## S/MIME

**Zertifikat vertrauen**

Prüfen Sie die Korrektheit des digitalen Fingerabdrucks durch Abgleich der durch Ihren Kommunikationspartner übermittelten Wörter.

Fingerprint (SHA-256): 1462a79d-d429b4f0-fca77cf7-167498f1-0df2ccab-2463a870-7c2d4c7b-0a5ccaac

Deutsch

Bravo	Infekte	Planer	Nörgelei
Stativ	Diadem	Raureif	Wadenbein
Zirkus	Ozonloch	Lorbeer	Wettergott
Büffel	Kaugummi	Oktett	Wagenrad
Beuger	Wanderweg	Serum	Plakette
Doktor	Inkasso	Pleite	Karibik
Lorbeer	Direktor	Hektik	Kniekehle
Beichten	Heuschrecke	Schweben	Popmusik

## PGP

**Öffentlichem OpenPGP-Schlüssel vertrauen**

Prüfen Sie die Korrektheit des digitalen Fingerabdrucks durch Abgleich der durch Ihren Kommunikationspartner übermittelten Wörter.

Fingerprint (SHA-1): 4fd5cc10-d85481f1-3ed32946-9c5bca30-5eda451c

Deutsch











Hochmoor	Stubentür	Serum	Autarkie
Taifun	Guggenheim	Magnum	Wagenrad
Füller	Spediteur	Drücker	Frauenchor
Otter	Helium	Schweben	Doppelkinn
Kaufhaus	Teekessel	Glühen	Camelot

☒ Schlüsselbund direkt vertrauen















Vertrauensstufe: Direktes Vertrauen (für Nachrichten)

# Schlüsselauswahl

## S/MIME

Allgemein	Zertifikate  						
Schlüsselbehälter							
<b>Zertifikate</b>	<b>Ausgestellt für</b>	<b>E-Mail-Adresse</b>	<b>Gültig bis</b>	<b>Ausgestellt von</b>	<b>Seriennummer</b>	<b>Aktionen</b>	+
Sperrlisten	DC=c10n,DC=ve,DC...	alice@mail.ve.c10n	31.08.2022 12:51:10	DC=c10n,DC=ve,DC...	788323d385f645ba1...	   	
OpenPGP-Schlüsselbunde	DC=c10n,DC=ve,DC...	alice@mail.ve.c10n	31.08.2022 12:49:58	DC=c10n,DC=ve,DC...	1226c863994ff93bbd...	   	
Empfängergruppen							
Log							
Über							

## PGP

GreenShield: Konfiguration							
Allgemein	OpenPGP-Schlüsselbunde 						
Schlüsselbehälter							
Zertifikate							
Sperrlisten							
<b>OpenPGP-Schlüsselbunde</b>	<b>Primäre Schlüssel-ID</b>	<b>Ausgestellt für</b>	<b>E-Mail-Adresse</b>	<b>Gültig ab</b>	<b>Gültig bis</b>	<b>Subkeys</b>	<b>Aktionen</b> +
Empfängergruppen	805C A1DA B74F 97A9	charlie@mail.ve.c10n (Signieren)	charlie@mail.ve.c10n	03.12.2021 03:51:20	03.12.2024 03:51:20		   
Log	CDE9 6E90 FB1E 3CF0	bob@mail.ve.c10n	bob@mail.ve.c10n	03.12.2021 03:50:05	03.12.2024 03:50:05		   
Über	98C3 5493 0738 DDA7	alice@mail.ve.c10n	alice@mail.ve.c10n	03.12.2021 03:49:49	03.12.2024 03:49:49		   

# 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

Auch X.509-Synthetisierung ist möglich, aber seltener

Fehlende  
Smartcard-  
Unterstützung  
von PGP wird  
umgangen

# 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

## 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

# Danke für Ihre Aufmerksamkeit

[www.cryptovision.com](http://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.

