cryptovision

Einführung in die VS-NfD-konforme E-Mail- und Datei-Verschlüsselung

OMNISECURE®

Marco Smeja,
cv cryptovision GmbH

1

Cryptovision

Marco Smeja

- Geschäftsführer bei cryptovision
- Seit über 20 Jahren für das Unternehmen aktiv
- Spezialist für sichere elektronische Identitäten und elektronische Ausweisdokumente

2

2

Agenda

01. E-Mail- und Datei-Sicherheit

02. VS-NfD

03. Erfolgsfaktoren

05. Lösungsbeispiel

05. Fazit

3

01. E-Mail und Datei-Sicherheit

4

E-Mail-Sicherheit

E-Mail Verschlüsselung und Signatur 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

5

5

Datei-Sicherheit

Datei Verschlüsselung seit den Neunziger-Jahren in Verwendung

Etwas weiter verbreitet als E-Mail-Sicherheit

Zahlreiche Ansätze: Winzip mit Passwort, Chiasmus, VeraCrypt, Festplatten-Verschlüsselung für Laptops

Für VS-Kommunikation genutzt, wenn auch mit Hürden

Auch Datei-Verschlüsse-lung ist keine Erfolgs-geschichte

6

6

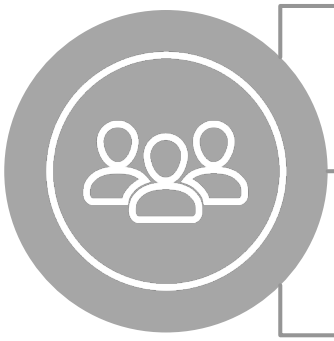
Gründe für die unbefriedigende Situation

- Mangelndes Interesse der Anwender
- Hohe Komplexität, Kosten
- Geringe Benutzer-freundlichkeit
- Keine Interoperabilität zwischen S/MIME und PGP

7

7

Mangelndes Interesse der Anwender

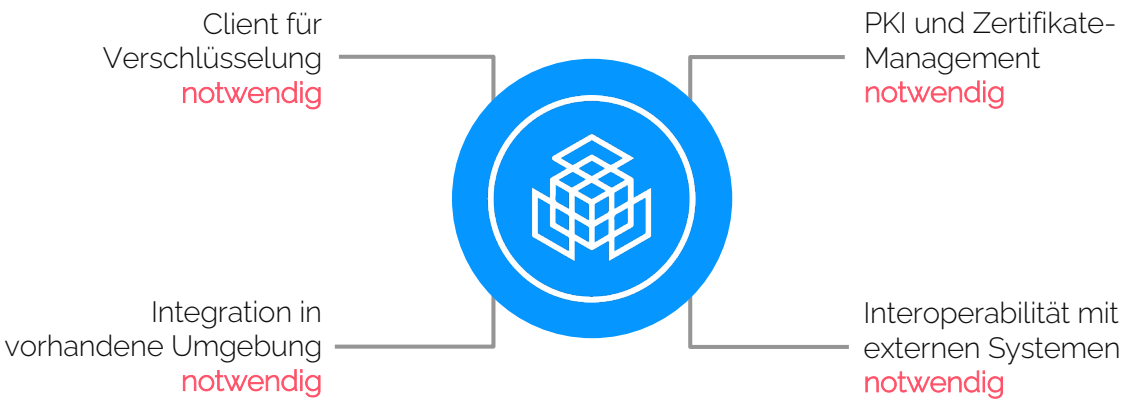


- Häufige Einstellung: „Es ist bisher immer gutgegangen“
- Paradigmenwechsel (auch interne Angriffe müssen verhindert werden) hatte nicht erhoffte Wirkung
- Aufwand aus Sicht des Anwenders zu hoch

8

8

Komplexität, Kosten



Vielen Organisationen ist Aufwand zu groß

9

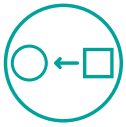
9

Geringe Benutzerfreundlichkeit

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

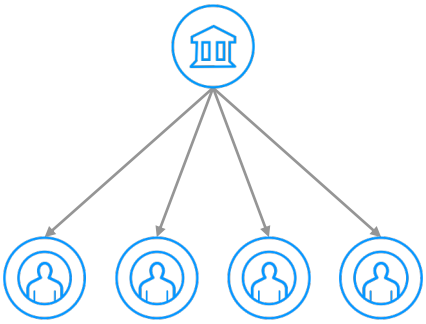
10

10

Keine Interoperabilität zwischen S/MIME und PGP

Chain of Trust (S/MIME)

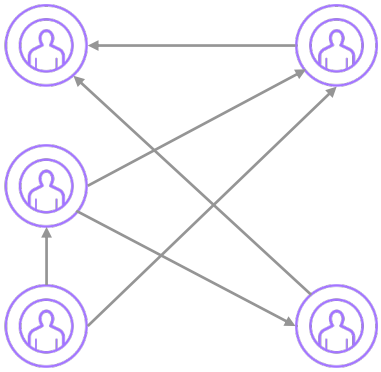
Zertifizierungsstelle



Anwender

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

Web of Trust (PGP)



Anwender

11

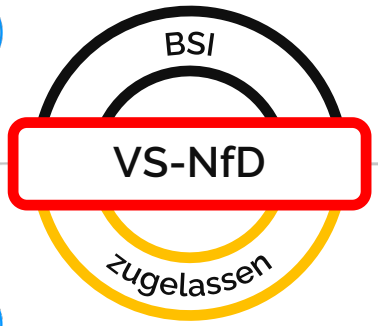
02. VS-NfD

12

Verschlüsselung von Verschlusssachen
Anwendungsbereich mit hohen Anforderungen

Die Bearbeitung von eingestuften Informationen ist durch VSA reglementiert

Die Verschlüsselung von eingestuften Informationen ist unter bestimmten Voraussetzungen notwendig



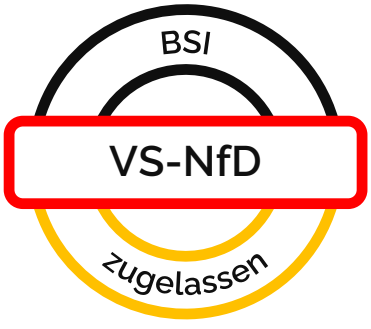
Verschlüsselungs-lösungen für eingestufte Informationen bedürfen einer Zulassung

Eine Zulassung erfordert einen hohen Sicherheitsstandard der Verschlüsselungslösung

13

13

Aktuelle Situation im Bereich VS-NfD



Schwierig für Anwender

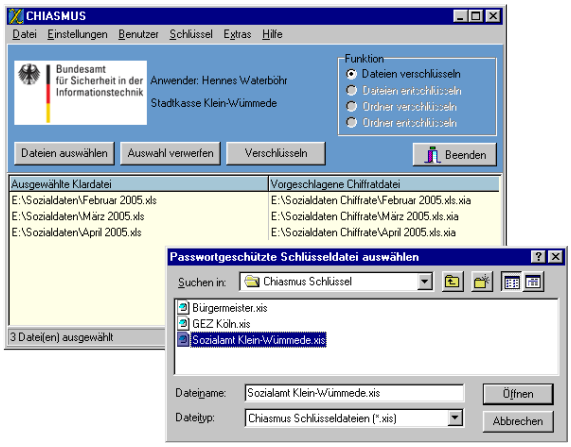
- Hohe Hürden
- Insellösungen
- Interoperabilität gering
- Mangelnde Benutzerfreundlichkeit

Akzeptanz der Anwender oft gering

14

14

Bisherige VS-NfD-Lösung: Chiasmus



Chiasmus

VS-NfD-Zulassung läuft in neun Tagen aus

15

15

03. Erfolgsfaktoren

16

VS-NfD-Lösungen müssen attraktiv sein!

- Nahtlose Integration
- Hoher Automatisierungs-grad
- Zentralisiertes Management
- Inter-operabilität
- Benutzer-freundlichkeit

17

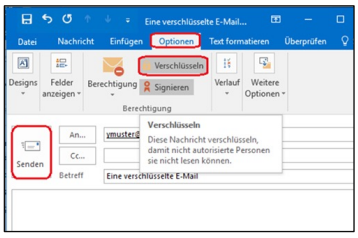
17

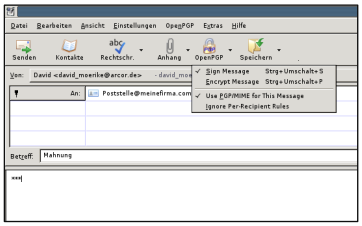
Wie Benutzerfreundlichkeit erreicht wird

18

18

S/MIME und PGP müssen unterstützt werden





Anforderungen:

- Einheitliche Lösung, die beides unterstützt
- Tests der Hersteller
- Synthetisierung von Zertifikaten

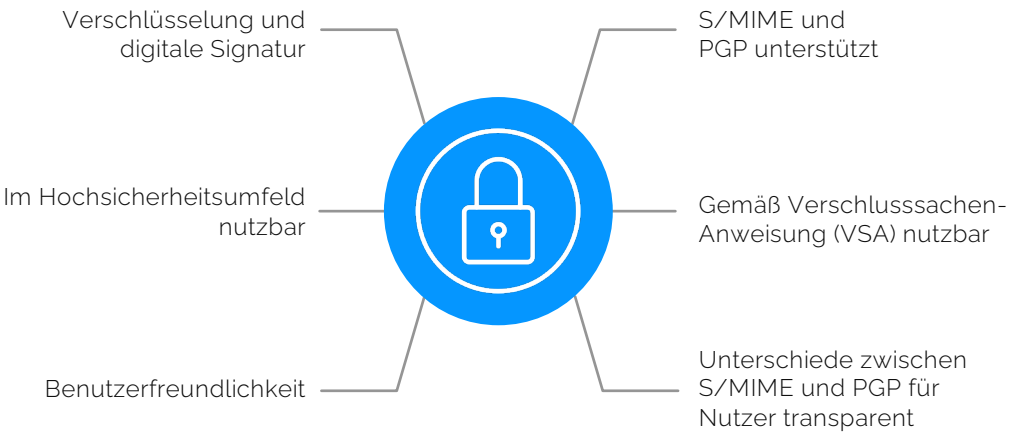
19

19

04. Lösungsbeispiel

20

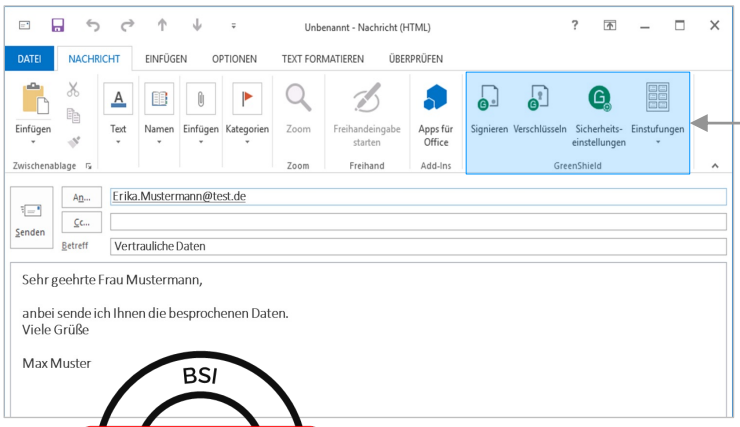
VS-NfD-E-Mail-Security-Client für Outlook und Notes

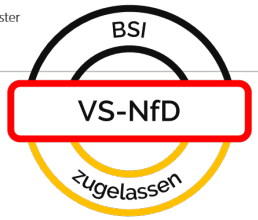


21

21

Modularität: GreenShield Mail für
Für Microsoft Outlook und HCL Notes





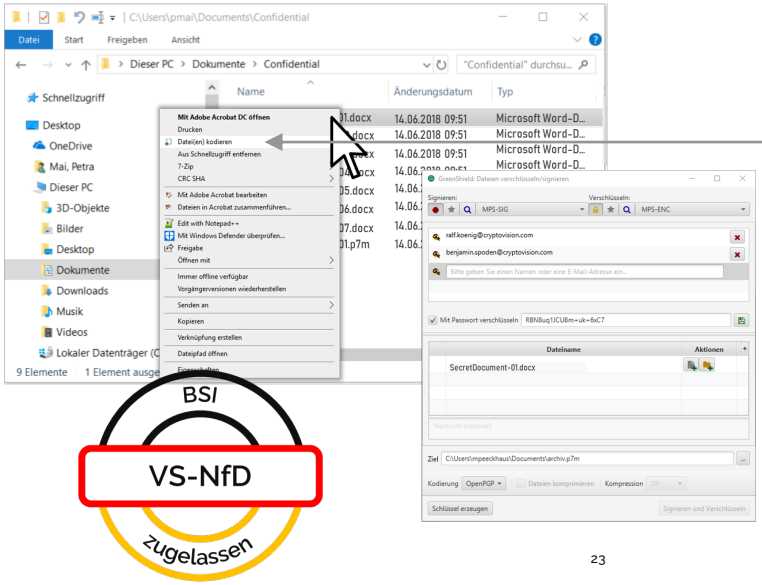
GreenShield Mail
Benutzerfreundliche E-Mail-Verschlüsselung mit S/MIME und PGP

STANAG-Labeling bereits integriert

22

22

Modularität: GreenShield File



GreenShield File
Benutzerfreundliche
Datei-Verschlüsselung
mit S/MIME und PGP

23

23

Usability bei S/MIME- und PGP-Unterstützung
Details

Vergleichbare
Warn-, Fehler-, und
Erfolgsmeldungen

Direkter Schlüsselaustausch
einheitlich

Schlüssel-Sperrung in
jeweils üblicher Form

Sperrlisten und OCSP
für X.509-Zertifikate

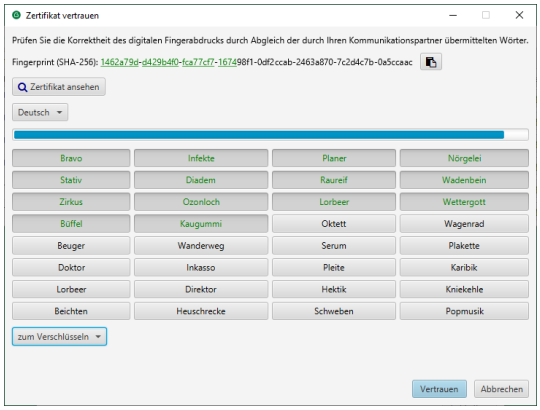
25

25

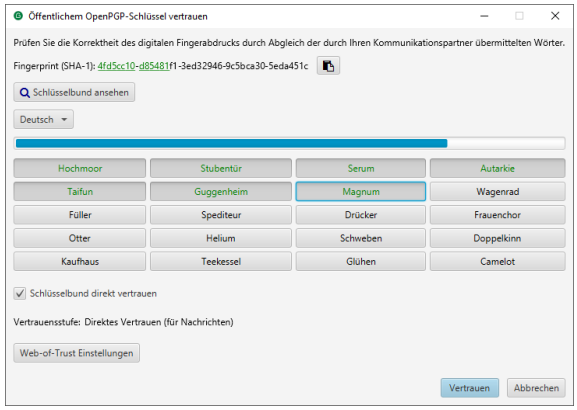
Direct Trust

Verifizierung der öffentlichen Schlüssel über benutzerfreundlich dargestellte Hashwerte:

S/MIME



PGP

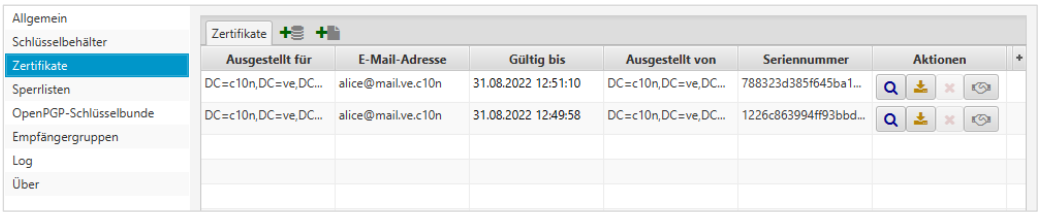


27

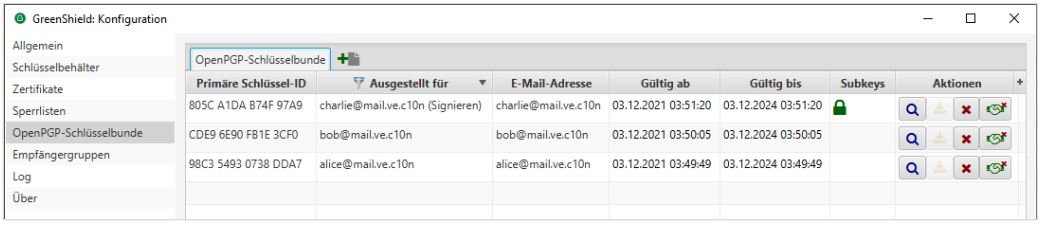
27

Schlüsselauswahl

S/MIME



PGP



28

28

Speicherung der privaten Schlüssel

Virtuelle Smartcard

- Befindet sich in einem geschützten Speicherbereich
- Speicherbereich wird durch 2FA geschützt
- Es ist keine separate Smartcard oder Lesegerät notwendig
- Stellen die gleichen kryptografischen Funktionen wie physische Smartcards bereit
- Nutzt die Rechenleistung des Anwender-PCs und ist somit deutlich schneller als eine physische Smartcard

29

29

05. Fazit

30

Fazit

Praktikable E-Mail- und Datei-Sicherheit für Verschlusssachen ist möglich!

E-Mail- und Datei-Verschlüsselung: keine Erfolgsgeschichte

Benutzer-freundlichkeit als Voraussetzung

Unterstützung von S/MIME und PGP notwendig

GreenShield bietet zuverlässige und integrierte Lösung

31

cryptovision

Danke für Ihre Aufmerksamkeit

www.cryptovision.com

cv cryptovision GmbH |
Munscheidstr. 14 | 45886 Gelsenkirchen

32