



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



Marco Smeja,
cv cryptovision GmbH



© Atos

Atos

1

Cryptovision



Marco Smeja

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

2

Atos

2

Agenda

- 01. E-Mail- und Datei-Sicherheit
- 02. VS-NfD
- 03. Erfolgsfaktoren
- 05. Lösungsbeispiel
- 05. Fazit

3

Atos

3

01. E-Mail und Datei-Sicherheit



Atos

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 goern keine Erfolgs- geschichte

Atos

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

Atos

6

6

Gründe für die unbefriedigende Situation



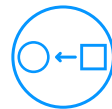
Mangelndes
Interesse der
Anwender



Hohe
Komplexität,
Kosten



Geringe
Benutzer-
freundlichkeit



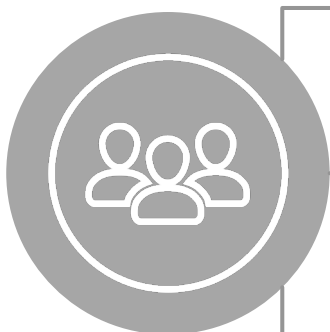
Keine Interoperabilität
zwischen S/MIME
und PGP

7

Atos

7

Mangelndes Interesse der Anwender



Häufige Einstellung: „Es ist bisher
immer gutgegangen“

Paradigmenwechsel (auch
interne Angriffe müssen
verhindert werden) hatte nicht
erhoffte Wirkung

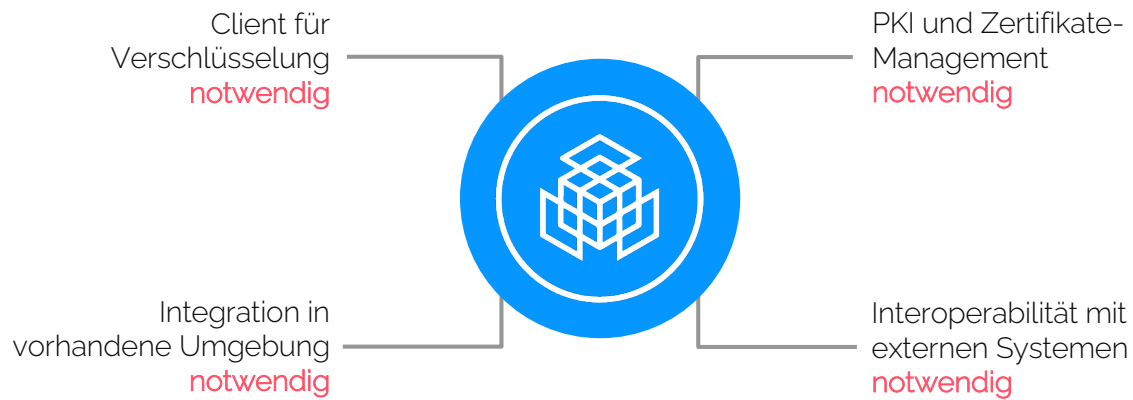
Aufwand aus Sicht des
Anwenders zu hoch

8

Atos

8

Komplexität, Kosten



Vielen Organisationen
ist Aufwand zu groß

Geringe Benutzerfreundlichkeit



Leichte
Beeinträchtigungen
unumgänglich



Nutzer muss mit
Schlüsseln,
Zertifikaten usw.
umgehen können



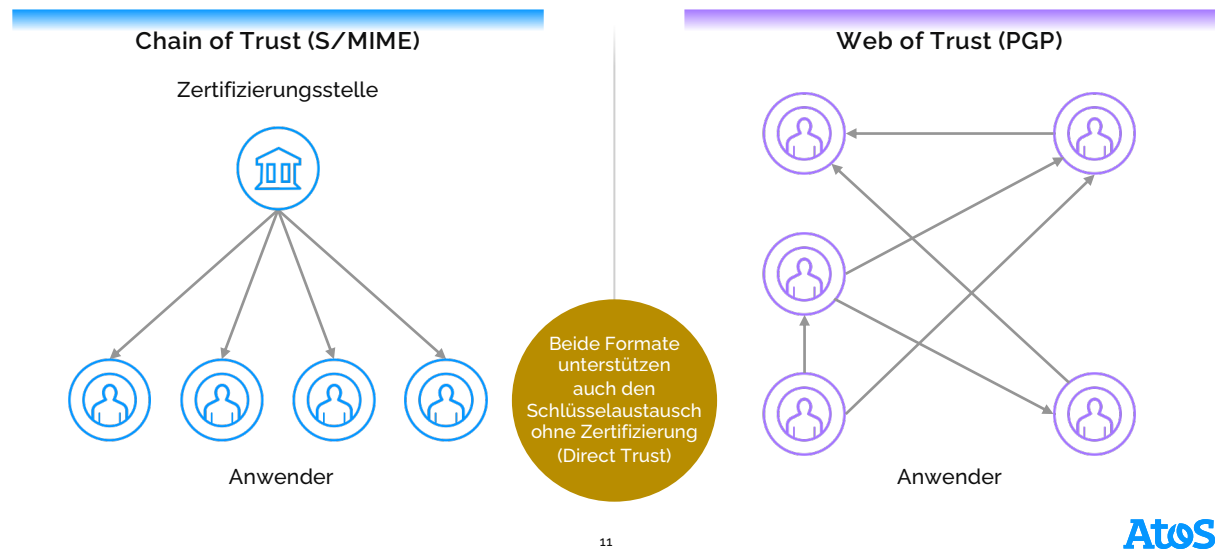
Geeignete Infrastruktur oft
nicht vorhanden (z. B.
Schlüssel auch auf
Smartphone verfügbar)



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

Nutzern ist
kaum zu
vermitteln,
dass es zwei
Standards gibt

Keine Interoperabilität zwischen S/MIME und PGP



11

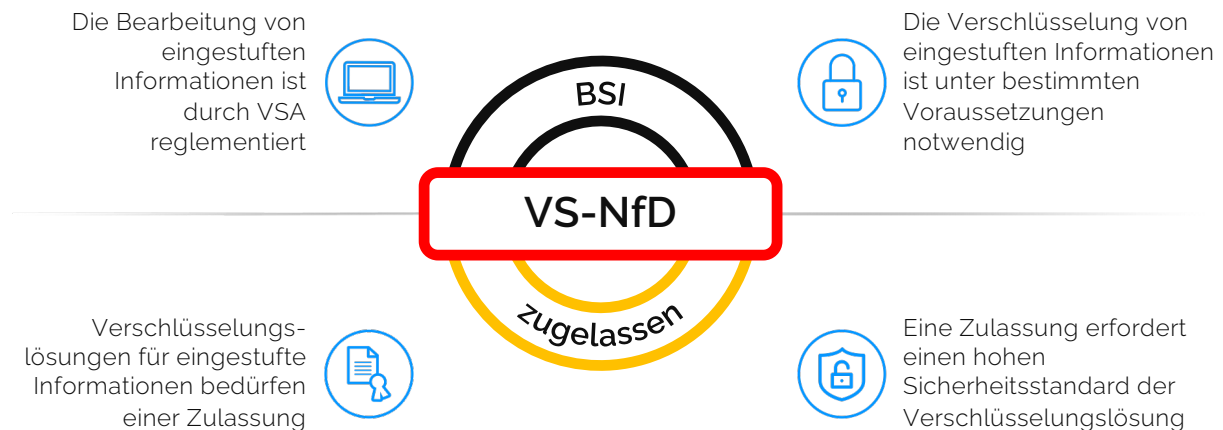
02. VS-NfD



12

Verschlüsselung von Verschlusssachen

Anwendungsbereich mit hohen Anforderungen

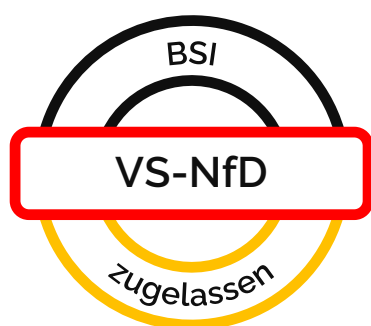


13

Atos

13

Aktuelle Situation im Bereich VS-NfD



Schwierig für Anwender

- Hohe Hürden
- Insellösungen
- Interoperabilität gering
- Mangelnde Benutzerfreundlichkeit

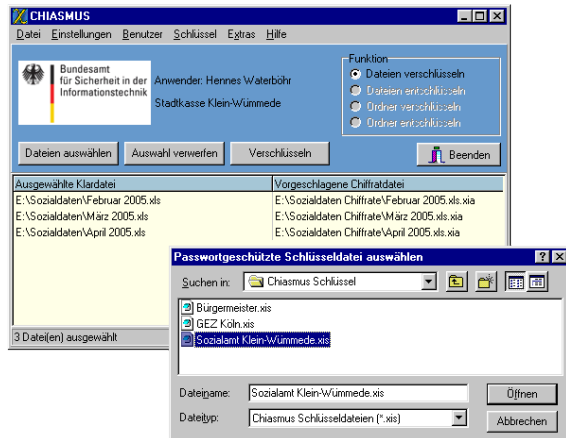
Akzeptanz der Anwender oft gering

14

Atos

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

Atos

17

Wie Benutzerfreundlichkeit erreicht wird

Automatisiertes
Enrollment und
Zertifikatserneuerung



Keine
Beeinträchtigung
bestehender Abläufe



Intuitive und
verständliche
Nutzung



Transparente Verwaltung
von Schlüsseln und
Zertifikaten

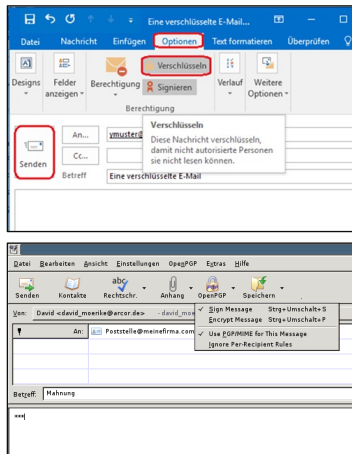


18

Atos

18

S/MIME und PGP müssen unterstützt werden



Anforderungen:

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

19

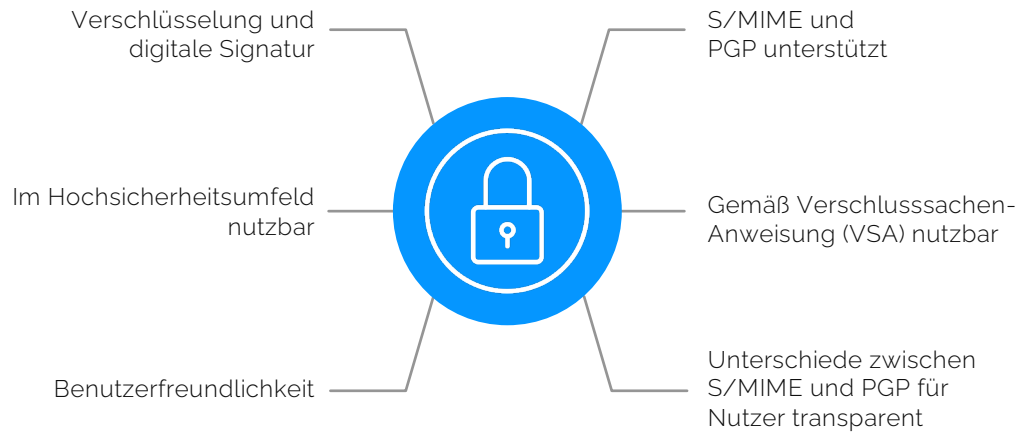
19

04. Lösungsbeispiel



20

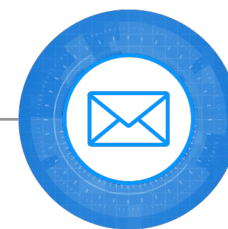
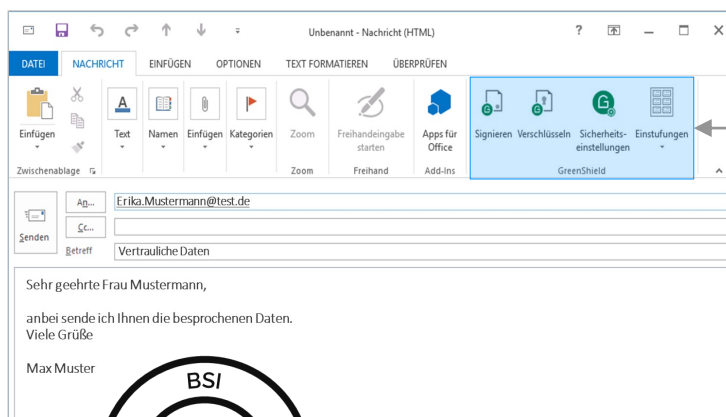
VS-NfD-E-Mail-Security-Client für Outlook und Notes



21

21

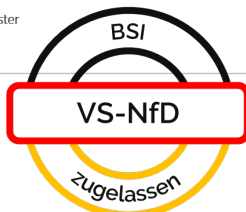
Modularität: GreenShield Mail für Für Microsoft Outlook und HCL Notes



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



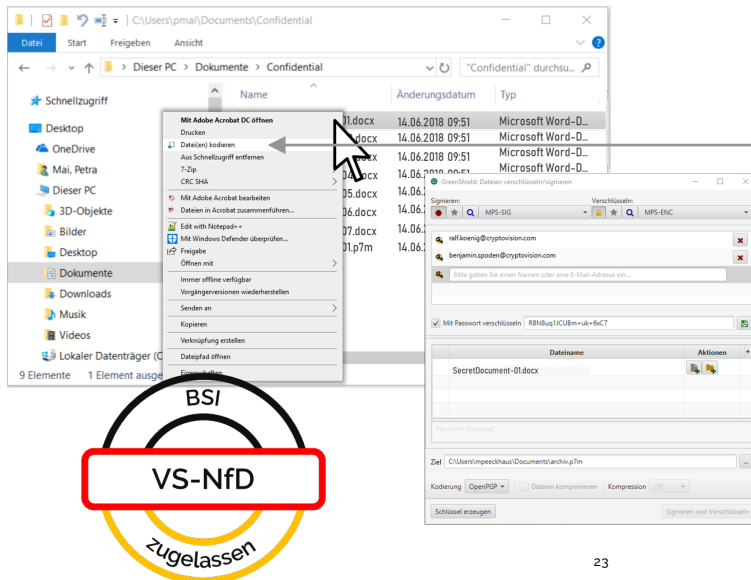
STANAG-Labeling
bereits integriert



22

22

Modularität: GreenShield File



23

23

Usability bei S/MIME- und PGP-Unterstützung

Details



25

25

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): **1462a7bd-d429bd40-fca77cf7-167498f1-0af2ccab-2463a870-7c2d4c7b-0a5ccaac**

Deutsch

Bravo	Infekte	Planer	Nörgelei
Stativ	Diadem	Raureif	Wadenbein
Zirkus	Ozonloch	Lorbeer	Wettergott
Büffel	Kaugummi	Okett	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	Drucker	Frauenchor
Otter	Helium	Schweben	Doppelkinn
Kaufhaus	Teekessel	Glühen	Camelot

☒ Schlüsselbund direkt vertrauen

Vertrauensstufe: Direktes Vertrauen (für Nachrichten)

27

27

Schlüsselauswahl

S/MIME

Allgemein	Zertifikate  					
Schlüsselbehälter						
Zertifikate	Ausgestellt für	E-Mail-Adresse	Gültig bis	Ausgestellt von	Seriennummer	Aktionen 
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=...	1226c863994f93bbd...	   
Empfängergruppen						
Log						
Über						

PGP

GreenShield: Konfiguration

Allgemein

Schlüsselbehälter

Zertifikate

Sperrlisten

OpenPGP-Schlüsselbunde

Empfängergruppen

Log

Über

OpenPGP-Schlüsselbunde

+

Primäre Schlüssel-ID	Ausgestellt für	E-Mail-Adresse	Gültig ab	Gültig bis	Subkeys	Aktionen
805C A1DA 874F 97A9	charlie@mail.ve.c10n (Signieren)	charlie@mail.ve.c10n	03.12.2021 03:51:20	03.12.2024 03:51:20		
CDE9 6E90 FB1E 3CF0	bob@mail.ve.c10n	bob@mail.ve.c10n	03.12.2021 03:50:05	03.12.2024 03:50:05		
98C3 5493 0738 DDA7	alice@mail.ve.c10n	alice@mail.ve.c10n	03.12.2021 03:49:49	03.12.2024 03:49:49		

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

Atos

29

05. Fazit



Atos

30

Fazit

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



31

Atos

31



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

32