

E-Mail-Sicherheit in einer Umgebung mit und ohne VS-Anforderungen – Eine Case Study

Martin Peeckhaus,
cv cryptovision GmbH



Cryptovision



Martin Peeckhaus

- tbd

Agenda

01. Anforderungen

02. Umsetzung

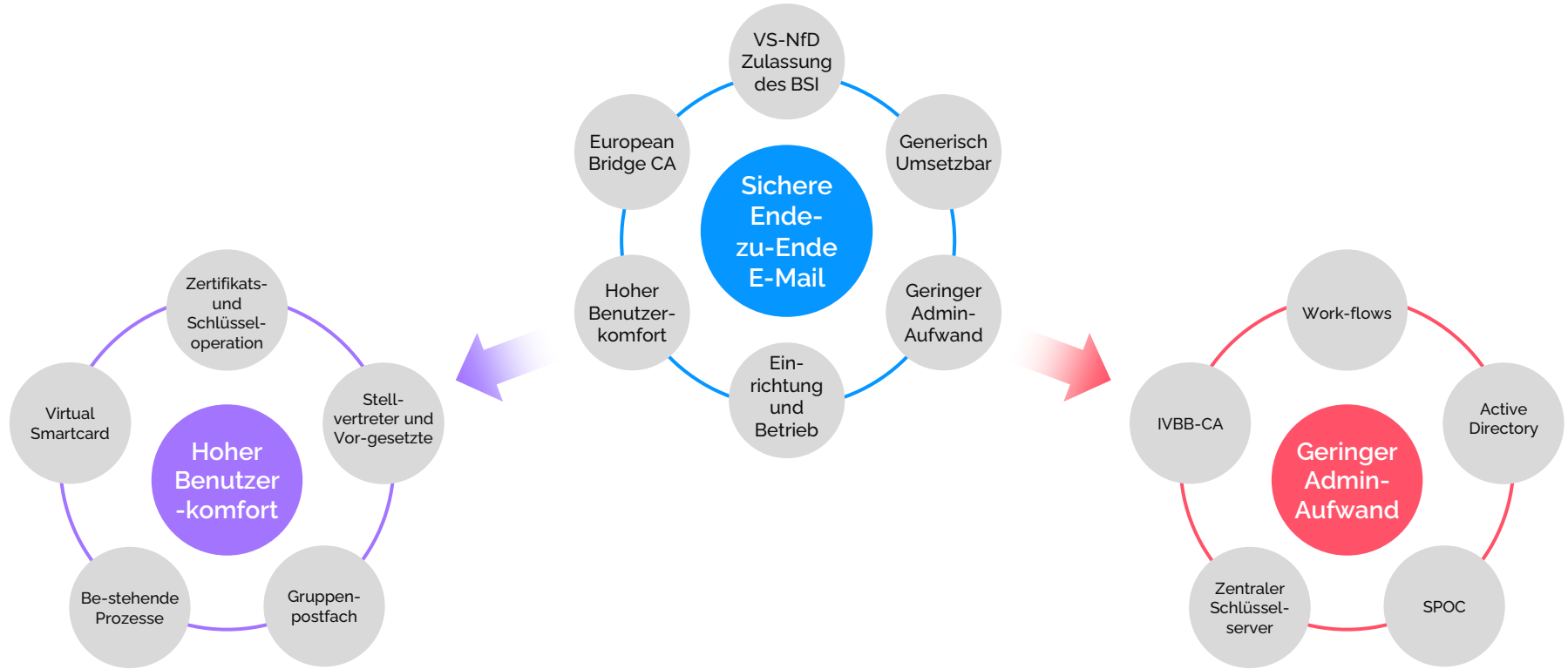
03. Fazit

01. Anforderungen



Anforderung im Projekt für eine Bundesbehörde

E-Mail-Sicherheit für eine Bundesbehörde



Verschlüsselung von Verschlusssachen

Anwendungsbereich mit hohen Anforderungen

Die Bearbeitung von eingestuften Informationen ist nur mit freigegebener VS-IT zulässig



Die Verschlüsselung von eingestuften Informationen ist unter bestimmten Voraussetzungen notwendig



VS-NfD

BSI

Zugelassen

Verschlüsselungs-lösungen für eingestufte Informationen bedürfen einer Zulassung



Eine Zulassung erfordert einen hohen Sicherheitsstandard der Verschlüsselungslösung



Generelle Anforderungen

Generelle Anforderungen an die Bundesbehörden-Lösung:



Hohes
Sicherheitsniveau



Hoher
Automatisierungs-
grad



Persönliche
Schlüssel und
Gruppenschlüssel



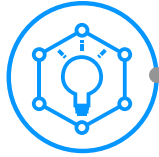
S/MIME
als Format



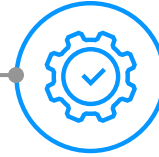
Benutzer-
freundlichkeit

Benutzerfreundlichkeit

Automatisierte Prozesse für das Enrollment und die Zertifikats-erneuerung



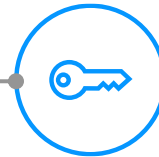
Keine Beeinträchtigung bestehender Abläufe



Intuitive und verständliche Nutzung



Transparente Verwaltung von Schlüsseln und Zertifikaten

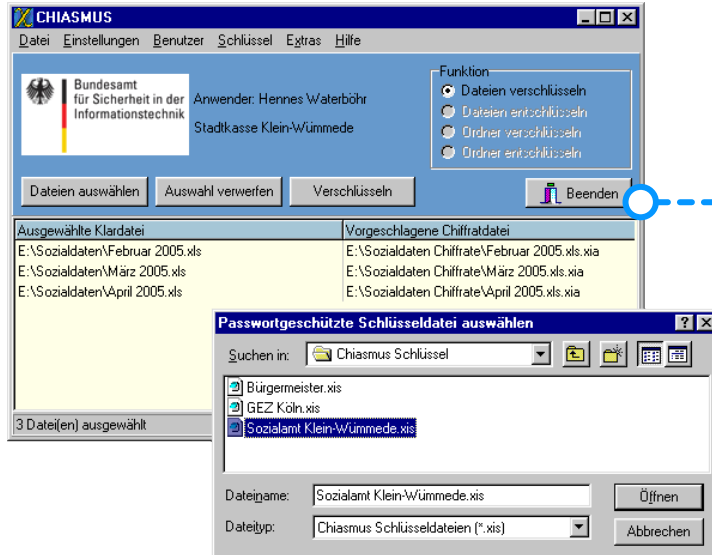


02. Umsetzung

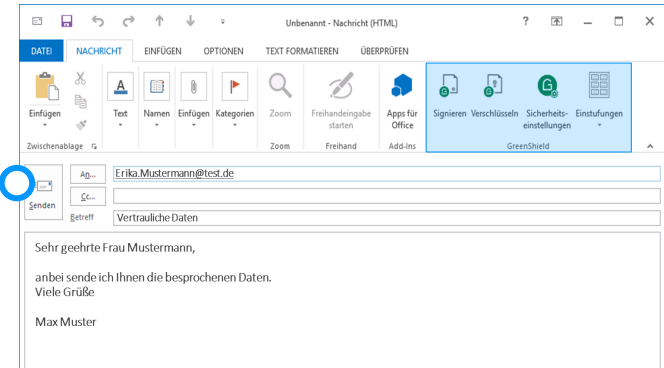


Bisherige VS-NfD-Lösung: Chiasmus

Chiasmus

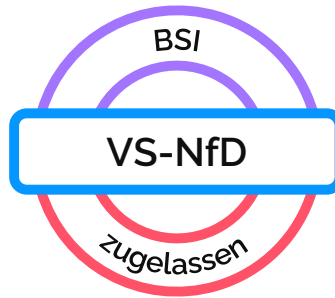
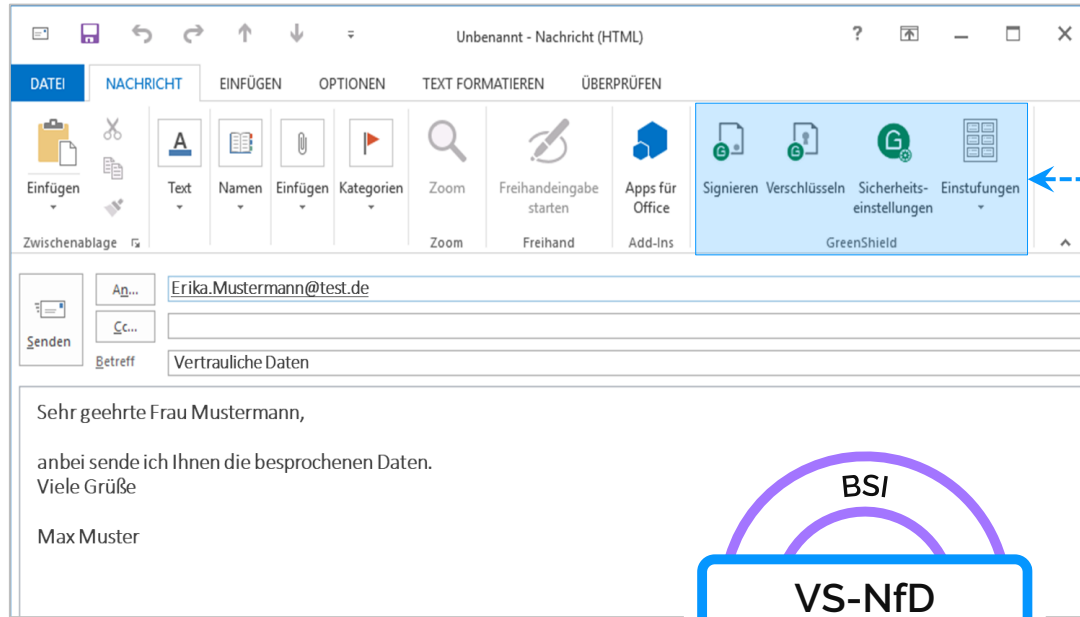


GreenShield



GreenShield Mail

Für Microsoft Outlook



GreenShield Mail
Benutzerfreundliche
E-Mail-Sicherheit

Umsetzung von Gruppenpostfächern



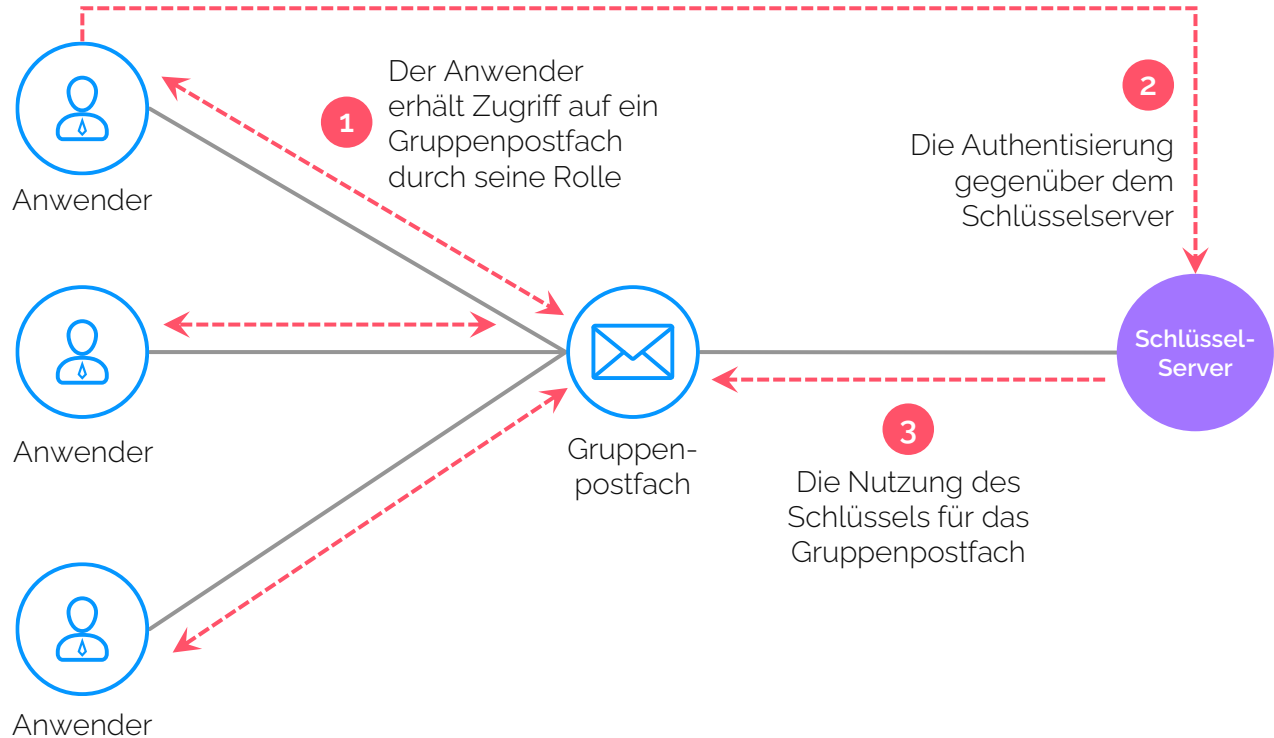
Gruppenpostfach

Privater Gruppenschlüssel
für Entschlüsselung

Privater Gruppenschlüssel
für digitale Signatur
(„Stempelsignatur“)

Use Case: Gruppenpostfach mit Schlüsselserver

Gruppenpostfach:
Mehrere Anwender
nutzen *ein* Postfach mit
einer E-Mail-Adresse





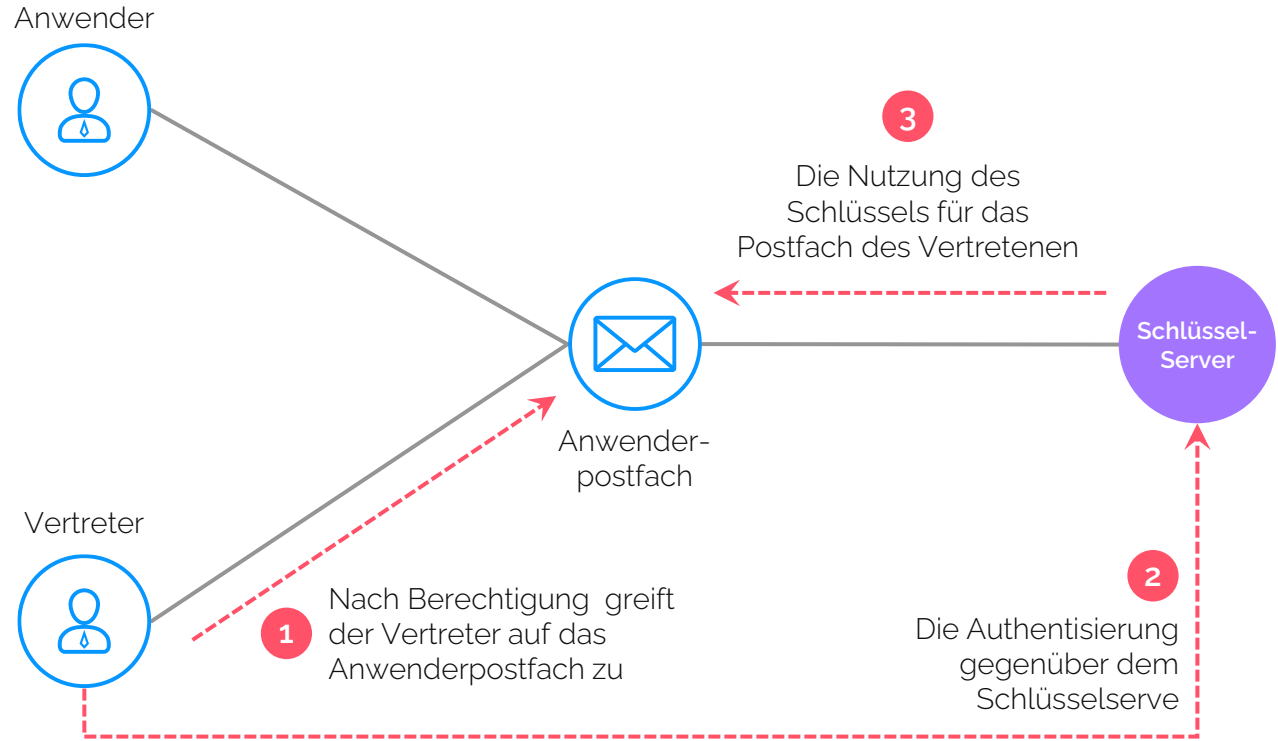
Fremdzugriff

Der Vertreter nutzt den privaten Schlüssel des Vertretenen zur Entschlüsselung von E-Mails

Der Vertreter nutzt seinen **eigenen** privaten Schlüssel für die Signatur („Im-Auftrag-von-Signatur“)

Use Case: Stellvertretung mit Schlüsselserver

Stellvertretung: Ein Vertreter hat Zugriff auf ein Postfach eines anderen Anwenders (z. B. Urlaubsvertretung, Chef-Postfach-Regelung)



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

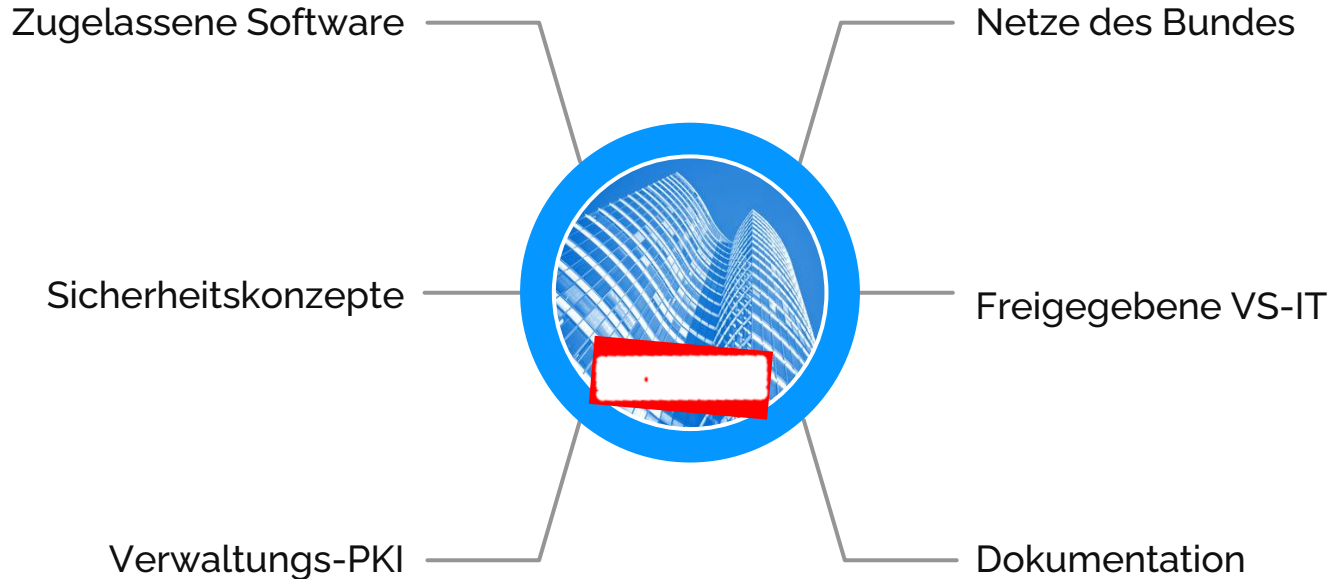


03. Fazit

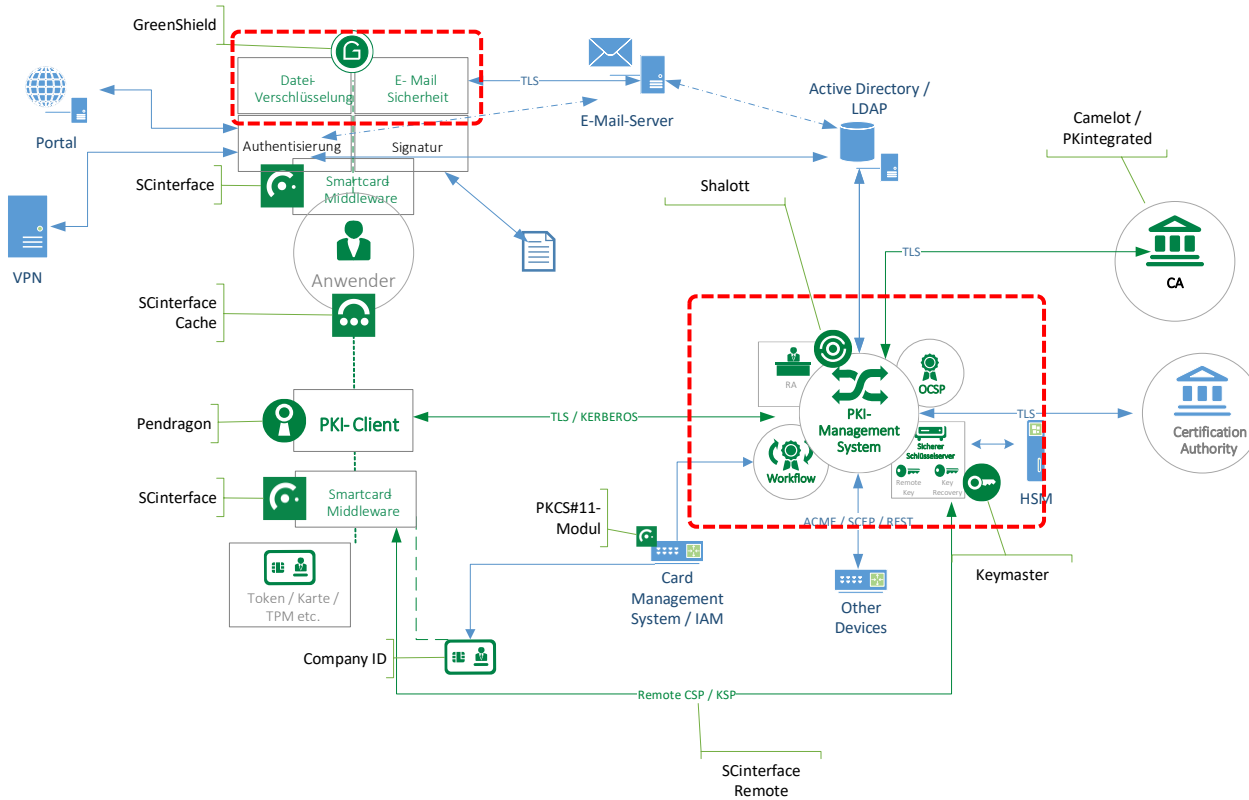


Das Fazit

E-Mail-Sicherheit für eine Bundesbehörde mit 2.500 Anwendern mit zwei verschiedenen Sicherheitskonzepten (VS und nicht-VS) ist möglich!

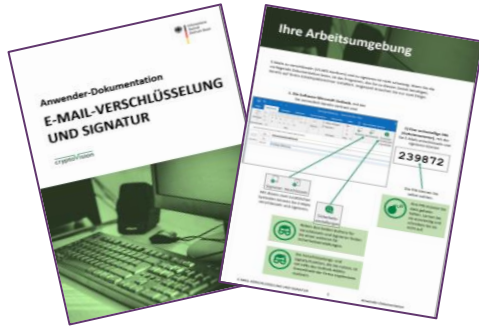


GreenShield Comfort



Anwender-Dokumentation

Attraktiv gestaltete Dokumentation



Materialien

- Anwender- Dokumentation
- Broschüren
- Schritt-für-Schritt- Anleitungen



Professionelle Videos mit

- Professionelle Moderatorin
- Screencams
- Animationen
- O-Ton von Prof.Dr. N. Pohlmann

Aktueller Stand des Projekts



Konzeptionsphase



Sicherheitskonzept



Implementierung



Customizing



Roll-Out



Pilotphase



Wirkbetriebseinführung



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.

