



**Mehr Sicherheit und Effizienz durch zentral  
automatisiertes Zertifikatsmanagement mittels  
Anbindung der DFN-TCS PKI an Mail-Gateway  
am Beispiel Studentenwerk Potsdam**

A. Nold, CCO und A. Renoncet, Account Manager

# Agenda

- 1 Unternehmensvorstellung
- 2 Bedrohungslage
- 3 Grundlagen E-Mail-Verschlüsselung
- 4 Produkte
- 5 Casestudy: Studentenwerk Potsdam
- 6 Angebot an die DFN Mitglieder

# Unternehmensvorstellung

---

# Unternehmensvorstellung & Referenzen

## Seit 2004 mit zentraler E-Mail-Verschlüsselung am Markt

- Unabhängiges, gründergeführtes Unternehmen
- > 100 Mitarbeiter, Standort Berlin
- Professionelle Lösungen für sicheren E-Mail- und Datenaustausch
- hohe Automatisierung, intuitive Bedienbarkeit, einfache Integration



## Auszug Referenzkunden



# Zertificons Kundenstruktur

Z1 Lösungen sind überall im Einsatz, wo E-Mails und Dateien geschützt werden müssen.



**Energie**



**Behörden**



**Kleinunternehmen**



**Banken**



**Legal**



**Mittelstand**



**Automotive**



**Handel**



**Großkonzerne**



**Health**



**Forschung**

**Mehr als 25% der TOP 100** der umsatzstärksten, deutschen Unternehmen haben sich bereits für Zertificon entschieden.

# Bedrohungslage

---

**25%**

der deutschen Unternehmen,  
v. a. Kleinunternehmen, erlitten  
durch Cyberangriffe nahezu  
existenzbedrohende Schäden

**55%**

der in der Bitkom-Studie befragten Führungs-  
kräfte wurden Opfer von Social Engineering

**9 von 10 Unternehmen**  
sind durch Cyberangriffe betroffen

Quellen: bsi.de, bitkom.org

**89%**

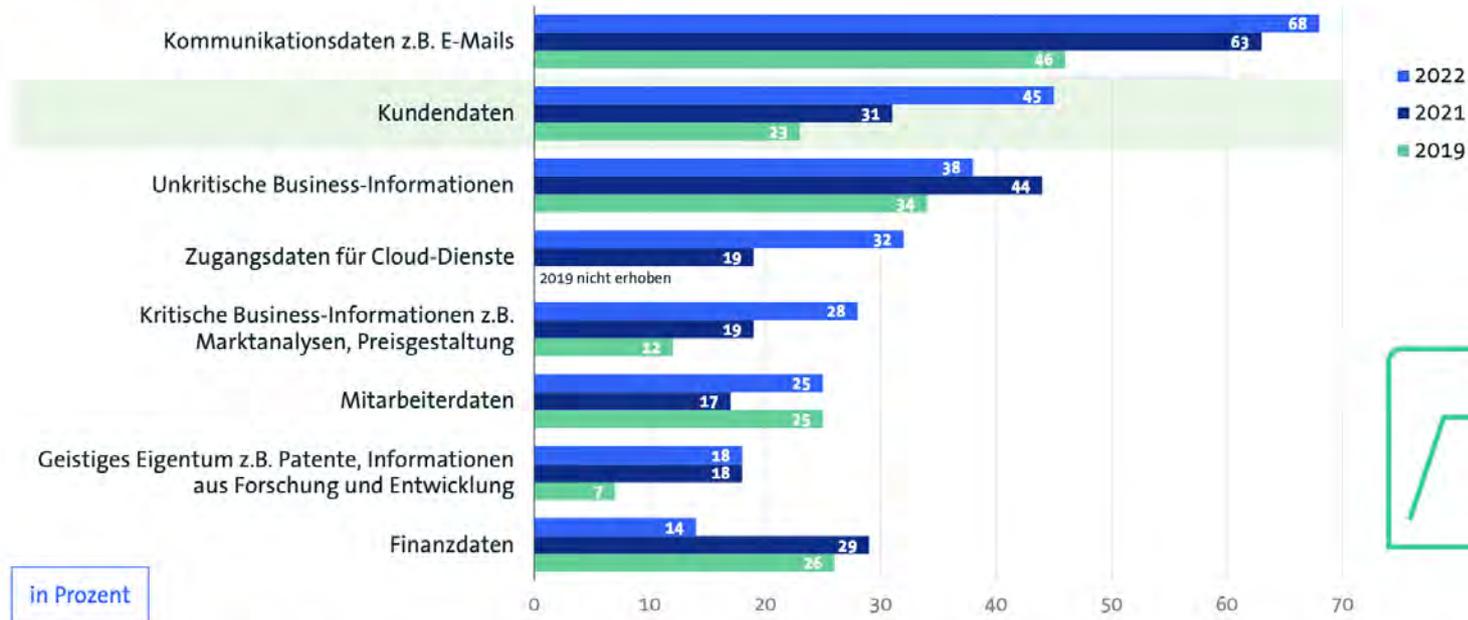
der Befragten  
der Bitkom-  
Studie von  
2020 sehen  
mehr Cyberattacken als im Vorjahr

Im Vergleich zum Vorjahr steigen Er-  
pressungsvorfälle, mit einem Ausfall  
von Informations- und Produktions-  
systemen sowie der Störung von  
Betriebsabläufen, um

**358%**

# Datendiebstahl: Immer öfter sind Dritte betroffen

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



in Prozent

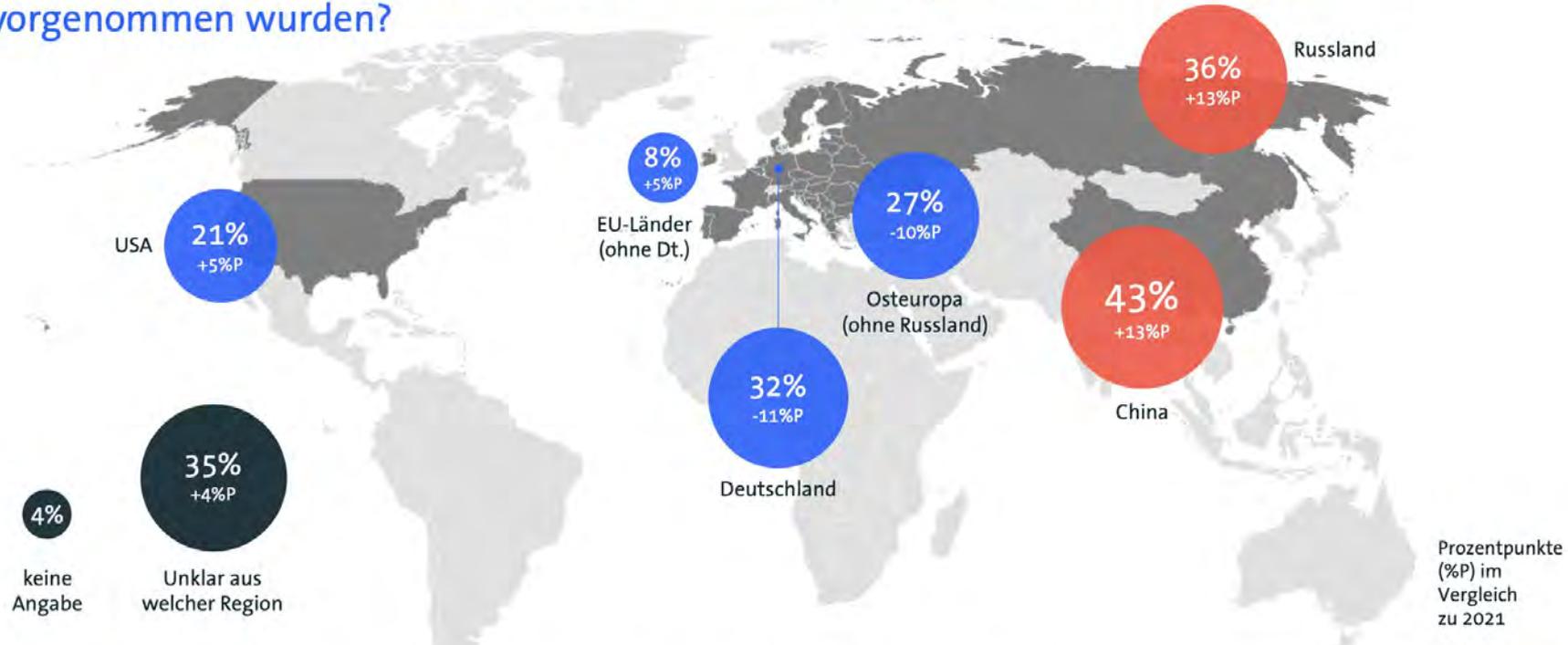


bitkom

4 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten (2019: 2 Jahren) von Diebstahl von sensiblen digitalen Daten betroffen waren (2022: n=383; 2021: n=330; 2019: n=229) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

# Angriffe auf Deutschland: Der Osten rückt in den Fokus

Konnten Sie feststellen, von wo aus bzw. aus welcher Region diese Handlungen vorgenommen wurden?



10 Basis: Alle befragten Unternehmen, die in den letzten 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2021: n=935) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2022

## Spitzenforschung in Gefahr

Die Wissenschaftslandschaft und damit auch die bayerischen Hochschulen und Universitäten sind im Rahmen wünschenswerter Initiativen zur Internationalisierung immer globaler geworden: Lehrende, Studierende und Mitarbeiter/innen aus der ganzen Welt kommen miteinander in Kontakt und tauschen wissenschaftliche Erkenntnisse aus - gerade im Bereich der Spitzenforschung.

Diese positive Entwicklung hat aber auch eine Schattenseite: viele Staaten beauftragen ihre Nachrichtendienste damit, wissenschaftliches Know-how durch Spionage auszuforschen, um dieses Wirtschaft und Wissenschaft des eigenen Landes zur Verfügung zu stellen. Dabei stehen in erster Linie innovative Technologien im Fokus aber auch sozial- und wirtschaftswissenschaftliche Themen sind von Interesse. Ausgeforscht werden dabei nicht nur neue technische, sondern auch strategisch wichtige Informationen.

### Grundsätzlich gilt:

**je besser desto begehrt.**

Auch an Ihrer Hochschule gibt es sensibles Know-how, für das sich Wissenschaftsspieler interessieren. Schätzen Sie daher die Bedrohung durch Spionage als ernstzunehmend ein und helfen Sie durch Ihren Beitrag mit, die Risiken zu minimieren.

## Bedenken Sie:

Alle Bereiche der Spitzenforschung (Drittmittel- und Kooperationsprojekte, Grundlagenforschung, F+E-Projekte) sind für ausländische Nachrichtendienste von Interesse, gerade im Hinblick auf deren wirtschaftliche Verwertbarkeit. Auch aus Ihrer Sicht „bekannte“ Details oder Hintergrundinformationen, die oft schon im Vorfeld einer Kooperation ausgetauscht werden, können für die Angreifer lohnenswert sein. Bedenken Sie bitte, dass auch Nachrichtendienste westlicher Länder aktiv sind.

## Externe Risikofaktoren:

Ausländische Mitarbeiter/innen oder Studierende werden von Nachrichtendiensten gezielt in relevante Bereiche von Hochschulen eingeschleust, um dort spezielles Know-how auszuspionieren. Daneben werden vor allem die vielfältigen elektronischen Spionagemöglichkeiten genutzt. Immer häufiger gelangen die Angreifer über sogenannte „Trojaner“ ins hauseigene Netzwerk. Eingeschleust werden diese mittels personalisierter E-Mails mit infiziertem Anhang. Die nötigen Informationen dazu stammen aus dem Internet (Homepage, Soziale Netzwerke, o. ä.) oder wurden gezielt bei der Person selbst ausgekundschaftet („Social Engineering“).

## Interne Risikofaktoren:

Nachrichtendienste suchen gezielt den Kontakt zu Personen aus dem Hochschulbereich, um so an interne Informationen zu gelangen – oft ist dies den Betroffenen gar nicht bewusst. Vom unabsichtlichen Verlust von Datenträgern bis hin zum gezielten Know-how-Diebstahl reicht die Bandbreite beim „Sicherheitsfaktor Mensch“ und umfasst alle Personen, die sich innerhalb des Hochschulbereiches bewegen!

## Lösungsansätze:

Definieren Sie besonders sensible Daten und legen Sie entsprechend abgestufte Zugriffsberechtigungen fest. Erarbeiten Sie für Ihre Hochschule allgemein verbindliche Sicherheitsrichtlinien, die kommuniziert, kontrolliert und fortgeschrieben werden.

**Last but not least: sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter.**

Das Bayerische Landesamt für Verfassungsschutz unterstützt Sie dabei gerne:  
neutral – vertraulich – kostenfrei



## Know-how-Schutz für Spitzenforschung



Informationen zu  
Prävention und Sicherheit

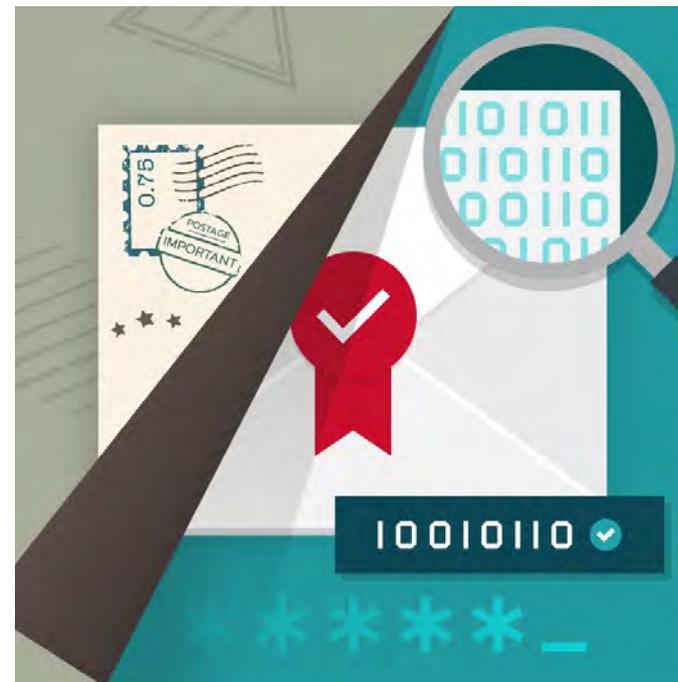
# E-Mail-Verschlüsselung

---

## Grundlagen

# Grundlagen E-Mail-Verschlüsselung

- Warum E-Mail-Verschlüsselung?
  - Sicherheit
  - Compliance
  - Digitalisierung
- PKI (Public Key Infrastructure):  
Vertrauenskonzept, Verbreitung und Anwendungen
- Asymmetrische Verschlüsselung: private und public Keys
- Alternative Wege der Mailverschlüsselung:  
Passwort, TLS, proprietäre Software, Microsoft OME



# E-Mail-Verschlüsselung & Signatur schützt Ihre Daten

Jede E-Mail ist eine virtuelle Postkarte – Sie kann mitgelesen und verfälscht werden.



## Ungesicherter E-Mail-Verkehr ist risikoreich und kann teuer werden!

Jedes Unternehmen und jede Behörde oder Institution ist spionagegefährdet, unabhängig von Größe, Branche, Zuständigkeitsbereich.

# Compliance-Vorgaben

## EU DS-GVO

- Personenbezogene Daten genießen besonderen Schutz
- Bei Verstößen drohen hohe Strafen

## IT-Sicherheitsgesetz (KRITIS)

- Verfügbarkeit und Sicherheit der IT-Systeme spielt eine besondere Rolle

## § 203 StGB – Verletzung von Privatgeheimnissen

- Freiheitsstrafen bis zu einem Jahr

...



# Einsatzgebiete für Verschlüsselung

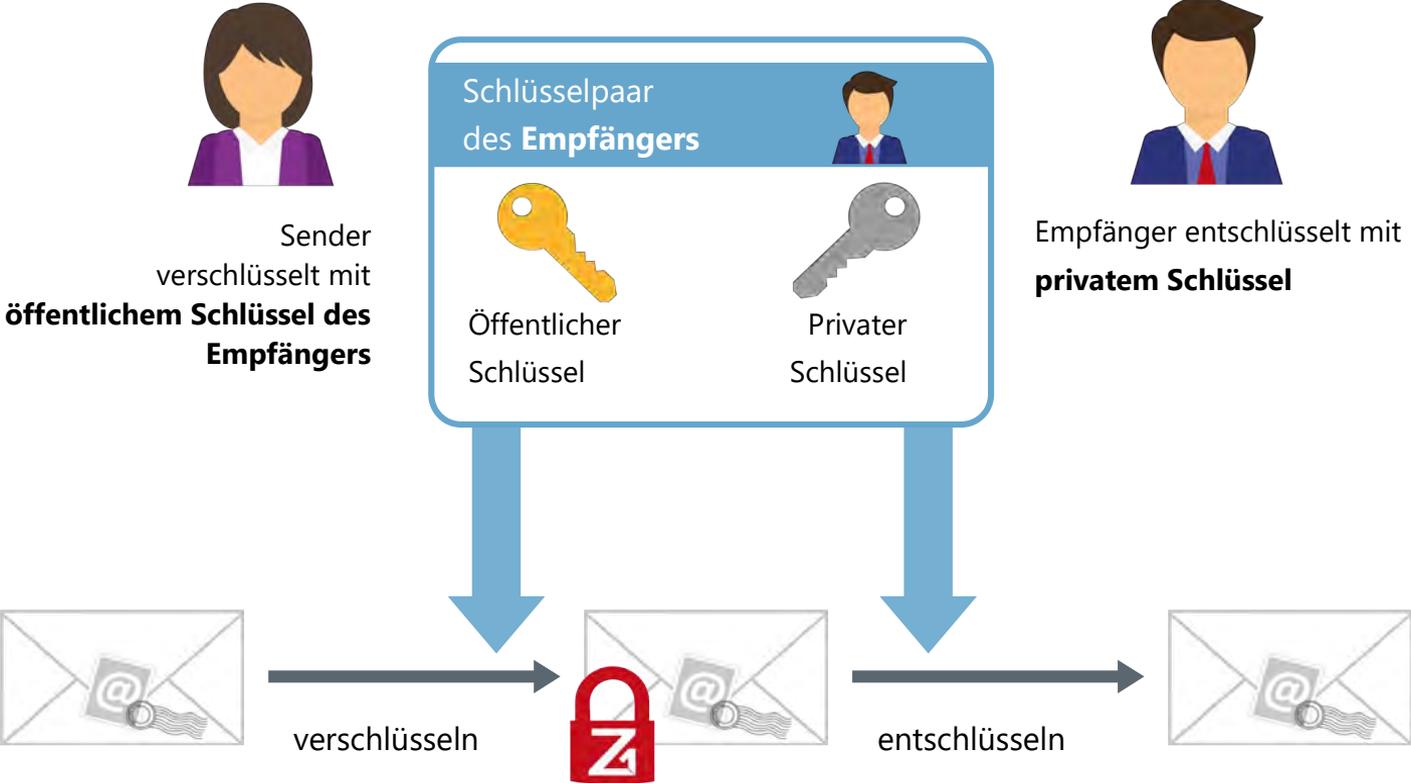
## Allgemein

- Schutz geistigen Eigentums (Forschung & Entwicklung)
- Schutz personenbezogener Daten (HR, Versicherung etc.)
- Revision, Steuerunterlagen, Wirtschaftsprüfung (Nachweis der Unverfälschtheit)
- Vertrauensbildende Maßnahme (Imagepflege)

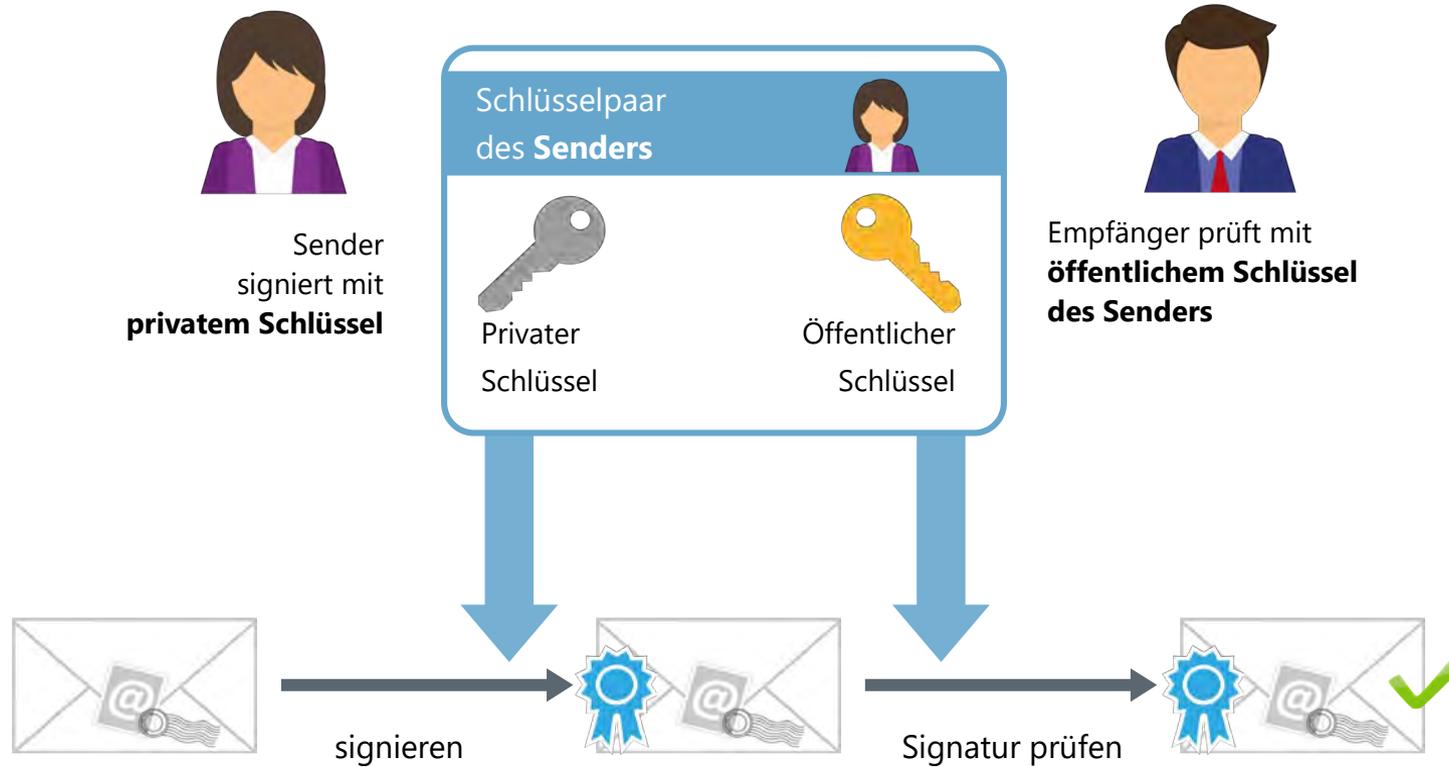
## Branchenspezifische Gründe

- **Automotive** verlangen von Zulieferern verschlüsselten Datenaustausch
- Insbesondere **Patentanwälte** schützen das geistige Eigentum ihrer Mandanten
- **Gesundheitsbranche** schützt sensible **personenbezogene Daten**
- **Pharmabranche** schützt **Forschungsergebnisse**
- u.S.W.

# PKI-Grundlagen – Asymmetrische Verschlüsselung



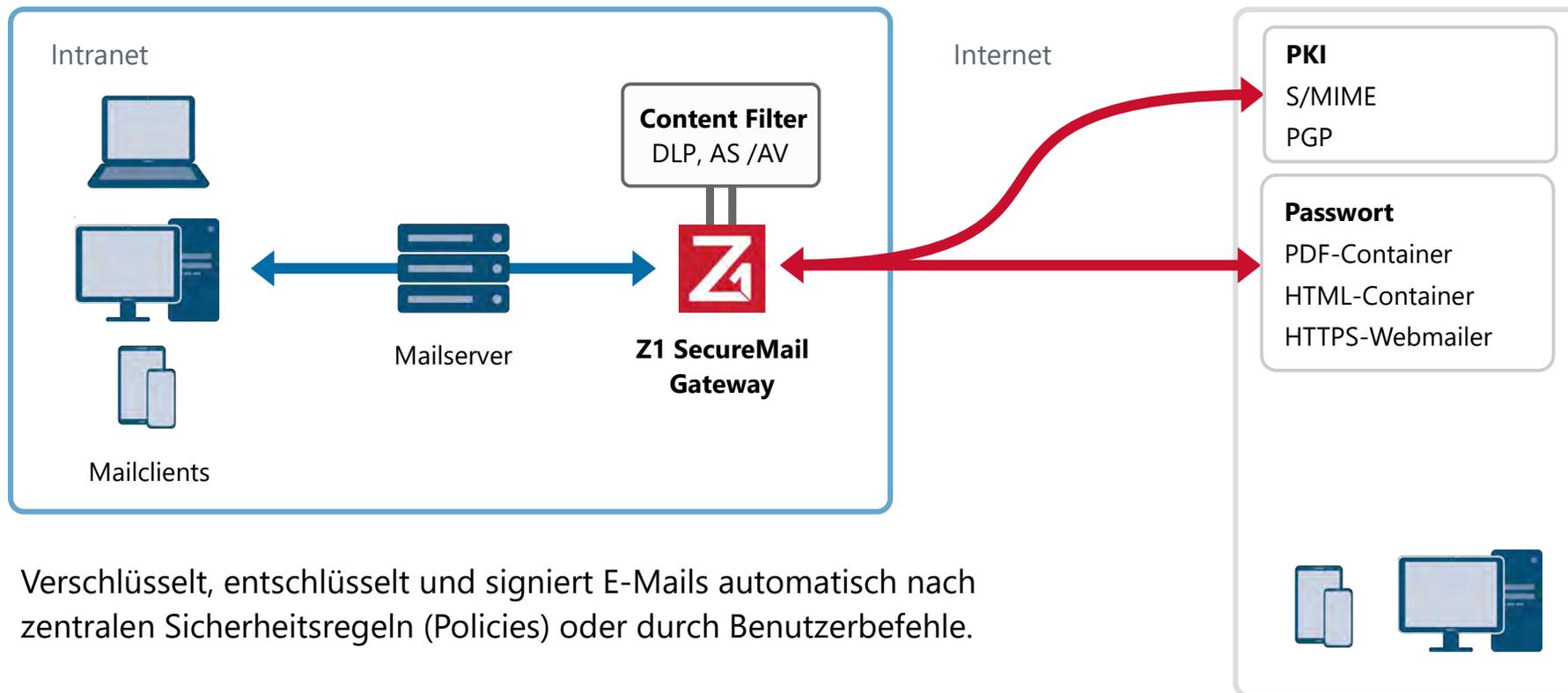
# PKI-Grundlagen – Elektronische Signatur



# Z1 Produkte

---

# Z1 SecureMail Gateway

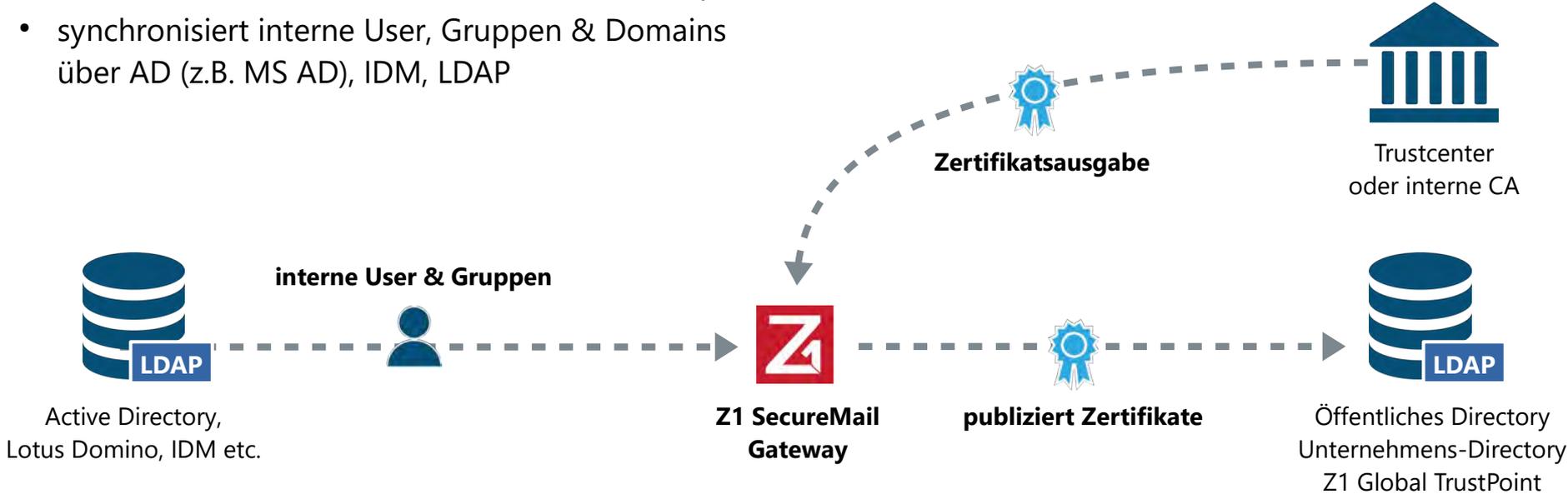


Verschlüsselt, entschlüsselt und signiert E-Mails automatisch nach zentralen Sicherheitsregeln (Policies) oder durch Benutzerbefehle.

 verschlüsselte E-Mails       unverschlüsselte E-Mails

# Z1 SecureMail Gateway – Internes User- & Zertifikatsmanagement

- erstellt und veröffentlicht Schlüssel-/Zertifikatspaare der Mitarbeiter
- synchronisiert interne User, Gruppen & Domains über AD (z.B. MS AD), IDM, LDAP



**Management der internen User,  
Gruppen & Domains**

**Schlüssel- / Zertifikatsmanagement  
der internen User**

# Anbindung der DFN TCS

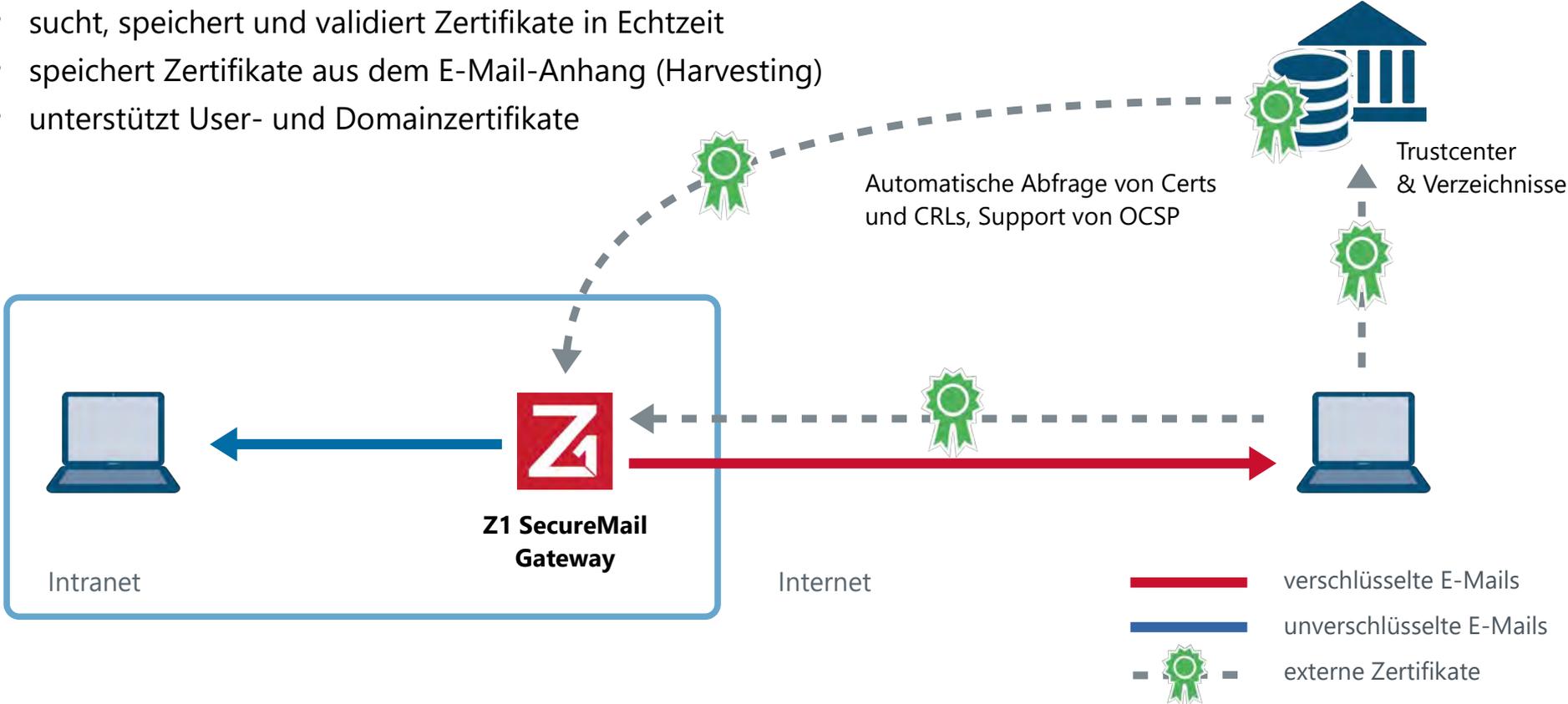
**Gültige Zertifikate**

**steven.hertel@studentenwerk-potsdam.de**  
 gültig ab 2022-10-11 bis 2023-10-11  
 Herausgegeben von GEANT Vereniging

<b>Besitzer</b>	Steven Hertel steven.hertel@studentenwerk-potsdam.de Studentenwerk Potsdam DE	<b>Herausgegeben von</b>	GEANT eScience Personal CA 4 GEANT Vereniging NL
<b>Zertifikatsignatur-Algorithmus</b>	SHA384WITHRSA		
<b>Public-Key-Algorithmus (Schlüssellänge)</b>	RSA (4096 bits)		
<b>Fingerabdruck (SHA256)</b>	91:F7:A8:5C:1C:22:9D:07:55:D2:72:F1:97:39:5F:4F:C0:4C:CF:3C:41:1E:88:BF:06:8B:EF:7D:E8:01:DE:00		
<b>Fingerabdruck (SHA1)</b>	E2:2E:20:76:2F:3F:F6:B0:FE:3E:79:77:52:D7:6A:F8:D6:BA:65:85		
<b>Seriennummer</b>	78:00:FD:F5:9A:C1:9B:3D:FC:F8:E2:50:68:C4:E3:8A		
<b>Schlüsselbenutzung</b>	Digitale Signatur, Schlüsselverschlüsselung		
<b>Gültig ab</b>	2022-10-11	<b>Gültig bis</b>	2023-10-11

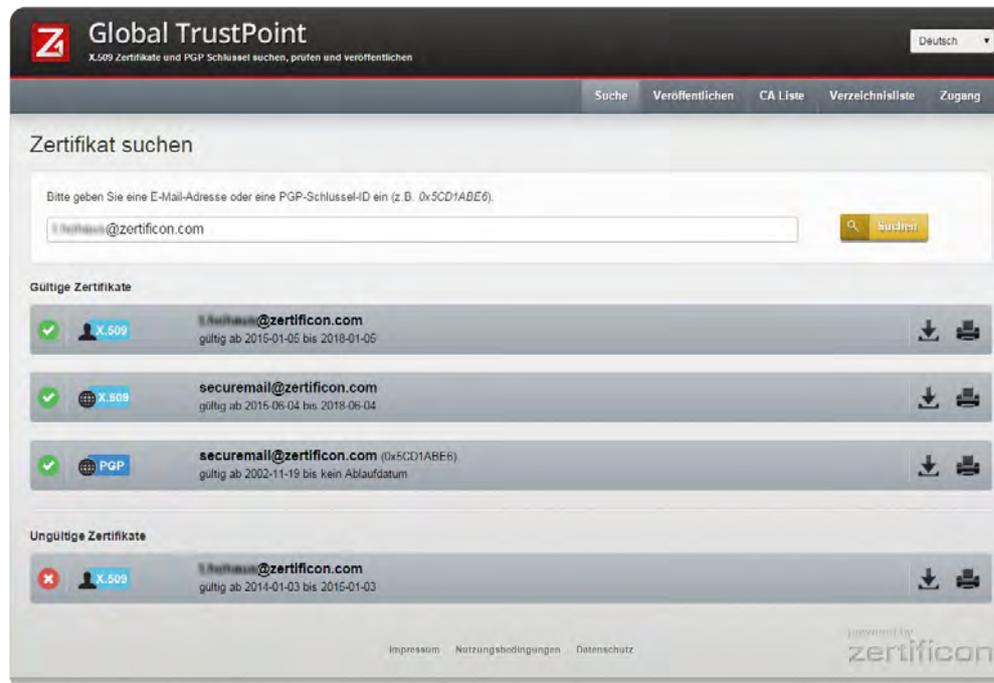
# Z1 SecureMail Gateway – Externes Zertifikatsmanagement

- sucht, speichert und validiert Zertifikate in Echtzeit
- speichert Zertifikate aus dem E-Mail-Anhang (Harvesting)
- unterstützt User- und Domainzertifikate



# Z1 Global TrustPoint & Certificate Portal

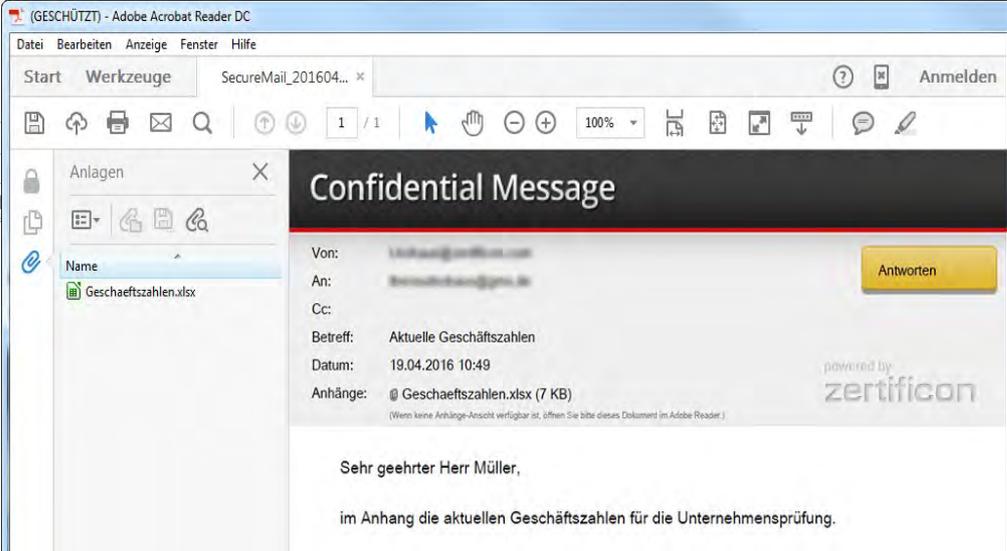
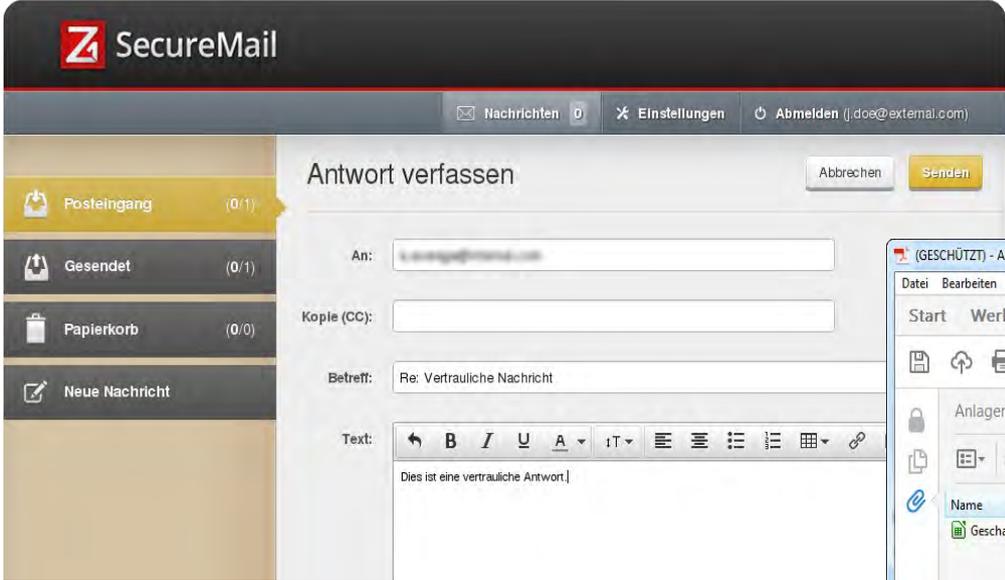
- Das maßgebende Zertifikatsportal im Internet für die Suche, Validierung und Veröffentlichung von Zertifikaten
- Metasuche in Verzeichnissystemen auf der ganzen Welt



<https://www.globaltrustpoint.com>

# Z1 SecureMail Gateway – Passwortbasierte Verschlüsselung

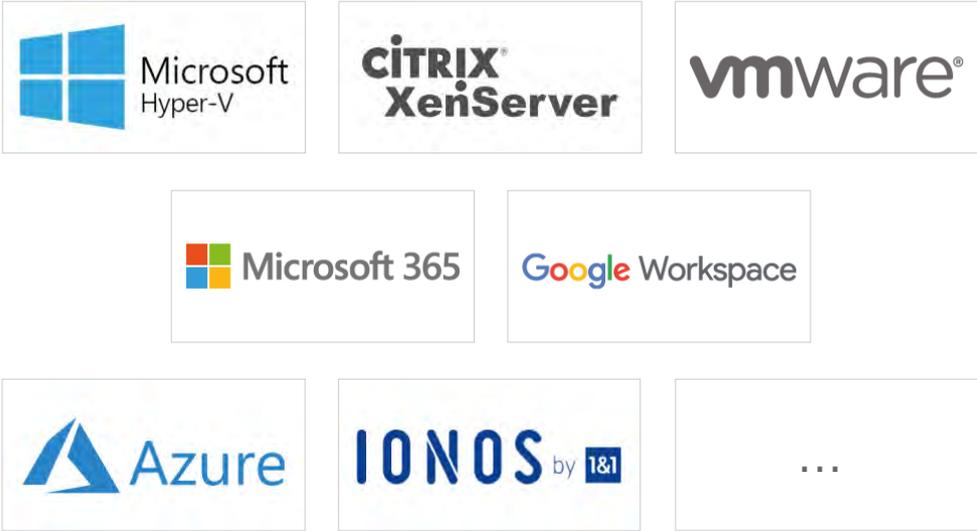
**Z1 WebSafe Account –**  
sicher antworten



**Z1 KickMail PDF**

# Betrieb von Z1 SecureMail Gateway

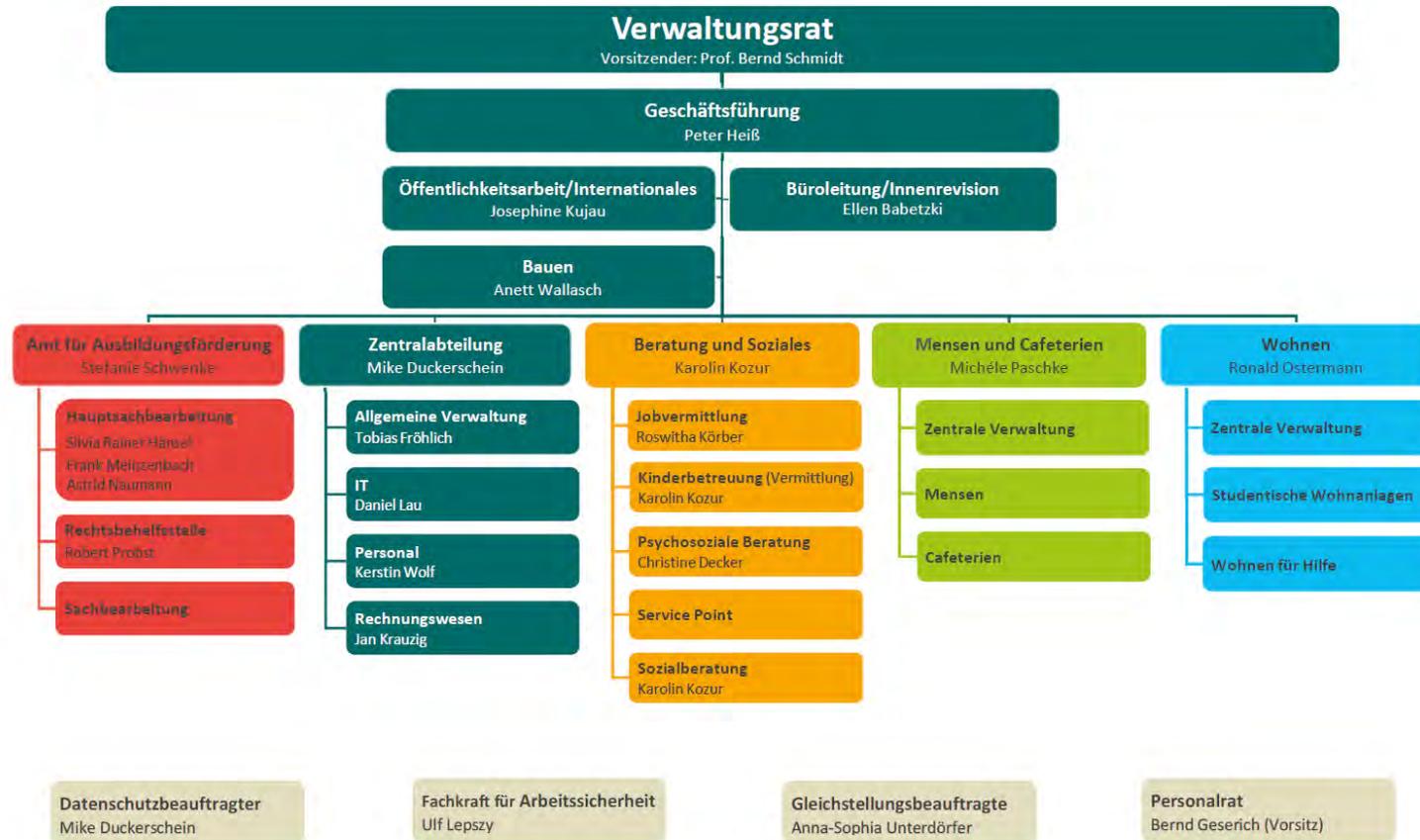
- wirtschaftlicher Betrieb auf Z1 Virtual Appliances
- kompatibel mit mit folgenden Virtualisierungsplattformen, Cloud Providern und Cloud Services
- schnell installiert & produktiv im Einsatz
- einfache Konfiguration und One-Click-Updates über das Admin-Portal



# Beispiel: Studentenwerk Potsdam

---

# Studentenwerk Potsdam - Vorstellung



# Herausforderungen der Verschlüsselung der E-Mails

– für das Studentenwerk Potsdam

Hohe Sicherheitsvorschriften

# Herausforderungen der Verschlüsselung der E-Mails

– für das Studentenwerk Potsdam

Hohe Sicherheitsvorschriften

Nicht IT-affine Anwender

# Herausforderungen der Verschlüsselung der E-Mails

– für das Studentenwerk Potsdam

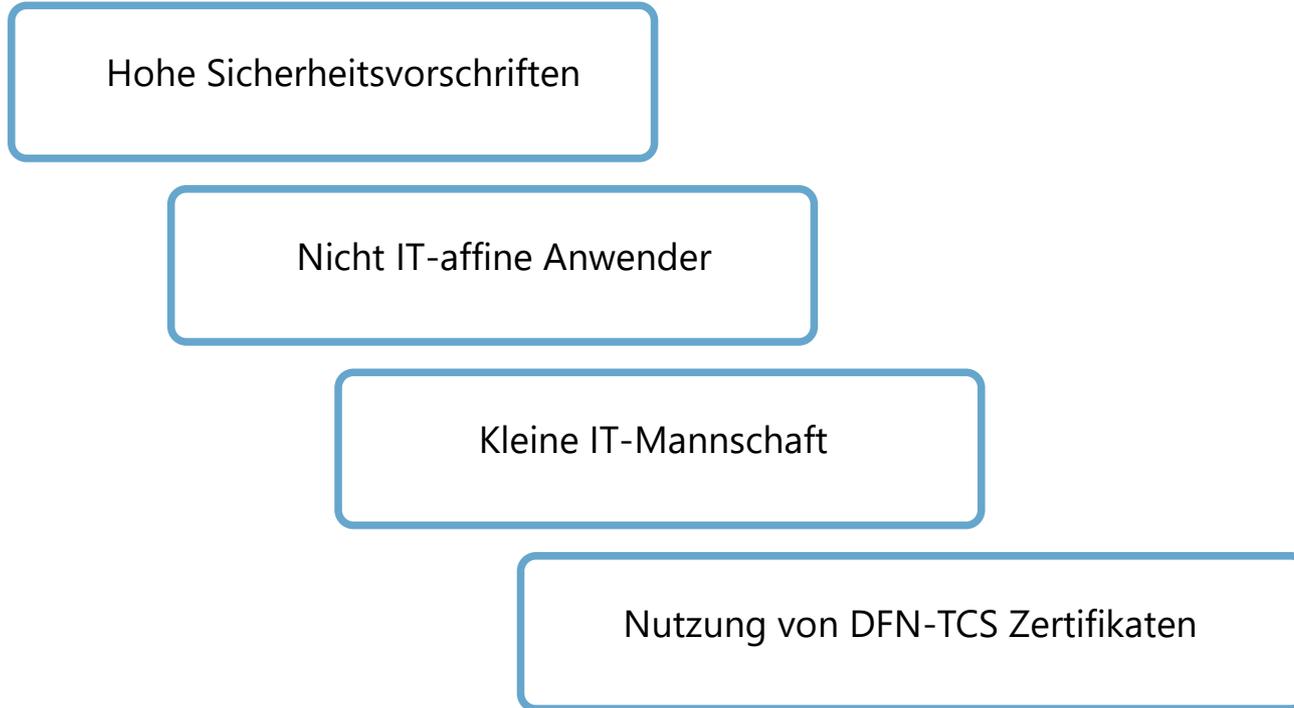
Hohe Sicherheitsvorschriften

Nicht IT-affine Anwender

Kleine IT-Mannschaft

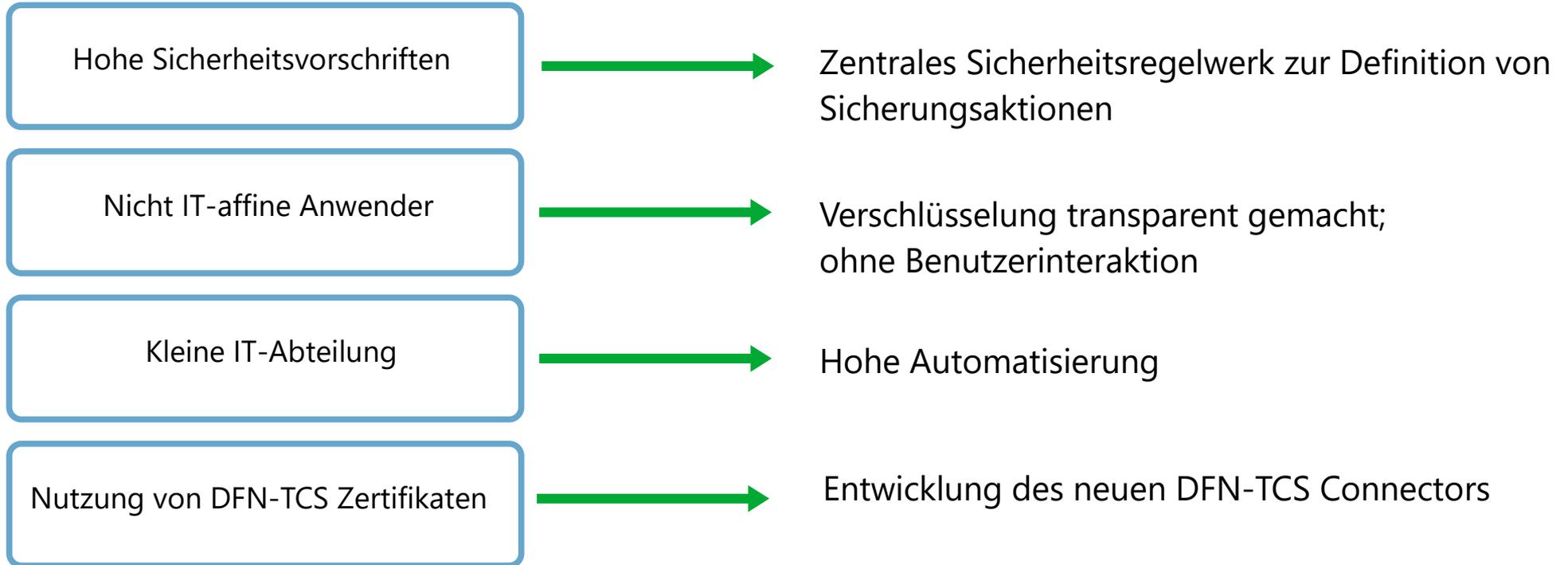
# Herausforderungen der Verschlüsselung der E-Mails

– für das Studentenwerk Potsdam



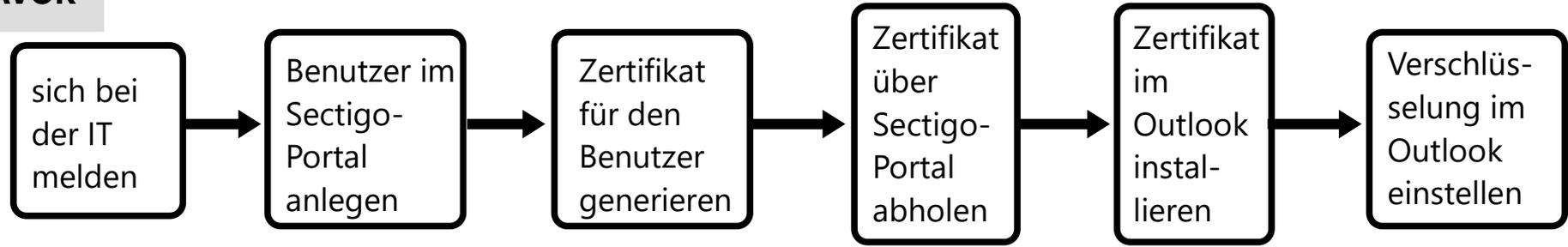
# Die Lösungen von Zertificon Solutions

– für das Studentenwerk Potsdam



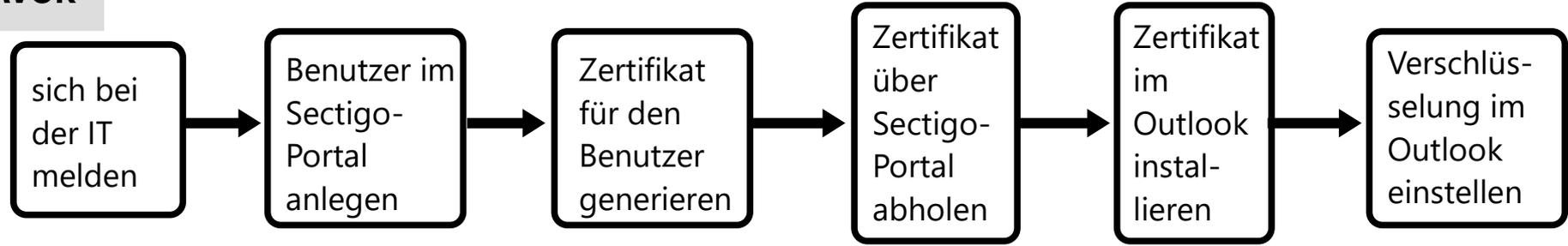
# Prozess der Einrichtung der E-Mail-Verschlüsselung vor der Automatisierung

DAVOR



# Prozess der Einrichtung der E-Mail-Verschlüsselung vor und nach der Automatisierung

## DAVOR



## DANACH



# **Bericht von Herrn Hertel,**

Projektmanager und IT-Systemadministrator  
Studentenwerk Potsdam  
Anstalt des öffentlichen Rechts

# Angebot an die Mitglieder des DFN

---

Für DFN Mitglieder unter Nennung der Mitgliedsnummer:

- Bei Bestellung in 2022: 50% Discount
- Bei Bestellung in Q1 2023: 30% Discount



**Vielen Dank für Ihre Aufmerksamkeit!**

Zertificon Solutions GmbH | Tel.: +49 30 5900 300-30 | [sales@zertificon.com](mailto:sales@zertificon.com) | [www.zertificon.com](http://www.zertificon.com)