



Nbjmwfstdimvfttfmvoh jn Voufsofinfo



Mailverschlüsselung im Unternehmen

Mailverschlüsselung im Unternehmen

Agenda

- Vorstellung
- Grundbegriffe
- Anforderungen an die eingesetzte Lösung
- Unser Partner für Mailverschlüsselung
- Einbindung in Ihre IT

Mailverschlüsselung im Unternehmen

Vorstellung

- Frank Agerholm
- Seit 2015 bei NetUSE AG
- TEC Infrastructure Team
- System Engineer mit Schwerpunkt Linux

Mailverschlüsselung im Unternehmen

Warum eigentlich Mails verschlüsseln ???

- Einhaltung von gesetzlichen Datenschutzvorschriften
 - „... geeignete technische und organisatorische Sicherheitsvorkehrungen ...“
- Wahrung der Privatsphäre oder der Geheimhaltung
- Sicherstellung der Integrität des Mail-Inhaltes

Mailverschlüsselung im Unternehmen

Grundbegriffe

Verschlüsselung

- Die Verschlüsselung ist die Umsetzung einer verständlichen Information (Klartext) in eine unverständliche (Geheimtext)
- Angreifer sollen die Originalinhalte nicht gewinnen können, wenn sie die verschlüsselten Informationen in die Hände bekommen
- Für das Ver- bzw. Entschlüsseln werden Schlüssel verwendet
- Die Verschlüsselung kann auf unterschiedliche Arten erfolgen
 - Symmetrisch
 - Absender und Empfänger benutzen den gleichen Schlüssel
 - Asymmetrisch
 - Absender und Empfänger benutzen unterschiedliche Schlüssel
 - Jeder Schlüssel besteht dabei aus einem Private- und einem Public-Key

Mailverschlüsselung im Unternehmen

Transportverschlüsselung vs. End2End

- Absender schickt per verschlüsselter Verbindung seine Mail
- Empfänger holt per verschlüsselter Verbindung seine Mail ab
- Aber wurde die Mail zwischen den Mailservern auch verschlüsselt übertragen ???

Mailverschlüsselung im Unternehmen

Digitale Signatur

- Mit Hilfe der Signatur kann der Empfänger die Integrität einer Nachricht überprüfen
- Signaturen setzen asymmetrische Schlüssel voraus
- Die Signatur wird mit dem Private-Key erzeugt...
- ... und mit Hilfe des Public-Keys verifiziert

Mailverschlüsselung im Unternehmen

Digitales Zertifikat

- Das digitale Zertifikat ist ein Dokument, mit dem Eigenschaften von Personen bestätigt werden
- Durch eine digitale Signatur kann die Authentizität und Integrität des Zertifikats geprüft werden
- Weit verbreitet sind X.509 Zertifikate, wie sie auch für Webserver verwendet werden

Mailverschlüsselung im Unternehmen

Beispiel eines digitalen Zertifikats

- Name des Ausstellers:
SwissSign Personal Gold CA 2014 – G22
- Ausgestellt für:
Frank Agerholm, fae@netuse.de,
NetUSE Aktiengesellschaft, Kiel, DE
- Gültig für den Schlüssel mit dem Fingerabdruck:
5F:C2:27:7D:F4:41:26:C2:4A:C9:F1:77:90:0D:FB:83:4E:B3:B4:0A
- Gültig ab:
06.12.2017
- Gültig bis:
06.12.2018



Mailverschlüsselung im Unternehmen

Das Problem der Zertifikatsverifizierung

- Ein Zertifikat ist digital signiert
- Henne-Ei-Problem
 - Wie überprüfe ich diese Signatur ???

Das Problem der Zertifikatsverifizierung

Trustcenter

- Trustcenter überprüfen die Identität von Personen oder Unternehmen und bestätigen diese mit einem digitalen Zertifikat
 - Die Trustcenter werden auch Certification Authority (CA) genannt.
- Eine Root CA ist die oberste Stelle in einer Zertifikatshierarchie
 - es gibt mehrere davon...
- Sub-CAs können verwendet werden, um CAs aufzugliedern
- Beispiel:
 - WebUSE Root CA
 - WebUSE VPN CA
 - WebUSE Mail CA
- Jedes Betriebssystem liefert bereits eine große Anzahl Root-Zertifikate mit
- Eigene CAs können im Unternehmen verwendet werden

Anforderungen an die eingesetzte Lösung

Mailverschlüsselung im Unternehmen

Anforderungen an die eingesetzte Lösung

- Ausgehende Mails sollen verschlüsselt und signiert werden
- Eingehende Mails sollen entschlüsselt und die Signatur überprüft werden
- Einfache Anwendung für den Benutzer
 - Keine aufwendige Suche nach öffentlichen Schlüsseln
 - Möglichst große Auswahl an verwendbaren Mailprogrammen
- Geringer Betriebsaufwand
- Rechtskonforme Archivierung der Mails soll möglich sein
- Ohne Mailverschlüsselung beim Kommunikationspartner soll sichere Übertragung möglich sein

Mailverschlüsselung im Unternehmen

Unser Partner für Mailverschlüsselung

Mailverschlüsselung im Unternehmen

Powered by Zertificon

zertificon[®]
Easy. Secure. Encrypted.

SecureMail Gateway



- Zertificon Solutions GmbH mit Sitz in Berlin
- Seit 2004 mit zentraler Mailverschlüsselung am Markt
- Im deutschen Markt weit verbreitet

Mailverschlüsselung im Unternehmen

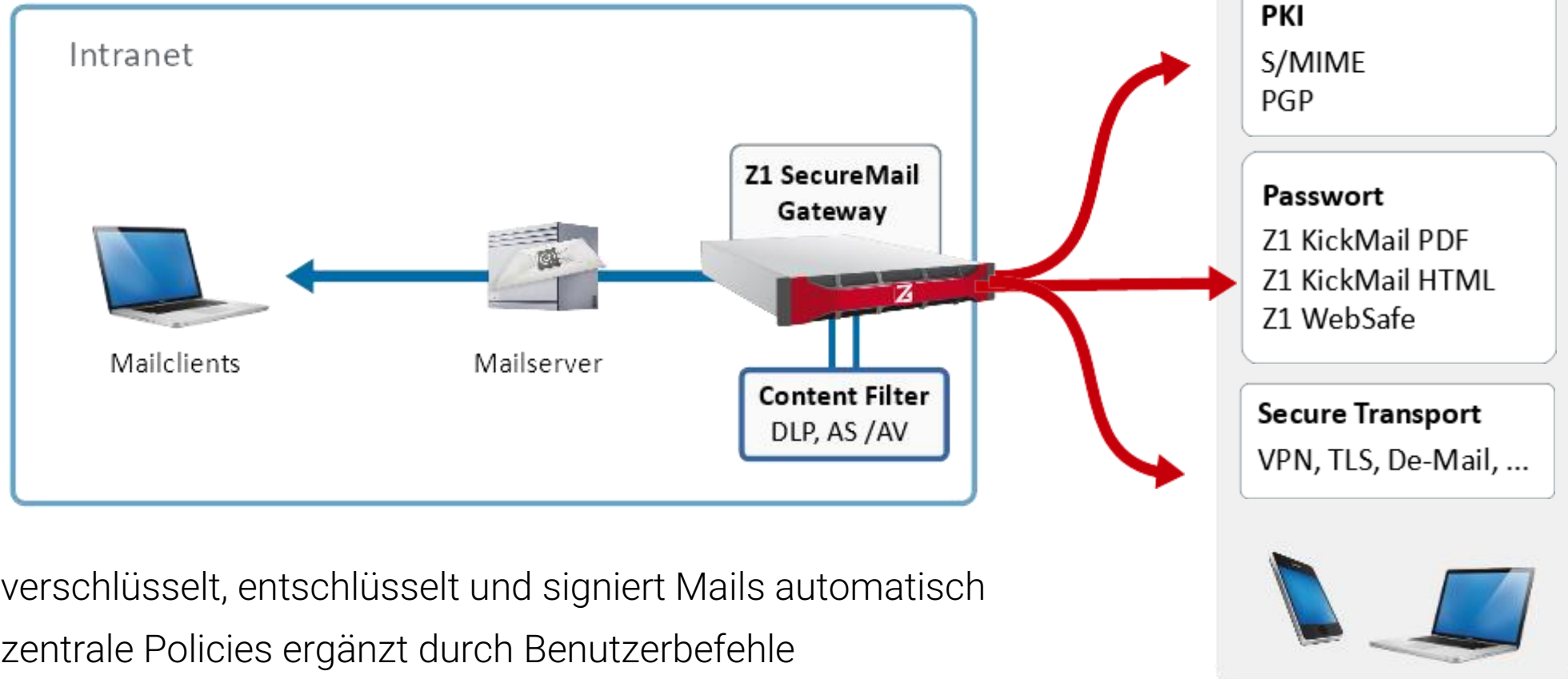


zertificon[®]
Easy. Secure. Encrypted.

Einbindung in Ihre IT

Mailverschlüsselung im Unternehmen

Einbindung am Firmengateway

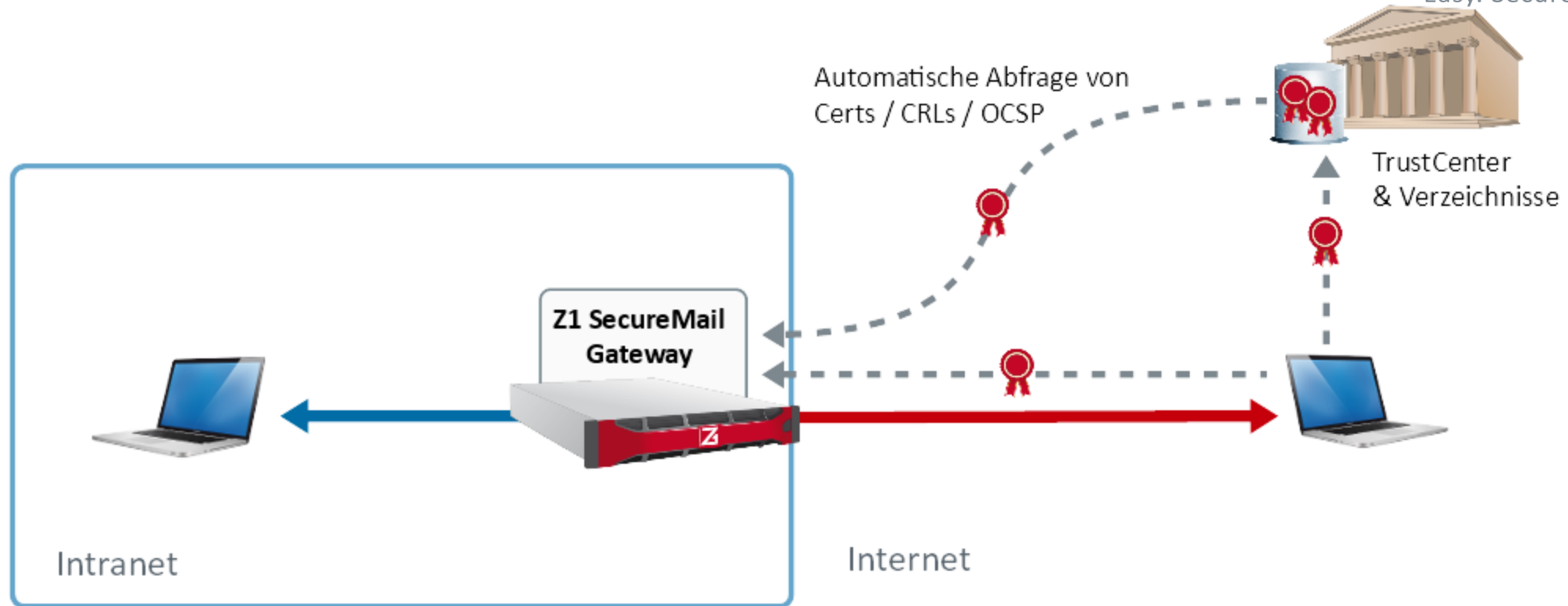


- verschlüsselt, entschlüsselt und signiert Mails automatisch
- zentrale Policies ergänzt durch Benutzerbefehle
- verwaltet interne & externe Schlüssel und Zertifikate

— verschlüsselte E-Mails
— unverschlüsselte E-Mails

Mailverschlüsselung im Unternehmen

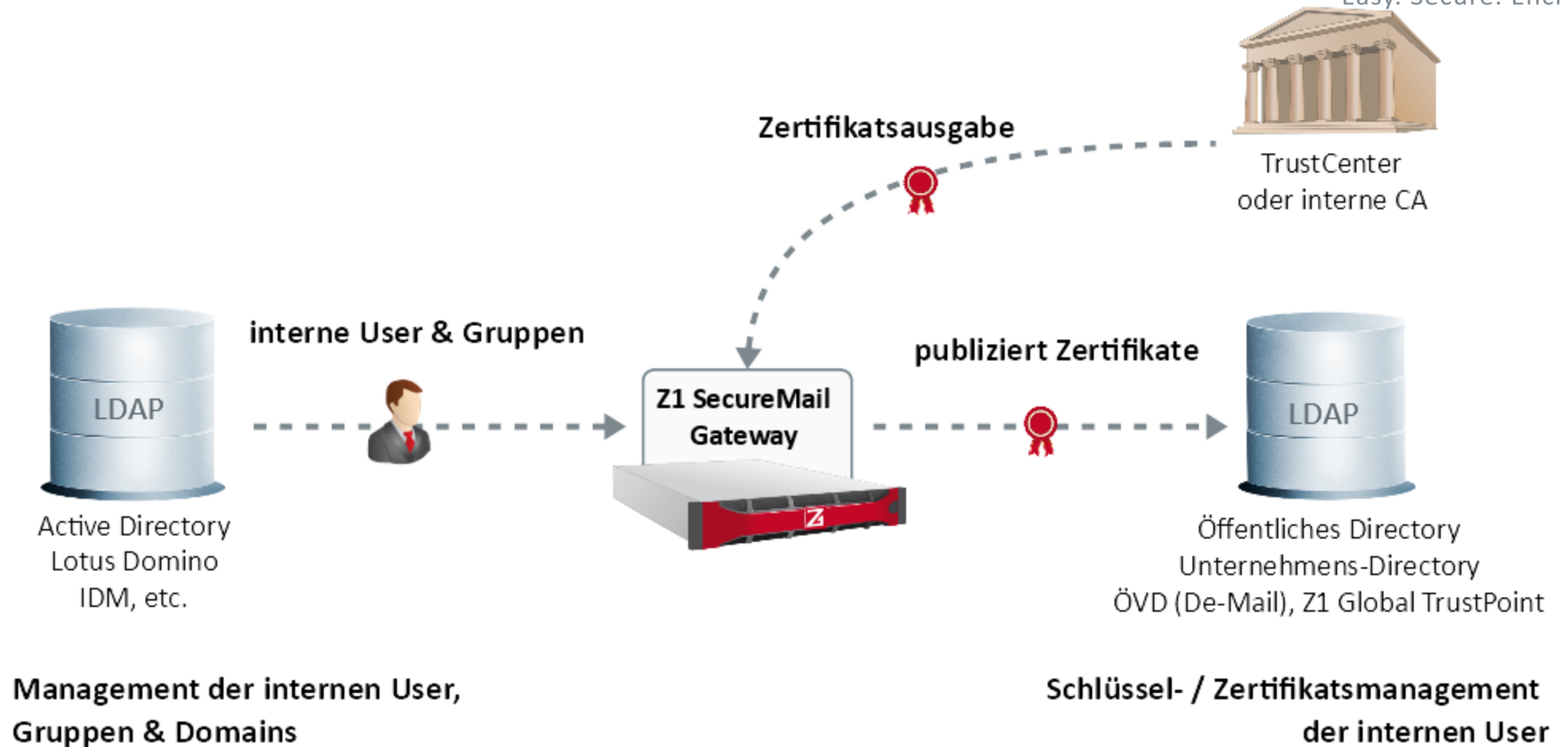
Automatische Suche nach Zertifikaten



- sucht, speichert und validiert Zertifikate in Echtzeit
- speichert Zertifikate aus dem Mail-Anhang

Mailverschlüsselung im Unternehmen

Benutzer- und Zertifikatsmanagement



Mailverschlüsselung im Unternehmen

www.globaltrustpoint.com



zertificon[®]
Easy. Secure. Encrypted.

The screenshot shows the Global TrustPoint website interface. At the top, there is a navigation bar with the Global TrustPoint logo and the text "Search for, validate and publish X.509 certificates and PGP keys". A language dropdown menu is set to "English". Below the navigation bar, there are tabs for "Search", "Publish", "CA List", "Repository List", and "Access". The main content area is titled "Search certificate" and contains a search input field with the placeholder text "Please enter an e-mail address or a PGP key ID (e.g. 0x5CD1ABE6)". The input field contains the email address "fao@netuse.de" and a "Search" button. Below the search input, there is a section titled "Valid Certificates" and "Indeterminate Certificates". The "Valid Certificates" section shows a single entry for "fao@netuse.de" with a green checkmark icon, an "X.509" label, and the text "valid from 2017-12-06 until 2018-12-06". The "Indeterminate Certificates" section shows a single entry for "fao@netuse.de (0x8E2D309E)" with a question mark icon, a "PGP" label, and the text "valid from 2016-04-21 until 2021-04-20". At the bottom of the page, there are links for "Contact", "Terms Of Use", and "Privacy Statement", and a "powered by zertificon" logo.

Mailverschlüsselung im Unternehmen

Z1 Secure Messenger



- Zugriff auf die Nachrichten über eine https-Verbindung mit dem Browser

Mailverschlüsselung im Unternehmen



zertificon[®]
Easy. Secure. Encrypted.

Portfolio der NetUSE AG

Mailverschlüsselung im Unternehmen

Portfolio der NetUSE AG



zertificon[®]
Easy. Secure. Encrypted.

- Managed Zertificon
 - geclustert in den Rechenzentren der NetUSE AG
 - Anbindung an Active Directory und Mailserver des Kunden möglich
 - Abrechnung nach Anzahl aktiver Benutzerlizenzen pro Monat
 - Nur in Verbindung mit NetUSE Mailrelay
 - Kombinierbar mit
 - NetUSE Threat Emulation E-Mail
 - NetUSE Virus-Scan-E-Mail
 - NetUSE Spam-Filter
 - NetUSE Service-Zone
- Consulting bei der Einführung
- Betrieb dedizierter Appliances für Kunden

Mailverschlüsselung im Unternehmen



zertificon[®]
Easy. Secure. Encrypted.

Vielen Dank für Ihre Zeit! Dürfen wir noch Fragen beantworten?