



präsentiert

Z1 SecureMail

Deutschlands fleissigste Virtuelle Poststelle

IKS – Security - Breakfast

17. Juni 2009

Zertificon Solutions entwickelt und vertreibt Software, die den Einsatz von Sicherheitstechnologien wie Verschlüsselung, elektronische Signatur und Zertifikatsverwaltung vereinfacht.

Die IT-Security-Produkte richten sich an professionelle Anwender in Unternehmen und Institutionen und zeichnen sich durch komfortable Bedienung und optimalen Administrationsaufwand aus.

Das Kern-Produkt Z1 SecureMail Gateway schützt den kompletten eMail-Verkehr einer Organisation durch zentrale Verschlüsselung und elektronische Signatur.

Gründung des Unternehmens:	1998
Beginn der Entwicklung des Systems:	1999
Markteinführung des Systems:	2001
Auszeichnungen:	„Best Product of Internet World 2002“ „IT-Sicherheitspreis NRW 2005“

Anzahl Mitarbeiter: 25

- Geschäftsführung: 2
- Vertrieb / Marketing: 5
- Professional Service: 6
- Entwicklung/Q-Mgmt.: 9
- Verwaltung: 3

Service / Support standardmäßig ...

- von 9 – 18 Uhr, Mo bis Fr
- mit 4 Stunden Reaktionszeit
- von qualifiziertem Personal

Wer liest Ihre eMail?



Elektronische Post ist heute

- Basis der Geschäftskommunikation
- schnell
- weltweit akzeptiert
- kostengünstig



aber **unsicher !!!**

- illegales Lesen
- illegales Ändern
- illegales Absendervortäuschen



ist bei Internet-eMail sehr einfach möglich

KonTraG, TKG und BDSG – Rechtliche Vorgaben für die IT-Sicherheit im Unternehmen



KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)

- Führt mit § 91 Abs. 2 AktG zu einer rechtlichen Verpflichtung zur Etablierung effektiver IT-Sicherheitsstrukturen
- Persönliche Haftung der Vorstände für Schäden aufgrund fehlender oder mangelhafter IT-Sicherheit

TKG (Telekommunikationsgesetz)

- § 88 TKG verpflichtet zur Wahrung des Fernmeldegeheimnisses

BDSG (Bundesdatenschutzgesetz)

- Datenverarbeiter sind aufgrund § 9 BDSG zur Herstellung von Sicherheitsstrukturen verpflichtet

Basel II und SOX – Wirtschaftliche Notwendigkeiten



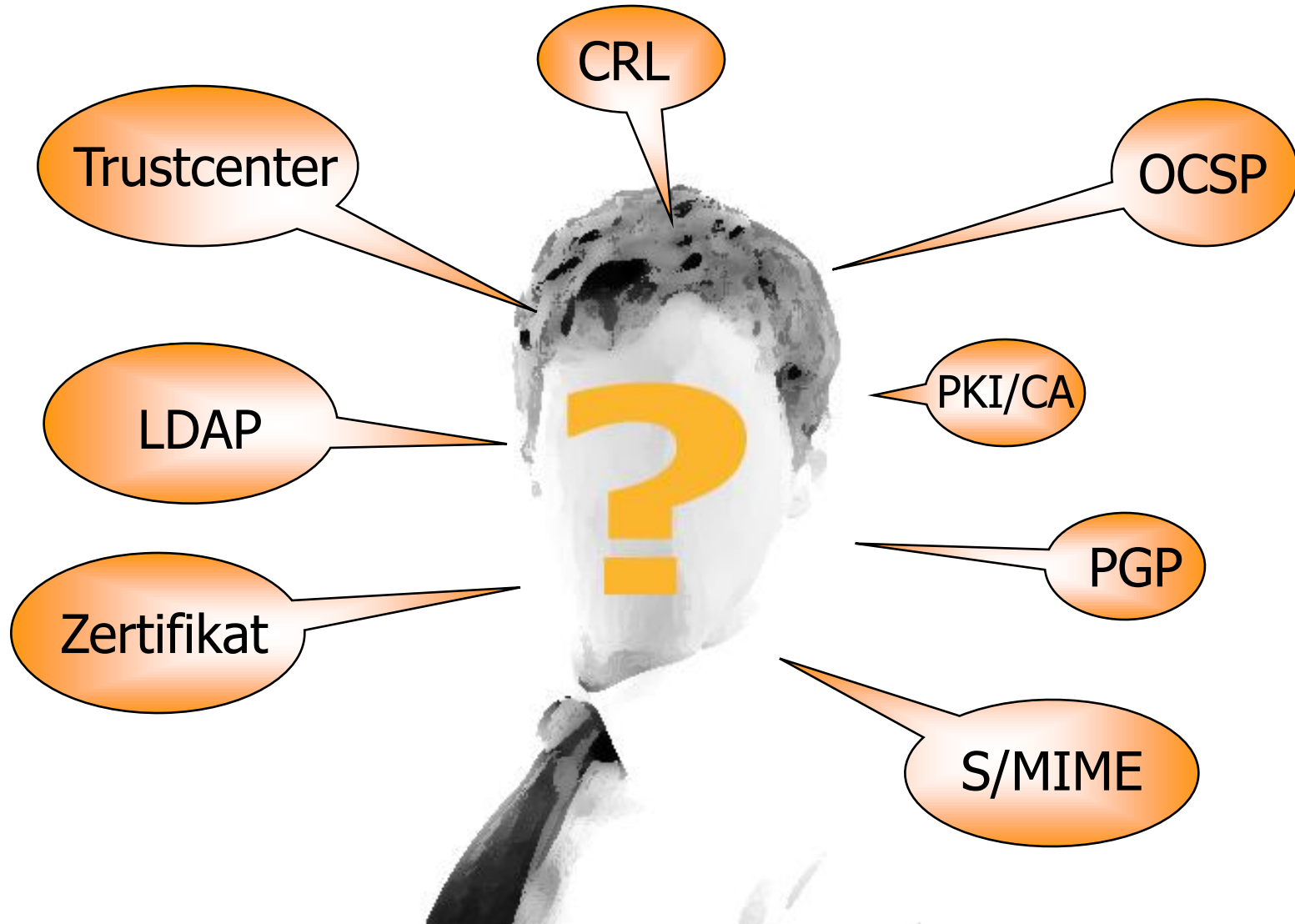
Basel II - Vorschläge des Baseler Ausschusses für Bankenaufsicht

- Nach den Vorschlägen von Basel II soll der für einzelne Bankkredite zu hinterlegende Betrag nach dem Ausfallrisiko im Einzelfall bemessen werden.
- Die Ermittlung des operativen Risikos eines Unternehmens erfasst auch IT-Sicherheitsspezifische Risikoeinschätzungen
- Ergebnis = je höher der belegbare IT-Sicherheits-Level, umso bessere Kreditkonditionen bei der Darlehensvergabe

SOX (Sarbanes Oxley Act)

- Compliance mit SOX setzt hohe Maßstäbe an Transparenz und Kontrollierbarkeit der Unternehmens-IT

Konventionelle eMail-Sicherheit mit PKI: zu komplex für Endanwender



Konventionelle eMail-Sicherheit mit PKI: zu aufwändig für Unternehmen



Die innovative, einfache Lösung: Z1 SecureMail Gateway + Messenger



Standardfunktionen:

- eMail-Verschlüsselung
- Elektronische Signatur von eMails
- eMail-Auslieferung über HTTPS

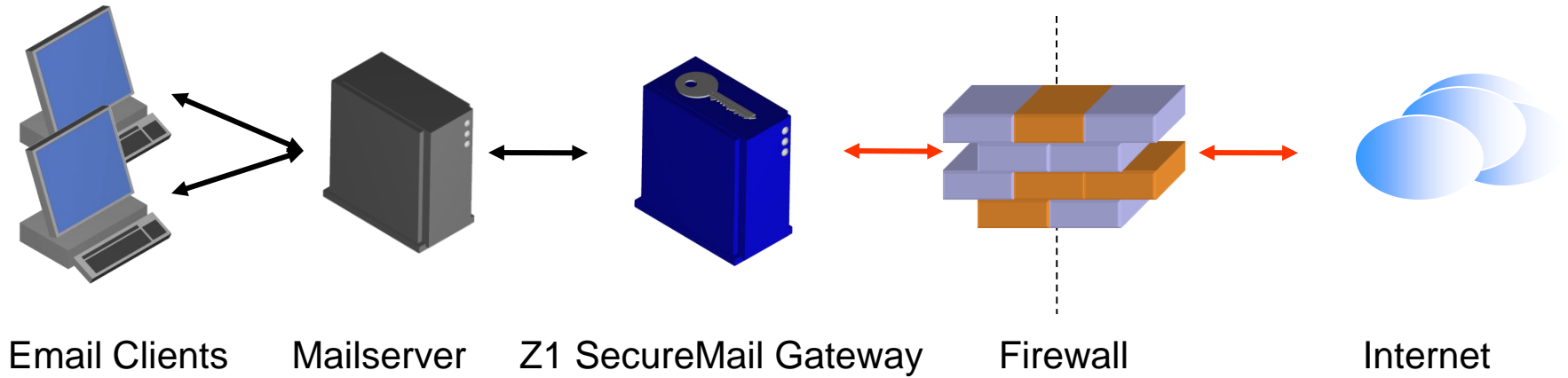
Produkterweiterungen (optional):

- Z1 SecureMail Enterprise Extension
- Z1 SecureMail ERP Connector
- Z1 SecureMail CA Connector
inkl. AutoCA
- Z1 SecureMail HSM Connector

Erweiterungen auf Projektbasis:

- Massen-Signatur („qualifizierte“ nach SigG)
- gesetzeskonforme Zeitstempel (RFC3161)
- ERP bzw. HR Integration
- PKI/CA (Realisierung und Anbindung)
- revisionssichere Protokollierung
- ... andere auf Anfrage

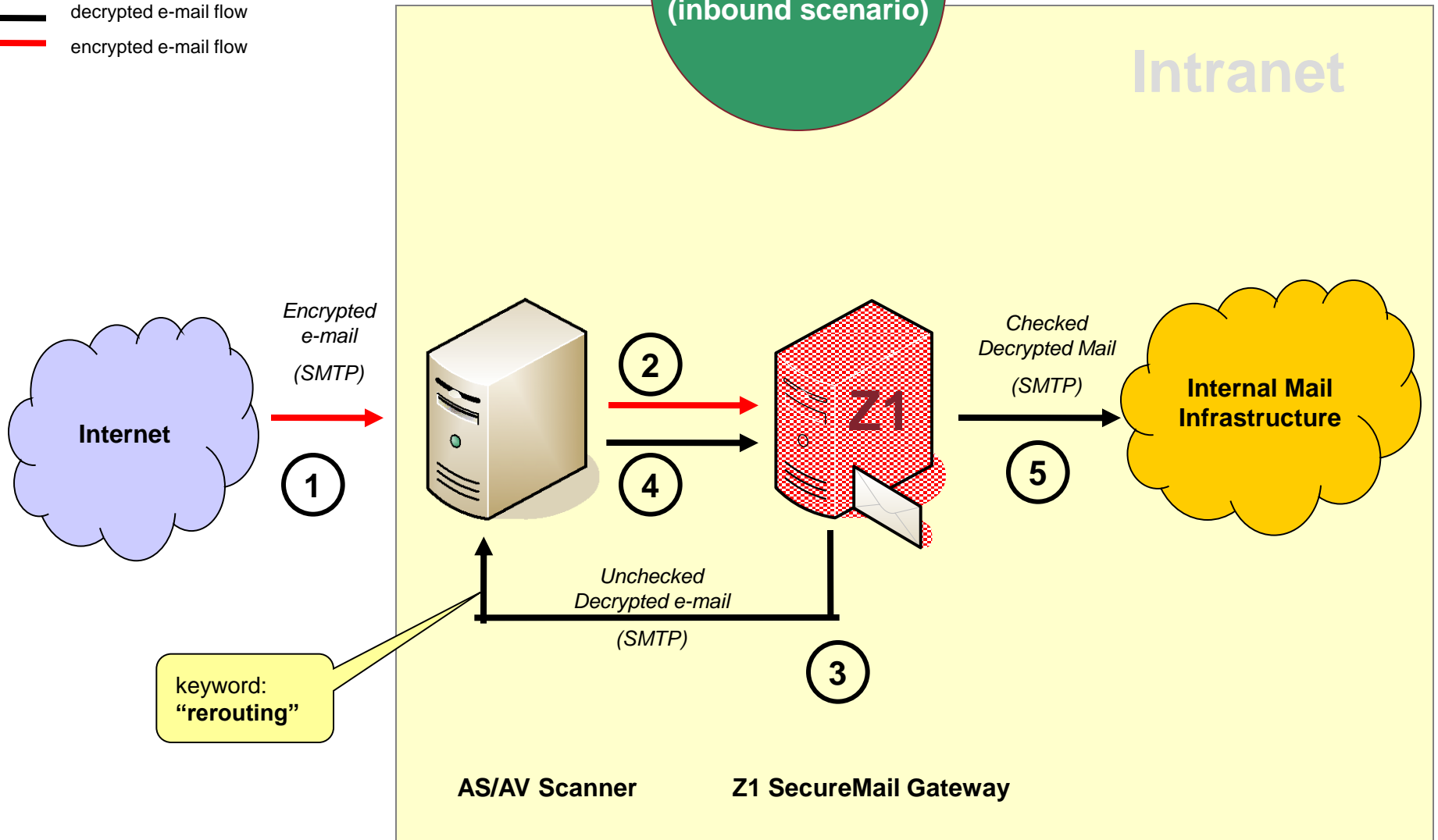
- **SMTP-Proxy**

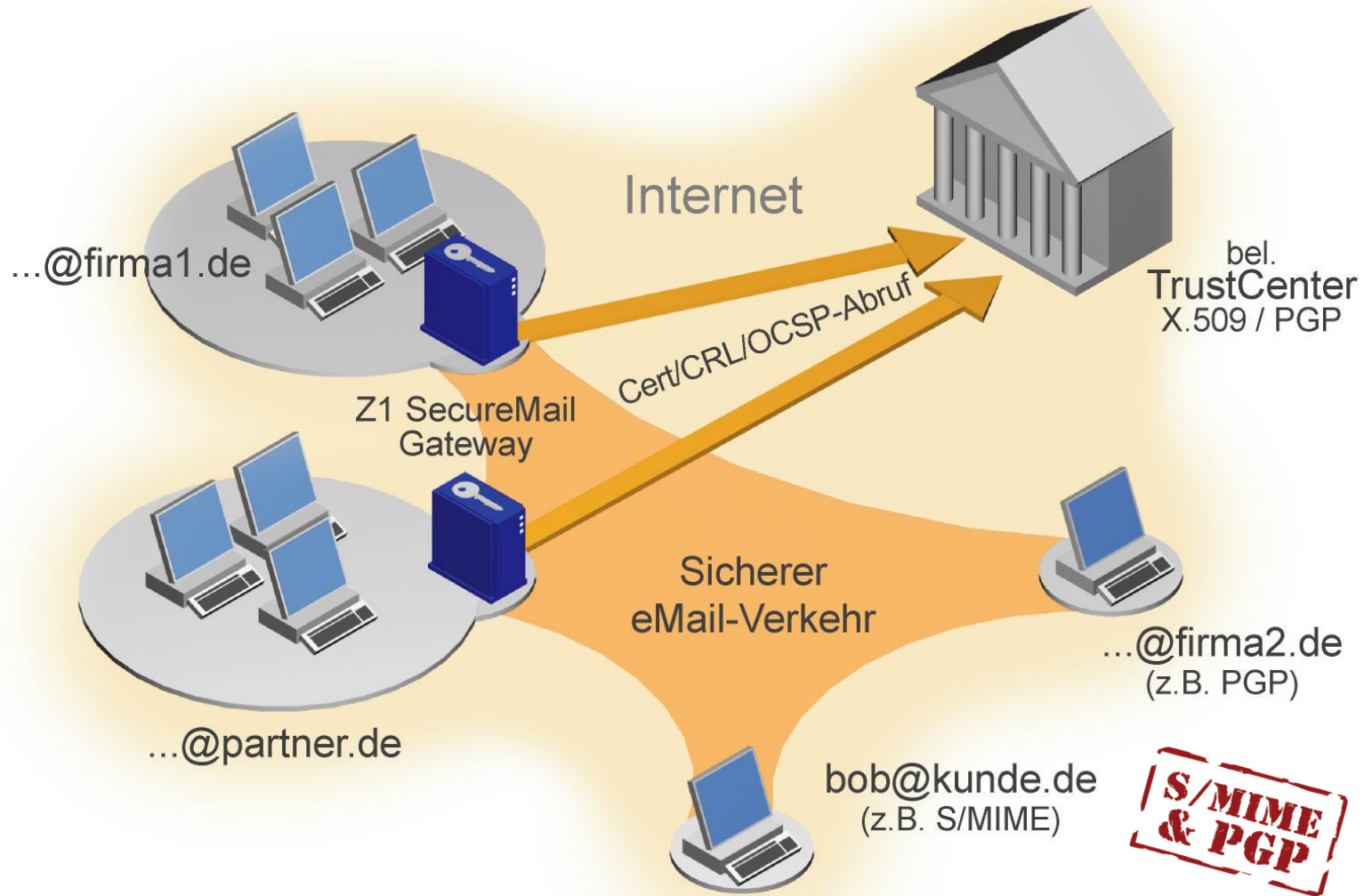


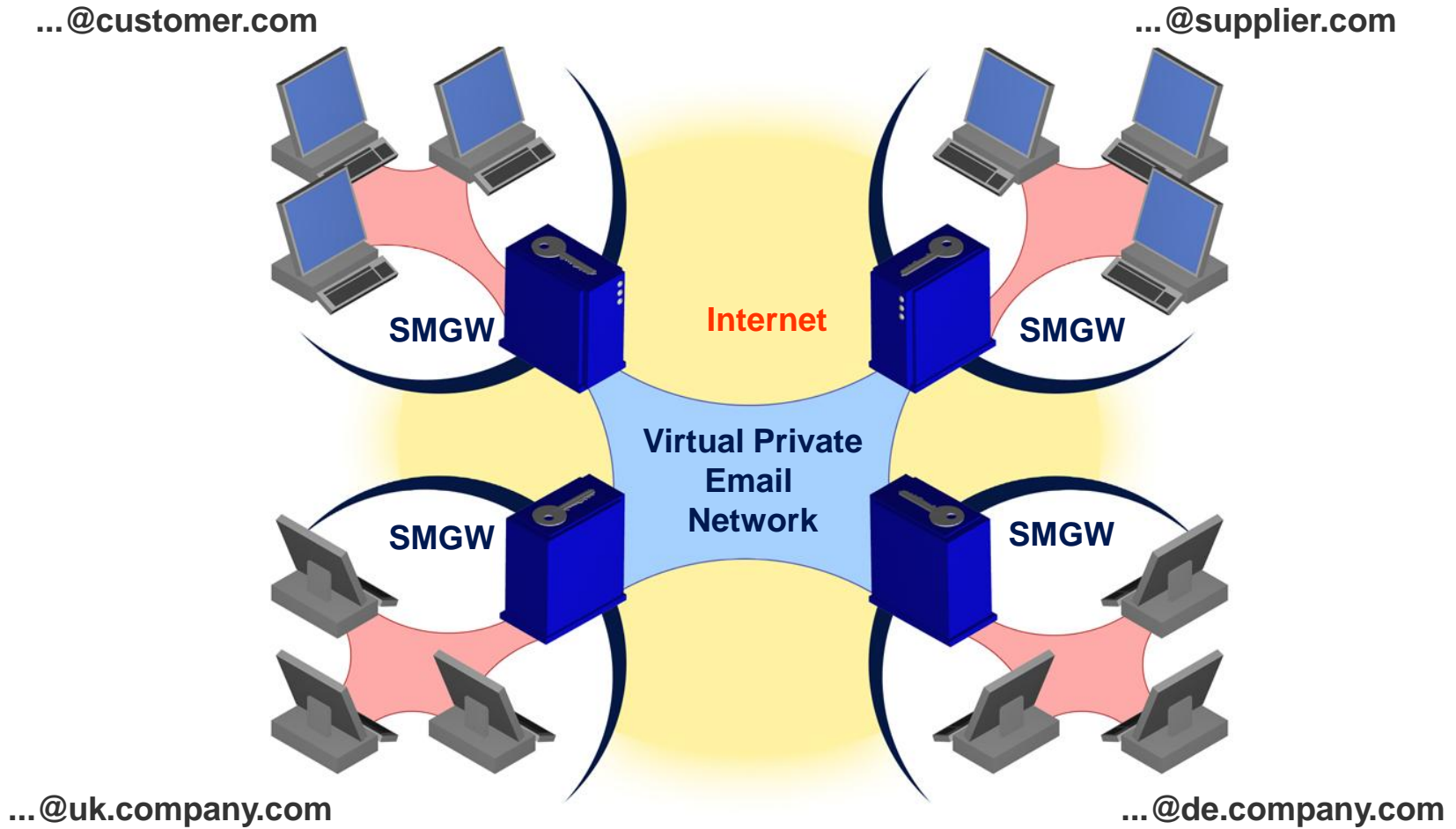
AS/AV Integration

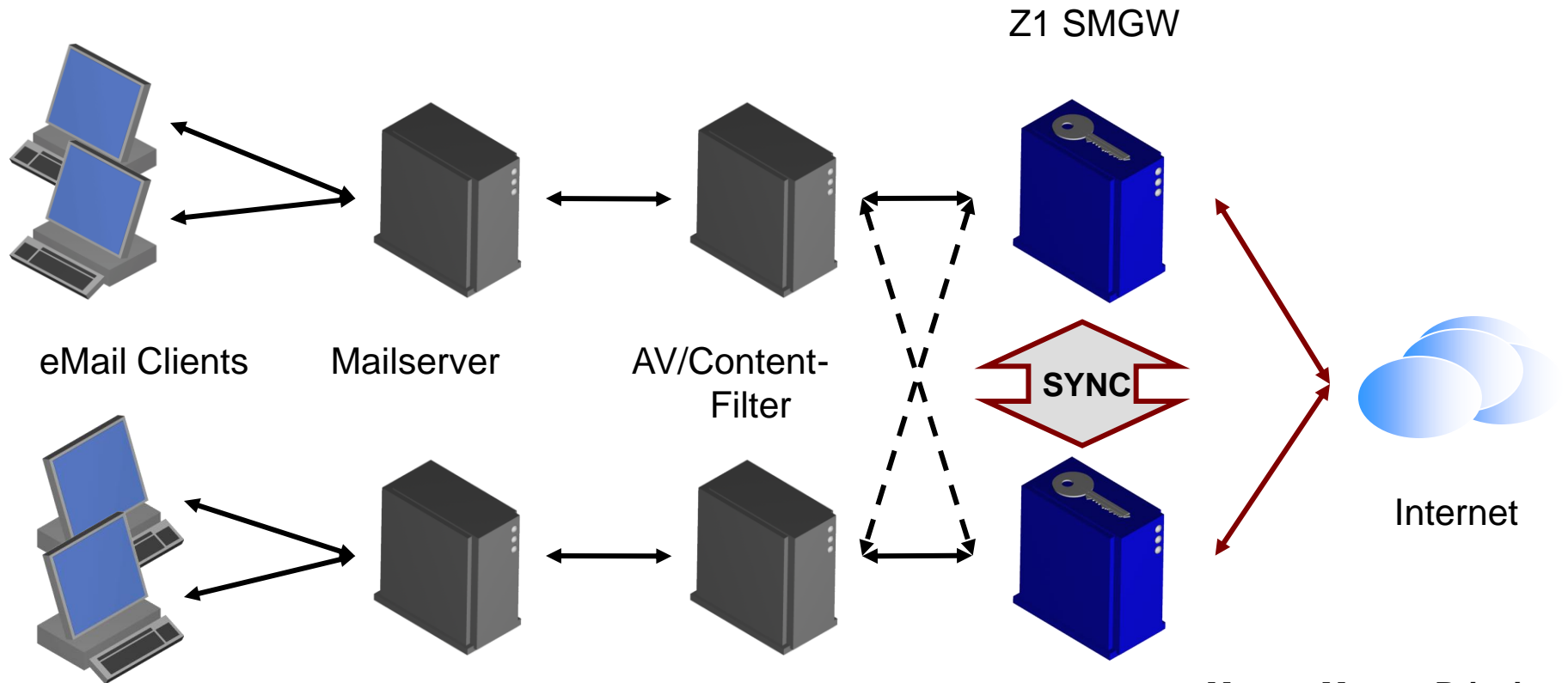
AS/AV scanning
between Internet
and Z1 SecureMail
(inbound scenario)

— decrypted e-mail flow
— encrypted e-mail flow

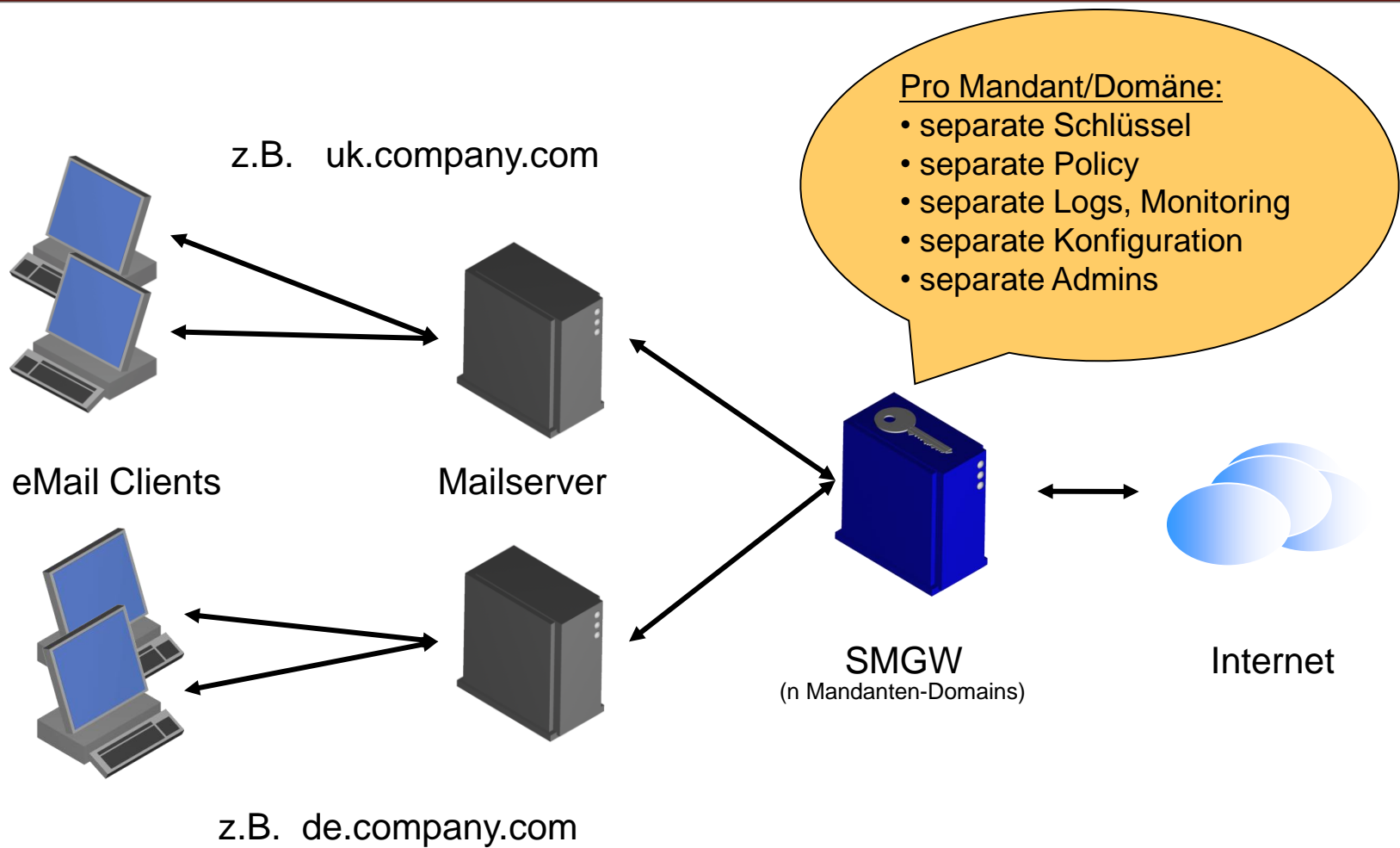




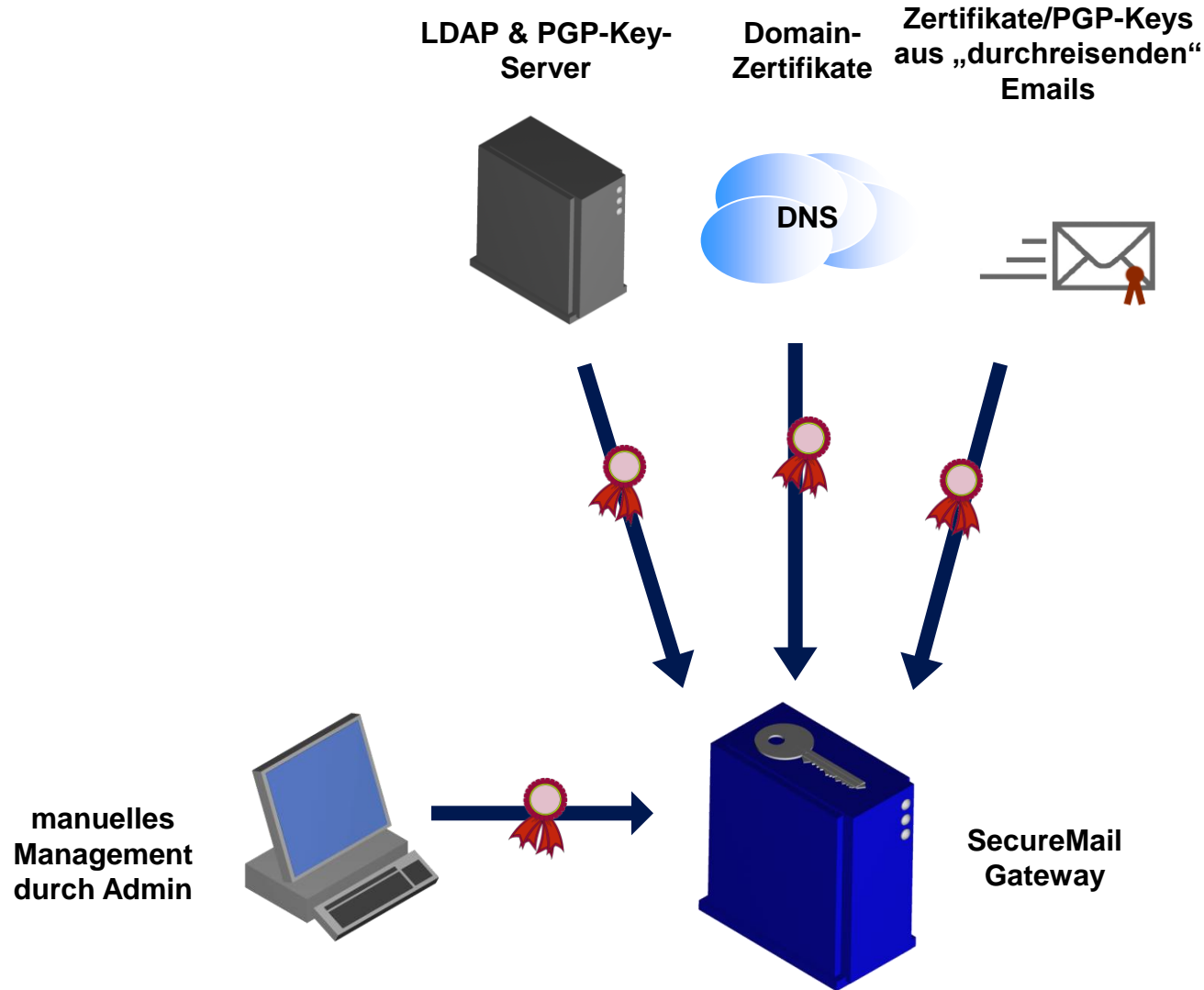




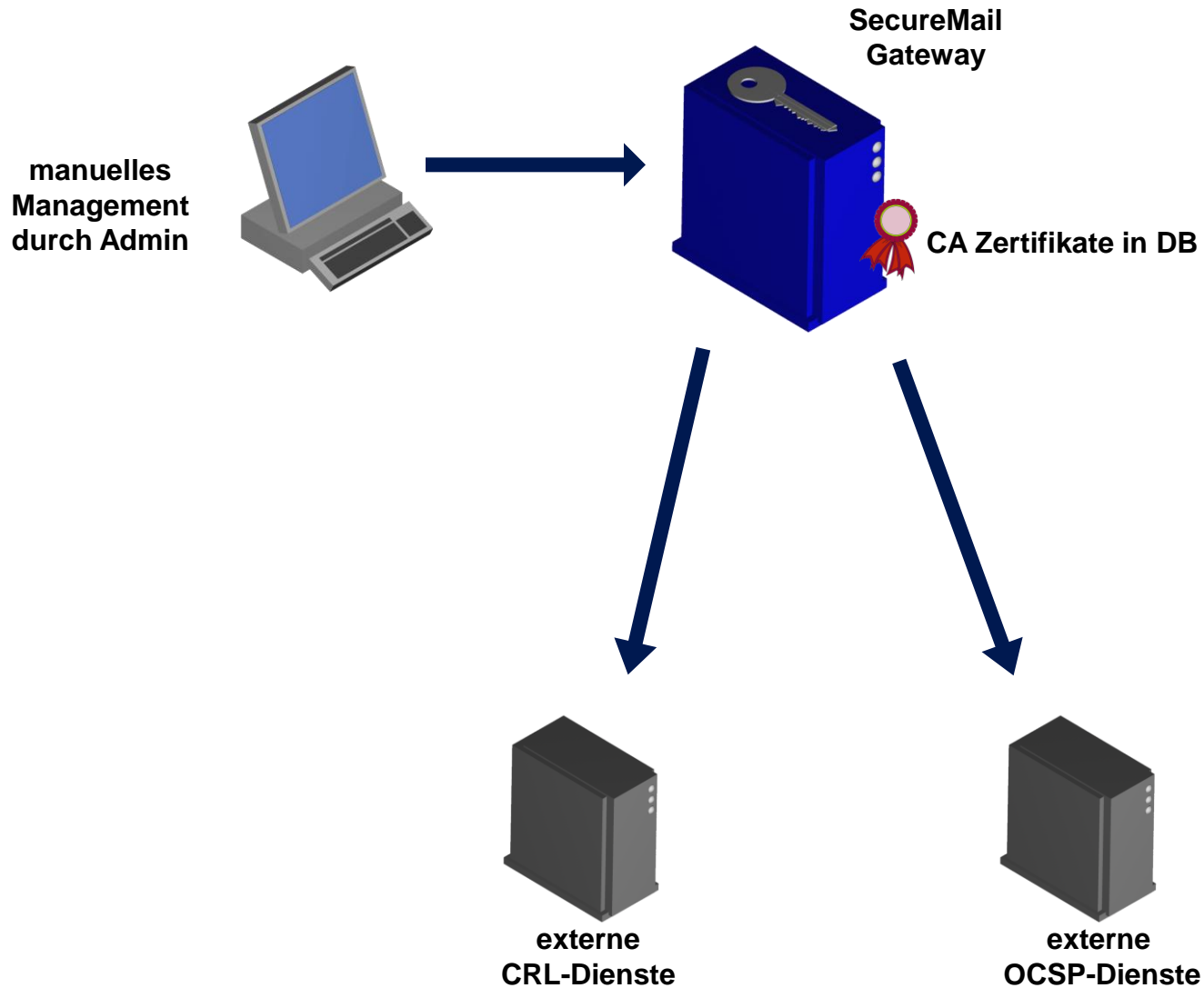
- Master-Master-Prinzip
- LoadBalancing
- Autom. Synchronisation
- Autom. Failover
- „beliebige“ Skalierbarkeit

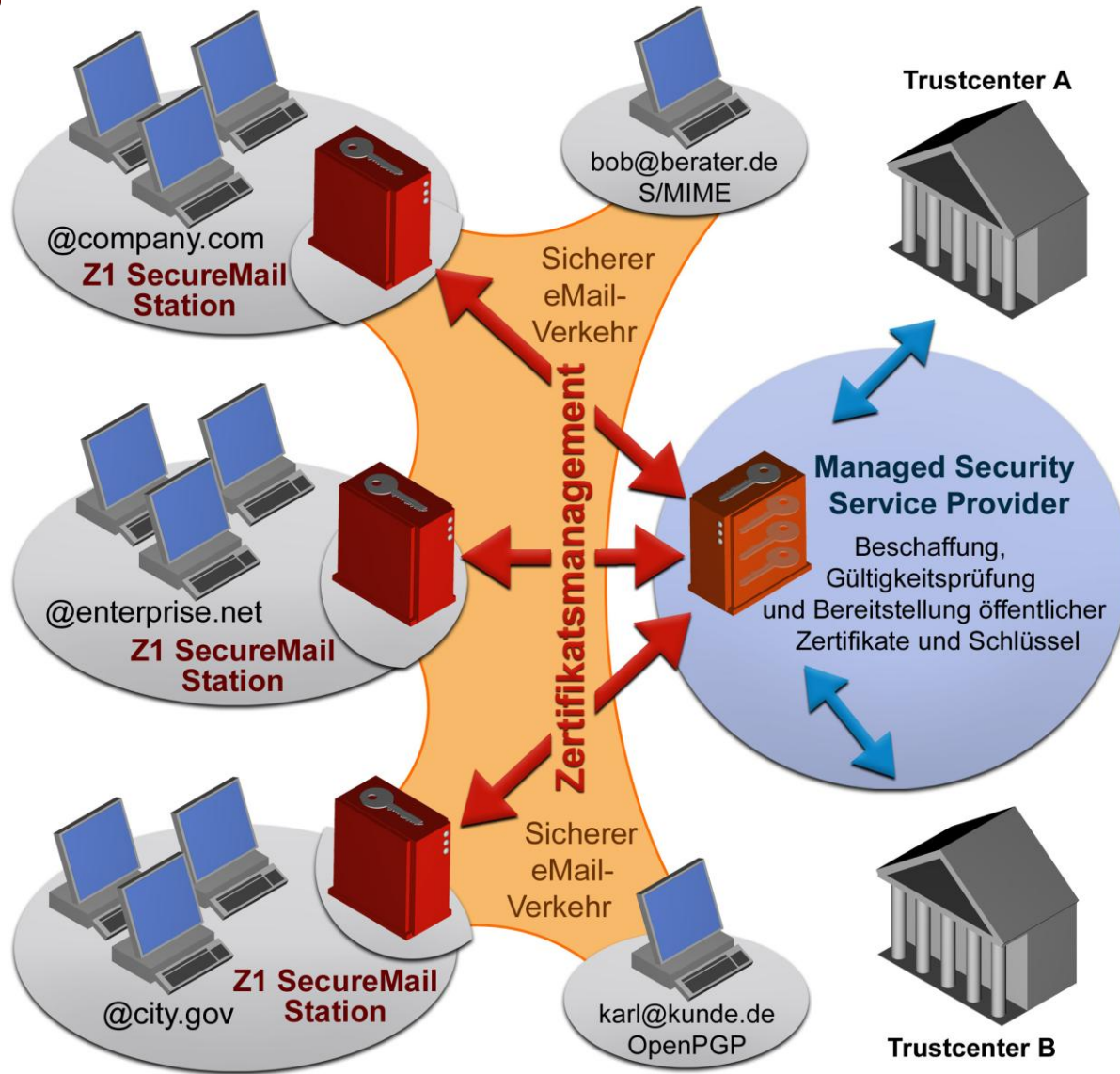


Externes Zertifikatsmanagement (automatische Beschaffung)



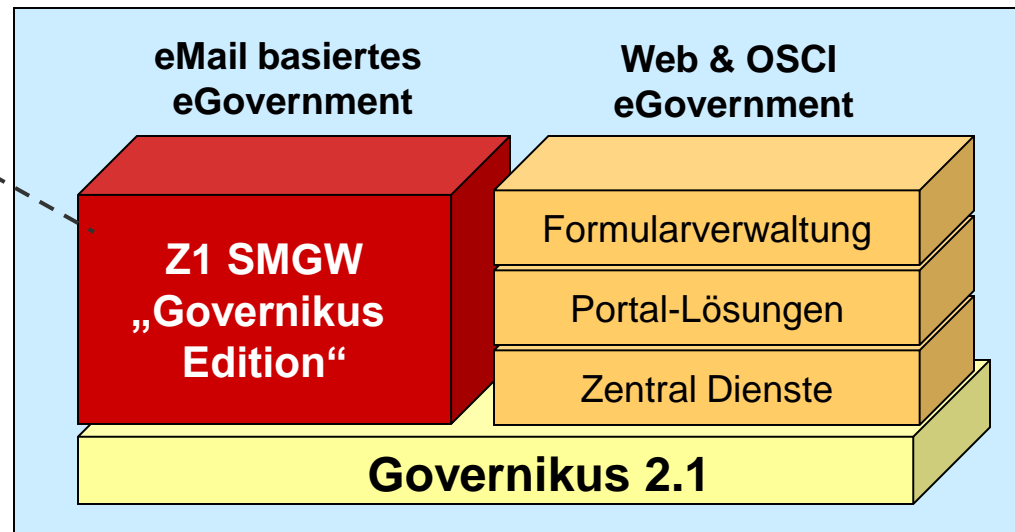
Externes Zertifikatsmanagement (automatische Validierung)





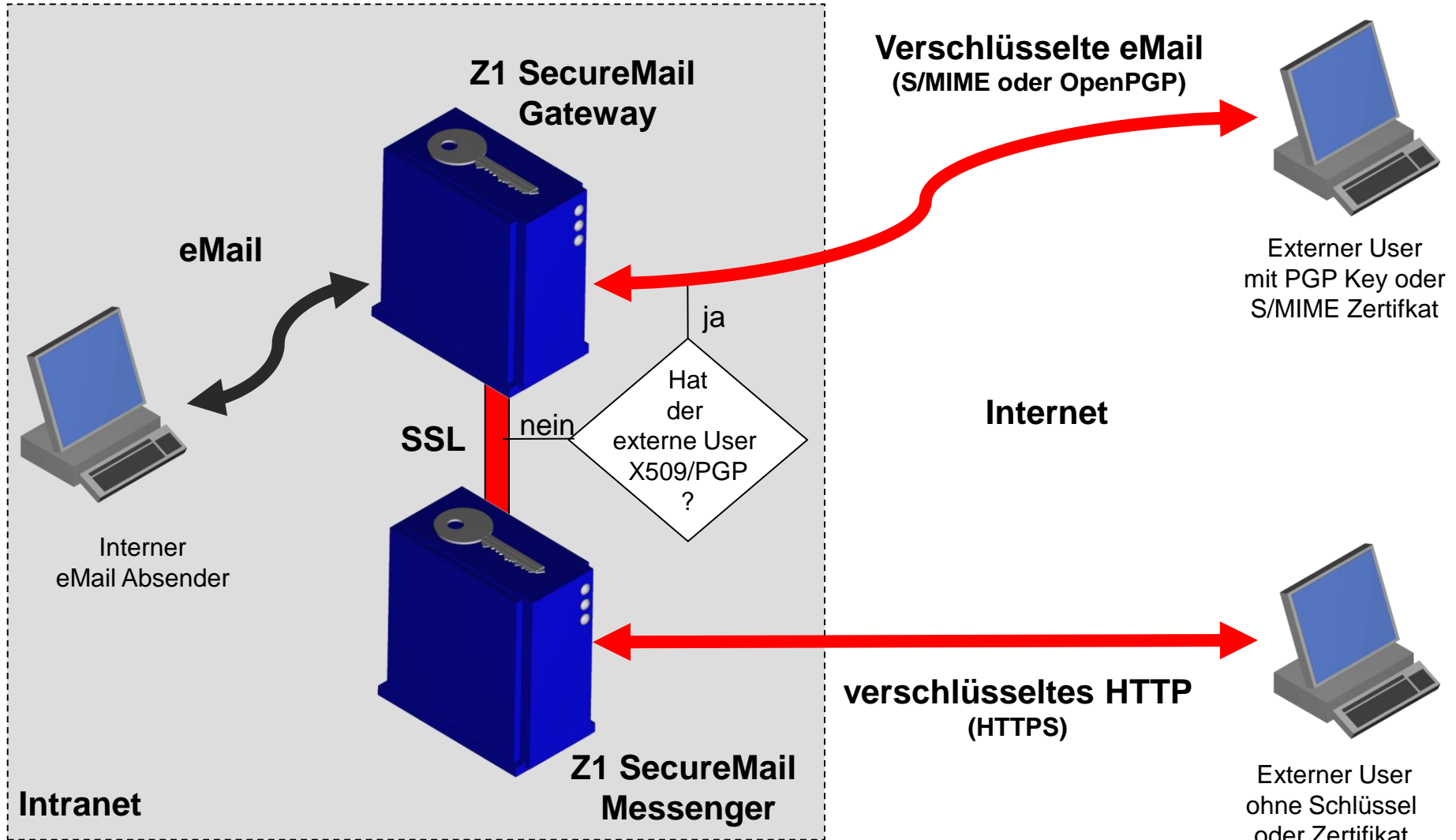


Virtuelle Poststelle im Behördenumfeld



Referenzen

- Land Brandenburg
- Land Sachsen



Unternehmenszertifikat vs. Personenzertifikat

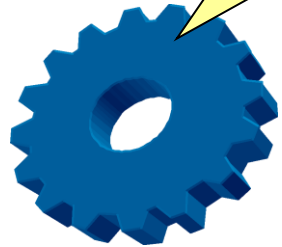
	PGP	S/MIME
Unternehmenszertifikat für Verschlüsselung	✓	✓
Unternehmenszertifikat für Signatur	✓	?
Personenzertifikate für Verschlüsselung	✓	✓
Personenzertifikate für Signatur	✓	✓

Z1 CA Connector

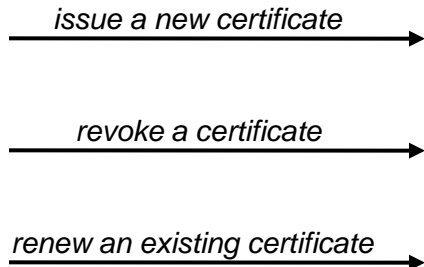


An action can be triggered:

- ✓ manually by the administrator (using the Z1 Admin Webclient)
- ✓ automatically by Z1 ERP Connector
- ✓ automatically by Z1 AutoTrigger

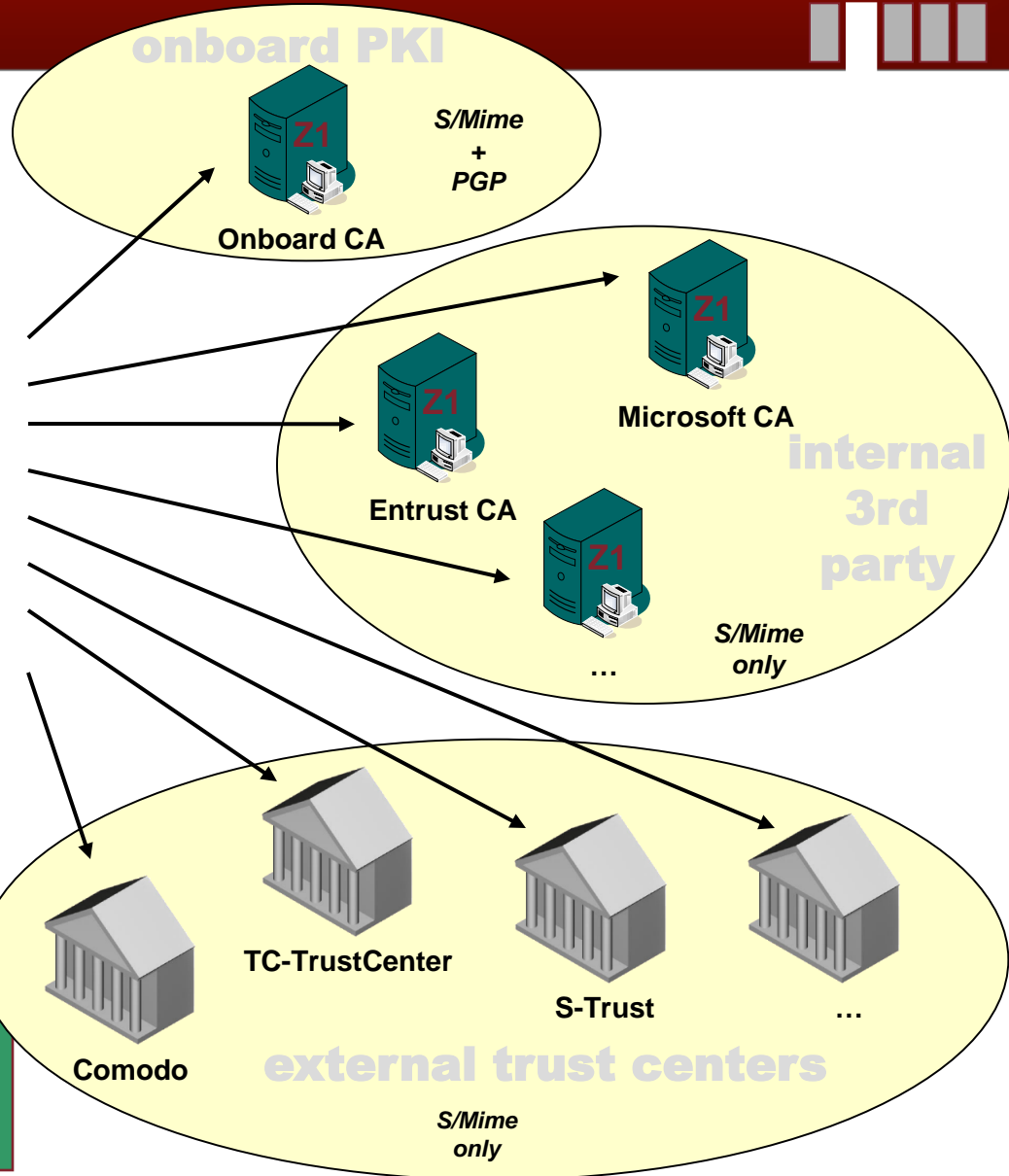


trigger



action

Z
1
C
A
C
o
n
n
e
c
t
o
r

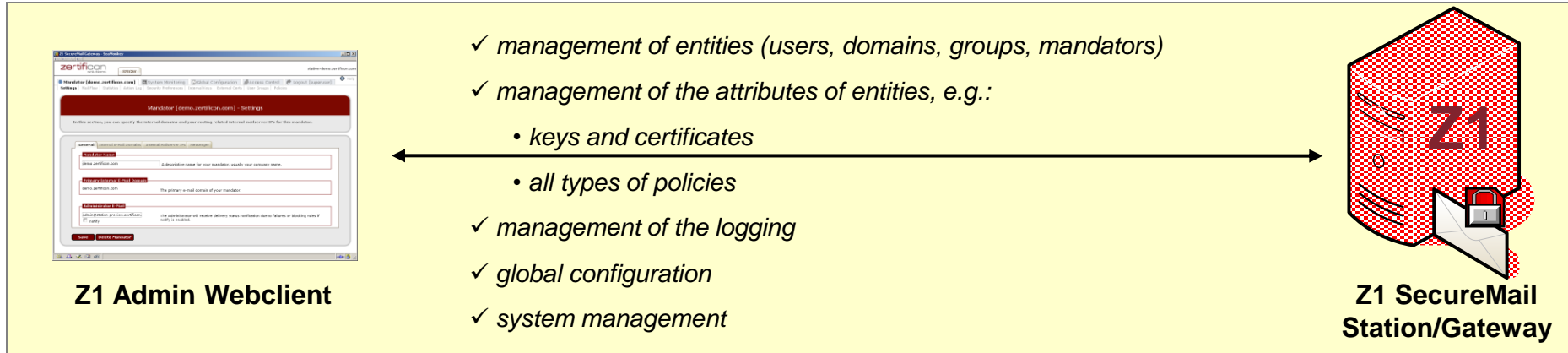


Use the CA Connector:

- ✓ to integrate the onboard PKI
- ✓ to integrate internal 3rd party PKIs
- ✓ to integrate external trust centers

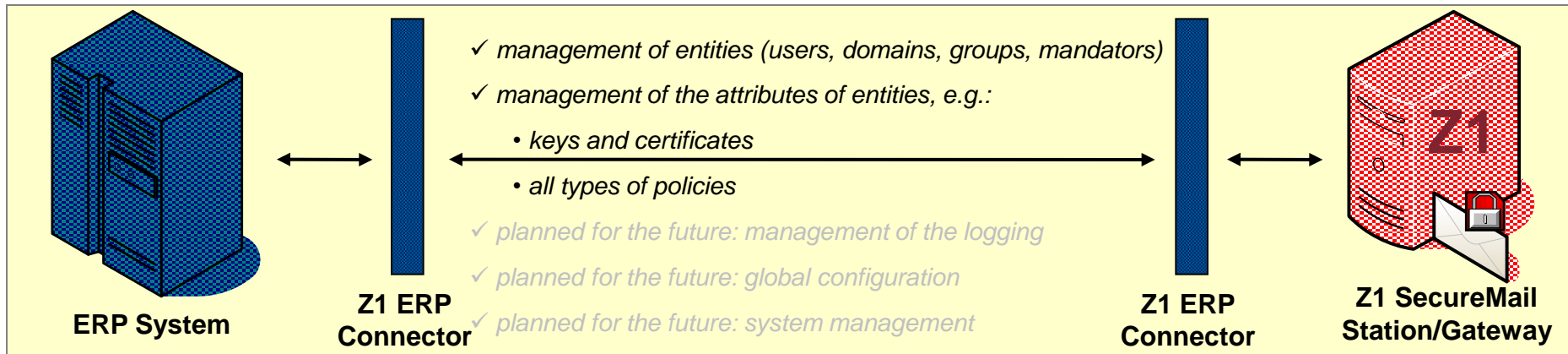


The **standard approach** to configure Z1 SecureMail Station/Gateway:



In the course of time, the ERP Connector will evolve into a full alternative to the Admin Webclient.

The **alternative approach** to configure Z1 SecureMail Station/Gateway:

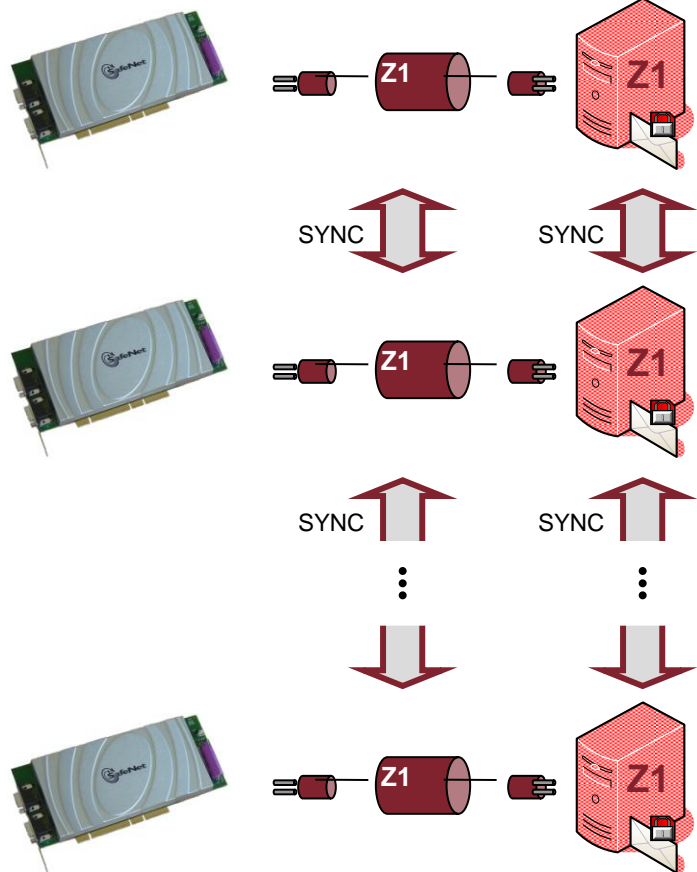


How to Protect the Private Keys with Hardware Security Modules



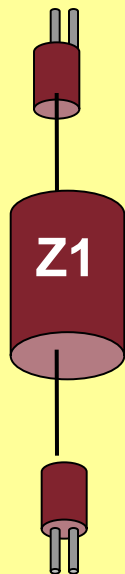
Scenario with Enterprise Requirements

... using crypto boards to provide high e-mail traffic



Maximize the security level of your Z1 SecureMail Solution by using Hardware Security Modules in combination with Z1 HSM Connector!

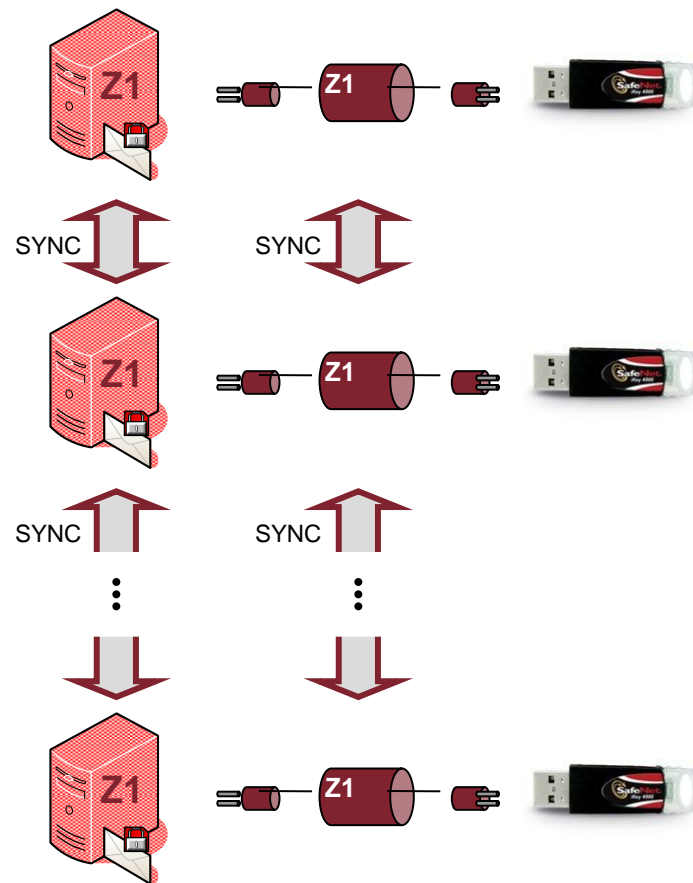
Z1 HSM Connector



- ✓ Can contain an unlimited number of keys!
- ✓ Is clusterable!
- ✓ Supports the whole private key live cycle!

Scenario with Standard Requirements

... using USB Crypto Tokens



Flexible, Fine-Adjustable Security Policy (Outbound)

Policy Name

Default Policy Outbound

Policy Description

The default policy for all outbound traffic.

Mail Delivery Options

Email Status	Plain	Already Signed	Already Encrypted
Forward	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Block	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use SecureMail Actions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

SecureMail Actions

Email Status	Plain	Already Signed	Already Encrypted
Text Embedding Actions			
Use Text Embedding	<input checked="" type="checkbox"/>		
Selected Text Embedding	Select a Text Embedding ... ▾		
Signature Actions			
Remove Signature		<input type="checkbox"/>	
Sign	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sign Failed	Forward ▾	Forward ▾	Forward ▾
Messenger Actions			
To Messenger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encrypt Actions			
Encrypt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Encrypt Type	Try PKI ▾	Try PKI ▾	Try PKI ▾
Preferred CertType	Try Domain, then User ▾	Try Domain, then User ▾	Try Domain, then User ▾
Encrypt Failed	Forward ▾	Forward ▾	Forward ▾
Options			
Preferred Method	S/Mime ▾	Default ▾	Default ▾
Preferred Modes	S/Mime Default ▾ OpenPGP Default ▾	S/Mime Default ▾ OpenPGP Default ▾	S/Mime Default ▾ OpenPGP Default ▾

Felixible, feinjustierbare Security Policy (Inbound)

Mandator [station-demo.zertificon.com] - Inbound Policy - Default Policy Inbound

Below you are able to modify the inbound policy 'Default Policy Inbound'.

All Policies **Inbound Policies** Outbound Policies

Default External Domain External Group External User Internal Group Internal User

Default Policy Inbound - Settings Mail Copy To

Policy Name
Default Policy Inbound

Policy Description
The default policy for all inbound traffic.

Mail Delivery Options

Email Status	Plain	Decryptable / SecureChannel	Not Decryptable	Signature OK	Signature Indeterminate	Signature Invalid
Forward	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Block	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use SecureMail Actions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

SecureMail Actions

Email Status	Plain	Decryptable / SecureChannel	Not Decryptable	Signature OK	Signature Indeterminate	Signature Invalid
Verify Actions						
Remove Signature				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Decrypt Actions						
Decrypt		<input checked="" type="checkbox"/>				
Delivery Options						
Internal Messenger	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save

Für den Benutzer läuft die Ver-/Entschlüsselung, die Signatur und Signatur-Validierung transparent ab!

Der Benutzer hat jedoch Eingriffsmöglichkeiten:

- durch Kommandos in der Betreff-Zeile,
- deren Syntax durch den Administrator definiert werden kann und
- die einzelnen Kommandos müssen vom Administrator „freigeschaltet“ werden.

Empfehlung: Sicherheitserhöhende Kommandos sollten erlaubt sein, sicherheitssenkende Kommandos nicht!

Eingehende eMails können am Ende einen Text enthalten, die den Benutzer über den Status der eMail informieren, wie z.B.: „Diese eMail war verschlüsselt und signiert. Die Signatur war korrekt“.

Der Text kann vom Administrator definiert werden.

Monitoring / Reporting / Logging: Mail Flow

Mandator [station-demo.zertificon.com] - Mail Flow

From Date : 30 4 2009 Till Date : 30 4 2009 Displaying : latest
 Internal : External : Subject :
 Using Filter : --Direction-- --Security-- --Status-- Auto Reload : **Apply Filter**

<< < [1] > >>

Date	Status	Time	Size	Internal	External	Subject	Security
Apr 30 08:00:20	OK	1.4s	1.8KB	internal@demo.zertificon.com <<	end2end@demo.com	Re: End To End	S
Apr 30 07:59:11	OK	0.6s	0.4KB	internal@demo.zertificon.com >>	end2end@demo.com	End To End	S
Apr 30 07:57:45	OK	1.1s	0.4KB	internal@demo.zertificon.com >>	end2end@demo.com	Signed	S
Apr 30 07:50:26	OK	0.3s	1.1KB	user@demo.zertificon.com <<	user@company.com	User encrypted	S
Apr 30 07:49:09	OK	1.0s	0.4KB	jan@demo.zertificon.com >>	i-have-two-keys@zertificon.com	Signed Encrypted Multiple Keys	S
Apr 30 07:48:01	OK	0.3s	1.1KB	user@demo.zertificon.com <<	user@company.com	Domain encrypted	S
Apr 30 07:47:20	OK	0.1s	0.5KB	internal.user@demo.zertificon.com <<	user@company.com	Re:	
Apr 30 07:47:15	OK	0.1s	0.5KB	internal.user@demo.zertificon.com <<	user@company.com	Re:	
Apr 30 07:46:56	OK	0.2s	0.4KB	internal.user@demo.zertificon.com >>	pgp.one.key@external.com	Smime signed	S
Apr 30 07:46:54	OK	0.2s	0.4KB	internal.user@demo.zertificon.com >>	pgp.one.key@external.com	Smime signed	S
Apr 30 07:45:51	OK	0.4s	0.8KB	internal.user@demo.zertificon.com <<	user@company.com	Signed & Verified	P
Apr 30 07:43:02	OK	1.3s	1.8KB	domain@demo.zertificon.com <<	user@company.com	domain smime encrypted	S
Apr 30 07:42:14	OK	0.4s	0.8KB	internal.user@demo.zertificon.com <<	user@company.com	Signed but not verified	P
Apr 30 07:42:03	OK	0.7s	1.8KB	domain@demo.zertificon.com <<	user@company.com	domain smime encrypted	S
Apr 30 07:40:52	OK	0.3s	0.5KB	internal.user@demo.zertificon.com <<	user@company.com	Test	

Monitoring / Reporting / Logging: Action Log

Mandator [station-demo.zertificon.com] - Action Log

Filter:

<< < [1, 2] >>

Time	Admin	Scope	Page	Action	Message
Apr 07 15:46:58	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Internal Keys	CREATE	Publish certificate "1223545833846371000"
Apr 07 15:45:51	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Cert Publishers	DELETE	Deleted ldap Cert Publisher[My Companies LDAP]
Apr 07 15:40:39	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Edit Publisher "Z1 Global TrustPoint Publisher"	UPDATE	Updated Z1 Backbone of Trust CertServer Publisher [Z1 Global TrustPoint Publisher].
Apr 07 15:40:01	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Cert Publishers	CREATE	Created certserver Cert Publisher [Z1 Global TrustPoint Publisher].
Apr 07 15:39:56	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Cert Publishers	DELETE	Deleted certserver Cert Publisher[GTP Publisher]
Apr 01 17:43:57	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Outbound Policies - External Domain	DELETE	Removed Policy External Domain lieferant.de Policy
Apr 01 17:43:51	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - Outbound Policies - External Domain	UPDATE	Added Policy External Domain lieferant.de Policy to the Domain lieferant.de
Apr 01 17:43:36	superuser	station-demo.zertificon.com	Mandator [station-demo.zertificon.com] - All Policies - Route	UPDATE	Added Policy Internal E-Mail aez@zertificon.com to External User b.wiegel@dbw.de Policy to the E-Mail aez@zertificon.com

Platforms That Are Supported by “Z1 SecureMail Station/Gateway”



supported for existing customers	recommended for new customers	future support
- Z1 Appliance	- Z1 Appliance	- all future versions of Z1 Appliance
- Debian 3.1 (Sarge) - Debian 4.0 (Etch)	- Debian 4.0 (Etch)	- all future versions of Debian
- Solaris 9 (sparc64) - Solaris 10 (sparc64)	- Solaris 10 (sparc64)	- all future versions of Solaris (sparc64)
- RHEL4 ES		
- SLES 9		

Other platforms are supported on request and on project basis.

last updated: 2008-05-23 (01:50 p.m.)



System Backup

- Auslieferung eines Backup-Scripts
- Automatisiertes, zyklisches Backup der Konfiguration / Zertifikate

Updates / Upgrades

- Appliance
 - Update-Server für Betriebssystem und Applikation
 - Kunden werden über neue Releases informiert
 - Automatische Update-Installation
- Auf eigener Hardware
 - Kunden werden über neue Releases informiert
 - SW-Download
 - Automatische Update-Installation

Support

- via Telefon,
- via eMail,
- und / oder via ...

Support & Ticket – System (<https://support.zertificon.com>)

(OTRS – Open Ticket Request System)

- Vorfälle / Anfragen werden zu Tickets zusammengefasst
- Bearbeitung und Status jedes Tickets wird dokumentiert
- Historie aller Tickets ersichtlich
- Tickets sind einer Person zugeordnet
- Tickets eines Unternehmens werden übersichtlich dargestellt

Vielen Dank für Ihre Aufmerksamkeit



Zertificon Solutions GmbH
Landsberger Allee 117
10407 Berlin

Herbert Nebel

Tel.: 030 / 5900300 - 0

Fax: 030 / 5900300 - 99

Mail: h.nebel@zertificon.com

<http://www.zertificon.com>