

Uwe Ulbrich, Net at Work GmbH, Paderborn
uwe.ulbrich@netatwork.de

DE-MAIL UND E-POST-BRIEF: SINNVOLL UND SICHER?

- Motivation für De-Mail
 - Anwendungsmöglichkeiten
- Das De-Mail Gesetz
 - Datensicherheit
 - Rechtssicherheit
- Konzept und Technik
 - Kommunikationsweg
 - Benutzersicht
 - Anbindung von Unternehmen/Behörden
- Datenschutz bei De-Mail

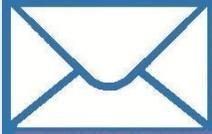
- Der heutigen E-Mail fehlen wichtige **Sicherheitseigenschaften**
 - E-Mails können mit wenig Aufwand **mitgelesen** werden.
 - Kommunikationspartner können nie vollständig sicher sein, **mit wem** sie gerade kommunizieren.
 - Es kann nicht nachgewiesen werden, dass die Nachricht im Postfach des Empfänger **angekommen** ist.
 - Weitere Probleme: SPAM, Phishing
- Existierende Sicherheitslösungen haben sich bisher nicht **in der Fläche** durchgesetzt (u.a. wg. zusätzlich erforderlicher Installationen)

- Verschlüsselte Übertragung über das Internet
- Authentische Absender und Empfänger
- Versand- und Eingangsbestätigungen
- Wirksame Bekämpfung von SPAM und Phishing

De-Mail soll **grundlegende** Sicherheitsfunktionen einfach nutzbar und dadurch **in der Fläche** breit verfügbar machen.



De-Mail: Analogie zu heutigen Postdiensten

Kommunikations- medium	Postdienste	De-Mail
Postkarte		Kein Angebot (entspricht normaler ungeschützter E-Mail)
Brief		De-Mail einfach (verschlüsselt, vor Veränderungen geschützt)
Einschreiben ohne Rückschein		De-Mail mit signierter Versandbestätigung
Einschreiben Einwurf		De-Mail mit signierter Eingangsbestätigung
Einschreiben Eigenhändig		De-Mail persönlich
Kein Angebot		De-Mail absenderbestätigt

De-Mail

Das De-Mail-Gesetz

- mit und ohne sichere Anmeldung – Anmeldeniveau „normal“ und „hoch“
- Sichere Anmeldung:
zwei unabhängige Sicherungsmittel
- ohne sichere Anmeldung: bei nur einem Sicherungsmittel (i.d.R. Passwort)
- Diensteanbieter muss zwei Verfahren zur sicheren Anmeldung bereitstellen
- ein Verfahren muss eID des nPA sein

- **Persönlich (Abs. 4)**
 - Nachricht kann nur mit Anmeldeniveau „hoch“ gelesen werden
- **Absenderbestätigt (Abs. 5)**
 - Nachricht wurde mit Anmeldeniveau „hoch“ erstellt/versandt

- auf Antrag des Senders
- enthält
 - Adresse des Senders und Empfängers
 - Datum und Uhrzeit des Versands vom Postfach des Senders
 - Namen des Diensteanbieters, der die Versandbestätigung erzeugt hat
 - Prüfsumme der Nachricht
- qualifiziert elektronisch signiert nach SiG

Verification.pdf - Adobe Reader
Datei Bearbeiten Anzeige Fenster Hilfe

Acknowledge-Message

Sender: uweulbrich@netatwork.de-mail.de
Subject: Test Mail im Mai
Text: Hallo Herr Krause, wieder mal eine Testmail. mfg Uwe Ulbrich

Hash: v=1; a=rsa-sha256; c=simple/simple; t=1305016581; d=null; h=From:Date:Subject:X-De-Mail-Return-Receipt:X-De-Mail-Disposition-Notify:X-De-Mail-Authoritative:X-De-Mail-Private:X-De-Mail-EBP-A-Sender:X-De-Mail-Chosen-Recipients:X-De-Mail-Auth-Level:X-De-Mail-Originator-BPDA:X-De-Mail-Message-Type; bh=gWsXQGC4vEVOkYf0Do0Nwi4iYSVejZrmB8WcC6KzsvM=; b= DtadSLVbvWXe/ZmNiS/1/xj07JKTGEA9BcwzHVtREC0=

Time: 1305016581340

Name	Value
X-De-Mail-Return-Receipt	yes
X-De-Mail-Disposition-Notify	yes
X-De-Mail-Private	no
X-De-Mail-Authoritative	no
X-De-Mail-Auth-Level	High
X-De-Mail-Message-Type	NORMAL
X-De-Mail-EBP-A-Sender	uweulbrich@netatwork.de-mail.de
X-De-Mail-Chosen-Recipients	to=henningkrause@netatwork.de-mail.de;cc=;bcc=
X-De-Mail-Actual-Recipients	to=henningkrause@netatwork.de-mail.de;cc=;bcc=
X-De-Mail-Originator-BPDA	t-systems.de-mail.de
X-De-Mail-Hash-Signature	v=1; a=rsa-sha256; c=simple/simple; t=1305016581; d=null; h=From:Date:Subject:X-De-Mail-Return-Receipt:X-De-Mail-Disposition-Notify:X-De-Mail-Authoritative:X-De-Mail-Private:X-De-Mail-EBP-A-Sender:X-De-Mail-Chosen-Recipients:X-De-Mail-Auth-Level:X-De-Mail-Originator-BPDA:X-De-Mail-Message-Type; bh=gWsXQGC4vEVOkYf0Do0Nwi4iYSVejZrmB8WcC6KzsvM=; b= DtadSLVbvWXe/ZmNiS/1/xj07JKTGEA9BcwzHVtREC0=

- auf Antrag des Senders
- erstellt vom Diensteanbieter des Empfängers
- enthält
 - Adresse des Senders und Empfängers
 - Datum und Uhrzeit des Eingangs im Postfach des Empfängers
 - Namen des Diensteanbieters, der die Empfangsbestätigung erzeugt hat
 - Prüfsumme der Nachricht
- qualifiziert elektronisch signiert nach SiG
- Wird ebenfalls an Empfänger versandt
- ohne sichere Anmeldung erst nach 90 Tagen durch Empfänger löscher

Empfangsbestätigung

Betreff: [Zugangsbestätigung] Test Mail im Mai

▶ E-Mail-Header erweitern

Von: de-mail-meldung@t-systems.de-mail.de

An: uweulbrich@netatwork.de-mail.de

Datum: 10.05.2011 10:36

Ihre Nachricht Test Mail im Mai versendet am 10.05.2011 10:36:21 mit der ID d52c616e-d766-4407-b014-6c5e8a4152fd@t-systems.de-mail.de wurde am 10.05.2011 10:36:22 erfolgreich an den Empfänger henningkrause@netatwork.de-mail.de zugestellt.

▶ Verific...ion.xml (5,6KB) ↕

▶ Verific...ion.pdf (5,7KB) ↕

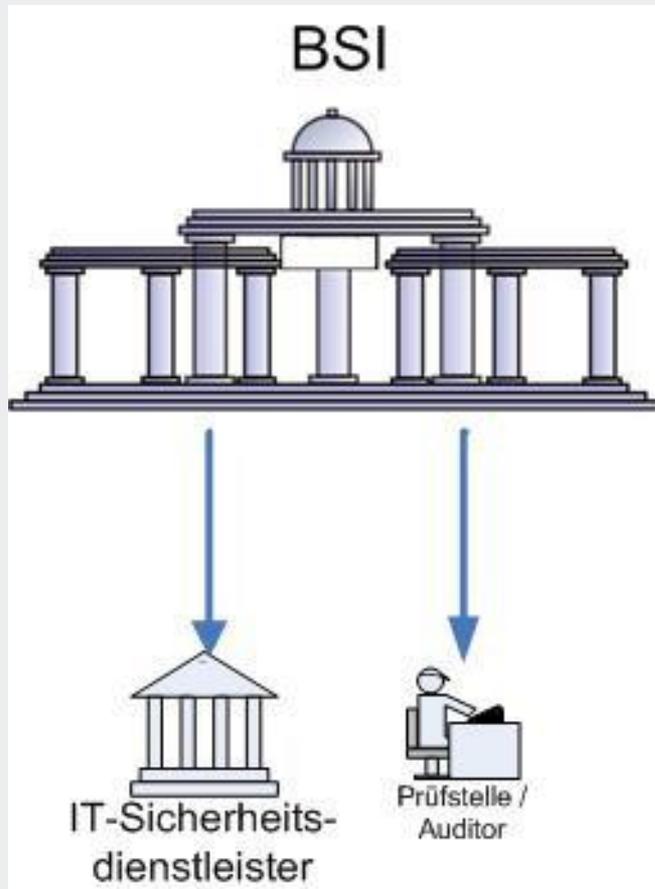
- Eine öffentliche Stelle, welche zur förmlichen Zustellung nach Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, berechtigt ist, kann eine Abholbestätigung verlangen.
- Wird bei sicherer Anmeldung erstellt.
- gilt als Nachweis der elektronischen Zustellung (§ 5a Abs. 3 Verwaltungszustellungsgesetz)
- ohne sichere Anmeldung erst nach 90 Tagen durch Empfänger löschar

- Änderung im Verwaltungszustellungsgesetz

„Ein elektronisches Dokument gilt in den Fällen des §5 Absatz 5 Satz 2 am dritten Tag nach der Absendung an das De-Mail-Postfach des Empfängers als zugestellt, wenn er dieses Postfach als Zugang geöffnet hat ...“

- **§§ 17 Abs. 1 und 2 De-Mail-Gesetz**
 - Diensteanbieter, die De-Mail-Dienste anbieten wollen, müssen sich auf schriftlichen Antrag von der zuständigen Behörde (§ 2: BSI) **akkreditieren** lassen.
 - Die Akkreditierung ist zu erteilen, wenn der De-Mail-Diensteanbieter nachweist, dass er die **Voraussetzungen nach § 18** erfüllt (...)

- **§ 18:**
 - Nr. 1: Zuverlässigkeit und Fachkunde
 - Nr. 2: Geeignete Deckungsvorsorge
 - Nr. 3: **Technische und organisatorische Anforderungen** an die Pflichten nach den §§ 3 bis 13 und 16 (...)
 - Nr. 4: Erfüllung der **datenschutzrechtlichen Anforderungen** bei Gestaltung und Betrieb der Dienste



- **BSI zertifiziert IT-Sicherheitsdienstleister**, die Testate ausstellen
- **BSI zertifiziert Auditoren und anerkennt Prüfstellen**, die die erforderlichen Prüfungen durchführen und Prüf-/Auditberichte erstellen
- Ziel: **Prüfung des DMDA** auf Erfüllung der Anforderungen aus § 18 De-Mail

De-Mail

Konzept und Technik

- Im einfachsten Fall wird De-Mail mit Web- Anwendungen genutzt, die **keine weiteren Installationen** auf dem Computer des Nutzers erfordern.
- De-Mail-Provider können **weitere Clients** anbieten (iPhoneApps, PlugIns, etc.)
- Unternehmen und Behörden können ihre existierenden (internen) E-Mail-Infrastrukturen oder auch ERP-Systeme über eine **zentrale Komponente** (ein sog. „Gateway“) an De-Mail anschließen.

De-Mail bietet eine Infrastruktur für die Kommunikation Aller mit Allen

- verschlüsselt
- authentisch und
- nachweisbar

realisiert durch De-Mail-Provider im „virtuellen“ Verbund

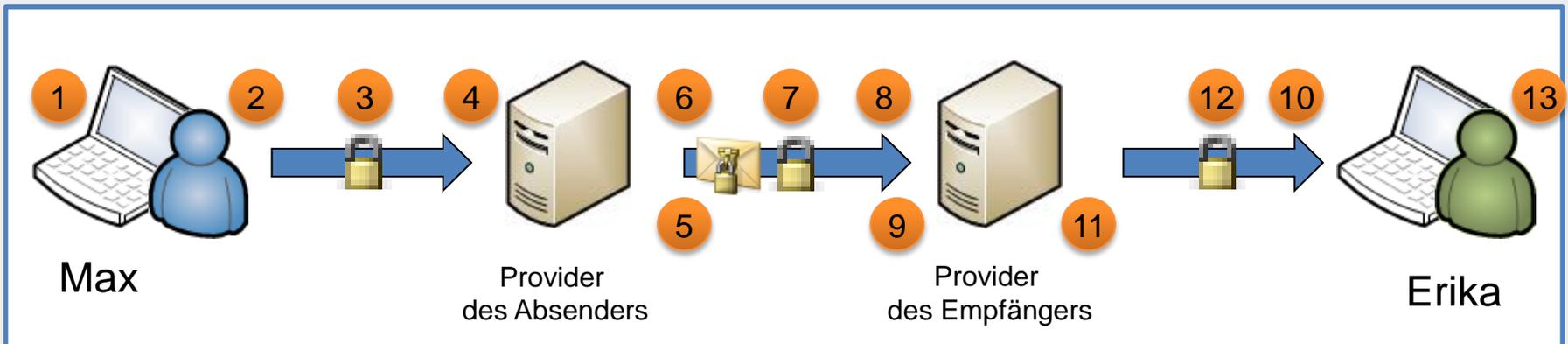
- Deutsche Telekom AG
- United Internet AG (WEB.DE, GMX)
- Mentana Claimsoft AG
- Deutsche Post AG

haben angekündigt, sich als De-Mail-Provider akkreditieren zu lassen.



Quelle: BSI, Mehrfeld/Schumacher

1. De-Mail erstellen
2. Aufbau eines verschlüsselten Kanals
3. Versenden der De-Mail
4. Kurzzeitige automatisierte Prüfung (Spam, Viren, De-Mail-Metadaten)
5. Verschlüsselung der De-Mail
6. Aufbau eines verschlüsselten Kanals
7. Übermittlung der De-Mail an Empfänger-Provider
8. Kurzzeitige automatisierte Entschlüsselung für Prüfung (Spam, Viren, Integrität)
9. Ablage De-Mail in Postfach
10. Aufbau eines verschlüsselten Kanals
11. Entschlüsselung der De-Mail
12. Übermittlung der De-Mail
13. Darstellung der De-Mail



- Verschlüsselte Kommunikationsverbindung zwischen Nutzer und Postfach
- Transportverschlüsselung zwischen den Providern
- E-Mail-Verschlüsselung zwischen den Providern

- De-Mail Adressformate
 - Natürliche Personen: Nachname, ggf. Vornamen, Teil des Vor- und Nachnamens
 - Juristische Personen: Kennzeichnung im Domainenteil
 - Pseudonyme

Morgens halb zehn in Deutschland...



- De-Mail-Gesetz § 5 Abs. 3 Satz 3
 - „Der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) bleibt hiervon unberührt.“
- Verzeichnis
 - Listet De-Mail Nutzer (freiwillig)
- Zertifikate
 - Können durch Anwender im Verzeichnis veröffentlicht werden

The screenshot shows a web browser window with the URL <https://service.gmx.net/de/cgi>. The page title is "De-Mail mit GMX" with the tagline "Einfach wie E-Mail, so sicher wie ein Brief!".

De-Mail macht digitale Kommunikation rechtssicher
De-Mail ist eine Initiative der Bundesregierung mit GMX, WEB.DE, der Deutschen Telekom AG und Partnern. Mit De-Mail können Sie Nachrichten und Dokumente sicher über das Internet versenden.

Jetzt De-Mail-Adresse reservieren - kostenlos und unverbindlich:

Vielen Dank!
Ihre De-Mail-Adresse wurde für Sie reserviert

Ihre De-Mail-Adresse
uwe.ulbrich.2@gmx.de-mail.de

ist für Sie reserviert. Bis zum offiziellen Start des De-Mail-Systems können Sie diese noch bearbeiten und ändern.

Wie geht es jetzt weiter?
In Kürze können Sie sich für De-Mail identifizieren lassen - wir werden Sie per E-Mail informieren!

Ihre Daten
Uwe Ulbrich

De-Mail-Adresse
uwe.ulbrich.2@gmx.de-mail.de
[Ändern](#)

Persönliche Daten
33104 Paderborn
Deutschland
[Ändern](#)

Pseudonyme
[Anlegen](#)

Sagen Sie's weiter!
Informieren Sie Ihre Freunde und Bekannte über Ihre De-Mail!
Noch sind die besten Adressen frei!

Buttons for social media sharing:

Navigation: [zurück](#)

Footer: [Impressum](#) | [AGB](#) | [Datenschutz](#) | So gehts! Ein Service von GMX

AGB und Datenschutz Hilfe

T-Systems

Anmeldung mit hohem Sicherheitsniveau

Bitte wählen Sie die gewünschte Zugangsart, um sich anzumelden.

Zusätzlich zu einem Einmal-Passwort (OneTimePass - OTP) wird Ihre vierstellige Server-PIN benötigt. Geben Sie diese unmittelbar nach Eingabe des 8-stelligen Einmal-Passworts ein.

[Zurück zur Startseite](#)

SMS-Sicherheitsschlüssel

Anmeldung mit einem Einmal-Passwort per SMS.

[Hier anmelden](#)

Login

Benutzername:

[OTP anfordern](#)

OneTimePass + Server-PIN:

[Anmeldung](#)

OTP-Sicherheitsschlüssel

Anmeldung mit einem Einmal-Passwort per OTP-Sicherheitsschlüssel.

[Hier anmelden](#)

Version 1.6.6 © T-Systems International GmbH 2010. Alle Rechte vorbehalten.

[Impressum](#) [Kontakt](#)

Seite 25

De-Mail Unterkonten erstellen/löschen

De-Mail Unterkonten

De-Mail Unterkonto 1:

@netatwork.de-mail.de



De-Mail Unterkonto 2:

:: Firma/Selbstständig

:: Zertifikate

:: Upload

:: Übersicht

:: Passwort ändern

:: Sicherheitsschlüssel verwalten

:: De-Mail Unterkonto

:: Verknüpfte E-Mail-Adresse

:: Benachrichtigungs-E-Mail-Adresse

Übersicht

Anzeige des X.509-Zertifikats

Issuer-DN: CN=Shared Business CA, OU=Trust Center Deutsche Telekom, O=T-Systems Enterprise Services GmbH, C=DE

Subject-DN: SERIALNUMBER=1,
EMAILADDRESS=uwe.ulbrich@netatwork.de, CN=Uwe Ulbrich,
OU=De-Mail, OU=T-Systems, O=Net at Work Netzwerkssysteme GmbH,
C=DE

Zertifikatsnummer: 12693

Gültig bis: 09.11.2013 12:59:59

Abbrechen

Löschen

@netatwork.de-mail.de



De-Mail Unterkonto 9:

@netatwork.de-mail.de

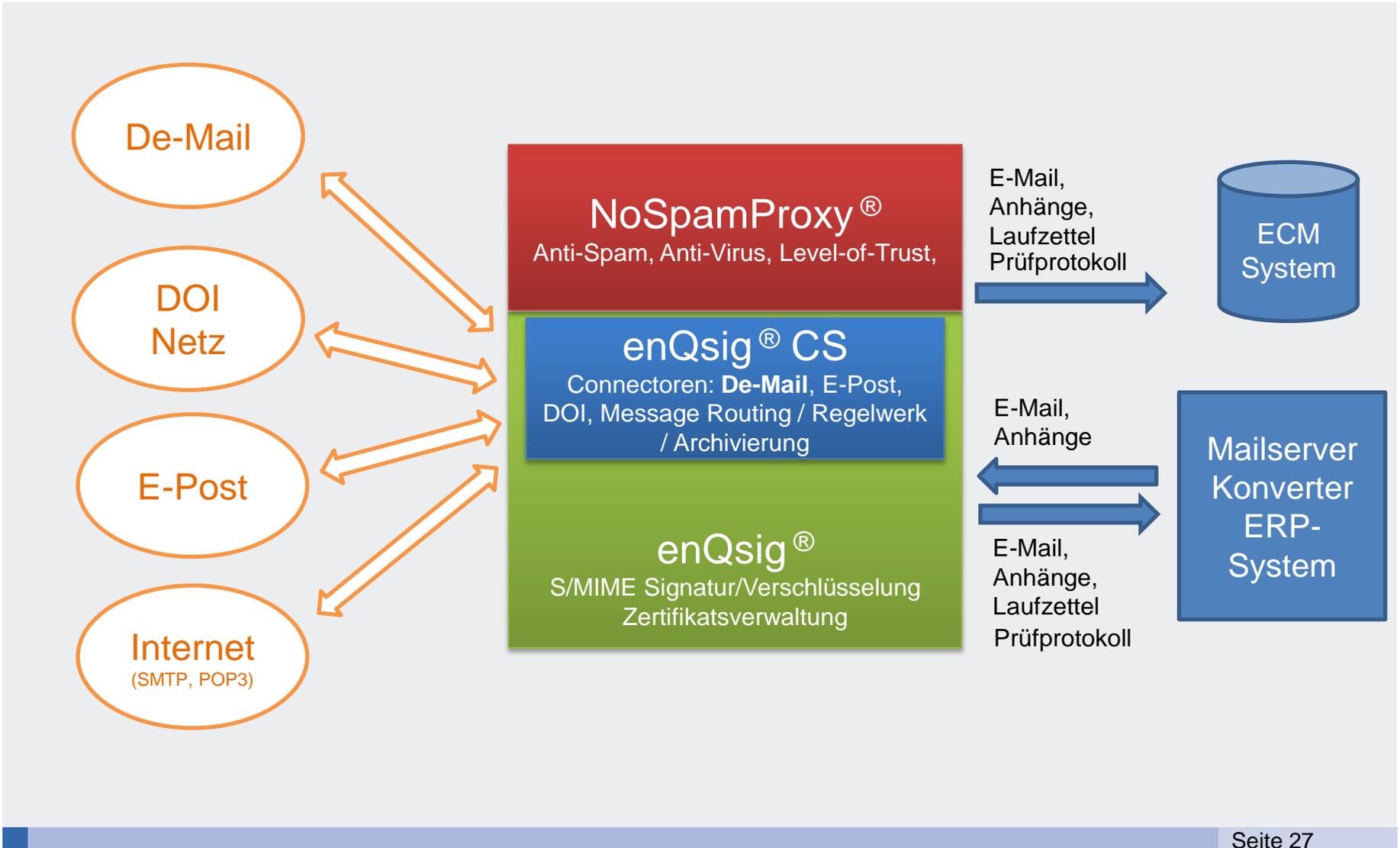


De-Mail Unterkonto 10:

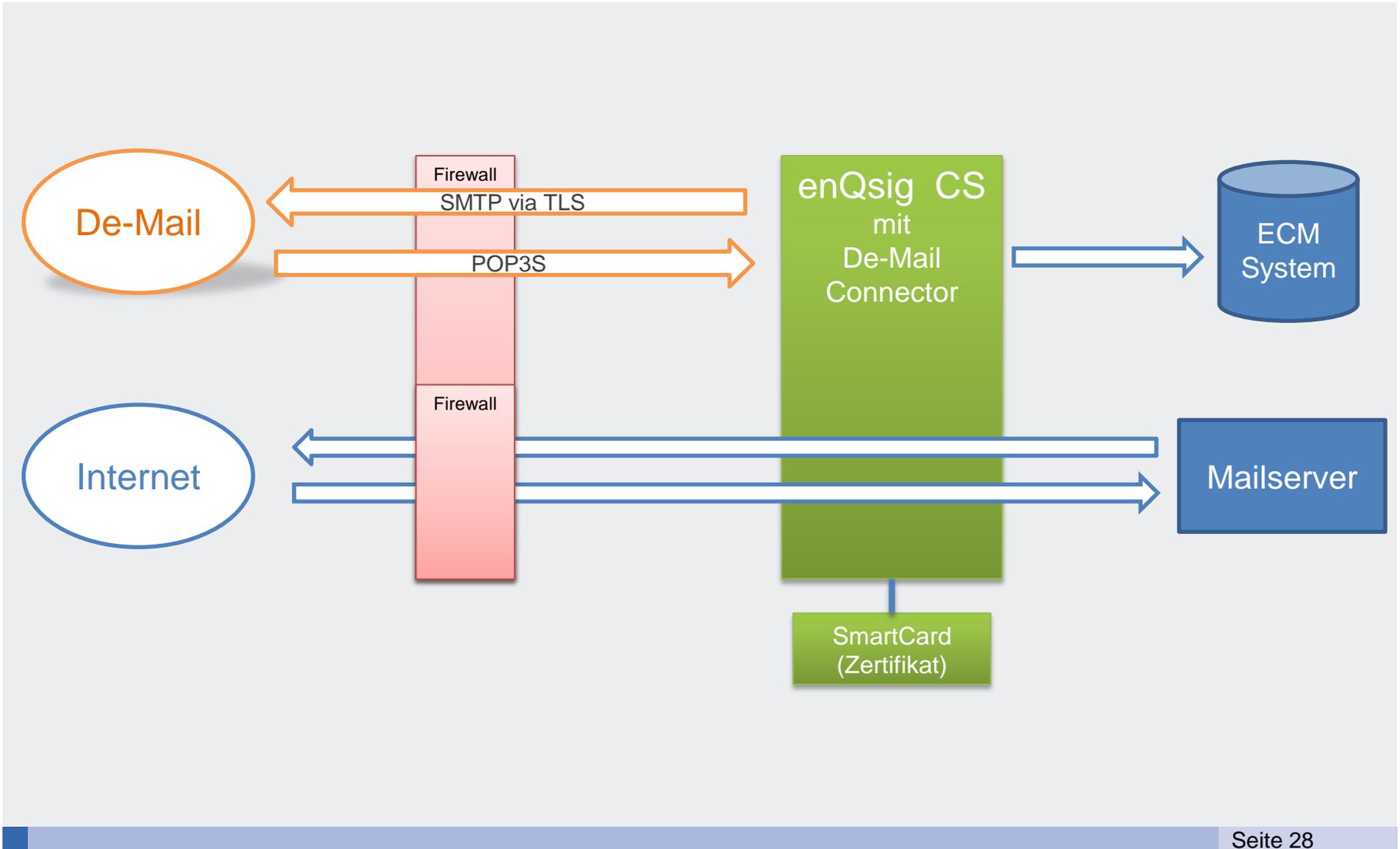
@netatwork.de-mail.de



Net at Work Mail Gateway



De-Mail-Anbindung - Architektur



- Sende-Konnektor
 - Routet alle De-Mails zum De-Mail Provider
- Empfangs-Konnektor
 - Stellt sicher, dass De-Mails nur vom Provider kommen und nicht aus dem Internet
- Unterstützung von SmartCards mit PIN
 - Hohes Authentisierungsniveau

Net at Work Mail Gateway Configuration - [Net at Work Mail Gateway]\Gateway Role\Mail Routing

File Action View Help

Net at Work Mail Gateway

- Gateway Role
 - Mail Routing
 - Topology
 - Mail Queues
 - Qualified Signature Issues
 - Certificate Management
 - Signature Inspection Rep
 - Rules
 - Address rewriting
 - Common Rule Settings
 - Text-message Provider
 - Archive Interface
 - Level of Trust
 - Domain Trust
 - Local Addresses
 - Subject flags
 - Advanced Settings
 - Troubleshooting
 - Licence
- UserManagement Role
- Reporting Role
- Event Log
- Server Performance
- Mail Gateway News

Inbound delivery

Inbound mails are forwarded to the server **localhost** on port **30**.
No authentication is used for connection to this smarthost.
Transport security is **allowed**.
[Modify inbound delivery](#) [Switch to queued inbound delivery](#)

Outbound delivery

Outbound mails are routed using the send connectors defined below. If multiple connectors are suitable for routing of a specific mail the connector with the least cost is chosen.

Acti...	Name	Type	Delivery method	Cost	DNS Routing restrictions
✓	Default connector for outbound mails	SMTP	Direct delivery via DNS	100	From * to *
✓	De-Mail connector	De-Mail	De-Mail smarthost	0	Recipients of De-Mail

[Add new send connector](#) Modify selected send connector Remove selected send connectors

Receive connectors

Receive connectors connects the GatewayRole to the internet to receive mails.

Acti...	Connector type	Binding	Other setting	Connecti... security
✓	SMTP	Any : 25	Blocking is 30 minutes Tarpting level is medium	StartTLS allowed
✓	SMTP	Any : 465	Blocking is disabled Tarpting is disabled	TLS
✓	De-Mail	demail.... 465	Download interval is 20 minutes Delivery to accounting@netatwork.de	TLS

[Add new receive connector](#) Modify selected receive connector
Remove selected receive connectors

- Durchgängige sichere Identifizierung des Nutzers von der Anwendung bis zum Gateway
 - Absender-Adressen automatisch umgeschrieben aus
henning.krause@netatwork.de
wird
henningkrause@netatwork.de-mail.de
 - Berechtigung von Nutzern für De-Mail
- Autorisierung des Gateway-nutzenden Systems
 - TLS zum internen System

Address rewriting



The address rewriting modifies the senders mail address on outbound mails. From the recipients point of view, the mail appears to be sent from the rewritten address instead of the original author. The rewriting process can be limited to a specific recipient domain.

▼ Detailed description

Filter (use '*' and '?' as wildcards):

Search

Internal address	External address	Namespace
henning.krause@contoso.com	henningkrause@de-mail.de	*.de-mail.de
uwe.ulbrich@contoso.com	uweulbrich@de-mail.de	*.de-mail.de

[Add new mapping](#)

Showing mapping 1 to 2 [Previous page](#) [Next page](#)

[Modify selected mapping](#)

[Remove selected mapping](#)

De-Mails werden mit einem Prüfbericht ausgestattet. Dieser wird in Form einer signierten Datei an die E-Mail angehängt.

- War die E-Mail signiert/verschlüsselt?
- Welche De-Mail Merkmale wurden verwendet?
 - Einschreiben, Zustellbestätigt, usw.

Prüfbericht - Nachricht (HTML) (Schreibgeschützt)

Von: Gesendet: Do 12.05.2011 15:19
An:
Cc:
Betreff: Prüfbericht

1. Zusammenfassung der Prüfergebnisse

Betreff: Standard DE-Mail
Nachrichten id:
Transport system: De-Mail
Ergebnis der Signaturprüfung: Die E-Mail besitzt keine digitale Signatur
Prüfzeitpunkt: 12.05.2011 15:18:45
Anzahl geprüfter Signaturen: 0
Entschlüsselte Inhalte: 0
Unterzeichnende Personen: 0
Geprüft durch: Net at Work Mail Gateway with enQsig

2. Detaillierte Prüfergebnisse

2.1 Ergebnis der Signaturprüfungen
Die E-Mail besitzt keine digitale Signatur, daher sind keine detaillierten Prüfergebnisse verfügbar.

2.2 Ergebnis der Entschlüsselung
Die E-Mail wurde unverschlüsselt übertragen.

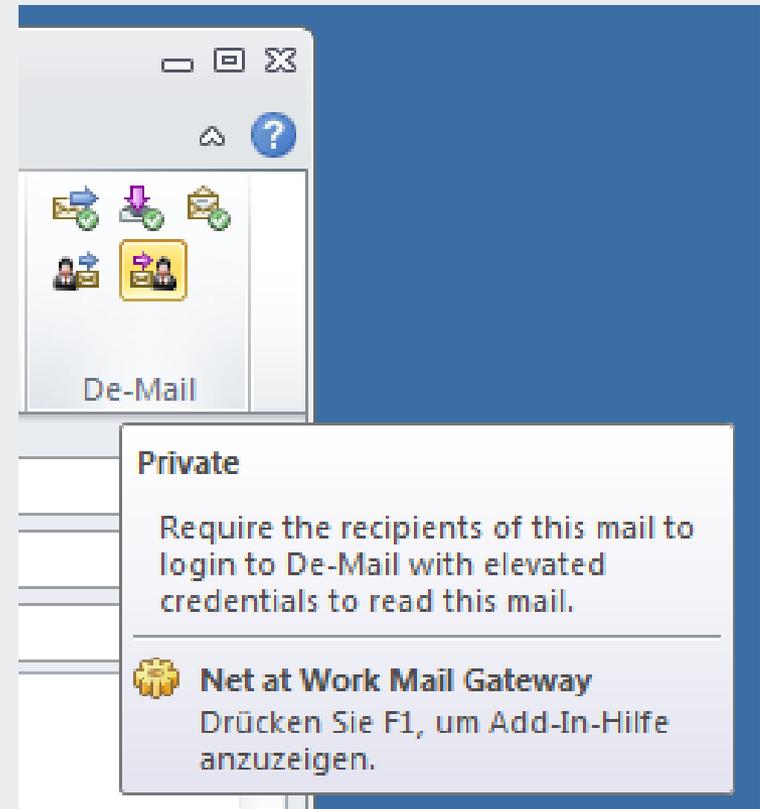
2.3 De-Mail

2.3.1 Standard Nachricht

Absender: henningkrause@netatwork.de-mail.de
Ursprüngliche Empfänger: An: alice@contoso.local
Cc: bob@fabrikam.local
Tatsächliche Empfänger: An: alice@contoso.local
Cc: bob@fabrikam.local

Authentisierungsniveau: Normal
Authentisierungs Mechanismus: password
Nachrichten id: message-id
De-Mail Provider des Absenders: Doller DE-Mail Provider
Provider Zertifikat:
Ausgestellt für: OID.2.5.4.65=TKS 09 A 06403, SERIALNUMBER=1, CN=TKS 09 A 06403, C=DE
Aussteller: OID.2.5.4.65=TKS CA 1:PN, SERIALNUMBER=1, CN=TKS CA 1:PN, OU=T-TeleSec, O=Deutsche Telekom AG, C=DE
Gültigkeit: Vom 25.08.2009 10:30:58 bis 25.08.2012

- Plugin für Outlook 2007/2010
- Im E-Mail-Dialog: Auswahl der De-Mail Versandarten und -optionen
 - Versandbestätigung,
 - Eingangsbestätigung,
 - Abholbestätigung,
 - Absenderbestätigt,
 - Persönlich



United Internet:

„Wir werden mit verschiedenen Preis- und Tarifmodellen starten. So ist es beispielsweise vorstellbar, dass PayMail Kunden zu günstigeren Tarifen De-Mail nutzen können. Die Preismodelle werden mit Produkteinführung vorgestellt. Ziel ist es jedoch, den Basisdienst allen Nutzern so günstig wie möglich zur Verfügung zu stellen.“

Die Kosten werden aber in jedem Fall weniger als 50 Prozent des heutigen Briefportos ausmachen.“

De-Mail

Datenschutz

Welche gesetzliche Datenschutzanforderungen gibt es?

- De-Mail-Gesetz seit dem 03.05.2011, z.B.
 - Funktionalitätsanforderungen (u.a. §§ 3-13, § 16)
 - explizite Sicherheitsanforderungen (z.B. Verschlüsselung zwischen Nutzer und Diensteanbieter sowie unter den Diensteanbietern, § 4 Abs. 3, § 5 Abs. 3)
 - Verweis auf Technische Richtlinie TR 01201
 - Regelungen für „Vertragsdaten“ des Nutzers (u.a. §§ 13, 15, 16)
- allgemeine datenschutzrechtliche Regelungen:
 - Bundesdatenschutzgesetz (BDSG)
 - Telekommunikationsgesetz (TKG)
 - Telemediengesetz (TMG)

- Akkreditierung der Anbieter durch das BSI (§ 18 De-MailG)
- Voraussetzungen:
 - **Testat** bezüglich IT-Sicherheit
 - über technische organisatorische Anforderungen
 - von BSI-akkreditierten Sachverständigen
 - Abnahme durch IT-Sicherheitsdienstleister
 - **Zertifikat** des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)
 - Gutachten: Prüfung durch anerkannte Sachverständige anhand eines Kriterienkatalogs
 - Kriterienkatalog mit TR 01201 verzahnt
 - „Vollprüfung“
 - Abnahme des Gutachtens durch den BfDI

- Beispiele für sinnvolle Verbesserungsmöglichkeiten:
 - Ende-zu-Ende-Verschlüsselung
 - nutzergesteuerte Delegationsmöglichkeiten
 - feingranulare lesende Zugriffsrechte (für Dritte) im Datensafe
 - Angebot von (zusätzlichen) De-Mail-Adressen mit beschränkter Gültigkeitsdauer
 - Online-Auskunftsverfahren
 - Darstellung von Datenschutzeigenschaften durch Icons
 - selbstbestimmte Filterung beim Versand von De-Mails

- Kurzzeitig unverschlüsselt
- Abholbestätigung ohne Öffnen der Nachricht
- Zustellfiktion, wann laufen Fristen
- De-Mail schwer an Domainnamen zu erkennen
- Auskunftsanspruch von Behörden und Privaten:
Brief-Geheimnis vs. Telekommunikations-
Geheimnis
- Nicht-anonyme Nutzung
- Ggf. schleichender Zwang zu De-Mail durch
Gebühren für herkömmlichen Papierbrief

- Deutlich verbesserter Datenschutz bei elektronischer Kommunikation
- Effizienzsteigerung durch Ablösung von Papierpost
- Einheitlicher Kommunikationskanal für Verbraucher
- Basis für Verbreitung der Ende-zu-Ende-Verschlüsselung
- Datenschutz-konform, mit Verbesserungspotential
- Rechtssicherheit muss geprüft werden

Ihre Fragen bitte !

Net at Work Netzwerkssysteme GmbH
Am Hoppenhof 32
33104 Paderborn
www.enqsig.de
Tel: 05251 304 600