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

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

Agenda

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

Motivation für die Entwicklung von De-Mail

Net at Work
Netzwerksysteme

- 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)

De-Mail löst viele dieser Probleme

- 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**

Net at Work
Netzwerksysteme

De-Mail

Das De-Mail-Gesetz

§ 4 - Anmeldung „normal“ und „hoch“

Net at Work
Netzwerksysteme

- 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

§ 5 - Versandoptionen

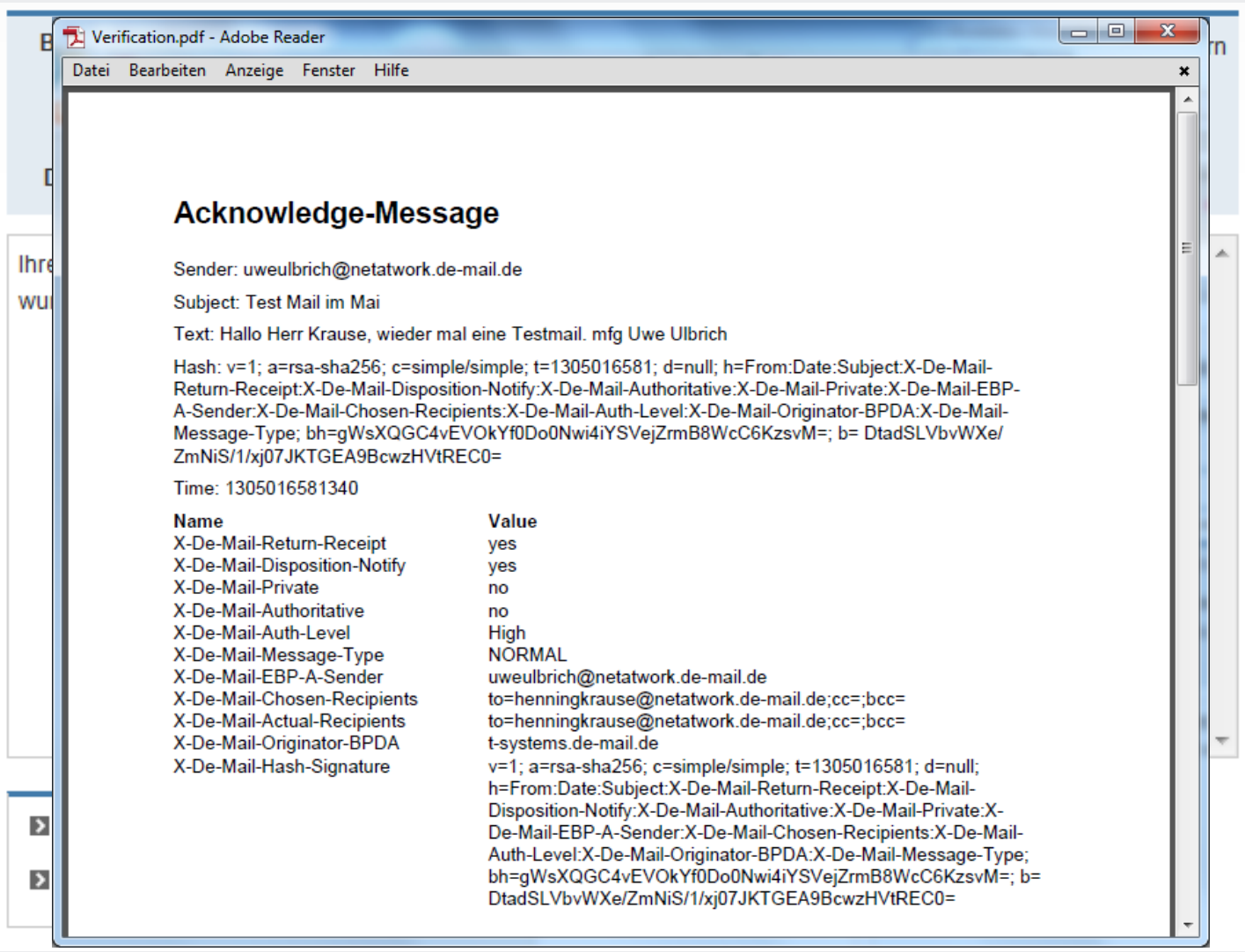
- Persönlich (Abs. 4)
  - Nachricht kann nur mit Anmeldeniveau „hoch“ gelesen werden
- Absenderbestätigt (Abs. 5)
  - Nachricht wurde mit Anmeldeniveau „hoch“ erstellt/versandt

§5 Abs. 7 - Versandbestätigung

Net at Work
Netzwerksysteme

- 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

Versandbestätigung



§5 Abs. 8 - Empfangsbestätigung

- 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 löschbar

Empfangsbestätigung

§5 Abs. 9 - Abholbestätigung

Net at Work
Netzwerksysteme

- 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 löschbar

Zustellfiktion nur mit Zugangsöffnung

- Änderung im Verwaltungszustellungsgesetz

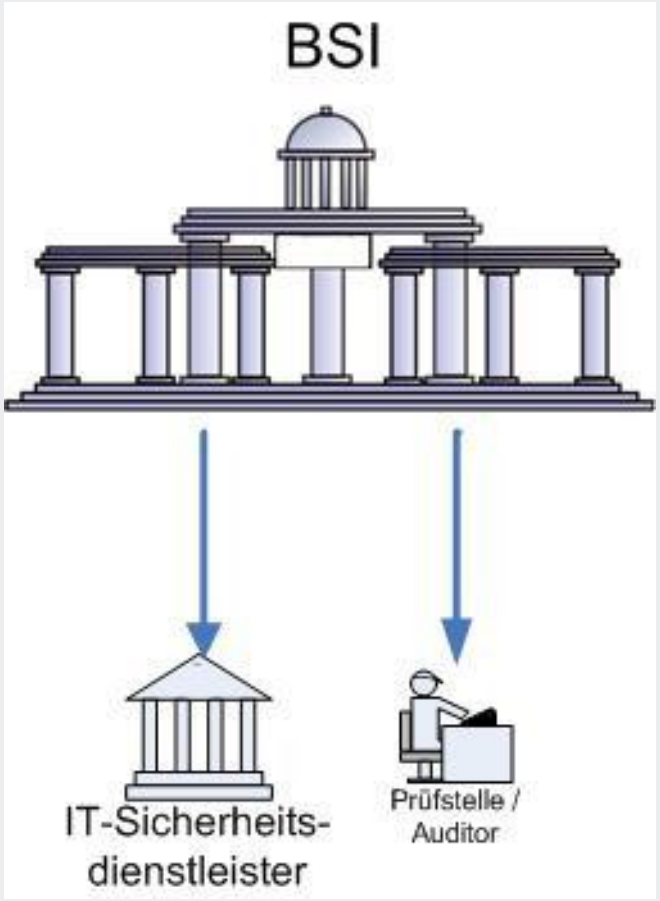
  „Ein elektronisches Dokument gilt in den Fällen des §5 Absatz 5 Satz 2 am dritten Tag nach der Absendung an das De-Mail-Postfach des Empfängers als zugestellt, wenn er dieses Postfach als Zugang geöffnet hat …“

Akkreditierung der Provider

- **§§ 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

Vertrauensanker: Prüfungen



- 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

Quelle: BSI, Mehrfeld/Schumacher

Net at Work
Netzwerksysteme

De-Mail

Konzept und Technik

Standardtechnologien als Basis

Net at Work
Netzwerksysteme

- 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.

Informationsverbund

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

- verschlüsselt
- authentisch und
- nachweisbar

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

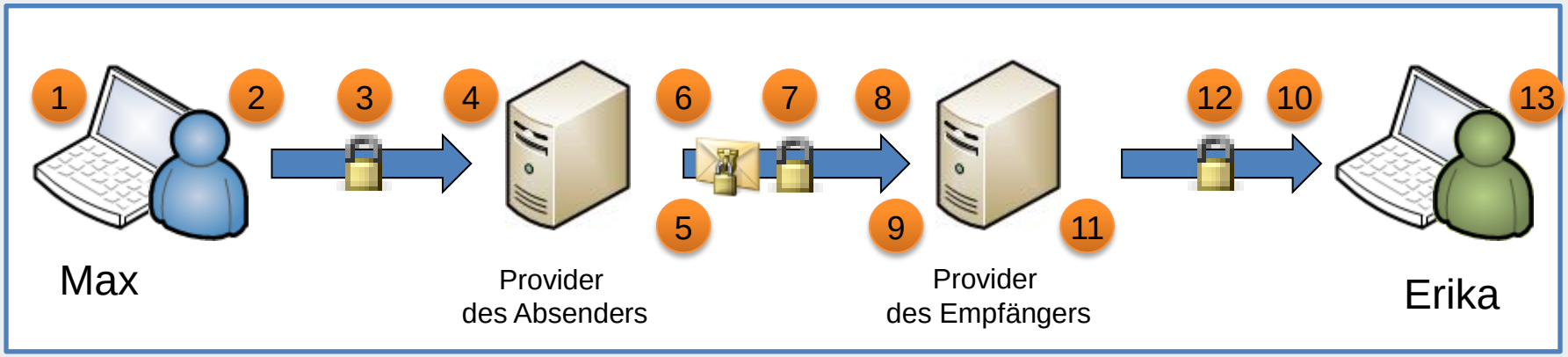
- Deutsche Telekom AG
- United Internet AG (WEB.DE, GMX)
- Mentana Claimsoft AG
- Deutsche Post AG

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

Quelle: BSI, Mehrfeld/Schumacher

Versandweg und Sicherheitsmechanismen

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



Kommunikationswege und Verschlüsselung

Net at Work
Netzwerksysteme

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

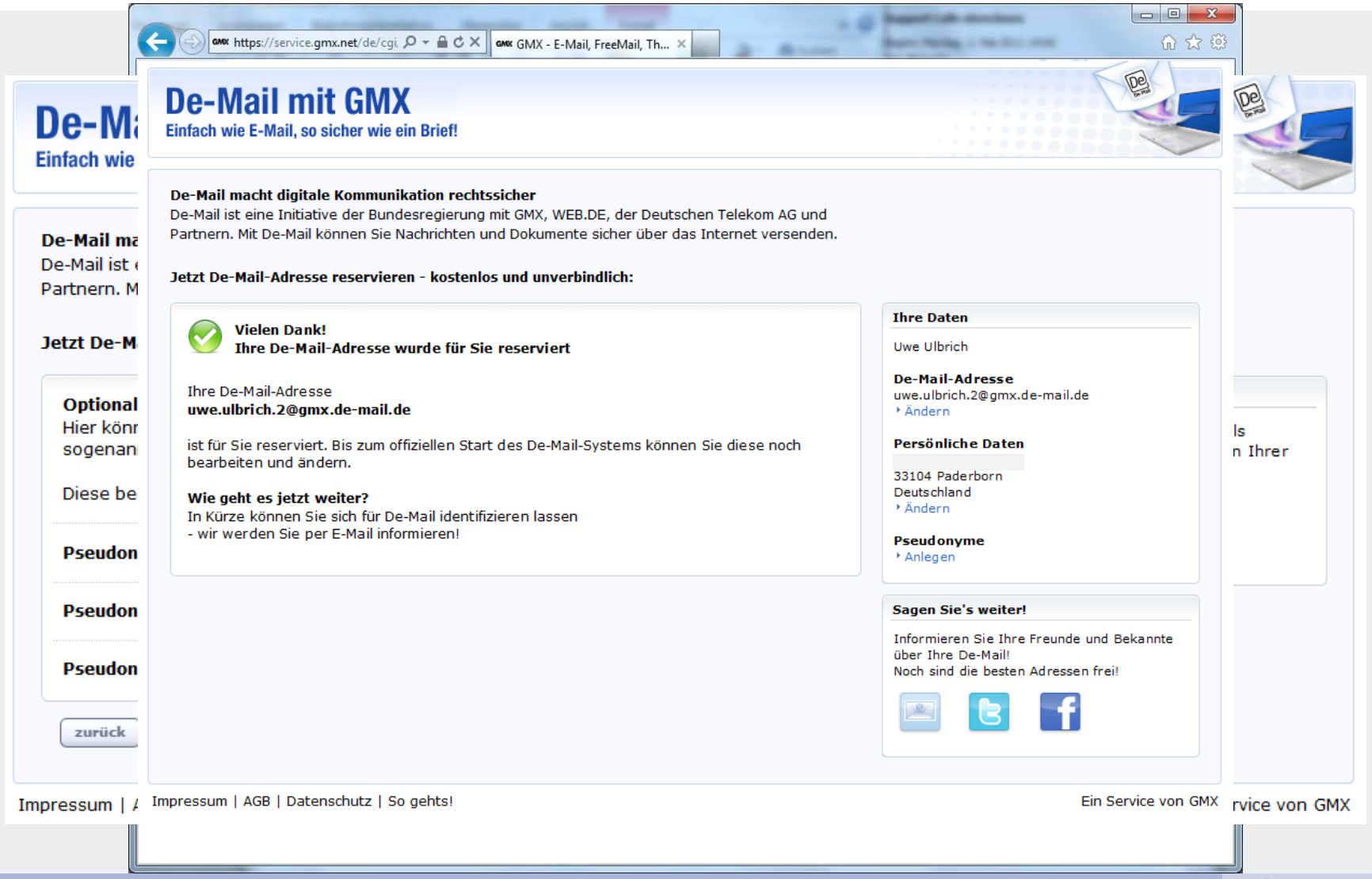
- De-Mail Adressformate
  - Natürliche Personen: Nachname, ggf. Vornamen, Teil des Vor- und Nachnamens
  - Juristische Personen: Kennzeichnung im Domainenteil
  - Pseudonyme

Morgens halb zehn in Deutschland…

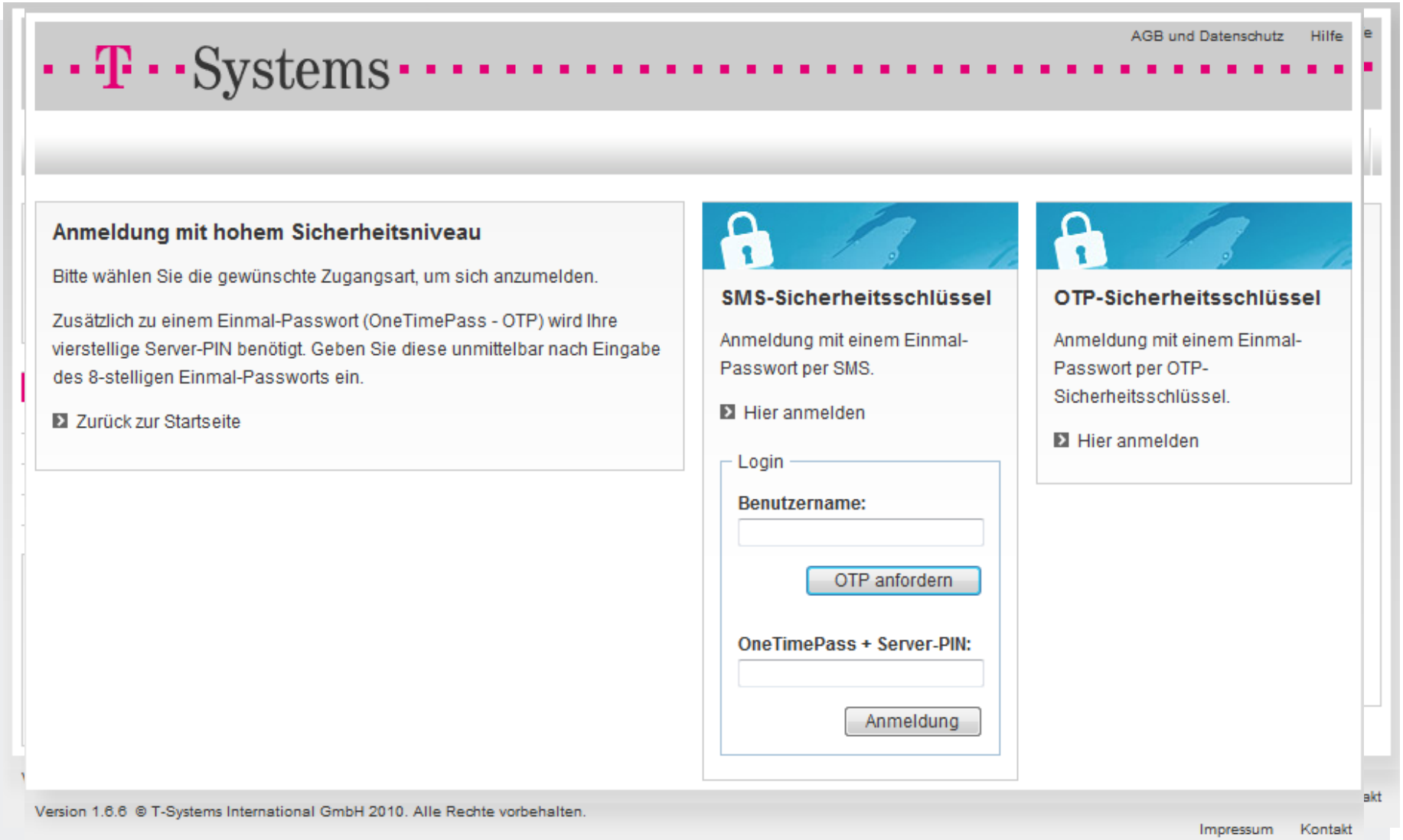
Ende-zu-Ende-Verschlüsselung

- 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

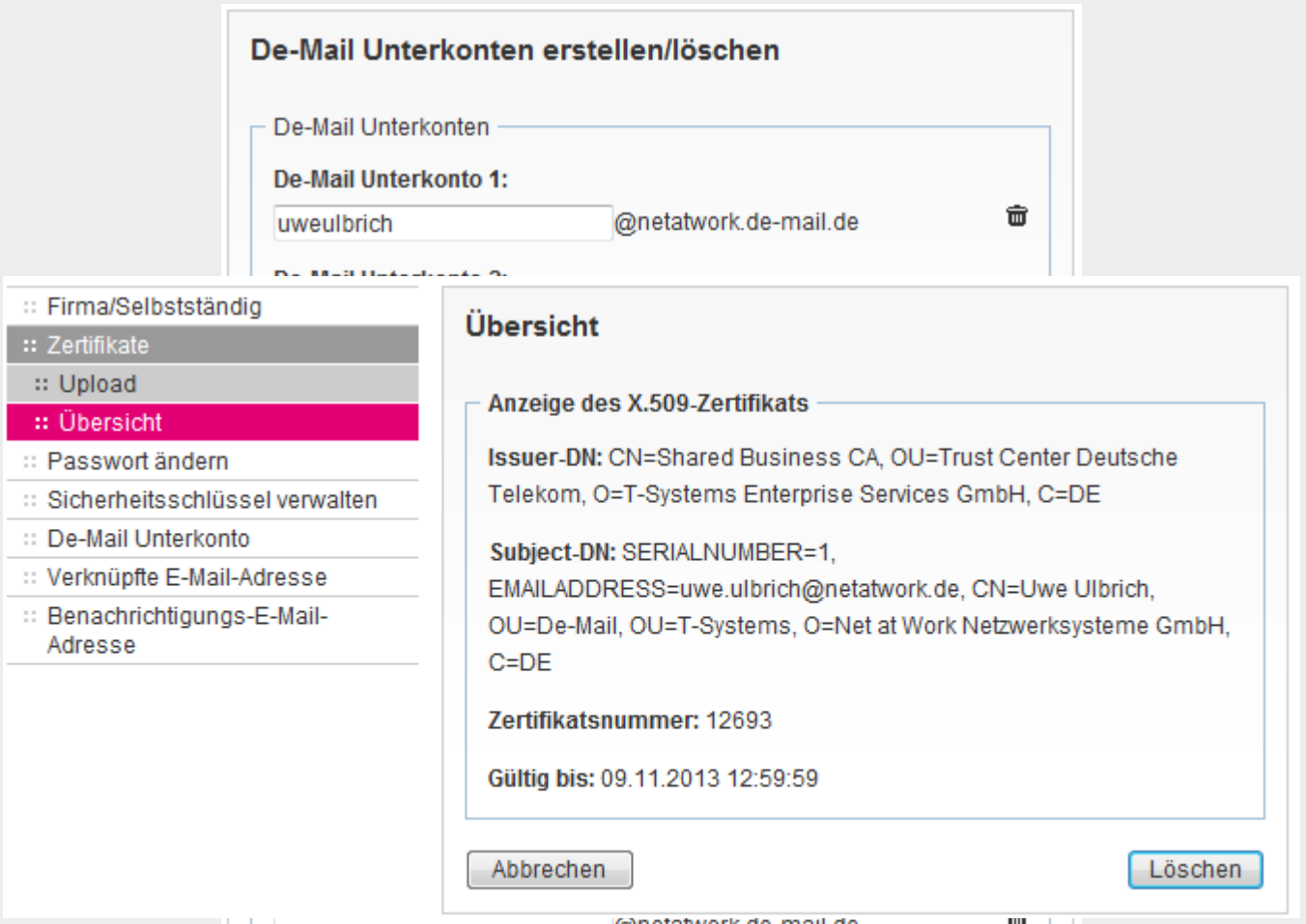
De-Mail Registrierung bei GMX (United Internet)



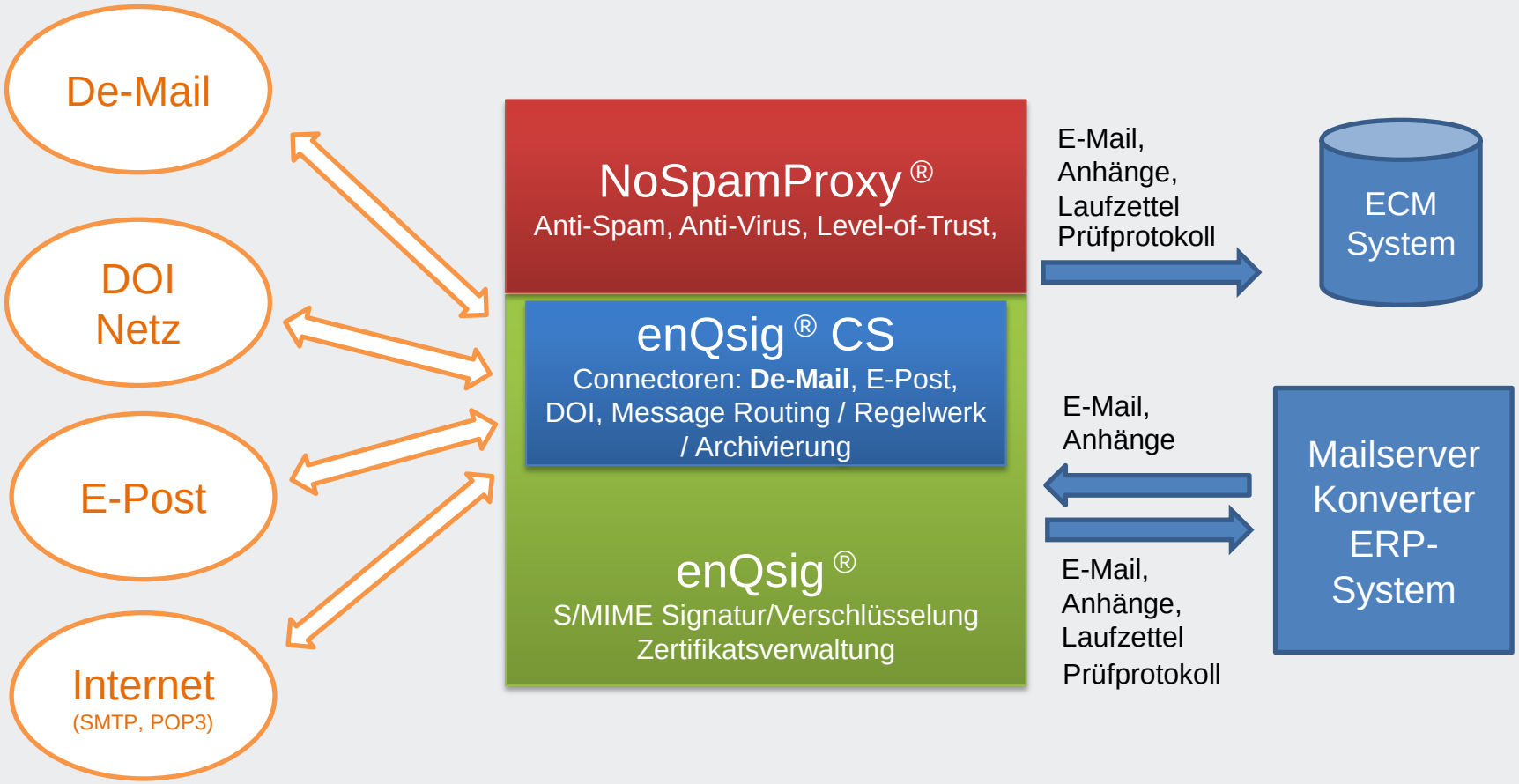
T-Systems De-Mail Postfach



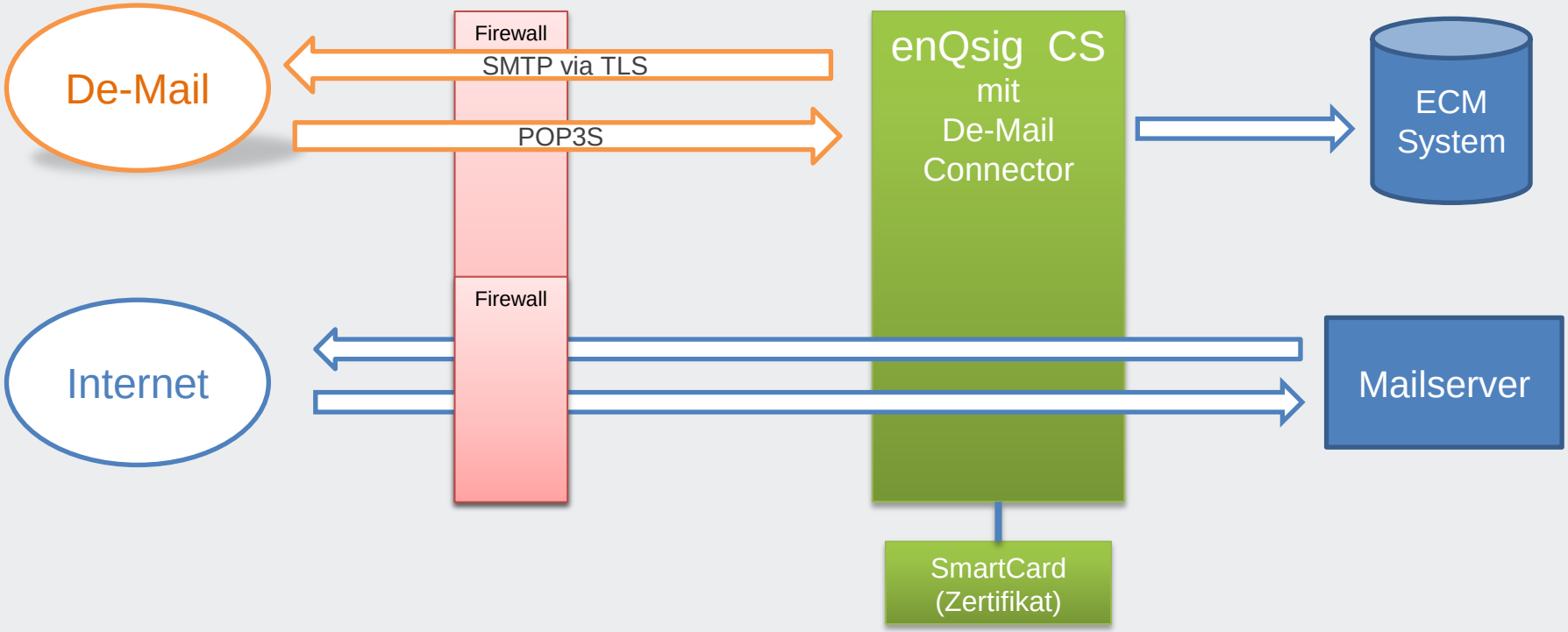
De-Mail Verzeichnis und Behörden-/Firmen-Konten



Net at Work Mail Gateway

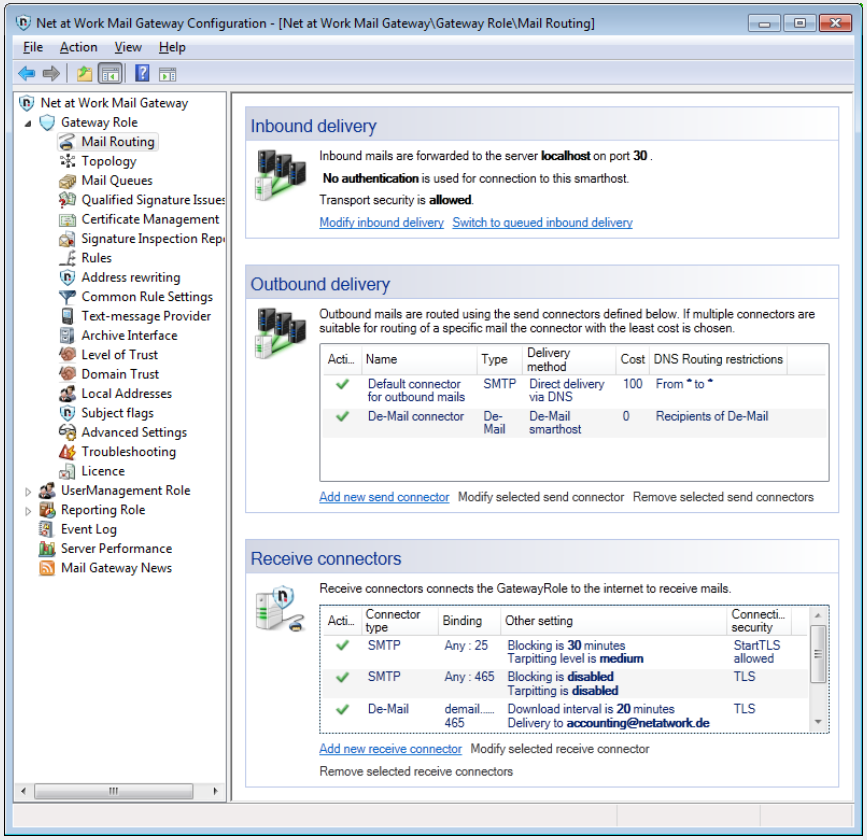


De-Mail-Anbindung - Architektur



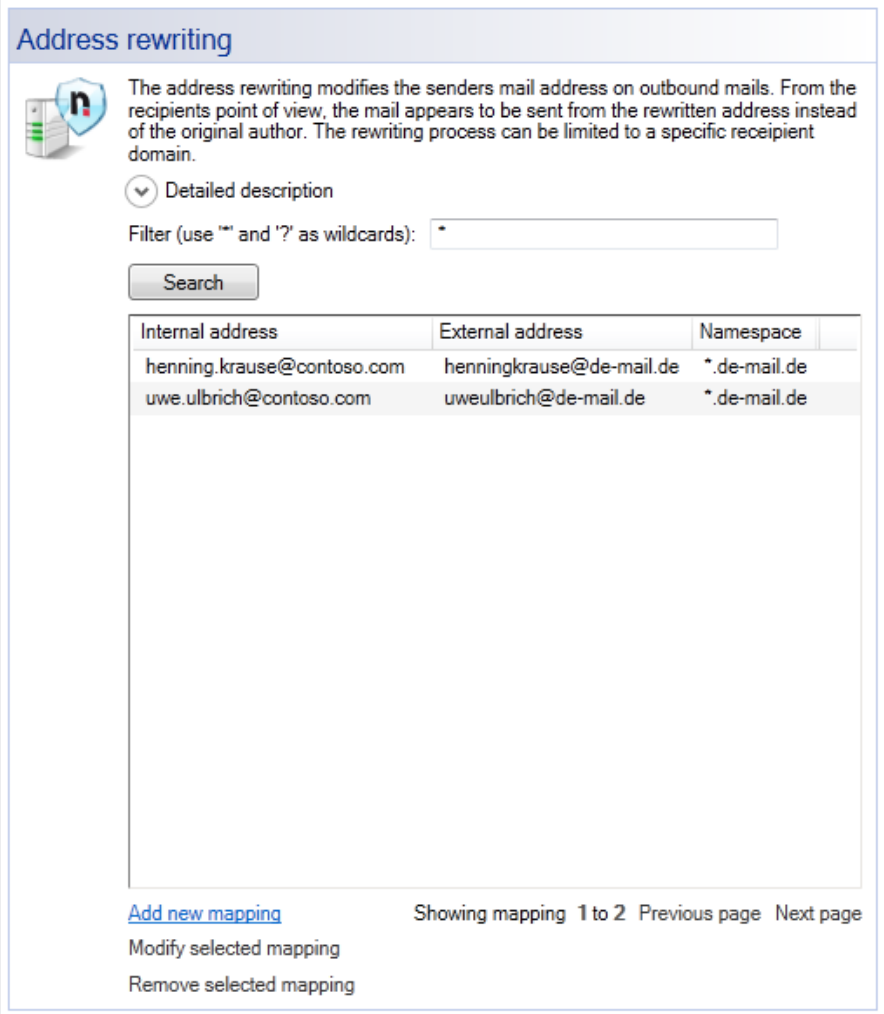
Konnektoren

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



Adressumschreibung

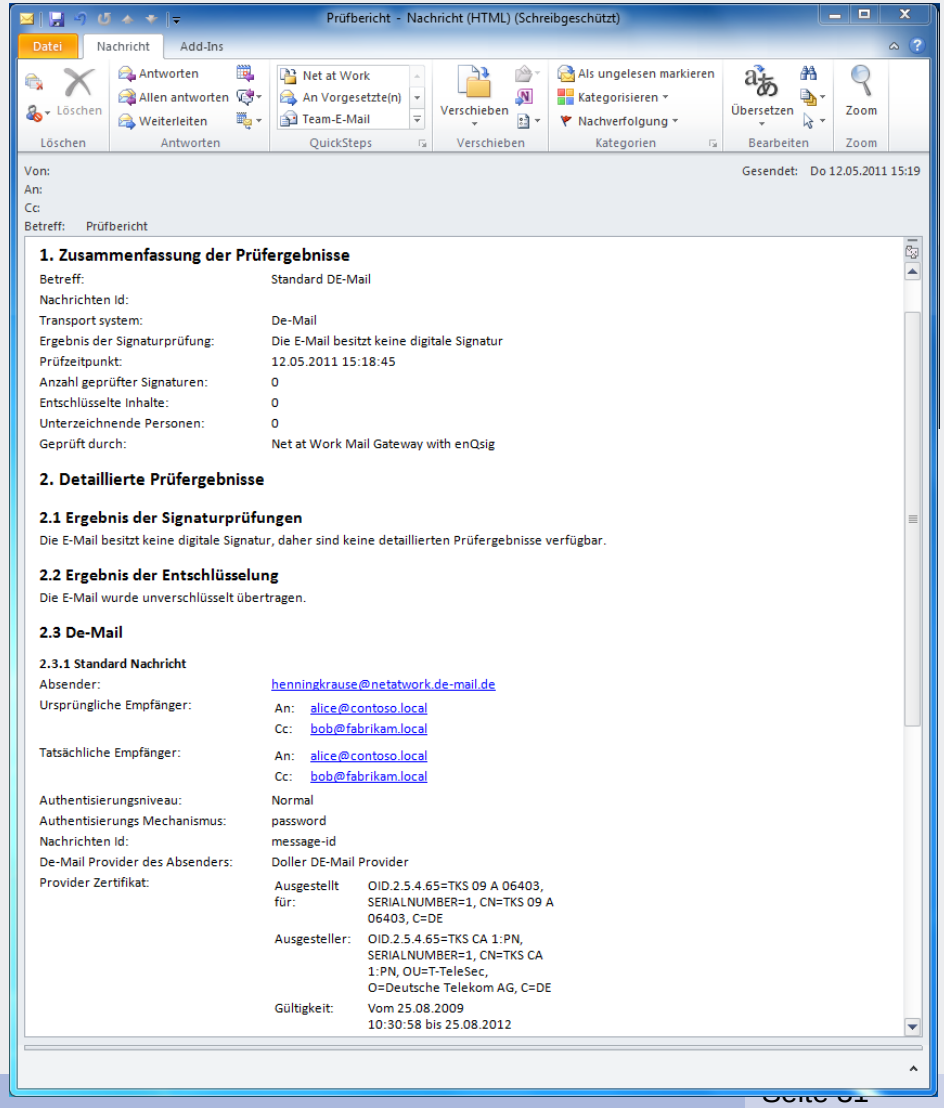
- Durchgängige sichere Identifizierung des Nutzers von der Anwendung bis zum Gateway
  - Absender-Adressen automatisch umgeschrieben
    aus
    henning.krause@netatwork.de
    wird
    henningkrause@netatwork.de-mail.de
  - Berechtigung von Nutzern für De-Mail
- Autorisierung des Gateway-nutzenden Systems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



Kennzeichnung

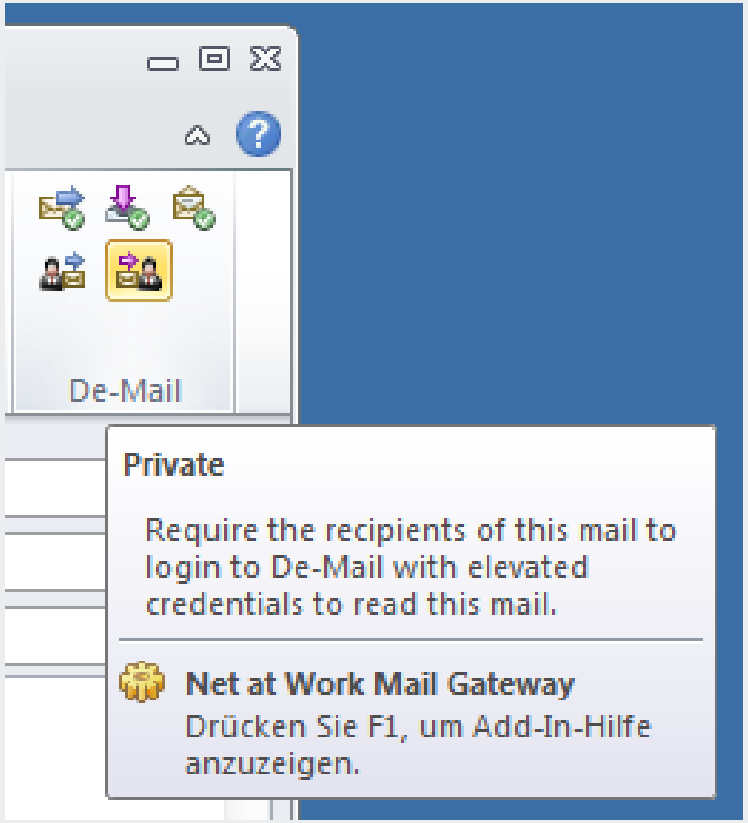
De-Mails werden mit einem Prüfbericht ausgestattet. Dieser wird in Form einer signierten Datei an die E-Mail angehängt.

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



Outlook Integration

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



Kosten von De-Mail

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?

Net at Work
Netzwerksysteme

- 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)

Wie wird die Einhaltung überprüft?

- 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

Verbesserungspotential im Datenschutz

- 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

Kritik an De-Mail

Net at Work
Netzwerksysteme

- 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

Fazit

- 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 Netzwerksysteme GmbH
Am Hoppenhof 32
33104 Paderborn
www.enqsig.de
Tel: 05251 304 600