



De-Mail

So einfach wie E-Mail so sicher wie Papierpost

Kurzvorstellung des Gesamtkonzepts
Aktueller Stand zum Gesetzgebungsverfahren

**Erwin Schwärzer, Leiter des Referates IT1
Jutta Keller-Herder, Referat IT1**

Bundesministerium des Innern



Motivation für die Entwicklung von 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 nicht in der Fläche durchgesetzt (v.a. wg. zusätzlich erforderlicher Installationen)



De-Mail löst viele dieser Probleme

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

- ⇒ **De-Mail soll grundlegende Sicherheitsfunktionen einfach nutzbar und so in der Fläche breit verfügbar machen**
- ⇒ **De-Mail soll so einfach zu nutzen sein wie E-Mail (insbesondere ohne zusätzliche Installationen beim Endnutzer).**





Die Wirtschaft setzt De-Mail um

De-Mail bietet

eine Infrastruktur für die
Kommunikation aller mit allen

- verschlüsselt
- authentisch
- nachweisbar und
- einfach nutzbar.

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





Staat und Wirtschaft agieren gemeinsam

- Die grundlegenden Anforderungen an Sicherheit, Funktionalität und Interoperabilität werden von BMI und BSI gemeinsam mit der Wirtschaft erarbeitet und in Form von Technischen Richtlinien festgeschrieben.
- Die Einhaltung dieser Richtlinien durch De-Mail-Provider wird in einem gesetzlich geregelten Akkreditierungs- und Zertifizierungsverfahren geprüft.
- Deutsche Telekom AG, 1 & 1 Internet AG (web.de, gmx), Mentana Claimsoft und Deutsche Post AG streben zügige Akkreditierung nach Inkrafttreten des Gesetzes an.



Potentielle Provider und interessierte Nutzer

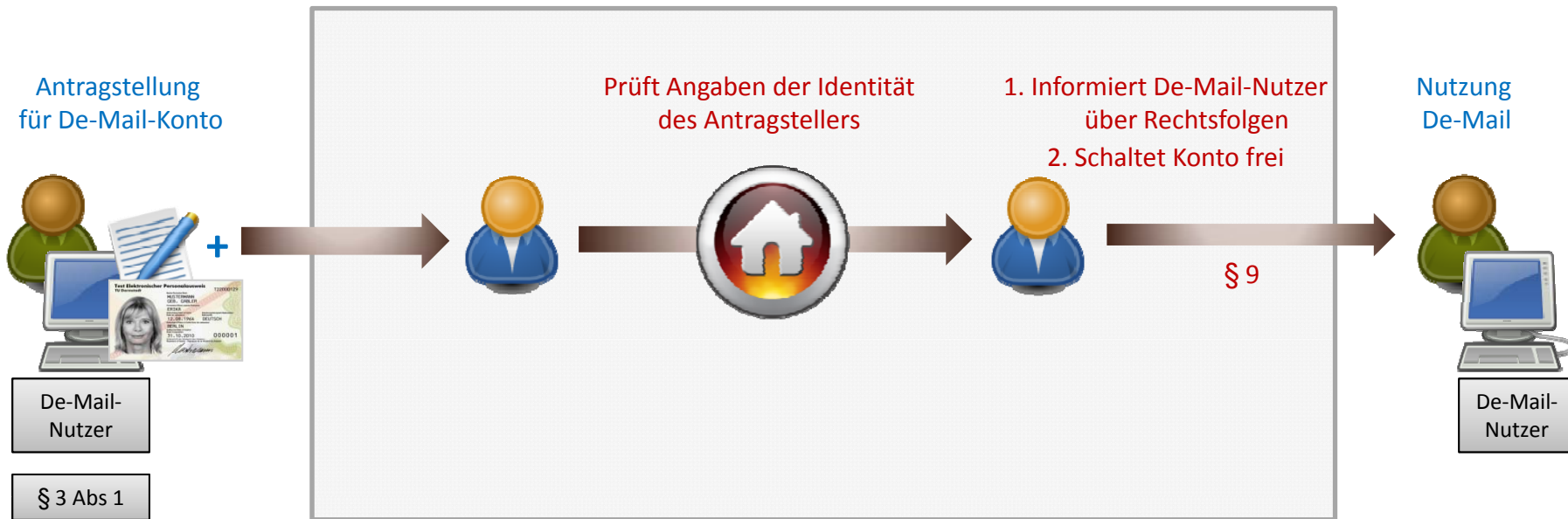
- Pilotierung in Friedrichshafen (Oktober 2009 bis März 2010) zeigte technisch und organisatorische Machbarkeit und Akzeptanz auf
- Provider, die eine Akkreditierung anstreben: DTAG, DPAG, web.de, gmx, menta-na claimsoft
- interessierte Nutzer: Versicherungen, Banken, IHKs
- Verwaltung weitere wichtige Nutzergruppe, allerdings nicht als „Behördenmail“
- existierende Systeme der Verwaltung (z.B. EGVP/OSCI) lassen sich über Gateways mit De-Mail verbinden





Eröffnung eines De-Mail-Kontos

Verantwortungsbereich des De-Mail-Anbieters





Postfach- und Versanddienst

- **Versandarten (§ 5)**
 - Normale De-Mail
 - Qualifizierte De-Mail
 - Für jedermann: (inkl. qualifiziert signierte Versand- und Eingangsbestätigung „De-Mail-Einschreiben“)
 - Nur für öffentliche Stellen: Abholbestätigung
 - Persönlich (Authentisierungsniveau des Empfängers „hoch“)
 - Absender-bestätigt (Authentisierungsniveau des Absenders „hoch“)
- **Zusätzliche Optionen**
 - Ende-zu-Ende-Verschlüsselung
(De-Mail-Provider bietet Verzeichnisdienst u. a. für Verschlüsselungszertifikate, § 7)
 - Qualifizierte elektronische Signatur
(auf Basis vorhandener Komponenten des Nutzers)



De-Ident, De-Safe, Verzeichnisdienst

- De-Ident für die sichere Übermittlung von Identitätsangaben

Altersnachweis

Hiermit wird die Richtigkeit folgender
Identitätsdaten des Absenders bestätigt:

Absender-De-Mail-Adresse

18 Jahre oder älter: ja

Datum: 22.09.2010



Adressnachweis

Hiermit wird die Richtigkeit folgender
Identitätsdaten des Absenders bestätigt:

Absender-De-Mail-Adresse

Name: Meier

Vorname: Hans

Strasse: Hauptstr. 36

PLZ: 01234

Ort: A-Dorf

Datum: 22.09.2010

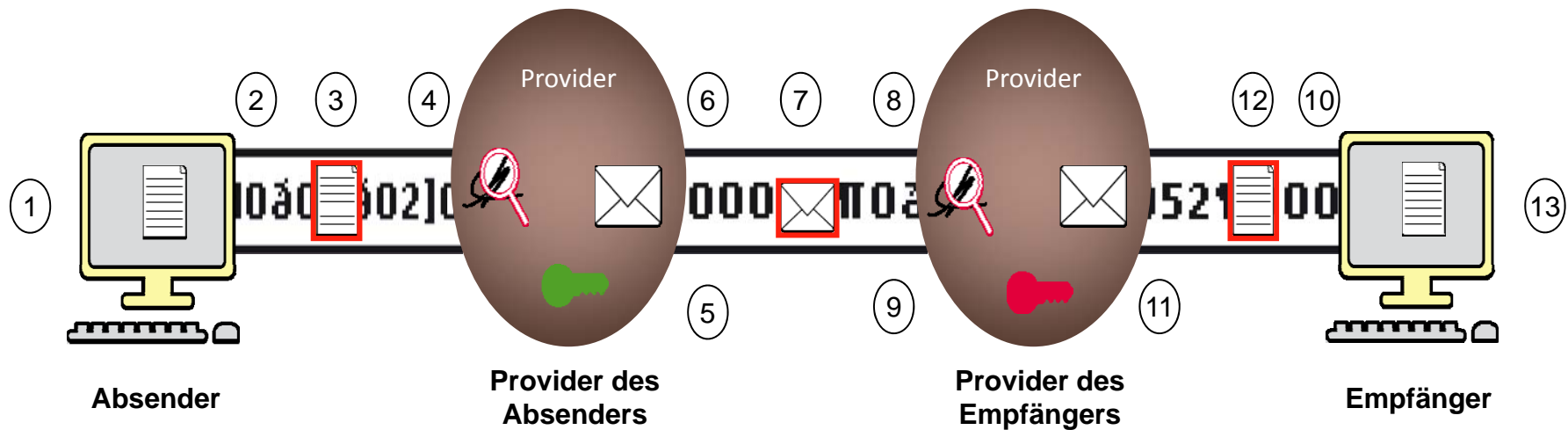


- De-Safe für sicheres Ablegen wichtiger Inhalte
- Verzeichnisdienst



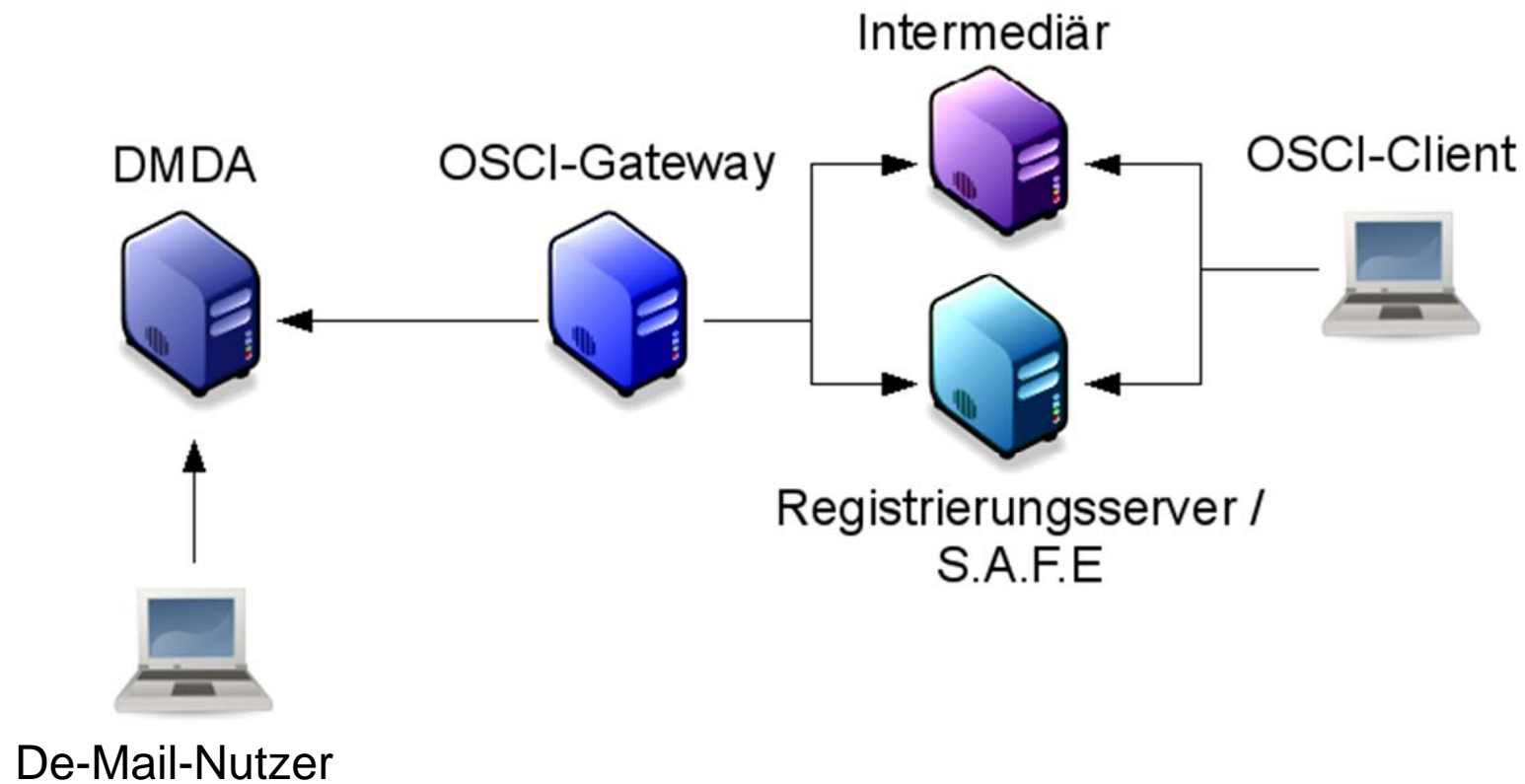
Ziel: grundlegende Sicherheitsfunktionen einfach nutzbar für den Anwender

1. De-Mail erstellen
2. Aufbau eines verschlüsselten Kanals
3. Versenden der De-Mail
4. Kurzzeitige automatisierte Prüfung (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 (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





Gateway zwischen EGVP/OSCI und De-Mail





Eckpunkte De-Mail-Gesetz (1)

Art. 1 De-Mail-Gesetz

- **Angebote der Provider**
 - Eröffnung De-Mail-Konto, § 3
 - (Sichere) Anmeldung („Einloggen“), § 4
 - Postfach- und Versanddienst , § 5
 - Identitätsbestätigungsdienst, § 6
 - Dokumentenablage, § 8
 - Verzeichnisdienst, § 7
- **Kontonutzung**
 - Informationspflichten ggü Nutzer, § 9
 - Kontosperrung und –auflösung, § 10
 - Einstellung Tätigkeit, Vertragsende § 11f
 - Dokumentation § 13 u Auskunft, § 16
- **Akkreditierung, § 17 und hierzu Voraussetzungen /Nachweise, § 18:**
 - Fachkunde/Zuverlässigkeit ,Nr. 1
 - Deckungsvorsorge, Nr. 2
 - Funktionalität /Interoperabilität/IT-Sicherheit, Nr. 3
 - Datenschutz, Nr. 4
- **zuständige Behörde, § 2 und Aufsicht, §§ 20 u 21: BSI**
- **Weiterentwicklung durch Ausschuss De-Mail-Standardisierung, § 22**



Eckpunkte De-Mail-Gesetz (2)

Art. 2 De-Mail-Gesetz: Änderung ZPO

- Änderung von § 174 Abs. 3 ZPO: Elektronische Dokumente können von Gerichten per De-Mail an Verfahrensbeteiligte (bei ausdrücklicher Zustimmung) zugestellt werden.
- Zur Wirksamkeit der Zustellung muss der Empfänger den Erhalt durch ein Empfangsbekenntnis bestätigen, welches an das Gericht zurückzusenden ist (§ 174 Abs. 4 ZPO). Dies geht (noch?) nicht per De-Mail (wg. § 130a ZPO-> weitere Anpassungen der Gesetzeslage notwendig).

Art. 3 De-Mail-Gesetz: Änderung VwZG

- Neuer § 5a: Elektronische Zustellung gegen Abholbestätigung über De-Mail-Dienste
- An Stelle des Empfangsbekenntnisses tritt die sog. „Abholbestätigung“
- Diese wird „ausgelöst“, wenn Empfänger sich an seinem De-Mail-Konto sicher angemeldet hat.

Art. 4 Evaluierung

- Anpassungs-/Ergänzungsbedarf von Regelungen insbesondere betreffend Zustellung und Verbraucherschutz Zertifizierung, spätestens nach 3 Jahren



Status und nächste Schritte

- Stand des Gesetzgebungsverfahrens (BT-Drs 17/3630, 17/4145)
 - Regierungsentwurf vom Bundeskabinett beschlossen 13.10.2010
 - 1. Lesung Bundestag 11.11.2010
 - Bundesrat 1. Durchgang 26.11.2010
 - Öffentliche Anhörung vor Innenausschuss BT 07.02.2011
 - Abschließende Beratung im Innenausschuss BT 23.02.2011
 - 2./3. Lesung Bundestag 25.02.2011
 - Bundesrat 2. Durchgang 18.03.2011
 - Verkündung Ende März 2011
- Die notwendigen Voraussetzungen für die Testierung (früher „Zertifizierung“) von De-Mail-Providern stehen zur Verfügung.
- Einführung von De-Mail angestrebt für Frühjahr 2011

Vielen Dank für Ihre Aufmerksamkeit!

Bundesministerium des Innern

Alt-Moabit 101D

10559 Berlin

Erwin Schwärzer, Leiter des Referates IT1

E-Mail: erwin.schwaerzer@bmi.bund.de

Telefon: 030 18 681-2326

Jutta Keller-Herder, Referat IT1

E-Mail: jutta.kellerherder@bmi.bund.de

Telefon: 030 18 681-1564