



# De-Mail

Gedanken zum E-Government 2.0

Matthias Matousek

12. Oktober 2010



- 1 Ziele
- 2 Was ist De-Mail?
  - Provider
  - Postfach- und Versanddienst
  - Verzeichnisdienst
  - De-Ident
  - De-Safe
- 3 Sicherheit
  - Technologie
  - Organisation
- 4 Kritik



# Umfrage

- Wer hat schon von De-Mail gehört?
- Wer weiß was De-Mail ist?
- Wer kennt Details der Funktionsweise und/oder des rechtlichen Stellenwerts von De-Mail?



## Ziele, die mit De-Mail erreicht werden sollen

- Die Gesellschaft ins digitale Zeitalter bringen
- Gleichstellung der elektronischen Kommunikation mit dem Papier-Brief
- Rechtssicherheit
- Vertrauliche Kommunikation ermöglichen
- Weniger Papierverbrauch → Kosteneinsparung und Umweltschutz
- Schneller als Papierpost



## Was ist De-Mail?

Mit *De-Mail* werden verschiedene Dienste bezeichnet, welche auf dem De-Mail Gesetz basieren (ursprünglich Bürgerportalgesetz). Das Gesetz wurde noch nicht verabschiedet. De-Mail soll noch im Jahr 2010 zur Verfügung stehen.



# Provider

- Dienstanbieter verlangen Gebühren für De-Mail Dienste
- Dienstanbieter werden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditiert
- Sie müssen nachweisen, dass:
  - sie organisatorische und technische Maßnahmen umsetzen, die den internen und externen Zugriff auf Daten durch Unberechtigte verhindern.
  - die angebotenen De-Mail Dienste interoperabel angeboten werden, also mit anderen Providern zusammenarbeiten.
- Genaue Testfälle in der entsprechenden Technischen Richtlinie des BSI



Bisher beteiligte Provider:

- GMX ([www.gmx.de-mail.de](http://www.gmx.de-mail.de))
- Mentana ([www.govmail.de-mail.de](http://www.govmail.de-mail.de))
- T-Home ([www.t-online.de-mail.de](http://www.t-online.de-mail.de))
- T-Systems ([www.t-systems.de-mail.de](http://www.t-systems.de-mail.de))
- WEB.de ([www.web.de-mail.de](http://www.web.de-mail.de))

Die Deutsche Post war ursprünglich beteiligt, hat aber jetzt stattdessen ihr eigenes Projekt, den E-Postbrief, gestartet.



# Nutzerkonten

- De-Mail Konten sowohl für natürliche als auch für juristische Personen möglich
- Jeder Benutzer muss sich identifizieren (z.B. mit elektronischem Personalausweis oder per Post-Ident)





# Postfach- und Versanddienst

- Kommunikation vergleichbar mit E-Mail
- Aber **keine** normalen E-Mails an De-Mail Adressen und umgekehrt
- Verschiedene Versandarten:
  - De-Mail
  - De-Mail-Einschreiben
- Weitere Optionen: *Persönlich, Absender-bestätigt, Versand-, Empfangs- und Abholbestätigung*
- Ende-zu-Ende Verschlüsselung nicht als Teil des Systems vorgesehen (Verzeichnisdienst des Providers für Zertifikate)



- De-Mail-Adresse der Form  
`<Vorname>.<Nachname>@<Provider>.de-mail.de`
- Zusätzlich Pseudonyme der Form  
`pn_<Pseudonym>@<Provider>.de-mail.de` möglich
- Diensteanbieter und juristische Personen erhalten Subdomains unter `de-mail.de`



# Verzeichnisdienst

- Provider bieten einen Verzeichnisdienst für eigene Zertifikate
- Somit soll Ende-zu-Ende Kryptographie unterstützt werden



# De-Ident

- Vgl. Post-Ident
- Z.B. für Altersnachweis bei Onlineshops
- Der Identitätsnachweis wird per De-Mail an den Empfänger gesendet



# De-Safe

- Langfristige Speicherung von digitalen Dokumenten
- Verschlüsselt und integritätsgesichert



- Alle Verbindungen sind verschlüsselt und gegenseitig authentisiert
- Eingesetzte Technologien:
  - SMTP
  - TLS
  - HTTP(S)
  - X.509
  - optional POP, IMAP, OSCI, ...
- Sobald der Provider eine Nachricht erhält, verschlüsselt er diese und sorgt für eine Integritätssicherung



- Provider müssen ihren Dienst so organisieren, dass kein einzelner Mitarbeiter Zugriff auf unverschlüsselte Daten hat.
- Verschiedene Authentisierungsniveaus:
  - *Normal*: Anmeldung mit Benutzername und Passwort; eingeschränkte Funktionalität
  - *Hoch*: Zusätzlich zur normalen Anmeldung "Besitz und Wissen" nachweisen (z.B. durch TAN, die an Mobiltelefon gesendet wird)



# Kritik

- Per Default keine Ende-zu-Ende Verschlüsselung (dadurch Mitlesen und Manipulation möglich)
- Die Verschlüsselung und Signierung wird durch die Provider durchgeführt
- Es existieren Zweifel an Zuverlässigkeit mancher Diensteanbieter
- Eine De-Mail gilt drei Tage nach dem Versenden als Zugestellt





- Personen- und Verbindungsdaten sind an einer zentralen Stelle zusammengeführt
- Die hinterlegten Daten sind für viele Behörden ohne richterliche Anordnung einsehbar
- Elektronisch vorhandene Daten sind leicht automatisiert überprüfbar
- Vorratsdatenspeicherung ist nicht ausgeschlossen



- De-Mail Adressen sind durch ihre klare Struktur leicht zu erraten (Spamanfällig?)
- Im Gegensatz zum Briefkasten muss man sich für De-Mail identifizieren
- Es ist ungeklärt, welche Beweiskraft die De-Mail haben wird und wer bei Missbrauch die Beweislast trägt



## Zusätzliche Kritik am E-Postbrief

- Fällt nicht unter das Briefgeheimnis
- Adresshandel
- Keine sichere Löschung der Daten (Nachrichten und Personendaten)
- Zum Teil teurer als Papierbrief
- *Security Through Obscurity*



# Umfrage

- Wer möchte De-Mail einsetzen?
- Wie ist eure Meinung zu De-Mail?



## Quellen

- [http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail\\_node.html](http://www.cio.bund.de/DE/IT-Projekte/De-Mail/demail_node.html)
- [https://www.bsi.bund.de/cln\\_156/DE/Themen/EGovernment/DeMail/DeMail\\_node.html](https://www.bsi.bund.de/cln_156/DE/Themen/EGovernment/DeMail/DeMail_node.html)
- Chaosradio-Folge "Digitale Postkarten"  
<http://chaosradio.ccc.de/cr159.html>
- Entsprechende Artikel in der Wikipedia (De-Mail und E-Postbrief)
- De-Mail-Gesetz Referentenentwurf  
<http://www.netzpolitik.org/2010/referentenentwurf-vom-de-mail-gesetz/>