De-Mail

A reliable and secure online communication platform

Armin Wappenschmidt (secunet)

More information: www.de-mail.de

Agenda

- Overview of De-Mail

- Implementation aspects

- Current status and outlook

- Summary

Agenda

- Overview of De-Mail

- Implementation aspects

- Current status and outlook

- Summary

De-Mail: A new approach for reliable and secure online communication

Why?
➢ Electronic communications with legal consequences

Note!
- Postal mail is used mostly for documents with legal consequences
- Email is a mass communication medium
- Email encryption technologies are not well accepted by users

How?
1. Use standard email as the basis technology
2. Implement security mechanisms by trustworthy service providers
3. Ensure reliable registration
4. Define legal framework

Solution! **De-Mail: simple as email and secure as postal mail**

Relevant aspects of the legal framework

■ Compared to existing email services, no additional logging of information is claimed

■ Opening of accounts/mail boxes is to one's own volition for citizens and legal entities

■ Identity of each user must be verified reliably

■ Each citizen may claim one or more pseudonym addresses

■ For communication with legal consequences, a strong authentication method must be used

■ Private service providers must prove the fulfillment of all requirements in an certification procedure

Certification aspects

- Functionality

- Interoperability

- Information security

- Privacy and data-protection

De-Mail services

- **De-Mail**
  - Mail service for reliable and secure electronic communication
  - Authentic addresses for senders and recipients, e.g.
    - Michael.Meyer@my-provider.**de-mail.de**
    - sales@my-company.**de-mail.de**
  - Confidential and tamper-proofed transmission
  - Reliable notification of transmission and delivery

- **De-Safe**
  - Long-term storage with protection against loss or manipulation

- **De-Ident**
  - Sending confirmed identity data on user's request, e.g. age or postal address

➢ Support of standard web browsers and email clients

Agenda

- Overview of De-Mail

- Implementation aspects

- Current status and outlook

- Summary

Accounts and addresses

- Accounts for citizens and legal entities

- Reliable initial registration for legal consequences of the communication

- Standardized address format for authentic addresses, e.g.
  - Michael Meyer: **Michael.Meyer**@my-provider.de-mail.de
  - Pseudonym: **pn**_mickeymouse@my-provider.de-mail.de
  - "My Company": sales@**my-company**.de-mail.de

![De-Mail logo]

Scalable security

- Authentication

  - From username/password to eID card

  - Examples for strong authentication

    - OTP-Token, OTP-Mobile SMS, smartcard
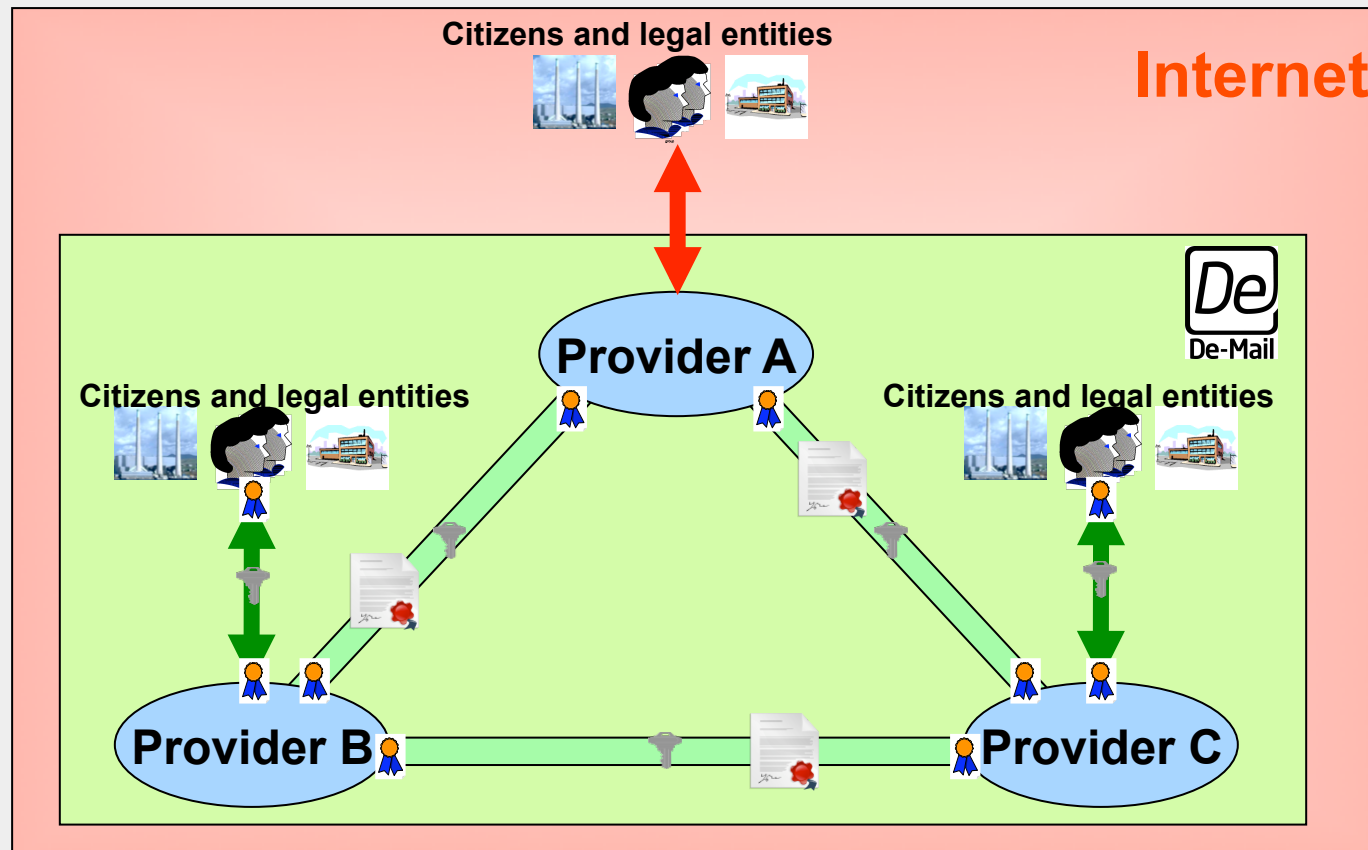
  - Required authentication level depends on usage
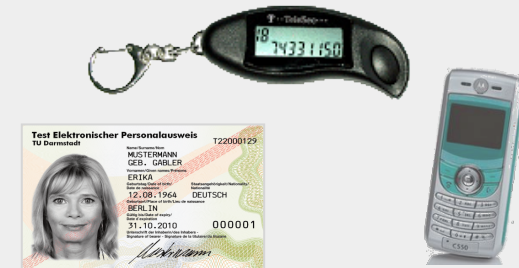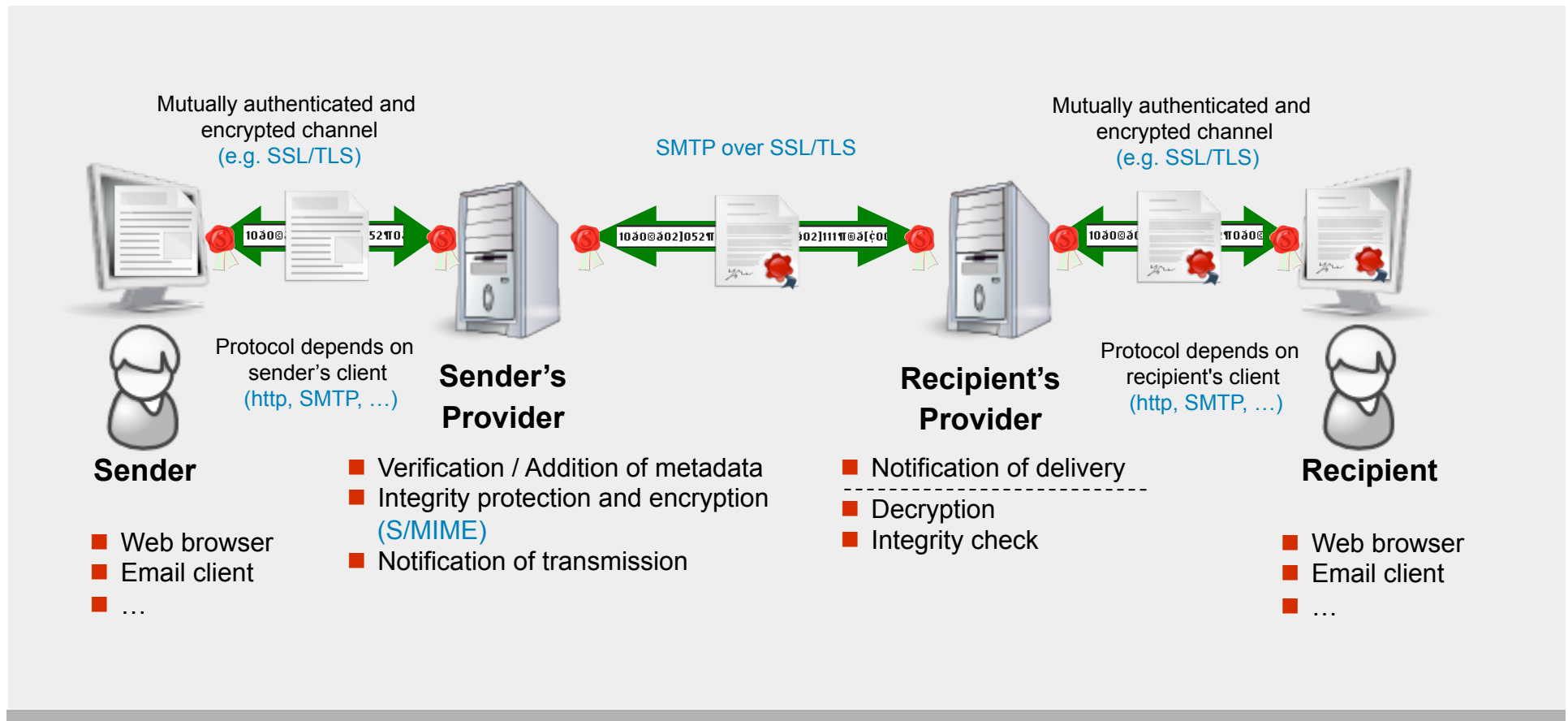
- Confidentiality and Integrity

  - Optional end-to-end encryption and (qualified) electronic signature

  - Supported by a directory for user certificates and by a verification service

Overview of the
reliable and secure communication

Default transmission security

Mutually authenticated and encrypted channel (e.g. SSL/TLS)

SMTP over SSL/TLS

Mutually authenticated and encrypted channel (e.g. SSL/TLS)

Protocol depends on sender's client (http, SMTP, …)

Sender's Provider

Protocol depends on recipient's client (http, SMTP, …)

Recipient's Provider

Sender

- Web browser
- Email client
- …

- Verification / Addition of metadata
- Integrity protection and encryption (S/MIME)
- Notification of transmission

- Notification of delivery
- Decryption
- Integrity check

Recipient

- Web browser
- Email client
- …

Linking legal entities to De-Mail
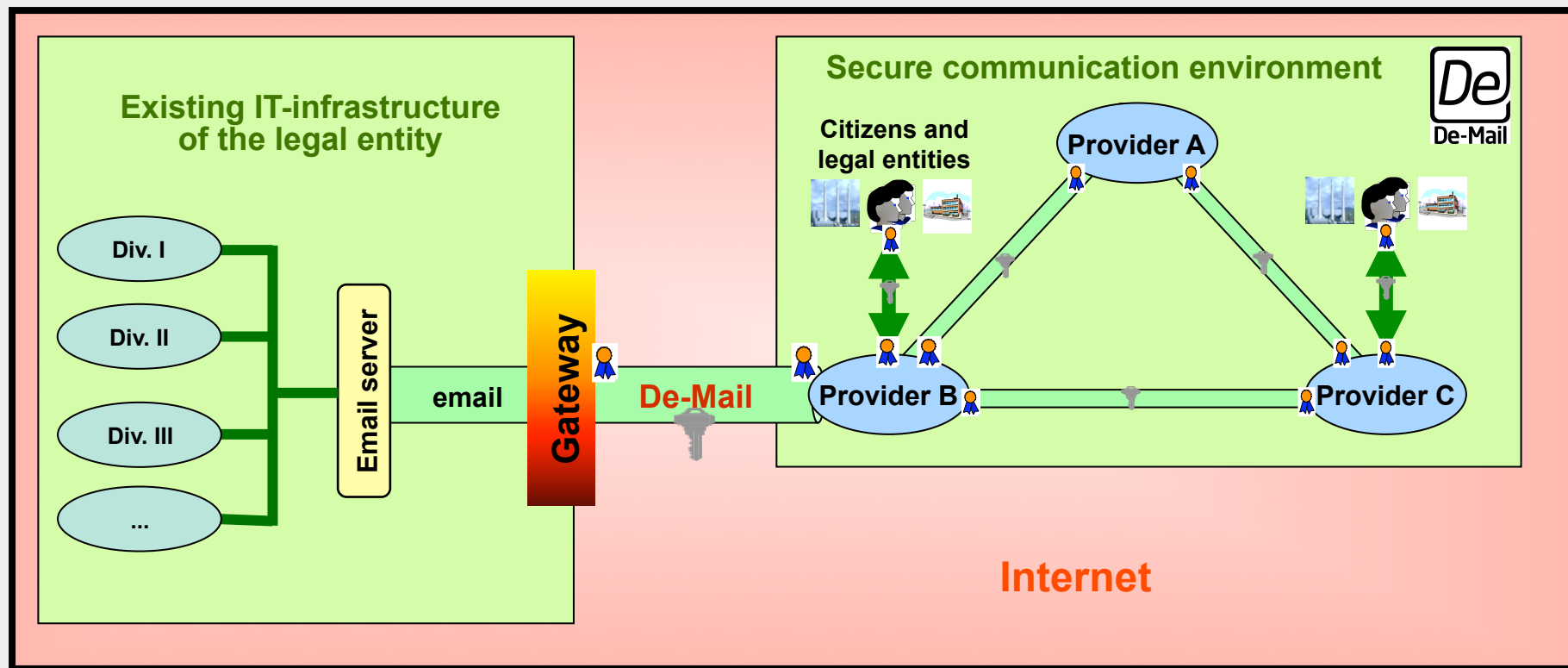
Agenda

- Overview of De-Mail

- Implementation aspects

- Current status and outlook

- Summary

Time schedule

De-Mail

2007	2008	2009	2010

- Technical conception
- Studies for acceptance, privacy-protection, law and interoperability
- Market analysis
- Conception of certification scheme
- Legislation

Pilot
- Preliminary
- Development, Implementation
- Operation

now

Pilot partners

De-Mail

Businesses and administrations: GDV – DIE DEUTSCHEN VERSICHERER, Gothaer, LVM Versicherungen, AMB GENERALI, HUK-COBURG – Aus Tradition günstig, FRIEDRICHSHAFEN, IHK Industrie- und Handelskammer Bodensee – Oberschwaben, Handwerkskammer Ulm, Volksbank Friedrichshafen eG, Sparkasse Bodensee, ZF, EADS DEFENCE & SECURITY

Providers: WEB.DE, united internet, GMX, T·Home, T·Systems, mentana claimsoft

Individuals: citizens, lawyers, notaries, tax consultants, public accountants, craftsmen, …

International activities

- ETSI – REM (Registered E-Mail)

  - Trusted delivery of e-mail equivalent to postal services

- UPU – .post

  - New top level domain for worldwide postal sector with strict policy for issuing domains

  - Guaranteeing the sender's authenticity

- EU – EIIS (European Interoperability Infrastructure Services) within IADBC

  - Study on potential reuse of service modules and components

- EU – SPOCS (Simple Procedures Online for Cross-border Services)

  - Work package 3: "Interoperable delivery, eSafe, secure and interoperable exchanges and acknowledgement of receipt"

Agenda

- Overview of De-Mail

- Implementation aspects

- Current status and outlook

- Summary

Benefits of De-Mail

- **Easy to use**
  - No additional technical equipment needed for users
  - Security mechanisms implemented by trustworthy providers

- **Authentic communication**
  - Addresses referring to reliable registered identities

- **Scalable security**
  - Different authentication levels
  - Support of end-to-end encryption and electronic signatures
  - Notifications as needed

De-Mail: simple as email and secure as postal mail

Thank you!

Armin Wappenschmidt
secunet SwissIT AG
wappenschmidt@swiss-it.ch

External consultant in the German project „De-Mail"