

The German "Bürgerportal" A Secure Email and e-Government System?

hg
Horst-Görtz Institut
für IT Sicherheit

Dr. Christoph Wegener

Dominik Birk

Horst Görtz Institute for IT Security

ISSE 2009, 6th of October 2009

The Hague, Netherlands

The Speaker



Dr. Christoph Wegener

- Research Assistant at the Horst Görtz Institute for IT Security (HGI)
- CISA, CISM, CBP



Dominik Birk

- Research Assistant at the Horst Görtz Institute for IT Security (HGI)
- Social Network and Web 2.0 Security

What will I talk about?

- Technical aspects
 - "De-Mail" (aka "D-Mail")
 - "Dokumentensafe light"
 - "Identifizierungsdienst light"
- Legal aspects
 - Many aspects to consider
 - Strongly related to laws in specific jurisdictions
 - Not the subject of this presentation



Bürgerportale

The Concept

- Part of the high-tech strategy of the German Federal Government
 - "[...] shall make the electronic communication as confidential and authoritative as the ordinary mail."
- Components
 - (Safe and secure) email (aka "De-Mail")
 - (Secure) document repository (aka "Dokumentensafe light")
 - (User-friendly) ID-verification (aka "Identifizierungsdienst light")
- Entities
 - Ordinary users aka "John Doe"
 - Bürgerportal Provider (BPDA)
 - Service provider



"De-Mail" (1)

Authentication

- Level "normal" (see specification version 0.96)
 - With user-ID and password
 - No security enhancement
- Level "high" (see specification Version 0.96)
 - With property (Token) and knowledge
 - Security enhancement depends on the method
- Level "very high" (see specification version 0.96)
 - With an official document (identity card (ePA))
 - Security enhancement only possible if mutual authentication methods are used (e.g. ePA with PACE on trusted device)

Phishing with De-Mail?

- When will we see the first Phishing attack on De-Mail?

```
[owner-c] type: ORG
[owner-c] fname: Max
[owner-c] lname: Muster
[owner-c] org: de-mail.net Verwaltungsgesellschaft
[owner-c] address: Platz der Republik 1
[owner-c] city: Berlin
[owner-c] pcode: 10775
[owner-c] country: DE
[owner-c] state: Berlin
[owner-c] phone: +49-3011-111111
[owner-c] fax: +49-3011-111111
[owner-c] updated: 2009-02-05 16:16:15
```



"De-Mail" (2)

Format of De-Mail Addresses

- Address format
 - **<firstname>.<lastname>[.<number>]@<BP-Domain of BPDA>.de-mail.de**
 - **<pseudonym|firstname>[.<number>]@<BP-Domain of BPDA>.de-mail.de**
 - **<company>@<BP-Domain>.de-mail.de**
- Also valid: ...@company-müller.de-mail.de
- Problem: Predictability of the addresses
- Problem: Possible deception of users
- Problem: Binding to BPDA
 - Why do we need a BPDA-Name in the address?

"De-Mail" (3)

Malware- and SPAM-Problems

- Due to the structure, addresses are predictable
 - Good news for SPAMmers (valid adresses (!))
 - Limitation at level „normal“
 - Maximum of 100 messages / 300 recipients per day(!)
 - In the age of botnets, is this still appropriate?
- Received SPAM/Malware will be delivered
 - Malware: Notification of the sender/receiver
 - But how will users react?
 - SPAM: Tagging of email



"De-Mail" (4)

Reception and Acknowledgment

- Only the content of the email present at the time of sending will be acknowledged
 - Is this really the content which should be sent?
 - How can the sender easily check this?
- Reception = reception?
 - Only the time of receipt by the De-Mail-**Provider** will be acknowledged, not the time of receipt by the user.
 - What happens in case of hardware problems after receipt but before fetching the De-Mail?

"De-Mail" (5)

Communication Scheme

- No trustworthy "Intermediary" for sending
 - Relationship of communication is directly understandable by the BPDA
 - Problematic: request to public authorities
- Acceptable for (highly personal) communication?
 - See discussion about telecommunications data retention
 - Will De-Mail be used voluntarily?



"Dokumentensafe light" (1)

Secure Access to Data

- Draft specification in version 0.96:
 - *"From the functional point of view, the documents in the Bürgerportal document safe are generally not encrypted."*
- Key Recovery (vgl. Key-Escrow) vs. Data Recovery
 - *"Optional: Key-Recovery is a possibility for ensuring availability of data in case of clientside encryption key loss"*

"Dokumentensafe light" (2)

Draft Specification cont'd

- Draft specification in version 0.98:
 - *"From the functional point of view, the documents in the Bürgerportal documents safe will be encrypted and decrypted through the BPDA. If needed, the client will also be able to encrypt parts, or all of their De-Mail data, on their client and put this encrypted data in the document safe"*
- Well done: Provider side encryption
- But E2E encryption is still OPTIONAL!
 - How will this options look?
 - Will these options be available and when?

"Dokumentensafe light" (3)

Key Management and Server Security

- Secure, permanent storage of important documents
 - Does a master key exist?
- What happens in the case that the BPDA no longer exists?
 - BPDA has to ensure future operating
 - Access to data?
 - Access to keys?
- "Dokumentensafe" on the Internet
 - Servers for data storage are connected to the Internet
 - When will the first document safe be owned?



"Identifizierungsdienst light"

Remote Identification

- User will choose assets to be confirmed
 - No freedom to choose identity schemes
- Identification provides "recognition"
 - Tracking possible
 - Analysis of buyers behaviour
- Draft specification "Identifizierungsdienst light"
 - *"[The BPDA has to assure a secure way of binding the remote identification to the current business process.]"*

Further Points to be considered (1)

- Bürgerportal infrastructure
 - *"For the technical addressing of the services and the servers among each other, each Bürgerportal provider has to allocate a faithful name service."*
 - What exactly is a faithful name service? ;)
 - Is DNS trustworthy enough?
 - No option to import/export personal address book!
- Identifizierungsdienst light
 - No (additional?) acquisition of the IBAN
 - PLZ-fields of variable length



Further Points to be considered (2)

- Account-Management
 - Responsible authority (=BSI) is able to induce blocking?
 - Who is in charge there?
 - If your password is not long enough, your account can be blocked!
 - How does the BPDA know my password?
 - What happens if I change my BPDA?
 - Can I take my De-Mail-Address with me?
- De-Mail
 - No direct relay of emails through the use of De-Mail-Address
 - Receiving: Redirection to associated email address
 - Sending: Associated email address as sender
 - Redirection to another De-Mail-Address optional



Conclusion

Technical Point of View

- Bürgerportals are an important step in the right direction!
 - Map ordinary processes onto the digital world
- (Technical) problems should be taken into account!
 - Real world and Internet are two different worlds
 - One-to-one-transfer does not work
 - Should not be business driven
- Further open discussion is necessary
 - The first step has been taken: <http://www.e-konsultation.de>
 - Unfortunately, the documentation is pretty confusing
 - Where is the discussion about the problems (=awareness)?

Thanks for Your Attention!



- Dominik Birk (dominik.birk@rub.de)
- Christoph Wegener (christoph.wegener@rub.de)

