Bundesministerium des Innern

e-government 2.0

Bürgerportale

Technische Konzeption der Bürgerportale

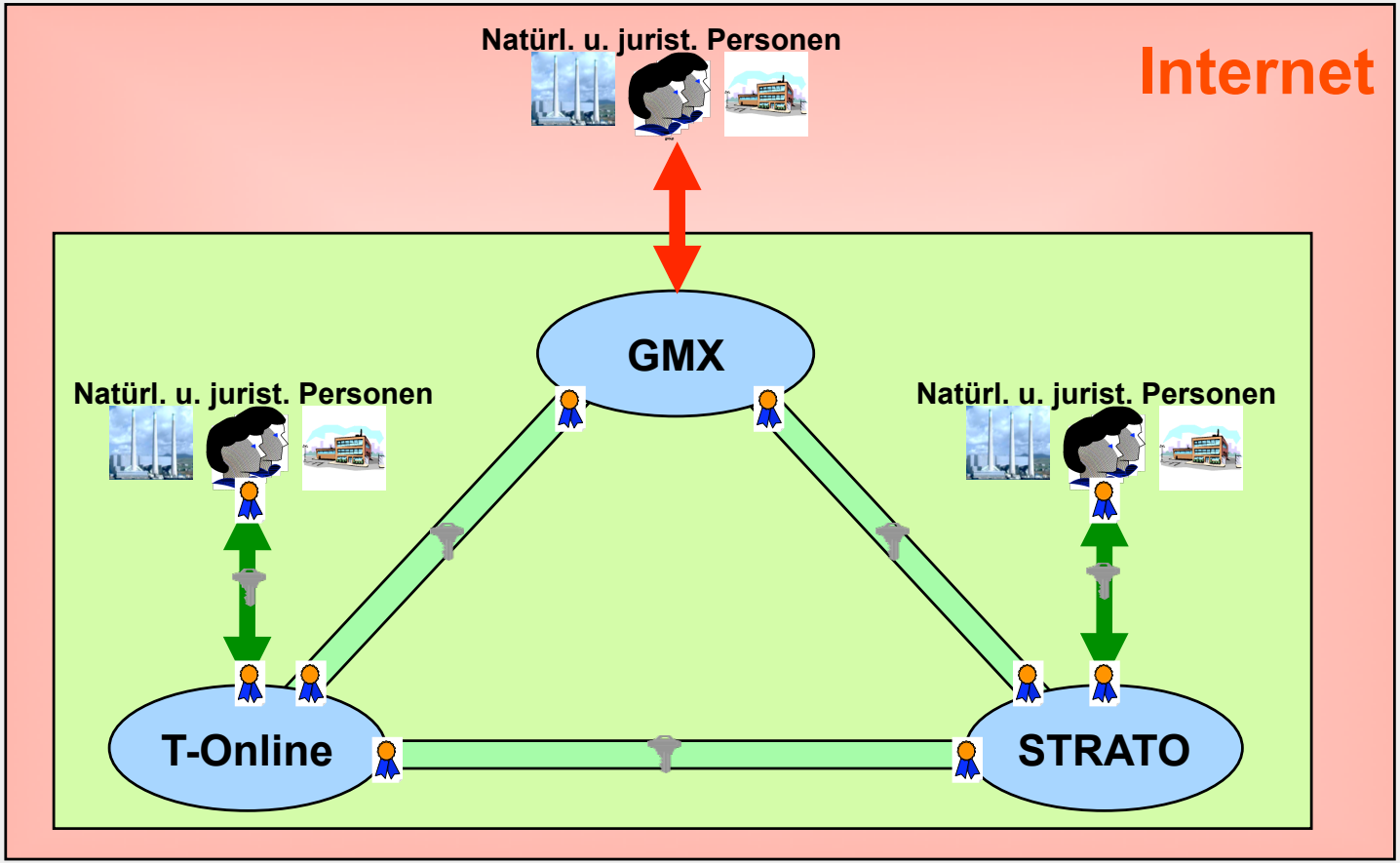
Armin Wappenschmidt (secunet)

Weitere Informationen unter www.buergerportale.de

Agenda

- Technische Übersicht über Bürgerportale
- Postfach- und Versanddienst
- Identifizierungsdienst Light
- Dokumentensafe Light
- Protokolle und Datenformate

Bürgerportale bilden einen sicheren Kommunikationsraum im Internet



Analogie eBanking

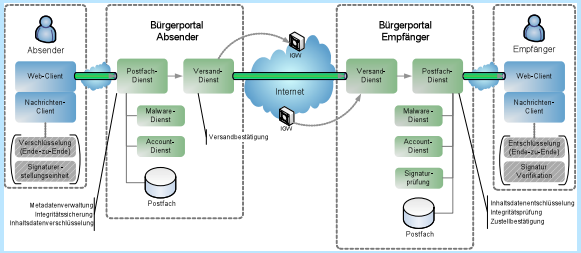
- Analogie eBanking: Statt „Geldbeträge“ werden Nachrichten übermittelt

	Banking	Bürgerportale
Zuverlässige Identität	■ Erhebung der Identitätsdaten bei Konto -Eröffnung ■ Zuordnung einer eindeutigen Konto-Nr. zum Konto-Inhaber	■ Erhebung der Identitätsdaten bei Eröffnung eines D-Mail-Accounts ■ Zuordnung einer eindeutigen elektr. Adresse zum Account-Inhaber
Sichere Transaktion	■ Hohes Auth.-Niveau der Nutzer (z.B. TAN) ■ Transport-Verschlüsselung Nutzer / Bank ■ Sichere Banken-Infrastruktur	■ Hohes Auth.-Niveau der Nutzer (z.B. TAN) ■ Transport-Sicherheit ■ Zertifizierte Infrastruktur der Diensteanbieter
Rechtliche Regelungen	■ Bankenrichtlinie, Kreditwirtschaftsgesetz, Überweisungsgesetz, etc.	■ Bürgerportal-Gesetz
Aufsicht	■ BaFin	■ Akkreditierer und Zertifizierer

- Optional: Qualifizierte Signatur und Ende-zu-Ende-Verschlüsselung transparent einsetzbar!

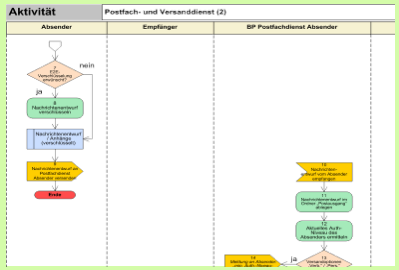
Konzepte der Bürgerportale

Grobkonzepte



- Beschreibung der Anforderungen (aus Nutzer-Sicht)

Feinkonzepte



- Technik-neutrale Beschreibung des prozeduralen Ablaufs

Interop-Spec

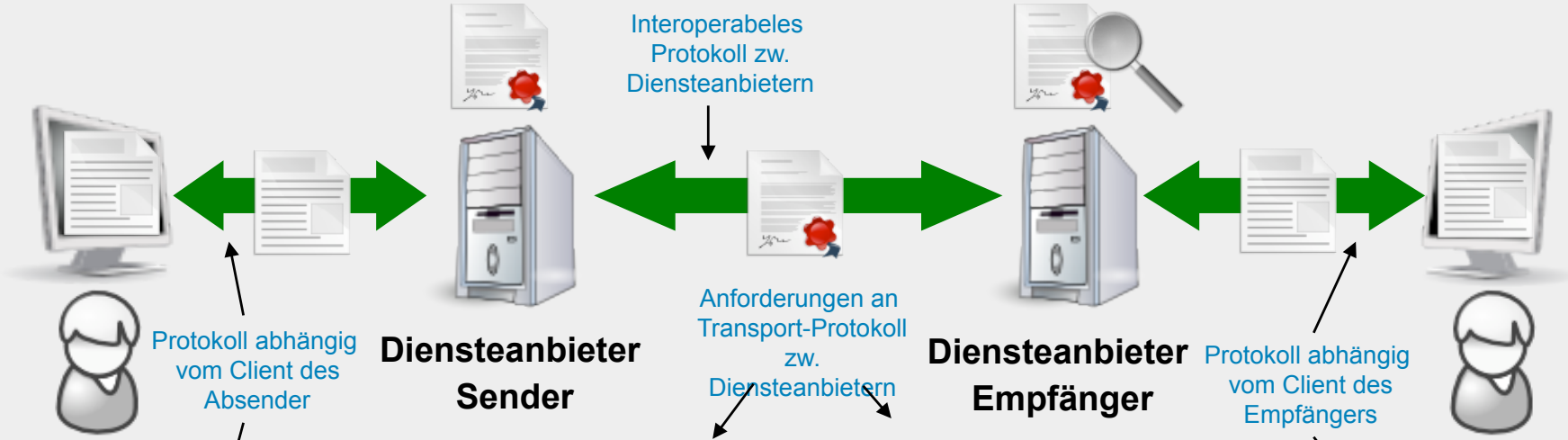
Nr.	Bezeichnung	Header-Name	Nachrichtentypen				
			N	B	M	I	E	W/F
1	Versandbestätigung	X-DMail-Return-Receipt	XX	o	o	o	o	wie original
2	Zustellbestätigung	X-DMail-Disposition-Notify	XX	x	o	x	x	wie original
3	Verbindlich	X-DMail-authoritative	XX	x	o	o	x	wie original
4	Persönlich	X-DMail-private	XX	o	o	XX	o	wie original
5	Absender-Adresse	X-DMail-eEP-A-Sender	XX	XX	XX	XX	x	wie original
6	Empfänger-Adresse(n) (auch für CC, BCC)	X-DMail-chosen-recipients	XX	XX	XX	XX	x	wie original
7	Betreff	X-DMail-Subject	XX	XX	XX	XX	o	wie original

- Beschreibung der Datenformate und Protokolle zwischen Diensteanbietern

Agenda

- Technische Übersicht über Bürgerportale
- Postfach- und Versanddienst
- Identifizierungsdienst Light
- Dokumentensafe Light
- Protokolle und Datenformate

Versand und Empfang von Nachrichten



Sender

- Webbrowser
- E-Mail-Client
- Plugin-Lösungen
- OSCI-Client
- …

- Prüfung / Ergänzung von Metadaten
- Sicherung von Integrität auf Nachrichtenebene
- Verschlüsselung auf Nachrichtenebene
- Versandbestätigung

- Zustellbestätigung
- Entschlüsselung
- Prüfung von Meta -Daten und Integrität

Empfänger

- Webbrowser
- E-Mail-Client
- Plugin-Lösungen
- OSCI-Client
- …

Umsetzung der Integritätssicherung und Verschlüsselung innerhalb der Bürgerportale

- Integritätssicherung und Verschlüsselung der Nachrichten unmittelbar nach Entgegennahme vom Absender
- Entschlüsselung und Prüfung der Integrität unmittelbar vor Übertragung der Nachrichten an Empfänger

- Verschlüsselung
  - Verschlüsselung des vollständigen Nachrichten-Body für das Bürgerportal des Empfänger und für das eigene Bürgerportal
- Integritätssicherung
  - Hashwert-Bildung über (Teile der) Metadaten und vollständigen Nachrichten-Body sowie Speicherung des Hashwertes in Metadaten
  - Keine Signatur des Hashwertes!

Technischer Hinweis: Nachrichten bestehen aus Metadaten und Nachrichten-Body (inkl. Anhänge)

„Persönliche“ und „verbindliche“ Nachrichten

- „Persönliche“ Nachrichten
  - Zugriff auf diese Nachrichten nur mit Authentisierungsniveau „hoch“
  - Sicherheitsziel Vertraulichkeit wird durch Zugriffsschutz realisiert
- „Verbindliche“ Nachrichten
  - Versand nur mit Authentisierungsniveau „hoch“ und expliziter Wahl der Versandoption „Verbindlich“ durch Absender
  - Nach Entgegennahme der Nachricht qual. Signatur des Hashwertes durch BPDA und Speicherung der Signatur in Metadaten der Nachricht
  - „Erklärung“ des BPDA:
    - Metadaten korrekt, insbesondere
      - Wahl der Versandoption „Verbindlich“ durch Absender
      - Authentisierungsniveau des Absenders mindestens „hoch“
      - Absender-Adresse korrekt
    - Nachrichteninhalt unverändert
  - Ziel: Nachvollziehbarkeit der Kommunikation durch Dritte

Versand- und Zustellbestätigungen

- Erstellung der Versandbestätigung durch Bürgerportal des Absenders
- Erstellung der Zustellbestätigung durch Bürgerportal des Empfängers
- Versand- und Zustellbestätigungen enthalten u.a.
  - aktuellen Zeitpunkt des Versands / der Zustellung
  - Metadaten der ursprünglichen Nachricht (inkl. Hashwert)

- Nachrichten mit Versand- und Zustellbestätigungen werden von dedizierten System-Adressen verschickt
- Ziel: einfache Plausibilitätsprüfung der Bestätigungen

Agenda

- Technische Übersicht über Bürgerportale
- Postfach- und Versanddienst
- Identifizierungsdienst Light
- Dokumentensafe Light
- Protokolle und Datenformate

Identifizierungsdienst Light

- Ident-Auftrag nur mindestens mit Authentisierungsniveau „hoch“
- Ident-Bestätigungen
  - Identitätsdaten: vom BPDA geprüfte Daten und nicht geprüfte Daten (Selbstauskunft)
  - Metadaten: insbesondere Zeitpunkt der Erstellung, eBP-A des Service Providers, Verifikationsstärke der jeweiligen Identitätsdaten (Selbstauskunft / geprüft)
  - Qualifizierte Signatur der Ident-Bestätigung durch BPDA des Ident-Auftraggebers
- Übermittlung der Ident-Bestätigungen in Nachrichten durch Postfach- und Versanddienst von dedizierter System-Adresse
  - alle Sicherheitsmechanismen des PVD greifen
  - Nachricht mit Versandoption „persönlich“ zum Schutz der personenbezogenen Daten
  - Kopie der Ident-Bestätigungs-Nachricht an Ident-Auftraggeber für Nachvollziehbarkeit

Agenda

- Technische Übersicht über Bürgerportale
- Postfach- und Versanddienst
- Identifizierungsdienst Light
- Dokumentensafe Light
- Protokolle und Datenformate

Dokumentensafe Light

- Zugriffsschutz
  - Zugriff auf Dokumente mit definierbaren Authentisierungsniveaus
  - Integritätssicherung und Verschlüsselung der Dokumente unmittelbar nach Entgegennahme durch Bürgerportal (vgl. Postfach- und Versanddienst)
  - Entschlüsselung und Prüfung der Integrität unmittelbar vor Übertragung der Dokumente (vgl. Postfach- und Versanddienst)
- Vertrauen zwischen Nutzer und BPDA
  - Erstellung eines vom BPDA qualifiziert signierten Protokolls, welche Dokumente eingestellt sind (auf explizite Anforderung vom Nutzer)
  - Ziel: Nachweis für den Nutzer gegenüber seinem BPDA, falls Dokumente verloren gegangen bzw. verändert worden sind

Agenda

- Technische Übersicht über Bürgerportale
- Postfach- und Versanddienst
- Identifizierungsdienst Light
- Dokumentensafe Light
- Protokolle und Datenformate

Transportverschlüsselung

- Sichert die Daten bei der Übertragung zwischen zwei BPDA
- wird mittels SSL / TLS realisiert
- Vorgaben in der Spezifikation:
  - Verwendung der Version (TLS 1.0 / 1.1)
  - einzusetzenden Verschlüsselungsalgorithmen
  - Prüfung der eingesetzten Zertifikate
- Einsatz von internationalen und weit verbreiteten Standardtechniken

Verzeichnisdienst

- Beschreibung der Verzeichniseinträge für
  - natürliche Personen
  - juristische Personen
- Schema bei allen BPDA einheitlich
  - Suchanfragen unterscheiden sich zwischen BPDA nicht
  - Erweiterungen des Standard-Schemata wurden auf ein Minimum reduziert
- Adressierung über DNS bzw. Suchpfad – ableitbar aus der eBP-A
- Authentisierung der Nutzer beim eigenen LDAP-Dienst
- Nutzung von Chaining-Mechanismen zur Nutzung weiterer Verzeichnisdienste anderer BPDAs

de-mail - Header

- Für de-mail-spezifische Informationen wurden als X-Header deklariert
  - Erweiterungen im Rahmen des RFC2822 (Internet Message Format)
  - Im Sinne des RFC sind X-Header-Zeilen “Optional fields”
  - Eine de-mail kann wie eine gewöhnliche Internet-E-Mail behandelt werden, wo keine speziellen Systeme zur Verarbeitung von de-mails zwingend erforderlich sind
  - Zuordnung der Header zu den verschiedenen Nachrichtentypen

de-mail - Header (2)

- Beispiele:
- X-DMail-Auth-level — Authentisierungs-Niveau
- X-DMail-Date-Sent — Versanddatum und -Zeit
- X-DMail-Return-Receipt — Versandbestätigung
- X-DMail-Disposition-Notify — Zustellbestätigung

- Definition

Feldname	Feldwertsyntax	Werte
X-Dmail-Disposition-Notify	Zeichenkette, case sensitive	„yes“, „no“

Melde- / Bestätigungsnachrichten

- … dienen der Benachrichtigung im Fehlerfall bzw. als Versand- oder Empfangsbestätigung einer de-mail

- Melde- / Bestätigungsnachrichten bestehen aus
  - ein PDF-Dokument, in dem der Inhalt für den Benutzer lesbar enthalten ist, dass frei durch den BPDA gestaltet werden kann
  - einem XML-Dokument für die automatische Auswertung

de-ident-Nachrichten

- de-ident-Nachrichten enthalten als Anhang
  - ein PDF-Dokument für manuelle und
  - eine XML-Datei für maschinen-behaftete Auswertungen

- XML-Struktur enthält die de-ident-Karteninformationen
  - SAML-Token
  - spätere Erweiterung des Ident-Dienst durch weitere Ident-Karten auf Basis von SAML einfach realisierbar

Herzlichen Dank für Ihre Aufmerksamkeit!

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

Externer Berater im Projekt „Bürgerportale“ des BMI