



Die Virtuelle Poststelle des Bundes

Dr. Sönke Maseberg

CAST-Workshop „PKI“

24. Januar 2008

datenschutz  nord 

Agenda



- Hintergrund
- Überblick über die Virtuelle Poststelle des Bundes (VPS)
- Evaluierungsverfahren
- zwei Highlights:
 - OCSP/CRL-Relay: zentrales Management von Verzeichnisisinformationen
 - Realisierung einer Batchsignatur
- Fazit

Hintergrund



Public Key Infrastrukturen (PKI)

- Umsetzung einer Idee
- Standards
 - X.509 / PKIX
 - Online Services Computer Interface (OSCI)
- Anwendungsbereich e-Government
 - BundOnline 2005

rechtlicher Rahmen

- Signaturgesetz und -verordnung (SigG/SigV)
- inkl. Prüfung gem. Common Criteria

„Generisches Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“

Intention der Virtuellen Poststelle



- e-Government und Kryptographie
 - neue Risiken bei der Nutzung des Internets
 - Kryptographie bietet wirksame Gegenmaßnahmen
 - Praxisprobleme bei Ende-zu-Ende-Kryptographie
 - deshalb: ausschließliche Nutzung von Ende-zu-Ende-Verfahren im e-Government nicht praxistauglich
 - Idee: zentrale (Server-) Lösung als Ergänzung

Anforderungen der VPS



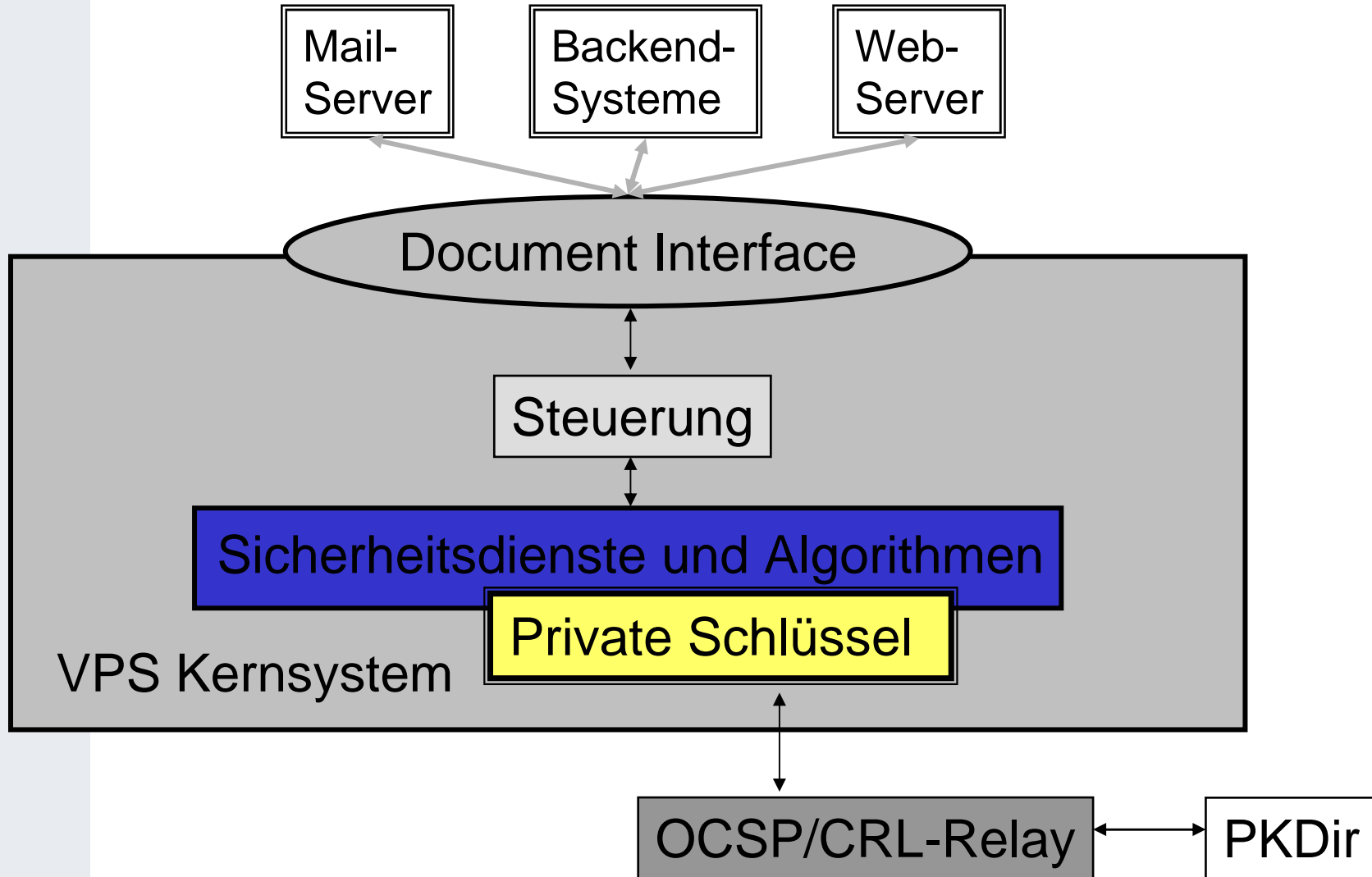
- zentralisierte Ver- und Entschlüsselung
zentral entschlüsselte Kommunikationsdaten werden dabei
 - im Klartext weitergeleitet oder
 - zur Weiterleitung im Hausnetz neu verschlüsselt
- Signaturbildung und -prüfung
- Abwicklung von Authentisierungsverfahren
- Bereitstellen und Prüfen von Zeitstempeln
- Einbindung von vorhandenen Virenscannern
- Dokumentation auf Laufzettel
- Einbindung interner und externer Verzeichnisdienste
- Bereitstellung von benutzerfreundlichen Client-Komponenten

Agenda

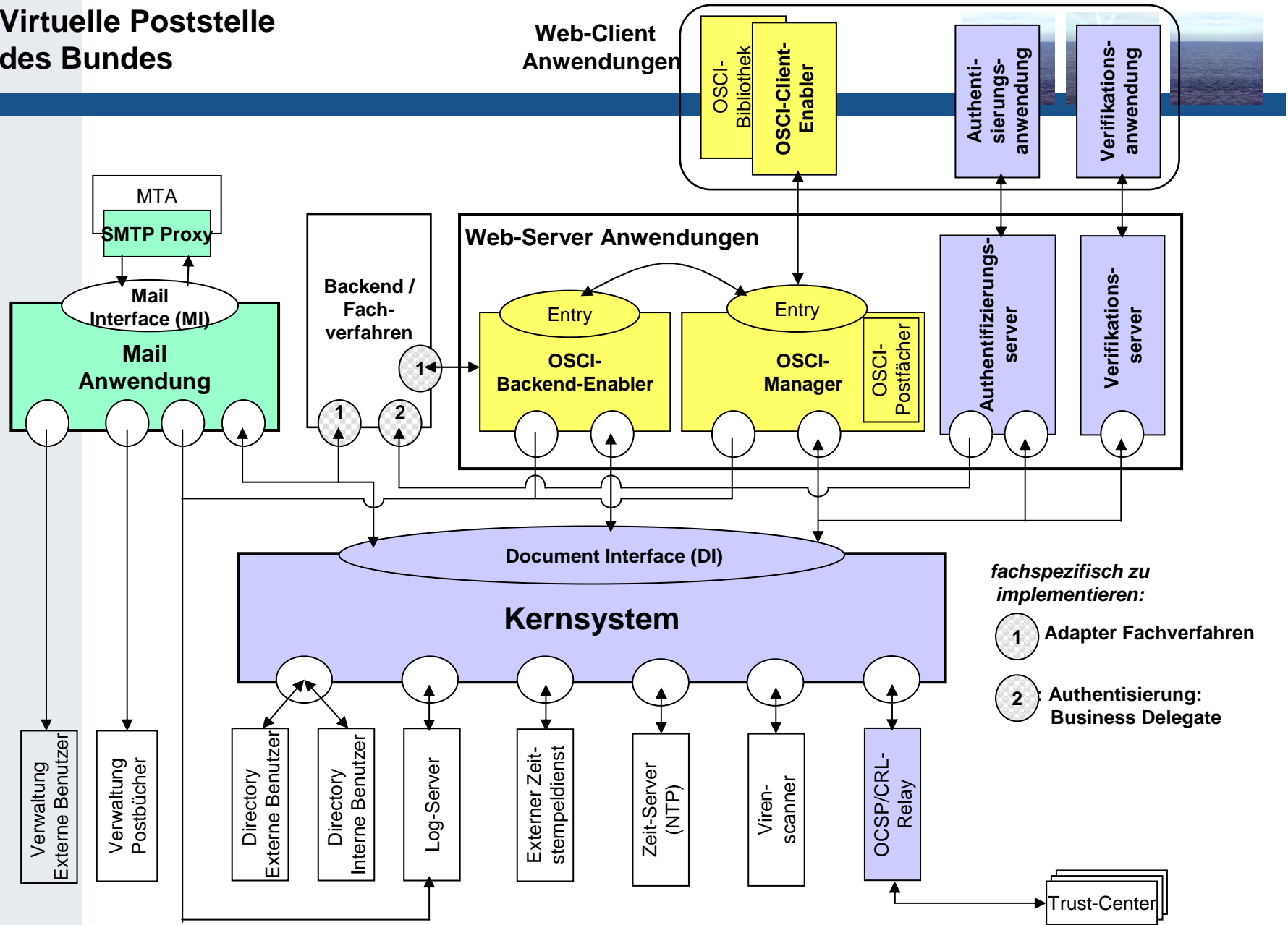


- Hintergrund
- Überblick über die Virtuelle Poststelle des Bundes (VPS)
- Evaluierungsverfahren
- zwei Highlights:
 - OCSP/CRL-Relay: zentrales Management von Verzeichnisisinformationen
 - Realisierung einer Batchsignatur
- Fazit

Design der VPS



Virtuelle Poststelle des Bundes



Agenda



- Hintergrund
- Überblick über die Virtuelle Poststelle des Bundes (VPS)
- **Evaluierungsverfahren**
- zwei Highlights:
 - OCSP/CRL-Relay: zentrales Management von Verzeichnisisinformationen
 - Realisierung einer Batchsignatur
- Fazit

Evaluierungsprozess



- zentrale Komponente von BundOnline 2005
- Bestätigung der SigG/-SigV-Konformität
- Bestätigung beinhaltet
 - Evaluierung und Zertifizierung nach Common Criteria EAL3+
 - Bestätigung der VPS als Signaturanwendungskomponente gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG sowie § 11 Abs. 3 SigV

Beteiligte



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

secunet Security Networks

Bundesnetzagentur

T-Systems International (TSI)

bremen online services

datenschutz nord

- Projektleiter / Sponsor
- Zertifizierungsstelle
- Bestätigungsstelle
- Beratung BSI
- zuständige Behörde
- Prüfstelle
- Entwicklung VPS
- Beratung bos

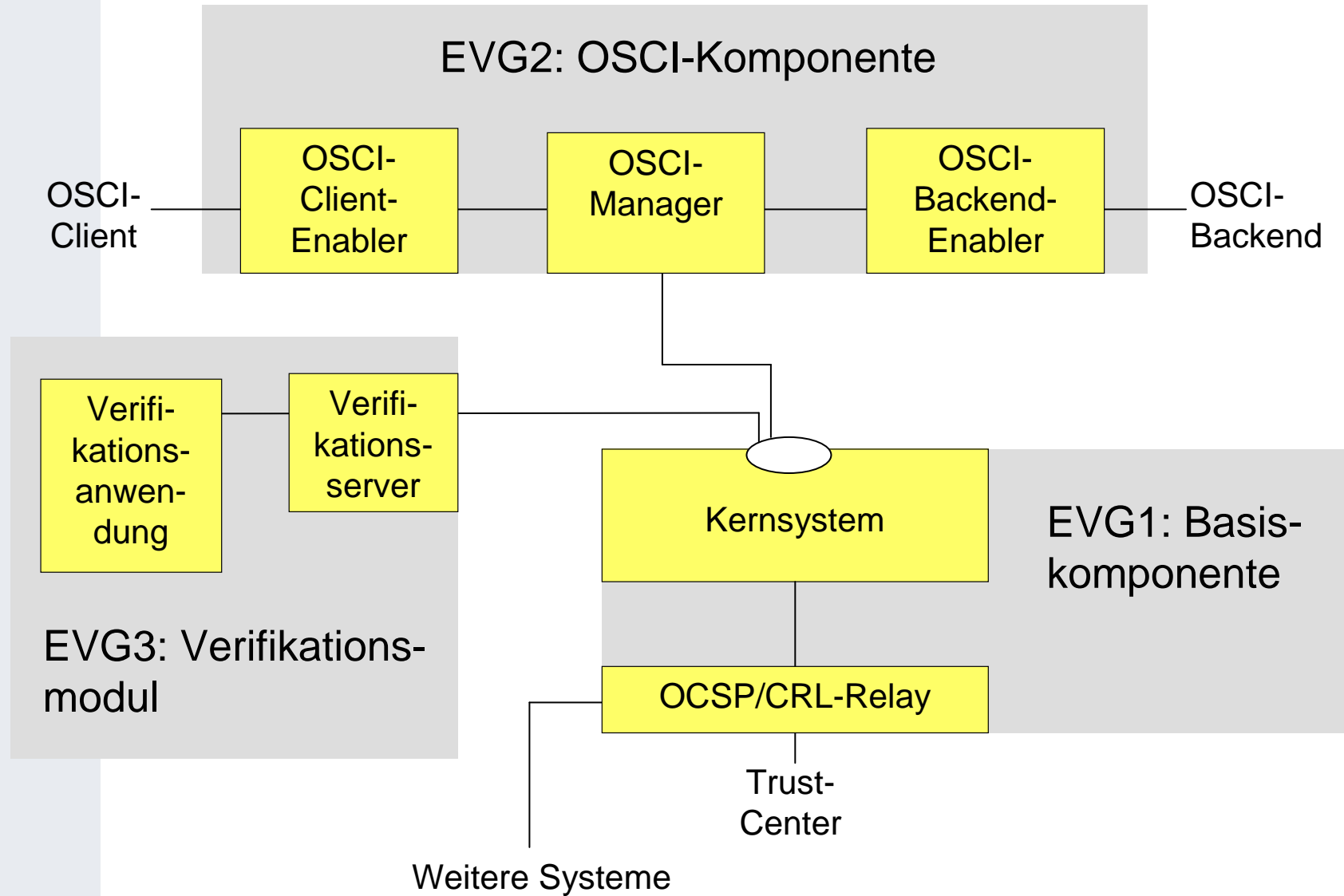
Vorgehensweise



- kompositive Evaluierung
- Aufteilung der VPS in drei logische Einheiten / drei eigenständige Evaluationsgegenstände (EVG)
- separat: evaluiert, zertifiziert und bestätigt
- EVG1: VPS, Version 2.2.2.6 (Basis)
- EVG2: VPS, Version 2.2.2.6 (OSCI)
- EVG3: VPS, Version 2.2.2.6 (Verifikationsmodul)
- Start: Mai 2004
- Verleihung von Zertifikaten und Urkunden: Dezember 2007

| | Zertifizierungs-ID | Bestätigungs-ID |
|--------------|---------------------------|-----------------------------|
| EVG1: | BSI-DSZ-CC-0331 | BSI.02070.TE.xx.2006 |
| EVG2: | BSI-DSZ-CC-0330 | BSI.02069.TE.xx.2006 |
| EVG3: | BSI-DSZ-CC-0332 | BSI.02071.TE.xx.2006 |

Virtuelle Poststelle des Bundes, Version 2.2



Agenda



- Hintergrund
- Überblick über die Virtuelle Poststelle des Bundes (VPS)
- Evaluierungsverfahren
- zwei Highlights:
 - OCSP/CRL-Relay: zentrales Management von Verzeichnisinformationen
 - Realisierung einer Batchsignatur
- Fazit

OCSP/CRL-Relay I



- Zertifikatsprüfung
- § 15 Abs. 2 Nr. 2 SigV: “Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Prüfung einer qualifizierten elektronischen Signatur
 - a) die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird und
 - b) eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren.“
- Realisierung komplex
- bei VPS: redundante Prüfungen: Performance wichtig

OCSP/CRL-Relay II



- zentrales Management im OCSP/CRL-Relay
 - Sperrlisten (CRL)
 - Statusinformationen (OCSP)
 - Verzeichnis (DIR) via LDAP
- Absicherung der Antwort des OCSP/CRL-Relays
- Einbindung in OSCI-Kontext als OSCI-Intermediär
- individuelle Validierung (über Verifikationsanwendung) möglich

Batchsignatur I



- § 15 Abs. 2 Nr. 1 SigV: „Signaturanwendungskomponenten nach § 17 Abs. 2 des Signaturgesetzes müssen gewährleisten, dass bei der Erzeugung einer qualifizierten elektronischen Signatur
 - a) die Identifikationsdaten nicht preisgegeben und diese nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden,
 - b) eine Signatur nur durch die berechtigt signierende Person erfolgt,
 - c) die Erzeugung einer Signatur vorher eindeutig angezeigt wird.“
- Batchsignatur: „eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur‘ im Betrag und der Zustelladresse unterscheiden – werden in einer besonders gesicherten Umgebung automatisiert abgearbeitet“.

Batchsignatur II



- Realisierung im NetSigner in Basiskomponente
- Voraussetzungen:
 - Multisignaturkarte
 - anforderndes System
- Absicherung der Anforderung:
 - Anforderung einer Batchsignatur nur durch ein berechtigtes anforderndes System
 - Erzeugung von Batchsignaturen nur innerhalb eines festen Zeitfensters oder für eine bestimmte Anzahl
- Anzeige:
 - für welches anfordernde System inkl. Zweck (Fachaufgabe)
 - innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen

Fazit



- „Meilenstein der PKI-Idee“
- Virtuelle Poststelle ist verfügbar
- umfassend geprüft
- praktisches Management von Verzeichnisisinformationen
- Batchsignatur

Vielen Dank für Ihre Aufmerksamkeit



Dr. Sönke Maseberg

datenschutz nord GmbH
Prüfstelle für IT-Sicherheit

Barkhausenstr. 2
27568 Bremerhaven
Tel.: 0471 / 300 11-19
Fax.: 0471 / 300 11-11

smaseberg@datenschutz-nord.de
www.datenschutz-nord.de

