

Einführung elektronischer Signaturen in der öffentlichen Verwaltung

Jörg-Udo Aden

Koordinierungs- und Beratungsstelle der Bundesregierung
für Informationstechnik in der Bundesverwaltung (KBSt)
im Bundesministerium des Innern
IT-Stab, Referat IT 2 (KBSt)

39. Erfahrungsaustausch KoopA ADV

Bund / Länder / kommunaler Bereich
Würzburg, 6. März 2002

KBSt

- KoopA ADV-Aktivitäten
- eGovernment-Initiative BundOnline 2005
- Sicherheit als Voraussetzung für eGovernment:
Basiskomponente „Datensicherheit“,
Kabinettsbeschluss „Sicherheit im elektroni-
schen Rechts- und Geschäftsverkehr“
- Umsetzung beim Bund / Zusammenarbeit

KBSt

Erstes Resümee KoopA ADV-Erfahrungsaustausch

3

- Sicherheit im Allgemeinen und Signatur im Besonderen wird große Bedeutung beigemessen
- Einführung muss pragmatisch angegangen werden, da teils noch ein „steiniger Weg“
- Andererseits ist bereits viel erreicht worden



KoopA ADV-Aktivitäten

4

- KoopA ADV-Beschluss zur PKI „Verwaltung“ einschließlich Aufbau gemeinsamer Verzeichnisse sowie zu OSCI
- KoopA ADV-AG „Kommunikation&Sicherheit“ und „eGovernment“
- „Organisatorische Rahmenbedingungen zur Einführung der Signatur“ (mit AK VI der IMK)
- Viele Einzelprojekte
 - *Schwerpunkt des Vortrags: Bund*



eGovernment-Initiative BundOnline 2005

5

- 40% der Bundesbürger über 14 Jahre sind online (Forsa)
- 58% davon möchten bereits in diesem Jahr Verwaltungsangelegenheiten online erledigen
- *Staat und Wirtschaft müssen den Anforderungen gerecht werden*

KBSt

BundOnline 2005-Umsetzungsplan

6

- Kabinettsbeschluss vom 14. November 2001
 - www.bundonline2005.de / Broschüre
- 376 Dienstleistungen bis 2005 online
- „Kompetenzentren“ werden zentral aufgebaut, „Basiskomponenten“ zentral bereitgestellt
 - **Datensicherheit**
 - Zahlungsverkehrsplattform
 - Content Management System
 - Formularserver
 - Call Center
 - Portal bund.de

KBSt

Rechtlicher Rahmen:

- ❖ Signaturrechtlinie (1999/99/EG) vom 13.12.1999
- ❖ SigG am 22.05.2001,
SigV am 22.11.2001 in Kraft getreten
- ❖ Formanpassungsgesetze:
 - Privatrecht (§ 126a BGB) am 01.08.2001 in Kraft getreten
 - Verwaltungsverfahrenrecht (Verwaltungsverfahrensgesetz, Sozialgesetzbuch X, Abgabenordnung) in Vorbereitung

Name	Technische Qualität	Rechtliche Wirkung
„Einfache“ elektronische Signatur	Nicht definiert	können benutzt werden, wenn keine besonderen
Fortgeschrittene elektronische Signatur Stufe 1	Mindestvoraussetzungen erfüllt (eindeutige Zuordnung zum und Identifizierung des Signierenden möglich, nachträgliche Änderung der signierten Daten erkennbar)	Formerfordernisse bestehen; als Beweismittel zugelassen
Qualifizierte elektronische Signatur Stufe 2	geprüfte Produkte, sichere Signaturerstellungseinheit (Chipkarte), sichere Schlüsselerzeugung	erfüllt in Verbindung mit den Formanpassungsgesetzen die rechtlichen
Zusatzoption: Qualifizierte elektronische Signatur mit Anbieterakkreditierung Stufe 3	wie vor, plus Bestätigung durch Akkreditierung	Anforderungen an eine Unterschrift in gleicher Weise wie eine handschriftliche Unterschrift

Sicherheitsniveau der Signatur II

9

- ❖ Keine Formerfordernis:
 - ❖ jede Form der elektronischen Kommunikation (Grundsatz der Formfreiheit)
- ❖ Formerfordernis:
 - ❖ qualifizierte elektronische Signatur (Stufe 2), auch bei Verwaltungsakten
 - ❖ zusätzliche Anforderungen bei Verwaltungsakten im jeweiligen Fachgesetz möglich hinsichtlich
 - dauerhafter Überprüfbarkeit und
 - technischer und administrativer Sicherheit

KBSt

Basiskomponente „Datensicherheit“ / Kabinettsbeschluss „Signatur“

10

- Kabinettsbeschluss „Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung“ vom 16. Januar 2002:

Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit bei der elektronischen Kommunikation

- von den Bundesverwaltung zu ihren Kommunikationspartner und
 - zur Bundesverwaltung
- sicherstellen

KBSt

Basiskomponente „Datensicherheit“ / Kabinettsbeschluss

11

- **Rechtsverbindlich handeln:** Qualifizierte elektronische Signaturen bei Schriftformerfordernis oder wenn es aus anderen Gründen erforderlich oder geboten ist
- **IT-Grundschutz bei der elektronischen Kommunikation:** E-Mail-Sicherheit (Signatur, Authentisierung, Verschlüsselung) flächendeckend
- **Leichtigkeit:** anwendungsbezogen angemessenes Sicherheitsniveau und Standards (ISIS-MTT)



Basiskomponente „Datensicherheit“ / Kabinettsbeschluss

12

Nicht nur Signatur:

- Signatur und Verschlüsselung
- Zertifizierungsinfrastrukturen (Public Key Infrastructures – PKI)
- Fortgeschrittene und qualifizierte elektronische Signaturen
- Infrastrukturen (PKI, Chipkarten) für mehrere Anwendungen nutzen
- ❖ Weitere Rahmenbedingungen (eGovernment-Handbuch, „virtuelle Poststelle“, Standards ISIS-MTT, OCSI, ...)



- ❖ **Rechtsverbindlich handeln**
 - ❖ qualifizierte elektronische Signaturen
 - ❖ anwendungsbezogen
 - ❖ BundOnline 2005-Dienstleistungen:
„Muster-Dienstleistungen“ bestimmen und
Signatur und Verschlüsselung beispielgebend
implementieren
 - ❖ Kooperationspartner suchen
(gemeinsame Chipkarten-Nutzung)

- ❖ **IT-Grundschutz bei der elektronischen
Kommunikation**
 - ❖ Vertraulichkeit, Integrität und Authentizität,
insbesondere im E-Mail-Verkehr (SPHINX)
 - ❖ flächendeckend bis 2003
 - ❖ ggf. Chipkarten (-lesegeräte), qualifizierte
Signaturen, Entscheidung durch die einzelnen
Behörden
 - ❖ Regelungen für das „Innenverhältnis“

- ❖ **Leichtigkeit des elektronischen Rechts- und Geschäftsverkehrs**
 - ❖ anwendungsbezogen angemessene Sicherheit
 - ❖ einheitliche Standards, insbesondere ISIS-MTT (Beginn mit MTT V.2)
 - ❖ technische, administrative u. a. Hemmnisse abbauen

- ❖ **Signaturen müssen interoperabel sein**
 - ❖ zwischen verschiedenen Software- und Hardwareprodukten
 - ❖ zwischen fortgeschrittenen und qualifizierten Signaturen (unabhängig vom Sicherheitsniveau, stufenübergreifend)
- ❖ **ISIS-MTT-Standard**
 - ❖ Vereinbarung zwischen den Herstellern (Arbeitsgruppen „Trustcenter“ und „MailTrusT“) und BMI / BMWi
 - ❖ Internet-interoperabel auf Basis von S/MIME und X.509 V3
 - ❖ Anwendbar für E-Mail und Dokumentensignatur
 - ❖ Entwurf V 1.0 liegt vor
 - ❖ ggf. Festlegungen zu Attributzertifikaten ergänzen

- ❖ Interoperable Zertifizierungsinfrastrukturen ...
 - ❖ Zertifizierungsinfrastruktur gemäß SigG
 - ❖ PKI „Verwaltung“
 - ❖ PCA beim BSI
 - ❖ Beschluss des KoopA ADV vom 24.04.2001
 - ❖ Bridge-CA
 - ❖ Träger: TeleTrust Deutschland e.V.
 - ❖ Initiative der Deutschen Bank und der Telekom unter Schirmherrschaft von BM Schily
- ... ergänzen sich

- www.kbst.bund.de
- Kabinettsbeschluss BundOnline 2005 (eGovernment) vom 14. November 2001: www.bundonline2005.de
- Kabinettsbeschluss „Signatur“: www.bmi.bund.de
- SigG / SigV u.a.: www.bmwi.de/Homepage/Politikfelder/Informationsgesellschaft/Medienrecht/Medienrecht.jsp
- Entwurf 3. VwVfÄndG: www.bmi.bund.de
- Bridge-CA: www.bridge-ca.org
- ISIS-MTT: www.teletrust.de und www.t7-isis.de
- SPHINX: www.bsi.bund.de/aufgaben/projekte/sphinx/index.htm
 - KBSt-Schriftenreihe Bände 42, 44, 46
 - KBSt-Schreiben vom 22. Januar 2001
- BSI-Projektbüro Signatur: www.bsi.bund.de/aufgaben/projekte/pbdigsig/index.htm