KBV

Zertifizierungsdienste im Gesundheitswesen

unter den Rahmenbedingungen des SigG, SGB I und SGB V

Attribute in Zertifikaten

„Public Key“-Infrastruktur / Zertifizierungsdiensteanbieter

Rechtliche Wirkung der elektronischen Unterschrift

KBV

Dokumente

- Richtlinie 1999/93/EG Rahmenbedingungen für elektronische Signaturen, 13.12.1999/19.01.2000
- SigG, 16.05./22.05.2001
- Begründung SigG (Fassung 16.08.2000)
- SigV, 16.11./22.11.2001
- Begründung SigV (Fassung 24.10.2001)
- Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, 13.07./01.08.2001
- 3. VwVerfÄndG, 21.08.2002
- Beschluss der Bundesregierung zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr, 16.01.2002
- SGB V (Neufassung, gültig ab 01.01.2004)

KBV

Richtlinie 1999/93/EG Rahmenbed. für elektronische Signaturen

Begriffbestimmungen:

- *Elektronische Signatur: Beigefügte Daten zur Authentifizierung*
- *Fortgeschrittene elektronische Signatur: Nur dem Unterzeichner zugeordnet / zur Identifizierung (Zertifikat), Werkzeuge unter alleiniger Kontrolle, Erkennbarkeit von Änderungen*
- *Zertifizierungsdiensteanbieter (ZDA): Stellt Zertifikate aus oder stellt Dienste für elektronische Signaturen bereit*
- *Qualifiziertes Zertifikat: Erfüllt Anhang I; ZDA erfüllt Anhang II*
- *Freiwillige Akkreditierung: Explizite Erlaubnis für Zertifizierungsdienste mit Auflagen einer öffentlichen oder privaten Stelle, die deren Einhaltung überwacht*
- *Sichere Signaturerstellungseinheit: Einheit, die Signaturdaten erzeugt und Anhang III erfüllt*

KBV

Richtlinie 1999/93/EG Rahmenbed. für elektronische Signaturen

Anhang I (Anforderungen an qualifizierte Zertifikate)

- Angabe „Qualifiziertes Zertifikat“
- Angabe des ZDA und des Staats der Niederlassung
- Platz für Bestimmungszweck-Attribut, Beschränkungen des Geltungsbereichs und Wertbegrenzung für Transaktionen
- Identitätscode des Zertifikats, Gültigkeitszeitraum
- Fortgeschrittene elektronische Signatur des ZDA
- Name oder Pseudonym des Signierenden
- Signaturprüfdaten (d. h. öffentlicher Prüfschlüssel)

KBV

Richtlinie 1999/93/EG Rahmenbed. für elektronische Signaturen

Anhang II (Anforderungen an ZDA, die qualifizierte Zertifikate ausstellen)

- *Sichere und schnelle Verzeichnisdienste / Widerrufdienste*
- *Geeignete Identitäts- und Attribut-Prüfung*
- *Ausreichende Finanzmittel für Haftungsrisiko*
- *Zertifikatarchiv*
- *Verbot der Speicherung / Kopierung von Signaturerstellungsdaten (d. h. private Schlüssel)*
- *Informationspflichten, Beschwerde- und Schlichtungsverfahren*
- *Sicherheitskonzept*

Richtlinie 1999/93/EG Rahmenbed. für elektronische Signaturen

Anhang III (Anforderungen an sichere Signaturerstellungseinheiten)

- ***Signaturerstellungsdaten (d. h. private Schlüssel) geheim und praktisch einmalig***
- ***Fälschungssicherheit der Signatur***
- ***Schutz vor Verwendung durch andere***
- ***Keine Veränderung zu unterzeichnender Daten***
- ***Darstellungsmöglichkeit der zu unterzeichnenden Daten vor dem Signieren***

KBV

Richtlinie 1999/93/EG Rahmenbed. für elektronische Signaturen

Gewünschte Rechtswirkung:

- ***Gleichsetzung mit handschriftlicher Unterschrift für Daten auf Papier (eigenhändige Unterschrift)***
- ***Beweismittel vor Gericht***

falls:

- ***Fortgeschrittene elektronische Signatur***
- ***Qualifiziertes Zertifikat (Standard)***
- ***Sichere Signaturstellungseinheit (Standard)***

aber: elektronische Form soll nicht diskriminiert werden; deshalb sollen qualifiziertes Zertifikat und Sichere Signaturerstellungseinheit keine K.O.-Kriterien sein

KBV

SigG

ZDA: Anzeige der Betriebsaufnahme (Sicherheitskonzept); freiwillige Akkreditierung

Qualifizierte Zertifikate: Auf Verlangen Vertretungsmacht, berufsbezogene und sonstige Angaben (Attribute); in diesen Fällen Einwilligung der zuständigen Stelle für eine Pseudonym-Verwendung und Sperrrecht dieser Stelle. Qualifizierte Signatur des ZDA. Separate qualifizierte Attribut-Zertifikate möglich. Bestätigung berufsbezogener Attribute durch die zuständige Stelle.

Qualifizierte Zeitstempel

Akkreditierung

- *Geprüfte Sicherheit mit regelmäßiger Wiederholung der Prüfung*
- *Notfalls Übernahme der Dokumentation durch die RegTP bei Betriebseinstellung*
- *Zertifikate der ZDA von der RegTP*

KBV

SigV

Bestätigung berufsbezogener Angaben auch elektronisch mit qualifizierter elektronischer Signatur, auch in Form eines Zertifikats

Zertifikatarchiv mind. 5 Jahre nach Ablauf, akkreditierte mind. 30 Jahre online

Wenn nicht anders vereinbart, persönliche Übergabe der Signaturerstellungseinheit

Zertifikate prüfbar, abrufbar nur nach Vereinbarung

Rufnummer für Sperrungen

Gültigkeit von Schlüssel-Zertifikaten max. 5 Jahre

KBV

Hinweise zu SigG / SigV

Auf Verlangen werden berufsbezogene Angaben vom ZDA in ein qualifiziertes Zertifikat aufgenommen.

- Hierzu muß eine schriftliche oder elektronische Bestätigung oder ein qualifiziertes Zertifikat der zuständigen Stelle vorgelegt werden
- Die Gültigkeit ist von der bestätigenden Stelle zu überwachen; ggf. ist zu sperren

Die Organisationen des Systems der Sozialen Sicherung können selbst ZDA sein und statt Bestätigungen Zertifikate ausstellen

Anmerkung: Das Sicherheitskonzept hat erheblich niedrigere Anforderungen umzusetzen, wenn Signaturerstellungseinheiten benutzt werden, welche die kryptografischen Schlüssel selbst generieren.

KBV

Empfehlungen:

- Zweckgebundene Bestätigungen nur für qualifizierte Zertifikate eines (akkreditierten?) ZDA mit Gültigkeit der Bestätigung von max. 30 Tagen
- Verbot der Kopplung persönlicher Zertifikate von Heilberufen an ein Pseudonym
- Sperrmöglichkeit ohne Angabe von Gründen vorsehen
- Dokumentation der Bestätigung oder Sperrung

KBV

Hinweise zu SigG / SigV

Fragen:

- Für welche Attribute sollen Bestätigungen ausgestellt werden?
- Sollen die Organisationen des Systems der Sozialen Sicherung (allein oder gemeinsam) ZDA werden?
  - für berufsbezogene Attribute der Vertragsärzte?
  - auch im Hinblick auf die Ausstattung eigener Mitarbeiter mit Signaturerstellungseinheiten?
  - auch für die Ausstattung von Praxis-Hilfspersonal mit Health-Professional-Cards?
  - auch für Secure Module Cards (SMCs)?
- Sollen sie Registrierungsstellen für einen ZDA Ärztekammern werden?
- Sollen sie einen ZDA gemeinsam betreiben?
  - mit anderen Leistungserbringerorganisationen?
  - mit den Krankenkassen?
  - mit anderen Trägern der Sozialversicherung?

KBV

Hinweise zu SigG / SigV

Motive zur Ausstellung von Zertifikaten:

- *Bestätigende Stelle signiert selbst und wird dadurch „sichtbar“ und prüfbar*
- *Standardisierte Zertifikate in einem öffentlichen Verzeichnisdienst*
  - *stehen für Anwendungen beliebiger Art als Datenquelle zur Verfügung.*
  - *diese Anwendungen müssen nicht im Vorhinein feststehen*
  - *diese Anwendungen können ohne Absprache von Dritten erstellt werden*

Zertifikate eignen sich besonders für organisationsübergreifende oder grenzüberschreitende Anwendungen

KBV

Gesetz zur Anpassung der Formvorschriften des Privatrechts

- *§ 126 (3) neu BGB : Die schriftliche Form kann (grundsätzlich) durch die elektronische Form ersetzt werden*
- *§ 126a (1): Bedingung: Ergänzung von Name + qualifizierter elektronischer Signatur*
  (2): Verträge durch jeweils gleichlautende elektronisch signierte Dokumente
- *§ 126b: Textform: Urkunde oder dauerhafte Wiedergabe von Schriftzeichen; Erkennbarkeit des Abschlusses der Erklärung, z. B. durch Nachbildung der Namensunterschrift*
- *§ 127 Telekommunikative Übermittlung oder Briefwechsel genügt für die Schriftform bei Rechtsgeschäften, soweit kein anderer Wille anzunehmen ist. Eine nachträgliche Beurkundung gem. § 126 kann verlangt werden. Wurde eine elektronische Signatur verwendet, genügt ggf. eine nachträgliche qualifizierte elektronische Signierung*
- *BGB: Für einige Formen (z. B. Zeugnisse, Bürgschaften) ist die elektronische Form ausgeschlossen*
- *ZPO*
  - *gestattet elektronische Dokumente (Formvorschriften!)*
  - *nimmt Echtheit bei qualifizierter elektronischer Signatur an*

KBV

3. VwVerfÄndG

VwVfG:

Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger einen Zugang eröffnet

- *Erneute Übermittlung in geeigneter Form kann verlangt werden*

Bei Schriftformerfordernis ist das elektronische Dokument qualifiziert elektronisch zu signieren; Pseudonyme sind nicht zulässig

- *Die dauerhafte Überprüfbarkeit der elektronischen Signatur kann bei Verwaltungsakten durch Rechtsvorschrift verlangt werden*

KBV

3. VwVerfÄndG

SGB I, § 36a (4):

Die Träger der Sozialversicherung, ..., die Leistungserbringer und die von ihnen gebildeten Organisationen ... verwenden Zertifizierungsdienste nach SigG über ihren jeweiligen Bereich hinaus, die eine gemeinsame und bundeseinheitliche Kommunikation und Übermittlung der Daten und die Überprüfbarkeit der qualifizierten elektronischen Signatur auf Dauer sicherstellen.

Diese Träger sollen über ihren jeweiligen Bereich hinaus Zertifizierungsdienste ... verwenden.

KBV

Sicherheit im elektronischen Rechts- und Geschäftsverkehr

Zielgruppe:

Bürger, Wirtschaft, Verwaltungen

Ziel:

Rechtsverbindlichkeit, IT-Grundschutz

- *durch jeweils angemessene Maßnahmen*
  - *Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit*
  - *Flächendeckender IT-Grundschutz*

Maßnahmen:

- *Einheitliche Standards (ISIS-MTT): Signatur + Verschlüsselung*
- *Flächendeckender Einsatz qualifizierter elektronischer Signaturen als Grundlage für BundOnline2005 durch die Bundesverwaltung*

KBV

SGB V (Neufassung)

Gesundheitskarte:

Die Gesundheitskarte ... muß technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen.

Elektronischer Berufsausweis:

Der Zugriff auf Daten ... mittels der elektronischen Gesundheitskarte darf nur in Verbindung mit einem elektronischen Heilberufsausweis, im Falle des ... (eRezept / eVerordnung) auch in Verbindung mit einem entsprechenden Berufsausweis, erfolgen, die jeweils über eine qualifizierte elektronische Signatur verfügen.

Eigene Signaturkarte des Bürgers:

Im Falle des ... (durch den Versicherten selbst oder für sie zur Verfügung gestellte Daten) können die Versicherten auch mittels einer eigenen Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt, zugreifen.

KBV

Weiteres

- *Authentisierungs- und Verschlüsselungsvorgänge werden nicht durch SigG / SigV / VerwVerfG / BGB geregelt*
- *SGB V geht auf Authentisierung ein, ohne umfassende Regelungen zu versuchen*
- *Attribut-Zertifikate – auch für qualifizierte elektronische Signaturen – müssen nicht dem SigG genügen (ggf. separate Hierarchien für Schlüssel- und Attributzertifikate möglich)*
- *Zertifizierungsdienste werden im Wettbewerb angeboten, müssen aber aus Wirtschaftlichkeitsgründen ggf. von Kooperationen der öffentlich-rechtlichen Organisationen selbst erbracht werden*
- *Zertifizierungsdienste werden nicht nur für Digitale Signaturen, sondern auch z.B. für Authentisierung, Verschlüsselung, Zeitstempel, Verbundadressbücher, Archivierung benötigt*

KBV

Quellen

- http://www.dud.de/
- http://www.iukdg.de/
- http://www.regtp.de/
- http://dip.bundestag.de/

KBV

Fragen?

mailto: Reinhold.A.Mainz@KBV.DE