Public-Key-Infrastrukturen für Sozialversicherungsträger

Johan Hesse[1] · Detlef Hühnlein[2]

secunet Security Networks AG
[1]Osterbekstraße 90b, 22083 Hamburg
[2]Sudetenstraße 16, 96247 Michelau
{j.hesse, huehnlein}@secunet.de

Zusammenfassung

Dieses Papier widmet sich dem Aufbau und der Anwendung von Public-Key-Infrastrukturen (PKI) in der deutschen Sozialversicherung. Neben einer Analyse der rechtlichen Rahmenbedingungen wird kurz auf relevante Infrastrukturen und insbesondere auch auf typische zertifikatsbasierte Anwendungen im Umfeld der deutschen Sozialversicherungsträger eingegangen.

1 Einleitung

Der Einsatz von Public-Key-Mechanismen zur sicheren Implementierung elektronischer Geschäftsprozesse in Wirtschaft und Verwaltung erfreut sich zunehmender Beliebtheit. Von zentraler Bedeutung ist hier die Verbindung zwischen der Identität einer Entität[1] und ihren öffentlichen Schlüsseln. Diese Verbindung (d.h. eindeutige Zuordnung) wird typischerweise durch das Ausstellen von X.509-Zertifikaten **[X.509]** durch eine vertrauenswürdige Stelle erreicht. Die Gesamtheit der zur Verwaltung dieser Zertifikate benötigten Systeme und Prozesse wird Public-Key-Infrastruktur (PKI) genannt. So umfasst dieser Begriff – wie in Abbildung 1 dargestellt - (zumindest) die Benutzerregistrierung, Zertifikatsbeantragung und -sperrung durch eine Registration Authority (RA), das Ausstellen von Zertifikaten (und ggf. vorher die Erzeugung von Schlüsseln) durch eine Certification Authority (CA), die Bereitstellung von Zertifikaten und Zertifikatsstatusinformationen in einem Directory (DIR) und natürlich entsprechende Anwendungskomponenten beim Benutzer (U).

[1] Hierbei kann es sich um natürliche oder juristische Personen, oder andere Instanzen, wie z.B. technische Gerätschaften handeln.

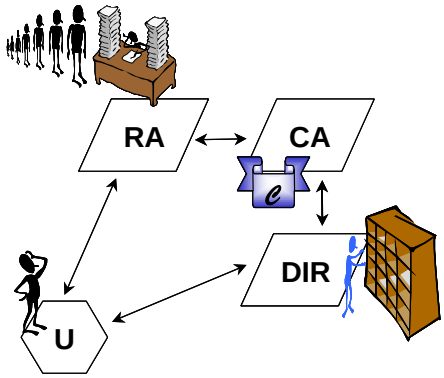

Abbildung 1: Kern-Komponenten einer PKI

Während die grundsätzliche Funktionalität dieser Komponenten unabhängig von konkreten Rahmenbedingungen einer bestimmten Branche sind, so unterscheiden sich die Anforderungen an diese Komponenten und die damit verbundenen Prozesse in verschiedenen Branchen unter Umständen erheblich.

Dieser Beitrag konzentriert sich auf die Anforderungen an, und Anwendungen von, PKIs im Umfeld der deutschen Sozialversicherung. Die branchenbedingten Besonderheiten bei der Verwaltung und Anwendung von Zertifikaten im Umfeld der Sozialversicherungsträger leiten sich insbesondere aus den gesetzlichen Rahmenbedingungen, d.h. u.a. aus der Sozialgesetzgebung, ab. Deshalb kommt der Analyse der anwendbaren Regularien in diesem Beitrag eine besondere Bedeutung zu. Außerdem wird kurz auf existierende Public-Key-Infrastrukturen und typische zertifikatsbasierte Anwendungen in der Sozialversicherung eingegangen.

Dieser Beitrag ist folgendermaßen gegliedert: Abschnitt 2 beschäftigt sich mit der Analyse der rechtlichen Rahmenbedingungen für die Verwaltung und Anwendung von Zertifikaten in der deutschen Sozialversicherung. Abschnitt 3 liefert einen kurzen Überblick über relevante PKI-Initiativen für Sozialversicherungsträger. Abschnitt 4 befasst sich mit typischen zertifikatsbasierten Anwendungen im Umfeld der Sozialversicherung. In Abschnitt 5 werden schließlich die wesentlichen Aspekte des vorliegenden Beitrages zusammengefasst.

2 Rechtliche Rahmenbedingungen

In diesem Abschnitt werden die wichtigsten[2] rechtlichen Rahmenbedingungen für den Aufbau und die Anwendung von Public-Key-Infrastrukturen bei Sozialversicherungsträgern zusammengetragen. Insbesondere wird in Abschnitt 2.1 auf die relevanten Aspekte der Sozialgesetzgebung und in Abschnitt 2.2 kurz auf die Signaturgesetzgebung eingegangen.

[2] Auf die Erörterung weiterer rechtlicher Rahmenbedingungen für den Einsatz von Zertifikaten, z.B. aus der E-Commerce- und Datenschutzgesetzgebung, dem Vergaberecht oder der Abgabeordnung soll in diesem Beitrag verzichtet werden.

2.1 Sozialgesetzgebung

Die Erhebung, Verarbeitung und Nutzung von Sozialdaten unterliegt dem strengen Schutz des Sozialgeheimnisses des Sozialgesetzbuchs, der über den allgemeinen Datenschutz im **[BDSG]** hinausgeht.

Nachfolgend wird insbesondere auf folgende rechtliche Anforderungen eingegangen:

- §35 **[SGB I]** und §67 **[SGB X]** (siehe Abschnitt 2.1.1)
- §78a **[SGB X]** (siehe Abschnitt 2.1.2)
- **[DEÜV]** (siehe Abschnitt 2.1.3)
- **[SVRV]** und **[SRVwV]** (siehe Abschnitt 2.1.4)
- **[VwVfÄndG]** (siehe Abschnitt 2.1.5).

2.1.1 §35 SGB I und §67 SGB X

In §35 **[SGB I]** ist das **Sozialgeheimnis** wie folgt bestimmt:

„Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (diese sind definiert in § 67 Abs. 1, **[SGB X]**) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet und genutzt werden (Sozialgeheimnis)“.

Dieser allgemeine Anspruch wird in weiteren Gesetzen und Verordnungen weiter ausgeformt.

Als Grundlage der weiteren Ausführungen seien zunächst die Begriffsbestimmungen des **[SGB X]** § 67 Abs. 1 auszugsweise aufgeführt:

- **Sozialdaten** sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Personen (Betroffener). Betriebs- und Geschäftsgeheimnisse sind alle betriebs- und geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.
- **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Sozialdaten.
- **Übermitteln** ist das bekannt geben von Sozialdaten an einen Dritten (durch Weitergabe oder die Ermöglichung des Abrufs oder der Einsicht in die Sozialdaten).
- **Nutzen** ist jede Verwendung von Sozialdaten, soweit es sich nicht um Verarbeitung handelt, auch die Weitergabe innerhalb der verantwortlichen Stelle.
- **Verantwortliche Stelle** ist jede Person oder Stelle, die Sozialdaten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
- **Empfänger** ist jede Person oder Stelle, die Sozialdaten erhält.
- **Dritter** ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

Ergänzend zur oben angeführten allgemeinen Formulierung des Sozialgeheimnisses gibt es außerdem spezifische Anforderungen und Einschränkungen bezüglich der Ausgestaltung des Sozialgeheimnisses:

- § 35 **[SGB I]**

- Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.
- Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.
- Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden.

- § 67c **[SGB X]**
  - Eine Speicherung, Veränderung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle erforderlich ist.
  - Sozialdaten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diesen Zweck verwendet werden.

2.1.2 §78a SGB X

Werden Sozialdaten automatisiert verarbeitet, so sind nach **[SGB X]** § 78a - und der näheren Begründung in **[SGB X§78]** dazu - technische und organisatorische Maßnahmen zu treffen, die in angemessenem Verhältnis zu dem angestrebten Schutzzweck stehen und je nach der Art der zu schützenden Sozialdaten geeignet sind, um

- **Zutrittskontrolle**

  Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen Sozialdaten verarbeitet werden, zu verwehren,

- **Zugangskontrolle**

  zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können,

- **Zugriffskontrolle**

  zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Sozialdaten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,

- **Weitergabekontrolle**

  zu gewährleisten, dass Sozialdaten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von Sozialdaten durch Einrichtungen zur Datenübertragung vorgesehen ist,

- **Eingabekontrolle**

  zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Sozialdaten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind,

- **Auftragskontrolle**

  zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können,

- **Verfügbarkeitskontrolle**

  zu gewährleisten, dass Sozialdaten gegen zufällige Zerstörung oder Verlust geschützt sind,

- **Trennungsgebot**

  zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.

2.1.3 DEÜV

In der Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung **[DEÜV]** ist festgelegt, wie Meldungen zur Sozialversicherung – insbesondere von Arbeitgebern an die Sozialversicherungsträger –zu behandeln sind. Im Hinblick auf den Einsatz von Zertifikaten sind – über die allgemeinen Anforderungen aus §78a **[SGB X]** hinaus - keine zusätzlichen Anforderungen definiert.

2.1.4 SVRV und SRVwV

In diesem Abschnitt werden die Anforderungen aus der *Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (Sozialversicherungs-Rechnungsverordnung – SVRV)* **[SVRV]** und aus der *Allgemeinen Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV)* **[SRVwV]** näher beleuchtet.

In **[SVRV]** erscheinen insbesondere folgende Regularien beachtenswert:

- §7 (Zahlungsanordnung)

  Die Zahlungsanordnung ist von dem zur Anordnung Befugten zu unterschreiben oder mit einer elektronischen Signatur gemäß Signaturgesetz[3] zu versehen.

- §9 (Feststellung der Belege)

[3] Durch Artikel 3 (2) **[SigG]** wurde §7 Abs. 3 der SVRV vom 15. Juli 1999 dahingehend geändert, dass der Originaltext „digitalen Signatur nach §2 Abs. 1 des Signaturgesetzes (Artikel 3 des Gesetzes vom 22. Juli 1997, BGBl. I S. 1870,1872)“ durch den Wortlaut „einer qualifizierten elektronischen Signatur nach dem Signaturgesetz“ ersetzt wurde.

Belege bedürfen der sachlichen und rechnerischen Feststellung. Dazu sind sie entweder zu unterschreiben oder mit einer digitalen Signatur gemäß Signaturgesetz zu versehen.

- § 14 (Aufbewahrung)

  fordert geeignete Maßnahmen gegen Verlust, Wegnahme und Veränderung der Bücher und aufbewahrungspflichtigen Unterlagen während der Aufbewahrungsfristen. Zusätzlich ist bei Aufzeichnung auf maschinell verwertbaren Datenträgern die Lesbarmachung und Ausdruckbereitschaft festgeschrieben.

- § 17 (Einsatz der automatisierten Datenverarbeitung)

  verpflichtet zum Erlass einer Dienstanweisung, mit der die Sicherheit des Verfahrens und die Grundsätze ordnungsmäßiger Datenverarbeitung zu gewährleisten sind.

- §19 (Fünfter Abschnitt: Durchführung von Aufgaben durch Dritte)

  Hier wird die Durchführung von Aufgaben des Rechnungswesens durch Dritte zugelassen. Der Versicherungsträger ist dabei für die Einhaltung der **[SVRV]** verantwortlich und muss diese einmal jährlich prüfen. Die Prüfrechte der Aufsichtsbehörde erstrecken sich auch auf die Einhaltung dieser Verordnung durch den Dritten. Der Versicherungsträger ist damit angehalten, diese Prüfrechte vertraglich zu vereinbaren. Damit werden die Anforderungen des §97 **[SGB X]** (Durchführung von Aufgaben durch Dritte) auf die Einhaltung der **[SVRV]** übertragen und detailliert. Diese Regelung ist insbesondere in Szenarien zu beachten, in denen externe Dienstleister beispielsweise die Archivierung von Belegen im Auftrag des Sozialversicherungsträgers durchführen würden.

Die Anforderungen der **[SVRV]** sind in der **[SRVwV]** weiter spezifiziert:

- § 12 (Zahlungsbegründende Unterlagen)

  Hier wird die Nutzung von Informationstechniken für die Übermittlung von zahlungsbegründenden Unterlagen gestattet, unter der Bedingung, dass die Sicherheitsanforderungen in einer Dienstanweisung (vgl. § 40) näher zu bestimmen sind.

- § 36 (Aufbewahrung)

  regelt die Archivierung ursprünglich schriftlicher Unterlagen auf Datenträger in bildlicher Form. Neben Forderungen zur Übereinstimmung des Abbildes mit dem Original und der Lesbarkeit der enthaltenen Daten erfolgt hier in Absatz (1), Ziffer 3, der Verweis auf die digitale Signatur.

  Zielsetzung ist dabei, die Übereinstimmung der bildlichen Wiedergabe mit der Unterlage zu bestätigen und die unbemerkte Veränderung der Unterlage auszuschließen. Für die Aufzeichnung, die Aufbewahrung der Datenträger und die bildliche Wiedergabe muss dabei nach Absatz (1) Ziffer 6 ein Verfahren vorgegeben sein, dass der Dienstanweisung nach § 40 **[SRVwV]** entspricht.

  In Absatz (2) wird die Aufbewahrung maschinell erzeugter Daten geregelt. Es gelten in diesem Fall grundsätzlich die selben Anforderungen wie in Absatz (1), ausgenommen der bildlichen Übereinstimmung. Die Forderung, dass die Unterlagen jederzeit in ihrer ursprünglichen Fassung inhaltlich unverändert erzeugt werden können, wird aus-

drücklich erhoben. Hieraus kann abgeleitet werden, dass auch bei der Aufbewahrung maschinell erzeugter Daten die digitale Signatur eingesetzt werden muss.

In Absatz (3) wird festgestellt, dass die digitale bzw. bildliche Archivierung sowie der Verzicht auf die Ausfertigung einer schriftlichen Unterlage unzulässig ist, wenn die Unterlagen für andere als Buchführungszwecke in Papierform aufzubewahren sind. Dies gilt sowohl für ursprünglich schriftliche als auch für ursprünglich digitale Unterlagen.

- § 40 (Sicherheit bei Einsatz der automatisierten Datenverarbeitung)

  Hier sind die technischen und organisatorischen Maßnahmen zum Schutz vor unbemerkter und unberechtigter Veränderung genauer beschrieben.

  In Absatz (2) wird der Regelungsumfang der angesprochenen Dienstanweisung definiert. Demnach hat diese Dienstanweisung zu enthalten:

  - Die technischen und organisatorischen Maßnahmen der Anlage zu § 78a SGB X, sowie
  - die Einzelheiten digitaler Signaturen nach § 2 Abs. 1 des Signaturgesetzes (Artikel 3 des Gesetzes vom 22. Juli 1997[4]).

  In Absatz (3) sind weitere Einzelheiten zum Regelungsumfang der Dienstanweisung aufgeführt, wie abgegrenzte Verantwortungsbereiche in der Datenverarbeitung, Sicherheit der Datenfernübertragung, Regelungen zu maximalen Zugriffszeiten auf Dateien.

- §41 (Digitale Signatur)

  Hier wird geregelt, dass sofern im Rahmen der **[SRVwV]** eine Unterschrift gefordert ist, diese auch mit einer elektronischen Signatur im Sinne des SigG erzeugt werden kann, wobei das Zertifikat, bzw. ein zugehöriges Attributzertifikat, die Unterschriftsberechtigung enthalten muss. Diese Unterschriftsberechtigung ist vor einer weiteren Verarbeitung zu überprüfen.

In den folgenden Regularien der SRVwV wird eine Unterschrift gefordert:

- § 5 (Abwicklung des Zahlungsverkehrs)

  Bei Übernahme der Barkasse von einem anderen Bediensteten ist der Kassenbestand ordnungsmäßig zu übergeben und durch eine Unterschrift zu bestätigen.

- §7 (Prüfung der Kasse und der Buchführung)

  Über den Umfang, Verlauf und das Ergebnis der Prüfung ist eine Niederschrift zu fertigen und vom Prüfer zu unterzeichnen.

- §10 (Form und Inhalt der Zahlungsanordnung) und §11 (Anordnung der Zahlung)

[4] Die derzeit vorliegende Fassung der SRVwV (vom 18.09.2000) bezieht sich naturgemäß auf die damals gültige Version des SigG. Hier ist analog zur Änderung der SVRV eine formale Überarbeitung zu erwarten, so dass auch hier qualifizierte elektronische Signaturen, möglicherweise sogar von Zertifizierungsdiensteanbietern mit Anbieterakkreditierung gemäß §15 SigG, gefordert werden.

Die Zahlungsanordnung ist mit einer Unterschrift zu versehen.

- §15 (Einzahlungsquittungen) und §16 (Auszahlungsquittung)

  Quittungen sind zu unterschreiben.

- §18 (Belege für Buchungen ohne Zahlungsvorgang)

  Auch hier sind, analog zur Zahlungsanordnung, mindestens die in §10 (1) genannten Punkte 1.,2. und 6.-10. vorzusehen. Unter Punkt 10. wird die Unterschrift des Anordnenden gefordert.

- §20 (Sachliche Feststellung)

  Nach (3) hat der Feststeller die sachliche Feststellung auf dem Beleg mit dem Vermerk "Sachlich richtig" durch Unterschrift mit Angabe des Datums zu bescheinigen.

- §21 (Rechnerische Feststellung)

  Nach (2) hat der Feststeller die rechnerische Feststellung auf dem Beleg mit dem Vermerk "Rechnerisch richtig" durch Unterschrift mit Angabe des Datums zu bescheinigen.

- §44 (Übergangsregelungen)

  Während die in SRVwV formulierten Anforderungen ab dem 16. Juli 1999 (Tag des Inkrafttretens) bindend sind, so ist in (4) geregelt, dass automatisierte Verfahren, die bereits vor diesem Tag im Einsatz waren, binnen fünf Jahren, d.h. bis zum 16. Juli 2004, an die Anforderungen der SRVwV anzupassen sind.

  In (5) ist festgelegt, dass die Speicherung von Unterlagen auf Bildträgern, wie Microfiche, nur bis zum 16. Juli 2004 zulässig ist.

2.1.5 VwVfÄndG

Vor dem Hintergrund des Inkrafttretens des Signaturgesetzes (siehe Abschnitt 2.2) und der Anpassung weiterer Formvorschriften, wie z.B. **[FormVG]**, existiert ein Gesetzesentwurf **[VwVfÄndG]** der verwaltungsverfahrensrechtliche Vorschriften an den modernen Geschäftsverkehr anpassen soll.

Von dieser (geplanten) Gesetzesänderung sind insbesondere die folgenden Aspekte betroffen:

- §36 SGB I (elektronische Kommunikation)

  In §36 wird die elektronische Kommunikation zwischen sozialdatenverarbeitenden Stellen zugelassen, sofern der Empfänger zustimmt. Außerdem kann, gemäß Abs. 2, die Schriftform durch die Verwendung einer qualifizierten Signatur erreicht werden. Abs. 4 erlaubt den Spitzenverbänden der Träger der Sozialversicherung den Betrieb eines Zertifizierungsdienstes nach SigG, sofern sie der Aufsicht einer obersten Bundesbehörde unterstehen und der Betrieb der Zertifizierungsstelle auf Dauer sichergestellt ist.

- SGB X, §30a (Beglaubigung von elektronischen Dokumenten)

  Analog zur schriftlichen Beglaubigung wird nun auch eine Beglaubigung elektronischer Dokumente vorgesehen. Hier ist insbesondere auf eine dauerhafte Überprüfbar-

keit, was in der Praxis nur im Rahmen der Anbieterakkreditierung gemäß §15 SigG sichergestellt ist, und eine Zeitstempelung zu achten.

- SGB X, § 33 (Bestimmtheit und Form des Verwaltungsaktes)

  Hier wird neben der schriftlichen Form auch eine elektronische Form zugelassen. Dies führt dazu, dass neben Verwaltungsakten[5], die der Schriftform genügen müssen und deshalb (nach §36, Abs. 2, SGB I) nur mit qualifizierten Zertifikaten durchgeführt werden können, auch ein elektronischer Verwaltungsakt ohne qualifizierte Signatur durchgeführt werden kann.

- SGB X, § 33a (Zusätzliche Anforderungen an elektronische Verwaltungsakte)

  Ist für einen Verwaltungsakt die Schriftlichkeit gefordert, so können auf dem Verordnungsweg weitere Anforderungen bzgl. der dauerhaften Überprüfbarkeit und technisch-organisatorischen Sicherheit festgelegt werden.

- SGB IV, §110a (Aufbewahrungspflicht)

  Hier wird festgelegt, dass (elektronische) Unterlagen ordnungsmäßig aufbewahrt werden müssen. Dies impliziert insbesondere, dass Signaturen für die Zeit der Archivierung nachprüfbar gehalten werden müssen, was in vielen Fällen nur bei qualifzierten Signaturen mit Anbieterakkreditierung gem. §15 SigG garantiert werden kann.

- SGB IV, § 110c (Verwaltungsvereinbarungen, Verordnungsermächtigung)

  Hier wird festgelegt, dass die Spitzenverbände der Sozialversicherung Näheres zu den Grundsätzen ordnungsmäßiger Aufbewahrung festlegen und die Bundesregierung ermächtigt wird, Verordnungen zu Details - wie z.B. Mindestfristen - der Aufbewahrung, Rückgabe und Vernichtung von Dokumenten zu erlassen.

- SGB IV, § 110d (Beweiswirkung)

  Werden die archivierten Unterlagen bei der Archivierung mit einer qualifizierten Signatur versehen, oder sind die Original-Unterlagen bereits mit einer qualifizierten Signatur versehen, so können die elektronischen Dokumente als Beweismittel verwendet werden.

Neben diesen für alle Sozialversicherungsträger gleichermaßen gültigen Regularien sollte eine Besonderheit für Träger der Rentenversicherung erwähnt werden. Aus naheliegenden Gründen werden an die Sicherheit der automatisierten Verfahren in der Rentenversicherung besonders hohe Anforderungen gestellt. Im Rahmen von **[VwVfÄndG]** wird eine Änderung von SGB VI (Rentenversicherung) §150, (Automatisiertes Verfahren in der Rentenversicherung) Abs. 2 vorgeschlagen[6]. Hier wird ein - in verbindlicher Abstimmung mit dem Bundes-

[5] Hier sei angemerkt, dass nach §53 SGB X - sofern das Erbringen der Leistungen im Ermessen des Leistungsträgers steht - anstatt der Eröffnung eines Verwaltungsaktes ein öffentlicher Vertrag geschlossen werden kann. Nach §56 ist aber auch ein öffentlich-rechtlicher Vertrag schriftlich zu schließen, soweit nicht durch Rechtsvorschrift eine andere Form vorgeschrieben ist.

[6] Hier sei darauf hingewiesen, dass es sich bei **[VwVfÄndG]** noch um einen – teilweise heftig diskutierten – Entwurf handelt. Derzeit ist es unklar, ob §150 SGB VI im Rahmen der Anpassung des Verwaltungsrechts tatsächlich eine Novellierung in der o.g. Form erfahren wird.

amt für Sicherheit in der Informationstechnik zu erstellendes - Sicherheitskonzept für die nach SGB X §78a geforderten Maßnahmen gefordert. Außerdem kann der Weiterbetrieb des Verfahrens bei Sicherheitsmängeln untersagt werden.

2.2 Signaturgesetzgebung

Das am 22.05.2001 in Kraft getretene deutsche Signaturgesetz **[SigG]** regelt die Sicherheitsanforderungen, die an eine PKI gestellt werden, um eine hohe Vertrauenswürdigkeit digitaler Signaturen, die unter diesen Bedingungen erzeugt werden, zu gewährleisten.

Wir begnügen uns in der vorliegenden Arbeit mit der Erwähnung der wichtigsten für Sozialversicherungsträger relevanten Aspekte und verweisen auf **[BrTe01]** für ausführliche Informationen.

Zweck des Signaturgesetzes ist die Schaffung von Rahmenbedingungen für elektronische Signaturen. Dieses Gesetz enthält in § 24 SigG die Ermächtigungsgrundlage für den Erlass einer Signaturverordnung zur Durchführung der Vorschriften des SigG. Diese Signaturverordnung **[SigV]** wurde am 24.10.2001 vom Kabinett verabschiedet. Außerdem wurde das Gesetz zur Anpassung der Formvorschriften im Privatrecht an den modernen Rechtsverkehr **[FormVG]** am 18.07.2001 im Bundesgesetzblatt veröffentlicht, das u.a. die Gleichstellung der gesetzeskonformen Signaturen mit der eigenhändigen Unterschrift unter den dort genannten Voraussetzungen regelt.

Nach dem Signaturgesetz sind ausdrücklich die Verwendung aller Signaturverfahren zugelassen. Allerdings mit unterschiedlichen Rechtsfolgen und Konsequenzen.

Die *„elektronische“* Signatur gemäß §2 Nr. 1 SigG und die *„fortgeschrittene elektronische“* Signatur gemäß § 2 Nr. 2 SigG unterliegen nicht den Anforderungen an qualifizierte Signaturen (s.u.) und damit ergeben sich nicht die Rechtsfolgen und Konsequenzen wie bei den „höherwertigen“ qualifizierten Signaturen.

Die *„qualifizierte elektronische“* Signatur nach § 2 Nr. 3 SigG und die *„qualifizierte elektronische Signatur mit Anbieterakkreditierung“* nach § 15 SigG dagegen unterliegen den Anforderungen der §§ 4 bis 14 bzw. § 23 des Gesetzes und der sich darauf beziehenden Vorschriften der Verordnung und erfahren folglich die Rechtsfolgen, die sich aus den Änderungen der sich darauf beziehenden Gesetze ergeben (wie z.B. die Gleichstellung mit der handschriftlichen Unterschrift im Rahmen des BGB § 126a). Im weiteren Text soll sich wegen der juristischen Konsequenzen, die sich aus diesem Tatbestand ergeben, der Begriff „signaturgesetzkonforme Signatur (bzw. Zertifikat)“ als Synonym für „qualifizierte elektronische Signatur (bzw. Zertifikat)“ benutzt werden.

Für Sozialversicherungsträger ist – auf Grund der Anforderungen in **[SVRV]** und **[SRVwV]** (vgl. Abschnitt 2.1.3) - insbesondere die letztgenannte „qualifizierte elektronische Signatur mit Anbieterakkreditierung“ gemäß §15 SigG von Bedeutung.

Diese Forderung impliziert, dass an die in Abbildung 1 dargestellten Kernkomponenten einer PKI besondere Anforderungen gestellt werden:

- Geprüftes und bestätigtes Sicherheitskonzept

  Nach §15, Abs. 2 SigG muss das gemäß §4, Abs. 2 Satz 4 SigG geforderte Sicherheitskonzept für den Betrieb der Zertifizierungsstelle von einer unabhängigen Stelle (gemäß §18 SigG) geprüft und bestätigt werden.

- Einsatz von geprüften und bestätigten Komponenten

  Nach §15, Abs. 7, SigG müssen die in §17, Abs. 1-3, SigG und SigV formulierten Anforderungen an die Produkte für qualifizierte elektronische Signaturen erfüllt sein.

  Die wichtigsten Anforderungen an die einzusetzenden Produkte lassen sich folgendermaßen zusammenfassen:

  - Sichere Signaturerstellungseinheit

    Nach §17, Abs. 1, SigG *müssen* sichere Signaturerstellungseinheiten eingesetzt werden. Gemäß der Anlage 1, Abschnitt I der SigV bedeutet dies, dass die Signaturerstellungseinheit mindestens gemäß ITSEC E3, bzw. CC EAL4+, jeweils mit Mechanismenstärke „hoch“, zu prüfen ist.

    Nach §17, Abs. 4 SigG muss die Erfüllung dieser Anforderung durch eine unabhängige Stelle gemäß §18 SigG bestätigt werden. Eine Herstellererklärung ist in diesem Fall *nicht* ausreichend.

  - Sichere Signaturanwendungs- und Darstellungskomponente

    Nach §17, Abs. 2, SigG *sollen* sichere Anwendungs- und Darstellungskomponenten eingesetzt werden, oder „andere geeignete Maßnahmen zur Sicherheit qualifizierter elektronischer Signaturen“ getroffen werden.

    Soll die Sicherheit der Anwendungskomponente nicht allein durch u.U. aufwendige organisatorische Maßnahmen erreicht werden, so muss die Signaturanwendungskomponente gemäß ITSEC E2, bzw. CC EAL3, jeweils mit Mechanismenstärke „hoch“, geprüft werden.

    Allerdings ist hier, nach §17, Abs. 4 SigG, eine Bestätigung durch eine unabhängige Stelle nicht zwingend erforderlich; es genügt eine Herstellererklärung. In diesem Fall kann sich der Hersteller, z. B. bei Haftungsansprüchen, nicht auf den mit der Bestätigung verbundenen „Nachweis der umfassend geprüften Sicherheit“ berufen; die Beweislast im Streitfall verbleibt bei ihm.

    Da der Signaturanwendungskomponente im Hinblick auf eine Integration der Signaturfunktionalität in diverse Anwendungen eine besondere Bedeutung zukommt, wollen wir etwas näher auf die wichtigsten Anforderungen eingehen, die man an Signaturanwendungskomponenten stellen sollte, um einen langfristigen Investitionsschutz zu erreichen. Während bei der Entwicklung der DSAC[7]-Architektur tiefergehende Anforderungen untersucht wurden, wollen wir uns hier mit der Erwähnung der wichtigsten begnügen:

    - Anwendungsunabhängigkeit

      Da die Signaturfunktionalität möglichst in beliebigen Server- und Client-Anwendungen (E-Mail, Office, Browser, pdf-Tools, ERP-System (wie SAP), Dokumentenmanagement-System, branchenspezifische Systeme (wie

[7] DSAC=Digital Signature Application Component - Konzept einer massiv-multiapplikationsfähigen Signaturanwendungskomponente

ISKV) ...) zur Verfügung stehen soll, ist die Anwendungsunabhängigkeit beim DSAC, insbesondere im Hinblick auf den Investitionsschutz, ein sehr wichtiger Aspekt. Diese ausgeprägte Integrationsfähigkeit bedingt ein außerordentlich ausgefeiltes Architekturkonzept, das in der Lage ist alle heutigen - und möglichst auch zukünftige - Technologien und Anwendungsgebiete ohne Veränderung der Basiskomponenten zu befriedigen.

- Anwendungsspezifische Sicherheitsregeln

  Obwohl ein DSAC von der Endanwendung unabhängig sein sollte, so müssen – in Abhängigkeit von der jeweiligen Applikation – verschiedene Sicherheitsregeln angewandt werden. Beispielsweise muss die Darstellungskomponente von DSAC bei einer vom Browser angestoßenen Signatur sicherstellen, dass kein „unsichtbarer Text“ vorhanden ist.

- Kapselung der sicherheitsrelevanten Funktionen

  Um die vom Gesetzgeber in §17, Abs. 2 SigG gewünschte ITSEC- oder CC-Evaluation der sicherheitsrelevanten Funktionen einer Signaturanwendungskomponente mit vertretbarem Aufwand zu ermöglichen, müssen die sicherheitsrelevanten Funktionen, wie die Schnittstelle zur Signaturerstellungseinheit, zur Darstellungskomponente oder des Verzeichnisdienstes eines TrustCenters, entsprechend gekapselt sein. Insbesondere ist darauf zu achten, dass bei der Unterstützung einer zusätzlichen Applikation oder einer anderen Signaturerstellungseinheit nicht die komplette DSAC-Komponente einer Re-Evaluation unterzogen werden muss. Dies ist gerade unter den Gesichtspunkten eines kostenminimalen Migrationskonzeptes (d.h. Ausbau auf weitere Applikationen zur Unterstützung zusätzlicher Workflowprozesse etc.) zu beachten, da jeder Re-Evaluations-Vorgang mit hohen Fixkosten verbunden ist.

  Die folgende Abbildung zeigt das Grundprinzip einer Signaturanwendungskomponente, die die eben skizzierten Anforderungen erfüllt:

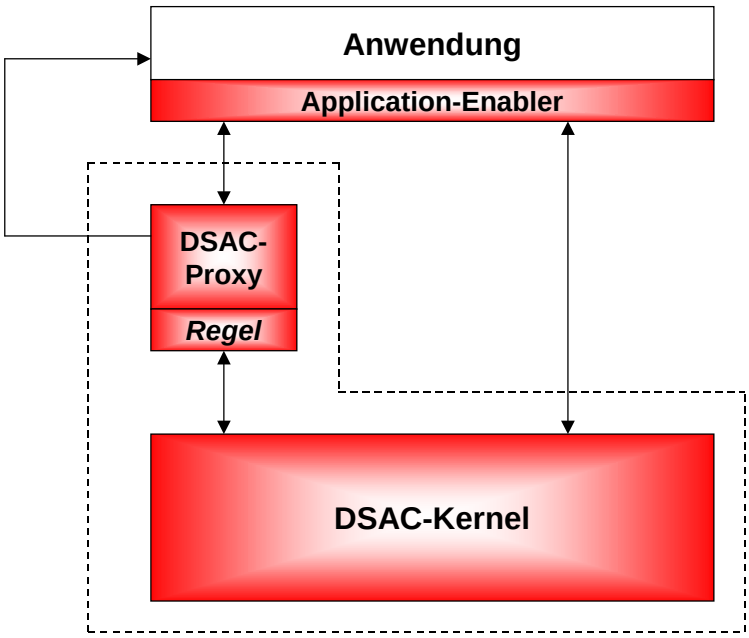

Abbildung 2: DSAC - Grundprinzip

Neben den oben genannten Anforderungen an die Signaturerstellungseinheit und die Signaturanwendungskomponente sind in §17, Abs. 3 SigG weitere – teilweise bestätigungspflichtige – Sicherheitsanforderungen an die technischen Komponenten eines TrustCenters formuliert.

Schließlich sei auf die mit der freiwilligen Akkreditierung des Zertifizierungsdiensteanbieters verbundene Verpflichtung hingewiesen, die qualifizierten Zertifikate nicht nur, wie in §4, Abs. 1, SigV festgelegt, 5 Jahre, sondern gemäß §4, Abs. 2, SigV sogar 30 Jahre, über den Zeitraum der Gültigkeit des Zertifikates hinaus, überprüfbar zu halten. Diese Garantie ist vor dem Hintergrund der in §36 **[SRVwV]** und SGB IV, §110a (vgl. **[VwVfÄndG]**) geforderten langfristigen Aufbewahrung von Unterlagen von besonderer Bedeutung.

Somit lassen sich die wichtigsten Anforderungen an die Kernkomponenten einer PKI, die qualifizierte Zertifikate (mit Anbieterakkreditierung) ausstellt wie in Abbildung 3 dargestellt zusammenfassen.

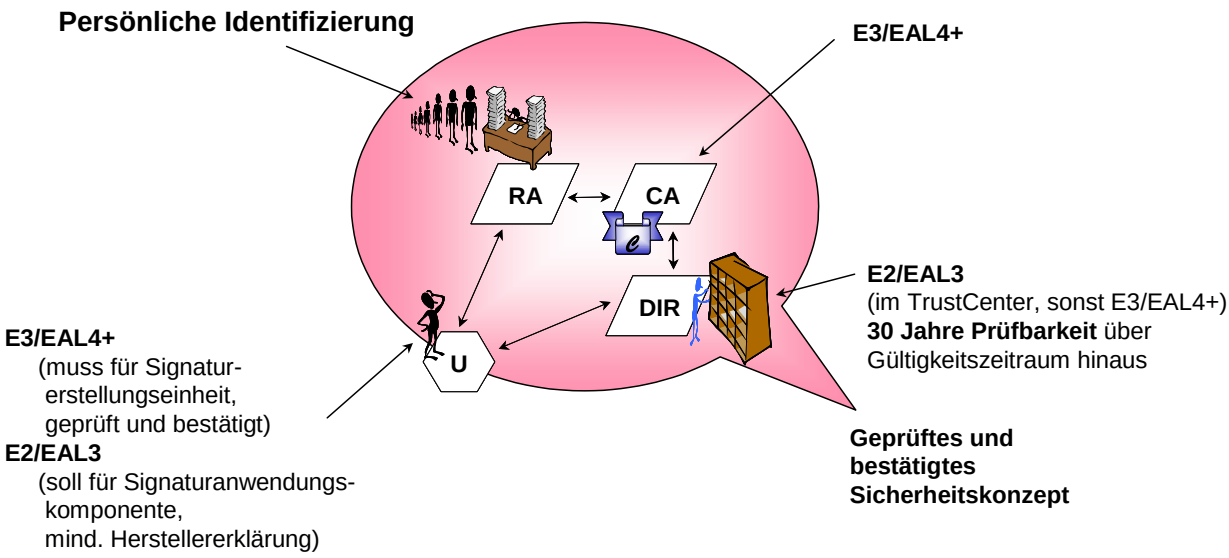

Abbildung 3: Anforderungen an PKI-Kernkomponenten für qualifizierte Signaturen (mit Anbieterakkreditierung)

2.3 Analyse der rechtlichen Rahmenbedingungen

In diesem Abschnitt sollen die vorher diskutierten rechtlichen Rahmenbedingungen einer groben Analyse unterzogen werden. Hierbei soll insbesondere auf die Frage eingegangen werden, für welche elektronischen Geschäftsprozesse bei Sozialversicherungsträgern (welche Art) Zertifikate eingesetzt werden müssen, bzw. für welche Geschäftsprozesse der Einsatz von Zertifikaten ratsam ist. Bei der nachfolgenden Betrachtung unterscheiden wir zwischen allgemeinen Anforderungen, die vor allem aus §78a SGB X erwachsen, und den Anforderungen aus SVRV und SRVwV.

Bezüglich des Aufbaus und der Anwendung von Public-Key Infrastrukturen lassen sich aus §78a und der Begründung in **[SGB X§78]** insbesondere folgende Anforderungen ableiten:

- Benutzerauthentisierung (Zugriffskontrolle, Eingabekontrolle)

  Dies betrifft alle sozialdatenverarbeitenden Systeme. Auf Grund der oft heterogenen Systemlandschaft bei Sozialversicherungsträgern ist hier u.a. an die Einführung von plattformübergreifenden Systemen zum Berechtigungsmanagement zu denken.

- Verschlüsselung (Weitergabekontrolle)

  Hier sind Daten, die über un- oder wenig geschützte Netze transportiert werden zu verschlüsseln. Kann der Schutz gespeicherter Informationen, z.B. auf mobilen PCs, kaum durch organisatorische Maßnahmen sichergestellt werden, so wäre der Einsatz von Mechanismen zur Dateiverschlüsselung ratsam. Werden Sozialdaten per E-Mail verschickt, so sind entsprechende E-Mail-Sicherheitsmechanismen vorzusehen.

- Datenintegrität (Eingabekontrolle, Weitergabekontrolle)

  Hier ist sicherzustellen, dass gespeicherte oder übertragene Daten nicht unbemerkt verändert werden können, und dass jede Änderung nachvollziehbar ist und einer Person zugeordnet werden kann. Diese Anforderung wird in der Praxis durch den "revisi-

onssicheren Betrieb" der IT-Systeme mit Benutzerauthentisierung und weiteren technisch-organisatorischen Maßnahmen erfüllt. Der Einsatz von nachrichtengebundenen Sicherheitsmechanismen und digitalen Signaturen - unabhängig von der Signaturgesetzgebung – minimiert hierbei die notwendigen Aufwände bzgl. organisatorischer Maßnahmen.

- Elektronischer Mitarbeiterausweis (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle)

  Um die Zutritts-, Zugangs- und Zugriffskontrolle zu implementieren, bietet sich der Einsatz von elektronisch lesbaren Mitarbeiterausweisen an. In Verbindung mit den oben genannten Anforderungen, wäre ein chipkartenbasierter Ausweis, der auch zur Authentisierung, Verschlüsselung und Signatur eingesetzt werden kann, ideal.

Bezüglich der Regularien des §78a **[SGB X]** oder dem **[BDSG]** ist festzuhalten, dass sich die dort festgelegten Anforderungen, wie Zugriffs-, Eingabe- und Weitergabekontrolle, mittels Zertifikatseinsatz elegant – und langfristig sicherlich kostenminimal - lösen lassen. Bei Einsatz von chipkarten-basierten Mitarbeiterausweisen ließen sich auch die Anforderungen bzgl. der Zutritts- und Zugangskontrolle elegant verwirklichen.

Eine zwingende Forderung für den Einsatz von Zertifikaten, oder gar signaturgesetzkonformen Zertifikaten, lässt sich aus §78a SGB X aber *nicht* ableiten.

Anders gestaltet sich dies bei den Anforderungen aus **[SVRV]** und **[SRVwV]**. Sollen die dort berührten Geschäftsprozesse elektronisch abgewickelt werden, so ist der Einsatz von SigG-konformen (d.h. qualifizierten) Zertifikaten zwingend erforderlich. Insbesondere sind hier die folgenden Prozesse zu betrachten:

- Zahlungsanordnung (siehe § 7 **[SVRV]** und §§10-11 **[SRVwV]**)
- Buchungen ohne Zahlungsvorgang (siehe §18 **[SRVwV]**)
- Feststellung der Belege (siehe §9 **[SVRV]** und §§19-21 **[SRVwV]**)
- Ggf. Zahlungsmittelfreigabe (Regelung oft in Dienstanweisung gemäß §40 SRVwV)
- Archivierung von Unterlagen (siehe §§36, 44 **[SRVwV]**)

Außerdem existieren Verwaltungsakte, die der Schriftform bedürfen und deshalb trotz der geplanten Änderung des §33 **[SGB X]** (siehe **[VwVfÄndG]**) nur mittels SigG-konformer Zertifikate abgewickelt werden können. Auch im Umfeld der Vergabeverordnung **[VgV]** und der elektronischen Rechnungsstellung (siehe **[StÄndG]**) müssen SigG-konforme Zertifikate eingesetzt werden. Neben diesen Anforderungen spricht der erhöhte Beweiswert, wie in SGB IV §110d explizit herausgestellt, für den Einsatz SigG-konformer Zertifikate.

Demnach ist der Einsatz von signaturgesetzkonformen Zertifikaten in vielen wichtigen Geschäftsprozessen der Sozialversicherungsträger nicht nur ratsam, sondern – insbesondere auf Grund von SVRV und SRVwV - explizit gefordert.

Sollen diese Geschäftsprozesse elektronisch abgewickelt werden, so müssen die Träger der Sozialversicherung signaturgesetzkonforme Zertifikate verwenden. Eine individuell zu klärende Frage ist hierbei schließlich, ob SigG-konforme Zertifikate flächendeckend eingeführt werden sollen, oder ob in bestimmten Bereichen, wie z.B. dem Austausch von Daten Dritter per E-Mail, mit etwas kostengünstigeren software-basierten Zertifikaten gearbeitet werden

soll. Eine weitere Frage ist, ob die jeweiligen Zertifikate von einem (akkreditierten) Trust-Center bezogen, oder selbst ausgestellt werden sollen; letzteres ist nach SGB I §36, Abs. 4 (siehe **[VwVfÄndG]**) nun auch (bald) möglich.

3 PKI-Initiativen im Umfeld der Sozialversicherungsträger

In diesem Abschnitt soll kurz auf die wichtigsten PKI-Initiativen im Umfeld der Sozialversicherungsträger eingegangen werden. Wir begnügen uns mit der Erwähnung der existierenden PKI der deutschen Sozialversicherungsträger in Abschnitt 3.1 und – auf Grund der Anforderungen aus **[SVRV]** und **[SRVwV]** – der Auflistung der signaturgesetzkonformen TrustCenter in Abschnitt 3.2. Für einen umfassenderen Überblick sei auf **[Hühn02]** verwiesen.

3.1 PKI der deutschen Sozialversicherungsträger

Die deutschen Sozialversicherungsträger betreiben eine PKI, die zur Absicherung des elektronischen Datenaustausches zwischen Trägern und Leistungserbringern in der Sozialversicherung verwendet wird. Neben der Übermittlung von Leistungsdaten gemäß §§300 ff. SGB V können auch die Meldungen gemäß **[DEÜV]** mit diesen Zertifikaten abgewickelt werden.

Hier existiert eine Policy-CA (PCA) unter der weitere operative CAs existieren:

- ITSG-CA (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH)
- DKTIG-CA (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH)
- BfA-CA (Bundesanstalt für Arbeit)
- VDR-CA (Verband Deutscher Rentenversicherungsträger)

Alle hier aufgeführten CAs stellen X.509v1-Zertifikate aus. Als Sicherheitsmechanismus, z.B. für den Datenaustausch zwischen den Krankenkassen und Leistungserbringern gemäß **[AOK01]**, kommt das mittlerweile etwas betagte PEM zum Einsatz.

Unglücklicherweise können diese Zertifikate weder für die heute weit verbreiteten SSL-Client-Authentifizierung noch im Zusammenhang mit marktüblichen Standard-E-Mail-Lösungen, wie z.B. Microsoft Outlook, Netscape Messenger oder Lotus Notes, eingesetzt werden. Außerdem sind die ausgestellten Zertifikate keine qualifizierten Zertifikate gemäß **[RFC3039]** und SigG; keines der o.g. CAs (oder der dahinterstehenden TrustCenter-Dienstleister, wie z.B. das CCI in Meppen als operativer Betreiber der ITSG-CA) kann bislang die geforderte Akkreditierung gemäß §15 SigG vorweisen.

Deshalb darf man gespannt sein, ob und wann diese Infrastruktur die hier skizzierten, operativen und gesetzlichen Anforderungen an PKIs für Sozialversicherungsträger in umfassender Art und Weise erfüllen kann.

3.2 Signaturgesetzkonforme TrustCenter

Da zur Erfüllung der Anforderungen aus **[SVRV]** und **[SRVwV]** signaturgesetzkonforme Zertifikate zum Einsatz kommen müssen, soll kurz auf die bislang akkreditierten TrustCenter,

die entsprechende qualifizierte Zertifikate für Sozialversicherungsträger ausstellen können, eingegangen werden.

Derzeit, d.h. im März 2002, existieren sechzehn akkreditierte signaturgesetzkonforme CAs, die alle unter der von der Regulierungsbehörde für Telekommunikation und Post (RegTP) **[RegTP]** betriebenen deutschen Wurzelinstanz angeordnet sind:

- Produktzentrum TeleSec der Deutschen Telekom AG, Netphen
- Bundesnotarkammer, Köln
- Deutsche Post Signtrust GmbH, Bonn
- DATEV eG, Nürnberg
- Steuerberaterkammer Nürnberg
- Medizon AG, Berlin
- Steuerberaterkammer Saarland
- Hanseatische Steuerberaterkammer Bremen
- Rechtsanwaltskammer Bamberg
- Rechtsanwaltskammer Koblenz
- Steuerberaterkammer Stuttgart
- Steuerberaterkammer München
- Steuerberaterkammer Berlin
- AuthentiDate International AG, Ratingen
- TC TrustCenter AG, Hamburg und
- D-Trust GmbH, Berlin.

Die technische Interoperabilität, z.B. bei der sicheren E-Mail-Kommunikation, zwischen den einzelnen CAs ist derzeit noch nicht vollständig gegeben. Bis Mitte 2002 ist jedoch durch die Implementierung der gemeinsam verabschiedeten ISIS/MTT-Spezifikation **[Tele01]** mit Abhilfe zu rechnen.

In der jüngsten Vergangenheit gab es die Ankündigung des Trust Centers der Deutschen Post Signtrust, den Betrieb einzustellen. Damit wird dieser Anbieter in Zukunft nicht mehr zur Verfügung stehen. Die weitere Nachprüfbarkeit der Zertifikate in einem solchen Fall wird von dem Signaturgesetz geregelt. Sollte sich kein anderer Zertifizierungsdienstleister finden, welcher die Kundenzertifikate der Signtrust übernimmt, so wird die Nachprüfbarkeit von der Regulierungsbehörde (RegTP) gewährleistet.

4 Zertifikatsbasierte Anwendungen für Sozialversicherungsträger

In diesem Abschnitt gehen wir kurz auf zertifikatsbasierte Anwendungen für Sozialversicherungsträger ein. Wie in **[HüJa01]** angedeutet, existieren beispielsweise die folgenden branchen-neutralen Basis-Anwendungen für Zertifikate:

- E-Mail-Sicherheit
- Datei-Verschlüsselung
- Workflow-Signaturen
- Code Signing
- Virtual Private Networks
- Sichere Client-Server Kommunikation
- Single Sign-On

Aus diesem Anwendungsrepertoire wollen wir den Bereich der Workflow-Signaturen herausgreifen und anhand der folgenden Anwendungen etwas näher beleuchten:

- Archivierung schriftlicher Unterlagen
- Abwicklung des Zahlungsverkehrs
- Elektronisches Rezept

Während die beiden ersten Anwendungen für alle Träger der Sozialversicherung relevant sind und auf Grund der in §44 **[SRVwV]** angegebenen Übergangsfrist einen akuten Handlungsbedarf implizieren, betrifft das Elektronische Rezept natürlich insbesondere die Krankenkassen und ist eher von strategischer Bedeutung.

4.1 Archivierung schriftlicher Unterlagen

Wie in Abschnitt 2.1.3 angedeutet, dürfen papiergebundene Unterlagen nach §36 **[SRVwV]** vor Ablauf der Aufbewahrungsfrist vernichtet werden, wenn die bildliche Übereinstimmung des elektronischen Abbildes mit dem Originalbeleg durch eine qualifizierte elektronische Signatur bestätigt wurde und die Verfügbarkeit und Sicherheit der Daten gewährleistet ist. Wie in §44 (5) **[SRVwV]** geregelt, ist die (alleinige) Speicherung von Unterlagen auf Bildträgern, wie z.B. Mircofiche, ab August 2004 nicht mehr zulässig. Deshalb sind fast[8] alle Sozialversicherungsträger von dieser Regelung betroffen.

Bei vielen Trägern der Sozialversicherung werden bereits heute schriftliche Unterlagen nicht mehr vollständig in Papierform verarbeitet, sondern beispielsweise in einem ersten Prozessschritt, z.B. in einer zentralen Poststelle, digitalisiert und fortan elektronisch weiterverarbeitet. Wie ein SRVwV-konformer Prozess für den Posteingang mit Archivierung schriftlicher Unterlagen aussehen könnte ist in Abbildung 4 angedeutet. Dieser Prozess könnte den Startpunkt für weitere elektronische Prozesse, ggf. unter Verwendung von Workflow-Steuerungs- und Dokumentenmanagement-Systemen, bilden.

Der grobe Ablauf ist wie folgt: Nach dem Posteingang wird danach unterschieden, ob ein Vermerk für die persönliche Zustellung vorhanden ist. Ist dies der Fall, so wird die Post wie gewohnt in Papierform zugestellt. Andernfalls wird die Post geöffnet, das Original gescannt

[8] Die verbleibende Alternative wäre lediglich die zusätzliche Aufbewahrung der Originalunterlagen, und ggf. zusätzlich die Verwendung derselben in papiergebundenen Prozessschritten. Beides wäre aus Kostengesichtspunkten sicherlich nicht optimal.

und (bei standardisierten Formularen) die relevante Information per Texterkennung extrahiert. Diese Informationen werden dem Posteingangs-Sachbearbeiter zur Überprüfung und ggf. Korrektur vorgelegt. Hier wird er insbesondere auch die Qualität des digitalen Abbildes und die Übereinstimmung mit dem Original überprüfen. Ist diese nicht gewährleistet, so führt er den Scan-Vorgang erneut durch. Andernfalls bestätigt er die Übereinstimmung mit einer qualifizierten elektronischen Signatur. Diese Signatur wird zusammen mit dem digitalen Abbild und ggf. den extrahierten Daten an das Archivsystem übergeben. Nachdem die ordnungsgemäße Ablage im Archiv überprüft wurde, können die Originalunterlagen vernichtet werden. Damit ist der Prozessablauf in der Poststelle beendet.

Der Sachbearbeiter hingegen erhält den Posteingang beispielsweise als E-Mail-Anhang und findet die zugehörigen Daten bereits im Enterprise Resource Planning (ERP) System. Später, oder falls Zweifel an der Integrität der Daten bestehen, kann der Sachbearbeiter die im Archiv abgelegten Daten auslesen und die Signatur überprüfen.

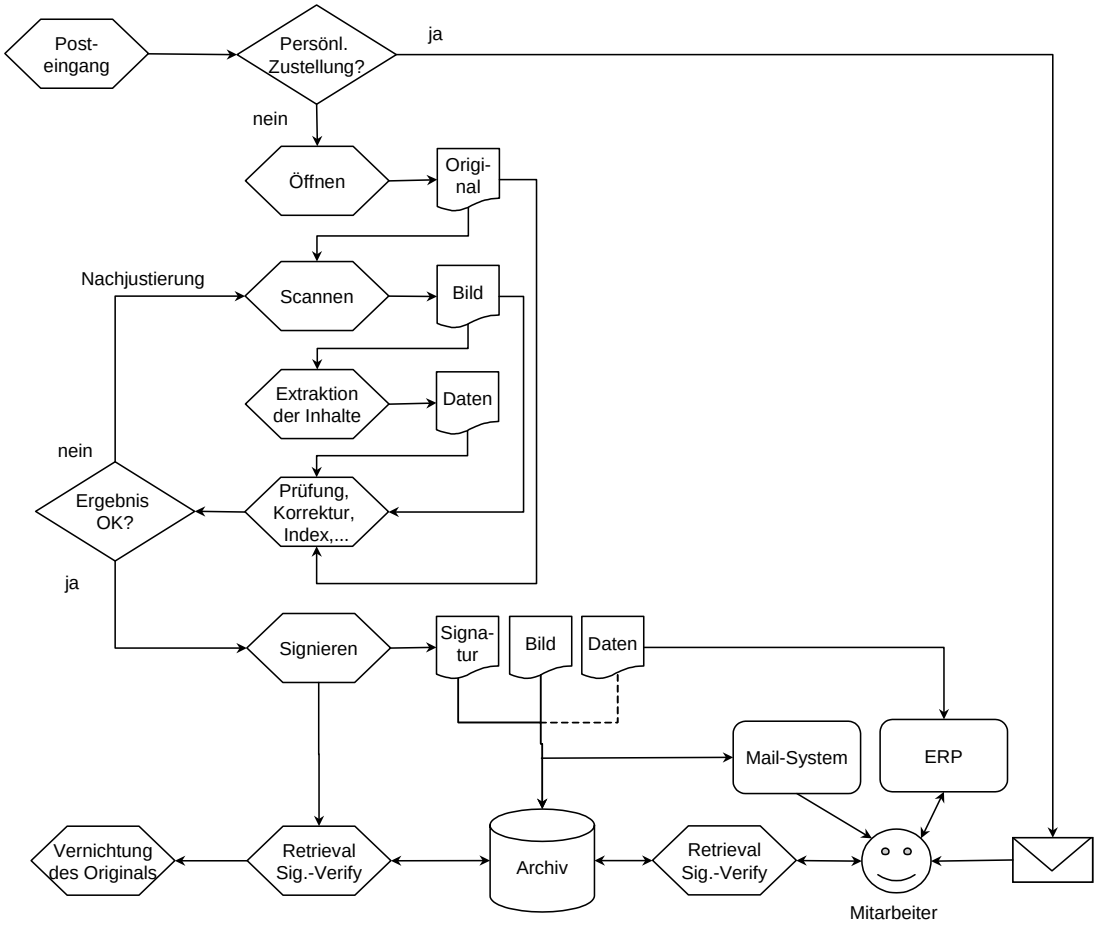

Abbildung 4: Möglicher Prozessablauf für Posteingang mit Archivierung

4.2 Abwicklung des Zahlungsverkehrs

Als weiteres in diesem Beitrag näher betrachtetes Beispiel soll die Workflow-gestützte Abwicklung des Zahlungsverkehrs dienen. Ermöglicht wird dies durch §40 SRVwV, wonach die in SRVwV geforderten Unterschriften durch qualifizierte elektronische Signaturen (mit Anbieterakkreditierung) ersetzt werden können.

Wir verzichten auf die umfassende Diskussion der organisatorischen Anforderungen aus SRVwV und begnügen uns, wie in Abbildung 5 ersichtlich, mit einer groben Skizze der wichtigsten Prozessschritte.

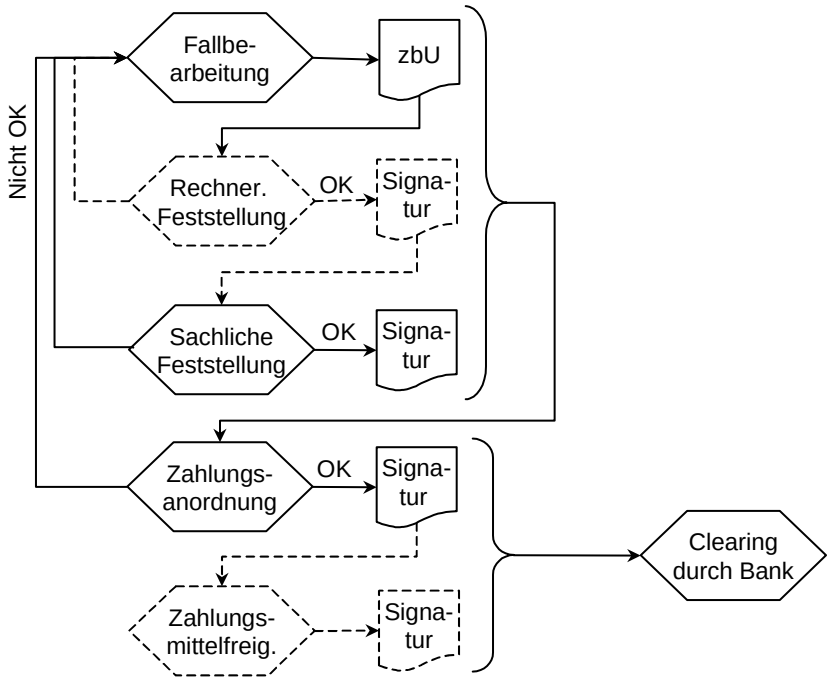

Abbildung 5: Möglicher Prozessablauf für Zahlungsverkehrsabwicklung

Die Initiierung des Zahlungsverkehrsprozesses liegt in der Bearbeitung eines Falles. Dort wird z.B. die Notwendigkeit einer Auszahlung an einen Versicherten oder Leistungserbringer erkannt. Bevor die Auszahlung gemäß §11 mittels elektronischer Signatur angeordnet werden kann, muss die sachliche (siehe §20) und ggf.[9] rechnerische (siehe §21) Richtigkeit des Vorganges festgestellt werden. Hierzu sind ggf. zahlungsbegründende Unterlagen (zbU) dem Arbeitsfluss beizufügen. Wird im Rahmen dieser mehrstufigen Prüfung ein Fehler offenbar, so wird der Fall an den zuständigen Sachbearbeiter zurückdelegiert. Ist dies nicht der Fall, so wird die Zahlungsanordnung mit einer zweiten[10] Signatur versehen und damit die Zahlungsmittel freigegeben.

Hier sei darauf hingewiesen, dass diese Prozessschritte gemäß §18 auch für Buchungen ohne Zahlungsvorgang angewandt werden müssen.

[9] Hier soll darauf hingewiesen werden, dass die rechnerische Feststellung in automatisierten Verfahren naheliegender Weise von IT-Systemen durchgeführt wird. So kann in der Dienstanweisung nach §40 SRVwV auf die explizite rechnerische Feststellung verzichtet werden, sofern z.B. ein integriertes IT-System diese Aufgabe übernimmt.

[10] In §4, Abs. 5, ist die Doppelzeichnung gegenüber dem Kreditinstitut gefordert. Sofern das konkrete technische und organisatorische Umfeld es erlaubt, kann dieses Vieraugenprinzip auch mit der Feststellung der Richtigkeit verbunden werden.

4.3 Elektronisches Rezept

Die elektronische Abwicklung der Arzneimittelverordnungen wurde bereits seit vielen Jahren diskutiert (siehe z.B. **[Stru92]** und **[Schu99]**) und hat in jüngster Zeit – insbesondere durch die gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenverbände im Gesundheitswesen am 03.05.2002 **[BMG+02]** – (wieder) starke Beachtung in der Öffentlichkeit gefunden.

Während derzeit noch technische, organisatorische und rechtliche Umsetzungsdetails für das elektronische Rezept erarbeitet werden, so steht die grundsätzliche Dimension des Einsparungspotenziales bereits fest. Um die Kosten und den Nutzen des elektronischen Rezeptes und einer leistungsfähigeren Krankenversichertenkarte transparent zu machen, wurden in **[DLS01]** neun verschiedene Szenarien untersucht. Diese Studie zeigt, dass das elektronische Rezept in Verbindung mit einer neuen Generation der Versichertenkarte den größten Nutzen bietet; der Break-Even-Point wird in diesem Fall bereits nach 12 Monaten erreicht. In den folgenden Jahren beträgt die prognostizierte Einsparung[11] mehr als 375 Mio. Euro.

Man darf gespannt sein, ob der Gesetzgeber im Zuge des elektronischen Rezeptes neben den unbedingt nötigen Gesetzesänderungen (siehe z.B. **[Schu99]** Kapitel E.4.5), auch die Regularien des Arzneimittelgesetzes (§ 43 AMG), wonach apothekenpflichtige Medikamente „nur in Apotheken und nicht im Wege des Versandes in den Verkehr gebracht werden“ dürfen, zugunsten von Versandapotheken anpassen wird, um so den Krankenkassen weitere Einsparungen zu ermöglichen.

Während die flächendeckende Einführung des elektronischen Rezeptes noch einige Jahre auf sich warten lassen wird, so sollten Krankenkassen diese Entwicklungen bei ihren langfristigen Überlegungen bzgl. der Einführung der elektronischen Signatur zumindest am Rande berücksichtigen.

5 Zusammenfassung

In diesem Beitrag wurden die wichtigsten – insbesondere gesetzlichen - Anforderungen an die Ausstellung und Anwendung von Zertifikaten im Umfeld der deutschen Sozialversicherungsträger zusammengetragen.

Die Analyse der rechtlichen Rahmenbedingungen in Abschnitt 2.3 zeigt insbesondere, dass der Einsatz von Zertifikaten, zur langfristig kostenminimalen Umsetzung der Anforderungen aus §78a **[SGB X]** zwar äußerst ratsam, aber per Gesetz und Verordnung nicht zwingend vorgeschrieben ist.

Anders sind hier die Anforderungen aus **[SVRV]** und **[SRVwV]** zu bewerten. Soll auf die kostenintensive papiergebundene Archivierung schriftlicher Unterlagen verzichtet werden, so müssen, gemäß §§36 und 44 SRVwV, ab August 2004 qualifizierte elektronische Signaturen (mit Anbieterakkreditierung gemäß §15 SigG) eingesetzt werden. Verwenden die Sozialversi-

[11] Den jährlichen Betriebskosten von 77 Mio. Euro stehen folgende jährlichen Einsparungen gegenüber: 71 Mio. Euro bei administrativen (papiergebundenen) Prozessen; 77 Mio. Euro durch eine verbesserte Abrechnungsprüfung; 153 Mio. Euro durch eine verbesserte Arzneimitteldokumentation; 24 Mio. Euro durch den Wegfall des alten KVK-Systemes.

cherungsträger solche Signaturen, so können auch die Kernprozesse der Leistungsabrechnung und Verwaltung, inklusive des Zahlungsverkehrs, elektronisch abgewickelt werden.

Derzeit erscheint es fraglich, ob die existierenden – in Abschnitt 3.1 skizzierten - Public-Key-Infrastrukturen der deutschen Sozialversicherungsträger in absehbarer Zeit in der Lage sind, die Anforderungen des Signaturgesetzes umzusetzen.

Da in Deutschland bereits *sechzehn* akkreditierte TrustCenter existieren, steht auch den Sozialversicherungsträgern bzgl. der elektronischen Abwicklung ihrer Geschäftsprozesse nichts grundsätzliches mehr im Weg. Das Einsparungspotenzial in Prozessen der öffentlichen Verwaltung kann nunmehr auch im Bereich der Sozialversicherung ausgeschöpft werden.

Hierbei sollte dem tatsächlichen Aufbau der IT-Infrastrukturen eine Analyse und Optimierung der Geschäftsprozesse vorangehen. Eine methodische Vorgehensweise für die risikominimale Realisierung elektronischer Geschäftsprozesse findet sich in **[eprocess]**.

Literatur

[AOK01] AOK Bundesverband: *Security Schnittstelle für das Gesundheitswesen für den Datenaustausch zwischen Leistungserbringern, Arbeitgebern und Krankenkassen*, Version 1.3 vom 23.07.2001, via http://www.itsg.de

[BDSG] *Bundesdatenschutzgesetz (BDSG)*, BGBl. 2001 Teil I Nr. 23, S. 904 ff., via http://www.bundesgesetzblatt.de/bgbl1f/b1findex.htm

[BMG+02] Bundesministerium für Gesundheit / Spitzenverbände im Gesundheitswesen: *Einigung mit Spitzenorganisationen auf elektronische Gesundheitskarte und elektronisches Rezept* (Pressemitteilung vom 03.05.2002), via http://www.bmgesundheit.de/presse/2002/2002/46.htm
Gemeinsame Erklärung des Bundesministerium für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen, via http://www.bmgesundheit.de/presse/2002/2002/46a.doc

[BrTe01] Bröhl G., Tettenborn A.: *Das neue Recht der elektronischen Signaturen: kommentierende Darstellung von Signaturgesetz und Signaturverordnung*, Bundesanzeiger-Verlag, ISBN 3-89817-045-4, 2001

[DEÜV] *Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung* (Artikel 1 der Verordnung zur Neuregelung des Meldeverfahrens in der Sozialversicherung), z.B. via http://jurcom5.juris.de/bundesrecht/de_v/htmltree.html

[DLS01] Debold & Lux / secunet: *Kommunikationsplattform im Gesundheitswesen – Kosten-Nutzen-Analyse – Neue Versichertenkarte und Elektronisches Rezept*, Studie im Auftrag der ABDA und des VdAK, 2001, via http://www.abda.de/ABDA/download/allgemeines/KNA1307.pdf

[eprocess] secunet Security Networks AG: *eprocess – Elektronische Geschäftsprozesse bei minimalen Risiken*, im vorliegenden Tagungsband

[FormVG] *Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr*, BGBl. 2001, Teil 1, Nr. 35, (18.07.2001), via http://www.dud.de

[HüJa01] Hühnlein D., Jaletzke A.: *Public-Key Infrastrukturen für Finanzdienstleister*, in Horster P. (Hrsg.): Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2001, ISBN 3-936052-00-X, SS. 155-167

[Hühn02] Hühnlein D.: *Public-Key Infrastrukturen in der Phase der Konsolidierung und Anwendung*, erschienen bei "Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung", ISBN 3-936052-04-02, IT-Verlag, 2002, SS. 365-382

[RegTP] RegTP - *Regulierungsbehörde für Telekommunikation und Post*: Homepage, siehe http://www.regtp.de

[RFC3039] RFC 3039: Santesson S., Polk W., Barzin P., Nystrom M.: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, via http://www.ietf.org

[Schu99] Schubert, F.: Das Elektronische Rezept: Chancen, Risiken und Gestaltungsmöglichkeiten, Diplomarbeit an der Uni Heidelberg / FH Heilbronn, 1999, via http://www.elektronisches-rezept.de/

[SGB I] SGB I: *Sozialgesetzbuch Erstes Buch (SGB I) Allgemeiner Teil*, in der Fassung vom 2. September 2001 (Fassung vom 7. August 1996 via http://www.sozialgesetzbuch.de)

[SGB IV] SGB IV: *Sozialgesetzbuch Viertes Buch (SGB IV) Gemeinsame Vorschriften für die Sozialversicherung*, in der Fassung vom 03.04.2001 (BGBl. I S. 467), via http://www.sozialgesetzbuch.de

[SGB X] SGB X: *Sozialgesetzbuch Zehntes Buch (SGB X) Verwaltungsverfahren, Schutz der Sozialdaten, Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten*, in der Fassung vom 18. Mai 2001 (Fassung vom 7. August 1996, via http://www.sozialgesetzbuch.de)

[SGB X§78] SGB X, §78a Rundschreiben: *Gemeinsames Rundschreiben der Spitzenverbände der Sozialversicherungsträger zu den datenschutzrechtlichen Vorschriften des SGB I und SGB X in der Fassung des Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001* (BGBl. I 904 ff.)

[SigG] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, BGBl. 2001 Teil I Nr. 22, S. 876 ff. (21.05.2001), via http://www.dud.de

[SigV] *Verordnung zur elektronischen Signatur*, vom Bundestag am 24.10.2001 verabschiedet, via http://www.dud.de

[SRVwV] *Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung*, (SRVwV) vom 15. Juli 1999, zuletzt geändert am 18. September 2000

[StÄndG] *Entwurf eines Gesetzes zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2001 - StÄndG 2001)*, via http://www.bundesfinanzministerium.de/Anlage4935/Entwurf-Steueraenderungsgesetz-2001.pdf

[Stru92] Struif, B.: *Das elektronische Rezept mit digitaler Unterschrift*, in Reimer H., Struif, B. (Hrsg.): Kommunikation und Sicherheit, Publikation des Teletrust Deutschland e.V., Bad Vilbel, Darmstadt, 1992

[SVRV] *Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (Sozialversicherungs-Rechnungsverordnung – SVRV)*, Bgbl. Teil I, S. 1627 (15. Juli 1999), via http://www.bundesgesetzblatt.de/bgbl1f/b1findex.htm

[Tele01] TeleTrusT e.V.: *ISIS-MTT-Spezifikation*, Version 1.0.1, 2001, via http://www.darmstadt.gmd.de/mailtrust/

[VgV] *Verordnung über die Vergabe öffentlicher Aufträge* (Vergabeverordnung - VgV), Bgbl. 2001, Teil I, Nr. 3, 18.01.2001, via http://www.bundesgesetzblatt.de/bgbl1f/b1findex.htm

[VwVfÄndG] *Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (VwVfÄndG)*, Entwurf vom 16.07.2001, via http://www.dud.de

[X.509] ITU-T Recommendation X.509: *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*, International Telecommunication Union, Genf, Schweiz, 1997 (dies ist äquivalent zu ISO/IEC 9594-8)