Aufbau einer Zertifizierungsinstanz (CA) an einer Hochschule Vorgehen, juristische Aspekte und Software-Unterstützung

Mario 'BitKoenig' Holbe
Hauptseminar Telematik
Institut für Praktische Informatik und Medieninformatik
Fakultät für Informatik und Automatisierung

30. März 2003

1 Motivation

Die derzeit dramatisch steigenden Studentenzahlen auch und aus unserem Blickwinkel insbesondere an der Technischen Universität Ilmenau, die zu zu einer immer deutlicher zunehmender Kommunikationsdichte führen und die althergebrachten Kommunikationswege des „persönlichen Kontakts“ zu verstopfen drohen, fordern geradezu nach effizienteren Mitteln und Wegen der Kommunikation untereinander.

Hier könnte die elektronische Kommunikation mittels und über das Internet via E-Mail, World Wide Web etc. einen Ausweg bieten. Um jedoch auch für diese Alternative die bisher gewohnte Vertrauensstellung der Kommunikationspartner untereinander, insbesondere die Identität der Gesprächspartner, die Authentizität der Kommunikation, der sogenannten Verbindlichkeit und ggf. deren Vertraulichkeit, die sich beim persönlichen Kontakt eher implizit ergeben, zu gewährleisten, sind bei diesem Medium spezielle Mechanismen der modernen Kryptographie notwendig.

2 Ziele

Ziel dieser Hauptseminarsarbeit soll sein, Know-How in den wichtigen Teilbereichen zu vermitteln, die beim Aufbau einer Zertifizierungsinstanz von Bedeutung

sind, um eine Entscheidungsgrundlage für die Wahl einer geeigneten CA-Form zu bilden.

Insbesondere sollen juristische, organisatorische und technische Voraussetzungen und Anforderungen beleuchtet werden.

3 Grundlagen

3.1 Historisches

Allgemein bekannt dürfte sein, daß die im Internetbereich verwendeten Protokolle, insbesondere das Internet Protocol (IP), unverschlüsselt sind, woraus sich offensichtlich ergibt, daß Kommunikation über das Internet von Dritten mit recht einfachen Methoden zumindest abgehört werden kann. Weniger offensichtlich, für unsere Bedürfnisse jedoch von eminenter Bedeutung ist die Tatsache, daß Kommunikation über das Internet dadurch beliebig modifizierbar wird und daß die Tatsache einer verfälschten Kommunikation von Sender und Empfänger einer Nachricht nicht notwendigerweise bemerkt wird oder gar auch nur bemerkbar ist.

Schon früh entwickelte sich aus diesen Umständen heraus insbesondere im Bereich der Fernadministration und -nutzung von Computern ein Bedarf an sicherer Datenübertragung, der primär die Abhörbarkeit von Datenverbindungen unterbinden wollte. Diesem Bedarf trugen Protokolle wie ssh (Secure Shell) Rechnung. Der Schwerpunkt hier lag offensichtlich auf dem Schutz der Vertraulichkeit von Kommunikationsverbindungen. Aus den zugrundeliegenden kryptopgraphischen Algorithmen ergibt sich üblicherweise zusätzlich eine implizite Authentizität der Verbindung, d.h. der Empfänger einer Nachricht kann nachträgliche Modifikationen derselben bemerken. Ähnliche Bedürfnisse erfüllte ursprünglich das https (Secure HTTP) im Bereich des World Wide Web. Im Bereich von E-Mail entwickelte sich PGP (Pretty Good Privacy) zum de-facto Standard, wobei hier aufgrund der speziellen Eigenschaft von E-Mails - eben Post zu sein - im Gegensatz zu den obigen Ansätzen von vornherein eher die Verbindlichkeit der Kommunikation, also die Identität der Kommunikationspartner und die Authentizität der kommunizierten Daten im Vordergrund stand. Grundlage all dieser Ansätze sind kryptographische Verfahren, insbesondere die Public Key Kryptographie.

3.2 Public Key Kryptographie

Im Jahre 1976 stellten Diffie und Hellman ein für die Kryptographie revolutionäres Verfahren vor [DH76], das sie zurecht mit *New Directions in Cryptography* überschrieben. Im Gegensatz zur symmetrischen Kryptographie, wo ein

Schlüssel von beiden Kommunikationspartnern zum Ver- und Entschlüsseln von Daten verwendet wird, stehen im Falle der Public Key Kryptographie jedem Kommunikationspartner zwei Schlüssel zur Verfügung: Ein Öffentlicher Schlüssel (Public Key), den er veröffentlicht und mit dem Nachrichten an den Inhaber verschlüsselt werden und ein Privater Schlüssel (Private Key), den er geheimhält und zum Entschlüsseln der mit dem Öffentlichen Schlüssel verschlüsselten Daten verwendet. Manche dieser Public Key Algorithmen bieten die angenehme Eigenschaft der Kommutativität, die es gestattet, beide zusammengehörigen Schlüssel in beliebiger Reihenfolge zu verwenden: Mit dem Öffentlichen Schlüssel verschlüsselte Daten können mit dem Privaten Schlüssel entschlüsselt werden und umgekehrt können auch mit dem Privaten Schlüssel verschlüsselte Daten mit dem Öffentlichen Schlüssel entschlüsselt werden. Somit ist der Inhaber des Privaten Schlüssels in der Lage, die Echtheit von Daten zu bestätigen, indem er sie verschlüsselt. Der Empfänger wiederum prüft dies durch Anwendung des ihm bekannten Öffentlichen Schlüssels. Im Allgemeinen ist es garnicht notwendig, die Daten tatsächlich zu verschlüsseln, es genügt bereits die Bildung eines Hashwertes über alle Daten, die der Empfänger entsprechend prüfen kann. Die Daten liegen somit weiter im Klartext vor. In diesem Fall spricht man von einer Signatur. Bekanntester Vertreter derartiger kommutativer Algorithmen ist der RSA-Algorithmus, benannt nach seinen Entwicklern Ronald Rivest Fiat Shamir und Leonard Adleman. Wie aus dem Verfahren ersichtlich wird, liegt nun das Augenmerk auf der Vertrauenswürdigkeit des Öffentlichen Schlüssels, insbesondere important ist die Frage, ob ein bestimmter Öffentlicher Schlüssel tatsächlich einer bestimmten Person gehört. Dieses Problem wird im Allgemeinen als Schlüsselverteilungsproblem bezeichnet. Für einen stark begrenzenten Personenkreis ist dies recht trivial über eine persönliche Übergabe aller Öffentlichen Schlüssel zu realisieren; nicht mehr praktikabel ist dieses Verfahren jedoch bei größeren Personenkreisen, hier werden besondere Infrastrukturen benötigt, die die Verteilung organisieren und insbesondere die Vertrauenswürdigkeit der Öffentlichen Schlüssel sicherstellen: die sogenannte Trust Infrastructure oder spezieller die Public Key Infrastructure. Im Falle von PGP existiert diese Infrastruktur in Form des sogenannten Web of Trust implizit, da jeder Schlüsselinhaber prinzipiell in der Lage ist, die Echtheit eines anderen Öffentlichen Schlüssels zu bestätigen. Im Falle von X.509(v3), mit dem sich dieses Dokument hauptsächlich beschäftigt, da es einen weit verbreiteten Standard darstellt, handelt es sich hierbei um einen hierarchisch organisierten Verbund sogenannter Zertifizierungsinstanzen, Certificate Authorities oder kurz CAs, die eine Zuordnung eines Öffentlichen Schlüssels zu einer bestimmten Person durch Ausstellung eines elektronischen Zertifikats bestätigen - zertifizieren. Damit reduziert sich das Schlüsselverteilungsproblem im Idealfall auf den Öffentlichen Schlüssel einer Wurzelinstanz,

die entweder direkt die Echtheit eines Öffentlichen Schlüssels einer Person oder die Echtheit eines Öffentlichen Schlüssels einer anderen Zertifizierungsinstanz bestätigt, die wiederum mit diesem die Echtheit eines Öffentlichen Schlüssels einer Person oder... usw. usf. In der Realität haben sich mehrere dieser Wurzelinstanzen etabliert, deren Menge ist jedoch dennoch überschaubar.

Eine weitere wichtige Aufgabe von Zertifizierungsinstanzen ist die Verwaltung sog. Widerrufslisten (Certificate Revocation Lists, CRLs): Listen mit zurückgenommenen Zertifikaten. Zertifikate können aus den verschiedensten Gründen zurückgenommen werden, beispielsweise weil die Ausstellung unter falschen Angaben erschlichen wurde oder weil der zu einem zertifizierten Öffentlichen Schlüssel gehörende Private Schlüssel kompromittiert wurde.

Da eine Zertifizierungsinstanz eine erhebliche Vertrauensstellung bei den Anwendern innehat bzw. innehaben will, ist es für sie unbedingt notwendig, sauber, klar und definiert zu arbeiten und dieses auch transparent an ihre Anwender und Dritte zu kommunizieren. Grundlage hierfür sind die sog. Zertifizierungsrichtlinien, auch Policy oder Certification Practice Statement, CPS genannt. Sie spezifizieren insbesondere:

- Wer zertifiziert: Die „Person“ Zertifizierungsinstanz, ihren Aufbau, ihre (Un)Abhängigkeiten, ihr Personal.
- Wer zertifiziert den Zertifizierer: Wer bestätigt die Echtheit der Zertifizierungsinstanz.
- Nach welchen Regeln und Richtlinien wird zertifiziert: ist es beispielsweise erforderlich, sich bei der Zertifizierungsinstanz persönlich vorzustellen und auszuweisen, um ein Zertifikat zu erhalten, oder reicht dazu eine (unsichere) E-Mail?
- Was wird zertifiziert: Auf jeden Fall bestätigt eine Zertifizierungsinstanz eine Bindung eines Öffentlichen Schlüssels an eine bestimmte Person. Darüber hinaus können jedoch noch viele weitere Attribute zertifiziert werden, wie z.B.
  - die Qualität eines bestimmten Schlüssels: wie fälschungssicher ist dieser, für wie lange, wie lange gilt er,
  - die Einhaltung bestimmter Regeln seitens der zertifizierten Person beispielsweise hinsichtlich der Vorsorge der Kompromittierung des Privaten Schlüssels,
  - wie schnell wird ein Widerruf eines Zertifikats publiziert,
  - welche Daten des Schlüsselinhabers werden gespeichert und wie lange,

– Garantien und Haftungsparamter der Zertifizierungsinstanz bzgl. falscher Zertifikate und daraus entstehender Schäden.

Diese Policy dient zwar in erster Linie der Information Dritter über die Arbeitsweise der Zertifizierungsinstanz, aber sie dient auch deren Absicherung, da sie genau spezifiziert, was die CA zertifiziert und wie sie dies tut. Dadurch vermeidet sie Mißverständnisse über die Bedeutung eines speziellen Zertifikats. Auf der anderen Seite ist ein Anwender, der einem Zertifikat vertrauen will, gut beraten, sich über die Policy der betreffenden Zertifizierungsinstanz zu informieren, um ebenjene Mißverständnisse auszuschließen.

4 Juristischer Hintergrund

Für den Betrieb einer Zertifizierunginstanz sind viele gesetzliche Vorschriften relevant. Die wichtigsten, weil am konkretesten auf Zertifizierungsinstanzen abzielenden, sind das deutsche Signaturgesetz mit der zugehörigen Signaturverordnung und die im zweiten Entwurf vorliegende EU-Richtlinie zur elektronischen Signatur. Darüber hinaus sind die Datenschutzgesetze der Bundesländer bzw. des jeweiligen Bundeslandes und des Bundes selbst maßgeblich.

4.1 Gesetz über Rahmenbedingungen für elektronische Signaturen

Das Gesetz über Rahmenbedingungen für elektronische Signaturen (auch Signaturgesetz oder kurz SigG) [Sig01a] ist in seiner Neufassung seit 16. Mai 2001 in Kraft. Diese löst seitdem die alte Fassung des Gesetzes zur digitalen Signatur vom 1. August 1997 ab, mit dem die Bundesrepublik Deutschland als eines der ersten Länder den Versuch unternommen hat, einen Rahmen für den Einsatz und die Anerkennung eines Äquivalents zur eigenhändigen Unterschrift in der digitalen Kommunikation zu schaffen. Die Neufassung verändert und vereinfacht an vielen Stellen die alte Rechtslage und orientiert sich an der EG-Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen [EGR99]. Das SigG zielt darauf ab, Rahmenbedingungen zu etablieren, unter denen elektronische Signaturen als sicher gelten und Fälschungen elektronischer Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können (§1 Abs. 1 SigG). Insofern ist es also eher ein Sicherungsinfrastruktur-Gesetz als ein Signaturgesetz und seine Bezeichnung leicht irreführend.

Der §2 SigG führt eine Reihe von Legaldefinitionen u.a. für einfache, fortgeschrittene und qualifizierte elektronische Signaturen und einfache und quali-

fizierte Zertifikate ein, wobei

- einfache elektronische Signaturen jegliche elektronische Daten sind, die zur Authentifizierung dienen und anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind (§2 Nr. 1 SigG),
- von fortgeschrittenen elektronischen Signaturen weiterhin die ausschließliche Zuordnung zum Inhaber, die Möglichkeit der Identifizierung des Inhabers, die alleinige Kontrolle des Inhabers über die zur Erzeugung verwendeten Mittel und eine Erkennbarkeit nachträglicher Veränderungen der signierten Daten (§2 Nr. 2 SigG) und
- von qualifizierten elektronischen Signaturen zusätzlich das Beruhen auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikats und die Erstellung mit einer sicheren Signaturerstellungseinheit (§2 Nr. 3 SigG) gefordert wird.

Damit ist beispielsweise jede E-Mail sozusagen bereits aufgrund ihres *From:* Headers einfach, jedoch nicht fortgeschritten elektronisch signiert. Jede mit PGP und einem nicht kompromittierten Schlüssel signierte E-Mail ist sozusagen im Sinne des Gesetzes fortgeschritten, jedoch nicht qualifiziert signiert.

Während einfache Zertifikate Signaturprüfschlüssel Personen zuordnen und dadurch ihre Identität bestätigen, können nach §2 Nr. 7 SigG qualifizierte Zertifikate ausschließlich für *natürliche* Personen ausgestellt werden. Dies bedeutet implizit, daß beispielsweise Unternehmen aber auch Webserver keine eigenen qualifizierten Zertifikate bekommen können. Dies macht aus der Sicht des Gesetzgebers durchaus Sinn, der ja die elektronische Signatur der eigenhändigen Unterschrift gleichstellen will - bekanntlich zeichnet für ein Unternehmen auch sein gesetzlicher Vertreter. Auch läßt sich hierdurch das Problem vermeiden, daß mehrere Personen mit dem gleichen Schlüssel rechtswirksam signieren können. Da jedoch §7 Abs. 1 Nr. 1 SigG explizit vorsieht, daß in einem Zertifikat an Stelle des Namens des Schlüsselinhabers auch ein dem Inhaber zugeordnetes unverwechselbares (jedoch kenntlich gemachtes) Pseudonym verwendet werden darf, könnten Zeichnungsberechtigte eines Unternehmens sich hierfür spezielle Schlüssel generieren und qualifiziert signieren lassen. Hierbei ist es nach §5 Abs. 2 SigG auch möglich, Angaben über ihre Vertretungsmacht für eine dritte Person (z.B. das Unternehmen) dem Zertifikat beizufügen.

Zu beachten ist, daß das SigG im weiteren ausschließlich auf qualifizierte Zertifikate abstellt. Insbesondere definiert der §2 Nr. 8 SigG: „Zertifizierungsdiensteanbieter [sind im Sinne dieses Gesetzes] natürliche oder juristische Personen, die qualifizierte Zertifikate oder qualifizierte Zeitstempel ausstellen“. Interessant

ist dieser Punkt aufgrund der Tatsache, daß das SigG und damit auch seine Vorschriften dadurch de facto für die Aussteller von einfachen Zertifikaten und für die Erstellung einfacher und fortgeschrittener Signaturen *nicht gilt* bzw. eben keine Vorschriften erläßt.

Der Anwendungsbereich des SigG umfaßt Zertifizierungsdienste. Deren Betrieb ist genehmigungsfrei, jedoch spätestens mit der Betriebsaufnahme der zuständigen Behörde anzuzeigen. Dies ist eine der Vereinfachungen gegenüber der alten Fassung des SigG, nach der es für den Betrieb einer Zertifizierungsinstanz einer *Genehmigung* der zuständigen Behörde bedurfte. Als zuständige Behörde wird im SigG die Regulierungsbehörde für Telekommunikation und Post ausgewiesen (§3 SigG i.V.m. §66 TKG [TKG98]). Der Betrieb eines Zertifizierungsinstanz ist nach §4 Abs. 2 SigG an vier Voraussetzungen geknüpft:

- Zuverlässigkeit des Betreibers,
- Fachkunde des in der Instanz tätigen Personals,
- Deckungsvorsorge des Betreibers und
- Erfüllung der technischen und organisatorischen Sicherheitsanforderungen des Gesetzes an die Zertifizierungsinstanz (Dieser Nachweis wird bei der Anzeige des Betriebs durch die Vorlage eines Sicherheitskonzeptes und dem Nachweis der geeigneten und praktische Umsetzung des Konzeptes erbracht).

Die zuständige Behörde muß den Betrieb einer Zertifizierungsinstanz untersagen, sobald obige Voraussetzungen nicht oder nicht mehr gegeben sind (§19 Abs. 3 SigG). Sie kann einer Sperrung qualifizierter Zertifikate anordnen, wenn sicher anzunehmen ist, daß sie gefälscht oder nicht hinreichend fälschungssicher sind, oder Sicherheitsmängel eine unbemerkte Verfälschung qualifizierter Signaturen oder qualifiziert signierter Daten zulassen (§19 Abs. 4 SigG).

Überdenkenswert ist, daß das SigG weiterhin auch eine Freiwillige Akkreditierung vorsieht, die zu erteilen ist, „wenn der Zertifizierungsdiensteanbieter nachweist, daß die Vorschriften nach diesem Gesetz [dem SigG] und der Rechtsverordnung nach §24 [der SigV] erfüllt sind“ (§15 Abs. 1 SigG). Akkreditierte Zertifizierungsdiensteanbieter „dürfen sich als akkreditierte Zertifizierungsdiensteanbieter bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen“ (§15 Abs. 1 SigG). Im Klartext bedeutet das wohl, daß sich der Zertifikatsnehmer erst bei akkreditierten Zertifizierungsdiensteanbietern wirklich sicher sein darf, daß diese gesetzeskonform arbeiten und daß nicht akkreditierte Zertifizierungsdiensteanbieter sich im Geschäftsverkehr eben nicht als gesetzeskonform bezeichnen dürfen. Eine durchaus interessante

Implikation. Desweiteren stellt die zuständige Behörde auch nur akkreditierten Zertifizierungsdiensteanbietern die für ihre Tätigkeit benötigten qualifizierten Zertifikate aus. Nicht akkreditierte Zertifizierungsdiensteanbieter müssen sich also ihre qualifizierten Zertifikate anderswoher besorgen.

4.2 Verordnung zur elektronischen Signatur

In §24 SigG wird die Bundesregierung ermächtigt, durch Rechtsverordnung Details zur elektronischen Signatur und zu SigG-Zertifizierungsinstanzen zu regeln, die im Signaturgesetz selbst ausgespart wurden. Dies betrifft alle wesentlichen Einzelheiten der Zertifizierung, der Pflichten einer Zertifizierungsinstanz und der Maßnahmen, mit denen ihre Einhaltung kontrolliert werden soll. Die Bundesregierung hat in der Verordnung zur elektronischen Signatur (auch Signaturverordnung oder kurz SigV) [Sig01b] die entsprechende Ausgestaltung der o.g. Bereiche geregelt.

Die SigV spezifiziert z.B.

- Form und Inhalt der Anzeige des Betriebs eines Zertifizierungsdienstes (§1 SigV),
- den Inhalt des Sicherheitskonzepts (§2 SigV),
- den Umfang der Dokumentation der Sicherheitsmaßnahmen zur Einhaltung des SigG und der SigV (§8 SigV),
- die Ausgestaltung der Deckungsvorsorge (§9 SigV),
- daß die Identifikation des in der SigV als Antragsteller bezeichneten Zertifikatnehmers bei der erstmaligen Beantragung anhand des Personalausweises oder des Reisepasses oder auf andere geeignete Weise vorzunehmen ist (bei Folgeanträgen kann von einer erneuten Identifikation abgesehen werden, wenn der Folgeantrag mit einer elektronischen Signatur des Antragstellers versehen ist) (§3 Abs. 1 SigV),
- daß der Zertifizierungsdiensteanbieter in einem öffentlich abrufbaren (§5 Abs. 1 S. 2) Zertifikatsverzeichnis jedes qualifizierte Zertifikat bis mindestens 5 Jahre nach Ablauf seiner Gültigkeit (§4 Abs. 1 SigV), ein akkreditierter Zertifizierungsdiensteanbieter sogar mindestens 35 Jahre nach Ablauf seiner Gültigkeit (§4 Abs. 2 SigV) zu führen hat und
- daß qualifizierte Zertifikate eine maximale Gültigkeitsdauer von fünf Jahren aufweisen dürfen (§14 Abs. 3 SigV).

Bereits das SigG erlegt der Zertifizierungsinstanz dem Zertifikatnehmer gegenüber eine Unterrichtungspflicht auf, sofern der Zertifikatnehmer nicht bereits unterrichtet wurde (§6 Abs. 3 SigG), die SigV ergänzt diese und verpflichtet die Zertifizierungsinstanz, die Informationen auf Antrag auch Dritten zugänglich zu machen. Die Unterrichtung hat in Form einer schriftlichen Belehrung zu erfolgen (§6 Abs. 3 SigG). Insbesondere ist der Zertifikatnehmer darüber zu unterrichten,

- welche Maßnahmen erforderlich sind, um seinen geheimen Signaturschlüssel vor unbefugtem Zugriff zu schützen (§6 Abs. 1 SigG, §6 Nr. 1, 2, 3 SigV),
- daß qualifiziert elektronisch signierte Daten bei Bedarf neu zu signieren sind, sobald die Signatur durch Ablauf ihrer Gültigkeit unsicher wird (§6 Abs. 1 SigG, §6 Nr. 5 SigV),
- daß eine qualifizierte elektronische Signatur im Rechtsverkehr der eigenhändigen Unterschrift weitgehend gleichgestellt ist (§6 Abs. 2 SigG),
- daß ein freiwilliges Akkreditierungssystem für Zertifizierungsdiensteanbieter existiert und
- daß es Beschwerde-, Schlichtungs- und Sperrmöglichkeiten gibt, die er in Anspruch nehmen kann.

Die bereits in der Fassung vom 22. Oktober 1997 etablierte Verpflichtung der Zertifizierungsinstanz zur unverzüglichen Sperrung beliebiger Zertifikate auf telefonische Anordnung der zuständigen Behörde hin nach geeigneter Authentifizierung des Anrufers, „wenn Tatsachen die Annahme rechtfertigen, daß qualifizierte Zertifikate gefälscht oder nicht hinreichend fälschungssicher sind oder daß sichere Signaturerstellungseinheiten Sicherheitsmängel aufweisen, die eine unbemerkte Fälschung qualifizierter elektronischer Signaturen oder eine unbemerkte Verfälschung damit signierter Daten zulassen“ (§19 Abs. 4 SigG) und die damit verbundene Gefahr, daß der Staat damit jederzeit in der Lage ist, den Betroffenen geradezu seiner digitalen Identität zu berauben, da „dies quasi der technisch durchgesetzten Beschränkung gleichkäme, keinerlei Verträge mehr unterzeichnen und sich nicht mehr ausweisen zu können“, wie in [Cam99] kritisiert wird, ist in der neuen Fassung ebenfalls enthalten. Lediglich der „telefonische Weg nach geeigneter Authentifizierung des Anrufers“ ist ersatzlos aus der SigV gestrichen worden.

Im Gegensatz zur alten Fassung der SigV spezifiziert die neue Fassung ebenfalls die Anforderungen an Produkte für qualifizierte elektronische Signaturen (§15 SigV). So müssen „sichere Signaturerstellungseinheiten“ beispielsweise gewährleisten, „daß der Signaturschlüssel erst nach Identifikation durch Besitz und

Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann“ und nicht preisgegeben wird. „Signaturanwendungskomponenten“ müssen u.a. gewährleisten, daß „eine Signatur nur durch die berechtigt signierende Person erfolgt“, „Die Erzeugung einer Signatur vorher eindeutig angezeigt wird“, bei Prüfung einer qualifizierten elektronischen Signatur „die Korrektheit der Signatur zuverlässig geprüft und zutreffend angezeigt wird“ und „eindeutig erkennbar wird, ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikat-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren“. Nach §17 Abs. 4 SigG sind die Anforderungen an Produkte für qualifizierte elektronische Signaturen durch anerkannte Stellen zu bestätigen. Bestätigte Produkte werden im Bundesanzeiger und z.B. in [RTP02a] veröffentlicht. Die RegTP hat weiterhin ein Rahmenwerk [RTP02b] verabschiedet, das die Einsatzbedingungen für Signaturanwendungskomponenten einheitlich spezifiziert.

5 Varianten einer Zertifizierungsinstanz

Die grundlegende Frage, die beim Aufbau einer Zertifizierungsinstanz zu beantworten ist, ist die nach der Einbettung in bestehende Zertifizierungsinfrastrukturen. Prinzipiell stehen hierfür 3 Alternativen zur Verfügung:

- Aufbau einer eigenen Root-CA
- Einbettung unterhalb der DFN-PCA
- Einbettung unterhalb einer SigG-konformen CA

Die Wahl der jeweiligen Variante ergibt sich direkt aus den Ansprüchen (etwa Rechtssicherheit, aber auch Personalaufwand), die an die aufzubauende Zertifizierungsinstanz gestellt werden.

Auf die jeweiligen Vor- und Nachteile der einzelnen Realisationsvarianten soll im folgenden eingegangen werden.

5.1 Aufbau einer eigenen Root-CA

Der Aufbau einer eigenen Root-CA stellt immer eine Insellösung dar. Der Vorteil dieser Variante ist die prinzipielle Unabhängigkeit von jeglichem politischen oder sozialen Umfeld. Dieser Vorteil ist jedoch auch gleichzeitig der große Nachteil einer Insellösung: Benutzer können nicht auf etablierte und evtl. bereits in Hard- und Software (Mail User Agents, Web Browser) unterstütze Zertifizierungsinfrastrukturen zurückgreifen, sondern sie sind gemeinsam mit dem Betreiber der CA darauf angewiesen, die Vertrauenswürdigkeit der Root-CA manuell herzustellen.

Insbesondere sind hier wieder klassische (Mensch-zu-Mensch) Kommunikationswege zur sicheren Übertragung des Root-Zertifikats zu beschreiten.

Es sollte eigentlich unnötig sein, zu erwähnen, daß die Bereitstellung der Zertifikate auf klassische Weise im Internet beispielsweise auf einer Webseite oder per E-Mail eine CA bereits ad absurdum führt, da diese ja eigentlich etabliert wird, weil vorher keine vertrauenswürdige Kommunikation über das Internet möglich ist. Leider wird diese Variante jedoch aus schlichter Unwissenheit immer wieder gewählt, daher soll an dieser Stelle dennoch in der gebotenen Kürze darauf eingegangen werden. Die Publikation einer Vertrauensbasis (und diese stellt das Zertifikat der Root-CA nun einmal dar) über nicht vertrauenswürdige Kanäle ist schlichter Unsinn: eine Kette ist bekanntlich so stark, wie ihr schwächstes Glied und daher kann das Vertrauen in ein Zertifikat niemals größer sein, als das Vertrauen in den zur Publikation verwendeten Kommunikationsweg. Ist das Vertrauen in den Kommunikationsweg jedoch groß genug, daß es akzeptiert wird, das Zertifikat darüber zu publizieren, braucht es eigentlich keine Zertifizierungsinstanz, die Vertrauen stärken soll. Daher kann man sich in diesem Spezialfall den Aufbau einer Zertifizierungsinstanz schlicht sparen.

Eine weitere vorteilhafte Ausprägung der Unabhängigkeit ist die freie Wahl der technischen Realisation, während man im Gegensatz dazu im Falle der Einbettung unterhalb einer anderen CA wohl häufig auf deren Vorgaben bzgl. unterstützter Zertifikate, Standards und evtl. auch Soft- und Hardware angewiesen ist.

Eine Root-CA kann sowohl SigG-konform als Zertifizierungsdiensteanbieter mit qualifizierten Zertifikaten als auch SigG-unkonform mit einfachen Zertifikaten aufgebaut werden. Da die Unterschiede hinsichtlich der Realisierung verglichen mit den anderen beiden Varianten marginal sind, wird an dieser Stelle darauf nicht weiter eingegangen. Die Realisierung einer „einfachen“ Root-CA ähnelt sehr stark der Realisierung einer CA unterhalb der DFN-PCA, wobei in diesem Falle jedoch keine weiteren Policies und Zertifizierungsrichtlinien zu beachten sind (auch wenn dies zumindest im Falle der DFN-PCA Policy durchaus empfehlenswert ist) und die Realisierung einer einer SigG-konformen CA ähnelt analog der Realisierung einer CA unterhalb einer anderen SigG-konformen CA. Lediglich der jeweils erforderliche Verhandlungs-, Abstimmungs- und Zertifizierungsaufwand entfällt, da das Root-Zertifikat jeweils selbst generiert wird.

5.2 Einbettung unterhalb der DFN-PCA

Die Einbettung einer CA unterhalb der DFN-PCA gestaltet sich aus organisatorischen Gesichtspunkten relativ einfach, da die DFN-PCA *kein* Zertifizierungsdiensteanbieter i.S.d. SigG ist. Dies impliziert unter anderem, daß Zerti-

fikate der DFN-PCA und damit auch alle Zertifikate von CAs unterhalb der DFN-PCA einfache Zertifikate sind und daß Anwender daher maximal fortgeschrittene Signaturen i.S.d. SigG erzeugen können. Insbesondere besteht daher für die Zertifizierungsinstanz keine Anzeigepflicht, keine Unterrichtungspflicht gegenüber dem Anwender und vor allem keine Haftung und keine Pflicht zur Deckungsvorsorge. Damit stellt sich jedoch natürlich ebenfalls direkt die Frage nach der zu erreichenden Rechtssicherheit derartiger Signaturen und Zertifikate. Auf diese wird leider nirgends eingegangen, es ist daher davon auszugehen, daß eine Rechtssicherheit per Gesetz nicht besteht. Einfache und fortgeschrittene Signaturen unterliegen allerdings selbstverständlich der freien Beweismittelwürdigung deutscher Gerichte, wie auch [Mar00] und [Wol99] feststellen. Es ist daher sinnvoll, diese zu unterstützen und die benötigte bzw. erwünschte Rechtssicherheit (beispielsweise die Bindung an die Signatur und geforderte Maßnahmen zur Sicherstellung der Vertraulichkeit des Signaturschlüssels) über entsprechende Verträge bzw. Satzungen herzustellen.

Auch wenn eine Zertifizierungsinstanz unterhalb der DFN-PCA nicht dem SigG unterliegt, so ist sie doch an die Certification Policy (RFC1422 [Ken93]) der ihr übgergeordneten CA gebunden, im Falle der DFN-PCA ist dies [DFN03]. Die Policy der DFN-PCA ist hinsichtlich ihrer Sicherheitsanforderungen wesentlich weniger restriktiv, als dies SigG/SigV sind. Das resultiert nicht zuletzt daraus, daß die im Rahmen der DFN-PCA eingesetzte Technik nicht den Anforderungen des SigG entspricht.

5.3 Einbettung unterhalb einer SigG-konformen CA

Die Einbettung eines Zertifizierungsdienstleisters i.S.d. SigG unterhalb eines anderen Zertifizierungsdienstleisters impliziert sämtliche Vor- und Nachteile des SigG. So sind insbesondere ein Sicherheitskonzept zu erstellen, von der RegTP bestätigte Produkte zu verwenden, eine Deckungsvorsorge zu errichten, der Betrieb anzuzeigen und eine fortlaufende Dokumentation der Tätigkeiten der CA vorzunehmen. Die Forderung nach bestätigten Produkten läßt den Einsatz von verbreiteter Standard-Hard- und -Software nahezu unmöglich erscheinen, es sei denn, der Zertifizierungsdienstleisters läßt ebenjene als geeignet i.S.d. SigG bestätigen. Viel wahrscheinlicher und vermutlich kostengünstiger ist der Einsatz bereits bestätigter Produkte. Auch dies jedoch dürfte sich gravierend in hohen Initialkosten wiederspiegeln.

Diese Alternative bietet natürlich dem Anwender die vollständige Rechtssicherheit, die das SigG schafft: die CA stellt qualifizierte Zertifikate aus, der Anwender kann qualifiziert signieren und hat damit im elektronischen Verkehr eine der eigenhändigen Unterschrift weitestgehend gleichstehende Identifikati-

onsmöglichkeit.

Demgegenüber steht die umfangreiche Haftung des Zertifizierungsdienstleisters nach §11 SigG und die geforderte Deckungsvorsorge mit mindestens 250.000 Euro pro Schadensfall nach §12 SigG und im Falle des Abschlusses einer Haftpflichtversicherung mit einer Mindestversicherungssumme von 2,5 Mio Euro pro Schadensfall nach §9 SigV.

Es dürfte leicht einsichtig sein, daß sich allein aus diesen Beträgen erhebliche laufende Kosten kalkulieren lassen, auch ohne den personellen und fortlaufenden Schulungs-Aufwand zu berücksichtigen.

Da auch der Anwender zur Erstellung qualifizierter elektronischer Signaturen von der RegTP bestätigte sichere Signaturerstellungseinheiten und sichere Signaturanwendungskomponenten zu verwenden hat, scheidet auch hier die Verwendung von verbreiteter Standard-Software aus und bedeutet insbesondere auch für jeden einzelnen Anwender eine nicht zu unterschätzende finanzielle Belastung aus der Beschaffung ebenjener Technik heraus.

5.4 Einbettung als Registrierungsinstanz (RA) unterhalb einer SigG-konformen CA

Im Gegensatz zu einer Zertifizierungsinstanz ist eine Registrierungsinstanz keine eigenständige Einheit, sondern sozusagen einer verlängerter bürokratischer Arm der Zertifizierungsinstanz zu der sie gehört. Eine RA stellt selbst keine Zertifikate aus, sondern nimmt nur Zertifizierungsanträge entgegen, identifiziert die Antragsteller und leitet den Antrag an die entsprechende CA weiter. Der Vorteil dieser Alternative ist die Tatsache, daß die juristische Verantwortung allein bei der zuständigen CA liegt, dies betrifft insbesondere Fragen der Haftung. Im allgemeinen wird daher das kalkulierte Haftungsrisiko in Form von Kosten pro zertifiziertem Schlüssel auf die Registrierungsinstanz zurückübertragen. Die RA ist hinsichtlich der Verfahrensweise bei Stellung eines Zertifizierungsantrags, hinsichtlich der verwendeten Hard- und Software etc. vollständig von den Vorgaben ihrer Zertifizierungsinstanz abhängig. Dadurch ergibt sich eine wesentlich transparentere Aufschlüsselung der Initial- und Folgekosten, wobei die laufenden Kosten, die eine RA verursacht, abgesehen von Personalkosten wiederum direkt von der Anzahl der zu signierenden Schlüssel abhängt.

Die Möglichkeit, eine RA unterhalb der DFN-PCA zu betreiben besteht nicht. Die DFN-PCA unterstützt dieses Verfahren nicht.

6 Technischer Hintergrund

Die Wahl der verwendeten technischen Realisierungen innerhalb einer Zertifizierungsinstanz hängt direkt mit der Wahl der CA-Form zusammen. So kann für eine SigG-konforme CA zwangsläufig nur von der RegTP bestätigte Technik [RTP02a] eingesetzt werden und zwar sowohl auf CA- als auch auf Anwender-Seite.

Für den Fall einer nicht-SigG-konformen CA sollte auf Seiten der Zertifizierungsinstanz freie Software, wie

- OpenSSL
- OpenCA: eine freie Plattform, die alle wichtigen Arbeitsschritte einer CA unter einer Web-Oberfläche zusammenführt und unterstützt
- evtl. PGP, wenn neben X.509v3 auch PGP-Zertifikate unterstützt werden sollen

verwendet werden, wie dies auch die DFN-PCA empfiehlt. Dadurch ergibt sich anwenderseitig die Möglichkeit, mit seiner vorhandenen Software, wie z.B. Mozilla, Netscape, Internet Explorer, Outlook, etc. wie bisher weiterzuarbeiten.

Als Zertifizierungs-Hardware empfihelt die DFN-PCA einen Laptop mit entsprechendem Diebstahlschutz, da dieser relativ einfach weggeschlossen werden kann.

Daß ein Zertifizierungs-System mit Ausnahme der Veröffentlichungsplattform keine Verbindung zum Internet benötigt oder haben sollte, versteht sich von selbst.

Die Wahl der benutzten Technik wird die Größe der Zielgruppe und die Akzeptanz der CA innerhalb der angestrebten Zielgruppe maßgeblich beeinflussen. Kann ein normaler Anwender seine Standard-Software verwenden, die er sowieso besitzt, wird er den Umgang mit Signaturen und Zertifikaten viel eher akzeptieren, als wenn er darauf angewiesen ist, sich teure zusätzliche Hard- und Software zu beschaffen oder alternativ Orte aufzusuchen, an denen diese existiert.

Daher könnte sich eine Entscheidung für freie Software und verbreitete Standards im Falle einer Universitäts-CA gravierend auf Erfolg oder Mißerfolg des Projekts auswirken.

7 Organisatorischer Hintergrund

Die Tätigkeiten, die zum Aufbau und zum Betrieb einer Zertifizierungsinstanz erforderlich sind, sind weitestgehend unabhängig von der Wahl der tatsächlichen

CA-Form. Lediglich der Aufwand der dafür im Einzelnen zu betreiben ist, wird verschieden sein. Im folgenden sollen diese Tätigkeiten kurz vorgestellt werden.

7.1 Im Vorfeld und der Aufbauphase einer CA

7.1.1 Erstellung eines Arbeitskonzepts

Wichtigster Schritt vor dem praktischen Aufbau einer Zertifizierungsinstanz ist die Planung derselben. Auch wenn diese eigentlich vor jedem Projekt stehen sollte, bekommt sie im Falle einer Zertifizierungsinstanz eine spezielle Bedeutung aufgrund der Tatsache, daß ebenjener von nahezu Fremden in hohem Umfang Vertrauen entgegengebracht werden soll. Allein deshalb ist die Schaffung einer Vertrauensbasis unumgänglich. Dies kann jedoch langfristig nur erreicht werden, wenn die Organisations-, Ablauf- und Aufbaustruktur einer CA transparent und somit prüfbar gemacht werden kann.

Die genaue Ausprägung des Arbeitskonzepts ist zwar u.U. abhängig von der gewählten CA-Form, da beispielsweise das SigG oder auch die DFN-PCA bestimmte Voraussetzungen diesbezüglich enthalten, aber in jedem Fall sollte ein Arbeitskonzept Verantwortungsbereiche, Sicherheitsrichtlinien und einen Notfallplan umfassen.

Verantwortungsbereiche abzugrenzen ist besonders wichtig, da die Mitarbeiter einer Zertifizierungsinstanz üblicherweise sehr verantwortungsschwangere Positionen bekleiden. Um diese ausfüllen zu können, ist ein Gefühl der Rechtssicherheit und der Eigenverantwortlichkeit für einen klar umgrenzten Bereich erforderlich, das durch ein verständliches Arbeitskonzept vermittelt werden kann. Auch Dritten, die beispielsweise Ansprechpartner innerhalb der CA suchen oder einfach deren Arbeitsweise verstehen wollen, helfen klar umrissene Verantwortungsbereiche. Im Arbeitskonzept sollten alle Tätigkeiten erfaßt sein, die zum Aufbau und zum Betrieb der Zertifizierungsinstanz notwendig sind, also auch Wartungs- und Datensicherungs-Tätigkeiten.

Ein Sicherheitskonzept sollte ebenfalls wesentlicher Bestandteil eines Arbeitskonzeptes einer CA sein. Das SigG fordert dies sogar explizit. Auch hier steht der Aspekt der Nachvollziehbarkeit und Vertrauensbildung für eigene Mitarbeiter und Dritte im Vordergrund der Erstellung.

Ein weiterer wichtiger Bestandteil eines Arbeitskonzepts ist ein Notfallkonzept. Erst ein von vornherein kalkulierter und geplanter Umgang mit Notfällen vermittelt einen seriösen Eindruck nach außen und hilft, die Mitarbeiter permanent auf den „Tag-X“ hin einzustellen und zu trainieren.

Einen hohen Stellenwert innerhalb des Arbeitskonzepts einer CA sollte dem sog. *Vier-Augen-Prinzip* oder allgemein *Mehr-Augen-Prinzip* eingeräumt sein: „Viele Angriffe erfolgen durch Insider, also durch Mitarbeiter oder sonstige An-

gehörige der geschädigten Institution. Daher sollten vorsorglich auch gegen Mißbrauch oder Schädigungen durch CA-Mitarbeiter Vorkehrungen getroffen werden. Hierzu zählt zum Beispiel, den Zugriff auf wichtige Ressourcen so zu regulieren, daß er nicht von einem Mitarbeiter alleine ausgeübt werden kann“ [CKLW00].

Hervorragende Quelle zum Umfang des Arbeitskonzeptes sind [Cam99] und [CKLW00].

7.1.2 Erstellung einer Policy

Die Erstellung einer Zertifizierungs-Policy ist häufig durch übergeordnete CAs, wie z.B. die DFN-PCA oder auch durch das SigG bereits vorgeschrieben, sollte jedoch in jedem Fall essentielle Dokumentation einer Zertifizierungsinstanz sein. Die Policy bildet die Grundlage fast aller Tätigkeiten einer CA und legt darüber hinaus Richtlinien fest, die von den unterhalb der CA zertifizierten CAs und Benutzern einzuhalten sind. Sie ist üblicherweise erster Anlaufpunkt für Dritte, die die Vertrauenswürdigkeit einer CA prüfen wollen.

7.2 Im Betrieb einer CA

7.2.1 Ausstellen von Zertifikaten, Veröffentlichung

Das Ausstellen von normalen, aber auch Widerrufs-Zertifikaten und deren Veröffentlichung ist die Haupt-Tätigkeit einer Zertifizierungsinstanz. Der genaue Ablauf dieser Tätigkeiten sollte im Arbeitskonzept spezifiziert sein. Die Mitarbeiter sollten diese Tätigkeiten aus Gründen der Nachvollziehbarkeit unbedingt dokumentieren. Hilfreich wäre eine Software-gestütze Dokumentation, evtl. sogar von der Zertifizierungssoftware zur Verfügung gestellt.

7.2.2 Datensicherung, Wartung, Training, Dokumentation

Alle diese Tätigkeiten fallen mehr oder weniger periodisch an. Auf jeden Fall sollte jedem Mitarbeiter auch bei diesen Tätigkeiten jederzeit die datenschutzrechtliche Brisanz *aller* Tätigkeiten im Zusammenhang mit einer Zertifizierungsinstanz gegenwärtig sein. Es versteht sich von selbst, daß eine Einbettung der Datensicherung in eventuell existierende organisationsweite Datensicherungsinfrastrukturen aufgrund der Brisanz der vorgehaltenen Daten kaum in Frage kommen dürfte.

Eine hervorragende Möglichkeit, den Mitarbeitern die Brisanz der betroffenen Daten permanent vor Augen zu halten, ist ein mehr oder weniger regelmäßiges Training der nicht alltäglichen Arbeitsabläufe, insbesondere derer im Notfall.

Ein weiterer wichtiger Aspekt ist die regelmäßige Schulung der Mitarbeiter in allen sie betreffenden Bereichen, wie z.B. Datenschutz, Kryptographie, Systemsicherheit, da Sicherheit immer ein dynamischer Prozess ist. Das Know-How aller Mitarbeiter ist das wichtigste Kapital einer Zertifizierungsinstanz.

7.3 Kosten

Die beim Aufbau und beim Betrieb anfallenden Kosten sind stark abhängig von der gewählten CA-Form, der Zahl der verwalteten Zertifikate und deren Änderungshäufigkeit.

Während sich die laufenden Kosten einer Zertifizierungsinstanz vorwiegend aus den Personalkosten ergeben, sind in der Aufbauphase zusätzlich auch Hard- und Software-Kosten zu kalkulieren. Diese hängen natürlich direkt von der verwendeten Hard- und Software ab. Eine gute Quelle für die im Aufbau und Betrieb einer (wohlgemerkt nicht SigG-konformen) Universitäts-CA anfallenden Kosten, die die Verwendung freier Software voraussetzt, ist [DFN02]. Hier werden die initialen Kosten mit ca. 8.000 Euro für die notwendige Hardware kalkuliert. Die Kosten für den Betrieb einer SigG-konformen CA dürften zum einen aufgrund der zu verwendenden von der RegTP bestätigten (kommerziellen) Technik, als auch zum anderen aufgrund der höheren Ansprüche an Dokumentation und Verfügbarkeit, sowie aufgrund der Deckungsvorsorge erheblich höher sein.

Wesentlich besser dürften die anfallenden Kosten im Falle einer Registrierungsinstanz zu kalkulieren sein, da sie sich da ja neben den Personalkosten in direkter Abhängigkeit von den zertifizierten Schlüsseln entwickeln.

7.4 Personal

Eine der wesentlichsten Fragen im Vorfeld des Aufbaus einer Zertifizierungsinstanz ist die nach dem erforderlichen Personalaufwand. Schon allein aufgrund der herausragenden Vertrauensstellung ist der Betrieb einer CA nicht einfach mit dem Betrieb anderer Dienste vergleichbar. Insbesondere sollte das Personal der CA klar und so eng wie möglich umrissen sein. Klar ist ebenfalls, daß eine Umsetzung des Vier-Augen-Prinzips mindestens zweier Mitarbeiter bedarf. Eine Zertifizierungsinstanz ist eine in sich geschlossene Einheit, in der kein sachfremdes Personal etwas zu suchen hat.

Eine gute Quelle für den Personalaufwand einer Universitäts-CA ist [DFN02]. Diese umreißt die Personalanforderungen mit:

kleine CA: 1 Stelle: $\frac{1}{2}$ Stelle Organisation, $\frac{1}{2}$ Stelle Technik

große CA: 3 Stellen: 2 Stellen Organisation, 1 Stelle Technik

Nicht unterschätzt werden sollte hierbei der initiale Aufwand zum einen zum Aufbau der CA, dieser wird mit 3 Mann-Monaten umrissen und auch die Phase der Erstvergabe von Zertifikaten. Bei einer angenommenen Menge von 5.000 auszustellenden Zertifikaten und einem abgeschätzten Arbeitsaufwand von ca. 5 Minuten für die Entgegennahme des Antrags samt Identifikation des Antragsstellers und ca. 10 bis 20 Minuten für sämtliche erforderlichen Tätigkeiten, wie das Zertifizieren, Veröffentlichen und Benachrichtigen des Antragstellers ergibt sich hier offenkundig ein Initialaufwand von ca. 1.600 Arbeitsstunden, das ergibt bei einer Regelarbeitszeit von 8 Stunden pro Tag und 5 Arbeitstagen pro Woche einen Personalaufwand von immerhin 208 Mann-Tagen, 41 Mann-Wochen oder 10 Mann-Monaten.

Der Personalaufwand für den Betrieb einer SigG-konformen CA dürfte diesen aufgrund der höheren Ansprüche an Dokumentation und Verfügbarkeit und nicht zuletzt aufgrund der geforderten Fachkunde der Mitarbeiter, der regelmäßig in Form professioneller Schulungen Rechnung getragen werden müßte erheblich überschreiten.

8 Zusammenfassung

Die Wahl der Form der aufzubauenden Zertifizierungsinstanz ist offensichtlich keineswegs trivial. Insbesondere hängt diese Wahl direkt vom Zweck der zu zertifizierenden Schlüssel ab:

- Sollen die Schlüssel wirklich einem umfassenden Rechtsverkehr im Internet dienen?
- Soll der Anwender mit diesem zertifizierten Schlüssel wirklich in der Lage sein, rechtswirksam Verträge abzuschließen?
- Will die Zertifizierungsinstanz dafür wirklich haften?

Die Form der CA hängt also direkt von der benötigten Rechtssicherheit ab. Insbesondere ist hier zu hinterfragen, ob für eine Kommunikation zwischen Universität und Studenten diese Rechtssicherheit nicht auch über das Satzungsrecht der Universität gewährleistet werden kann.

Der zu investierende Personalaufwand im Rahmen eines Zertifizierungsdiensteanbieters nach SigG dürfte den einer eingeschränkten, dafür jedoch nicht SigG-konformen CA um ein Vielfaches übersteigen und bereits der ist bei ca. 10.000 zu verwaltenden Zertifikaten keineswegs im Bereich von „wir machen das mal so nebenbei“ einzuordnen.

Auch die Frage nach den aufzubringenden Kosten dürfte eine genaue Analyse unumgänglich machen, ob die Rechtssicherheit des SigG für eine Kommunikation zwischen Universität und Studenten tatsächlich benötigt wird.

Insbesondere zum Sammeln von Erfahrungen im Umgang mit Zertifikaten und Widerrufslisten, hinsichtlich des Verständnisses und der Akzeptanz elektronischer Signaturen seitens der Anwender und der Wahl von Hard- und Software sowohl auf Seiten der CA als auch auf Seiten der Anwender dürfte es jedoch in jedem Fall sinnvoll sein, zuerst - möglicherweise im Rahmen eines Pilotprojekts - eine einfache Zertifizierungsinstanz zu realisieren.

9 Ausblick

Der Aufbau auch einer einfachen Zertifizierungsinstanz als Basis einer vertrauenswürdigen elektronischen Kommunikation kann wertvolle Erfahrungen insbesondere im organisatorischen und technischen Bereich liefern.

Ob diese CA unterhalb der DFN-PCA oder als eigene Root-CA aufgebaut wird, spielt keine besonders große Rolle, da eine nachträgliche Zertifizierung durch die DFN-PCA jederzeit möglich ist.

Es kann dadurch ebenfalls der tatsächliche Bedarf an Rechtssicherheit seitens der Anwender und das tatsächliche Anwendungsspektrum beobachtet werden, Erfahrungen im juristischen Umgang mit einer Zertifizierungsinstanz sind äußerst wichtig für deren reibungslosen Betrieb.

Wenn dann festgestellt werden sollte, daß der Bedarf an einem SigG Zertifizierungsdiensteanbieter tatsächlich besteht, kann durchaus versucht werden, die bestehende CA in eine SigG-konforme umzuwandeln, wahrscheinlich wäre es jedoch dann sinnvoller, eine Registrierungsinstanz eines bestehenden Zertifizierungsdiensteanbieters zu etablieren und für weniger rechtskritische Anwendungen weiterhin die bestehende CA zu nutzen.

Literatur

[Cam99] Ingmar Camphausen. Entwurf eines Konzepts für eine Zertifizierungsstelle für die Freie Universität Berlin. Master's thesis, Technische Universität Berlin, Institut für Angewandte Informatik, Fachgebiet Informatik und Gesellschaft, 1999.
`http://userpage.fu-berlin.de/~ingmar/diplomarb/`.

[CKLW00] Ingmar Camphausen, Stefan Kelm, Britta Liedtke, and Lars Weber. *DFN-PCA Handbuch - Aufbau und Betrieb einer Zertifizierungsin-*

stanz. DFN-CERT - Zentrum für sichere Netzdienste GmbH, March 2000.

[DFN02] DFN-PCA: Aufwand beim Betrieb einer Uni-CA, December 2002. `http://www.dfn-pca.de/certify/aufwand-print.html`.

[DFN03] Die Policies der DFN-PCA, January 2003. `http://www.dfn-pca.de/certification/policies/`.

[DH76] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976.

[EGR99] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt Nr. L 013 vom 19. Januar 2000 S. 0012 - 0020, 1999.

[Ken93] S. A. Kent. Privacy enhancement for Internet electronic mail: Part II: certificate-based key management. RFC 1422, Internet Engineering Task Force, February 1993.

[Mar00] Alexander Marschall. Online Ticketing - der sichere Ticketverkauf von zuhause aus, May 2000. `http://www.mmsc-hessen.de/archiv/vortraege/slides/2704/marshall/`.

[RTP02a] Produkte für qualifizierte elektronische Signaturen / Technische Komponenten, October 2002. `http://www.regtp.de/tech_reg_tele/in_06-02-02-00-00_m/07/index.html`.

[RTP02b] Rahmenwerk für die einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten, May 2002. `http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/118.pdf`.

[Sig01a] Gesetz über Rahmenbedingungen für elektronische Signaturen vom 16. Mai 2001, BGBl. I, S. 876, 2001.

[Sig01b] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001, BGBl. I, S. 3074, 2001.

[TKG98] Telekommunikationsgesetz (TKG) vom 25. Juli 1996, BGBl. I, S. 1120, geändert durch Art. 2 Abs. 34 des Begleitgesetzes zum Telekommunikationsgesetz vom 17. Dezember 1997, BGBl. I, S. 3108, geändert durch Art. 2 Abs. 6 des Sechsten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen vom 26. August 1998, BGBl. I, S. 2544, 1998.

[Wol99] Stephen Wolthusen. Sicherheit im Internet - Grundlage für sichere Geschäftsprozesse?, October 1999. http://www.mmsc-hessen.de/archiv/vortraege/slides/wolthusen/.