

Geschlechtsneutrale Bezeichnungen:

In der folgenden Ausarbeitung wird i.d.R. der Plural verwendet. Im Hinblick auf eine leichtere Lesbarkeit wurde auf die jeweils weibliche und männliche Form verzichtet. Der Plural soll selbstverständlich beide umfassen.

Verfasser:

Arbeitskreis "Digitales Rathaus" im Deutschen Städtetag, Arbeitsgruppe 2

Tina Siegfried, Difu Berlin

Dr. Christian Mrugalla, BSI Bonn

Gerd Thurau, Stadt Hagen,

Gunnar Wolf, Landeshauptstadt Stuttgart

Ulf Steinmetz, Stadt Köln

Stand: Oktober 2002

© Deutscher Städtetag, Köln

Lindenallee 13 – 17

50968 Köln

Alle Rechte vorbehalten

Seite - 3 -

Abkürzungsverzeichnis:

AK DigRa	Arbeitskreis „Digitales Rathaus“ des Deutschen Städtetags
CA	„Certification Authority“; (Vertrauenswürdige) Stelle, die Schlüsselzertifikate für die asymmetrische Kryptographie ausstellt
G2B	„Government to Business“; (elektronische) Kommunikation zwischen Verwaltung und Unternehmen
G2C	„Government to Citizen“; (elektronische) Kommunikation zwischen Verwaltung und Bürgern
G2G	„Government to Government“; (elektronische) Kommunikation zwischen Verwaltungen
ISIS-MTT	Interoperabilitätsstandard für Systeme zur kryptographischen Absicherung der Internet-Kommunikation (Industrial Interoperability Specification & MailTrust)
IuK	Information und Kommunikation
OSCI	Online Services Computer Interface; Im Rahmen des Media@Komm-Programms entwickeltes Kommunikationsprotokoll, das insbesondere für die strukturierte Kommunikation im Rahmen von E-Government angewendet werden kann
PDF	„Portable Document Format“; Dateiformat der Fa. Adobe, für das kostenlose Leseprogramme zur Verfügung stehen
PIN	„Personal Identification Number“; „Geheimzahl“ zur Authentisierung von Zugriffen auf Systeme
PKI	Public Key Infrastructure; System zur Erzeugung, Verbreitung und Management öffentlicher kryptographischer Schlüssel
RegTP	Regulierungsbehörde für Telekommunikation und Post
RSA	Asymmetrisches kryptographisches Verfahren benannt nach den Erfindern (Rivest, Shamir, Adleman)
SigG	Signaturgesetz
SigV	Signaturverordnung (Ausführungsverordnung zum SigG)
SMTP	„Simple Mail Transport Protocol“; Standard-Protokoll für E-Mails
SSL	Verfahren zur Absicherung der Kommunikation im WWW (Secure Socket Layer)
VwVfG	Verwaltungsverfahrensgesetz
W3C	World Wide Web Consortium; Offene, internationale Organisation zur Erarbeitung von Spezifikationen für das Internet
XML	eXtensible Markup Language; Spezifikation zur strukturierten Beschreibung von Dokumenten und Daten, vom World Wide Web Consortium (W3C) gepflegter, offener "Standard", der sowohl "lesbar" als auch automatisiert auswertbar ist.

Inhalt

Management Summary

Wo ist der Schlüssel zum digitalen Rathaus?.....	1
Keymanagement und Infrastrukturen im kommunalen E-Government.....	1
1 Einleitung.....	11
2 Allgemeine Rahmenbedingungen der Kommunikation.....	13
2.1 Kryptographische Grundlagen.....	14
2.1.1 Verschlüsselungsverfahren.....	14
2.1.2 Signaturverfahren.....	16
2.2 Einsatz von technischen Signierverfahren.....	17
2.2.1 Elektronische Unterschrift.....	18
2.2.2 Authentisierungsverfahren.....	19
2.3 Web-Sicherheit durch SSL.....	19
2.4 Funktionstauglichkeit und Interoperabilität.....	21
2.5 Vertrauen in die Sicherheit.....	22
3 Schlüsselmanagement.....	24
3.1 Einleitung.....	24
3.2 Schlüsseltrennung.....	25
3.3 Zertifikate und Public Key Infrastructures (PKI).....	26
3.4 Möglichkeiten und Grenzen der Identifizierung durch Zertifikate.....	29
4 Infrastrukturen der Kommunikation.....	31
4.1 Kommunikationspartner und Kommunikationskanal.....	34
4.2 Dienste eines Kommunikationsservers.....	36
4.3 Organisatorische Anforderungen.....	41

Anhänge:

A - Umfang und Grenzen der Sicherheit durch SSL

B - Sprechstunde in der virtuellen Amtsstube

C - Vertrauliche und authentische Kommunikation zwischen Bürger und Verwaltung

Management-Summary

1. Kommunikationssicherheit und kryptographische Verfahren

Auch wenn ein Großteil der Verwaltungsdienstleistungen im formfreien Bereich angesiedelt ist und daher auch bei elektronischer Abwicklung nicht unbedingt einer qualifizierten elektronischen Signatur bedarf, ist im Rahmen der Weiterentwicklung von kommunalen Internetangeboten hin zu einem digitalen Rathaus mit interaktiven Dienstangeboten der Gewährleistung einer sicheren, rechtsverbindlichen Kommunikation große Bedeutung bei zu messen. Kryptographischen Technologien, insbesondere Verschlüsselungsverfahren und der elektronischen Signatur, wie sie im Signaturgesetz beschrieben und festgelegt sind¹, kommen hierbei (im doppelten Wortsinne!) eine Schlüsselrolle zu. Durch den Einsatz dieser Verfahren können Schutzziele wie

- Vertraulichkeit
- Integrität
- Authentizität
- Rechtssicherheit
- Datenschutz

sichergestellt werden. Nutzung und der Einsatz dieser Verfahren unterliegen einer Vielzahl von technisch-organisatorischen Fragen, für die jeweils auf verschiedenen Ebenen Lösungen gefunden werden müssen. Dabei kommt es darauf an, zwischen den teilweise konkurrierenden Zielen

- der maximalen Flexibilität, Geschwindigkeit und Transparenz für den Bürger und
- dem Schutz des internen kommunalen Netzes und der intern gespeicherten Informationen

¹ zu Einzelheiten siehe Darstellung im Band "Welche Signaturen braucht die Kommunalverwaltung" des Deutschen Städtetages - Köln, Mai 2002

Seite - 6 -

in angemessener Weise zu vermitteln.

Kryptografische Verfahren mit asymmetrischen Schlüsselpaaren sind die Basistechnologien für Signatur, Verschlüsselung und Authentifizierung. Bei diesen Verfahren kommen jeweils zwei kryptographische Schlüssel zum Einsatz: ein geheimer Schlüssel, der unter ausschließlicher Kontrolle des Inhabers steht und ein öffentlicher Schlüssel, der „jedermann“ zur Verfügung gestellt werden kann. Die Sicherheitsziele werden jeweils durch die „richtige“ Kombination des Einsatzes dieser Schlüssel umgesetzt. Die von einer Zertifizierungsinstanz, dem sog. Trustcenter ausgestellten **Zertifikate** gewährleisten eine (je nach garantiertem Sicherheitsniveau des Anbieters verlässliche) Zuordnung von öffentlichen Schlüsseln zu den Personen, die das private Gegenstück in ihrer Verfügungsgewalt haben.

2. Einsatzfelder von kryptografischen Verfahren

Mit dem „richtigen“ Einsatz kryptografischer Verfahren können bei der Übertragung von Daten zwischen Bürgern und der Verwaltung, wie auch bei der Übertragung zwischen Behörden, die zuvor genannten Anforderungen an die elektronische Kommunikation weitestgehend abgedeckt werden. Durch **Verschlüsselungsverfahren** kann die Vertraulichkeit der Kommunikationsinhalte gewährleistet werden. Die nachträglich feststellbare rechtsverbindliche Urheberschaft für ein Dokument wird dabei ebenso wie die sofortige Feststellung jeglicher nachträglicher Veränderung an einem Dokument (Integritätsschutz) durch den Einsatz der **elektronischen Signatur** erreicht. Des Weiteren kann durch **Authentisierungsverfahren** geprüft werden, dass der Kommunikationspartner auch derjenige ist, der er vorgibt zu sein.

3. Schlüsselmanagement

Sicherheit und Wirksamkeit der Anwendung kryptografischer Verfahren erfordern ein planvolles, den Einsatzanforderungen angemessenes **Schlüsselma-**

Seite - 7 -

nagement, das sowohl auf „lokaler“ (Behörde, Endanwender) als auch auf „globaler“ (externe Dienstleister, übergreifende Infrastrukturen) Ebene umgesetzt werden muss. Hierdurch muss u.a. sichergestellt werden, dass

- die Verwaltungsmitarbeiter im erforderlichen Umfang mit den benötigten Schlüsseln ausgestattet werden,
- private Signatur- und Entschlüsselungsschlüssel vor missbräuchlicher Verwendung geschützt werden und
- die erforderlichen öffentlichen Signaturprüf- und Verschlüsselungsschlüssel (Zertifikate) bei den Kommunikationspartnern vorhanden und hinsichtlich ihrer Echtheit und Gültigkeit prüfbar sind.

Zu den üblicherweise „lokal“ zu erledigenden Aufgaben gehört neben der internen Verteilung von Schlüsselmaterial und Anwendungssoft- und -hardware auch die Auswahl von für die jeweilige Dienstleistung/Kommunikation geeigneten kryptographischen Verfahren und Zertifikatstypen.

Die Erzeugung, Bereitstellung und Pflege von Schlüsseln und Zertifikaten sind die Aufgaben von Trustcentern (Zertifizierungsdiensteanbietern), die in aller Regel in eine übergreifende **Public Key Infrastruktur (PKI)** eingebunden sind. Aufbau und Betrieb von Trustcentern und PKIs gehören üblicherweise schon aus wirtschaftlichen Erwägungen (insbesondere im Umfeld qualifizierter Signaturzertifikate) zu dem nicht von den Kommunen selbst zu betreibenden Schlüsselmanagement.

Bei Auswahl und Einsatz der diversen Verfahren und Zertifikatstypen sollte darauf geachtet werden, dass für die unterschiedlichen Anwendungen (Verschlüsselung, elektronische Unterschrift und Authentisierung) auch jeweils unterschiedliche Schlüssel verwendet werden. Außerdem müssen die Anforderungen der Fachverfahren an die Feststellbarkeit der Identität eines Verwaltungskunden mit den durch die jeweiligen Zertifikate gelieferten Informationen abgeglichen werden.

4. Infrastrukturen

Der Aufbau einer Infrastruktur zur Nutzung der kryptografischen Verfahren wird im wesentlichen von zwei unterschiedlichen Faktoren bestimmt:

- von den Kommunikationspartnern und
- vom gewählten Kommunikationskanal (unstrukturiert per Mail oder strukturiert durch Formulare)

Auf Seiten der Verwaltung ist die Frage, wer Empfänger der Nachricht ist, für die daraus abzuleitenden Maßnahmen und Konsequenzen von erheblicher Bedeutung. Außerdem ist zu beachten, dass die Verwaltung in der Regel nur für sich selbst, meist aber nicht für den Kunden verbindliche Regelungen und Vorgaben durchsetzen kann.

Wird eine **Ende-zu-Ende Kommunikation** zwischen Bürger und Sachbearbeiter angestrebt, so sind an jedem Arbeitsplatz die Voraussetzungen zur Entschlüsselung und Signaturprüfung von elektronischen Nachrichten einzurichten, was zum einen erhebliche finanzielle Auswirkungen hat, zum anderen weitreichende organisatorische Maßnahmen etwa bei der Schlüsselverwaltung erfordert. Als Alternative *oder Ergänzung* kommt eine **Ende-zu-Server Kommunikation** im Sinne einer **virtuellen Poststelle** in Betracht. Auf einem zentral betriebenen Kommunikationsserver können dann u.a. folgende Dienste angeboten werden:

- Entschlüsselung
- Signaturprüfung
- Signaturerstellung (bei entsprechenden technisch-organisatorischen Randbedingungen)
- Durchführung von Authentisierungsverfahren
- Prüfung auf Schadinhalte etc.
- Einholung oder Erstellung von Zeitstempeln

Seite - 9 -

Diese Vorgehensweise bietet für die Kommunen, insbesondere bei der Schlüsselverwaltung, eine Reihe von Vorteilen und entspricht im übrigen auch dem Wunsch vieler Kunden der Verwaltung, unabhängig von Zuständigkeiten eine konkrete Dienstleistung zu erhalten oder abzuliefern.

Mit der Einrichtung einer solchen virtuellen Poststelle müssen daneben Regelungen für verschiedene Fragestellungen im Zusammenhang mit Empfang, Weiterbearbeitung und Beantwortung von elektronischen Kommunikationseingängen, oftmals in Ergänzung bzw. Erweiterung von bereits vorhandenen Dienstanweisungen, gefunden werden. Auf technischer Ebene müssen Entscheidungen über einzuhaltende Standards, wie z.B. OSCI und ISIS-MTT, getroffen werden.

Eine sinnvolle Kombination von Ende-zu-Ende- und Ende-zu-Server-Kommunikation, die den Anforderungen der jeweiligen Kommunikationstypen und Dienstleistungen gerecht wird, sollte wesentlicher Bestandteil einer behördenweiten **Kommunikationsstrategie** sein. Diese sollte auch eine „Informatikpolitik“ der Behörde festschreiben, die unter anderem sicherstellt, dass den Kunden an geeigneter Stelle mitgeteilt wird, welche kryptographischen Verfahren und Zertifikatstypen sie aktuell akzeptieren kann.

Ein Hinweis auf die Signaturverfahren, die von der jeweiligen Kommune technologisch verarbeitet werden können, sollte im Web-Angebot ebenfalls nicht fehlen und wird in der Neufassung des Verwaltungsverfahrensgesetzes in § 3a sogar verbindlich festgelegt².

5. Förderung der Akzeptanz

Bei der Verbreitung von elektronischen Signaturen spielen eine Reihe von akzeptanzfördernden Maßnahmen wie z.B. Schaffung von Standards/Interoperabilität, Preisgestaltung, Anwenderfreundlichkeit usw. eine ent-

² Einzelheiten zur Frage der Zugangseröffnung werden in einem weiteren Arbeitspapier des AK DigRa behandelt

Seite - 10 -

scheidende Rolle. Diese Faktoren können von der Kommunalverwaltung jedoch nur in geringem Maße beeinflusst werden. Bei der Bereitstellung von Anwendungen, die zu einer breiten Marktdurchdringung führen könnten, ist hingegen der Mut der Kommunen gefordert, sich dieses Themenkomplexes anzunehmen. Insbesondere die letzten Ergebnisse der MEDIA@Komm-Städte³ und die daraus abgeleiteten Modelle und Standardisierungsversuche dürften hier als Wegbereiter angesehen werden und warten nur auf weitere Kommunen, die die weitere Entwicklung nachhaltig mit unterstützen.

³ s. www.mediakomm.net

1 Einleitung

Der Einsatz von Signatur- und Verschlüsselungsverfahren, Chipkarten und auch die Möglichkeit des elektronischen Bezahls werden zu einer Weiterentwicklung und zu einer weiteren Verbreitung von Online-Dienstleistungen der Kommunen führen. Sicher scheint, dass nicht mehr die Frage im Vordergrund steht, ob die Verwaltungen überhaupt elektronische Dienstleistungen anbieten, sondern welche das im einzelnen sein werden und wie diese intern abgewickelt werden können. Zur Zeit sind viele Kommunen dabei, praktische Erfahrungen bei der Planung und Umsetzung von virtuellen Rathäusern zu sammeln und diskutieren dabei auch verschiedene Aspekte des Technikeinsatzes und der Organisation.⁴

Dabei erfordert die Bereitstellung anspruchsvoller Dienstleistungen von (Kommunal-) Verwaltungen innerhalb eines "digitalen Rathauses" (E-Government-Dienstleistungen) zwingend, dass die Vertraulichkeit und Verbindlichkeit der Kommunikation zu einem gewissen – von der Art der zu erbringenden Dienstleistung abhängigen – Grad mit kryptographischen Mechanismen abgesichert wird. Das hier vorliegende Papier beschäftigt sich mit dem Teilaspekt der Nutzung von Public-Key-Infrastrukturen, also der praktischen Frage, welche technischen und administrativen Vorbereitungen und Maßnahmen auf Seiten der Kommunen ergriffen werden müssen, um sichere elektronische Kommunikation zwischen Bürgern (G2C) und Wirtschaft (G2B) auf der einen und der Verwaltung auf der anderen Seite sowie die Kommunikation zwischen den Verwaltungen (G2G) zu ermöglichen. Zielgruppe des Papiers sind in erster Linie die Fachverantwortlichen für die Umsetzung von digitalen Rathäusern. In den Anhängen A - C werden darüber hinaus für interessierte Fachleute technische Einzelheiten weiter vertieft beschrieben.

Welche Einsatzfelder für Schlüsselzertifikate auf Seiten des Bürgers, der Rechner und der Verwaltung prinzipiell bedacht werden sollten, hat der Deutsche Städtetag in

⁴ Eine Übersicht über Projekte ist sowohl unter www.Mediakomm.net als auch unter www.difu.de erreichbar.

Seite - 12 -

seiner Broschüre "Schritte auf dem Weg ins digitale Rathaus" (DST-Beiträge zur Informationsgesellschaft und Stadtforschung Reihe H, Heft 45) aufgezeigt.

Die Frage, welche kryptographischen Schlüssel in welcher Weise im digitalen Rathaus benötigt werden, ist wesentlich davon abhängig, welche Art der Kommunikation zwischen Bürger und Verwaltung genutzt werden soll und wie diese im Detail technisch realisiert wird.

Grundsätzlich sind verschiedene Arten der elektronischen Kommunikation zwischen Bürger und Behörde denkbar und praktikabel. Dabei ist u.a. stets abzuwägen zwischen den (mindestens teilweise) konkurrierenden Zielen *maximaler Flexibilität, Geschwindigkeit und Transparenz für den Bürger* einerseits und einem adäquaten Schutz der internen Netze der Verwaltung mitsamt den dort gespeicherten, vielfach auch personenbezogenen Daten andererseits. Je nachdem, welchen Schutzbedarf man im Einzelfall ausmachen wird und wie groß die Möglichkeit der Automatisierung einer bestimmten Dienstleistung und damit der Wunsch nach möglichst automatischer Übernahme der Daten in Workflowsysteme ist, wird man sich für jeweils verschiedene Kommunikationsplattformen und Sicherungsszenarien entscheiden.

Nicht betrachtet werden in der vorliegenden Ausarbeitung Fragen der Weiterbehandlung der Daten in den Hintergrundsystemen der Behörde (Workflowsysteme, Dokumentenmanagementsysteme, Archivierung) sowie der Schutz der Daten innerhalb der Verwaltungsnetze. Diese Fragen werden in späteren Versionen oder anderen Papieren des AK DigRa behandelt. Ebenso nicht betrachtet werden Fragen der Sicherheit des eingesetzten Online-Zahlungssystems. Eine ausführlichere Darstellung von Zahlungssystemen wird an anderer Stelle vorgenommen⁵.

⁵ Als weiterführende Lektüre kann in diesem Zusammenhang auch der Band 10 der BSI-Schriftenreihe zur IT-Sicherheit "Sicherheitsaspekte bei Electronic Commerce", der über den Bundesanzeiger Verlag beziehbar ist, empfohlen werden

2 Allgemeine Rahmenbedingungen der Kommunikation

Zum besseren Verständnis der Detailfragen ist es erforderlich, bestimmte allgemeine Rahmenbedingungen der elektronischen Kommunikation abzustecken.

Unabhängig von technischen Lösungen hat die elektronische Kommunikation den folgenden allgemeinen Sicherheitszielen zu entsprechen:

- **Vertraulichkeit**

Es muss sichergestellt werden, dass die zu übermittelnden Inhalte auch nur durch den "richtigen" Empfänger in Empfang genommen und gelesen werden.

- **Integrität**

Der Empfänger der Nachricht muss erkennen, dass die Nachricht während des Transports inhaltlich nicht verändert worden ist.

- **Authentizität**

Der Urheber bzw. die Quelle einer elektronischen Nachricht muss für den Empfänger mit hinreichender Sicherheit erkennbar sein.

Mit der Einhaltung dieser grundlegenden Sicherheitsziele können weitere Ziele in der Kommunikation zwischen Bürger und Behörde gewährleistet werden. Dazu gehören insbesondere:

- **Rechtssicherheit**

Der Empfänger der Daten muss darauf vertrauen können, dass der Inhalt der Nachricht auch der Willenserklärung des Absenders entspricht und damit Rechtsfolgen bewirkt werden. Dies setzt Integrität und Authentizität der Nachricht voraus.

- **Datenschutz**

Der Absender der Informationen hat ein Recht darauf, dass die erhobenen Daten nur für den Zweck verwendet werden, der Grundlage für die Erhebung der Daten war. Dies setzt Vertraulichkeit der Daten bei der Übertragung voraus.

Seite - 14 -

Die besondere Herausforderung bei der Realisierung der elektronischen Kommunikation liegt darin, dass die genannten Sicherheitsziele nicht isoliert betrachtet werden können, sondern immer in Summe und von Anfang an in einem Lösungsansatz enthalten sein müssen.

2.1 Kryptographische Grundlagen

Kryptographische Techniken kommen sowohl beim Schutz von Vertraulichkeit und Integrität der Kommunikationsinhalte, bei der Herstellung bzw. Gewährleistung der Rechtssicherheit bezüglich der abgegebenen Erklärungen als auch für Zwecke der Authentisierung und Identifizierung der Kommunikationspartner zum Einsatz. Die Funktionsweise dieser Verfahren soll hier *kurz* dargestellt werden.⁶

2.1.1 Verschlüsselungsverfahren⁷

Allgemein betrachtet bestehen Kryptoverfahren aus zwei Komponenten. Ein spezielles, **Kryptoalgorithmus** genanntes Programm verwandelt den Klartext in ein unlesbares "Chiffre" und wandelt dieses beim Empfänger wieder in den Klartext zurück. Entscheidend ist dabei, dass beide Operationen nur dann vorgenommen werden können, wenn der Absender bzw. der Empfänger über einen weiteren Datensatz, den sog. **(kryptographischen) Schlüssel** verfügt. Bei (guten) Kryptoverfahren hängt die Sicherheit der Kommunikation ausschließlich von der Güte und Geheimhaltung dieser Schlüssel ab.

Symmetrische Verschlüsselung

⁶ Für eine ausführliche Beschreibung sei auf den Band "*Schritte auf dem Weg zum digitalen Rathaus*" des Deutschen Städtetags verwiesen, der die entsprechenden Verfahren insbesondere auch im Hinblick auf ihre Verwendung im kommunalen Umfeld hin untersucht.

⁷ Weitere Einzelheiten können Teil B, Kapitel 1 der Broschüre "*Schritte auf dem Weg ins digitale Rathaus*" entnommen werden

Seite - 15 -

Die klassische Methode der Kryptographie ist die **symmetrische**. Hierbei verwenden Absender und Empfänger den gleichen – von beiden geheimzuhaltenden – Schlüssel, der sowohl zum Ver- als auch zum Entschlüsseln eingesetzt wird. Moderne symmetrische Verschlüsselungsverfahren ermöglichen eine beliebig hohe Sicherheit und erlauben es, auch längere Texte in sehr kurzer Zeit zu ver- und entschlüsseln. Problematisch bei symmetrischen Verfahren ist die Tatsache, dass zunächst ein geheimer Schlüssel zwischen Absender und Empfänger – und nur zwischen diesen (!) – ausgetauscht werden muss. Voraussetzung für die vertrauliche Kommunikation ist also eine vertrauliche Kommunikation! Wegen dieser Problematik werden rein symmetrische Verfahren heute überwiegend dann eingesetzt, wenn keine Kommunikation vorausgesetzt wird (z.B. Festplattenverschlüsselung) oder wenn verschlüsselte Dateien in kleinen Benutzergruppen ausgetauscht werden.

Asymmetrische Verschlüsselung

Aus dem Dilemma der sensiblen Verteilung geheimer Schlüssel kann man sich mit Hilfe der **asymmetrischen** Kryptografie befreien. Hier erzeugt der *Empfänger* ein Schlüsselpaar. Einen dieser Schlüssel ("*privater Schlüssel*") behält er für sich, den anderen ("*öffentlicher Schlüssel*") gibt er **öffentlich** bekannt. Es gibt hier also kein gemeinsames Geheimnis zwischen Absender und Empfänger. Voraussetzung für eine sichere Anwendung der asymmetrischen Kryptographie ist, dass die Entschlüsselung **nur** mit dem privaten Schlüssel möglich ist und dass dieser beim Empfänger absolut geheimgehalten wird. Die Berechnung des privaten Schlüssels aus dem öffentlichen muss *praktisch unmöglich*, d.h. in "überschaubaren" Zeiträumen mit "realistischem Rechenaufwand" nicht durchführbar sein. Gelänge einem Angreifer eine solche Berechnung könnte er jede asymmetrisch verschlüsselte Nachricht mitlesen. Es ist diese "Einwegigkeit" der asymmetrischen Kryptographie, die dazu geführt hat, dass erst mit der Einführung "leistungsfähiger" elektronischer Rechner – also etwa seit Mitte der 70er Jahre – brauchbare Verfahren existieren. Beim Verfahren RSA-1024 beispielsweise, das derzeit als von den meisten Experten als hinreichend sicher angesehen wird, verwendet man ca. 150-stellige(!) Primzahlen als

Seite - 16 -

Schlüssel. Die Länge der bei asymmetrischen Verfahren benötigten Schlüssel führt dazu, dass diese Verfahren nur einen geringen Datendurchsatz aufweisen.

Eine rein asymmetrische Verschlüsselung längerer Texte ist daher nicht praxistauglich.

Hybride Verschlüsselung

Die Vorteile symmetrischer und asymmetrischer Kryptoverfahren werden in sogenannten **hybriden Verfahren** kombiniert. Es wird dabei ein *Sitzungsschlüssel* *S* erzeugt, der zur symmetrischen (=schnellen) Verschlüsselung der eigentlichen Kommunikation verwendet und durch ein asymmetrisches Verfahren abgesichert übermittelt wird. Zum Schlüsselaustausch wird der Sitzungsschlüssel (= relativ kleine Datenmenge) mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt. Auf diese Weise erhält nur der Empfänger Kenntnis von diesem Schlüssel.

Hybride Verfahren werden heutzutage in praktisch allen gängigen Systemen zur Absicherung von E-Mail- oder Web-Verbindungen eingesetzt.

Sofern die Kommune ihren Kunden ermöglichen möchte, ihr eine verschlüsselte Nachricht zukommen zu lassen, muss sie vorab ein entsprechendes Zertifikat zur Verfügung stellen. Dies kann z.B. durch eine Veröffentlichung auf der Webseite geschehen.

2.1.2 Signaturverfahren

Grundidee der digitalen Signatur ist eine *Umkehrung* der asymmetrischen Verschlüsselung. Der Absender "verschlüsselt" das elektronische Dokument mit seinem *privaten* Schlüssel; der Empfänger "entschlüsselt" mit dem *öffentlichen* Schlüssel des Absenders. Nur der Besitzer des privaten Schlüssels kann somit den Inhalt eines Dokuments gestaltet haben; Integrität und Authentizität (sofern dieser Besitzer zwei-

Seite - 17 -

felsfrei ermittelt werden kann) sind damit gewährleistet. Wegen des geringen Datendurchsatzes (sicherer) asymmetrischer Algorithmen ist diese einfache Vorgehensweise aber nicht praktikabel.

Die existierenden Signaturprodukte umgehen diese Schwierigkeit, indem der zu signierende Text zunächst durch einen sog. **Hash-Algorithmus** extrem komprimiert wird. Eine – speziell für Signaturanwendungen – wesentliche Eigenschaft von Hash-Algorithmen ist die sog. **Kollisionsfreiheit**, die besagt, dass es *nicht* möglich sein darf, zwei unterschiedliche und jeweils *sinnvolle* Texte mit dem gleichen Hashwert zu finden. Ein kollisionsfreier Hash-Algorithmus erzeugt eine "kleine" Datei, die den "großen" Ausgangstext in der gleichen Weise repräsentiert, wie ein "kleiner" Fingerabdruck einen "großen" Menschen erkennbar macht. Hashwerte von elektronischen Texten werden daher auch als *digitaler Fingerabdruck* bezeichnet.

Bei der *Signaturerstellung* wird zunächst der Hashwert des zu signierenden Textes gebildet und dieser "Fingerabdruck" (= relativ kleine Datenmenge) dann mit dem privaten Schlüssel des Absenders "verschlüsselt", wobei die für jeden Text und jeden privaten Signaturschlüssel einzigartige **Signatur** entsteht. Anschließend werden *sowohl der Ausgangstext als auch die Signatur* an den Empfänger übersendet. Dieser unterzieht nun den Ausgangstext ebenfalls dem – allgemein bekannten – Hash-Algorithmus und "entschlüsselt" anschließend die Signatur mit dem öffentlichen Schlüssel des Absenders. Die eigentliche *Signaturprüfung* besteht nun im Vergleich der beiden so erhaltenen Hashwerte. Stimmen diese überein, so sind Integrität und Authentizität – wie eingangs erläutert - gewährleistet.⁸

2.2 Einsatz von technischen Signierverfahren

Verfahren zur Erstellung digitaler Signaturen können je nach Einsatzkontext zu verschiedenen Zwecken genutzt werden. Diese werden im Folgenden dargestellt.

⁸ An dieser Stelle ist die Kollisionsfreiheit des Hash-Algorithmus entscheidend, da ansonsten die Möglichkeit bestünde, bei der Signaturprüfung unbemerkt einen "kollidierenden" Text unterzuschieben und so die Willenserklärung des Absenders zu verfälschen.

2.2.1 Elektronische Unterschrift

Zweck der elektronischen Unterschrift ist es, verbindlich die Urheberschaft für ein elektronisches Dokument zu übernehmen. Dies kann sinnvollerweise nur dann geschehen, wenn die **Integrität des Dokuments** durch die Technologie mit sichergestellt wird. Sie erfüllt für elektronische Erklärungen damit den gleichen Zweck wie die eigenhändige Unterschrift unter ein Papierdokument. Die Tatsache, dass durch Anwendung der Signaturtechnik Integrität und Authentizität des Dokuments hinreichend sichergestellt werden, ist die Voraussetzung dafür, dass eine solche Erklärung verantwortlich abgegeben werden kann und dass diese in einem eventuellen Rechtsstreit auch tatsächlich Beweiskraft erlangen kann. Das Signaturgesetz (SigG) und die zugehörige Rechtsverordnung (SigV)⁹ beschreiben im Rahmen der EU-Richtlinie über elektronische Signaturen technisch-organisatorische Rahmenbedingungen für **qualifizierte Signaturen**¹⁰, die diesem hohen Anspruch genügen können. Im Bereich des Privatrechts ist eine weitestgehende Gleichstellung von qualifizierter Signatur und eigenhändiger Unterschrift bereits verwirklicht; im öffentlichen Recht wird ein solcher Rahmen zum Zeitpunkt der Erstellung dieses Textes noch festgelegt.

Die Anbringung einer elektronischen Unterschrift setzt ihrer Funktion nach einen *Willensakt* voraus, der grundsätzlich nur nach vorheriger Kenntnisnahme und Überprüfung des Inhalts durch den Unterzeichnenden vorgenommen werden sollte. Dies schließt jedoch nicht aus, dass in einer geeignet abgesicherten Umgebung und unter Einhaltung bestimmter Rahmenbedingungen auch automatisierte elektronische Unterschriften unter "Massensendungen" (man denke etwa an Steuerbescheide o.ä.) erstellt werden können. Hierbei ist zu beachten, dass die Anbringung einer Signatur aus Gründen des Integritäts- und Authentizitätsschutzes selbst dann sinnvoll ist, wenn keine Formvorschriften zu erfüllen sind.

⁹ Text bzw. download unter www.iid.de/iukdg/gesetz/index.html

¹⁰ Vgl. Broschüre Deutscher Städtetag "Welche elektronische Signatur braucht die Verwaltung?" Mai 2002

2.2.2 Authentisierungsverfahren

Bei der elektronischen Kommunikation zwischen Bürger und Verwaltung werden nicht in jedem Fall rechtsverbindliche Erklärungen mit hohem Beweiswert ausgetauscht werden müssen. In bestimmten Fällen kann es aber dennoch notwendig sein, sich (vorab oder im nachhinein) mit hinreichender Sicherheit von der Identität des Kommunikationspartners zu überzeugen. Als Beispiel sei etwa der Zugriff auf bestimmte Informationen, die nur einem bestimmten Personenkreis zur Verfügung stehen dürfen (etwa Ratsinformationssysteme, Bürgerakten,...) oder die zielgerichtete Versendung eines (verschlüsselten) Dokuments an eine bestimmte Person genannt. Auch zu diesem Zweck können (unter anderem) asymmetrische Schlüssel eingesetzt werden. Bei sog. **Challenge-Response-Verfahren** übermittelt dazu ein Kommunikationspartner ("Anna") – vollständig auf Rechner Ebene automatisiert - dem anderen ("Bert") eine zufällige "Nachricht" ("Challenge"), die dieser vorab nicht kennt – etwa eine Zufallszahl. Bert "signiert" diese mit seinem privaten Schlüssel und sendet diese "Signatur" an Anna zurück (Response). Wenn es Anna gelingt, mit Berts öffentlichem Prüfschlüssel ihre Challenge zu rekonstruieren, so kann sie sicher sein, dass sie tatsächlich mit Bert kommuniziert. Der sich authentisierende Kommunikationspartner (hier "Bert") muss dazu seinen privaten Authentisierungsschlüssel bewusst freigeben (durch Eingabe einer PIN), hingegen ist es unnötig und auch nicht zweckmäßig, dass Anna und Bert den genauen Inhalt der Challenge überhaupt zur Kenntnis nehmen. Aufgrund der Tatsache, dass im Vergleich zu "echten" Texten nur sehr kurze Challenges verwendet werden, ist in aller Regel auch der Einsatz einer Hash-Funktion entbehrlich. Die unterschiedlichen Anwendungen des *gleichen* kryptografischen Verfahrens unterscheiden sich also *technisch-organisatorisch* erheblich voneinander.

2.3 Web-Sicherheit durch SSL

Die derzeit wohl am meisten genutzte Implementierung der asymmetrischen Kryptographie zur Absicherung ist die SSL-Technologie. Aufgrund ihrer Verbreitung und –

Seite - 20 -

wahrscheinlich – noch zunehmenden Bedeutung soll sie hier gesondert beschrieben werden. SSL ist die Abkürzung für **Secure Socket Layer**. Dabei sind mit Layer die Transportschichten angesprochen, mit denen der Datenaustausch zwischen Rechnern dargestellt wird. Bei Nutzung der SSL-Technologie sind keine Änderungen in den Applikationen und in den Transportprotokollen erforderlich. SSL schafft durch folgende Mechanismen eine gesicherte Verbindung:

- Der Inhalt der Web-Seiten geht nur verschlüsselt über das Netz
- der Server authentisiert sich zertifikatsgestützt gegenüber dem Nutzer (benötigt: Serverzertifikat)
- der Nutzer authentisiert sich zertifikatsgestützt gegenüber dem Server (benötigt: Clientzertifikat)
- kryptographische Algorithmen prüfen, ob die Daten authentisch und unverändert den Empfänger erreichen.

Zur tatsächlichen Nutzung der Mechanismen ist anzumerken, dass in der gegenwärtigen Praxis fast ausschließlich die Server-Authentisierung genutzt wird. Die mögliche Authentisierung der Clients (Nutzer) scheitert fast immer an der extrem geringen Verbreitung und Nutzung der benötigten Client-Zertifikate.

Der Browser-Aufruf **https://...** (statt **http://...**) initiiert eine SSL-Verbindung. Hierdurch erkennt der Browser, dass vom Ziel-Server ein Zertifikat und der öffentliche Schlüssel anzufordern ist. Beide Elemente werden - hier greift der kryptographische Algorithmus - mit Prüfsumme und einem besonderen Identifizierungsmerkmal an den Browser zurückgemeldet. Dieser kann anhand des Zertifikats die Identität eines Servers überprüfen. Er kann mit einem asymmetrischen Verschlüsselungsverfahren auf einem sicheren Weg einen nur für diese Sitzung gültigen Schlüssel an den Server senden. Dieser ausgetauschte Schlüssel gilt für die restliche Dauer der Verbindung. Die Verschlüsselung der Sitzung erfolgt dann mit einem symmetrischen Verfahren unter Verwendung der ausgetauschten Chiffre-Schlüssel (hybrides Verschlüsselungsverfahren; s.o.).

Seite - 21 -

Zur *Authentisierung* der Teilnehmer (d.h. in der Praxis meist nur der Server) werden Zertifikate verschiedener Anbieter¹¹ eingesetzt. In den gängigen Browsern, wie Netscape Navigator und Internet Explorer, sind die Zertifikate der wichtigsten Zertifizierungsfirmen bereits enthalten. Wenn ein Browser ein ihm unbekanntes Zertifikat von einem Webserver erhält, kann er mit Hilfe der vorinstallierten Trust-Center-Zertifikate prüfen, ob es offiziell unterschrieben und damit gültig ist, oder nicht. Der Aufbau der SSL-Verbindung und der Austausch aller dafür notwendigen Daten erfolgt dabei vollkommen selbständig und automatisch. Ein solches offizielles Zertifikat ist aber nicht zwingend erforderlich. Wenn der Unterzeichner eines gesendeten Zertifikats nicht feststellbar ist, muss der Empfänger eigenständig über die Glaubwürdigkeit des Zertifikates entscheiden. Diese Entscheidungslage wird dabei in mehreren Dialogschritten vom Nutzer erfragt. Nach erfolgter Datenprüfung des Browsers (Verbindungsweg angegebener Server / angewählte URL) wird dem Nutzer eine entsprechende Information (in der Regel ein geschlossenes Bügelschloss) angezeigt.

Über die beschriebenen Mechanismen kann SSL zur Verbesserung der Vertraulichkeit und Verbindlichkeit von web-basierter Kommunikation beitragen. Dabei ist jedoch zu beachten, dass die SSL-Technologie – wie jede Sicherheitstechnologie – ihre spezifischen Möglichkeiten **und Grenzen** besitzt. Die Grenzen der SSL-Technologie werden wesentlich durch Mängel im Zertifikatsmanagement und in der Benutzerregistrierung bestimmt. Näheres hierzu wird im Anhang unter „Umfang und Grenzen der Sicherheit durch SSL“ dargelegt. Bei der Entscheidung über die Nutzung von SSL sollten diese Möglichkeiten und Grenzen mit den applikationsspezifischen Anforderungen abgeglichen werden.

2.4 Funktionstauglichkeit und Interoperabilität

Die für den Einsatz von Signaturen zu installierende Software war nach bisherigen Anwendererfahrungen oft fehlerhaft bzw. komplett funktionsuntüchtig und für Laien nur unter erschwerten Bedingungen zu installieren. Berichte über komplette und un-

¹¹ Es sei darauf hingewiesen, dass sich hierbei durchgängig **nicht** um Zertifizierungsdiensteanbieter im Sinne des Signaturgesetzes handelt.

Seite - 22 -

widerrufliche Systemabstürze beim Installationsversuch sind leider keine Ausnahmen gewesen. Solche für den Nutzer ärgerliche "Kinderkrankheiten" stehen einer verbreiteten Nutzung jedenfalls erheblich im Weg.

Um zumindest das Problem der fehlenden Interoperabilität von digitalen Signaturen verschiedener Anbieter zu überwinden, sind inzwischen erste konkrete Schritte unternommen worden. Im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi) haben der TeleTrusT e.V. und die Trustcenter-Vereinigung T7 eine Spezifikation (ISIS-MTT) zur Anwendung elektronischer Signaturen erarbeitet.¹²

2.5 Vertrauen in die Sicherheit

Die Frage von Vertrauen bestimmt ganz wesentlich die Akzeptanz. Vertrauen bezieht sich dabei nicht alleine auf den Bereich des Datenschutzes, also die Vermutung oder vertraglich festgelegte Regelungen, wie mit den Daten des Kunden umgegangen wird. Vertrauen bezieht sich auch darauf, dass der Anbieter von Geschäftsbeziehungen in den Augen des Kunden im Umgang mit Signaturen als vertrauenswürdig gilt. Und last but not least gilt, dass das Vertrauen in das Verfahren der Signatur als solcher vorhanden sein muss.

Das häufig fehlende Vertrauen der Bürger in die Datensicherheit ist ein erheblicher Hemmnisfaktor bei Onlinetransaktionen. Dieses Hemmnis könnte durch den Einsatz von elektronischen Signatur- und Verschlüsselungstechniken beseitigt werden. Die Sicherheit der Chipkarte (nach SigG) selbst, also der Schutz vor einer missbräuchlichen Verwendung der Karte, die den Schlüssel des Anwenders enthält, scheint gewährleistet zu sein, weil die darauf gespeicherten Schlüssel nicht ausgelesen werden können und die Karte mit einer PIN geschützt ist. Darüber hinaus werden verschiedene biometrische Verfahren erprobt, um die Karte einer Person zuordnen zu können, also eine zweifelsfreie Identifikation des Inhabers zu gewährleisten. Solche Karten sind mit Foto- oder Fingerabdruck versehen, um persönliche und nicht fälschbare Merkmale einer Person festzustellen, bevor ein Zugang zu oder die Benutzung von geschützten Systemen gewährt wird. Solche persönlichen Merkmale sind z.B. Gesicht, Bewegung der Mundpartie sowie ein Stimmuster und sollen – wenn die derzeit

Seite - 23 -

noch bestehenden gravierenden Sicherheitsmängel ausgeräumt werden können - die eindeutige Identifikation ermöglichen¹³.

¹² zum aktuellen Stand der Entwicklung von ISIS-MTT: www.t7-isis.de (nur in englischer Sprache)

¹³ zum aktuellen Diskussionsstand zum Thema "Biometrie" siehe z.B. www.teletrust.de (AG 6) und www.biotrust.de

3 Schlüsselmanagement

3.1 Einleitung

Durch die asymmetrische Kryptographie stehen heute Verfahren zur Verfügung, die es ermöglichen, auch in offenen Nutzergruppen und über unsichere Netze wie das Internet vertraulich und (rechts-) verbindlich zu kommunizieren. Ihr Einsatz dürfte gerade im (kommunalen) E-Government von herausragender Bedeutung sein. Die durch die Nutzung dieser Verfahren angestrebten Sicherheitsziele lassen sich aber nur dann verlässlich erreichen, wenn die Erzeugung, Nutzung und Verwaltung – also das **Management** – der entsprechenden kryptographischen Schlüssel den Anforderungen der Kommunikations- und Anwendungsszenarien gerecht wird. Hierzu sind eine Reihe von technischen und organisatorischen Maßnahmen sowohl auf Seiten der Anbieter als auch auf Seiten der Anwender erforderlich, von denen einige in der Praxis besonders zu beachtende in diesem Kapitel dargestellt werden sollen.

Beim Management kryptographischer Schlüsselpaare ist zunächst zwischen privaten und öffentlichen Schlüsseln zu unterscheiden. Während erstere im wesentlichen „lediglich“ geheim zu halten sind¹⁴, was durch entsprechende technische („abgeschottete“ Chipkarte) oder auch organisatorische Maßnahmen beim Besitzer des Schlüssels zu gewährleisten ist, ist die verlässliche und effiziente Verteilung von öffentlichen Schlüsseln ein Problem, das sowohl „lokal“ – also im Verantwortungsbereich des Endanwenders bzw. seiner Dienststelle – als auch „global“ gelöst werden muss.

Die Lösung der „globalen“ Schlüsselmanagementaufgaben in Eigenregie dürfte für einzelne Kommunen in aller Regel wirtschaftlich nicht sinnvoll sein; insbesondere zeigen die bisherigen Erfahrungen, dass die flächendeckende Ausstattung von Bürgern mit kryptographischen Schlüsseln keine sinnvolle und wirtschaftlich leistbare Aufgabe für Kommunen ist. Hier ist die Nutzung externer Anbieter und Dienstleister unabdingbar. Dennoch stellen sich für die kommunalen Verantwortlichen zahlreiche

¹⁴ Auf das Problem des geordneten (Fremd-) Zugriffs auf private Entschlüsselungsschlüssel im Vertretungsfall wird im Kapitel 4.2 noch einzugehen sein.

Seite - 25 -

Fragestellungen im Zusammenhang mit dem Schlüsselmanagement, insbesondere was die Verteilung und Nutzung von Schlüsseln innerhalb der Behörden und die Auswahl eines geeigneten Anbieters von entsprechenden Produkten und Dienstleistungen betrifft. Hierzu sollen in diesem Kapitel Informationen und Entscheidungshilfen bereitgestellt werden.

3.2 Schlüsseltrennung

Viele kryptographische Verfahren – so etwa das weit verbreitete RSA – eignen sich sowohl für Verschlüsselungs- als auch für Signaturanwendungen. Es müssen dazu lediglich die Rollen von öffentlichem und privatem Schlüssel vertauscht werden. Diese Eigenschaft scheint es nahe zu legen, *ein* Schlüsselpaar für alle drei kryptographischen Funktionen (Verschlüsselung, Signatur, Authentisierung) gemeinsam zu nutzen. Eine solche "universelle" Schlüsselnutzung sollte jedoch auf alle Fälle vermieden werden. Sinnvoll ist es vielmehr, für jede kryptographische Funktion ein eigenes Schlüsselpaar zu verwenden. Neben subtilen *sicherheitstechnischen* Erwägungen, deren Erörterung hier zu weit führen würde, sprechen vor allem *organisatorische* Gründe für eine solche **Schlüsseltrennung**.

Bei der **Trennung von Verschlüsselungs- und Signaturschlüsseln** steht vor allem die Frage nach Gruppenschlüsseln und Vertretungsregelungen im Vordergrund. Während es beim Verschlüsseln durchaus sinnvoll sein kann, einer Gruppe von Personen (etwa einer Organisationseinheit der Verwaltung) ein gemeinsames Schlüsselpaar zuzuordnen oder durch Schlüsselhinterlegung das Entschlüsseln dienstlicher Texte auch bei Abwesenheit des "Inhabers" (etwa in Folge plötzlicher Erkrankung) zu ermöglichen, sollten sich private Signaturschlüssel unter *ausschließlicher Kontrolle* des Schlüsselinhabers befinden. Jede Möglichkeit, dass ein solcher Schlüssel bekannt würde, entwertet die (gerichts feste) Zurechenbarkeit einer elektronischen Erklärung oder die Verlässlichkeit einer persönlichen Authentisierung.

Eine **Trennung von "Unterschrift"- und Authentisierungsschlüssel** sollte ebenfalls erfolgen. Bei Authentisierungsverfahren werden wie erwähnt zumeist Zufallszah-

Seite - 26 -

len "signiert". Ein Anwender hat dabei keine Möglichkeit, sich davon zu überzeugen, dass eine zugesandte "Challenge" nicht etwa der Hash-Wert eines ihm unbekanntes Textes ist. Bei Verwendung des "Unterschrift"-Schlüssels – insbesondere, wenn es sich dabei um einen Schlüssel nach den Anforderungen des Signaturgesetzes handelt – würde dann ohne Wissen des Anwenders eine rechtsgültige Signatur dieses Textes erstellt. Die Verwendung eines dezidierten Authentisierungsschlüssels verhindert diesen Missbrauch.

Es sei an dieser Stelle ausdrücklich darauf hingewiesen, dass eine mögliche Mehrfachnutzung von kryptographischen Schlüsseln durch die *Kunden* der Kommunalverwaltung durch die Verwaltung in der Regel nicht wirksam nachgewiesen oder gar verhindert werden kann. Da das Risiko einer solchen Mehrfachnutzung aber in aller Regel der Anwender selbst trägt, dürften hierdurch für die Behörden in der Praxis kaum Probleme entstehen. Hingegen sollte bereits bei der Konzeption des Einsatzes kryptographischer Komponenten in den Kommunalbehörden aus den genannten Gründen darauf geachtet werden, dass die ausgewählten Produkte eine konsequente Schlüsseltrennung unterstützen oder sogar erzwingen.

3.3 Zertifikate und Public Key Infrastructures (PKI)

Bei der Überprüfung von Signaturen wird ein öffentlicher Schlüssel eingesetzt. Genau betrachtet haben wir also ein "unterschiedenes" elektronisches Dokument dem Benutzer des zugehörigen privaten Schlüssels zugeordnet oder diesen im Rahmen einer Challenge-Response-Authentisierung als Kommunikationspartner erkannt.¹⁵ Dies wird aber in so abstrakter Form den fachlichen Anforderungen normalerweise nicht genügen. Es kommt in aller Regel vielmehr darauf an, den Unterzeichner oder Kommunikationspartner als Person oder wenigstens als Institution (mehr oder weniger) eindeutig zu identifizieren. Hierzu dienen im Rahmen der asymmetrischen Kryptographie Zertifikate.¹⁶

¹⁵ Analoges gilt bei der Nutzung eines öffentlichen Verschlüsselungsschlüssels.

¹⁶ Es sei an dieser Stelle ausdrücklich erwähnt, dass in der Praxis abhängig vom Schutzbedarf der Kommunikation und von der technischen Ausstattung auch nicht-kryptographische Authentisierungsverfahren (etwa das aus dem Bereich des Online-Banking bekannte PIN/TAN-Verfahren) zum Einsatz kommen können

Seite - 27 -

Eine grundsätzliche Angriffsmöglichkeit bei asymmetrischen Verfahren besteht darin, dass sich ein Fälscher ("Fritz") ein eigenes Schlüsselpaar erzeugen und versuchen kann, gegenüber "Anna" seinen öffentlichen Schlüssel als denjenigen von "Bert" auszugeben. Gelingt dieser Angriff bei einem Schlüsselpaar zur Verschlüsselung, kann anstelle von "Bert" nur noch "Fritz" die für "Bert" bestimmte vertrauliche Information lesen. Bei Signaturschlüsseln könnte "Fritz" auf "Berts" Namen verbindliche Erklärungen abgeben oder in einer Kommunikation die Identität von "Bert" vortäuschen. Die Bindung eines (öffentlichen) Schlüssels an eine Person muss also von einer vertrauenswürdigen Stelle (**Trustcenter, Zertifizierungsstelle, Certificate Authority, CA**) in einem sog. **Zertifikat** so dokumentiert werden, dass sie nachprüfbar und authentisch, d.h. nicht unbemerkt fälschbar, ist. Zu diesem Zweck werden sie meist vom Trustcenter mit einer Signatur versehen. Bei der Zertifikatsprüfung ergibt sich nun die Notwendigkeit, den zugehörigen öffentlichen Schlüssel der CA authentisch und integer zu erhalten. Mit anderen Worten: Die CA benötigt ebenfalls ein Zertifikat! Dieses kann sie zum Beispiel nach dem oben beschriebenen Schema von einer übergeordneten CA erhalten, die wiederum ein Zertifikat benötigt. Ein Verfahren, das sich prinzipiell über beliebig viele Stufen erstrecken kann. Die so entstandene *Zertifikatshierarchie* muss an irgend einer Stelle beendet werden. Die an dieser Stelle angesiedelte CA, die **Root-CA**, die die „Wurzel“ des Vertrauens in alle darunter erzeugten Zertifikate repräsentiert und von allen Teilnehmern als vertrauenswürdig anerkannt wird, signiert ihr Zertifikat selbst.¹⁷

Das Zertifikat sollte weiterhin mindestens eine Angabe über die beabsichtigte *Schlüsselnutzung* enthalten (s. Abschnitt "Schlüssel trennung" in Kapitel 3.2) und einen maximalen Gültigkeitszeitraum definieren. Als weitere Angaben können – insbesondere bei Signaturzertifikaten – Hinweise über berufliche Eigenschaften (etwa "Mitarbeiter der Stadt X", "Landrat des Kreises Y", "Geschäftsführer der Z GmbH",...) oder eine (monetäre) Nutzungsbeschränkung enthalten sein. Eine ausführliche Diskussion der

¹⁷ Zur Verbesserung der nachträglichen Überprüfbarkeit der Zertifikate kann der öffentliche Schlüssel der Root-CA zusätzlich in einem externen, „unfälschbaren“ Medium – etwa in Form einer Papier-Publikation – veröffentlicht werden; „externer Vertrauensanker“.

Seite - 28 -

Einsatzmöglichkeiten solcher "Attribute" findet sich im bereits angesprochenen Band *"Schritte auf dem Weg zum digitalen Rathaus"* des Deutschen Städtetags.

Beim Einsatz von kryptographischen Verfahren können die vom Empfänger benötigten Zertifikate entweder vorab übersandt bzw. (im Falle der Signatur) mit der Nachricht mitgeschickt werden, oder, insbesondere wenn höhere Sicherheitsansprüche bestehen, von einem vertrauenswürdigen **Verzeichnisdienst** bezogen werden. In jedem Fall sollte es möglich sein, über den Verzeichnisdienst zu erfragen, ob ein bestimmtes Zertifikat nicht etwa in der Zwischenzeit von seinem Benutzer gesperrt wurde. Bei qualifizierten Signaturen nach Signaturgesetz ist die Möglichkeit einer solchen "Online-Abfrage" eine Pflichtdienstleistung der Zertifizierungsdiensteanbieter.

*Ein „globales“, also den Verantwortungsbereich eines Einzelnutzers überschreitendes technisch-organisatorisches System für Erzeugung, Verbreitung und das Management öffentlicher Schlüssel (bzw. Zertifikate) wird als **Public Key Infrastructure (PKI)** bezeichnet.* Sichere Aufbewahrungs- und Nutzungskomponenten für private Schlüssel (sog. „personal security environment“; PSE) sowie Verzeichnis- und Sperrdienste sind charakteristische Komponenten eines solchen Systems.

Eine spezielle PKI ist gesetzlich im Signaturgesetz (SigG) für akkreditierte Zertifizierungsdiensteanbieter beschrieben. Hier fungiert die Regulierungsbehörde für Telekommunikation und Post (RegTP) als Root-CA für die akkreditierten TrustCenter, die wiederum Zertifikate an Endanwender ausgeben. Selbst für große kommunale Gebietskörperschaften dürfte es aus finanziellen Gründen heraus nicht sinnvoll sein, eine signaturgesetzeskonforme PKI selbst aufzubauen. Hingegen könnte der Aufbau nicht SigG-konformer PKIs etwa für Zwecke der (internen) Verschlüsselung und Authentisierung sehr wohl in bestimmten Fällen für Kommunen sinnvoll sein. Da sich das Signaturgesetz darüber hinaus nur mit Fragen der Signatur (im Sinne der „elektronischen Unterschrift“) befasst, müssen Anbieter von Verschlüsselungs- und Authentisierungsdienstleistungen zwangsläufig PKIs außerhalb des Signaturgesetzes aufbauen. Im kommunalen Einsatz müssen also sowohl bei eigenen Ausschreibun-

gen als auch bei der Beurteilung der Eignung „fremder“ Strukturen Fragen der Qualität und Ausgestaltung von PKIs berücksichtigt werden.

3.4 Möglichkeiten und Grenzen der Identifizierung durch Zertifikate

Durch Einsatz von Zertifikaten können Verschlüsselungsschlüssel oder Signaturen auf die im Zertifikat genannte "Person" zugeordnet werden. Die Verlässlichkeit dieser Zuordnung hängt dabei im wesentlichen von der Qualität der eingesetzten technischen Komponenten, der Sorgfalt des Benutzers und der Güte und Zuverlässigkeit der zertifikatausgebenden Stelle ab. Im Bereich der qualifizierten elektronischen Signatur werden durch Signaturgesetz und Verordnung hier verbindliche Mindeststandards vorgeschrieben.

Für die "Brauchbarkeit" eines Zertifikats ist jedoch neben den genannten technisch-organisatorischen Rahmenbedingungen auch der *Zertifikatsinhalt* von großer Bedeutung. So führt z.B. ein Zertifikat, das auf ein Pseudonym ausgestellt ist, nicht dazu, das man den Besitzer des zugehörigen privaten Schlüssel ohne weiteres - d.h. mittels des Zertifikats selbst - identifizieren kann.

Zertifikate von *qualifizierten Signaturen* nach SigG enthalten möglicherweise nur die gesetzlich vorgeschriebenen Mindestinhalte¹⁸. Dabei handelt es sich lediglich um den Namen des Zertifikatinhabers,¹⁹ der nur im Falle einer Verwechslungsmöglichkeit - innerhalb des Verzeichnisdienstes dieses Anbieters!- mit einem Zusatz versehen wird (also etwa "Hans Müller1", "Hans Müller 2",...). Weitere Inhalte werden nur auf Wunsch und in der Regel auf Kosten (!) des Zertifikatsinhabers hinzugefügt. Dieses reicht im Allgemeinen für eine eindeutige Identifizierung nicht aus.

Bei Verschlüsselungszertifikaten gibt es überhaupt keine verbindlichen Regeln, welche Inhalte das Zertifikat enthalten soll und ob diese überhaupt zutreffend sind. Allein auf Grund eines Verschlüsselungszertifikats ist es nicht unbedingt möglich zu ent-

¹⁸ Vergl. §7 SigG. Diese Pflichtinhalte sind bereits in der EU-Richtlinie über elektronische Signaturen verbindlich und abschließend festgelegt.

¹⁹ Oder sogar nur ein als solches gekennzeichnetes Pseudonym.

Seite - 30 -

scheiden, ob z.B. ein Auszug aus dem Seuchenregister nun für den Internisten Dr. Fritz Schulz oder für den Philologen Dr. Fritz Schulz verschlüsselt wird. Um solche Verwechslungsmöglichkeiten auszuschließen und ein Verschlüsselungszertifikat eindeutig einer Person zuordnen zu können, sind weitere technisch-organisatorische Maßnahmen durch die Kommune unabdingbar.

In konkreten Kommunikationssituationen müssen die Kommunikationspartner also aufgrund ihrer Sicherheitsanforderungen und der gesetzlichen Rahmenbedingungen entscheiden, welche Identifizierungsgüte sie als Voraussetzung für die elektronische Kommunikation verlangen. Ergänzend zu den Mindestinhalten eines Zertifikats nach SigG kann dabei etwa ein Attributzertifikat mit Meldedaten eingesetzt werden. Denkbar ist auch eine vorherige (oder gleichzeitige) Registrierung, sei es durch einmaliges persönliches Erscheinen oder durch die Abgabe einer rechtsverbindlich signierten Erklärung mit ergänzenden Angaben zur Person, wie dies ja in den meisten Formularen durch Ausfüllen der entsprechenden Felder ohnehin geschieht. Dabei sollte beachtet werden, dass praktisch alle Möglichkeiten zur weitergehenden Identifizierung zusätzlichen Aufwand des Kommunikationspartners und evtl. datenschutzrechtliche Schwierigkeiten im Verfahren zur Folge haben. Die Festlegung eines wirklich angemessenen Niveaus ist hier von besonderer Bedeutung. Dabei sollte auch beachtet werden, dass beim Einsatz qualifizierter Signaturen eine *nachträgliche* eindeutige Identifikation des Zertifikatsinhabers im Falle des Missbrauchsverdachts über die Dokumentation des Zertifizierungsdiensteanbieters möglich ist. Bleiben also die durch fälschliche Authentisierung potentiell entstehenden Schäden gering oder ist eine nachträgliche Haftung des Verursachers ausreichend, so wird man in vielen Fällen auf weitergehende Mechanismen zur Identifizierung des Zertifikatsinhabers verzichten können²⁰.

²⁰ Eine vollständige systematische Übersicht möglicher Lösungsansätze steht derzeit noch aus.

4 Infrastrukturen der Kommunikation

Der Zugang zur Verwaltung war in der Vergangenheit auf drei klassische Kommunikationsformen

- persönliche Vorsprache
- Sprachkommunikation - Telefon
- Schriftform

sowie die dabei aufgetretenen Derivate und Verzweigungen beschränkt. Die verbindliche Reaktion der Kommunalverwaltung erfolgte dabei in der überwiegenden Zahl der Fälle aus Gründen der Rechtssicherheit und Verbindlichkeit in Schriftform. Die Regeln im Umgang mit diesen Technologien sind seit vielen Jahren fester Bestandteil der Verwaltungspraxis und haben ihren Niederschlag in den entsprechenden Dienstvereinbarungen und –anweisungen gefunden.

Mit der schnellen Verbreitung des Internets haben sich die Kommunikationsmöglichkeiten und damit der Zugang zu den Dienstleistungen der Kommunalverwaltung noch um die Variante des digitalen Zuganges verändert.

Dabei werden zwei grundsätzlich unterschiedliche Zugangswege durch die Verwaltung angeboten, die technologisch über das gleiche Transportmedium bereitgestellt werden. In der Betrachtung werden daher zwei technische Kommunikationskanäle nämlich **E-Mail** und **web-basierte Kommunikation**, für die sich im folgenden durchaus unterschiedliche Einsatzmöglichkeiten und Sicherungsmechanismen ergeben werden, unterschieden.

In Abhängigkeit von den gewählten Kommunikationskanälen sind unterschiedliche Anforderungen an eine kommunale Verwaltungs-PKI zu stellen. Die Art der Datenübermittlung wiederum bietet der Verwaltung mehrere Möglichkeiten, die übermittelten Informationen in ihren internen Geschäftsprozess einzubinden.

Seite - 32 -

Typische Domäne der **E-Mail-Kommunikation vom Bürger zur Behörde** ist die formfreie, unstrukturierte Anfrage nach bestimmten Dienstleistungen, insbesondere Informationsabfragen. Aufgrund der Tatsache, dass die Behörde für diese Form der Kommunikation nur ein Mindestmaß an technischer Infrastruktur bereithalten muss, ist die E-Mail-Kommunikation häufig das erste Angebot, das in der "Frühphase" eines E-Government-Projekts zur Verfügung gestellt wird. Dafür kommt der Mail-Standard SMTP (simple mail transport protocol) zum Einsatz.

Bei der Bereitstellung von anspruchsvollen Dienstleistungen, die einen entsprechenden Bearbeitungsaufwand im Hintergrund erfordern, erweist sich die E-Mail-Kommunikation aber zunehmend als nachteilig, weil die Daten die Behörde (bei einfacher Mail-Kommunikation) in unstrukturierter Form erreichen und der die E-Mail empfangende Sachbearbeiter quasi als "Nadelöhr" der Kommunikation fungiert, denn er prüft die Eingaben und sendet die Daten manuell ins Hintergrundsystem der Verwaltung. Das eigentliche Hausnetz bleibt vollständig vom Internet getrennt. Die hohe Sicherheit für die internen Systeme wird hier dadurch erkauft, dass bezogen auf die Kommunikation keine nennenswerte Vereinfachung der Geschäftsprozesse erzielt wird und fehlerträchtige Medienbrüche in Kauf genommen werden.

Eine strukturierte **Kommunikation vom Bürger zur Verwaltung** erreicht man durch die Gestaltung von **Web-Formularen**, welche die Datenübergabe in strukturierter Form (Feld für Feld) ermöglichen. Eine Integration in Hintergrundsysteme wird durch diese (meist datenbankgestützte) Technik wesentlich erleichtert. Dabei wird es in der Regel erforderlich sein, dem Bürger (Online-) Hilfestellungen beim Ausfüllen des Formulars anzubieten. Sinnvoll sind Prüfroutinen mit möglichst interaktiver Benutzerführung zur Fehlerkorrektur. Im Vergleich zur E-Mail-Kommunikation bietet die Web-basierte Bereitstellung von Online-Formularen über das in allen gängigen Browsern bereits vorinstallierte SSL-System²¹ zusätzliche, benutzerfreundliche Möglichkeiten zur Absicherung von Vertraulichkeit, Integrität und (in gewissen Grenzen) auch Authentizität der Kommunikation.

²¹ Einzelheiten können dem **Anhang A** "Umfang und Grenzen der Sicherheit durch SLL" entnommen werden

Seite - 33 -

Für den Bereich der strukturierten Kommunikation ist im Rahmen des Projektes MEDIA@Komm das Kommunikationsprotokoll OSCI (Online Services Computer Interface) entwickelt worden. OSCI ist eine XML-Anwendung, und berücksichtigt weitgehend W3C-konforme Standards wie XML-encryption and XML-signature. OSCI sieht die notwendigen Ausprägungen dieser Standards für die rechtsverbindliche Kommunikation mit der Verwaltung vor, insbesondere die Konformität zum Signaturgesetz. OSCI berücksichtigt das besondere Rollenmodell der öffentlichen Verwaltung (viele Empfänger, Gewährleistung von Datenschutz) durch den Einsatz eines Intermediärs. Dieser Intermediär übernimmt weitgehend diejenigen Funktionen, die im Folgenden in den Ausführungen zur virtuellen Poststelle aufgelistet werden. OSCI ist also ein Kommunikationsprotokoll für web-basierte Online-Transaktionen. Darüber hinaus sieht OSCI die Standardisierung von semantischen Datenstrukturen vor, wie z.B. die Beschreibung des Meldedatensatzes in der Teilprotokollmenge XMeld. Ähnliche Initiativen gibt es in den Bereichen Bau (Xbau) und Justiz (Xjustiz)²².

Die **Kommunikation von der Behörde zum Bürger** kann je nach vorhandener Ausstattung ebenfalls sowohl per E-Mail als auch web-basiert erfolgen. Bei web-basierter Kontaktaufnahme des Bürgers und einem automatisierten Hintergrundprozess, der in "Echtzeit" antworten kann, ist sicher die vollständige Leistungserbringung das Ziel. Ist eine abschließende Erbringung der Dienstleistung ausgeschlossen - was stets dann der Fall sein wird, wenn manuelle Eingriffe in das Verfahren notwendig sind oder sogar ein Ermessenspielraum bei den zugrundeliegenden Entscheidungen besteht - kann je nach Ausstattung und Art der Dienstleistung sowohl der E-Mail- als auch der Web-Kanal (in gewissen Fällen sogar der Postweg) bei der Antwort sinnvoll sein. Diese Fälle werden im Weiteren näher diskutiert.

Zusammenfassend kann an dieser Stelle die Feststellung getroffen werden, dass bei der Einrichtung der PKI zwei Punkte von besonderer Bedeutung sind, welche die Struktur der PKI bestimmen. Dies sind

²².weitere Informationen unter www.osci.de

Seite - 34 -

- die Kommunikationspartner
- der Kommunikationskanal

Im weiteren Verlauf der Ausführungen soll näher auf diese beiden Hauptpunkte eingegangen werden.

4.1 Kommunikationspartner und Kommunikationskanal

Bei den Kommunikationspartnern unterscheiden wir zwei grundsätzliche Arten

- die Ende-zu-Ende-Kommunikation
- die Ende-zu-Server-Kommunikation

Bei der **ersten Variante** der Kommunikation wird zwischen Bürger(in) und Verwaltungsmitarbeiter(in) ein Kontakt hergestellt, im zweiten Falle erfolgt die eigentliche Kommunikation zwischen Bürger(in) und einem Rechner.

Bei jeder Kommunikationsart kann dann der Kommunikationskanal

- unstrukturierter Mail-Verkehr
- formularbasierter Datenaustausch

zur Anwendung kommen. Unter Berücksichtigung der sicherheitsspezifischen Anforderungen, sind in den vorgenannten Kontext zwei Hauptfelder zu berücksichtigen. Dies sind

- die Verschlüsselung
- die Signatur

Beim Einsatz von elektronischer Signatur und Verschlüsselung wird stets summarisch davon gesprochen, dass "der Empfänger" Nachrichten entschlüsselt oder Sig-

Seite - 35 -

naturen prüft. Während auf Bürgerseite klar sein dürfte, dass dieser Empfänger der Bürger persönlich ist, ist die Frage, wer auf Seiten der Verwaltung als "Empfänger" einer Bürgernachricht fungiert, mit großen technischen und organisatorischen Konsequenzen behaftet. Die Verwaltung muss hierbei frühzeitig entscheiden, welche der beiden gegensätzlichen Ansätze für welche Anwendungsfälle zum Einsatz kommen soll.

Ende-zu-Ende-Kommunikation zwischen Bürger und Sachbearbeiter

Bei diesem Szenario wird der Behördenmitarbeiter mit einem individuellen personenbezogenen Entschlüsselungsschlüssel ausgestattet. Verschlüsselte Nachrichten des Bürgers werden von diesem unmittelbar an den zuständigen Sachbearbeiter gesendet, der sie auf seinem Arbeitsplatz-PC entschlüsselt und weiterverarbeitet. Diese Form der Kommunikation bietet ein Höchstmaß an Vertraulichkeit bis zu den Endpunkt der Kommunikation. Sie ist die etablierte Form der persönlichen E-Mail-Kommunikation im Internet (soweit hier überhaupt Verschlüsselung verwendet wird). Der dabei gegebene Personenbezug hat aber zur Folge, dass Vorkehrungen notwendig werden, um eine Nachricht auch dann zu entschlüsseln, wenn der Sachbearbeiter - aus welchen Gründen auch immer - nicht selbst verfügbar ist. Denkbar ist hier beispielsweise die Hinterlegung des privaten Schlüssels bei einer vertrauenswürdigen Stelle in der Verwaltung²³.

Ende-zu-Server-Kommunikation ("virtuelle Poststelle")

Hier richtet der Bürger seine (verschlüsselte) Nachricht an eine zentrale Eingangsstelle auf einem Kommunikationsserver in der virtuellen Amtstube. Dabei ist denkbar, dass entweder ein Server als zentrale "Posteingangsstelle" der Behörde fungiert oder mehrere fachbezogene Poststellen parallel zur Verfügung zu stellen.

Die Nachricht wird im Server entschlüsselt und - sofern erforderlich - eine Signaturprüfung vorgenommen und das Ergebnis sicher archiviert. Die entschlüsselte Nachricht steht dem für dieses "Postfach" zuständigen Sachbearbeiter (dieser wird ggf.

²³ Alle denkbaren Maßnahmen haben aber in jedem Fall ein Aufbrechen der strengen Ende-zu-Ende Sicherheit zur Folge.

Seite - 36 -

über eine Datenbank automatisch ermittelt) zur weiteren Bearbeitung zur Verfügung. Der Abruf kann in aller Regel innerhalb des gesicherten Hausnetzes der Behörde unverschlüsselt erfolgen (auch heute werden Anträge etc. in aller Regel ohne besondere Absicherung innerhalb der Behörde im Postumlauf weitergeleitet). In den (wenigen) Fällen, wo dies nicht hinnehmbar erscheint, kann eine weitere hausinterne Verschlüsselung der Kommunikation zwischen Server und Bearbeiter-PC erfolgen.

4.2 Dienste eines Kommunikationsservers

Eine typische "**virtuelle Poststelle**" benötigt aber auch Schnittstellen zu operativen Verfahren im Hausnetz der Verwaltung (ggf. auch zu Workflowmanagement- und Archivierungssystemen etc.). Diese Schnittstellendienste könnten auf einem Kommunikationsserver implementiert werden und *beispielsweise* folgende Funktionen abdecken:

Eingehende Nachrichten:

- Die Nachricht wird gemäß einem der von der Verwaltung zum Zweck der Verschlüsselung zur Verfügung gestellten Zertifikate entschlüsselt.
- Die automatische Überprüfung des verwendeten Signaturzertifikats durch eine online-Abfrage beim Zertifikatsaussteller.
- Durchführung von Authentisierungsverfahren (sofern realisiert und erforderlich) beispielsweise für Bürgerabfragen zum Status eines Verwaltungsvorgangs.
- Die Prüfung der Nachricht auf Schadinhalte (nach Entschlüsselung).
- Die Registrierung des Vorgangs und Dokumentation mit Zeitstempel.
- Die Bestätigung des Eingangs gegenüber dem Absender.
- Die Generierung und Versendung von Benachrichtigungen bei fehlerhaften Eingängen (z.B.: Nachricht nicht zu entschlüsseln).
- Die Weiterleitung der Nachricht an ein operatives Verfahren oder einen Sachbearbeiter (ggf. unter Verwendung verwaltungsinterner Verschlüsselungszertifikate).

Ausgehende Nachrichten:

- Die mit dem verwaltungsinternen Nachrichtensystem verschlüsselten Nachrichten entschlüsseln (Gatewayfunktion).
- Die Nachricht an den Bürger verschlüsseln (sofern gewünscht/erforderlich und möglich). Das Verschlüsselungszertifikat des Bürgers könnte dazu mit oder ohne ein vorausgegangenes Authentifizierungsverfahren bei seiner Antragstellung gespeichert werden. Mit angemessener und fallbezogener Authentisierung könnten dann auch Anfragen zum Stand eines Verfahrens automatisiert beantwortet werden.
- Eine vollautomatische Signierung aller Nachrichten bzw. Dokumente ist nicht unproblematisch. Einerseits ist es erforderlich, elektronische Texte zu signieren oder mit einem Zeitstempel zu versehen, wenn man ihre Fälschung verhindern will. Andererseits verbindet man mit einer Unterschrift stets auch eine gewisse Verantwortung für den Inhalt des Dokuments. Eine automatisierte Erstellung gerade

Seite - 38 -

qualifizierter Signaturen erfordert in jedem Fall die Einhaltung bestimmter technisch-organisatorischer Rahmenbedingungen wie zum Beispiel die Einrichtung eines besonderen Zugriffsschutzes für die Signaturkarte oder die Freischaltung für eine begrenzte Anzahl von Signaturen.

- Je nach Anforderung des Verfahrens kann entweder ein verwaltungsinterner oder ein qualifizierter Zeitstempel der Nachricht beigefügt werden.
- Die erzeugten Nachrichten auf Schadinhalte zu prüfen und dies dem Empfänger gegenüber bestätigen, könnte ein zusätzlicher Service sein.
- Die Registrierung des Vorgangs ggf. mit Schnittstelle zu einem Dokumentenmanagement-System.

Nicht jedes Verwaltungsverfahren und erst recht nicht jeder Nachrichtenverkehr erfordert alle vorgenannten Dienste. Vorteilhaft für die Umsetzung von Prozessabläufen wäre es allerdings, wenn man sich je nach Bedarf derer Module bedienen könnte, die für den umzusetzenden Bürgerservice notwendig oder hilfreich sind.

Ein Bürger wendet sich in aller Regel nicht deshalb an die Verwaltung, um einen persönlichen Kontakt mit einem bestimmten Sachbearbeiter zu pflegen, sondern um eine konkrete Dienstleistung *der Verwaltung* zu erhalten. Diesem Gedanken folgend bietet sich für den Einsatz im E-Government ein Kommunikationsserver in einer "virtuellen Poststelle" in besonderer Weise an. Sie ist sowohl für die Verwaltung als auch für den Bürger mit einer Reihe von Vorteilen verbunden. Es sei schon an dieser Stelle darauf hingewiesen, dass bei Einsatz einer (SSL-abgesicherten) Web-Verbindung der Web-Server der Behörde quasi automatisch die Rolle einer (ggf. rudimentären) virtuellen Poststelle einnimmt. Ein Ende-zu-Ende-Szenario ist hier quasi von vorneherein ausgeschlossen.

Der Einsatz einer Ende-zu-Server-Kommunikation darf andererseits die Ende-zu-Ende-Kommunikation nicht unmöglich machen. Sie ist in Einzelfällen durchaus erforderlich, sowohl für standardisierte Arbeitsabläufe als auch für die individuelle Kommunikation Einzelner.

Seite - 39 -

Nachstehend sollen die Vorteile einer solchen Kommunikationsserver-Strategie herausgestellt werden:

- **Einfacheres Schlüsselmanagement (intern)**

Die Anzahl der innerhalb der Verwaltung auszugebenden und zu administrierenden Entschlüsselungsschlüssel wird minimiert. Schlüsselwechsel etwa aufgrund von unbrauchbar gewordenen Chipkarten oder nicht mehr geeigneter Schlüssellängen lassen sich wesentlich einfacher durchführen.

- **Einfacheres Schlüsselmanagement (extern)**

Dem Bürger müssen nur einer oder wenige öffentliche Verschlüsselungsschlüssel für die Server bekannt gegeben und aktualisiert werden, nicht jedoch die Schlüssel für alle Mitarbeiter der Behörde. Es würde sich anbieten, die wenigen öffentlichen Schlüssel auf der Web-Site zum Down-Load anzubieten.

- **Geringerer Kostenaufwand**

Die Kosten einer nahezu umfassenden Ausstattung der Beschäftigten mit Chipkarten und Lesegeräten, sowie die Ausbildungskosten können minimiert werden. Mindestens wird eine gleitende Entwicklung ermöglicht, die sich organisatorisch und finanziell steuern lässt.

- **Reduzierter Administrations- und Bedienungsaufwand**

Die technisch oft nicht unkomplizierten Programme zur Entschlüsselung und Signaturprüfung müssen nicht auf jedem einzelnen Mitarbeiter-PC installiert und gepflegt werden, sondern nur auf wenigen Serversystemen. Die in bestimmten Fällen durchaus nicht einfache Entscheidung darüber, ob etwa eine bestimmte Signatur wirklich gültig ist, kann automatisiert werden und muss nicht vom Sachbearbeiter getroffen werden. Umfangreiche "Massenschulungen" werden vermieden, das Risiko durch Bedienungsfehler von ungeübtem Personal minimiert.

- **Unkomplizierte Umsetzung von Vertretungsregelungen**

Bei planmäßigem oder ungeplanten "Ausfall" von einzelnen Mitarbeitern oder bei Umbesetzungen innerhalb der Verwaltung ist es lediglich erforderlich, die entsprechenden Datenbankeinträge anzupassen um eine automatische Weiterleitung auf den Arbeitsplatz des jetzt (vertretungsweise) zuständigen Bearbeiters zu veranlassen. Dem hingegen müssen bei Ende-zu-Ende-Kommunikation aufwendige Maßnahmen zur Schlüssel hinterlegung bzw. Schlüsselrekonstruktion umgesetzt werden, die obendrein immer zunächst ein potentiell Sicherheitsrisiko mit sich bringen.

- **Möglichkeit zur Prüfung auf Schadinhalte**

Die in Firewallsystemen integrierten Mechanismen zur Prüfung eingehender Dateien (und damit auch Mails) auf Viren, Trojanische Pferde und andere möglicherweise schädliche Software werden bei Verwendung einer Ende-zu-Ende-Verschlüsselung außer Kraft gesetzt, da sich verschlüsselte Inhalte natürlich nicht entsprechend überprüfen lassen.

- **Entlastung der Mitarbeiter/innen**

Auch dem einzelnen Beschäftigten wird ein Kommunikationsserver eine Menge Zeitersparnis bringen. Er muss auch nicht besonders in der Handhabung dieser für ihn in der Regel fachfremden Thematik geschult werden.

- **Bürgerfreundlichkeit:**

Dem Bürger kann durch das Angebot der Kommunikation mit zentralen Posteingangsstellen nicht nur die Suche nach dem passenden öffentlichen Schlüssel sondern im selben Zug auch die Suche nach der zuständigen Stelle abgenommen werden, was ja für etliche ein Ärgernis ist.

4.3 Organisatorische Anforderungen

Die elektronische Kommunikation zwischen Verwaltung und Bürger kann auf verschiedenen Wegen erfolgen. Eine unstrukturierte, freie Kommunikation per E-Mail ist sicher bürgerfreundlich, stellt aber auch hohe Anforderungen an die technische Infrastruktur und setzt eine Reihe konkreter organisatorischer Vereinbarungen voraus. Die strukturierte Kommunikation mittels Web-basierender Formulare dürfte daher für viele Verwaltungen ein erstrebenswertes Ziel sein. Für welche Variante man sich auch entscheidet, für die Binnenorganisation der Verwaltung müssen eine Reihe von Faktoren berücksichtigt werden.

Information über sichere elektronische Kommunikationswege

Werden Onlinedienstleistungen für Bürger angeboten, empfiehlt es sich, den Bürgern auch Hinweise darauf zu geben, welche technischen Voraussetzungen dazu notwendig sind und unter welchen Bedingungen (z.B. Akzeptanz welcher Signaturverfahren) elektronische Transaktionen stattfinden können. Dazu sollten die Städte ihren Bürgern zunächst an zentraler Stelle auf der Homepage mitteilen, für welche Dienstleistungen welche Online-Möglichkeiten zur Verfügung stehen (z.B. Download von Formularen oder Informationen oder Einreichen signierter Anträge oder elektronische Bezahlungsmöglichkeiten). Zum anderen sollten die Voraussetzungen für Online-Abwicklungen detailliert beschrieben werden, d.h. es müssen unbedingt Hinweise vorhanden sein, welche Dienstleistungen welche Signatur des Bürgers erfordern (z.B. fortgeschrittene, qualifizierte) und welche Signaturverfahren von der Stadt verifiziert werden können. Ebenso sind die Verschlüsselungszertifikate der Kommune zur Verfügung zu stellen. Bisher gibt es noch keine einheitlichen Vorgehensweisen, wie Städte diese Hinweise am besten gestalten und wo sie sinnvollerweise zu platzieren wären²⁴.

²⁴ Diese Fragestellung wird ausführlich in einer Ausarbeitung des AK Dig Ra zum Thema "Zugangseröffnung" dargestellt

Seite - 42 -

Beispielhaft sei hier das Vorgehen in den MEDIA@Komm-Städten genannt. In Bremen gibt es für alle Online-Services eine eigene Internetadresse²⁵, die von den Bremer Bürgern angesteuert werden muss, wenn sie mit der Stadt elektronische Geschäfte abwickeln wollen. Auf dieser Seite werden die Nutzer darüber informiert, ob die hinterlegten Formulare signiert zurückgeschickt werden können oder ob sie ausgedruckt und per Post gestellt werden müssen. Geplant ist in Bremen eine Erweiterung der Informationen z.B. dahin gehend, dass auch das notwendige Signaturniveau angezeigt wird und Informationen über die elektronischen Bezahlungsmöglichkeiten angegeben werden. In Nürnberg arbeitet man derzeit an einer problemorientierten Benutzeroberfläche, auf der mehrere elektronische Dienstleistungen zusammengefasst werden sollen. Über diese sollen dann im einzelnen Auskünfte über das verlangte Signaturniveau und die von der Verwaltung akzeptierten Signaturkarten sowie weitere notwendige Informationen und Hilfetexte gegeben werden.

Onlineservices mit Signatur

Viele Städte bieten ihren Bürgern Onlineservices in unterschiedlichen Formen an. Die Angebote reichen dabei wie beschrieben vom Herunterladen von Formularen (z.B. im pdf-Format), die man sich ausdrucken und ausgefüllt an die Verwaltung zurückschicken kann, bis hin zu elektronisch signierten Anträgen. Die Frage, welche Dienstleistungen der Verwaltung mit einfachen E-Mails abgewickelt werden können und wann qualifizierte oder akkreditierte Signaturen zum Einsatz kommen, lässt sich nicht pauschal beantworten. Laut Verwaltungsverfahrenrecht besteht grundsätzlich Formfreiheit des Verwaltungsverfahrens, d.h. man kann in vielen Fällen Anträge an die Verwaltung auch telefonisch stellen. Bei einer ganzen Reihe von Verwaltungsverfahren ist jedoch aufgrund der Bestimmungen in Fachgesetzen die Schriftform zwingend vorgeschrieben. Um auch diese Verwaltungsverfahren den Anforderungen an die elektronische Abwicklung anzupassen, wurde das Verwaltungsverfahrensgesetz des Bundes in enger Abstimmung mit den Ländern überarbeitet. Entsprechend § 3a VwVfG wird durch eine Generalklausel die gesetzlich angeordnete Schriftform grundsätzlich - d.h. soweit in den Fachgesetzen nichts anderes bestimmt ist - der mit

²⁵ www.bremer-online-service.de

Seite - 43 -

einer qualifizierten elektronischen Signatur im Sinne des neuen § 2 Nr. 3 SigG verbundenen elektronischen Form gleichgestellt. Die Unsicherheiten hinsichtlich der Zulässigkeit elektronischen Handelns im schriftformgebundenen Verwaltungsverfahren werden dadurch in absehbarer Zeit beseitigt sein, zumal die Länder eine entsprechende Anpassung ihrer Verwaltungsverfahrensgesetze anstreben. Solange in den Fachgesetzen nicht ausdrücklich etwas anderes bestimmt ist, darf die elektronische Form (d.h. ein mit einer qualifizierten elektronischen Singnatur versehenes Dokument) also immer auch dann verwandt werden, wenn das Gesetz Schriftlichkeit anordnet.

Verantwortlichkeit für die Organisation des Gesamtprozesses

Bisher ist in deutschen Städten die Zuständigkeit für Onlineservices unterschiedlich geregelt. Das Ergebnis einer Umfrage des Deutschen Instituts für Urbanistik aus dem Jahr 2001 zeigt, daß es eine breite Streuung von möglichen Verantwortungsbereichen gibt, die von der Pressestelle, den Zentralen Diensten, der EDV-Stabstellen bis hin zum Hauptamt reicht. Eine zusätzlich durchgeführte, nicht repräsentative E-Mail-Umfrage unter den Städten, die im Januar 2002 über den Listserver des AK DigRa zu erreichen waren (zur Zeit 22 Teilnehmer), hat dieses Ergebnis nochmals bestätigt. Sehr häufig laufen die Fäden im Hauptamt zusammen, verantwortlich für die Koordination der Inhalte sind meist die Ämter für Presse- und Öffentlichkeitsarbeit und für die technische Umsetzung entweder die städtischen IuK-Abteilungen oder die kommunalen Rechenzentren. Eigene Projektgruppen oder Stabsstellen mit Verantwortung für Onlineservices gibt es in Karlsruhe, Köln, Berlin, Hagen, Stuttgart und München. In Bremen gibt es ein Referat "E-Government und Neue Medien" in der Abteilung Personal- und Verwaltungsmanagement.

Eine zentrale Stelle zur Koordination aller kommunalen E-Governmentaktivitäten (ob nun Stabsstelle oder Projektgruppe genannt) läßt sich zur Zeit also vor allem in größeren Städten beobachten. Die im Zuge der Verwaltungsreform eingeführte dezentrale Leistungs- und Budgetverantwortung hat hier offenbar ihre Grenzen erreicht; eine Tendenz zur Rezentralisierung ist deutlich erkennbar. Die zentrale Koordination

Seite - 44 -

erscheint vor allem wichtig, um die eine gemeinsame Strategie für Onlineservices der Kommune zu entwickeln, die dann gemeinsam mit den betroffenen Dienststellen sowie der für die IuK-Technik zuständigen Abteilung umzusetzen ist. Die Stabsstelle hat dabei die Aufgabe, Politik und Verwaltungsspitze bei der Strategieentwicklung zu unterstützen. Festgelegt werden sollte dabei zunächst, welche Dienste elektronisch angeboten werden können und müssen. Parallel dazu sollten die Erwartungen, Möglichkeiten und Zielsetzungen der Fachdienststellen abgefragt werden. Auf dieser Basis kann dann ein Konzept erstellt werden, welche Onlinedienste wann in welcher Tiefe umgesetzt werden. Die Stabsstelle hat dabei die Aufgabe, die notwendigen Ressourcen (Technikausstattung, Finanzierung, notwendige Schulungen des Personals und das verwaltungsinterne Wissensmanagement) zu planen und Zeitpläne für die Umsetzung von Teilschritten zu entwerfen.

Organisatorischer Regelungsbedarf

Der organisatorische Aufwand für die Kommunen bei der Bearbeitung elektronisch ein- bzw. ausgehender Geschäftsvorfälle ist nicht zu unterschätzen. Beim Konzept der virtuellen Poststelle wären die einzelnen Mitarbeiter von der Aufgabe entlastet, die Prüfung von Signatur und Verschlüsselung zu übernehmen. Übernimmt keine zentrale Poststelle die Prüfung der ein- und ausgehenden Post, verbleibt die Aufgabe bei den Mitarbeitern. In diesem Fall stellt sich die Frage, ob jeder bzw. ausgewählte Mitarbeiter Signaturkarten eines Trustcenters erhalten und wie die Rechte und Pflichten jedes einzelnen Mitarbeiters geregelt sind. Da qualifizierte Signaturen nur an natürliche Personen ausgegeben werden, muß jeder Mitarbeiter eine eigene Signaturkarte erhalten, auf der im Haupt- oder Attributzertifikat seine Eigenschaft als Mitarbeiter der Stadtverwaltung X festgehalten wird. Intern muß dann geregelt sein, welche Mitarbeiter welche Zeichnungsberechtigung haben. Die Kosten und der organisatorische Aufwand für die Kommunen bei dieser Lösung sprechen gegen diese Variante, denn bei jeder Beförderung und bei jedem Ausscheiden eines Mitarbeiters müssten die entsprechenden Zertifikate der jeweiligen Mitarbeiter geändert werden.

Seite - 45 -

Wenn verwaltungsintern geklärt ist, wie der Postein- und -ausgang geregelt wird, müssen zusätzlich Regelungen beispielsweise für folgende Bereiche gefunden werden:

- Fristen für die Postbearbeitung,
- Regelungen für die interne Weiterleitung (Ablauforganisation, Zuständigkeiten, Vertretungsregelungen),
- Aktivierung von Virenschutzprogrammen,
- Datensicherheitslösungen und Verschlüsselungskonzepte,
- einheitliche Gestaltung von Briefköpfen, E-Mails, Vordrucken
- Nutzung von Verzeichnisdiensten und Sperrlisten
- Nutzung von Pseudonymen
- Nutzung von privaten und dienstlichen Signaturen
- Revisionsicherheit von Verwaltungsvorgängen
- Erweiterung der vorhandenen Dienstanweisungen zur elektronischen Kommunikation
- ...

Die in dieser Ausarbeitung beschriebenen Wege und Lösungsansätze - insbesondere zur virtuellen Poststelle - können nicht losgelöst von weiteren Entwicklungen hin zum E-Government betrachtet werden. Hierzu werden auch zukünftig Ausarbeitungen des Arbeitskreises Digitales Rathaus des Deutschen Städtetages Hilfestellung für die Kommunen geben.

Seite - 46 -

Quellen / weitergehende Informationen:

Deutscher Städtetag (Mai 2002) " Welche elektronische Signatur bracht die Kommunalverwaltung?" Berlin/Köln

Deutscher Städtetag (2000): Schritte auf dem Weg zum Digitalen Rathaus, Berlin/Köln, Dezember 2000

Deutscher Städtetag (1999): Digitale Signatur auf der Basis multifunktionaler Chipkarten, Köln 1999 (nur elektronisch verfügbar)

Gesellschaft für Informatik e.V. / Informationstechnische Gesellschaft im VDE (2000): Memorandum "Electronic Government als Schlüssel der Modernisierung von Staat und Verwaltung", September 2000

Grabow, Busso (2000): Städte auf dem Weg zum virtuellen Rathaus, Deutsches Institut für Urbanistik, Berlin, März, 2001

Bundesministerium für Wirtschaft und Technologie, Berlin (2000 und 2001)

Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, IT-Grundschutzhandbuch

Bundesamt für Sicherheit in der Informationstechnik (BSI): Bonn, E-Government-Handbuch, BSI Schriftenreihe zur IT-Sicherheit, Band 11

Links:

Informationen der Begleitforschung zum Thema "Grundlagen der elektronischen Signatur und ihre Anwendung in der kommunalen Praxis": www.mediakomm.net

Linksammlung der Zeitschrift Datenschutz und Datensicherheit zum Thema deutsches und internationales Signaturrecht: www.datenschutz-und-datensicherheit.de

Liste der von der Regulierungsbehörde für Post und Telekommunikation zertifizierten Trust-Center sowie zum Thema "Sicherheit von Signaturen": www.regtp.de/

Teletrust Verein, Informationen zur Kryptographie: www.teletrust.de

Neuigkeiten und Informationen zu ISIS-MTT (nur in Englisch): www.t7-isis.de/

E-Government Handbuch des BSI: www.e-government-handbuch.de/

World Wide Web Consortium: www.w3.org

XML-encryption Beschreibung: www.w3.org/encryption/2001/

XML-signature Beschreibung: www.w3.org/signature

Anhang A

Umfang und Grenzen der Sicherheit durch SSL

Die Absicherung einer Web-Kommunikation durch die SSL-Technologie ist vielleicht die derzeit am weitesten (auch und gerade außerhalb geschlossener „Gemeinden“ von „Power-Usern“) verbreitete Anwendung der asymmetrischen Kryptographie. Sie wird in zunehmendem Maße von immer mehr Anbietern gerade auch in sensiblen Bereichen wie etwa E-Commerce oder Homebanking eingesetzt und hat sich dort im Praxiseinsatz bewährt. Zu den herausragenden Eigenschaften dieser Technologie gehört ihre **einfache Bedienbarkeit**. Viele Internet-Nutzer dürften bislang nicht einmal bemerkt haben, dass auch sie diese Technologie genutzt haben. Es steht zu erwarten, dass SSL auch in Web-gestützten E-Government-Applikationen eine große Bedeutung erlangen wird. Hierdurch dürfte das Sicherheitsniveau der elektronischen Verwaltungsdienstleistungen im Vergleich zu „einfachen“ Nutzung des Internet erheblich profitieren.

Der durch den SSL-Einsatz erzielte Sicherheitsgewinn darf jedoch auf der anderen Seite die Betreiber der Web-Seiten und die Nutzer nicht zu dem Fehlschluss verleiten, dass durch die Installation einer SSL-Komponente auf dem Server alle Sicherheitsprobleme der Web-Kommunikation beseitigt wären. Tatsächlich bietet SSL – wie letztlich alle Sicherheitstechniken – einen bestimmten Grad an Sicherheit, der durch verschiedene Randbedingungen eingegrenzt ist. Zu diesen Restriktionen gehören u.a.:

SSL sichert die Kommunikation, nicht die Inhalte

Durch Anwendung von SSL bleibt die Kommunikation für Dritte uneinsehbar und die Herkunft und Unverfälschtheit der Daten, die vom Eigentümer eines SSL-Zertifikats gesendet worden, ist nachprüfbar. Dies bedeutet aber **nicht**, dass sich auf einer Web-Seite mit SSL keine schädlichen Inhalte wie Viren, Trojanische Pferde u.ä. befinden können. In vielen Firewalls in Behörden und Unternehmen wird der Aufruf von

Seite - 48 -

SSL-Seiten sogar bewusst verhindert, da die SSL-Verschlüsselung eine Überprüfung der Kommunikationsdaten auf solche Schadinhalte in der Firewall ausschließt.

Unterschiedliche Verschlüsselungsstärke

Bedingt durch die früher geltenden US-amerikanischen Exportrestriktionen unterstützen vor allem *ältere* Internet-Browser teilweise nur asymmetrische Kryptoverfahren mit Schlüssellängen, die heute von Experten als nicht uneingeschränkt geeignet zu Schutz vor *qualifizierten Angriffen* (d.h. „professionelle“ Täter) angesehen werden.

Benutzerfreundlichkeit vs. Transparenz der Sicherheit

Die angesprochene Benutzerfreundlichkeit der SSL-Implementierungen verbunden bringt als „Kehrseite“ eine oft unzureichende Information des Nutzers mit sich. In der Regel werden die verwendeten Zertifikate im Hintergrund gegen vom Hersteller des Browsers vorab „eingebaute“ CA-Zertifikatsdatenbanken oder (eher selten) gegen vom Nutzer nachträglich eingestellte weitere Zertifikate geprüft. Aktiviert der Nutzer die Option sich die Inhalte der Zertifikate anzeigen zu lassen (was meist ein „Durchklicken“ durch mehrere Menüebenen erfordert), so erhält er oftmals eher „kryptische“ oder nur wenig aussagekräftige Informationen (Bsp.: „Keiner der Zwecke dieses Zertifikats konnte bestätigt werden“...). Eine gezielte Anpassung der Einstellungen auf die eigenen Sicherheitsbedürfnisse und eine fallweise Überprüfung des implementierten Sicherheitsniveaus erfordert detaillierte Kenntnisse in PKI-Technologien und im SSL-Protokoll und ist somit für den „Normalnutzer“ praktisch unmöglich.

„Einseitige“ Zertifikatsverteilung

SSL bietet wie erwähnt die Möglichkeit der *gegenseitigen* Authentisierung von Server („Behörde“) und Client („Bürger“). Diese Möglichkeit, die gerade in E-Government-Anwendungen äußerst nützlich sein könnte, setzt jedoch voraus, dass der Bürger über ein sog. Client-Zertifikat verfügt. Obwohl dies erheblich preiswerter ist als ein Server-Zertifikat (je nach Anbieter etwa 50 € jährlich im Vergleich zu etwa 1000 €) haben bisher nur sehr wenige Internetnutzer ein solches Client-Zertifikat erworben. („Henne-Ei-Problem“?)

Mängel bei Registrierung und Sperrmanagement

Die Sicherheit von Asymmetrischen Kryptoverfahren beruht wie erwähnt wesentlich auf der Güte der Registrierung der Zertifikatsinhaber und der Verlässlichkeit und Schnelligkeit von Zertifikatssperrungen. Ein Fall aus dem Januar 2001²⁶ zeigt, dass es hier in der SSL-Infrastruktur durchaus noch Verbesserungsmöglichkeiten gibt. Damals gelang es einer Person ein Zertifikat einer renommierten amerikanischen Zertifizierungsstelle zur Signatur von downloadbaren Programmen zu erhalten, das ihn *fälschlicherweise* als Mitarbeiter eines großen Softwareanbieters auswies. Hier lag also offenkundig ein (niemals ganz auszuschließendes) Versäumnis bei der Registrierung vor. Diese Person könnte also über SSL-Verbindungen z.B. Schadprogramme in den Umlauf bringen, die von den gängigen Browsereinstellungen als authentisch vom besagten Hersteller stammend und damit als „sicher“ eingestuft (und ausgeführt) würden. Tatsächlich wurde dieser Fehler nach zwei Tagen bemerkt und das Zertifikat umgehend gesperrt. Aufgrund von bestimmten Details in der Implementierung der SSL-Technologie²⁷ wird diese Sperrung von den Browsern jedoch **nicht umgesetzt**; das Zertifikat wird also weiterhin technisch als „gültig“ akzeptiert.

Die obenstehende Diskussion soll in keiner Weise eine Empfehlung gegen den Einsatz von SSL aussprechen. Der durch diese Technologie tatsächlich erreichbare Sicherheitsgewinn kann aber nur dann wirklich durchgängig erzielt werden, wenn die Restriktionen bei der Anwendung berücksichtigt und mit dem Schutzbedarf der zu übertragenden Daten abgestimmt werden.

Inwieweit sich die offenkundig vorhandenen technisch-organisatorischen Unzulänglichkeiten des SSL-Zertifikatsmanagements durch neue Browserversionen und/oder die Einrichtung von Zertifizierungsstellen mit für die Bedürfnisse des E-Government angepasstem nachprüfbarem Registrierungsmechanismus und Zertifikatsforma-

²⁶ Eine detaillierte Beschreibung dieses Falls und seiner Konsequenzen gibt H. Mack in seinem Artikel „Sperren von Zertifikaten in der Praxis – eine Fallanalyse“ veröffentlicht in der Fachzeitschrift Datenschutz und Datensicherheit, Ausgabe 8/2001, S. 464-466.

²⁷ Das im X.509-Zertifikatsformat *optional* erlaubte Attribut „CRL-Distribution Point“, d.i. eine Internet-Adresse, an der der Browser eine entsprechende Sperrliste herunterladen kann, wurde nicht genutzt. Hierdurch ist eine *automatische* Aktualisierung von Sperrinformationen im Browser unmöglich.

Seite - 50 -

ten/Zertifikatsmanagement verbessern lassen, kann derzeit nicht vorhergesagt werden.

Anhang B

Sprechstunde in der virtuellen Amtsstube - Ein Kommunikationsszenario in acht Akten

Die Akteure und ihre Requisiten

Die Personen

- **Der Bürger**²⁸ (*Schlüsselpaare für Authentisierung und Signatur; internetfähiges Zahlungssystem*)
- **Der Verwaltungsmitarbeiter (kurz: Mitarbeiter)** (*Schlüsselpaar für Signatur*)

Die Maschinen

- **Der Kommunikationsserver (kurz: Server)** (*Schlüsselpaare für Verschlüsselung und Authentisierung, System zur Entgegennahme von Zahlungen*)
- **Das Hintergrundsystem**²⁹

Anmerkung: Bei der genannten Ausstattung handelt es sich um *Minimalanforderungen*. Es werden also nur diejenigen Schlüsselpaare erwähnt, die für die betrachtete Kommunikation tatsächlich benötigt werden. In der Praxis dürfen sich auf den betreffenden Chipkarten weitere Schlüsselpaare befinden.

Die Vorgeschichte

Der Bürger hat sich die Zertifikate des Kommunikationsservers vorab auf „vertrauenswürdigem“ Weg beschafft und kann sich bei Bedarf über Verzeichnisdienste von der aktuellen Gültigkeit dieser Zertifikate überzeugen.

Die Zertifikate des Bürgers und des Verwaltungsmitarbeiters sind zu Beginn der Kommunikation bei den jeweiligen Partnern noch nicht vorhanden und müssen des-

²⁸ Selbstverständlich kann hier genauso auch eine Bürgerin agieren.

²⁹ Die Rollen von Kommunikationsserver und Hintergrundsystem können von mehreren Rechnern parallel gespielt werden.

Seite - 52 -

halb mitversendet werden. Der Bürger und die Verwaltung verfügen jedoch über Zugang zu Verzeichnisdiensten zur Überprüfung der Zertifikate.

Regieanweisung

Gemäß der Grundidee des E-Government handeln sowohl Bürger als auch Mitarbeiter möglichst wenig direkt, sondern überlassen dies weitestgehend ihren jeweiligen Rechnern. Wo immer eine direkte, persönliche Aktion nötig ist, wird dies durch **Fett-druck** hervorgehoben. Falls kein Fettdruck verwendet wird agieren nur die Rechner, ohne dass dies von den Menschen bemerkt wird (solange keine Fehler auftreten und alle Überprüfungen erfolgreich sind)

1. Akt „Kontaktaufnahme mit Identifizierung“

Bürger: **startet seinen PC und surft auf die Webseite der Verwaltung; durch Anklicken eines entsprechenden Buttons bringt er seinen Wunsch nach Erbringung einer vertraulichen und verbindlichen Verwaltungsdienstleistung zum Ausdruck;** Sein PC übersendet an den Kommunikationsserver eine entsprechende technische Initialisierungsnachricht.

Server: bestätigt die Initialisierungsnachricht und informiert Bürger darüber, dass eine vertrauliche Kommunikationsbeziehung aufgebaut werden soll und bittet Bürger, jetzt seine Chipkarte einzusetzen.

Bürger: **steckt die Chipkarte in den Leser, aktiviert diese und bestätigt diese Aktion durch Mausklick,** sein PC erzeugt eine Zufallszahl („Challenge“) C_1 und übersendet diese an den Server

Server: „verschlüsselt“ C_1 mit seinem privaten Authentisierungsschlüssel und übersendet das Ergebnis („Response“ R_1) an den Bürger; erzeugt eine weitere Zufallszahl C_2 und übersendet diese ebenfalls an den Bürger

Bürger: überprüft ggf. die Gültigkeit des bekannten Zertifikats der Verwaltung und entschlüsselt mit dem öffentlichen Schlüssel R_1 . Ist das Ergebnis gleich C_1 , hat sich der Server erfolgreich authentisiert; er verschlüsselt C_2 mit seinem Authentisierungsschlüssel (Ergebnis: R_2) und übersendet dieses zusammen mit seinem Authentisierung-Zertifikat an den Server

Server: überprüft das Zertifikat des Bürgers und entschlüsselt mit dem dabei erhaltenen öffentlichen Schlüssel R_2 . Ist das Ergebnis gleich C_2 , hat sich der Bürger erfolgreich authentisiert; der Server übersendet eine entsprechende „Erfolgsmeldung“ an den Bürger

2. Akt „Der Schlüsseltausch“

Bürger: erzeugt einen Sitzungsschlüssel (Zufallszahl) S entsprechend den Anforderungen des gewählten hybriden Verschlüsselungsverfahrens, verschlüsselt S mit dem öffentlichen Verschlüsselungsschlüssel des Servers (ggf. nach

Seite - 53 -

vorheriger Überprüfung des Zertifikats) und übersendet das Ergebnis an den Server

Server: entschlüsselt die Nachricht des Bürgers mit seinem privaten Schlüssel und erhält so ebenfalls den Sitzungsschlüssel S

Anmerkungen:

- Von jetzt an findet die **gesamte** Kommunikation zwischen Bürger und Server³⁰ verschlüsselt (mit S) statt, ist also für einen externen „Lauscher“ nicht mehr einsehbar. Die einzige Information, die dieser erhalten hat, ist also die Tatsache, dass eine solche Kommunikation stattfindet; er weiß jedoch *nichts* über deren Inhalte, also nicht einmal, welche Dienstleistung nachgefragt wurde.
- Es gibt auch Verfahren, bei denen der Sitzungsschlüssel in Kooperation von Bürger und Server erzeugt wird.

3. Akt „Das Formular“

Bürger: wählt durch Mausklick eine konkrete Dienstleistung der Verwaltung aus.

Server: gibt die Anfrage des Bürgers zusammen mit dessen Identität an das Hintergrundsystem weiter

Hintergrundsystem: erzeugt ein vorpersonalisiertes Formular und gibt dies an den Server zurück

Server: sendet dem Bürger das vorpersonalisierte Formular

Bürger: **füllt das Formular „online“ aus, signiert dieses und sendet es – zusammen mit der Signatur – an den Server zurück,** sein PC fügt automatisch das zugehörige Signaturzertifikat hinzu

Server: prüft das Formular auf Vollständigkeit und (soweit möglich) auf Plausibilität, prüft die Gültigkeit des Zertifikats und mit dem erhaltenen öffentlichen Signaturschlüssel die Signatur, dokumentiert das Prüfergebnis (revisionssicher), [die folgenden Schritte erfolgen nur, wenn Signatur- und Zertifikatprüfung erfolgreich waren] überträgt die Formulareingaben in eine für das Hintergrundsystem unmittelbar verständliche Form, sendet diese Daten an das Hintergrundsystem und informiert den Bürger, dass sein Antrag entgegengenommen wurde

Bürger: **beendet die Sitzung** (falls die Bearbeitung des Antrags nicht sofort abgeschlossen werden kann)

³⁰ Für die Kommunikation zwischen Server und Hintergrundsystem ist eine solche Verschlüsselung i.d.R. nicht notwendig, da sie vollständig im abgeschotteten Hausnetz der Behörde stattfindet.

Seite - 54 -

Der Sitzungsschlüssel wird auf dem Server und dem PC des Bürgers gelöscht.

4. Akt „Die Bearbeitung“

Hintergrundsystem: bearbeitet den Antrag, erstellt einen lesbaren elektronischen „Bescheid“ und leitet ihn an einen zeichnungsbefugten Mitarbeiter zu

Mitarbeiter: **prüft den Bescheid abschließend, signiert ihn und gibt ihn wieder ins Hintergrundsystem**

Hintergrundsystem: vervollständigt die elektronische Akte und gibt Bescheid und Signatur an den Server

5. Akt „Kontaktaufnahme mit Identifizierung (Reprise)“

Server: sendet E-Mail mit dem Inhalt „Ihr Bescheid liegt jetzt vor“ an den Bürger

Bürger: **liest die Mail, surft auf den Web-Server der Verwaltung und signalisiert per Mausklick, dass er jetzt seinen Bescheid abholen möchte**

Es folgen die Schritte des Authentisierungsprozesses aus dem 1. Akt mit jeweils neuen Challenges C₃ und C₄

6. Akt „Schlüsselaustausch (Reprise)“

Wie im 2. Akt wird jetzt ein neuer Sitzungsschlüssel zwischen Server und Bürger ausgetauscht. Mit diesem wird dann die gesamte weitere Kommunikation verschlüsselt

7. Akt „Bezahlung“

Server: informiert den Bürger über die Höhe der anfallenden Verwaltungsgebühren und fordert ihn zur deren Begleichung auf

Bürger: **aktiviert das Bezahlsystem und überweist die Gebühr elektronisch an den Server**

Server: prüft den korrekten Eingang der Zahlung und sendet einen entsprechenden Vermerk ins Hintergrundsystem

Die folgenden Schritte dieses Akts laufen „parallel“ zum weiteren Geschehen und verzögern dessen Fortgang nicht

Hintergrundsystem: „verbucht“ den Zahlungseingang und erstellt ggf. eine Quittung, die an einen zeichnungsberechtigten Mitarbeiter zugeleitet wird

Mitarbeiter: **prüft die Quittung abschließend, signiert diese und sendet Quittung und Signatur ans Hintergrundsystem**

Hintergrundsystem: leitet Quittung und Signatur an den Server weiter

Seite - 55 -

tem:

Server: versendet Quittung, Signatur und Signaturzertifikat an den Bürger (ggf. per E-Mail)

8. Akt „Der Bescheid“

Server: versendet (online oder per E-Mail) den Bescheid, die zugehörige Signatur und des benötigte Signaturzertifikat des Mitarbeiters an den Bürger, ggf. wird auch eine vom Bürger zu signierende Empfangsquittung erstellt

Bürger: **signiert ggf. die Empfangsquittung und sendet diese mit seinem Signaturzertifikat an den Server; beendet die Kommunikation**

Server: registriert ggf. die Quittung und sendet sie ans Hintergrundsystem

Anhang C

Vertrauliche und authentische Kommunikation zwischen Bürger und (kommunaler) Verwaltung – Ein Modell

Das Arbeitsmodell beschreibt *eine mögliche* vertrauliche und authentische Kommunikation zwischen einem Bürger und seiner (kommunalen) Verwaltung. Andere Lösungen sind u.U. durchaus denkbar.

Das Szenario

Ein Bürger nimmt über einen Web-Server Kontakt mit seiner Stadt (Landkreis, Gemeinde etc..) auf. Er stellt einen elektronischen „Antrag“ und erhält einen kostenpflichtigen, rechtsverbindlichen „Bescheid“. Sowohl der Antrag als auch der Bescheid sollen über ein öffentliches Netz (Internet...) vertraulich übermittelt werden.³¹

Der städtische Web-Server übergibt die Antragsdaten an ein elektronisches Hintergrundsystem der Stadt, in dem der Antrag bearbeitet wird.

Randbedingungen:

- Die entsprechenden Rechtsvorschriften gestatten es sowohl dem Bürger als auch der Stadtverwaltung elektronische Dokumente formgerecht abzufassen, wenn sie mit einer qualifizierten Signatur nach dem Signaturgesetz (SigG) versehen sind („Schriftformersatz). Dies bedingt, dass normalerweise seitens der Stadt ein „Sachbearbeiter“ als natürliche Person die Signatur erstellen muss.
- Bürger und Stadt verfügen über interoperable Kommunikationssysteme, die wechselseitige Entschlüsselung und Signaturprüfung sowie eine Online-Bezahlung ermöglichen.
- Zum Vertraulichkeitsschutz wird ein *hybrides* Verschlüsselungsverfahren eingesetzt. Dies entspricht der gängigen Praxis (etwa SSL, HBCI etc.) und ermöglicht eine schnelle Kommunikation mit abgesichertem Schlüsselaustausch.

³¹ Durch Weglassen der entsprechenden Schritte kann das Modell leicht für eine nicht kostenpflichtige oder nicht formgebundene Antragstellung oder Leistung modifiziert werden.

„Akteure“ und kryptographische Schlüssel

Für sämtliche asymmetrischen Schlüsselpaare gebe es Verzeichnisdienste, bei denen eine authentische Zertifikatsprüfung nach SigG (für Signaturschlüssel) bzw. vergleichbaren Sicherheitsniveaus (für Entschlüsselungs- und Authentisierungsschlüssel) erfolgen kann. Ggf. besteht für die Stadt die Möglichkeit die Zertifikate ihrer Bürger in einem eigenem Verzeichnis („Einwohnermeldeamt“) abzulegen. Dieses müsste natürlich – etwa durch Bezug von Sperrlisten – regelmäßig mit den externen Verzeichnisdiensten abgeglichen werden.

1. Bürger

- öffentlicher S_B und privater s_B Signaturschlüssel nach SigG
- öffentlicher V_B und privater v_B Verschlüsselungsschlüssel
- öffentlicher A_B und privater a_B Authentisierungsschlüssel

2. Städtischer Web-Server

- öffentlicher A_S und privater a_S Authentisierungsschlüssel

3. Städtischer „Sachbearbeiter“

- öffentlicher S_A und privater s_A Signaturschlüssel nach SigG mit zugehörigem Attributzertifikat (Eigenschaft als städtischer Mitarbeiter und ggf. Dienststellung)³²

Ausgetauschte Nachrichten, Notation

- I „Initialisierungsnachricht“: Wunsch des Bürgers nach abgesicherter Kommunikation. Diese – nicht vertrauliche - Nachricht muss nicht zwangsläufig per E-Mail oder ähnlichem erfolgen, sondern kann auch etwa durch Anklicken eines entsprechenden Web-Links erfolgen.
- A: Anforderung des Formulars
- C „Zufallsnachricht“: In den üblichen „Challenge-Response-Verfahren“ wird dem Kommunikationspartner K, von dem man eine Authentisierung erwartet eine „zufällige“ Nachricht (Challenge) zugesendet, die dieser mit seinem privaten Authentisierungsschlüssel verschlüsselt und zurücksendet (Response). Entscheidend ist

³² Auf der Chipkarte des Mitarbeiters können sich natürlich noch weitere Schlüssel befinden; diese spielen jedoch in dem betrachteten Kommunikationsmodell keine Rolle.

Seite - 58 -

hierbei, dass K die Nachricht vorab nicht kennt. Es bietet sich an, für C etwa eine Zufallszahl zu nehmen.³³

- F „Formular“: Das mit den im Hintergrundsystem abgelegten persönlichen Daten des Antragstellers (Meldedaten etc.) vorkonfigurierte Antrags“formular“.³⁴

F* : Das vom Bürger ausgefüllte Formular

- N: Benachrichtigung an den Bürger, dass der Bescheid abgerufen werden kann. N ist nicht vertraulich, da keine Details über die Art des Bescheids übermittelt werden.
- R: Rechnung
- B: Der städtische Bescheid

(A,B,C,): Gemeinsames Verschicken der „Nachrichten“ A,B und C

S[X]: Nachricht X **symmetrisch** verschlüsselt mit Schlüssel S

S{X}: Nachricht X **asymmetrisch** verschlüsselt mit (öffentlichem) Schlüssel S

<X,S>: Nachricht X „signiert“ mit (privatem) Schlüssel S; hierbei kann S sowohl ein SigG-konformer Signaturschlüssel als auch ein Authentisierungsschlüssel sein.

Zert(X): Zertifikat für den öffentlichen Schlüssel X








³³ Dieser Vorgang läuft i.d.R. komplett im „Hintergrund“ ab; der Benutzer merkt davon – solange die Authentisierung gelingt – nichts.

³⁴ Dies muss nicht unbedingt die elektronische Version eines üblichen Formulars sein.

Das Modell

Vorbemerkung: Die mit „*“ gekennzeichneten Schritte sind optional. Diejenigen Schritte, die ein direktes („manuelles“) Eingreifen der Kommunikationspartner erforderlich sind, sind durch ein Fettdruck; alle übrigen Schritte laufen automatisch im Hintergrund ab.

1) Antrag

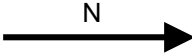
	Web-Server (Stadt)	Internet	Bürger
1)		(I, C ₁)	erzeugt Initialisierungsnachricht I und Challenge C₁
2)	„signiert“ C ₁ mit a _S erzeugt Challenge C ₂	(<C ₁ , a _S >, Zert(A _S), C ₂) 	
3)			überprüft Zert(A _S)* prüft „Signatur“ von C ₁
4)		(<C ₂ , a _B >, Zert(A _B), V _B)	„signiert“ C ₂ mit a _B ³⁵
5)	prüft Zert(A _B) prüft „Signatur“ von C ₂		
6)	erzeugt Sitzungsschlüssel S 	V _B {S}	
7)			entschlüsselt S mit v _B
8)		S[A] 	erzeugt Anfrage A
9)	Hintergrundsystem erzeugt vorphonalisiertes Formular F	S[F] 	
10)		(S[F*], <F*, s _B >, Zert(S _B))	füllt F aus signiert F* mit s_B
11)	entschlüsselt F* prüft Zert(S _B) prüft Signatur		

³⁵ Aus Sicherheitsgründen bietet es sich an, diesen Vorgang vom Nutzer bestätigen zu lassen.



2) Bearbeitung

Im (städtischen) Hintergrundsystem wird der Antrag bearbeitet und der Bescheid B sowie eine Benachrichtigung N und eine Rechnung R erstellt. Der Bescheid vom einem „Sachbearbeiter“ mit seinem privatem Signaturschlüssel s_A SigG-konform signiert. Alle Dokumente werden dem Web-Server übergeben.

3) Lieferung des Bescheids

	Web-Server (Stadt)	Internet	Bürger
1)			

Es folgen die Authentisierungsschritte 1)-5) aus Übersicht 1 mit neuen „Challenges“ C_3 und C_4

	Web-Server (Stadt)	Internet	Bürger
7)	erzeugt Sitzungsschlüssel 	$(T[R], V_B\{T\})$	
			entschlüsselt T mit v_B entschlüsselt R mit T
8)			überweist online Rechnungsbeitrag
9)	Nach Zahlungseingang: 	$(T[B], \langle B, s_A \rangle, \text{Zert}(S_A))$	
10)			entschlüsselt B mit T überprüft $\text{Zert}(S_A)^*$ prüft Signatur von B^*