



ITWM-Trier

Fraunhofer Management
Gesellschaft

**Trust Center -
Zertifizierungsstelle
nach SigG u. SigV**

Preprint 97-04
ISSN 1433-8106

**Hans-Jürgen Görg
Christoph Meinel
Thomas Engel**

Trust Center - Konzeption einer Zertifizierungsstelle nach Signaturgesetz u. Signaturverordnung

Trust Center – Konzeption einer Zertifizierungsstelle nach Signaturgesetz und Signaturverordnung

Von entscheidender Bedeutung für die Sicherheit der Datenübertragung in offenen Netzen ist die Lösung zweier Probleme. Zum einen muß sichergestellt werden, daß Unberechtigten der Zugriff auf übertragene Daten verwehrt ist, zum anderen muß eindeutig feststellbar sein, daß übertragene Daten auch tatsächlich von einem berechtigten Absender stammen. Der folgende Beitrag beschäftigt sich mit der Konzeptionierung einer den Anforderungen des Signaturgesetzes und der Signaturverordnung entsprechenden Zertifizierungsstelle, die die Grundlage für Verschlüsselung und elektronische Unterschriften schafft.

Hans-Jürgen Görg
Christoph Meinel
Thomas Engel

Vorwort

Die Entwicklung der Online-Dienste, insbesondere des Internet, vom ursprünglich rein wissenschaftlich genutzten Netz der Universitäten und Forschungseinrichtungen zur „Datenautobahn“ für die Wirtschaft und alle interessierten Bürger rund um den Globus schuf für die Nutzer vielfältige Risiken, da das Datennetz nicht unter Sicherheitsaspekten entwickelt, sondern historisch gewachsen ist. Sicherheitsrisiken bestehen vor allem bei der Übertragung vertraulicher Daten, da die Übertragungswege für jedermann zugänglich sind. Jeder andere Nutzer, insbesondere der in Anspruch genommene Provider, kann die Daten einsehen, manipulieren und im schlimmsten Falle auch mißbräuchlich nutzen. Veränderungen oder Fälschungen übertragener Nachrichten und deren Absender sind nicht erkennbar. Öffentlich in den Netzen verfügbare Software erlaubt zudem eine systematische Suche nach genau definierbaren Informationen. Es ist daher von größter Notwendigkeit sicherzustellen, daß beim Datentransfer in Netzwerken Unberechtigte nicht in die Lage versetzt werden, fremdes Datenmaterial einzusehen. Die Gewährleistung eines sicheren Datenschutzes ist folglich unabdingbar, um eine dauerhafte Funktionsfähigkeit der Netze zu erreichen und zu erhalten und damit sowohl der Gesellschaft, als auch den Nutzern selbst Schutz vor Schäden an verfassungsrechtlich garantierten Rechtsgütern, insbesondere bezüglich ihres Rechts auf informationelle Selbstbestimmung, zu bieten.

Das ITWM-Trier als gemeinnützige Forschungs- und Entwicklungseinrichtung hat sich die Aufgabe gestellt, mit Hilfe seiner umfassenden Infrastruktur und seiner Fachkompetenz in den Bereichen Internet / Intranet sowie auf mathematisch-kryptographischem und juristischem Gebiet, die Rolle einer vertrauenswürdigen dritten Person bei Erzeugung, Vergabe und Zuordnung öffentlicher Schlüssel zu übernehmen und damit wie ein elektronischer Notar eine Gewähr für sichere und authentische Datenübertragung und für zuverlässigen Datenschutz zu bieten. Es sieht sich darüberhinaus prädestiniert, mit Infrastruktur- und Organisationsberatung Aufbau- und Managementhilfe bei der Konzeption, der Realisierung und dem Betrieb von Trust Centern zu bieten und so seinen Innovationsspielraum auszuweiten und Standards für eine möglichst hohe Interoperabilität in der Wirtschaft zu setzen.

Grundlagen digitaler Signaturen – Ein Überblick

Von entscheidender Bedeutung für die Gewährleistung der Datenübertragungssicherheit in offenen Netzwerken und damit für den Rechtsgüterschutz des jeweiligen Nutzers ist die Lösung zweier Probleme. Zum einen muß sichergestellt werden, daß Unberechtigten der Zugriff auf übertragene Daten verwehrt ist, zum anderen muß eindeutig feststellbar sein, daß übertragene Daten auch tatsächlich von einem berechtigten Absender stammen. Im ersten Fall geschieht dies durch eine Verschlüsselung der Daten, für die unterschiedliche, teilweise sehr sichere Methoden zur Verfügung stehen. Eine solche Verschlüsselung wird auch als Enkryption bezeichnet. Im zweiten Fall wird auf eine elektronische Unterschrift, eine sog. digitale Signatur, zurückgegriffen, die als Berechtigungsnachweis des Absenders dient. Dies wird allgemein als Authentisierung bezeichnet.¹

Sowohl für die Enkryption des übertragenen Datenmaterials, als auch für die Authentisierung des Absenders der Daten werden heute sog. asymmetrische Kryptographieverfahren verwendet. Diese auch als Public-Key-Verfahren bezeichneten Methoden beruhen auf der Vorstellung, daß ein Absender einem Empfänger eine verschlüsselte Nachricht übermitteln kann, ohne daß er irgendeine Geheiminformation mit dem Empfänger gemeinsam hat. Jeder Nutzer in einem offenen Netz besitzt ein elektronisches Schlüsselpaar, das aus einem geheimen und einem öffentlich zugänglichen Schlüssel besteht. Letzterer wird in einer öffentlich zugreifbaren Datenbank oder in einem öffentlichen Datenverzeichnis für jedermann zugänglich bereitgehalten. Der Absender eines Dokumentes verschlüsselt dieses mit dem öffentlichen Schlüssel des Empfängers, der Empfänger allein kann mit seinem privaten Schlüssel, der weltweit einmalig existiert, die Nachricht entschlüsseln und damit nur für sich lesbar machen. Alle anderen Nutzer bleiben von der Kenntnis des Inhalts des Dokumentes ausgeschlossen. Sie können die Nachricht lediglich in verschlüsselter Form zur Kenntnis nehmen. Eine Dechiffrierung ohne Kenntnis des geheimen Schlüssels des vorgesehenen Empfängers erfordert einen so hohen technischen Aufwand, daß der unberechtigte Angreifer in einem praktisch noch relevanten Zeitraum sein Ziel nicht erreichen kann. In verhältnismäßig kurzen Zeitabständen kann die Sicherheit der technischen Entwicklung regelmäßig angepaßt werden. Dies geschieht typischerweise durch die Verwendung einer größeren Schlüssellänge. Die technische Möglichkeit einer unberechtigten Entschlüsselung chiffrierter übertragener Datenmaterials ist daher rein theoretischer Natur. Der Sicherheitsstandard derart versendeter Dokumente kann, in Abhängigkeit der sicherheitsrelevanten Erfordernisse unterschiedlicher Geheimhaltungsstufen und Sensibilitätsbereiche, als außerordentlich hoch angesehen werden.

Die Authentisierung des Absenders eines Dokumentes durch eine elektronische Unterschrift ist eine Variante des kryptographischen Public-Key-Verschlüsselungsverfahrens. Sinn und Zweck einer solchen digitalen Signatur ist es, die wesentlichen Merkmale einer handschriftlichen Unterschrift (Echtheit, Identität, Verifikation und Rechtsverbindlichkeit) in elektronischer Form zu realisieren. Der Absender einer Nachricht erzeugt dazu mit seinem geheimen, privaten Schlüssel eine Signatur, quasi als spezielles Unterschriftenmerkmal, unter Verwendung einer mathematisch komprimierten Form des zu verschickenden Dokumentes, einer sog. Einweg- oder kryptographischen Hashfunktion. Dadurch wird der Text zur Vermeidung späterer Änderungen in die Signatur miteinbezogen. Dokument und Signatur werden dem Empfänger übersendet, wobei natürlich auch das Dokument seinerseits wieder, wie oben bereits dargestellt, mit dem öffentlichen Schlüssel des Adressaten chiffriert und damit dessen Inhalt vor unberechtigter Kenntnisnahme geschützt werden kann. Der Empfänger entschlüsselt die Nachricht mit seinem privaten Schlüssel in Klartextform, komprimiert diesen Text mit der vorerwähnten Hashfunktion und vergleicht dieses Komprimat mit dem in der elektronischen Signatur des Absenders enthaltenen Komprimat, das sich durch Entschlüsseln der Signatur mit dem öffentlich verfügbaren Schlüssel des Absenders ergibt. Stimmen beide Komprimat inhaltlich überein, so steht zum einen fest, daß das verschickte und das angekommene Dokument identisch sind, also keine Veränderungen vorgenommen wurden oder Übertragungsfehler aufgetreten sind. Zum anderen sind die Identität und die Authentizität des Absenders eindeutig erkennbar, da nur der bestimmte Absender mit seinem geheimen Schlüssel die digitale Unterschrift erzeugt haben kann. Anderenfalls wäre eine Dechiffrierung mit seinem öffentlichen Schlüssel und damit eine Umwandlung der elektronischen Signatur auf das ursprüngliche Komprimat nicht möglich gewesen.

¹ Gelegentlich wird dafür auch der Begriff „Authentifikation“ verwendet.

Sowohl das Ver- und Entschlüsseln eines Dokumentes, als auch das Signieren mit einer digitalen Unterschrift und deren Verifizierung sind für den Nutzer, trotz der komplexen mathematischen Vorgänge, die dabei ablaufen, weitgehend unkompliziert. Der Rechner mit seiner graphischen Benutzeroberfläche verlangt lediglich das Anklicken der entsprechenden Buttons, die Funktionen laufen rechnerintern selbstständig ab, was ein rationelles Arbeiten ermöglicht. Auf diese Art und Weise lassen sich nicht nur Textdokumente, sondern auch Bilder, Graphiken, Töne, Software und anderes geistiges Eigentum signieren, was für den Urheberrechtsschutz zunehmend an Bedeutung gewinnen wird, zumal eine wesentlich höhere Sicherheit im Vergleich zu einer handschriftlichen Unterschrift erreicht werden kann.

Die Einführung und Durchsetzung eines solchen Verfahrens zur Generierung digitaler Unterschriften und deren verbindliche Anerkennung im Rechtsverkehr erfordert, neben einer entsprechenden Organisation und einer sicheren Infrastrukturumgebung, insbesondere rechtliche Sicherheit bei der Authentifizierung des Inhabers eines öffentlichen Schlüssels. Inhaber und öffentlicher Schlüssel müssen eindeutig und rechtssicher einander zugeordnet werden können, um zu verhindern, daß ein Unberechtigter sich mit Hilfe eines seiner Person nicht zuzuordnenden öffentlichen Schlüssels eine falsche Identität verschaffen kann. Es bedarf daher eines vertrauensvollen Dritten, der durch ein Zertifikat wie ein „elektronischer Notar“ bestätigt, daß der öffentlich zugängliche Schlüssel einmalig und fest einer bestimmten natürlichen Person zugeordnet ist.

Mit Wirkung zum 1. August 1997 trat das neue Informations- und Kommunikationsdienstegesetz (IuKDG) mit dem Ziel in Kraft, eine verlässliche Regelungsgrundlage für die sich dynamisch entwickelnden Angebote im Bereich der Informations- und Kommunikationsdienste zu schaffen und einen Ausgleich zwischen freiem Wettbewerb, berechtigten Nutzerbedürfnissen und öffentlichen Ordnungsinteressen herbeizuführen (Zitat aus der amtlichen Begründung). Das darin enthaltene Signaturgesetz mit der dazugehörigen Signaturverordnung bietet die rechtliche Grundlage für den Aufbau einer juristischen, informationstechnologischen und mathematischen-kryptographischen Sicherheitsinfrastruktur sowie für die funktionale und organisatorische Abwicklung sämtlicher mit einer digitalen Signatur verbundenen Dienstleistungen. Dabei geht es in erster Linie um eine vertrauenswürdige, authentische und manipulationssichere Verknüpfung des kryptographisch erzeugten öffentlichen Signaturschlüssels mit einer bestimmten natürlichen Person zum Zwecke der Nutzung elektronischer Unterschriften mitsamt einer rechtssicheren und zuverlässigen Zertifikaterstellung für den Rechtsverkehr („Certification Authority“). Die vom Gesetzgeber dafür vorgesehenen Organisationseinheiten werden als Zertifizierungsstellen oder auch Trust Center bezeichnet. Sie bieten die Basis für eine manipulationssichere Datenübertragung in Netzwerken und für die rechtsverbindliche Anerkennung elektronischer Unterschriften durch die Gerichte.

Die Begriffe „Trust Center“ und „Zertifizierungsstelle“ werden oftmals nebeneinander verwendet. Gelegentlich wird auch die englische Bezeichnung „Trusted Third Party“ benutzt, um die Funktionen eines vertrauenswürdigen Dritten bei der Zertifizierung öffentlicher Schlüssel zu charakterisieren. Die Synonymität dieser Begriffe ist dabei nie als ganz eindeutig anzusehen. So verstehen manche z. B. unter dem Begriff „Trust Center“ ausschließlich die technische und infrastrukturelle Realisierung einzelner vom Signaturgesetz und der Signaturverordnung vorgesehener Aufgaben. Andere bezeichnen mit diesem Begriff die Organisation, die mit diesen Aufgaben betreut ist. Das gleiche gilt für den vom Gesetzgeber geprägten Ausdruck „Zertifizierungsstelle“. Auch hier wird dessen Funktionalität gelegentlich abweichend von der gesetzgeberischen Intention allein für die technische und sicherheitsinfrastrukturelle Umsetzung der von Signaturgesetz und Signaturverordnung vorgesehenen Anforderungen verwendet, ohne daß dabei auch die eigentliche Ablauforganisation mitsamt ihren äußerst sicherheitsrelevanten Betriebsabläufen und Dienstleistungen miteinbezogen wird.

Im hiesigen Zusammenhang werden beide Begriffe synonym verwendet, wobei jeweils sowohl die vom Signaturgesetz und der Signaturverordnung beschriebenen funktionalen Dienstleistungen¹, als auch die dort als deren Grundlage vorgeschriebenen technischen, sicherheitsinfrastrukturellen und organisatorischen Realisationsmöglichkeiten umfaßt sein sollen. Dies entspricht auch der Intention des Gesetzgebers, der unter einer Zertifizierungsstelle eine Organisationseinheit versteht, die in erster Linie für die authentische, integre (d. h. verlässliche und unangreifbare) und unmanipulierbare Verknüpfung von kryptographischem Schlüsselmaterial mit natürlichen Personen verantwortlich ist.

¹ Vgl. dazu näher unten „Zu den Funktionalitäten einer Zertifizierungsstelle“.

Zu den Funktionalitäten einer Zertifizierungsstelle

Signaturgesetz und Signaturverordnung sehen gewisse Funktionalitäten im Rahmen des organisatorischen Ablauf beim Betrieb einer Zertifizierungsstelle vor, damit diese ihre Anforderungen an die Erzeugung und Vergabe von Schlüsselpaaren erfüllen sowie eine Zertifizierung öffentlicher Signaturschlüssel zu bestimmten, genau identifizierbaren natürlichen Personen wahrnehmen und von jedem Nutzer nachvollziehbar dokumentieren kann. Es handelt sich dabei um die folgenden Funktionalitäten, die ihrerseits die zu erbringenden Dienstleistungen einer Zertifizierungsstelle vorgeben¹:

- Schlüsselgenerierung für die Zertifizierungsstelle

Die Zertifizierungsstelle muß für sich selbst ein eigenes Schlüsselpaar erzeugen, bestehend aus einem öffentlichen und einem privaten Schlüssel, welches mit dem gewählten Verfahren zur Bildung digitaler Signaturen korrespondiert. Dieses Schlüsselpaar wird von der zuständigen Regulierungsbehörde als Wurzelinstanz für die Zertifizierungsstelle zertifiziert. Die Zertifizierungsstelle benötigt das Schlüsselpaar ihrerseits für die Zertifizierung der öffentlichen Schlüssel der Teilnehmer an dem Verfahren für digitale Signaturen. Die Schlüsselpaarerzeugung muß in einer geeigneten und sicheren Umgebung innerhalb der Zertifizierungsstelle stattfinden und es muß sichergestellt werden, daß ein unautorisierter Zugriff auf den privaten Schlüssel der Zertifizierungsstelle verhindert wird.

- Teilnehmeridentifizierung und –registrierung

Jeder Teilnehmer am Verfahren für digitale Signaturen muß sich gegenüber der Zertifizierungsstelle ausweisen. Ihm wird bei positiver Identifizierung ein geeigneter und eindeutiger Name zugewiesen, unter dem er digitale Signaturen erzeugen kann. Wünscht ein Teilnehmer gegenüber Dritten nicht mit seinem Namen aufzutreten, so kann der Name in Form eines Pseudonyms zugeteilt werden, so daß die Identität gegenüber anderen nicht unmittelbar erkennbar wird. Der so identifizierte Teilnehmer ist anschließend zu registrieren.

- Schlüsselerzeugung für die Teilnehmer

Darüberhinaus ist für den Fall, daß ein Teilnehmer nicht über ein selbst generiertes Schlüsselpaar verfügt, von der Zertifizierungsstelle ein Schlüsselpaar für diesen Teilnehmer zu erzeugen. Der so generierte private Schlüssel wird vom Teilnehmer für die Bildung digitaler Signaturen, der öffentliche Schlüssel für die Verifikation der Signaturen benötigt. Wichtig ist, daß der private Schlüssel nach der Übergabe an den Teilnehmer in der Zertifizierungsstelle vernichtet wird und daß jedes Schlüsselpaar nur einmal vorkommt.

- Zertifikatserstellung

Um eine authentische Zuordnung der vom Teilnehmer erzeugten digitalen Signaturen zu ermöglichen, muß die Zuordnung des Schlüsselpaares zu diesem Teilnehmer ebenfalls in authentischer Weise erfolgen. Für jeden Teilnehmer am Verfahren ist daher von der Zertifizierungsstelle ein Zertifikat zu erzeugen, das ein Identifizierungsmerkmal für diesen Teilnehmer, den öffentlichen Schlüssel des Teilnehmers und einen Gültigkeitszeitraum enthalten muß. Diese Inhalte werden authentisch und unverfälschbar durch eine digitale Signatur, die mittels des privaten Schlüssel der Zertifizierungsstelle gebildet wird, miteinander verknüpft.

- Personalisierung des Trägermediums

Bei der Personalisierung werden Teilnehmerdaten, Zertifikat des öffentlichen Schlüssels des Teilnehmers, privater Schlüssel des Teilnehmers, öffentlicher Schlüssel der Zertifizierungsstelle und Möglichkeit zur Aktivierung des Benutzer-Authentisierungsverfahrens des Trägermediums (z.B. über Paßwort oder PIN) auf einem geeigneten Trägermedium gespeichert.

¹ Vgl. zu den Dienstleistungen einer Zertifizierungsstelle im Einzelnen unten.

- Verzeichnisdienst

Es sind in einem Verzeichnis authentisch und integer alle Schlüsselzertifikate aller Teilnehmer der Zertifizierungsstelle festzuhalten und aufzubewahren. Gesperrte Zertifikate sind darüberhinaus in eine Sperrliste einzutragen, die Auskunft über den Zeitpunkt des Eintretens der Sperrung enthält. Die Sperrinformationen sind jederzeit für jeden abrufbar zu halten zwecks Überprüfbarkeit der Zertifikate. Die Zertifikate selbst bzw. einzelne Informationen daraus (z. B. Teilnehmernamen, öffentlicher Schlüssel u.a.) dürfen nur bei Erlaubnis des Teilnehmers für Dritte zugänglich gemacht werden.

- Zeitstempeldienst

In bestimmten Fällen ist es notwendig, digitale Daten authentisch mit einem bestimmten Zeitpunkt zu verknüpfen, um später nachvollziehen zu können, zu welchem Zeitpunkt ein Dokument digital signiert wurde (z. B. Feststellung des Zeitpunktes der Rechtswirksamkeit eines Vertrages zur Beurteilung der Gefahrtragung). Die Dokumente werden dazu mit der vom Zeitstempeldienst anzubietenden vertrauenswürdigen Zeit digital verknüpft und das Ergebnis anschließend von diesem digital signiert. Der Zeitstempeldienst ist folglich Teilnehmer der eigenen Zertifizierungsstelle. Anschließend werden die so unterschriebenen Daten an den Teilnehmer zurückgeschickt.

- Sonstige Funktionalitäten

An sonstigen Funktionalitäten hat ein Trust Center insbesondere Maßnahmen zur Datensicherung und zur Datenarchivierung zu ergreifen, ein Notfallmanagement zur Regelung von nicht vorhersehbaren Ausnahmesituationen bereitzustellen, ein Sperrmanagement für Kompromittierung oder Verlust privater Schlüssel oder nicht mehr gültiger Zertifikate zu organisieren und Reaktionsmechanismen bei gebrochenen Kryptoalgorithmen zu schaffen.

Zur Sicherheitsinfrastruktur einer Zertifizierungsstelle

Um den Anforderungen des Signaturgesetzes und der Rechtsverordnung zu genügen, ist es dringend erforderlich, eine Sicherheitsinfrastruktur aufzubauen, durch die die authentische Zuordnung der öffentlichen Signaturschlüssel zu natürlichen Personen durch das Zertifikat möglich wird. Das Gesetz gibt hierfür eine Sicherheitsinfrastruktur vor, bei der eine zweistufige Hierarchie von Zertifizierungsstellen wie folgt festgeschrieben wird:

Eine neue Regulierungsbehörde übernimmt die oberste Rolle einer Wurzelinstanz und zertifiziert ihrerseits ausschließlich Zertifizierungsschlüssel genehmigter Zertifizierungsstellen, die auf der nächsten Hierarchieebene unter der Wurzelinstanz angesiedelt sind. Diese eigentlichen Zertifizierungsstellen im hiesigen Sinne zertifizieren dann ihrerseits die Signaturschlüssel der bei ihr angeschlossenen Teilnehmer.

Dienstleistungen einer Zertifizierungsstelle

- Schutzbedarfsanalyse der Dienstleistungen

Sämtliche Dienstleistungen einer Zertifizierungsstelle bedürfen eines spezifischen Schutzes bezüglich der Kriterien

- Vertraulichkeit
- Integrität und
- Verfügbarkeit.

Aus einer Analyse dieses Schutzbedarfes lassen sich dann die jeweiligen Anforderungen an die die Dienstleistungen unterstützenden informationstechnologischen Anwendungen, informationstechnologischen Systeme und Kommunikationssysteme ableiten.

Der typischerweise zugrunde zulegende Schutzbedarf der einzelnen Dienstleistungen ist davon abhängig, ob die Schadensauswirkungen

- vernachlässigbar sind bzw. begrenzt und überschaubar bleiben,
- für den Teilnehmer oder die Zertifizierungsstelle beträchtlich sind oder
- ein existentiell bedrohliches, katastrophales Ausmaß erreichen können.

- Übersicht über die Dienstleistungen

Bei dem Betrieb einer Zertifizierungsstelle sollte der folgende Organisationsablauf eingehalten werden, da er die gesetzlich vorgesehenen Dienstleistungen in einer sinnvollen Reihenfolge integriert:

- Antragstellung durch den Teilnehmer
- Identifizierung und Registrierung des Teilnehmers
- Schlüsselgenerierung und Zertifikatserstellung für den Teilnehmer
- Personalisierung des Trägermediums und Übergabe an den Teilnehmer
- Speicherung und Vorhaltung zu veröffentlichender Daten in einem Verzeichnis
- Vorhaltung eines Zeitstempeldienstes
- Einrichten eines Spermanagements und Maßnahmen der Notfallvorsorge

Wechselwirkungen

Die zuvor spezifizierten Dienstleistungen operieren, mit Ausnahme des Zeitstempels, der losgelöst arbeiten kann, nicht unabhängig voneinander. Sie stehen in einer Wechselwirkung miteinander, wie die im folgenden Kapitel beschriebene Ablauforganisation zeigt.

Beschreibung der Ablauforganisation

Die folgende Beschreibung einer Betriebsablauforganisation eines Trust Centers veranschaulicht die Wechselwirkungen zwischen den einzelnen bereits dargestellten Funktionalitäten innerhalb einer Zertifizierungsstelle. Die Realisierung einer solchen Stelle legt diesen Organisationsablauf ihrer informationstechnologischen und juristischen Planung zugrunde.

1. Identifizierung und Registrierung des Teilnehmers und Zertifikatsbeantragung

Zunächst läßt sich der Teilnehmer bei der Registrierungsstelle identifizieren und registrieren und beantragt, daß ihm durch ein Zertifikat die Zuordnung seines Namens zu einem öffentlichen Schlüssel bescheinigt wird.

2. Schlüsselerzeugung

Vom Teilnehmer selbst oder vom Schlüsselerzeugungsdienst der Zertifizierungsstelle wird ein Schlüsselpaar erzeugt, wobei die zweite Alternative in der Praxis die gängigere sein wird.

3. Zertifizierung des öffentlichen Schlüssels des Teilnehmers

Der Zertifizierungsdienst der Zertifizierungsstelle verknüpft die Identität des Teilnehmers mit dessen öffentlichem Schlüssel und erstellt darüber ein Zertifikat. Diese übermittelt er sowohl an die Personalisierungsstelle, als auch an den Verzeichnisdienst.

4. Personalisierung des Trägermediums

Die Personalisierungsstelle überträgt die für den Teilnehmer relevanten Daten, die noch nicht auf dem Trägermedium vorhanden sind (evtl. auch das Schlüsselpaar), auf das Trägermedium, das dann dem Teilnehmer ausgehändigt werden kann.

5. Aufnahme der zu veröffentlichen Daten in den Verzeichnisdienst

Die Daten, die öffentlich zugänglich gehalten werden müssen, werden durch den Verzeichnisdienst erfaßt und über öffentliche Kommunikationseinrichtungen für jeden erreichbar gehalten.

6. Verknüpfung von Daten mit einem bestimmten Zeitpunkt

Der Zeitstempeldienst verknüpft beliebige signierte Daten oder das Zertifikat mit einem bestimmten Zeitpunkt. Er kann sowohl vom Teilnehmer, als auch vom Registrierungsdienst oder dem Zertifizierungsdienst in Anspruch genommen werden. Er ist nicht explizit in den vorgegebenen Organisationsablauf eingebunden.

Anmerkung

Die Realisationsmöglichkeiten des dargestellten Konzepts eines Trust Centers sowie die organisatorischen Einzelheiten des Betriebsablaufes einer Zertifizierungsstelle bleiben einem gesonderten Beitrag vorbehalten, der wie der vorliegende in der Preprint-Schriftenreihe des ITWM-Trier erscheint.