TeleTrusT Deutschland e. V.
Erfurt, 23.09.2002

Thesen zum Signaturbündnis

Ziel des Signaturbündnisses ist die Beschleunigung der Verbreitung von Chipkarten und Zertifizierungsdienstleistungen für einen vertrauenswürdigen elektronischen Geschäfts- und Rechtsverkehr. Um dieses Ziel zu erreichen, hält TeleTrusT die folgenden Maßnahmen für erforderlich:

1. **Zielführende Strategie: Wirtschaftlich stabile und vertrauenswürdige Infrastrukturen schaffen**
   Das Signaturbündnis muss dem Umstand Rechnung tragen, dass eine nachhaltig wirksame Infrastruktur für PKI-gestützte Geschäftsprozesse nur entsteht, wenn der Nutzen aus verschiedenen Anwendungszusammenhängen gebündelt werden kann und flexible und skalierbare Lösungen angeboten werden. Die neue Herausforderung im Bündnis besteht darin, die Bedingungen dafür zu schaffen, dass bei Bedarf (zur Erfüllung von Formvorschriften des Privatrechts oder Vorschriften des Verwaltungsrechts) die qualifizierte elektronische Signatur in eine stabile und verbreitete Infrastruktur eingebettet werden kann. Die andauernde Diskussion über höchste Anforderungen an elektronische Signaturen und die damit verbundene Barriere für die Verbreitung von Chipkarten, Zertifikaten und Anwendungen sowie für die wirtschaftlich erfolgreiche Tätigkeit von Zertifizierungsdiensteanbietern (ZDA) muss beendet werden.
   Eine solche Vorgehensweise ist auch deshalb erforderlich, weil bisher praktische Erfahrungen zu massenhafter Verbreitung, zum Umgang mit und zur Akzeptanz von PKI-gestützten Geschäftprozessen fehlen und auf diese Weise – unter aktiver Beteiligung der Nutznießer aus unterschiedlichen Anwendungsbereichen – gewonnen werden können.

2. **Pragmatisches Vorgehen, Bestands- und Investitionsschutz**
   Das Signaturbündnis muss die Zusammenführung von praktischen Erfahrungen organisieren und bestehende Konzepte so integrieren, dass die angestrebte nachhaltige Wirkung erzielt wird.
   - Es ist mit bereits entwickelten Anwendungen (auf der Basis von SmartToken wie der z.B. der Chipkarte) zu beginnen. Die Evaluierung des SmartToken, die Zertifizierung der Anwendung, die Akkreditierung des ZDA darf nicht Voraussetzung sondern bestenfalls Migrationsziel im Sinne einer Idealvorstellung sein.
   - Zur Förderung der „Leichtigkeit des elektronischen Rechts- und Geschäftsverkehrs“ muss die von TeleTrusT bereits vorgeschlagene „MultiserviceCard“ schon bald geeignet sein, die Zertifikate verschiedener ZDA für unterschiedliche elektronische Signaturen zuverlässig und anwenderfreundlich zu verarbeiten.

   Das Signaturbündnis schafft dadurch für Anbieter von Produkten und Anwendungen, Chipkartenherausgeber und ZDA sowie die Nutzer Sicherheit für Investitionsentscheidungen.

3. **Wirtschaftlichkeit**
   Die Herausgeber von Chipkarten (oder anderen SmartToken) müssen durch die deutsche Politik gefördert und selbst gefordert werden, in ihre SmartToken neben den herausgeberbezogenen Anwendungen (z.B. Mitarbeiterausweis, Bankkarte usw.) die Signaturfunktionalität wirtschaftlich verträglich und anwenderfreundlich zu integrieren. Alle Barrieren, die eine dafür erforderliche flexible Kooperation von Chipkartenherausgeber, ZDA und Anwender behindern, sind zu beseitigen.

4. **Einheitliche Rechtssytematik**
   Nur eine durchgängige deutsche Rechtssystematik im Sinne der Europäischen Rahmenrichtlinien für elektronische Signaturen kann gesetzliche Rahmenbedingungen bieten, die die wirtschaftlich motivierte Entwicklung von Produkten, Dienstleistungen und Lösungen für PKI-gestützte Anwendungen stimulieren.
   Dies zu erreichen, sind eine Novellierung des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) sowie eine grundsätzliche Veränderung des Umgangs mit deren Regulierungsrahmen unumgänglich.
   Insbesondere sind
   - die Einschränkungen in den Definitionen des SigG (z.B. „fortgeschrittene elektronische Signatur“, „Signaturschlüsselinhaber“, „Zertifizierungsdienste-anbieter“ etc.) gegenüber der EU-RL aufzuheben,
   - die Bindung der elektronischen Signatur an eine natürliche Person im Interesse unternehmens- und behördenübergreifender Geschäfts- und Verwaltungsprozesse durch die Bindung an eine juristische Person zu ergänzen bzw. zu ersetzen,
   - die Anforderungen an die Spezifikation des Zertifikatsmanagements für SigG-Root und SigG-CA’s so zu gestalten, dass sie konform zu internationalen, mindestens jedoch zu europäischen Standards abbildbar und
   - SigG und SigV so zu vereinfachen, dass sie mit wirtschaftlich vertretbarem Aufwand international konkurrenzfähig umzusetzen sind.

5. **Vertrauensbildende Begleitung**
   Im Rahmen einer solchen durchgängigen deutschen Rechtssystematik muss die Regulierungsbehörde für Telekommunikation und Post ihre Aufgabenschwerpunkte den wirtschaftlichen Erfordernissen anpassen.
   Hierzu gehört die Erweiterung ihrer Tätigkeit über die alleinige Umsetzung des §15 SigG (Akkreditierung von ZDA) hinaus durch vertrauensbildende Begleitung (Aufsicht) von Konzepten im Rahmen von §4 SigG (angezeigte Zertifizierungsdienste für qualifizierte Signaturen) und für fortgeschrittene Signaturen.

6. **Internationale Standards**
   Die ISIS-MTT-Spezifikation soll Grundlage aller signaturbasierten Internetanwendungen im Signaturbündnis werden, da sie internationale Standards profiliert und Interoperabilität gewährleistet. Inkl. des zugehörigen Testbeds ist sie ein aktiver Beitrag der deutschen Wirtschaft zu Weiterentwicklung und Umsetzung der europäischen Signaturstandardisierung.

7. **Mustervertrag ‚Anwendung fortgeschrittener Signaturen'**
   Das Signaturbündnis muss dazu beitragen, den durch den allgemeinen Sprachgebrauch („SigG-konform", „Nicht-SigG-konform") etablierten, jedoch falschen Eindruck zu korrigieren, nur mit qualifizierten Signaturen (ggf. mit Anbieterakkreditierung) sei Rechtsverbindlichkeit elektronischer Geschäftsprozesse gewährleistet. Diese Sichtweise hat in den zurückliegenden Jahren zu einer wirtschaftlich nicht vertretbaren Fehlleitung von Ressourcen geführt.
   Zu diesem Zweck soll zwischen zwei geeigneten Teilnehmern des Signaturbündnisses aus der Wirtschaft ein Mustervertrag zur gegenseitigen Anerkennung der Rechtsverbindlichkeit und individuellen Haftungsbegrenzung von fortgeschrittenen Signaturen für individuell vorab vereinbarte Geschäftsverfahren ausgearbeitet werden.

8. **Interoperabilität von Anwendungen**
   Es ist Interoperabilität von in Deutschland rechtsverbindlichen Anwendungen mit Internet-Lösungen, z.B. zum Zwecke des Austauschs verschlüsselter Dateien oder bezüglich der parallelen Integration von fortgeschrittenen und qualifizierten Signaturlösungen auf einem Endanwender System, umzusetzen.

9. **Entwicklung stabiler Rahmenbedingungen**
   Mittelfristige Aufgaben des Signaturbündnisses sollen sein:
   - Unterstützung der weiterführenden Anpassung der Spezifikation für standardkonforme PKI-Anwendungen (ISIS-MTT),
   - Entwicklung einer vertrauenswürdigen Selbstregulierung für die Belange der MultiserviceCard und der dafür erforderlichen Zertifizierungsdienste.

10. **Die Rolle von TeleTrusT im Signaturbündnis**
    Als unabhängige und neutrale Institution ist TeleTrusT mit seinen Mitgliedern aus Wirtschaft, öffentlicher Verwaltung und Anwendung bereit und willens, im Signaturbündnis einerseits eine integrierende und andererseits eine die Entwicklung forcierende Rolle einzunehmen.
    Hierzu wird TeleTrusT seine Kompetenz vor allem aus der Entwicklung der ISIS-MTT-Spezifikation und dem zugehörigen Testbed sowie dem Betrieb der European Bridge-CA einbringen.