Entwurf der Technischen und administrativen Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur

Erläuterungen

1 Einleitung

Die Technischen und administrativen Vorschriften (TAV) über die Dienste der elektronischen Zertifizierung wurden im Jahr 2001 erarbeitet. In der Zwischenzeit wurden neue internationale Normen mit genauerer Beschreibung der Politiken, Praxis und Organisation der Anbieter von Zertifizierungsdiensten veröffentlicht, insbesondere vom ANSI (American National Standards Institute), von der ISO (International Organization for Standardization) und der EESSI (European Electronic Signature Standardization Initiative).

Die TAV von 2001 wurden in der Folge diesen internationalen Veröffentlichungen der jüngsten Zeit gegenübergestellt. Dabei zeigten sich wesentliche Unterschiede. Diese wurden analysiert und vor dem Hintergrund des vom neuen Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) abgesteckten Rahmens sowie der Förderung einer gesunden Marktentwicklung, der Interoperabilität und der internationalen Harmonisierung evaluiert.

In diesem Zusammenhang galt es auch zu prüfen, inwieweit die alten TAV angepasst werden können und wo ein Verweis auf anerkannte Normen sinnvoll ist.

2 Verfahren zur Ausarbeitung der Technischen und administrativen Vorschriften

2.1 Normungsstellen und deren Veröffentlichungen im Bereich der elektronischen Signatur

Die Analyse der von den Normungsstellen durchgeführten Arbeiten erlaubten einerseits eine Bestandesaufnahme der Veröffentlichungen vorzunehmen und andererseits das Verfahren betreffend die Erarbeitung und Aktualisierung der Standards zu verstehen und schliesslich die Rezeption der Normen in der Wirtschaft zu bewerten.

2.1.1 ANSI X9.79 - PKI policy and practices framework

Auf dem Gebiet der Finanzdienstleistungen hat das ANSI (American National Standards Institute) einen Rahmen für die Politik und Praxis bezüglich der Public-Key-Infrastrukturen (PKI) gesetzt. Die Norm ANSI X9.79*: Public Key Infrastructure (PKI) Practices and Policy Framework* umfasst in Anhang 2 spezifische Anforderungen an die Betreiber von PKI. Diese sind jedoch nicht verpflichtet, besondere Anforderungen zu befolgen. Sie können aus den Anforderungen bezüglich der Politik diejenigen frei auswählen, die den Zielen ihrer eigenen Politik am besten entsprechen.

Obwohl diese Norm für die spezifischen Bedürfnisse des Finanzsektors gedacht war, fand sie im Markt für die Anerkennung von PKI eine breite Verwendung. Sie wird vom PKI-Forum, einer internationalen Gruppierung von Anbietern und Benutzern von PKI, empfohlen. Die Norm ANSI X9.79 wurde ausserdem vom AICPA/CICA (American and Canadian institutes for accountants) im Rahmen des WebTrust-Programms aufgenommen, bei dem die Angemessenheit und Effizienz der von den Zertifizierungsbehörden ausgeübten Kontrollen beurteilt wird.

2.1.2 ISO CD 21188-1 - PKI policy and practices framework

Ende 2001 verabschiedeten die Mitglieder des TC68-Ausschusses der ISO (International Organization for Standardization) einen Vorschlag des ANSI (American National Standards Institute) zur Ausarbeitung einer Norm für die Praxis und Politik im Bereich der Public-Key-Infrastrukturen in den Finanzdiensten gestützt auf die Norm ANSI X9.79 an.

Die meisten europäischen ISO-Mitglieder sprachen sich für dieses Projekt aus unter der Voraussetzung, dass bei den Arbeiten die europäische Richtlinie und die ETSI-Spezifikation TS 101 456 *Policy requirements for certification authorities issuing qualified certificates* berücksichtigt werde.

Die erste Phase der Arbeiten führte im Oktober 2002 zur Veröffentlichung eines ersten Entwurfs (Committee Draft ISO CD 21188-1).

Das European Telecommunication Standardization Institute (ETSI) machte zahlreiche Anregungen für eine vereinfachte Anpassung an die eigenen Spezifikationen. Die Kommentare im Anschluss an diese erste Konsultation wurden in den Redaktionsprozess aufgenommen, der 2004 zu einem zweiten Entwurf und 2005 zur endgültigen Veröffentlichung führen sollte.

Im Gegensatz zu der bei der Ausarbeitung als Referenzdokument verwendeten Norm ANSI X9.79 bietet ISO 21188-1 keinen allgemeinen Rahmen, der sich auf verschiedene Sektoren anwenden liesse, sondern richtet sich im Wesentlichen an den Finanzsektor.

2.1.3 European Electronic Signature Standardization Initiative (EESSI)

2.1.3.1 Hintergrund

Die «Richtlinie 1999/93/EG des europäischen Parlamentes und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen» definiert eine besondere Form der elektronischen Signatur gestützt auf ein qualifiziertes Zertifikat als Voraussetzung ihrer gesetzlichen Anerkennung. In den Anhängen der Richtlinie werden die Mindestanforderungen für die Anbieter von Zertifizierungsdiensten genannt, die qualifizierte Zertifikate ausstellen, sowie die Sicherheitsmassnahmen, die während der Ausarbeitung und Überprüfung der Signatur einzuhalten sind, und die Datenstruktur, die zu wählen ist.

Für eine einfachere Umsetzung in den verschiedenen innerstaatlichen Gesetzgebungen und zur Erreichung der Interoperabilität ist ein Verweis auf anerkannte Normen im Bereich der elektronischen Signaturen vorgesehen.

2.1.3.2 Standardisierungsarbeiten

Zu diesem Zweck lancierte das European ICT Standards Board 1999 mit der Unterstützung durch die Europäische Kommission und der aktiven Teilnahme von Industrie, Behörden, Sachverständigen und anderen Marktteilnehmern die «European Electronic Signature Standardization Initiative» (EESSI).

Als erstes wurde der Standardisierungsbedarf in Bezug auf die Anforderungen der Richtlinie erhoben. Die Beurteilung der verfügbaren Normen und anderen laufenden weltweiten Initiativen förderte anschliessend einen Mangel an Übereinstimmung und Kohärenz sowie auch gewisse Defizite zutage, welche die Notwendigkeit von zusätzlichen Standardisierungstätigkeiten rechtfertigten.

Die Ausarbeitung der Normen wurde dem Europäischen Komitee für Normung (CEN) sowie dem ETSI übertragen, die noch heute aktiv sind. Diese Tätigkeit wird ausserdem von einer «Steering Group» überwacht, in der die verschiedenen Marktteilnehmer vertreten sind.

Die Arbeit dieser Normungsstellen steht allen interessierten Parteien offen, was die Ausarbeitung qualitativ hoch stehender und konsensorientierter Spezifikationen erlaubt. Im Übrigen arbeiten das ETSI und das CEN gegenseitig und mit allen anderen, auf diesem Gebiet anerkannten Gremien eng zusammen, um die Interoperabilität und internationale Harmonisierung der Entwicklung zu sichern.

So werden Kontakte mit folgenden Stellen gepflegt:

- APEC-TEL eStg (Asia-Pacific Economic Community, Telecommunication and information Working Group, eSecurity Task Group)
- IETF – PKIX (Internet Engineering Task Force)
- Amerikanische Regierung im Rahmen des Programms US Federal PKI
- ISO (International Organization for Standardization)
- Asia PKI Forum
- Japan PKI Forum
- China PKI Forum

Neben dem Informationsaustausch ermöglicht diese Zusammenarbeit insbesondere eine Analyse der Übereinstimmung zwischen den Normen der verschiedenen Organisationen und trägt zur Qualität der neuen und aktualisierten Veröffentlichungen bei.

Bisher haben das CEN und das ETSI zahlreiche, über die Grenzen Europas hinaus anerkannte technische Spezifikationen für eine vereinfachte Einführung von Infrastrukturen und Diensten herausgegeben. Das nächste Kapitel enthält eine Bestandesaufnahme der wichtigsten Dokumente über die Zertifizierungsdienste.

Die im Laufe der ersten technischen Umsetzungen gesammelten Erfahrungen erlaubten eine Bewertung der Spezifikationsqualität und zeigten die Schwachpunkte auf. Diese Informationen konnten bei der Überarbeitung dieser Normen genutzt werden.

Das ETSI hat das Dokument mit dem Titel ETSI TS 101 456 *Policy requirements for certification authorities issuing qualified certificates* veröffentlicht. Dieses Dokument, das die europäische Richtlinie über die elektronische Signatur ergänzt, beschreibt die Sicherheitsanforderungen, die für die Zertifizierungsstellen (CA) gelten, die qualifizierte Zertifikate generieren wollen. Diese technische Spezifikation wurde bereits im April 2002 revidiert, und weitere Revisionsarbeiten laufen seit 2003. Das ETSI sollte sie vor Ende 2004 abschliessen.

Die niederländische Regierung startete ein Projekt für die Vereinfachung des Verfahrens zur Anerkennung der Anbieter von Zertifizierungsdiensten, welches die Veröffentlichung von Leitlinien in Bezug auf die Spezifikation ETSI TS 101 456 (*TTP.NL Guidance on ETSI TS 101 456*) nach sich zog. Das Dokument, an dessen Erarbeitung mehrere privatwirtschaftliche Unternehmen wie KPN, KPMG und PricewaterhouseCoopers beteiligt waren, ergänzt die ETSI-Veröffentlichung und beugt Auslegungsproblemen vor.

Im Bewusstsein um die Nützlichkeit eines solchen Dokuments hat das ETSI die Ausarbeitung einer Anleitung in Angriff genommen, die den Inhalt des holländischen Dokuments *TTP.NL Guidance on ETSI TS 101 456* übernimmt, um die Beurteilung der Konformität zu erleichtern.

Die technische Spezifikation ETSI TS 101 456 und die Richtlinie *TTP.NL Guidance on ETSI TS 101 456* verweisen mehrfach auf die Norm ISO 17799 *Information technology – Code of pratice for Information security management*, um die Anforderungen für die Anbieter von Zertifizierungsdiensten zu präzisieren.

2.1.3.3 Veröffentlichungen der EESSI

Das ETSI und das CEN haben die folgende Dokumentenreihe zur Förderung der Richtlinienumsetzung veröffentlicht:

- TS 101 456 *Policy Requirements for CAs issuing Qualified Certificat*es
- TS 101 733 *Electronic Signature Formats*
- TS 101 903 *XML Advanced Electronic Signatures (XAdES)*
- TS 101 861 *Time Stamping Profile*
- TS 101 862 *Qualified Certificate Profile*
- CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures*
- CWA 14167-2 *Cryptographic Module for CSP Signing Operations -Protection*
- *Profile (MCSO-PP)*
- CWA 14169 *Secure Signature-Creation Devices Version EAL4+*

2.2 Vergleich und Feststellung der Unterschiede

Nach dieser Bestandesaufnahme der Akteure im Bereich der Standardisierung und der erwähnten Veröffentlichungen wurden diese mit den TAV von 2001 verglichen. Die Schlüsse aus diesem Vergleich waren die Grundlage für den Entscheid, welche Anforderungen künftig noch notwendig sind.

2.3 Verweis auf Normen

Zur Förderung der Interoperabilität und internationalen Harmonisierung musste geprüft werden, inwieweit die neuen TAV auf anerkannte und verwendete Normen verweisen könnten.

Der Nutzen von Verweisen auf Normen wird durch die Feststellungen einer im Auftrag der Europäischen Kommission durchgeführten Studie (*The Legal and Market Aspects of Electronic Signatures*, Studie des «Interdisciplinary Centre for Law & Information Technology» und der Universität Leuven, Belgien) bestätigt. Darin heisst es:

> *(Seite 6)*
> *Qualified electronic signatures need to be in compliance with the requirements as stated by the first three annexes of the Directive. It is, therefore, important that the annexes are correctly transposed into national legislation. … The only risk is related to interoperability problems which might occur if technical implementations of annex I diverge by, for example, not using TS 101862, or other common format for encoding the requirements of annex I. The Commission should therefore promote the use of interoperability standards for the technical implementations of annex I.*
>
> *(Seiten 6 et 7)*
> *For the implementation of annex II, implementation levels are sometimes quite varying, meaning that the establishment and running of a CSP will differ considerably. Any organization wishing to establish a CSP business in several countries must therefore adapt itself to different requirements and procedures. Product vendors will also have difficulties building products for this very fragmented market. In addition, several countries put additional detailed and unnecessary requirements on the CSP, thus creating barriers for the establishment of a CSP.*
>
> *(Seite 10)*

Since EESSI already has published a number of valuable documents in this area it is recommended that supervisory authorities be encourage to make use of these specifications.

(Seite 13)
The Commission and Member States must ensure that all member States correctly implement presumption of conformity with standards referenced in the Official Journal.

(Seite 119)
In order to achieve interoperability, standards are required.

Diese Meinung wird im Übrigen von der «International Chamber of Commerce» geteilt, die in den «*ICC comments on the 2003 review of the E-Signatures Directive (1999/93/EC)*» vom 26.09.2003 folgendes festhält:

To remedy the existing divergence in Member States' transpositions of the Directive and to increase the uptake in use of electronic signatures in the EU, ICC recommends that the Commission:
[…]
Press Member States to refrain from imposing additional requirements on ordinary electronic signatures beyond the Directive's definition of electronic signature;
[…]

Im Rahmen der verschiedenen Konsultationen wurde ausserdem der Wunsch nach einem Verweis auf anerkannte und insbesondere europäische Normen geäussert.

2.4 Warum ein Verweis auf die EESSI-Spezifikationen?

Die Ausführungsvorschriften bezwecken ebenso wie das Gesetz (Art. 1 ZertES) und die Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur, dass ein breites Angebot an sicheren Zertifizierungsdiensten zur Verfügung steht und auch angewendet wird sowie die internationale Anerkennung von Anbieterinnen und ihren Dienstleistungen zu fördern. Zur Erreichung dieser Ziele müssen bei der Ausarbeitung der Technischen und administrativen Vorschriften die internationale Harmonisierung und die Interoperabilität eine wichtige Rolle spielen. Die Nutzung von anerkannten und im Rahmen ähnlicher Gesetze verwendeter Normen und die Verweisung auf dieselben sind wichtige Instrumente dafür.

In einer Bestandesaufnahme der weltweit anerkannten Normen nehmen die EESSI-Dokumente eine prominente Stellung ein. Deren Übernahme in nationales Recht scheint auch in Anwendung von Art. 20 Abs. 1 ZertES geboten. Dass diese Dokumente international anerkannt sind, wird im Übrigen durch die Tatsache bestätigt, dass die Niederlande und Luxemburg sie bereits für die Anerkennung der Anbieter von Zertifizierungsdiensten verwenden. Durch die Übernahme der Terminologie (Art. 2 ZertES) und gar bestimmter Textteile (Art. 6 ZertES) unterstreicht das ZertES den Willen des Gesetzgebers, sich dem europäischen Gesetzesrahmen anzunähern.

Die Kompetenz der an der Ausarbeitung beteiligten Experten, die enge Zusammenarbeit mit anderen Normungsstellen und die Seriosität der Verfahren bei der Erarbeitung und Aktualisierung der Standards bürgen für ihre Qualität.

Die Tatsache, dass die Arbeit der EESSI zu einer umfassenden Sammlung von äusserst nützlichen Dokumenten für die Anerkennung der Anbieter von Zertifizierungsdiensten geführt

hat, stellt ebenfalls einen weiteren Vorteil dar, der für einen Verweis auf die EESSI-Normen spricht.

2.5 Definition des Inhalts

Die neue Version der Technischen und administrativen Vorschriften bezieht sich aus diesen Gründen weitgehend auf die europäischen Spezifikationen (EESSI).

Der Vergleich zwischen den Normen zeigt, dass eine erhebliche Anzahl von Anforderungen der TAV von 2001 in den verschiedenen internationalen Normen nicht enthalten ist.

Im Laufe der Ausarbeitung der neuen TAV musste der Nutzen dieser Zusatzanforderungen beurteilt werden. Dabei wurde berücksichtigt, dass zu grosse Abweichungen zwischen den verschiedenen nationalen Bestimmungen die Interoperabilität und internationale Harmonisierung gefährden könnten.

2.6 An der Ausarbeitung beteiligte Parteien

Um die Qualität bei der Ausarbeitung der Technischen und administrativen Vorschriften zu gewährleisten, wurde die Erfahrung und Kompetenz der verschiedenen Marktteilnehmer berücksichtigt. Die wichtigsten Anbieter von Zertifizierungsdiensten (Keyon, SwissCert, Swisssign und Wisekey), die Anerkennungsstelle (KPMG), die Akkreditierungsstelle (SAS) sowie das BIT als Betreiber einer umfangreichen Public-Key-Infrastruktur beteiligten sich an dieser Ausarbeitung.

Das BAKOM zog ausserdem einen international anerkannten Sachverständigen hinzu, der von Beginn weg an den Arbeiten der EESSI beteiligt war. Herr Denis Pinkas, der als Sicherheitsberater bei der Firma Bull beschäftigt ist und dadurch über eine besondere Markt- und Praxisnähe verfügt, arbeitete direkt an der Abfassung verschiedener Dokumente der EESSI und der IETF (Internet Engineering Task Force) mit. Seine Kompetenzen werden auch im Rahmen bestimmter Arbeiten der ISO sowie bei der Revision der französischen Gesetzgebung im Bereich der Zertifizierungsdienste genutzt.

Das Ausarbeitungsverfahren sieht ausserdem eine so genannt «öffentliche» Konsultation vor, bei der verschiedene direkt oder potenziell betroffene Kreise sich vor der Veröffentlichung der Endversion zu den Arbeiten äussern können.

3 Erläuterungen in Bezug auf die Ausarbeitung der neuen Technischen und administrativen Vorschriften

Der Einfachheit und besseren Vergleichbarkeit halber entsprechen die neuen TAV hinsichtlich ihrer Gliederung der Struktur der internationalen Normen.

Die aktuelle Struktur des Dokuments muss die Suche nach bestimmten Anforderungen sowie Vergleiche, Aktualisierungen und das Einfügen neuer Anforderungen erleichtern. Sie kann auf Grund der im Verlauf der verschiedenen Konsultationen gemachten Vorschläge geändert werden.

3.1 Kapitel 2, Prinzip der Anerkennung der CSP

Die Schweizerische Akkreditierungsstelle (SAS) verwaltet und veröffentlicht auf ihrer Website die Liste der akkreditierten Anerkennungsstellen.

Die SAS ist auch für das Führen und die Veröffentlichung der Informationen betreffend die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten verantwortlich. Sie gibt zu diesem Zweck auf ihrer Website den Ort und das elektronische Format an, das für diese Daten verwendet wird, damit sie durch Softwares abgefragt werden können.

3.2 Kapitel 1.1, Geltungsbereich

Die Technischen und administrativen Vorschriften stützen sich auf das Bundesgesetz sowie die Verordnung des Bundesrates über Zertifizierungsdienste im Bereich der elektronischen Signatur. Folglich gelten sie nur für die vom Gesetz vorgesehene Zertifikatsart.

Ein Anbieter von Zertifizierungsdiensten, der andere Zertifikatsarten anbietet, kann sich gemäss einer internationalen Norm seiner Wahl anerkennen lassen, jedoch keinen Anspruch auf eine Anerkennung seiner elektronischen Signatur in privatrechtlichen Beziehungen erheben.

3.3 Kapitel 1.2, Referenzen

Die Verweise auf internationale Normen sind statisch. Dies bedeutet, dass ausschliesslich die in Kapitel 1.2 erwähnten Dokumentversionen zu berücksichtigen sind.

Die Veröffentlichung einer späteren Version setzt eine Analyse durch das BAKOM und gegebenenenfalls eine Anpassung der Technischen und administrativen Vorschriften voraus. Diese könnte jedoch innerhalb einer kurzen Frist erfolgen, weil die Anpassung der TAV in der alleinigen Verantwortung des BAKOM liegt.

Eine andere Frage ist, inwieweit die Berücksichtigung einer neuen Version oder einer neuen Norm die auf der Grundlage der alten Referenz anerkannten Anbieter von Zertifizierungsdiensten betrifft. In diesem Fall obliegt es dem BAKOM, diese Änderungen in den Übergangsbestimmungen zu regeln und eine Anpassungsfrist zu setzen.

3.4 Kapitel 3.1, Grundsatz

Kapitel 3 bezieht sich weitgehend auf die Spezifikation ETSI TS 101 456. Dieses Dokument wird zurzeit überarbeitet und sollte im Laufe dieses Jahres fertig gestellt werden. Allerdings ist es wegen der Unklarheit betreffend den Umfang der Änderungen und das Datum der Veröffentlichung der neuen Version noch nicht möglich, diese Änderungen für das Inkrafttreten der Technischen und administrativen Vorschriften bereits zu referenzieren.

Das im Kapitel 3.1 zitierte Dokument *TTP.NL Guidance on ETSI TS 101 456* soll dem Leser der Spezifikation ETSI TS 101 456 zusätzliche Informationen liefern, um jegliche Auslegungsprobleme zu beseitigen. Im Laufe der Überarbeitung der Spezifikation ETSI TS 101 456 ist zudem vorgesehen, eine ETSI-Version dieses Dokuments auszuarbeiten. Die Anpassung dieser Referenz in den TAV hängt also auch in diesem Fall von der Entwicklung der Arbeiten des ETSI ab.

3.5 Kapitel 3.4.1, Format der Zertifikate

Um die Interoperabilität und insbesondere die Analyse des Zertifikats durch die Softwares zu ermöglichen, übernimmt dieses Kapitel den Inhalt der Spezifikation ETSI 101 862 Qualified Certificate Profile, mit Ausnahme der vom ZertES auferlegten Besonderheiten. So verlangt das ZertES, dass das Zertifikat die qualifizierte elektronische Signatur der Anbieterin von Zertifizierungsdiensten enthält, während eine fortgeschrittene elektronische Signatur im europäischen Kontext genügt. Es unterscheidet sich zudem dadurch, dass sie die Angabe verlangt, ob eine Anbieterin anerkannt ist oder nicht. Falls sie anerkannt ist, ist zudem der Name der Anerkennungsstelle anzugeben.

Das Kapitel verweist auf die neuen Versionen der RFC-Normen von Anfang 2004.

Die erste Spalte der Tabelle in Kapitel 3.4.3.1 der TAV listet die Anforderungen aus Artikel 7 ZertES auf. Die beiden anderen Spalten beschreiben die Mittel, die angewandt werden müssen, um den Inhalt des Zertifikats gemäss den gesetzlichen Anforderungen zu definieren.

Die Angabe, ob eine Anbieterin anerkannt ist oder nicht, und im ersteren Fall die Angabe des Namens der Anerkennungsstelle sind Informationen, die kommuniziert werden, indem die Namen der SAS, der Anerkennungsstelle und der Anbieterin von Zertifizierungsdiensten in der Erweiterung «issuerAltName» des Zertifikats angeben werden. Mit diesen Informationen ist aber die Anerkennung der Anbieterin von Zertifizierungsdiensten noch nicht garantiert. Zur Bestätigung sollte die Website der SAS konsultiert werden, auf der die Liste der anerkannten Anbieterinnen verfügbar ist.

Die Angabe, dass es sich um ein qualifiziertes Zertifikat handelt, und die Angabe betreffend den Wert der Transaktionen sind Informationen, die in Form einer Erklärung geliefert werden. Das Zertifikat enthält in Wirklichkeit einen Objektbezeichner der Erklärung (object identifier – OID), der im Dokument ETSI TS 101 862 definiert ist.

Die erwähnten Erklärungen basieren bewusst auf der Richtlinie 1999/93/EG des Europäischen Parlamentes und des Rates über einen gemeinschaftlichen Rahmen für die elektronischen Signaturen. Zwar ist diese Richtlinie für die Schweiz nicht bindend. Die Definition der neuen OID für nationale Erklärungen wäre zwar möglich, praktisch bestünde aber die Gefahr, dass solche generische Erklärungen von den Softwares nicht interpretiert werden könnte.

BAKOM/1.6.04