

Von TR-03125 über TR-VELS zu TR-ESOR

Dr. Ulrich Kampffmeyer
Agnieszka Wasniewski



PROJECT CONSULT
Unternehmensberatung
Dr. Ulrich Kampffmeyer GmbH

Hamburg, Oktober 2011

Von TR-03125 über TR-VELS zu TR-ESOR

Von Dr. Ulrich Kampffmeyer

Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH

Ulrich.Kampffmeyer@project-consult.com

Agnieszka Wasniewski

Redaktionsleiterin der PROJECT CONSULT Unternehmensberatung GmbH,

Agnieszka.Wasniewski@project-consult.com

Das BSI hat im Juli 2009 eine „Technische Richtlinie zur vertrauenswürdigen elektronischen Langzeitspeicherung (TR-VELS, TR-03125)“ vorgelegt. In der TR-VELS werden auf der Grundlage bestehender rechtlicher Normen und technischer Standards sowie nationaler und internationaler Erfahrungen, Anforderungen und Kriterien für die langfristige, beweissichere Aufbewahrung elektronischer Dokumente spezifiziert. Die Technische Richtlinie ist modular aufgebaut und kann der Seite des BSI heruntergeladen werden. Die TR-VELS hat etliche kritische Stimmen erhalten, woraufhin das BSI und der VOI vor der CeBIT 2010 in einer gemeinsamen Erklärung angekündigt haben, sowohl eine sprachliche, als auch eine technische Überarbeitung der TR 03125 durch zu führen. Der neue Titel der TR 03125 soll "Beweiswerterhaltung kryptographisch signierter Dokumente" lauten, kurz TR-ESOR¹. Diese Entwicklungen wurden in der XING Gruppe Information and Document Management² kontrovers diskutiert.

Was ist die TR-03125?

Die Technische Richtlinie 03125 des BSI beschreibt in einem differenzierten Katalog von verpflichtenden (Muss), von empfohlen (Soll) und auch von optionalen (Kann) Anforderungen im Hinblick auf alle Elemente und Bereiche, in denen ein Gestaltungsbedarf besteht, um für Behörden und Institutionen wirkungsvolle, zukunftssichere und wirtschaftliche technische Szenarien für eine vertrauenswürdige Langzeitarchivierung elektronischer Dokumente und Daten aufzubauen. Im Wesentlichen werden dabei empfohlene Dokumentenformate, ein empfohlenes Speicherformat für Archivdatenobjekte, Empfehlungen zu einer IT-Referenzarchitektur oder alternativen Architekturen, Anforderungen an Komponenten und an Module sowie deren Zusammenspiel behandelt. Auf der Basis des vorliegenden Anforderungskatalogs sollen nun, so das BSI, Anbieter und Produkthersteller zu dieser Richtlinie konforme Lösungsangebote entwickeln.

¹ https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/Kommentierung/Arbeitsergebnisse_140910.html

² <https://www.xing.com/net/informationlifecyclemangement/digital-preservation-332785/de-vertrauenswurdige-archivierung-nur-mit-elektronischer-signatur-26619628/35754787/#35754787>



Im Folgenden wird zunächst auf die Entwicklung der TR-VELS (Technische Richtlinie zur vertrauenswürdigen elektronischen Langzeitspeicherung) eingegangen, die eine branchenweite Diskussion im XING- Forum der Gruppe Information and Document Management gefunden hat. Nicht zuletzt durch diese Diskussion begründet, startete der BSI zusammen mit dem VOI (Verband Organisations- und Informationssysteme e.V) eine Revision der TR-VELS. Das Ergebnis dessen ist die TR-ESOR. Im weiteren Verlauf werden die Darstellung der Entwicklung und die Unterschiede zwischen beiden Richtlinien behandelt.

TR-VELS Vertrauenswürdige elektronische Langzeitspeicherung

Kritik an der TR-VELS / TR-03125

Im Nestor-Projekt entstanden das Handbuch zur vertrauenswürdigen Archivierung und der Kriterienkatalog vertrauenswürdige digitale Archive. Nun gibt das BSI seit Juli 2009 mit seiner technischen Richtlinie TR-03215 den Rahmen für ein Zertifizierungsverfahren vor und definiert technisch, was denn nun unter "vertrauenswürdig" zu verstehen sei und wer allein diese Vertrauenswürdigkeit bescheinigen darf. Erste Anbieter, wie z.B. Fujitsu / OpenLimit, haben bereits Lösungen nach dem dort beschriebenen Kriterien auf den Markt gebracht.

Die BSI TR 03125 / VELS Richtlinie fasste eine Reihe von Projektergebnissen zusammen, deren Nutzen für den praktischen Einsatz umstritten ist. Zu dem erhob die TR VELS den Anspruch, das einzige und erste Konzept für "rechtssichere", "vertrauenswürdige" und "beweissichere" Archivierung zu sein und zugleich auch die "revisionssichere Archivierung" einzuschließen. Diese TR sollte für Produktzertifizierungen genutzt werden. Nur zertifizierte Produkte hätten so den Anspruch gehabt "rechtssicher", "vertrauenswürdig" und "beweissicher" zu sein. Dies soll für alle Branchen und alle Arten von Anwendungen mit Archivierungsbedarf etabliert werden, wie aus Vorträgen, Artikeln, Presse und der TR-VELS selbst zu entnehmen ist. Das Dokument selbst war zu diesem Zeitpunkt in einem Zustand, der keine Normung erlaubte, weder vom Inhalt noch vom Anspruch. Es handelte sich um einen deutschen Sonderweg zur Förderung der qualifizierten elektronischen Signatur in einem Bereich, wo "schwach werdende" und "durch Nachsignieren abzusichernde" kryptische Anhängsel nichts verloren haben.

Von den Initiatoren der BSI TR VELS wurde eine Terminologie eingeführt, die das Verfahren nach TR VELS begrifflich in die Nähe der nestor-Initiative rückte. Der für Laien kaum wahrnehmbare Unterschied zwischen "Langzeitspeicherung" und "Langzeitarchivierung" in den Bezeichnungen machte dies deutlich. Wie die Webseiten, Vorträge, Artikel, Produktdatenblätter und andere Äußerungen zeigten, machen die Protagonisten selbst diesen Unterschied nicht.

Allerdings fragte man sich etwas, was denn nun Nestor mit dem BSI-Zertifizierungsverfahren zu tun hat?!



Die TR 03125 bietet das volle Arsenal der qualifizierten elektronischen Signatur³ auf - Archisafe, Krypto, ArchiSig usw. Positiv war der Versuch, für das OAIS - Modell nach ISO 14721 ein XAIP - Format zu definieren. Die TR 03125 macht sich auch die Mühe, revisionssicher, rechtssicher, beweissicher und langfristig abzugrenzen. Für rechtssicher und beweissicher bleibt jedoch nur die Archivierung mit elektronischer Signatur, in der Form, wie sie von BNetzA aus gegeben wird.

In der XING - Gruppe Information and Document Management⁴ wurde hierüber kontrovers diskutiert. Hieß das nun,

- dass alle elektronischen Archivsysteme, die nicht nach TR 03125 arbeiten, nicht rechtssicher oder beweissicher sind?
- dass man Systeme, die nicht der TR 03125 folgen, auch nicht in der öffentlichen Verwaltung einsetzen darf?
- dass hierdurch alle großen internationalen Anbieter, die nicht speziell etwas für den deutschen Archivierungsmarkt bauen wollen oder können vom Wettbewerb ausgeschlossen sind?
- dass alle bestehenden Archive in der öffentlichen Verwaltung in rechtssichere Archive mit elektronischer Signatur zu migrieren sind?
- dass auch Langzeitarchive im internationalen Umfeld, z.B. der "Trusted Archive Initiative" jetzt die qualifizierte elektronische Signatur deutscher Prägung mit Anbieterakkreditierung und Archisig-Verfahren einsetzen, um weiterhin ein trusted Archive zu haben?
- dass alle archivierten Dokumente ohne qualifizierte elektronische Signatur nicht rechtssicher sind?
- dass Verfahren wie LTANS/ERS obsolet sind?
- dass man elektronische Signaturen in historischen Archiven über die Lebenszeit (>300) aktuell halten muss, da ja sonst Authentizität und Integrität nicht nachweisbar sind?

Fragen über Fragen und die Hoffnung, in der Langzeitarchivierung käme man in einem vertrauenswürdigen Archiv bei einer vertrauenswürdigen Institution ohne den ganzen "Krypto-Signatur-Wasserzeichen-Nachsignieren-und-sonstigen-kaum-interpretierbaren-Zusatz-Schnickschanck-zum-eigentlichen-Informationsobjekt" aus schwindet.

³ <https://www.bsi.bund.de/cae/servlet/contentblob/798514/publi...>

⁴ <https://www.xing.com/net/informationlifecyclemanagement/digital-preservation-332785/de-vertrauenswuerdige-archivierung-nur-mit-elektronischer-signatur-26619628/35754787/#35754787>



Wofür war die elektronische Signatur noch einmal gedacht - zur Absicherung von Archiven? Zum Nachweis des vollständigen Einscannens von Dokumenten in Sozialversicherungen? Zur Absicherung elektronischer Rechnungen gegen Umsatzsteuer-Missbrauch? Oder gab es da noch einen anderen Zweck für die elektronische Signatur wie sie in der RLES für Europa im Jahr 1999 festgelegt worden war?

Durch die Zertifizierung nach TR-VELS würde für alle folgendes gelten: Rechtssichere und beweissichere elektronische Archivierung gibt es nur mit der qualifizierten elektronischen Signatur - zumindest in Deutschland. Dieses Zertifikat kann man sich dann auch auf die Produktpackungen der Software und der Hardware kleben - egal, was der Anwender in die Systeme hineintut, wie er die Lösungen betreibt und die Systeme nutzt.

Problematisch war besonders der "Anspruch" der TR-VELS. Natürlich gab es die meisten "Einzelteile" schon vorher, aber die TR-VELS kam mit einer Art "Alleinvertretungsanspruch" daher was "beweissicher", "rechtssicher" und "vertrauenswürdig" angeht.

Was soll jemand in der freien Wirtschaft tun, wenn ihm ein "beweissicheres", "rechtssicheres" und "vertrauenswürdiges" Archiv (als Appliance!) angeboten wird und er es mit anderen Archivsystemen vergleichen soll, die sich nicht mit der TR-03125 schmücken. Wofür wird man sich auf der Managementebenen entscheiden, wo es nicht mehr um die feinen Unterschiede bei Begriffen, Technik und Anwendungen ankommt? Da steht jetzt im Raum (siehe auch Broschüren und Präsentationen von Anbietern) es gibt die vom BSI abgesegnete "Rechtssicherheit" als Produkteigenschaft.

Störend ist hierbei, dass mit Hilfe des BSI Konzepte der elektronischen Signatur in die elektronische Archivierung übertragen werden, wo sie keinen Sinn machen: "Das Bundesamt für Sicherheit in der Informationstechnik schafft bei der elektronischen Archivierung Sicherheit für Hersteller und Anwender aus der öffentlichen Verwaltung und der Privatwirtschaft." Damit werden alle anderen Formen der Archivierung - diejenigen ohne die ausführlich behandelten Signaturkonzepte - als nicht-sicher und nicht-vertrauenswürdig deklassiert.

Kritik am Vorgehen des BSI und an der geplanten DIN-Umsetzung der TR-VELS

Im Forum der XING-Gruppe Information & Document Management wird die Diskussion seit einiger Zeit mit regem Interesse verfolgt. Mitdiskutanten, die gleichzeitig Mitglieder des VOI (Verband Organisations- und Informationssysteme e.V) sind verfassten einen offenen Brief⁵ des VOI an das BSI. Der Tenor der Stellungnahme war ablehnend mit der Bitte um Rücknahme der TR VELS und Beendigung der seit Dezember 2009 stattfindenden Außendarstellung mit Wirkung außerhalb der Bundesverwaltung. Die wesentlichen Gründe sind:

Mit der seit Dezember 2009 geführten öffentlichen Darstellung um die Sinnhaftigkeit und den Anwendungsbereich dieser Verfahren auch außerhalb der

⁵ <http://www.voi.de/downloads/?dlid=145>



Bundesverwaltung werden die bereits existierenden Lösungen am Markt diskreditiert, obwohl sich die Rechtsgrundlagen zur Aufbewahrung von Unterlagen für die Anwender nicht geändert haben. Für die Stellen der Bundesverwaltung mag das nun anders sein, da das BSI hier Regelungsbefugnis hat. Aber eben nur dort. Das BSI hat natürlich das Recht zu sagen, wir in der Bundesverwaltung haben wir andere Ansprüche an die Aufbewahrung und diese lauten so und so und das sind die Technischen Richtlinien, die den Rahmen zur Erfüllung dieser Ansprüche umsetzen. Es sollte aber bitte diese Umsetzung erst einmal im eigenen Bereich umsetzen und nicht mit aktiver Öffentlichkeitsarbeit den gesamten DMS-Markt mit einer Meinung überziehen, die ziemlich isoliert dasteht und wohl auch so entstanden ist. Weder der Branchenverband VOI mit seinen diversen Arbeitsgruppen und Competence Centern, auch nicht die marktführenden Hersteller wurden hier um Input gebeten.

Mit diesem Außenauftritt wird allen Anwendern suggeriert, dass nun etwas nicht mehr ordnungsgemäß ist, was vorher den geltenden regulatorischen Vorschriften entsprochen hat, obwohl sich keinerlei Rechtsvorschriften zur Aufbewahrung in irgendeiner Form geändert haben. Das ist entweder kühn oder unbedacht. Beides wäre nicht akzeptabel für ein "Bundesamt". Die öffentlich geäußerte Meinung des Bundesamtes für Sicherheit in der Informationstechnik hat Orientierungswirkung im gesamten Markt, auch wenn die Regelungsbefugnis faktisch nur einen sehr kleinen Bereich umschließt.

Man definiert damit einen neuen Maßstab für Vertrauenswürdigkeit bei der Aufbewahrung aufbewahrungspflichtiger Unterlagen, ohne das Kriterium "Langzeit" positiv oder negativ abzugrenzen. Das ist eine seltsame Kategorisierung. Es gibt doch keine Sorgfaltspflicht, deren Qualität sich nach der Dauer der Aufbewahrungsfrist richtet. Darf eine mittelfristige Aufbewahrung (was auch immer das sein soll) weniger sorgfältig sein, als die Langzeitaufbewahrung. Welcher Revisor sagt: Ja, ok, 95% ist ok, muss ja nur 10 Jahre aufbewahrt werden. Was ist denn das für eine seltsame Definition? Die Kategorisierung ist an keiner Stelle in Einklang zu bringen mit der Rechtswirklichkeit der Anwender. Es ist doch ganz einfach: Ein Beleg (Rechnung, Buchung, Vertragsurkunde), welcher vor 1 Sekunde entstanden ist, muss ebenso geschützt aufzubewahren wie ein Beleg, der 9 Jahre, 11 Monate und 30 Tage ist oder ein Beleg, der 30 Jahre alt ist. Es gibt keine gesetzliche Erleichterung, die sich aus dem Kriterium Aufbewahrungsfrist ableitet.

Gerade in Steuer- und Handelsrecht gibt es hier keine Unterschiede, und dieses kaufmännische Recht ist die für die meisten DMS-Anwender rahmengebende Rechtsgrundlage. Für eine nach Fristen definierte Abstufung sind die rechtlichen Grundlagen nicht vorhanden. Durch diese Semantik wirkt die TR VELS aber faktisch in der Außenwirkung für alle Belege in einem DMS. Der sprachliche Kunstgriff "wir meinen ja nur Langzeit" wirkt wie eine Ausflucht aus der Argumentationsnot, weil da Kriterium "Langzeit" a) keine Grundlage hat und b) die Absicht des BSI nach unten nicht abgrenzend definiert. Daher werden durch die Außendarstellung der TR VELS alle DMS/Archivlösungen tangiert, und eben nicht nur irgendwelche wenigen Ausnahmen.

Technische Kritik an der TR-VELS

Es gibt außer den oben genannten Kritikpunkten eine Reihe technischer Aspekte, die die TR VELS bei vielen Anwendern als Handlungsoption ausschließen.

Problematisch ist, dass es bei der TR-VELS fast ausschließlich um die Verankerung der elektronischen Signatur und des Nachsignierens in der Archivierung geht. Mit Absicht wurde von den Promotoren der BSI TR VELS eine Bezeichnung gewählt - Vertrauenswürdige elektronische Langzeitspeicherung - (in der TR 03125 selbst wird fast ausschließlich von Archivierung gesprochen), die das Signatur-orientierte Verfahren gezielt in die begriffliche Nähe der Vertrauenswürdigen elektronischen Langzeitarchivierung rückt.

Die qualifizierte elektronische, personengebundene Signatur kann gern bei den unterschiedlichsten Verfahren (Zitate) "als Sicherheit gegen Verfälschung", "Nachweis der Identität der unterzeichnenden Person", "Nachweis des Rechnungserstellers beim Signaturdienstleister", "Massensignaturverfahren beim Scannen" und "kryptographisch erzeugte Sicherheit" eingesetzt werden. Das Nachsignieren muss aber vom Tisch. Es verträgt sich grundsätzlich nicht mit der Archivierung - egal bei einer Aufbewahrungsfrist von 10 Minuten, einer Woche, 10 Jahren, 300 Jahren oder ewig. Wenn die Signatur beim Eingang geprüft wurde und das Objekt dann sofort in ein revisionssicheres Archiv geht, muss dies reichen!

Das Nachsignieren ist eine ständige Manipulation des Archives und widerspricht dem Langzeit-Gedanken! Es ist nicht davon auszugehen, dass über den Zeitraum der Langzeitspeicherung (bis zu 100 Jahre) die verwendeten Technologien gleich bleiben. Dennoch sollen auf dieser Basis Produkte vom BSI als rechtssicher zertifiziert werden

Das Thema Übersignieren als dt. Besonderheit verwundert wohl die meisten Archiv-Anbieter. Ergänzend bleibt zu sagen, dass die meisten Dokumente ja keine Schriftform erfordern und entsprechend so oder so nicht signiert sind (Scannen nach SGB ausgenommen). Sie müssen aber dennoch revisionssicher aufbewahrt werden (ohne hier eine Begriffsdiskussion zu eröffnen, siehe dazu u.a. PROJECT CONSULT Newsletter vom 21.10.2009). Wenn also die Notwendigkeit der Revisionssicherheit existiert und das Archiv beim Kunden als revisionssicher betrachtet wird, gilt diese Eigenschaft nun mal notwendigerweise auch für die Signaturen. Und für signierte Rechnungen ist ein Übersignieren ja bereits obsolet.

WORM-Eigenschaft vs. Nachweis der Unveränderbarkeit

Diese beiden Eigenschaften werden nicht klar voneinander getrennt. Zum einen die "WORM-Eigenschaft" eines Speichersystems (wie auch immer sie hergestellt wird), die eine Veränderung der Daten ausschließt und auch das Löschen unter besonderen Schutz stellt. Es lässt sich weder durch Hash-Werte alleine noch qual. Zeitstempel erreichen, dass im SAN abgelegte Dokumente beliebig manipuliert werden können und auch beliebig (meist versehentlich) gelöscht werden können. Außerdem kann der qual. Zeitstempel ebenfalls gelöscht werden. Dies bedeutet nicht, dass man immer ein WORM-Speicher benötigt. Aber SAN + qual. Zeitstempel



alleine reichen nicht, ohne Verfahrensdokumentation geht hier auch nichts! Zum anderen, der Nachweis der Unveränderbarkeit:

Hier helfen qual. Zeitstempel sicherlich - wobei sie NICHT in der ZPO verankert sind (außer in §17 SigV ist deren Anwendung nicht gesetzlich verankert), so dass man dem Landrichter immer noch erklären muss, dass diese Zeitstempel unheimlich sicher sind, in der Hoffnung, dass man dem Landrichter nicht noch die ERS klären muss, da der Zeitstempel zwischenzeitlich übersigniert werden musste.

Im Positivfall, wenn das Dokument also nicht manipuliert wurde, kann man hiermit den Nachweis erbringen, dass es seit Zeitpunkt x unverändert vorliegt. Wie bereits bemerkt, reichen QES hierfür nicht (die kann man auf der Fahrt zum Gericht noch erzeugen). Ohne einen qual. Zeitstempel muss man sich aber wohl auch keine Sorgen machen. Hierfür ist ja gerade die Verfahrensdokumentation gedacht oder die pragmatische Vorgehensweise, dass beide Parteien vor Gericht Ihre Dokumente in Anschein.

Alles Gesagte wird obsolet, wenn der Prozess bis ins Archiv "unsicher" ist. Ergo: auch hier ist trotz BSI TR 03125 wieder Verfahrensdokumentation notwendig. Ein wesentlicher Einwand gilt insb. in Bezug auf die oft zu finden Behörden-Sichtweisen, zunächst im Rahmen der Vorgangsbearbeitung die Dokumente in einem DOMEA-konformen System oder aber auch in Fachanwendungen zu halten und erst mit der z.D.A. Verfügung zu archivieren und die Anforderungen gemäß BSI TR 03125 anzulegen).

TR-VELS sollte sogar eine DIN-Norm werden!

Am 29.01.2010 erschien ein "Aufruf zur Beteiligung am Normungsprojekt des Arbeitskreises "Rechtsichere Aufbewahrung von digital signierten Dokumenten"⁶:

„Der Arbeitskreis " Rechtsichere Aufbewahrung von digital signierten Dokumenten" im NABD 15 "Schriftgutverwaltung und Langzeitverfügbarkeit digitaler Informationsobjekte" hat sich zum Ziel gesetzt, die TR-VELS in eine Norm zu überführen. Die Erarbeitung der geplanten Norm soll auf einer möglichst soliden Basis erfolgen, die die Anforderungen aller Interessierten Kreise berücksichtigt.

Um das Thema "Vertrauenswürdige elektronische Langzeitspeicherung" angemessen bearbeiten zu können ruft der NABD alle interessierten Unternehmen, Behörden, Hochschulen oder sonstigen Organisationen auf, an dem genannten Thema mit ihrem technischen Sachverstand mitzuarbeiten.“

In der DIN arbeitet schon seit längerem eine Gruppe an zwei Normentwürfen für die "vertrauenswürdige elektronische Langzeitarchivierung" und die "vertrauenswürdige elektronische Langzeitspeicherung". Der Aufruf der DIN zur Mitarbeit kann nicht das Ziel sein, einige "technische Unpässlichkeiten" aus der BSI TR-VELS "glatt zu bügeln". Ziel muss sein, generell zu verhindern, dass sich ein solches Konzept als der Standard für die elektronische Archivierung in Deutschland etabliert.

⁶ <http://indi.langzeitarchivierung.de/aktuell/>



Das BSI ist nicht der eigentliche Adressat der Kritik solange die BSI TR 03125 kein Standard ist. Dies würde sich ändern, wenn das Dokument als DIN Norm veröffentlicht wird! Dann gilt es nicht nur für die Bundesverwaltung sondern ist der Maßstab für sichere elektronische Archivierung generell. Selbst bei "Überarbeitung" und "Diskussion" würde sich die elektronische Archivierung mit qualifizierter elektronischer Signatur als entscheidendem Kriterium für die Qualität ("Rechtssicher", "Beweissicher", Vertrauenswürdig", "Revisionssicher") durchsetzen. Während heute nur in einigen speziellen Bereichen (z.B. Sozialversicherungen) und Fachanwendungen (z.B. elektronisches Standesamt) die elektronische Signatur bei der Archivierung ("100 Jahre Langzeitspeicherung" IST de facto Archivierung) in Deutschland verbreiten, würde eine DIN Norm Beachtung in allen Branchen finden (müssen). Wir kennen dies zur Genüge - aus der DIN Norm und der BSI TR-VELS wird dann sehr schnell wieder ein einfach gesetztes KO-Kriterium in Ausschreibungen - es ist ja der Standard, ob es nun Sinn macht oder nicht..

Der DIN tut sich keinen Gefallen, die BSI Richtlinie in eine Norm umzusetzen und sie damit auf eine Anerkennungsstufe wie die Vertrauenswürdige elektronische Langzeitarchivierung zu heben und für alle Branchen als Messlatte zu etablieren. Die Norm soll die Anerkennung der VELS "psychologisch" untermauern und den Geltungsbereich von der öffentlichen Verwaltung in die Privatwirtschaft erweitern. Der DIN darf sich hier nicht instrumentalisieren lassen. Die Normierungsbestrebungen für die TR VELS sollten einfach eingestellt werden. Die Bundesbehörden - oder gegebenenfalls die gesamte öffentliche Verwaltung - können auch ohne eine Deutsche Industrie Norm auskommen.

Es gibt viele Argumente, warum der DIN Ausschuss NABD 15 AK 6 Arbeitskreis „Rechtssichere Aufbewahrung von digital signierten Dokumenten“ die BSI Technische Richtlinie TR-VELS „Vertrauenswürdige elektronische Langzeitspeicherung“ nicht in eine DIN Norm überführen sollte. Technische Argumente, die auf Fehler und Unzulänglichkeiten im BSI Dokument verweisen. Rechtsbegriffliche Gründe, die den Anspruch der „Rechtssicherheit“ und der „Beweissicherheit“ kritisieren. Marktordnende Gründe, die den Anspruch, dass nur Archivsysteme nach BSI TR-VELS „vertrauenswürdig“, „rechtssicher“ und „beweissicher“ seien – und alle anderen nicht – ablehnen. Prinzipielle Eigenschaften der elektronischen Archivierung, die das Nachsignieren nicht nur überflüssig sondern als grundsätzliche Beeinträchtigung des Wertes archivierter Dokumente auffassen. Und es gibt „politische Gründe“ wie z.B. die Ausdehnung des Geltungsbereiches der BSI TR-VELS auf alle Organisationen, Betriebe und Verwaltungen durch die Fassung in eine DIN Norm.

Bei den politischen Begründungen wurde jedoch ein wichtiges Argument bisher wenig beachtet. Eine DIN Norm zum Nachsignieren auf Basis der Qualifizierten elektronischen Signatur (QES) deutscher Prägung stellt einen deutschen Sonderweg dar. Besonders da sie das Root-Zertifikat der BNA Bundesnetzagentur verlangt und die kartengebundene QES mit ihren Besonderheiten international nicht verbreitet ist. Eine solche DIN Norm hätte nie die Chance in eine europäische oder gar internationale ISO Norm zu münden. Dieser nationale Sonderweg passt jedoch in die generelle Strategie des DIN Deutsches Institut für Normung, auch wenn der Anteil



nationaler Normen in Europa bei ca. nur 10% liegt und die meisten Vorhaben sich mit der Umsetzung internationaler Normen beschäftigen.

Die europäische Kommission will die Normung zentralisieren. Sie sieht europaweit geltende Normen als wesentlichen Faktor für die Schaffung eines europäischen Wirtschaftsraumes an. Gerade für mittelständische Unternehmen sollen Hürden im internationalen Handel durch einheitliche internationale Normen abgebaut werden. Dies soll zur Reduzierung von Aufwänden bei der Erstellung von Produkten führen. Nationale Normungsinstitutionen würden dadurch nicht nur an Bedeutung verlieren sondern mittelfristig gänzlich entfallen. Der Widerstand gegen diesen zentralistischen Vorstoß der Europäischen Kommission ist unterschiedlich stark. Dies hängt auch mit der Organisationsform der Normungsinstitutionen zusammen. Während zum Beispiel in Spanien und England die Normung privatwirtschaftlich organisiert ist wurde sie in Frankreich unter staatlicher Hoheit betrieben. In Deutschland wendet sich der DIN massiv gegen den zentralisierten europäischen Ansatz und verweist auf das erfolgreiche Konzept mit Tausenden von freiwilligen Fachleuten sehr effektiv und kostengünstig zu arbeiten. Und das es natürlich neben den internationalen Normen natürlich auch weiterhin nationaler Normen bedarf. Hier wird jedes nationale Norm und jedes nationale Normungsvorhaben natürlich argumentativ besonders gehätschelt und gepflegt, um eine möglichst große Zahl wichtiger nationaler Standards vorweisen zu können und damit die Bedeutung der nationalen Normung zu stärken. Ähnlich sieht das auch der BDI, der Bundesverband der deutschen Industrie. Sonst bleibt für nationale Normungsorganisationen lediglich eine reine Übersetzertätigkeit europäischer und internationaler Normen übrig.

Und genau hier kommt – neben anderen – auch das Normungsvorhaben für das Nachsignieren ins Spiel. Mit der Umsetzung der BSI TR VELS wird ein rein nationales Normungsprojekt betrieben (auch wenn die Signatur-Fraktion meint, dass am deutschen Signatur-Wesen die Welt genesen soll). So hat der DIN auch aus europapolitischen Gründen kein Interesse, die Normung der BSI Vorlage einzustellen. Vielmehr wird das Gremium sich zusammenfinden (heute am 21.04.2010 bei der PTB in Braunschweig) um die Schritte für die weitere Arbeit zu definieren, die Felder festlegen, wo Verbesserungen der BSI TR VELS notwendig sind, und sich in die Gremienarbeit stürzen. Allenfalls wird man sich auf eine Vertagung einigen, aber abblasen wird man das Vorhaben nicht.

Die elektronische Signatur ist in vielen Anwendungsgebieten sehr sinnvoll und notwendig. Dies betrifft besonders die Bereiche der Kommunikation, E-Commerce und E-Business wie auch den Bereich elektronischer Urkunden bei Entstehung, Versand und Empfang. Auch lassen sich „ab gelegenerere“ Anwendungen wie beim Scannen noch gerade akzeptieren, um weitere, zusätzliche Anwendungsmöglichkeiten für die Signaturkarten zu schaffen. Jedoch ist das Nachsignieren zum vermeintlichen „Beweiswerterhalt“ nicht nur sinn frei und unnötig sondern auch für die Akzeptanz der Signatur schädlich. Das Nachsignieren hat nichts in der elektronischen Archivierung verloren! Was technisch machbar ist muss nicht unbedingt gemacht werden. Wo es in der elektronischen Welt durch die Nutzung von Software um Verbesserungen und Erleichterungen geht, dürfen nicht noch weitere künstliche Hürden aufgebaut werden. Im Interesse der Wirtschaft



müssen nationale Sonderwege verhindert werden. Dies zeigen auch die zukünftige Handhabung der elektronischen Rechnung, wie sie von der Europäischen Kommission initiiert wurde, und Initiativen zur Abschaffung der elektronischen Signatur bei elektronischen Rechnungen mit kleineren Beträgen. Im Zuge dieser Entwicklungen darf es keine Normen wie die geplante DIN 31647 geben, denn sie baut neue Hürden auf ohne einen Nutzen zu bringen. Und dieses DIN Vorhaben darf nicht einfach nur zu einem Spielstein im Überlebenskampf des DIN angesichts der europäischen Initiative zur Zentralisierung der Normung werden!

Trotz Gespräch mit dem VOI sind die Dokumente, die Vorträge, die Artikel, die Texte weiterhin im Internet. Man begibt sich nun in die Gremienarbeit zur Verbesserung der TR 03125. Es geht also nur um Bereinigung der Unstimmigkeiten, etwas psychologische Kosmetik beim Geltungsbereich und die Rückendeckung durch den Verband und ECM-Branche ... es haben dann ja alle an der TR VELS mitgearbeitet.

Wie sieht es denn nun bei der DIN-Normung aus? Die Umsetzung der BSI TR 03125 in eine DIN Norm wurde nicht von der Tagesordnung genommen. Der zuständige DIN Arbeitskreis NABD 15 AK 6 "Arbeitskreis Rechtssichere Aufbewahrung von digital signierten Dokumenten" traf sich am 21.04.2010 in Braunschweig bei der Physikalisch-Technische Bundesanstalt (PTB) (wir erinnern uns ... das waren doch die Verfasser von ArchiSafe und einer der Verfechter des Nachsignierens?!). Mal sehen, welche Richtung das Vorhaben nun nimmt.

Und dann ist da noch § 17 SigV. Einige Länderdatenzentralen wollen sich gegen das vom BSI mit der TR VELS vorgeschlagene Verfahren positionieren wollen, und dass man im zuständigen Ministerium BMWi eine Änderung bewirken will. Es tut sich also an einigen Stellen etwas zum Thema § 17, man weiß aber nicht wie viel, in welche Richtung und durch wen. Die von mir eingeforderte Transparenz und Öffentlichkeit der Diskussion beginnt sich in die geschlossenen Gremien zu verziehen.

Das Ergebnis der Diskussion um die TR-VELS

Die Sprachregelung passte sich an. Man spricht inzwischen von Beweiswerterhaltung. "Vertrauenswürdig", "Rechtssicher" und "Langzeitspeicherung" sind nicht mehr so "in" wie früher. Dementsprechend hat sich auch die DIN-Gruppe passender umbenannt.

Inzwischen wurde im stillen Kämmerlein an der Neufassung der TR VELS / 03125 gewerkelt. Denn - einmal veröffentlichte "Technische Richtlinien" werden vom BSI grundsätzlich nicht zurückgezogen. Also wird es eine modifizierte, dann von Verbänden wie dem VOI mitgetragene und mit zu verantwortende, neue Version geben. Diese wird dann auch die Grundlage für den erneuten Anlauf der DIN sein.

Das Kürzel TR-VELS ist vom Tisch, dafür heißt es jetzt TR-ESOR. Das Umfeld ist geblieben, auch wenn der Anspruch deutlich zurückgefahren wurde. Es soll auf Basis der TR-ESOR auch wieder Produktzertifizierungen geben und auch soll das Ganze wieder in den DIN eingebracht werden.



Was ist nun aus der BSI TR 03125 geworden? Die Richtlinie wurde überarbeitet, aber das ursprüngliche Dokument findet sich immer noch im Netz⁷. Der DIN wartet mit der Normung des BSI-Vorstoßes und die Branchenverbände reden und schreiben sogar vielleicht mit. Das BSI muss ebenfalls das Gesicht wahren und so wird nur marginal geändert und der Fokus angepasst. Generell ist auch die elektronische Signatur in der Diskussion, siehe z.B. die elektronische Rechnung andererseits aber auch die Signatur beim ePA, im elektronischen Standesamt, bei der Entsorgung usw. Viele sind der Meinung, das Nachsignieren zum "Beweiswerterhalt" sei unnötig. Die Signaturbranche lässt sich nicht einfach ihr Geschäftsmodell kaputt machen und setzt weiterhin auf die qualifizierte Signatur in nur allen denkbaren Varianten der Einsatzgebiete.

TR-ESOR Richtlinie zur Beweiswerterhaltung kryptographisch signierter Dokumente

Wesentliche Ziele der TR-ESOR

Wie auch schon die Vorgängerversion TR-VELS besteht die TR-ESOR (aktuell BSI TR-03125 Version 1.1) aus einem Hauptdokument und einer Vielzahl von Anhängen:

Technische Richtlinie # BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente (PDF, 1,37 MB)

1) Module:

Anlage TR-ESOR-M.1: ArchiSafe-Modul (PDF, 589,09 KB)

Anlage TR-ESOR-M.2: Krypto-Modul (PDF, 673,5 KB)

Anlage TR-ESOR-M.3: ArchiSig-Modul (PDF, 903,88 KB)

2) Schnittstellen

Anlage TR-ESOR-S: Schnittstellenspezifikation (PDF, 1,46 MB)

Anlage TR-ESOR-E: Konkretisierung der Schnittstellen auf Basis des eCard-API-Framework (PDF, 997,56 KB)

Anlage TR-ESOR-F: Formate und Protokolle (PDF, 3,08 MB)

In Punkto Anlagen hat sich thematisch und inhaltlich erwartungsgemäß wenig getan.

⁷ https://www.bsi.bund.de/ContentBSI/Presse/Kurzmitteilungen/Kurzmit2009/TRVELS_041209.html



Der wesentliche Fokus liegt auf der Nachsignatur kryptografisch signierter Objekte. Die Formulierungen der früheren Version konnten als Universalarchivanspruch für alle Branchen und jede Art der ordnungsgemäßen Aufbewahrung missverstanden werden. Dieser Punkt ist mit der neuen Version nun abschließend klargestellt.

- Das Einsatzfeld der TR 03125 ist dann gegeben, wenn eine gesetzliche Notwendigkeit oder der freiwillige Wunsch zur Nachsignatur besteht. Für die meisten Anwendungsfälle elektronischer Dokumente im DMS-Markt in Deutschland dürfte die TR-ESOR allerdings keine Anwendung finden, da diese Dokumente entweder nicht initial signiert werden müssen oder keine Nachsignatur erforderlich ist, obwohl sie initial signiert wurden.
- Vornehmlicher Anwendungsbereich der vorliegenden Technischen Richtlinie sind die Bundesbehörden im Rahmen der gesetzlichen Aufbewahrungspflichten. Andere Unternehmen können frei entscheiden, ob sie diese Spezifikation oder andere Verfahren einsetzen, solange die gesetzlichen Anforderungen eingehalten werden.



Module du Anlagen

Vergleich TR-ESOR und TR-VELS - BSI Technische Richtlinie 03125

TR-ESOR – Beweiswerterhaltung kryptographisch signierter Dokumente, Version 1.1, 18.02.2011	TR-VELS – Vertrauenswürdige Elektronische Langzeitspeicherung, Version 1.0, 31.07.2009
Module	
Anlage TR-ESOR-M.1 ArchiSafe-Modul, 18.02.2011	Anlage TR-VELS-M.1 ArchiSafe-Modul , 31.07.2009
Anlage TR-ESOR-M.2 Krypto-Modul, 18.02.2011	Anlage TR-VELS- M.2 Krypto-Modul, 31.07.2009
Anlage TR-ESOR-M.3 ArchiSig-Modul, 18.02.2011	Anlage TR-VELS-M.3 ArchiSig-Modul, 31.07.2009
Anlagen	
	Anlage TR-VELS-M.4 Langzeitspeicher (in Vorbereitung)
	Anlage TR-VELS-M.5 XML-Adapter zur Anbindung von Geschäfts- Anwendungen an das Archiv (in Vorbereitung)
	Anlage TR-VELS-S.1 Schnittstelle zwischen Krypto-Modul und ArchiSafe, 31.07.2009
	Anlage TR-VELS-S.2 Schnittstelle zwischen ArchiSig und Langzeitspeicher, 31.07.2009
Anlage TR-ESOR-S Definition der Schnittstellen der Referenzarchitektur, 18.02.2011	Anlage TR-VELS-S.3 Schnittstelle zwischen Krypto-Modul und ArchiSig, 31.07.2009
	Anlage TR-VELS-S.4 Schnittstelle zwischen dem XML-Adapter und ArchiSafe, 31.07.2009
	Anlage TR-VELS-S.5 Schnittstelle zwischen ArchiSafe und dem Langzeitspeicher, in Vorbereitung
	Anlage TR-VELS-S.6

Von TR-03125 über TR-VELS zu TR-ESOR



	Schnittstelle zwischen ArchiSafe und ArchiSig, 31.07.2009
Anlage TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, 18.02.2011	Anlage TR-VELS-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks, 31.07.2009
Anlage TR-ESOR-F Formate und Protokolle, 18.02.2011	Anlage TR-VELS-F Formate und Protokolle, 31.07.2009

Inhalte

Vergleich TR-ESOR und TR-VELS - BSI Technische Richtlinie 03125

TR-ESOR – Beweiserhaltung kryptographisch signierter Dokumente Version 1.1, 18.02.2011	TR-VELS – Vertrauenswürdige Elektronische Langzeitspeicherung, Version 1.0, 31.07.2009
Inhalte	
1. Vorbemerkungen	1. Einführung
1.1 Titel	2. Übersicht
1.2 Kennzeichnung	3. Funktionale Anforderungen an die Schnittstelle
1.3 Fachlich zuständige Stelle	4. Definition der Schnittstelle
1.4 Versionsverwaltung	4.1 VerifyRequest
1.5 Änderungsdienst / Fortschreibung	4.1.1 version
	4.1.2 requestData
2. Anwendungsbereich	4.1.3 requestControls
3. Allgemeines und Übersicht	4.2 VerifyResponse
3.1 Aufbau und Inhalte der Technischen Richtlinie	4.2.1 version
3.2 Untersuchungsgegenstand und Begriffsdefinitionen	4.2.2 status
3.3 Übersicht	4.2.3 responseData
4. Allgemeine Anforderungen an eine beweiserhaltende Aufbewahrung	4.2.4 responseControls
4.1 Bundesarchivgesetz und Landesarchivgesetze	4.3 SignRequest
4.2 Rechtliche Rahmenbedingungen	4.3.1 version
4.2.1 Deutsches Signaturrecht	4.3.2 requestData
4.2.2 Europäische Signaturrechtlinie	4.3.3 requestControls
4.2.3 Sarbanes-Oxley-Act (SOX)	4.4 SignResponse
4.2.4 Naibutousei - SOX auf Japanisch	4.4.1 version
4.3 Funktionale Anforderungen an die Beweiserhaltung kryptographisch signierter Dokumente	4.4.2 status
4.3.1 Nachweis von Integrität und Authentizität	4.4.3 responseData
5. Funktionen einer Middleware zum Beweiserhalt	4.4.4 responseControls
5.1 Anwendungsfälle	5. Sicherheitstechnische Anforderungen an die



	Schnittstelle
5.1.1 Archivierung signierter und unsignierter Daten	
5.1.2 Ändern von bereits archivierten Daten	
5.1.3 Abruf (Rückgabe) archivierter Daten	
5.1.4 Abruf von Beweisdaten	
5.1.5 Löschen archivierter Daten	
5.2 Organisatorische Anforderungen	
5.2.1 Die Einrichtung der Middleware zum Beweiswerterhalt	
5.2.2 Anforderungen an die Einsatzumgebung	
5.2.3 Datenschutz, Datensicherheit und Vertraulichkeit	
6. Abgeleitete technische Anforderungen	
6.1 Systemtechnische Anforderungen	
6.2 Empfohlene Dokumentformate	
6.3 Empfohlene Speicherformate	
6.4 IT-Infrastruktur	
6.5 IT-Anwendungen beim Einsatz von Archivierungsverfahren	
7. IT-Architektur	
7.1 Empfohlene IT-Referenzarchitektur	
7.2 Alternative Architekturen	
7.3 Komponenten und Module	
7.3.1 ArchiSafe-Modul (TR-ESOR-M.1)	
7.3.2 Krypto-Modul (TR-ESOR-M.2)	
7.3.3 ArchiSig-Modul (TR-ESOR-M.3)	
7.3.4 XML-Adapter zur Anbindung von Geschäftsanwendungen an die Middleware	
7.3.5 Die Kommunikationskanäle und Schnittstellen	
7.4 Zusammenspiel der Komponenten	
7.4.1 Ablage elektronischer Unterlagen	
7.4.2 Ändern archivierter Daten	
7.4.3 Abfrage archivierter Daten	
7.4.4 Rückgabe technischer Beweisdaten	
7.4.5 Löschen von Archivdaten	
8. IT-Sicherheitskonzept	



8.1 Sicherheitsziele	
8.2 Maßnahmen	
8.2.1 Übergreifende Maßnahmen	
8.2.2 Maßnahmen zum Schutz der Vertraulichkeit	
8.2.3 Maßnahmen zum Schutz der Authentizität, Integrität und Verbindlichkeit	
8.2.4 Maßnahmen zum Schutz der Verfügbarkeit	
8.2.5 Maßnahmen zur Autorisierung (Vertraulichkeit, Integrität)	
9. Konformität und Interoperabilität	
9.1 Konformität und Konformitätsprüfung	
9.2 Beteiligte Instanzen bei der Konformitätsprüfung	
9.2.1 Antragsteller	
9.2.2 Prüfgegenstand	
9.2.3 Prüfstelle	
9.2.4 Bestätigungsstelle	
9.3 Abwicklung der Konformitätsprüfung	
9.3.1 Vorphase	
9.3.2 Durchführung der Konformitätsprüfung	
9.3.3 Konformitätsbestätigung	
9.4 Interoperabilität	
10. Anlagen	
10.1 TR-ESOR-M.1 ArchiSafe-Modul	
10.2 TR-ESOR-M.2 Krypto-Modul	
10.3 TR-ESOR-M.3 ArchiSig-Modul	
10.4 TR-ESOR-S Schnittstellen	
10.5 TR-ESOR-F Formate und Protokolle	
10.6 TR-ESOR-E Konkretisierung der Schnittstellen auf Basis des eCard-API-Frameworks	
11. Abkürzungsverzeichnis	
12. Glossar	
13. Quellenverzeichnis	



Anschrift des Autors

PROJECT CONSULT GmbH, Büro Hamburg
Breitenfelder Str. 17
D-20251 Hamburg
Tel.: 040 / 460 762 20
Fax: 040 / 460 762 29
E-Mail: Presse@PROJECT-CONSULT.com
Web: www.PROJECT-CONSULT.com

Autorenrecht und CopyRight

Autor: Dr. Ulrich Kampffmeyer
PROJECT CONSULT Unternehmensberatung GmbH
Breitenfelder Str. 17
D-20251 Hamburg
Tel.: 040 / 460 762 20
Fax: 040 / 460 762 29
E-Mail: Presse@PROJECT-CONSULT.com
Web: www.PROJECT-CONSULT.com

© PROJECT CONSULT Unternehmensberatung GmbH 2011. Alle Rechte vorbehalten

Der gesamte Inhalt ist, sofern nicht gesondert zitiert, ein Originaltext des Autors. Jeglicher Abdruck, auch auszugsweise oder als Zitat in anderen Veröffentlichungen, ist durch den Autor vorab zu genehmigen. Die Verwendung von Texten, Textteilen, grafischen oder bildlichen Elementen ohne Kenntlichmachung der Autorenschaft ist ein Verstoß gegen geltendes Urheberrecht. Belegexemplare, auch bei auszugsweiser Veröffentlichung oder Zitierung, sind unaufgefordert einzureichen.