VOI e.V. - Postfach 140 231 - 53057 Bonn

An den Präsidenten des
Bundesamtes für Sicherheit in der Informationstechnik
Herrn Michael Hange
Godesberger Allee 185 - 189

53175 Bonn

VOI - Verband Organisations-
und Informationssysteme e.V.
Postfach 140 231
53057 Bonn

Tel.: 0228 - 9 08 20 89
Fax: 0228 - 9 08 20 91
E-Mail: b.zoeller@voi.de
www.voi.de

26. Januar 2010

Offener Brief an das BSI zu TR 03125 (TR VELS)

Sehr geehrter Herr Hange,

der Verband Organisations- und Informationssysteme e.V. (VOI) ist mit 230 Mitgliedern der führende Fachverband der DMS/ECM-Industrie im deutschsprachigen Raum. Assoziationen mit internationalen Verbänden - z.B. AIIM, Aproged (Frankreich) - stellen den Know-how-Austausch auf internationaler Ebene her und verhindern die Ausprägung international nicht transportierbarer Interpretationen zu Kernthemen wie Rechtsgrundlagen, Speichertechnologien etc. Der VOI und seine Mitgliedsfirmen sind vernetzt in nationalen Gremien der Bundesrepublik Deutschland wie AWV, IDW, Bitkom und anderen Organisationen, in denen die relevanten Interpretationen der regulatorischen Anforderungen bezüglich der gesetzeskonformen Aufbewahrung elektronischer Unterlagen erarbeitet werden.

Mitglieder wie Canon, Docuware, EASY, ELO, EMC, IBM, Kodak, Microsoft, Open Text, SAPERION, Windream und viele andere bieten zum Teil seit über 25 Jahren Systeme zur revisionssicheren elektronischen Aufbewahrung an. Tausende dieser Systeme sind bei Anwendern in Deutschland quer über alle Branchen zur Aufbewahrung und Verwaltung von kaufmännischen und operativen Dokumenten und Unterlagen in Betrieb und von Wirtschaftsprüfern, Finanzverwaltungen, Prüfverbänden und anderen Organisationen mit Regelungs- und Sanktionsbefugnis als regelkonforme Infrastrukturkomponenten der IT-Landschaft akzeptiert und abgenommen. Diese Systeme sorgen dort nicht nur für einen effizienteren Ablauf der dokumentbasierten Geschäftsprozesse, sondern auch – dies ist seit Bestehen des Marktes eine Kernfunktion solcher Lösungen - für die rechtskonforme Aufbewahrung sowohl nach Steuer- und Handelsrecht als auch nach anderen Rechtsvorschriften, die nicht selten eine Aufbewahrung über mehrere Jahrzehnte erfordern (wie zum Beispiel Lebensversicherungen, Dokumente aus dem Anlagebau, alle Arten Vertragsunterlagen mit langer und manchmal unbestimmter Laufzeit etc.).

Diese seit über einem Vierteljahrhundert (die ersten Systeme wurden in Deutschland bereits 1983 installiert) vorhandene Akzeptanz durch Finanzverwaltung,

Wirtschaftsprüfer u.a. basiert nicht etwa auf willkürlichen Einzelfallabwägungen, sondern auf allgemein bekannten Rechtsgrundsätzen und Interpretationen der gesetzlichen Vorschriften, die im Auftrag des deutschen Gesetzgebers und der Wirtschaftsverbände erlassen wurden, so etwa nachzulesen in der GOBS von 1995[1], in der demnächst erscheinenden GOBIT[2] (Nachfolger der GOBS, an deren Erstellung Mitgliedsfirmen des VOI mitgearbeitet haben), in den Interpretationen des Fachausschusses für Informationstechnik des Instituts der deutschen Wirtschaftsprüfer (insbesondere IDW FAIT 3[3]), sowie vielen anderen ergänzenden Erläuterungen und Interpretationen der gesetzlichen Aufbewahrungspflichten für elektronische Unterlagen.

Der VOI-Vorstand wurde Ende Dezember 2009 auf die in der Öffentlichkeit sehr kontrovers geführte Diskussion zur BSI TR 03125 aufmerksam und hat nach erster Sichtung und Bewertung eine Arbeitsgruppe[4] benannt. Das vorliegende Schreiben wurde von dieser Arbeitsgruppe unter Leitung von Oliver Berndt (Leiter des VOI Competence Center Elektronische Signaturen) und Bernhard Zöller (stellvertretender Vorstandsvorsitzender des VOI), im Auftrag des VOI Vorstands erstellt. Wir haben die TR VELS mit folgendem Ergebnis genauer analysiert und kommen zu folgender Wertung:

Die TR VELS vermittelt den Eindruck, dass sie erstmalig ein Lösungsmodell zur rechtssicheren, dauerhaften Aufbewahrung elektronischer Unterlagen anbietet, was für uns als Branchenverband in einer 25jährigen Industrie nicht nachvollziehbar ist. Außerdem weist die TR VELS eine Reihe inhaltlicher Mängel auf (einige Details im vorliegenden Dokument). Aus unserer Sicht besteht daher dringender Änderungsbedarf, denn die TR VELS

- diskreditiert Zehntausende installierter Lösungen und das Produkt- und Lösungsangebot der deutschen und internationalen Anbieter,

- ist technisch fehlerhaft und berücksichtigt keine nicht-technischen Kriterien, wie zum Beispiel die geforderte Ordnungsmäßigkeit des Gesamtverfahrens.

Diskussions- und Handlungsbedarf sehen wir vor allem in den folgenden Punkten, die wir z.T. im Rest des Briefes weiter detaillieren, die aber einer ausführlicheren Diskussion bedürfen:

- Die postulierte Zielsetzung für TR VELS stellt andere - seit Jahrzehnten anerkannte - Archivierungsverfahren als „nicht vertrauenswürdig, rechts- und revisionssicher“ dar.

- Die Komplexität der Lösung ist – wenn überhaupt –nur für qualifiziert signierte Dokumente erforderlich, welche bisher in vielen Unternehmen kaum anzutreffen und auch in Behörden noch wenig verbreitet sind. Außerdem lassen sich die Anforderungen – auch unter Beachtung von Standards – durch diverse andere Verfahren erfüllen.

- Unter Langfristaspekten wesentliche weitere Mängel (und damit Verstöße gegen die VOI-Merksätze) sind:

1 GOBS = GoBS = Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, veröffentlicht mit BMF-Schreiben vom 7. November 1995, IV A 8 - S 0316 - 52/95- BStBl 1995 I S. 738
2 GOBIT = Grundsätze ordnungsgemäßer IT-Buchführung. Erstellt im AWV, derzeit (Stand: Januar 2010) beim BMF zur Kommentierung.
3 Fachausschuss für Informationstechnologie des IDW, Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren (IDW RS FAIT 3), verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 11.07.2006. Billigende Kenntnisnahme durch den HFA am 6.9.2006
4 Mitglieder der Arbeitsgruppe: Dr. Martin Bartonitz, Saperion AG; Oliver Berndt, B&L Management Consulting GmbH; Dr. Gregor Joeris, SER Software Solutions GmbH; Wolfgang Heinrich, Easy Software AG; Bernhard Zöller, Zöller & Partner GmbH

  - Die TR VELS greift erst nach Abschluss der Bearbeitung, was viel später als der Posteingang sein kann
  - Sicherstellung der „Unveränderbarkeit“ kann durch die Signatur nicht geleistet werden
  - Anwendungsunabhängige Recherche ist nur optional, wäre aber zwingend notwendig

- Es soll ein Zertifikat für ein technisches System vergeben werden, ohne die Betrachtung der Prozesse und der Organisation beim Einsatz. Dies hat u. E. einen geringeren Wert als eine klassische GoBS-Zertifizierung und kann somit keine höhere Beweissicherheit für sich beanspruchen. Das Gegenteil ist der Fall.

- Das BSI vermittel hier durch diverse Veröffentlichungen seit Dezember 2009 einen Allgemeingültigkeitsanspruch, der nach unserer Auffassung dem BSI nicht zusteht. Anstatt sich auf die Spezifikation der Anforderungen und die Bewertung technischer Lösungen (für die Bundesverwaltung) zu beschränken, wird die technische Lösung gleich mitgeliefert und diese als allgemeine Empfehlung für ALLE Anwender postuliert. Hinzu kommt, dass die TR VELS nur EINE technologische Variante berücksichtigt – trotz Verfügbarkeit zahlreicher Handlungsoptionen –nämlich die Qualifizierte Elektronische Signatur (QES) mit Nachsignatur. Diese ist in Ihrer Verbreitung weit hinter den Erwartungen geblieben, was sich nach aktueller Einschätzung auf EU-Ebene auch nicht ändern wird.

- Das BSI macht sich hier zum Protagonisten einer technischen Nischenlösung und behindert damit Fortschritt und Gestaltungsfreiheit, wenn es – wie hier – ein sehr komplexes technisches Verfahren zur Bedingung für „Rechtssicherheit“ macht.

- TR VELS wird von Protagonisten als „Standard“ bezeichnet, obwohl es sich lediglich um die Zusammenführung einiger spezifischer Projektergebnisse handelt, an denen keine unabhängigen Organisationen (dann wäre es evtl. eine Norm) beteiligt waren und der auch bisher keine Marktverbreitung hat (dann wäre es evtl. ein De-Facto Standard).

- Eine internationale Anerkennung ist nicht nur nicht absehbar, sondern ausgeschlossen, weil es in den meisten Ländern an der Umsetzung der QES und insbesondere des Nachsignierens mangelt und eine Änderung diesbezüglich nicht absehbar ist. Entsprechende Diskussionen führen regelmäßig zu völligem Unverständnis bei den ausländischen Gesprächspartnern. Ein deutscher Alleingang, der Internationalität ausschließt, ist aber nicht sinnvoll, nicht wirtschaftlich und nicht mit EU-Recht vereinbar.

Änderungsbedarf bzgl. des Anspruchs der TR VELS

Natürlich betrachtet auch der VOI die ArchiSig-Konzepte als einen diskussionsfähigen Ansatz für die langfristige Beweiswerterhaltung qualifiziert signierter Dokumente, nicht jedoch die in der TR-VELS abgeleiteten Architektur-Konzepte und Anforderungen an einen Archiv-Service.

Der in der TR erhobene Anspruch ist für uns allerdings inakzeptabel, weil die meisten der hier „erstmalig gelösten Probleme“ – nämlich die sichere Einhaltung regulatorischer Anforderungen - schon seit 25 Jahren gelöst sind.

Begriff „Langzeitspeicherung“
Es ist an keiner Stelle definiert, was das BSI mit „Langzeit“ meint und welche Systeme/Lösungen NICHT unter diesen Begriff fallen, weil sie aus Sicht des BSI das zeitliche Kriterium nicht erfüllen. Der Begriff suggeriert auch, dass mit zunehmender Aufbewahrungsdauer die Anforderungen an das Aufbewahrungssystem steigen. Die Güte der notwendigen Sicherheit ist aber doch keine Frage der Aufbewahrungsdauer. Für die anzuwendende Sorgfaltspflicht bei der Aufbewahrung – beispielsweise einer Eingangsrechnung oder eines Versicherungsantrags – spielt es keine Rolle, ob ein Beleg 1 Sekunde alt ist oder gar 30 Jahre. Alle diese Unterlagen, die einer gesetzlichen Pflicht zur „ordnungsgemäßen Aufbewahrung“ unterliegen, müssen – unabhängig von Alter und Aufbewahrungsfrist – gleich aufbewahrt werden: nämlich gegen unzulässige Manipulationen geschützt und reproduktionsfähig bezüglich der aufbewahrungspflichtigen Inhalte.

Bindungswirkung und Anspruch von BSI und TR
Wenn Konsens bei den Beteiligten an diesem Diskurs besteht, dass man zeitlich nicht wirklich eingrenzen kann (Wie ist der zeitliche Unterschied zwischen „Langzeit-“ und – gibt es so etwas – „Nichtlangzeit-“Speicherung?) und den Anspruch des BSI versteht, nicht nur die Bundesverwaltung, sondern auch die breite Anwenderschaft in Deutschland zu adressieren: dann sind praktisch ALLE DMS-Anwender in Deutschland von dieser Richtlinie und ihrer Wirkung in der Öffentlichkeit betroffen, auch wenn sie einfach nur 100 Rechnungen am Tag scannen und 10 Jahre ordnungsgemäß in einem der marktgängigen DMS-Produkte aufbewahren. Mit anderen Worten: mit der mangelnden Eingrenzung der verwendeten zentralen Begriffe („Langzeitspeicherung“, „rechtssicher“) und dem öffentlich geäußerten Allgemeinvertretungsanspruch der TR 03125 disponiert das BSI über die Rechtmäßigkeit von Tausenden installierter Lösungen und greift in die wirtschaftliche und technisch-konzeptionelle Selbstbestimmung der DMS-Industrie und ihrer Kunden ein.

Verbliebene Hürden zur Vertrauenswürdigkeit
Textauszug der BSI Website zur TR 03125: „*Die vorliegende Technische Richtlinie zielt darauf ab, eine der wesentlichen verbliebenen Hürden auf dem Weg zu einer möglichst vollständigen digitalen Dokumentenverarbeitung zu beseitigen – die vertrauenswürdige elektronische Langzeitspeicherung von elektronischen Dokumenten, Akten und sonstigen Daten aller Art.*“

Das ist ein Angriff auf die Lösungen der DMS-Anbieter und deren Kunden, denen das BSI suggeriert, ihre Lösungen seien nicht vertrauenswürdig. Mit der Formulierung „wesentliche verbliebene Hürden“ unterstellt das BSI kategorisch die mangelnde Vertrauenswürdigkeit sämtlicher am Markt befindlicher Systeme, deren Einsatz bei Kunden teilweise vom TüV-IT gemäß VOI PK-DML Richtlinien geprüft und von Wirtschaftsprüfern abgenommen wurden.

Textauszug: „*Durch die immer schneller fortschreitende „Virtualisierung“ von Vorgängen und Dokumenten in die elektronische Form ergeben sich neue Herausforderungen*“

Auch hier wiederholen wir uns: seit einem Vierteljahrhundert automatisieren Zig-Tausende Anwender alleine in Deutschland ihre dokumentenbasierten Prozesse und Abläufe bei gleichzeitiger Einhaltung zahlreicher, unterschiedlicher regulatorischer Anforderungen bzgl. der Aufbewahrungspflichten. In Deutschland ist daraus eine Industrie entstanden, die funktional und architektonisch mit internationalen Anbietern auf Augenhöhe konkurriert. Welche neuen Herausforderungen hat das BSI identifiziert, die in der DMS Industrie (national oder international) nicht nur etwa nicht erkannt, sondern nach Meinung des BSI seit langem nicht abgedeckt werden? Mit Verlaub: aber die Virtualisierung, Digitalisierung von Dokumenten und Automation von

dokumentenbasierten Prozessen ist – auch in der Bundesverwaltung, siehe DOMEA – eine alltägliche Selbstverständlichkeit. Wenn hier Regelungsbedarf innerhalb der Bundesverwaltung besteht, mag das sein. Aber auch in diesem Fall würden wir Ihnen dringend raten, das Rad nicht neu zu erfinden, sondern zumindest die bereits vorhandenen Lösungen und Handlungsoptionen in Betracht zu ziehen. Das scheint uns hier nicht der Fall gewesen zu sein. Sonst wäre man nicht auf die Idee gekommen, eine Signatur-basierte Lösung als einzige Handlungsoption zu positionieren.

Stabile Speicherformate, Migrationsnotwendigkeit
Textauszug: „*Bislang wird diesen Herausforderungen entweder dadurch begegnet, dass die Lösung des Problems – insbesondere im Hinblick auf stabile Speicherformate und die Unabhängigkeit von den Produkten einzelner Hersteller – unter dem Hinweis auf fehlende Standards und Richtlinien in die Zukunft vertagt wird, oder die Daten und elektronischen Dokumente zum Ende ihrer operativen Relevanz wieder in die klassisch archivierbare Papierform gebracht werden. Beide Strategien sind unbefriedigend, unzureichend und auch unwirtschaftlich*."

Das mag für die Stellen der Bundesverwaltung gelten. Die DMS-Anwender sowohl in der Privatindustrie aber auch in vielen Bereichen der öffentlichen Verwaltung achten seit Jahren darauf, dass bei Anschaffung von Systemen Migrationsmöglichkeiten von Dokumenten und Metadaten verfügbar sind, die den Technologie- oder Anbieterwechsel ermöglichen. Dies ist eine zwar unbeliebte, aber doch geübte Praxis. Die TR VELS löst hier keinesfalls ein vorher ungelöstes Problem. Sie ist daher bestenfalls eine weitere Handlungsoption, die wir aber aus technisch/architektonischer Sicht für nicht problemfrei bewerten (siehe weiter unten).

Nicht bedachte Handlungsoption im ArchiSig-Projekt
In den zugrundeliegenden Projekten ist eine Alternative zu einer technischen Lösung für qualifiziert signierte Dokumente nicht diskutiert worden. Ein Vorschlag bzgl. einer klareren Definition zum Bedarf der Neusignierung hätte dazu führen können, dass im Falle der Nutzung revisionssicherer Archive dieser Bedarf nicht besteht, da das System selbst vertrauensvoll für den Schutz vor Veränderung sorgt. Für den Fall des Exports wäre ein erneutes Signieren, z.B. über einen Zeitstempel, eine technisch deutlich leichtgewichtigere Variante gewesen.

An dieser Stelle soll auch erwähnt werden, dass z.B. der ETSI Standard TS 101 733 ein gänzlich anderes Verfahren als ArchiSig vorschlägt. Interessanterweise finden sich die ETSI Standards zwar im Quellenverzeichnis. Im Text sind sie aber keine Erwähnung wert, obwohl die TR ansonsten eine Vielzahl von Standards aufführt. Durch die ausschließliche Berücksichtigung des ArchiSig-Verfahrens koppelt sich die TR damit von europäischen Entwicklungen ab.

Defizite der Referenz-Architektur und des ArchiSafe-Konzepts
Die TR-VELS macht sehr konkrete Vorgaben zur Umsetzung einer Referenz-Architektur. Auch wenn diese Architektur nur „empfohlen" ist, so ist eine technische Konformität zur TR-VELS nur durch Implementierung der in der Referenz-Architektur definierten Schnittstellen und XML-Formate für das sog. XAIP (XML Archival Information Package) möglich. Hierdurch erfolgt ein weitgehender Markteingriff durch das BSI, der dringend zu überdenken ist, zumal diese technischen Aspekte nicht im Rahmen eines offenen Standardisierungsverfahren erstellt wurden, sondern auf Ergebnissen einzelner Projekte (vor allem ArchiSig und ArchiSafe) beruhen. Insbesondere die Ergebnisse des ArchiSafe-Projekts werden in der DMS/ECM-Branche aber als überaus zweifelhaft angesehen.

Wir dürfen diese Sichtweise kurz anhand von Beispielen erläutern und auch aufzeigen:

1. **Zugriff nur per AOID erfüllt nicht die Anforderungen an Revisionssicherheit**
   Da der Zugriff nur per AOID möglich ist, ist bei Verlust der ID gar kein Zugriff mehr gegeben. Entsprechend kann der Zugriff auch nur über die jeweils archivierenden Geschäftsanwendungen erfolgen, die zur Ermittlung der AOID dann andere Indexdaten heranziehen können. Hieraus folgt wiederum, dass die Geschäftsanwendungen einschließlich der beschreibenden Metadaten über den gesamten Lebenszyklus der Aufbewahrung der Dokumente verfügbar sein müssen – genau das Gegenteil dessen, was man mit der Archivierung erreichen möchte!

2. **ArchivSafe-Service ist erst nach Vorgangsabschluss für eine vertrauenswürdige Speicherung nutzbar**
   Das Konzept der Verwendung von AIPs führt dazu, dass der Archiv-Service für eine vertrauenswürdige Speicherung erst nach Vorgangsabschluss eingesetzt werden kann, da sich während der Vorgangsbearbeitung beschreibende Metadaten oder Aufbewahrungsfristen ändern, die im XAIP bereits unveränderbar eingebettet sind. Eine sinnvolle und vor allem transaktionsgesicherte Versionierung sieht die Referenz-Architektur nicht vor.

   Die TR-VELS beschränkt sich selbst auch auf den Einsatz nach Vorgangsabschluss (S. 57). Der VOI-Grundsatz lautet dagegen: „Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren“. Bei eingehenden Dokumenten ist dies der Zeitpunkt nach dem Scannen.

   Da eine vertrauenswürdige Speicherung aber logischerweise nicht erst im Archiv beginnen kann, sondern beim Posteingang beginnen muss, müssen die Geschäftsanwendungen selbst für eine solche vertrauenswürdige Speicherung Sorge tragen (siehe hierzu auch A6.5-1 der TR VELS).

   Dies schließt auch alle Funktionen gemäß ArchiSig-Konzept ein, da ein Nachsignieren bei lang laufenden Vorgängen (Gerichtsverfahren, Planfeststellungsverfahren etc.) notwendig werden kann, bevor die signierten Dokumente überhaupt im ArchiSafe-Service angekommen sind. Das würde ein TR VELS konformes Verfahren bereits innerhalb der ERP-Lösungen erfordern, ohne allerdings jemals TR VELS konform sinnvoll anwenden zu können, weil sich Metadaten zu Vorgänge und Dokumenten noch häufig ändern. Das ist ein nicht auflösbarer Widerspruch.

   Die Notwendigkeit, im Fall lang laufender Vorgänge ein Nachsignieren in den Geschäftsanwendungen unterstützen zu müssen, ergibt sich aber aus den ggf. kurzfristigen Zeiträumen für das Nachsignieren: Wir erinnern hier an die rückwirkende (!) Feststellung der BNetzA vom 05.02.2008, dass SHA-1 bereits für Ende 2007 nicht mehr als sicherheitsgeeignet eingestuft wurde. Hier bestand nur eine Übergangsfrist von weniger als 6 Monaten zum Nachsignieren.

   Welcher Sinn hat aber eine Archiv-Middleware für eine Geschäftsanwendung, die alle Funktionen dieser Middleware zuvor selbst realisieren und auch noch den Zugriff auf die archivierten Dokumente per AOID über Jahrzehnte vorhalten muss?

3. **Referenz-Architektur erzwingt die Erzeugung von Archivzeitstempeln gemäß ArchiSig auch für nicht-signierte Dokumente**
   Während die Art der Schutzfunktion für die Ablage nicht-signierter Dokumente im Anforderungskatalog mehr oder weniger freigestellt ist, erfolgt in der Referenz-

Architektur jede Ablage über das ArchiSig-Modul. Dies ist in der Referenz-Architektur auch nicht anders möglich, da das ArchiSig-Modul (nicht das ArchiSafe-Modul) für die Erzeugung der AOID und die Speicherung im Speichersystem verantwortlich ist. Dieser Architektur-Ansatz ist nicht nur unter Gesichtspunkten des Software-Engineering fragwürdig, sondern nimmt auch jede Entscheidungsfreiheit bei der Art der Ablage nicht-signierter Dokumente – die nach wie vor mit weitem Abstand überwiegen.

4. **Kein Schutz vor Veränderung**
   Während Signaturen Veränderungen an einem Dokument zuverlässig aufdecken, so bieten sie keinen Schutz vor verschiedenen Arten der Manipulation (bewusste/versehentliche Änderung/Löschung von Dokument/Signatur), die dazu führen, dass der Beweiswert nicht erhalten werden kann, da es keine gültige Signatur bzw. kein gültigen Evidence Record mehr zum Dokument gibt oder gar das Dokument nicht wieder auffindbar ist.

   Auch wenn solche Veränderungen nur am Archiv-Service vorbei möglich sind, so gibt es eine Reihe von WORM-Speichertechnologien, die von allen namhaften Storage-Hersteller (EMC, Hitachi, HP, IBM, NetApp, ergänzt um UDO-Jukeboxen) angeboten werden, um solche Veränderungen effektiv auszuschließen.

   Diesen Aspekten widmet sich die TR-VELS nur unzureichend. Gleichzeitig stellt sich die Frage, ob solche im breiten Einsatz befindliche Technologien nicht auch eine hinreichende Alternative zum Schutz der elektronischen Signaturen darstellen, selbst wenn deren Algorithmen nicht mehr als sicherheitsgeeignet eingestuft werden. Eine Anpassung des §17 SigV wäre hierzu anzustreben, um andere Schutzmaßnahmen zu zulassen, da der technische Aufwand trotz ArchiSig-Konzept für ein Nachsignieren im Falle des „Neu-Hashens“ enorm ist und gerade eine dringend notwendige Verbreitung elektronischer Signaturen bremst.

Formale Mängel

Die TR enthält eine Vielzahl von Aussagen, die entweder falsch oder praxisfremd sind oder schlicht einen falschen Anschein erwecken. Nur exemplarisch führen wir hier einige Punkte auf.

- Auf Seite 17 werden Schnittstellen mit Datenarchivierungsfunktionen gleichgesetzt. Dies sind zwei grundsätzlich verschiedene Dinge, die nicht mal einen direkten Zusammenhang haben.

- Die Inhalte der Matrix auf Seite 19 sind fehlerhaft. Beispielsweise

  - umfasst AO natürlich den Schutz vor Verlust, aber nicht im Text, sondern in der Interpretation des Begriffs der Ordnungsmäßigkeit (Vollständig, zeitgerecht, unveränderbar etc.).

  - definiert die GDPdU natürlich auch die Aufbewahrungsfrist für die Daten (durch Bezug auf AO).

  - ist der Schutz vor unberechtigtem Zugriff nicht nur eine Anforderung des BDSG, sondern auch Voraussetzung für Integrität des Archivs und der Dokumente.

- Auch die Differenzierung zwischen Archivierung und Backup auf Seite 14 ist falsch. Archivierung ist nicht einfach Langzeit-Backup, wie hier suggeriert wird, sondern organisatorisch sowie technisch etwas völlig anderes.

Bereits in der Vergangenheit haben wir uns über Empfehlungen des BSI zum Thema elektronische Archivierung gewundert und geärgert (Konkret: die Kapitel zum Thema Archivierung der BSI Grundschutzkataloge in der Version vom Oktober 2008), weil sie inhaltlich grob fehlerhaft oder faktisch nicht umsetzbar sind und daher in der Praxis weitgehend ignoriert wurden. Beispiel: Die Grundschutzkataloge vom Oktober 2008 enthalten trotz Hinweis durch den VOI nicht einhaltbare Empfehlungen zur Archivierung, zur Verwendung von WORM-Speichern, die es alle ausnahmslos (!) nicht mehr gibt. Beispielsweise werden in dieser Ausgabe 12- Zoll und 14 Zoll WORM-Systeme empfohlen, die es seit 15 Jahren nicht mehr am Markt gibt.

Aus den genannten und zahlreichen ungenannten Gründen – der Umfang eines normalen Briefes ist hier wohl bereits überschritten -, fordern wir das BSI daher auf, eine technische Konformitätsprüfung zur Referenz-Architektur und ihren Schnittstellen bis auf Weiteres auszusetzen und das gesamte Architekturkonzept zu überdenken.

Sehr geehrter Herr Hange, abschließend möchten wir Sie an Ihre Aussagen auf der BSI-Website erinnern: „Mit *unserem Angebot wenden wir uns aber auch an die Hersteller sowie die privaten und gewerblichen Nutzer und Anbieter von Informationstechnik, denn nur gemeinsames Handeln kann wirkungsvoll sein*“. Und weiter: „*Eine noch engere Zusammenarbeit mit allen Akteuren der IT- und Internetbranche auf dem Gebiet der IT-Sicherheit ist daher unser Anliegen*“.

Diese gewünschte Gemeinsamkeit, das Einbinden vorhandenen Branchen-Knowhows in vorliegenden und anderen Fällen empfinden unsere Mitglieder als Lippenbekenntnisse, denen zum Schaden der Anwender und Anbieter keine Taten folgten. Der VOI und seine Mitglieder wurden nicht um Mitarbeit gebeten – trotz eines früheren Angebotes aus 2006, welches bereits nach einer Diskussion um die Grundschutzkataloge entstand (die Mitarbeit durch VOI Fachleute wäre für das BSI unentgeltlich gewesen). Statt für mehr Sicherheit zu sorgen, entsteht faktisch eine kontraproduktive Verwirrung, weil uneingeweihte Interessierte den Texten des BSI oder des VOI (je nachdem, wo man zuerst recherchiert) Glauben schenkt. Es kann nicht im Sinne des BSI sein, wenn Anwender aus Verwirrung darüber, wer denn nun Recht hat, gar nichts tun, weil sie mindestens mitbekommen, dass es eine kontroverse Diskussion zu diesen Themen gibt.

Wir würden uns daher freuen, wenn der VOI dem BSI behilflich sein darf, Ihre Wünsche zur gemeinsamen Arbeit in die Tat umzusetzen.

Mit freundlichen Grüßen

Bernhard Zöller

Stellvertretender Vorstandsvorsitzender des VOI
(Verband Organisations- und Informationssysteme e.V.)