Technische Richtlinie zur vertrauenswürdigen Langzeitarchivierung

P. Rehäußer[1], W. Zimmer[1], U. Korte[2], D. Hühnlein[3],
S. Fischer-Dieskau[2], U. Gnaida[2]

[1]CSC Deutschland Solutions GmbH
{prehaeus, wzimmer2}@csc.com

[2]Bundesamt für Sicherheit in der Informationstechnik
{ulrike.korte, stefanie.fischer-dieskau, utz.gnaida}@bsi.bund.de

[3]secunet Security Networks AG
detlef.huehnlein@secunet.com

Zusammenfassung

Die zunehmende Verbreitung elektronischer Daten und Dokumente in Unternehmen und öffentlicher Verwaltung hat vor allem für die „dauerhafte“ und beweiskräftige Aufbewahrung der elektronischen Unterlagen weit reichende Folgen. Elektronische Dokumente sind per se virtuell und erfordern daher geeignete technische und organisatorische Maßnahmen, mit denen ihre Integrität, Authentizität und Verkehrsfähigkeit für lange Zeiträume gewährleistet werden kann. Die Technische Richtlinie zur vertrauenswürdigen Langzeitarchivierung [BSI09] spezifiziert auf der Grundlage bestehender rechtlicher Normen und technischer Standards sowie nationaler und internationaler Erfahrungen in einem modular aufgebauten Gesamtkonzept, bestehend aus IT-Architektur, technischen Prozessen und Datenformaten, einen Kriterienkatalog für die langfristige, rechts- und revisionssichere Aufbewahrung elektronischer Daten und Dokumente.

1 Einführung und Überblick

Unternehmen, öffentliche Verwaltung und die Justiz sind schon seit längerem bestrebt, ihre Geschäftsprozesse möglichst weitgehend in elektronischer Form durchzuführen und die zugehörigen Unterlagen auch in digitaler Form aufzubewahren. Allerdings verfügen Papierdokumente auf Grund ihrer Körperlichkeit über Eigenschaften, die elektronische Dokumente per se nicht aufweisen. Aus sich heraus können elektronische Dokumente weder wahrgenommen oder gelesen werden, noch geben sie Anhaltspunkte für ihre Integrität und Authentizität. Diese Eigenschaften aber sind entscheidend für eine rechtlich verbindliche Wirkung elektronischer Dokumente. Sie müssen daher beim Übergang zu elektronischen Dokumenten zwingend bedacht und nicht zuletzt unter dem Gesichtspunkt der längerfristigen Aufbewahrung durch geeignete technische und organisatorische Maßnahmen hergestellt und zumindest für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen erhalten werden.

P. Horster (Hrsg.) · Konferenzname · syssec (Jahr) pp.

Zu bedenken ist hierbei auch, dass mit Blick auf gesetzlich vorgeschriebene Mindestaufbewahrungszeiten die üblichen Lebenszyklen moderner Datenträgertechnologien sowohl hinsichtlich Haltbarkeit als auch Lesbarkeit in vielen Fällen viel zu kurz greifen. Abbildung 1 zeigt dazu beispielhaft einige Anforderungen an Mindestaufbewahrungszeiten auf. Für die elektronische Langzeitarchivierung sollte daher die Wahl des Speichermediums eine eher untergeordnete Rolle spielen. Die oben geforderten Merkmale eines vertrauenswürdigen und rechtssicheren Archivsystems müssen daher anderweitig realisiert werden.

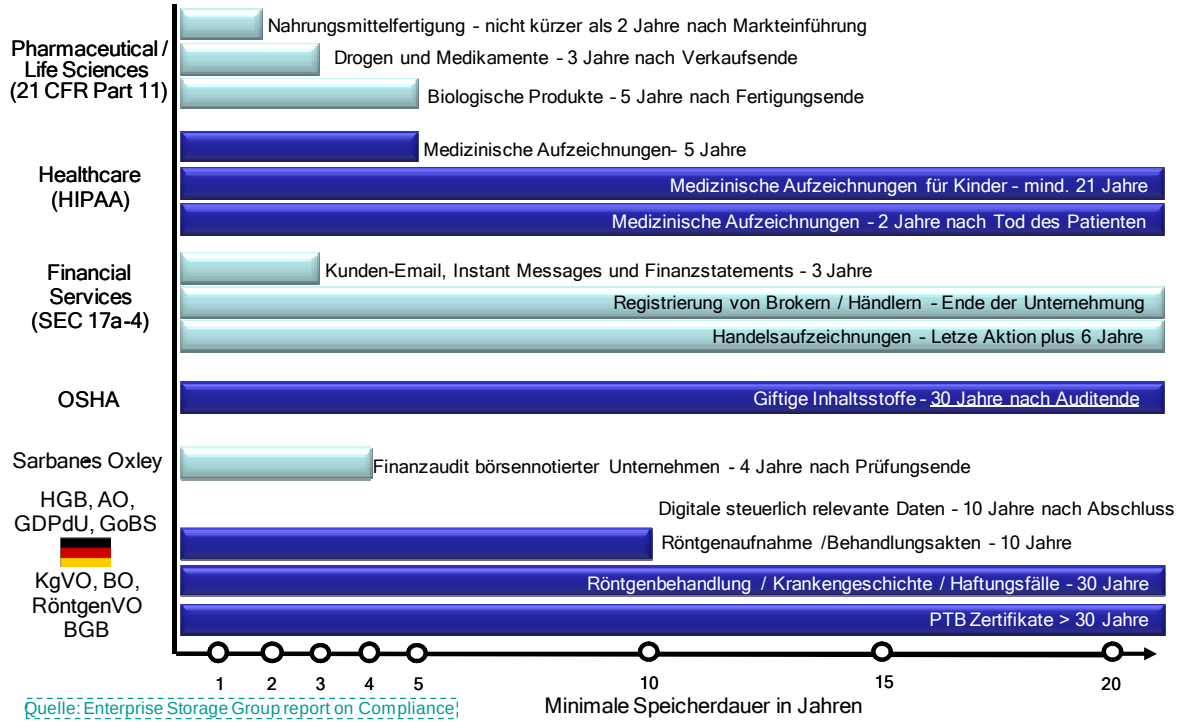

Abbildung 1: Mindestaufbewahrungsdauer

Diese Aufgabe nachhaltig zu unterstützen ist Ziel der „**Technischen Richtlinie zur vertrauenswürdigen elektronischen Langzeitarchivierung (TR-VLA)**“. Die Technische Richtlinie spezifiziert auf der Grundlage bestehender rechtlicher Normen und technischer Standards sowie nationaler ([HaRo08], [RoSc05], www.archisafe.de, www.archisig.de, [BSI08]) und internationaler Erfahrungen (siehe bspw. [Glad07], [OAIS02], [VERS95], [CCSD08]) in einem bislang einzigartigen und modular aufgebauten Gesamtkonzept anwendungsübergreifende Anforderungen und Kriterien für die langfristige, rechts- und revisionssichere Aufbewahrung elektronischer Dokumente. Sie gibt damit Unternehmen ebenso wie der öffentlichen Verwaltung eine verlässliche Orientierung bei der Auswahl und dem adäquaten Einsatz geeigneter Sicherungsmittel für den langfristigen Erhalt der Lesbarkeit und Vollständigkeit sowie der Integrität und Authentizität elektronischer Dokumente.

Auf der Basis einer hersteller- und produktunabhängigen Referenzarchitektur werden sicherheitstechnische Mindestanforderungen an Systeme, Komponenten und Schnittstellen sowie ihr Zusammenspiel definiert, auf deren Grundlage vertrauenswürdige und funktional konforme elektronische Langzeitaufbewahrungssysteme aufgebaut, überprüft und in Betrieb genommen werden können.

Der Beitrag beleuchtet in einem Abriss die wesentlichen Inhalte der technischen Richtlinie:

- im Abschnitt 2 die nationalen und internationalen Rahmenbedingungen sowie die aus den bestehenden rechtlichen Normen bestimmten allgemeinen Anforderungen,
- im Abschnitt 3 den Dokument-zentrierten Lösungsansatz auf der Grundlage offener Standards und einer modularen und skalierbaren IT-Architektur, mit dem die für eine rechtssichere Ablage erforderlichen Prozesse adäquat abgebildet werden können sowie
- im Abschnitt 5 einen Ausblick auf die weiteren Arbeiten, u.a. die Definition der Anforderungen an eine hersteller- und produktunabhängige Konformitätsprüfung zu dieser Technischen Richtlinie.

2 Aktuelle Situation und allgemeine Anforderungen

Die Aufbewahrungspflicht von (elektronischen) Dokumenten und Unterlagen dient vor allem dem Schutz und der Wahrung von Rechtsansprüchen des Ausstellers oder Dritter und dem Nachweis der Ordnungsmäßigkeit im elektronischen Rechts- und Geschäftsverkehr. Die deutsche Rechtsordnung kennt zum Zeitpunkt der Veröffentlichung dieser Richtlinie allerdings kein anwendungsübergreifendes „Aufbewahrungsgesetz“ – weder für papierbasierte noch für elektronische Dokumente (siehe [RFJK07]). Ähnliches gilt für das EU-Recht. Es ist daher unumgänglich, die im Einzelfall geltenden Anforderungen an die Dokumentation und Aufbewahrung aus übergreifenden sowie für den jeweiligen Sach- oder Geschäftsbereich relevanten Zweckbestimmungen, Normen und Vorschriften zu bestimmen.

Von zentraler Bedeutung und Wirkung ist hier insbesondere das Signaturrecht ([SigG], [SigV]), das im Zusammenhang mit [JKomG], [ZPO], [FormAnpG] und [VwVfG] die Voraussetzungen und Anforderungen an die beweisrechtliche Anerkennung und den Erhalt des beweisrechtlichen Wertes elektronischer Unterlagen normiert.

Unabhängig von einer konkreten Zweckbestimmung muss ein vertrauenswürdiges elektronisches Archivsystem jedoch imstande sein, die Authentizität, Integrität und Verfügbarkeit der elektronisch gespeicherten Unterlagen (Daten und Dokumente) für die Dauer gesetzlich vorgeschriebener Aufbewahrungsfristen - zum Teil bis zu 100 Jahren - zu gewährleisten. Dazu gehört, dass die im Langzeitspeicher abgelegten Dokumente und Daten

- in Form und Inhalt authentisch und vollständig sowie technisch verfügbar und wiedergabefähig, auf zum Zeitpunkt der Wiedergabe dem Stand der Technik entsprechenden elektronischen Geräten aufbewahrt werden,
- nicht unberechtigt eingesehen, weitergegeben oder veröffentlicht werden können,
- vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind sowie
- Rechtsansprüche und Nachweispflichten zu gewährleisten imstande sind.

Um den zuverlässigen Zugriff auf die im Langzeitspeicher aufbewahrten Daten für externe IT-gestützte Geschäftsanwendungen zu ermöglichen, muss ein Archivsystem dabei zumindest die folgenden Funktionen über definierte Schnittstellen zur Verfügung stellen:

- die Ablage (Archivierung) unsignierter/signierter elektronischer Daten und Dokumente,
- den Abruf archivierter Daten und Dokumente,
- den Abruf beweisgeeigneter elektronischer Nachweise über die Authentizität und Integrität der aufbewahrten Daten und Dokumente,
- das Löschen von Daten und Dokumenten.

3 Auftretende Problemstellungen

Wie oben erwähnt regelt das Signaturrecht die Anforderungen an die beweisrechtliche Anerkennung von Daten und Dokumenten. Daher sind das Signaturrecht und die damit verknüpften kryptographischen Verfahren der elektronischen Signatur selbstverständlich eine wichtige Grundlage für ein elektronisches Langzeitarchiv.

Eine wesentliche Problemstellung, die bei der Aufbewahrung elektronischer Dokumente auftritt, ist die „Alterung" der zur Sicherung der Integrität und Authentizität eingesetzten kryptographischen Verfahren. Damit ist gemeint, dass die Fortentwicklung der Hardware, Software und Kryptoanalyse die Sicherheitseignung der Algorithmen und verwendeten Schlüssellängen nach und nach schwächt bzw. ganz aufhebt. Es müssen also Mittel und Wege gefunden werden, der Alterung von Signaturverfahren und Hashalgorithmen zu begegnen und zu verhindern, dass bei einer Kompromittierung des Signaturverfahrens die archivierten Daten unbemerkt verändert werden können und damit nicht mehr **integer** sind. Nebenbedingung dabei ist, dass nicht regelmäßig alle bereits signierten Unterlagen nochmals (von ihren ursprünglichen) Autoren signiert werden müssen. Zum einen ist dies in Enterprise-Umgebungen alleine durch die schiere Masse nicht möglich, zum anderen sind viele Autoren nach einigen Jahren gar nicht mehr im Unternehmen. Man möchte das Archiv, dessen Prozesse und Kosten ja zudem auch vereinfachen und nicht verkomplizieren. Eine offensichtliche Lösung scheint das Verwenden von manipulationssicheren Datenträgern wie WORM oder DVD zu sein. Darauf wird nachfolgend eingegangen.

Ein weiteres nicht ganz offensichtliches Problem ist die langfristige Lesbarkeit des Datenträgers und des Datenformates, in dem die Unterlagen archiviert wurden. Wie oben gezeigt, besteht in einzelnen Fällen durchaus der Bedarf zur Archivierung auf 20, 30 oder gar 100 Jahre. Viel schneller als die Medien altern, werden sie heute von neuen Technologien überrannt. Ein Diskettenlaufwerk ist heute in kaum noch einem PC eingebaut, Netbooks und manche Nettops verzichten schon auf DVD- und CD-Laufwerke. Statt rotierender Medien nutzt man beispielsweise USB-Sticks, um Daten von einem Ort zum anderen zu tragen.

Dieses Problem adressiert die **Verfügbarkeit** der Unterlagen und zeigt, dass man nicht blind einem (Hardware-)Hersteller, einem Medientyp oder einem Dateiformat vertrauen darf – auch wenn ggf. alle Drei zum aktuellen Zeitpunkt eine marktbeherrschende Stellung einnehmen. Auch hier dienen die offensichtlichen Lösungen wie regelmäßiges Umkopieren auf neue Datenträger, regelmäßiges Konvertieren in neue/aktuelle Dateiformate, etc. nicht wirklich zur Vereinfachung des Archivs.

Die **Vertraulichkeit** der Unterlagen im Archiv muss natürlich auch bedacht werden. Wird der Zugriff auf Papierakten bis heute durch das Archiv-Personal quasi geregelt und beschränkt, könnte durch ein unternehmensweit zentrales elektronisches Archivsystem schnell und einfach ein unbemerkter und vor allem unberechtigter Zugriff auf vertrauliche Unterlagen möglich sein. Noch größer sind die Herausforderungen bei so genannten Outsourcing-Lösungen, bei denen ein Dienstleister sein elektronisches Archiv vielen Unternehmen gleichzeitig anbietet. In solchen Fällen ist die Möglichkeit einer strikten Trennung einzelner Datenbereiche (Mandanten) und Zugriffs- und Berechtigungskonzept innerhalb des Archivs. und einer strikten Durchsetzung eines sicheren Zugriffs- und Berechtigungskonzeptes zwingend geboten.

Abschließend wird noch auf die Problematik der **Authentizität** von Dokumenten im Archiv eingegangen. Wie stellt man fest, ob ein 50 Jahre altes elektronisches Dokument tatsächlich von Hans Müller, und zwar vom „richtigen“ Hans Müller, stammt? Dazu genügt eine qualifizierte elektronische Signatur dieses Dokumentes. Aber kann man in 50 Jahren diese Signatur wirklich noch nachprüfen? Können wir heute davon ausgehen, dass die Zertifizierungsdiensteanbieter auch in 50 Jahren noch verlässliche Daten über das für die Signatur verwendete Zertifikat besitzen und zur Verfügung stellen? Elektronische Unterschriften und die zugehörigen elektronischen Zertifikate müssen daher vor bzw. bei der Archivierung geprüft und die Prüfergebnisse gemeinsam mit den zugehörigen Daten im Archiv abgelegt werden.

4 Standard-Datenformate und modulare Architektur

Ausgehend von den oben geschilderten Problemstellungen dürfen die für die Langzeitspeicherung eingesetzten Verfahren und technischen Lösungen darüber hinaus die weitere Verwendbarkeit der elektronischen Dokumente für unterschiedliche Anwendungszwecke und in unterschiedlichen Anwendungssystemen (Fachverfahren) nicht beeinträchtigen. Insbesondere dürfen keine Behinderungen entstehen für:

- den Austausch von Dokumenten zwischen Anwendungssystemen,
- den Wechsel von Datenformaten in Anwendungssystemen,
- den Austausch von Anwendungssystemen oder –komponenten,
- die Migration gespeicherter Daten und Dokumente auf neue Systeme.

Das erfordert nicht nur den Einsatz langfristig verfügbarer und verkehrsfähiger Datenformate für die zu archivierenden Dokumente, sondern darüber hinaus auch eine flexible IT-Infrastruktur (siehe hierzu auch [RoSc05], [HaRo08]).

4.1 Datenformate

Auf der Grundlage der Ergebnisse des ArchiSig- und des ArchiSafe-Projektes (siehe www.archisig.de und www.archisafe.de) sollen deshalb die zu speichernden Daten und Dokumente in standardisierten offenen Formaten (wie bspw. PDF/A) gemeinsam mit allen, für eine revisionsfeste Rekonstruktion der Geschäftsprozesse erforderlichen Metainformationen in einem abgeschlossenen und selbsterklärenden XML-basierten Archivdatenobjekt (im folgenden Text „XML Container“ genannt) aufbewahrt werden, das im Falle elektronisch signierter Dokumente zudem um kryptographische Daten zum dauerhaften Nachweis der Integrität und Authentizität angereichert wird.

Abbildung 2: XML-Containerstruktur

Abbildung 2 zeigt die innere Struktur dieses XML-Containers auf oberster Ebene.

Der **Package Header** enthält Informationen über den gesamten Container (z.B. Zeitpunkt der Archivierung, Mindestaufbewahrungsdauer) und fungiert zudem als eine Art „Inhaltsver-

zeichnis“. Hier wird die innere logische Struktur des Containers abgebildet. Die **MetaData-Section** enthält pro Nutzdatenobjekt in der DataObjectSection Meta-Informationen, die sich einerseits auf den Geschäftsvorfall, andererseits auch auf den Datentyp oder die Darstellungsweise der Nutzdaten beziehen können. In der MetaDataSection sollen also alle Informationen abgelegt werden, die für die spätere Verwendung der Nutzdaten (technisch und auch aus Sicht des Unternehmens) relevant sein könnten. Die **DataObjectSection** enthält schließlich die eigentlichen Nutzdaten. Es können hier – abgesehen von technischen Einschränkungen wie z.B. maximale Dateigröße im Archiv – beliebig viele Einzel-Objekte (Dateien) abgelegt werden. Über den Package Header können diese Einzelobjekte auch strukturiert und somit z.B. Hierarchien, Gliederungen und Ordner-Strukturen abgebildet werden. In der optionalen **CredentialsSection** liegen – im Fall von signierten Nutzdaten – schließlich die (kryptographischen) Daten, welche die Authentizität der Nutzdaten zum Zeitpunkt der Archivierung bestätigen. Im Wesentlichen sind dies also die Zertifikate der signierenden Personen und die OCSP-Responses der Zertifizierungsdiensteanbieter sowie deren Zertifikate.

Um den Nachweis der Integrität und damit auch der Authentizität des gesamten Containers auch noch nach langer Zeit führen zu können, sollen zudem kryptographische Repräsentanten (Hashwerte) des XML-Containers zusätzlich in einem Merkle-Hashbaum [Merk80] gesichert werden. Die unmittelbar bei der Archivierung erzeugten Hashwerte sichern die **Integrität** des XML-Containers. Die Hashwerte selbst werden über einen qualifizierten Zeitstempel mit qualifizierter elektronischer Signatur geschützt – den so genannten **Archivzeitstempel** (Archiv Time Stamp, ATS). Kommen neue Container ins Archiv, kommen auch neue Hashwerte dazu. Diese neuen Hashwerte werden zusammen mit dem bereits vorhandenen Zeitstempeln wiederum mit einem Zeitstempel geschützt. So entsteht im Lauf der Zeit ein Hash-Baum, wie in Abbildung 3 angedeutet.

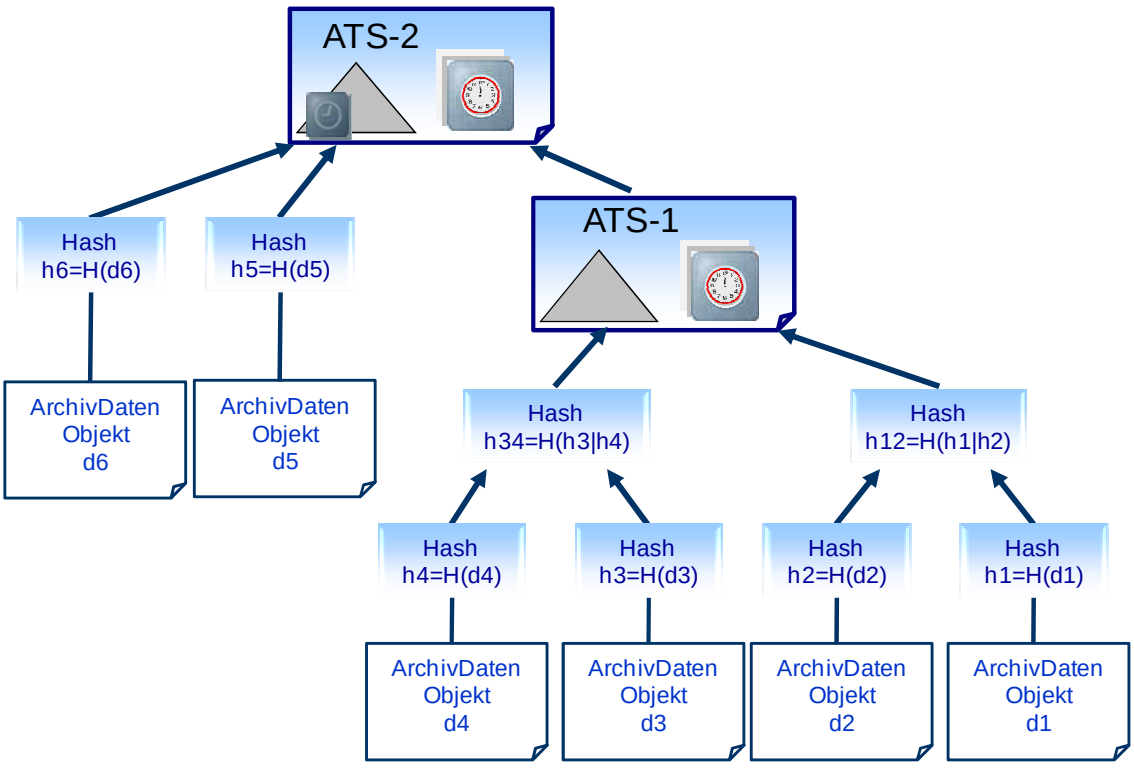

Abbildung 3: Archivzeitstempel

Die Verwendung von qualifizierten Zeitstempeln mit qualifizierter elektronischer Signatur verwirklicht gleichzeitig eine effiziente Erneuerung ggf. vorhandener qualifizierter Signaturen der Nutzdatenobjekte. Somit ist auch die **Authentizität** der Dokumente gesichert. Für die Hashwertbildung als auch die qualifizierten Signaturen der Dokumente und Zeitstempel macht die Technische Richtlinie keine konkreten Vorgaben. Es wird in diesem Zusammenhang auf die jährliche Bekanntmachung der Bundesnetzagentur über die geeigneten Algorithmen verwiesen [BNetzA].

Der kryptographisch geschützte Hashbaum erlaubt nicht nur ein wirtschaftliches Verfahren zur Erneuerung elektronischer Signaturen (da man nicht pro Dokument einen eigenen Zeitstempel benötigt), sondern darüber hinaus auch den Abruf technischer Beweisdaten für die Integrität und Authentizität der gespeicherten elektronischen Dokumente gemäß der im RFC 4998 [GoBP07] standardisierten **Evidence Record Syntax** (ERS) (siehe auch [Gond07]).

Der Vorteil dieses Verfahrens liegt darin, dass man für den Nachweis der Integrität bzw. Authentizität eines einzelnen Archivdatenobjektes nicht den gesamten Hashbaum nachrechnen muss, sondern nur den „Pfad“ von der Wurzel des Baumes bis zum relevanten Archivdatenobjekt. Dieser „Pfad“ wird auch **reduzierter Hashbaum** genannt und ist in Abbildung 4 mittels der nicht verblassten Elemente angedeutet.

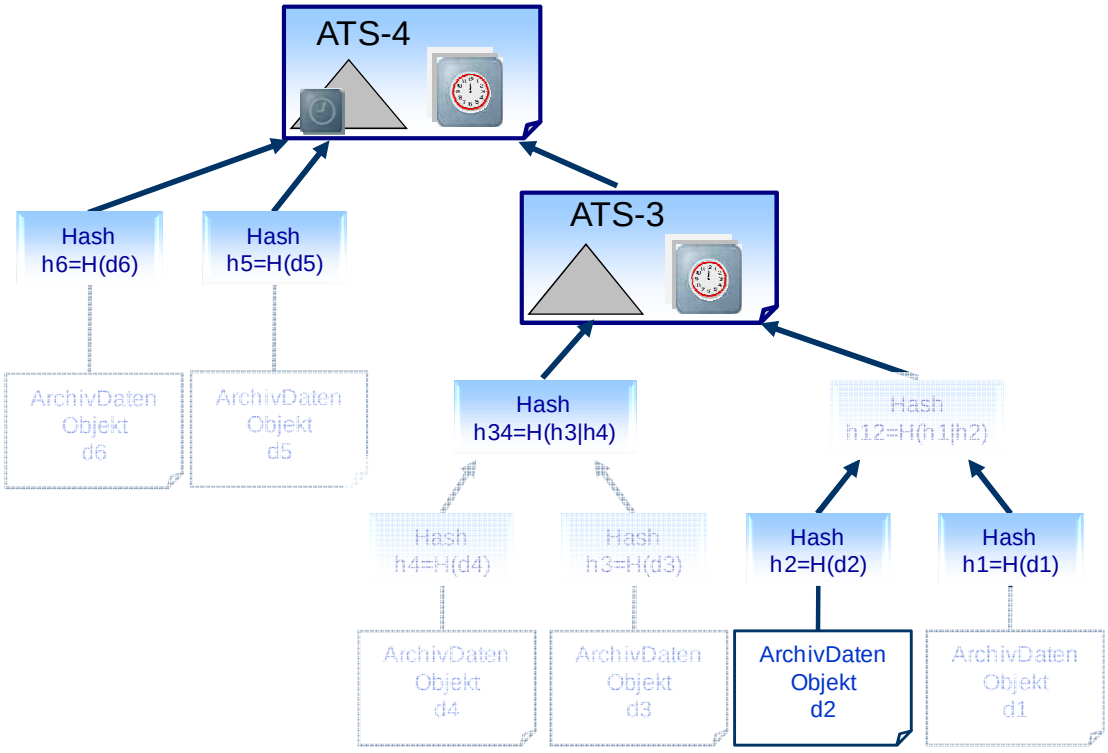

Abbildung 4: Reduzierter Hashbaum

4.2 IT-Architektur

Die Technische Richtlinie empfiehlt, neben den Datenformaten und Strukturen, für eine konkrete Implementierung eines vertrauenswürdigen Archivsystems eine hersteller- und produktunabhängige, modulare und skalierbare IT-Referenzarchitektur, die im Stande ist, alle rechtlichen und sicherheitstechnischen Anforderungen zu erfüllen (siehe Abbildung 5).

Die IT-Referenzarchitektur besteht im Wesentlichen aus den folgenden logischen Komponenten und Schnittstellen:

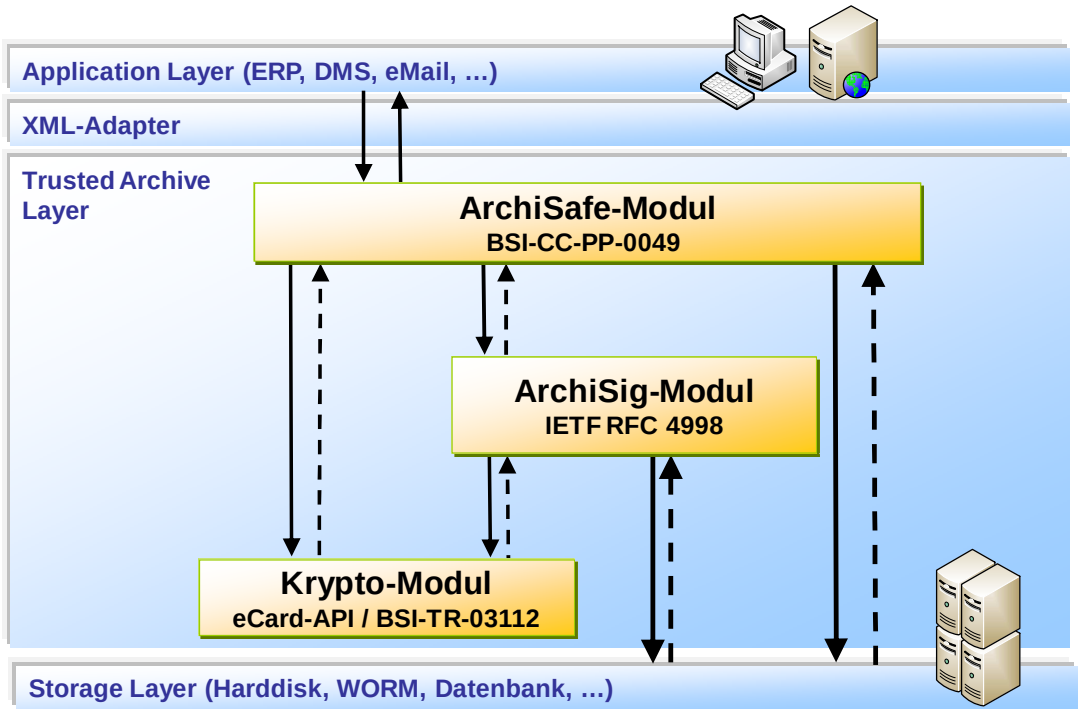

Abbildung 5: IT Referenzarchitektur

- Vorgelagerte Geschäftsanwendungen (bspw. ein ERP-System, ein DMS-System, ein E-Mail-System und weitere), die das Archivsystem für die langfristige, rechts- und revisionssichere Ablage elektronischer Daten und Dokumente nutzen. Ziel ist hierbei natürlich, dass alle Anwendungen eines Unternehmens mit Archivierungsbedarf an das Archiv angeschlossen werden.
- Ein anwendungsspezifischer XML-Adapter (Konnektor), der die Geschäftsanwendung technisch mit dem Archiv koppelt und vor allem auch die Struktur des XML-Containers „kennt“. Dieser Adapter ist dafür zuständig, dass die zu archivierenden Daten zunächst in die entsprechende Form und in den Container korrekt verpackt werden. Ebenso entpackt er den Container und übergibt die Nutzdaten an die Anwendung, falls diese Daten aus dem Archiv abruft.
- Ein Archiv-Gateway (in Abbildung 5: ArchiSafe-Modul), das für eine Entkopplung von Anwendungssystemen und Archivsystem sowie für eine effektive und zuverlässige **Zugriffskontrolle** auf das Archiv sorgen soll. Die funktionalen Anforderungen an dieses Gateway wurden ursprünglich im ArchiSafe-Projekt (www.archisafe.de) festgelegt und in der Technischen Richtlinie verfeinert. Hierbei handelt es sich hauptsächlich um die Fähigkeit, den XML-Container an Hand unternehmensspezifischer Regeln und gegen ein XML Schema zu prüfen. Die sicherheitstechnischen Anforderungen sind in einem Common Criteria Protection Profile [PhBs08] definiert. Da diese Komponente ein sehr sicherheitskritisches Element des Archivs ist, sollten sich entsprechende Produkte gegen dieses Protection Profile zertifizieren lassen. Es handelt sich hier um die Zugriffskontrollfunktion sowie um eine Informationsflusskontrolle, so dass nur zulässige „Kommandos“ und Daten an das Archiv übermittelt werden können.

- Ein Krypto-Modul, das alle erforderlichen Funktionen für die Prüfung und (optional) die Erstellung elektronischer Signaturen und Zeitstempel zur Verfügung stellt. Das Krypto-Modul ist insbesondere für die Prüfung von Signaturen von Nutzdaten sowie für die Bildung von Hashwerten zuständig. Für die vollständige Prüfung von Signaturen werden über das Krypto-Modul auch bei Bedarf die Zertifikate der signierenden Personen von den Zertifizierungsdiensteanbietern abgefragt und die Zertifikate selbst auf Gültigkeit zum Zeitpunkt der Signatur geprüft. Sollte das Krypto-Modul nicht selbst in der Lage sein, qualifiziert signierte Zeitstempel zu erzeugen, muss das Krypto-Modul diese von einem akkreditierten Zeitstempeldiensteanbieter einholen. Das Krypto-Modul benötigt dafür und für die vollständige Prüfung der Zertifikate eine in der Abbildung nicht dargestellte Verbindung zu den entsprechenden Diensteanbietern.
  Die Schnittstellen des Krypto-Moduls sollten sich nach dem eCard-API Framework [BSI08] richten, was einen möglichen Wechsel des Krypto-Moduls erleichtert.
- Ein ArchiSig-Modul, das die erforderlichen Funktionen für die rechtskonforme Beweiswerterhaltung der archivierten Datenobjekte bereitstellt. Dieses Modul ist für die Verwaltung der Hash-Bäume zuständig, delegiert die rein kryptographischen Operationen jedoch an das Krypto-Modul. Des Weiteren ist dieses Modul für das Erstellen der RFC4998-konformen reduzierten Archivzeitstempel im Beweisfall verantwortlich. Die generelle Funktionsweise wurde im ArchiSig-Projekt spezifiziert (www.archisig.de) und in der Technischen Richtlinie in den Gesamtkontext eines Archivsystems gesetzt.
- Einem (oder mehreren) Langzeitspeicher(n) zur eigentlichen Datenspeicherung. Es werden nahezu keine funktionalen Anforderungen an den Langzeitspeicher gestellt. Es kann sich daher prinzipiell um jede Art von physischen Datenträgern (z.B. Bänder, Festplatten) und jede Form der logischen Organisation (z.B. Dateisystem, Datenbank) handeln. Es muss jedoch sichergestellt sein, dass der Speicher im Stande ist, eine bitgenaue Reproduktion der ursprünglich archivierten Daten zurückzuliefern. Diese geringen Anforderungen sollen die Migration auf einen anderen Langzeitspeicher unterstützen.

Ausgehend von der IT-Referenzarchitektur beschreibt die Technische Richtlinie ausführlich die im Zusammenhang mit der rechtssicheren Ablage elektronischer Unterlagen erforderlichen Anwendungsfälle, Abläufe (Prozesse) und das Zusammenspiel der in der Referenzarchitektur definierten logischen Komponenten. Dazu gehören

- das Archivieren signierter und unsignierter elektronischer Daten,
- der Abruf gespeicherter Daten,
- das Löschen gespeicherter Daten zusammen mit der Frage, wann überhaupt von wem gelöscht werden darf,
- der Abruf technischer Beweisdaten für einzelne gespeicherte Daten.

Für die Archivierung (signierter) elektronischer Unterlagen ist bspw. der in Abbildung 6 skizzierte grundsätzliche Ablauf vorgesehen, der allerdings keine der möglichen Fehlersituationen darstellt (z.B. kein Zugriff auf Archiv, Signatur falsch, Zertifikat ungültig, etc.).

Noch innerhalb der Geschäftsanwendung wird vom Benutzer entschieden, ob die zu archivierenden Daten (qualifiziert) signiert werden sollen (1). Die Signatur kann dabei zeitlich weit vor der Archivierung erfolgen. Erst in einem zweiten Schritt wird über die Geschäftsanwendung die Archivierung angestoßen (2). Der XML-Adapter erzeugt aus den Rohdaten einen XML-Container (3) und leitet diesen an das Archiv-Gateway, das ArchiSafe-Modul, weiter

(4). Je nach konkreter Architektur fällt bei den Schritten (3) oder (4) die Identifizierung und Authentifizierung gegen das Archivsystem an, welche das ArchivSafe-Modul prüft (5).

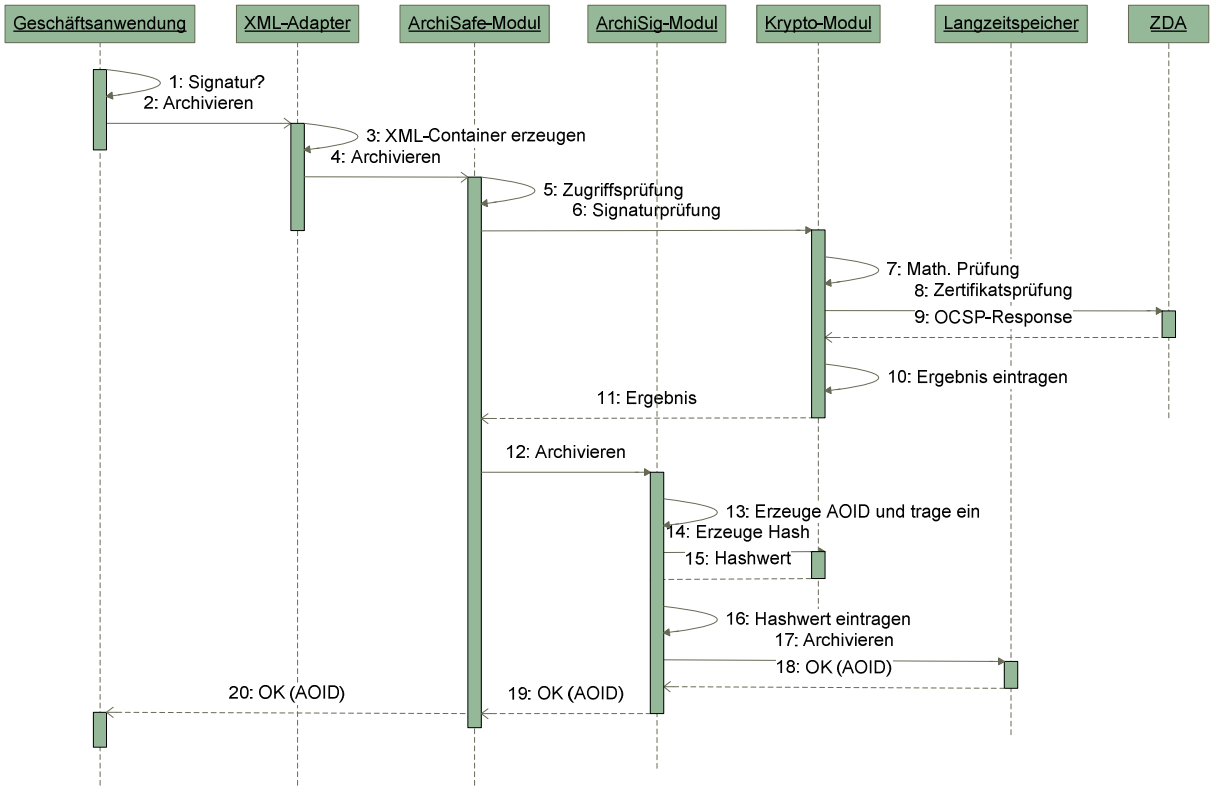

Abbildung 6: Typischer Archivierungsablauf

Falls die Nutzdaten eine Signatur enthalten, leitet das ArchiSafe-Modul die Daten zur eigentlichen Signatur-Prüfung an das Krypto-Modul weiter (6). Hier erfolgt die rein mathematische Verifikation der Signatur (7) sowie die Prüfung der Zertifikate (8), (9). Das Krypto-Modul trägt die Ergebnisse der Prüfung sowie alle dabei angefallenen Beweisdaten (z.B. die OCSP-Responses) in den XML-Container in die CredentialsSection ein (10). Der XML-Container wird wieder an das ArchiSafe-Module zurück geliefert (11) und anschließend an das ArchiSig-Module übergeben (12). Dieser Schritt ist insofern wichtig, da nur so eine unmittelbare Aufnahme in den Hash-Baum sichergestellt ist. Das ArchiSig-Modul erzeugt nun eine eindeutige ID für den XML-Container, die Archive Object ID – AOID, und trägt diese in den XML-Container ein (13). Erst jetzt wird der Container wieder an das Krypto-Modul übergeben, damit dieses einen Hash-Wert darüber bilden kann (14), (15). Das ArchiSig-Module fügt den erzeugten Hash-Wert dem Hash-Baum hinzu (16) und speichert den XML-Container final im Langzeitspeicher (17). Die Rückgabewerte enthalten mindestens die AOID, mit deren Hilfe die Geschäftsanwendung zu einem späteren Zeitpunkt wieder auf den XML-Container zugreifen kann (18), (19), (20).

5 Zusammenfassung und Ausblick

Die Technische Richtlinie definiert und spezifiziert erstmalig in einem umfassenden und modular angelegten Gesamtkonzept hersteller- und produktunabhängig, rechtliche und technische Mindestanforderungen an die Entwicklung und Einführung vertrauenswürdiger und rechtssi-

cherer elektronischer Archivsysteme. Sie beschreibt und spezifiziert einen Katalog weiterer Anforderungen, deren Umsetzung für eine langfristige rechtssichere Archivierung elektronischer Daten und Dokumente beachtet werden sollen und können.

Die Technische Richtlinie erläutert darüber hinaus ausführlich, wie die für eine rechtssichere Ablage elektronischer Daten erforderlichen kryptographischen Operationen und Funktionen auf der Grundlage des eCard-API Frameworks [BSI08] umgesetzt werden können [HFG+09].

Die Technische Richtlinie definiert schließlich die Grundzüge einer funktionalen und technischen Konformitätsprüfung von Komponenten oder ganzen Archivsystemen mit den Zielen und Anforderungen dieser Richtlinie.

Die Technische Richtlinie soll auch in Zukunft kontinuierlich mit Vertretern der öffentlichen Verwaltung und Herstellern funktional und modular ergänzt und fortgeschrieben werden.

Literatur

[BNetzA] Geeignete Kryptoalgorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, jeweils aktuell gültige Fassung, siehe http://www.bundesnetzagentur.de/

[BSI08] Bundesamt für Sicherheit in der Informationstechnik (BSI): eCard-API-Framework, Technische Richtlinie (TR) des BSI Nr. 03112, Teil 1-8, http://www.bsi.de/literat/tr/tr03112/index.htm, 2008

[BSI09] Bundesamt für Sicherheit in der Informationstechnik (BSI): VLA – Vertrauenswürdige elektronische Langzeitarchivierung, Technische Richtlinie (TR) des BSI Nr. 03125, in Vorbereitung, 2009

[CCSD08] The Consultative Committee for Space Data Systems, XML FORMATTED DATA UNIT (XFDU), CCSDS 661.0-B-1, September 2008, siehe unter http://public.ccsds.org/publications/archive/661x0b1.pdf

[FormAnpG] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr, vom 13. Juli 2001, BGBl I, Nr. 35, S. 1542-1549; siehe unter http://www.dud.de/documents/formvorschriften-10713.pdf

[Glad07] Gladney, H. M.: Preserving Digital Information, Springer Publ., 2007

[GoBP07] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), Request For Comments – RFC 4998. http://www.ietf.org/rfc/rfc4998.txt, August 2007

[Gond07] Gondrom, T.: Evidence Record Syntax in: N. Pohlmann et al.: ISSE/SECURE 2007 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, Vieweg + Teubner, 2007, 367 ff.

[HaRo08] Siegfried Hackel und Alexander Roßnagel: Langfristige Aufbewahrung elektronischer Dokumente, in Informationelles Vertrauen für die Informationsgesellschaft, (Hrsg.) D. Klumpp, H. Kubicek, A. Roßnagel und W. Schulz, Springer-Verlag, 2008, SS. 199-207

[HFG+09] Detlef Hühnlein, Stefanie Fischer-Dieskau, Utz Gnaida, Ulrike Korte, Peter Rehäußer, Wolf Zimmer, Langfristig beweiskräftige Signaturen mit dem eCard-API-Framework, im vorliegenden Tagungsband D-A-CH Security 2009

[JKomG] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) in der Fassung der Bekanntmachung vom 22. Marz 2005 (BGBl. IS. 837)

[Merk80] Ralph Merkle: Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA), SS. 122-134, 1980

[OAIS02] CCSDS 650.0-B-1: Reference Model for an Open Archival Information System (OAIS). Blue Book (Standard). Issue 1. January 2002. siehe unter http://public.ccsds.org/publications/archive/650x0b1.pdf

[PhBs08] Physikalisch-technische Bundesanstalt, Bundesamt für Sicherheit in der Informationstechnik, Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents Version 1.0, 2008, siehe http://www.bsi.bund.de/cc/pplist/pplist.htm#PP0049

[RFJK07] A. Rossnagel, S. Fischer-Dieskau, S. Jandt, M. Knopp: Langfristige Aufbewahrung elektronischer Dokumente, Band 17 der Reihe „Der elektronische Rechtsverkehr“, 1. Auflage, Nomos-Verlag, 2007.

[RoSc05] Alexander Roßnagel und Paul Schmücker: Beweiskräftige elektronische Archivierung - Bieten elektronische Signaturen Rechtssicherheit? Ergebnisse des Forschungsprojekts „ArchiSig“, Economica Verlag, 2005

[SigG] Gesetz über die Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG) vom 16.5.2001, BGBl. 2001, Teil I Nr. 22, S. 876 ff., geändert durch Art 1 G v. 4.1.2005 I 2, siehe unter http://www.bundesnetzagentur.de/media/archive/2247.pdf

[SigV] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001, BGBl. 2001, Teil I Nr. 59, S. 3075 ff., geändert durch Art 2 G v. 4.1.2005 I 2,
siehe unter http://www.bundesnetzagentur.de/media/archive/5264.pdf

[VERS95] Victorian Electronic Records Strategy, siehe unter http://www.prov.vic.gov.au/vers

[VwVfG] Verwaltungsverfahrensgesetz (VwVfG) in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), geändert durch Artikel 4 Abs. 8 des Gesetzes vom 5. Mai 2004 (BGBl. IS. 718), siehe unter www.gesetze-im-internet.de/bundesrecht/vwvfg/gesamt.pdf

[ZPO] Zivilprozessordnung, siehe unter www.gesetze-im-internet.de/zpo