Vertrauenswürdige VoIP Archivierung nach DIN-31644

Philipp Kathmann · Giacomo Gritzan
Olav Hoffmann · Richard Sethmann

Hochschule Bremen
{philipp.kathmann | giacomo.gritzan | olav.hoffmann
richard.sethmann}@hs-bremen.de

Zusammenfassung

Im Rahmen des BMWi-Forschungsprojektes[1] Integrität und Nicht-Abstreitbarkeit multimedialer VoIP-Streams (INTEGER[2]), soll unter anderem untersucht werden, wie eine vertrauenswürdige Langzeitarchivierung der erfolgten Gespräche in Deutschland realisiert werden kann. In dieser Veröffentlichung wird ein Überblick über die Grundlagen der vertrauenswürdigen Langzeitarchivierung in Deutschland gegeben. Für die im Rahmen von INTEGER entwickelte Kommunikationslösung werden unter der Anwendung von DIN-31644[3] Anforderungen an die Anwendung erarbeitet. INTEGER basiert auf einem Hardwarevertrauensanker, dem Trusted Platform Module (TPM). Es kann gezeigt werden, dass die DIN-31644 zur Herleitung von Anforderungen an eine vertrauliche Langzeitarchivierung im Anwendungsfeld multimedialer Kommunikation, im speziellen VoIP, geeignet ist und die entsprechenden Anforderungen exemplarisch für das Projekt INTEGER angewendet werden können. Im weiteren Verlauf von INTEGER muss evaluiert werden, ob und wie ein Lösungskonzept, sowie eine prototypische Umsetzung basierend auf den aus DIN-31644 resultierenden Anforderungen, im Rahmen des Projekts erfolgen kann.

1 Einleitung und Motivation

Viele Verbraucher sind schon einmal in der Situation gewesen, dass sie Vertragsänderungen oder Vertragsabschlüsse über ein Call-Center abwickeln mussten. Auf die Aufzeichnung der Gespräche haben Verbraucher im Nachhinein oftmals keinen Zugriff. Sie sind daher darauf angewiesen, dass die besprochenen Einzelheiten korrekt vom jeweiligen Hotline-Mitarbeiter in die schriftliche Form übernommen werden. Im Rahmen von INTEGER, das sich mit der Integrität und Nicht-Abstreitbarkeit von internetbasierter multimedialer Kommunikation am Beispiel von VoIP und dessen Aufzeichnung und Archivierung beschäftigt, soll untersucht werden, wie eine vertrauliche Langzeitarchivierung der erfolgten Gespräche realisiert werden kann. Für die sichere Langzeitarchivierung existiert in Deutschland unter anderem die DIN-31644. Diese soll die Vertraulichkeit, Integrität und Authentizität der archivierten Daten und somit z.

[1] Die Autoren danken dem BMWi-ZIM für die Förderung und allen INTEGER-Projektpartnern für die gute Zusammenarbeit.

[2] Das Forschungsprojekt INTEGER https://www.integer-project.de

[3] DIN-31644 – Kriterien für vertrauenswürdige digitale Langzeitarchive

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 192-203.

B. die Wahrung der Details eines besprochenen Vertragsabschlusses oder einer Vertragsänderung für einen Verbraucher gewährleisten. Diese Veröffentlichung nutzt die in der DIN-31644 definierten Kriterien und zeigt, wie diese zur Herleitung von Anforderungen für eine Langzeitarchivierungslösung im Bereich von VoIP-Daten angewendet werden können. Die Norm besteht aus einem allgemeinen Kriterienkatalog und enthält keine konkreten Handlungsanweisungen, wie es in anderen Branchen wie z. B. bei Smart Metering Systemen üblich ist (vgl. [D31612], vgl. [GSHD14]). Der innerhalb von INTEGER beschriebene Ablauf sieht dabei folgendermaßen aus: Zwei Geschäftspartner kommunizieren über eine VoIP-Telefonverbindung und einigen sich im Laufe ihres Gesprächs auf bestimmte Vertragsinhalte. Zu einem bestimmten Zeitpunkt innerhalb dieser Verhandlung wird durch die Geschäftspartner beschlossen, den Vertrag mündlich abzuschließen, um Zeit und Ressourcen zu sparen. Beide Parteien besitzen ein zur Signierung der Gesprächsdaten geeignetes Endgerät, in Form eines Softphones, welches ebenfalls eine im Rahmen von INTEGER entwickelte Identifizierungs- und Authentifizierungsmöglichkeit für die Gesprächspartner zur Verfügung stellt. Der Beginn der Gesprächsaufzeichnung muss von beiden Seiten explizit eingeleitet werden und wird auf dem jeweiligen Telefon signalisiert. Durch das Auslösen der Aufzeichnung wird auch der Signierprozess gestartet: Empfangene Audiodaten werden aus den VoIP-Paketen extrahiert und vom Empfänger signiert. Die Signatur wird vom Absender bestätigt, welcher das Prozedere ebenfalls durchführt. Mindestens eine der beiden am Gespräch teilnehmenden Parteien benötigt ein angebundenes Archiv, um eine Archivierung der Aufzeichnung gewährleisten zu können. Im Rahmen des Prozesses authentifizieren sich beide Gesprächspartner gegenseitig über entsprechende Zertifikate. Das Gespräch wird explizit durch das Drücken eines Buttons auf dem Gerät oder durch Auflegen beendet. Der im Gespräch aufgezeichnete Vertrag wird zur Beweissicherung und Dokumentation durch einen oder beide beteiligten Gesprächspartner archiviert. Kommt es durch einen Fehler zum Abbruch der Vertragsaufzeichnung, werden die bis zu diesem Zeitpunkt angefallenen Daten durch die beteiligten Gesprächspartner ebenfalls archiviert. Das archivierende Softphone verwendet zudem einen Hardwarevertrauensanker, in Form eines Trusted Platform Module (TPM)-Chip der Trusted Computing Group, um die Sequenzen der Gesprächsaufzeichnung durch Signaturen miteinander zu verketten. Die sogenannte Hashkette dient als zusätzlicher Beweis der Integrität der Aufzeichnung (vgl. [Hett06]). Der TPM ist dabei in der Lage, das zur Signierung verwendete Schlüsselmaterial zu schützen und bietet sichere kryptographische Funktionen, welche vom System verwendet werden können (vgl. [BSI018]). Im Fall eines Rechtsstreits über die Inhalte oder die Existenz eines Vertrags kann die entsprechende Aufzeichnung auch vor Gericht verwendet und durch sogenannte „Inaugenscheinnahme“ zur Feststellung beweiserheblicher Tatsachen dienen. Eine Inaugenscheinnahme ist jede sinnliche Wahrnehmung von Beweismitteln, wozu auch akustische Abläufe gehören. Ein technischer Gutachter kann anhand der Aufzeichnung nachweisen, ob die digitale Signatur gültig und in einem unveränderten Zustand ist. Hierdurch werden die Existenz und der entsprechende Inhalt des Gesprächs nachgewiesen. Das in dieser Arbeit beschriebene Archiv stellt für die Gesprächsteilnehmer, neben einer Langzeitarchivierung, eine Überprüfungsmöglichkeit für die Gesprächsdaten zur Verfügung.

2 Literatur zur vertrauenswürdigen Archivierung

Es existieren unterschiedliche Standards und Normen, die sich mit der Langzeitarchivierung digitaler Daten beschäftigen. Die in dieser Arbeit genauer betrachtete DIN-31644 basiert im Wesentlichen auf ISO-14721 (OAIS – Open Archival Information Systems). Diese beschreibt ein Referenzmodell für ein dynamisches, erweiterbares Archivinformationssystem und wurde

2012 als ISO-Standard veröffentlicht. Hierzu stellt OAIS ein normiertes Vokabular, Konzepte und Modelle bereit, welche zur Kommunikation der Problematik der digitalen Langzeitarchivierung und passender Lösungsansätze dienen (vgl. [Schr12], vgl. [ISO112]). Eine weitere Verordnung welche in allen EU-Mitgliedsstaaten Anwendung findet, ist die Signaturverordnung eIDAS. Diese definiert einen grenzübergreifenden EU-Standard für die Signierung und die Beglaubigung elektronischer Dokumente. Die eIDAS-Verordnung trat am 17.09.2014 in Kraft und hob damit das damalige deutsche Signaturgesetzt und die EU-Signaturrichtlinie 1999/93/EG auf. Anzuwenden ist die Verordnung seit dem 01.07.2016. und „legt einen Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung fest“ [eIDA14, Artikel 1.c]. Weiter regelt eIDAS die europaweite Anerkennung elektronischer Identifizierungsmittel für natürliche und juristische Personen und spezifiziert Vorschriften für Vertrauensdienste (vgl. [eIDA14]). Die DIN-31645 beschreibt den Prozess der Übernahme von Informationen aus bereits bestehenden Informationssystem in ein Langzeitarchiv. Dabei wird vor allem die organisatorische Ebene dieser Problematik betrachtet. Hierzu definiert die Norm organisatorische Leitlinien für die Informationsübernahme und verweist darauf das für dessen Anwendung sowohl DIN-31644 als auch die ISO-14721 erforderlich sind. Da der Fokus dieser Veröffentlichung aber auf der direkten Übernahme der Daten vom Softphone, ohne eine vorherige Zwischenspeicherung in einem zusätzlichen Informationssystem liegt, wurden zur Erarbeitung der an das Archiv zu stellenden Anforderungen stattdessen die DIN-31644 und dass aus der ISO-14721 stammende OAIS Modell verwendet (vgl. [D31611]). Eine weitere in diesem Problemfeld vorhandene Norm ist die DIN-31646 diese ermöglicht die Prüfung der Vertrauenswürdigkeit von PI[4]-Systemen welche eine zuverlässige Identifizierung und Adressierung von archivierten Objekten gewährleisten. Auch diese Norm enthält normative Verweise zu DIN-31644, DIN-31645 und ISO-14721, wird aber im Rahmen dieser Veröffentlichung nicht weiter betrachtet (vgl. [D31613]). Weiterhin ist auch der Erhalt des Beweiswerts von kryptografisch signierten Dokumenten für ein Langzeitarchiv maßgeblich, hierfür legt die DIN-31647 fachliche und funktionale Anforderungen fest und ergänzt ein digitales Langzeitarchiv somit um Funktionen, die für den Erhalt des Beweiswerts der Daten notwendig sind. Somit könnte nach der Erarbeitung des Archivs nach DIN-31644 eine Betrachtung nach der DIN-31647 erfolgen, um die auch im speziellen Fall des INTEGER-Projekts umzusetzende Nachsignierung dementsprechend abzugleichen (vgl. [D31615]). Die technische Richtlinie TR-03125 des BSI[5] beschreibt eine IT-Komponente zur Beweiserhaltung kryptografisch signierter elektronischer Dokumente. Diese hat dabei nicht das Ersetzen von etablierten Anforderungen und Begriffsdefinitionen im Fokus, sondern definiert vielmehr das Konzept einer Middleware, welche die Funktionen zur kryptografischen Beweiserhaltung signierter elektronische Dokumente bündelt. Die Richtlinie richtet sich dabei vor allem an Bundesbehörden und besitzt darüber hinaus auch empfehlenden Charakter und kann somit für bereits bestehende Archive die Beweiserhaltung der signierten elektronischen Dokumente sicherstellen (vgl. [T03118]). Da die Richtlinie das Konzept einer Middleware umsetzt und im Kontext des INTEGER-Projekts beschlossen wurde auf Zeitstempel einer vertrauenswürdigen dritten Instanz zu setzen, findet die Richtlinie im Projekt, sowie in diese Veröffentlichung keine Verwendung.

[4] Persistent Identifier

[5] Bundesamt für Sicherheit in der Informationstechnik

3 Vertrauenswürdige Langzeitarchivierung

3.1 Die Archivblöcke

Das Resultat des Signierprozesses sind insgesamt drei verschiedene Datenblöcke *Archiv-Metadaten-Block, Archiv-Block* und *Archiv-Stop-Block* siehe Abbildung 1.

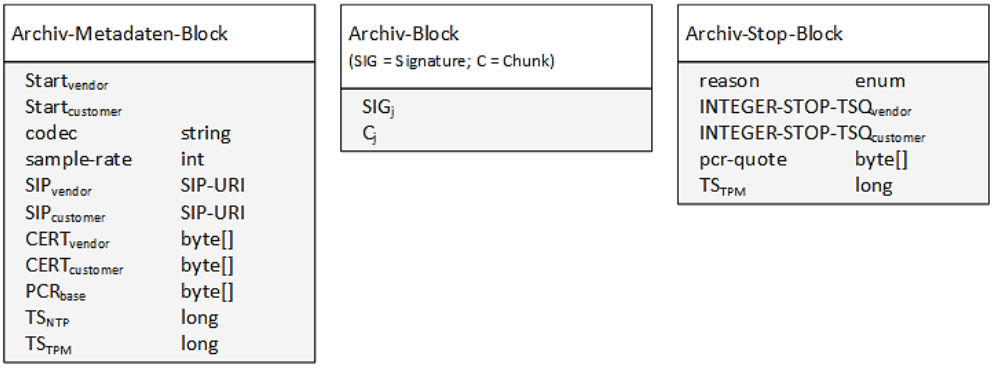

Abb. 1: Archivierungsblöcke

Der *Archiv-Metadaten-Block* wird pro Signierungssitzung einmalig erstellt und wird zum Start einer Archivierungssitzung an das Archiv übertragen. In ihm sind alle Metadaten enthalten, die das Archiv benötigt, um ein Gespräch zu identifizieren und später wiederzugeben. Die beiden Start-Blöcke der Gesprächspartner dokumentieren die Parameteraushandlung zu Beginn der Signierungssitzung. Zudem wird z. B. die maximale Größe des jeweiligen Chunks[6] benötigt, um die archivierten Daten später interpretieren zu können. Das Feld PCR[7]$_{base}$ enthält den zum Zeitpunkt des Beginns der Signierungssitzung gültigen Wert des TPM PCRs, das zur Bildung der Hashkette verwendet wird. Dieser Startwert ist für eine spätere Verifikation des Archivinhalts unter Verwendung der Hashkette notwendig. Der NTP-Zeitstempel TS[8]$_{NTP}$ beschreibt die lokale Zeit des jeweiligen Gesprächspartners, zu der die Signierungssitzung begonnen wurde. Der TPM-Zeitstempel TS_{TPM} ist der Wert des TPM-Zeitgebers zu genau diesem Zeitpunkt. Er wird benötigt, um mit dem entsprechenden Wert aus dem Archiv-Stop-Block die genaue Dauer der Signierungssitzung zu ermitteln.

Der *Archiv-Block* enthält jeweils einen Chunk-Block, welcher Audioinformationen, die Blocknummer und die dazugehörige Signatur beinhaltet. Er wird dazu verwendet die Gesprächsdaten an das Archiv zu übertragen.

Mit dem *Archiv-Stop-Block* wird eine Archivsitzung beendet. Er enthält den Grund der Beendigung, z.B. einen technischen Fehler oder einen ordentlichen Abschluss. Weiterhin ist der qualifizierte Zeitstempel mit den Signaturen beider Teilnehmer enthalten, sofern dieser erstellt werden konnte. Im Falle eines Abbruchs können ein oder beide Felder keine Daten enthalten. Zusätzlich beinhaltet der Datenblock den PCR-Endwert des TPM und den Wert des TPM-Zeitgebers TS_{TPM} zum Zeitpunkt der Beendigung der INTEGER-Sitzung. Die Kombination aus einem Archiv-Metadaten-Block, mehreren Archiv-Blöcken und einem Archiv-Stop-Block wird in einzelnen Sequenzen an das Archiv übertragen und muss von diesem gespeichert werden.

---

[6] Teilstück der stattfindenden Kommunikationsdaten

[7] Platform Configuration Register eines TPM-Moduls

[8] Time Stamp

3.2 Der Überprüfungsprozess

Durch den Überprüfungsprozess kann das Archiv oder ein unabhängiges System die aus dem Signierprozess erzeugten Blöcke im Nachhinein überprüfen. Die dazu benötigten Informationen sind in den Blöcken selbst enthalten. Somit ist es möglich sicherzustellen, dass die enthaltene Audioaufzeichnung ihren Urhebern zugeordnet und gleichzeitig eine nachträgliche Manipulation der Daten ausgeschlossen werden kann.

3.2.1 Überprüfung der gegenseitigen Signierung

Im ersten Schritt werden die im Archiv-Metadaten-Block enthaltenen Zertifikate auf ihre Gültigkeit hin geprüft. Es handelt sich hierbei um Zertifikate vom Typ X.509. Die Überprüfung gliedert sich in vier Teilschritte: Überprüfung der Signatur, Überprüfung der Gültigkeitsdauer, Überprüfung des Widerrufsstatus und Überprüfung des Zertifikatspfades. Somit kann der Initiator einer Sitzung über sein Zertifikat eindeutig zugeordnet werden. Weiter können durch die SIP[9]-URI[10] Initiator und Teilnehmer über den SIP-Provider identifiziert werden. Die Chunk-Blöcke innerhalb der Archiv-Blöcke, welche die Audiodaten enthalten, werden durch die Zertifikate der Gesprächsteilnehmer alternierend signiert. Entsprechende Signaturen sind Teil der Archiv-Blöcke. Die alternierende Signierung wird anhand der zuvor überprüften Zertifikate nachvollzogen. Dabei muss die fortlaufende Blocknummer der Chunk-Blöcke ebenfalls beachtet werden, um sicherzustellen, dass keine Pakete ausgelassen wurden. Der Archiv-Stop-Block enthält den qualifizierten Zeitstempel, welcher durch den Initiator angefordert wird. Dies geschieht in dem der Initiator über die Archiv-Blöcke einen Hashwert bildet. Dieser Hashwert wird an eine vertrauenswürdige dritte Partei[11] gesendet, welche hierfür einen Zeitstempel erstellt und diesen zurückgibt. Durch den Signierprozess wurde dieser Zeitstempel durch Teilnehmer und Initiator signiert. Zur Überprüfung des Zeitstempels werden die Signaturen, die diesen bestätigen, überprüft. Im zweiten Schritt wird sichergestellt, dass der Zeitstempel zum Ergebnis der über die Kette von Daten-Blöcken angewendeten Hashfunktion passt. Somit kann der Erstellungszeitpunkt der Aufzeichnung nachvollzogen und eine Manipulation ausgeschlossen werden.

3.2.2 PCR-Check

Da der PCR-Startwert und der PCR-Endwert bekannt ist, kann nachvollzogen werden, welche Pakete vom TPM des archivierenden Gesprächsteilnehmers signiert wurden. Hierzu wird der PCR-Startwert mit den einzelnen Hashwerten der Archivpakete fortlaufend verknüpft und ein neuer Hashwert gebildet. Das Ergebnis der fortlaufend angewendeten Hashfunktion muss mit dem PCR-Endwert übereinstimmen.

4 Einführung in DIN-31644

Bei der digitalen Langzeitarchivierung sollen Informationen in Form von digitalen Daten über lange Zeiträume hinweg erhalten werden. Die Informationsobjekte werden dabei als digitale Repräsentationen durch Computer verarbeitet und gespeichert. Da es momentan noch keine zeitlich unbegrenzt haltbaren Datenträger gibt, müssen die Repräsentationen der Objekte im Laufe der Archivierung immer wieder auf neue Medien übertragen werden. Das Hauptziel der

[9] Session Initiation Protocol

[10] Adresse von Teilnehmern SIP-basierter Gespräche

[11] Qualifizierte Zeitstempel werden von zertifizierten Anbietern ausgestellt.

Langzeitarchivierung ist es dabei die abgelegten Informationen trotz all dieser Übertragungen unverfälscht zu erhalten. Dabei gilt es die archivierten Daten vor dem Verlust oder Minderung ihrer Vertraulichkeit, Integrität und Authentizität zu schützen. Überdies müssen sie gegen Verlust geschützt sowie ihre Verfügbarkeit und Nutzbarkeit gewährleistet werden (vgl. [D31612], S.4). "Herausforderungen für die Langzeitarchivierung stellen, neben den allgemeinen Sicherheitsbedrohungen unter dem Aspekt der Langfristigkeit, besonders die nicht beständige Bindung der Information an die Datenträger, die physische Alterung der Datenträger sowie die rapiden Veränderungen der für die Interpretation der Repräsentationen erforderlichen technischen Infrastruktur dar." ([D31612], S.4). Um diesen Risiken entgegenzuwirken und im speziellen das Risiko eines Verlustes der Informationen zu verhindern, werden organisatorische als auch technische Maßnahmen ergriffen (vgl. [D31612], S.4).

5 Anforderungen nach Kriterien aus DIN-31644

Die Archivanwendung nimmt die im Signierprozess entstehenden Daten entgegen, welche eine signierte Audioaufzeichnung enthalten. Im Folgenden sollen die für die Archivanwendung relevanten Kriterien aus der DIN-31644 ausgewählt und die für sie zutreffenden Inhalte erläutert werden. Der Schwerpunkt liegt dabei in der Erarbeitung der Anforderungen an die Archivierungslösung im Kontext einer Kommunikationsanwendung und der Konzeption der dazugehörigen Archivierungslösung. Somit sollen im Folgenden jene Kriterien, welche vertragliche Verantwortlichkeiten, rechtliche Fragen, finanzielle, personelle und organisatorische Aspekte sowie IT-Struktur und deren Sicherheit betreffen, nicht betrachtet werden. Die Kriterien K2, K6-K12, K20 und K31-K34 wurden daher nicht einbezogen (vgl. [D31612]).

5.1 Auswahl der digitalen Objekte (K1)

Das erste für die Archivanwendung relevante Kriterium laut DIN-31644 ist die Auswahl der Repräsentationsinformationen für die im digitalen Langzeitarchiv abzulegenden Informationsobjekte. Daher ist im INTEGER-Projekt vorgesehen, dass alle Daten archiviert werden müssen, die die Identifikation der Gesprächsteilnehmer, die Überprüfung der Integrität der Daten und die Nicht-Abstreitbarkeit der zu archivierenden Konversation sicherstellen. Zusätzlich müssen bei der Archivierung der Audioinformationen aus der VoIP-Konversation alle für die jeweilige Sitzung relevanten Audiodaten gesichert werden. Im Signierungsprozess fallen weitere Metadaten an, die den Status des Abschlusses der Verbindung belegen. Diese Informationen müssen anschließend ebenfalls gesichert werden (vgl. [D31612]).

5.2 Zielgruppen (K3)

Nach DIN-31644 wird die Identifikation von Zielgruppen empfohlen. Für die Archivanwendung wurden im INTEGER-Projekt drei Gruppen identifiziert: *Initiatoren, Teilnehmer* und *Gutachter*. *Initiatoren* eröffnen Signierungssitzungen und stellen Teilnehmern die archivierte Sitzung zur Verfügung, wenn der jeweilige Teilnehmer kein eigenes Archiv besitzt. Indem er Inhalte an das Archiv übermittelt, nimmt ein Initiator nach DIN-31644 die Rolle des *Produzenten* ([Schr12], S.17) ein und übermittelt somit alle von beiden Gesprächspartnern anfallenden Daten an das eigene Archiv. Gleichzeitig sind Initiatoren nach DIN-31644 aber auch *Nutzer* ([Schr12], S.17), da sie nach dem Abschluss einer Signierungssitzung auf die zuvor aufgezeichneten Daten und die Überprüfungsfunktion des Gesprächs zugreifen. Als Partei, welche

grundsätzlich über ein Archiv verfügen muss, kümmert sich der Initiator auch um eine gegebenenfalls notwendige Nachsignierung der archivierten Daten[12]. *Teilnehmer* können wie Initiatoren ebenfalls über ein eigenes Archiv verfügen, welches zusätzlich zur eigenen Archivierung der Sitzung genutzt werden kann, sie treten daher nach DIN-31644 ebenfalls als *Produzenten* auf. Besitzt der Teilnehmer hingegen kein eigenes Archiv, füllt er laut DIN-31644 allein die Rolle des *Nutzers* aus und ihm wird obligatorisch Zugriff auf das Archiv des Initiators gewährt. Wie der Initiator kann auch der Teilnehmer eine Überprüfung der Vertrauenswürdigkeit der jeweiligen Sitzung durchführen. *Gutachter* werden im Falle von Rechtsstreitigkeiten hinzugezogen und erhalten einen vollständigen Zugriff auf die im Archiv vorliegenden Informationsobjekte. Diese können durch sie auf ihre Vertraulichkeit hin geprüft und ausgewertet werden.

5.3 Zugang (K4)

Aus dem INTEGER-Projekt ergibt sich die Anforderung, dass Kunden, welche nicht selbst über ein Archiv verfügen, Zugriff auf das Archiv ihres Vertragspartners erhalten müssen. Laut DIN-31644 muss allen Zielgruppen auf angemessene Art und Weise der Zugang zum Archiv gewährt werden. Die Archivanwendung sollte die Bereitstellung der archivierten Inhalte und die Möglichkeit zur Überprüfung dieser durch eine im Internet bereitgestellte Webapplikation realisieren, welche wiederum durch eine REST[13]-Schnittstelle auf das Archiv zugreifen würde. Die Aufteilung in REST-Schnittstelle und der dazugehörigen Webapplikation sollte gewählt werden, um eine zukunftssichere Zugangsmöglichkeit zum Archiv zu schaffen. Sie soll gewährleisten, dass bei technologischen Veränderungen der Zugang zum Archiv weiterhin sichergestellt wird, z. B. durch die Erstellung neuer Applikationen unter der Verwendung neuer Technologien, ohne die Notwendigkeit das vorhandene Archivsystem maßgeblich verändern zu müssen.

5.4 Interpretierbarkeit (K5)

DIN-31644 fordert dazu auf Maßnahmen zu definieren, die die langfristige Interpretierbarkeit wenigstens einer archivierten Repräsentation gewährleisten. Im INTEGER-Projekt werden Repräsentationsinformation wie die internen Datenstrukturen dokumentiert und veröffentlicht, um eine langfristige Interpretierbarkeit der Daten gewährleisten zu können. Die Wiederherstellung des Archives muss durch das Bereitstellen von Gebrauchsanweisungen, Installationsanleitungen und Hilfetexte unterstützt werden. Die langfristige Interpretierbarkeit der Metadaten als auch der Inhaltsdaten muss sichergestellt sein. Hierzu sollen offene Standards und Datenformate eingesetzt werden. Somit ist es möglich, auch bei einem Technologiewechsel in der Zukunft eine Kompatibilität zu den historischen Daten zu gewährleisten.

5.5 Signifikante Eigenschaften (K13)

Für die durch das Softphone übersendeten Repräsentationen muss das Archiv für die Langzeitarchivierung relevante, signifikante Eigenschaften für den Erhalt der Informationsobjekte definieren. Die signifikanten Repräsentationsinformationen für die Informationsobjekte sind

---

[12] Eine Nachsignierung der archivierten Daten ist eine Anforderung, die sich aus ([D31615], S. 20) ergibt. Sollte die vom Archiv verwendete kryptographische Einwegfunktion ihre Sicherheitseignung in der Zukunft verlieren, muss eine Nachsignierung stattfinden können.

[13] Representational State Transfer

dabei die folgenden Teile der an das Archiv übertragenden Datenobjekte. Für den konkreten Anwendungsfall sind das *Gesprächsmetadaten, Gesprächsdaten* und *abschließende Pakete*, die erhalten und archiviert werden müssen. Diese werden durch die zuvor erwähnten Datenblöcke übertragen. *Gesprächsmetadaten* beinhalten Informationen, welche die Gesprächspartner identifizieren und die Integrität und Nicht-Abstreitbarkeit der Aufzeichnung überprüfen können, wie die SIP-URI, das zur Signatur verwendete Zertifikate und der PCR-Startwert des Initiators. Weiter werden Informationen über den verwendeten Audiocodec übermittelt, welche zum erneuten Abspielen der Konversation nötig sind. Lokale Zeitstempel stellen ein zusätzliches signifikantes Merkmal dar. *Gesprächsdaten* bestehen aus den vom Softphone extrahierten Audioinformationen mehrerer VoIP-Pakete und der dazugehörigen Signatur. Die *abschließenden Pakete* enthalten den Grund des Abschlusses der INTEGER-Sitzung (Fehlercode oder regulärer Abschluss), die gegenseitigen Bestätigungen der Teilnehmer in Form der Signaturen, den PCR-Endwert nach Abschluss der Signierung und den von beiden Teilnehmern signierten qualifizierten Zeitstempel.

5.6 Integrität: Aufnahme, Archiv und Nutzung (K14 - K16)

Um die Wahrung der Integrität der aus den Transferpaketen stammenden Datenobjekte durch die drei Verarbeitungsphasen Aufnahme (en: Ingest), Archivablage (en: Archival Storage) und Nutzung (en: Access) gewährleisten zu können, sollten nach DIN-31644 die Schnittstellen der Archivanwendung so abgesichert sein, dass Änderungen nur durch authentifizierte und autorisierte Nutzer erfolgen können. Während des Informationsgewinnungsprozesses aus den Datenobjekten der Transferpakete, der Speicherung der Archivpakete und der in ihnen enthaltenden Informationsobjekte sowie deren anschließende Umwandlung zu Nutzungspaketen, sollten während jedem dieser Schritte die Integrität der enthaltenden Informationen durch einen im Archiv enthaltenden Überprüfungsprozess validiert werden siehe Abschnitt 3.2. In der Aufnahmephase sollten zusätzlich Maßnahmen auf Protokollebene ergriffen werden, um eventuell auftretende Paketverluste korrigieren zu können. Während der Archivierungsphase sollte in regelmäßigen Abständen der bereits erwähnte Überprüfungsprozess zu Sicherung der Integrität der abgelegten Daten durchgeführt werden. In der Nutzungsphase muss allen drei Nutzerzielgruppen der Integritätsstatus der Daten mitgeteilt werden, um ihnen eine richtige Interpretation der zur Verfügung gestellten Daten zu ermöglichen.

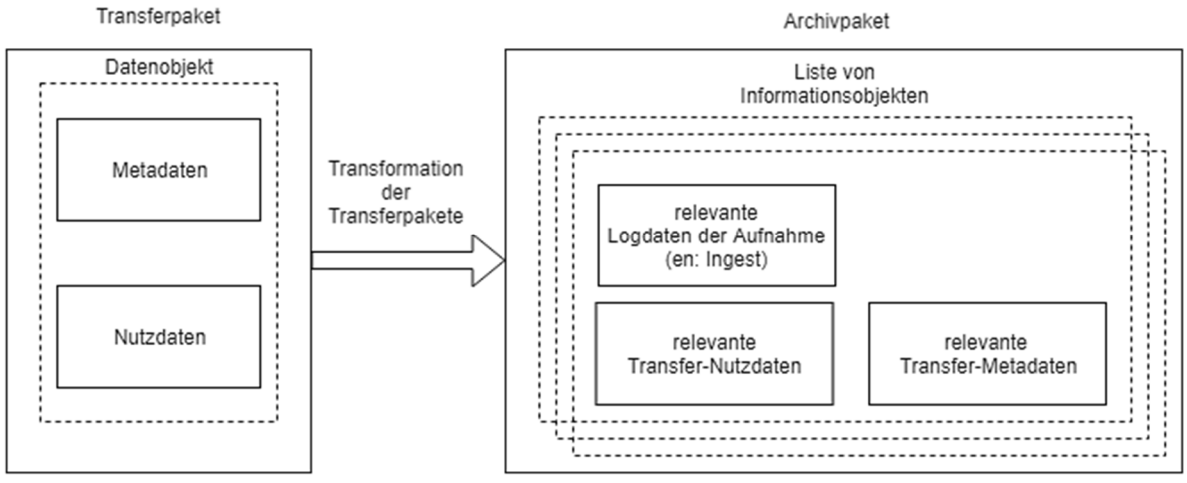

Abb. 2: Transformation von Transferpaketen zu Archivpaketen

5.7 Authentizität: Aufnahme, Erhalt, Nutzung (K17- K19)

Als Authentizität wird laut DIN-31644 verstanden, dass die zu archivierenden Informationen der Repräsentationen auf den drei Stufen *Aufnahme, Erhaltungsmaßnahmen* und *Nutzung* nicht verändert wurden. Bei der *Aufnahme* werden die Informationsobjekte teilweise in ein anderes Datenformat gewandelt. DIN-31644 schlägt hier einen Überprüfungsprozess vor, bei dem der Produzent bestätigt, dass die signifikanten Eigenschaften der ursprünglichen Repräsentationen der Informationsobjekte in den neu hergestellten Repräsentationen erhalten bleiben. Da die Integrität und Nicht-Abstreitbarkeit anhand der Informationsobjekte selbst überprüft werden kann, ist eine Bestätigung hier nicht notwendig, da sie durch die bereits genannten technischen Mechanismen ohnehin gewährleistet wird. *Erhaltungsmaßnahmen:* Zur Archivierung werden die Informationsobjekte in eine neue Repräsentation überführt. Hierbei müssen alle signifikanten Eigenschaften erhalten bleiben. Manipulationen, welche im konkreten Anwendungsfall für die Archivierung nicht notwendig sind, müssen lückenlos nachgewiesen werden. Die Überprüfung der verlustfreien Überführung kann ebenfalls durch den Überprüfungsprozess erfolgen. Auf der Ebene der *Nutzung* werden dem Anwender Informationen über die Herkunft und eventuell durchgeführte Veränderungen zur Verfügung gestellt. Somit kann der Nutzer die Authentizität bewerten. Das Ergebnis des Überprüfungsprozesses muss dem Benutzer ebenfalls visualisiert werden.

5.8 Transferpakete (K21)

Das Kriterium 21 der DIN-31644 sieht die Spezifikation von Transferpaketen vor. Transferpakete beinhalten die ursprünglichen Inhaltsdaten und reichern diese zusätzlich mit Metadaten an, welche beim Transport an das Archiv anfallen. So werden Absender, Versende- und Eingangszeitpunkt zusätzlich in diesen abgelegt.

5.9 Transformation der Transferpakete (K22)

Wie in Abbildung 2 zu sehen, werden die Transferpakete bei der Transformation in Archivpakete mit zusätzlichen Metadaten, in diesem Fall mit den relevanten Logdaten der Aufnahme, angereichert. Weiterhin zeigt Sie mehrere als Informationsobjekte gespeicherte Datenobjekte aus Transferpaketen, welche gesammelt und anschließend einem Archivpaket hinzugefügt werden.

5.10 Archivpakete (K23)

Die Repräsentationsdaten werden beim Übergang von Transferpaketen in Archivpakete in Form von Informationsobjekten nicht verändert. DIN-31644 schlägt die Transformation in Archivdateiformate vor, für Audioformate z. B. WAVE [Micr17]. Die Transformation bzw. Konvertierung des ursprünglichen Bitstroms, der die Audiodaten repräsentiert, würde dazu führen, dass der Überprüfungsprozess nicht mehr zu verwenden ist, da dieser ein unverändertes Bitmuster erwartet. Aus diesem Grund werden die Audiodaten nicht konvertiert. Archivpakete werden dabei typsicher Weise in einer relationalen Datenbank abgelegt.

5.11 Interpretierbarkeit der Archivpakete (K24)

Die Interpretierbarkeit der Archivpakete wird durch die regelmäßige Überprüfung sichergestellt. Sollten Bitfehler erkannt werden, etwa durch einen Festplattendefekt, kann ein Backup

eingespielt werden[14]. Das verwendete Datenformat muss dokumentiert und den Nutzergruppen zugänglich gemacht werden. Durch die Veröffentlichung des Datenformats und die Berücksichtigung offener Standards ist es möglich Inhaltsdaten auch in Zukunft wiederherstellen zu können, im Falle eines Wechsels der Technologie Kompatibilität zu schaffen und Daten losgelöst vom Archiv interpretieren zu können.

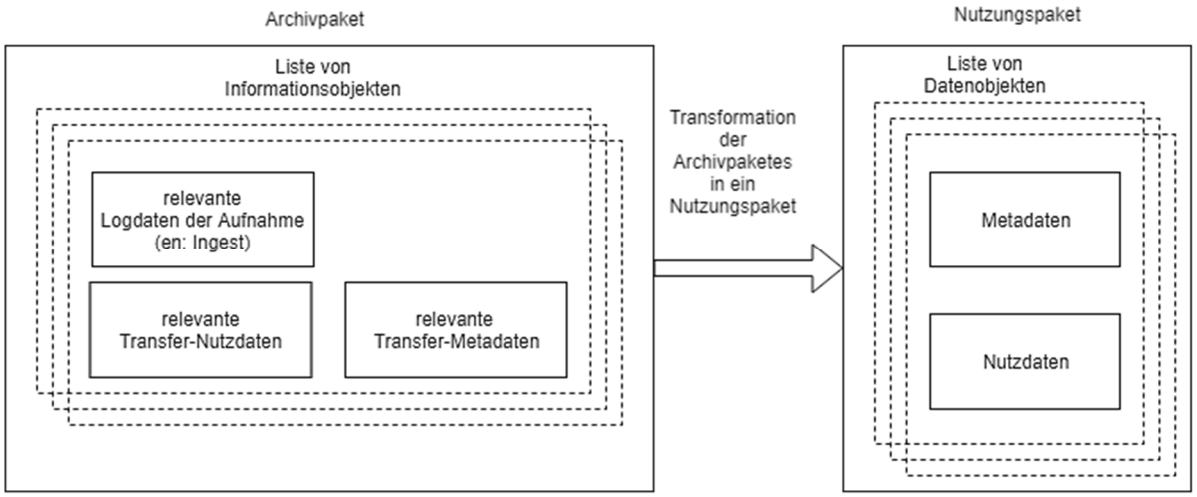

Abb. 3: Transformation der Archivpakete in Nutzungspakete

5.12 Wandlung Archivpakete (K25) & Nutzungspakete (K26)

Bei der Transformation der Archivpakete in Nutzungspakete wird eine vollständige Signierungssitzung für die entsprechenden Benutzergruppen aufbereitet siehe Abbildung 3.

Der Initiator vertraut auf den Überprüfungsmechanismus des Archivs, dessen Ergebnis ihm angezeigt wird. Weiter müssen Metadaten wie das Aufzeichnungsdatum und die Identitätsgebenden Merkmale (SIP-URI, Zertifikate) dargestellt werden können. Weiter wird für diese Benutzergruppe die gespeicherte Audioaufzeichnung in ein gängiges Audioformat konvertiert, um eine komfortable Wiedergabe zu gewährleisten. *Der Teilnehmer* muss die ursprünglichen Datenobjekte, die an das Archiv übermittelt wurden, abrufen können. Zusätzlich werden dem Teilnehmer, analog zum Initiator, aufbereitete Audio- und Metadaten angeboten. *Gutachter* erhalten Zugang zu den ursprünglichen Datenobjekten, welche sie benötigen, um den ursprünglichen Signierprozess seitens der Softphones nachvollziehen zu können. Die Daten können anhand ihrer Signaturen und Zeitstempel auf Validität geprüft werden. Zur Beurteilung der vertrauenswürdigen Archivierung wird dem Gutachter zudem Zugang zu Logdaten gegeben. Somit gibt es drei Ausführungen der Nutzungspakete, welche mit zusätzlichen Metadaten und teilweise mit migrierten Daten ergänzt wurden.

5.13 Identifizierung (K27)

Gemäß DIN-31644 sollen Informationsobjekte und ihre Repräsentationen durch eine eindeutige Kennung intern und extern identifizierbar gemacht werden. Je neu im Archiv abgelegten

[14] Ein geeignetes Backupkonzept für verwendete Datenspeicher wird vorausgesetzt und nicht gesondert behandelt.

Gespräch wird ein neues Archivpaket mit entsprechender UUID[15] angelegt. Die darin enthaltenden Informationsobjekte werden in der Liste bis zum Ende des Gesprächs hinzugefügt und jeder Eintrag enthält jeweils eine UUID zur eindeutigen Identifikation nach innen und außen. Informationsobjekte und ihre Repräsentationen werden durch UUID identifiziert, welche auch zur globalen Identifikation (intern und extern) verwendet werden. Da Archivpakete eine abgeschlossene INTERGER-Sitzung repräsentieren, kann es sinnvoll sein, diese neben der UUID durch einen Alias zusätzlich identifizierbar zu machen.

5.14 Metadatentypen (K28-K30)

Für das Langzeitarchiv müssen nach DIN-31644 drei unterschiedliche Metadatentypen spezifiziert werden *beschreibende Metadaten, strukturelle Metadaten* und *technische Metadaten*. Die *beschreibenden Metadaten* enthalten das vom Archiv verwendete Audioformat und können über zusätzliche Metadaten verfügen. So sollte bei der Verwendung des offenen Standards Opus[16] mit den entsprechenden Metadatenfeldern gearbeitet werden, um beschreibende Informationen zur Audiodatei zu erfassen. *Strukturelle Metadaten:* Innerhalb der Archivanwendung werden insgesamt drei verschiedene Strukturobjekte, das Archivpaket, das Nutzungspaket und das Transferpaket, verwendet. Das Archivpaket enthält eine Liste von Datenobjekten. Das Nutzungspaket enthält, je nach Zielgruppe, unterschiedliche Metadaten, Datenobjekte oder gerierte Metadaten. Das Transferpaket enthält je ein Datenobjekt. Als *technische Metadaten* fallen Protokolldaten an, welche interne Prozesse, wie den Überprüfungsprozess, festhalten. Weiter wird die Nutzung des Archives mit Hilfe eines Logs permanent protokolliert. Somit werden Datenzugriffe und Manipulationen festgehalten und können im Nachhinein nachvollzogen werden.

6 Fazit und Ausblick

In der vorliegenden Arbeit konnten anhand der in DIN-31644 beschriebenen Kriterien Anforderungen für die im Rahmen des INTEGER-Projekts zu entwickelnde Langzeitarchivierungslösung identifiziert und ausgearbeitet werden. Einige der in der DIN-Norm enthaltenen Kriterien befassen sich mit rechtlichen, organisatorischen, finanziellen oder personellen Fragestellungen, welche durch den Betreiber einer späteren Umsetzung bearbeitet werden müssen. Innerhalb des INTEGER-Forschungsprojektes stehen hingegen hauptsächlich die technischen Anforderungen an die zu entwickelnde Archivanwendung im Fokus. Die Anforderungen in dieser Veröffentlichung können einen potenziellen Betreiber bei der praktischen Umsetzung einer Langzeitarchivierung von VoIP-Daten in Bezug auf das Projekt INTEGER unterstützen. Im nächsten Schritt folgt nun die Entwicklung eines entsprechenden Architekturkonzeptes, dass im Rahmen von INTEGER umgesetzt werden soll. Da durch die Archivanwendung fortlaufend Logdaten generiert werden, die unter anderem Benutzerzugriffe und Informationen über erfolgte Konvertierungsvorgänge enthalten, muss sichergestellt werden, dass diese, für die vertrauliche Langzeitarchivierung wichtigen Daten, vor Manipulation geschützt werden. Im Projektkontext werden bereits qualifizierte Zeitstempel eingesetzt, um spätere Manipulationen und Rückdatierungen nachweisen zu können. Die Qualifizierten Zeitstempel haben aber den Nachteil, dass pro Anforderung Kosten für den Inhaber des Archivs entstehen, welche sich über die Zeit aufsummieren. Ein Lösungsansatz hierfür könnte z. B. die Verwendung qualifizierter Zeitstempel in Kombination mit einem Hardwarevertrauensanker

[15] Universally Unique Identifier

[16] http://opus-codec.org/

innerhalb des Archives sein, um alle an den Daten durchgeführten Änderungen in einem Hash-Baum miteinander zu verknüpfen und nur in regelmäßigen Abständen mit qualifizierten Zeitstempeln abzusichern. Weiterführend sollten wie bereits erwähnt ergänzend sowohl DIN-31646 als auch DIN-31647 Beachtung finden, um eine dauerhafte zuverlässige Identifizierung/Adressierung und den Erhalt des Beweiswerts der Daten sicherzustellen.

Literatur

[GSHD14] Genzel, Sethmann, Hoffmann, Detken: Sicherheitskonzept zum Schutz der Gateway-Integrität in Smart-Grids. in V. Lotz, E. Weippl (Hrsg.): Sicherheit 2014 – Sicherheit, Schutz und Zuverlässigkeit, GI-Edition (2014).

[Hett06] C. Hett: Security and Non-Repudiation for Voice-over-IP conversations (2006).

[D31612] DIN-31644 Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive (2012).

[D31611] DIN-31645 Information und Dokumentation – Leitfaden zur Informationsübernahme in digitale Langzeitarchive (2011).

[D31613] DIN-31646 Information und Dokumentation – Anforderungen an die langfristige Handhabung persistenter Identifikatoren (Persistent Identifier) (2013).

[D31615] DIN-31647:2015-05 Information und Dokumentation – Beweiswerterhalt kryptografisch signierter Dokumente (2015).

[eIDA14] Europäisches Parlament und Rat: Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, (2014).

[T03118] Bundesamt für Sicherheit in der Informationstechnik: Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), TR 03125 V. 1.2.1, https://www. bsi. bund. de/ DE/ Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, (2018).

[Schr12] S. Schrimpf: Das OAIS-Modell für die Langzeitarchivierung: Anwendung der ISO 14721 in Bibliotheken und Archiven (April 2012).

[ISO112] International Organization for Standardization: ISO 14721:2012; Space data and information transfer systems - Open archival information system - Reference model, 2nd Edition, 2012.

[Micr17] Microsoft Developer Network: WAVEFORMAT, https://msdn.microsoft.com/ en-gb/en-%20us/library/ms713498(VS.85).aspx, (abgerufen: 28 März 2018).

[BSI018] Bundesamt für Sicherheit in der Informationstechnik: Das Trusted Platform Module (TPM) und vertrauenswürdige Informationstechnik, https://www.bsi.bund. de/ DE/ Themen/ Cyber-Sicherheit/ Aktivitaeten/ TrustedComputing/ Trusted Platform ModuleTPM/ dastrustedplatformmoduletpm_node.html, (abgerufen: 04 Juni 2018)