einheitliches XML-basiertes Transportverfahren

Sicherheit und Verfügbarkeit in einem eXTra-spezifischen Datenübermittlungsverbund

Version 1.0

Final

Herausgeber:

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e. V.
Düsseldorfer Str. 40
65760 Eschborn
Vereinsregister 73 VR 5158, Amtsgericht Frankfurt am Main
Telefon: 0 61 96/4 95-3 74
Fax: 0 61 96/4 95-3 51
Mail: info@awv-net.de
Web: www.extra-standard.de, www.awv-net.de.

Das vorliegende Dokument zum einheitlichen XML-basierten Transportverfahren „eXTra“ wurde von Mitarbeiterinnen und Mitarbeitern des AWV-Arbeitskreises 2.1 „Vereinheitlichung von Datenübermittlungssystemen“ im Fachausschuss 2 „Verwaltungsvereinfachung und Entbürokratisierung im personalwirtschaftlichen Umfeld“ entwickelt.

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Allgemeines

Eine der wichtigsten Aufgaben eines Datenübermittlungsverbundes ist, die Sicherheit des gesamten Verfahrens im laufenden Betrieb sicher zu stellen, d.h. eine angemessene Security Policy zu formulieren und die zu deren Umsetzung erforderlichen Komponenten einzusetzen.

Zur Security Policy in einem Datenübermittlungsverbund gehören im engeren Sinn die Themenbereiche

- Registrierung der Teilnehmer,
- Authentifizierung der Teilnehmer,
- Vertraulichkeit der Daten und
- Nachweis der Urheberschaft und Integrität der Daten,

welche mit bestimmten Verfahren (z.B. Signatur- und Verschlüsselungsverfahren) realisiert sind und die wiederum bestimmte Informationen (z.B. Zertifikate) und Informationsträger (in Software oder in Hardware, z.B. SmartCards) erfordern, die im Rahmen der Registrierung (z.B. von einer autorisierten Stelle, idR einem TrustCenter) ausgegeben werden.

Zur Sicherheit im weiteren Sinnen gehören folgende Themenbereiche, die für den täglichen, möglichst störungsfreien und wirtschaftlichen Betrieb von großer Bedeutung sind:

- Verfügbarkeit des Gesamtsystems
- Nachvollzug von Vorgängen

Welche Security-Policy für einen Datenübermittlungsverbund adäquat ist, hängt vom Sicherheits- und Schutzbedürfnis der Teilnehmer, der angeschlossenen Fachverfahren, der auszutauschenden Daten und den Anforderungen an die Verfügbarkeit des Gesamtsystems ab; die Bandbreite ist entsprechend groß. Verantwortlich für die Security-Policy ist das jeweilige Fachverfahren bzw. das Gremium des Datenübermittlungsverbundes mit entsprechender Entscheidungskompetenz.

Welche Security-Policy für einen konkreten Datenübermittlungsverbund adäquat ist und was sie regeln soll, wird hier nicht betrachtet. Gegenstand der folgenden Betrachtung ist vielmehr, inwieweit die **Anforderungen einer gegebenen Security Policy bei einem Datenübermittlungsverbund** – im Besonderen bei einem eXTra-spezifischen Datenübermittlungsverbund – mit den Sprachmitteln des eXTra Standards umgesetzt werden können.

Hierzu ist erforderlich, das Thema Sicherheit ganzheitlich zu betrachten: Im realen Betrieb eines Datenübermittlungsverbundes tauschen Fachverfahren elektronisch fachliche Daten per DFÜ aus. Die folgende Betrachtung umfasst also unter Berücksichtigung der konkreten Topologie des Datenübermittlungsverbundes alle beteiligten (Teil-) Systeme und Instanzen, die auf dem Weg der fachlichen Daten vom erzeugenden bis zum verwertenden Fachverfahren durchlaufen werden.

Ausgehend von einem abstrakten Architekturmodell und von drei exemplarischen Topologiebeispielen wird die Problematik der Sicherheit, der Verfügbarkeit und des Nachvollzugs bei einem allgemeinen Datenübermittlungsverbund geschildert. Im abschließenden Kapitel 4 werden diese Problemstellungen bei einem eXTra spezifischen Datenübermittlungsverbund untersucht und dargestellt, welche Unterstützung der eXTra Standard hierbei leisten kann.

2. Ausgangspunkt

2.1. Das Architekturmodell

Ausgangspunkt ist das abstrakte Architekturmodell eines allgemeinen Datenübermittlungsverbundes. Die Übertragung des allgemeinen Architekturmodells auf einen konkreten Übermittlungsverbund in der Realität wird anhand von drei Topologiebeispielen gezeigt. Das Architekturmodell und die Topologiebeispiele geben den Rahmen für die folgende Diskussion vor.

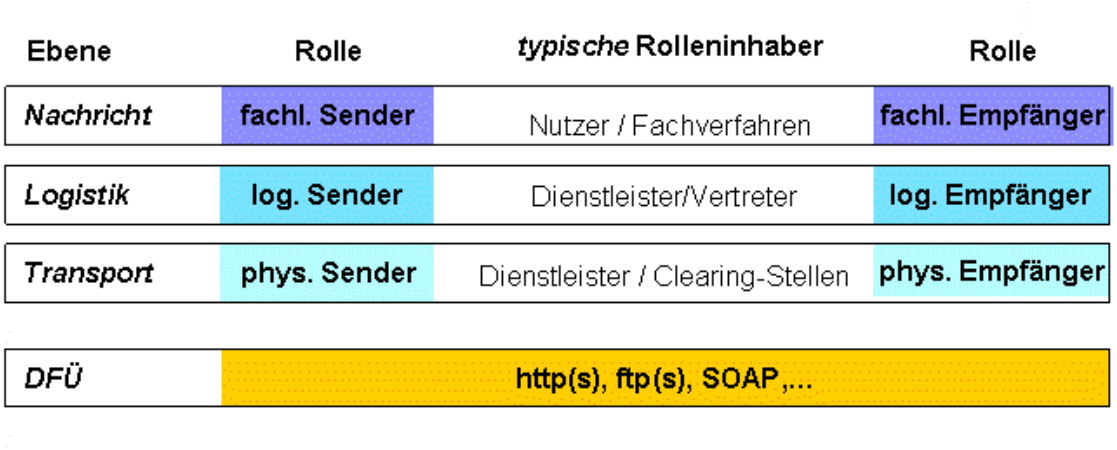

BILD 1: Das abstrakte Architekturmodell eines allgemeinen Datenübermittlungsverbundes sowie die Rollen und die typischen Rolleninhaber.

Das folgende Bild 2 zeigt anhand des Weges der Daten vom Erzeuger – dem fachlichen Sender – bis zum fachlichen Empfänger – dem Verwerter –, in welcher Beziehung die verschiedenen Ebenen zueinander stehen.

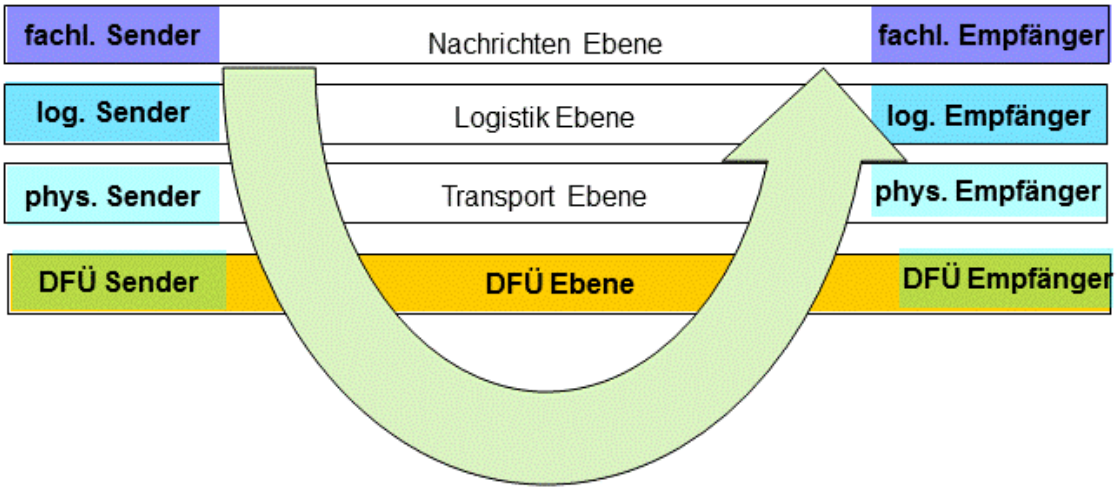

BILD 2: Der Weg der Daten vom Erzeuger (fachliche Sender) zum Verwerter (fachlicher Empfänger).

Bild 2 zeigt weiterhin, dass es für die einzelnen Instanzen, wie z.B. dem fachlichen Sender, sowohl eine vertikale, direkte Kommunikationsbeziehung zum logischen Sender als auch eine horizontale, indirekte Kommunikationsbeziehung zu seinem Gegenpart auf Empfängerseite, dem fachlichen Empfänger, gibt. Die direkte Kommunikation der Sender- mit der Empfängerseite erfolgt ausschließlich über die DFÜ-Ebene. Die einzige direkte horizontale Kommunikationsbeziehung des Datenübermittlungsverbundes ist somit auf der DFÜ Ebene angesiedelt.

2.2. Die Security Domains

Analog zu den Ebenen des Architekturmodells und entsprechend der horizontalen Kommunikationsbeziehung der einzelnen Instanzen sind die Security Domains definiert. D.h., eine Security Domain regelt die Sicherheit der horizontalen Kommunikationsbeziehung einer Ebene.

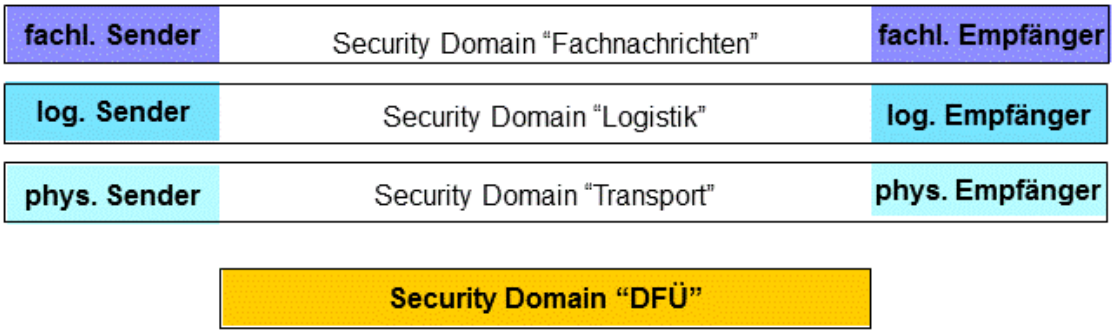

BILD 3: Die Security Domains eines Datenübermittlungsverbundes

Um die Security Policy eines Datenübermittlungsverbundes präzise und problemorientiert formulieren zu können, ist es ideal, wenn die unterschiedlichen Sicherheitsaspekte wie Authentifikation der Teilnehmer, Vertraulichkeit und Nachweis der Urheberschaft sowie Integrität für jede Security Domain getrennt und unabhängig voneinander geregelt werden können. Dabei muss als prinzipielle Rahmenbedingung gelten, dass die Regelungen, die in einer Security Domain gelten, nicht auf dem Weg der Daten über die verschiedenen Ebnen hinweg durch die Security Domains der anderen Ebenen in Frage gestellt, verfälscht oder gar aufgehoben werden können. Der Kontrakt zwischen Sender und Empfänger innerhalb einer Ebene muss auf jeder anderen Ebene erhalten bleiben. Das gezeigte Architekturmodell bietet hierfür den theoretischen Rahmen, um pro Ebene gegebenenfalls unterschiedliche Legitimationsmittel und/oder Verfahren wählen zu können.

Bei der Frage, welche Sicherheitsaspekte bei welcher Security Domain zu beachten sind, ist es sinnvoll, den Wirkungsbereich der jeweiligen Security Domain zu betrachten, der im folgenden Bild 4 gezeigt wird.

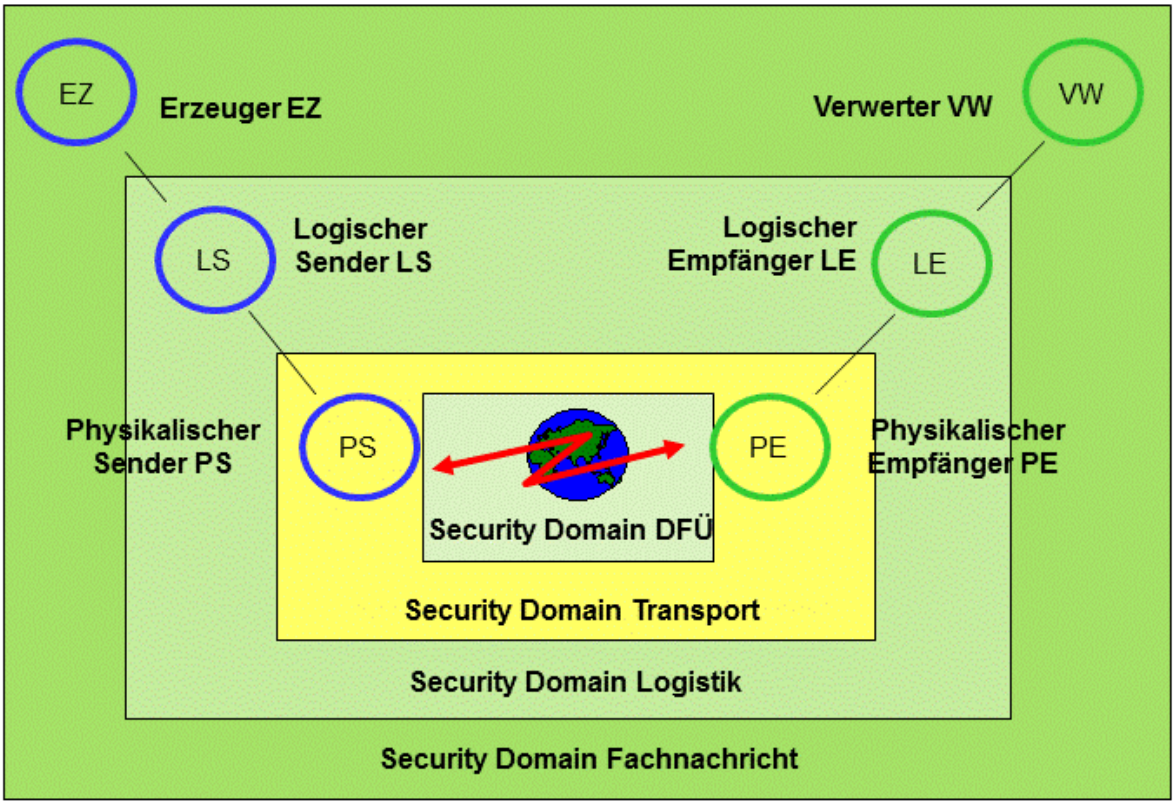

BILD 4: Der Wirkungsbereich der Security Domains eines Datenübermittlungsverbundes

Die Aufgabenstellungen der Security Domains

Bild 4 zeigt, dass zur Aufgabenstellung der Security Domain der Fachnachrichten (der Security Domain mit dem größten Wirkungsbereich) die Vertraulichkeit und Integrität von fachlichen Dokumenten gehört, die ein Erzeuger am Anfang der Kommunikationskette mit einem Verwerter am Ende der Kommunikationskette austauscht. Dies wird als **End-zu-Ende Vertraulichkeit** bzw. **End-zu-Ende Integrität** bezeichnet.

Auf Grund der unterschiedlichen Wirkungsbereiche der jeweiligen Security Domain ist zudem klar, dass jeder Security Domain eine spezifische Aufgabenstellung zugeordnet ist. Zur Aufgabenstellung der Security Domain der Fachnachrichten gehört es, gegebenenfalls die Ende-zu-Ende Vertraulichkeit und/oder Ende-zu-Ende Integrität sicherzustellen. Die primäre Aufgabenstellung der Security Domain DFÜ besteht hingegen darin, zweierlei abzudecken: Einerseits - je nach Datenschutzklasse der fachlichen Daten - gegebenenfalls die Vertraulichkeit und/oder Integrität beim Transport über das gewählte Netz – in der Regel das Internet - sicherzustellen, andererseits die Verfügbarkeit des gesamten Datenübermittlungssystems

dadurch abzusichern, dass insbesondere Bedrohungen und Angriffsversuche aus der Internet Welt - wie z.B. DoS (denial-of-service) Attacken - abgewehrt werden.

Wenn eine konkrete Security Policy für die Security Domain DFÜ bspw.. fordert, dass sich die beiden Kommunikationspartner auf DFÜ-Ebene gegenseitig authentifizieren müssen und für alle über das Internet übertragenen Daten (Steuerungsdaten wie fachliche Daten) das Gebot der Vertraulichkeit zu wahren ist, dann wird damit die Wahl des DFÜ-Protokolls entscheidend beeinflusst. In Frage kommt dann z.B. das DFÜ-Protokoll https, ftps oder darauf aufbauend ein mittels SOAP realisierter Webservice.

Eine naheliegende Strategie der Security-Policy bei der Zuordnung der Sicherheitsaspekte zu den verschiedenen Security Domains ist, möglichst viele Sicherheitsaspekte bereits auf die Security Domain DFÜ und „nur“ die restlichen Sicherheitsanforderungen den anderen Security Domains zu übertragen. In der Empfängersphäre ist das DFÜ-System die erste Instanz, welche die übermittelten Daten entgegennimmt. Wenn dort bereits ein entsprechendes Sicherheitsniveau erreicht werden kann, vereinfachen sich die sicherheitstechnischen Aufgabenstellungen aller weiteren Instanzen.
Auf der anderen Seite sind die sicherheitstechnischen Möglichkeiten der Security Domain DFÜ dadurch begrenzt, weil dort der gesamte übermittelte Bytestrom einheitlich behandelt wird. Eine individuelle sicherheitstechnische Behandlung der in einer Sendung enthaltenen Fachnachrichten übersteigt deshalb dessen Möglichkeiten – dafür wird die Umsetzung des Architekturmodells und dessen Ebenenkonzept mit den zugeordneten Security Domains benötigt.
Damit wird exemplarisch klar, dass keine Security Domain für sich genommen in der Lage wäre alle Sicherheitsaspekte einer Security Policy auf sich zu vereinen – es sei denn, dass die Topologie des Datenübermittlungsverbundes eine Zusammenfassung mehrerer Security Domains zu einer einzigen zulässt (vgl. Kapitel 2.3 Topologie 1).

2.3. Die Topologie und die „eigenständigen Systeme“

Bei der Realisierung eines verbundspezifischen Datenübermittlungssystems gibt es eine große Bandbreite an Gestaltungsmöglichkeiten der Sender- und Empfängersphäre. Dies berührt die Frage, wie die Instanzen der verschiedenen Ebenen auf Sender- bzw. Empfängerseite zu einem oder mehreren „eigenständigen Systemen“ zusammengefasst werden. In einem Extrem sind die Instanzen aller vier Ebenen des abstrakten Architekturmodells in einem einzigen System („all-in-one“, siehe unten Topologie 1) zusammengefasst. Im anderen Extrem ist jede Ebene des abstrakten Architekturmodells als „eigenständiges System“ realisiert (siehe unten Topologie 3).
Die so bezeichneten „eigenständigen Systeme“ innerhalb der Sender- bzw. Empfängersphäre sind u.a. dadurch gekennzeichnet, dass sie über geeignete Schnittstellen miteinander kommunizieren und die spezifischen Sicherheitsaspekte erfüllen müssen, die ihrer Aufgabenstellung zugeordnet sind und die die Security Policy des jeweils angeschlossenen Fachverfahrens fordert.

Sofern die Untergliederung der Sender- bzw. Empfängersphäre in „eigenständige Systeme“ so weitreichend ist, dass die Systeme auch räumlich voneinander getrennt sind (siehe unten Topologie 2 und 3), treten die potentiell spezifischen Sicherheitsaspekte besonders deutlich hervor. In einem solchen Fall ist in den jeweils miteinander kommunizierenden „eigenständigen Systemen“ auch ein DFÜ-System für die vertikale Kommunikation integriert, womit die bei der Security Domain DFÜ geschilderte Problematik in ähnlicher Weise bei jedem örtlich getrennten „eigenständigen System“ auftritt. Jedes derartige „eigenständige System“ muss also sowohl die in der Security Policy festgelegten Sicherheitsaspekte der zugeordneten Security Domain sowohl bei der horizontalen Kommunikation als auch bei der vertikalen Kommunikation benachbarter „eigenständiger Systeme“ erfüllen

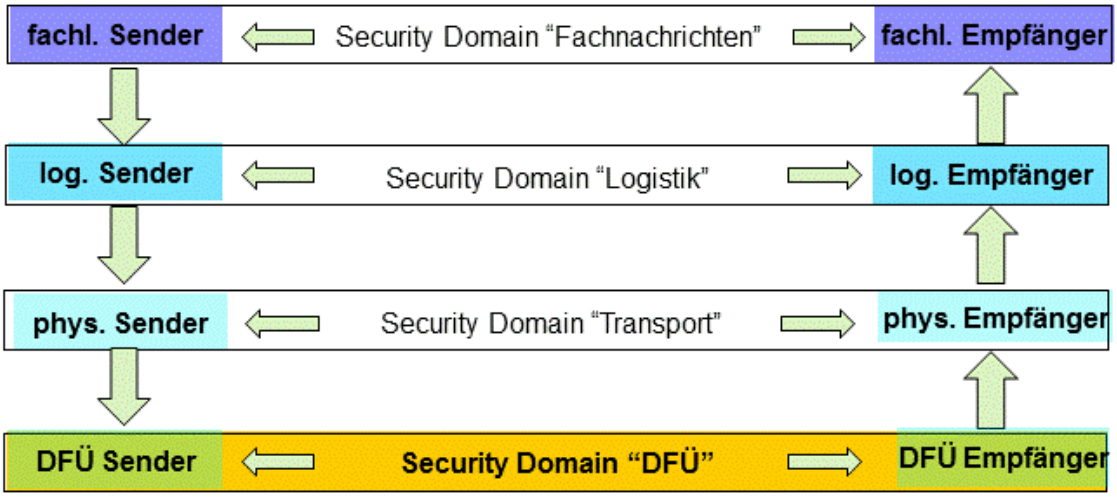

BILD 5: Die Wirkung der horizontalen und vertikalen Kommunikation auf die Ebenen eines Datenübermittlungssystems und deren Security Domains

Exemplarische Topologiebeispiele

Der Einfluss der Topologie auf die Untergliederung der Sender- bzw. Empfängersphäre in „eigenständige Systeme" wird nachfolgend an drei Beispielen verdeutlicht.

Topologie 1: vollintegrierte Anwendungen

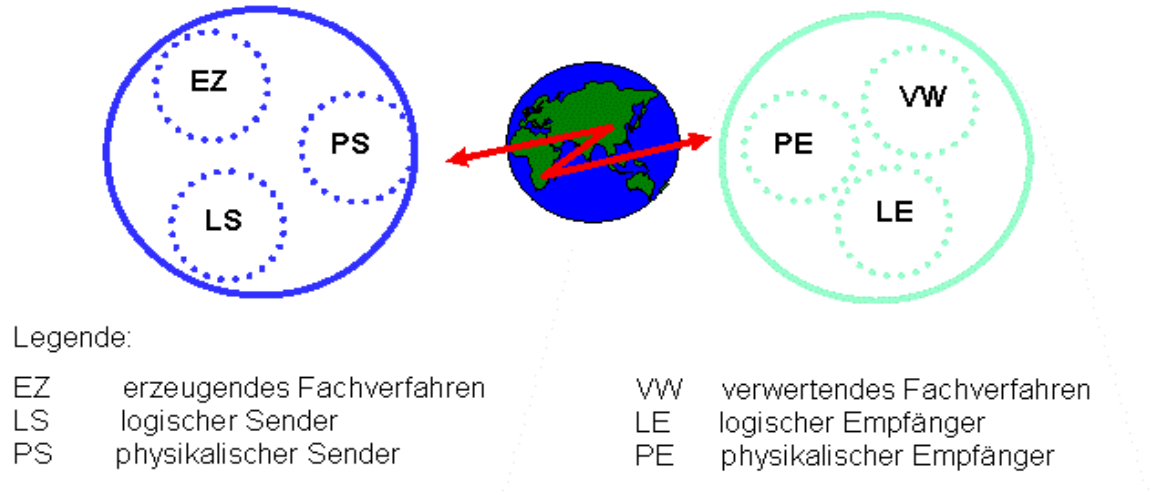

BILD 6: Kommunikation zweier vollintegrierter Anwendungen

Die Anwendung auf Sender- wie auf Empfängerseite ist ein einziges System, in das jeweils das DFÜ-System, der physikalische Sender/Empfänger, der logische Sender/Empfänger und das erzeugende bzw. das verwertende Fachverfahren integriert sind. Entsprechend sind die im abstrakten Architekturmodell vorhandenen vier Security Domains – unabhängig von der tatsächlichen internen Architektur der Anwendung – von außen betrachte zu einer einzigen Security Domain verschmolzen.

Sicherheitstechnisch muss eine solche vollintegrierte Anwendung („all-in-one“) alle Sicherheitsaspekte abdecken, welche die Security Policy fordert.

Topologie 2: Trennung in mehrere „eigenständige Systeme“

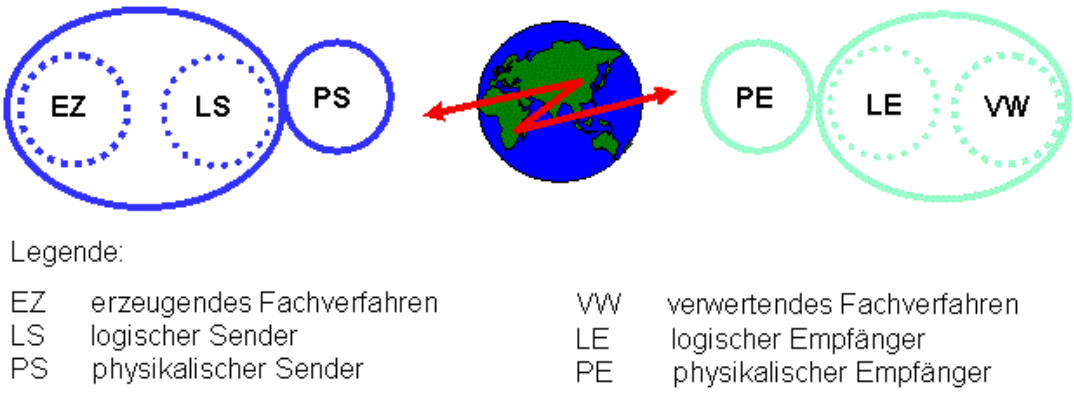

BILD 7: Kommunikation mehrerer „eigenständiger Systeme“

Das erzeugende Fachverfahren auf Senderseite bildet in Bild 7 ebenso wie das verwertende Fachverfahren auf Empfängerseite zusammen mit dem logischen Sender bzw. Empfänger ein „eigenständiges System“, das vom Transportsystem – dem zweiten „eigenständigen System“ – strikt getrennt ist. Im Transportsystem ist der physikalische Sender bzw. Empfänger und das DFÜ-System integriert. In jeder Sphäre gibt es demnach jeweils zwei „eigenständige Systeme“, in denen jeweils von außen betrachte zwei Security Domains zusammengefasst sind, in denen jeweils auch das sicherheitstechnische Problem der vertikalen Kommunikation auftritt.

Ein Beispiel für diese Topologie in der Empfängersphäre ist der Datenübermittlungsverbund der GKV mit dem zentralen GKV-Kommunikationsserver und den einzelnen DAVen (Datenannahme- und Verteilstellen) sowie der Datenübermittlungsverbund der Finanzverwaltung „Elster“ mit der zentralen Elster-Clearingstelle und den einzelnen Bundesländern. In beiden Fällen sind die „eigenständigen Systeme“ räumlich getrennt angesiedelt.

Die sicherheitstechnische Problematik der vertikalen Kommunikation, die bei der Topologie 2 bei einem „eigenständigen Transportsystem“ zu lösen ist, kann bei der folgenden Topologie 3 auf die Kommunikation aller „eigenständigen Systeme“ miteinander per DFÜ übertragen werden.

Topologie 3: völlig verteilte „eigenständige Systeme“

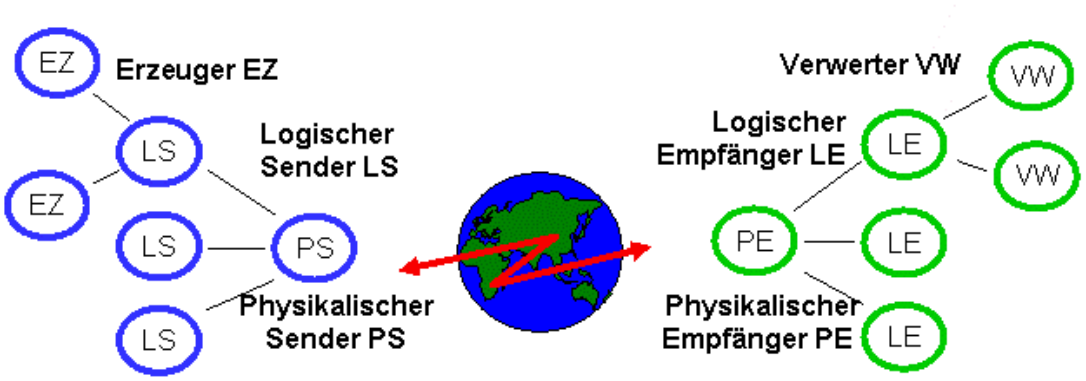

BILD 8: Kommunikation völlig verteilter „eigenständiger Systeme“

Jede Instanz, beginnend mit dem erzeugenden Fachverfahren über den logischen und physikalischen Sender, dem DFÜ-System, dem physikalischen und logischen Empfänger bis hin zum verwertenden Fachverfahren bildet ein „eigenständiges System“.

Als reales Beispiel für diese Topologie ist derzeit in der Sendersphäre nur der Verbund von Kanzleien mit dem DATEV-Rechenzentrum bekannt. Hierbei sind das erzeugende System, der

logische und der physikalische Sender jeweils als „eigenständige Systeme“ angelegt, wobei sich das „eigenständige System“ des logischen und physikalischen Senders am selben Ort befindet.

2.4. Verfügbarkeit, Nachvollzug und Auskunftsfähigkeit

Für die Akzeptanz bei den Teilnehmern und für den wirtschaftlichen Betrieb eines Datenübermittlungsverbundes ist nicht nur die Leistungsfähigkeit des Datenübermittlungssystems und der angeschlossenen Fachverfahren entscheidend, sondern auch die Verfügbarkeit des Gesamtsystems Datenübermittlungsverbund sowie - im Sinne eines effizienten Störfallmanagements - die Existenz von Auskunftsfunktionen mit der Möglichkeit des Nachvollzugs von Vorgängen. Je höher die Verfügbarkeit des Gesamtsystems Datenübermittlungsverbund ist und je besser die technischen Mittel des Störfallmanagements sind, desto größer wird die Akzeptanz der Teilnehmer und die Entlastung der Hotline des Betreibers - mit entsprechend kostendämpfender Wirkung.

Ein Datenübermittlungsverbund ist gehalten, den störungsfreien Betrieb während der definierten Betriebszeiten sicherzustellen bzw. bei kurzfristigen, temporären Störungen Mechanismen zur Verfügung zu stellen, die eine automatisierte Fortsetzung der von der Störung betroffenen Vorgänge ermöglichen (Förderung der „Robustheit“ des Gesamtsystems). Die Verfügbarkeit kann durch gezielte Angriffe von außen – Stichwort Denial-of-Service (DoS) Attacken – in Mitleidenschaft gezogen werden, aber auch durch Fehlfunktionen im Netz oder innerhalb des Datenübermittlungsverbundes selbst.

Angriff auf die Verfügbarkeit von außen

Erfolgt die horizontale Kommunikation zwischen Sender- und Empfängersphäre bzw. die vertikale Kommunikation zwischen „eigenständigen Systemen“ innerhalb der Sender- oder Empfängersphäre über das Internet, so ist der Datenübermittlungsverbund den vielfältigen und unterschiedlichen Angriffen aus der Internetwelt ausgesetzt (z.B. die erwähnten Denial-of-Service [DoS] Attacken). Tauscht der Datenübermittlungsverbund XML-Nachrichten aus, so ist er zudem auch potentiell spezifischen Angriffen ausgesetzt, die gerade auf der XML- und/oder WebService Technologie beruhen. Speziell in diesem Bereich der XML- und WebService-Security gibt es eine Reihe weiterer Herausforderungen, auf die nur prinzipiell aufmerksam

gemacht werden soll. Für eine detaillierte Betrachtung wird im Folgenden auf entsprechende Informationsmöglichkeiten verwiesen.

Ein Großteil der spezifischen Angriffe im Bereich der XML- und WebService-Security (z.B. XML-DoS) kann durch spezielle XML-Firewalls, die dem neustem Stand der Technik entsprechen (meist leistungsfähige Harware-Appliances, welche auf XML-Verarbeitung spezialisiert sind) abgewehrt werden. Speziell zu XML-WebServices-Attacken, die z.B. auf XML-Signature-Wrapping eingehen, sei auf http://ws-attacks.org/ verwiesen. Eine gute Anlaufstelle ist in diesem Bereich auch das Cloud and Web Service Security Lab http://www.clawslab.org/ der Ruhr-Universität Bochum. Die zentrale Anlaufstelle für alle Aspekte von Anwendungssicherheit, die im Rahmen einer XML-Verarbeitung auftreten können, ist das Open-Web-Application-Security-Projekt https://www.owasp.org. Hier sind gängige Attacken (inkl. XML-Bezug) sowie Gegenmaßnahmen und Security-Bibliotheken für alle etablierten Entwicklungsplattformen zu finden.

Eingeschränkte Verfügbarkeit durch Fehlfunktionen im Netz oder innerhalb des Datenübermittlungsverbundes

Im laufenden Betrieb kann es zu temporären Störungen kommen, welche die korrekte Durchführung von einzelnen Übermittlungsvorgängen verhindern. Beim Sender bleibt die Unsicherheit, ob eine Übermittlung vollständig und korrekt beim Empfänger angekommen ist und an das Fachverfahren weitergeleitet werden konnte. Wenn diese Information des Empfängers nicht beim Sender ankam und die Übermittlungsvorgänge an dieses Fachverfahren mit diesem Typus in einer definierten Sequenz stattfinden müssen, ist der Sender für alle weiteren gleichartigen Übermittlungsvorgänge blockiert. Der Betrieb kann erst dann fortgesetzt werden, wenn - in der Regel telefonisch - der Systemzustand beim Empfänger geklärt werden konnte. Gäbe es jedoch einen Mechanismus des Datenübermittlungsverfahrens, mit dem der Sender den tatsächlichen Zustand beim Empfänger erfragen kann, dann könnte er mit diesem Wissen automatisch den Übermittlungsvorgang wiederholen oder mit dem nächsten Vorgang fortfahren. Die temporäre Störung des Betriebs würde dann weder bei der Hotline aufschlagen oder ggf. beim Betriebspersonal zu Eingriffen führen, noch wäre dies für den menschlichen Teilnehmer des Datenübermittlungsverbundes erkennbar.

Nachvollzug und Auskunftsfähigkeit

Wenn der Weg der fachlichen Nachrichten in der Empfängersphäre über mehrere „eigenständige Systeme“ führt (Topologie 2 oder 3), ist keineswegs immer sichergestellt, dass eine fachliche Nachricht auch beim fachlichen Verwerter ankam und dort definiert verarbeitet werden konnte. Der nachweislich rechtzeitige Eingang und Verarbeitung im Fachverfahren ist für den Sender dann von besonderem Interesse, wenn mit dem Ausbleiben oder der verspäteten Abgabe einer fachlichen Nachricht gesetzlich geregelte Sanktionen oder sonstige Strafmaßnahmen verbunden sind. Daher erwarten die Teilnehmer vom Datenübermittlungsverbund entsprechende Mechanismen, um gegebenenfalls die tatsächliche und rechtzeitige Übermittlung sowie die korrekte Verarbeitung der Fachnachrichten durch das verwertende Fachverfahren nachweisen zu können.

Wenn ein Teilnehmer zwar die Bestätigung erhielt, dass seine fachlichen Nachrichten in der Empfängersphäre angekommen sind und weitergeleitet wurden, aber das verwertende Fachverfahren keine Rückmeldung über das Ergebnis der Verarbeitung erstellt hat, wird der Teilnehmer eine Klärung des Sachverhalts fordern. Dies kann über die Hotline erfolgen oder durch Anwendung von Mechanismen des Datenübermittlungsverbundes, mit denen sich der Teilnehmer selbst über den aktuellen Sachstand erkundigen kann (Nachvollzug des Werdegangs des zu klärenden Übermittlungsvorgangs). Danach kann dann gezielt und effizient die Behebung des Problems in Angriff genommen werden.

3. Sicherheit im laufenden Betrieb eines Datenübermittlungssystems

Im folgenden wird erörtert, wie die Festlegungen der Security-Policy eines Fachverfahrens für den laufenden Betrieb und dem zum Einsatz kommenden DFÜ-System umgesetzt werden können, d.h. es werden die Themen Registrierung, Authentifizierung, Vertraulichkeit, Integrität und Nachweis der Urheberschaft behandelt.

Die Frage, ob sich aus Sicht eines Fachverfahrens die Teilnehmer überhaupt registrieren lassen müssen und wie gegebenenfalls der Registrierungsprozess auszugestalten ist, wird nicht erörtert. Wenn also die Security-Policy eines Fachverfahrens festlegt, dass sich die Teilnehmer registrieren müssen, wird davon ausgegangen, dass die Teilnehmer die für eine Teilnahme am

laufenden Betrieb erforderlichen Informationen (z.B. Zertifikate) und Informationsträger (in Software oder in Hardware, z.B. SmartCards) bereits erhalten haben.

Für die Authentifizierung, die Vertraulichkeit, die Integrität und den Nachweis der Urheberschaft wird üblicherweise ein Signatur-, Authentifizierungs- bzw. Verschlüsselungsverfahren eingesetzt, das jeweils auf der Basis von Zertifikaten arbeitet. Dies gilt sowohl für die Instanz DFÜ-System – sofern ein entsprechendes DFÜ-Protokoll wie z.B. ftps, https oder darauf aufsetzend SOAP eingesetzt wird – als auch für die Instanzen der anderen Ebenen. Bei diesen Verfahren wird davon abgeraten, proprietäre Lösungen einzusetzen, da die Weiterentwicklung von Verfahren im Sicherheitsbereich einer hohen Dynamik unterliegen. Um Schritt mit der Weiterentwicklung im Sicherheitsbereich zu halten, ist es ratsam, sich auf entsprechende internationale Standards abzustützen, insbesondere den beiden w3c-Standards XML-Encryption und XML-Signature für Verschlüsselung und Signaturen. Allerdings geht damit ein gewisses Sicherheitsrisiko einher, weil ein Standard erfahrungsgemäß erst mit zeitlicher Verzögerung auf neue Bedrohungen reagieren kann. Die Abwägung, wie hoch dieses Risiko gegenüber den Vorteilen eines Standards einzuschätzen ist, kann nur im Einzelfall anhand der Schutzwürdigkeit der fachlichen Daten bei der Festlegung der Security Policy erfolgen.

Um der hohen Dynamik im Sicherheitsbereich Rechnung zu tragen, ist zudem ratsam, sich nach den Einschätzungen und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu den unterschiedlichen Sicherheitsverfahren und den einzusetzenden Legitimationsmitteln zu erkundigen.
Auf der Homepage des BSI findet man unter http://www.bsi.bund.de/ im Themenbereich „Internet-Sicherheit“ und „Absicherung Datentransport“ entsprechende Informationen.

3.1. Sicherheit bei einer vollintegrierten Anwendung (Topologie 1)

Eine vollintegrierte Anwendung („all-in-one“, vgl. Topologie 1) muss alle in der Security-Policy festgelegten Sicherheitsaspekte abdecken. Eine gewisse Vereinfachung ist dadurch gegeben, dass - von außen betrachtet - nur die Sicherheitsaspekte der Registratur, der Authentifizierung, Vertraulichkeit und Integrität bei horizontale Kommunikation des DFÜ-Systems sowie die Bedrohungsszenarien aus der Internet-Welt relevant sind, nicht hingegen die Problematik bei der vertikalen Kommunikation. Bei der Gestaltung der internen Architektur ist man im Prinzip frei bei der Entscheidung, ob die im Modell existierenden vier Ebenen beibehalten oder ob sie teilweise oder gänzlich miteinander verschmolzen werden und welche interne Komponente dabei welche Sicherheitsaspekte abdecken muss.

Wenn sowohl auf Sender- wie auf Empfängerseite eine solche vollintegrierte Anwendung zum Einsatz kommt, dann kann z.B. allein durch die Wahl des https-Protokolls auf DFÜ-Ebene eine Ende-zu-Ende Vertraulichkeit erreicht werden.

Wenn jedoch nur auf Senderseite eine vollintegrierte Anwendung vorliegt, auf der Empfängerseite jedoch teilweise oder vollständig verteilte „eigenständige Systeme“ existieren (Topologie 2 oder 3), dann spricht manches dafür, einige oder alle Ebenen des Architekturmodells beizubehalten. Dies gilt insbesondere dann, wenn die Security Policy eine Ende-zu-Ende Vertraulichkeit oder Integrität fordert.

3.2. Sicherheit bei teilweise verteilten Instanzen eines Datenübermittlungssystems (Topologie 2)

Bei teilweise verteilten Instanzen stellt sich nicht nur die Frage, welche Festlegungen die Security Policy des Fachverfahrens getroffen hat, sondern auch, ob und wie die verschiedenen Sicherheitsanforderungen auf die beiden eigenständigen Systeme – zum einen dasjenige mit integriertem Transportsystem und zum anderen das eigenständige System, in welches der logische Empfänger und das Fachverfahren integriert sind – verteilt werden.

Für die weitere Erörterung sei angenommen, dass die Security Policy fordert, dass Authentifizierung, Vertraulichkeit und Integrität samt Nachweis der Urheberschaft gegeben sein muss.

- Wenn die Security Policy zudem fordert, dass im Sinne der Risikominimierung durch mögliche Angriffsszenarien aus dem Internet und zugleich der Minimierung der gesamten Systembelastung durch nicht zugelassene Teilnehmer dies zum frühest möglichen Zeitpunkt erkannt und entsprechend behandelt werden muss, dann sollte bereits das im Transportsystem integrierte DFÜ-System über ein geeignetes DFÜ-Protokoll (z.B. https oder ftps) auf der Basis von Zertifikaten die Authentifizierung der Teilnehmer, die Vertraulichkeit der Daten und die Integrität der übermittelten Daten auf der Wegstrecke über das Internet übernehmen. Auf diese Weise kann ein recht hohes Sicherheitsniveau erreicht wenn, insbesondere dann, wenn zudem die Security Policy sowohl eine Server- als auch eine Client-Autentifizierung vorschreibt.

- Wenn jedoch ein DFÜ-Protokoll verwendet werden soll, das die Sicherheitsaspekte Authentifizierung, Vertraulichkeit und Integrität nicht wahrnehmen kann (z.B. http oder ftp), dann muss die Instanz physikalischer Sender/Empfänger im Transportsystem diese Aufgabenstellung übernehmen, gegebenenfalls ergänzt um entsprechende Sicherheitsmaßnahmen im eigenständigen System „logischer Empfänger + Fachverfahren“.

Die Security Policy könnte außerdem festlegen, dass in der Topologie 2 das eigenständige Transportsystem (und dessen Bedienpersonal) aus Datenschutzgründen und wegen der organisatorischen Trennung der Zuständigkeit keine Kenntnis über die übermittelten fachlichen Daten haben darf, dass also die Vertraulichkeit über die gesamte Wegstrecke bis zum verwertenden Fachverfahren sichergestellt werden muss. Im Architekturmodell ist für diesen Zweck eine zweite Ebene – die Logistik- oder die Nachrichten-Ebene – vorgesehen und auf dieser Ebene die fachlichen Daten zu verschlüsseln. Die Logistik-Ebene kommt in Frage, wenn mehrere fachliche Nachrichten des gleichen Typs übermittelt werden sollen und sich das Gebot der Vertraulichkeit bzw. Integrität nicht auf jede einzelne fachliche Nachricht, sondern auf den gesamten fachlichen Inhalt der Logistik-Ebene bezieht. Wenn jedoch das verwertende Fachverfahren jede fachliche Nachricht getrennt verarbeiten will oder die Vertraulichkeit

und/oder Integrität jeder einzelnen fachlichen Nachricht gefordert ist, dann wäre die Nachrichten-Ebene angemessen.

3.3. Sicherheit bei vollständig verteilten Instanzen eines Datenübermittlungssystems (Topologie 3)

Wenn die Security Policy bei dieser Topologie des Datenübermittlungsverbundes sehr hohe Anforderungen vorschreibt, indem sich jedes „eigenständige System“ authentifizieren muss - angefangen vom DFÜ-System bis hin zum eigenständigen System des Fachverfahrens - und wenn die Vertraulichkeit und Integrität jeder einzelnen fachlichen Nachricht im Sinn einer Ende-zu-Ende Vertraulichkeit oder Integrität sicherzustellen ist, dann sind hierfür alle Ebenen des Architekturmodells erforderlich.

Wenn im extremsten Fall die „eigenständigen Systeme“ miteinander per DFÜ über das öffentliche Internet kommunizieren, ist die sicherheitstechnische Problematik der horizontalen Kommunikation der DFÜ-Ebene auf die vertikale Kommunikation aller „eigenständigen Systeme“ untereinander zu übertragen.

4. Unterstützung durch den eXTra Standard bei Sicherheit, Verfügbarkeit und Nachvollzug

4.1. Das Architekturmodell des eXTra Standards

Das abstrakte Architekturmodell eines Datenübermittlungsverbundes (siehe Kapitel 2.1) ist gleichzeitig die Grundlage für das Architekturmodell des eXTra Standards.

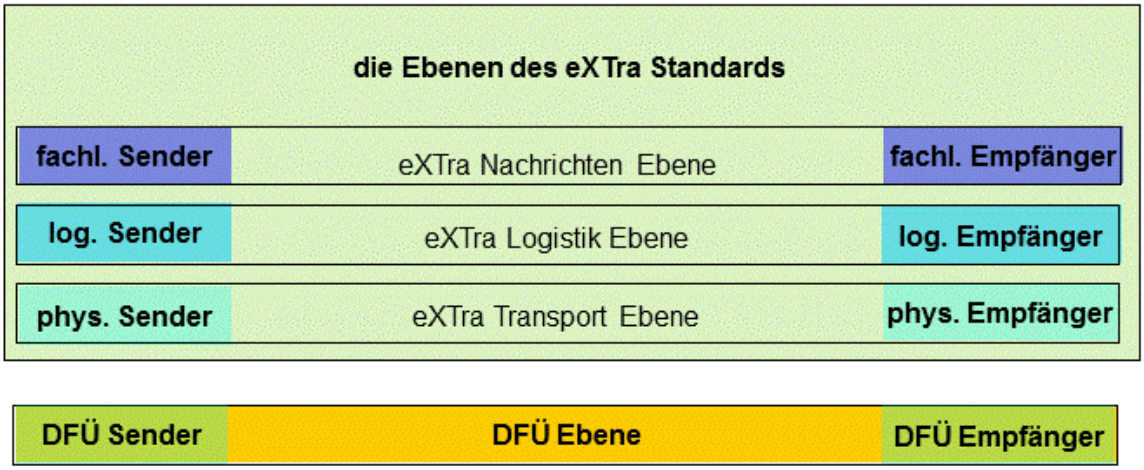

BILD 9: Das Architekturmodell des eXTra Standards und dessen Ebenen.

Dem eXTra Standard sind zwar alle vier Ebenen des abstrakten Architekturmodells bekannt, behandelt aber nur die drei Ebenen der Nachrichten-, Logistik- und Transportebene explizit. Die DFÜ-Ebene ist nicht Gegenstand des eXTra Standards.

4.2. eXTra Standard und Sicherheit

Horizontale Kommunikation

Der eXTra Standard bietet entsprechende Sprachmittel für die Absicherung der horizontalen Kommunikation innerhalb einer eXTra Ebene, d.h. für die Spezifikation der zugehörigen Security Domain. Auf jeder eXTra Ebene kann die Authentifizierung, Vertraulichkeit, Integrität und Nachweis der Urheberschaft durch die Angabe entsprechender Verfahren festgelegt werden, unabhängig von der Spezifikation anderer Ebenen.

Wenn die Security Policy fordert, pro Ebene jeweils unterschiedliche Legitimationsmittel und/oder Verfahren einzusetzen, ermöglicht der eXTra Standard eine solch differenzierte Festlegung.
Wenn die Security Policy eine End-zu-Ende Vertraulichkeit und/oder Integrität fordert, kann dies mit Hilfe der eXTra Ebene der Fachnachrichten erreicht werden.

Vertikale Kommunikation

Im Gegensatz zur horizontalen Kommunikation wird die Frage der vertikalen Kommunikation von Ebene zu Ebene innerhalb der Sender- bzw. Empfängersphäre und der dort zu behandelnden Sicherheitsaspekte und der Schnittstellen zwischen den einzelnen „eigenständigen Systemen“ im eXTra Standard nicht behandelt.

Sicherheitsspezifische Verfahren und Algorithmen

Der eXTra Standard schreibt keine spezifischen Algorithmen oder Verfahren vor, empfiehlt jedoch die Verwendung der w3c-Standards XML-Encryption und XML-Signature für Verschlüsselung und Signaturen. Sollte die Security Policy eines Datenübermittlungsverbundes Authentifizierungs-, Signatur- oder Verschlüsselungsverfahren vorschreiben, die mit diesen beiden Standards nicht abgebildet werden können, so besteht die Möglichkeit, über das PlugIn DataTransforms die gewünschten Verfahren einzubinden, wobei aus Sicht des eXTra Standards diese Möglichkeit insbesondere als Erleichterung der Migration eines bestehenden Datenübermittlungsverbundes hin zu eXTra gedacht ist. Die Migration wird dadurch erleichtert, dass nicht zugleich ein Wechsel der Sicherheitsverfahren erzwungen wird.
Gleichwohl wird empfohlen, für Authentifizierung, Vertraulichkeit, Integrität und den Nachweis der Urheberschaft ein Signatur-, Authentifizierungs- bzw. Verschlüsselungsverfahren einzusetzen, das auf der Basis von Zertifikaten arbeitet, um damit ein entsprechend hohes Sicherheitsniveau zu erreichen.
Sollte es erforderlich sein, im Zuge der Datenübermittlung auch X.509 Zertifikate auszutauschen, so steht hierfür das PlugIn Certificates zur Verfügung.

eXTra und die DFÜ-Ebene

Wenn die Security Policy die authentifizierte Kommunikation der beiden DFÜ-Partner, die Vertraulichkeit aller über das Internet transportierten Daten und/oder die Verfügbarkeit des

gesamten Datenübermittlungssystems fordert, kann der eXTra Standard die Security Policy bei der Umsetzung von Anforderungen, die sich auf die DFÜ Ebene beziehen, nicht unterstützen, weil die DFÜ Ebene nicht Gegenstand des eXTra Standards ist. Diese Anforderungen müssen deshalb außerhalb des eXTra Standards gelöst werden. Dies gilt in gleicher Weise für die Angriffe aus der Internet-Welt (siehe auch Kapitel 2.4 „Angriff auf die Verfügbarkeit von außen“).

4.3. eXTra Standard, Verfügbarkeit und Nachvollzug

Verfügbarkeit des eXTra Systems in der Empfängersphäre

Wenn in der Empfängersphäre die Instanz des DFÜ-Systems die Kontrolle und die Daten an das eXTra System - genauer an die eXTra Instanz „physikalischer Empfänger“ - weitergeben will, aber diese Instanz derzeit nicht verfügbar ist, sollte der Sender über diesen Systemzustand des Empfängers mit einer aussagekräftigen Meldung informiert werden. Zu diesem Zweck gibt es im eXTra Standard ab Version 1.2 die Fehlermeldung „ExtraError“, die dem Sender anzeigt, dass das eXTra System auf Empfängerseite derzeit nicht verfügbar ist.

Eingeschränkte Verfügbarkeit

Im Kapitel 2.4 wird unter „eingeschränkte Verfügbarkeit durch Fehlfunktionen im Netz oder innerhalb des Datenübermittlungsverbundes“ ein Szenario geschildert, bei dem der Sender unsicher ist, ob seine Übermittlung vollständig und korrekt beim Empfänger ankam und an das Fachverfahren weitergeleitet werden konnte. Als Lösung wurde ein Mechanismus des Datenübermittlungsverfahrens skizziert, mit dem der Sender den tatsächlichen Zustand beim Empfänger erfragen kann. Der eXTra Standard bietet ab der Version 1.3 als Lösung dieser Problematik die Standardnachricht RepeatResponse an, mit der der Sender den Empfänger auffordert, ihm zu einem spezifizierbaren Sendevorgang den damaligen Systemzustand des Empfängers in Form einer eXTra Response mitzuteilen, die der Sender damals hätte erhalten sollen.

Nachvollzug und Auskunftsfähigkeit

Im Kapitel 2.4 werden unter „Nachvollzug und Auskunftsfähigkeit“ Szenarien geschildert, bei denen der Teilnehmer im Klärungsfall einerseits nachweisen will, dass er seine Fachnachrichten

tatsächlich und rechtzeitig übermittelt hat, und andererseits, dass seine Fachnachrichten korrekt verarbeitet werden konnten.
Weiterhin fordert der Teilnehmer Unterstützung durch das Datenübermittlungssystem z.B. für den Fall, dass er zwar die Bestätigung für den Empfang seiner Fachnachrichten erhielt, aber kein Ergebnis der Verarbeitung seiner Fachnachrichten erhältlich ist. Oder für den Fall, dass das verwertende Fachverfahren beim Teilnehmer das Ausbleiben seiner Fachnachrichten reklamiert, obwohl ihm die rechtzeitige Übermittlung bestätigt wurde.

Der eXTra Standard bietet für solche Fälle Unterstützung an:
Den Nachweis, wann genau die Übermittlung seiner Fachnachrichten erfolgt ist und ob sie erfolgreich empfangen und übernommen wurden, erhält der Teilnehmer mit der zugehörigen eXTra Response zum Sendevorgang in Form eines Zeitstempels der eXTra Instanz „physikalischer Empfänger“ sowie einer Meldung, ob der Sendevorgang erfolgreich abgeschlossen werden konnte oder hierbei Fehler auftraten.
Weiterhin bietet der eXTra Standard ab der Version 1.3 mit der Standardnachricht StatusRequest eine Auskunftsfunktion an, mit der sich ein Teilnehmer erkundigen kann, was mit seinen Fachnachrichten geworden ist, indem der Weg seiner damaligen Fachnachrichten durch die verschiedenen eXTra Instanzen in der Empfängersphäre mit einer entsprechenden Erfolgs- oder Fehlermeldung nachvollzogen werden kann. Mit den so automatisch gewonnenen detaillierten Informationen können strittige Fälle effizient und schnell geklärt werden, ohne dass hierzu die Hotline bemüht werden müsste. In vielen Fällen dürften diese Informationen auch genügen, um den Fall gezielt und erfolgreich klären zu können.

4.4. Registrierung als eXTra spezifisches Datenübermittlungsverfahren

Ein Datenübermittlungsverbund bzw. dessen zuständiges Gremium oder Betreiber hat die Möglichkeit, das Datenübermittlungsverfahren offiziell registrieren und mit entsprechender Dokumentation auf der eXTra Homepage eintragen zu lassen. Dazu ist erforderlich, beim eXTra Gremium eine Reihe von Dokumenten einzureichen [KOMP]. Diese dienen dazu, die Konformität zu eXTra nachzuweisen. Darüber hinaus wird gegenüber den am Datenübermittlungsverbund interessierten Teilnehmern vollständig und präzise dargelegt, welche Teilnahmebedingungen existieren, mit welchen Strukturen der Austausch fachlicher Daten zu erfolgen hat und welche DFÜ- und Sicherheitsverfahren einzusetzen sind. Damit umfasst die Dokumentation weit mehr als die eXTra-spezifischen Aspekte, es müssen die Regularien der Teilnahme an einem Datenübermittlungsverbund darlgelegt und spezifiziert werden, wie der laufende Betrieb des dazugehörigen Datenübermittlungsverfahrens gestaltet ist – dies betrifft die vier Ebenen des abstrakten Architekturmodells, also der drei eXTra Ebenen sowie der DFÜ Ebene.

5. Anhang

5.1. Referenzen

Kurzname	Quelle
DSIG	*eXTra Design Guidelines*, zu finden unter www.extra-standard.de
EINF	*Einführung in den eXTra Standard,* zu finden unter www.extra-standard.de
EMSG	*eXTra Standardnachrichten, Schnittstellenbeschreibung,* zu finden unter www.extra-standard.de
EXSEC	*Sicherheit und Verfügbarkeit in einem eXTra spezifischen Datenübermittlungsverbund,* zu finden unter www.extra-standard.de
EXWS	*eXTra und Webservices*, zu finden unter www.extra-standard.de
IFACE	*eXTra Transport Schnittstellenbeschreibung,* zu finden unter www.extra-standard.de
IMPL	*eXTra Implementierung*
KOMP	*eXTra Kompendium,* zu finden unter www.extra-standard.de
RFC2119	*Request for Comments: 2119*, S. Bradner, Harvard University, March 1997, http://www.ietf.org/rfc/rfc2119.txt
PROF	*eXTra Profilierung,* zu finden unter www.extra-standard.de
XENC	*XML Encryption*, http://www.w3.org/TR/xmlenc-core/
XML	*XML Recommendation 1.0, 3rd Edition*, http://www.w3.org/XML
XSD	*XML Schema Definition*, http://www.w3.org/TR/xmlschema-0/
XSIG	*XML Signature*, http://www.w3.org/TR/xmldsig-core/
XSL	*XML Stylesheet Language*, http://www.w3.org/TR/1999/REC-xslt-19991116, http://www.w3.org/TR/xslt20/