

DIN ISO 9735-5



ICS 35.240.60

**Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) –
Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4,
Syntax-Releasenummer: 1) –
Teil 5: Sicherheitsregeln für Batch-EDI (Authentizität, Integrität und
Unbestreitbarkeit des Ursprungs) (ISO 9735-5:2002)**

Electronic data interchange for administration, commerce and transport (EDIFACT) –
Application level syntax rules (Syntax version number: 4, Syntax release number: 1) –
Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)
(ISO 9735-5:2002)

Échange de données informatisé pour l'administration, le commerce et le transport
(EDIFACT) –

Règles de syntaxe au niveau de l'application (Numéro de version de syntaxe: 4, numéro
d'édition de syntaxe: 1) –

Partie 5: Règles de sécurité pour EDI par lots (authenticité, intégrité et non-répudiation de
l'origine) (ISO 9735-5:2002)

Gesamtumfang 48 Seiten

Normenausschuss Bürowesen (NBü) im DIN

Die Internationale Norm ISO 9735-5:2002 „Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4, Syntax release number: 1) – Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)“ ist unverändert in diese Deutsche Norm übernommen worden.

Nationales Vorwort

Diese Norm wurde vom Normenausschuss Bürowesen (NBü), Arbeitsausschuss 3 „EDI/EDIFACT“ (NBü-AA 3), erarbeitet. Der NBü ist u. a. für normative Festlegungen im Anwendungsbereich des elektronischen Datenaustausches im weiteren Sinn auch Electronic Commerce zuständig.

Die vorliegende Norm enthält die deutsche Übersetzung der ISO 9735-5:2002, die zusammen mit den anderen Normen dieser Reihe gemeinhin als **EDIFACT-Syntax, Version 4, Release 1**, bekannt ist.

Die komplette Version 4, Release 1, der EDIFACT-Syntax setzt sich aus insgesamt 10 Teilen zusammen, die neben der Batch-Verarbeitung (ISO 9735-1 und ISO 9735-2) auch den interaktiven Datenaustausch (ISO 9735-3), den Service-Nachrichtentyp CONTRL (ISO 9735-4) und die Einbindung von Fremddaten (ISO 9735-8) innerhalb von UN/EDIFACT beschreibt. Darüber hinaus wurden sicherheitsrelevante Aspekte aufgegriffen und berücksichtigt (ISO 9735-5, ISO 9735-6, ISO 9735-7 und ISO 9735-9).

Da die praktische Umsetzung der Version 4, Release 1, der EDIFACT-Syntax nur zögernd vorstatten geht und gleichzeitig bestehende EDIFACT-Anwendungen im Wesentlichen noch auf der älteren Version 3 basieren, wurde von ISO entschieden, neben der aktuellen Ausgabe der Version 4 auch die ältere Version 3 in den ISO-Listen weiter zu führen.

Aus diesem Grund entschied der NBü-AA 3, analog zu der ISO-Entscheidung auch die entsprechenden Deutschen Fassungen als Deutsche Normen zu veröffentlichen. Daher gibt es neben den Normen der Reihe DIN ISO 9735, Teile 1 bis 10, auf Basis der ISO 9735-1 bis ISO 9735-10 (= Version 4, Release 1 der EDIFACT-Syntax) auch die DIN ISO 9735, die die Version 3 der EDIFACT-Syntax beschreibt.

DIN ISO 9735 *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) – Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1)* besteht aus:

- Teil 1: *Syntax-Regeln, die für alle Teile gemeinsam sind*
- Teil 2: *Syntax-Regeln für Batch-EDI*
- Teil 3: *Syntax-Regeln für Interaktiv-EDI*
- Teil 4: *Syntax- und Servicebericht für Batch-EDI (Nachrichtentyp – CONTRL)*
- Teil 5: *Sicherheitsregeln für Batch-EDI (Authentizität, Integrität und Unbestreitbarkeit des Ursprungs)*
- Teil 6: *Sicherheits-Authentisierung und -Bestätigung (Nachrichtentyp – AUTACK)*
- Teil 7: *Sicherheitsregeln für Batch-EDI (Vertraulichkeit)*
- Teil 8: *Eingebundene Daten in EDI*
- Teil 9: *Sicherheitsschlüssel- und Zertifikats-Verwaltung (Nachrichtentyp – KEYMAN)*
- Teil 10: *Syntax-Service-Verzeichnisse*

Zum Vorwort:

Die im Vorwort der ISO-Fassung genannte ISO 9735-10 beinhaltet das komplette Service-Verzeichnis nach der EDIFACT-Syntax, Version 4, Release 1, einschließlich des zum Zeitpunkt der Veröffentlichung aktuellen Service-Codes-Verzeichnisses.

Das DIN Deutsches Institut für Normung e. V. veröffentlicht die deutschen Übersetzungen zu den EDIFACT-Verzeichnissen – inklusive der Service-Verzeichnisse – im Rahmen der regelmäßigen Aktualisierungen des Implementierungswerkzeuges EdiFix. EdiFix kann über die DIN Software GmbH, 10772 Berlin, Tel.: (0 30) 26 01-0, bezogen werden. Nähere Informationen auf Anfrage.

Zu Abschnitt 3:

Für die im Abschnitt 3 angegebenen Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

Normen der Reihe
ISO 9735-x Siehe DIN ISO 9735-x

ANMERKUNG Hier sind ausschließlich die Teile 1 bis 10 der Normen der Reihe DIN ISO 9735 gemeint, die die EDIFACT-Syntax nach der Version 4, Release 1, beschreiben. Die allein stehende DIN ISO 9735 ohne Teilbezeichnung beschreibt die ältere, aber weiterhin gültige Version 3 der EDIFACT-Syntax (siehe nationales Vorwort).

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO 9735:2002-11, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (ISO 9735:1988 + Amd 1:1992)*.

Deutsche Übersetzung

Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT)

Syntax-Regeln auf Anwendungsebene
(Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1)

Teil 5: Sicherheitsregeln für Batch-EDI (Authentizität, Integrität und Unbestreitbarkeit des Ursprungs)
(ISO 9735-5:2002)

Inhalt

	Seite
Vorwort	5
Einleitung	6
1 Anwendungsbereich	6
2 Konformität	6
3 Normative Verweisungen	7
4 Begriffe	7
5 Regeln für die Verwendung der Sicherheitskopf- und der Sicherheitsende Segmentgruppen bei Batch-EDI	8
6 Regeln für die Verwendung der Sicherheitskopf- und der Sicherheitsende- Segmentgruppen für Übertragungsdateien und Gruppen bei Batch-EDI	16
Anhang A (informativ) EDIFACT-Sicherheitsrisiken und -lösungen	20
Anhang B (informativ) Schutz einer EDIFACT-Struktur	24
Anhang C (informativ) Beispiele für den Nachrichtenschutz	27
Anhang D (informativ) Filterfunktionen für die UN/EDIFACT-Zeichensätze A und C	36
Anhang E (informativ) Sicherheitsdienste und -algorithmen	39
Literaturhinweise	48

Vorwort

Die ISO (Internationale Organisation für Normung) ist die weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedskörperschaften). Die Erarbeitung Internationaler Normen obliegt den Technischen Komitees der ISO. Jede Mitgliedskörperschaft, die sich für ein Thema interessiert, für das ein Technisches Komitee eingesetzt wurde, ist berechtigt, in diesem Komitee mitzuarbeiten. Internationale (staatliche und nichtstaatliche) Organisationen, die mit der ISO in Verbindung stehen, sind an den Arbeiten ebenfalls beteiligt. Die ISO arbeitet bei allen Angelegenheiten der elektrotechnischen Normung eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Internationale Normen werden in Übereinstimmung mit den Regeln nach den ISO/IEC-Direktiven, Teil 3, erarbeitet.

Die vorrangige Aufgabe der Technischen Komitees liegt in der Vorbereitung Internationaler Normen. Die von den Technischen Komitees verabschiedeten internationalen Norm-Entwürfe werden den Mitgliedskörperschaften zur Abstimmung vorgelegt. Die Veröffentlichung als Internationale Norm erfordert Zustimmung von mindestens 75 % der abstimmenden Mitgliedskörperschaften.

Es ist zu beachten, dass einige Elemente dieses Teils der ISO 9735 Patentrechten unterliegen können. ISO kann nicht zur Rechenschaft gezogen werden, diese Patentrechte zu identifizieren.

ISO 9735-5 wurde von dem Technischen Komitee ISO/TC 154 *Prozesse, Datenelemente und Dokumente in Verwaltung, Wirtschaft und Industrie* in Zusammenarbeit mit UN/CEFACT durch die Joint Syntax Working Group (JSWG) vorbereitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 9735-5:1999). Dennoch behält, wie in Abschnitt 2 begründet, ISO 9735:1988 einschließlich Änderung 1:1992 vorläufig ihre Gültigkeit.

Aus Pflegegründen wurden die Syntax-Service-Verzeichnisse aus diesem und allen anderen Teilen der ISO 9735 entfernt und in einem neuen Teil, ISO 9735-10, zusammengeführt.

Zur Zeit der Veröffentlichung von ISO 9735-1:1998 wurde ISO 9735-10 ursprünglich als Teil für „Sicherheitsregeln für interaktives EDI“ vorgesehen. Da der Bedarf der Anwender jedoch ausblieb, wurde dieser Teil in dieser Form nicht veröffentlicht und alle entsprechenden Referenzen darauf in dieser zweiten Ausgabe von ISO 9735-5 entfernt.

Die Definitionen aus allen Teilen der Norm-Reihe ISO 9735 wurden in ISO 9735-1 zusammengefasst.

ISO 9735 besteht aus den folgenden Teilen unter dem allgemeinen Titel *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene* (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1):

- Teil 1: *Syntax-Regeln, die für alle Teile gemeinsam sind*
- Teil 2: *Syntax-Regeln für Batch-EDI*
- Teil 3: *Syntax-Regeln für Interaktiv-EDI*
- Teil 4: *Syntax- und Servicebericht für Batch-EDI (Nachrichtentyp – CONTRL)*
- Teil 5: *Sicherheitsregeln für Batch-EDI (Authentizität, Integrität und Unbestreitbarkeit des Ursprungs)*
- Teil 6: *Sicherheits-Authentisierung und -Bestätigung (Nachrichtentyp – AUTACK)*
- Teil 7: *Sicherheitsregeln für Batch-EDI (Vertraulichkeit)*
- Teil 8: *Eingebundene Daten in EDI*
- Teil 9: *Sicherheitsschlüssel- und Zertifikats-Verwaltung (Nachrichtentyp – KEYMAN)*
- Teil 10: *Syntax-Service-Verzeichnisse*

Weitere Teile können folgen.

Die Anhänge A bis E dieses Teils der ISO 9735 dienen nur zur Information.

Einleitung

Dieser Teil der ISO 9735 beinhaltet die Regeln auf Anwendungsebene für die Strukturierung von Daten im Austausch elektronischer Nachrichten in einem offenen System. Dabei dienen entweder die Anforderungen der Batch- oder die der Interaktiv-Verarbeitung als Basis. Die Syntax-Regeln für den Elektronischen Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) wurden von der Wirtschaftskommission der Vereinten Nationen für Europa (UN/ECE) vereinbart. Sie sind Bestandteil des Verzeichnisses für den Handelsdatenaustausch der Vereinten Nationen (UNTDID), das darüber hinaus die Nachrichten-Entwicklungsrichtlinien für Batch und Interaktiv enthält.

Kommunikationsbeschreibungen und -protokolle befinden sich außerhalb des Anwendungsbereichs dieses Teils der ISO 9735.

Dies ist ein neuer Teil, der ISO 9735 ergänzt. Er beschreibt die Möglichkeit zur Absicherung von Batch-EDIFACT-Strukturen, d. h. Nachrichten, Pakete, Gruppen oder Übertragungsdateien.

1 Anwendungsbereich

Dieser Teil der ISO 9735 legt die Syntax-Regeln für die Sicherheit bei EDIFACT fest. Er stellt ein Verfahren bereit, das sich an die Authentizität, Integrität und an die Unbestreitbarkeit des Ursprungs auf Nachrichten-/Paket-Ebene, Gruppen-Ebene und Übertragungsdatei-Ebene richtet. Die Regeln stehen in Übereinstimmung mit bestehenden Sicherheitsmechanismen.

2 Konformität

Bei Verwendung dieses Teils müssen im Muss-Datenelement 0002 (Syntax-Versionsnummer) die Versionsnummer „4“ und im Kann-Datenelement 0076 (Syntax-Releasenummer) die Releasenummer „1“ eingetragen werden. Beide sind im Segment UNB (Nutzdaten-Kopfsegment) enthalten. Übertragungsdateien, die weiterhin die in früher veröffentlichten Ausgaben definierte Syntax verwenden, müssen zur Unterscheidung die folgenden Syntax-Versionsnummern tragen:

- ISO 9735:1988 — *Syntax-Versionsnummer: 1*
- ISO 9735:1988 (geändert und neu gedruckt 1990) — *Syntax-Versionsnummer: 2*
- ISO 9735:1988 einschließlich Änderung 1:1992 — *Syntax-Versionsnummer: 3*
- ISO 9735:1998 — *Syntax-Versionsnummer: 4*

Konformität zu einer Norm bedeutet, dass alle ihre Anforderungen einschließlich aller Optionen unterstützt werden. Werden nicht alle Optionen unterstützt, muss jeder Anspruch auf Konformität eine Angabe beinhalten, die diejenigen Optionen identifiziert, für die Konformität beansprucht wird.

Ausgetauschte Daten sind konform, wenn die Struktur und Darstellung der Daten mit den in diesem Teil der ISO 9735 festgelegten Syntax-Regeln übereinstimmen.

Einrichtungen, die diesen Teil der ISO 9735 unterstützen, sind konform, wenn sie in der Lage sind, die Daten strukturell und von der Darstellung in Übereinstimmung mit diesen Teil der ISO 9735 zu erzeugen und/oder zu interpretieren.

Konformität mit diesem Teil der ISO 9735 muss die Konformität mit Teil 1, Teil 2, Teil 8 und Teil 10 der ISO 9735 einschließen.

Sofern in diesem Teil der ISO 9735 angegeben, bilden in zugehörigen Normen definierte Bestimmungen einen Bestandteil der Konformitätskriterien.

3 Normative Verweisungen

Die folgenden normativen Dokumente enthalten Festlegungen, die durch Verweisungen in diesem Text Bestandteil dieser Internationalen Norm sind. Bei datierten Verweisungen gelten spätere Änderungen oder Überarbeitungen dieser Publikationen nicht. Anwender dieser Internationalen Norm werden jedoch gebeten, die Möglichkeit zu prüfen, die jeweils neuesten Ausgaben der nachfolgend angegebenen normativen Dokumente anzuwenden. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen normativen Dokuments. Mitglieder von ISO und IEC führen Verzeichnisse der gültigen Internationalen Normen.

ISO 9735-1:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 1: Syntax-Regeln, die für alle Teile gemeinsam sind.*

ISO 9735-2:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 2: Syntax-Regeln für Batch-EDI.*

ISO 9735-6:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 6: Sicherheits-Authentisierung und -Bestätigung (Nachrichtentyp – AUTACK).*

ISO 9735-7:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 7: Sicherheitsregeln für Batch-EDI (Vertraulichkeit).*

ISO 9735-8:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 8: Eingebundene Daten in EDI.*

ISO 9735-10:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 10: Syntax-Service-Verzeichnisse.*

ISO/IEC 10181-2:1996, *Informationstechnik — Kommunikation Offener Systeme — Rahmenrichtlinien für IT-Sicherheit in Offenen Systemen — Teil 2: Authentifikation.*

ISO/IEC 10181-4:1997, *Informationstechnik — Kommunikation Offener Systeme — Rahmenrichtlinien für IT-Sicherheit — Teil 4: Nicht-Verweigerung.*

ISO/IEC 10181-6:1996, *Informationstechnik — Kommunikation Offener Systeme — Rahmenrichtlinien für IT-Sicherheit — Teil 6: Integrität.*

4 Begriffe

Für die Anwendung dieses Teils der ISO 9735 gelten die in ISO 9735-1 angegebenen Begriffe.

5 Regeln für die Verwendung der Sicherheitskopf- und der Sicherheitsende-Segmentgruppen bei Batch-EDI

5.1 Sicherheit auf Nachrichten-/Paket-Ebene — Integrierte Sicherheit

5.1.1 Allgemeines

Die Sicherheitsrisiken bei der Nachrichten-/Paket-Übertragung und die darauf ausgerichteten Sicherheitsdienste sind in den Anhängen A und B beschrieben.

Dieser Abschnitt beschreibt den Aufbau der Sicherheit auf Nachrichten-/Paket-Ebene bei EDIFACT.

Die in diesen Teil der ISO 9735 angesprochenen Sicherheitsdienste werden durch das Einfügen von Sicherheitskopf- und Sicherheitsende-Segmentgruppen nach dem Segment UNH und vor dem Segment UNT derart bereitgestellt, dass dies auf jede bestehende Nachricht angewendet werden kann. Für Pakete erfolgt das Einfügen nach dem Segment UNO und vor dem Segment UNP.

5.1.2 Sicherheitskopf- und Sicherheitsende-Segmentgruppen

Bild 1 zeigt eine Übertragungsdatei, die auf Nachrichtenebene gesichert ist.

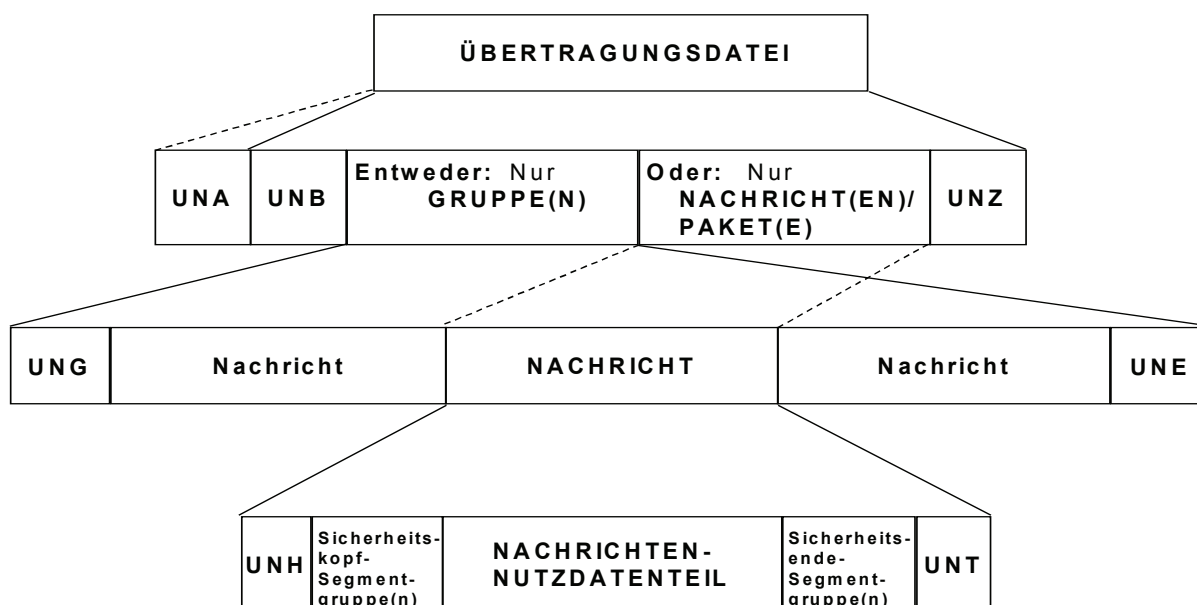


Bild 1 — Übertragungsdatei mit einer gesicherten Nachricht (schematisch)

Bild 2 zeigt eine Übertragungsdatei, die auf Paketebene gesichert ist.

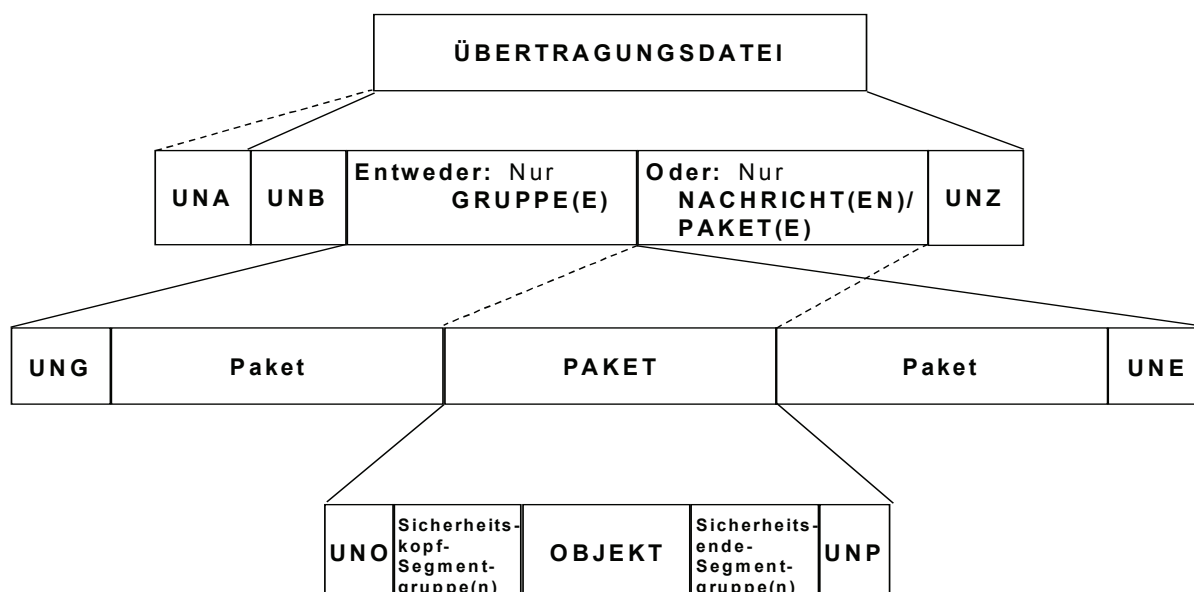


Bild 2 — Übertragungsdatei mit einem gesicherten Paket (schematisch)

5.1.3 Struktur der Sicherheitskopf- und Sicherheitsende-Segmentgruppen

Tabelle 1 — Tabellarische Segmentübersicht der Sicherheitskopf- und Sicherheitsende-Segmentgruppen (Sicherheit auf Nachrichtenebene)

BEZ	Name	S	WDH	
UNH	Nachrichten-Kopfsegment	M	1	
-----	Segmentgruppe 1 -----	K	99	-----+
USH	Sicherheits-Kopfsegment	M	1	I
USA	Sicherheits-Algorithmus	K	3	I
-----	Segmentgruppe 2 -----	K	2	-----+ I
USC	Zertifikat	M	1	I I
USA	Sicherheits-Algorithmus	K	3	I I
USR	Sicherheitsergebnis	K	1	-----+
	Nachrichten-Nutzdatenteil			
-----	Segmentgruppe n -----	K	99	-----+
UST	Sicherheits-Endesegment	M	1	I
USR	Sicherheitsergebnis	K	1	-----+
UNT	Nachrichten-Endesegment	M	1	

Tabelle 2 — Tabellarische Segmentübersicht der Sicherheitskopf- und Sicherheitsende-Segmentgruppen (Sicherheit auf Paketebene)

BEZ	Name	S	WDH	
UNO	Objekt-Kopfsegment	M	1	
-----	Segmentgruppe 1 -----	K	99	-----+
USH	Sicherheits-Kopfsegment	M	1	I
USA	Sicherheits-Algorithmus	K	3	I
-----	Segmentgruppe 2 -----	K	2	----+ I
USC	Zertifikat	M	1	I I
USA	Sicherheits-Algorithmus	K	3	I I
USR	Sicherheitsergebnis	K	1	-----+
	Objekt			
-----	Segmentgruppe n -----	K	99	----+
UST	Sicherheits-Endesegment	M	1	I
USR	Sicherheitsergebnis	K	1	----+
UNP	Objekt-Endesegment	M	1	

ANMERKUNG Das vollständige Verzeichnis zur Festlegung der Segmente und der Datenelemente einschließlich des Nachrichten-Kopfsegments UNH, des Nachrichten-Endesegments UNT, des Objekt-Kopfsegments UNO und des Objekt-Endesegments UNP sind in ISO 9735-10 festgelegt. Sie sind in diesen Teil nicht weiter beschrieben.

5.1.4 Segmentbeschreibung

Segmentgruppe 1: USH-USA-SG 2 (Sicherheitskopf-Segmentgruppe)

Eine Gruppe von Segmenten zur Identifizierung des angewendeten Sicherheitsdienstes und der Sicherheitsmechanismen. Sie enthält die notwendigen Daten zur Durchführung der Prüfwertberechnungen.

Es kann mehrere unterschiedliche Sicherheitskopf-Segmentgruppen innerhalb der gleichen Nachricht bzw. des gleichen Pakets geben, wenn verschiedene Sicherheitsdienste auf die Nachricht bzw. das Paket angewendet werden (z. B. Integrität und Unbestreitbarkeit des Ursprungs) oder wenn der gleiche Sicherheitsdienst von mehreren Beteiligten angewendet wird.

USH, Sicherheits-Kopfsegment

Ein Segment zur Angabe eines Sicherheitsdienstes, der auf die Nachricht bzw. das Paket, in der/das Segment enthalten ist, angewendet wird.

Die am Sicherheitsdienst Beteiligten (Sicherheitselemente des Urhebers und des Empfängers) können in diesem Segment identifiziert werden, sofern sie nicht eindeutig bei Verwendung asymmetrischer Algorithmen durch Zertifikate (Segment USC) identifiziert sind.

Die Datenelementgruppe „Sicherheitsidentifikation“ (S500) muss im Segment USH verwendet werden, entweder:

- wenn symmetrische Algorithmen verwendet werden, oder
- wenn asymmetrische Algorithmen verwendet werden und zwei Zertifikate vorhanden sind, um zwischen den Zertifikaten des Urhebers und des Empfängers zu unterscheiden.

Im letzteren Fall muss die Identifikation des Beteiligten in S500 (jedes der Datenelemente S500/0511, S500/0513, S500/0515, S500/0586) gleich der des Beteiligten sein, der in einen der vorhandenen S500 im Segment USC in Segmentgruppe 2 als „Zertifikatseigner“ qualifiziert ist. Dabei identifiziert das Datenelement S500/0577 die Funktion (Urheber oder Empfänger) des Beteiligten.

Das Datenelement „Schlüsselname“ in der Datenelementgruppe „Sicherheitsidentifikation“ (S500/0538) kann zur Festlegung der Schlüsselbeziehung zwischen den sendenden und empfangenden Beteiligten verwendet werden.

Diese Schlüsselbeziehung kann darüber hinaus durch die Verwendung des Datenelements „Algorithmischer Parameter, Wert“ in der Datenelementgruppe „Algorithmischer Parameter“ (S503/0554) des Segments USA in Segmentgruppe 1 festgelegt werden.

S500/0538 in Segment USH kann verwendet werden, wenn kein Bedarf besteht, ein Segment USA in der Segmentgruppe 1 mitzuführen (weil die kryptographischen Mechanismen vorab zwischen den Beteiligten vereinbart wurden).

Dennoch wird dringend empfohlen, entweder S500/0538 im Segment USH oder S503/0554 mit dem geeigneten Qualifier im Segment USA zu verwenden, jedoch nicht beide innerhalb der gleichen Sicherheitskopf-Segmentgruppe.

Das Segment USH kann die Filterfunktion festlegen, die für die Binärfelder des Segments USA innerhalb der Segmentgruppe 1 und für das Segment USR der korrespondierenden Sicherheitsende-Segmentgruppe verwendet wird.

Das Segment USH kann eine Sicherheits-Folgenummer beinhalten, um die Sequenzintegrität und das Datum der Erstellung der Sicherheitselemente anzugeben.

USA, Sicherheits-Algorithmus

Ein Segment zur Identifizierung eines Sicherheits-Algorithmus, der entsprechend zugrunde liegenden technischen Anwendung und zur Angabe der erforderlichen technischen Parameter. Der angegebene Algorithmus muss demjenigen entsprechen, der direkt auf die Nachricht bzw. das Paket angewendet wird. Dieser Algorithmus kann entweder symmetrisch, eine Hashfunktion oder ein Komprimierungsalgorithmus sein. Für eine digitale Unterschrift beispielsweise kennzeichnet er die zu verwendende nachrichtenabhängige Hashfunktion.

Asymmetrische Algorithmen dürfen nicht direkt in diesem Segment USA innerhalb der Segmentgruppe 1 verwiesen werden. Sie können nur innerhalb der Segmentgruppe 2, die von einem Segment USC getriggert wird, angegeben werden.

Drei Auftritte des Segments USA sind erlaubt. Ein Auftritt wird für den symmetrischen Algorithmus oder der Hashfunktion verwendet, der für den im Segment USH festgelegten Sicherheitsdienst erforderlich ist. Die beiden anderen Auftritte sind in ISO 9735-7 beschrieben.

Sofern zutreffend kann ein Auffüllmechanismus angezeigt werden.

Segmentgruppe 2: USC-USA-USR (Zertifikat-Gruppe)

Eine Gruppe von Segmenten, die die notwendigen Daten zur Bestätigung der auf die Nachricht bzw. das Paket angewendeten Sicherheitsverfahren enthält, sofern asymmetrische Algorithmen verwendet werden. Die Zertifikats-Segmentgruppe muss verwendet werden, wenn asymmetrische Algorithmen zur Identifizierung des asymmetrischen Schlüsselpaars eingesetzt werden, auch wenn keine Zertifikate verwendet werden.

Im Segment USC muss entweder die vollständige Zertifikats-Segmentgruppe (einschließlich des Segments USR) vorhanden sein oder es müssen nur die für die eindeutige Identifikation des verwendeten asymmetrischen Schlüsselpaars notwendigen Datenelemente angegeben werden. Das Vorhandensein eines vollständigen Zertifikats kann vermieden werden, wenn das Zertifikat bereits vorab zwischen den beiden Beteiligten ausgetauscht worden ist oder über eine Datenbank wiedererlangt werden kann.

Wenn auf ein nicht-EDIFACT-Zertifikat (z. B. X.509) Bezug genommen wird, muss die Zertifikat-Syntax und -Version im Datenelement 0545 des Segments USC angegeben werden. Derartige Zertifikate können in einem EDIFACT-Paket transportiert werden.

Es sind zwei Auftritte dieser Segmentgruppe erlaubt, wobei eine das Zertifikat des Nachrichten-/Paket-Absenders darstellt (wird vom Nachrichten-/Paket-Empfänger zur Prüfung der Unterschrift des Absenders verwendet) und die andere das Zertifikat des Nachrichten-/Paket-Empfängers (nur für die Zuordnung auf die Zertifikatsreferenz), wenn der öffentliche Schlüssel des Empfängers vom Absender für die Vertraulichkeit der symmetrischen Schlüssel verwendet wird.

Sind beide Auftritte innerhalb einer Sicherheitskopf-Segmentgruppe vorhanden, erlaubt die Datenelementgruppe „Sicherheitsidentifikation“ (S500) zusammen mit dem Datenelement „Zertifikatsreferenz“ (0536) eine Unterscheidung beider.

Diese Segmentgruppe wird ausgelassen, wenn kein asymmetrischer Algorithmus verwendet wird.

USC, Zertifikat

Ein Segment, das die Beglaubigungen des Zertifikatseigners enthält und die berechnete Zertifizierungsinstanz identifiziert, die das Zertifikat ausgestellt hat. Das Datenelement „Filterfunktion, codiert“ (0505) muss die für die Binärfelder der Segmente USA und USR innerhalb der Segmentgruppe 2 verwendete Filterfunktion identifizieren.

Das Zertifikats-Segment kann zwei Auftritte von S500 enthalten: eine für den Zertifikatseigner (zur Identifizierung des Beteiligten, der mit dem privaten Schlüssel unterschreibt; dabei steht dieser Schlüssel mit dem in diesem Zertifikat enthaltenen öffentlichen Schlüssel in Verbindung) und eine für den Zertifikatsaussteller (berechnete Zertifizierungsinstanz oder CA).

USA, Sicherheits-Algorithmus

Ein Segment zur Identifizierung eines Sicherheits-Algorithmus, der entsprechend zugrunde liegenden technischen Anwendung und zur Angabe der erforderlichen technischen Parameter. Die drei verschiedenen Auftritte in diesem Segment USA in der Segmentgruppe 2 identifizieren:

- 1 den vom Zertifikatsaussteller verwendeten Algorithmus zur Berechnung des Hashwertes des Zertifikats (Hashfunktion);
- 2 den vom Zertifikatsaussteller verwendeten Algorithmus zur Erstellung des Zertifikats (d. h., um das Ergebnis der aus dem Zertifikatsinhalt berechneten Hashfunktion zu unterschreiben) (asymmetrischer Algorithmus);
- 3a entweder den vom Absender verwendeten Algorithmus zur Signierung der Nachricht bzw. des Pakets (d. h., um das Ergebnis der aus dem Nachrichten-/Paket-Inhalt berechneten, im Segment USH beschriebenen Hashfunktion zu unterschreiben) (asymmetrischer Algorithmus);
- 3b oder den vom Empfänger verwendeten Algorithmus zur Verschlüsselung des Schlüssels, der durch einen auf den Nachrichten-/Paket-Inhalt angewendeten symmetrischen Algorithmus erforderlich ist und durch die vom Segment USH getriggerten Segmentgruppe 1 verwiesen wird (asymmetrischer Algorithmus).

Sofern zutreffend, kann ein Auffüllmechanismus angezeigt werden.

USR, Sicherheitsergebnis

Ein Segment, das das Ergebnis der Sicherheitsfunktionen enthält, die von der berechtigten Zertifizierungsinstanz auf das Zertifikat angewendet wurden. Dieses Ergebnis ist die Unterschrift des Zertifikats, die von der berechtigten Zertifizierungsinstanz durch Signierung der aus den Beglaubigungsdaten berechneten Hashfunktion bestimmt wird.

Die Berechnung der Unterschrift für das Zertifikat beginnt mit dem ersten Zeichen des Segments USC (namentlich dem „U“) und endet mit dem letzten Zeichen des letzten Segments USA (einschließlich des Trennzeichens, das diesem Segment USA folgt).

Segmentgruppe n: UST-USR (Sicherheitsende-Segmentgruppe)

Eine Gruppe von Segmenten für die Angabe einer Verbindung zwischen der Sicherheitskopf-Segmentgruppe und dem Ergebnis der auf die Nachricht bzw. das Paket angewendeten Sicherheitsfunktionen.

UST, Sicherheits-Endesegment

Ein Segment zur Festlegung einer Verbindung zwischen der Sicherheitskopf- und der Sicherheitsende-Segmentgruppe und zur Angabe der Anzahl der Sicherheits-Segmente, die in diesen Gruppen enthalten sind.

USR, Sicherheitsergebnis

Ein Segment, das das Ergebnis der Sicherheitsfunktionen enthält, die, wie in der verbundenen Sicherheitskopf-Segmentgruppe festgelegt, auf die Nachricht bzw. das Paket angewendet wurde. Abhängig von den in der verbundenen Sicherheitskopf-Segmentgruppe festgelegten Sicherheitsmechanismen wird dieses Ergebnis berechnet:

- entweder direkt auf die Nachricht bzw. das Paket mit dem im Segment USA innerhalb der Segmentgruppe 1 der Sicherheitskopf-Segmentgruppe festgelegten Algorithmus,
- oder durch die Signierung eines Hashergebnisses mit einem asymmetrischen Algorithmus, der im Segment USA innerhalb der Segmentgruppe 2 der Sicherheitskopf-Segmentgruppe festgelegt ist. Das Hashergebnis selbst wird berechnet auf die Nachricht bzw. das Paket mit dem im Segment USA innerhalb der Segmentgruppe 1 der Sicherheitskopf-Segmentgruppe festgelegten Algorithmus.

5.1.5 Anwendungsbereich der Sicherheit

Es gibt zwei Möglichkeiten für den Einsatz der Sicherheitsanwendung:

1. Die Berechnung aller Werte für die Integrität und Authentizität sowie der digitalen Unterschriften beginnt mit der gegenwärtigen Sicherheitskopf-Segmentgruppe – und schließt diese ein – sowie dem Nachrichten-Nutzdatenteil oder dem Objekt. In diesem Fall dürfen keine anderen Sicherheitskopf- oder Sicherheitsende-Segmentgruppen im Rahmen dieses Anwendungsbereichs enthalten sein.

Die Sicherheitskopf-Segmentgruppe müssen vom ersten Zeichen, namentlich ein „U“, bis zum Trennzeichen, das diese Segmentgruppe beendet, gezählt werden. Dabei sind beide Zeichen enthalten. Dies gilt auch für den Nachrichten-Nutzdatenteil oder das Objekt, die vom ersten dem Trennzeichen der letzten Sicherheitskopf-Segmentgruppe nachfolgenden Zeichen bis zum Trennzeichen gezählt werden, das dem ersten Zeichen der ersten Sicherheitsende-Segmentgruppe vorangestellt ist.

Daher ist die Folge, in der die in dieser Form integrierten Sicherheitsdienste ausgeführt werden, nicht vorgeschrieben. Sie sind vollständig unabhängig voneinander.

Das Bild 3 veranschaulicht diesen Fall (der Anwendungsbereich des Sicherheitsdienstes, der in der Sicherheitskopf-Segmentgruppe 2 definiert ist, ist durch die schraffierten Boxen dargestellt):

UNH/ UNO	Sicherheitskopf-Segmentgruppe 3	Sicherheitskopf-Segmentgruppe 2	Sicherheitskopf-Segmentgruppe 1	NACHRICHTEN-NUTZDATENTEIL/ OBJEKT	Sicherheitsende-Segmentgruppe 1	Sicherheitsende-Segmentgruppe 2	Sicherheitsende-Segmentgruppe 3	UNT/ UNP
-------------	---------------------------------	---------------------------------	---------------------------------	--------------------------------------	---------------------------------	---------------------------------	---------------------------------	-------------

Bild 3 — Anwendungsbereich: Nur Sicherheitskopf-Segmentgruppe und Nachrichten-Nutzdatenteil/Objekt (schematisch)

2. Die Berechnung beginnt mit der gegenwärtigen Sicherheitskopf-Segmentgruppe – und schließt diese ein – bis zur entsprechenden Sicherheitsende-Segmentgruppe. In diesem Fall umfasst der Anwendungsbereich die gegenwärtige Sicherheitskopf-Segmentgruppe, den Nachrichten-Nutzdatenteil oder das Objekt sowie alle weiteren eingebetteten Sicherheitskopf- und Sicherheitsende-Segmentgruppen.

Der Anwendungsbereich umfasst jedes Zeichen vom ersten, namentlich ein „U“, der gegenwärtigen Sicherheitskopf-Segmentgruppe bis zum Trennzeichen, das dem ersten Zeichen der entsprechenden Sicherheitsende-Segmentgruppe vorangestellt ist. Dabei sind beide Zeichen enthalten.

Das Bild 4 veranschaulicht diesen Fall (der Anwendungsbereich des Sicherheitsdienstes, der in der Sicherheitskopf-Segmentgruppe 2 definiert ist, ist durch die schraffierten Boxen dargestellt):

UNH/ UNO	Sicherheitskopf-Segmentgruppe 3	Sicherheitskopf-Segmentgruppe 2	Sicherheitskopf-Segmentgruppe 1	NACHRICHTEN-NUTZDATENTEIL/ OBJEKT	Sicherheitsende-Segmentgruppe 1	Sicherheitsende-Segmentgruppe 2	Sicherheitsende-Segmentgruppe 3	UNT/ UNP
-------------	---------------------------------	---------------------------------	---------------------------------	--------------------------------------	---------------------------------	---------------------------------	---------------------------------	-------------

Bild 4 — Anwendungsbereich: Von der Sicherheitskopf-Segmentgruppe bis zur Sicherheitsende-Segmentgruppe (schematisch)

Für jeden ergänzten Sicherheitsdienst kann einer der beiden Fälle gewählt werden.

In beiden Fällen wird die Beziehung zwischen den Sicherheitskopf- und den entsprechenden Sicherheitsende-Segmentgruppen durch die Datenelemente „Sicherheits-Referenznummer“ in den Segmenten USH und UST gegeben.

5.2 Grundsätze der Anwendung

5.2.1 Wahl des Sicherheitsdienstes

Die Sicherheitskopf-Segmentgruppe kann die folgenden allgemeinen Informationen einschließen:

- angewendeter Sicherheitsdienst;
- Identifikation der Beteiligten;
- verwendeter Sicherheitsmechanismus;
- „eindeutiger“ Wert (Folgenummer und/oder Zeitstempel);
- Anfrage zur Unbestreitbarkeit des Empfangs.

Ist mehr als ein Sicherheitsdienst für die gleiche EDIFACT-Struktur erforderlich, kann die Sicherheitskopf-Segmentgruppe mehrmals auftreten. Dies ist der Fall, wenn mehrere Beteiligte involviert sind. Sind mehrere Dienste zwischen den beiden gleichen Beteiligten erforderlich, können diese in einem einzelnen Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaar zusammengefasst werden, da bestimmte Dienste andere implizit enthalten.

5.2.2 Authentizität

Ist die Authentisierung des Absenders einer EDIFACT-Struktur erforderlich, muss sie in Übereinstimmung mit den in ISO/IEC 10181-2 definierten Grundsätzen durchgeführt werden. Dabei wird ein entsprechendes Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaar verwendet.

Der Sicherheitsdienst für die Authentisierung des Absenders muss in dem Segment USH festgelegt werden. Der Algorithmus muss im Segment USA in der Segmentgruppe 1 identifiziert werden. Es muss ein symmetrischer Algorithmus sein.

Der Sicherheits-Urheber muss einen Authentizitätswert berechnen, der im Segment USR der Sicherheitsende-Segmentgruppe befördert wird. Der Sicherheits-Empfänger muss den Authentizitätswert prüfen.

Dieser Dienst kann den Integritätsdienst einschließen, wobei er selbst als ein Nebenprodukt des Dienstes „Unbestreitbarkeit des Ursprungs“ hervorgehen kann.

Wenn eine entsprechende Implementierung diesen „Authentisierung des Absenders“-Dienst auf Basis fälschungssicherer Hardware verwendet, kann sie als ein Beispiel des Dienstes „Unbestreitbarkeit des Ursprungs“ betrachtet werden. Eine derartige Praxis muss in der Datenaustauschvereinbarung definiert werden.

5.2.3 Integrität

Ist die Datenintegrität einer EDIFACT-Struktur erforderlich, muss sie in Übereinstimmung mit den in ISO/IEC 10181-6 definierten Grundsätzen durchgeführt werden. Dabei wird ein entsprechendes Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaar verwendet.

Der Sicherheitsdienst für die Integrität muss in dem Segment USH festgelegt werden. Der Algorithmus muss im Segment USA in der Segmentgruppe 1 identifiziert werden. Es muss eine Hashfunktion oder ein symmetrischer Algorithmus sein.

Der Sicherheits-Urheber muss einen Integritätswert berechnen, der im Segment USR der Sicherheitsende-Segmentgruppe befördert wird. Der Sicherheits-Empfänger muss den Integritätswert prüfen.

Dieser Dienst kann als ein Nebenprodukt des Dienstes „Authentisierung des Absenders“ oder „Unbestreitbarkeit des Ursprungs“ hervorgehen.

Ist eine Integrität der Reihenfolge erforderlich, muss entweder eine Sicherheits-Folgenummer bzw. ein Sicherheits-Zeitstempel oder beides in der Sicherheitskopf-Segmentgruppe enthalten sein. Darüber hinaus muss entweder der Dienst „Datenintegrität“ oder „Authentisierung des Absenders“ oder „Unbestreitbarkeit des Ursprungs“ verwendet werden.

5.2.4 Unbestreitbarkeit des Ursprungs

Ist die Unbestreitbarkeit des Ursprungs einer EDIFACT-Struktur erforderlich, muss sie in Übereinstimmung mit den in ISO/IEC 10181-4 definierten Grundsätzen durchgeführt werden. Dabei wird ein entsprechendes Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaar verwendet.

Der Sicherheitsdienst für die Unbestreitbarkeit des Ursprungs muss in dem Segment USH festgelegt werden. Der Hash-Algorithmus muss im Segment USA in der Segmentgruppe 1 und der für die Unterschrift verwendete asymmetrische Algorithmus in den USA-Segmenten der Segmentgruppe 2 identifiziert werden, sofern Zertifikate verwendet werden.

Wird das Zertifikat nicht in der Nachricht bzw. das Paket befördert, muss der asymmetrische Algorithmus beim Empfänger bereits bekannt sein. In diesem Fall muss der asymmetrische Algorithmus in der Datenaustauschvereinbarung definiert werden.

Der Sicherheits-Urheber muss eine digitale Unterschrift berechnen, die im Segment USR der Sicherheitsende-Segmentgruppe befördert wird. Der Sicherheits-Empfänger muss den Wert der digitalen Unterschrift prüfen.

Dieser Dienst bietet auch die Dienste „Datenintegrität“ und „Authentisierung des Absenders“.