

DIN ISO 9735-6



ICS 35.240.60

**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 9735-6:2002)**

Electronic data interchange for administration, commerce and transport (EDIFACT) –
Application level syntax rules (Syntax version number: 4, Syntax release number: 1) –
Part 6: Secure authentication and acknowledgement message (message type – AUTACK)
(ISO 9735-6:2002)

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 6: Message de sécurité pour l'authentification et la connaissance (type de
message – AUTACK) (ISO 9735-6:2002)

Gesamtumfang 36 Seiten

Normenausschuss Bürowesen (NBü) im DIN

Die Internationale Norm ISO 9735-6:2002 „Electronic data interchange for administration, commerce and transport (EDIFACT) – Application level syntax rules (Syntax version number: 4, Syntax release number: 1) – Part 6: Secure authentication and acknowledgement message (message type – AUTACK)“ 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 9735-6:2002, 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 vonstatten 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 6: Sicherheits-Authentisierung und -Bestätigung (Nachrichtentyp – AUTACK) (ISO 9735-6:2002)

Inhalt

	Seite
Vorwort	5
Einleitung	6
1 Anwendungsbereich	6
2 Konformität	6
3 Normative Verweisungen	7
4 Begriffe	7
5 Regeln für die Anwendung der Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht	7
Anhang A (informativ) Beispiele für AUTACK-Nachrichten	14
Anhang B (informativ) Sicherheitsdienste und -Algorithmen	28
Literaturhinweise	36

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 9735-6 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 9735-6:1999). 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 9735-6 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 und B 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, durch eine Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht.

1 Anwendungsbereich

Dieser Teil der ISO 9735 für die Sicherheit bei EDIFACT definiert die Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht AUTACK.

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 5 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 9735-5:2002, *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 9735-10:2002, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4, Syntax-Releasenummer: 1) — Teil 10: Syntax-Service-Verzeichnisse.*

4 Begriffe

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

5 Regeln für die Anwendung der Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht

5.1 Funktionsbeschreibung

Die AUTACK ist eine Nachricht zur Authentisierung von gesendeten oder zur gesicherten Bestätigung von empfangenen Übertragungsdateien, Gruppen, Nachrichten oder Paketen.

Eine Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht kann verwendet werden für:

- a) eine gesicherte Authentisierung, Integrität oder Unbestreitbarkeit des Ursprungs von Nachrichten, Paketen, Gruppen oder Übertragungsdateien;
- b) eine gesicherte Bestätigung oder Unbestreitbarkeit des Empfangs von gesicherten Nachrichten, Paketen, Gruppen oder Übertragungsdateien.

5.2 Anwendungsbereich

Die Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht (AUTACK) darf sowohl im nationalen als auch im internationalen Handel verwendet werden. Sie basiert auf allgemeiner Praxis und ist nicht auf bestimmte Geschäftsarten oder Wirtschaftsbereiche beschränkt.

5.3 Grundsätzliches

5.3.1 Allgemeines

Die angewendeten Sicherheitsverfahren müssen zwischen den Handelspartnern vereinbart und in einer Datenaustauschvereinbarung festgeschrieben werden.

Die Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht (AUTACK) wendet Sicherheitdienste auf andere EDIFACT-Strukturen (Nachrichten, Pakete, Gruppen, Übertragungsdateien) an und bietet eine gesicherte Bestätigung auf gesicherte EDIFACT-Strukturen. Sie kann auf Kombinationen von EDIFACT-Strukturen angewendet werden, die zwischen zwei Beteiligten gesichert werden müssen.

Die Sicherheitsdienste werden durch kryptographische Mechanismen bereitgestellt, die auf den Inhalt der originalen EDIFACT-Strukturen angewendet werden. Die Ergebnisse dieser Mechanismen bilden den Nutzdatenteil der AUTACK-Nachricht, unterstützt durch relevante Daten wie beispielsweise Referenzen der verwendeten kryptographischen Methoden, die Referenznummern der EDIFACT-Strukturen und das Datum und die Uhrzeit der originalen Strukturen.

Die AUTACK-Nachricht muss die genormten Sicherheitskopf- und Sicherheitsende-Segmentgruppen verwenden.

Die AUTACK-Nachricht kann auf eine oder mehrere Nachrichten, Paketen oder Gruppen von einer oder mehreren Übertragungsdateien oder auf eine oder mehrere Übertragungsdateien angewendet werden. Als ein Beispiel beschreibt Bild 1 eine Übertragungsdatei, die eine AUTACK-Nachricht zusammen mit einer oder mehreren Nachrichten verwendet.

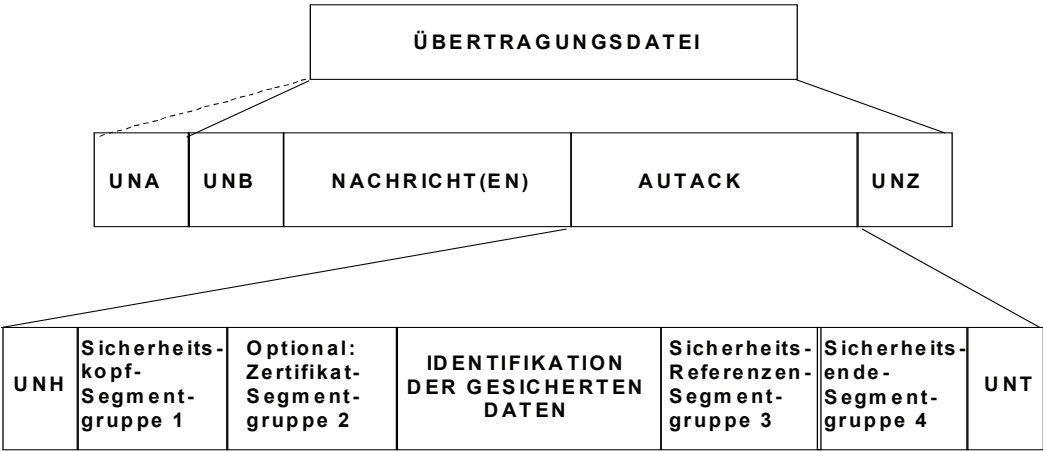


Bild 1 — Übertragungsdatei, die durch eine AUTACK-Nachricht auf Nachrichtenebene geschützt ist (schematisch)

5.3.2 Verwendung der AUTACK für die Authentisierungsfunktion

5.3.2.1 Allgemeines

Eine als Authentisierungs-Nachricht verwendete AUTACK wird vom Aussteller einer oder mehrerer anderer EDIFACT-Strukturen oder von einem Beteiligten, der im Einvernehmen mit dem Aussteller in dessen Auftrag handelt, gesendet. Die AUTACK erleichtert die Anwendung der in ISO 9735-5 definierten Sicherheitsdienste, d. h. die Authentizität, die Integrität und die Unbestreitbarkeit des Ursprungs der verbundenen EDIFACT-Strukturen.

Eine AUTACK-Authentisierungs-Nachricht kann auf zwei Arten angewendet werden. Die erste Methode transportiert die Hashwerte der referenzierten EDIFACT-Strukturen, die durch die AUTACK selbst gesichert werden. Bei der zweiten Methode wird die AUTACK nur dazu verwendet, die digitalen Unterschriften der referenzierten EDIFACT-Strukturen zu transportieren.

5.3.2.2 Authentisierung mittels Hashwerte der referenzierten EDIFACT-Strukturen

Die gesicherte EDIFACT-Struktur muss in einem Auftreten des Segmentes USX (Sicherheits-Referenzen) referenziert werden. Für jedes USX muss es mindestens ein korrespondierendes Segment USY (Sicherheit zu Referenzen) geben, welches das Sicherheitsergebnis, wie beispielsweise den Hashwert der auf die referenzierte EDIFACT-Struktur durchgeführten Sicherheitsfunktion, enthält.

Einzelheiten über die durchgeführte Sicherheitsfunktion sind in der Sicherheitskopf-Segmentgruppe der AUTACK enthalten. Die Segmente USY und USH für die referenzierte EDIFACT-Struktur müssen durch das Datenelement „Sicherheits-Referenznummer“ in beiden Segmenten verknüpft werden.

Als ein abschließender Schritt muss die gesamte in der AUTACK transportierte Information durch die Verwendung mindestens eines Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaares gesichert werden.

ANMERKUNG AUTACK verwendet das Segment USX, um eine oder mehrere Nachrichten, Pakete oder Gruppen in einer oder mehreren Übertragungsdateien zu referenzieren oder um eine komplette Übertragungsdatei zu referenzieren. Für jedes Segment USX enthält ein korrespondierendes Segment USY das Hash-Ergebnis, die Authentisierung oder das Unbestreitbarkeits-Verfahren, welches auf die referenzierte EDIFACT-Struktur angewendet wurde.

5.3.2.3 Authentisierung mittels digitaler Unterschriften der referenzierten EDIFACT-Strukturen

Die gesicherte EDIFACT-Struktur muss in einem Auftreten des Segmentes USX (Sicherheits-Referenzen) referenziert werden. Für jedes USX muss es mindestens ein korrespondierendes Segment USY (Sicherheit zu Referenzen) geben, welches die digitale Unterschrift der referenzierten EDIFACT-Struktur enthält. Einzelheiten über die durchgeführte Sicherheitsfunktion sind in der Sicherheitskopf-Segmentgruppe der AUTACK enthalten. Da eine einzelne referenzierte EDIFACT-Struktur mehr als einmal gesichert sein kann, müssen das entsprechende USY und die Sicherheitskopf-Segmentgruppe durch das Datenelement „Sicherheits-Referenznummer“ in beiden Segmenten verknüpft werden.

Wenn die digitale Unterschrift der referenzierten EDIFACT-Struktur in der AUTACK enthalten ist (mehr als nur ein Hashwert), muss die AUTACK selbst nicht gesichert werden.

5.3.3 Die Anwendung der AUTACK für die Bestätigungsfunktion

Eine für die Bestätigungsfunktion verwendete AUTACK-Nachricht muss vom Empfänger einer oder mehrerer vorher empfangener gesicherten EDIFACT-Strukturen oder von einem Beteiligten, der im Einvernehmen mit dem Empfänger in dessen Auftrag handelt, gesendet werden. Die AUTACK erleichtert die Anwendung der Empfangsbestätigung, die Prüfung der Datenintegrität, die Prüfung auf Vollständigkeit und/oder die Unbestreitbarkeit des Empfangs der verbundenen EDIFACT-Strukturen.

Die Bestätigungsfunktion darf nur auf gesicherte EDIFACT-Strukturen angewendet werden. Die gesicherte EDIFACT-Struktur muss in einem Auftreten des Segmentes USX (Sicherheits-Referenzen) referenziert werden. Für jedes USX muss es mindestens ein korrespondierendes Segment USY (Sicherheit zu Referenzen) geben, welches entweder den Hashwert oder die digitale Unterschrift der referenzierten

EDIFACT-Struktur enthält. Das USY muss mit einer Sicherheitskopf-Segmentgruppe entweder der referenzierten EDIFACT-Struktur oder mit einer diese Struktur sichernde AUTACK-Nachricht durch das Datenelement „Sicherheits-Referenznummer“ verknüpft sein. Der korrespondierende, auf die referenzierte EDIFACT-Struktur bezogene Sicherheitskopf enthält die Einzelheiten über die vom Absender der originalen Nachricht auf die referenzierte EDIFACT-Struktur durchgeführten Sicherheitsfunktion.

Als ein abschließender Schritt bei der Generierung der Bestätigungs-Nachricht muss die gesamte in der AUTACK transportierte Information durch die Verwendung mindestens eines Sicherheitskopf- und Sicherheitsende-Segmentgruppenpaares gesichert werden.

Die AUTACK darf ebenso für die Nicht-Bestätigung verwendet werden, wenn Probleme mit der Prüfung der Sicherheitsergebnisse auftreten.

ANMERKUNG Die Sicherheits-Bestätigung ist nur für gesicherte EDIFACT-Strukturen sinnvoll. Die Sicherung von EDIFACT-Strukturen wird entweder durch die Verwendung integrierter Sicherheits-Segmente (siehe ISO 9735-5) oder der AUTACK-Authentisierung erreicht.

Um Endlosschleifen zu vermeiden, darf eine für die Bestätigungsfunktion verwendete AUTACK beim Empfänger nicht die Rücksendung einer AUTACK-Bestätigungs-Nachricht anfordern.

5.4 Nachrichtendefinition

5.4.1 Segmentbeschreibung

0010 UNH, Nachrichten-Kopfsegment

Ein Service-Segment, mit dem eine Nachricht beginnt und das diese eindeutig identifiziert.

Die Nachrichtentyp-Kennung für die Sicherheits-Authentisierungs- und -Bestätigungs-Nachricht ist AUTACK. Das Datenelement „Nachrichtentyp-Unterfunktion, Identifikation“ wird verwendet, um die Verwendung der AUTACK entweder als Authentisierung, Bestätigung oder Zurückweisung anzuzeigen.

Nachrichten des Typs „Sicherheits-Authentisierung und -Bestätigung“, die mit dieser Norm übereinstimmen, müssen die folgenden Daten im Segment UNH, Datenelementgruppe S009, enthalten:

Datenelement	0065	AUTACK
	0052	4
	0054	1
	0051	UN

0020 Segmentgruppe 1: USH-USA-SG2 (Sicherheitskopf-Segmentgruppe)

Eine Gruppe von Segmenten zur Identifizierung der angewendeten Sicherheitsdienste und Sicherheitsmechanismen. Darüber hinaus enthält sie die für die Durchführung der Prüfberechnungen (wie in ISO 9735-5 definiert) notwendigen Daten.

Diese Segmentgruppe muss den Sicherheitsdienst und die Sicherheitsalgorithmen festlegen, die auf die AUTACK-Nachricht oder die referenzierte EDIFACT-Struktur angewendet sind.

Jede Sicherheitskopf-Segmentgruppe muss mit einer Sicherheitsende-Segmentgruppe verknüpft werden. Darüber hinaus können auch USY-Segmente verknüpft sein.

0030 USH, Sicherheits-Kopfsegment

Ein Segment zur Angabe eines Sicherheitsdienstes, der auf die Nachricht bzw. das Paket, in der/das Segment enthalten ist, oder auf die referenzierte EDIFACT-Struktur (wie in ISO 9735-5 definiert) angewendet wird.

Das Datenelement „Sicherheitsdienst“ muss die auf die AUTACK-Nachricht oder referenzierte EDIFACT-Struktur angewendete Sicherheitsfunktion festlegen:

- die Sicherheitsdienste „Authentisierung des Nachrichtenursprungs“ und „Unbestreitbarkeit des Ursprungs“ dürfen nur für die AUTACK-Nachricht selbst verwendet werden;
- die Sicherheitsdienste „Integrität der referenzierten EDIFACT-Struktur“, „Authentisierung des Ursprungs der referenzierten EDIFACT-Struktur“ und „Unbestreitbarkeit des Ursprungs der referenzierten EDIFACT-Struktur“ dürfen nur vom Absender verwendet werden, um die mittels der AUTACK referenzierten EDIFACT-Strukturen zu sichern;
- die Sicherheitsdienste „Authentisierung des Empfangs“ und „Unbestreitbarkeit des Empfangs“ dürfen nur vom Empfänger der gesicherten EDIFACT-Strukturen verwendet werden, um die Bestätigung zu sichern.

Der Anwendungsbereich des Sicherheitsdienstes muss nach ISO 9735-5 festgelegt werden. In einer AUTACK-Nachricht gibt es vier mögliche Anwendungen der Sicherheitsapplikation:

- die ersten beiden Fälle sind in ISO 9735-5:2002, Abschnitt 5, definiert;
- der dritte Fall schließt die gesamte EDIFACT-Struktur ein, d. h., die Sicherheitsapplikation reicht vom ersten Zeichen (namentlich ein „U“) bis einschließlich letzten Zeichen der referenzierten Nachricht, des Pakets, der Gruppe oder der Übertragungsdatei;
- der vierte Anwendungsbereich ist benutzerdefiniert und wird zwischen dem Absender und Empfänger gesondert vereinbart.

0040 **USA, Sicherheits-Algorithmus**

Ein Segment zur Angabe eines Sicherheits-Algorithmus, der entsprechend zugrunde liegenden technischen Anwendung und der erforderlichen technischen Parameter (wie in ISO 9735-5 definiert).

0050 **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 (wie in ISO 9735-5 definiert).

0060 **USC, Zertifikat**

Ein Segment, das die Beglaubigungen des Zertifikatseigners enthält und die berechnete Zertifizierungsinstanz identifiziert, die das Zertifikat ausgestellt hat (wie in ISO 9735-5 definiert).

0070 **USA, Sicherheits-Algorithmus**

Ein Segment zur Angabe eines Sicherheits-Algorithmus, der entsprechend zugrunde liegenden technischen Anwendung und der erforderlichen technischen Parameter (wie in ISO 9735-5 definiert).

0080 **USR, Sicherheitsergebnis**

Ein Segment, das das Ergebnis der Sicherheitsfunktionen enthält, die von der berechtigten Zertifizierungsinstanz auf das Zertifikat angewendet wurden (wie in ISO 9735-5 definiert).

0090 **USB, Identifikation der gesicherten Daten**

Dieses Segment enthält die Identifikation des Absenders und des Empfängers der Übertragungsdatei und einen sicherheitsbezogenen Zeitstempel der AUTACK. Darüber hinaus muss darin festgelegt werden, ob eine Sicherheits-Bestätigung vom Empfänger der AUTACK-Nachricht erforderlich ist oder nicht. Wenn eine Bestätigung erforderlich ist, erwartet der Nachrichten-Absender eine vom Nachrichten-Empfänger zurückzusendende AUTACK-Bestätigungs-Nachricht.