

	EDIFACT Anwendungsregeln Teil 15: Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten	DIN 16560-15
--	--	--

ICS 35.240.60

EDIFACT — Implementation guide — Part 15: Use of the service message type AUTACK for conveying of integrity and authenticity data of send user data

EDIFACT — Guide d'implémentation — Partie 15: Utilisation du type de message de service AUTACK pour transmettre les données concernant l'intégrité et l'authenticité de données envoyées par un utilisateur

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 (EDI) im weiteren Sinn auch Electronic Commerce zuständig.

Die vorliegende Norm basiert auf den Service-Nachrichtentyp AUTACK „Sicherheits-Authentisierung und -Bestätigung“ nach ISO 9735-6:2002.

Die Norm ist – soweit notwendig – mit der Norm DIN 16560-16 harmonisiert, die die Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten beschreibt.

Der Anhang A dient nur zur Information.

DIN 16560 *EDIFACT — Anwendungsregeln* besteht aus:

- Teil 1: *Service-Segmente*
- Teil 4: *Prüfbescheinigung der Chemischen Industrie – QUALITY D.99A*
- Teil 15: *Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten*
- Teil 16: *Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten*

Fortsetzung Seite 2 bis 44

Normenausschuss Bürowesen (NBü) im DIN Deutsches Institut für Normung e. V.

Einleitung

Mit der Anerkennung des elektronischen Dokuments mit elektronischer Signatur als Äquivalent zum herkömmlichen Papierdokument wurden etwa 450 Formvorschriften im zivilrechtlichen Bereich dahingehend geändert, dass die elektronische Form, alternativ zur Schriftform, anerkannt wird.

Die digitale Signatur ist eine Art elektronisches Siegel, das die Rechtsverbindlichkeit wichtiger Vorgänge in der elektronischen Kommunikation herstellt.

Die Sicherheit der digitalen Signatur liegt in dem asymmetrischen Verschlüsselungsverfahren. Die Signatur basiert auf der Anwendung zweier Schlüssel: Einem privaten Schlüssel zur Erstellung der Signatur und einem öffentlichen Schlüssel zur Prüfung der Signatur.

Ziel der digitalen Signatur ist ein System, in dem jeder mit jedem ohne Gefahr der Informationsverfälschung kommunizieren kann. Sie dient zur Feststellung

- der Datenintegrität,
- der Authentisierung des Absenders der Nachricht und
- der Unbestreitbarkeit des Ursprungs der Nachricht.

Die in dieser Norm beschriebene Anwendung der AUTACK erfüllt die aktuellen Anforderungen des Geschäftsdatenaustausches im e-Business.

Die in dieser Norm beschriebene Anwendung des Nachrichtentyps AUTACK entstand aus dem Bedürfnis heraus, für die im Deutschen Bundestag am 15. Februar 2001 beschlossene Anpassung des Signaturgesetzes an die europäischen Vorgaben (siehe Richtlinie 1999/93/EG) eine Lösung für den elektronischen Geschäftsdatenaustausch bereitzustellen.

Der in dieser Norm vorliegende „AUTACK-Guide“ beschreibt

die Signierung und Authentifizierung der zur Versendung freigegebenen Nutzdaten.

Die parallel zu dieser Norm veröffentlichte DIN 16560-16 beschreibt zusätzlich die

Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten.

Mit der Anwendung der o. g. Normen ist es möglich, dass

- die Daten zur Authentifizierung und Signatur als letzte EDIFACT-Nachricht mittels AUTACK-Nachricht in die originale Übertragungsdatei, nach dem Ein-Interchange-Ansatz, eingefügt werden;
- die Nutzdaten in einer Übertragungsdatei und die Daten zur Authentifizierung und Signatur in einer zweiten Übertragungsdatei, nach dem Zwei-Interchange-Ansatz, übermittelt werden.

Da der Nachrichtentyp AUTACK erstmalig mit der Syntax-Version 4 veröffentlicht wurde, sind bei seiner Anwendung die Mindestanforderungen der Syntax-Version 4 anzuwenden. Diese Mindestanforderungen betreffen die Segmente UNA, UNB und UNH sowie den Inhalt des Nachrichtentyps AUTACK. Sofern Nutzdaten entsprechend Syntax-Version 3 generiert wurden (UNH ... UNT), sind automatisch die Mindestanforderungen der Syntax-Version 4 erfüllt.

1 Anwendungsbereich

Diese Norm beschreibt die Anwendung des Service-Nachrichtentyps AUTACK nach ISO 9735-6 zur Übermittlung von Integritäts- und Authentizitätsinformationen im elektronischen Datenaustausch beispielsweise für den Abrechnungs- und Zahlungsverkehr.

2 Normative Verweisungen

Diese Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation (einschließlich Änderungen).

DIN 16557-3:1994, *Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) — Teil 3: Allgemeine Einführung für Einheitliche Nachrichtentypen (UNSMs)*.

DIN 16560-16:2003, *EDIFACT — Anwendungsregeln — Teil 16: Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten*.

ISO 9735-1:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, syntax release number: 1) — Part 1: Syntax rules common to all parts*.

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)*.

3 Hinweise zum Lesen der Anwendungsregeln

3.1 Allgemeines

Zum besseren Verständnis der Festlegungen in Abschnitt 4 dienen die folgenden Hinweise (siehe auch DIN 16557-3):

- a) Das angegebene dreistellige Kurzzeichen zur Identifikation eines Segmentes ist der offizielle EDIFACT-Segmentbezeichner (BEZ).
- b) In der tabellarischen Segmentübersicht der Nachricht (siehe 4.1) und im Nachrichtenaufbau-Diagramm (siehe 4.2) ist die maximale Anzahl des Auftretens (WDH) der Segmentgruppe (SG) oder des Segments an dieser Stelle der Nachricht angegeben, die im Rahmen dieser Anwendungsregeln vorgesehen ist. Hierdurch soll die Verarbeitung der dokumentierten Nachricht erleichtert werden.
- c) Datenelemente sind durch vierstellige Kennungen identifiziert. Mehrere Datenelemente können eine Datenelementgruppe bilden, die durch eine dreistellige Nummer mit einem vorangestelltem „S“ gekennzeichnet ist.

ANMERKUNG Im Gegensatz zu den Datenelementgruppen in Service-Segmenten werden bei Nutzdaten-Segmenten die Datenelementgruppen durch eine dreistellige Nummer und einem vorangestellten „C“ (composite) gekennzeichnet.

- d) Zu jedem Datenelement ist in 4.4 neben der Nutzungsangabe die Darstellung angegeben: „an“ bedeutet alphanumerisch, „n“ numerisch, und hinter den zwei Punkten ist die maximale Stellenanzahl angegeben (z. B. n..18, an..3). Eine Angabe ohne Punkte legt eine feste Stellenzahl fest (siehe auch 3.2).
- e) Qualifier sind Codes, die die Bedeutung eines Segmentes oder eines Datenelementes näher festlegen. In der vorliegenden Anwendungsdokumentation sind für Qualifier und teilweise für Codes „erlaubte“ Werte angegeben. Zur Erleichterung der Verarbeitung solcher Nachrichten wird dringend empfohlen, die angegebenen Werte zu verwenden. Darüber hinaus wird auf die offiziellen Codelisten des EDIACT-Verzeichnisses verwiesen, das weitere Codes enthalten kann.
- f) Die Struktur jedes einzelnen Segments wurde komplett dargestellt, auch wenn einzelne Bestandteile des Segmentes nicht verwendet werden.
- g) Unter „Kommentar“ (jeweils am Ende eines beschriebenen Segmentes) finden sich in 4.4 allgemeine Angaben zum Segment, während unter „Codierungsbeispiel“ die in der jeweiligen tabellarischen Darstellung des Segmentes in der Spalte „Beispiel“ angegebenen Werte hier summarisch als EDIFACT-Übertragungskette dargestellt sind.

ANMERKUNG Die komplette EDIFACT-Übertragungskette bzw. -datei ist in der Musternachricht in 4.5 dargestellt.

3.2 Strukturen

Die in dieser Norm zur Anwendung dokumentierte EDIFACT-Service-Nachricht schließt die Beschreibung der Service-Segmente UNB und UNZ ein. Darüber hinaus kann die Anwendung der Trennzeichenvorgabe UNA und der Gruppen-Segmente UNG und UNE erforderlich sein (siehe ISO 9735-1).

Eine EDIFACT-Übertragungsdatei ist prinzipiell nach Bild 1 aufgebaut.

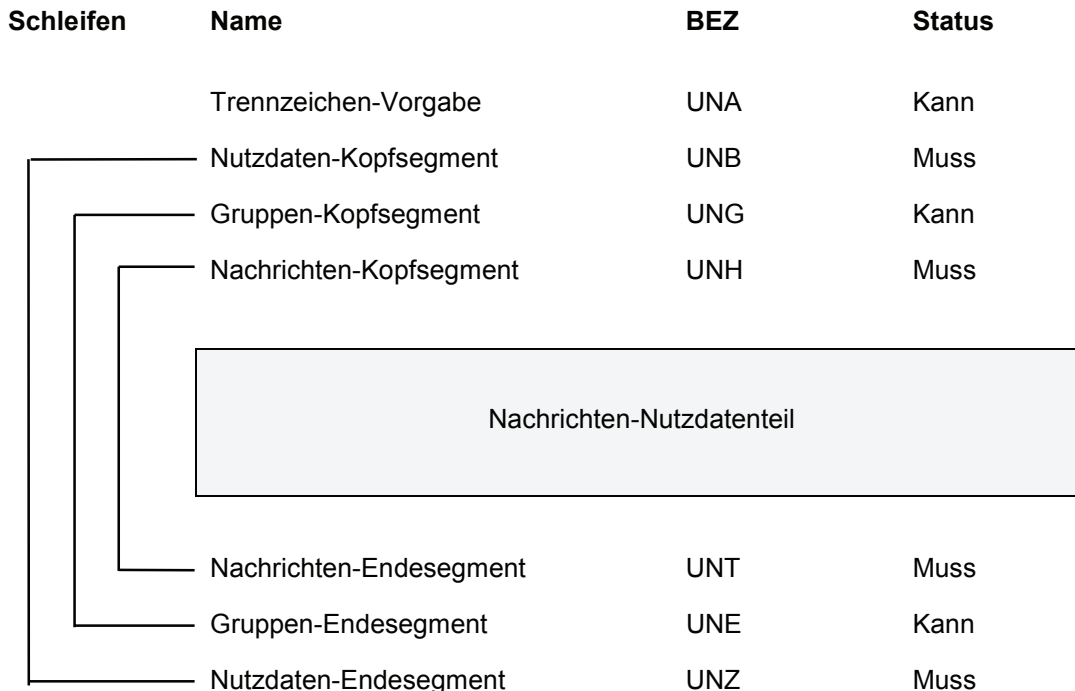


Bild 1 — Struktur einer EDIFACT-Übertragungsdatei

Die darin enthaltenen Service-Segmente übernehmen folgende Funktionen:

UNA (Trennzeichen-Angabe) – Eine optionale Zeichenkette, die am Beginn einer Übertragungsdatei steht, um die darin verwendeten Servicezeichen (Trennzeichen) festzulegen.

UNB (Nutzdaten-Kopfsegment) – Dient dazu, eine Übertragungsdatei zu identifizieren.

UNG (Gruppen-Kopfsegment) – Dient dazu, eine Gruppe von Nachrichten und/oder Paketen zu eröffnen, sie zu identifizieren und zu beschreiben. Dies kann zur internen Weiterleitung verwendet werden und einen oder mehrere Nachrichtentypen und/oder Pakete enthalten.

UNH (Nachrichten-Kopfsegment) – Dient dazu, eine Nachricht zu eröffnen, sie zu identifizieren und zu beschreiben.

UNT (Nachrichten-Endesegment) – Dient dazu, eine Nachricht zu beenden und sie auf Vollständigkeit zu prüfen.

UNE (Gruppen-Endesegment) – Dient dazu, eine Gruppe zu beenden und sie auf Vollständigkeit zu prüfen.

UNZ (Nutzdaten-Endesegment) – Dient dazu, eine Übertragungsdatei zu beenden und sie auf Vollständigkeit zu prüfen.

3.3 Dokumentationskonventionen

Folgende Konventionen gelten für die vorliegende Dokumentation:

a	alphabetische Zeichen
n	numerische Zeichen
an	alphanumerische Zeichen
a3	3 alphabetische Zeichen fester Länge
n3	3 numerische Zeichen fester Länge
an3	3 alphanumerische Zeichen fester Länge
a..3	bis zu 3 alphabetische Zeichen
n..3	bis zu 3 numerische Zeichen
an..3	bis zu 3 alphanumerische Zeichen

3.4 Statusindikatoren

Nach den EDIFACT-Regeln gibt es nur die Statuswerte „M“ (mandatory = Muss) und „C“ (conditional = Kann) zur Nutzung der Segmente, der Datenelementgruppen und der Datenelemente. Während Muss-(M-) Datenelemente oder -Datenelementgruppen aus Segmenten ihren EDIFACT-Status auch in der Anwendung behalten, wird der EDIFACT-Status „Kann“ bedarfsgerecht durch einen der fünf in Tabelle 1 gegebenen Statustypen ersetzt.

Tabelle 1 — Umsetzung des EDIFACT-Status „C“ in der Anwendung

Statustyp (engl. Name)	Status	Beschreibung
ERFORDERLICH (required)	R	Gibt an, dass die Nutzung dieses Elements erforderlich ist und daher verwendet werden muss.
EMPFOHLEN (advised)	A	Gibt an, dass die Nutzung dieses Elements empfohlen wird.
ABHÄNGIG (dependent)	D	Gibt an, dass die Nutzung dieses Elements von bestimmten Bedingungen abhängt, die in entsprechenden Hinweisen angegeben sind.
OPTIONAL (optional)	O	Gibt an, dass die Nutzung dieses Elements optional ist und die Verwendung im Ermessen des Anwenders liegt.
Nicht benötigt (not used)	N	Gibt an, dass dieses Element bei der Ausführung nicht beachtet wird.

3.5 Abhängigkeiten

Abhängigkeitshinweise (Dependency notes), die in ISO 9735-1 und ISO 9735-6 zu einzelnen Datenelementgruppen beschrieben sind, wurden in dieser Norm in Textform aufgelöst.

4 Anwendungsdokumentation

4.1 Tabellarische Segmentübersicht der Nachricht

ANMERKUNG Die USR-Segmente werden in dieser spezifischen Ausführung der AUTACK nicht verwendet. Die laufende Nummerierung zur Identifizierung der Segmente übergeht daher die USR-Segmente; sie ist identisch mit der entsprechenden Nummerierung der Segmente im Nachrichtenaufbau-Diagramm (siehe 4.2), in der Segmentbeschreibung (siehe 4.4) und in der Musternachricht (siehe 4.5).

Tabelle 2 — Tabellarische Segmentübersicht der Nachricht

Lfd. Nr.	BEZ	S	WDH	Segment(gruppe)
1	UNB	M	1	Nutzdaten-Kopfsegment
2	UNH	M	1	Nachrichten-Kopfsegment
	SG1	M	99	USH-USA-SG2
3	USH	M	1	Sicherheits-Kopfsegment
4	USA	R	3	Sicherheits-Algorithmus
	SG2	R	2	USC-USA
5	USC	M	1	Zertifikat
6	USA	R	3	Sicherheits-Algorithmus
	USR	N	1	Sicherheitsergebnis
7	USB	M	1	Identifikation der gesicherten Daten
	SG3	M	9999	USX-USY
8	USX	M	1	Sicherheits-Referenzen
9	USY	M	9	Sicherheit zu Referenzen

Tabelle 2 (fortgesetzt)

	SG4	M	99	UST
10	UST	M	1	Sicherheits-Endesegment
	USR	N	1	Sicherheitsergebnis
11	UNT	M	1	Nachrichten-Endesegment
12	UNZ	M	1	Nutzdaten-Endesegment
Legende: BEZ Bezeichner S Status WDH max. Wiederholung				

4.2 Nachrichtenaufbau-Diagramm

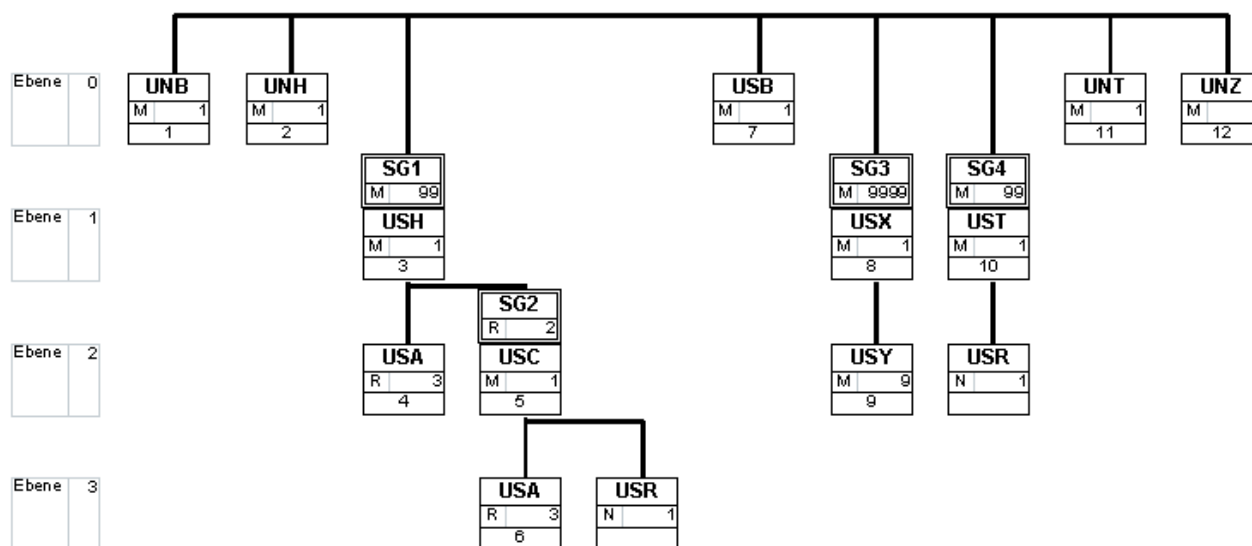


Bild 2 — Nachrichtenaufbau-Diagramm

Jede in der Segmentbeschreibung (siehe 4.4) beschriebene Segment- und Segmentgruppenvariante erscheint im Nachrichtenaufbau-Diagramm (siehe Bild 2) genau einmal, auch wenn ein Segment bzw. eine Segmentgruppe mehr als einmal verwendet wird. Der Buchstabe in der jeweiligen zweiten Zeile eines Kästchens gibt den Status, der dahinter angegebene numerische Wert die maximale Anzahl der Wiederholung an. Die numerische Angabe im unteren Teil der Kästchen ist ein Hinweis auf die laufende Segmentnummer in der Segmentbeschreibung.

4.3 Verwendete Sicherheits-Service-Segmente der AUTACK

Die in der AUTACK verwendeten Sicherheits-Service-Segmente übernehmen folgende Funktionen:

USA (Sicherheits-Algorithmus) – Dient dazu, den zur Bildung eines Prüfwertes verwendeten Sicherheits-Algorithmus zu identifizieren.

USB (Identifikation der gesicherten Daten) – Dient dazu, die Angaben des UNB-Segmentes, in der sich die AUTACK befindet, wiederzugeben.

USC (Zertifikat) – Dient dazu, die Beglaubigung des Zertifikatseigners anzugeben und die Zertifizierungsinstanz zu identifizieren.

USH (Sicherheits-Kopfsegment) – Dient dazu, einen Sicherheitsdienst, der auf eine Übertragungsdatei, eine Nachrichtengruppe oder eine Nachricht angewendet wurde, zu identifizieren.

UST (Sicherheits-Endesegment) – Dient dazu, eine Verbindung zwischen der Sicherheitskopf-Segmentgruppe und der Sicherheitsende-Segmentgruppe festzulegen.

USX (Sicherheits-Referenzen) – Dient dazu, eine Referenz auf die gesamte Übertragungsdatei, auf eine darin enthaltene Nachrichtengruppe oder eine darin enthaltene Nachricht anzugeben.

USY (Sicherheit zu Referenzen) – Dient dazu, die Verknüpfung zur Sicherheitskopf-Segmentgruppe und das Ergebnis der auf die referenzierte EDIFACT-Struktur angewendeten Sicherheitsdienste anzugeben.

4.4 Segmentbeschreibung

Segment: **UNB** Ifd. Nr.: 1 Ebene: 0 Nutzdaten-Kopfsegment
Status: M Max. Wdh.: 1

Beschreibung: Nutzdaten-Kopfsegment

Formale Beschreibung des Segmentes:

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
UNB	Nutzdaten-Kopfsegment	M	M	UNB	Angabe der Syntax-Kennung und des Zeichensatzes. Hier handelt es sich um einen aus zwei Codierungen zusammengesetzten Wert, der den verwendeten Zeichensatz festlegt. Die ersten drei Buchstaben legen die verantwortliche Stelle für die Pflege dieses Zeichensatzes fest – hier steht ‚UNO‘ für die EDIFACT-Syntax, der vierte Buchstabe legt die Ausgabe fest. Folgende Identifikationen werden empfohlen: Code: UNOA UN/ECE-Zeichensatz A Code: UNOB UN/ECE-Zeichensatz B Angabe der Syntax-Version. Hier wird die verwendete Syntax-Version festgelegt. Es ist die Zahl „4“ gemäß der seit 1999 gültigen Syntax-Version einzusetzen. Code: 4 Version 4
S001	Syntax-Bezeichner	M	M		
0001	Syntax-Kennung	M a4	M	+UNOB	
0002	Syntax-Versionsnummer	M an1	M	:4	
S002	Absender der Übertragungsdatei	M	M		
0004	Absenderbezeichnung für Übertragungsdatei	M an..35	M	+ABSEN- DER-ID	Identifikation des Absenders dieser Übertragungsdatei. Diese Bezeichnung kennzeichnet den Absender und muss eindeutig in einem Netzwerk oder einer Benutzergruppe definiert sein. Innerhalb dieser Organisation muss es eine verantwortliche Stelle geben, die die Eindeutigkeit sicherstellt. Grundsätzlich wird diese Bezeichnung vom Absender dem Empfänger vorgegeben. Weitgehend eindeutige Bezeichnungen sind z. B. ILN oder die DUNS-Nummer. Verwendet werden können auch die Telefon- oder Telexnummern. Die Verwendung von uncodierten Absenderbezeichnungen ist möglich, doch ist die Sicherstellung der Eindeutigkeit schwierig. Als uncodierte Angabe kann z. B. der Firmenname verwendet werden. Vorrangig sollten jedoch nur codierte Absenderbezeichnungen verwendet werden.

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
0007	Teilnehmerbezeichnung, Qualifier	C an..4	O	:14	Verwendung ist optional. Falls die Absenderbezeichnung codiert angegeben wird, muss in diesem Feld der entsprechende Qualifier eingetragen werden, der der codierten Angabe in DE 0004 eine bestimmte Bedeutung zuordnet. Der Qualifier z. B. für Telefon ist der Codeliste zum DE 0007 zu entnehmen. Identifikation der Organisation, die für die vorstehende Codeliste verantwortlich ist, z. B. Code: 14 EAN (European Article Numbering Association) Code: 55 BIC Business Identifier Code Code: 59 ODETTE (Organization for Data Exchange) Code: 91 Zugewiesen durch den Verkäufer oder dessen Agenten Code: 92 Zugewiesen durch den Käufer oder dessen Agenten
S003	Empfänger der Übertragungsdatei	M	M		
0010	Empfängerbezeichnung für Übertragungsdatei	M an..35	M	+EMPFAEN-GER-ID	Identifikation des Empfängers dieser Übertragungsdatei. Es gelten sinngemäß die Ausführungen zu S002_0004. Die Empfängerbezeichnung wird dem Absender vom Empfänger mitgeteilt.
0007	Teilnehmerbezeichnung, Qualifier	C an..4	O	:14	Verwendung ist optional. Falls die Absenderbezeichnung codiert angegeben wird, muss in diesem Feld der entsprechende Qualifier eingetragen werden, der der codierten Angabe in DE 0004 eine bestimmte Bedeutung zuordnet. Der Qualifier z. B. für Telefon ist der Codeliste zum DE 0007 zu entnehmen. Identifikation der Organisation, die für die vorstehende Codeliste verantwortlich ist, z. B. Code: 14 EAN (European Article Numbering Association) Code: 55 BIC Business Identifier Code Code: 59 ODETTE (Organization for Data Exchange) Code: 91 Zugewiesen durch den Verkäufer oder dessen Agenten Code: 92 Zugewiesen durch den Käufer oder dessen Agenten
S004	Datum und Uhrzeit der Erstellung	M	M		
0017	Datum der Erstellung	M n8	M	+20011015	Erstellungsdatum der Übertragungsdatei im Format JJJJMMTT.
0019	Uhrzeit der Erstellung	M n4	M	:1005	Erstellungszeit der Übertragungsdatei im Format HHMM.

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
0020	Datenaustauschreferenz	M an..14	M	+DIN AUT001	Angabe einer eindeutigen Datenaustauschreferenz, vergeben vom Sender. Identisch mit der Angabe in UNZ_0020. Jede Übertragungsdatei, die zwischen dem in S002_0004 und S003_0010 identifizierten Absender und Empfänger ausgetauscht wird, hat eine eindeutige Identifizierung. Diese Referenz ist partnerspezifisch. Es sollte eine lückenlos aufsteigende Nummer als Referenz gewählt werden, weil mit Plausibilitätsprüfungen Doppel- und Fehlübertragungen festgestellt werden können. Für diese Methode gilt dann auch weiterhin, dass eine niedrigere Nummer auch einen älteren Zeitstempel (in DE 0017, DE 0019) haben muss. Hinweis: Die Datenaustauschreferenz wird vom Sender der Übertragungsdatei generiert und dient der eindeutigen Identifikation jeder Übertragungsdatei. Sollte der Sender der Übertragungsdatei Datenaustauschreferenzen wiederverwenden wollen, wird empfohlen, jede Nummer bzw. alphanumerische Nummernkombination (z. B. XANA000001) innerhalb eines Jahres nur einmal zu verwenden. Zur Sicherstellung der Eindeutigkeit sollte die Datenaustauschreferenz (DE 0020) mit der Absenderidentifikation (DE 0004) verbunden werden.
S005	Referenz/Passwort des Empfängers	C	N		Wird bei der Ausführung nicht beachtet.
0022	Referenz oder Passwort des Empfängers	M an..14	M +		Wird bei der Ausführung nicht beachtet.
0026	Anwendungsreferenz	C an..14	N +		Wird bei der Ausführung nicht beachtet.
0029	Verarbeitungspriorität, Code	C a1	N +		Wird bei der Ausführung nicht beachtet.
0031	Bestätigungsanforderung	C n1	N +		Wird bei der Ausführung nicht beachtet.
0032	Austauschvereinbarungskennung	C an..35	N +		Wird bei der Ausführung nicht beachtet.
0035	Test-Kennzeichen	C n1	O +1'		Verwendung ist optional. Angabe eines Testkennzeichens, wenn erforderlich. Dieses Datenelement sollte nur dann verwendet werden, wenn tatsächlich ein Test vorliegt. In diesem Fall muss es auf „1“ gesetzt werden. Die Übermittlung von Test-Nachrichten sollte dem Empfänger angekündigt und im IA vereinbart werden. Code: 1 Allgemeiner Test

Kommentar:

Dieses Segment dient dazu, eine Übertragungsdatei zu identifizieren.

Codierungsbeispiel:

UNB+UNOB:4+ABSENDER-ID:14+EMPFAENGER-ID:14+20011015:1005+DIN AUT001+++++1'

Segment:

UNHIfd. Nr.: 2
Status: MEbene: 0
Max. Wdh.: 1**Nachrichten-Kopfsegment****Beschreibung: Nachrichten-Kopfsegment****Formale Beschreibung des Segmentes:**

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
UNH 0062	Nachrichten-Kopfsegment Nachrichten-Referenznummer	M M an..14	M M	UNH +AUT000001	Angabe einer eindeutigen Nachrichten-Referenznummer, vergeben vom Sender. Laufende Nummer der Nachrichten im Datenaustausch. Identisch mit der Angabe in UNT_0062. Diese Nummer wird vom Absender vergeben und identifiziert eine Nachricht innerhalb einer Übertragungsdatei eindeutig. Das verwendete Nummernsystem sollte die Erkennung von Doppel- und Fehlübertragungen ermöglichen. Beispiele für mögliche Nummernsysteme, die diese Anforderungen erfüllen. Innerhalb einer Übertragungsdatei werden alle Nachrichten mit „1“ beginnend, lückenlos aufsteigend durchnummeriert.
S009 0065	Nachrichtenennung Nachrichtentyp-Kennung	M M an..6	M M	+AUTACK	Angabe der Nachrichtentyp-Kennung. Code: AUTACK Sicherheits-Authentisierung und -Bestätigungs-Nachricht
0052	Versionsnummer des Nachrichtentyps	M an..3	M	:4	Nummer des Service-Nachrichten-Directory (nicht Nummer eines EDIFACT-Anwendungs-Directory). Code: 4 Service-Nachricht-Version
0054	Freigabenummer des Nachrichtentyps	M an..3	M	:1	Angabe der Freigabenummer im Service-Directory. Code: 1 Erste Ausgabe
0051	Verwaltende Organisation, codiert	M an..3	M	:UN	Angabe der verwaltenden Organisation für diesen Nachrichtentyp. Hier wird der Code der für die Pflege des Nachrichtentyps verantwortlichen Organisation eingetragen. Für Nachrichtentypen mit Status 1 oder 2 der UN ist immer der Wert „UN“ einzutragen. Für Nachrichten, die von anderen Organisationen gepflegt werden, sind die entsprechend der Codeliste zutreffenden Codes einzutragen. Eine andere Organisation ist z. B. ODETTE. Code: UN UN/ECE/TRADE/WP.4
0057	Anwendungscode der Zuständigen Organisation	C an..6	O	:EAN002'	Verwendung ist optional. Versionsangabe für die Anwendungs-Empfehlung. Code, der von einer Organisation vergeben wurde, zur Definition einer besonderen Ausprägung des Einheitlichen Nachrichtentyps (Subset). Dieses DE Datenelement muss verwendet werden, falls ein Subset zur Anwendung kommt. Liegt kein Subset vor, wird dieses Feld nicht benutzt. Folgende Codierungen werden empfohlen: Code: EAN002 EAN Versionsnummer Code: ZKA02 ZKA Versionsnummer

Kommentar:

Mit diesem Segment beginnt die Nachricht. Das Segment enthält die eindeutige Identifizierung der Nachricht.

Codierungsbeispiel:

UNH+AUT000001+AUTACK:4:1:UN:EAN002'

Gruppe: **SG1** Status: M Max. Wdh.: 99 USH-USA-SG2
 Diese Gruppe von Segmenten dient zur Identifizierung der angewendeten Sicherheitsdienste und Sicherheitsmechanismen. Darüber hinaus enthält sie die für die Durchführung der Prüfberechnungen notwendigen Daten.

Segment: **USH** lfd. Nr.: 3 Ebene: 1 **Sicherheits-Kopfsegment**
 Status: M Max. Wdh.: 1

Beschreibung: Sicherheits-Kopfsegment

Formale Beschreibung des Segmentes:

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
USH 0501	Sicherheits-Kopfsegment Sicherheitsdienst, codiert	M M an..3	M	USH +7	Angabe der Nachrichtenfunktion/ Sicherheitsdienstes. Code: 7 Unbestreitbarkeit des Ursprungs der (in dieser Nachricht) referenzierten EDIFACT-Struktur
0534	Sicherheits-Referenznummer	M an..14	M	+1	Nummer, die vom Sicherheitsurheber zur eindeutigen Referenzierung des Paares von Sicherheitskopf- und Sicherheitsende- Segmentgruppen (USH_0534 und UST_0534) und des Prüfwerts in USY_0534 zugeordnet wurde.
0541	Umfang der Sicherheitsanwendung, codiert	C an..3	R	+3	Angabe des Datenumfangs, der vom zugehörigen Signierungsprozess berücksichtigt wird. Siehe hierzu auch Segment USX. Code: 3 Ganze zugehörige Nachricht, Gruppe oder Übertragungsdatei
0503	Antwortart, codiert	C an..3	O	+1	Code: 6 Vom ersten Nachrichten- Kopfsegment bis zum letzten Nachrichten-Endesegment Verwendung ist optional. Angabe, ob eine Bestätigung gewünscht wird. Ob und welche Art von Bestätigungsnachrichten verwendet wird, ist in entsprechenden Vereinbarungen zu regeln. Anmerkung: Bestätigungen können erzeugt werden vom Konverter (Empfang der Übertragungsdatei) mit der EDIFACT-Nachricht CONTRL, vom Sicherheitsmodul (Sicherheitsbestätigung) mit der EDIFACT- Nachricht AUTACK oder von der entsprechenden Anwendung (Anwendungsbestätigung) mit der EDIFACT-Nachricht APERAK.
0505	Filterfunktion, codiert	C an..3	R	+2	Code: 1 Keine Bestätigung gefordert Angabe der Filter-Funktion für binäre Felder im Segment USA. Hinweis: Diese Angabe beschreibt, wie die binäre Information, z. B. die digitale Unterschrift in einem „lesbaren Format“, dargestellt werden kann. Z. B. könnte der Binäre Wert „01111111 00111011“ (der möglicherweise „keine lesbare“ Darstellung besitzt) mit der hexadezimalen Filterfunktion zu hexadezimal „7F 3B“ codiert werden. Code: 2 Hexadezimaler Filter

EDIFACT AUTACK					Beschreibung
BEZ	Beschreibung	S Format	S	Beispiel	Datenelement-Inhalte
0507	Originale Zeichensatzcodierung, codiert	C an..3	R	+1	Angabe des Zeichensatzes, in dem die ursprüngliche Nachricht vorlag, bevor die Unterschrift erzeugt wurde. Code: 1 ASCII 7 bit Code: 2 ASCII 8 bit Code: 3 Code Tabelle 850 (IBM PC Multinational) Code: 4 Code Tabelle 500 (EBCDIC Multinational No. 5)
0509	Rolle des Sicherheitsanbieters, codiert	C an..3	N	+	Wird bei der Ausführung nicht beachtet.
S500	Sicherheitsidentifikation	C	N		Wird bei der Ausführung nicht beachtet.
0577	Sicherheitsbeteiligter, Qualifier	M an..3	M	+	Wird bei der Ausführung nicht beachtet.
0520	Sicherheits-Folgenummer	C an..35	N	+	Wird bei der Ausführung nicht beachtet.
S501	Sicherheit, Datum und Uhrzeit	C	R		
0517	Datum und Uhrzeit, Qualifier	M an..3	R	+1	Datum und Uhrzeit der Willenserklärung, die durch die Signatur bestätigt wird. Code: 1 Sicherheits-Zeitstempel
0338	Datum des Ereignis	C n..8	R	:20011017	Datumsformat JJJJMMTT.
0314	Uhrzeit des Ereignis	C an..15	R	:110522	Zeitformat HHMMSS.
0336	Zeitversatz	C n4	O	:0100'	Verwendung ist optional. Angabe der Zeitdifferenz gegenüber GMT. Hinweis: Das Format ist HHMM und muss bei negativer Zeitdifferenz mit einem vorangestellten Minuszeichen dargestellt werden.

Kommentar:

Dieses Segment dient zur Angabe eines Sicherheitsdienstes, der auf eine Übertragungsdatei, eine Nachrichtengruppe oder eine Nachricht angewendet wurde.

Codierungsbeispiel:

USH+7+1+3+1+2+1++++1:20011017:110522:0100'