

Anwendungsregeln

Teil 16: Anwendung des Service-Nachrichtentyps KEYMAN zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten

DIN**16560-16**

ICS 35.240.60

EDIFACT — Implementation guide — Part 16: Use of the service message type KEYMAN for conveying security keys and certificates

EDIFACT — Guide d'implémentation — Partie 16: Utilisation du type de message de service KEYMAN pour transmettre les clés et certificats de sécurité

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 KEYMAN „Sicherheitsschlüssel- und -Zertifikats-Verwaltung“ nach ISO 9735-9:2002.

Die Norm ist – soweit notwendig – mit der Norm DIN 16560-15 harmonisiert, die die Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen zu versendeten Nutzdaten beschreibt.

DIN 16560 *EDIFACT — Anwendungsregeln* besteht aus:

- Teil 1: *Service-Segmente*
- Teil 2: *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 16

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 des Nachrichtentyps KEYMAN erfüllt die aktuellen Anforderungen des Geschäftsdatenaustausches im e-Business.

Die in dieser Norm beschriebene Anwendung des Nachrichtentyps KEYMAN 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 „KEYMAN-Guide“ beschreibt

die Verwaltung von Sicherheitsschlüsseln und -zertifikaten.

Die parallel zu dieser Norm veröffentlichte DIN 16560-15 beschreibt zusätzlich die

Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten.

Da der Nachrichtentyp KEYMAN 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 KEYMAN. 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 KEYMAN nach ISO 9735-9 zur Übermittlung von Sicherheitsschlüsseln und -zertifikaten 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 16560-15:2003, *EDIFACT — Anwendungsregeln — Teil 15: Anwendung des Service-Nachrichtentyps AUTACK zur Übermittlung von Integritäts- und Authentizitätsinformationen über versendete Nutzdaten*.

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 9735-5:2002, *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 9735-9:2002, *Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, syntax release number: 1) — Part 9: Security key and certificate management message (message type – KEYMAN)*.

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 EDI-FACT-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 ein vorangestelltes „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 EDIFACT-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.

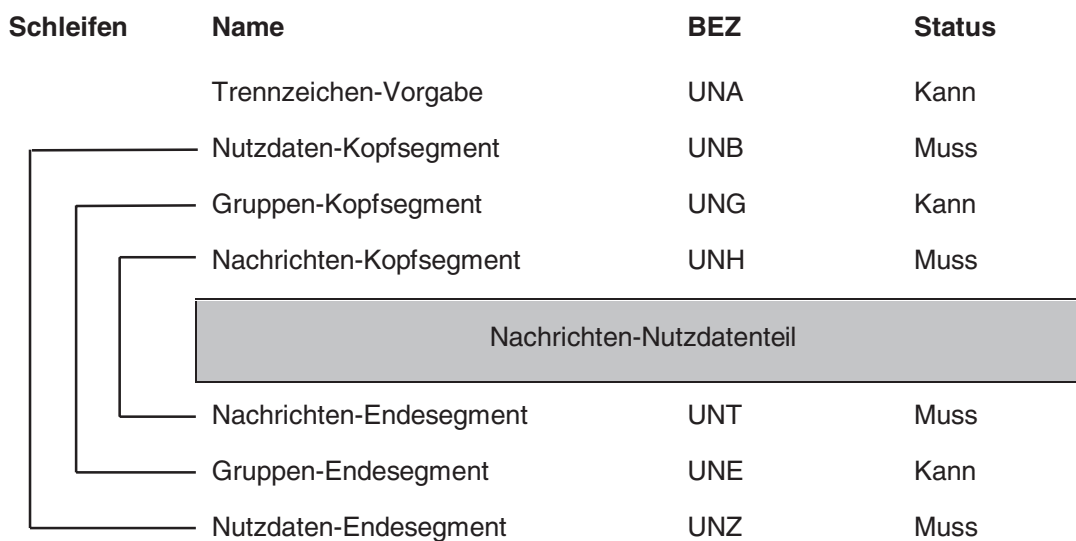


Bild 1 — Struktur einer EDIFACT-Übertragungsdatei

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.