

DIN ISO 9735-9

ICS 35.240.60

**Elektronischer Datenaustausch für Verwaltung, Wirtschaft und Transport (EDIFACT) –
Syntax-Regeln auf Anwendungsebene (Syntax-Versionsnummer: 4,
Syntax-Releasenummer: 1) –
Teil 9: Sicherheitsschlüssel- und Zertifikats-Verwaltung
(Nachrichtentyp – KEYMAN) (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)
(ISO 9735-9:2002)

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 9: Clé de sécurité et message de gestion de certificat (type de message –
KEYMAN) (ISO 9735-9:2002)

Gesamtumfang 28 Seiten

Normenausschuss Bürowesen (NBü) im DIN

Die Internationale Norm 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)“ 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 9735-9:2002, 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 9: Sicherheitsschlüssel- und Zertifikats-Verwaltung (Nachrichtentyp – KEYMAN) (ISO 9735-9:2002)

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 Sicherheitsschlüssel- und Zertifikats-Verwaltungs-Nachricht	7
Anhang A (informativ) KEYMAN-Funktionen	12
Anhang B (informativ) Sicherheitstechniken, die auf KEYMAN-Nachrichten anzuwenden sind	16
Anhang C (informativ) Verwendung von Segmentgruppen in KEYMAN-Nachrichten	17
Anhang D (informativ) Ein Modell für die Schlüsselverwaltung	19
Anhang E (informativ) Beispiele für KEYMAN-Nachrichten	22

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 9735-9 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 9735-9:1999). 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 9735-9 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 Verwaltung von Sicherheits-schlüsseln und Zertifikaten.

1 Anwendungsbereich

Dieser Teil der ISO 9735 für die Sicherheit bei Batch-EDIFACT definiert die Nachricht zur Sicherheits-schlüssel- und Zertifikats-Verwaltung KEYMAN.

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 Sicherheitsschlüssel- und Zertifikats-Verwaltungs-Nachricht

5.1 Funktionsbeschreibung

Die KEYMAN ist eine Nachricht zur Verwaltung von Sicherheitsschlüsseln und -Zertifikaten. Ein Schlüssel kann ein mit symmetrischen Algorithmen verwendeter Sicherheitsschlüssel oder ein mit asymmetrischen Algorithmen verwendeter öffentlicher bzw. privater Schlüssel sein.

5.2 Anwendungsbereich

Die Sicherheitsschlüssel- und Zertifikats-Verwaltungs-Nachricht (KEYMAN) 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

Die Nachricht darf verwendet werden, um Sicherheitsschlüssel, Zertifikate oder Zertifikationspfade (dies beinhaltet die Anfrage nach weiteren Schlüssel- und Zertifikats-Verwaltungs-Aktionen, wie beispielsweise die Erneuerung, der Austausch oder die Widerrufung von Zertifikaten, sowie die Lieferung weiterer Informationen, wie beispielsweise den Zertifikatsstatus) anzufragen bzw. zu liefern. Sie kann darüber hinaus Zertifikatslisten (beispielsweise zur Anzeige der aufgehobenen Zertifikate) bereitstellen. Die KEYMAN-Nachricht kann durch die Verwendung von Sicherheitskopf- und Sicherheitsende-Segmentgruppen gesichert werden. Die Strukturen dieser Segmentgruppen sind in ISO 9735-5 definiert.

Eine Sicherheitsschlüssel- und -Zertifikats-Verwaltungs-Nachricht kann verwendet werden zur:

- a) Anfrage von Aktionen in Bezug auf Schlüssel und Zertifikate;
- b) Auslieferung von Schlüsseln, Zertifikaten und entsprechender Informationen.

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 Sicherheitsschlüssel- und Zertifikats-Verwaltungs-Nachricht ist KEYMAN.

Nachrichten des Typs „Sicherheitsschlüssel- und Zertifikats-Verwaltung“, die mit dieser Norm übereinstimmen, müssen die folgenden Daten im Segment UNH, Datenelementgruppe S009, enthalten:

Datenelement 0065	KEYMAN
0052	4
0054	1
0051	UN

0020 Segmentgruppe 1: USE-USX-SG2

Eine Gruppe von Segmenten, die alle notwendigen Informationen zur Übermittlung von Schlüsseln, Zertifikaten oder Zertifizierungspfaden zwecks Verwaltung von Anfragen, Auslieferung oder Benachrichtigungen enthält.

0030 USE, Sicherheitsnachricht-Bezug

Ein Segment zur Angabe einer Beziehung zu einer vorangegangenen Nachricht wie beispielsweise eine KEYMAN-Anfrage.

0040 USX, Sicherheits-Referenzen

Ein Segment zur Angabe einer Verbindung zu einer vorangegangenen Nachricht wie beispielsweise eine Anfrage. Die Datenelementgruppe „Sicherheitsdatum und -uhrzeit“ kann das ursprüngliche Datum und die Uhrzeit der Erstellung der referenzierten EDIFACT-Nachricht enthalten.

0050 Segmentgruppe 2: USF-USA-SG3

Eine Gruppe von Segmenten, die einen einzelnen Schlüssel, ein einzelnes Zertifikat oder eine Sammlung von Zertifikaten, die einen Zertifizierungspfad bilden, enthält.

0060 USF, Schlüsselverwaltungs-Funktion

Ein Segment zur Angabe der Funktion der Gruppe, welche es triggert. Dies kann entweder eine Anfrage oder eine Auslieferung sein. Wenn die Gruppe zur Anzeige von Elementen des Zertifizierungspfades verwendet wird, muss die Zertifikats-Folgenummer die Position des folgenden Zertifikats innerhalb des Zertifizierungspfades anzeigen. Das Segment kann selbst dazu verwendet werden, um eine Liste ohne vorliegendes Zertifikat wiederherzustellen. Wenn mehr als ein Schlüssel oder ein Zertifikat verwaltet werden soll, kann es mehrere verschiedene Segmente USF innerhalb der gleichen Nachricht geben. Eine Mischung aus Anfragefunktionen und Auslieferungsfunktionen darf aber nicht auftreten. Das Segment USF kann darüber hinaus die für die Binärfelder des folgenden Segmentes USA verwendete Filterfunktion festlegen.

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). Dieses Segment muss für die Anfrage, die Einstellung oder die Auslieferung von symmetrischen Schlüsseln verwendet werden. Es darf auch verwendet werden, wenn ein asymmetrisches Schlüsselpaar angefordert wird.

0080 Segmentgruppe 3: USC-USA-USR

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). Diese Gruppe muss bei Anfragen oder Auslieferungen von Schlüsseln und Zertifikaten verwendet werden.

Im Segment USC sind entweder die komplette Zertifikat-Segmentgruppe (einschließlich des Segments USR) oder nur die für die eindeutige Identifizierung des verwendeten asymmetrischen Schlüsselpaares notwendigen Datenelemente enthalten. Die Präsenz eines kompletten Zertifikats kann vermieden werden, wenn das Zertifikat bereits zwischen den beiden Beteiligten ausgetauscht worden ist oder wenn es aus einer Datenbank erhalten werden kann.

Wenn der Wunsch besteht, auf ein nicht-EDIFACT-Zertifikat zu verweisen (wie beispielsweise bei X.509), müssen die Zertifikats-Syntax und -Version im Datenelement 0545 des Segmentes USC identifiziert werden. Derartige Zertifikate können in einem EDIFACT-Paket befördert werden.

0090 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). Dieses Segment muss für Zertifikatsanfragen wie beispielsweise die Erneuerung, oder für Anfragen nach asymmetrischen Schlüssel wie beispielsweise eine Einstellung und für Zertifikatsauslieferungen verwendet werden.

0100 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). Dieses Segment muss für Zertifikatsanfragen, wie beispielsweise eine Beglaubigungs-Registrierung, und für Zertifikatsauslieferungen verwendet werden.

0110 USR, Sicherheitsergebnis

Ein Segment, das das Ergebnis der Sicherheitsfunktionen enthält, die auf das Zertifikat von der Zertifizierungsinstanz angewendet wurde (wie in ISO 9735-5 definiert). Dieses Segment muss für die Zertifikatsprüfung oder Zertifikatsauslieferung verwendet werden.

0120 Segmentgruppe 4: USL-SG5

Eine Gruppe von Segmenten mit Listen von Zertifikaten oder öffentlichen Schlüsseln. Die Gruppe wird zur Gruppierung von Zertifikaten ähnlicher Status verwendet, d. h. die noch gültig sind oder die aus einem bestimmten Grund ungültig sein können.