

DIN EN 17367

ICS 13.030.40

Einsprüche bis 2019-05-15

Entwurf

**Abfallwirtschaft –
Datenkommunikation zwischen dem Kommunikationsmanagementsystem
und dem nachgeordneten Verwaltungssystem für Stationärcontainer;
Deutsche und Englische Fassung prEN 17367:2019**

Waste Management –

Data communication between communication management system and the back office system
for stationary containers;

German and English version prEN 17367:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-03-15 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs
besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nkt@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Kommunale Technik (NKT), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 44 Seiten

DIN-Normenausschuss Kommunale Technik (NKT)

Nationales Vorwort

Dieses Dokument (prEN 17367:2019) wurde vom Technischen Komitee CEN/TC 183 „Abfallwirtschaft“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Für die deutsche Mitarbeit ist der Arbeitsausschuss NA 051-05-01 AA „Identifizieren und Wägen (Spiegelgremium für CEN/TC 183/WG 3)“ im DIN-Normenausschuss Kommunale Technik (NKT) verantwortlich.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 8601 siehe DIN ISO 8601

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO 8601, *Datenelemente und Austauschformate — Informationsaustausch — Darstellung von Datum und Uhrzeit*

Abfallwirtschaft — Datenkommunikation zwischen dem Kommunikationsmanagementsystem und dem nachgeordneten Verwaltungssystem für Stationärcontainer

*Waste Management — Data communication between communication management system and the back office
system for stationary containers*

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: CEN-Umfrage
Dokument-Sprache: D

STD Version 2.9p

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Domain Model	8
4.1 Allgemeines	8
4.2 Übersicht über die Systeme	8
4.3 Aktivitätsdiagramme	8
5 Kommunikationsprotokoll	9
5.1 Allgemeines	9
5.2 Definitionen (MUSS)	9
5.2.1 Die Kommunikation erfolgt über RESTful Web-Services	9
5.2.2 Der Transport wird durch SSL sichergestellt	10
5.2.3 Die Authentifizierung erfolgt über einen geheimen API-Schlüssel und HMAC	10
5.2.4 API-Versionierung	10
5.3 Konventionen (MUSS)	10
5.3.1 Das Standarddatenformat ist JSON	10
5.3.2 Datum und Uhrzeit befolgen ISO 8601	10
5.3.3 HTTP-Verbs	10
5.3.4 HTTP-Statuscodes	11
5.3.5 Big Endian für Hex-Werte	11
5.4 Empfehlungen (SOLLTE)	11
5.4.1 XML-Daten sollten unterstützt werden	11
5.4.2 Ratenbegrenzung	11
6 Schnittstellendokumentation	12
Anhang A (normativ) HMAC-Authentifizierung	16
A.1 Was ist HMAC-Authentifizierung?	16
A.2 Verwendungsfluss für API-Schlüssel — HMAC-Authentifizierung:	16
A.2.1 Allgemeines	16
A.2.2 Fluss auf Client-Seite:	16
A.2.3 Fluss auf Server-Seite:	17
A.2.4 Wichtige Anmerkung:	17
A.2.5 Verweis:	17
Anhang B (normativ) Code-Listen	18
B.1 Allgemeines	18
B.2 Lieferanten-Code	18
B.3 Transaktionsarten	18
B.4 Arten von Zugangschips	19
B.5 Auslösecodes	19
B.6 Messcodes	20
B.7 Fehlfunktionscodes	20
B.8 Systeminformationscodes	21
B.9 Einstellungscodes	21

B.10	Maßnahmengcodes	21
B.11	Öffnungszustandcodes	21
	Literaturhinweise.....	22

Europäisches Vorwort

Dieses Dokument (prEN 17367:2019) wurde vom Technischen Komitee CEN/TC 183 „Abfallwirtschaft“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Einleitung

Die Abfallverarbeitungsbranche hat bereits seit einigen Jahren digitale Informationen ausgetauscht. Außerdem hat die Verwendung von Chips zur Erkennung von Zugangschips und Behältern ebenfalls Tradition in dieser Branche. Die Abfallverarbeitungsunternehmen erfahren die Vorteile von elektronischem Informationsaustausch und der Erkennung von Behältern und Zugangschips, allerdings auch, dass der elektronische Informationsaustausch oder die Erkennung von Behältern und Zugangschips auf Grundlage verschiedener Spezifikationen nicht optimal ist: Es erfordert einiges an Arbeit, Zeit und Geld, um Informationen mit anderen auszutauschen oder von ihnen zu erhalten.

Um die aktuelle Situation dahingehend flexibler zu gestalten, dass die Identifikation von Karten und Containern mit verschiedenen Systemen und Anbietern verwendet werden können, und um den Informationsaustausch zwischen verschiedenen Systemen zu ermöglichen, ist es notwendig, Normen zu festzulegen. Mit diesen Normen kann Interoperabilität in der Branche hergestellt werden, was den Zusammenschluss von Systemen erleichtert und ein besseres Zusammenwirken zwischen verschiedenen Systemen ermöglicht. Im Hinblick auf Marktzugang für Käufer und Endkunden zielt diese Norm darauf ab, den Markt dank der Kompatibilität zwischen Zugangskontrollserver und der Management-Software Dritter zu öffnen.

1 Anwendungsbereich

Dieses Dokument legt die Norm zur Implementierung einer Standard-Lieferanten-Schnittstelle fest, die auf den Austausch von stationärer Abfallsammelbehälterinformation und -konfiguration ausgelegt ist.

Dieses Dokument definiert die Art des Datenaustauschs zwischen „Kommunikations-Managementsystemen“ und „Hintergrundsystemen“.

Der Datenaustausch zwischen „Sammelbehältersystemen“ und „Kommunikations-Managementsystemen“ oder „Hintergrundsystemen“ bleibt ausgenommen.

Dieses Dokument zielt auf zwei Informationsflüsse in der Abfallverarbeitungsbranche ab:

- die Verarbeitung von Informationen zur Abfalllagerung, zwischen Kommunikations-Managementsystemen und den Hintergrundsystemen;
- die Verarbeitung von Konfigurationsinformationen zwischen den Hintergrundsystemen und Kommunikations-Managementsystemen.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

Kommunikations-Managementsystem CMS

(en: Communication Management System)

Anwendung, die sich an Regeleinrichtung, Tiefensensor oder allgemein an ein in einem Behälter angebrachtes elektronisches Registrierungsgerät anschließen lässt

3.2

Hintergrundsystem BOS

(en: Back-Office System)

Anwendung(en) zur Verwaltung von Autorisierung, Registrierung und Rechnungsstellung von Abfalllagerung usw. durch den Kunden

3.3

Lesegerät

auf einem Sammelbehälter platziertes Gerät, das zum Lesen der auf einem Chip enthaltenen Informationen befähigt ist

3.4

Regeleinrichtung

zur Interaktion mit einem Lesegerät sowie zur Übertragung der Information von einem Chip auf wiederverwendbare Informationen befähigtes Gerät

3.5

Chip

Datenträger, der von einem Lesegerät erkannt werden kann

3.6

Zugangschip (z. B. Karte oder Marke)

Gerät (beispielsweise eine Kreditkarte), das in der Lage ist, einen Chip zu tragen. Marken oder jede andere Art, einen Anwender für die Zugangskontrolle zu identifizieren, werden ebenfalls angepasst

3.7

Sammelbehälter

Behälter, der Abfall für mehr als einen Haushalt oder ein Gebäude aufbewahren kann

3.8

Sammelbehältersystem

Behälter, der Abfall für mehr als einen Haushalt oder ein Gebäude aufbewahren kann, einschließlich der gesamten Elektronik zur Verwaltung des Systems

3.9

schwarze Liste

Autorisierungsliste mit Identifikationsnummern, die beim Lesen vom System nach Anwendung des Registers abgelehnt werden sollten

3.10

weiße Liste

Autorisierungsliste mit Identifikationsnummern, die beim Lesen vom System nach Anwendung des Registers verarbeitet werden sollten

3.11

Autorisierungsliste

Register mit Identifikationsnummern, die vom System nach Anwendung des Registers abgelehnt oder verarbeitet werden sollten

3.12

Management- und Konfigurationssystem

vom Lieferant bereitgestelltes System zur Verwaltung und Konfiguration des Sammelbehältersystems oder des Systems

3.13

Abfallverarbeitungs-Hintergrundsystem

Systeme, die die Abfallverarbeitungsunternehmen verwenden, um die Sammlung von Abfall, Behältern und andere relevante interne Prozesse zu verwalten

4 Domain Model

4.1 Allgemeines

Dieses Kapitel beschreibt die Modelle, auf denen die Norm aufbaut. Übersicht über die Systeme und Aktivitätsdiagramme.

4.2 Übersicht über die Systeme

Bild 1 zeigt den Kontext, in dem die Standardschnittstelle nützlich ist.

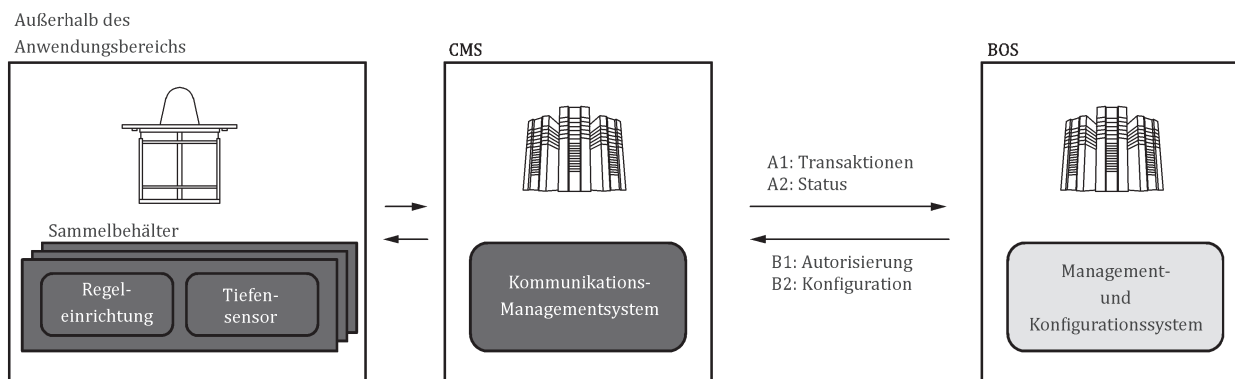


Bild 1 — Übersicht über die Systeme

4.3 Aktivitätsdiagramme

Bilder 2 und 3 zeigen die Aktivitätsdiagramme, die die Prozesse definieren, bei denen die Norm Anwendung findet.

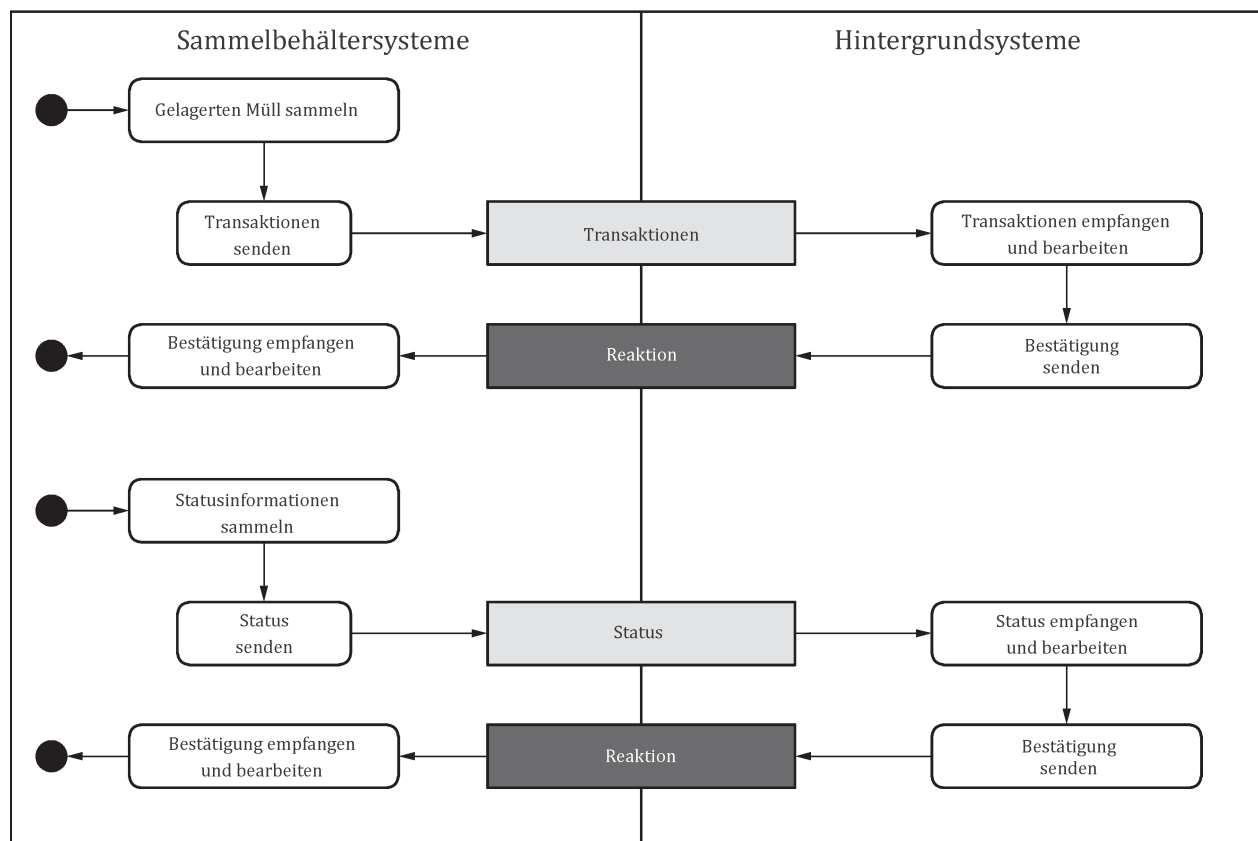


Bild 2 — Aktivitäten von CMS bis BOS

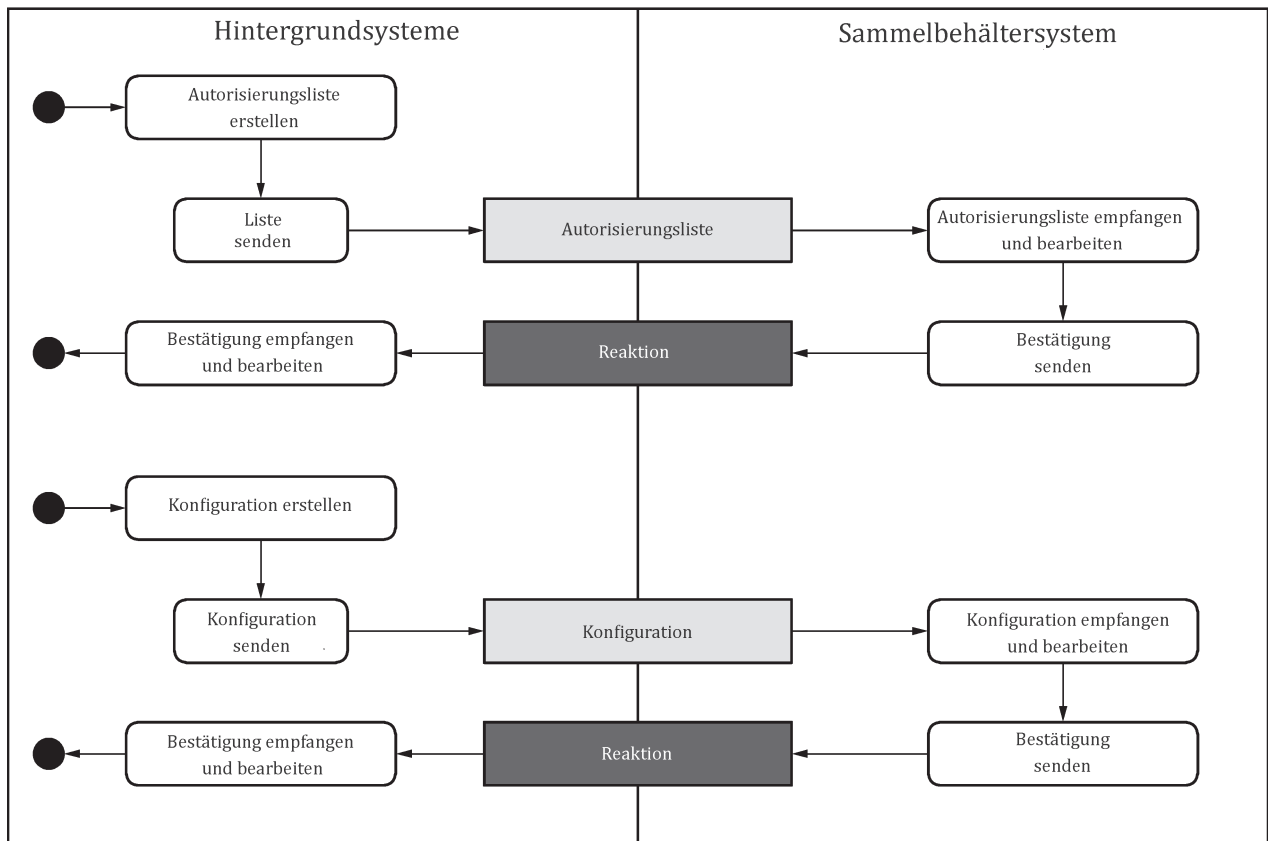


Bild 3 — Aktivitäten von BOS bis CMS

5 Kommunikationsprotokoll

5.1 Allgemeines

Dieser Abschnitt beschreibt die Standardregeln für die Implementierung des Kommunikationsprotokolls.

Um die Norm einzuhalten, müssen alle Definitionen vom Protokoll implementiert und unterstützt werden.

Andere Normen und Festlegungen müssen berücksichtigt werden, wenn sie in diesem Dokument Erwähnung finden.

Empfehlungen sollten durch die Implementierung des Protokolls unterstützt werden.

5.2 Definitionen (MUSS)

5.2.1 Die Kommunikation erfolgt über RESTful Web-Services

RESTful Web-Services sind der Industriestandard zum Erstellen effizienter Schnittstellen zwischen verteilten Systemen. Es gibt eine große Anzahl an Ressourcen, um die Entwickler in nahezu jeder verfügbaren Programmiersprache zu unterstützen.

5.2.2 Der Transport wird durch SSL sichergestellt

Immer SSL verwenden. Ohne Ausnahme. Heute kann von überall aus auf Ihre Web-APIs zugegriffen werden, wo es Internet gibt (wie u. a. Büchereien, Cafés, Flughäfen). Nicht alle davon sind sicher. Viele verschlüsseln ihre Kommunikation überhaupt nicht, was müheloses Eavesdropping oder Identitätsbetrug ermöglicht, wenn Authentifizierungsinformationen entwendet werden.

Ein weiterer Vorteil der ausnahmslosen Verwendung von SSL liegt darin, dass die garantiert verschlüsselte Kommunikation Authentifizierungsversuche vereinfacht. Sie benötigen nur einfache Zugriffstoken, anstatt jedes Mal eine API-Anforderung auszustellen.

Bei Nicht-SSL-Zugriff auf API-URLs ist Vorsicht geboten. Diese nicht an ihre SSL-Entsprechungen weiterleiten. Geben Sie stattdessen einen Hard Error aus! Sie können es sich nicht leisten, schlecht konfigurierte Clients, die Anfragen an einen unverschlüsselten Endpunkt verschicken, zum tatsächlichen, verschlüsselten Endpunkt durchzuwinken.

5.2.3 Die Authentifizierung erfolgt über einen geheimen API-Schlüssel und HMAC

Dabei handelt es sich um einen Mechanismus zur Berechnung eines Nachrichtenauthentifizierungscodes mittels einer Hash-Funktion in Verbindung mit einem von beiden am Senden und Empfangen der Daten beteiligten Parteien gemeinsam benutzten Geheimschlüssel (Client Front-End und http-Service Back-End). Die Hauptanwendung für HMAC zur Verifizierung von Integrität, Authentizität und Identität des Versenders der Nachricht.

Siehe Anhang A.

5.2.4 API-Versionierung

Die Versionierung muss in der URL erfolgen, um die Browser-Funktionsfähigkeit der Ressourcen versionsübergreifend sicherzustellen. Zum Beispiel:

- `"/store/api/v1"`
- `"/store/api/v2"`

5.3 Konventionen (MUSS)

5.3.1 Das Standarddatenformat ist JSON

Um Mehraufwand zu minimieren, werden in RESTful Web-Services gewöhnlich Daten vom Typ JSON verwendet. Allerdings unterstützen die meisten Implementierungen beide Datenformate. Der Datentyp im Body (JSON oder XML) MUSS im Header der Anfrage mit Hilfe des Tags „Content-Type“ spezifiziert werden.

5.3.2 Datum und Uhrzeit befolgen ISO 8601

Das geläufige Datumsformat lautet „**YYYY-MM-DDTHH:mm:ssZ**“

Das geläufige Zeitformat lautet „**HH:mm:ssZ**“

5.3.3 HTTP-Verbs

Da die Norm nur PUSH-Verhalten festlegt, ist das einzige akzeptierte HTTP-Verb **POST**.

5.3.4 HTTP-Statuscodes

Es MUSS der Standard-HTTP-Statuscode verwendet werden. Insbesondere:

- **200 — OK:** Die Anfrage war erfolgreich.
- **400 — Ungültige Anforderung:** Die Anfrage konnte aufgrund nicht wohlgeformter Syntax vom Server nicht verarbeitet werden. Der Client SOLLTE die Anfrage NICHT ohne Modifikationen wiederholen.
- **401 — Nicht autorisiert:** Wenn keine oder ungültige Authentifizierungsinformationen eingegeben werden.
- **500 — Interner Serverfehler:** Der Server ist auf ein unerwartetes Problem gestoßen und kann daher die Anfrage nicht bearbeiten.
- **501 — Nicht implementiert:** Der Server unterstützt die zum Bearbeiten der Anfrage erforderliche Funktion nicht. Dies ist die passende Meldung, wenn der Server die Anfragemethode nicht erkennt und für keine Ressource unterstützen kann.

5.3.5 Big Endian für Hex-Werte

Alle Identifikationschipnummern MÜSSEN im „Big Endian“-Format (MSB) versendet werden.

5.4 Empfehlungen (SOLLTE)

5.4.1 XML-Daten sollten unterstützt werden

Um Mehraufwand zu minimieren, werden in RESTful Web-Services gewöhnlich Daten vom Typ JSON verwendet. Wenn jedoch vom Kunden das XML-Format erwünscht wird, sollte dies mit Hilfe des Tags „Content-Type“ im Header möglich sein.

5.4.2 Ratenbegrenzung

Die zurückgegebenen HTTP-Header jeder API-Anfrage geben Ihren aktuellen Ratenbegrenzungsstatus wie in Tabelle 1 an.

Tabelle 1 — Ratenbegrenzungsstatus

Name des Headers	Beschreibung
X-RateLimit-Limit	Die maximale Anzahl der innerhalb einer Stunde erlaubten Anfragen.
X-RateLimit-Remaining	Die Anzahl an Anfragen, die im aktuellen Ratenbegrenzungsrahmen bleiben.
X-RateLimit-Reset	Der Zeitpunkt, zu dem der aktuelle Ratenbegrenzungsrahmen zurückgestellt wird. ISO 8601 Datums- und Zeitformat: YYYY-MM-DDThh:mm:ssTZD.

6 Schnittstellendokumentation

Die API für diese Norm wird in der folgenden RAML-Definition festgelegt:

Zugangschip

```
#%RAML 1.0 DataType
type: "object"
displayName: "AccessChip"
properties:
  UID:
    type: "string"
    required: true
    description: |
      The unique number assigned to the chip by the manufacturer of the card. The uniqueness of this
      number is guaranteed by the ISO/IEC 14443 series that defines the (information on the) chips. The
      number shall follow the Big-endian or MSB format.
    minLength: 8
    maxLength: 14
    pattern: "Hexadecimal"
  CardType:
    type: "string"
    required: true
    description: |
      Type of the access chip used from a list of predefined values:

      x-chip-register — Registration (access chip that can be used to make deposits)
      x-chip-service — Service (not counted in maximum container opening count)
      x-chip-empty — Emptying (not counted in maximum container opening count)
      x-chip-call-outbound — Outbound call (container calls VCMS)
      x-chip-call-inbound — Inbound call (container waits for contact from the communication
      management system)
      x-chip-reset — Reset (warm-boot)
      x-chip-reset-battery — Reset battery counter
      x-chip-test-lock — Lock test (this access chip only test the lock, not counted in maximum container
      opening count)
      x-chip-show-opening-count — Show current opening count
      x-chip-show-signal — Show GPRS signal level
    enum: ["x-chip-register", "x-chip-reset", "..."]
```