SLOVENSKI STANDARD
oSIST prEN 17367:2019

01-maj-2019

Ravnanje z odpadki - Podatkovne komunikacije med komunikacijskim sistemom upravljanja in zalednim sistemom za nepremične posode

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

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

Ta slovenski standard je istoveten z: **prEN 17367**

ICS:

13.030.40	Naprave in oprema za odstranjevanje in obdelavo odpadkov	Installations and equipment for waste disposal and treatment
35.240.99	Uporabniške rešitve IT na drugih področjih	IT applications in other fields

oSIST prEN 17367:2019 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 17367

March 2019

ICS 13.030.40

English Version

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

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

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 183.

If this draft becomes a European Standard, CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (prEN 17367:2019) has been prepared by Technical Committee CEN/TC 183 “Waste management”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

Introduction

The waste processing industry has been exchanging digital information for quite some years now. Besides, the use of chips to recognize access chips and containers also has a history in this industry. The waste processing companies are experiencing the advantages of exchanging information electronically and recognizing containers and access chips, but are also experiencing that exchanging information, or recognizing containers and access chips based on different specifications is not optimal: it requires quite some work, time and money to exchange or receive information from other parties.

To change the current situation to a flexible situation in which the identification of cards and containers can be used with different systems and different suppliers, and to make it possible to exchange information between the different systems it is necessary to define standards. With these standards interoperability in the industry can be achieved, leading to easier coupling of systems and increased interoperability between different systems. In terms of market access for buyers and final customers, this standard is aimed to open the market thanks to the compatibility between the access control server and the third-party management software.

1 Scope

This document defines the standard for implementing a standard inter-vendors interface aimed at exchanging stationary waste container information and configuration.

This document defines the way to exchange data between the “Communication Management Systems” and the “Back-Office Systems”.

The exchange of data between the “Collection Container Systems” and the “Communication Management Systems” or the “Back-Office Systems” is excluded.

This document targets two streams of information in the waste processing industry:

— The processing of information from the deposit of waste, between communication management systems and the back office systems.

— The processing of configuration information, between the back-office systems and the communication management systems.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
Communication Management System
CMS
application that connects to the controller, depth sensor or in general, an electronic registration device installed in a container

3.2
Back-Office System
BOS
application(s) that the customer uses to manage authorization, registration and invoicing of waste deposits, etc.

3.3
reader
device, placed on a collection container, capable of reading the information contained on a chip

3.4
controller
device capable of interaction with a reader and transferring the information from a chip to reusable information

3.5
chip
device carrying data, which can be recognized by a reading device

3.6
access chip (e.g. Card or Tag)
device (like a credit card) capable of carrying a chip. Also assimilated are the Tags or any other way of identifying a user for the access control

3.7
collection container
reservoir capable of containing waste for more than one household or building

3.8
collection container system
reservoir capable of containing waste for more than one household or building together with all its electronics to manage the system

3.9
black list
authorization list that contains identification numbers that when read should be refused by the system using the register

3.10
white list
authorization list that contains identification numbers that when read should be handled by the system using the register

3.11
authorisation list
register containing identification numbers that should be refused or handled by the system using the register

3.12
management and configuration system
system provided by the supplier of a system to manage and configure the collection container system or the system

3.13
waste processing back office
systems that the waste processing companies use to manage the collection of waste, containers and all other relevant internal processes

4 Domain Model

4.1 General

This chapter describes the models on which the standard is based. Overview of the systems and activity diagrams.

4.2 Overview of the systems

Figure 1 exposes the context in which the standard interface is useful.

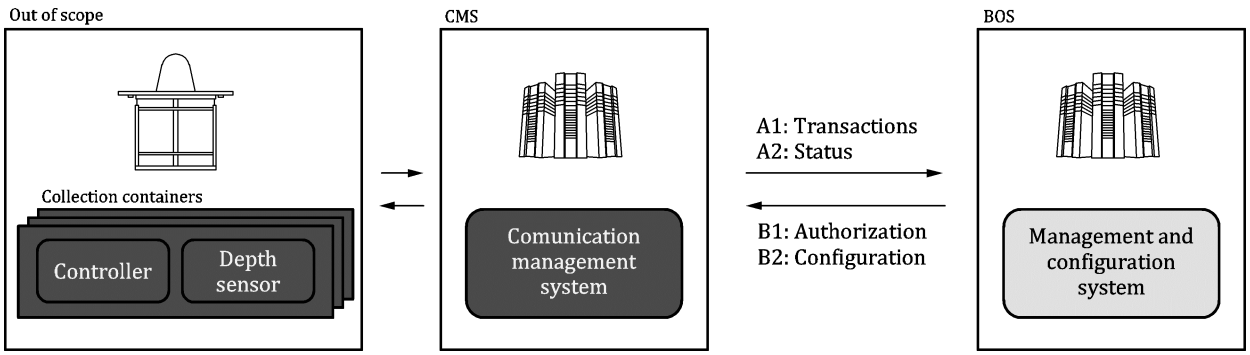

Figure 1 — Overview of the systems

4.3 Activity diagrams

Figures 2 and 3 shows the activity diagrams that define the processes in which the standard is used.

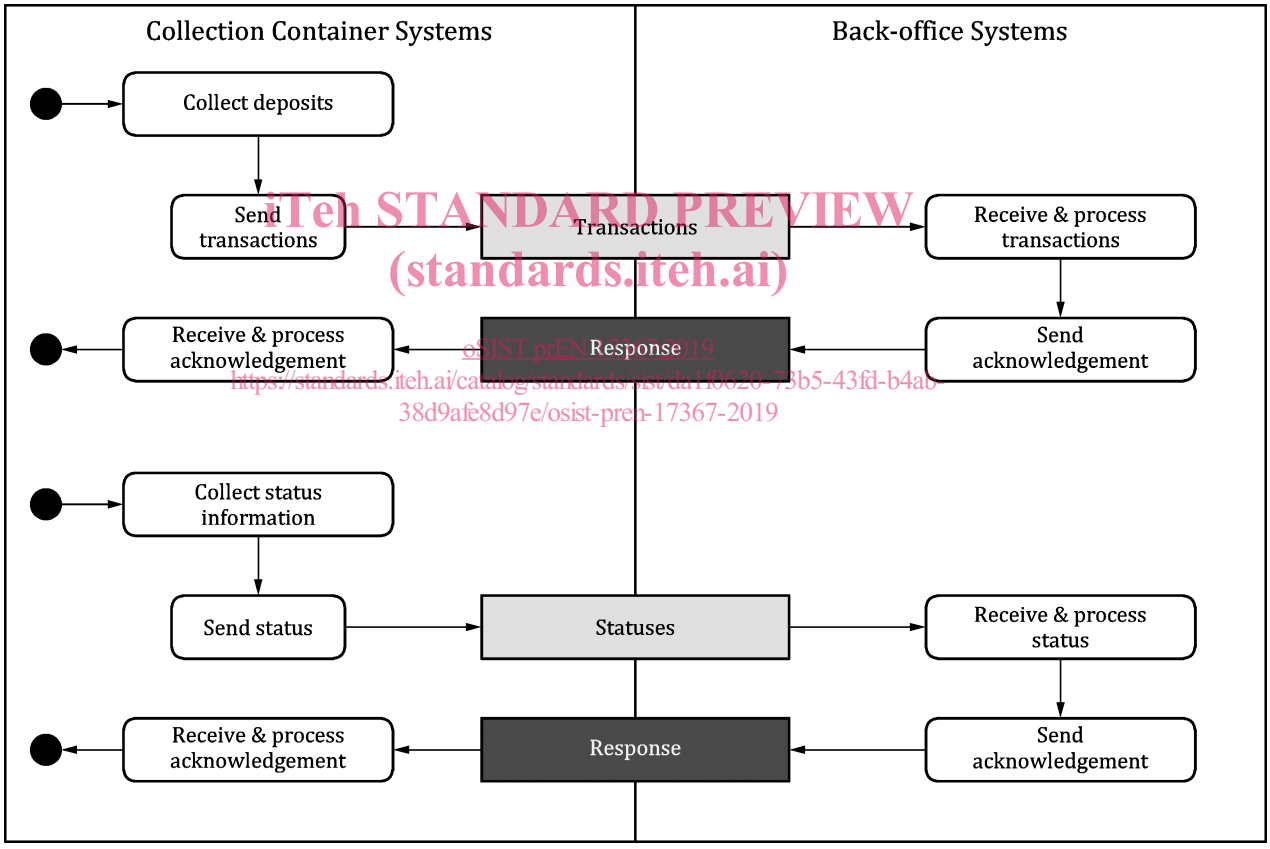

Figure 2 — Activities from CMS to BOS

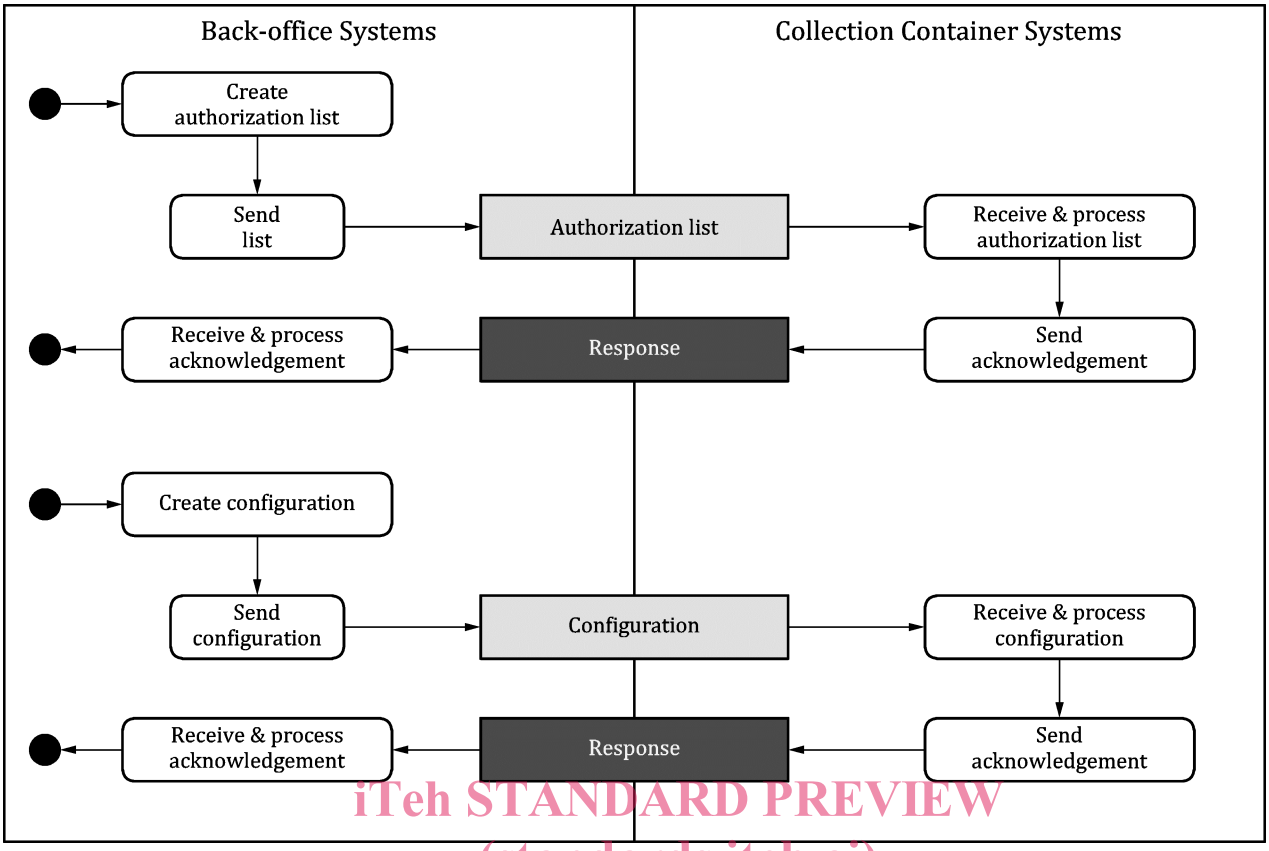

Figure 3 — Activities from BOS to CMS

5 Communication protocol

5.1 General

This section describes the standard rules for the implementation of the communication protocol.

To comply with the standard, all definitions shall be implemented and supported by the protocol.

Other standards and conventions shall be respected when they are mentioned in this document.

Recommendations should be supported by the implementation of the protocol.

5.2 Definitions (SHALL)

5.2.1 Communication is done through RESTful web-services

Restful web-services are the industry standard for building efficient interfaces between distributed systems. There is a large number of resources to assist the developers in almost any available programming language.

5.2.2 Transport is secured with SSL

Always use SSL. No exceptions. Today, your web APIs can get accessed from anywhere there is internet (like libraries, coffee shops, airports among others). Not all of these are secure. Many don't encrypt communications at all, allowing for easy eavesdropping or impersonation if authentication credentials are hijacked.

Another advantage of always using SSL is that guaranteed encrypted communications simplifies authentication efforts — you can get away with simple access tokens instead of having to sign each API request.

One thing to watch out for is non-SSL access to API URLs. Do not redirect these to their SSL counterparts. Throw a hard error instead! The last thing you want is for poorly configured clients to send requests to an unencrypted end point, just to be silently redirected to the actual encrypted end point.

5.2.3 Authentication is done using an API Key/Secret and HMAC

It is a mechanism for calculating a message authentication code using a hash function in combination with a shared secret key between the two parties involved in sending and receiving the data (Front-end client and Back-end HTTP service). The main use for HMAC to verify the integrity, authenticity, and the identity of the message sender.

See Annex A.

5.2.4 API versioning

Versioning SHALL be done in the URL to ensure browser explorability of the resources across versions. For instance:

— "/store/api/v1"

— "/store/api/v2"

5.3 Conventions (SHALL)

5.3.1 The standard data format is JSON

In order to minimize overhead, the type of data are usually JSON in RESTful web-services. However, a majority of implementations support both data formats. The type of data in the body (JSON or XML) SHALL be specified in the header of the request using the "Content-Type" tag.

5.3.2 Dates and Times are following the ISO 8601

The common format for dates is "***YYYY-MM-DDTHH:mm:ssZ***"

The common format for time is "***HH:mm:ssZ***"

5.3.3 HTTP Verbs

As the standard only defines PUSH behaviour, the only accepted HTTP Verb is ***POST.***

5.3.4 HTTP Status Codes

The standard HTTP status codes SHALL be used. In particular:

— ***200 — OK***: The request has succeeded.

— ***400 — Bad Request***: The request could not be understood by the server due to malformed syntax. The client SHOULD NOT repeat the request without modifications.

— ***401 — Unauthorized***: When no or invalid authentication details are provided.

— ***500 — Internal Server Error***: The server encountered an unexpected condition which prevented it from fulfilling the request.

— ***501 — Not Implemented***: The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.