Horizon 2020

COLLECTION CARE

Innovative and affordable service for PC monitoring of individual Cultural Artefacts during display, storage, handling and transport

Procedure and guidelines to associating sensing node to cloud

Deliverable number: D4.4

Version 1.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 814624.

Project Acronym:	CollectionCare
Project Full Title:	Innovative and affordable service for PC monitoring of individual Cultural Artefacts during display, storage, handling and transport
Call:	H2020-NMBP-ST-IND-2018-2020
Topic:	NMBP-33-2018
Type of Action:	IA
Grant Number:	814624
Project URL:	www.collectioncare.eu

Deliverable nature:	Report
Dissemination level:	Public
WP n^0:	4
WP title:	Design of the Wireless sensing system
Contractual Delivery Date:	September 2020
Delivery Date:	30th September 2020
Number of pages:	17
Keywords:	Connectivity, cloud, enrolment
Authors:	Ángel Perles, UPV Jaime Laborda, UPV
Reviewers:	Ana María García-Castillo, UPV

Abstract

Deliverable 4.4 entitled “Procedure and guidelines to association sensor to cloud”, is within the framework of WP4, Task 4.4, subtask 4.4.6. Its aim is to establish the connections between the data transmitted by the sensor nodes and the cloud architecture created un Task 3.1 and save the collected data according to the storage architecture of Task 3.2.

The document includes 4 sections. The first is the introduction describing the aim of Task 4.4.

Section 2 describe the current procedure that is used for the sensor enrolment process in the cloud for the different radiofrequency technologies as well as explains the sensor data adaptor used for the cloud infrastructure connection.

Following, section 3 describes an association to the cloud proposal for the end users and gives some guidelines in order to improve the current procedure for a more user-friendly experience.

The last section, section 4, is a summary of the conclusions found and a description of the next steps of the Task 4.4.

Abbreviations and Acronyms Glossary

API	Application Programming Interface
AWS	Amazon Web Services
D	Deliverable
DB	Database
JSON	JavaScript Object Notation
LoRaWAN	Long-Range Wide-Area Network
REST	Representational State Transfer
RF	Radiofrequency
UPV	Universitat Politècnica de València
VM	Virtual Machine
WP	Work Package

List of figures

Contents

1. Introduction

This deliverable presents the methodology and procedures for associating the "basic" sensor nodes developed in T4.3 with the cloud infrastructure developed by ATOS in T3.1 with the aim of loading and storing the sensor data in almost real time to the CollectionCare storage architecture proposed in T3.2. This task implies writing new data adaptors in the cloud infrastructure for both Sigfox and LoRaWAN in order to adapt the data to the correct format and then to upload it through the CollectionCare secure API developed by ATOS.

Furthermore, in this deliverable some guidelines for future sensing node association procedures are described in order to facilitate the sensor to cloud registration for the end users.

2. Current procedure for sensor node enrolment

2.1 Network server registration of the sensor nodes

For the sensor node to properly transfer data to the cloud infrastructure is crucial for the device to be properly identified and registered on the network server. This network server acts as an interface between the gateways that collect the data, using the LoRaWAN or Sigfox protocol, and the end-user database where the sensor data will be stored.

The registration procedure of the "basic" sensor nodes is quite a manual task, as the device identification parameters have to be manually uploaded to the network server. Nevertheless, this process is expected to be changed in future revisions and the process of registration of the device on the network will be done in an automated way as part of the assembly and testing of the nodes.

This process is different depending on the technology used by the sensor nodes. LoRaWAN nodes need to be provisioned in a LoRaWAN Network Server, and Sigfox nodes are registered in the Sigfox backend. Nevertheless, although the processes are different, they are in fact quite similar.

2.1.1 LoRaWAN Network Server

The LoRaWAN Network Server is the brain and controller of a LoRaWAN network, where the Gateways and devices are registered and connected together. The Network Server is responsible for connecting sensors, gateways as well as end-user applications, and ensures reliable and secure data routing all along the LoRaWAN network.

This is the place where the sensor nodes have to be registered with their credentials so that the gateways that route their messages can understand their packets and route them to their corresponding end-user application.

LoRAWAN alliance [LoRaWAN Security FAQs] defines the specifications for LoRaWAN networks and determines the methods to authenticate and register devices in the network.

There are two methods of authentication, Activation-by-Personalization (ABP) and Over-the-Air-Activation (OTAA). The second one is more secure as the session keys used for message encryption are negotiated by the device for each session when it connects to the network, so the risk of a man-in-the-middle attack is reduced as the keys change. CollectionCare's "basic" sensor node uses OTAA activation for enrollment with the network server.

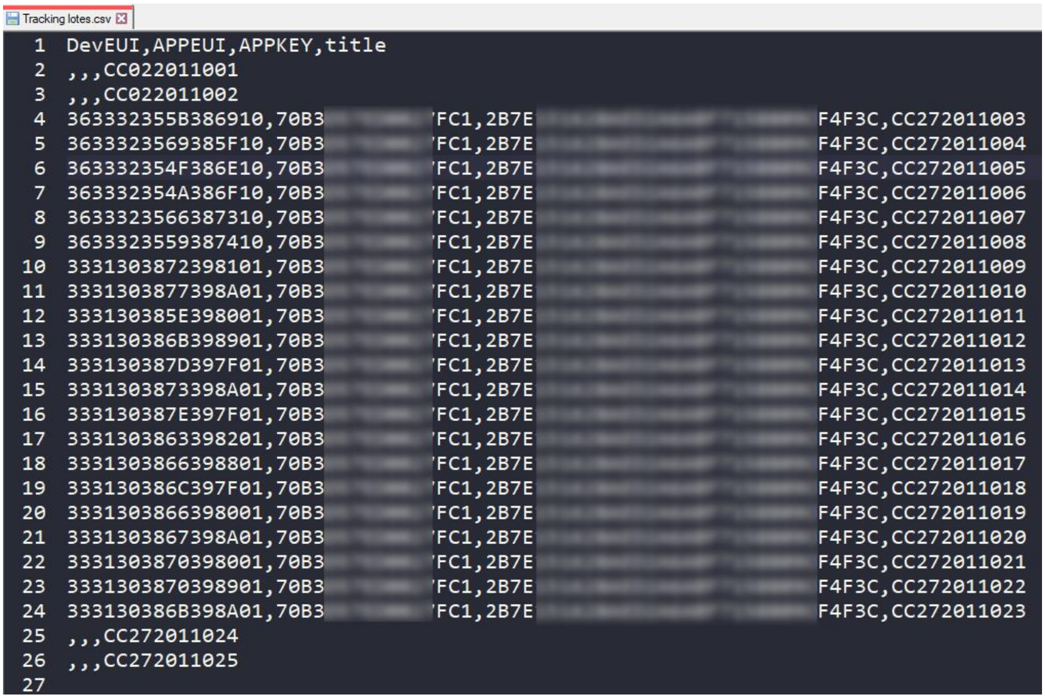
For OTAA provisioning, three parameters are needed for registering the device on the network:

- DevEUI: IEEE EUI64 [IEEE. Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)] unique identification for the end device
- AppEUI: 64-bit number linked to the Application Server so that the end node knows where to send their messages
- AppKey: Encryption key used to encode the messages between the end nodes and the Application Server

Each end device has its own identification number on the network, known as the DevEUI. This is a kind of

Physical Address like the MAC for Internet networks. This is unique for each device and is linked to the serial number of the hardware.

Device identification and credentials for the manufacturing batch of “basic” sensor nodes are stored in a comma-separated file (Figure 1). This file contains all the necessary keys to register all the manufactured “basic” sensor nodes.



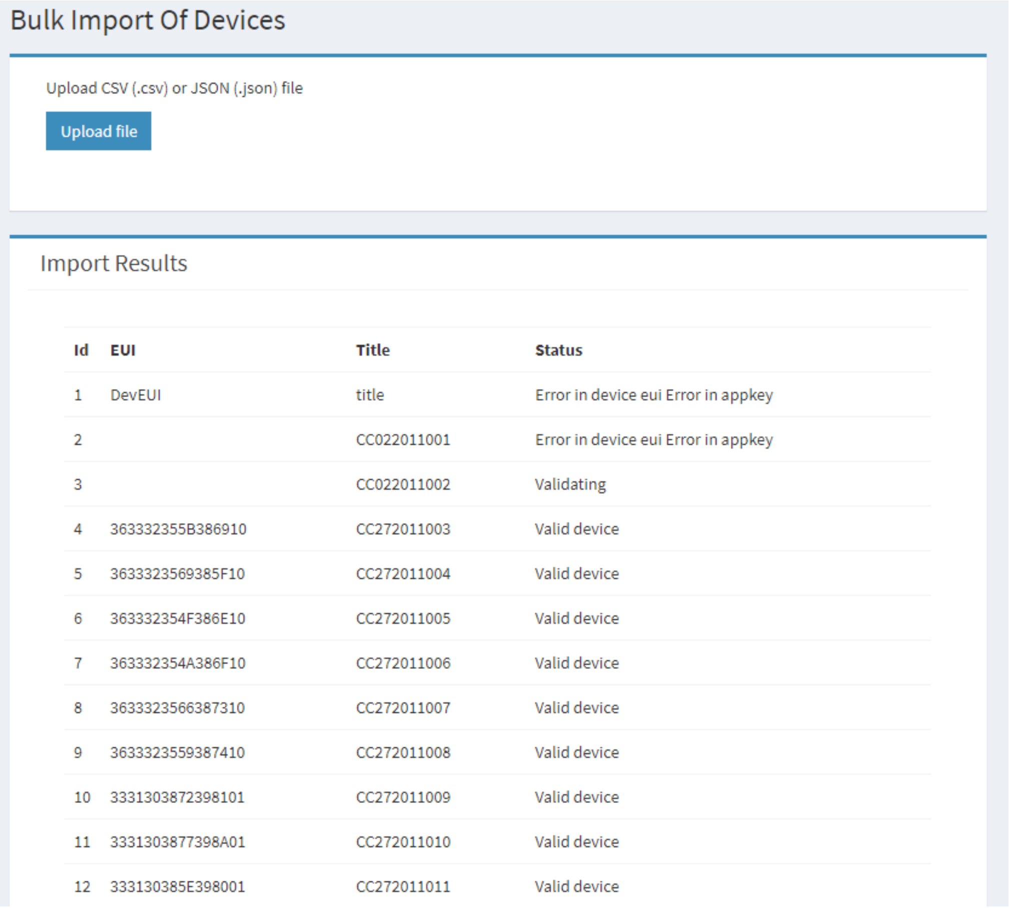
```
DevEUI,APPEUI,APPKEY,title
,,,CC022011001
,,,CC022011002
363332355B386910,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011003
3633323569385F10,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011004
363332354F386E10,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011005
363332354A386F10,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011006
363332356387310,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011007
363332355938741 0,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011008
333130387239810 1,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011009
3331303877398A01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011010
333130385E398001,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011011
333130386B398901,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011012
333130387D397F01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011013
3331303873398A01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011014
333130387E397F01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011015
3331303863398201,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011016
3331303866398801,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011017
333130386C397F01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011018
3331303866398001,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011019
3331303867398A01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011020
3331303870398001,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011021
3331303870398901,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011022
333130386B398A01,70B3[redacted]FC1,2B7E[redacted]F4F3C,CC272011023
,,,CC272011024
,,,CC272011025

```

Figure 1. CSV file of first batch device credentials

The AppEUI is common to all the sensor nodes. This is because all sensors share the same application server as well as the same end-user application, so messages from all sensor nodes must go to the same place to be processed correctly as will be described in future chapters.

In this particular case, the AppKey is also common to all devices. This is not important for a prototype, but should be improved in the future for a real scenario, as it will increase security. The recommendation for this key is that it is randomly generated within the device and shared with the server on the network where it will be securely stored during programming and testing of the device.

The CSV file is uploaded and imported in the network server, which is accessed through the web user interface using a web browser. At the end of this process, the sensor nodes have successfully enrolled into the LoRaWAN Network Server and are able to start uploading their sensing parameters to the cloud infrastructure.



Bulk Import Of Devices

Upload CSV (.csv) or JSON (.json) file

Import Results

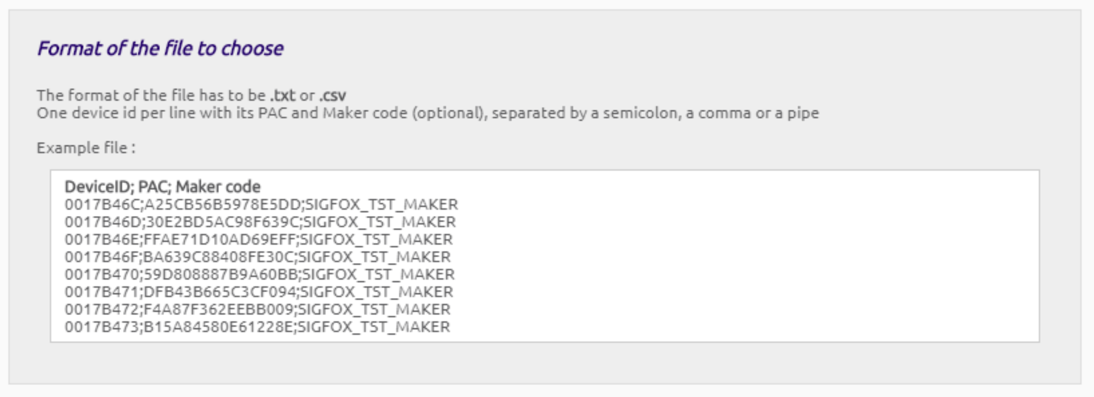
Id	EUI	Title	Status
1	DevEUI	title	Error in device eui Error in appkey
2		CC022011001	Error in device eui Error in appkey
3		CC022011002	Validating
4	363332355B386910	CC272011003	Valid device
5	3633323569385F10	CC272011004	Valid device
6	363332354F386E10	CC272011005	Valid device
7	363332354A386F10	CC272011006	Valid device
8	3633323566387310	CC272011007	Valid device
9	3633323559387410	CC272011008	Valid device
10	3331303872398101	CC272011009	Valid device
11	3331303877398A01	CC272011010	Valid device
12	333130385E398001	CC272011011	Valid device

Figure 2. Importing the CSV credentials file into the network server

2.1.2 Sigfox backend

For the Sigfox node the enrollment process is quite similar to the LoRaWAN one. Devices have a Device Identification (DevId) and a Personal Access Code, known as a DevPac, that is the password token for accessing the network.

All the credentials of the sensor node batch to be registered are stored in a comma-separated file with the format described in Figure 3. This file will include the device identification and the password for each sensor of the sensor nodes to be registered.



Format of the file to choose

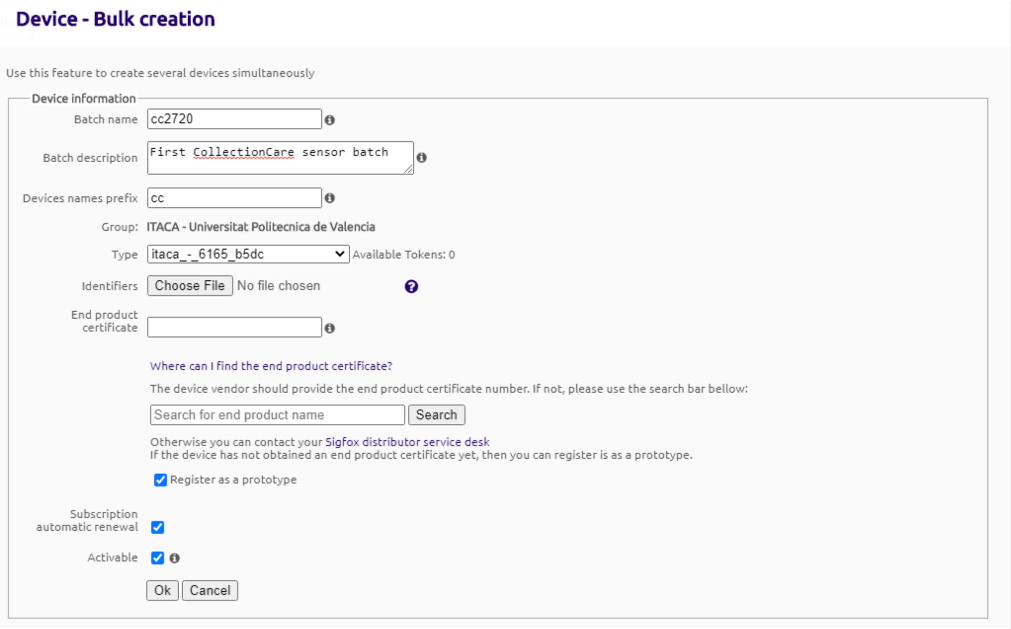
The format of the file has to be **.txt** or **.csv**
One device id per line with its PAC and Maker code (optional), separated by a semicolon, a comma or a pipe

Example file :

```
DeviceID; PAC; Maker code
0017B46C;A25CB56B5978E5DD;SIGFOX_TST_MAKER
0017B46D;30E2BD5AC98F639C;SIGFOX_TST_MAKER
0017B46E;FFAE71D10AD69EFF;SIGFOX_TST_MAKER
0017B46F;BA639C88408FE30C;SIGFOX_TST_MAKER
0017B470;59D808887B9A60BB;SIGFOX_TST_MAKER
0017B471;DFB43B665C3CF094;SIGFOX_TST_MAKER
0017B472;F4A87F362EEBB009;SIGFOX_TST_MAKER
0017B473;B15A84580E61228E;SIGFOX_TST_MAKER
```

Figure 3. CSV credentials file format for Sigfox device registration

This CSV file must be uploaded to the Sigfox Backend web interface with some batch identifications and a prefix to identify the devices. It also has to be linked to a predefined Device Type, which is equivalent to the Application in LoRaWAN, where a Sigfox Callback is configured to send the payload data to the user's application.



Device - Bulk creation

Use this feature to create several devices simultaneously

Device information

Batch name	cc2720
Batch description	First CollectionCare sensor batch
Devices names prefix	cc
Group:	ITACA - Universitat Politecnica de Valencia
Type	itaca_-_6165_b5dc Available Tokens: 0
Identifiers	Choose File No file chosen
End product certificate	

Where can I find the end product certificate?

The device vendor should provide the end product certificate number. If not, please use the search bar bellow:

Search for end product name [Search]

Otherwise you can contact your Sigfox distributor service desk
If the device has not obtained an end product certificate yet, then you can register is as a prototype.

☑ Register as a prototype

Subscription automatic renewal ☑

Activable ☑

Figure 4. Bulk import enrolment process

Set the "Register as a prototype" option, as we don't have yet the proper product certification from Sigfox.

2.2 Sensor data adaptor description to CollectionCare cloud infrastructure

2.2.1 LoRaWAN

In order to upload the sensing data collected by the networks servers, either using LoRaWAN or Sigfox, to the CollectionCare cloud infrastructure it is mandatory to process, decode, and adapt it to match the correct format proposed by ATOS (see D.3.2).

The adaptor interface has been developed using NodeRED, a flow-based development tool for visual programming originally written in Node.JS by IBM. It allows connecting Internet of Things devices to different online services providing a web browser-based flow editor for this task. Figure 5 shows the flow used for the data adaptor used.

Data comes either from the LoRaWAN network server or from Sigfox Backend. In the case of the Loriot LoRaWAN network server, data is collected from a WebSocket and for Sigfox, the data is collected using an API endpoint. Using NodeRED simplifies development efforts and it is ready for production use.

Loriot's Network Server allows secure websockets as an output in order to connect to your application. Thus, the user's application is connected through the use of bidirectional full-duplex secure TCP socket. To use this function, Loriot provides a URL or a web-socket, as well as a secure token to connect to the socket. In this way, both servers are connected to each other and the information received by the network server is tunnelled directly to the NodeRED application server.

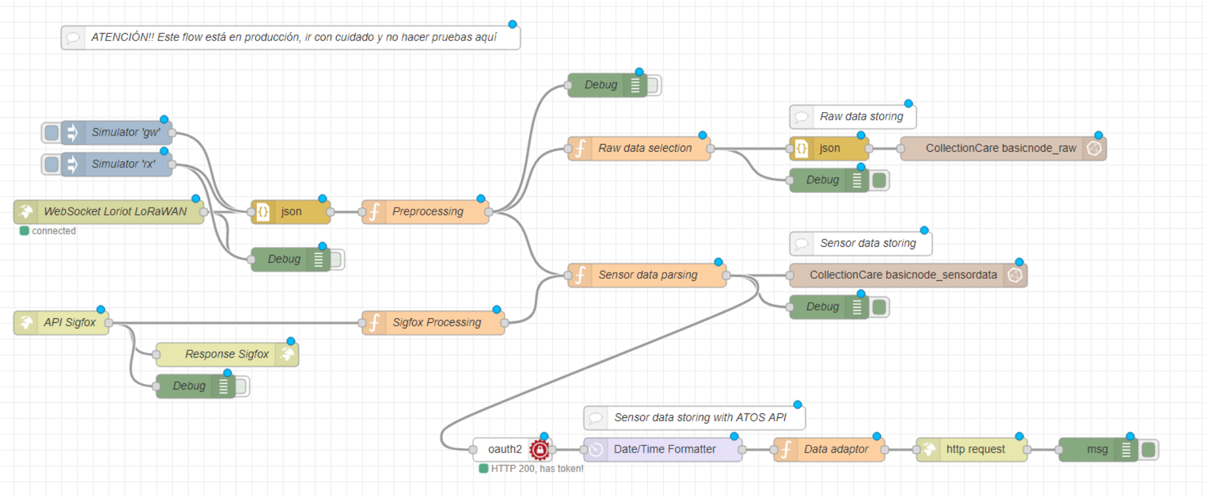


Figure 5. Data adaptor interface for CollectionCare infrastructure upload

The data coming from LoRaWAN nodes is stored in two different databases (Figure 5). In one the raw data from the gateways is stored in string format to be analyzed later if needed. This string contains useful metadata as to how many gateways have received the data, as well as their corresponding signal strength, gateway location and signal to noise ratio among others. This information will be helpful in the future in order to analyze the behavior of the system and improve it if necessary.

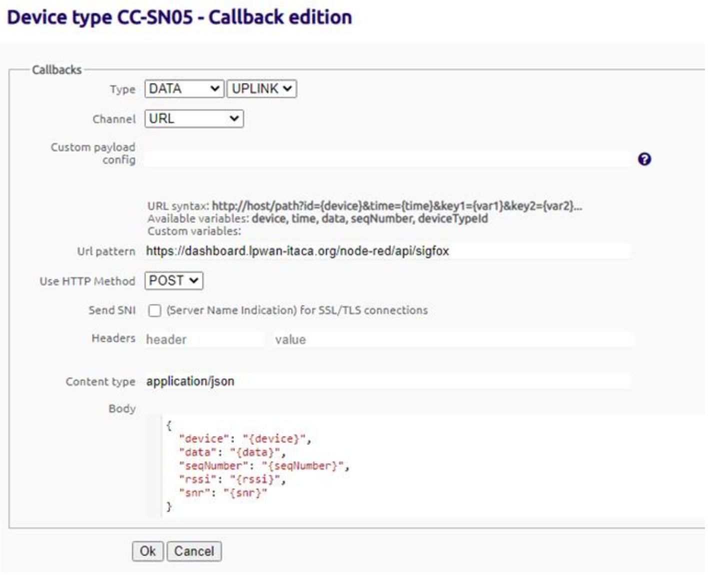
The second stream decodes the payload from the sensor that is transmitted, and stores the decoded environmental records in a second InfluxDB database.

LoRaWAN Network Server reports the payload data for a specific device DevEUI, however, it is desirable that the information is stored in the database related with the hardware serial number that identifies the device. DevEUI is linked with the hardware serial number stored in a file using JSON format.

Finally, a third flow that inherits the decoded data from the second one is responsible for uploading the sensor data into the CollectionCare Database through the secure API developed by ATOS. This API requires a special token to be able to load the data securely, as described in D3.2. This is an OAuth2 token and it is achieved by using a NodeRED node and a username and password in order to obtain the token. This ensures privacy and access to the database.

2.2.2. Sigfox

Sigfox backend does not support Websocket to send the data to the user application. Instead they offer what they call "Custom callback" (Figure 6), which is just a customizable HTTP call that will make a HTTP request to the API configured by the user. The end user application exposes an API method in order to be called by the Sigfox backend. This is achieved in NodeRED using the "http in" block, that allows to create an HTTP endpoint using the desired method. A HTTP POST method has been created and configured in Sigfox in order to be able to transfer the data records.



Device type CC-SN05 - Callback edition

Callbacks

Type: DATA, UPLINK

Channel: URL

Custom payload config:

URL syntax: http://host/path?id={device}&time={time}&key1={var1}&key2={var2}...
Available variables: device, time, data, seqNumber, deviceTypeId
Custom variables:

Url pattern: https://dashboard.lpwan-itaca.org/node-red/api/sigfox

Use HTTP Method: POST

Send SNI: □ (Server Name Indication) for SSL/TLS connections

Headers: header value

Content type: application/json

Body:

```
{
  "device": "{device}",
  "data": "{data}",
  "seqNumber": "{seqNumber}",
  "rssi": "{rssi}",
  "snr": "{snr}"
}
```

Figure 6. Sigfox Custom Callback configuration

As can be seen in Figure 6, Sigfox custom callbacks allow to define the format of the information to be sent. This allows us to adapt the JSON to match the one sent by the LoRaWAN network. In this way all the developed functions remain valid.

3. Association to the cloud for the end user proposal

The aim of the CollectionCare system is to be an affordable service for the monitoring of cultural artefacts and therefore no technical expertise or skills should be required for the installation of sensor nodes or cloud association.

For this reason, the association of the device with the cloud infrastructure must be as simple and transparent as possible for the end user. It is therefore important to address this task so that the user has the best possible experience.

3.1 Device identification proposal

Each device is identified by several parameters that are all linked together for the purpose of identifying each sensor in a unique manner.

A hardware device serial number, that is the sequential number for the assembled PCB.

This serial number is intended to identify the hardware manufactured for the sensor node. This is important when it comes to identifying each device in a unique way and being able to track it. That is to say, with which hardware revision it has left the factory, which version of the firmware was installed, to which client or museum it was sent, etc.

The serial number format is the following:

CC-2013-88-003

- CC (##): Prefix that identifies the hardware
- 2013 (YYWW): Year and Week of manufacturing (for batch identification)
- 88 (##): Hardware revision and manufacturing site
- 003 (###): Sequential number

The hardware serial number is used internally to link information such as the serial number of the microcontroller, the DevEUI for LoRaWAN registration and the DevId for the Sigfox network, so that the device can be properly recognized and identified on the network.

3.2 Association procedure

For the association procedure of the sensor nodes, the devices to be delivered will be previously registered and configured in the CollectionCare network and will be ready for immediate use. This is to ensure that end users only have to link them to their museum account and to the artefacts of interest using their credentials.

Users will be provided with a label with a QR code that will be placed on each sensor node (Figure 7). This QR code will include a secure URL to the CollectionCare platform where the user will be asked to log in and select which artwork (or artworks) he/she wants to link to the sensor node, as well as the corresponding sensor metadata (room, location, internal museum identification, etc.).

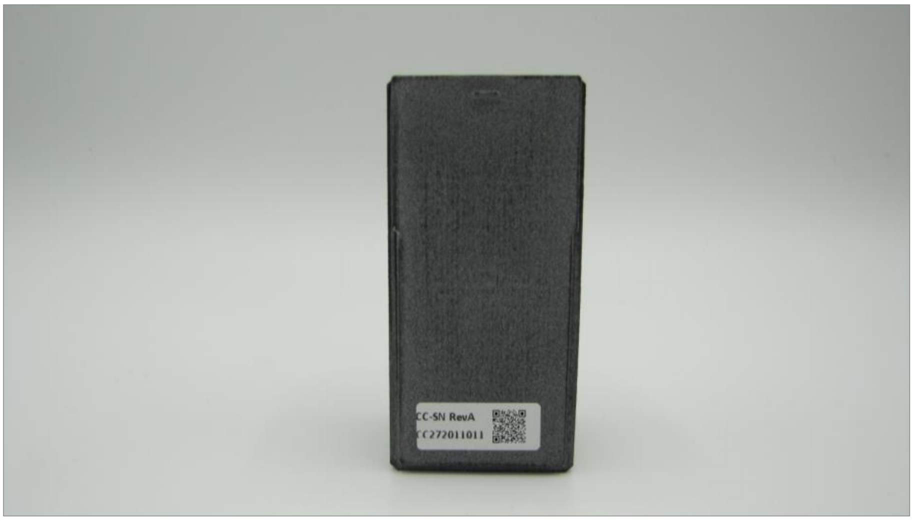


Figure 7. Back of the sensor with the QR code label

The requirement for registration will be an active Internet connection to access a website, and the availability of a camera on the device used for the registration stage. For devices without a camera, the user may manually enter the serial number. The use of a web page for the registration process allows the use of mobile devices and personal computers without the need to develop a specific application.

The same web access using the QR code can be used for other purposes such as sensor unenrollment, Artefact de-association, etc.

4. Conclusions and next steps

Although the actual process of connecting the sensor node to the CollectionCare cloud infrastructure is valid, it is a rather manual and technical task. This process needs to be improved to facilitate usability and make sensor node registration easier. This will involve developing some cloud data connectors to manage this registration process, as well as a web application to facilitate this association of the cloud to the end user.

Bibliography

Zach Pfeffer. DevEUI, AppEUI (JoinEUI) and AppKey
https://www.centennialsoftwaresolutions.com/post/deveui-appeui-joineui-and-appkey

LoRa Alliance. LoRaWAN Security FAQ
https://lora-alliance.org/resource-hub/lorawanr-security-faq

IEEE. Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)
https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf

ATOS. D3.2 CollectionCare database storage I