|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  | Project acronym: **IoTrust**  Project title: **Secure trust bootstrapping and peer to peer network connection in the Internet of Things**  Third Party: **DW/ODINS**   |  |  | | --- | --- | | Digital Worx GmbH (DW) - Germany |  | | Odin Solutions SL (ODINS) - Spain |  |   Deliverable D.2  Open Standards based IoTrust Development   |  |  | | --- | --- | | **Deliverables leader:** | **Odins Solutions SL (ODINS)** | | **Authors:** | Silke Capo, Mihaly Virag, Mirko Ross, Rafael Marin-Perez, Antonio Skarmeta Gomez, | | **Due date:** | 31-03-2021 | | **Actual submission date:** | 25-03-2021 | | **Dissemination level:** | Public / confidential | |

Abstract: Please provide a brief description

**Disclaimer**

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Commission. The European Commission is not responsible for any use that may be made of the information contained therein.

**Copyright**

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the NGI Consortium. In addition, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

All rights reserved.

This document may change without notice.

**Table of contents**

[1 Introduction 1](#_Toc26358819)

[2 Activities carried out to complete the deliverable 1](#_Toc26358820)

[3 Technical description 1](#_Toc26358821)

[4 Conclusions and next steps 1](#_Toc26358822)

[Appendix 2](#_Toc26358823)

Nb: The deliverable structure below is only provided for guidance and you may adapt in a free form manner the structure to fit your needs.

# Introduction

Shortly introduce the objective of the deliverable within the overall implementation of your project, explaining how it is inter-related to other deliverables, outputs or milestones.

# Activities carried out to complete the deliverable

Shortly summarise the activities undertaken to produce the deliverable and how you addressed any technical or other unforeseen issues that may have arisen.

# Technical description

Describe briefly the key technical characteristics of the deliverable and explain how they are related to the final results expected to be achieved by the project.

You can choose to include or annex relevant documents, mock-up, weblinks, screenshots, etc).

## LoRaWAN Network Deployment

The employed LoRaWAN module in IoTrust is the RN2483[[1]](#endnote-1) by Microchip. The RN2483 is a market ready integrated module that implements a LoRaWAN Class A and C stack. The RN2483 is a certified LoRaWAN device, this is, the LoRa Alliance guarantees the RN2483's compatibility with any LoRaWAN network that follows the official LoRaWAN Specification v1.0.2[[2]](#endnote-2). This solution was preferred over other LoRaWAN chip models due its popularity in both academia and industry. The communications with the module are done via ASCII commands over a UART, which enables accelerates development and debugging tasks.

The employed LoRaWAN server for IoTrust, the ChirpStack.io project, runs using the micro-service technology Docker. This improves portability and guarantees that the deployment will not suffer from broken library compatibility or missing dependencies due to all the container images being stored in Docker's official repositories. The official ChirpStack developers provide deployment configuration files[[3]](#footnote-1) via its own repository. This design choice dramatically facilitates the deployment and management of IoTrust solutions in different scenarios, due to Docker's wide-spread availability.

## Secure Lightweight Bootstrapping

### SCHC

Static Context Header Compression (SCHC)[[4]](#endnote-3) is one of the key enabling technologies for the IoTrust project. It is a technology aimed at enabling the interoperability of devices using Low-Power Wide-Area Networks (LP-WANs) with the Internet. In order to do so, SCHC applies a series of header compression and packet fragmentation steps over that allow the transmission of IPv6 packets over low bandwidth technologies. It leverages on the key idea that end-devices run specific applications during their entire lifetime. Thus, the data-flows employed by the device are typically well-known during the design stage. This enables the creation of a data table, known as context in SCHC jargon, that will indicate the header compression and packet fragmentation mechanisms how each header field is processed. If the target values of the header fields are known beforehand, this shifts their contents away from the network into to the static context, avoiding their transmission over radio, thus saving battery power and bandwidth. The more header field values are known, the better the compression will be. Instead of building the context during execution, it is defined during the development phase. Thus, it is expected that each project and application employing SCHC will have its own configuration customized to the deployment needs. Furthermore, different end-devices might have different context within the scope of the same project, depending on the final application that is to be run.

LP-WANs implement a thin network layer that does not take interoperability into consideration. However, SCHC can be tailored to the specifics of each LP-WAN technology as specified in different Internet Drafts authored by the IETF lpwan Work Group. Currently, these Internet Drafts define the compression and fragmentation procedure for NB-IoT, SigFox, and LoRaWAN. In IoTrust we take into consideration the specifics of the Internet Draft for implementing SCHC over LoRaWAN[[5]](#endnote-4), as defined by the IETF lpwan Work Group. LoRaWAN application payloads include a header field called fPort. This is an octet employed locally by the user to differentiate applications or verticals. Hence, in the specific case of SCHC, it is employed to transport the first byte of the SCHC packet. This saves a byte of each transmission, since the fPort is mandatory.

## FUOTA and Trust Monitoring

It is the second critical component of the IoTrust project after the bootstrapping. It focuses on facilitating security patches to the IoT devices and generate dynamic trust score. This is all accomplished by multiple open-source technical components. The following sections give more details about them.

### Blockchain

The Blockchain is employed to store critical device and firmware information in an immutable and distributed ledger. It is chain of blocks which are sequentially linked with cryptographic methods. Each block has cryptographic hash of its parent block.

Block

Blockchain diagram

Deployment

### IPFS

InterPlanatery File System (IPFS) is a peer-to-peer storage network.

### Customer Platform

The customer platform facilities a dashboard to manage and control IoT devices and their firmware.

# Conclusions and next steps

Outline any conclusions on the results achieved and any lessons learned for the next stage of the project.

Describe briefly the next steps in the project development and how you will build on this deliverable to complete the work.

Appendix

* E.g. mock-ups, screenshots
* References
* Etc.

1. https://www.microchip.com/wwwproducts/en/RN2483 [↑](#endnote-ref-1)
2. Alliance, L., Sornin, N., Luis, M., Eirich, T., Kramp, T., & Hersent, O. (2016). LoRaWAN TM Specification v1.0.2. *LoRaTM Alliance*. https://lora-alliance.org/resource-hub/lorawantm-specification-v102 [↑](#endnote-ref-2)
3. https://github.com/brocaar/chirpstack-docker [↑](#footnote-ref-1)
4. Minaburo, A., Toutain, L., Gomez, C., & Barthel, D. (2020). *SCHC: Generic Framework for Static Context Header Compression and Fragmentation* (Request for Comments, Issue 8724). RFC Editor. https://doi.org/10.17487/RFC8724 [↑](#endnote-ref-3)
5. Gimenez, O., & Petrov, I. (2021). *Static Context Header Compression (SCHC) over LoRaWAN* (Issue draft-ietf-lpwan-schc-over-lorawan-14). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-schc-over-lorawan-14 [↑](#endnote-ref-4)