ZDMP: Zero Defects Manufacturing Platform

WP5: ZDMP Core Services and Middleware

EU ID: D062: T5.2 Robust Industrial Network - Vs: 1.0.0A

ZDMP ID: D5.2a

Deliverable Lead and Editor: Leticia Montalvillo, IKER

Contributing Partners: IKER, ITI

Date: 2020-06

Dissemination: Public

Status: EU Approved

Abstract

The deliverables for this task, and all WP5-8 tasks, are software and are of EU type “OTHER”. The software and accompanying material (eg description, instructions) is available on the ZDMP software repository which is updated dynamically. However, for EU formal reporting purposes, this brief cover document provides a formalised pointer to the downloadable software and related content. This deliverable should read in conjunction with the D006-D020 deliverables which document the software process/status for each WP/Task. This deliverable represents the status as at M18 with further living editions at M18 and M48

Grant Agreement: 825631

Document Status

Deliverable Lead	Leticia Montalvillo, IKER
Internal Reviewer 1	Santiago Cáceres Elvira, ITI
Internal Reviewer 2	Paulo Maheiro, PTM
Internal Reviewer 3	Stuart Campbell, ICE
Type	Deliverable
Work Package	WP5: ZDMP Core Services and Middleware
ID	D062: T5.2 Robust Industrial Network
Due Date	2020-06
Delivery Date	2020-06
Status	EU Approved

History

See Annex A.

Status

This deliverable is subject to final acceptance by the European Commission.

Further Information

www.zdmp.eu and mailto:info@zdmp.eu

Disclaimer

Project Partners:

Executive Summary

The main objective of “WP5: Core Services and Middleware” is to deliver the core Industrial IoT/Network support of data acquisition, interoperability, and AI/analytics supported by orchestration, monitoring and autonomous computing.

The deliverables of this work package and the WP1 Management work package are divided into software packages and document/reports. In terms of reporting:

- **Process/Status:** This report corresponds to D009 Technical Management: WP5 Report of WP1 Management: Procedures, Metrics, Coordination, and Reporting and, as identified in the DOA, focuses on the process/status of the work accomplished in WP5
- **Software:** All WP5 software deliverables of T5.1-T5.6 (type “OTHER”) are available in the ZDMP public repository with access details and install instructions further described in this report which is a ‘current’ extract of the repository

“WP5: ZDMP Core Services and Middleware” consists of six main parts: Data Acquisition, Network Support, Data Harmonisation, Orchestration and Monitoring, Distributed and Autonomous Computing, and AI and Analytics. The tasks of WP5 are the following:

- T5.1: Data Acquisition and IIoT
- T5.2: Robust Industrial Network Support
- T5.3: Data Harmonisation and Interoperability
- T5.4: Orchestration, Monitoring, and Alerting
- T5.5: Distributed and Autonomous Computing
- T5.6: AI and Analytics

This deliverable represents Task T5.2 Robust Industrial Network Support which in turn is composed of the following components:

- Secure Authentication and Authorisation
- Secure Communication
- Secure Installation

As reported in the architecture deliverable the purpose of these components is: “To provide the mechanisms that guarantee the secure installation of zApps. This also verifies that any zApp installed in the platform is trustworthy and delivered by a legitimate developer”, “To provide a Public Key Infrastructure (PKI) for components to implement a secure communication framework across the platform. This is responsible for managing certificates associated to the developers, who need to sign every zApp published in the Marketplace, as well as enabling devices to establish secure encrypted channels.” and “To provide secure authentication and authorisation with the aim to protect resources from unauthorised accesses. This applies to users, components, assets, etc.”

Each of the components is structured into the following sections:

- General Description
- Architecture Diagram
- Features
- Requirements
- Installation
- How to Use
- Functional Requirements Implementation Status (M18)

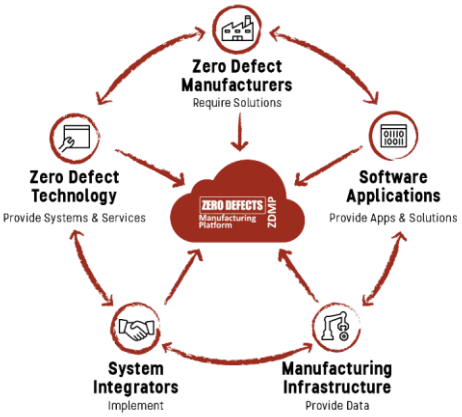
This report covers the period from the project start until M18 with most activity in the M13-M18 period. Further formal deliverables are due M30 and M48 as well as an informal iteration at 24.

Table of Contents

0 Introduction

Due to the cover nature of this deliverable; this introduction is presented in short-form only. For further information please consults D006 - Technical Management: Overview Report.

0.1 ZDMP Project Overview



ZDMP – Zero Defects Manufacturing Platform – is a project funded by the H2020 Framework Programme of the European Commission under Grant Agreement 825631 and conducted from January 2019 until December 2022. It engages 30 partners (Users, Technology Providers, Consultants and Research Institutes) from 11 countries with a total budget of circa 16.2M€. Further information can be found at www.zdmp.eu.

ZDMP aims at providing such an extendable platform for supporting factories with a high interoperability level, to cope with the concept of connected factories to reach the goal of zero-defect production. For this, the platform provides the tools to allow following each step of production, using data acquisition to automatically determine the functioning of each step regarding the quality of the process and product.

0.2 Deliverable Purpose and Scope

The deliverables for this task, and all WP5-8 tasks, are software and are of EU type "OTHER". The software and accompanying material (eg description, instructions) is available on the ZDMP software repository which is updated dynamically. However, for EU formal reporting purposes, this brief cover document provides a formalised pointer to the downloadable software and related content. This deliverable should read in conjunction with the D006-D020 deliverables which document the software process/status for each WP/Task. This deliverable represents the status as at M18 with further living editions at M18 and M48. Specifically, the DOA states the following regarding this Deliverable:

T5.2	**Robust Industrial Network Support**			**SOFT**	**Six Monthly**
D062 D063 D064	Robust Industrial Network Support	OTHER (Prototype)	PU	18, (24), 30, 48, Reporting via T1.4.x Series	RDI3-6, 8
This task will develop and deploy a robust concept for privacy and security handling in the context of an industrial ZDMP network. This Industrial Network security concept will minimize attack surfaces, will maintain cyber-risks at acceptable levels, and will help to mitigate any possible incident associated to cyber-attacks or accidents. The ruling principles of the security concept will be the isolation and zoning of communications (eg using Virtual LAN Segregation, Proxy Servers, Domain Controllers, Virtual Private Networks, Demilitarised Zones), the implementation of robust encryption at different levels (eg using both asymmetric elliptic curve algorithms and symmetric lightweight algorithms), the enforcement of robust access control policies (eg based on XACML 3.0 standard), the authentication of entities (eg based on OpenID, OAuth 2.0). In addition, the enforcement of a Secure Continuous Monitoring system will be necessary (eg based on the SCAP protocol, which permits both measuring the overall security of a system and the application of enhancements to achieve higher security levels). ZDMP needs to ensure networks can be designed and implemented to meet a client's specification whilst remaining secure. The ZDMP tasks will take the lead in providing such a basis. ZDMP security will be pervasively available and applied to other ZDMP components and to build Apps.					

0.3 Target Audience

The primary target audience for this document are the partners and WPs of the project, as well as the EU and reviewers.

0.4 Deliverable Context

The deliverable context is as per Section 0.2:

Primary Preceding documents:

- **D006: Technical Management Overview Report:** Represents the general software status of the project including information on commits and WP5-8 Risks and mitigations
- **D009: Technical Management: WP5 Report:** Represents the process/status and future actions of this work package, including this task. It also includes related KPIs and their status
- **D055: Technical Specification and Update:** Describes the different APIs of the components

0.5 Document Structure

This deliverable is broken down into the following sections:

- **Section 1: Component: Secure Authentication and Authorisation**
- **Section 2: Component: Secure Communication**
- **Section 3: Component: Secure Installation**

0.6 Document Status

This document is listed in the Description of Action as “public” since it represents the open nature of the project’s software deliverables.

0.7 Document Dependencies

- None

0.8 Glossary and Abbreviations

A definition of common terms related to ZDMP, as well as a list of abbreviations, is available at http://www.zdmp.eu/glossary.

0.9 External Annexes and Supporting Documents

- See the ‘Resources’ grid within the General Description Section of each component

0.10 Reading Notes

- None

0.11 Document Updates

- This is the first version of this document

1 Component: Secure Authentication and Authorisation

1.1 General Description

This module provides Authentication and Authorisation for ZDMP assets (eg users, components, zApps, etc). In case of a successful authentication, an associated access token is issued to the corresponding ZDMP asset, which would later be used for authorization. This module provides: Identity Service (for authentication), Authorisation service (for authorization), and basic intrusion detection service (for detecting unauthorized requests to protected resources).

Resource	Location
Source Code	Link
Latest Release (v1.0.0)	Download
X Open API Spec	Link
Video	Coming soon

The date of generation of this component content is: 2020-06-26

1.2 Architecture Diagram

The following diagram shows the position of this component in the ZDMP architecture.

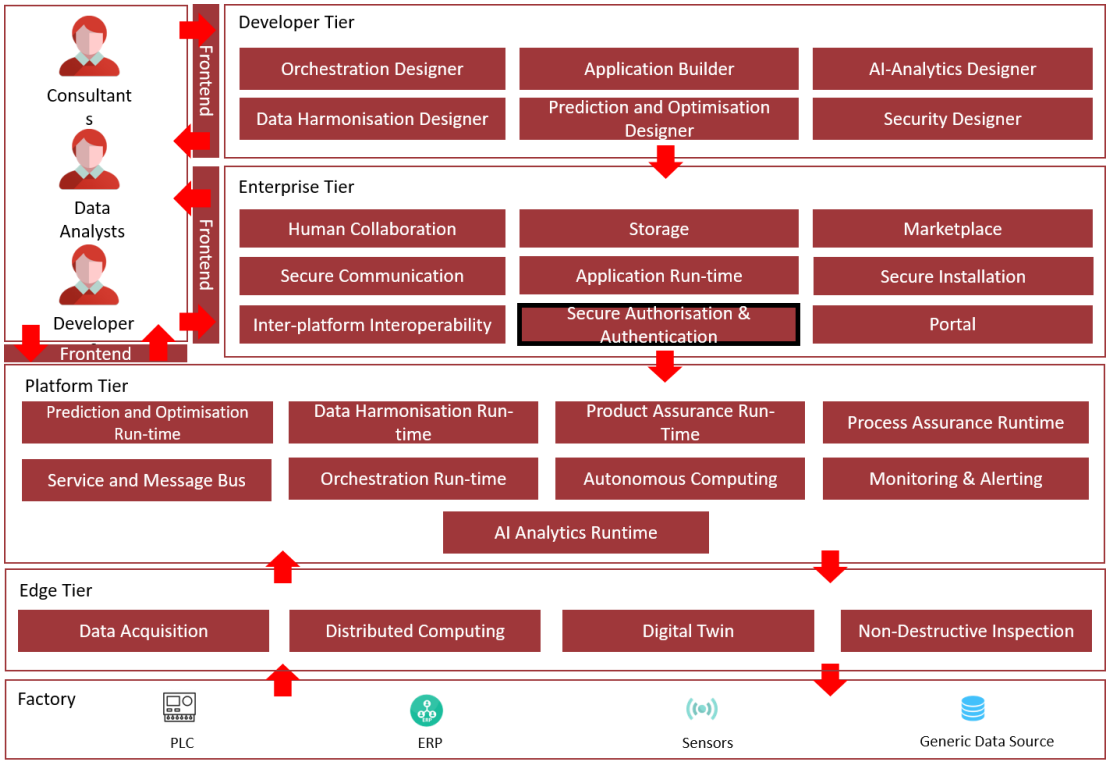


Figure 1: Position of Component in ZDMP Architecture

1.3 Features

The functions and features of the Identity Service are the following:

- **Authentication analyses**: Authentication requests are analysed to decide if they are legitimate or not: once the evaluations have been conducted, a decision is made and if the authentication is valid, an access token is granted. This access token is used subsequently in the authorisation process
- **ZDMP asset info and credentials management**: ZDMP asset (eg users, clients) information and the associated authentication credentials are stored
- **Token management**: The issued access tokens are stored which are those associated to the different authenticated ZDMP assets
- **Auth logging**: Every authentication attempt, successful or not, is registered. Events tracked are: Successful ZDMP asset logins, failed ZDMP asset logins, ZDMP asset account changes, Password changes

The functions and features of the Authorisation Service are the following:

- **Policy enforcement and decision**: Every request made from a specific ZDMP asset is intercepted. The decisions are primarily based on the authorisation policies administrated
- **Policy administration**: Authorisation policies are stored and retrieved when requested
- **Policy information provision**: Additional attributes, coming from multiple sources, are retrieved to enable more informed decision during the authorisation process (based on Role-based Access Control (RBAC))

The Intrusion Detection Service conducts certain verifications over each authorisation request. It provides the following features:

- **Detect suspicious activity**: The Intrusion Detection Service monitors all communications among ZDMPS assets and Authorisation Service to find out possible cases of cyberattacks
- **Logging suspicious activity**: When the Intrusion Detection Service detects any suspicious activity, this module registers it in a secure log database, which can be analysed by the administrators

1.4 System Requirements

Minimal requirements needed:

- Computer with Docker Engine installed (tested in v19.03.8, on Windows)
- The average resources needed to run this component are: 2 CPUs, 2GB memory and 10GB free space on disk

1.5 Installation

The installation of this component is done through docker commands to run docker images. The Secure Authentication and Authorisation component can be installed via docker-compose:

1. Download the latest source code from ZDMP's GitLab repository Download
2. Unzip the folder in the desired workspace

3. Through the command line, go to the orchestration folder and run docker-compose command as follows:

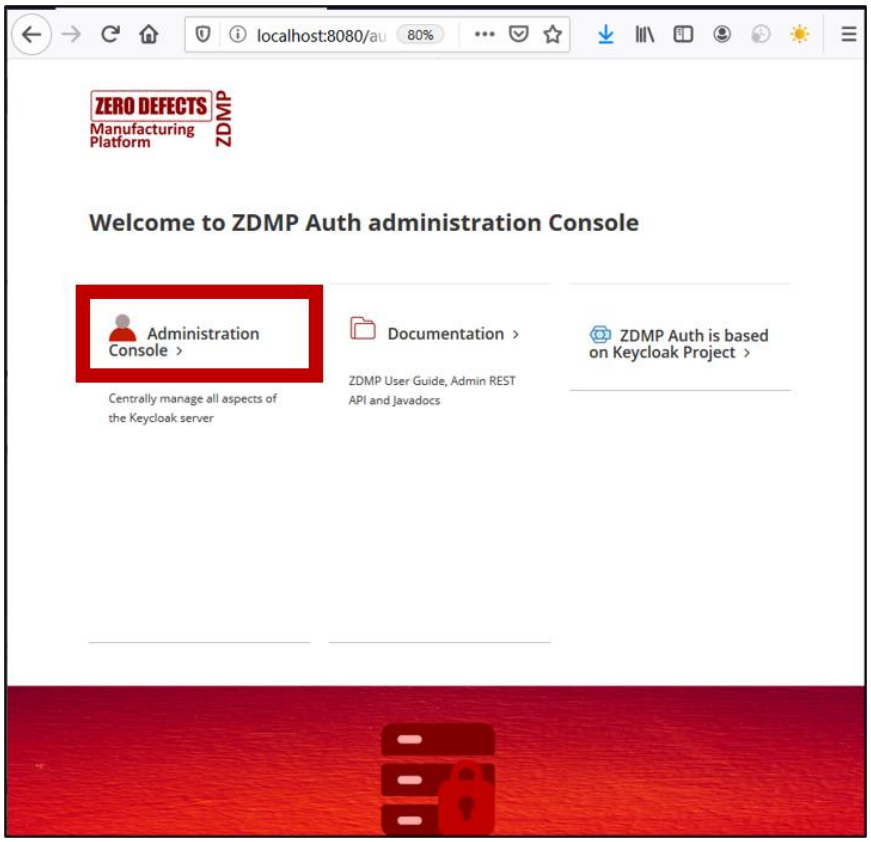
```
zdmpadmin@localhost: cd t5.2-secure-authentication-and-authorization-master/orchestration

zdmpadmin@localhost:~$ docker-compose up -d
```

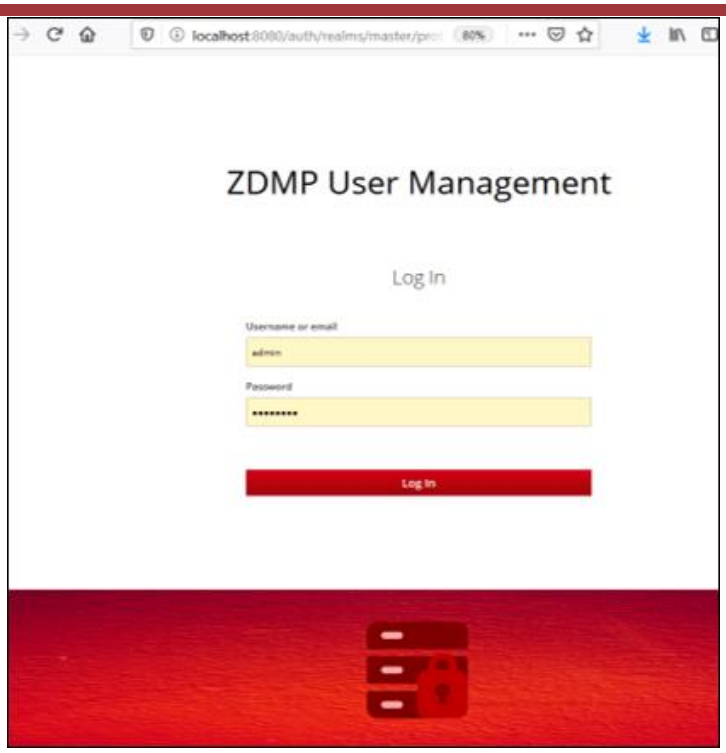
This will deploy three docker containers in the host machine where the `docker-compose up -d` command was launched.

1.6 How to use

After installation, the Authentication and Authorisation service UI is available at: http://localhost:8080/auth. The browser would render the following page:



Click on the “Administration console”, which will redirect to the admin login form:



The credentials to access the administration console are the following:

- Username: admin
- Password: Pa55w0rd

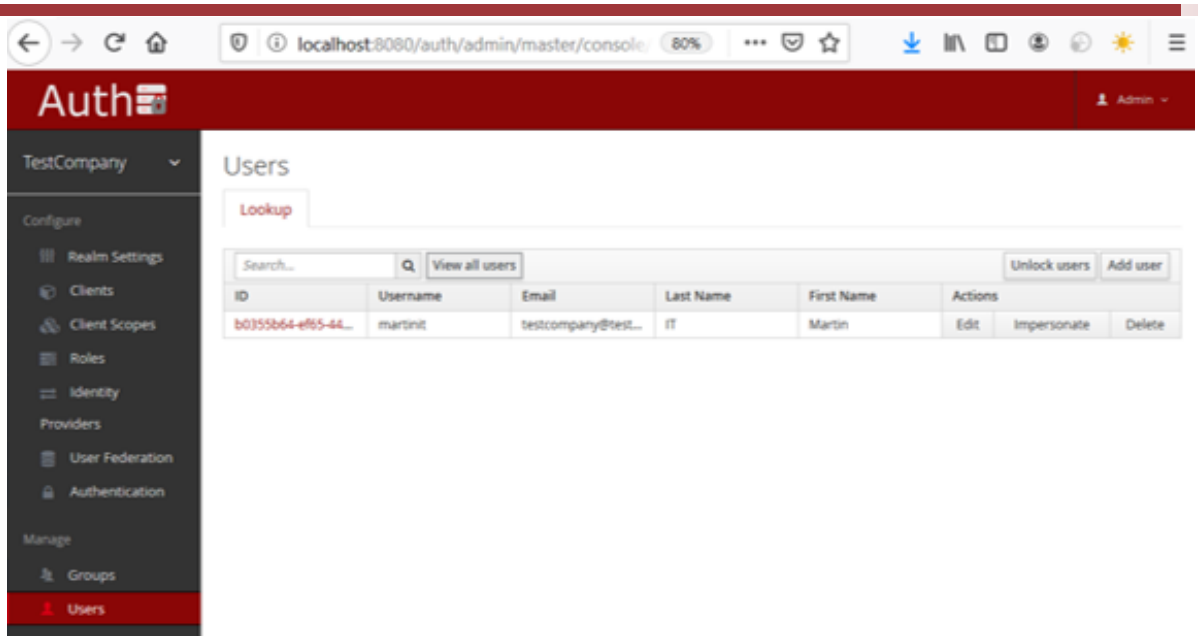
These credentials are intended to be used by the IT administrator deploying the component, ie an IT administrator of a supplier company. Herein, the IT administrator can have access/view to all its client's organizations.

By default, the Authentication and Authorisation component is initialized with a fictitious company named "testCompany" so that supplier IT administrator can evaluate what the component offers. Afterwards, the supplier company's clients, can create organizations from the portal, which will programmatically create a "realm" for that client in the Authentication and Authorisation component.

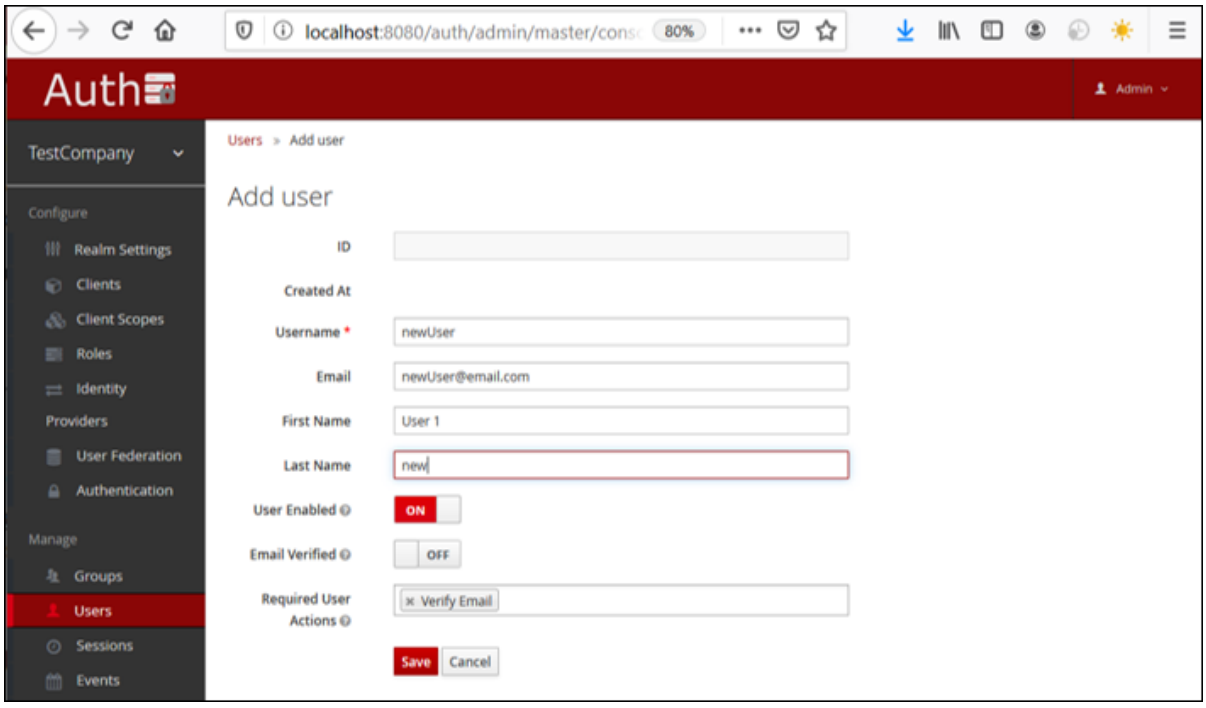
1.6.1 Manage users

The Authentication and Authorization component allows the creation of users for a given organization. When an organization is created through the Portal, the IT admin of that company can access the Authentication and Authorisation component and create more users within its realm (see next).

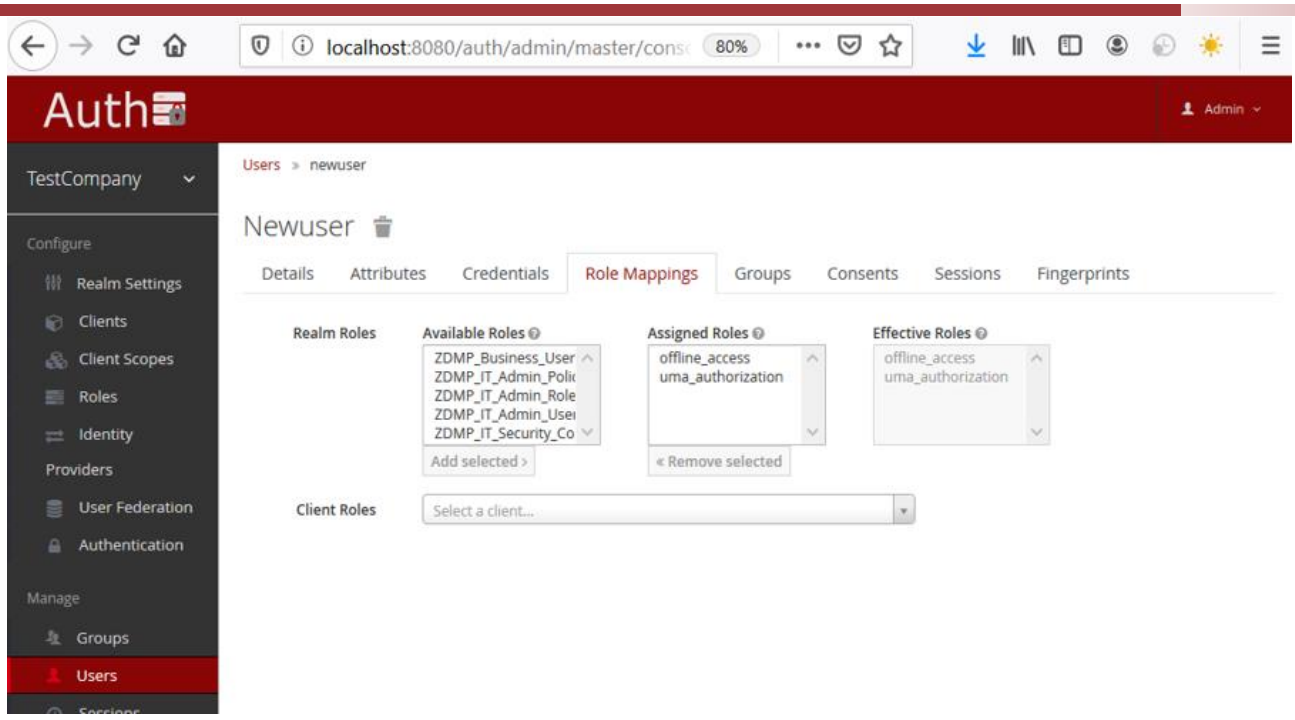
By clicking on the left menu "Users", the list of users will be displayed. Initially, there would only be one user registered: the IT administrator user who created the organization account through the portal.



The admin can create more users by clicking on the upper right button “Add user”, which will prompt the following form:

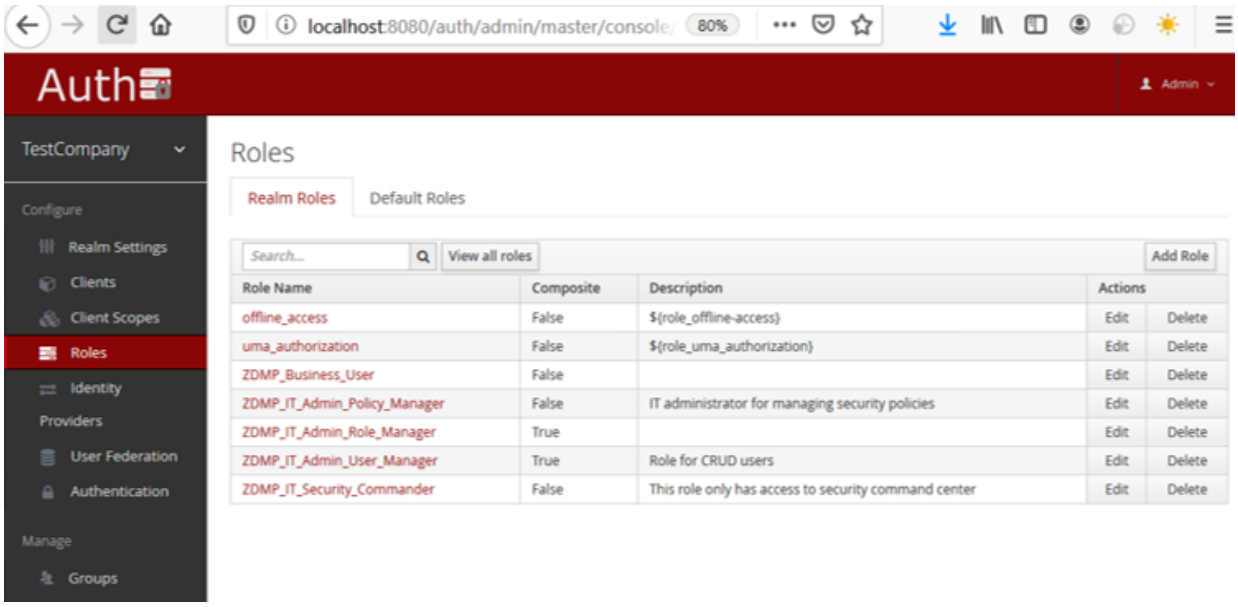


Additionally, the IT admin user can configure additional properties, such as the ZDMP roles the user is mapped to. By default, the Secure Authentication and Authorisation component comes with a set of predefined roles, so that mapping users to roles is straightforward and access to core components can be given.



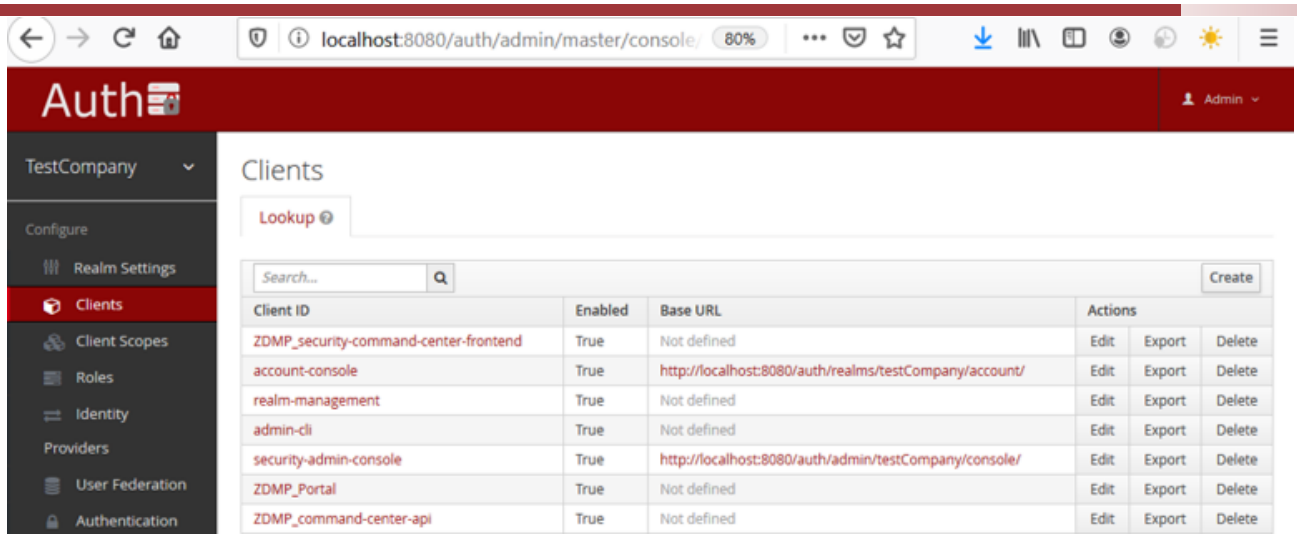
1.6.2 Manage roles

If more roles are needed (to manage access control to resource) the Authentication and Authorisation component provides forms to create them. These can later be mapped to users as already shown.



1.6.3 Manage clients/applications

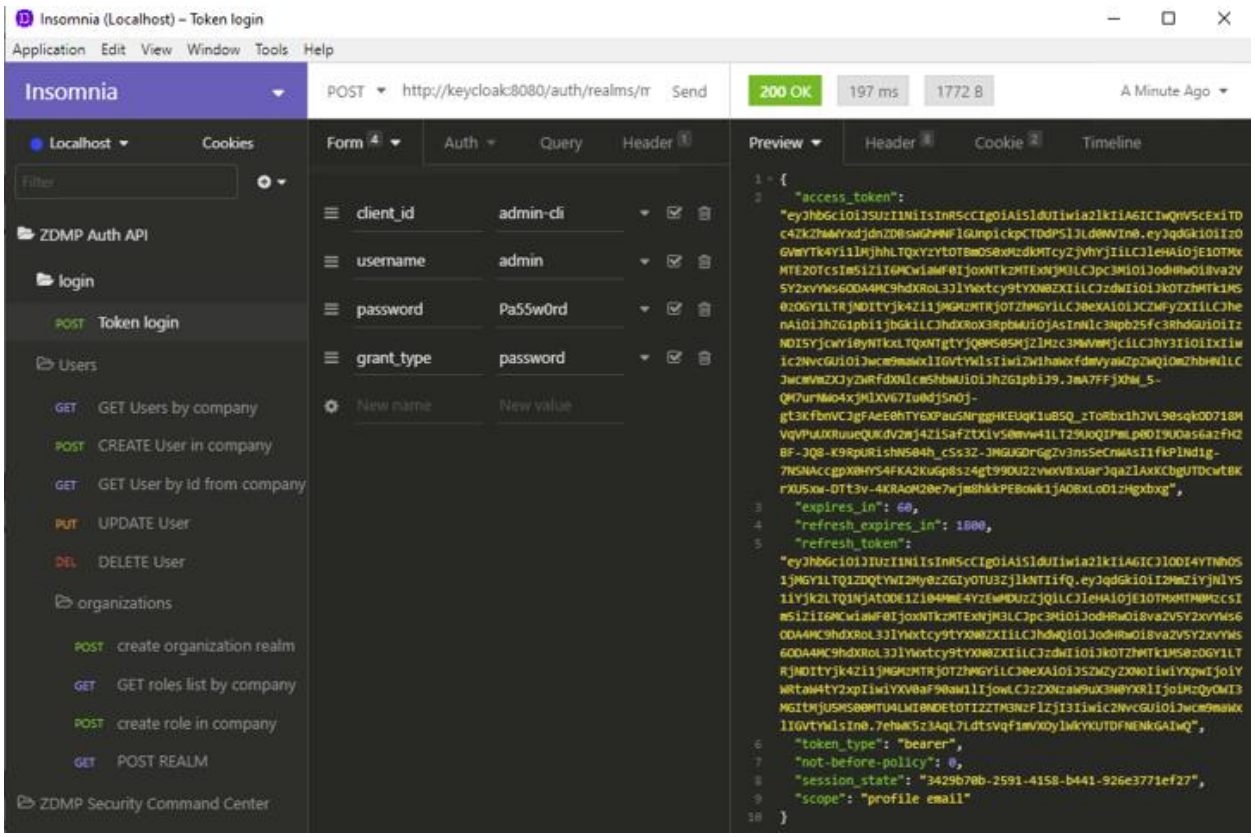
By default, on company account creation, there are already a set of ZDMP applications registered in the Secure Authentication and Authorisation component (eg ZDMP portal, ZDMP Marketplace), as shown in the image below. Eventually more clients/application will be listed, eg when zApps are installed into the company a new entry will appear in the list below.



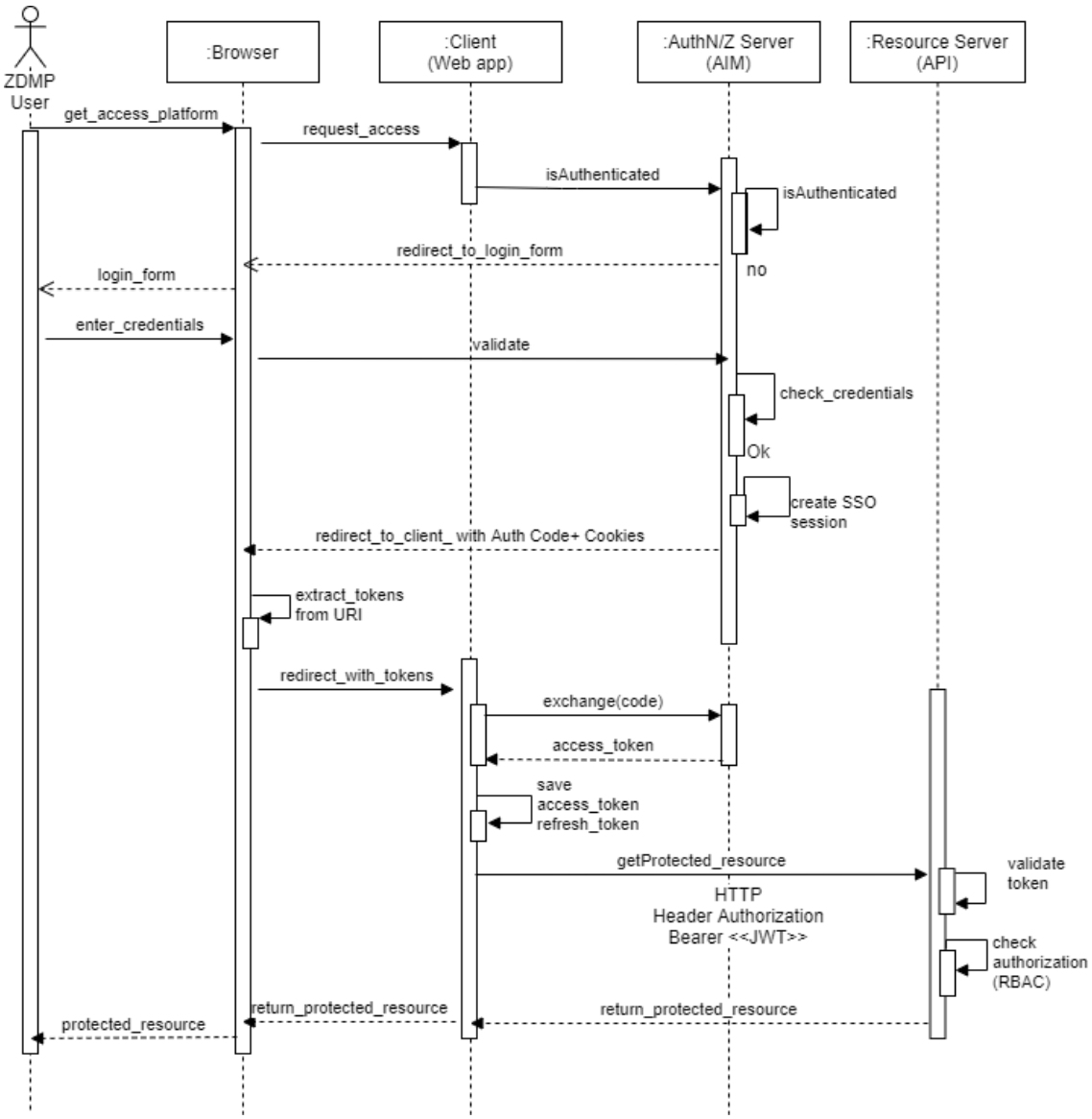
1.6.4 Interface to Authentication and Authorization module

Other ZDMP components can programmatically access the Secure Authentication and Authorisation component, for both authentication and authorisation purposes, as well as, to crud users, roles, security policies. To this end the component provides a REST API interface.

An Insomnia collection that groups every API call is provided, which can be used to test each endpoint separately. The collection assumes the user runs the Docker Compose file in localhost (if not, it can be performed by editing the calls with the correct URL) Link. After importing the file to Insomnia, the flowing endpoints will be loaded, which can later be executed:



The first API endpoint “token login” can be used to generate a valid access token for authentication purposes (see in the image above left right “access token”). Once the token is generated, it can later be used for authorization to protected resources by embedding it into the “Authorization” HTTP Header, following the OAuth 2.0 flow as defined in the following diagram:



1.7 Functional Requirements Implementation Status (M18)

The actual implementation status vis-à-vis the functional requirements implementation at M18 is provided in the annex of the D006 Technical Management Overview Report. This represents the general software status of the project and this WP/Task including information on commits and WP5-8 Risks and mitigations. Below is shown a dummy example for a security component.

Functional requirement	Description	Status	Progress	Comments
T52A013 - Issue New certificates	New client certificates are created. These certificates include the details that permit the identification of the subject (physical device, gateway or server).	Working	90%	Beta version, requires integration API with security command centre for credentials tokenization

2 Component: Secure Communication

2.1 General Description

The Secure Communication component installs, issues, and revokes digital certificates, which are strictly necessary to securely exchange information between ZDMP assets and external resources. From the Security Command Centre UI, the administrator can revoke, renew, and install certificates.

This component includes a Certification Authority (CA) and a Registration Authority (RA). These are the core of this component and is responsible for issuing/revoking certificates and matching identities with certificates, respectively.

Resource	Location
Source Code	Link
Latest Release (v1.0.0)	Download
Open API Spec	Link
Video	Coming soon

The date of generation of this component content is: 2020-06-26

2.2 Architecture Diagram

The following diagram shows the position of this component in the ZDMP architecture.

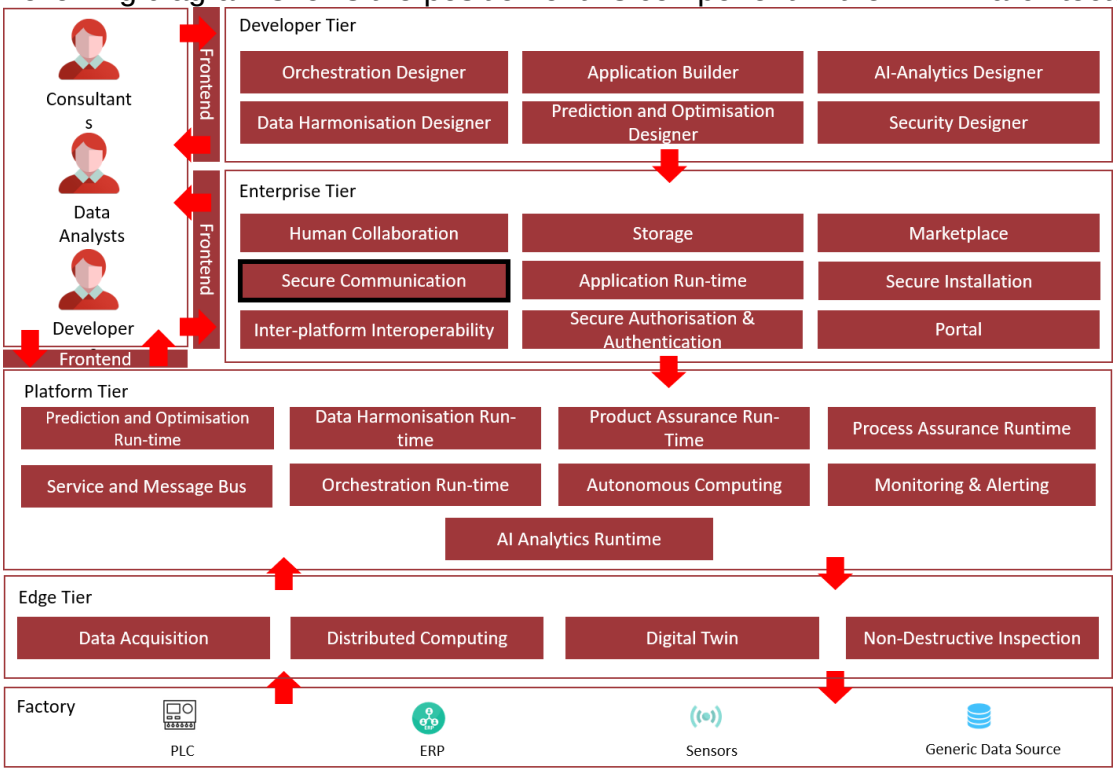


Figure 2: Position of Component in ZDMP Architecture

2.3 Features

This component offers the following features:

- **Retrieve certificates**: Recover details (status) of a given certificate
- **Certificate issuer**: Enable T5.2 Authentication & Authorization to request new certificates for new users managed by the Security Command Centre
- **Certificate download**: To download generated certificates in different formats. This will enable the user to download the certificate on demand, directly, given correct credentials
- **Server Certificate issuer**: Request an installed CA to create and store server certificate, with different possible hash methods (initially assume sha256, other possibilities)
- **Client certificate issuer**: To request an installed CA to create and store client certificates, with different possible hash methods (initially assume sha256, other possibilities)
- **Install Certificate Authorities**: To install and manage Certificate Authorities
- **Inspect details on issued certificates**: To request a list of installed certificates and CAs with detailed information
- **Manage certificates life cycle**: To manage revoked certificates, to renew them, or add them to a CRL list

2.4 System Requirements

Minimal requirements needed:

- Computer with Docker Engine installed (tested in v19.03.8, on Windows)
- Security Command Centre

2.5 Installation

The installation of this component is done through docker commands to run docker images. The Secure Communication component can be installed via docker-compose:

1. Download the latest source code from ZDMP's GitLab repository Download
2. Unzip the folder in the desired workspace
3. Through the command line, go to the orchestration folder and run docker-compose command as follows:

```
zdmpadmin@localhost: cd t5.2-secure-communication-master/orchestration
zdmpadmin@localhost:~$ docker-compose up -d
```

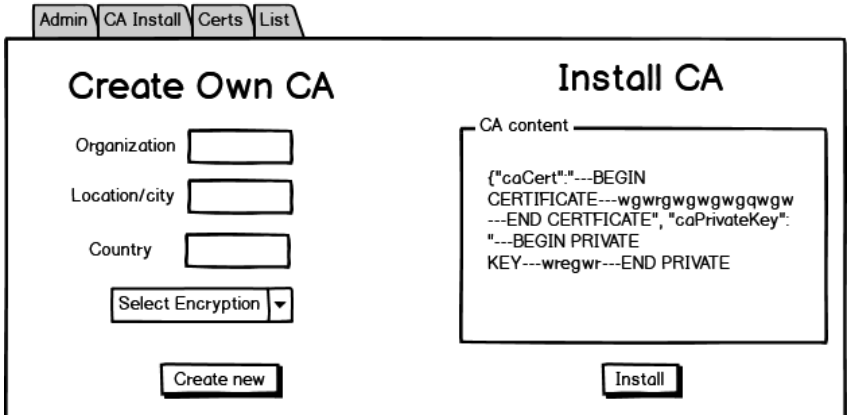
This will deploy three docker containers in the host machine where the `docker-compose up -d` command was launched.

2.6 How to use

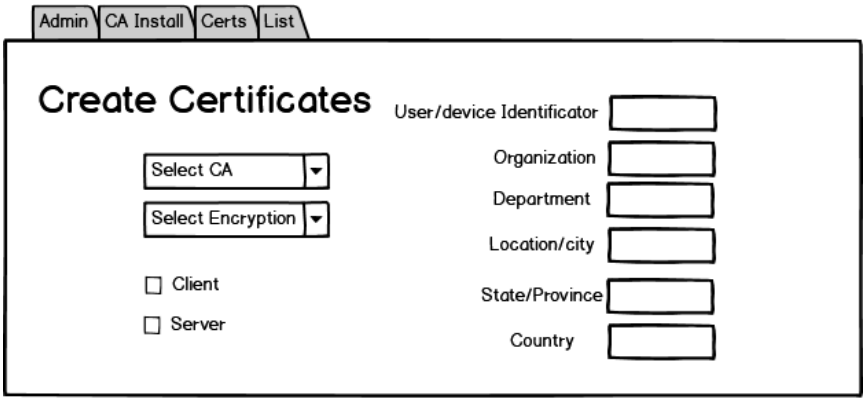
The final usage of this component is envisaged to be through the UI of the Security Command Centre. Nevertheless a POSTMAN collection is provided, which groups every API call to be tested unitarily, given the user has deployed the Docker Compose file in localhost (if not, it can be performed by editing the calls with the correct URL).

Although the backend functionality of the Security Communication component is implemented, currently, the Command Centre does not yet implement the required forms to interact with the Security Communication component. Nevertheless, there are some sketches that illustrate the functionality the Security command Centre will provide to IT administrators.

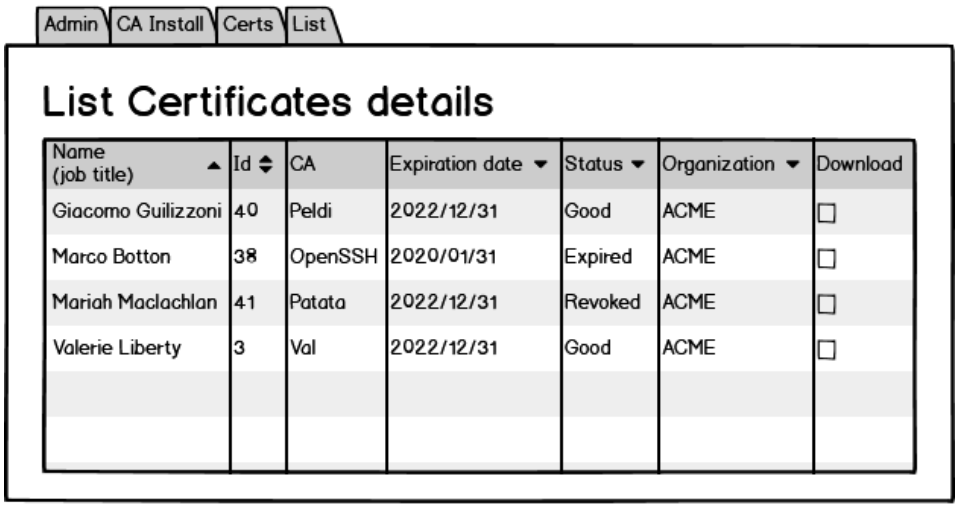
IT administrators will be able to install a Certificate Authority (CA) through the Security Command Centre UI by providing the CA content and filling additional parameters such as the encryption algorithm, country, location, and organization name.



Once the CA is installed, the IT administrator can issue device certificates with the installed CA.



The IT administrator can manage certificates life cycle by revoking already issued certificates, issuing new certificates, or revoking existing ones.



2.7 Functional Requirements Implementation Status (M18)

The actual implementation status vis-à-vis the functional requirements implementation at M18 is provided in the annex of the D006 Technical Management Overview Report. This represents the general software status of the project and this WP/Task including information on commits and WP5-8 Risks and mitigations. Below is shown a dummy example for a security component.

Functional requirement	Description	Status	Progress	Comments
T52A013 - Issue New certificates	New client certificates are created. These certificates include the details that permit the identification of the subject (physical device, gateway or server).	Working	90%	Beta version, requires integration API with security command centre for credentials tokenization

3 Component: Secure Installation

3.1 General Description

The Secure Installation component provides means to securely install applications on the ZDMP platform. This component acts on behalf on the user when they request an installation of a zApp through the ZDMP Marketplace (the trustworthy Marketplace developed for hosting zApps). It allows a secure downloading process from the Marketplace, and the policies the zApp is requesting (eg access to databases). A given zApp is not directly installed in the ZDMP platform unless it passes the review of the IT administrator. By leveraging the Security Command Centre UI, the IT Administrator can then accept or reject the policies a given zApp is requesting. Once approved, the IT administrator can then install the zApp (deploying it into the Application Runtime). Additionally, through the Security Command Centre UI the IT administrator can install a Certificate Authority (CA), as well as issue client certificate for any of the installed CAs.

Resource	Location
Source Code	Link
Latest Release (v1.0.0)	Download
X Open API Spec	Link
Video	Coming soon

The date of generation of this component content is: 2020-06-26

3.2 Architecture Diagram

The following diagram shows the position of this component in the ZDMP architecture

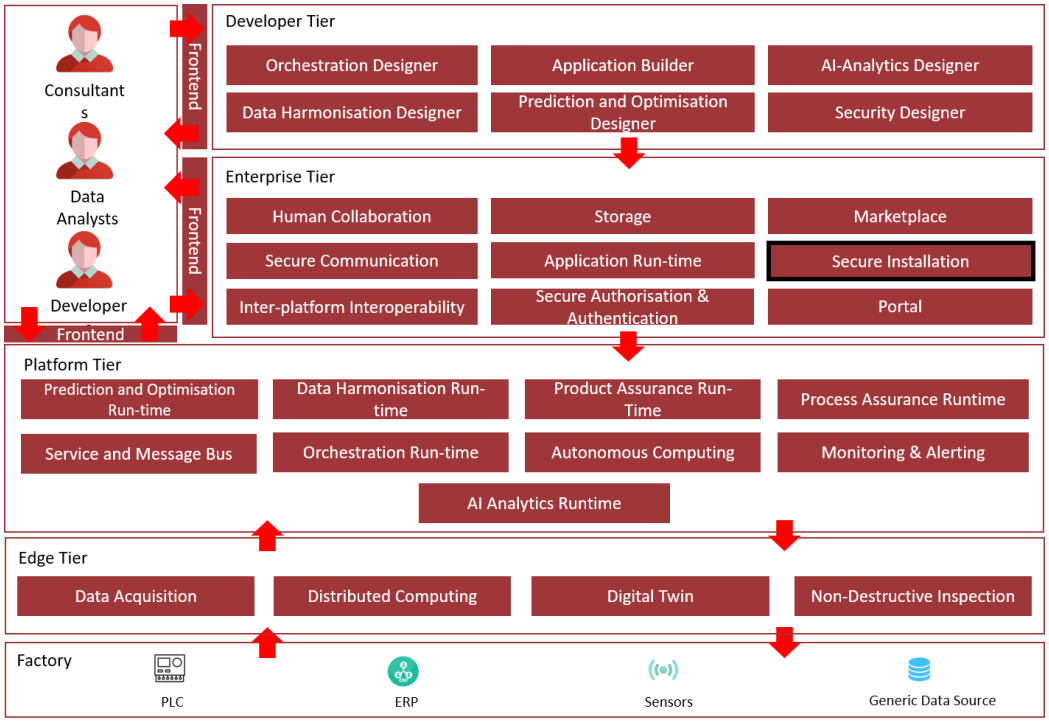


Figure 3: Position of Component in ZDMP Architecture

3.3 Features

The features to achieve the functionality of this component are itemised below and eplained there after:

- Security Command Centre
- Installation Broker

3.3.1 Security Command Centre

The Security Command Centre is the main subcomponent of the security component architecture. It provides the following features:

- **Security policies creation**: Security policies can be created/reviewed in this GUI. This process is conducted each time that a new zApp is approved for installation, so that its access permissions are well established
- **User policies creation**: Security administrators can register and edit roles for users and zApps that permit access to ZDMP resources (eg to the storage component) in this GUI
- **Security certificates control**: In this function, the installation of new root certificates and the revocation of user certificates can be done. These actions are critical to keep the ZDMP platform secure and can be triggered either manually by a security administrator

3.3.2 Installation Broker

The Installation Broker Service is the module that supports the Security Command Centre in the downloading and installation of a new zApp. It provides the following features:

- **ZApps download**: Users request the Installation Broker Service the download of the zApp package through the Secure Installation API. Then, the broker contacts the Marketplace and gets the corresponding zApp package
- **ZApps verification**: The Installation Broker Service conducts the security checks, such the manifest signature verification, on the downloaded zApp package
- **ZApp permissions creation**: When the security checks are successful, the Installation Broker Service requests the Security Command Centre to create relationships between the user, the zApp and the required permissions

3.4 System Requirements

Minimal requirements needed:

- Computer with Docker Engine installed (tested in v19.03.8, on Windows)
- The average resources needed to run this component are: 2 CPUs, 2GB memory and 10GB free space on disk

3.5 Installation

The installation of this component is done through docker commands to run docker images. The Secure Installation component can be installed via docker-compose:

1. Download the latest source code from ZDMP's GitLab repository Download
2. Unzip the folder in the desired workspace
3. Through the command line, go to the orchestration folder and run docker-compose command as follows:

```
zdmpadmin@localhost: cd t5.2-secure-installation-master/orchestration
zdmpadmin@localhost:~$ docker-compose up -d
```

This will deploy three docker containers in the host machine where the `docker-compose up -d` command was launched.

3.6 How to use

The insights on how to use this component are itemised below and explained there after:

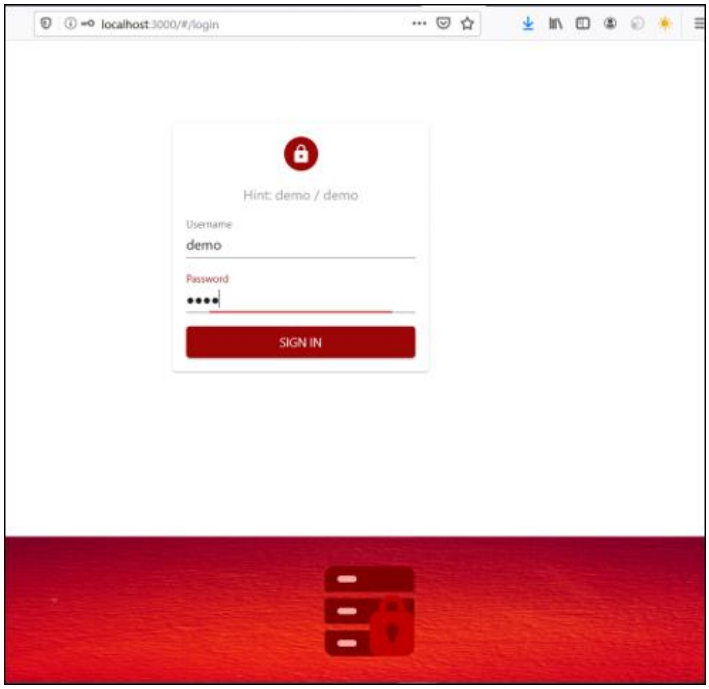
- Access to the Security Command Centre UI
- Retrieving zApp Installation Requests
- Reviewing zApp Policies
- zApp Manifest

3.6.1 Access to the Security Command Centre UI

Once subsystems are launched the Security Command Centre UI can be accessed at http://localhost:3000 The browser would render the following login page:

The credentials to access the Security Command Centre are the followings:

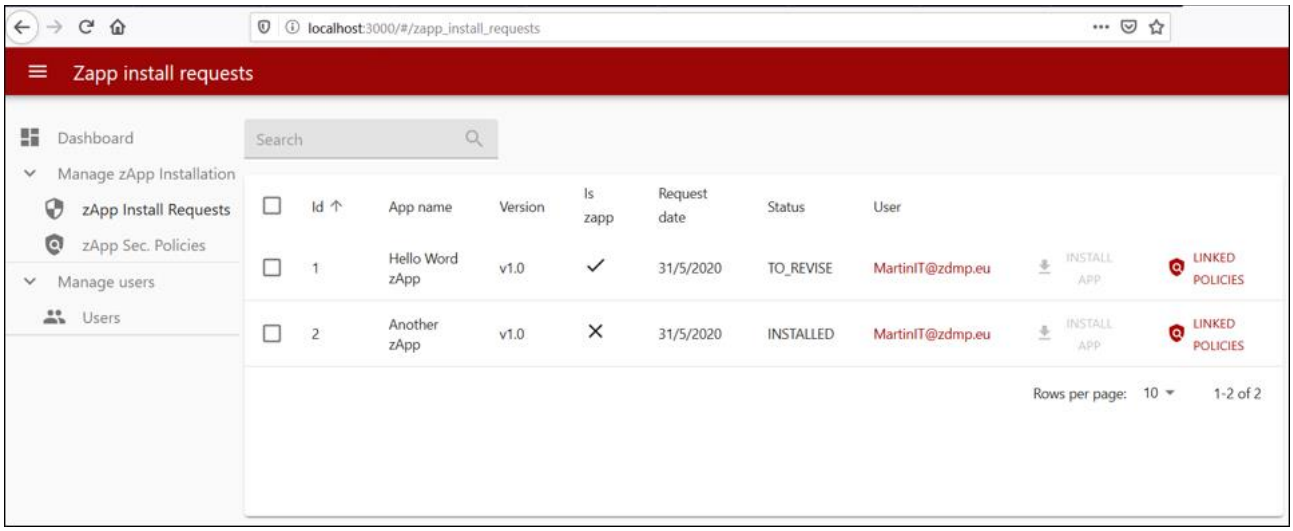
- Username: demo
- Password: demo



3.6.2 Retrieving zApp installation requests

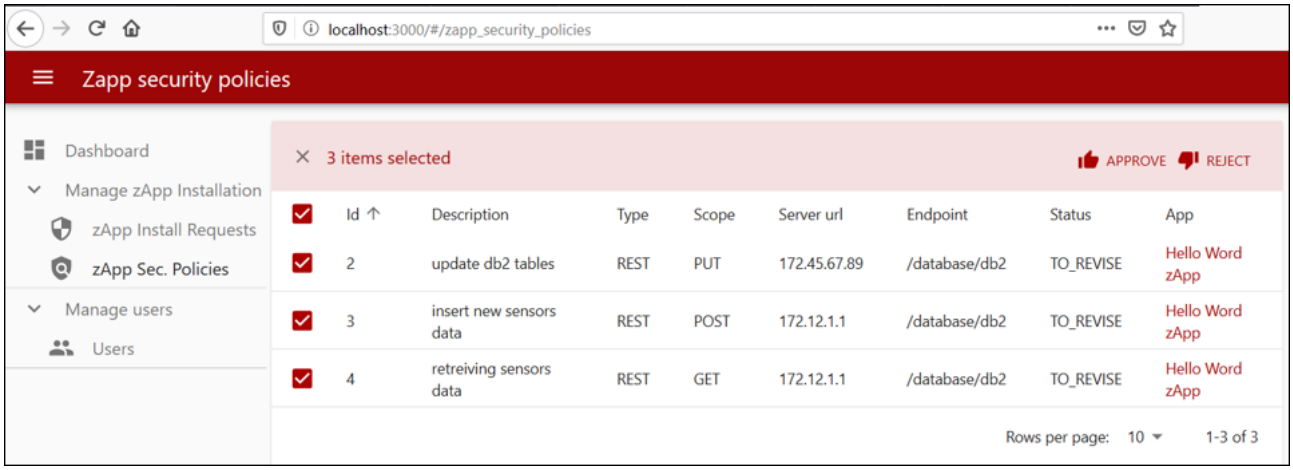
Once logged-in, the zApp installation requests list can be viewed clicking on the left menu “zApp Install Requests”.

Here the IT administrator can view the zApps already installed (status is *INSTALLED*), and can also inspect which have been requested to be installed, but are pending to revise (status is *TO_REVISE*).



3.6.3 Reviewing zApp policies

The IT admin can review the list of policies that a given zApp is requesting either by clicking on “Linked policies” from the zApp Install Requests table, or by accessing the left menu item “zApp Policies”. Here the IT admin can go one by one reviewing the requested policy and accept or deny them. Once all the policies are reviewed (no one remains in a status *TO_REVISE*), the IT administrator can go back to zApp installation request panel and click on “Install App” button. This action calls to the Application Runtime component so that it can deploy the zApp.



3.6.4 zApp Manifest

To standardize the specification of a zApp, and to ease integration between the ZDMP components that allow installing zApps, the concept of manifest has been introduced. The manifest defines every aspect of a zApp to allow its security inspections and its later installation and deployment. Below is an example of a manifest file in JSON format.

```
{
  "zdmp": true,
  "author": "authorName",
  "name": "zApp",
  "description": "a sample zApp",
  "dependencies": [
    "supportApp",
    "bestLibrary",
    "storageMongo"
  ],
  "binaryFile": "bestapp",
  "frontendUri": "/web/index.html",
  "restUri": "/api/",
  "backendUri": "/web/backend.html",
  "configurationUri": "/web/settings.html",
  "iconHDUri": "/web/icon.png",
  "processEndpoints": [
    " "
  ],
  "securityPermissions": [
    {
      "type": "REST",
      "policy_name": "getting storage data"
      "server": "http://server.url.eu",
      "URI": "/api/v1/storage/a",
      "scope": "GET"
    },
    {
    "type": "MESSAGING",
    "policy_name": "publishing in queue topic",
    "topic": "/device/1/do",
    "action": "pub",
    }
  ],
"compose.0.socket": "true",
  "compose.1.serviceName": "myDB",
  "compose.1.image": "apache/couchdb",
  "compose.1.environment.COUCHDB": "http://myDB/db/api",
  "compose.1.environment.COUCHUSER": "dbUser",
  "compose.1.environment.COUCHPASS": "verySecret"
}
```

A zApp manifest contains a set of metadata associated with the application, such as, its name, description, author, and zApp version. As for the security, it contains a set of security policies: these are “final resources” that a given zApp is requesting access to. Herein, the zApp states its “intention” within the ZDMP platform. This is stated as a set of

permissions that zApps request: eg App “A” requests access to the component “X” to do “Y”. In ZDMP, there are broadly two types of components types: (1) REST-full components, and (2) messaging queues (broker). Hence, the security policies would be of either type.

3.7 Functional Requirements Implementation Status (M18)

The actual implementation status vis-à-vis the functional requirements implementation at M18 is provided in the annex of the D006 Technical Management Overview Report. This represents the general software status of the project and this WP/Task including information on commits and WP5-8 Risks and mitigations. Below is shown a dummy example for a security component.

Functional requirement	Description	Status	Progress	Comments
T52A013 - Issue New certificates	New client certificates are created. These certificates include the details that permit the identification of the subject (physical device, gateway or server).	Working	90%	Beta version, requires integration API with security command centre for credentials tokenization

4 Conclusions

This deliverable is the first deliverable in the reporting series for T5.2 Robust Industrial Network Support. The deliverables for this task, and all WP5-8 tasks, are software and are of EU type “OTHER”. The software and accompanying material (eg description, instructions) is available on the ZDMP software repository which is updated dynamically. However, for EU formal reporting purposes, this brief cover document provides a formalised pointer to the downloadable software and related content.

This deliverable should read in conjunction with the D006-D020 deliverables which document the software process/status for each WP/Task vs its content. This deliverable represents the status as at M18 with further living editions at M18 and M48 and an informal iteration at M24.

ZERO DEFECTS
Manufacturing
Platform
ZDMP

www.zdmp.eu