D1.6
RAMP data API 1.0
version 1.0

PUBLIC

Panagiotis Bouklis
European Dynamics S.A.
209, Kifissias Av. & Arkadiou Str.
15124 Maroussi
Athens, Greece

panagiotis.bouklis@eurodyn.com
+30 210 8094500

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 951813.

Project acronym Better Factory	**Project title** Grow your manufacturing business		**Grant agreement No.** 951813
Deliverable No. D6	**Deliverable title** RAMP data API 1.0		**Version** 1.0
Type DEMONSTRATOR	**Dissemination level** PUBLIC		**Due date** 31.10.2022
Lead beneficiary ED			**WP No.** 1
Main author Panagiotis Bouklis		**Reviewed by** Duc Ta	
Accepted by Project Coordinator Päivi Mikkonen		**Accepted by Technical Coordinator** Ali Muhammad	
Contributing author(s)			**Pages** 22
VTT archive code VTT-R-01382-20		**Lead beneficiary archive code**	

Abstract

Better Factory task "T3.1 Access to cloud infrastructure" aims to offer services that will allow Manufacturing SMEs to use applications and cloud data without the need of local infrastructure and in-house IT expertise. Likewise, technology providers can offer applications on the RAMP cloud without the need of dedicated infrastructure. A secure API allows the use of only authorized 3rd-party applications addressing security concerns of users.

The implementation elements that materialize the cloud access service of RAMP is described in this document.

Project Coordinator contact
Päivi Mikkonen
VTT Technical Research Centre of Finland Ltd
Visiokatu 4, PL 1300, 33101 Tampere, Finland
E-mail: paivi.mikkonen@vtt.fi
Tel: +358 40 820 6139

Technical Coordinator contact
Ali Muhammad
European Dynamics SA
E-mail: ali.muhammad@eurodyn.com
Tel: +358 400 560 851

Notification

The use of the name of any authors or organization in advertising or publication in part of this report is only permissible with written authorisation from the VTT Technical Research Centre of Finland Ltd.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951813

HISTORY OF CHANGES

Date	Version	Author	Comments
10/01/2023	**1.0**	**Panagiotis Bouklis**	**Version 1.0**

TABLE OF CONTENT

EXECUTIVE SUMMARY

RAMP, the Robotics and Automation marketplace, aims to accelerate production in manufacturing SMEs, by facilitating access to automation and digitization technologies. While RAMP aims to offer a wide spectrum of different services, enabling access to the cloud is one of the objectives that go beyond the current state-of-the-art and transition into the true 'Connected Factories' concept.

The main aim of the cloud access for RAMP is to allow data and application use on the cloud, without the need for on-premise infrastructure, application and database maintenance, and is a part of whole composite RAMP offering (Figure 1).

Access to cloud is enabled by utilizing 3 elements:

- RAMP IoT platform: the RAMP IoT platform which provides mainly a) the FIWARE Orion Context Broker as a message broker, b) QuantumLeap, as an adapter for the persistent storage of data that pass through the FIWARE Orion Context Broker, c) any other adapters needed for connecting to the specific local infrastructure (databases, devices, etc.),
- RAMP cloud broker: a cloud broker that manages the communication between the cloud applications, but also with the local part (RAMP IoT platform deployed on premises), and
- Data storage (on RAMP): cloud data storage for manufacturers and cloud applications.

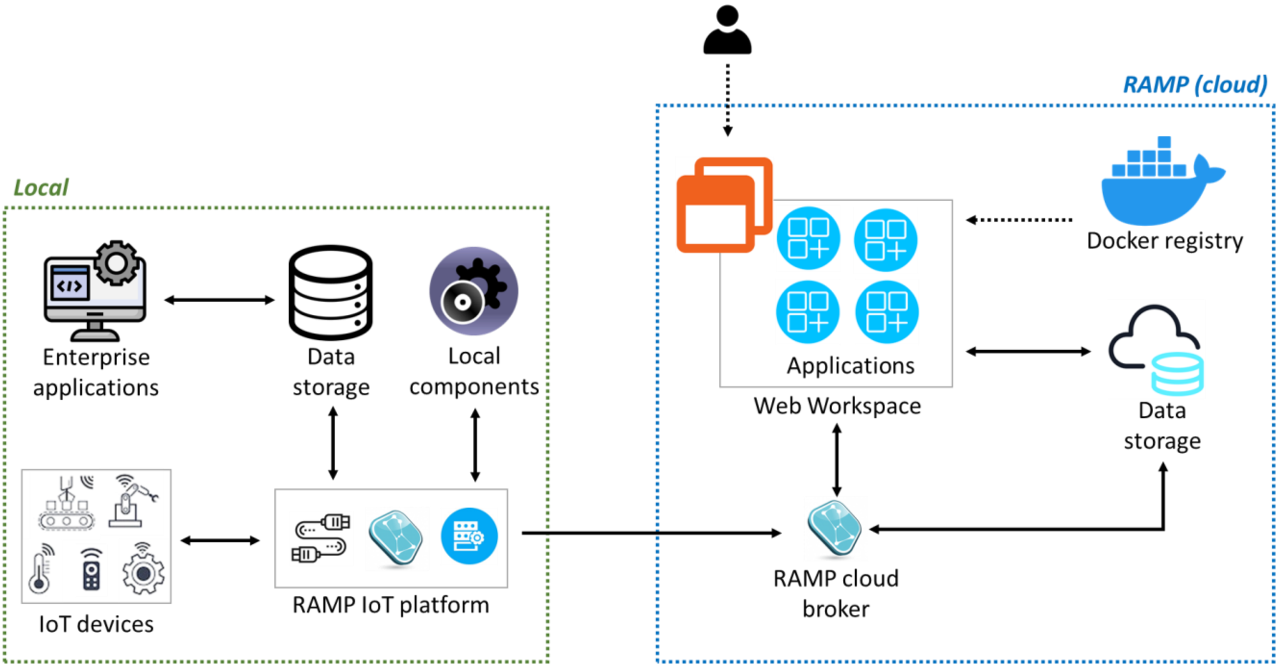


Figure 1: Composite RAMP offering.

1 Introduction

1.1 Scope and purpose of this document

RAMP, the Robotics and Automation marketplace, aims to accelerate production in manufacturing SMEs, by facilitating access to automation and digitization technologies. While RAMP aims to offer a wide spectrum of different services, enabling access to the cloud is one of the objectives that go beyond the current state-of-the-art and transition into the true ’Connected Factories’ concept.

This document is concerned about the distinct services on RAMP that facilitate the transition of manufacturing SMEs on the cloud, and how this is enabled by the RAMP infrastructure and accompanying software, more specifically the RAMP IoT platform, the RAMP cloud broker and the RAMP cloud storage.

1.2 Objective

Better Factory task ”T3.1 Access to cloud infrastructure” aims to offer services that will allow Manufacturing SMEs to use applications and cloud data without the need of local infrastructure and in-house IT expertise. Likewise, technology providers can offer applications on the RAMP cloud without the need of dedicated infrastructure. A secure API allows the use of only authorised 3rd-party applications addressing security concerns of users.

1.3 Document structure

Chapter 1introduces the document.

Chapter 2 elaborates the specification of the system of enabling the access to cloud for the Manufacturing SMEs.

Chapter 3 demonstrates the current status of the API.

Chapter 4 concludes the document, with the current status and the follow up.

2 System specification

2.1 Background and scope

The main aim of the cloud access for RAMP is to allow data and application use on the cloud, without the need for on-premise infrastructure, application and database maintenance. This is closely linked to the RAMP Collaboration space, which practically is the user perspective in accessing these services, and is part of an overall offering in RAMP, depicted in Figure 2.

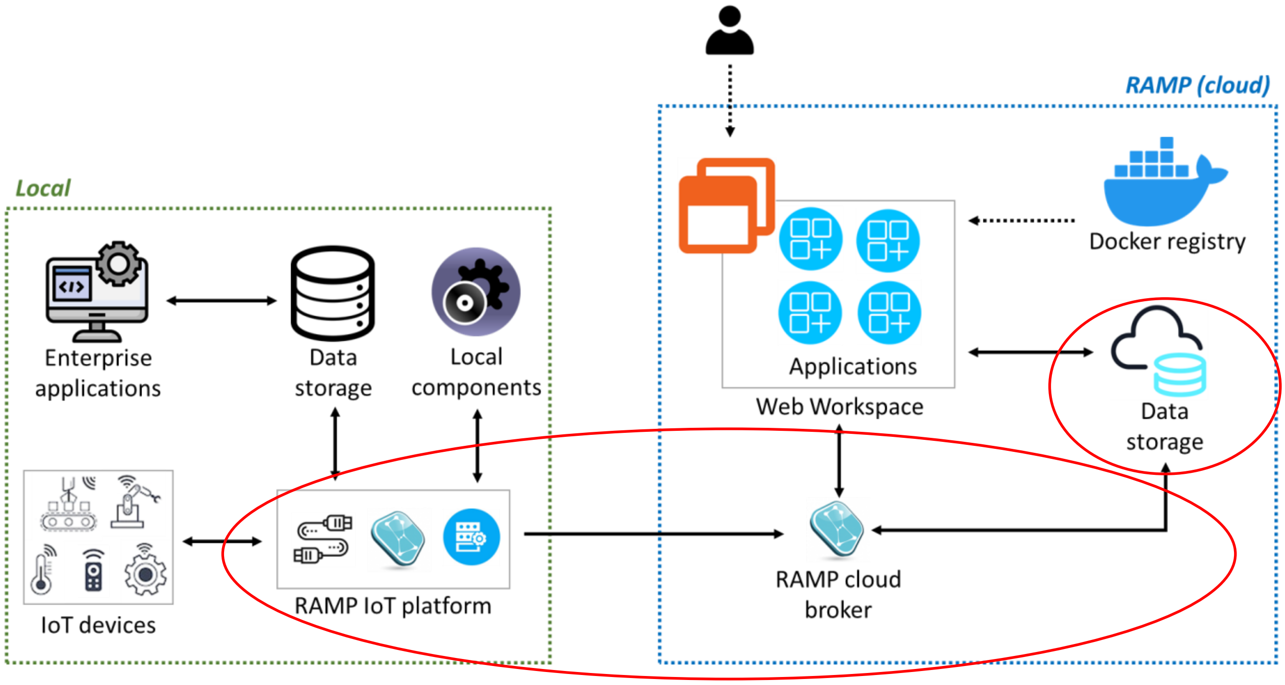


Figure 2: Composite RAMP offering.

The composite RAMP offering consists of several different tools:

- A local part, intended to be deployed on the premises of the manufacturer, which consists of:
  - Enterprise applications: the applications that the manufacturer has already in place, and may continue to use.
  - Data storage: local database that is already used by the manufacturer, and may be utilised for additional data that the local installation of the RAMP IoT platform may require.
  - Local components: any components (e.g., APPS) that the user acquires through RAMP and are deployed locally.
  - RAMP IoT platform: the RAMP IoT platform which provides mainly a) the FIWARE Orion Context Broker as a message broker, b) QuantumLeap, as an adapter for the persistent storage of data that pass through the FIWARE Orion Context Broker, c) any other adapters needed for connecting to the specific local infrastructure (databases, devices, etc.)
  - IoT devices: local devices, like sensors, machinery, robots, that are connected to the RAMP IoT platform through the FIWARE Orion Context Broker.
- The RAMP-cloud part, which consists of:
  - Web Workspace: a desktop-like web environment that integrates the use of different web-based tools under a common user interface providing a seamless user experience.
  - Docker registry: a registry for storing and deploying docker images, public and private.
  - Data storage: cloud data storage for manufacturers and cloud applications.
  - RAMP cloud broker: a cloud broker that manages the communication between the cloud applications, but also with the local part (RAMP IoT platform deployed on premises).

It should be noted that the above-mentioned solution is not meant to be used only as a whole, but can be utilised partially, depending on the user case and the desired applications that are needed per user.

While the above are summarised for a better understanding of the overall RAMP solution, this document focuses on the how the cloud access is offered, with a focus on the Manufacturing SME users. The cloud access service is materialised by a part of the above-mentioned elements:

- RAMP IoT platform
- RAMP cloud broker
- Data storage (on RAMP)

The service to offer cloud data storage on RAMP was based on the experience gained from the Better Factory experiments. In the experiments, it was decided that the data will remain on-premise, as it is expected that Manufacturing SMEs would be more willing to adopt the RAMP solutions if the data is not stored out of the factory. However, this posed the following difficulties in the adoption potential, which are targeted to be :

- The Manufacturing SME needs to connect the RAMP IoT platform with a database. While the RAMP IoT platform has packaged a Crate database and the QuantumLeap component that transfers data from the broker to the database, the configuration was not always straightforward for the SMEs.
- Defining the database schema was not always straightforward for the Manufacturing SMEs. Despite the fact that database setting up and maintenance is a common activity in modern industry, Manufacturing SMEs lack the in-house expertise to take care of this task.
- Network and firewall access (opening ports to RAMP servers) is needed for each application that needs data, while data access is not properly managed and logged across the different applications.

2.2 Objectives

The system aims to enable the following services that are related to access to cloud infrastructure for the Manufacturing SMEs:

1. Connect factory IoT agents with RAMP cloud applications,
2. Store factory data on the RAMP cloud,
3. Give access to the cloud-stored data to different cloud applications, offered in the RAMP co-creation space,

These services are inter-depedent as follows:

1. Service (1) may be offered indepedently,
2. Service (2) requires service (1),
3. Service (3) requires service (3) (and consequently, service (1) as well)

2.3 Modes of operation

As previously mentioned, the services are materialised by the RAMP IoT platform, RAMP cloud broker, Data storage and docker registry. Depending on the service, these elements are utilised as explained in the following paragraphs.

2.3.1 Connect factory to RAMP

Connecting the factory to RAMP is the core service of the access to cloud offering and it means connecting the local IoT agents to RAMP. Once the data is transmitted from on-premise to RAMP it can be used for two reasons: 1) For being consumed by cloud applications on the RAMP cocreation space, or/and 2) Being stored on the RAMP cloud data storage.

The ’RAMP IoT platform’ and the ’RAMP cloud broker’ are needed for this service. Both of these are based on the FIWARE Orion Context Broker[1] for enabling the connection between the factory and the RAMP cloud. The RAMP IoT platform needs to be installed on the factory premises, and IoT agents, like sensors, local applications, etc., need to be connected. The ’RAMP cloud broker’ is installed on the cloud by RAMP.

[1] https://fiware-orion.readthedocs.io/

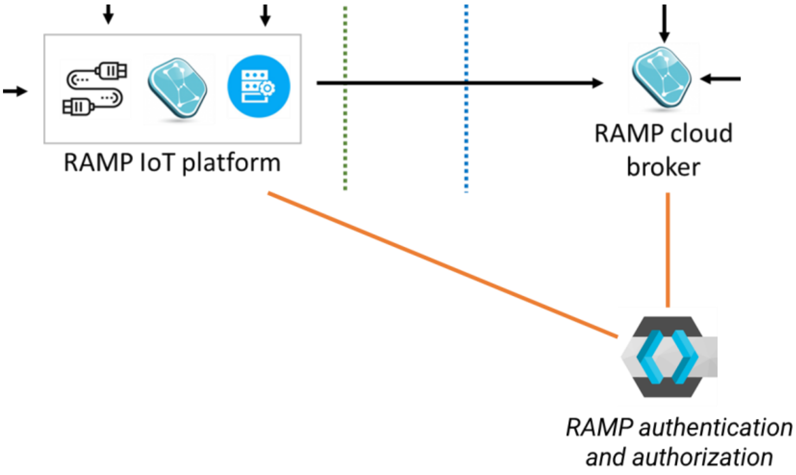


Figure 3: RAMP IoT platform is a 'Context Provider' to the RAMP cloud broker.

The RAMP IoT broker plays the role of the ’Context provider’ to the RAMP cloud broker. This has the following benefits:

- RAMP IoT platform can still operate its functions at local level, if for any reason it gets disconnected by the RAMP cloud.
- RAMP cloud broker can be used with multitenancy features, hence being ready as infrastructure to enable sharing context and data across different organisations, factories and service and technology providers.
- Use of network bandwidth is minimised as much as possible:
  - Data that is produced and consumed locally is brokered by the RAMP IoT platform, with no data transmission over the internet.
  - Data that has been previously stored on the cloud data storage, or is produced by cloud applications and needs to also be consumed by another cloud application is managed by the RAMP cloud broker, with no data transmission over the internet.
  - Data is transmitted over the internet only on two occasions: 1) When data needs to be stored on the cloud storage, or 2) when a local application/IoT agent produces a value that needs to be consumed by a cloud application as ’context’.

The architecture of the 2 brokers for context provision work as follows[2]: if the RAMP cloud broker receives a query or update operation and it cannot find the targeted context element on the cloud (i.e. in its internal database) but the RAMP IoT platform is registered for that context element, then the RAMP cloud broker will forward the query/update request to the RAMP IoT platform. In this case, the RAMP cloud broker acts as a pure "NGSI proxy" (i.e. doesn't cache the result of the query internally) and, from the point of view of the client (application) issuing the original request, the process is mostly transparent.

The RAMP authentication and authorisation module plays the role of the central security mechanism. This allows the 2 brokers to manage user access, while for the RAMP cloud broker, it also allows multitenancy features, for enabling the shared use of one broker across different organisations.

2.3.2 Cloud data storage

This service allows users to store data on the cloud. The data needs to be accessible to the RAMP cloud server. The data storage service needs to be enabled by the RAMP administrator. As the FIWARE Orion Context Broker use MongoDB as its internal database, which is a schemaless type of database, a certain level of configuration for a specific use case needs to take place.

[2] https://fiware-orion.readthedocs.io/en/1.4.0/user/context_providers/index.html

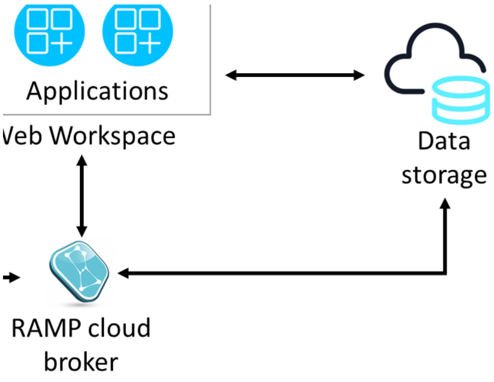


Figure 4: Data can be stored on the RAMP cloud storage once it is available on the RAMP cloud broker.

The cloud data is saved on a relational database. The service will be implemented with one of the following options:

- Crate, by utilizing the FIWARE QuantumLeap[3] component
- MySQL, by utilizing the FIWARE Draco[4] or the FIWARE Cygnus[5] component
- PostgreSQL, by utilizing the FIWARE Draco or the FIWARE Cygnus component

Storing the Data on the RAMP cloud, in a relational type database, allows also the direct use of the RAMP Dashboard for data visualization, without the need for any other configuration on-premise.

2.3.3 Access to cloud data

Access to data that is stored on the cloud refers to 2 sub-services:

1. View and fetch data that is stored on the cloud,
2. Give access to cloud data to cloud applications.

Sub-service 1 is similar to the common cloud data storage service offered in the market. Data that is stored on the RAMP cloud can be remotely viewed by the user (owner of the data) and fetched, using the common database APIs.

Sub-service 2 is the more RAMP-focused one. In this case, user can directly give access to their data that is stored on the RAMP cloud to other cloud applications that are offered through the RAMP cocreation space. Cloud applications can be either offered by RAMP, RAMP partners or 3rd-parties. More information on the cloud applications and how these can be included, integrated and used in RAMP is given in the relevant Better Factory deliverable, D2.8 SME and artists co-creation space 2.0.[6]

2.4 User classes

The following user classes, i.e., categories and subcategories of users that use the system, are identified:

- RAMP administrator
- RAMP development
- Application provider
- Solution provider
- Manufacturing SME user

2.4.1 Organisational structure

The organization of the user classes and their relationship with the co-creation space are illustrated in Figure 5.

[3] https://quantumleap.readthedocs.io/
[4] https://fiware-draco.readthedocs.io/
[5] https://fiware-cygnus.readthedocs.io/
[6] See chapter 4 ”Accessing applications and benefits”

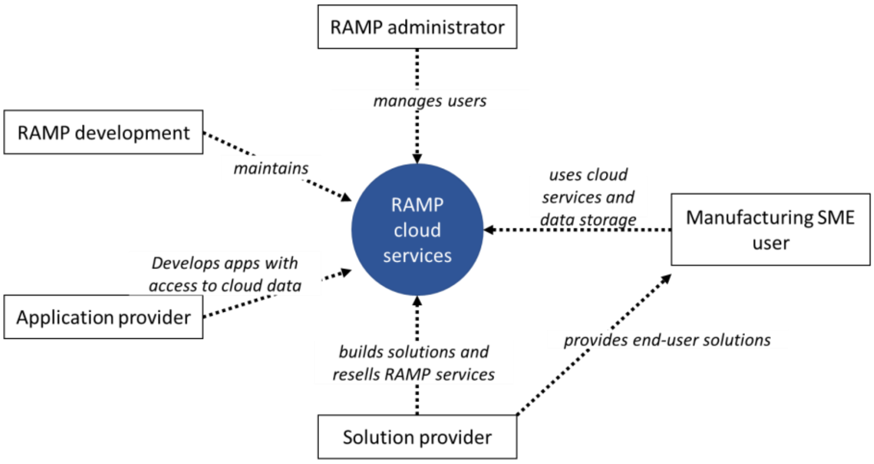

RAMP administrator
manages users
RAMP development
maintains
RAMP cloud services
uses cloud services and data storage
Manufacturing SME user
Develops apps with access to cloud data
Application provider
builds solutions and resells RAMP services
provides end-user solutions
Solution provider

Figure 5: Organisation of user classes and relationship with the RAMP cloud services.

2.4.2 Profiles of user classes

The profile of each user class, along with its subclasses, is described below:

- **RAMP administrator**: It is the administration team of RAMP. RAMP administrator manages the access of users to the different services, approves the access of applications to cloud data and the setting up of the link between the RAMP IoT platform and the RAMP cloud broker.
- **RAMP development**: RAMP development maintains the software side of the services, setups and configures cloud data storage (databases) and the RAMP cloud broker, supports application providers to make their applications able to interact with the RAMP cloud data storage, and provides technical support to users.
- **Application provider**: Develops web-based applications and makes them available on the RAMP co-creation space. These applications may be able to interact with the RAMP cloud broker and the RAMP cloud data storage.
- **Solution provider**: An organization that provides complete solutions to manufacturing SMEs, and of which solution, RAMP cloud services may be a part of.
- **Manufacturing SME user**: The end user of the RAMP cloud services, that use cloud applications or/and cloud data storage.

2.5 Support environment

In order to use the RAMP cloud services the following infrastructure is needed by the Manufacturing SME user, and also utilised by RAMP (Figure 6):

- Infrastructure and configurations required to be done by the Manufacturing SME:
  - The Manufacturing SME user has to deploy the RAMP IoT platform on premise and connect the local IoT nodes (e.g., sensors, equipment, robots, etc.) and other enteprise software that is needed to interact with the RAMP services (cloud application or/and data storage.
  - The Manufacturing SME user has to also define the data models and the entities that are part of the context. Certain data entities may be already defined by the cloud applications; in this case the Manufacturing SME user has to ensure that the data produced by its end (i.e., data produced by the local IoT agents) follows the already established data models.
  - The Manufacturing SME user also needs to ensure that the local RAMP IoT platform is accessible by the RAMP cloud broker, i.e. open firewall to allow traffic between the local network and the RAMP servers.
- Infrastructure utilised on the RAMP cloud:
  - The RAMP cloud broker is offered as-a-service. In order to connect the cloud broker to the on-premise RAMP IoT platform, certain information may be needed to be shared, like the IP of the RAMP IoT platform.
  - The RAMP cloud storage is based on database servers, and is also offered as-a-service. The configuration for using this service is done by the RAMP side – no user action is needed.

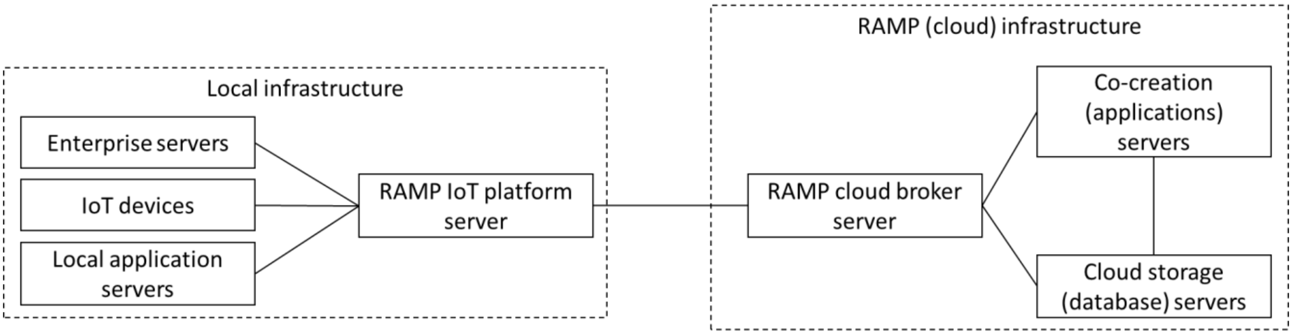

RAMP (cloud) infrastructure
Local infrastructure
Enterprise servers
IoT devices
Local application servers
RAMP IoT platform server
RAMP cloud broker server
Co-creation (applications) servers
Cloud storage (database) servers

Figure 6: Infrastructure setup for enabling the RAMP cloud services.

2.6 Benefits

Cloud data storage brings benefits that have been proven in other sectors, as well RAMP-specific benefits, such as:

- **Data security** and **disaster recovery**, not only in terms of securing data from unauthorised access and theft, but also from accidental loss, corruption or destruction. ED where RAMP servers are located, is certified with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems – Requirements) and ISO/IEC 9001:2015 (Quality management systems – Requirements), and users state-of-the-art cybersecurity tools and established processes for data management. This way Manufacturing SMEs gain access to related expertise that is not available in-house.
- **Cost efficiency**, as the Manufacturing SME does not need to purchase, setup, maintain and updated the data storage infrastructure and software.
- **Scalability**, as the Manufacturing SME user is able to scale-up and scale-down according to specific needs and avoid unnecessary investments and running costs.
- **Data sharing,** as the data is already stored on the cloud it is easy to give access to this data to other users (e.g., technology/solution providers or other partners).
- **Conveniency**, as the data is online and can be viewed by any device that is connected to the internet, with the RAMP account.
- Use of **cloud applications** is done quickly and without the need to separetely setup, configure and maintain each one of them. These are rather offered as ready-to-use by the RAMP side, and the user has only to start using the applicaton or define shared use os applications. The cloud applications need to be available in the RAMP co-creation space.

2.7 Considerations

2.7.1 Limitations

Regarding the connection of the RAMP IoT platform and the RAMP cloud broker, the setup that was chosen, i.e. RAMP IoT platform being the 'Context provider' to the RAMP cloud broker, allows only one-way context sharing. This means that context produced at the RAMP cloud side cannot be transfered to the local RAMP IoT platform, hence is not available as context. A workaround for making data available is that the application stores data on the cloud storage and this data is accessed by the local applications through the standard database API, taking into account time delays that will occur.

Another limitation is that the Manufacturing SME still has to open their firewall towards the RAMP server. While the Manufacturing SME does not need now to setup the whole data store infrastructure[7], the factory's IT department still needs to be involved and appropriate permissions have to be given at management level.

[7] This was one of the drawbacks identified during the experiments, as many Manufacturing SMEs do not have the relevant expertise in-house

2.7.2 Alternatives considered

Regarding the link between the 2 brokers (RAMP IoT platform and RAMP cloud broker) it is possible to instead of having the current setup to make the context sharing bi-directional. However, this would require that each applications is extended with a micro-service for enabling this. For easier and faster deployment, as well as to not impose additional development work on application providers, the current setup of the RAMP IoT platform being the Context Provider was selected.

Regarding the cloud data storage, during the experiments the setup of not having the data stored on the cloud at all was tested, however this was not proven to have the adoption potential that initially was expected, as described earlier in this document (see §2.1 Background and scope).

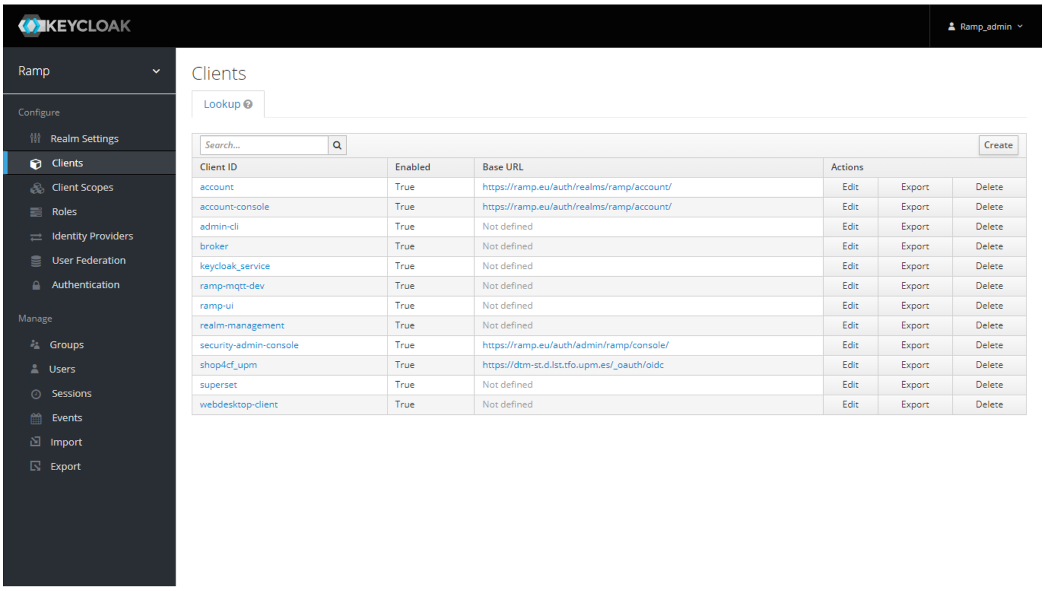
Another alternative for the cloud storage was to use a 3rd-party infrastructure provider to offer the service. This meant that while the use of the service would be transparent for the user, the physical location of the data would be at 3rd-party servers instead of the RAMP servers. While data protection can be ensured by selecting certified and GDPR-compliant infrastructure providers, as well as investigated on a set of RAMP data handling requirements, the investigation showed that the business aspect of this approach would be difficult to handle. More specifically, future pricing of this RAMP service to its users would be difficult to define, as the cost of the infrastructure itself is way too liquid and too broad based on different options that the user may need, like type of database, storage space, number of processors of the server, number of concurrent data transfer sessions, reduntancy and many others. Even a slight change in these options may generate huge differences in the infrastructure purchase cost. Additionally, another aspect that is charged high by cloud providers in such infrastructure is the network bandwidth used. Considering the load of data that factories (future RAMP customers) produced and needs to be stored, as well as the data that need to be transfered back to applications (be it RAMP applications or 3rd-party), but also the liquidity of the infratructure cost, this is not a viable option in monetary terms. Hence, it was decided that the cloud storage will be offered within the RAMP server infrastructure.

3 RAMP API guide

3.1 Introduction

This section demonstrates how 3rd-party applications gain access to the RAMP services by authenticating and hence authorising the users on their access permissions for the cloud broker and data.

The open-source authentication and authorisation component Keycloak[8] has been integrated within RAMP and is used to provide authentication to 3rd-party applications. New applications, hereforth refered as ’clients’ in respect to RAMP, can be quickly added. The RAMP administrator is able to quickly review and edit the RAMP clients (Figure 7).



Client ID	Enabled	Base URL	Actions		
account	True	https://ramp.eu/auth/realms/ramp/account/	Edit	Export	Delete
account-console	True	https://ramp.eu/auth/realms/ramp/account/	Edit	Export	Delete
admin-cli	True	Not defined	Edit	Export	Delete
broker	True	Not defined	Edit	Export	Delete
keycloak_service	True	Not defined	Edit	Export	Delete
ramp-mqtt-dev	True	Not defined	Edit	Export	Delete
ramp-ui	True	Not defined	Edit	Export	Delete
realm-management	True	Not defined	Edit	Export	Delete
security-admin-console	True	https://ramp.eu/auth/admin/ramp/console/	Edit	Export	Delete
shop4cf_upm	True	https://dtm-st.d.lst.tfo.upm.es/_oauth/oidc	Edit	Export	Delete
superset	True	Not defined	Edit	Export	Delete
webdesktop-client	True	Not defined	Edit	Export	Delete

Figure 7: List of current RAMP clients (includes internal ’clients’ from RAMP modules).

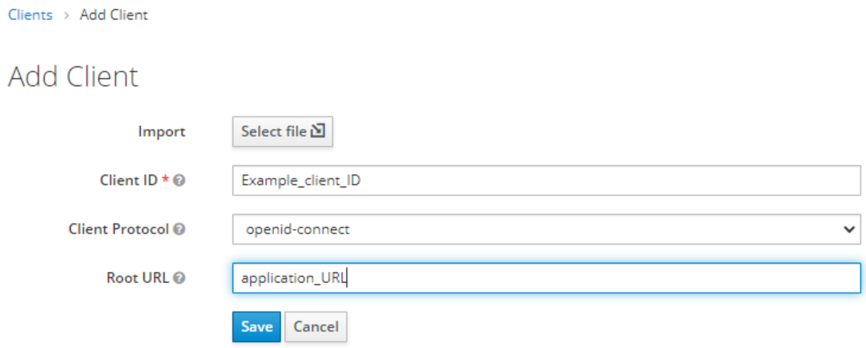
3.2 Setting up a new client

Adding and setting up a client (i.e., giving permissions to a new application to use the RAMP services) is done in the following steps:

First the basic information of the application are configured (Figure 8). These are:

- **Client ID**: A unique ID for the client.
- **Client Protocol**: ’openid-connect’ is the protocol supported by RAMP.
- **Root URL**: This is the URL where the application is located (it can be either external, or internal, i.e., a URL that is not shown, but is accessible by the RAMP servers).

[8] https://www.keycloak.org



Import

Client ID * : Example_client_ID

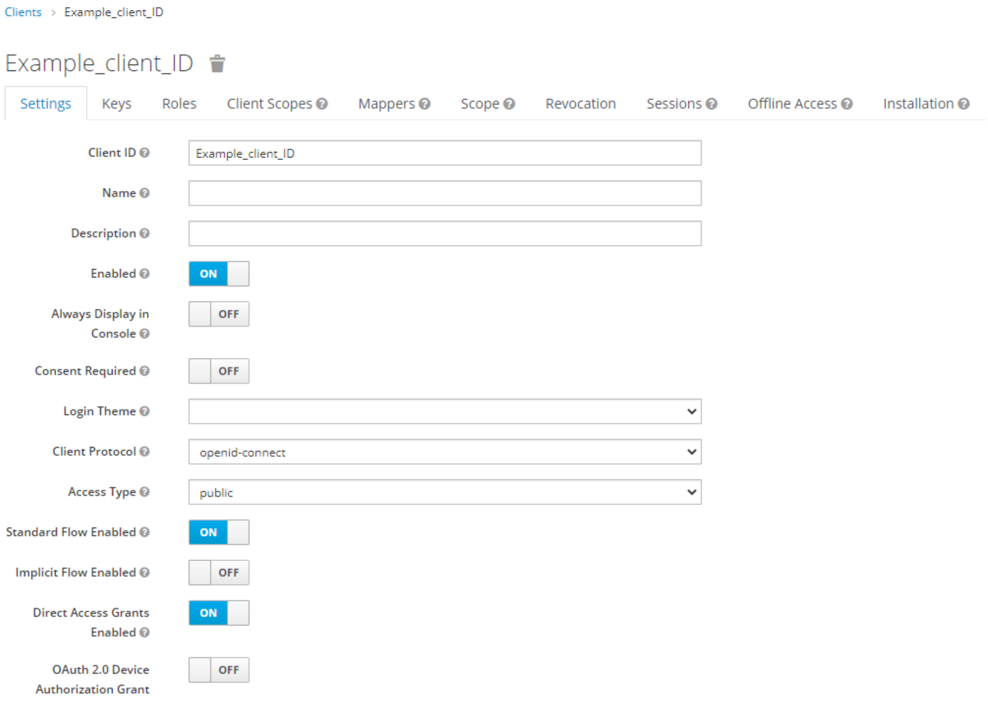
Client Protocol: openid-connect

Root URL: application_URL

Figure 8: Basic information for setting up access for a new application.

Additional settings can be defined per client (Figure 9). The most important ones for RAMP include:

- **Name**: The display name of the client.
- **Description**: The description of the client.
- **Valid Redirect URIs**: Specifies values where the user is redirected back after logging in or/and giving consent.
- **Logo URL**: The logo of the application that is displayed when user is giving consent.
- **Policy URL**: When the application processes or/and stores data with a different policy that RAMP, this allows to view the application's policy when giving consent.
- **Terms of service URL**: The terms of service of the application, to view when giving consent.
- **Backchannel Logout URL**: This is the URL that allows RAMP to force the user logout from the client.



Client ID: Example_client_ID

Name:

Description:

Enabled: ON

Always Display in Console: OFF

Consent Required: OFF

Login Theme:

Client Protocol: openid-connect

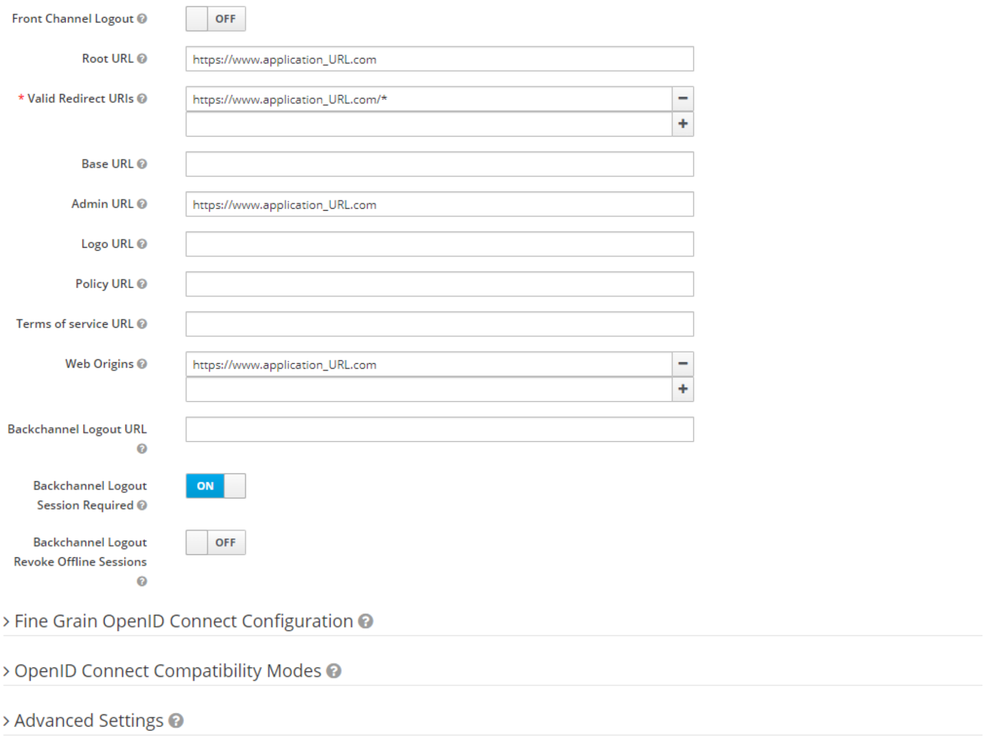
Access Type: public

Standard Flow Enabled: ON

Implicit Flow Enabled: OFF

Direct Access Grants Enabled: ON

OAuth 2.0 Device Authorization Grant: OFF



Front Channel Logout: OFF

Root URL: https://www.application_URL.com

* Valid Redirect URIs: https://www.application_URL.com/*

Base URL:

Admin URL: https://www.application_URL.com

Logo URL:

Policy URL:

Terms of service URL:

Web Origins: https://www.application_URL.com

Backchannel Logout URL:

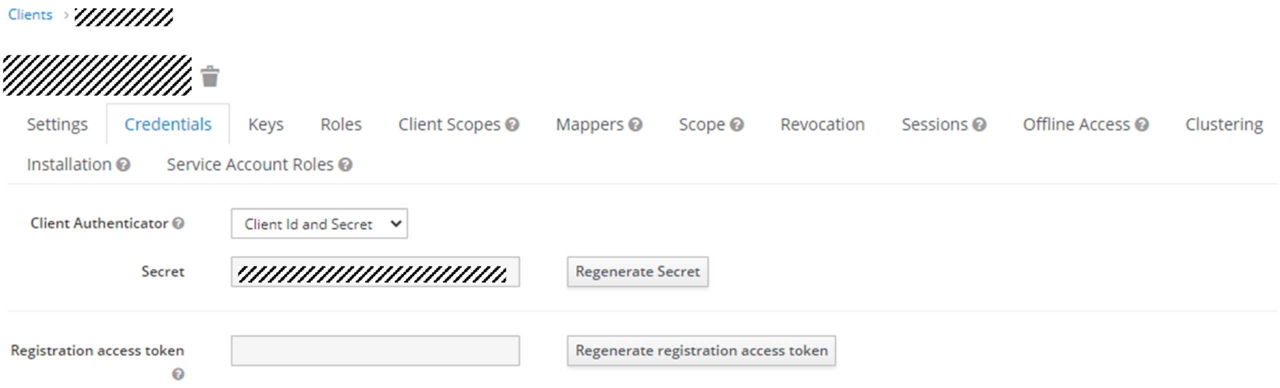
Backchannel Logout Session Required: ON

Backchannel Logout Revoke Offline Sessions: OFF

› Fine Grain OpenID Connect Configuration
› OpenID Connect Compatibility Modes
› Advanced Settings

Figure 9: Settings for RAMP clients.

Another set of client configuration options concerns the application's credentials (Figure 10). This is practically an application secret (i.e., password) that is used by the application on initiating the communication with RAMP to ensure that it is authorised to access the user authentication mechanism. It is possible to also provide a 'Registration access token', i.e. allow an application to register new users to RAMP, initiating the process from the application instead of RAMP. In the majority of cases, such option will not be provided to the applications, but the functionality is available in case such a need arises in the future.



Clients › [redacted]

[redacted]

Client Authenticator: Client Id and Secret

Secret: [redacted]

Registration access token:

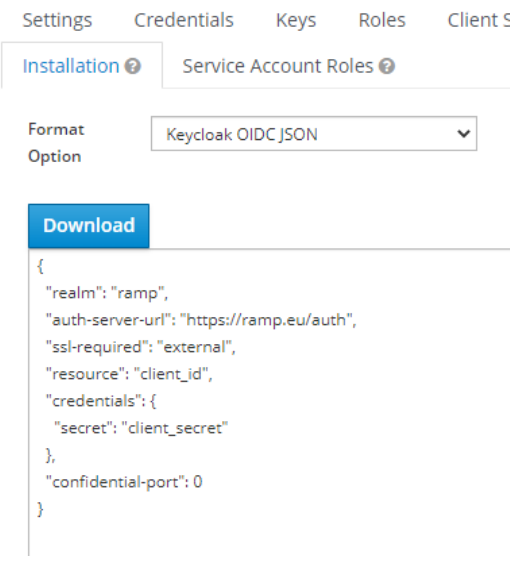
Figure 10: Configuring the client credentials.

Other client options include defining the permissions of the application in respect to using RAMP functions and specific user data that are accessible by the application. Regarding security monitoring, it is also possible to view active client sessions, and to revoke them. It is also possible to revoke all access tokens for the applications, regardless of if they are currently active.

Once the application has authenticated itself and the user, it gets a token from RAMP which is used for its interaction with other modules, like the RAMP cloud broker, data storage and other applications.

3.3 Installation

RAMP quickly generates the POST messages that the client needs to use for initiating the authentication (Figure 11). The message can be shared with the application developer for quick integration.



```
{
  "realm": "ramp",
  "auth-server-url": "https://ramp.eu/auth",
  "ssl-required": "external",
  "resource": "client_id",
  "credentials": {
    "secret": "client_secret"
  },
  "confidential-port": 0
}
```

Figure 11: Generation of POST message to used by the application.

3.4 Example demonstration

An example of a 3rd-party application is demonstrated in this paragraph. In this case, the user data is made available to the 3rd-party developer, therefore user consent is required and the application is not allowed to automatically launch the log in process. When RAMP is responsible for the data processing, the process is automated and transparent for the user (no log in action or consent needed), but the user is directly logged in on opening the application.

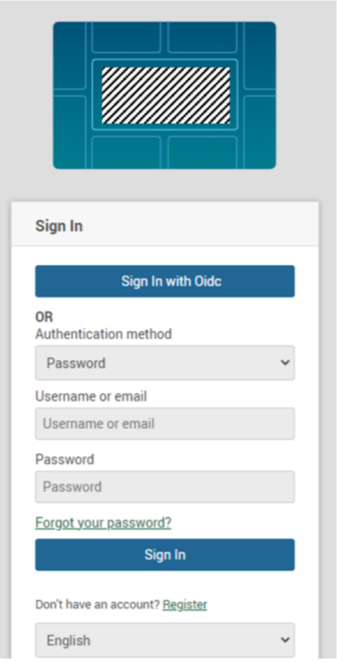
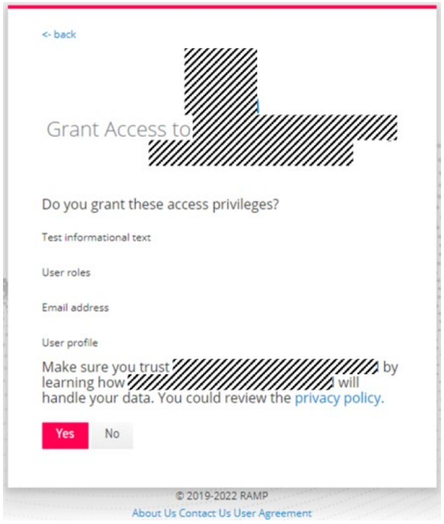


Figure 12: Example start screen of an application.

In Figure 12 an example start screen of a 3rd-party application is shown. For the RAMP co-creation space, it will not be allowed that 3rd-party application show fields to log in specifically in the application with separate user credentials (username, password). User needs to launch the log in process by clicking the relevant button (in this case 'Sign in with Oidc').

In the next step, the user is presented with the consent confirmation window. If the user is not already logged in in RAMP, they are presented with the RAMP login screen. The log in screen is not expected to be shown when the user uses an application through the RAMP cocreation space, as they will always be already logged in. This presents clearly the needed information:

- Organisation/legal entity that processes the user data,
- User data that will be processed/accessed,
- Privacy policy regarding the data handling.



<- back

Grant Access to [redacted]

Do you grant these access privileges?

Test informational text

User roles

Email address

User profile

Make sure you trust [redacted] by learning how [redacted] will handle your data. You could review the privacy policy.

Figure 13: Giving consent for processing user data.

Once the user confirms (gives consent), the user is automatically logged in and the access token is sent to the application. The application uses the token to get from RAMP the user's protect resources, like name, email, etc. Both the token, as well as the session itself, have a limited lifespan, including cases when the session is idle. This is set individually to each web application, and depends on the expected use of the app itself. After the token or session has expired, the user will be required to confirm again the use of their data by the application.

4 Conclusions

4.1 Current status

From the elements that are required for the cloud access the current status is:

- The central authentication and authorization API is ready and able to quickly add and configure client applications.
- The RAMP IoT platform is developed outside the scope of this task. Currently the RAMP IoT platform has been deployed and used in experiments. The authentication flow with the RAMP central mechanism has been implemented but not tested in experiments.
- The RAMP cloud broker and cloud data infrastructure have not yet been deployed.

4.2 Follow up

The follow up concerns the deployment and configuration of the two remaining elements that are needed for the RAMP service of providing access to the cloud.

Regarding the RAMP cloud broker, the FIWARE Orion Context broker will be deployed and configured for multitenancy, using the central RAMP authentication and authorisation component. It will be also prepared as to quickly configured for the different instances of RAMP IoT platform that will be needed as ’Context Providers’.

Regarding the cloud data storage, first the relevant database infrastructure (hardware, servers) will be first secured. Then the database software and FIWARE adapter (as previously mentioned Draco or Cygnus) will be setup. The deployment will be divided in two phases. In the first phase the setup of the database instances for each Manufacturing SME user will be done manually by the RAMP development. This phase is for the main testing of the concept and to identify any needed modifications. In the second phase, any required improvements and new requirements will be implemented, while feasibility of automated deployment for new users, utilizing the OpenStack[9] cloud infrastructure platform will be investigated.

[9] https://www.openstack.org/

H2020 Innovation Action – This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951813.