BONSAPPS

AI-as-a Service for the Deep Edge

# Technical Roadmap D1.1

| | |
|---|---|
| Grant Agreement No. | 101015848 |
| Project Name | BonsAPPs |
| Work Package No. | WP1 |
| Lead Beneficiary | BCA |
| Delivery Date | June 30th |
| Author(s) | Nikola Milojevic (BCA), Vladimir Mujagic (BCA), Kurt Tutschku (BTH), Nurul Nomen (BTH), Roman-Valentyn Tkachuk (BTH), Tim Llewellynn (BCA), Jean-Marc Bonnefous (BCA) |
| Contributor(s) | BCA, BTH |
| Editor(s) | BCA, BTH |
| Reviewer(s) | FBA, ISDI, ST-I, HES-SO |
| Nature [1] | Report |
| Dissemination Level | Public |

[1] Confidentiality level:
PU = Public
PP = Restricted to other programme participants (including the EC services);
RE = Restricted to a group specified by the Consortium (including the EC services);
CO = Confidential, only for members of the Consortium (including the EC services).
INN - Internal only, only the members of the consortium (excluding the EC services)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101015848. Neither the European Commission (EC) nor any person acting on behalf of the Commission is responsible for how the following information is used. The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the views of the EC

# Document Revision History

| Version | Date | Modification Reason | Modified by |
|---|---|---|---|
| V0.1 | April 2021 | Initial version of the deliverable | BCA |
| V0.2 | May 2021 | Internal review | BTH, ISDI, FBA |
| V0.3 | June 2021 | Internal review | ISDI, FBA, ST-I |
| V1.0 | July 2021 | Final version of the deliverable | BCA |
| V2.0 | 23th July 2021 | Final version of the deliverable sent to coordinator for review | BCA |
| V2.2 | 26th July 2021 | Submitted version of the deliverable | HES-SO |

**Copyright notice**

# Abbreviations

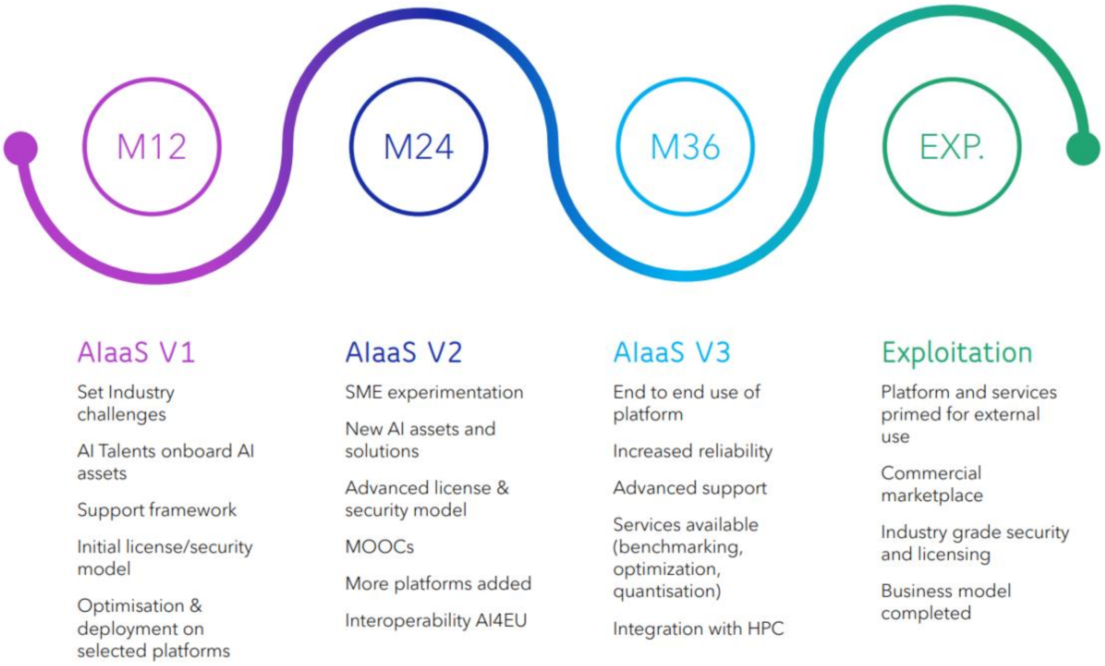
**EC:** European Commission
**DoA**: Description of Action
**GA**: Grant Agreement
**TRL:** Technology Readiness Level
**SME**: Small and Medium Enterprise
**ML:** Machine Lerning
**SOTA:** State-of-the-Art
**BMP:** Bonseyes AI Marketplace
**SVP:** Secure Virtual Premise
**USF:** User Support Framework
**LPDNN:** Low-power Deep Neural Networks
**AIaaS:** AI-as-a-Service
**SaaS:** Security-as-a-Service
**HPC**: High performance computing
**AI:** Artificial intelligence
**CPU/GPU/NPU**: Central processing unit / Graphic processing unit / Neural processing unit
**API:** Application programming interface
**ZIP**: File format specification
**HTTP**: Hypertext transfer protocol
**IP**: Internet protocol
**DRM:** Digital rights management
**VPN**: Virtual private network
**ACL**: Access control list
**ORDL**: Object relational description language
**CLI Tool**: Command line interface tool
**PEP:** Policy enforcement point
**ASCII**: American Standard Code for Information Interchange
**CIA:** confidentiality integrity availability
**CSRF:** cross side request forgeries
**XSS**: Cross-Site Scripting
**SSL/HTTPS**: Secure Sockets Layer/ Hypertext Transfer Protocol Secure
**SVP:** Secure Virtual Premise
**SVP-RH:** SVP Rendezvous Host
**XML**: Extensible Markup Language
**JSON:** JavaScript Object Notation
**GIT**: version control system
**DNN**: Deep Neural Network
**NAS:** Neural Architecture Search
**USF:** User Support Framework
**ONNX**: Open Neural Network Exchange
**BSP:** Board Support Package
**KOP**: Kudelski Obfuscation Process

# Executive Summary

This document specifies the technical roadmap of the H2020 ICT-49 BonsAPPs project, which aspires to develop the AI-as-a-Service layer for the AI-on-Demand platform, available on the Bonseyes AI Marketplace.

The document is structured as follows. Chapter 2 describes an overview of the Bonseyes AI Marketplace, explains the problems in the traditional AI Solution development, introduces main concepts, definitions, user personas and user journeys, security and licensing mechanism. Furthermore, Chapter 3 explains the main components of the Bonseyes AI Marketplace Platform i.e., Bonseyes AI Marketplace, Secure Virtual Premise and CLI Tool.

Chapter 4 delineates a roadmap of the BonsAPPs AIaaS. The roadmap is separated into the three main release cycles, V1, V2 and V3. The V1 release will provide integrated AIaaS into the AI Marketplace, interoperability with the AI-on-demand platform, connection with the HPC clouds, definition of Use Cases that will be the outcome of the first round of Open Calls.  The V2 release is focused on learned lessons from the first round of Use Cases; new services and functionalities will be integrated and ready for use in the second round of specific Use Cases selected from 2nd Open Call. The V3 release is planned to additionally enhance features or solve bugs/inefficiencies detected during the second round of Use Cases. This roadmap deliverable will be updated with each platform release as required.



**AIaaS V1**
- Set Industry challenges
- AI Talents onboard AI assets
- Support framework
- Initial license/security model
- Optimisation & deployment on selected platforms

**AIaaS V2**
- SME experimentation
- New AI assets and solutions
- Advanced license & security model
- MOOCs
- More platforms added
- Interoperability AI4EU

**AIaaS V3**
- End to end use of platform
- Increased reliability
- Advanced support
- Services available (benchmarking, optimization, quantisation)
- Integration with HPC

**Exploitation**
- Platform and services primed for external use
- Commercial marketplace
- Industry grade security and licensing
- Business model completed

# Table of Contents

Abbreviations - 2 -

Executive Summary - 3 -

1 Introduction - 8 -

2 Bonseyes AI Marketplace - 9 -

2.1 Main concepts - 9 -
2.1.1 The Bonseyes AI Marketplace - 10 -
2.1.2 AI Assets and AI Artifacts – definitions - 12 -
2.1.2.1 AI Assets - 12 -
2.2 Multi-Party Collaborative AI Development - 15 -
2.2.1 User Personas - 16 -
2.2.1.1 Target Users - 16 -
2.2.1.2 Personas - 17 -

3 Bonseyes AI Marketplace Platform - 18 -

3.1 Bonseyes AI Marketplace Platform Components - 18 -
3.1.1 Bonseyes AI Marketplace - 18 -
3.1.2 Secure Virtual Premise - 19 -
3.1.3 Bonseyes command line (CLI) tool - 20 -
3.2 Security - 20 -
3.2.1 Initial BonsAPPs Security Architecture - 20 -
3.2.2 Overview of the Security Architecture - 21 -
3.2.3 Industrialization and Security Services - 22 -
3.2.4 Focus Areas of Engineering the Security-as-a-Service Concept in the BonsAPPs Architecture - 22 -
3.2.5 System-Wide Services for Security - 23 -
3.2.6 Security Concepts and Mechanisms in the Development Tool Chain - 23 -
3.2.6.1 Frontend Security Engineering - 24 -
3.2.6.2 Secure Transfer, Storage and Marketplace Interoperability Tools - 24 -
3.2.6.3 Trusted Computing as a Service Tool: Enhancing the SVP to a Hardened and Distributed Development Environment - 24 -
3.2.7 Reliable management and distributed setup of a multi-site SVP: - 24 -
3.2.7.1 Handling of additional generic types of AI Artifacts by the Bonseyes Layer - 25 -
3.2.7.2 Security Concepts and Mechanisms in the Deployment Tool Chain - 26 -
3.2.8 AI Artifact Licensing - 26 -
3.2.9 Open Digital Rights Language and System Overview - 26 -
3.2.10 Overview of the BonsAPPs Licence Management System - 27 -
3.3 Bonseyes AI Marketplace Interoperability - 28 -
3.3.1 Bonseyes AI Marketplace API - 28 -

4 BonsAPPs AIaaS Roadmap - 30 -

4.1 AIaaS V1 - Supply Activation - 33 -
4.1.1 Bonseyes AI Marketplace (BMP) - 34 -
4.1.1.1 Platform Infrastructure - 34 -
4.1.1.2 Enhancement of the Major Features - 34 -
4.1.1.3 Interoperability of the Service Layer with the AI-on-Demand platform - 35 -
4.1.1.4 Integration of Community Layer - 36 -
4.1.1.5 BMP Services integration - 36 -
4.1.1.6 Development of new services visible on AI4EU - 37 -

4.1.1.7 Analysis of the strong integration/merger between two platforms ........ - 38 -
4.1.1.8 Interoperability and connectivity with HPC Clouds ........ - 39 -
4.1.2 User Support Framework........ - 39 -
4.1.2.1 Developer Community ........ - 39 -
4.1.2.2 AI Assets Marketplace ........ - 39 -
4.1.2.3 Users and Organization Profiles ........ - 41 -
4.1.2.4 Bonseyes AI Asset Container ........ - 41 -
4.1.2.5 Bonseyes AI Containers for Edge and Deep Edge ........ - 43 -
4.1.2.6 User Support Documents ........ - 43 -
4.1.2.7 Developer Platforms | Board Support Packages (BSP)........ - 44 -
4.1.2.8 User Guide Features ........ - 45 -
4.1.3 Security........ - 46 -
4.1.3.1 4.1.3.1 Gantt Chart for Security Activities in AIaaS V1 ........ - 46 -
4.1.4 Industry Challenges 1 (AI Assets) ........ - 47 -
4.1.4.1 Automotive ........ - 48 -
4.1.4.2 Healthcare........ - 48 -
4.1.4.3 Manufacturing ........ - 50 -
4.1.4.4 Robotics ........ - 51 -
4.2 AIaaS V2 – Demand Activation ........ - 52 -
4.2.1 Bonseyes AI Marketplace........ - 52 -
4.2.1.1 User Support Framework........ - 53 -
See User Framework deliverable D 5.1. ........ - 53 -
4.2.1.2 AI Asset Container ........ - 53 -
See User Framework deliverable D 5.1. ........ - 53 -
4.2.1.3 MOOC ........ - 53 -
4.2.2 Security as a Service........ - 55 -
4.2.2.1 Gantt Chart for Security Activities in AIaaS V2 ........ - 55 -
4.2.3 Industry Challenges 2 (AI Apps)........ - 56 -
4.2.3.1 Automotive........ - 56 -
4.2.3.2 Healthcare ........ - 57 -
4.2.3.3 Manufacturing........ - 58 -
4.2.3.4 Robotics........ - 58 -
4.3.1 Bonseyes AI Marketplace........ - 59 -
4.3.2 Security........ - 59 -
4.3.2.1 Gantt Chart for Security Activities in AIaaS V3 ........ - 60 -
Bibliography........ - 61 -

# List of Figures

Figure 1 Service comparison matrix of the main existing SOTA platform and initiatives .................................. - 9 -
Figure 2 Bonseyes AI Marketplace Ecosystem ........................................................................................ - 10 -
Figure 3 Multi-party collaborative AI Development process ................................................................. - 11 -
Figure 4 Physical architecture of the SVP ............................................................................................. - 16 -
Figure 5 Overview of the implemented architecture ............................................................................ - 18 -
Figure 6 Bonseyes AI Marketplace ........................................................................................................ - 19 -
Figure 7 AI Assets and AI Artifacts available on the AI Marketplace platform ...................................... - 19 -
Figure 8 Bonseyes CLI Tool interface. ................................................................................................... - 20 -
Figure 9 Concept BonsApps Security Architecture. .............................................................................. - 21 -
Figure 10 Concept of a Multi-site SVP.................................................................................................... - 25 -
Figure 11 KOP’s c object code obfuscation mechanism ....................................................................... - 26 -
Figure 12 ODRL information model for specifying digital rights, cf [ORDL18a]...................................... - 27 -
Figure 13 Example licenses written in JSON ......................................................................................... - 27 -
Figure 14 Overview of the Bonseyes ecosystem and the BonsAPPs Licence Management System with the different licensing modules (in red). ..................................................................................................... - 28 -
Figure 15 AI marketplace API description ............................................................................................. - 29 -
Figure 16 Edge Deployment Challenges ............................................................................................... - 30 -
Figure 17 BonsAPPs AIaaS Layer ........................................................................................................... - 31 -
Figure 18 AIaaS releases overview......................................................................................................... - 32 -
Figure 19 Categorized service layer ...................................................................................................... - 32 -
Figure 20 High level roadmap ............................................................................................................... - 33 -
Figure 21 AI-aaSv1 and AI-aaSv2........................................................................................................... - 34 -
Figure 22 Gant chart for the development activities in AIaaS V2 (ex-security)..................................... - 35 -
Figure 23 Bonseyes APIs for interoperability ........................................................................................ - 37 -
Figure 24 Interoperability and AI4EU community access to Bonseyes Marketplace ............................ - 38 -
Figure 25 Interoperability architecture for interconnecting Bonseyes with AI4EU ............................... - 38 -
Figure 26 AI Assets landing page on the Bonseyes AI Marketplace ...................................................... - 40 -
Figure 27 Deployment Capabilities of the AI Assets .............................................................................. - 41 -
Figure 28 Experimentation to industrialization pipeline supported with the Service Layer in AI Asset Container - 42 -
Figure 29 AI Asset container architecture............................................................................................. - 43 -
Figure 30 Board Support Packages on AI Marketplace .......................................................................... - 44 -
Figure 31 Gant chart for the SaaS activities in AIaaS V1 ........................................................................ - 47 -
Figure 32 Open Call workflow ................................................................................................................ - 47 -
Figure 33 Automotive vertical: challenges, applications, use cases ...................................................... - 48 -
Figure 34 Health vertical: challenges, applications, use cases .............................................................. - 49 -
Figure 35 Manufacturing vertical: challenges, applications, use cases ................................................. - 50 -
Figure 36 Robotics vertical: challenges, applications, use cases ........................................................... - 51 -
Figure 37 AIaaS V2 – Demand Activation............................................................................................... - 52 -
Figure 38 MOOC courses description .................................................................................................... - 53 -
Figure 39 Gantt chart for the SaaS activities in AIaaS V2 ...................................................................... - 56 -
Figure 40 Challenges workflow .............................................................................................................. - 56 -
Figure 41 Potential Automotive use cases for AIaaS V2 industry challenges ......................................... - 57 -
Figure 42 Potential Health use cases for AIaaS V2 industry challenges ................................................ - 57 -
Figure 43 Potential Manufacturing use cases for AIaaS V2 industry challenges .................................... - 58 -
Figure 44 Potential Robotics use cases for AIaaS V2 industry challenges ............................................. - 58 -

Figure 45 Gant chart for the SaaS activities in AIaaS V3 ... - 60 -

# List of Tables

Table 1 Overview of Personas ... - 17 -
Table 2 User and Organization Profile Features ... - 41 -
Table 3 Supported Developer Platforms ... - 45 -
Table 4 User Guide Features ... - 45 -
Table 5 Always above the table ... - 61 -

# 1 Introduction

This deliverable will provide the general technical framework of the Bonseyes AI Marketplace Platform (BMP), and the BonsAPPs AI-as-a-Service (AI-aaS) layer that will be accessible on the Bonseyes AI Marketplace. The document will evaluate existing BMP tools and establish a technical roadmap to get the BonsAPPs service layer ready for demonstration and operation over the two rounds of Open Calls and for the subsequent exploitation phase and to enable the interoperability of this service layer with the AI-on-Demand platform, in coordination with AI4EU.

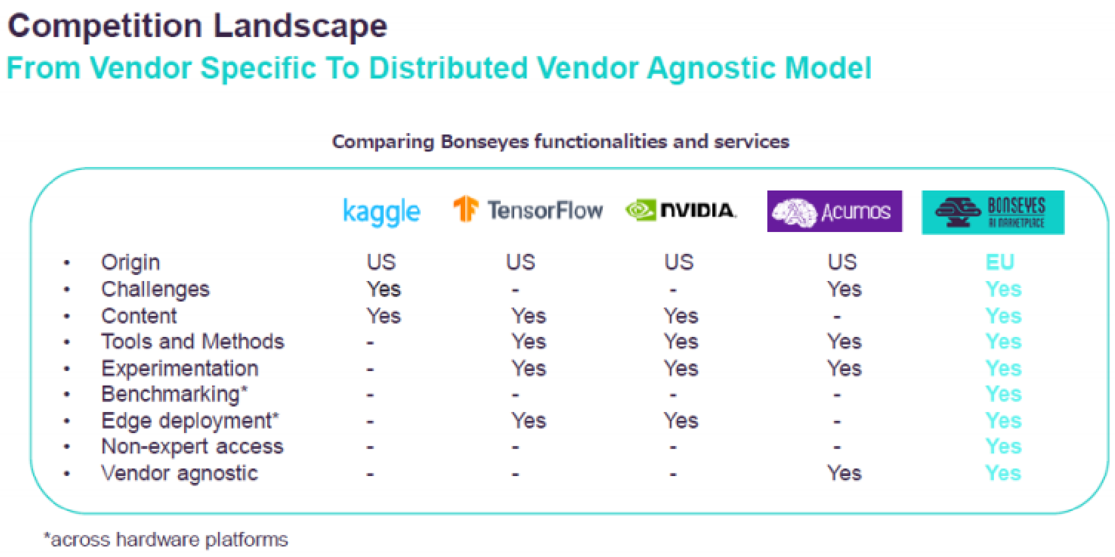
# 2 Bonseyes AI Marketplace

## 2.1 Main concepts

The Bonseyes AI Marketplace is a platform that connects researchers, developers, and companies to build and trade AI Applications. Its goal is to facilitate collaboration between researchers and industry to accelerate the process, reduce the cost, and improve the performance of building and deploying AI-based solutions to solve real-world challenges defined by the industry. As mentioned in the introduction, the BonsAPPs AI-as-a-Service (AI-aaS) layer will be accessible on the Bonseyes AI Marketplace.

Developing AI Applications to solve industry challenges requires a number of AI Artifacts produced by different stakeholders with support of service providers to access critical infrastructure, tools, skills, and data resources. This activity becomes even more challenging when targeting deployment to resource constrained devices such as deeply embedded systems found in healthcare devices, cars, and robots. The deployment of AI in such systems demands meeting many non-functional requirements in addition to stringent accuracy targets and complex system integration skills.

Various platforms such as Kaggle[1], TensorFlow Lite[2], NVIDIA Jetson[3], and Acumos[4] provide fragmented approaches to help developers and data scientists tackle these challenges; however, they fall short of providing significant impact for a Edge and Deep Edge ecosystem as they do not provide users with the full end-to-end functionalities and features that will be available in the Bonseyes ecosystem presented ion Figure 1 below.



Competition Landscape

From Vendor Specific To Distributed Vendor Agnostic Model

Comparing Bonseyes functionalities and services

| | kaggle | TensorFlow | NVIDIA | Acumos | BONSEYES AI MARKETPLACE |
|---|---|---|---|---|---|
| • Origin | US | US | US | US | EU |
| • Challenges | Yes | - | - | Yes | Yes |
| • Content | Yes | Yes | Yes | - | Yes |
| • Tools and Methods | - | Yes | Yes | Yes | Yes |
| • Experimentation | - | Yes | Yes | Yes | Yes |
| • Benchmarking* | - | - | - | - | Yes |
| • Edge deployment* | - | Yes | Yes | - | Yes |
| • Non-expert access | - | - | - | - | Yes |
| • Vendor agnostic | - | - | - | Yes | Yes |

*across hardware platforms

*Figure 1 Service comparison matrix of the main existing SOTA platform and initiatives*

[1] https://www.kaggle.com/ - Kaggle is the world's largest data science community with powerful tools and resources to help you achieve your data science goals.

[2] https://www.tensorflow.org/lite - TensorFlow Lite is the official framework to run inference with TensorFlow models supporting Android, iOS, Linux-based IoT devices and microcontrollers.

[3] https://www.nvidia.com/de-de/autonomous-machines/embedded-systems/ NVIDIA Jetson is the world's leading embedded AI computing platform.

[4] https://www.acumos.org/ - Acumos AI is a platform and open source framework that makes it easy to build, share, and deploy AI apps.

- Origin: native European platform with GDPR and licensing framework aligned with European values on data-privacy and ethics;
- Challenges: ability to present real-world data-driven industry Challenges to the user community both in open/public and private/confidential modalities;
- Content: provide access to extensive content and resources such as code and papers delivered in a re-usable containerized format;
- Tools and Methods: use of state-of-the-art tools and methods to support the development of marketable solutions to the users' challenges, especially targeting embedded and resource constrained devices;
- Experimentation: ability for users to perform experimentation and iterate on playground with Proofs-of-Concepts (PoC) and pilots on the platform at the pre-production stage;
- Benchmarking: access to benchmarking services and model optimization for AI solutions on various heterogeneous hardware platforms;
- Edge Deployment: capabilities with a fully functional cycle for the development of AI Apps at the Edge and Deep Edge on low power and resource constrained hardware platforms;
- Non-Expert Access: makes data-driven solutions easier to be incorporated by SMEs with reduced internal technological capabilities and/or low technology sectors;
- Vendor Agnostic: functionalities and services available on a number of heterogeneous hardware platforms outside any vendor-specific supply chain;

The goal of the Bonseyes AI Marketplace is to overcome the shortcomings of existing platforms and provide end-to-end procurement platform for industry for Edge and Deep Edge AI Applications while connecting researchers, developers and industry together through an ecosystem as depicted in Figure 2.

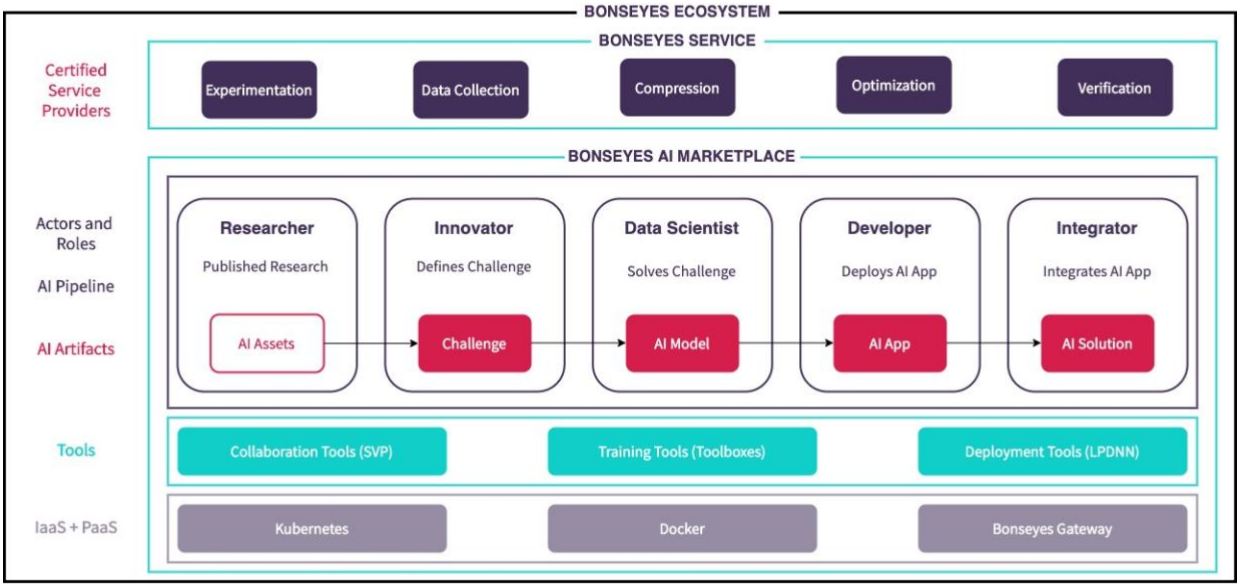


*Figure 2 Bonseyes AI Marketplace Ecosystem*

### 2.1.1 The Bonseyes AI Marketplace

The Bonseyes AI Marketplace defines programming interfaces for all the AI Artifacts involved so that they can be integrated in a fully automated procurement process, enabling the right AI Artifact to be produced by the right actor at the right time. Bonseyes, being a multi-sided market, brings together multiple interdependent target end-users with a clear focus on the following groups:

1 **Innovators** who are looking to solve industry challenges using data-driven software systems and incorporating Artificial Intelligence into solutions.
2 **Researchers** who are looking to research Artificial Intelligence to develop new algorithms, methods, and tools which can be then applied to solve societal and industry relevant challenges.
3 **Developers** and **Data Scientists** who want to access Artificial Intelligence in order to build AI Applications and Solutions to then sell their products and services to companies.
4 **Companies** who want to either integrate Artificial Intelligence into their products or services who may or may not be technology users themselves or act as service providers who want to value-added services to the target end-users of the platform.

These end-user groups interact on the marketplace using:

1. **AI Assets** consisting of published reproducible research, datasets, data and evaluation tools used to support the development of industry-driven Challenges. AI Assets are typically unstructured and are the outcome of research in the area of AI.
2. **AI Artifacts** consisting of Challenges, AI Applications, Developer Platforms, and AI Solutions are structured and containerized with standard interfaces.

Figure 3 depicts how these different end-user groups interact with the multi-party AI development process of Bonseyes. Please note that some steps are optional, such as “Publish” and “Feedback”, however are incentivized on the platform.

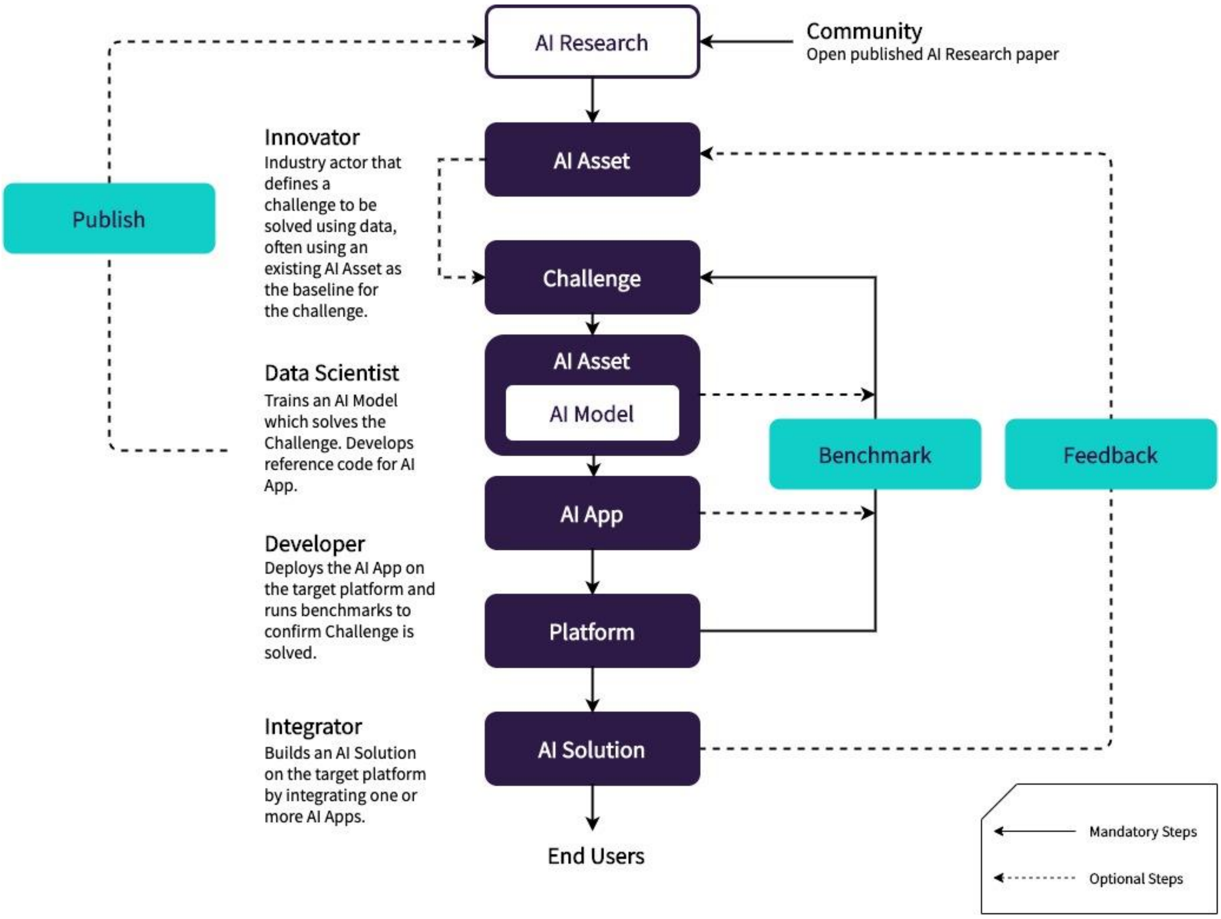

AI Research
Community
Open published AI Research paper
Publish
Innovator
Industry actor that defines a challenge to be solved using data, often using an existing AI Asset as the baseline for the challenge.
AI Asset
Challenge
Data Scientist
Trains an AI Model which solves the Challenge. Develops reference code for AI App.
AI Asset
AI Model
Benchmark
Feedback
Developer
Deploys the AI App on the target platform and runs benchmarks to confirm Challenge is solved.
AI App
Platform
Integrator
Builds an AI Solution on the target platform by integrating one or more AI Apps.
AI Solution
End Users
Mandatory Steps
Optional Steps

*Figure 3 Multi-party collaborative AI Development process*

## 2.1.2 AI Assets and AI Artifacts – definitions

The Marketplace allows  transition from unstructured Assets that are the direct output of research to highly standardized Artifacts that can be automatically integrated into an industrialized workflow.

The AI Research produces papers and associated implementation code that can be used to reproduce the original research and also create models out of publicly available datasets. The marketplace allows the importation and structuring of such Assets by defining an industry-driven challenge. The challenge is then the starting point that allows for the creation of an AI app that answers the specific use cases of the marketplace users.

More in detail, the challenge is used to drive the industrialization process that consists of gathering in-context data, retraining the models with such data, optimising the models (e.g., for speed and size) and finally benchmark them. The challenge consists of verification data, benchmarking code and target KPIs. The AI app resulting from the process includes a trained model that has been compressed and the corresponding execution code optimized for CPU/GPU/NPU. The AI app can be benchmarked and includes an API that allows its integration in a complete AI solution.

### *2.1.2.1 AI Assets*

AI Research
AI Research is documented scientific research, published in open-access repositories which may or may not be verified by domain experts (peer review). AI Research in the Bonseyes AI Marketplace intends to provide a starting position for the Data Scientist and necessary foreknowledge to implement and reproduce experiment results. The innovator may use them as a reference inside the challenge description.

AI Assets
AI Assets represents a scientific paper with related source code implementation, one AI Research can have no existing open implementation or can have multiple. An AI Asset provides Innovators, Data Scientist, and Developers a ready-to-use implementation of the AI Research. An AI Asset can be integrated into the Bonseyes platform by following certain best practices guidelines [REF to Bonseyes D2.4]. AI Assets, incorporating AI Models, can be integrated by providing a Bonseyes Layer for testing and deployment using containerization technology such as Docker[5]. The objective of the AI Assets usage is to decrease AI development time and to improve the quality of the AI solution incorporating state-of-the-art implemented research. AI Assets cover a variety of machine learning domains, such as computer vision, natural language processing, medical, time series, speech, etc.

The Innovator can use an AI Assets as a plugin component of either complex AI Solution with multiple AI Apps or as a baseline to create a specific single app solution e.g. face detection with landmarks can be used for eye detection. AI Assets enables the Innovator to discover and evaluate state-of-the-art research within their own domain or with their own data before creating a Challenge and to integrate it as a part of an existing or new Challenge.

[5] https://www.docker.com/ - Docker is a set of platform as a service (PaaS) products that use OS-level virtualization to deliver software in packages called containers.

Datasets
Datasets represent a community and commercial collection of data for specific domain. Datasets can be represented in different modalities e.g., images, audio, tables, point clouds, etc, and can be used for solving one or many tasks. In machine learning, datasets represent one of the crucial components which is used for model training and evaluation. The AI Marketplace will provide details of the specific dataset, references to the papers and website and will connect the datasets with the AI Assets that employ them.

Data Tool
Data tools are used to encapsulate training and evaluation data of a challenge. The data tools are capable of downloading and processing data from a repository in the local environment in which they are executed. They may also perform data conversion so that their output is compatible with training, evaluation and deployment tools.

Evaluation Tool
Evaluation tools are used to evaluate AI Assets or AI Apps for specific Challenges. They consist of the evaluation procedure, evaluation code and evaluation report. Evaluation tools can put into service one or more data tools related to the challenge, with the intention of evaluating functional metrics of the AI App, like accuracy, inference time and non-functional metrics like CPU, memory usage and network throughput.

AI Artifacts
The AI procurement process requires several Artifacts produced by different stakeholders. In order to facilitate the procurement process the approach taken in the marketplace is to define programming interfaces for all the Artifacts involved so that they could be integrated in a potentially fully automated procurement process. The Artifacts share some common features: they all have meta-data, that describes, for instance, who created them; their human readable description, etc. and are subject to licensing rules. The interface to these features is kept common across all Artifacts, while each specific type of Artifact has additional specific interfaces.

Challenge
The challenge is a document created by the Innovator that formally describes a problem that can be solved applying machine learning techniques supported by examples and data. From the AI Marketplace developers' perspective, a challenge represents a call, public or private, for multi-party collaboration in AI system development, where the outcome is called an AI Application developed for a specific hardware or deployment platform.

Unlike normal requirement documents, the challenge does not define the exact mapping between inputs and outputs; instead, it provides a set of example inputs and its corresponding outputs and the training data and its ground truth. This data can be used to automatically generate the software module function using machine learning. The usual input/output interfaces definitions are also included in the challenge to guarantee successful integration in the solution being created by the innovator.

Since the challenge uses examples to define the desired input/output mappings, it is critical for the innovator to be able to measure if the function successfully achieves the desired robustness and generalization performance with other examples from its problem domain. In order to specify the expectations, the innovator must include in the challenge an evaluation procedure, which is a software module that can be used to test the function, that uses evaluation data to generate metrics for which the innovator can define targets.

The challenge author can also use the evaluation procedure to set targets for metrics such as resource consumption and execution time on the selected hardware and software environment.

Concretely, a challenge is a directory that contains:

- a top-level manifest;
- generic metadata;
- a reference to a parameterizable API along with its corresponding parameters;
- links to docker-based tools to fetch data and to perform the evaluation.

AI Model

An AI Model is a formal description of a parameterizable algorithm, set of parameters, preprocessing and postprocessing algorithms that are capable of generating outputs compatible with the training data provided in a challenge. The value of each parameter can be in part or completely generated by using machine learning from the training data. The AI Model is produced by a Data Scientist and is used as input to a deployment tool to automatically generate an AI App for a specific Developer Platform.

AI App

An AI App is a binary software module that is capable of solving a challenge using an AI Model. This software module can run on the target hardware and software environment while satisfying target metrics defined in the challenge. The AI App concrete implementation depends on the environment for which it is built. It can be a ZIP file containing a shared library and header files or a docker image containing an HTTP server that provides access to the AI App function. The AI App is a directory that contains:

1. a top-level manifest that specifies AI App metadata (description, related challenge, and target platform);
2. evaluation report;
3. configuration;
4. binary sources;
5. redistribution license of the AI App. The owner of the AI App can make it publicly available on the AI Marketplace, as a reusable component that can be procured for development of AI Solutions. Developers and integrators have an interest in reusing AI App to reduce necessary development time and costs.

Developer Platform

A Developer Platform is a package of software that can be used to build and execute an AI App for a given target hardware/software environment (such as a Raspberry Pi4 or NVIDIA Jetson Xavier) and provides access to a board support package. The platform package simplifies the setup and usage of the platform for some common functions that are necessary in the process of procurement of an AI App, including the installation of an operating system for the target hardware.

The platform contains a support docker that helps the user build the software for the target hardware and set up the hardware/software combination. It also contains a builder docker that allows the user to cross-compile software for the target hardware/software environment. This is used by the deployment tool to build an AI App for the target environment from an AI model. Finally, the developer platform includes a manager docker that exposes an API to control a configured target environment.

AI Solution

An AI Solution is the software that addresses an industry use case and is a fully executable application that can be deployed to the target hardware. Unlike the AI App, which behaves like a data processing block, the AI Solution contains the code that is capable of reading inputs from the physical sensors available on the target hardware and provides a user interface that allows the end user to interact with the solution itself.

## 2.2 Multi-Party Collaborative AI Development

The Bonseyes AI Marketplace aims to streamline processes, providing standardized templates and tools to automate the provision of AI Apps, as well as efficient tools to benchmark AI Apps for specific target platforms. Figure 2 in Section 1.1 illustrates the relationships among the main users and the outputs of their cooperation.

At the core of the interaction between the different actors lies the benchmarking process. The innovator can communicate his/her expectations by providing evaluation code that will test the produced AI Apps not only for accuracy but also for non-functional requirements such as latency, throughput or memory consumption. Thanks to this code, the AI App can then be automatically tested for these criteria during the benchmarking phase. This approach reduces the development time as the developer and the data scientist can immediately and continuously test their work for acceptance criteria established by the innovator in an unambiguous way.

To enable automatic testing of non-functional requirements, the benchmarking procedure relies on the deployment tool developed by Bonseyes and refined by the developer. This allows the conversion of the model created by the data scientist to an executable application that can be executed on the target hardware and tested by the evaluation procedure on it. Thanks to the platform support package shared by all actors, it is then possible to make sure that the results produced by the evaluation procedure are always consistent.

The integrator is an embedded developer who sources existing AI apps and development platforms, integrates the AI apps and the platform, potentially creates a UI to create a full solution to the innovators use case. Thanks to the platform, the integrator has access to high quality AI apps that have been optimized for the use case.

At a later stage of development, the Bonseyes AI Marketplace will attract and respond to the needs of different AI service providers, completing and enhancing the experience of the four main users, all details regarding Bonseyes users and user journeys are explained in Section 4.3.

In order to facilitate the collaboration in a technical way, the Bonseyes project developed and implemented the SVP (Secure Virtual Premise), cf. Section 10 and [D1.3 AI-aaS release V2]. The SVP is a platform tool that combines the required compute, storage and execution environments, cf. Figure 4. Participants of the marketplace can use the SVP to securely and trustfully execute AI Assets, either remotely or locally, and to orchestrate automatic chains of AI Assets, the so-called AI pipelines. The AI Assets can either be selected, procured and transferred from the marketplace or they can be developed locally by the user.

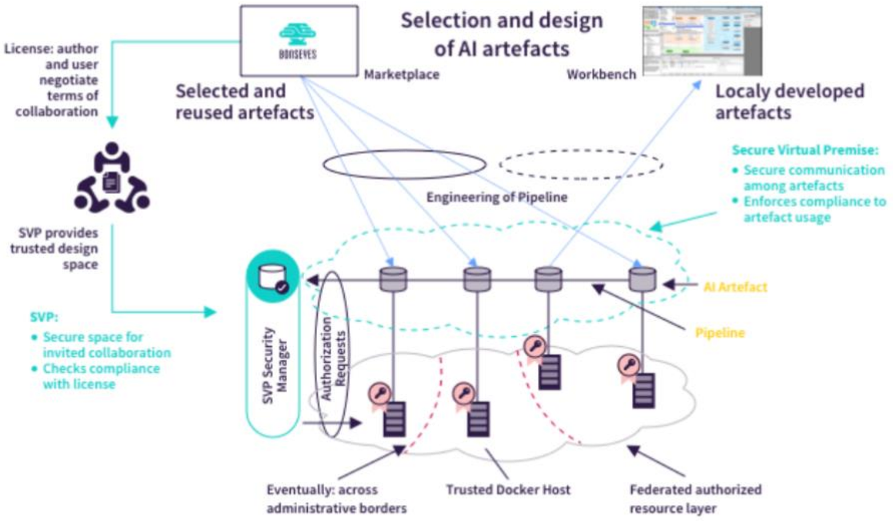

Selection and design of AI artefacts
BONSEYES
Marketplace
Workbench
License: author and user negotiate terms of collaboration
Selected and reused artefacts
Localy developed artefacts
Engineering of Pipeline
Secure Virtual Premise:
• Secure communication among artefacts
• Enforces compliance to artefact usage
SVP provides trusted design space
SVP:
• Secure space for invited collaboration
• Checks compliance with license
SVP Security Manager
Authorization Requests
AI Artefact
Pipeline
Eventually: across administrative borders
Trusted Docker Host
Federated authorized resource layer

*Figure 4 Physical architecture of the SVP*

### 2.2.1 User Personas

User personas are the definitions of the different potential users, that will use product or service. Identifying personas helps to understand their needs, pain-points, and behaviors. They describe the main characteristics and needs common to a certain group of heterogenous real people. In the case of a website like the Bonseyes AI Marketplace, personas represent major user groups and give a clear picture of the user's expectations and the needs the website can respond to. Personas are the base of user experience: once they are defined, they drive the design of the website's frontend components and backend architecture.

#### 2.2.1.1 Target Users

The current version of Bonseyes AI Marketplace defines and targets following users:

i. **Researchers:** are individuals who conduct research, i.e., an organized and systematic investigation of the topics related to the domain of the AI. They are publishers of the AI Research or AI Asset.

ii. **Innovators:** are individuals who represent a company or academic institution that would like to solve a data-driven problem using AI technologies. Innovators are creators of the challenge, providing a description of the problem, data, resources constraints, and target performances.

iii. **Data Scientists:** are highly skilled professionals or researchers in the field of data science. They are the creators of AI Artifacts and AI Models that enables the creation of AI Apps as a solution to a challenge

iv. **Developers:** are highly skilled professionals experienced with the deployment process of the AI Models into the various hardware platforms. They are creators of AI Applications that embed AI Models on specific Developer Platforms containing Target Hardware, which may include meeting non-functional requirements in embedded systems.

v. **Integrators:** are highly skilled companies or professionals in the field of deployment and integration of the AI Apps into the final industry solution. They create AI Solutions that are comprised of multiple AI Apps in conjunction with the supplementary user interface, platform integration, synchronization, and orchestration code.

#### 2.2.1.2 Personas

The Bonseyes AI Marketplace offers a unique value proposition for each of the following personas, providing a quick entry point for each target group and leads the user efficiently to the section of their interest. The following table gives an overview.

*Table 1 Overview of Personas*

| Persona | Background & Needs | Value Proposition |
|---|---|---|
| Researcher (Scientist) | Is organizing and executing a systematic investigation of AI related topics. Low-conversion in research monetization. | Gains the opportunity to expand the possibilities of his research and participate in its monetization. |
| Innovator (Industry) | Industry player. Looking for experts to develop an AI solution for a given business use case. | Can present public or private challenge, participation on invitation only with trusted parties.<br>Community Feature of the Marketplace allows them to quickly find suitable experts. |
| Innovator (University) | Looking for experts to develop an AI solution for a given problem | Can present public calls for challenges, recommending these challenges to suitable experts. |
| Data Scientist (AI company) | Looking for a platform to publish and monetize his IP. | Quickly deploy own AI Models into AI Apps, publish them and sell. |
| Data Scientist (Individual) | Highly skilled professionals in the field of data science looking for interesting challenges and attractive employers. | Expose skills to potential business partners and find interesting Challenges and Labs to contribute to. Prove expertise by benchmarking of apps and Artifacts provided to the Marketplace as well as by ranking and appraisal by others. Monetize the AI Artifacts created. |
| Developer (Embedded System Engineer) | Highly skilled professional in the field of deployment of AI Applications looking on one hand at ways to fast tracking deployment process and on the other hand for interesting challenges to contribute to. | The developer can reduce their costs/speed up their work by leveraging the tools and formats defined by the marketplace. Common formats and processes allow the developer to focus resources on differentiating capabilities and not on interfacing with other actors. Common tools allow them to reduce the cost of development of common infrastructure code. By developing plugins to the deployment tool, the developer can also transform his/her knowledge into a product. Additionally, it exposes skills to potential collaborators. Users can prove his expertise by the benchmarks of apps published to the Marketplace. |

| | | |
|---|---|---|
| Integrator (AI Development Company) | Highly skilled companies and startups and professionals in the field of deployment of AI Applications, looking at ways to develop AI solutions as well as for interesting challenges to contribute to. | Bonseyes helps speed up the deployment process. The Bonseyes AI Marketplace provides ready-to-use AI Apps compatible with each other and pretested to run on specific hardware platforms. Bonseyes provides the software package as well to set up the platforms and procurement information regarding the platform and the needed accessories. |

# 3 Bonseyes AI Marketplace Platform

The Bonseyes AI Marketplace platform consists of a web marketplace, an environment for secure multi-party collaboration and a Bonseyes CLI tool that facilitate and support industries, researchers, data scientists, developers and integrators to produce, manage, publish and download data-driven Challenges, AI Apps, Developer Platform Environments and AI Solutions. A holistic view of the Bonseyes  AI Marketplace platform shows three distinct main components, as depicted in Figure 5.

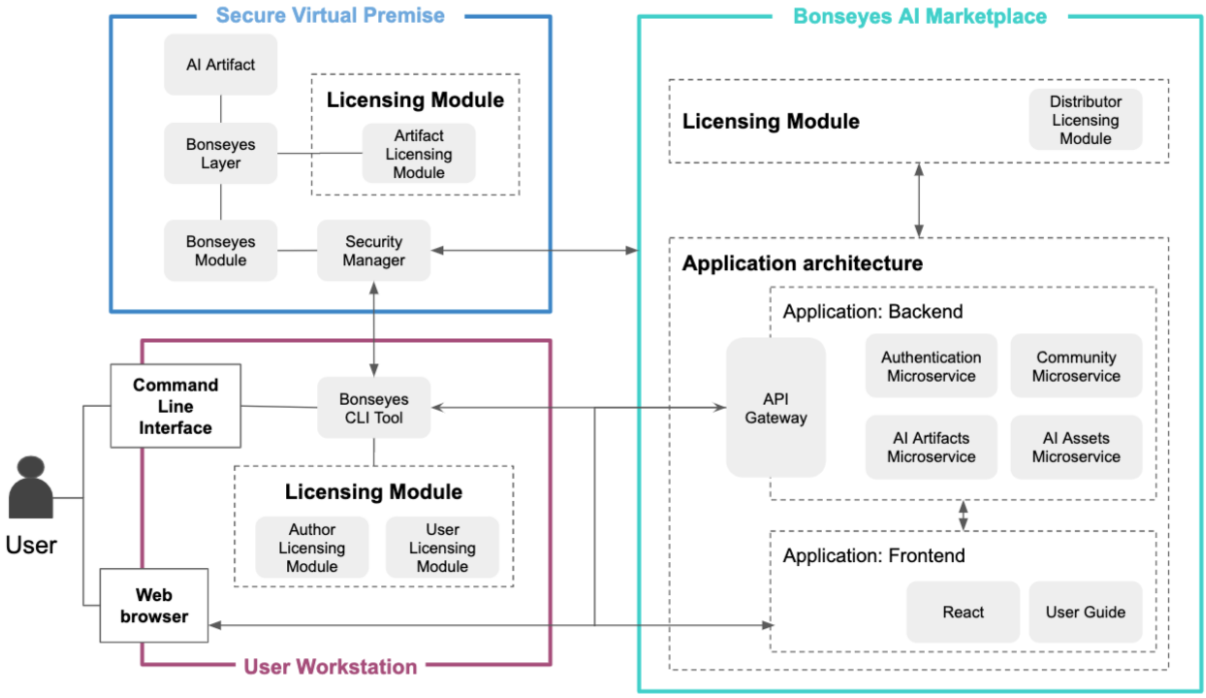


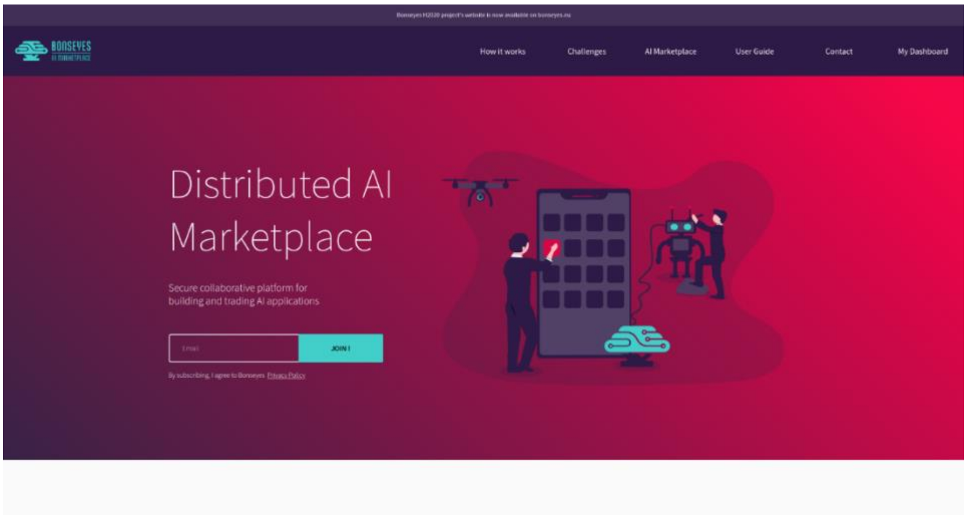
*Figure 5 Overview of the implemented architecture*

## 3.1 Bonseyes AI Marketplace Platform Components

### 3.1.1 Bonseyes AI Marketplace

The Bonseyes AI Marketplace is a web platform that connects researchers, developers, and companies to procure, collaboratively build, and trade AI Applications. This section describes the functionalities and architecture in more details.

The AI Marketplace is designed applying the microservice architecture approach. We can distinguish two high-level components (i.e., clusters), Frontend and Backend. The AI Marketplace allows new users to register and access the platform, with the aim of connecting and collaborating with the other members of the Bonseyes Community.



Bonseyes H2020 project's website is now available on bonseyes.eu

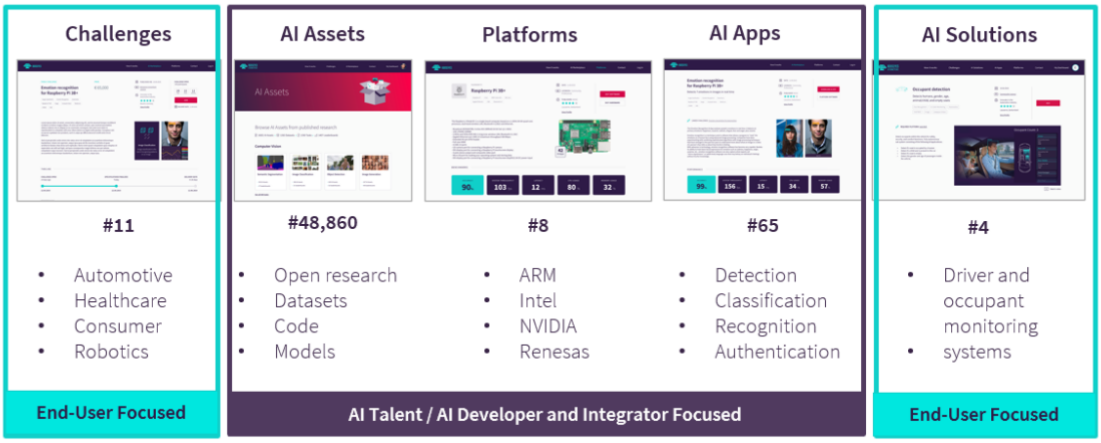
Distributed AI Marketplace

Secure collaborative platform for building and trading AI applications

By subscribing, I agree to Bonseyes Privacy Policy

*Figure 6 Bonseyes AI Marketplace*

The Bonseyes AI Marketplace provides to the researchers, data scientists, developers and industries the various number of AI Assets and AI Artifacts.  Users can search, browse and bookmark AI Assets from the collection, as well they can create, publish, download, sell and buy AI Artifacts from the AI Marketplace. Industries can create a challenge and open a tender for its solution, on the other side developers and data scientists can join the challenge with the aim to solve the challenge and monetize their expertise. Figure 7 depicts the numbers of available AI Artifacts and AI Assets on the AI Marketplace.



Challenges

#11

- Automotive
- Healthcare
- Consumer
- Robotics

End-User Focused

AI Assets

#48,860

- Open research
- Datasets
- Code
- Models

Platforms

#8

- ARM
- Intel
- NVIDIA
- Renesas

AI Apps

#65

- Detection
- Classification
- Recognition
- Authentication

AI Talent / AI Developer and Integrator Focused

AI Solutions

#4

- Driver and occupant monitoring
- systems

End-User Focused

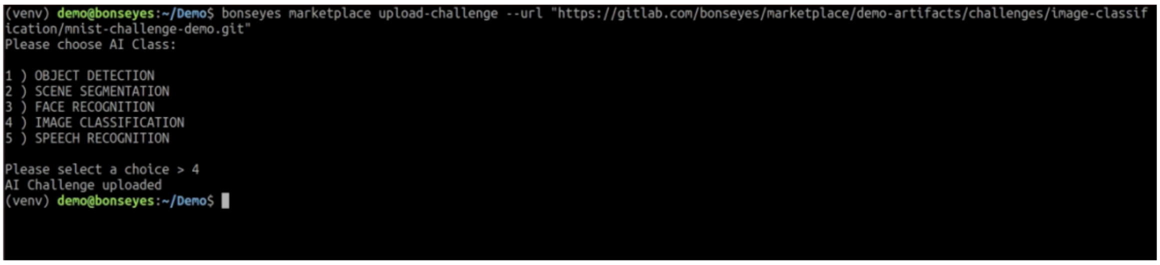
*Figure 7 AI Assets and AI Artifacts available on the AI Marketplace platform*

### 3.1.2 Secure Virtual Premise

Secure Virtual Premise is a platform tool that facilitate and secure collaboration with the privacy sensitive Artifacts in the process of the AI Solutions development. The SVP federates the required compute, storage, and execution environments. Marketplace users can use the SVP to securely and trustfully execute AI Assests, either remotely or locally, and orchestrate automatic chains of AI Assets, so-called AI pipelines.

### 3.1.3 Bonseyes command line (CLI) tool

The CLI tool is a Python-based tool for manipulating the various AI Artifacts developed or procured through the whole chain of the AI Solution development. From the AI Marketplace's perspective, the CLI tools enable functionalities for publishing and downloading purchased AI Artifacts. Figure 8 illustrates the CLI tool interface.



```
(venv) demo@bonseyes:~/Demo$ bonseyes marketplace upload-challenge --url "https://gitlab.com/bonseyes/marketplace/demo-artifacts/challenges/image-classif
ication/mnist-challenge-demo.git"
Please choose AI Class:

1 ) OBJECT DETECTION
2 ) SCENE SEGMENTATION
3 ) FACE RECOGNITION
4 ) IMAGE CLASSIFICATION
5 ) SPEECH RECOGNITION

Please select a choice > 4
AI Challenge uploaded
(venv) demo@bonseyes:~/Demo$ █
```

*Figure 8 Bonseyes CLI Tool interface.*

The CLI tool can be used to create challenges and use them (for instance to download data associated with a challenge and evaluation procedures). It can be used to create algorithm configurations that are the source of AI apps (they define how the neutral network models must be used and the pre/post-processing that is required). It can use deployment tools to generate AI apps from these configurations. Moreover, it allows users to manipulate the platform support packages: to build them and use them to set up some target hardware. Finally, it can be used to benchmark and demo AI apps on target hardware.

The CLI tool uses docker to execute the different tools and relies on the software shipped in platform packages to control and setup target hardware. It uses HTTP APIs to interact with the marketplace.

## 3.2 Security

The BonsAPPs project will provide a "Security-as-a-Service" (SaaS) concept that accelerates AI application design by off-loading AI developers from security engineering tasks and provides users with secure access to services and tools, enforcing IP rights of owners and enabling the industrialization of the collaborative innovation process. These tasks handle AI Artifact security and DRM management.

Next, we outline in the major concepts and techniques of BonsAPPs' security architecture such that the project's technology roadmap and implementation timeline can be understood. The technical details of the security architecture and mechanisms, however, will be described to a deeper extent in the upcoming BonsAPPs deliverable D3.1 on the "Initial Security Architecture", cf. [D3.1].

### 3.2.1 Initial BonsAPPs Security Architecture

An assessment of the AI development and deployment tools chains, of the project's implementation capabilities, and of the security risks has been carried out at the beginning of the BonsAPPs project. The starting point for the assessment and technical work was the original Bonseyes system architecture and security concept described in [Bonseyes D2.4]. The assessment led to refinement of this architecture which is depicted in Figure 9.

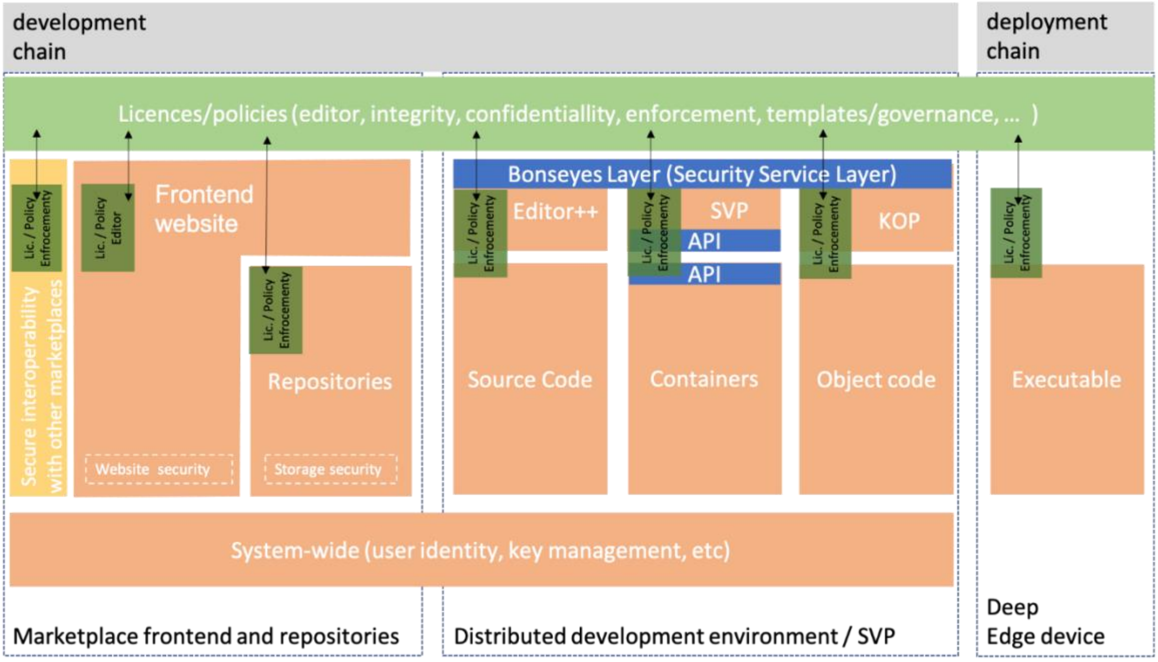

development chain
deployment chain
Licences/policies (editor, integrity, confidentiallity, enforcement, templates/governance, ... )
Lic. / Policy Enforcement
Secure interoperability with other marketplaces
Lic. / Policy Editor
Frontend website
Lic. / Policy Enforcement
Repositories
Website security
Storage security
Bonseyes Layer (Security Service Layer)
Lic. / Policy Enforcement
Editor++
Lic. / Policy Enforcement
SVP
API
API
Lic. / Policy Enforcement
KOP
Source Code
Containers
Object code
Lic. / Policy Enforcement
Executable
System-wide (user identity, key management, etc)
Marketplace frontend and repositories
Distributed development environment / SVP
Deep Edge device

*Figure 9 Concept BonsAPPs Security Architecture.*

### 3.2.2 Overview of the Security Architecture

This service concept is enabled by a consistent use of licenses for the AI Artifacts throughout the BonsAPPs systems. This system-wide use is indicated in Figure 5 by spanning the specification and enforcement process of licenses and policies over the whole system. The licenses and policies are facilitated by using machine- and, if possible, human-readable syntax, e.g., using the syntax permitted by the ORDL format. The enforcement of licenses is implemented locally by *policy enforcement points (PEPs)*.

Furthermore, the security architecture aims at handling the complexity of developing as well as deploying of AI applications. The complexity in these two steps originate from the handling and use of the different programming languages, operating systems and hardware capabilities at developer environments and at Edge and Deep Edge devices. Hence, the architecture addresses this by considering two different tool chains, cf. Figure 9:

1. the *Development Tool Chain*, which focuses on the collaborative AI development process and
2. the *Deployment Tool Chain*, which focuses on the generation, deployment, and execution of an AI application for use on the Edge or Deep Edge device.

Moreover, the development workflow in BonsAPPs's AI application design process spans over two different sub-architectures: i) the central entities for engaging the AI developers with each other, i.e., the BMP frontend, the interoperability mechanisms with other AI marketplaces, and the central repositories for storing AI Artifacts (which will make the access to Artifacts persistent), and ii) the and collaborative, distributed, and secure development environment, the *Secure Virtual Premise (SVP).*

The BonsAPPs' SVP enables the developer tool chain to handle and secure three major types of generic objects and AI Artifacts:

- Source code / pure data objects: these objects are each a single file containing AI code or AI data (with or without comments; written using a human-readable programming language) usually formatted as plain ASCII text.
- Docker images objects: this object type the is read-only template used to build container to store and ship applications
- Object code and library objects: this object is a sequence of statements or instructions in a machine code language (i.e., binary) or an intermediate language

The SVP will handle these generic object types in a consistent way and enforces the licenses and policies attached to them. The consistent enforcement is coordinated by the *Bonseyes Layer.* It acts a separator, i.e., it shields the object from direct access, and provides APIs to the development and deployment tools chains. The layer checks the authenticity and authorization of the developers which use these APIs.

### 3.2.3 Industrialization and Security Services

The BonsAPPs project focuses on the industrialization of the Bonseyes' collaborative AI development process. Hence, the assessment of the BonsAPPs development and deployment tool chains revealed that the concepts and techniques for secure application deployment on devices are complex but already well investigated and available. Thus, BonsAPPs applies already available technologies in this chain. The assessment revealed also that the major hurdles in the industrialization are the consistent support of security in the development tool chains. Hence, major project resources will to be devoted to supporting this part of the development process, see below.

### 3.2.4 Focus Areas of Engineering the Security-as-a-Service Concept in the BonsAPPs Architecture

Given the wealth of security objectives in the development and deployment chains, their assessment guided the BonsAPPs project to focus on six main areas for security tools, functions, and service for the Security-as-a-Service Concept: four security tools and toolkits and two additional system-wide service areas:

1. A *License Management tool:* this tool will enable the joint definition and agreement of licenses by stakeholders in AI development and which have engaged in the BMP.
2. A *Secure Deployment tool:* this tool supports the secure deployment of software on end devices, i.e., it supports the Deployment Tool Chain.
3. *Secure Transfer, Storage and Marketplace Interoperability Tools:* this tool is a set program and functions to enable the secure transfer of AI Artifact among interoperable marketplaces, from marketplaces to developers, and the secure and long-term storage of AI Artifacts for later use.
4. *Trusted Computing as a Service Tool:* this tool is the refinement of the Bonseyes SVP tool such that the SVP and the Bonseyes Layer can handle a larger variety of generic types of AI Artifacts, (see above) and that the distributed execution environment becomes more defensible against attacks.
5. *Frontend Security:* this group of activities addresses the security of marketplace web frontend, which is the first visible BMP entity for any user .
6. *System-wide Services for Security:* services that enable the concise and correct operation of BonsApps security mechanisms in all entities within the development tool chain.

### 3.2.5 System-Wide Services for Security

In addition to the above-described development of tools, certain system-wide services for security mechanisms in the for BonsAPPs' "Security-as-a-Service" concept are needed to enable the use of the tools and to enforce of system policies and licenses. These services do not directly enforce policies but their concise and correct operation enables system-wide trust in the security mechanisms. These base security services are: a) a concise User Identity management for developers and b) a scalable and efficient Cryptographic Key and Certificate management for developers.

**a) User Identity**

In order to ensure compatibility across various platforms, BonsAPPs is going to inherit the user identity and key management strategies from the Bonseyes project, as described in the corresponding project deliverable (Section 11.2 in [Bonseyes D2.4]). In the context of BonsAPPs community as well as associated external platforms, user identity and key management is an interoperability component that permits identity exchange and makes accessible public data of individuals, and organizations. External Authentication and Authorization Identity Providers can be integrated into the BonsAPPs identity system to provide straightforward onboarding of new users from domain-related platforms. For instance, checking and validating the admin or user's identity during server or website access will be implemented through standard procedures, e.g., SSH authorized keys check, basic authentication protocol, Kubeconfig / k8s token, and client-side certificate.

Single Sign-On is an authentication scheme that allows a user to access multiple federated and domain related platforms with single credentials, directly providing better user experience and reducing the necessity of the user to have dedicated credentials for each of the platforms. However, BonsAPPs User Identity Management component will be subjected to investigation regarding the implementation feasibility of SSO (Single Sign-On) Identity Consumer. It has the potential to enable integration mechanism with the external SSO Identity Providers, including AI4EU/AI-on-Demand platform, which could allow the user to access the BonsAPPs AI Marketplace skipping the login step if it's already logged into the some of the external partner platform which Identity Provider is connected. Though it brings usability related advantages in this scenario, a careful evaluation is required to ensure the optimum threshold for balancing and defining tradeoff against functionality throughout the platforms. In general, authentication of the new users can be achieved through the external application authorization system that implements one of the industry-standard decentralized authentication protocols (SAML, OpenID, OAuth, etc.).

**b) Key Management**

In Secure Virtual Premise (SVP), the Public Key Infrastructure (PKI) was implemented with OpenSSL version 1.1.0. The entire PKI is based on X.509 public-key certificates. For generation, the OpenSSL tool is used within the Linux OS environment. First, the root certificate is generated to establish root certificate authority. Next, an intermediate certificate authority is generated to further issue a public certificate and private key pairs to all SVP participants who have a valid license. Further, users have to provide their certificate, public key, and valid license to establish HTTPS communication with the SVP and conduct the AI engineering process.

### 3.2.6 Security Concepts and Mechanisms in the Development Tool Chain

The security concepts and mechanisms for the development tool chains are structured into two categories. First, the security of the centralized BonsAPPs entities: *Frontend Security, License Management tool, Secure Transfer,* and *Storage and Marketplace Interoperability Tools.*

Second, the enhancement of the distributed SVP such that it becomes a hardened, collaborative development environment. This category comprises the activity for the Trusted Computing as a Service Tool.

#### 3.2.6.1 Frontend Security Engineering

*Frontend Website Security:* The security *mechanisms for the frontend of the BMP* will be designed and benchmarked using the CIA triad model (Confidentiality, Integrity and Availability). The security design will consider the implementation of the following website security mechanisms for the frontend: SSL/HTTPS, Cross site scripting (XSS) protection, Cross site request forgeries (CSRF) protection, SQL injection protection, Clickjacking protection.

*Frontend Admin Access Control:* The BMP implements multiple regulation techniques to restrict what and who can access the resources in computing environments (servers, websites, and others) for the BMP frontend. The control is achieved by IP restrictions for administration and website development environments that shouldn't be exposed to public and VPN only access for admins and developers.

*Frontend User Access Control:* The AI marketplace frontend aims at openness and attracting AI developers for enabling network effects in AI development. Once the developers find it useful to engage with each other by the website, system-wide identities will be provided (see above) and access and usage policies will be enforced on the website using these identities. Here, no IP restrictions or VPN restrictions are enforced.

#### 3.2.6.2 Secure Transfer, Storage and Marketplace Interoperability Tools

This group of tools and activities mainly aims at secure interoperability and the technologies need to be defined mainly in accordance with the collaborating marketplaces and projects, e.g AI4EU. However, parts of the Bonseyes architecture will be improved in parallel and hereby the focus is on integrating, access management and improving the security of offered AI Artifact storage entities.

*User Access to AI Artifact Repositories and AI Artifact Storage:* The access control mechanisms for centralized AI Artifact storage locations and repositories are inherited from providers such as GitLab and interconnected with the BonsAPPs licenses.

A more detailed discussion of the interoperability techniques and mechanisms with respect to AI Artifact functionality and semantic is provided in Section 3.3.

#### 3.2.6.3 Trusted Computing as a Service Tool: Enhancing the SVP to a Hardened and Distributed Development Environment

The Bonseyes SVP [TIT20] has demonstrated the technical capabilities of Bonseyes' collaborative AI development concept on TRL level 3/4 [Bonseyes D2.4]. The aims of BonsAPPs activities on *Trusted Computing as a Service* are to increase the TRL level and security levels, as well as to improve the distributed management and orchestration of the AI development. Hence, the development and refinement of the SVT tool comprises two categories of activities:

### 3.2.7 Reliable management and distributed setup of a multi-site SVP:

Figure 10 shows the concept of a multi-site SVP [Bonseyes D2.4]. Here, an SVP user can choose from many execution resources located at different sites at an SVP Rendezvous Host (SVP-RH). A user can reserve and combine the selected computing nodes from different locations/sites and bind them securely into a dedicated SVP instance. Furthermore, the SVP-RH manages interoperable user profiles, including their cryptographic key and certificates. This implementation shows that a virtual and flexible on-demand edge developing environment can be achieved.

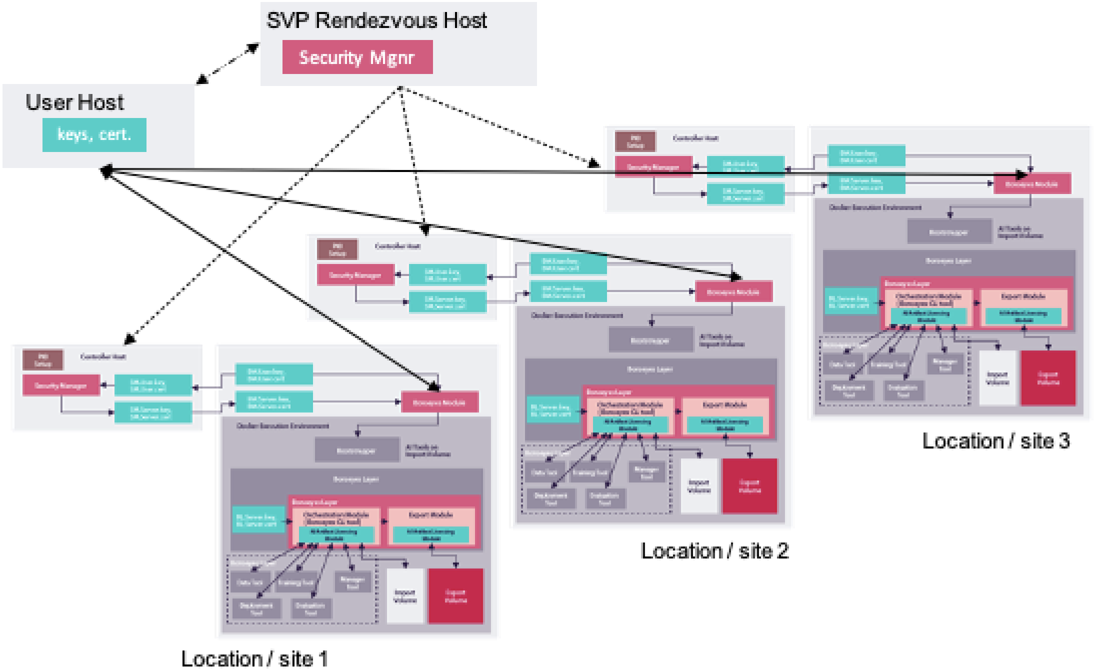
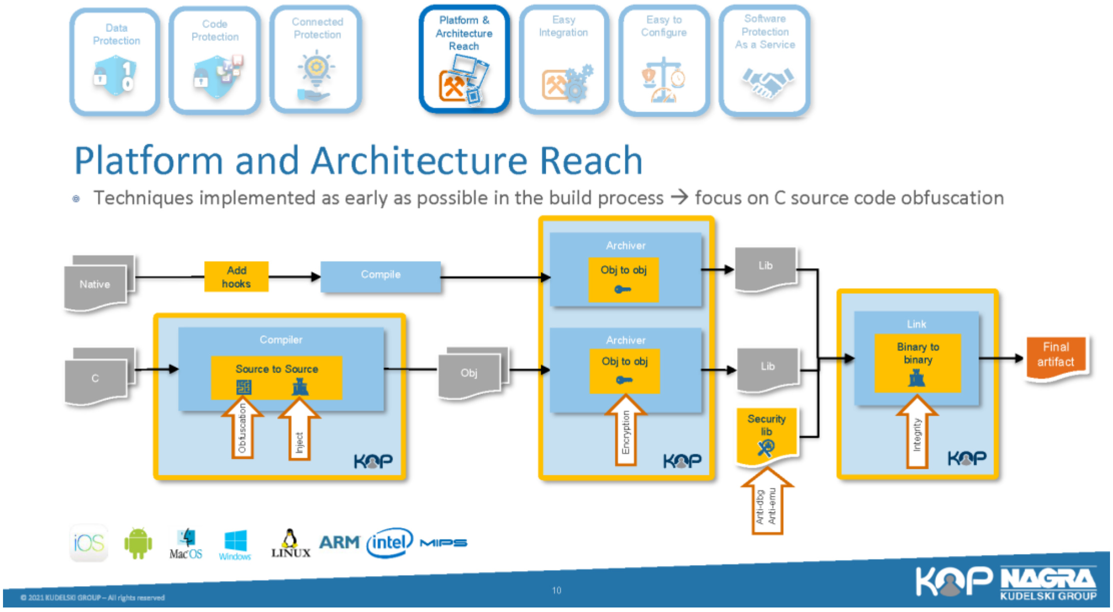


*Figure 10 Concept of a Multi-site SVP*

### *3.2.7.1 Handling of additional generic types of AI Artifacts by the Bonseyes Layer*

The technical readiness level (TRL) of the SVP is further increased by permitting two more generic AI object categories:

1. *Source code / pure data objects:* it is currently considered to offer and to embed an encryption and decryption mechanisms for editors for source code / data into the Bonseyes Layer. Hereby, the Bonseyes Layer validates the authenticity and authorization of developers toward the license for this Artifact and shields the Artifact from unauthorized access to its content.
2. *Object code and library objects:* An object code obfuscation mechanism is applied here which is based on the technologies provided by Kudelski's KOP and IoT keySTREAM™ tools [keySTREAM]. A brief outline on the code obfuscation process of Kudelski's KOP tool is provided in Figure 11.



Platform and Architecture Reach

- Techniques implemented as early as possible in the build process → focus on C source code obfuscation

*Figure 11 KOP's c object code obfuscation mechanism*

### 3.2.7.2 Security Concepts and Mechanisms in the Deployment Tool Chain

BonsAPPs will re-use such an established industrial solution for supporting the final software deployment.

The security for deploying and executing an AI application binary on the Edge or Deep Edge device will be enabled by using Kudelski's KOP and IoT keySTREAM™ tools and products [keySTREAM]. KOP provides mechanisms for encrypting functions, object files or static libraries of any native language. In addition, it protects the integrity all the binary and prevents the debugging or the emulation of the application.

## 3.2.8 AI Artifact Licensing

A collaborative AI development process is an attractive alternative to the monolithic "do-all-yourself" approach, cf. [Bonseyes D2.4]. It increases the speed of development, allows for risk sharing, and reduces the cost of ownership. Such a collaborative process, however, is difficult for the companies to implement as they fear the loss of control over their AI Artifacts, such as data or trained models, due to the threats by potential misuse or IPR theft when sharing these AI Artifacts with third parties.

One way to tackle this problem is to provide an end-to-end licensing support along the complete development and supply chain. Owner of AI Artifacts issue a redistribution license to the distributor (the BMP in our case), that allows the marketplace to perform certain actions. The BMP itself together with the engaged stakeholder, can then create appropriate licenses for the end-users (buyers) of an AI Artifact. These licenses need to be enforced whenever an action is to be performed on the actual AI Artifact.

## 3.2.9 Open Digital Rights Language and System Overview

The BonsApps architecture will use the Open Digital Rights Language (ODRL) [ORDL18a, ORDL18b] to describe and exchange licenses. ORDL has become a standard for defining licenses, especially in the publishing market. Technically ODRL licenses can be represented in XML, RDF, or JSON, and for the purposes of the BMP we used JSON to represent the licenses [ORDL21]. Figure 12 shows an excerpt from the *information model* of an ODRL license.

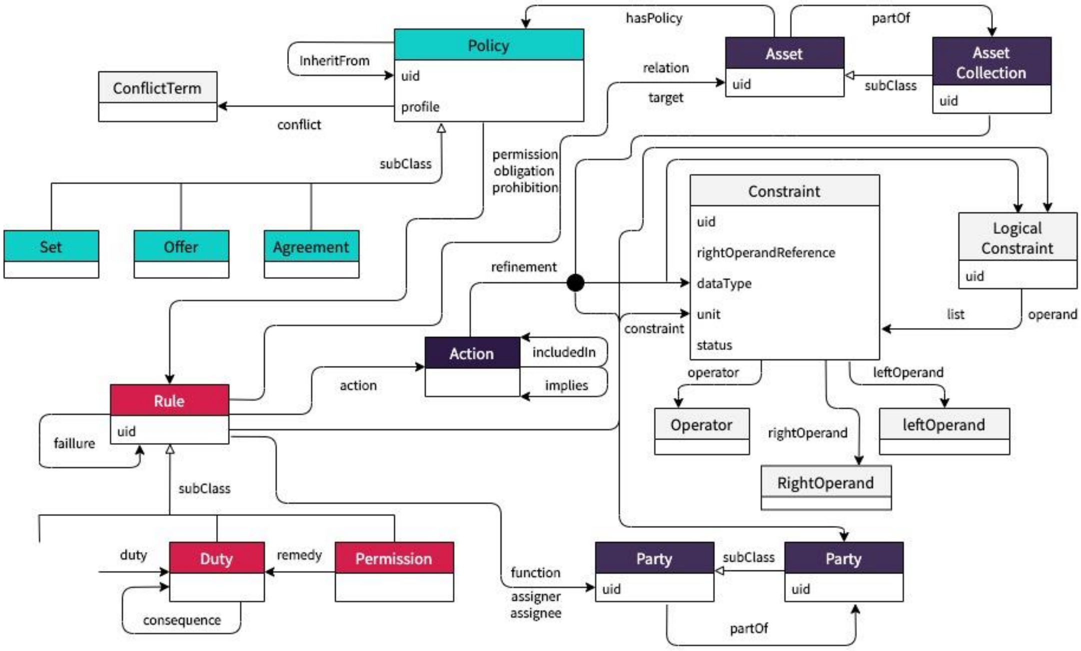
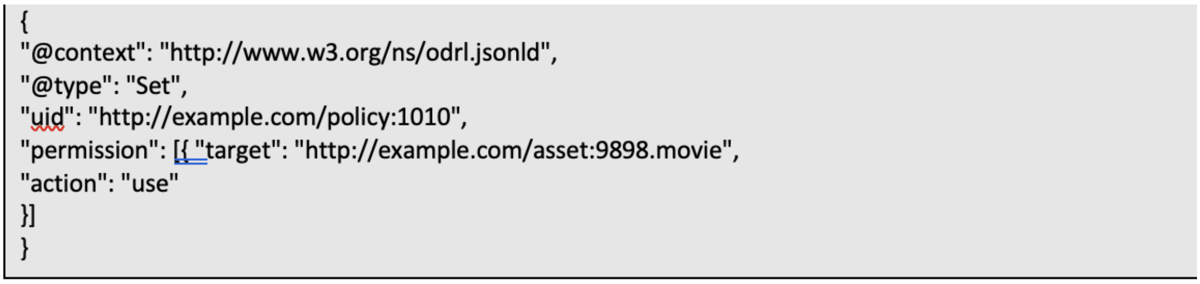


*Figure 12 ODRL information model for specifying digital rights, cf [ORDL18a]*

*The ODRL information model:* A *Policy* can be created for an AI Asset and is made up of a set of *Rules*. A Rule itself applies to a specific *Action* and can be further refined using a set of *Constraints*. A Rule itself is either a *Permission* (an Action the licensee can perform), or a *Prohibition* (an Action the licensee is not allowed to perform). For the purposes of the BMP, we will make no use of the *Duty* object. Figure 13 shows an ODRL example policy can be read as "Movie 9898 can be used", cf. also [ORDL21].



```
{
"@context": "http://www.w3.org/ns/odrl.jsonld",
"@type": "Set",
"uid": "http://example.com/policy:1010",
"permission": [{ "target": "http://example.com/asset:9898.movie",
"action": "use"
}]
}
```

*Figure 13 Example licenses written in JSON*

### 3.2.10 Overview of the BonsAPPs Licence Management System

The licenses for AI Artifacts are handled by the *BonsAPPs Licence Management System* which is outlined in Figure 14. The system is based on the license concept developed in Bonseyes [Bonseyes D2.4]. The system starts on the Authors premises, where once an AI Artifact has been created, a *Redistribution License* needs to be created (with support from templates provided by the BMP) which defines the rights for engagement among developers on the BMP. This functionality is provided by the *Author Licensing Tool,* which is also support by an online editor component in the BMP. The tool supports the authors with the creation of these licenses as well as other technical aspects related to this. The *Distributor Licensing Module* enhances the BMP with an API to work with these redistribution licenses. The BMP can retrieve information from such a license in order to provide the end-user flows in the BMP user interface. Additionally, this module can create end-user licenses that are distributed to the user of an AI Artifact. Lastly, the *Artifact Licensing Module* enforces end-user licenses in the actual AI Artifact. This includes verifying that the license has not been tampered with, and that the action a user would like to perform is allowed given a specific license.

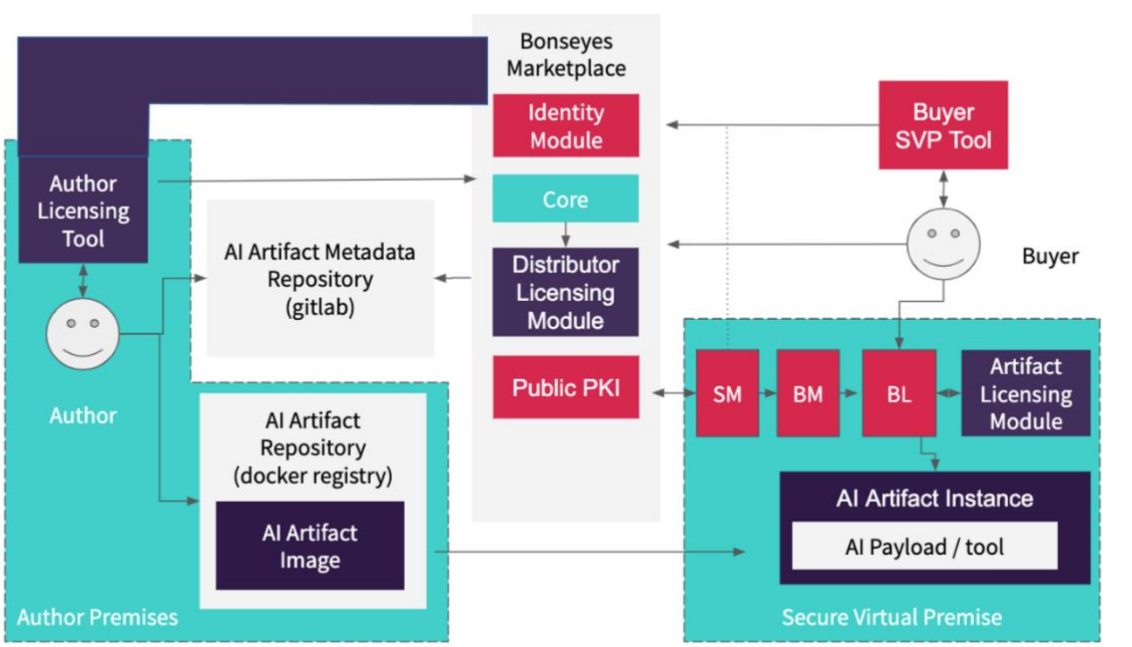


*Figure 14 Overview of the Bonseyes ecosystem and the BonsAPPs Licence Management System with the different licensing modules (in red).*

## 3.3 Bonseyes AI Marketplace Interoperability

### 3.3.1 Bonseyes AI Marketplace API

The AI Marketplace API provides an interface to the Bonseyes AI Marketplace services. From the conceptual side Marketplace API services can be broken down into two main parts.

- **Community** service is oriented around ‘Actors’, specialized professionals (Users) and Organizations that they are representing, providing a professional networking platform for matchmaking in both directions. Finding the right professional for the AI Solution development or state-of-the-art industry challenges to work on. AI Marketplace User and Organization profiles can be managed through the API.
- **AI Artifact** service provides discovering, searching and management of the AI Artifacts. Each AI Artifact distribution and usage permission is defined with the license and secured with the Licensing Module. AI Artifacts in the domain of the AI solutions development represent reusable components that can speed up the process and reduce development costs. Manipulation with the AI Artifacts is also available through the Bonseyes CLI Tool.

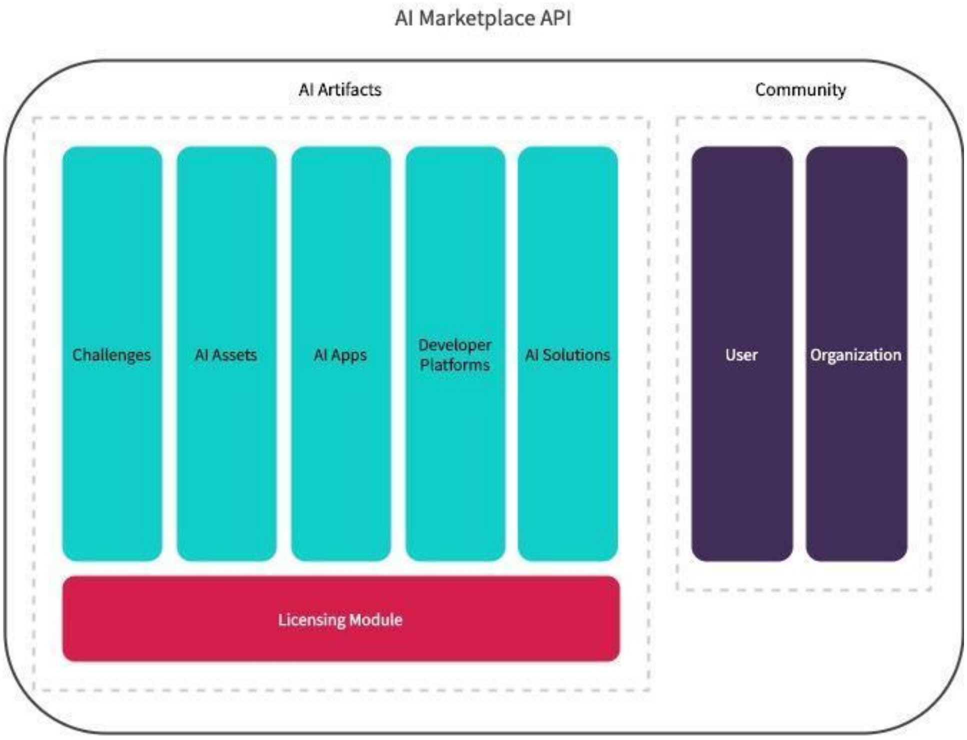


*Figure 15 AI Marketplace API description*

Available functionalities provided through the Marketplace API can be divided in four main categories:

a) **Search and Discovery of the AI Artifacts:** One of the main functionalities of the AI Marketplace is to provide discovery and search of the AI Artifacts to the interested parts. All AI Artifacts available on the AI Marketplace can be discovered and searched through the API, providing different filtering options.
b) **Publishing and management of the AI Artifacts:** AI Artifacts can be published on the AI Marketplace through the API, respecting required format for the specific AI Artifact. Challenge, AI App and Developer platform needs to be in a form of the git repository hosted on the GitLab, containing manifest files and redistribution license inside the repository sources. AI Asset publishing requires paper and code references.
c) **Downloading of the AI Artifacts:** Downloading of the AI Artifacts is provided through the API, downloadable AI Artifacts are joined Challenges or AI App and Developer Platforms that the user has a right to download (that are purchased).
d) **User and Organization management:** Users and Organizations represent different 'Actors' in the process of the AI Solution development. Through the API each User can create Organization, and can be listed as an organization member. User and Organization information can be changed performing different API functions.

In order to enable interoperability and add new services on the AI4EU platform, BonsAPPs will define and propose a dedicated API to this effect. If agreed by both parties, an API could also be provided to allow new services developed by BonsAPPs to store and retrieve data on AI4EU related to these new services (see 3.1.1.3).

# 4 BonsAPPs AIaaS Roadmap

Edge AI leverages the fact that training and deployment processes for a ML model are completely decoupled. It allows a trained ML model to be embedded in devices with limited memory and computational resources — enabling their execution in an offline fashion.

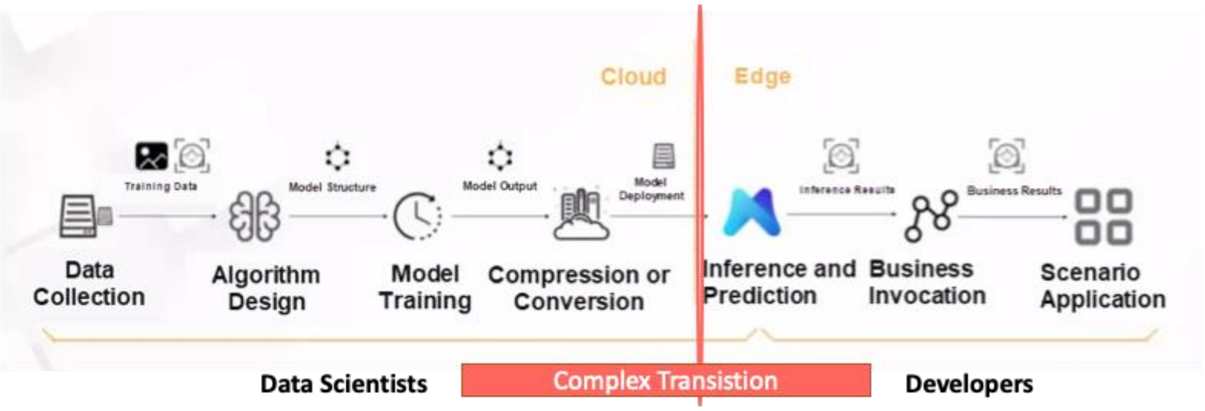


*Figure 16 Edge Deployment Challenges*

Unfortunately, deploying ML models on edge devices still remains a very challenging task. This complex process involves both the cloud and edge devices, requiring data scientist, developers and embedded developers to work together to implement the related applications. In particular, the following factors need to be considered while designing an Edge AI solution:

- **Model design:** The goal is to reduce the model's inference time on the device. Deep Neural Networks (DNNs) often require storing and accessing a large number of parameters that describe the model architecture. We thus need to design DNN architectures with reduced number of parameters. SqueezeNet is a good example of efficient DNN architecture, optimized for Computer Vision use-cases. Neural Architecture Search (NAS) can also be used to discover edge efficient architectures.
- **Model optimization:** Edge devices have limitations not only in terms of computational resources, but also memory. There are mainly two ways to perform neural network optimization: Lowering precision and fewer weights (pruning). By default, model parameters are float32 type variables, which lead to large model sizes and slower execution times. Post-training quantization tools, e.g., Onnxruntime, can be used to reduce the model parameters from float32 bits to unit8, at the expense of (slightly) lower precision. Pruning works by eliminating the network connections that are not useful to the NN, leading to reduction in both memory and computational overhead.
- **Model conversion and export:** Model conversion and export represent quite intensive engineering jobs that require hands-on experience with the tooling and inference engines for the targeted formats. If not automated, this task can drastically slow down the process of the model deployment.
- **Model repository:** storing and tracking of the trained, pre-trained and exported models requires a systematic approach in order to deal with the complexity where new models come as AI Artifacts from different processes, compression, quantization and training experiments.
- **Hardware (Device) considerations:** Machine learning/Deep learning algorithms are characterized by extensive linear algebra, matrix and vector data operations. Traditional processor architectures are not optimized for such workloads, and hence, specialized

processing architectures are necessary to meet the low latency requirements of running complex ML algorithm operations. As such, factors to be considered while choosing the edge device include balancing the model architecture (accuracy, size, operation type) requirements with device programmability, throughput, power consumption and cost.

*To address the above challenges, The AI-as-a-Service layer (AIaaS) layer (Figure 17) enhances the Bonseyes AI Marketplace Platform described in the previous section to provide an end-to-end experimentation to industrialization pipeline for AI solutions at the Edge and Deep Edge.*

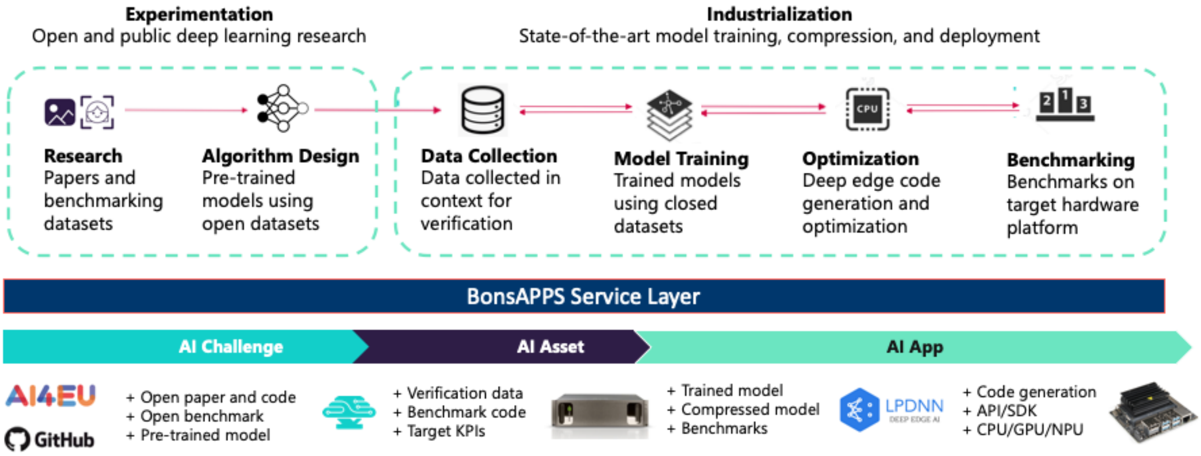


*Figure 17 BonsAPPs AIaaS Layer*

In the following sections, we are presenting a detailed roadmap of the planned services and functionalities (see Figure 18), chronologically ordered into the releases:

1. **AIaaS v1 (month 12)**: Integrated AIaaS, interoperable with AI-on-demand platform and connected with HPC clouds, will be ready to be used by specific industry use cases from the first Round (M13-M17). The scope of some services and functionalities may be limited (see Table 1)
2. **AIaaS v2 (month 24)**: Apart from V1 improvements resulting from the lessons learnt from the first Round of Use Cases [WP5.5], new services and functionalities will be integrated and ready to be used by specific Use Cases from the second round (M25-M34).
3. **AIaaS v3 (month 36):** Improvements to solve bugs/inefficiencies detected during the second round of challenges. Aspects requiring further improvements will be incorporated into the end-of-project technical roadmap and guide future AIaaS releases foreseen in the Exploitation and Sustainability Plan [D6.6]

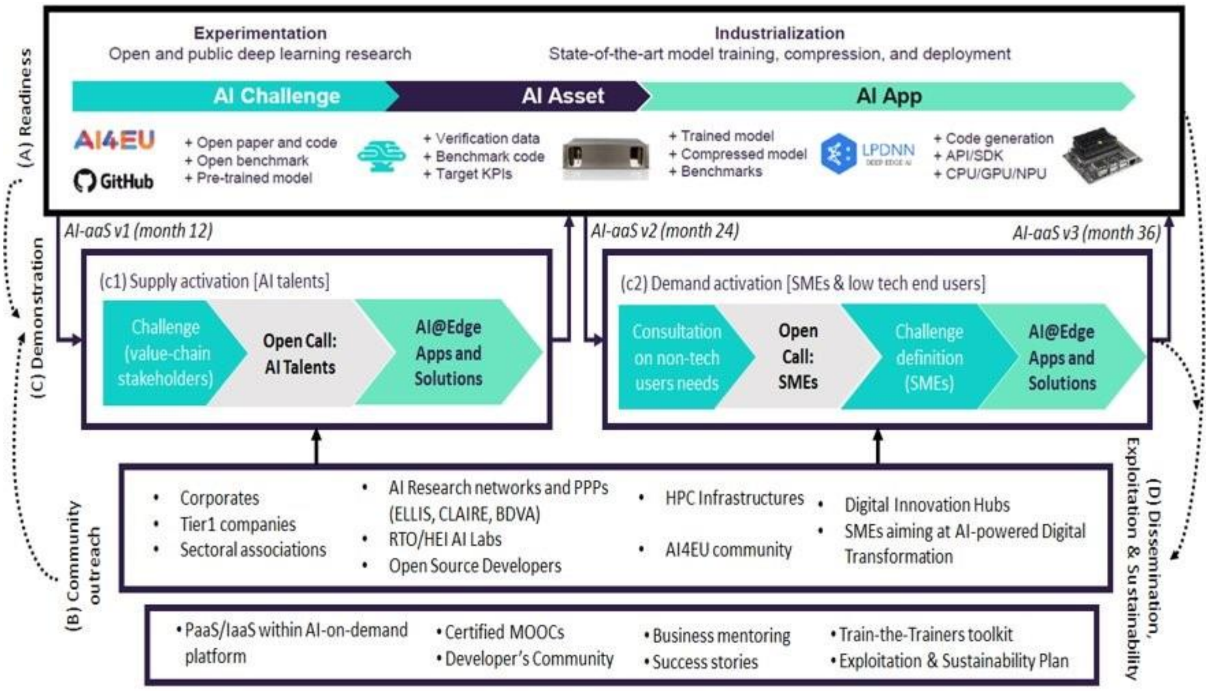


*Figure 18 AIaaS releases overview*

The service layer for the Edge and Deep Edge can be categorized into the three categories (see Figure 19): services used in training, deployment services and support tools.

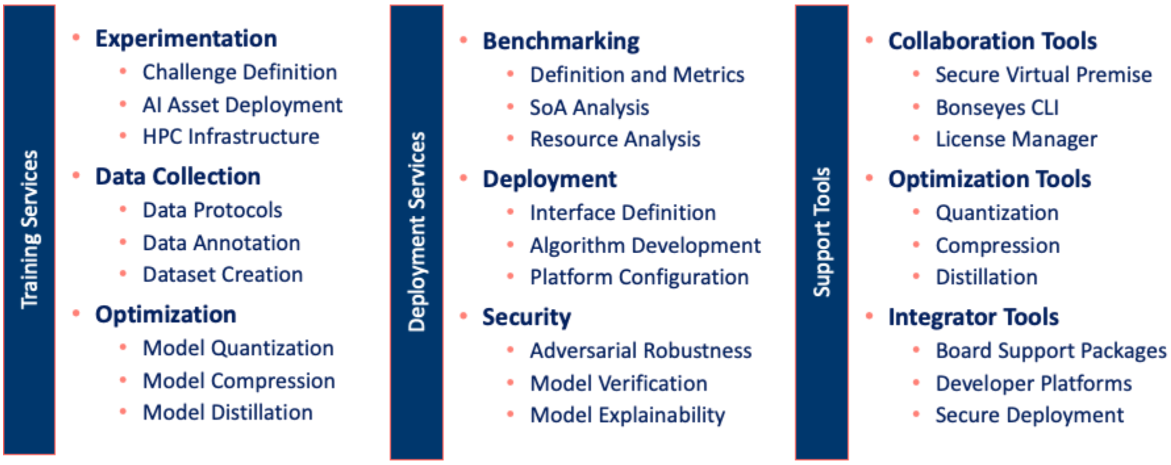
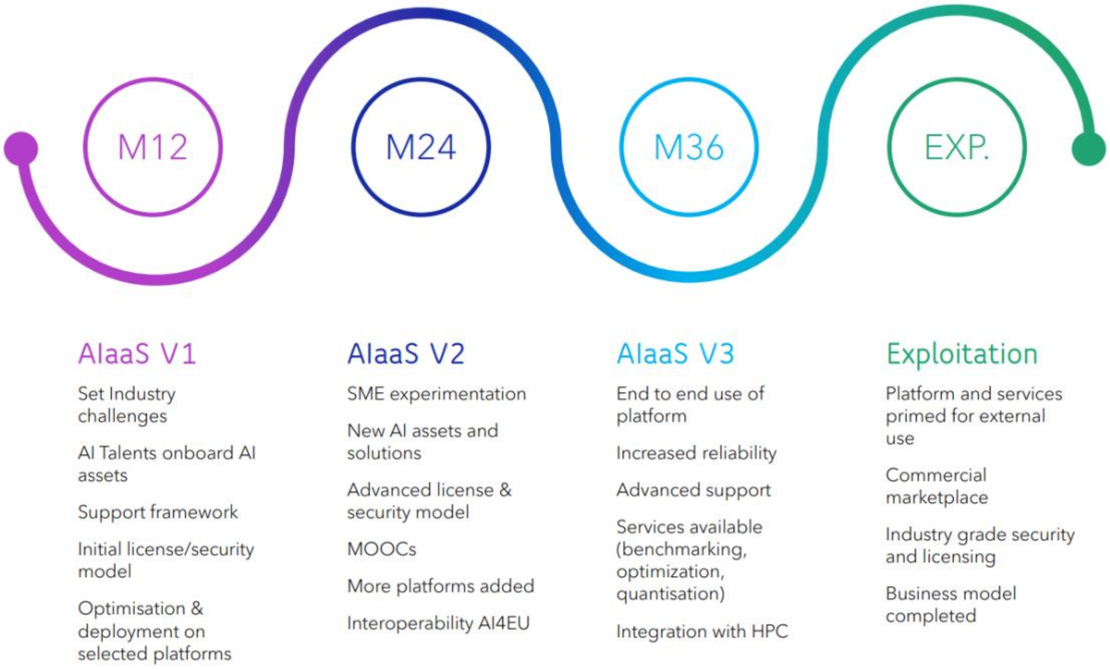


*Figure 19 Categorized service layer*

The roadmap for the three versions of the Services layer as well as exploitation is represented in the following diagram (Figure 20). A detailed technical description of the three releases is to be found in this section.



AIaaS V1

Set Industry challenges

AI Talents onboard AI assets

Support framework

Initial license/security model

Optimisation & deployment on selected platforms

AIaaS V2

SME experimentation

New AI assets and solutions

Advanced license & security model

MOOCs

More platforms added

Interoperability AI4EU

AIaaS V3

End to end use of platform

Increased reliability

Advanced support

Services available (benchmarking, optimization, quantisation)

Integration with HPC

Exploitation

Platform and services primed for external use

Commercial marketplace

Industry grade security and licensing

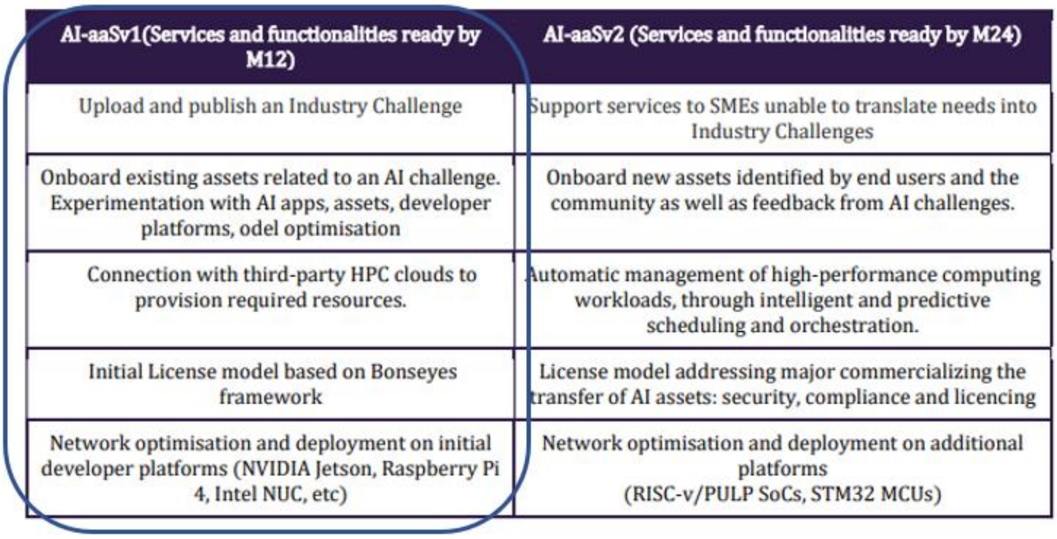
Business model completed

*Figure 20 High level roadmap*

## 4.1 AIaaS V1 - Supply Activation

The first release is focused on the ‘supply’ side of the Marketplace, represented by AI Talents, with a view to provide a specific AI-as-a-service (AIaaS) for the development and integration of AI solutions at the Edge and Deep Edge, based on the AI distributed marketplace concept tested and validated during the Bonseyes project.

Additional features will be added to bring AI innovation into the market, including a secure computing environment; a licensing model that allows re-use of AI Assets while respecting privacy and ownership of data; and a wide range of deployment possibilities, covering the most relevant developer platforms. These functionalities will be used by AI Talents during the first Open Call and learning will be incorporated in the service set-up.



| AI-aaSv1(Services and functionalities ready by M12) | AI-aaSv2 (Services and functionalities ready by M24) |
|---|---|
| Upload and publish an Industry Challenge | Support services to SMEs unable to translate needs into Industry Challenges |
| Onboard existing assets related to an AI challenge. Experimentation with AI apps, assets, developer platforms, odel optimisation | Onboard new assets identified by end users and the community as well as feedback from AI challenges. |
| Connection with third-party HPC clouds to provision required resources. | Automatic management of high-performance computing workloads, through intelligent and predictive scheduling and orchestration. |
| Initial License model based on Bonseyes framework | License model addressing major commercializing the transfer of AI assets: security, compliance and licencing |
| Network optimisation and deployment on initial developer platforms (NVIDIA Jetson, Raspberry Pi 4, Intel NUC, etc) | Network optimisation and deployment on additional platforms<br>(RISC-v/PULP SoCs, STM32 MCUs) |

*Figure 21 AI-aaSv1 and AI-aaSv2*

## 4.1.1 Bonseyes AI Marketplace (BMP)

The Bonseyes AI (Data) Marketplace represents one of the main components developed in the previous Bonseyes project. In order to assess the maturity of the platform, four validation use-cases [Validation Report D2.5] were conducted as a different industry representative. Subsequent to validation use-cases it was assessed that Bonseyes AI Marketplace meets the criteria for technology readiness level 5 (TRL5) [TRL].

Continuation of Bonseyes AI Marketplace development, as well as the development of the AI-as-a-service layer through the BonsAPPs project, sets as one of the main objective increase of the technology readiness level. In order to meet the objective, addressed are crucial points: platform infrastructure, enhancement of the major features and enhancements based on a feedback collected from the first open calls.

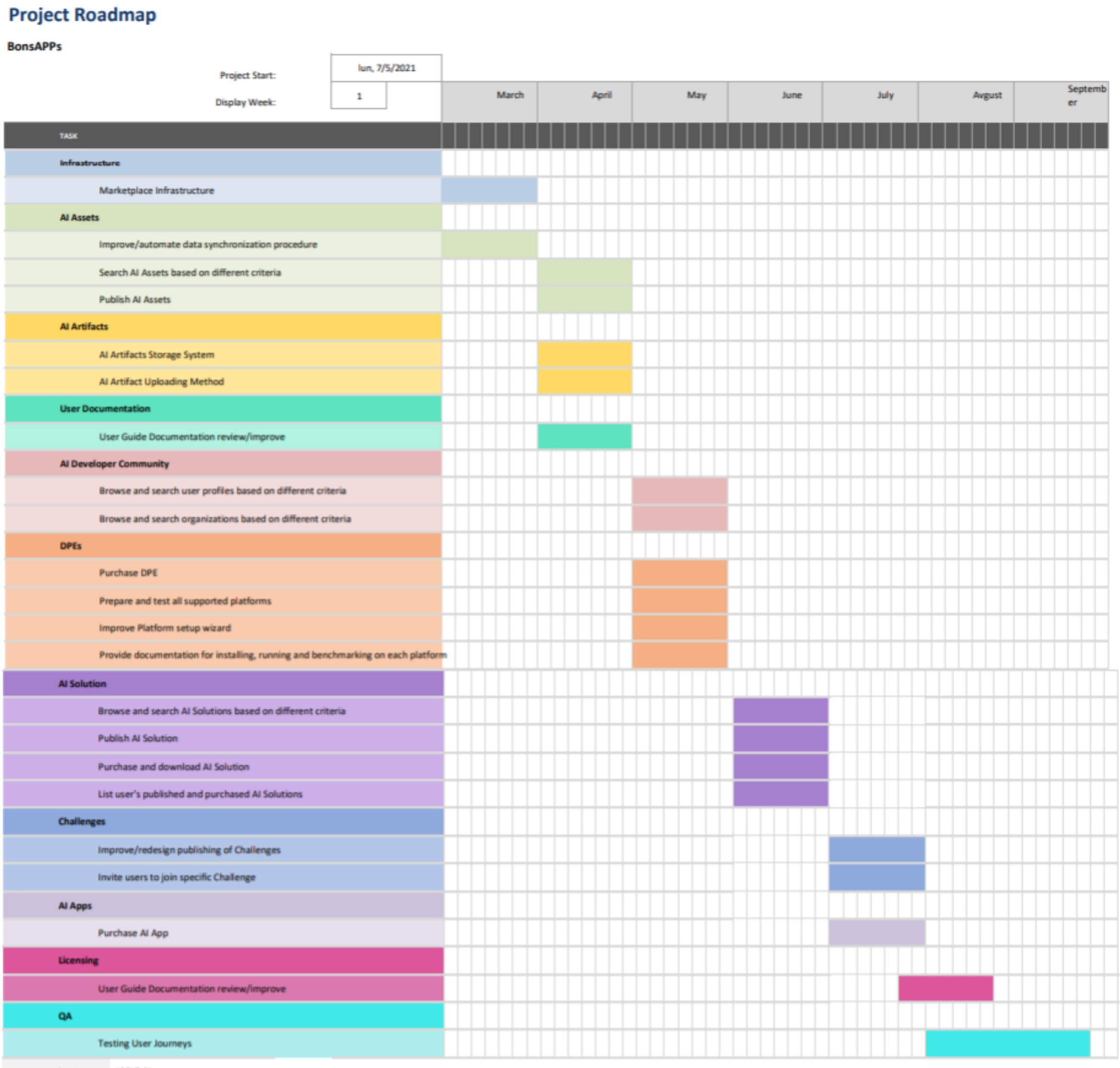
### *4.1.1.1 Platform Infrastructure*

The selection and configuration of the infrastructure on which the platform will be hosted is a very sensitive question. In order to increase the platform market readiness level, the following platform infrastructure criteria need to be met:

- Increase reliability of the platform,
- Increase security and attack prevention and signalizing system,
- Enable system failure self-healing,
- Enable vertical and horizontal scalability both on the computational power and storage size,
- Enable easy integration with the HPC providers.

### *4.1.1.2 Enhancement of the Major Features*

Developers' activities summary - Gantt chart (AIaaS V1): The diagram in Figure 22 summarizes the planned activities from the project developers towards implementing AIaaS V1. These cover all functionalities, AI Asset, AI Artifacts and infrastructure aspects being developed outside Security items.



**Project Roadmap**

BonsAPPs

Project Start: lun, 7/5/2021

Display Week: 1

| TASK | March | April | May | June | July | August | September |
|---|---|---|---|---|---|---|---|
| **Infrastructure** | | | | | | | |
| Marketplace Infrastructure | ■ | | | | | | |
| **AI Assets** | | | | | | | |
| Improve/automate data synchronization procedure | ■ | | | | | | |
| Search AI Assets based on different criteria | | ■ | | | | | |
| Publish AI Assets | | ■ | | | | | |
| **AI Artifacts** | | | | | | | |
| AI Artifacts Storage System | | ■ | | | | | |
| AI Artifact Uploading Method | | ■ | | | | | |
| **User Documentation** | | | | | | | |
| User Guide Documentation review/improve | | ■ | | | | | |
| **AI Developer Community** | | | | | | | |
| Browse and search user profiles based on different criteria | | | ■ | | | | |
| Browse and search organizations based on different criteria | | | ■ | | | | |
| **DPEs** | | | | | | | |
| Purchase DPE | | | ■ | | | | |
| Prepare and test all supported platforms | | | ■ | | | | |
| Improve Platform setup wizard | | | ■ | | | | |
| Provide documentation for installing, running and benchmarking on each platform | | | ■ | | | | |
| **AI Solution** | | | | | | | |
| Browse and search AI Solutions based on different criteria | | | | ■ | | | |
| Publish AI Solution | | | | ■ | | | |
| Purchase and download AI Solution | | | | ■ | | | |
| List user's published and purchased AI Solutions | | | | ■ | | | |
| **Challenges** | | | | | | | |
| Improve/redesign publishing of Challenges | | | | | ■ | | |
| Invite users to join specific Challenge | | | | | ■ | | |
| **AI Apps** | | | | | | | |
| Purchase AI App | | | | | ■ | | |
| **Licensing** | | | | | | | |
| User Guide Documentation review/improve | | | | | ■ | ■ | |
| **QA** | | | | | | | |
| Testing User Journeys | | | | | | ■ | ■ |

*Figure 22 Gant chart for the development activities in AIaaS V2 (ex-security)*

### 4.1.1.3 Interoperability of the Service Layer with the AI-on-Demand platform

The BonsAPPs project is tasked with defining and developing new services to be exposed and accessed by the AI4EU community with a focus on real-world application services necessary to resolve industry challenges, in particular with respect to edge intelligence solutions deployed on low-power cyber physical systems. The AI4EU project is focused on a broader scope beyond machine learning applications; also, it is limited to the community layer functionalities rather than the industry facing value-added services, which are the focus of BonsAPPs. The current AI4EU platform development roadmap envisages the interoperability with external services, specially to provide ‘experimentation services’ (trial spaces, playground, benchmarking) as well as access to computing infrastructures. This line of work reflects the conclusions of preliminary work done in AI4EU’s Working Group on ‘Interoperability and External Partners’ and mentions, as an example of the type of added-value external services that need to be added to AI4EU’s catalogue of services, the Bonseyes AI Marketplace Platform.

The BonsAPPs project intends to provide resources to implement interoperability with AI4EU. A particular focus will be on:

1. profile and identity management (single sign-on);
2. search function (bidirectional);
3. access to Asset/resources catalogue;
4. exchanging components with the other platforms such as the Bonseyes platform which will also integrate the new services developed by BonsAPPs.

Also, in order to enable interoperability and add new services on the AI4EU platform, BonsAPPs will define and propose a dedicated API to this effect. Such an API will be developed by the project and will ensure security and fairness of resources allocation, while preserving platform integrity. If agreed by both parties, an API could also be provided to allow new services developed by BonsAPPs to store and retrieve data on AI4EU related to these new services. To guarantee proper follow up of this process and coordination on a technical level, BonsAPPs is also present at the Technical Governance Board set up by AI4EU.

The key integration points that have been discussed are:

1. Integration of Community Layer (create, discover, search, deliver)
2. BMP services accessibility through the AI-on-demand platform
3. Development of new services on BMP visible on AI4EU

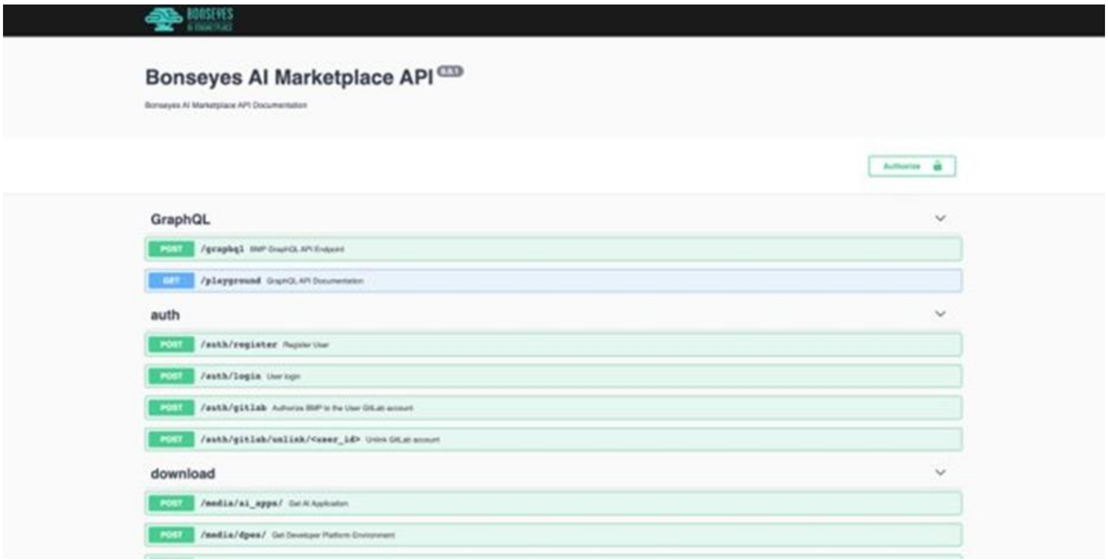
#### *4.1.1.4 Integration of Community Layer*

Create, discover, search and deliver. This layer defines data structures, denoted as metadata data structures, that describe AI Assets and AI Artifacts. Furthermore, it describes the translation of these data structures into similar metadata structures of other marketplaces. In addition, it provides APIs for forwarding searches to other marketplaces, indexing available Assets at these marketplaces, and publishing the Bonseyes Assets into other platforms such as AI4EU.

Bonseyes Interoperability focuses on describing, searching, browsing, discovery, publishing and categorization of AI Artifacts. By using the Bonseyes AI Marketplace APIs, external platforms can search and browse for AI Artifacts and display the results in their own system. The Bonseyes security layer permits only meta-data exchange between Bonseyes AI Marketplace and external platforms, keeping sources of the AI Artifact secured, respecting the permissions, prohibitions and distribution details defined inside the Redistribution License.

#### *4.1.1.5 BMP Services integration*

BMP services to be accessible through the AI-on-Demand-Platform (as playground and infrastructure services provided by external partners). BonsAPPs will define and propose a dedicated API(s) to this effect. There are already APIs in place to initiate the process.



Bonseyes AI Marketplace API

Bonseyes AI Marketplace API Documentation

GraphQL

POST /graphql BMP GraphQL API Endpoint

GET /playground GraphQL API Documentation

auth

POST /auth/register Register User

POST /auth/login User login

POST /auth/gitlab Authorize BMP to the User GitLab account

POST /auth/gitlab/unlink/<user_id> Unlink GitLab account

download

POST /media/ai_apps/ Get AI Application

POST /media/dpes/ Get Developer Platform Environment

*Figure 23 Bonseyes APIs for interoperability*

### *4.1.1.6 Development of new services visible on AI4EU*

The availability or access of new services developed by BonsAPPs on the AI4EU platform depends on a number of requirements and decisions to be clarified by AI4EU.

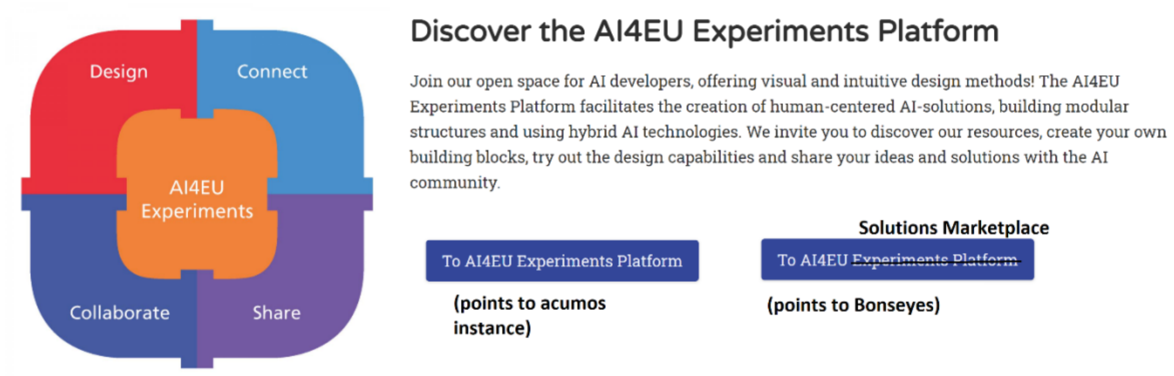
BonsAPPs will propose to the AI4EU Technical Governance Board (TGB) to initially focus on the first stage in terms of interoperability which is to enable single sign on access (SSO) to the Bonseyes AI Marketplace for the AI4EU community, where users will be able to access the functionalities, tooling and services developed by BonsAPPs and other projects.

Single Sign-On is an authentication scheme that allows a user to access multiple federated and domain-related platforms with single credentials, directly providing better user experience and reducing the necessity of the user to have dedicated credentials for each of the platforms. Bonseyes Identity Management component implements SSO (Single Sign-On) Identity Consumer that enables integration mechanism with the external SSO Identity Providers, that will allow user to access the Bonseyes AI Marketplace skipping the login step if it is already logged into the some of the external partner platform which Identity Provider is connected. Authentication of the new users can be achieved through the external application authorization system that implements one of the industry-standard decentralized authentication protocols (SAML, OpenID, OAuth, etc.).

The proposal for initial interoperability is as follows:

1. Create a separate page on the AI4EU platform called Bonseyes AI Marketplace (BMP) with link to the signup page, using the AI4EU identity provider. This page will point to Bonseyes AI Marketplace, and the community will be ab already le to create a BMP account with AI4EU account.
2. To achieve this BCA will need to gain access to identity provider, so as to enable SSO.
3. This is basically replicating the process in place between AI4EU platform and Acumos, and will enrich the platform with enhanced functionalities, with initially a focus on additional content on BMP and the ability to conduct experimentations end-to-end including deployment of AI solutions on embedded systems platforms (Edge and Deep Edge devices).

The diagram below (Figure 24) illustrates how the A44EU website could point to the Bonseyes AI Marketplace for access to services and functionalities benefiting the AI4EU Community and provide value-added access under SSO.


Design
Connect
AI4EU Experiments
Collaborate
Share
To AI4EU Experiments Platform
To AI4EU ~~Experiments Platform~~

Discover the AI4EU Experiments Platform

Join our open space for AI developers, offering visual and intuitive design methods! The AI4EU Experiments Platform facilitates the creation of human-centered AI-solutions, building modular structures and using hybrid AI technologies. We invite you to discover our resources, create your own building blocks, try out the design capabilities and share your ideas and solutions with the AI community.

Solutions Marketplace

(points to acumos instance)

(points to Bonseyes)

*Figure 24 Interoperability and AI4EU community access to Bonseyes AI Marketplace*

In a further stage (4Q 2021), Bonseyes AI Marketplace Platform will provide APIs to AI4EU integrate further and enable bilateral traffic. These APIs are available to be deployed. This will enable access to Asset/resources catalogue; and exchanging components with the other platforms such as the BMP which will also integrate the new services developed by BonsAPPs. This will also require more resources to be deployed to achieve this stage.

### 4.1.1.7 Analysis of the strong integration/merger between two platforms

This analysis has been partially conducted and the next step is dependent on the sustainability model and entity to be put in place by the AI4EU project to maintain the platform beyond the end of the AI4EU project (December 2021). We have reviewed several options from a basic interoperability to a full integration between the two projects. Discussions will continue with the AI4EU representatives and the other ICT-49s to this effect.

In the longer term, the BonsAPPs services will in any case remain available and accessible on the Bonseyes AI Marketplace.

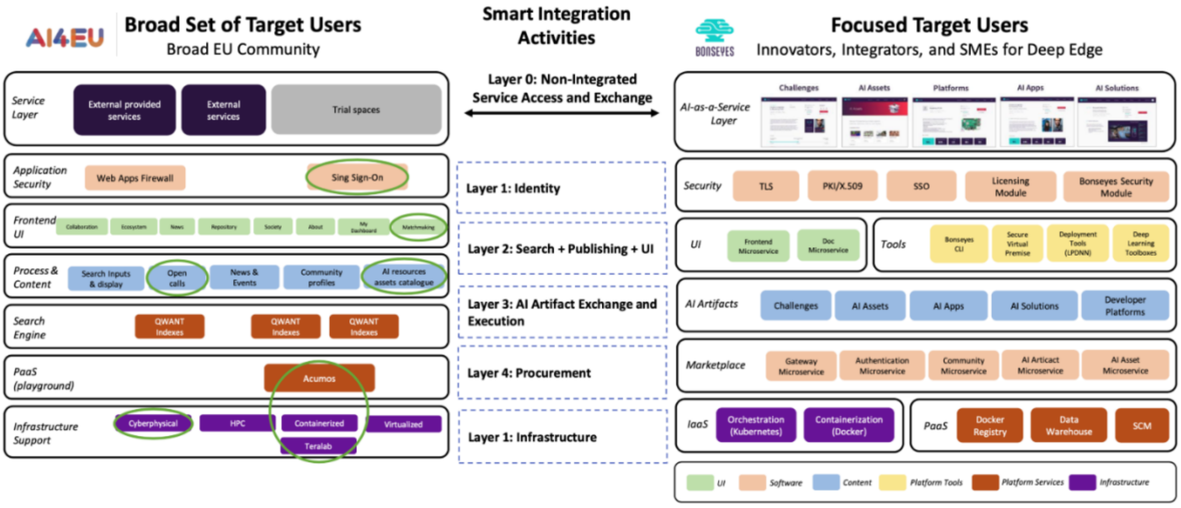


*Figure 25 Interoperability architecture for interconnecting Bonseyes AI Marketplace with AI4EU*

#### *4.1.1.8 Interoperability and connectivity with HPC Clouds*

Connectivity to the HPC cloud providers and software will enable automatic management of high-performance computing workloads. This will include definition of requirements and connectivity to on-premise HPC infrastructure for hybrid cloud computing in cases where sensitive data cannot travel to the cloud.

### 4.1.2 User Support Framework

For the AIaaS to be fully operative for third-party use, the technology development process described above must run in parallel to the development of appropriate mechanisms guiding the users of AIaaS. These mechanisms must be scalable and provide appropriate support to both end-users and AI Talents in a way that does not require high-intensity involvement by technical experts. The User Support will be based on three main components:

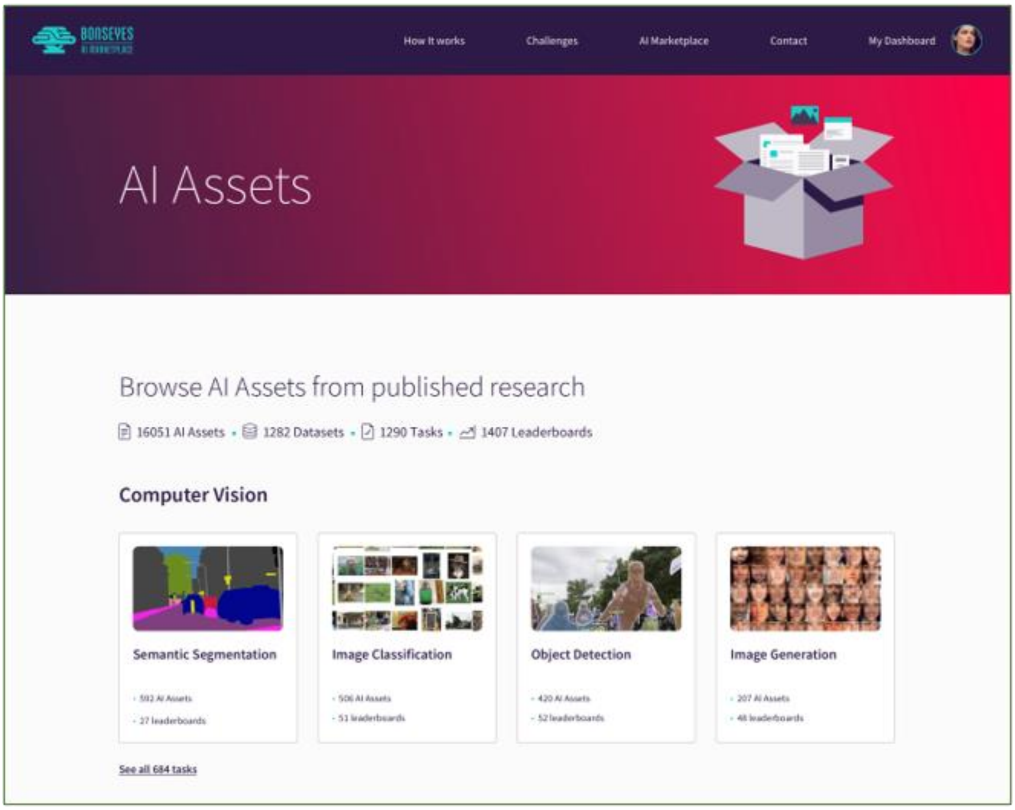
1. **Developer Community:** with the goal of providing collection of the open-source AI paper implementations (AI Assets), populated with the support of all technical partners. This will allow providing detailed User Documentation and Tutorials, and provide updates and clarification to the whole community, when required. Networking opportunity through the connection with the individuals or organizations that joined the Bonseyes AI Marketplace.
2. **AI Asset Container:** a Bonseyes AI Asset Container comprises of a Deployment Framework to provide a complete Python based workflow for end-to-end deployment of Deep Learning models to supported embedded hardware target platforms, Dependency Profiles for Target Environments to enumerate target runtime environments on various target hardware platforms supported by Bonseyes Developer Environments, Containers for Deep Learning providing a stable set of pre-installed software packages, and a definition of a Virtualized Host Environment to ensure combability where executing and running Bonseyes AI Asset Containers on various host systems.
3. **Certificate-supported Massive Online Open Course (MOOC) platform and 3 modules:** turning the existing User Documentation and Tutorials into a training cycle that will serve as a quality system to certify the proficiency of BMP users (end users, AI Talents) in the use of the AIaaS. This is also expected to be of special relevance to support the validation of entities offering AI services willing to participate in the second round of experiments. The implementation of this USF component is planned for the second year after the initial open calls.

#### *4.1.2.1 Developer Community*

In the V1 phase, the Developer Community will provide functionalities organised around three components: AI Assets (AI Research implementations), User and Organization Profiles and User Guides.

#### *4.1.2.2 AI Assets Marketplace*

In order to facilitate and accelerate the development of the AI systems, the Bonseyes AI Marketplace will provide a collection of the AI Assets that will be categorized by AI category (e.g., Computer Vision, Natural Language Processing), each category is sub-categorized by the AI task (e.g, Image Classification, Scene Segmentation). For the specific AI task, related AI Assets are ordered based on the benchmark results; benchmarks are data-driven and consist of specific dataset and evaluation metrics in order to assess the model performances. AI Assets are ordered by most credible benchmarks, providing leaderboard details of the evaluated models. Following that approach, AI Talents can quickly find the state-of-the-art AI Assets.



AI Assets

Browse AI Assets from published research

16051 AI Assets • 1282 Datasets • 1290 Tasks • 1407 Leaderboards

Computer Vision

Semantic Segmentation
- 592 AI Assets
- 27 leaderboards

Image Classification
- 506 AI Assets
- 51 leaderboards

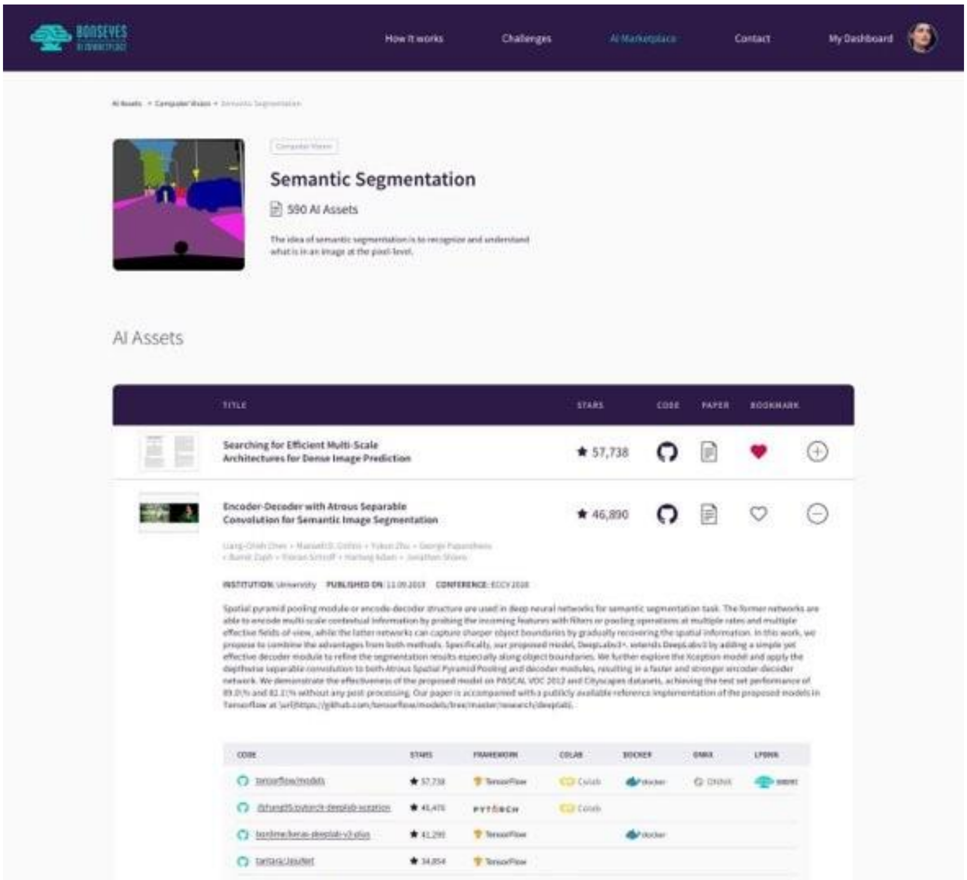
Object Detection
- 420 AI Assets
- 52 leaderboards

Image Generation
- 207 AI Assets
- 48 leaderboards

See all 684 tasks

*Figure 26 AI Assets landing page on the Bonseyes AI Marketplace*

The Bonseyes AI Marketplace provides additional information for AI Assets, which provides insights into deployment capabilities of the AI Assets. The depicted information is community relevance of the implementation by presenting GitHub stars, ML framework that has been used for the implementation, Colab implementation for the quick demonstration, dockerization of the implementation, interoperability model format in ONNX and support of the implementation layers in the LPDNN (Low-power Deep Neural Networks) inference engine.



AI Assets > Computer Vision > Semantic Segmentation

Computer Vision

Semantic Segmentation

590 AI Assets

The idea of semantic segmentation is to recognize and understand what is in an image at the pixel-level.

AI Assets

| | TITLE | STARS | CODE | PAPER | BOOKMARK | |
|---|---|---|---|---|---|---|
| | Searching for Efficient Multi-Scale Architectures for Dense Image Prediction | ★ 57,738 | | | | |
| | Encoder-Decoder with Atrous Separable Convolution for Semantic Image Segmentation | ★ 46,890 | | | | |

Liang-Chieh Chen • Maxwell D. Collins • Yukun Zhu • George Papandreou • Barret Zoph • Florian Schroff • Hartwig Adam • Jonathon Shlens

INSTITUTION: University PUBLISHED ON: 11.09.2019 CONFERENCE: ECCV 2018

Spatial pyramid pooling module or encode-decoder structure are used in deep neural networks for semantic segmentation task. The former networks are able to encode multi-scale contextual information by probing the incoming features with filters or pooling operations at multiple rates and multiple effective fields-of-view, while the latter networks can capture sharper object boundaries by gradually recovering the spatial information. In this work, we propose to combine the advantages from both methods. Specifically, our proposed model, DeepLabv3+, extends DeepLabv3 by adding a simple yet effective decoder module to refine the segmentation results especially along object boundaries. We further explore the Xception model and apply the depthwise separable convolution to both Atrous Spatial Pyramid Pooling and decoder modules, resulting in a faster and stronger encoder-decoder network. We demonstrate the effectiveness of the proposed model on PASCAL VOC 2012 and Cityscapes datasets, achieving the test set performance of 89.0\% and 82.1\% without any post-processing. Our paper is accompanied with a publicly available reference implementation of the proposed models in Tensorflow at \url{https://github.com/tensorflow/models/tree/master/research/deeplab}.

| CODE | STARS | FRAMEWORK | COLAB | DOCKER | ONNX | LPDNN |
|---|---|---|---|---|---|---|
| tensorflow/models | ★ 57,738 | TensorFlow | Colab | docker | ONNX | [illegible] |
| jfzhang95/pytorch-deeplab-xception | ★ 41,470 | PYTORCH | Colab | | | |
| bonlime/keras-deeplab-v3-plus | ★ 41,290 | TensorFlow | | docker | | |
| [illegible] | ★ 34,854 | TensorFlow | | | | |

Figure 27 Deployment Capabilities of the AI Assets

Information of the deployment capabilities facilitates the process of finding suitable AI Assets for industrialization using ML deployment framework AI Asset Container [3.2.2].

### 4.1.2.3 Users and Organization Profiles

Bonseyes AI Marketplace users and organizations have an opportunity to connect with different industries or individuals aiming to collaborate or be employed on the AI Challenge initiatives. Under the Community page on the Bonseyes AI Marketplace, users can browse, search, and connect with other AI Marketplace users and organizations. The community component of the Marketplace is planned to be developed at the end of M12.

Table 2 User and Organization Profile Features

| Component | Feature |
|---|---|
| Profile | Browse |
| Profile | Search |
| Profile | Connect |
| Organization | Browse |
| Organization | Search |
| Organization | Connect |

### 4.1.2.4 Bonseyes AI Asset Container

Bonseyes AI Asset container enables accelerated deployment of deep learning models to resource constrained low power embedded systems (Edge and Deep Edge). These containers deliver powerful and easy-to-deploy building blocks for creating complex AI systems of systems that use cyber-physical systems. By taking care of many of end-to-end tooling dependencies and providing standardized interfaces, Bonseyes AI Asset Containers enable users to focus on producing optimal solutions while allowing faster feedback during the implementation of end user requirements.

The goal is to facilitate easier deployment to the Edge and Deep Edge with the Bonseyes AI Marketplace and to offer a series of modular services — such as experimentation, model compression, optimization, benchmarking, and deployment on hardware and security — that will increase AI usage among enterprises and SMEs which currently lack internal innovation capabilities.

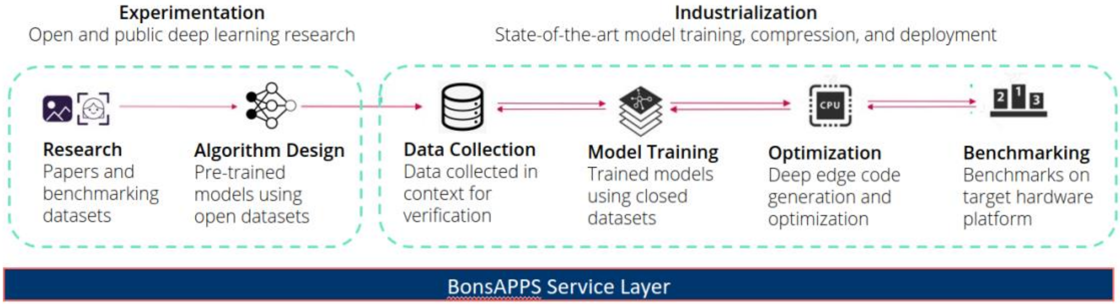

Experimentation
Open and public deep learning research
Industrialization
State-of-the-art model training, compression, and deployment
Research
Papers and benchmarking datasets
Algorithm Design
Pre-trained models using open datasets
Data Collection
Data collected in context for verification
Model Training
Trained models using closed datasets
CPU
Optimization
Deep edge code generation and optimization
2 1 3
Benchmarking
Benchmarks on target hardware platform
BonsAPPS Service Layer

*Figure 28 Experimentation to industrialization pipeline supported with the Service Layer in AI Asset Container*

Representing end-to-end framework AI Asset container provides the following services:

- **Environment Setup:** Provides a versioned reference to the original algorithm implementation via git submodule and mechanism for applying git patches without need to modify original git. Provides docker files enabling user to build and run containers in a virtualized environment for training and deployment purposes. Manage system dependencies so original implementation can be reproduced consistently.
- **Model Training:** Provides a standardized data download script, a wrapper for the main training script including parameters of the experiments, and a standardized way of storing training configuration files using YAML.
- **Model compression:** Provides a standardized data download script, a wrapper for the main compression script (training-aware or data-free), and a standardized way of storing compression configuration files using YAML.
- **Model quantization:** Provides a standardized data download script, a wrapper for the main quantization script (training-aware or data-free), and a standardized way of storing quantization configuration files using YAML.
- **Model repository:** Provides standardized mechanism and naming conventions for storing pretrained and exported models.
- **Export:** Provides reusable export scripts of the models compatible with inference engines and compilers as LPDNN, TensorRT, and ONNX.
- **Deploy:** Provides algorithm and algorithm result abstract classes, reusable scripts for image, audio, video and camera processing. Also provides http server and client.
- **Evaluation:** Provides template code and guide how to perform multi-scale cross-engine evaluation using original evaluation code.
- **Test:** Provides test scripts for algorithm extraction and exports on python level and test framework for C++ to Python translation.

- **Documentation:** Provides static site documentation generation and API documentation.

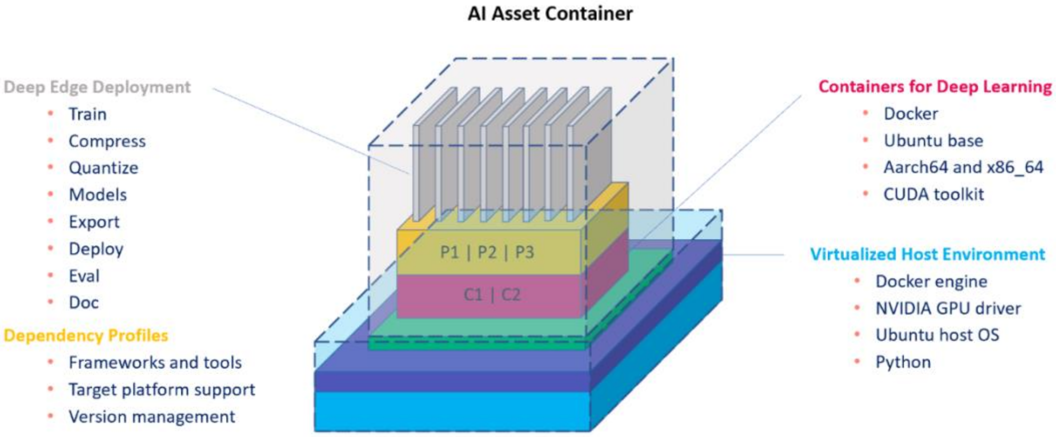


*Figure 29 AI Asset container architecture*

### 4.1.2.5 Bonseyes AI Containers for Edge and Deep Edge

A common problem in deployment to the Edge and Deep Edge is that when training and optimizing models in a cloud or host environment, often a model is created with a set of dependencies that do not match the target hardware platform environment. These dependency differences can create subtle and accumulative errors, which make exact replication of models at deployment difficult and make debugging model performance complex and sometime impossible. Additionally, specialized tools are often required to program specialized hardware circuits which may require a very specific dependency set to function correctly.

To alleviate these developer pain points, Bonseyes AI Marketplace provides dependencies profiles for target environments for Edge and Deep Edge platforms such as Raspberry Pi, NVIDIA Jetson and Xavier, and as well as the NXP i.MX8 edge computing platforms. The dependency profile contains versioning information of common middleware and driver components so that the Bonseyes AI Asset Container can mirror the target deployment environment as closely as possible.

Containers for Deep Learning are a set of Docker containers with key data science frameworks, libraries, tools and runtime inference engines for LPDNN, TensorRT, and ONNX. These containers provides performance-optimized, consistent environments that help deploy AI Assets to the Edge and Deep Edge. They provide stable and versioned environments for both training of models and the deployment of models support x86_64 and aarch64.

Containers for Deep Learning images can be configured to include various frameworks, libraries, and tools. Version management of the various components are configured using Dependency Profiles that track versioning information for emulation and ensuring compatibility.

### 4.1.2.6 User Support Documents

**AI Asset Container generator**

Contains step by step guide on how to create new AI Asset container including: git setup, instantiating the new container with template values and creating new AI Asset repository.

**AI Asset Container development guidelines**

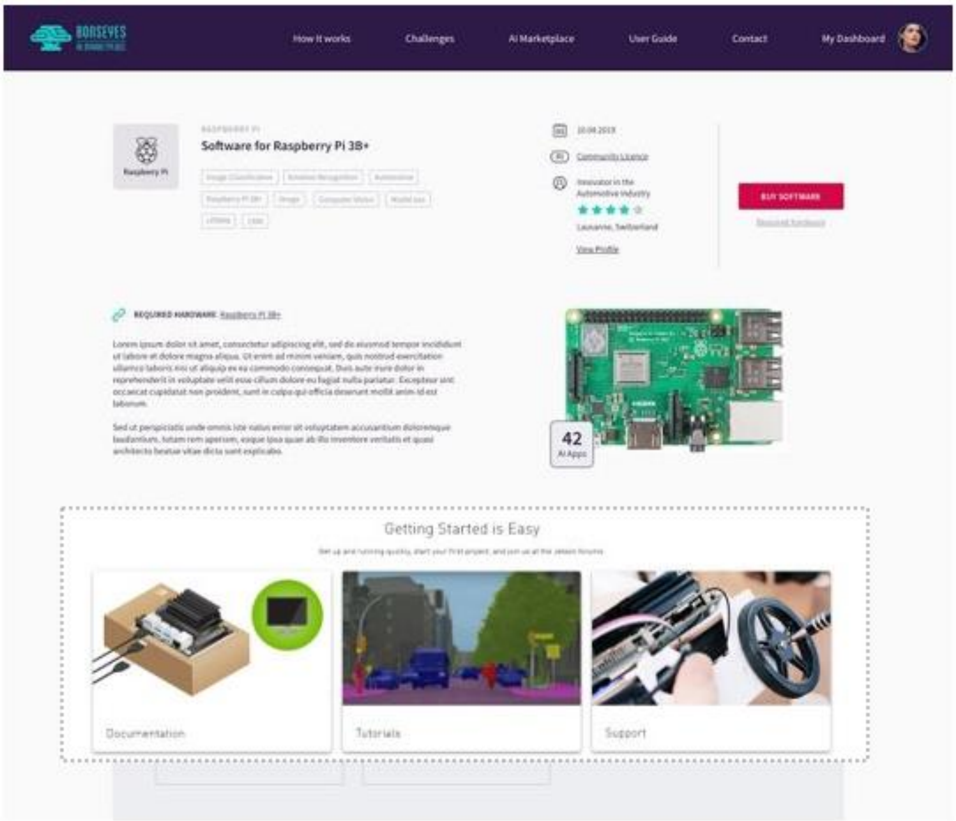
Contains step by step guide on how to use created container and python package to fully develop new AI Asset including: attachment of original research paper implementation, definition of development flow per component, list of files that require implementation, list of files that can be instantly reused and combined with other components, procedures how to document results or issues during implementation.

**Contributing to AI Asset container**
Describes development procedures (git flow, issue tracking, code formatting) in multi collaborative environment also provides list of active AI Asset contributors

#### *4.1.2.7 Developer Platforms | Board Support Packages (BSP)*

A Developer Platform is a digital package containing the full software stack (operating system, drivers, middleware components, etc.) and documentation required to procure, set up and control target hardware for the execution of AI apps. Moreover, the platform provides a cross-compilation environment and tooling that is capable of creating executables for the target hardware on the developer workstation. The platforms are composed of various components:

1. **Support docker:** the container used to build the platform package and setup target hardware.
2. **Builder docker:** the container used to cross-compile binaries for the target hardware.
3. **Manager docker:** the container used to control the target hardware.
4. **Clean metadata:** the full metadata that is used for the listing on the Bonseyes AI Marketplace.



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo.

*Figure 30 Board Support Packages on Bonseyes AI Marketplace*

*Table 3 Supported Developer Platforms*

| Name | Vendor | Version |
|---|---|---|
| x86_64-ubuntu18 | Ubuntu | V1.0 |
| x86_64-ubuntu20 | Ubuntu | V1.0 |
| raspberry4b_64-ubuntu20 | Raspberry Pi | V1.0 |
| jetson_nano-jetpack4.4 | Nvidia | V1.0 |
| Jetson_xavier-jetpack4.4 | Nvidia | V1.0 |
| nvidia_drive_agx-software10.0 | Nvidia | V1.0 |
| **imx8m_nano_evk-yocto_imx_5.10.9_1.0.0** | NXP | V1.0 |
| imx8qm_mek-yocto_imx_5.10.9_1.0.0 | NXP | V1.0 |
| imx8m_plus_evk-yocto_imx_5.10.9_1.0.0 | NXP | V1.0 |

### 4.1.2.8 User Guide Features

*Table 4 User Guide Features*

| Tutorial | Format |
|---|---|
| 1. Setup Developer Workstation<br>2. **The User Guide represents a developer's documentation that explains how the user can start with the Bonseyes AI Maketplace Platform, including AI Marketplace and Bonseyes CLI Tool. It will provide a comprehensive guide on how to create, use and manage AI Artifacts on the local workstation and AI Marketplace. Table X depicts all planned enhancements of the User Guide.** | Text |
| Install CLI Tool | Text, video |
| How to obtain a platform from the Bonseyes AI Marketplace | Text, video |
| How to setup a target hardware | Text, video |
| How to obtain an AI app from the Bonseyes AI Marketplace | Text |
| How to benchmark AI App | Text, video |
| How to create challenge | Text |
| How to upload a challenge to the Bonseyes AI Marketplace | Text, video |
| How to obtain a challenge from the Bonseyes AI Marketplace | Text, video |
| How to generate AI App | Text, video |
| How to upload AI app to the Bonseyes AI Marketplace | Text, video |
| How to create a platform package | Text |
| How to upload a platform to the Bonseyes AI Marketplace | Text, video |
| How to create an AI Artifact package | Text |
| How to create Data Tool | Text |
| How to create Evaluation Tool | Text |
| How to find and select AI Asset | Text |
| How to use AI Asset Container Generator | Text, video |
| How to use AI Asset services for the Edge and Deep Edge | Text, video |

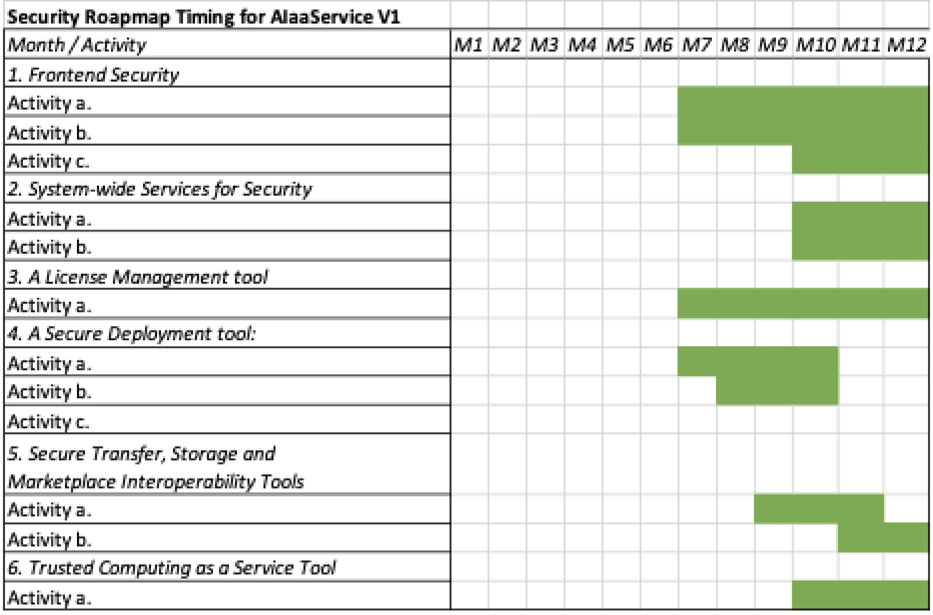
### 4.1.3 Security

The aim of AIaaS V1 is to support the AI developers as they offer their AI Artifacts on the BMP. Hence, the Security-as-a-Service (SaaS) activities in AIaaS V1 focus on the mechanisms for system-wide and basic support of security, on the frontend website and on the deployment security at the edge devices since the devices expected to be the first ones to be exposed to security challenges. The SaaS activities in AIaaS V1 are:

- *Frontend Security:*
    - Secure developer access
    - Implement a system-wide user management
    - Connect to the system-wide identity management
- *System-wide Services for Security:*
    - Implement a system-wide identity management
    - Implement a system-wide certificate and key management
- *A License Management tool:*
    - Define an initial set of licenses and make is accessible and bindable to Artifacts
- *A Secure Deployment tool:*
    - Implement until October a PoC for the alignment of the KOP tool into the Bonseyes deployment chains
    - Define a requirement and compatibility matrix for the hard- and software regarding the security and used in the deployment chain and at the Edge and Deep Edge devices
    - Implement until end of AIaaS V1 a working integration of the KOP into the deployment chain for a defined subset of devices (incl. ODRL compatibility or integration with KOP)
- *Secure Transfer, Storage and Marketplace Interoperability Tools:*
    - Identify security requirements and security capabilities for centralized and persistent AI Artifact repositories
    - Implement an integrate initial authorization policies for centralized AI Artifact
- *Trusted Computing as a Service Tool:*
    - Implement a first PoC for the integration of the KOP tool into the development chains

#### *4.1.3.1 4.1.3.1 Gantt Chart for Security Activities in AIaaS V1*

The timing of the activities in the Security-as-a-Service activities in AIaaS V1 are depicted in Figure 31. Hereby, the description of the subtasks is replaced by the task number (a. to c.) in the task areas. Please observe, the timing starts with month M1, which is the start of the project.



| Security Roapmap Timing for AIaaService V1 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Month / Activity* | *M1* | *M2* | *M3* | *M4* | *M5* | *M6* | *M7* | *M8* | *M9* | *M10* | *M11* | *M12* |
| *1. Frontend Security* | | | | | | | | | | | | |
| Activity a. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Activity b. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Activity c. | | | | | | | | | | 🟩 | 🟩 | 🟩 |
| *2. System-wide Services for Security* | | | | | | | | | | | | |
| Activity a. | | | | | | | | | | 🟩 | 🟩 | 🟩 |
| Activity b. | | | | | | | | | | 🟩 | 🟩 | 🟩 |
| *3. A License Management tool* | | | | | | | | | | | | |
| Activity a. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| *4. A Secure Deployment tool:* | | | | | | | | | | | | |
| Activity a. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | | |
| Activity b. | | | | | | | | 🟩 | 🟩 | 🟩 | | |
| Activity c. | | | | | | | | | | | | |
| *5. Secure Transfer, Storage and Marketplace Interoperability Tools* | | | | | | | | | | | | |
| Activity a. | | | | | | | | | 🟩 | 🟩 | 🟩 | |
| Activity b. | | | | | | | | | | | 🟩 | 🟩 |
| *6. Trusted Computing as a Service Tool* | | | | | | | | | | | | |
| Activity a. | | | | | | | | | | 🟩 | 🟩 | 🟩 |

*Figure 31 Gant chart for the SaaS activities in AIaaS V1*

### 4.1.4 Industry Challenges 1 (AI Assets)

Industry Challenges have been defined in association with the Industry, taking input from the Industry Workshop day that took place in June 2021, and will be conducted in the Bonseyes AI Marketplace, demonstrating the pertinence of the collaborative innovation process.

The following diagram describes and maps the functionalities of the platform with the input from the challenges defined with the input from industry participants during the Industry Day for the first Open Call and will also describes the overall workflow.

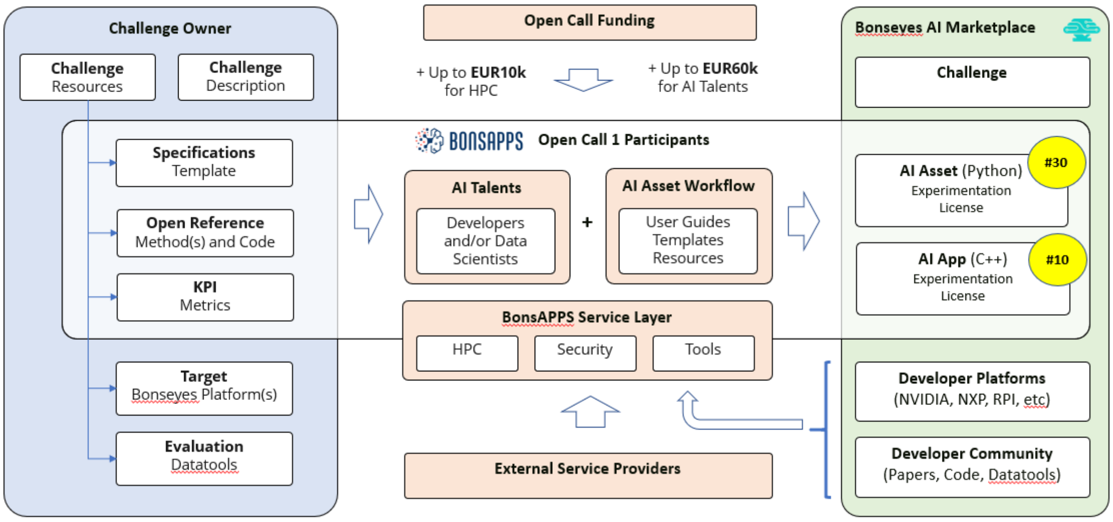

Challenge Owner
Challenge Resources
Challenge Description
Specifications Template
Open Reference Method(s) and Code
KPI Metrics
Target Bonseyes Platform(s)
Evaluation Datatools
Open Call Funding
+ Up to EUR10k for HPC
+ Up to EUR60k for AI Talents
BONSAPPS Open Call 1 Participants
AI Talents
Developers and/or Data Scientists
+
AI Asset Workflow
User Guides Templates Resources
BonsAPPS Service Layer
HPC
Security
Tools
External Service Providers
Bonseyes AI Marketplace
Challenge
AI Asset (Python) Experimentation License
#30
AI App (C++) Experimentation License
#10
Developer Platforms (NVIDIA, NXP, RPI, etc)
Developer Community (Papers, Code, Datatools)

*Figure 32 1st Open Call workflow*

The industry verticals selected for the first release of the AIasaS layer are as follows.

### 4.1.4.1 Automotive

The targeted challenges for the Automotive vertical are driver monitoring, interior monitoring, and in-cabin gesture recognition.

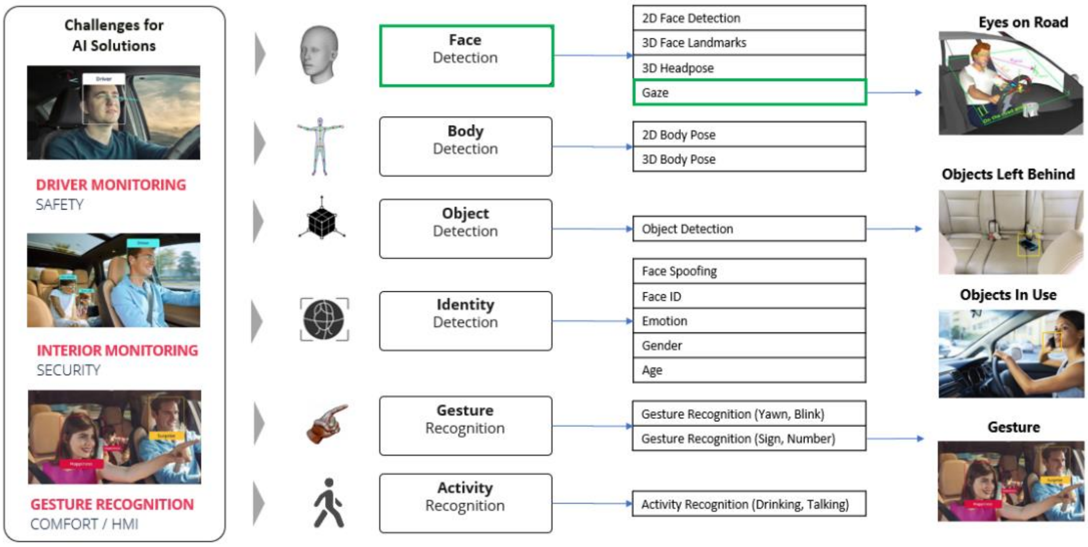


*Figure 33 Automotive vertical: challenges, applications, use cases*

- **Driver monitoring** (safety): Advanced driver monitoring system (DMS) that can detect distracted and drowsy drivers by accurately measuring eye and head position, attention and fatigue. The DMS alerts the driver and integrated safety systems upon detection of a risk such as drowsiness or distraction. This feedback enables the driver and vehicle to take action before safety is compromised.
- **Interior monitoring** (security): With the interior monitoring system, it is not only the driver who is the focus of attention. The camera is positioned in such a way that all seats are in its field of vision. The system can detect the presence of any other occupant, front passengers, and can thus deactivate the airbag if, for instance, a child safety seat is present.
- **In-cabin Gesture recognition** (comfort): The automotive HMI of the future is going to use a host of new technologies to respond more intelligently to a driver's needs, increasing safety and letting you control your car in a way that's natural and easy. It will likely be powered by facial and gesture recognition, voice control, visual displays, eye tracking, and haptic technology.

### 4.1.4.2 Healthcare

The targeted challenges for the Health vertical are driver health assessment, patient monitoring and workflow support monitoring.

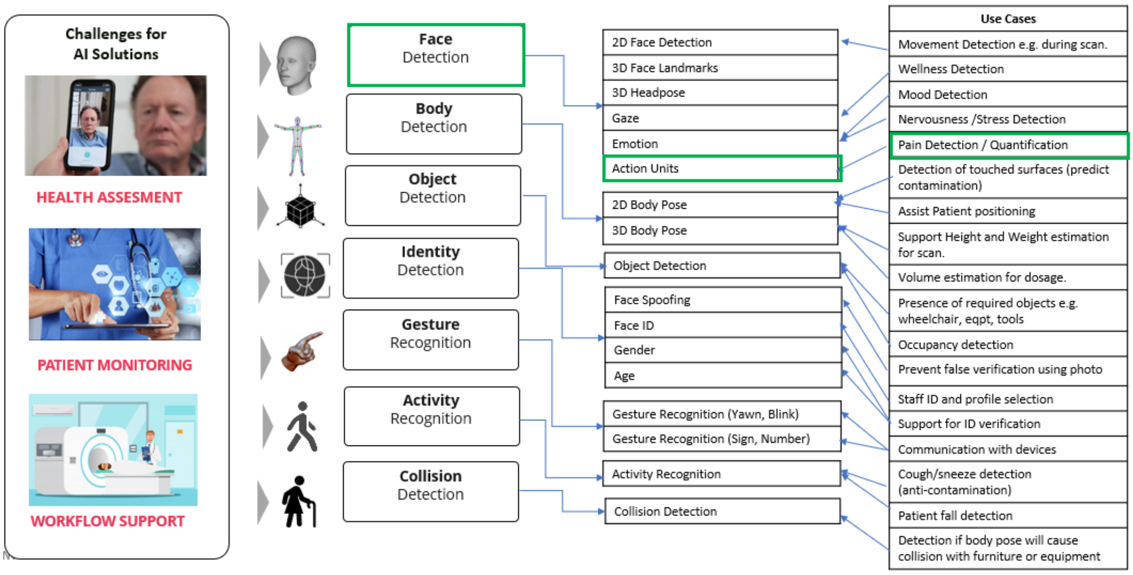

Challenges for AI Solutions
HEALTH ASSESMENT
PATIENT MONITORING
WORKFLOW SUPPORT
Face Detection
Body Detection
Object Detection
Identity Detection
Gesture Recognition
Activity Recognition
Collision Detection
2D Face Detection
3D Face Landmarks
3D Headpose
Gaze
Emotion
Action Units
2D Body Pose
3D Body Pose
Object Detection
Face Spoofing
Face ID
Gender
Age
Gesture Recognition (Yawn, Blink)
Gesture Recognition (Sign, Number)
Activity Recognition
Collision Detection
Use Cases
Movement Detection e.g. during scan.
Wellness Detection
Mood Detection
Nervousness /Stress Detection
Pain Detection / Quantification
Detection of touched surfaces (predict contamination)
Assist Patient positioning
Support Height and Weight estimation for scan.
Volume estimation for dosage.
Presence of required objects e.g. wheelchair, eqpt, tools
Occupancy detection
Prevent false verification using photo
Staff ID and profile selection
Support for ID verification
Communication with devices
Cough/sneeze detection (anti-contamination)
Patient fall detection
Detection if body pose will cause collision with furniture or equipment

*Figure 34 Health vertical: challenges, applications, use cases*

- **Health assessment:** Real-time health assessments can assist medical staff and care assistants in both prevention and treatment of conditions. Using AI powered visual observation for measurement of vital signs, assessment of pain levels in non-communicative and pre-verbal patients, and assessment of mood and fatigue levels information can be gathered to assist in decision making leading to improved patient outcomes whilst delivering increased efficiencies. One example application is pain monitoring where AI has the ability to transform pain management for vulnerable patients with innovative facial muscle movement analytics. This enables more accurate pain assessment of patients with communication difficulties such as dementia or with pre-verbal children.
- **Patient monitoring**: Monitoring of patients throughout their care experience from admission through treatment to discharge, integrated with hospital information systems, can lead to a safer, more secure, smoother and more patient centric experience with faster and improved outcomes. Highly accurate biometrics analysis helps in reliable identification of patients by precisely recognizing their unique characteristics to ensure patient security confirming identity throughout the treatment journey along with the observation of vital signs, management of stress when under treatment and observation of overall mood in order to provide a better experience. Additionally, observations of body movements can help identify medical emergencies such as collapse. Further, monitoring of patients in their interactions with machinery can ensure correct alignment with medical equipment and also prevent accidental collisions with those items.
- **Workflow support**: Monitoring of both patient and staff identities and activities throughout the patient journey, both within clinical zones, at the bedside and in the home care environment can lead to significantly improved outcomes and efficiencies as well as enhancing security. AI enables patient emotional profiling to address various challenges in communication and medical procedures. Examples could be when patients are submitted to potentially claustrophobic procedures signs of panic can be quickly identified and estimation of patient volume to cross check dosing decisions. AI can be used to monitor facilities and objects, for example to ensure correct sterilisation process and tool preparation have been followed, correct patient positioning for automated processes has been made, and potential contamination sources identified (e.g. where touch has taken place).

### 4.1.4.3 Manufacturing

The manufacturing industry challenges are inspired by real world problems that the manufacturing industry is facing. The following meta-challenges will be considered as an input for the Industry workshop during which more accurate description of the individual challenges will be elaborated.

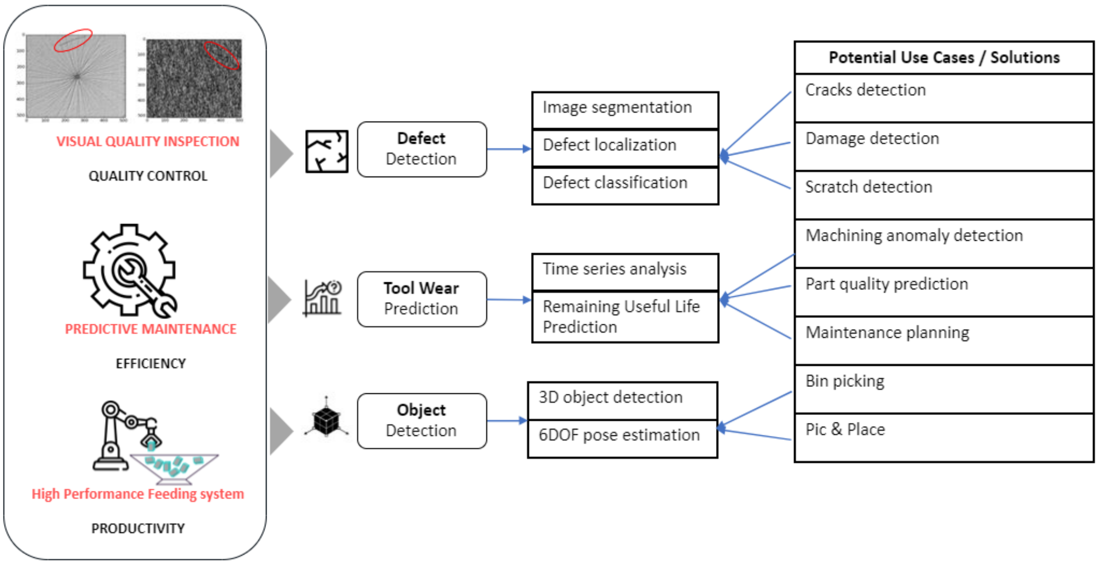


*Figure 35 Manufacturing vertical: challenges, applications, use cases*

- **Zero Defect Manufacturing**: Manufacturing Industry is facing a major challenge in achieving a twofold objective of productivity/efficiency and Quality. While production efficiency is pushed to its maximum, manufactured products must conform to the required quality. Zero defect Manufacturing refers here to ability of a manufacturing industry to deliver only product with the right level of quality. In preliminary discussions with industrial partners, two AI-based technologies can lead to zero-defect manufacturing:
  - Vision-based high precision quality control powered by AI
  - Product quality prediction based on manufacturing process and condition monitoring
- **Predictive Maintenance**: Equipment downtime is a major efficiency killer in manufacturing shop floors. Measured based on KPI provided by the Overall Equipment Efficiency (OEE) Framework, the equipment efficiency represents a major lever for manufacturing industry competitiveness. AI opens interesting perspectives to predict and therefore avoid failure of equipment. The following specific capabilities are expected to profit from AI.
  - Remaining lifetime estimation of equipment
  - Anomaly prediction

  The industry workshop will be leveraged to have detailed discussions with industrial partners in order to select and specify the particular challenge to consider and the equipment to be considered for the challenge.
- **High-Performance Feeding System in Production Lines**. Feeding systems are often the bottleneck in production lines. This is the case because feeding systems have to execute several operations before placing the parts on the right places. As parts often arrive in bulk, feeding systems have to disentangle them, sort them, pick the and finally place them. A part can only be picked and placed if it is in the right pose and orientation. Recognizing part pose and orientation is therefore a critical capability that feeding

systems have to include. Vision-based AI techniques can be leverages to provide this capability.

### *4.1.4.4 Robotics*

The Robotics industry challenges are inspired from real world problems that industrial companies are facing. The following meta-challenges will be considered as an input for the Industry workshop during which more accurate description of the individual challenges will be elaborated.

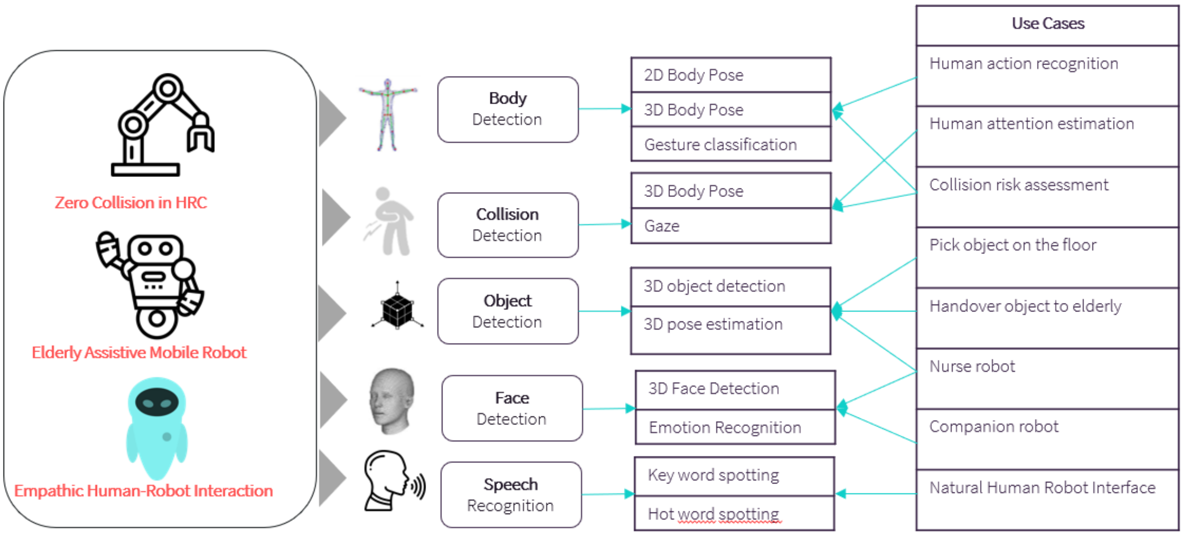


*Figure 36 Robotics vertical: challenges, applications, use cases*

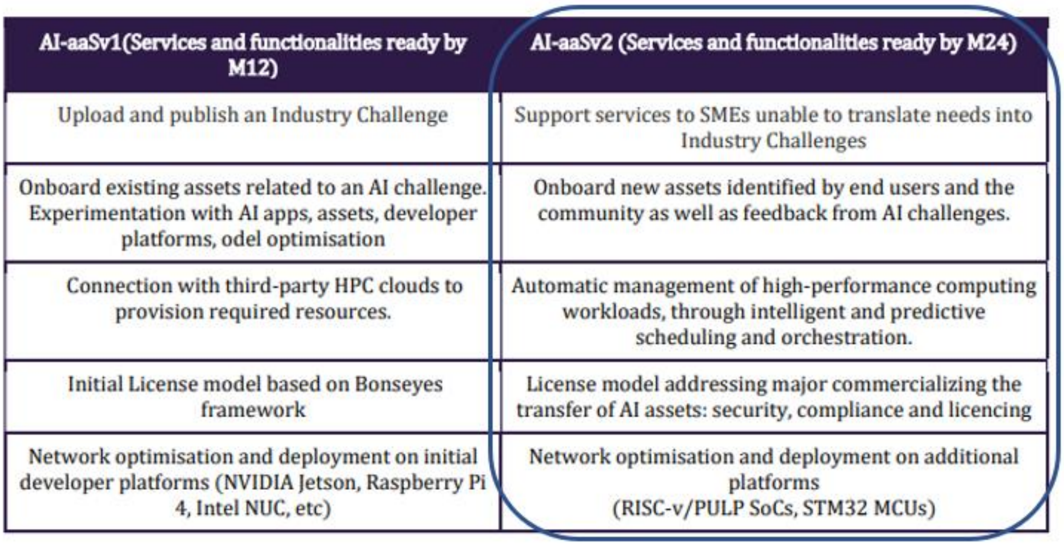
- **Zero Collision Interaction for Safe Human-Robot Collaboration**: The main problem to be addressed in this project is human safety in human-robot interaction while executing collaborative tasks. Safety is a non-negotiable requirement for any human-robot collaboration in the workplace. A recent study from McKinsey[6] clearly shows that one of the major challenges for a large deployment of robots is related to safety concerns. To unlock the full potential of collaborative robotics in industry and society, human safety must be guaranteed. To do so, collaborative robots must be equipped with technologies that reinforce safety. Collision detection is a typical capability that can use vision-based AI to predict and avoid collision between humans and robots. Typical AI models that can be used are:
    - Human pose detection
    - Gesture detection and recognition
    - Work zone delimitation
- **Elderly Assistive Mobile Robot**: The demographic changes leading to more people requiring care in old age and the lack in numbers of skilled caretakers are demanding innovative solutions to handle the gap between supply and demand of care. Elderly assisting service robots are a good mitigation to this problem if they have the appropriate capabilities. Vision-based AI can be used to make service robots more interactive and cooperative. Tasks picking up unknown objects from the floor can benefit from vision-based AI. Typical AI models that can be used are:
    - Human detection
    - Gesture detection and recognition
    - Object detection

[6] https://www.mckinsey.com/industries/advanced-electronics/our-insights/growth-dynamics-in-industrial-robotics

- **Empathic Human-Robot Interaction**. This generic meta-challenge aims at developing robotic capabilities which intend to make robots more interactive and more aware about the emotional state of humans with whom they interact. Typical AI models that can be used are:
    - Face detection
    - Emotion recognition
    - Attention detection

## 4.2 AIaaS V2 – Demand Activation

The second release of the AIaaS will be focused on further increasing the services and functionalities to accommodate the 'demand' side of the Bonseyes AI Marketplace represented by SMEs and users looking to solve Industry Challenges consuming AI Assets, services and solutions, and also host challenges experimentations defined by SMEs selected during the 2nd Open Call. It will further enhance the level of services and functionalities developed in the first AIaaS release and ensure re-usability of the AI Components & Solutions developed by AI talents and users, subject to a licensing model that protects data privacy and ownership of data from the original end users but grants AI Talents rights to re-use and commercialize.



| AI-aaSv1(Services and functionalities ready by M12) | AI-aaSv2 (Services and functionalities ready by M24) |
|---|---|
| Upload and publish an Industry Challenge | Support services to SMEs unable to translate needs into Industry Challenges |
| Onboard existing assets related to an AI challenge. Experimentation with AI apps, assets, developer platforms, odel optimisation | Onboard new assets identified by end users and the community as well as feedback from AI challenges. |
| Connection with third-party HPC clouds to provision required resources. | Automatic management of high-performance computing workloads, through intelligent and predictive scheduling and orchestration. |
| Initial License model based on Bonseyes framework | License model addressing major commercializing the transfer of AI assets: security, compliance and licencing |
| Network optimisation and deployment on initial developer platforms (NVIDIA Jetson, Raspberry Pi 4, Intel NUC, etc) | Network optimisation and deployment on additional platforms<br>(RISC-v/PULP SoCs, STM32 MCUs) |

*Figure 37 AIaaS V2 – Demand Activation*

### 4.2.1 Bonseyes AI Marketplace

With the AIaaS V2 release, the Bonseyes AI Marketplace will be able to support services to SMEs looking to translate their needs into Industry Challenges; it will provide automatic management of computing workloads, as well as access to model optimisation and the ability to deploy solutions on a number of additional SoC platforms. This will be available within an advanced licensing and security framework that will enable the safe sharing and collaboration around AI Assets and AI Artifacts.

#### *4.2.1.1 User Support Framework*

See User Framework deliverable D 5.1.

#### *4.2.1.2 AI Asset Container*

See User Framework deliverable D 5.1.

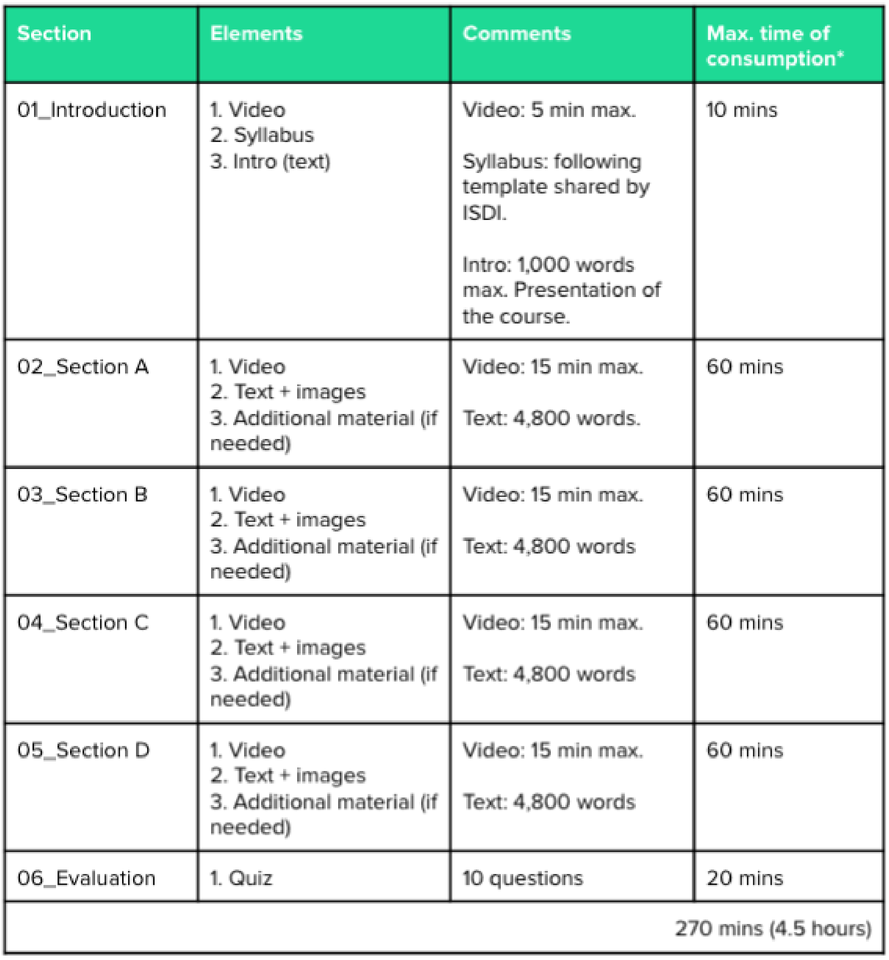
#### *4.2.1.3 MOOC*

As part of the User Support Framework, a digital, human-centric and user-friendly MOOC platform will be developed, along with training courses that will serve as a quality system to certify the proficiency of BMP users (end users, AI talents) in the use of AI-as-a-Service.

The MOOC platform will be powered by OpenEdX, and the courses themselves will leverage ISDI's background in content creation, including its in-house content expert, a staffed AV video and years of proven expertise.

The courses themselves will be created using a pedagogical approach to structure the courses, presenting knowledge in the form of text, video, extra resources, links and relevant images. Learning attainment will be tested at the end of each module and at the end of the whole course.

Both the content and the structure of the MOOC courses will be defined more closely after the first Open Call, but a potential structure and table of content can be seen below.



| Section | Elements | Comments | Max. time of consumption* |
|---|---|---|---|
| 01_Introduction | 1. Video<br>2. Syllabus<br>3. Intro (text) | Video: 5 min max.<br>Syllabus: following template shared by ISDI.<br>Intro: 1,000 words max. Presentation of the course. | 10 mins |
| 02_Section A | 1. Video<br>2. Text + images<br>3. Additional material (if needed) | Video: 15 min max.<br>Text: 4,800 words. | 60 mins |
| 03_Section B | 1. Video<br>2. Text + images<br>3. Additional material (if needed) | Video: 15 min max.<br>Text: 4,800 words | 60 mins |
| 04_Section C | 1. Video<br>2. Text + images<br>3. Additional material (if needed) | Video: 15 min max.<br>Text: 4,800 words | 60 mins |
| 05_Section D | 1. Video<br>2. Text + images<br>3. Additional material (if needed) | Video: 15 min max.<br>Text: 4,800 words | 60 mins |
| 06_Evaluation | 1. Quiz | 10 questions | 20 mins |
| | | | 270 mins (4.5 hours) |

*Figure 38 MOOC courses description*

The table of content of the MOOC will be as follows:

1. Introduction

    Description of the course, basic contents of the course organisation, etc

2. Section A: Introduction to AI Assets
    - a. Deep learning concepts and workflow:
        - i. Data collection
        - ii. Training
        - iii. Deployment
    - b. Challenges of porting deep learning to embedded devices:
        - i. Large computational and memory requirements
        - ii. System dependencies
        - iii. High expertise needed
    - c. AI Assets for accelerated deployment of deep learning models to resource constrained low power embedded systems:
        - i. AI Asset introduction
        - ii. AI Asset workflow

3. Section B: AI Assets workflow (Set-up, training &amp; Optimisations)
    - a. Clone an AI Asset on local machine, install dependencies (git, docker)
    - b. Build docker images based on platform choice
    - c. Training example
        - i. Download dataset
        - ii. Train model
    - d. Compress &amp; quantise example

4. Section C: AI Assets workflow (Export and platform setup)
    - a. Refer to trained model or show pre-trained model if already available
    - b. Export to ONNX or TensorRT
    - c. Set up platform
        - i. Connect to BMP, install cli-tool
        - ii. Download platform
        - iii. Set up platform

5. Section D: AI Assets workflow (Deployment)
    - a. Pull docker image on embedded device
    - b. Download pre-trained models or move converted model from previous section to embedded device
    - c. Test model
    - d. Explain different execution options for demo
        - i. Image
        - ii. Video
        - iii. Camera
        - iv. Http
    - e. Run demo

6. Evaluation
    - a. Run evaluation tool
    - b. Wrap up results and submit

The MOOC learning experience will consist of a full cycle of three courses, going from basic to advanced. Each learner's progress and credits will be automatically registered on the MOOC platform and will serve as a basis for issuing certificates. Those learners who complete the entire cycle will receive a certificate, serving as proof of accomplishment of the necessary training and competency of the user in the service layer. This certificate can be used In future applications.

These courses are expected to be of special relevance to support the validation of entities offering AI services willing to participate second round of experiments. The implementation of this USF component is planned for the second year after the initial open calls.

Furthermore, FBA will use the material in the MOOC courses to create a DIH train-the-trainers toolkit [D6.6].

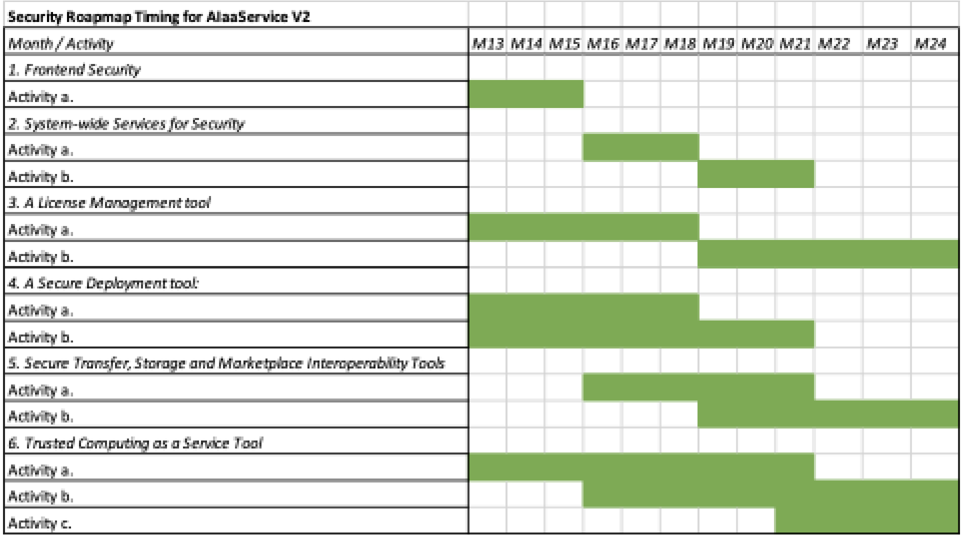
### 4.2.2 Security as a Service

The aim of the AIaaS V2 is to support AI developers as they increase their interest sourcing and using AI Artifacts from the BMP. Hence, the Security-as-a-Service (SaaS) activities in AIasS V2 focus on the mechanisms for a trusted and secure engagement of developers with each other, securing their collaboration when they jointly develop AI Artifacts, and support the developers when they need to regulate their collaboration by licenses. The SaaS activities in AIaaS V2 are:

- *Frontend Security:*
    - Verify and enhance the scalability of the system-wide user management
- *System-wide Services for Security:*
    - Verify and enhance the scalability of the system-wide management
    - Verify and enhance the scalability of the system-wide certificate and key management
- *A License Management tool:*
    - Implement a secure collaborative editor on the BMP frontend for specifying the licenses
    - Implement a library of predefined licenses
- *A Secure Deployment tool:*
    - Verify and enhance the requirement and compatibility matrix for the hard- and software regarding the security and used in the deployment chain and at the Edge and Deep Edge devices; include ST-I device
    - Implement until end of AIaaS V2 a working integration (TRL8) of end system security into the deployment chain for ST-I Edge and Deep Edge devices
- *Secure Transfer, Storage and Marketplace Interoperability Tools:*
    - Implement the required secure, centralized and persistent AI Artifact repositories for BMP
    - Implement the enforcement of BonsAPPs licenses at BonsAPPs centralized AI Artifact repositories
- *Trusted Computing as a Service Tool:*
    - Implement a comprehensive integration of the KOP tool into the development chains addressing the needs of libraries and containers
    - Implement a scalable and secure multi-site support for the SVP
    - Provide a proof-of-concept (PoC) implementation of a secure source code editor

#### *4.2.2.1 Gantt Chart for Security Activities in AIaaS V2*

The timing of the activities in the Security-as-a-Service activities in AIaaS V2 are depicted in Figure 39. Hereby, the description of the subtasks is replaced by the task number (a. to c.)  in the task areas.



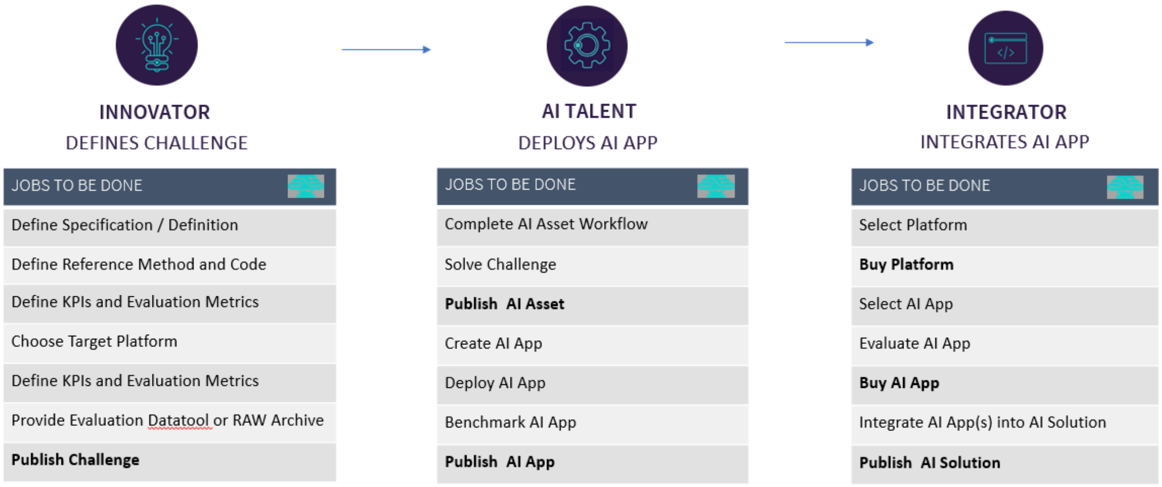
| Security Roapmap Timing for AlaaService V2 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Month / Activity* | *M13* | *M14* | *M15* | *M16* | *M17* | *M18* | *M19* | *M20* | *M21* | *M22* | *M23* | *M24* |
| *1. Frontend Security* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| *2. System-wide Services for Security* | | | | | | | | | | | | |
| Activity a. | | | | 🟩 | 🟩 | 🟩 | | | | | | |
| Activity b. | | | | | | | 🟩 | 🟩 | 🟩 | | | |
| *3. A License Management tool* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| Activity b. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| *4. A Secure Deployment tool:* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | |
| Activity b. | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| *5. Secure Transfer, Storage and Marketplace Interoperability Tools* | | | | | | | | | | | | |
| Activity a. | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| Activity b. | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| *6. Trusted Computing as a Service Tool* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| Activity b. | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 |
| Activity c. | | | | | | | | | 🟩 | 🟩 | 🟩 | 🟩 |

*Figure 39 Gantt chart for the SaaS activities in AIaaS V2*

### 4.2.3 Industry Challenges 2 (AI Apps)

The Industry Challenges defined with the input from the 2nd Industry Day will map out with the second Open Call focused on the demand side of the AI-as-a-Service layer using the Bonseyes AI Marketplace functionalities and tools.

The Challenges presented below can be processed and published on the Bonseyes AI Marketplace. Here is a summary description of the personas and tasks to be completed to solve AI Industry challenges with the marketplace.



INNOVATOR
DEFINES CHALLENGE

JOBS TO BE DONE
- Define Specification / Definition
- Define Reference Method and Code
- Define KPIs and Evaluation Metrics
- Choose Target Platform
- Define KPIs and Evaluation Metrics
- Provide Evaluation Datatool or RAW Archive
- **Publish Challenge**

AI TALENT
DEPLOYS AI APP

JOBS TO BE DONE
- Complete AI Asset Workflow
- Solve Challenge
- **Publish AI Asset**
- Create AI App
- Deploy AI App
- Benchmark AI App
- **Publish AI App**

INTEGRATOR
INTEGRATES AI APP

JOBS TO BE DONE
- Select Platform
- **Buy Platform**
- Select AI App
- Evaluate AI App
- **Buy AI App**
- Integrate AI App(s) into AI Solution
- **Publish AI Solution**

*Figure 40 Challenges workflow*

#### 4.2.3.1 Automotive

The demand activation in AIaaS V2 in the automotive vertical aims at allowing automotive industries with limited internal AI competences to access to AI solutions that can address their challenges. The detailed scope of the industry challenges will be specified based on two factors: a) the advances made by AI talents to solve the AIaaS V1 challenges and b) the development progress of the BMP service layer. Figure 41 illustrates the potential uses cases that can form the scope for AIaaS V2 industry challenges in Automotive.

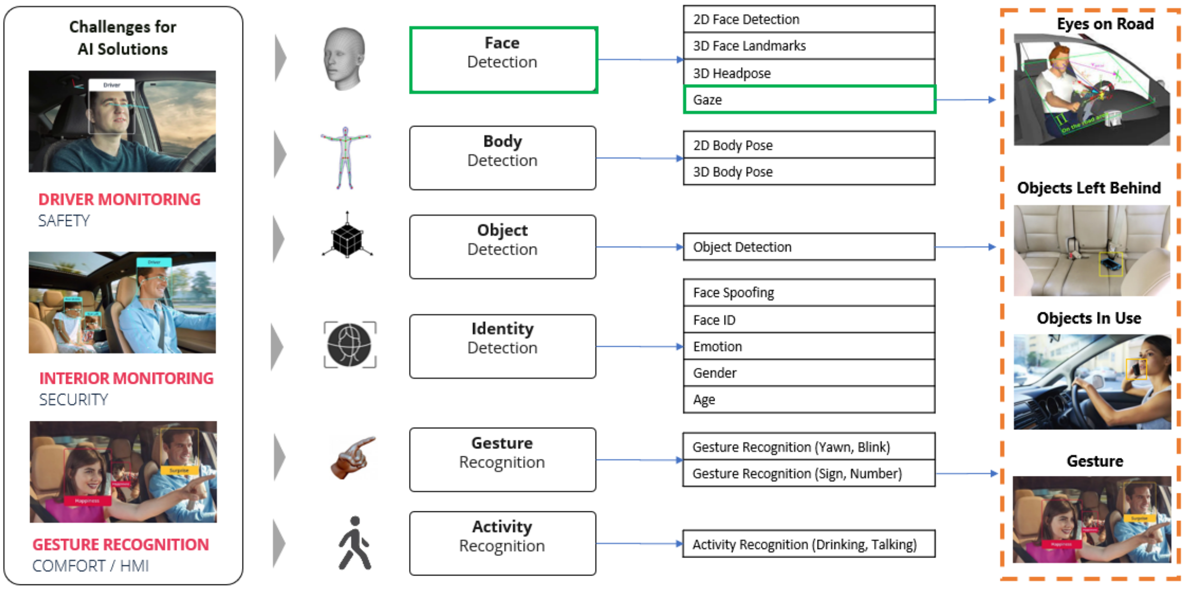


*Figure 41 Potential Automotive use cases for AIaaS V2 industry challenges*

### 4.2.3.2 Healthcare

The demand activation in AIaaS V2 in the robotics vertical aims at allowing robotics industries with limited internal AI competences to access to AI solutions that can address their challenges. The detailed scope of the industry challenges will be specified based on two factors: a) the advances made by AI talents to solve the AIaaS V1 challenges and b) the development progress of the BMP service layer. Figure 42 illustrates the potential uses cases that can form the scope for AIaaS V2 industry challenges in Healthcare.

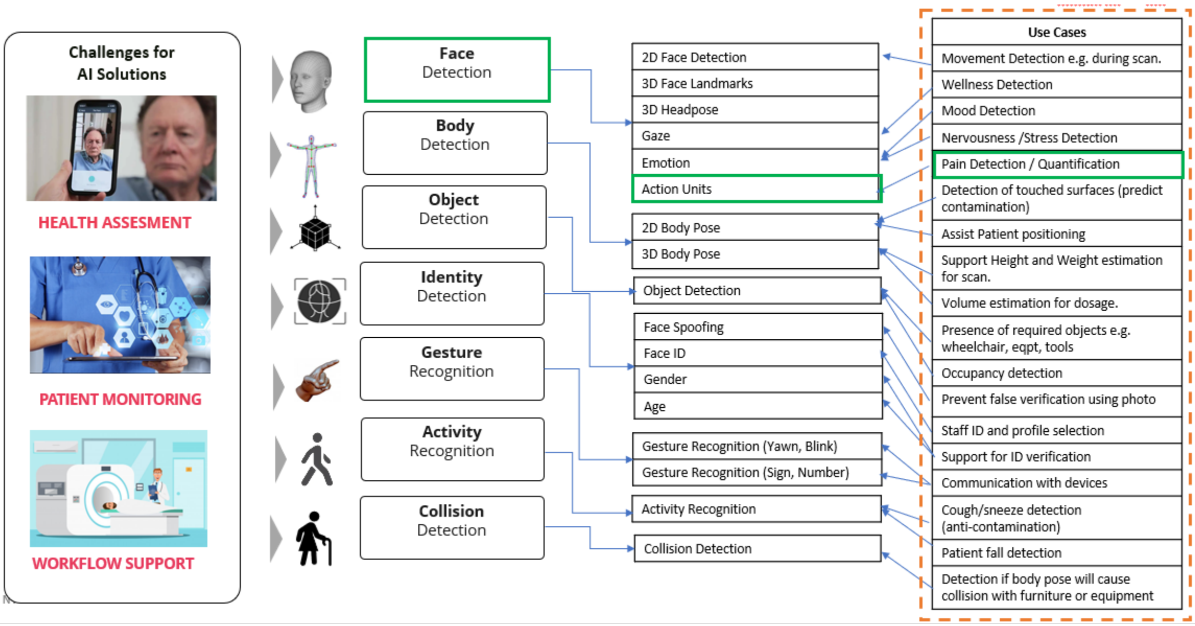

Challenges for AI Solutions
HEALTH ASSESMENT
PATIENT MONITORING
WORKFLOW SUPPORT
Face Detection
Body Detection
Object Detection
Identity Detection
Gesture Recognition
Activity Recognition
Collision Detection
2D Face Detection
3D Face Landmarks
3D Headpose
Gaze
Emotion
Action Units
2D Body Pose
3D Body Pose
Object Detection
Face Spoofing
Face ID
Gender
Age
Gesture Recognition (Yawn, Blink)
Gesture Recognition (Sign, Number)
Activity Recognition
Collision Detection
Use Cases
Movement Detection e.g. during scan.
Wellness Detection
Mood Detection
Nervousness /Stress Detection
Pain Detection / Quantification
Detection of touched surfaces (predict contamination)
Assist Patient positioning
Support Height and Weight estimation for scan.
Volume estimation for dosage.
Presence of required objects e.g. wheelchair, eqpt, tools
Occupancy detection
Prevent false verification using photo
Staff ID and profile selection
Support for ID verification
Communication with devices
Cough/sneeze detection (anti-contamination)
Patient fall detection
Detection if body pose will cause collision with furniture or equipment

*Figure 42 Potential Health use cases for AIaaS V2 industry challenges*

### 4.2.3.3 Manufacturing

The demand activation in AIaaS V2 in the manufacturing vertical aims at allowing manufacturing industries with limited internal AI competences to access to AI solutions that can address their challenges. The detailed scope of the industry challenges will be specified based on two factors: a) the advances made by AI talents to solve the AIaaS V1 challenges and b) the development progress of the BMP service layer. Figure 43 illustrates the potential uses cases that can form the scope for AIaaS V2 industry challenges in Manufacturing.

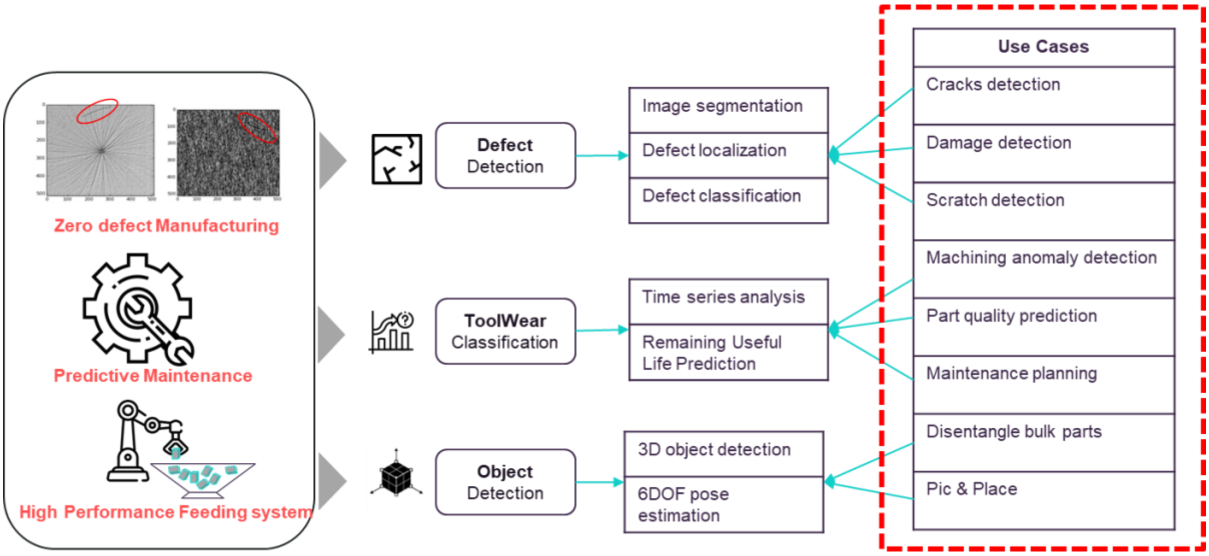


*Figure 43 Potential Manufacturing use cases for AIaaS V2 industry challenges*

### 4.2.3.4 Robotics

The demand activation in AIaaS V2 in the robotics vertical aims at allowing robotics industries with limited internal AI competences to access to AI solutions that can address their challenges. The detailed scope of the industry challenges will be specified based on two factors: a) the advances made by AI talents to solve the AIaaS V1 challenges and b) the development progress of the BMP service layer. Figure 44 illustrates the potential uses cases that can form the scope for AIaaS V2 industry challenges in Robotics.

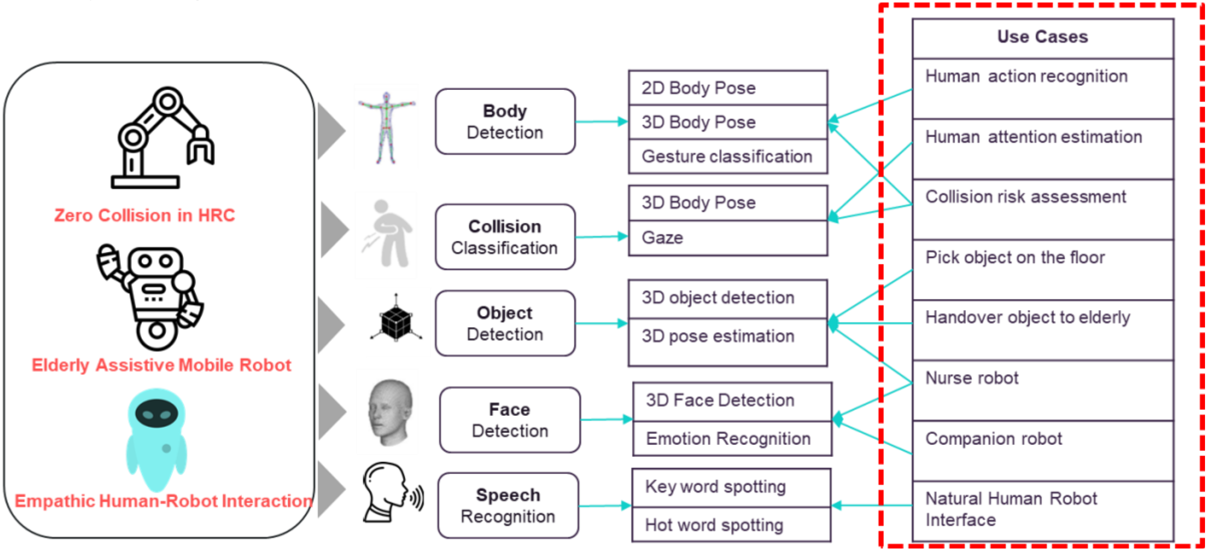


*Figure 44 Potential Robotics use cases for AIaaS V2 industry challenges*

## 4.3 AIaaS V3 – Sustainability

After the supply activation (AIaaS V1) and the demand activation (AIaaS V2), the third AIaaS release will focus on enabling the full network effect of the new services and functionalities hosted on the Bonseyes AI Marketplace and interoperable with the AI-on-demand platform, allowing for a multi-stakeholder collaborative innovation process using ML with end-to-end automation and re-usability of the AI component and services developed by the participants.

This advanced release will incorporate the learnings from the two rounds of Open Calls and of the BonsAPPs. It will lay the groundwork for a sustainable exploitation model of the BonsAPPs services layer on the Bonseyes AI Marketplace and the ability of the marketplace to host other services developed by the various ICT-49 projects as required and after discussion with the other projects.

### 4.3.1 Bonseyes AI Marketplace

The more advanced stage of the Bonseyes AI Marketplace will enable end to end functionalities and access to more services as developed by the BonsAPPs project.

The main activities will center around:

1. Further developing the technical architecture to accommodate operating/exploitation model; there will be further iteration to accommodate the needs expressed by the users during the earlier phases of the project.
2. Developing an operating model for exploitation of BonsAPPs services on BMP; thus will be done in the exploitation plan to be developed by BCA, the aim being to deliver services that can be used, and paid for as relevant, with a commercial business model as required;
3. Ensure growth and sustainability of AI on Demand platform by building it with modular/containerized services and Assets that can interoperate with the AI on demand platform and other ICT 49 services/results.

### 4.3.2 Security

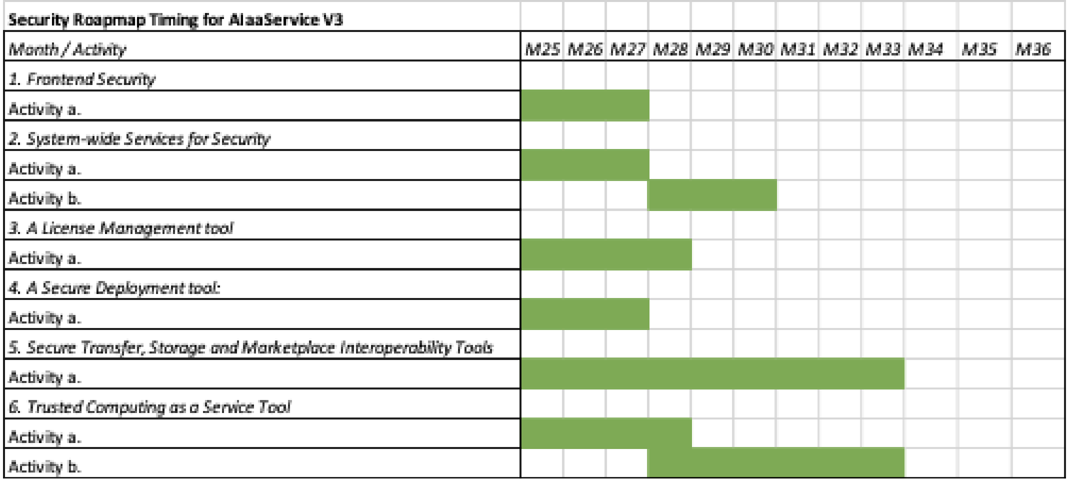
The aim of AIaaS V3 is to unleash the full AI developer for security and to unlock the network effects when Bonseyes AI Marketplace become interoperable and attract enterprise end users with high security and privacy requirements. Hence, the SaaS activities in AIasS V3 focus on the mechanisms for interconnecting marketplaces and their repositories, supporting licenses across the marketplaces and to improve the collaboration and development of AI Artifacts. The SaaS activities in AIaaS V3 are:

- *Frontend Security:*
  - Secure integration and linking to other AI marketplaces
- *System-wide Services for Security:*
  - Demonstration and implementation of an interoperable identity management mechanism
  - Demonstration and implementation of an interoperable identity certificate and key management
- *A License Management tool:*
  - Enhancement of the library of predefined licenses
- *A Secure Deployment tool:*
  - Verify and enhance the requirements and compatibilities matrix for hard- and software regarding the security used in the deployment chain and at the Edge and Deep Edge devices
- *Secure Transfer, Storage and Marketplace Interoperability Tools:*

    - Identify the requirements and implement suitable interoperability mechanisms for the BonsAPPs frontend and the persistent AI Artifact repositories with selected other marketplaces and repositories
    - Investigate and, if necessary, implement common user authentication and authorization mechanisms with AI4EU marketplaces.
- *Trusted Computing as a Service Tool:*
    - Verify the scalable and secure multi-site support for the SVP
    - Provide a secure source code editor for the SVP

#### *4.3.2.1 Gantt Chart for Security Activities in AlaaS V3*

The timing of the activities in the Security-as-a-Service activities in AIaaS V3 are depicted in Figure 45. However, since AIaaS V3 is the iteration which is most far away in time, it is difficult to predict at the moment the exact timing of the subtasks. Again, the description of the subtasks is replaced by the task number (a. to c.) in the task areas.



| Security Roapmap Timing for AlaaService V3 | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *Month / Activity* | *M25* | *M26* | *M27* | *M28* | *M29* | *M30* | *M31* | *M32* | *M33* | *M34* | *M35* | *M36* |
| *1. Frontend Security* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| *2. System-wide Services for Security* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| Activity b. | | | | 🟩 | 🟩 | 🟩 | | | | | | |
| *3. A License Management tool* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | | | |
| *4. A Secure Deployment tool:* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | | | | | | | | | |
| *5. Secure Transfer, Storage and Marketplace Interoperability Tools* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |
| *6. Trusted Computing as a Service Tool* | | | | | | | | | | | | |
| Activity a. | 🟩 | 🟩 | 🟩 | 🟩 | | | | | | | | |
| Activity b. | | | | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | | | |

*Figure 45 Gant chart for the SaaS activities in AIaaS V3*

This technical roadmap document will be updated as required as the AIaaS V1 and V2 are developed and implemented, and lessons are learnt from the Open Calls activities.

BonsAPPs, July 2021

# Bibliography

[Data Marketplace Report D2.4] Bonseyes Data Marketplace Report, Deliverable D2.4, Bonseyes Project, available at https://www.bonseyes.eu/

[Validation Report D2.5] Bonseyes Validation Report, Deliverable D2.5, Bonseyes Project, available at https://www.bonseyes.eu/

[TRL] Technology Readiness Level, Wikipedia, available at https://en.wikipedia.org/wiki/Technology_readiness_level

[KEYSTREAM] Nagravision SA: “Kudelski keySTREAMTM: IoT Security Enablement: Securely Connect, Manage & Update Your IoT Devices”, Fact Sheet, available at https://global-uploads.webflow.com/5fa429174cc2b89c3d4b6bd4/60a7be49adcd697f956bd0e5_keyStream-Factsheet-v2.0_site.pdf , 2021.

[ODRL] Open Digital Rights Language, Wikipedia, available at https://en.wikipedia.org/wiki/ODRL

[ORDL18a] W3C: “ODRL Information Model 2.2”; World Wide Web (W3C) Community Recommendation, available at https://www.w3.org/TR/odrl-model/ ; Feb. 2018

[ORDL18b] W3C: “ODRL Vocabulary & Expression 2.2”; World Wide Web (W3C) Community Recommendation, available at https://www.w3.org/TR/odrl-vocab/ ; Feb. 2018

[ORDL21] W3C: “ODRL Implementation Best Practices”; World Wide Web (W3C) Community Draft Group Report, available at https://w3c.github.io/odrl/bp/#styles ; Apr. 2021

[D2.4] Tim Llewellynn (edt.): Data Marketplace Report, Bonseyes project deliverable D2.4, available at www.bonseyes.eu, July 2020

[TIT20] Tkachuk, Roman-Valentyn, Dragos Ilie, and Kurt Tutschku. "Towards a Secure Proxy-based Architecture for Collaborative AI Engineering.", CANDARW, Japan, Nov. 2020

[D3.1] BonsApps project (edt.) “Security-as-a-Service Requirements and Initial Architecture”, BonsApps project deliverable D3.1, Expected to be available in June, 2021