BONSAPPS

AI-as-a Service for the Deep Edge

D3.1 - Security-as-a-Service Architecture Requirements and Initial Architecture

Grant Agreement No.	101015848
Project Name	BonsAPPs
Work Package No.	WP3
Lead Beneficiary	BTH
Delivery Date	October 30th, 2021
Author(s)	Kurt Tutschku (BTH), Nurul Nomen (BTH), Roman-Valentyn Tkachuk (BTH), Nikola Milojevic (BCA), Vladimir Mujagic (BCA), Jean-Marc Bonnefous (BCA)
Contributor(s)	BTH, BCA
Editor(s)	BTH, BCA
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	June 2021	Initial draft of the deliverable's structure/content and coordination with D1.1	BTH
V0.2	October 19 2021	Preview-version	BTH
V0.3	October 28 2021	Version for internal review	BTH
V0.9	November 18 2021	Version with review comments	HES-SO, NVISO, BCA
V1.0	November 24 2021	Final version of the deliverable	BTH
V1.2	November 25 2021	Final version of the deliverable (reviewed by HES-SO)	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
Sec-aaS:	Security-as-a-Service
HPC:	High performance computing
AI:	Artificial intelligence
CPU:	Central processing unit
GPU:	Graphic processing unit /
NPU:	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-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

The **BonsAPPs security architecture aims at *building robust and strong trust among the stakeholders in an AI economy for developing applications for the deep edge. This is implemented at large by a* Security-as-a-Service (Sec-aaS) layer.**

The BonsAPPs security architecture and the Sec-aaS comprises many mechanisms for security and trust building. They range from a safe frontend, user identities, licence management, code and data encryption, secure edge software deployment to trusted development environments. The mechanisms need to ***address all major malicious or non-malicious violations of the economical rules* of the AI marketplace.** Furthermore, the ***security mechanisms need to be on a sufficient high technical maturity, robustness, and security level (aka TRL, Technical Readiness Level).***

This document fulfils three tasks. a) First , it provides a streamlined and concise description of the initial BonsAPPs Sec-asS architecture and the security mechanisms, aiming to make this document a refence that enables developers to obtain the required TRL. b) The document describes the new security concepts and mechanisms, which are needed but weren't yet addressed in the Bonseyes H2020 project or were identified after the project's finalization (examples for such mechanisms are Kudelski's secure device deployment and KOP – Kudelski Obfuscator Process, or the concept to specify different security levels). c) This deliverable outlines the workplan to reach the technical readiness level of TRL8 for the mechanisms infors the Sec-aaS layer.

In addition, the document provides an overview of the approach and current work on the interoperability of the BonsAPPs platform with other AI marketplaces, in particular the ones that are foreseen for AI4EU and other ICT49 platforms, if this AI platform decide to have their own marketplaces.

The major risk for the BonsApps architecture at large and its use, is a missing concise use and implementation of basic security services offered by the BonsAPPs Sec-aaS layer. Advanced mechanism, such as the KOP mechanisms in the deployment and development chains are apparently easier to master since they can be addressed separately. The major difficulty and, in turn, thread to the security, the missing of system-wide user management and of an easy authentication mechanism for users. However, a solution is already considered by an improved project management highlighting these issues and by a coordinated implementation of the user management mechanisms among the different AI-as-a-service layers in BonsAPPs. The mechanisms for user and security in the deployment and development chains are expected to be decisive for the adoption of the BonsAPPs concept, since they are a USP within the AI engineering. To our knowledge, BonsAPPs is one of the very first projects to attempt Sec-asS for AI and to offload AI developers from non-domain-specific industrialization tasks.

Table of Contents

List of Figures

List of Tables

1 Introduction

The BonsAPPs project is built around the thrilling idea of enabling, building, and sustaining an *economy for developing AI applications for the edge and the deep edge*. This economy comprises the acceleration of the development, the improvement of the accuracy of AI applications, as well as new processes in software engineering for developing such AI systems, e.g., involving many stakeholders in the AI development process as well as considering the specifics of the edge and deep edge devices

An economy involves typically many stakeholders, e.g., suppliers which cater the demand, consumers which absorb the supply, or hardware platform providers. The basic stakeholder, i.e., suppliers and consumers in this context (the term consumer is here the AI developers), might have conflicting views. This conflict starts eventually already by different assumptions of the cost and price of goods. While the economical discussions might be resolved by mechanisms like *pricing models, auctions,* or even *game theory* to find a price, the underlying assumption is that the economics is supported by ***trust among the stakeholders and*** **implemented by robust mechanism to enforce the aimed security, incl. data privacy**. The description of the mechanisms and the roles of entities are the general objectives of the BonsAPPs security architecture.

This trust is typically a result by two characteristics of the system that will support this security: first, the system and its mechanisms need to be comprehensive, i.e., they need to able to ***address all major malicious or non-malicious violations of the economical rules***. Second, these mechanisms need to be on a ***sufficient high technical maturity and robustness*** such that they can counter the relevant violations, e.g., to withstand concerted infringements of the economical rules.

The BonsAPPs H2020 project is a significant continuation and enhancement of the previous Bonseyes project. BonsAPPs will develop, implement, and mature an AI-as-a-Service (AI-aaS) layer that will be accessible thorough the Bonseyes AI Marketplace (BMP), cf. [D1.1] and [D2.4]. A major subsystem of BonsAPPs AI-aaS is the Security-as-a-Service (Sec-aaS) layer. This subsystem will provide a *security service layer* that is able to establish sufficient trust and security for the BonsAPPs AI-aaS system. An main objective of the Sec-aaS layer is to off-load the AI developer from non-AI-specific development tasks, such as designing security mechanisms to counter copyright infringements, support software licensing, or enable secure deployment of software on edge devices.

This document aims at summarizing the requirements and describing the concepts and the initial technologies, for this stage of the project, for the Sec-aaS subsystem in BonsAPPs' AI-aaS architecture. The document has three detailed objectives:

a) in first place, it aims at providing a streamlined and concise description of the initial BonsAPPs Sec-asS architecture and the security mechanisms; the objective is to use this documents as reference that enables developers to obtain the required TRL level, b) it will describe the new security concepts and mechanisms, which are needed but weren't yet addressed in Bonseyes, or were identified after the project's finalization, e.g. Kudelski[1]'s KOP

[1] Kudelski, part of the Nagra group, is project subcontractor expert providing cryptographic and digital security technologies.

mechanisms or the approach to specify and handle different security levels (cf. Section 4 and Sections 6), and c) it outlines a workplan to reach the expected high technical readiness level of TRL8 for the mechanisms.

This document is structured as follows: Chapter 1 provides a short introduction of the objectives of this document. Chapter 2 and Chapter 3 summarize and document the BMP, its requirements and the security architecture of the BMP. Chapter 3 also provides a discussion of the interoperability of the BMP with other AI marketplaces. Chapter 4 outlines the matching of the AI development process and the development and deployment toolchains with the with Kudelski's security mechanisms. The description in Chapter 4 works towards a BonsAPPs Sec-aaS layer. Chapter 5 outlines the project planning within the context of the three AIaaS releases of BonsAPPs for implementing the various Sec-aaS mechanisms. Chapter 6 provide a first approach on how to evaluate the security and privacy levels in the BonsAPPs Sec-aaS layer and for later specification of flexible and adaptive security levels and their inclusion in licenses (assuming that not always every security mechanism is needed, but instead a developer should be empowered to decide on the choice of the security level and the mechanisms). Finally, Chapter 7 summarizes the documents and details current risks in the implementation of BonsAPPs' Sec-aaS layer.

2 Bonseyes AI Marketplace

In this section, we will describe and summarize the Bonseyes AI Marketplace platform. This is to a certain extend a repetition of the findings and documentation from the BMP [D2.4]. Therefore, some of the paragraphs below contain a summary of the initial general architecture documents of the BonsAPPs project [D1.1]. The aim is to give the reader a *concise and technical description of the BonsAPPs Sec-aaS layer.*

2.1 Context

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. The BonsAPPs AI-as-a-Service (AI-aaS) layer [D1.1] will be accessible on the Bonseyes AI Marketplace and deployable on the AI-on-Deamnd platform (AI4EU). Furthermore, the platform will enable the BonsAPPs Security-as-a-Service (SaaS) layer to operate across all the integrated services.

Developing AI Applications to solve industry challenges requires several *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 on resource-constrained devices* such as deeply embedded systems found in healthcare devices, cars, and robots. The deployment of AI in such systems demands to meet many non-functional requirements in addition to stringent accuracy targets and complex system integration skills. Similarly, a dynamic strategy to handle security requirement will be needed to deploy such that the ever-evolving challenges posed by various adversaries can be addressed. Hence, BonsAPPs Security-as-a-Service (SaaS) will play a key role to fulfil the necessity on demand and by design.

2.2 The Bonsyes AI Marketplace: A Trusted Platform for 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 providing efficient tools to benchmark AI Apps for specific target platforms. For a detailed description of the AI engineering processes and roles, please see [D2.4, D1.1].

Underlying the many interaction among the different actors in the marketplace, is the *process to increase the accuracy of the AI application*. An innovator can communicate his/her expectations by providing evaluation code in the marketplace that will test the produced AI Apps not only for accuracy but also for non-functional requirements such as latency, throughput, or memory consumption. To enable automatic testing of non-functional requirements, the benchmarking procedure relies on the deployment tool available through the BMP 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.

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. 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, namely Researchers, Innovators, Data scientists, and Developers. The corresponding personas along with their requirements and value propositions were described in [D1.1].

The Bonseyes AI Marketplace platform consists of a web marketplace (also denoted as WebUI – Web-based User Interface), an environment for secure multi-party collaboration (denoted as the Secure Virtual Premise, SVP) and a Bonseyes CLI tool. This is a direct tool that facilitates and supports 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 1.

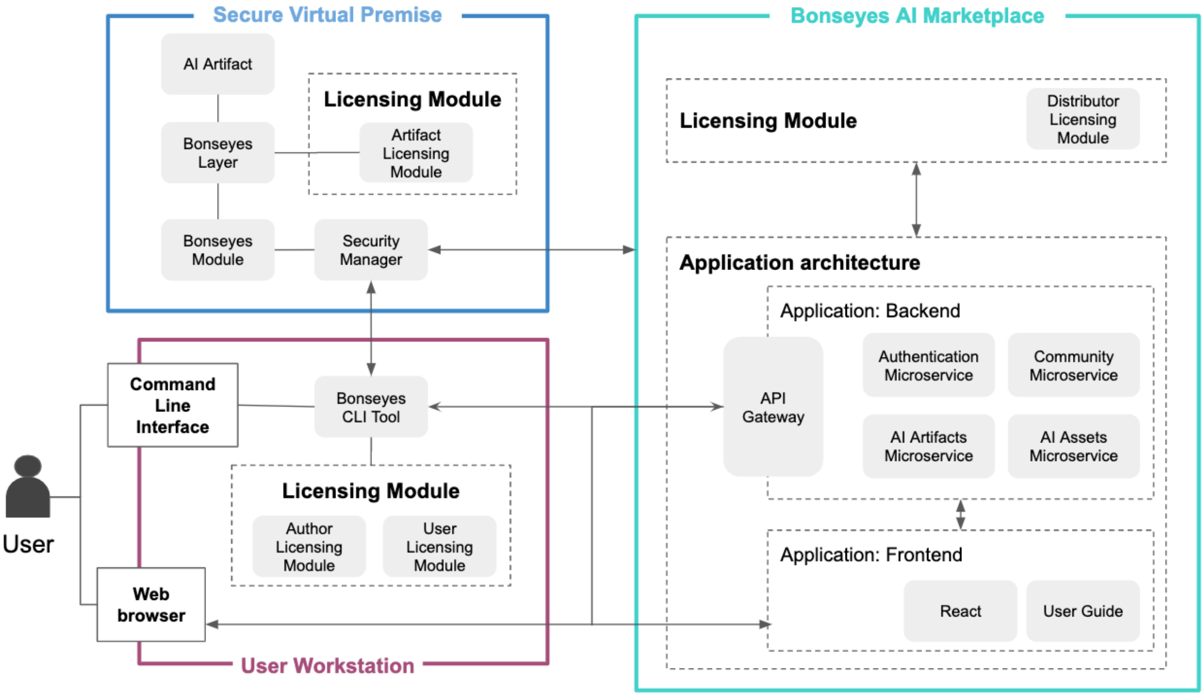
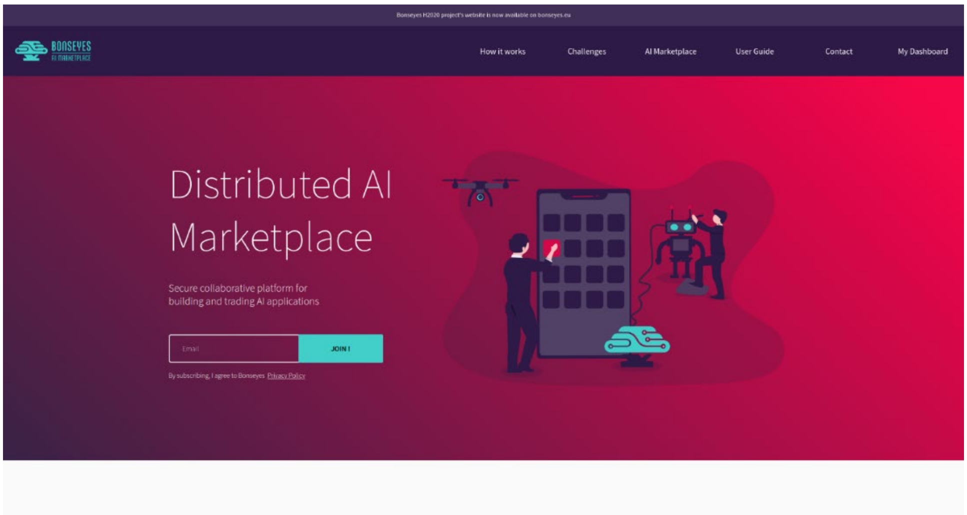


Figure 1: Overview of the implemented architecture

2.2.1 WebUI: Bonseyes AI Marketplace

The Bonseyes AI Marketplace is a major user interface, cf. Figure 2, and a web platform that connects researchers, developers, and companies to procure, collaboratively build, and trade AI Applications. This section describes its functionalities and architecture.

The AI Marketplace is applying the typical microservice architecture and which distinguishes between Frontend and Backend of the marketplace. 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

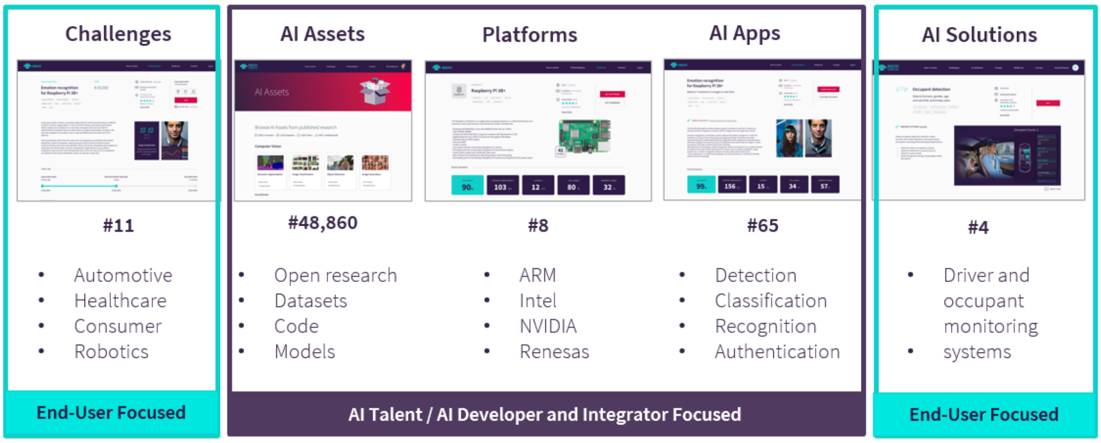
Distributed AI Marketplace

Secure collaborative platform for building and trading AI applications

By subscribing, I agree to Bonseyes Privacy Policy

Figure 2: 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 an AIChallenge and open a tender for its solution, on the other side developers and data scientists can join the AI Challenge with the aim to solve the challenge and monetize their expertise. Figure 3 depicts 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 3: AI Assets and AI Artifacts available on the AI Marketplace platform

2.2.2 Secure Virtual Premise (SVP)

Secure Virtual Premise (SVP) is a platform tool that facilitate and secure collaboration with the privacy sensitive Artifacts in the process of the AI solutions development. The SVP provides ***an application-specific trusted execution environment for edge AI development***. It follows therefore the call for trusted execution environment as suggested by Google [Wired20] and the ACM and academics to protect data [Benz20, Peis21]. However, the SVP has chosen a different technological concept of sidecar proxies since it needs to handle source code and its economics [TIT20].

The SVP is shown in Figure 4. It is a platform tool which federates the required compute, storage, and execution environments. Marketplace's users can use the SVP to execute AI Assets securely and trustfully, 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. The orchestration can be guided automatically, for example, by the aims of the benchmark process.

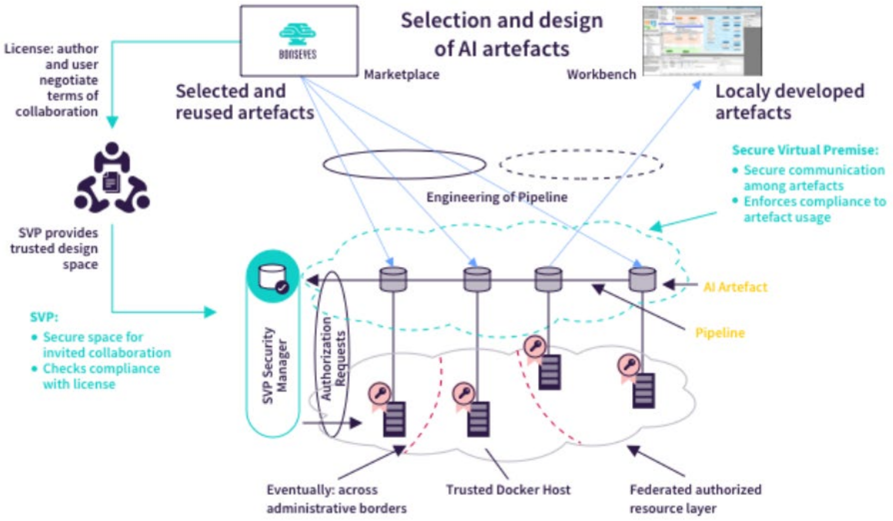
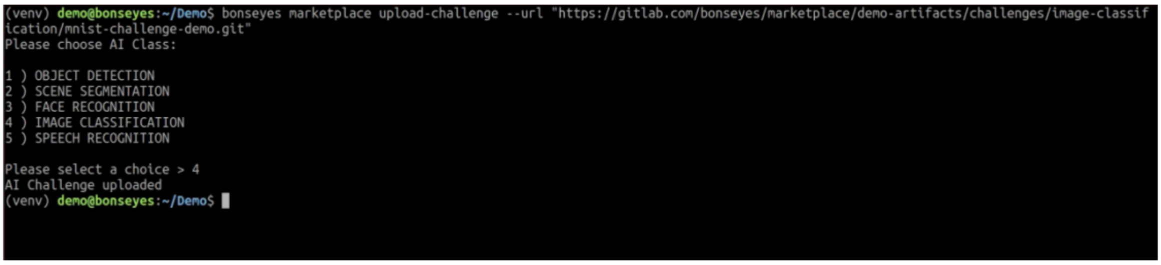

Selection and design
of AI artefacts
BONSEYES
Marketplace
Workbench
License: author and user negotiate terms of collaboration
Selected and reused artefacts
Localy developed artefacts
Secure Virtual Premise:
• Secure communication among artefacts
• Enforces compliance to artefact usage
Engineering of Pipeline
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

2.2.3 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 5 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 5:Bonseyes CLI Tool interface.

The CLI tool can be used to create and consume AI Challenges (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 containers 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.

2.3 Bonseyes AI Marketplace API Concept: Enabling Programmability

The Bonseyes AI Marketplace aims at providing first APIs (Application Programming Interfaces) that enable a programmability of the frontend service of the Bonseyes AI Marketplace. An initial structure of the API concept is given in Figure 6. These APIs are initially categorized into two main classes: 1) APIs for community services and 2) APIs managing the economics of the AI Artefact including their exchange and business settlement.

1. **Community** service is oriented around 'Actors', specialized professionals (Users) and Organizations that 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.
2. **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.

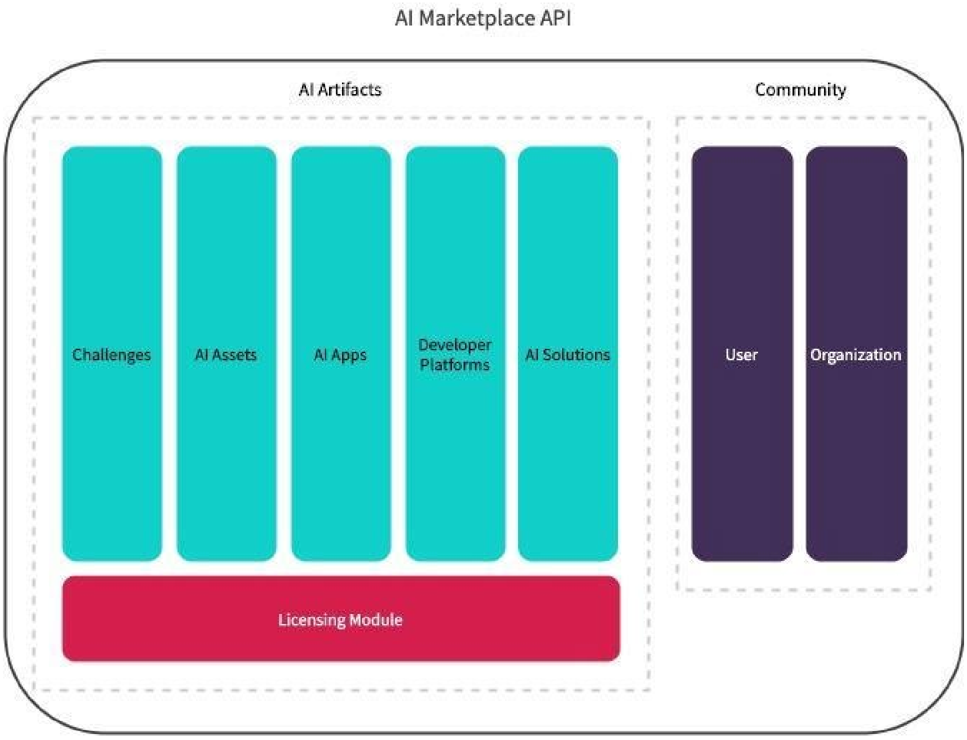


Figure 6:AI Marketplace API description

Available functionalities provided through the Marketplace API can be further divided into four subcategories:

1. **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.

2. **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. AI 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.

3. **Downloading of the AI Artifacts:** Downloading of the AI Artifacts is provided through the API, downloadable AI Artifacts are joined AI Challenges or AI App and Developer Platforms that the user has a right to download (I.e., they are purchased).

4. **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 an Organization and can be listed as an organization member. User and Organization information can be changed performing different API functions.

To enable interoperability and add new services on the AI4EU platform, BonsAPPs will define and propose a dedicated APIs to this effect. If agreed by AI4EU and BonsAPPs, the new APIs could allow new services developed by BonsAPPs to store and retrieve data on AI4EU related to these new services (see Section 3.14).

3 Security for Bonseyes AI Marketplace Platform

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 providing 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 detail the major concepts and techniques of BonsAPPs' security architecture such that the project's technology roadmap and implementation timeline can be understood.

3.1 The BonsAPPs Security Architecture

An assessment of the AI development and deployment toolschains 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 BMP system architecture and security concept described in [D2.4]. The assessment led to refinement of this architecture which is depicted in Figure 7.

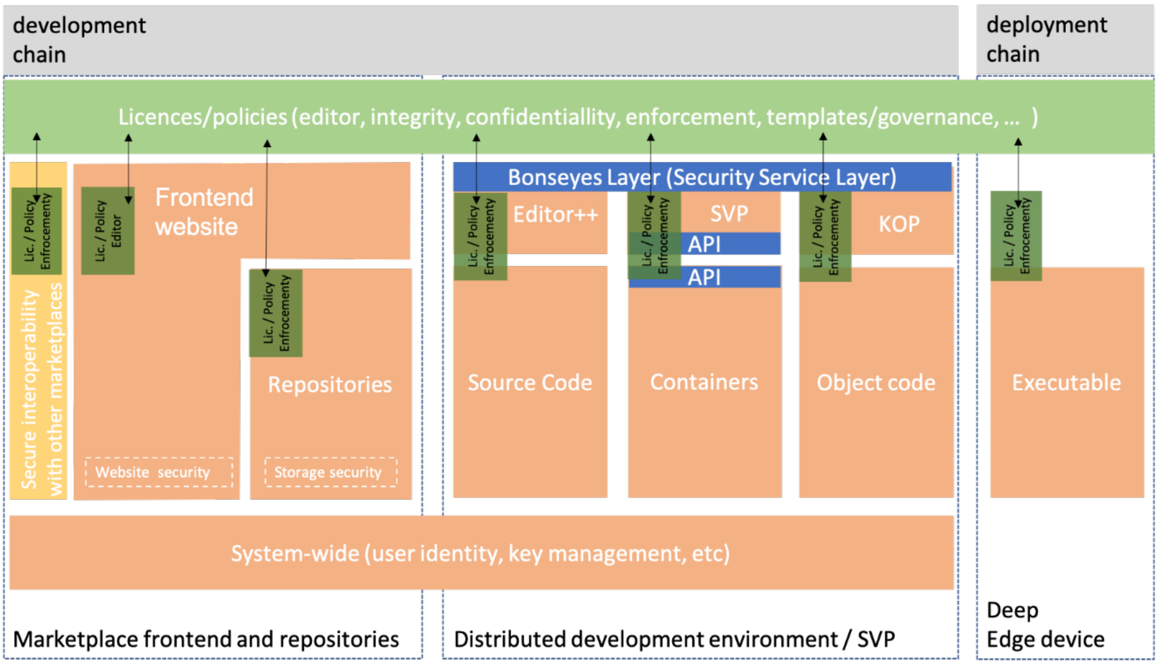

development chain
deployment chain
Licences/policies (editor, integrity, confidentiallity, enforcement, templates/governance, …)
Lic. / Policy Enforcementy
Secure interoperability with other marketplaces
Lic. / Policy Editor
Frontend website
Website security
Lic. / Policy Enforcementy
Repositories
Storage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

Figure 7: Concept BonsAPPs Security Architecture.

3.2 Overview of the Security Architecture

This service is enabled by a consistent use of licenses for the AI Artifacts throughout the BonsAPPs system. This system-wide use is indicated in Figure 7 by spanning the specification and enforcement process of licenses and policies over the whole system (green block in the figure on ”Licences/policies”). 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 [ORDL]. The enforcement of licenses is implemented locally by P*olicy Enforcement Points (PEPs)*.

Furthermore, the security architecture aims at handling the complexity of developing AI applications as well as deploying them. 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 at the Cloud, the developer’s desktop, the edge and Deep Edge devices. Hence, the architecture addresses this by considering two different tool chains, cf. Figure 7:

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

Moreover, the development workflow in the 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 AI Artifacts persistent), and ii) the collaborative, distributed, and secure development environment, the *Secure Virtual Premise (SVP).*

The BonsAPPs' SVP enables the developer toolchain 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 *BMP Sec-aaS Layer*, previously known as *Bonseyes Layer.* It acts as a separator, i.e., it shields the object from direct access, and provides APIs to the development and deployment toolschains. The layer checks the authenticity and authorization of the developers which use these APIs.

3.3 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 toolchains 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 toolchains. Hence, major project resources will be devoted to supporting this part of the development process, see below.

3.4 Focus Areas the Sec-aaS Paradigm 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 services for the Security-as-a-Service Concept: four security tools and toolkits and two additional system-wide service areas:

- 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.
- A ***Secure Deployment tool****:* this tool supports the secure deployment of software on end devices, i.e., it supports the Deployment Toolchain.
- ***Secure Transfer, Storage and Marketplace Interoperability Tools****:* this tool is a set program and functions to enable the secure transfer of AI Artifacts among interoperable marketplaces, from marketplaces to developers, and the secure and long-term storage of AI Artifacts for later use.
- ***Trusted Computing as a Service Tool****:* this tool is the refinement of the BMP SVP tool such that the SVP and the BMP Security Service 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.
- ***Frontend Security****:* this group of activities addresses the security of marketplace web frontend, which is the first visible BMP entity for any user.

- ***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.

3.5 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 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 Management

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 [D2.4]). In the context of BonsAPPs community as well as associated external platforms, user identity and key management is an interoperability component that allows 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) Cryptographic Key and Certificate Management

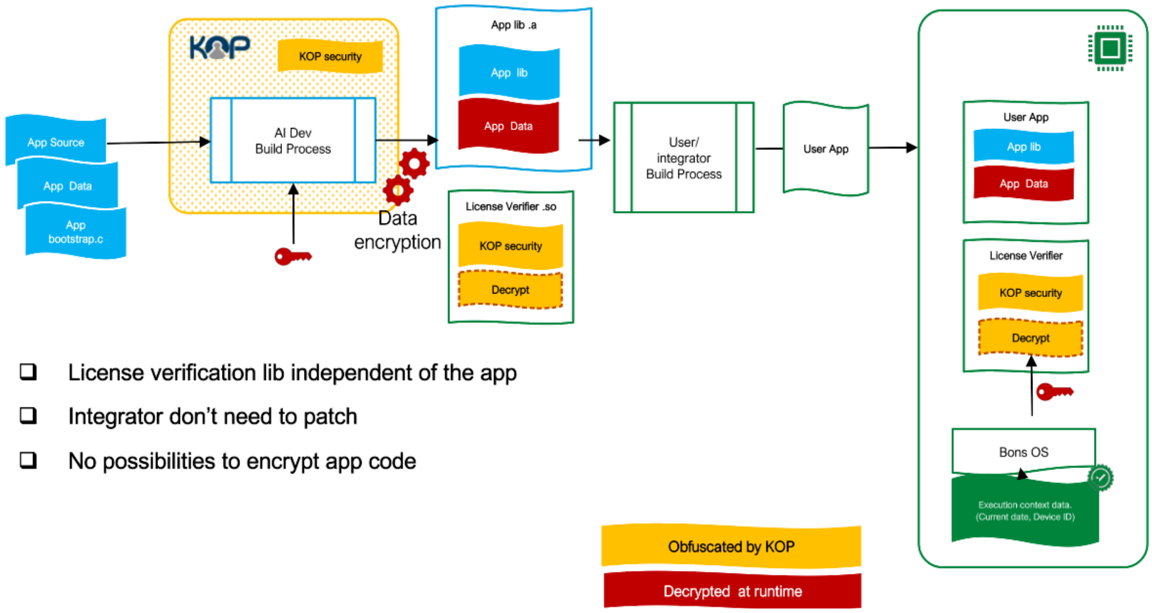
In Secure Virtual Premise (SVP), the Public Key Infrastructure (PKI) was implemented with OpenSSL version 1.1.0. The entire PKI is based on X.509 public-key certificates. For generation, the OpenSSL tool is used within the Linux OS environment. First, the root certificate is generated to establish root 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 must provide their certificate, public key, and valid license to establish HTTPS communication with the SVP and conduct the AI engineering process.

3.6 Security Concepts and Mechanisms in the Development Toolchain

The security concepts and mechanisms for the development toolchains 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.

3.7 Encryption and Code Obfuscation for AI Artifacts

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™ products [keyST].



- ❑ License verification lib independent of the app
- ❑ Integrator don't need to patch
- ❑ No possibilities to encrypt app code

Figure 8: KOP's encryption and code obfuscation of AI artifacts for a scenario that contains static AI library and dynamic decryption delivered to the integrator.

As illustrated in Figure 8, KOP provides mechanisms for encrypting arbitrary code functions (which will be merged with the "AI Dev(eloper) Build Process") and linking with object files or static libraries of any native programming language. In addition, it provides mechanisms to protect the integrity of all the binaries deployed at the deep edge device, including preventing its debugging or the emulation of the application.

3.8 Detailed Security Aspects of the AI Platform

3.8.1 Frontend Security Engineering

Frontend Website Security: The end user facing the frontend website is the first contact point for a user as well as the first visible element expected to be attacked. However, since it uses standard web technologies it also uses standard security concepts and technologies to harden the website against attacks. 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 should not be exposed to the public and the VPN should be only used by administrators and developers.

Frontend User Access Control: The AI marketplace frontend's objectives are openness and attracting AI developers for enabling network effects in AI development. The user access control in the front will assign a system-wide digital entity identity and representation for the user. It will check for and enforce access and usage policies on the website. Here, no IP access lists (nor IP white nor blacklisting) or restrictions with VPN only access will occur. Ideally, a sort of single-sign-on (SSO) with unique user identities should be enforced.

3.8.2 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 3.14 and [D1.1].

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

The BMP SVP [TIT20] has demonstrated the technical capabilities of BMP' collaborative AI development concept on TRL level 3 – 4 [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 SVP tool comprises two categories of activities:

Reliable Management and Dsitrubuted Setup of a Multi-Site SVP

Figure 9 shows the concept of a multi-site SVP [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.

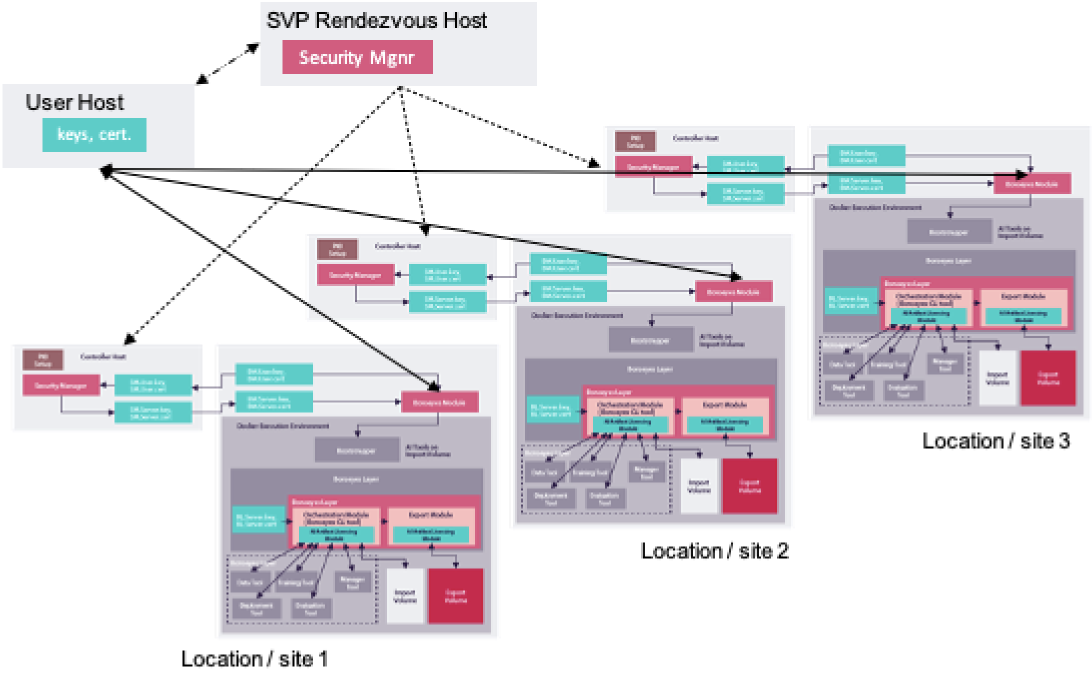


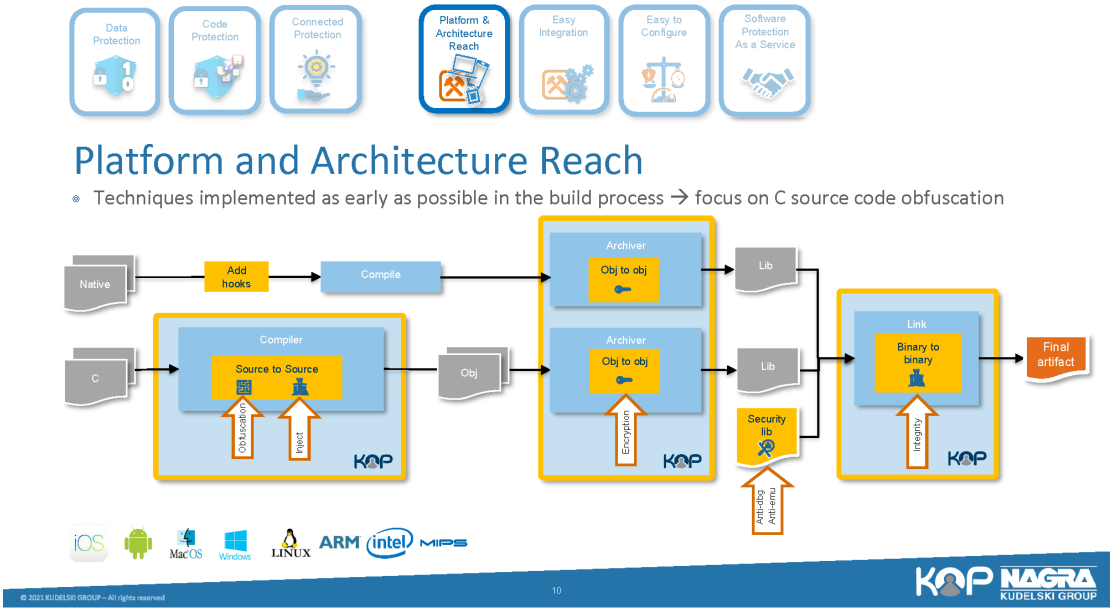
Figure 9: Concept of a Multi-site SVP

Handling of Additional Generic Type sof AI Artifacts by the SVP

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 BMP Security Service Layer. Hereby, the BMP Security Service Layer and the SVP validates the authenticity and authorization of developers toward the license for this AI Artifact and shields the AI Artifact from unauthorized access to its content.
2. *Object code and library objects:* An object code encryption and eventually obfuscation mechanism is applied here which is based on the technologies provided by Kudelski's KOP and

IoT keyStream™ tool [keyST]. A brief outline on the code obfuscation process of Kudelski's KOP tool is provided in Figure 10.


Platform and Architecture Reach

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

Figure 10: KOP's c object code obfuscation mechanism

3.9 AI Artifact Licensing

A collaborative AI development process is an attractive alternative to the monolithic "do-all-yourself" approach, cf. [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.

Furthermore, the technology from Kudelski will ensure that the license management is enforced throughout the platform by using technology from the KOP suit, cf. Figure 11. This figure was developed by the Kudelksi team in cooperation with the BonsAPPs WP3 team and considering the both the security capabilities by KOP and the security and requirements by BonsAPPs. This license support is indicated in the figure by icon of a license between the "Certificate Generator" and the "Cert. Verifier". The mechanisms will be specified further during the development work in BonsAPPs for this Sec-aaS layer feature.

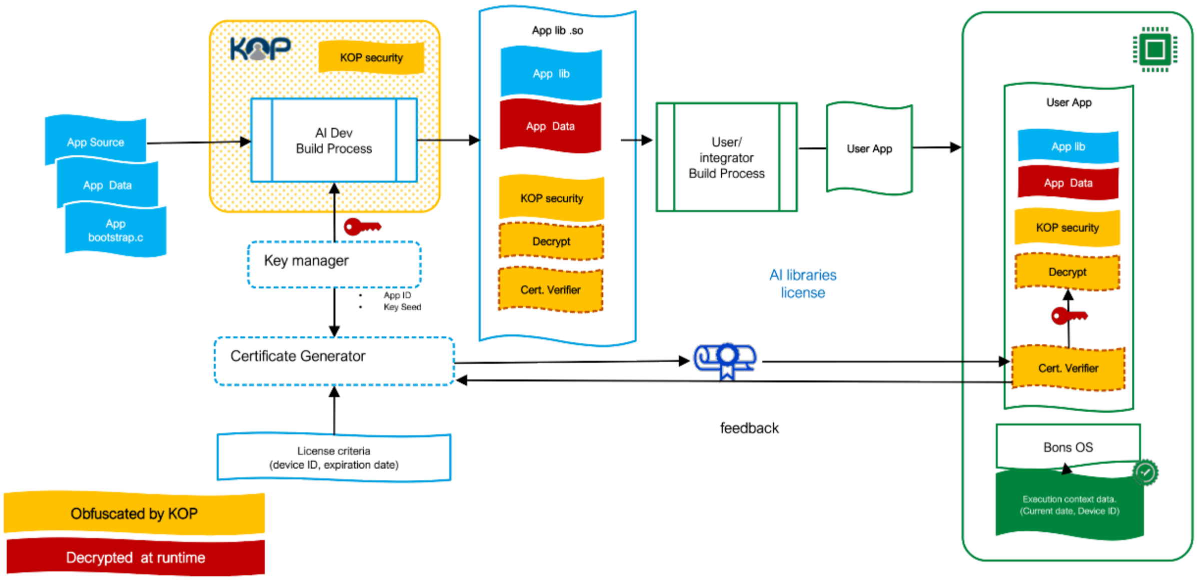


Figure 11: An overview of Kudelski's license management strategy to protect the AI libraries throughout the BonsAPPs platform.

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.

3.10 Open Digital Rights Language and System Overview

The BonsAPPs architecture will use the Open Digital Rights Language (ODRL) [ORDL, 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.

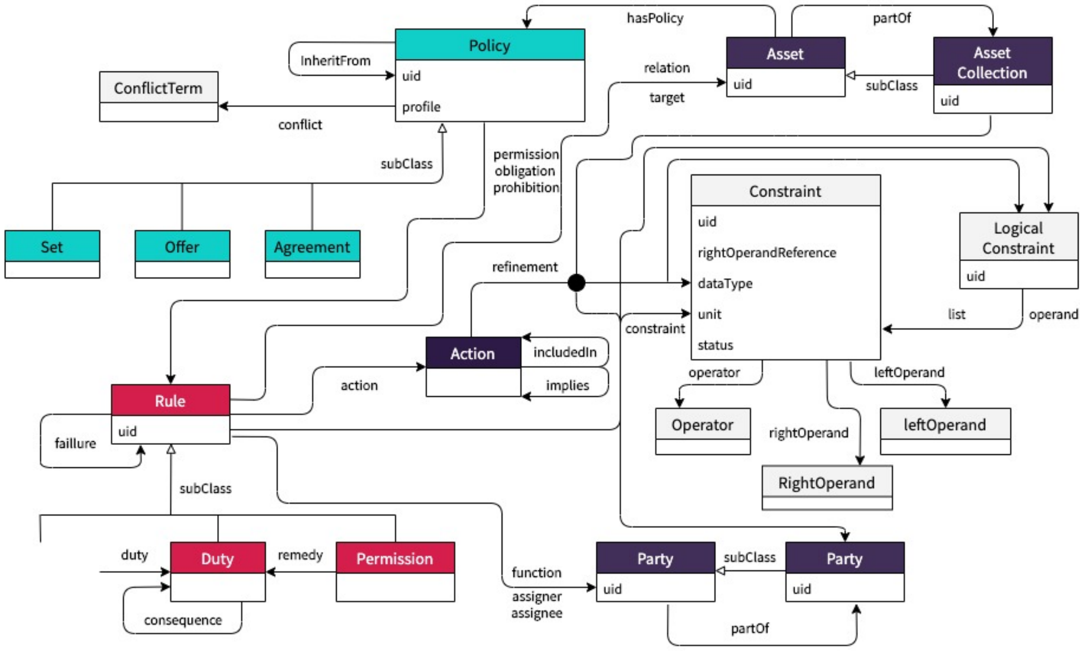
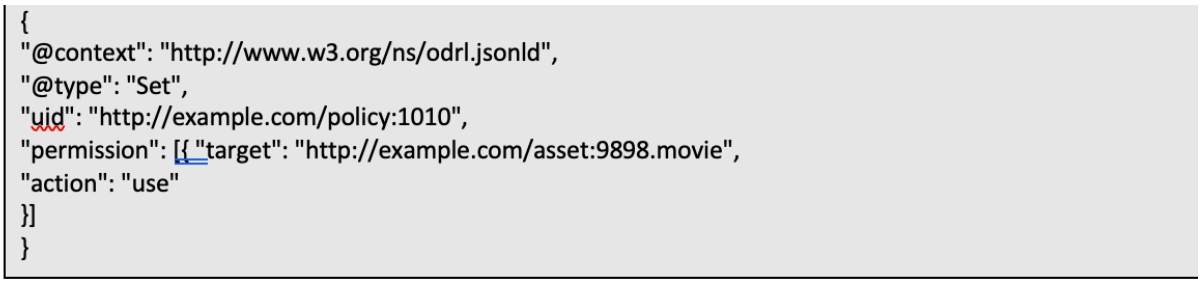


Figure 12: ODRL information model for specifying digital rights, cf [ORDL18a]

The ODRL information model: A *Policy* can be created for an AI Asset (a kind of AI Artifact) 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

3.11 Overview of the Planned BonsAPPs Licence Management System

The licenses for AI Artifacts will be handled by the *BonsAPPs Licence Management System* which is outlined in Figure 14. The system is based on the license concept developed in the BMP [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 supported 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 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.

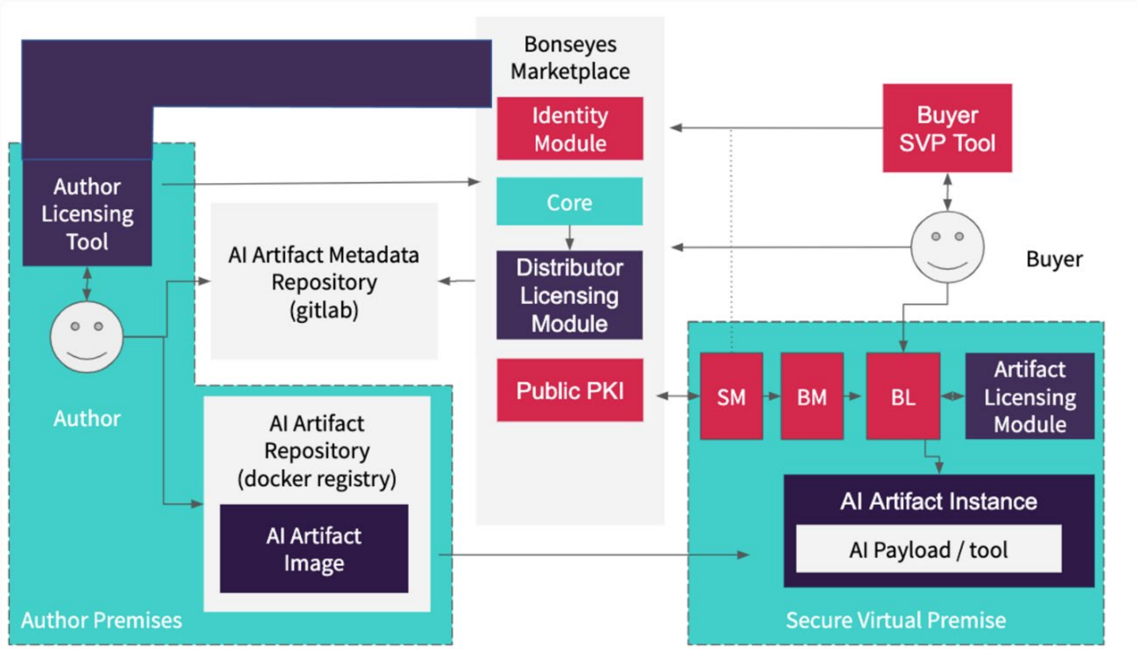


Figure 14: Overview of the BMP ecosystem and the BonsAPPs Licence Management System with the different licensing modules (in red).

3.12 Bonseyes AI Marketplace Interoperability

3.12.1 Overall Interoperability Concept

An interoperability framework is key to be able to deploy the BonsAPPs services available on the BMP to the AI-on-Demand platform (AI4EU) and other platforms as relevant. BonsAPPs interoperability concept can be best explained by assuming an example use case of two companies or stakeholders joining forces to design a future, smart AI application and by detailing the used and provided technologies. In this use case, by using the Bonseyes AI Marketplace and its SVP, a company innovating in AI systems ("Industry Innovator") can securely share a specification with a designated AI developer ("AI Company"), cf. Figure 15. The Industry Innovator can benchmark a given AI application connected to the SVP without sharing any secret data. The AI Company can securely share such a developed AI application with the Industry Innovator. The AI application will only run within the SVP and may only be used for benchmarking as indicated by the developer-specified license. The SVP ensures that all AI Artifacts remain on the designated machines and cannot be used for purposes other than specified.

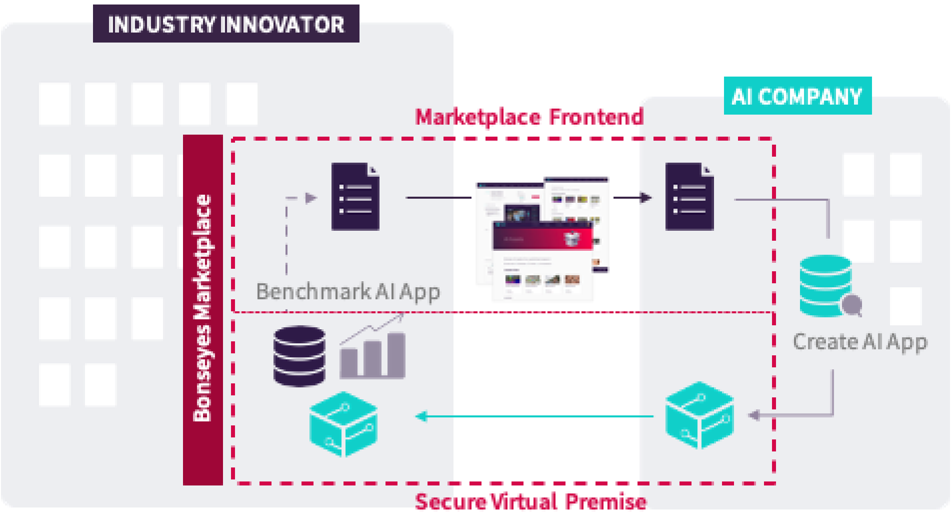


Figure 15: Use Case of Two Companies Interaction in by the Bonseyes Marketplace

Network Effects and Interoperability

Networking effects in economics and business are the *result from adding more users and goods to a supply-and-demand system*. If such an effect is present, then *the value of a product or a service increases according to the number of users consuming them*. Additional network effects by interoperable marketplaces are:

- **Growth and quality:** A user can choose from more options and take the one which is most suited.
- **Defragmentation and faster access: A** user can find the required resources much faster.
- **Competition, supply, and specialization:** Users can request a larger community to develop a solution, while suppliers are able to provide a solution based on a previous development.
- **Normalization of workflows:** Similar steps in a workflow can be performed using the best resources available, while maintaining development speed and enabling individual solutions.

Interoperability Levels in AI Software Ecosystems

Interoperability in software ecosystems, however, imposes significant challenges. The complexity of these challenges increase in collaborative and commercial environments since additional functionality needs to be considered. Interoperability should resolve fragmentation of resources and provide integration and normalization of resources, objects, API, algorithms, data, workflows, and policies.

While compatibility for searching resources and platform-independent execution of software becomes increasingly available in AI marketplaces, e.g., using containerization platforms such as Docker, the new challenges for interoperability came from the consideration of economic needs of AI assets. The cost-efficient procurement and the licensing of AI software and AI solutions becomes of increased importance, instead of exploiting open-source concepts, due to the high cost for AI development and data collections. Additional challenges in data-driven AI systems arise from the needs of compliant use of data, models, and processes, e.g., high data privacy requirements (e.g., GDPR) or certified model correctness within financial, health, legal or defense applications.

Interoperability is in general the ability of different information systems, devices and applications ('systems') to access, exchange, integrate and cooperatively use data, algorithms, models, and tools, in a coordinated manner, within and across organizational, regional and national boundaries. Hereby four levels of interoperability and capability classes can be considered for AI marketplaces:

- **Basic Technical Foundation (Level 1)** – establishes the requirements and solutions for securely interconnecting marketplaces and exchanging metadata about AI Artifacts and the AI Artifacts themselves. The solution comprises the specification of secure transfer protocol and the mechanisms for trusted identity and certificate management, e.g., for authenticating users and resources.
- **Structure and Semantic of Metadata (Level 2)** – defines the organization, format, and syntax of metadata about AI Artifacts and objects in the marketplace as well as APIs for using the marketplace. These APIs include functions for searching, publishing, listing (catalogue) and transferring of AI Artifacts in the marketplace and among the participants.
- **AI Artifact Management (Level 3)** – provides for common underlying models and codification of the AI Artifacts including API to use the functions of AI Artifacts. These APIs might be specific to the capabilities of the AI Artifacts, e.g., start/stop model training, pre-process and extracting of images, etc.
- **Workflows and Governance (Level 4)** – includes workflows, licenses, governance, legal, and ethical considerations to facilitate the secure, trusted, and collaborative use of AI Artifacts, both within and between organizations, entities, and individuals. This level defines integrated end-user processes and workflows as well as shared consent (e.g., the licenses) and trust.

BMP Interoperability Layers

Departing from the above detailed level of interoperability, the BMP has developed a four-layer interoperability concept for its AI marketplace for increasing the suppliers' and users' benefits. This concept addresses the needs of technical compatibility as well as it stretches into the commercial, legal, and compliance requirements. *Each interoperability layer provides a distinct value and functions set to the user of the marketplace.* The fours layers are, cf. Figure 16:

- **Authentication and Infrastructure Compatibility (Layer 1)** – This layer defines basic and fundamental data structures and mechanisms to enable interworking of the Bonseyes AI Marketplace with other marketplace, such a common user profile (incl. security certificate and cryptographic key management), a single-sign-on (SSO) service, the specification of the container structure or the data warehousing subsystems (git, container registry, etc.).

  Use case equivalent: The "Industry Innovator" and the "AI Company" agree on a common user profile and user authentication (e.g., SSO) such that authenticated people can engage between the stakeholder and can interconnect trustfully to other marketplaces.

- **Describing, Searching, Indexing, and Publishing of AI Artifacts (Layer 2)** – 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 BMP assets into other marketplaces.

Use case equivalent: First, a search by an "Industry Innovator" for an AI Asset is forwarded automatically using the proper syntax to another marketplace. Subsequently, the result can be used by the "Industry Innovator", eventually using trustfully the agreed policies (see the layer 3 and layer 4 of this concept). Second, an "AI Company" can publish the developed AI Assets and other users outside the BMP system be able to use them. Their usage might be subject to the trust, security and license policies supported by the BMP' SVP (see the layer 3 and layer 4 of this concept).

- **Secure AI Artifact Remote Execution (Layer 3)** – This layer of the interoperability describes the infrastructure needs, mechanisms, and the APIs to share securely and trustfully, access, execute and orchestrate AI Artifacts, AI Assets and AI Pipelines in decentralized ways using distributed and off-premises executions environment. This layer comprises mechanisms to secure federate compute, execution, and storage resources and to enforce trust and licenses across these locations.

  Use case equivalent: An "Industry Innovator" can a) select and combine arbitrary distributed execution environments into a "virtual premise", b) populate the "premise" with AI Assets contributed from one or more "AI Company", and c) conduct the execution of an AI training pipeline to generate an AI Application. The distributed, trusted and virtual nature of this layer permits the use of the "compute-to-data principle", i.e., if sufficient compute power is available, algorithms and their execution can be moved to locations where data is located. This might resolve data privacy issues at the involved companies (both "Industry Innovator" and "AI Company") as well as it enables the new role of a trusted high performance computing provider.

- **Procurement Workflows (Layer 4)** – This layer permits trusted procurement workflows for AIs Assets within the Bonseyes AI Marketplace and across others. It facilitates the agreeing to the terms on how to acquire AI Assets by a tendering or competitive bidding process. This layer provides support for the trusted specification of licensing using the ODRL language and certification of the integrity of these licenses across marketplaces. Furthermore, it might comprise mechanisms for contract settlement, accounting, and payment.

  Use case equivalent: An "Industry Innovator" can publish a tender or challenge for an AI Asset across various marketplaces. An "AI company" can achieve an agreement with the "Industry Innovator" on the providing this AI Asset and both can formulate an agreement using ORDL for mutual benefit. The Bonseyes AI Marketplace may certify the integrity of the agreement such that it can be enforced automatically. Furthermore, the "Industry Innovator" and "AI company" may use the BMP provided and certified agreement templates for addressing societal governance requirements such as GDPR. Finally, this layer might comprise procurement mechanisms based on AI workflows. An example is *benchmarking*. The acquisition of an AI Asset by an "Industry Innovator" may be based on the *benchmarking* of this AI Asset. Both partners may agree to use a standardized benchmarking workflow, which is supported by the Bonseyes AI Marketplace. The latter even opens the opportunity of third parties providing *Benchmarking-as-a-Service (BasS).*

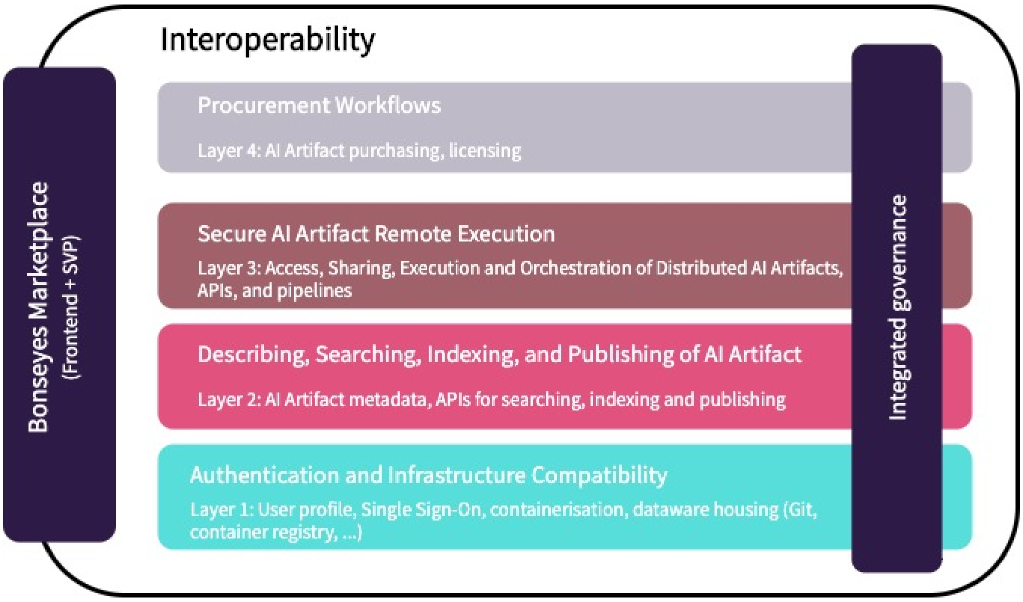

Interoperability
Bonseyes Marketplace (Frontend + SVP)
Procurement Workflows
Layer 4: AI Artifact purchasing, licensing
Secure AI Artifact Remote Execution
Layer 3: Access, Sharing, Execution and Orchestration of Distributed AI Artifacts, APIs, and pipelines
Describing, Searching, Indexing, and Publishing of AI Artifact
Layer 2: AI Artifact metadata, APIs for searching, indexing and publishing
Authentication and Infrastructure Compatibility
Layer 1: User profile, Single Sign-On, containerisation, dataware housing (Git, container registry, ...)
Integrated governance

Figure 16:Bonseyes Interoperability Layers

3.12.2 Layer 1: Authentication and Infrastructure Compatibility

Layer 1 of the BMP Interoperability focuses on simplifying collaboration through established authentication of users and ensuring compatibility of infrastructure focusing on the core elements of identity management, third party identity providers, and infrastructure compatibility.

Identity Management and SSO Third Party Identity Providers
Identity Management is an interoperability component that permits identity exchange and makes accessible public data of individuals, and organizations that are part of the BMP community to external platforms. External Authentication and Authorization Identity Providers can be integrated into the BMP identity system to provide straightforward onboarding of new users from domain-related platforms.
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.
The BMP 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 one of the external partner platform . 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.).

Infrastructure Compatibility
Infrastructure compatibility imposes the collaborators in the process of data-driven development of the AI systems, to align their infrastructure components (Data Warehouse, Source Code Management, and Containerization) to utilize all benefits that the BMP platform and tools provide. Data Warehouse component enables storage and management of the complex data, and data collection workflows, providing support to the collaborators to exchange AI Artifacts using specialized protocols. Source Code Management component enables management of the AI Artifacts source code, version history, version releases and a

mechanism for collaboration on the AI Artifact source code. Containerization represents a process where source code and all dependencies are packaged into the standardized units of software, e.g., Docker.

3.12.3 Layer 2: Describing, Searching, Indexing, and Publishing of AI Artifacts

Layer 2 of the BMP 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 BMP 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.

Search
The AI Artifact search represents a fundamental feature for the AI Artifact discovery. Browsing of the AI Artifacts follows a breakdown by type, with the possibility to apply various search parameters, i.e., search according to the classification problem, industry, or refine search with the more detailed data. Currently, the BMP exposes a collection of different AI Artifacts where currently published numbers are depicted in Figure 16.

Indexing
The BMP contains a master resources catalogue which is divided by AI Artifact types into the following categories of Challenges, AI Assets, Developer Platforms, AI Apps, and AI Solutions. AI Artifact APIs allow third party search engines to collect, parse, index and store meta-data of the AI Artifacts from the resources catalogue to facilitate fast and accurate information retrieval. The technology of the AI Artifact APIs also permits for the external requestor to specify only data that he would like to retrieve, providing a chunking and nested queries mechanism.

Publishing
Publishing of the AI Artifact demands a special form defined by the AI Artifact type. AI Artifacts needs to be provided in a form of a git repository, where AI Artifact sources needs to have compulsory standardised meta-file(s) that describes and gives insights into the AI Artifact, and license that specify permissions, prohibitions, and distribution details of the AI Artifact. Challenge, AI App and Developer Platform can be published to the AI Marketplace by providing git repository URL as a parameter to the API call or following publishing wizard with the BMP CLI Tool. AI Asset publishing requires a mandatory AI Research paper to be provided, and optionally reproducible source code of the AI Research.

3.12.4 Layer 3: Secure AI Artifact Remote Execution

Layer 3 of the BMP' interoperability concept focuses on the secure remote execution of AI Artifacts, AI Assets, APIs, and Pipelines. This layer builds on the mechanisms and APIs provided by the SVP (*Secure Virtual Premise),* which is the BMP' distributed, federated and secure execution environment for AI Assets. The access to the SVP's APIs for the execution, orchestration, and management of the AI Assets at distributed locations is monitored and validated for compliance with respect to the rules specified in a license file for an AI Asset. Only authenticated and authorized users are allowed to use the APIs of an AI Asset. Interoperability on this layer is achieved by a) translating user authenticated and user authorization between trusted execution environments and by b) providing a flexible translation mechanism for the semantic of APIs.

Furthermore, an enhanced version of the SVP is currently under development, which allows the arbitrary federation of trusted execution environments, cf. Figure 9. An SVP user can choose from execution resources at an SVP Rendezvous Host (SVP-RH), reserve and federate the selected computing nodes at different locations/sites and bind them securely into a specific SVP instance. Furthermore, the SVP-RH manages interoperable user profiles, including their cryptographic key and certificates.

AI Artifact Management

The BMP CLI Tool is a comprehensive command line tool that supports AI Artifacts management and orchestration of the AI Workflows and AI Pipelines. It provides interfaces to all major BMP components: AI Marketplace, SVP, Deep Learning Toolbox, Inference Engine and Deployment Tool (LPDNN) and BMP License Module to facilitate and accelerate the development process of the data-driven AI Solutions.

3.12.5 Layer 4: Procurement Workflows

Normalization of Procurement Workflows and Licenses

Layer 4 of the BMP interoperability concept focuses on the normalization of procurement workflows, i.e., on an increased exchangeability and automation of the acquisition process for AI Assets. It targets the automatic enforcement of procurement agreements. The procurement layer enables the BMP users as well as users from other, interoperable marketplaces to jointly agree on tenders, competitions, procurement rules, usage policies and their enforcement for AI Artifacts. The use of ODRL (Open Digital Rights Language) [ORDL] normalises the specification of license agreements between suppliers and consumers of AI Artifacts. ODRL is a machine-readable format, which permits the automated enforcement of licenses in the BMP SVP as well as the future settlement of contracts. In addition, normalized licenses by the Bonseyes AI Marketplace might comprise specifications for obeying compliance and governance policies, e.g., for legal and ethical requirements in AI application development.

Example Workflow: Benchmarking-as-a-Service

Benchmarking is a major part of the engineering workflow for data-driven AI applications. It determines the quality of an AI application. Interoperable benchmarking across engineering platforms, e.g., by Benchmarking as a Service (BaaS), is expected to make the AI engineering process more verifiable and may make the procurement process more understandable. The acquisition of an AI Asset can be made dependent on its performance for a provided benchmark.

3.12.6 Integration with AI4EU

Overview

BMP' network effects are maximized when integrating with AI marketplaces that provide a particularly large number of AI Assets and users. Moreover, the BMP aims at strengthening the European efforts to enable its innovative SME community with mechanisms for an accelerated adoption of AI technologies that quickens AI application development. Hence, the

BMP's objective is the integration with the AI marketplace of Europe's flagship AI community project AI4EU (www.ai4eu.eu). Hereby, the BMP focuses on its core technologies and AI Assets for engineering AI at the edge and on its outstanding support for the commercialization and procurement of AI Assets.

Required Integration Activities

The interoperability of both marketplaces is based on the interconnection of the BMP AI stack with AI4EU's layers, their service access points and interfaces by using functions from the above outlined BMP interoperability layers. The integration with AI4EU attaches the BMP layer to the seven architecture layers of AI4EU. Moreover, the BMP enhances the AI4EU marketplace interfaces and adds new capabilities for the open, trusted and secure procurement of AI Assets. The seven AI4EU architecture layers are:

- Use of public Internet: being accessible from all communities and platforms
- Applicative Security Layer: Identity management (including OAuth capabilities)
- Frontend UI Layer: Website and CMS giving access to services, one of the major contents being the AI resources catalogue and repository (Catalog API will be published later)
- Services Layer: Builds on associated content, Search layer to support indexation and Search services of above contents (Search API will be also partially open for interoperability)
- PaaS Layer: Where in the future AI resources might be assembled and tested in the studio like environment
- Infrastructure support / IaaS Layer: Providing computing resources to above services

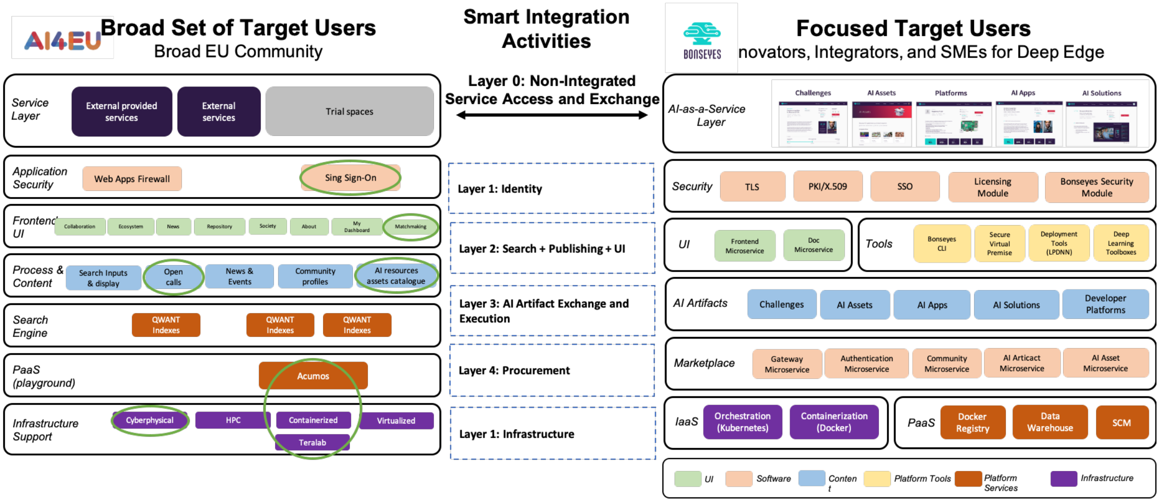


Figure 17: Interoperability architecture for interconnecting BMP with AI4EU

Figure 17 shows the interconnection of the AI4EU marketplace stack (left part of Fig. 17) with the one of BMP (right part of Fig. 17) by using smart integration and interoperability activities and techniques (center part of Fig. 17). The integration activities on each layer are summarized in Table 1. In the figure and the table, we omit the Internet layer of AI4EU since both platforms build generally on unrestricted access to the public Internet using the IPv4/IPv6 protocol. In addition, we assume as *layer 0 interoperability* the open interconnection and rather unrestricted use of AI service APIs of both platforms through Internet protocols and applications.

To guarantee the proper implementation of this process, the Bonseyes Community Association (BCA, https://bonseyes-association.org/) will nominate a representative to AI4EU for coordinating architecture integration and the software development for these activities.

Table 1:Interconnection Activities per AI4EU Layer

BMPs Layer	**AI4EU layer**	**Integration activities**
AI-as-a-Service layer	Service layer	Open, remote and rather unrestricted use of AI service APIs (interoperability on layer 0)
Security Layer	Applicative Security	Joint use of a Single-Sign-On (SSO) system, e.g., based on the OAuth protocol, and joint management of cryptographic keys
UI layer	Frontend UI	Functions for cross-marketplace AI Asset publication and search. Displaying origin of AI Assets and eventually informing the user when transiting between marketplace UIs and to other tools (e.g., BMP SVP)
AI Artifact layer	Process and Context	Mechanism to transfer AI4EU assets into BMP' execution environment and to execute-orchestrate them.
UI layer	Search Engine	Overlapping with Frontend UI: translation services for AI Artifact metadata and AI Artifacts indexes
Marketplace layer	PaaS	Mechanism to exchange challenges and to jointly agree on licenses (incl. machine-readable version); Functions to secure the integrity of the licenses (incl. encryption).
IaaS, PaaS layers	Infrastructure Support	Specification of infrastructure requirements for compute environments and code/data repositories, e.g., Docker version or Git repositories, etc.

4 Matching AI and Security Development Process

As a rapid-evolving AI platform, BonsAPPs will require an equally, if not faster paced security development process. To facilitate an equilibrium of supply of security development process and demand from the AI platform, Kudelski Obfuscator Process (KOP) will be used to harden the security of software for multiple devices throughout the BonsAPPs platform. The KOP mechanisms and other mechanisms will be matched to fit with the overall BonsAPPs security architecture.

4.1 Facilitating a Dynamic Security Development

KOP concept implements the main software hardening techniques to counter the main piracy threats on software: Reverse, Tampering and Code lifting. The KOP solution is based on artefact modifications at different steps of a software build. This is also outlined in Figure 18 which was provided by Kudelski's KOP team. These steps are:

1. Source code annotation
2. Source to source transformation (on C standard only)
3. Object to object transformation
4. Additional library linking
5. Binary patching

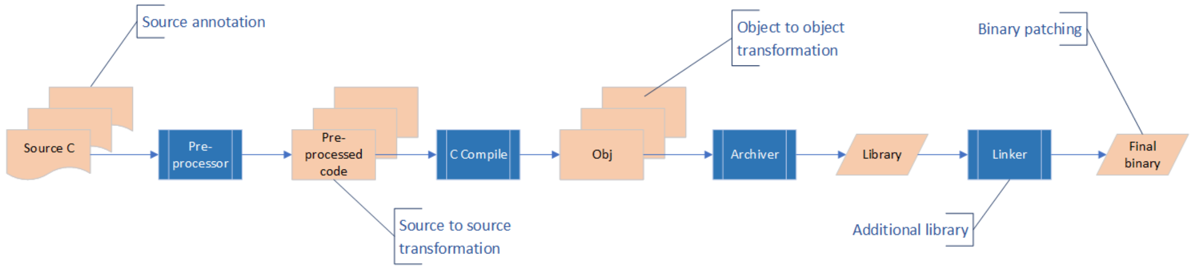


Figure 18: An overview of KOP's software hardening process.

The advantage here is that KOP is designed for a large range of devices and for use in many integration contexts. For example, a software can be "pre-hardened" by one team and integrated by another one. To reduce issues and dependencies on the BonsAPPs's development and deployment toolchains, platform or architecture, protections are applied by KOP as early as possible in the software build process. Source transformation is preferred to object transformation which is preferred to binary transformation.

4.2 Platform-wide Security Deployment

The challenge for the KOP's obfuscation mechanism is to combine the different techniques and transformations to enforce the overall security: code obfuscation, integrity checks, function calls hiding, code and data encryption, anti-debug, and anti-emulation mechanisms. Software hardening requires constant evolution to prevent new attacks, which is the primary goal for KOP to deliver. The KOP's initial placement in the above-mentioned development and deployment tools chains are partly indicated in Figure 19

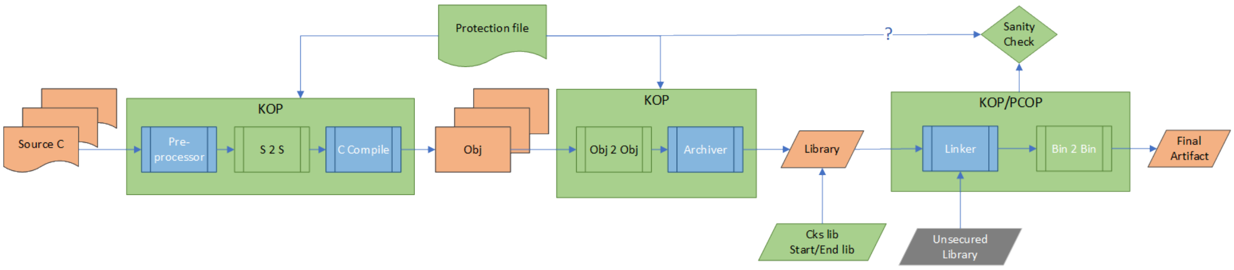
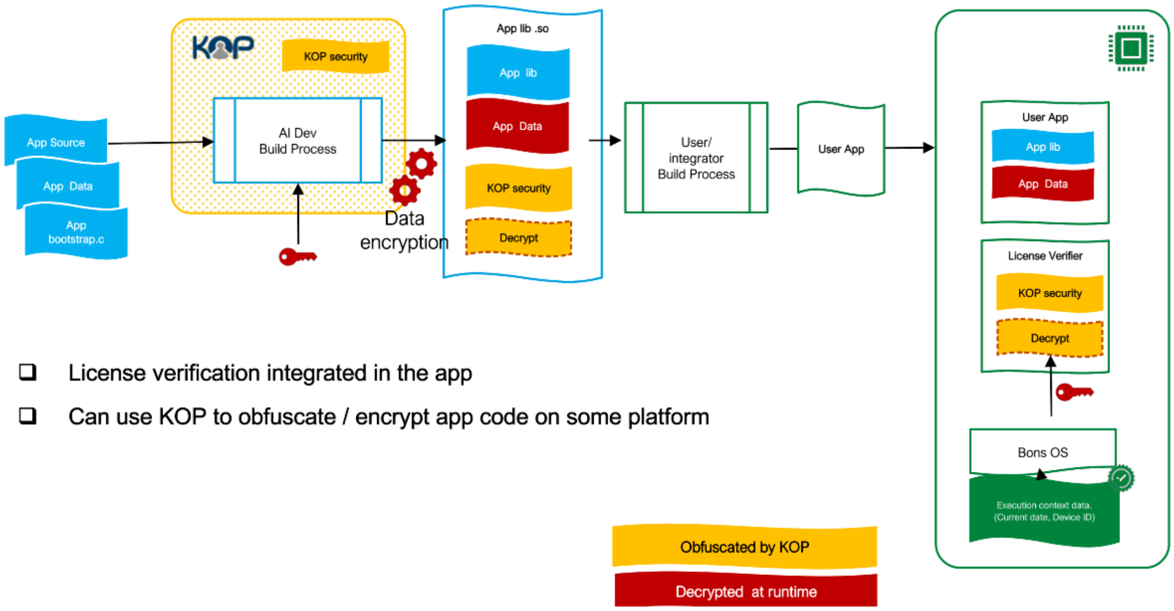


Figure 19: KOP's placement in the toolchain.

4.3 Accommodating both Static and Dynamic Scenarios

Kudelski's KOP will also be responsible to ensure integration and delivery of both static and dynamic AI Artifacts throughout the platform. Although this requirement imposes challenges, a solution for the accommodation of static and dynamic libraries is suggested by the Kuldeski team and suggested in Figure 20



- ❑ License verification integrated in the app
- ❑ Can use KOP to obfuscate / encrypt app code on some platform

Figure 20: An overview of KOP's strategy to deliver an integrated dynamic library to the integrator.

5 Implementation Paradigms and Initial Roadmap for the BonsAPPs Sec-aaS Layer

Next, we will outline the how the implementation work for the Sec-aaS layer is structure in reference to the BonsAPPs functional needs (i.e., development chain vs. deployment chain) and to the BonsAPPs project implementation, i.e., the project's overall approach which comprises multiple phases to sustain a lasting AI economy.

5.1 Overall Paradigms

Development Chains vs. Deployment Chain

Typical Edge AI leverages the fact that training and deployment processes for ML models are highly decoupled. This allows a trained ML model to be embedded in devices with limited memory and computational resources — enabling their execution in an offline fashion. In this typical scenario Edge AI models are developed and trained in a very computational capable Cloud environment; cf. left side of Figure 21. The Edge part of this development in implementation process considers the inference at the edge device as main technical function but also the needs for business invocation and enabling the application scenario; cf. right part of Figure 21.

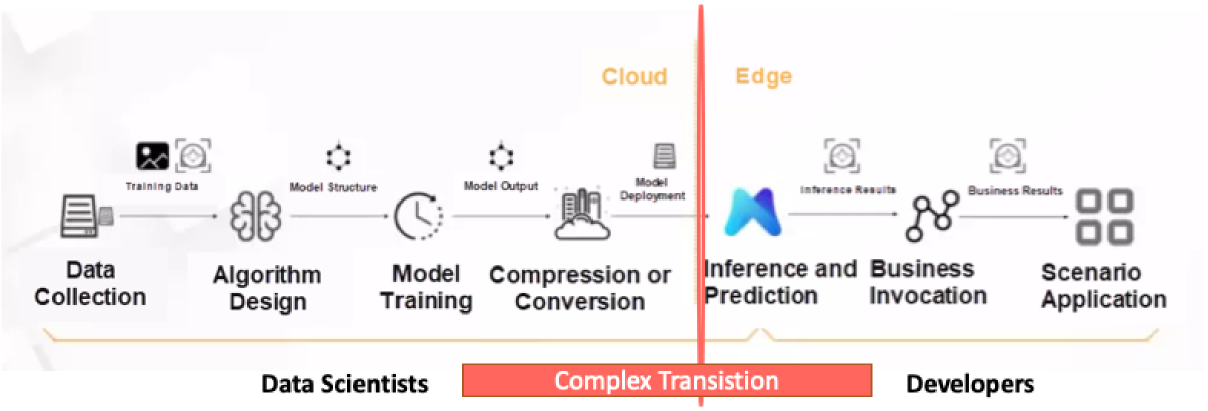


Figure 21: Edge Deployment Challenges

BonsAPPs will at first apply largely the more conservative approach of decoupling the development chain from the deployment chain. However, in future BonsAPPs might extend the development chain in the deployment chain for being able to continuously integrate new or improved ML models into deep edge device and in turn also to feedback eventual model improve (e.g., done by local learning) in the development chain.

Moreover, deploying ML models on edge devices remains a very challenging task. As indicated, 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 many 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., Onnx runtime, 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.

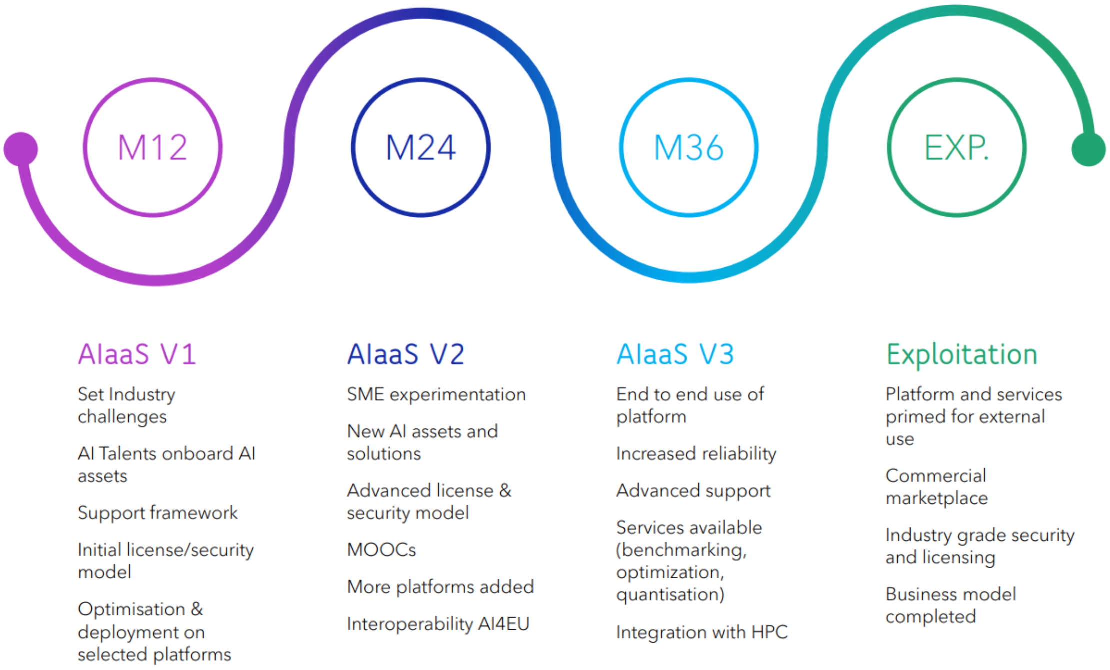
- **Model conversion and export:** Model conversion and export represent quite intensive engineering jobs that require hands-on experience with the tooling and inference engines for the targeted formats. If not automated, this task can drastically slow down the process of the model deployment.

- **Model repository: S**toring and tracking of the trained, pre-trained and exported models requires a systematic approach 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.

BonsAPPs Phases for Building a Sustained and Lasting AI Economy

The BonsAPPs project applies three phases within its runtime to build and sustain its objective of a sustained AI economy and which are depicted in Figure 22. These phases noted as AIaaS V1, AIaaS V2, and AIaaS V3.



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 22: High level roadmap

- **AIaaS v1 (month 12 – Supply Activation)**: 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

- **AIaaS v2 (month 24 – Demand Activation)**: 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 in M25 to M34.

- **AIaaS v3 (month 36 – Sustainability):** 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 of BonsAPPs.

5.2 Security and Interoperability Features in AIaaS V1 - Supply Activation

The aim of AIaaS V1 is to support the AI developers as they offer their AI Artifacts on the BMP. Hence, the Sec-aaS activities in AIaaS V1 focus on mainly 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. In addition, certain activities for establishing the interoperability of the BonsAPPs platform with the AI4EU platform and other ICT49 projects are planned, and which require a long lead-in time before they come effective, e.g., platform-wide and cross-platform user identities.

5.2.1 Security

The foreseen Sec-aaS activities in AIaaS V1 are:

1. *Frontend Security:*
   a. Secure developer access
   b. Implement a system-wide user management
   c. Connect to the system-wide identity management
   d. Increase security and attack prevention and signalizing system
   e. Enable system failure self-healing,
2. *System-wide Services for Security:*
   a. Implement a system-wide identity management
   b. Implement a system-wide certificate and key management
3. *A License Management tool:*
   a. Define an initial set of licenses and make is accessible and bindable to AI Artifacts
4. *A Secure Deployment tool:*
   a. Implement until October a PoC for the alignment of the KOP tool into the Bonseyes deployment chains
   b. 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
   c. 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)
5. *Secure Transfer, Storage and Marketplace Interoperability Tools:*
   a. Identify security requirements and security capabilities for centralized and persistent AI Artifact repositories
   b. Implement an integrate initial authorization policies for centralized AI Artifact
6. *Trusted Computing as a Service Tool:*
   a. Implement a first PoC for the integration of the KOP tool into the development chains

5.2.2 Interoperability and Activities

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, 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.

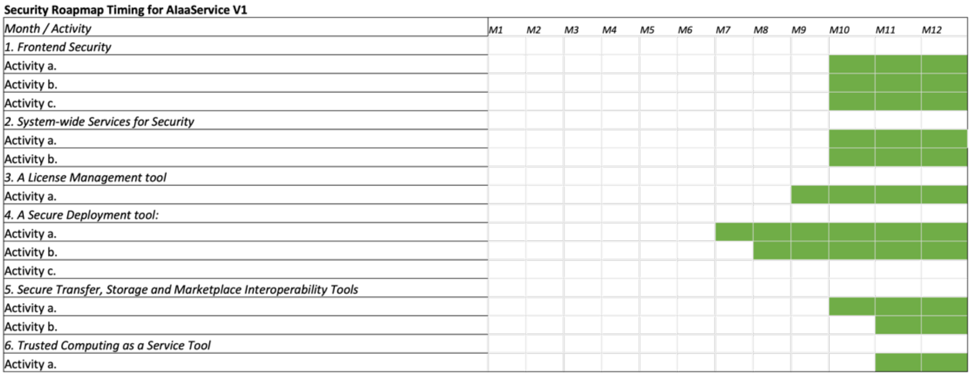
The BonsAPPs project intends to provide resources to implement interoperability with AI4EU. A particular focus will be on:

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

Also, 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.

5.2.3 Gantt Chart for Security Activities in AIaaS V1

The timing of the activities in the Security-as-a-Service activities in WP3 for AIaaS V1 are depicted in Figure 23. 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. Remark: some work for improving the security of the UI and frontend platform activities and for the interoperability are not carried out in WP3.



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 23: Gantt chart for the SaaS activities in AIaaS V1

5.3 Security Features for AIaaS V2 – Demand Activation

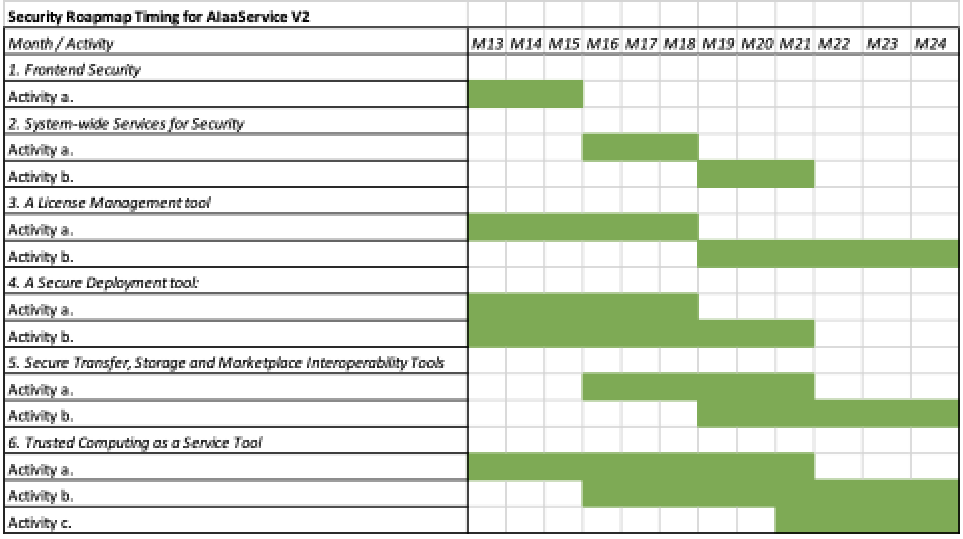
The aim of the AIaaS V2 is to support AI developers as they increase their interest sourcing and using AI Artifacts from the BMP. Hence, the Security-as-a-Service (SaaS) activities in AIasS V2 focus on the mechanisms for a trusted and secure engagement of developers with each other, securing their collaboration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

1. *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:*
    a. Implement a secure collaborative editor on the BMP frontend for specifying the licenses
    b. Implement a library of predefined licenses
- *A Secure Deployment tool:*
    a. 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 devices
    b. 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

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 24. 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 24: Gantt chart for the SaaS activities in AIaaS V2

5.4 Security Features in AIaaS V3 – Sustainability

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:*
    a. Demonstration and implementation of an interoperable identity management mechanism
    b. 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

3 *Secure Transfer, Storage and Marketplace Interoperability Tools:*

- o Identify the requirements and implement suitable interoperability mechanisms for the BonsAPPs frontend and the persistent AI Artifact repositories with selected other marketplaces and repositories

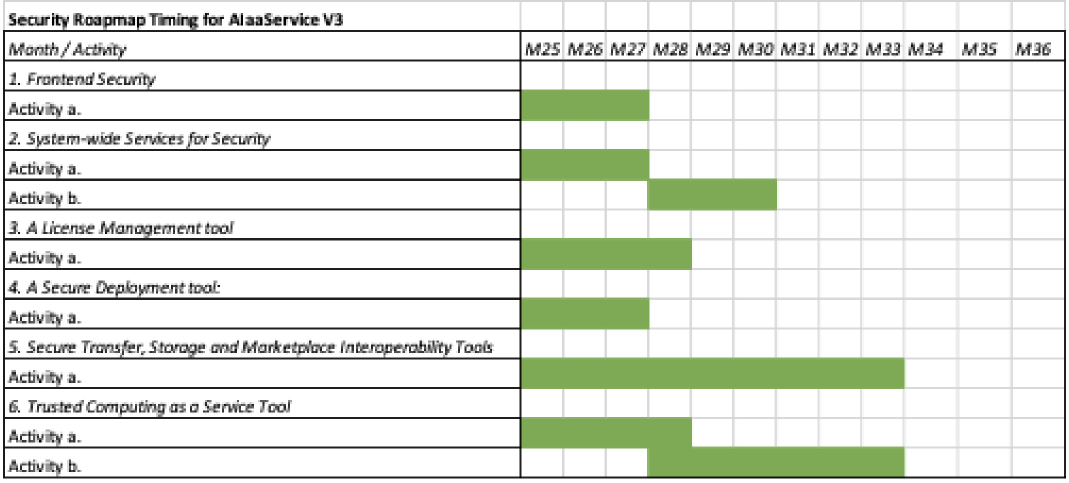
- ○ Investigate and, if necessary, implement common user authentication and authorization mechanisms with AI4EU marketplaces.

4 *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

Gantt Chart for Security Activities in AIaaS V3

The timing of the activities in the Security-as-a-Service activities in AIaaS V3 are depicted in Figure 25. However, since AIaaS V3 is the iteration, which is most far away in time, it is difficult to predict now 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 AIaaService 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 25: Gant chart for the SaaS activities in AIaaS V3

6 Security and Privacy Evaluation

To deal with an ever-evolving digital sphere that poses security and privacy challenges through variable dimensions, a dynamic platform like BonsAPPs needs a continuous security and data privacy (S&P) evaluation strategy. In addition, the required S&P levels might vary between the developers and implementers of edge AI solutions. Hence, a fluid as well as an adaptable S&P policy scheme should be in place, which could facilitate renewable policy-clauses to handle the latest vulnerabilities and threats including the ones that are yet to be encountered in the foreseeable future. Hereby, the focus is on embedding and including S&P levels in the economical acting of the marketplace participants (i.e., negotiating the S&P level with eventual impact on licensing and costs) and on how the S&P levels can be implemented in the development and deployment chains. In this section, we outline a first approach for BonsAPPs Sec-aaS layer to address, specify and implement adaptive S&P levels.

Figure 26 shows an overview of the iterative and interactive process to ensure the presence and operation of a versatile S&P policy throughout the development and deployment toolchains of the BonsAPPs platform.

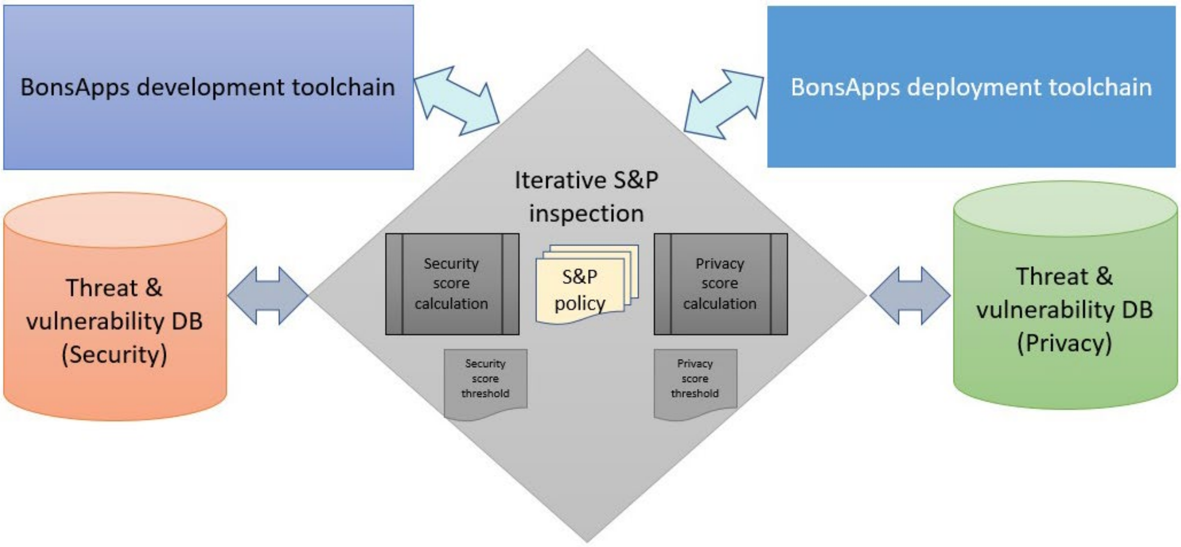

BonsApps development toolchain
BonsApps deployment toolchain
Iterative S&P inspection
Security score calculation
S&P policy
Privacy score calculation
Security score threshold
Privacy score threshold
Threat & vulnerability DB (Security)
Threat & vulnerability DB (Privacy)

Figure 26: An overview of the iterative and interactive process to ensure the presence and operation of a versatile S&P policy throughout the development and deployment toolchain of BonsAPPs platform.

6.1 Security risks evaluation

Initially, the entire platform will be subjected to a security risk evaluation. Later, the newer modules and artifacts will go through the process along with a system-wide re-evaluation due to interoperability. Table 2 depicts an empty instance of security evaluation matrix, which will populated over time.

Table 2: Security evaluation matrix (to be updated upon revelation of new risk factors).*

Risks	Effects on individuals	Main sources of risks	Main threats	Existing or planned measures	Severity	Likelihood
Illegitimate access						
Unwanted modification						
Loss of asset						
…						

An introduction of new module / artifact would trigger the security evaluation process by asking a series of questions:

1. Through what means could an adversary exploit the BonsAPPs platform and its AI Assets?
2. How could an adversary get one or a combination of components of the BonsAPPs platform to make a bad decision?
3. What critical aspects of the AI platform's decision-making process are susceptible to adversary exploitation?

Parallelly, a risk mitigation strategy will be formulated to map them according to the available techniques and solutions introduced by Kudelski's KOP. For instance:

i. Code encryption
ii. Data encryption
iii. Code obfuscation

6.2 Privacy risks evaluation

Initially, the entire platform will be subjected to a privacy risk evaluation. Later, the newer modules and artifacts will go through the process along with a system-wide re-evaluation due to interoperability. Furthermore, a privacy impact assessment, preferably CNIL's PIA methodology could be adopted to scrutinize the entire process and all the AI Artifacts.

An introduction of new module / artifact would trigger the privacy evaluation process by asking a series of questions:

1. Through what means could an adversary exploit the BonsAPPs platform and its assets?
2. How could an adversary get one or a combination of components of the BonsAPPs platform to make a bad decision?
3. What critical aspects of the AI platform's decision-making process are susceptible to adversary exploitation?

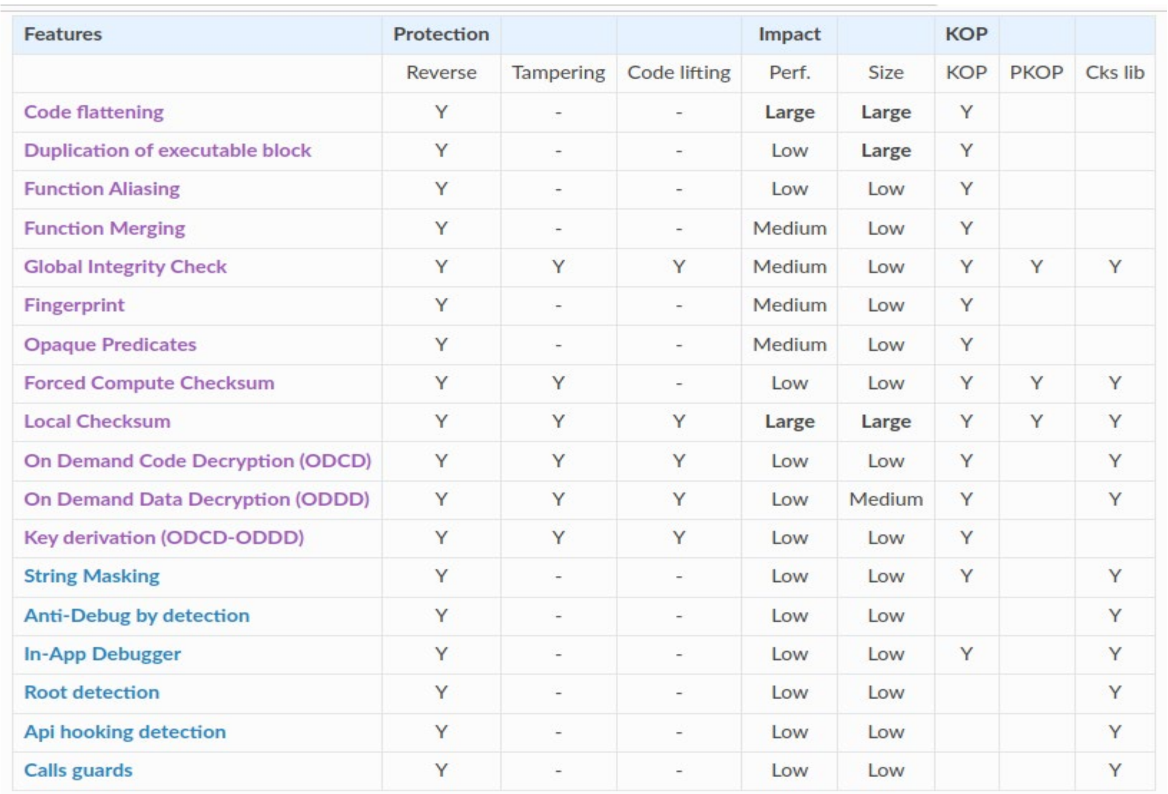
Parallelly, a risk mitigation strategy will be formulated to map them according to the available techniques and solutions introduced by the state-of-the-art research. For instance:

1. Federated learning
2. Differential privacy
3. Homomorphic encryption

6.3 Risk mitigation strategy

For each of the threats and its corresponding security / privacy issues should will be mapped in the design process by the work in WP3 directly (or partially) to the features list provided by Kudelski.

Table 3: List of features offered by Kudelski's KOP to address security issues.



Features	Protection			Impact		KOP		
	Reverse	Tampering	Code lifting	Perf.	Size	KOP	PKOP	Cks lib
Code flattening	Y	-	-	**Large**	**Large**	Y		
Duplication of executable block	Y	-	-	Low	**Large**	Y		
Function Aliasing	Y	-	-	Low	Low	Y		
Function Merging	Y	-	-	Medium	Low	Y		
Global Integrity Check	Y	Y	Y	Medium	Low	Y	Y	Y
Fingerprint	Y	-	-	Medium	Low	Y		
Opaque Predicates	Y	-	-	Medium	Low	Y		
Forced Compute Checksum	Y	Y	-	Low	Low	Y	Y	Y
Local Checksum	Y	Y	Y	**Large**	**Large**	Y	Y	Y
On Demand Code Decryption (ODCD)	Y	Y	Y	Low	Low	Y		Y
On Demand Data Decryption (ODDD)	Y	Y	Y	Low	Medium	Y		Y
Key derivation (ODCD-ODDD)	Y	Y	Y	Low	Low	Y		
String Masking	Y	-	-	Low	Low	Y		Y
Anti-Debug by detection	Y	-	-	Low	Low			Y
In-App Debugger	Y	-	-	Low	Low	Y		Y
Root detection	Y	-	-	Low	Low			Y
Api hooking detection	Y	-	-	Low	Low			Y
Calls guards	Y	-	-	Low	Low			Y

7 Summary and Outlook

The BonsAPPs security architecture aims at ***building robust and strong trust among the stakeholders in an AI economy for developing applications for the Edge and the Deep Edge.*** BonsAPPs calls this security architecture **Security-as-a-Service (Sec-aaS**) layer which is fully integrated in the overall BonsAPPs AI-as-a-Service concept [D1.1]. The mechanisms of the Sec-aaS layer need to ***address all major malicious or non-malicious violations of the economical rules*** of the Bonseyes AI Marketplace. Furthermore, they need to be on a ***sufficient high technical maturity and robustness level.***

Hence, the Sec-aaS layer and its security mechanisms comprise technologies to counter copyright infringements, support software licensing, or enable secure deployment of software on edge devices as well as system-wide security services like mechanisms for unique user identities, kinds of single-sign-one (SSO) mechanisms, and website and security.

This document fulfilled three tasks: a) it worked towards and provided a streamlined and concise description of the initial status of the BonsAPPs Sec-asS architecture and its security mechanisms, b) it described the new security concepts and mechanisms which are needed but weren't yet addressed in previous version of BMP o, e.g. Kudelski's KOP mechanisms or the concept to evaluate the security and, from this, deriving the security levels that can be specified in licenses (cf. Section 4 and Sections 6) , and c) it outlined a workplan to reach the expect high technical readiness level of TRL8 for the mechanisms.

In addition, the document provided an overview on the approach and current work on the interoperability of the BonsAPPs platform with the one of AI4EU and eventually other AI marketplaces and ICT49 platforms.

The initial major risk for the architecture and its employment is a concise implementation of basic security services. Advanced mechanism, such as the KOP mechanisms in the deployment and development chains are apparently easier to master since they can be addressed separately. A major difficulty and, in turn, thread to security, is expected in system-wide concepts services, such as user management or single-sign-on mechanisms since they involve multiple stakeholders in the engineering of the BonsAPPs platform and are crucial if attacked or bypassed. However, a solution is already considered by an improved project management highlighting and focusing on these issues and based on this technical document.

Bibliography

[Benz20] T. Benzel: "Cybersecurity research for the future." Communications of the ACM, Vol.: 64, No. 1, 2020.

[D1.1] Nicola Milojevic et al. (edt.): Technical Roadmap, BonsAPPs project deliverable D1.1, available at www.BonsAPPs.eu, July 2021

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

[keyST] Nagravision SA: "Kudelski keySTREAM™: 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.

[ORDL] 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

[Peis21] S. Peisert: "Trustworthy scientific computing.", Communications of the ACM, Vol.: 64, No. 5, 2021.

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

[Wired20] L. Hay Newman: "Google Moves to Secure the Cloud From Itself"; Wired, available at: https://www.wired.com/story/google-cloud-confidential-virtual-machines/ 2020-07-14.