**ITEA 3 Call 7**

**OMD**

**Optimal Management on Demand**

Project Number : ITEA-2021-20003

Project Start Date : 01.01.2022

Project Duration : 36 Months

**AI web services standards and market**

**References :**

Work Package : WP6

Task : T6.2 Standardization

Deliverable Document : D6.2 AI web services standards and market

Version : V0.0 Jun 7, 2023

Dissemination Level : Public

**Authors :** in alphabetical order

| **Company** | **Name Surname** | **E-mail** |
| --- | --- | --- |
| ARD Group | Bilge Başdemir  Esin Soycan  Özgün Sapmaztürk | bilge.basdemir@ardgrup.com.tr  esin.soycan@ardgrup.com.tr  ozgun.sapmazturk@ardgrup.com.tr |
| BEIA Gmbh | George Suciu | george@beia.ro |
| Caretronic d.o.o. | Simona Brezar | simona@caretronic.com |
| Dogus Technology | Utku Colak  Alper Gun | [utku.colak@d-teknoloji.com.tr](mailto:utku.colak@d-teknoloji.com.tr)  [alper.gun@d-teknoloji.com.tr](mailto:alper.gun@d-teknoloji.com.tr) |
| Experteam | Taner Ulusinan | [taner.ulusinan@experteam.com.tr](mailto:taner.ulusinan@experteam.com.tr) |
| FrontEndART Software | Tibor Bakota | tibor.bakota@frontendart.com |
| FTP - LDA | Germano Pinto | germano.pinto@ftpporto.com  isabel.ribeiro@ftpporto.com |
| ISEP | Goreti Marreiros | mgt@isep.ipp.pt |
| Strategy Big data | Alberto Oliva | alberto.olivia@strategybigdata.com |

Summary :

OMD is a software tool that helps service providers from various domains to use their resources effectively, to provide agile solutions, to conserve their knowledge base, to allocate each call unmistakably to the right expert / provider, and with the best solution of the particular problem at hand.

This document summarizes the effort on activities about the opportunities of defining and promoting a standard for OMD workflows for as many different use cases as possible. For all use cases we checked whether similar works are on the market, whether provided services are covered by any standards, and if not, what standards can be a starting point of defining a new one.

Table of Contents

[**1. Introduction 4**](#_wulr9to99zmw)

[**2. AI Web services 4**](#_v3ytgo641qs9)

[2.1. Tickota Use Case 4](#_c9zaiih3bqhy)

[2.1.1. API Usage (AIResult Web Service) 5](#_menvuhead11w)

[2.1.2. Service File Structure 6](#_nh35502utoh1)

[2.2. Equality in Justice Use Case 6](#_den5dmng28x5)

[2.3. SmartFix Use Case 7](#_iir5yhb7qker)

[2.4. Optimal Software Maintenance Task Assignment Use Case 7](#_eizgs4x3fxab)

[2.5. Healthcare Use Case 8](#_ze9epg2g5fcg)

[2.6. Recommend4U 9](#_ff9uurir2vrp)

[2.6.1. System Architecture 10](#_ljnnymlajx0s)

[2.6.2. System Interface 10](#_t0fmufmnazjp)

[2.6.3. API Gateway: Chatbot Service Recommendation Service 11](#_5rxt78of3v1b)

[2.6.4. Service Standards 12](#_nqn4c9yirg5a)

[**3. Applicable Standards 13**](#_v8qvxksvb4cg)

[3.1. ISO/IEC 27001 13](#_6y9cq66tn1vw)

[3.2. ISO/IEC 20000 14](#_suauiy99ylyf)

[3.3. ISO/IEC 42001 15](#_rbwhnxvvr59t)

[3.4. ISO/IEC 23894 15](#_nbu4cmle3q2g)

[3.5. ISO/IEC 24027 16](#_w4lorcm39zrw)

[3.6. ISO/IEC 24028 16](#_7hyxdbo55a6s)

[3.7. ISO/IEC 20546 16](#_yvrs6glv98pk)

[3.8. ITIL PRACTICES 17](#_oaf1mujgwv1n)

[3.9. GDPR 18](#_syi5ctx9vsmf)

# Introduction

The main objective of WP6 is to facilitate dissemination and exploitation activities. Task 6.2 is responsible for identifying those standards and best practices in the domain of AI-based web services that are applicable and in the long term (during the future exploitation of the results) should be applied in the different use cases.

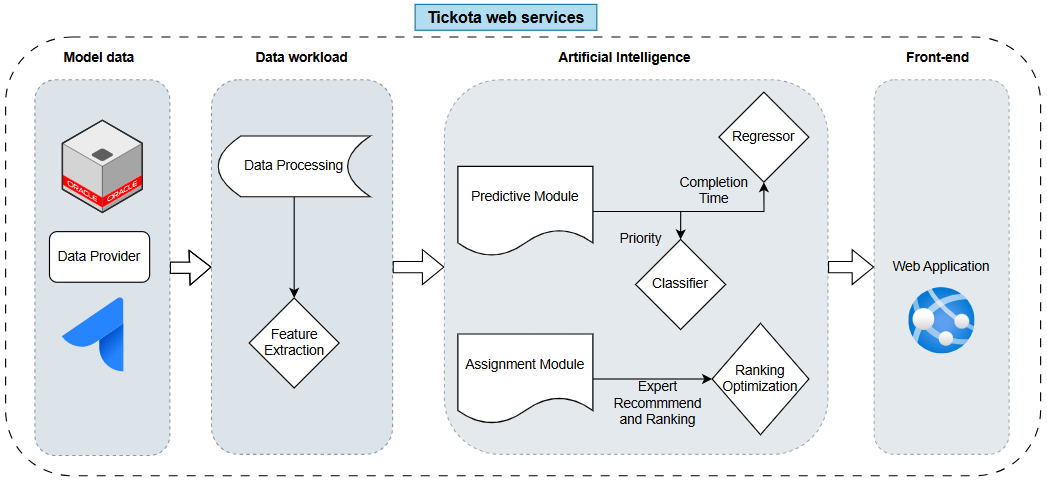
# AI Web services

## Tickota Use Case

Aim: to involve AI and machine learning to categorize and prioritize tickets. System analyzes the content, efficiently routing them to the appropriate experts. This ensures quality, minimizes response times and reduces the likelihood of SLA penalties.

Tickota is based on a three-stage approach:

1. Predicting the completion (resolution) time of a new Ticket coming into the system
2. Classification of the priority status of a Ticket that is new to the system
3. Routing the Ticket that is new to the system to the most appropriate solution team or expert



The data coming from the data provider goes through a data preprocessing process. In this way, data vectors that we can use in our algorithms are prepared. The attribute vectors requested by the models are processed in the relevant module and return prediction, classification and assignment/recommendation results.

We have designed a Regression algorithm to estimate the completion time. Regression algorithm is used to estimate numerical values.

Text classifier methods are used for our classifier algorithms.

The assignment recommendation module is designed with a SBERT based LLM. As a result of semantic analyses, it scores the ten most suitable experts for ticket resolution.

In the optimisation phase, another scoring is performed using the vectors describing the expert personnel from the assignment module. The optimal result is produced with methods such as Analytic Hierarchy Process and Promethee.

Our Ai web services are designed to connect the relational links of these modules, data pools and results with interfaces.

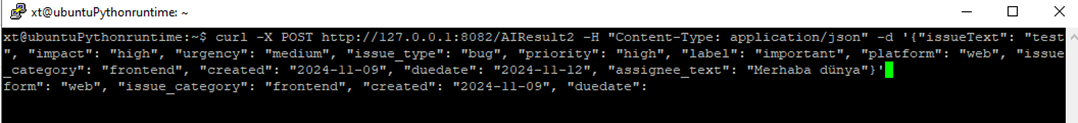
### API Usage (AIResult Web Service)

This page shows how to make predictions using the AIResult web service and classify different parameters. Below are examples and necessary instructions for using the service.

How to Use the Service

You can use a tool like Postman or `curl` to test the API. By sending a POST request, you can get predictions for various parameters.

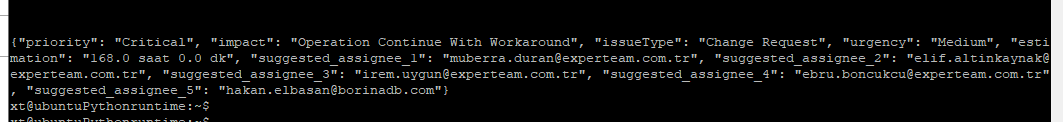
**Example Request**



**curl -X POST http://127.0.0.1:8082/AIResult2 \  
 -H "Content-Type: application/json" \  
 -d '{  
 "issueText": "test",  
 "impact": "high",  
 "urgency": "medium",  
 "issue\_type": "bug",  
 "priority": "high",  
 "label": "important",  
 "platform": "web",  
 "issue\_category": "frontend",  
 "created": "2024-11-09",  
 "duedate": "2024-11-12",  
 "assignee\_text": "Hello world"  
 }'**

This request is a POST request where all the required fields are provided, and predictions are obtained. The relevant parameters are inputted, and the service processes this information and returns a response.

**Example Response**



**{  
 "priority": "Critical",  
 "impact": "Operation Continue With Workaround",  
 "issueType": "Change Request",  
 "urgency": "Medium",  
 "estimation": "168.0 hours 0.0 mins",  
 "suggested\_assignee\_1": "**[**muberra.duran@experteam.com.tr**](mailto:muberra.duran@experteam.com.tr)**",  
 "suggested\_assignee\_2": "**[**elif.altinkaynak@experteam.com.tr**](mailto:elif.altinkaynak@experteam.com.tr)**",  
 "suggested\_assignee\_3": "**[**irem.uygun@experteam.com.tr**](mailto:irem.uygun@experteam.com.tr)**",  
 "suggested\_assignee\_4": "**[**ebru.boncukcu@experteam.com.tr**](mailto:ebru.boncukcu@experteam.com.tr)**",  
 "suggested\_assignee\_5": "**[**hakan.elbasan@borinadb.com**](mailto:hakan.elbasan@borinadb.com)**"  
}**

The response provides information based on the provided inputs, including priority, impact level, issue type, urgency, estimated resolution time, and suggested assignees.

### Service File Structure



## Equality in Justice Use Case

The **Equality in Justice** use case aims to help victims to find the most appropriate legal aid in their cases. It is mostly aimed for vulnerable groups and provides recommendations of the most competent, experienced, closest, and appropriate lawyers for their cases. By the nature of the data required both for training the AI recommendation model and for using the system, transparency, explainability, fairness, ethics, security and privacy are key factors. Thus, the **ISO/IEC 27001 standard on security and cybersecurity**, **ISO/IEC 24028 on AI trustworthiness**, and **ISO/IEC 24027 standard on biases in AI systems** are all important and “must” standards. Besides, as AI is involved in the system, **ISO/IEC 42001 on how to manage AI systems** and **ISO/IEC 23894 on how to perform risk management for AI-based systems** are also important standards for the development and maintenance phases, as well as **ITIL** practices.

## SmartFix Use Case

The **SmartFix** use case aims to provide a solution for the automatic categorization of customer tickets describing some issues in the consumer electronics domain, with the promise to use the technology in any aftersales customer reclamation management processes. This domain and solution do not particularly include the handling of sensitive data, but must be trustworthy and reliable. Trustworthiness of AI systems is concerned by the **ISO/IEC 24028 standard**, while **ISO/IEC 24027 on the biases of AI systems and their use** and **ISO/IEC 23894 on the general risk management of AI systems** applies, as, for example, over-reliance on the recommendations might result in some ill-handled issues which might undermine the positive results of the solution. As the domain of consumer electronics is huge, the recommendation system must work with big data, thus the **ISO/IEC 20546 standard on big data** also applies. Standards like **ISO/IEC 20000 on service management of general IT systems** or **ISO/IEC 42001 on service management of AI systems** and **ITIL practices** help to maintain these services in the long term.

## Optimal Software Maintenance Task Assignment Use Case

The **Optimal Software Maintenance Task Assignment** use case aims to provide a service for entities carrying out software development and maintenance tasks that helps these entities to better assign the tasks to the developers. The service is based on the following approach:

* The user provides data on its development project by providing access to different data sources like its source code management and issue management systems. As some companies have very strict IP protection and security rules, the credentials and identifiers of these accesses must be well protected.
* A background system (CODEE, used and extended in the OMD project, but otherwise is not a part of it) then processes the historical data of these data sources and stores and provides several measures and aggregated information on them. Due to the very strict IP protection and security rules of some companies, this is usually done in-house at the user’s side, which ensures that no raw data of the company is leaked out.
* The advisor that provides task assignment recommendations is set up on the project. This works from the data collected by the background system, and it first initiates the training of a project data specific OSMTA recommendation model. The advisor data can be provided on the CODEE user interfaces, or, to enable automation and better integration with the user’s systems, an API is also provided.
* When the project specific OSMTA model is ready, the user is able to ask for recommendations for the assignment of open issues in their issue management system. The model will provide three developers who are thought to be the best for the given task. The recommendations do not need to be specifically explainable, but must be reliable in order to achieve savings for the user by following them.
* The recommendation can be accessed in two ways. First, through the CODEE user interfaces among several other data that are provided by the CODEE system. Second, in order to enable the user to smoothly use and even somehow automatize the use of the recommendations, an API endpoint is provided where recommendations can be accessed in a structured form. The use of this API can then be integrated in the user’s systems which can lead even to the automatic assignment of the tasks. However, full automation is not recommended.

As can be seen, intellectual property protection is crucial in this use case. Thus standards like **ISO/IEC 27001 on security and cybersecurity** and **ISO/IEC 42001 on AI management systems** that also concerns data management and security in AI related systems apply to this use case. Another important field is the trustworthiness of the AI. The **ISO/IEC 24028 standard on the trustworthiness of AIs** applies as the exploitation of the results would be impossible without the user accepting the recommendations provided by the AI model. But there are also risks in using the system. Too much trust and unconditional automation and acceptance of the recommendations can also be harmful. Standards **ISO/IEC 23894 on risk management of using solutions** and **ISO/IEC 24027 on biases in AI and AI-based decisions** are very useful not only for us, the service providers, but also for the users of these systems.

## Healthcare Use Case

**AI web services standards and the market for healthcare** are essential for ensuring interoperability, security, and compliance, as well as for supporting innovation in AI-driven solutions like Speech2Service. Here’s a breakdown of the key standards, along with market trends and demands in healthcare AI:

* **Interoperability Standards**:
  + **FHIR (Fast Healthcare Interoperability Resources)**: FHIR is a widely adopted standard for exchanging healthcare information electronically. It provides APIs that enable the seamless sharing of healthcare data across different systems, crucial for AI applications needing real-time access to patient records.
  + **HL7 (Health Level Seven)**: HL7 standards govern data exchange between health systems, including data formats and standards for clinical information systems, which support the structured exchange necessary for training and integrating AI models.
  + **DICOM (Digital Imaging and Communications in Medicine)**: For AI applications that analyze medical imaging, DICOM ensures standardized image formats and metadata, supporting AI-based diagnostics and visualization tools.
* **Data Security and Privacy Standards**:
  + **HIPAA (Health Insurance Portability and Accountability Act)** in the United States and **GDPR (General Data Protection Regulation)** in Europe are critical standards. These regulations ensure that AI systems protect patient data, enforce encryption and access controls, and include data anonymization where necessary.
  + **ISO/IEC 27001**: This international standard focuses on data security management, including requirements for data protection, encryption, and secure storage, ensuring AI services maintain high security standards.
* **AI-Specific Standards**:
  + **ISO/IEC 20546**: Focused on big data, this standard helps guide the management and use of large datasets often required for training healthcare AI models.
  + **Ethics and Bias Management (ISO/IEC TR 24028)**: In healthcare, AI must be fair and unbiased. This standard addresses transparency, bias mitigation, and ethical considerations for AI applications.
  + **Explainability and Trustworthiness**: Standards like **ISO/IEC 22989** guide how AI models should be transparent and interpretable, ensuring that healthcare providers understand AI-driven recommendations.
* **Cloud and Web API Standards**:
  + **OAuth 2.0** and **OpenID Connect**: For secure authorization and authentication, especially crucial in healthcare environments where user data must be protected.
  + **RESTful APIs**: REST APIs are commonly used for accessing and integrating AI services, with healthcare-specific extensions like FHIR APIs facilitating connectivity to electronic health records (EHRs).
  + **gRPC (Google Remote Procedure Call)**: An efficient alternative to REST, often used in real-time AI applications that demand low latency.

The healthcare AI market is rapidly growing, driven by demand for solutions that enhance patient care, improve efficiency, and reduce costs. Key trends include a surge in AI-powered diagnostics, especially in image analysis (radiology, pathology) and real-time monitoring, with significant adoption as these models gain accuracy and trust. NLP in documentation is also rising, as solutions like Speech2Service help reduce clinician burnout and improve documentation efficiency, emphasizing real-time processing and EHR interoperability. Personalized medicine and predictive analytics, using patient data to predict outcomes and manage chronic conditions, require high data standards to analyze diverse data accurately. Telemedicine and virtual care, supported by AI services like real-time transcription and triage, align with the market’s shift toward remote care, accelerated by the pandemic. Investment from major tech firms and partnerships with healthcare providers further drive competition and innovation, with a focus on explainable, ethical AI for trusted clinical decisions. The healthcare AI market emphasizes interoperable, secure, and explainable solutions that improve patient outcomes, operational efficiency, and accessibility across clinical and remote environments.

## Recommend4U

Finding the perfect product to meet users' needs can be a challenging endeavor, especially when users possess limited or no knowledge about the product they require. Several factors contribute to this complexity. Firstly, the market is saturated with numerous alternatives that differ across various criteria such as price, brand, size, and performance. Secondly, users often lack clarity regarding which alternatives or products can best cater to their needs because they are unaware of the evaluation criteria. Lastly, users may find it challenging to identify the type of product that aligns with their requirements.

It is a common practice for individuals to seek guidance from store experts to make informed decisions about their product choices. During these interactions, experts aim to comprehend the user's needs, address their queries, offer recommendations, and ultimately assist them in identifying the most suitable product. These dialogues can assume various forms, including information-seeking, inquiry, and even persuasion when experts aim to promote a specific product.

The primary objective is to develop recommendation and search services and applications designed to present customers with the most appropriate products based on their search criteria and further refine search results through subsequent interactions. Users should have the capability to use voice commands to search for products and request recommendations, with the system acting as a knowledgeable store expert.

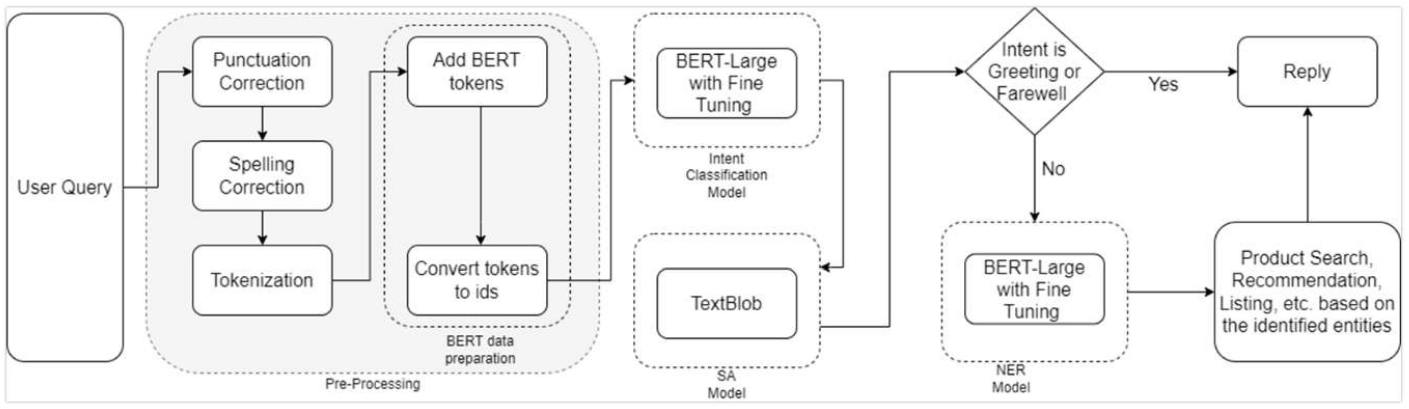
The challenge we are tackling in this use case is exceptionally intricate because we assume that user searches have a continuous nature. For example, a user might begin by searching for a "computer with a high-quality graphics card priced below 500€, and then, based on the initial results, adjust search criteria or add new ones. Consequently, the system must exhibit a degree of awareness regarding the evolving search process.

The anticipated outcomes include:

* Intelligent search services and applications leveraging Natural Language Processing to present products that align with customers' unique requirements.
* Recommendation services and applications powered by Machine Learning algorithms.
* An Intelligent Agent or Chatbot that serves as the customers' trusted store expert.
* The design and development of an e-commerce web platform.
* The integration of the developed AI models into the e-commerce web platform.
* The integration of the developed e-commerce web platform into the company's ERP system.

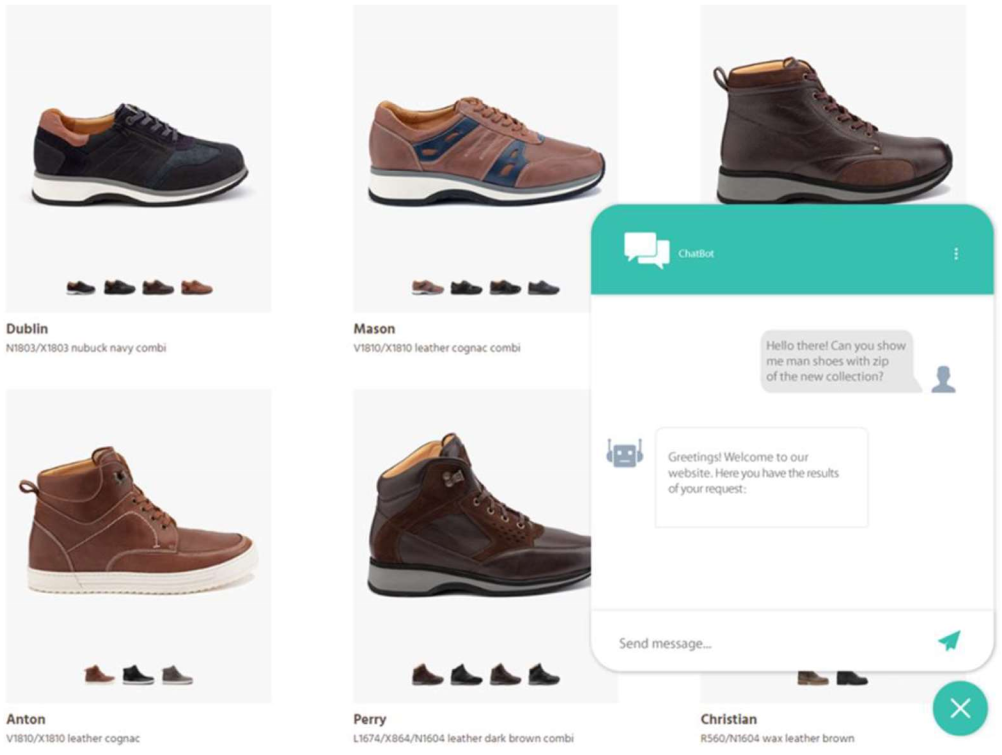
### System Architecture

Based on the evaluation of similar works given previously, we first decided to use the RASA platform to construct our chatbot. However, this tool only offers a free trial, and while you may use it for moderate traffic quantities, if those numbers rise, you must switch to a paid plan. A further aspect to consider is that spaCy, one of Rasa’s default pipelines for processing user inputs, consumes a significant amount of resources. We decided to build our architecture after acknowledging that there are more powerful state-of-the-art models than spaCy for using the same resources as Bert, which we verified with some preliminary testing in addition to the related works. An architecture was planned to develop this chatbot considering the needs of the footwear e-commerce platform which uses this chatbot. A user who is a final consumer (B2C) or another business (B2B) interacts with the platform where a chatbot is available to help with their needs. This chatbot can search, list, and recommend products based on user inputs. Fig 1. shows the proposed chatbot architecture and workflow. The user’s query, in addition to available information about previous purchases, available products, and user information in the footwear e-commerce database, is retrieved and provided to the chatbot. With this information, the chatbot uses intent classification and sentiment analysis to process the user query after this query is preprocessed. After the preprocessing is complete, based on the intent of the user, whether or not it is a greeting or farewell, a reply is sent back to the user through the footwear e-commerce platform. In the case of the intent being Change, See, or Remove. The query is sent to the Name Entity Recognition model, where entities are extracted. With these extracted entities, they are sent to the Hybrid Recommendation System to recommend products based on them. The chatbot then receives these recommendations and sends them to the user through the platform. This process is done utilizing Dialogue Roll-out, a method used to plan the dialogue between the chatbot and the user.



### System Interface

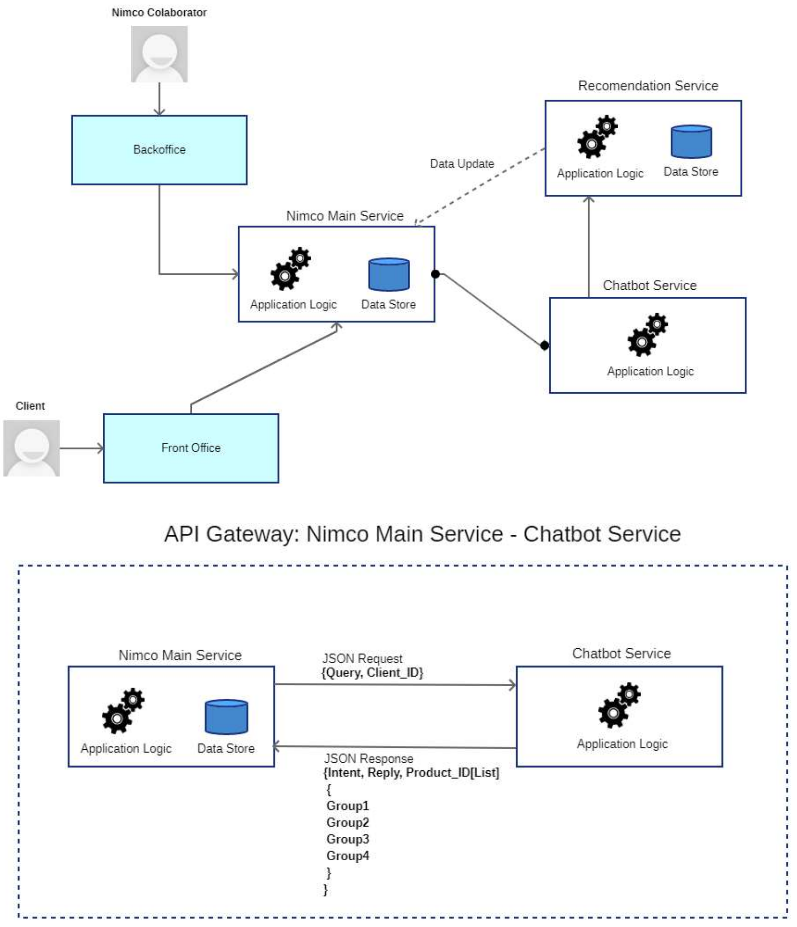
The Chatbot recommender system has been developed with an interface to retrieve search parameters and provide different recommendations of products according to these parameters.



### API Gateway: Chatbot Service Recommendation Service

The communication between the modules was maintained through a proxy-to-proxy layer, using a "service mesh" architecture pattern. This initialization process was triggered by user requests. The integration of the services enabled the enhancement of recommendation processes and direct pre-configurations of customizable materials, as the "service mesh" effectively managed communication between microservices that do not have direct user input. Additionally, the information from the generated operations was recorded in a database for result validation purposes.

We present the operating scheme of the "User Interface and Modules Integration Description."



### Service Standards

Within the framework of a 'mesh architecture' system, several key standards were carefully integrated during the development of the provided solution. These essential standards are detailed as follows:

* **Security**: The implementation of robust security measures, including encryption (mTLS), authentication, and authorization, is an integral part of service-to-service communication, sparing the need for ongoing security-related development.
* **Service Discovery**: The system dynamically locates and communicates with services without any hard-coded dependencies, reducing the need for ongoing development efforts.
* **Load Balancing**: Load balancing is an inherent feature of the architecture, ensuring even traffic distribution among service instances for enhanced reliability and performance, without requiring continuous development work.
* **Observability**: Monitoring, logging, and tracing capabilities are already in place, providing the necessary insights to diagnose issues and maintain service health, all without additional development effort.
* **Resilience**: Implement retries, timeouts, and circuit breakers to handle failures gracefully and prevent cascading failures.
* **Error Handling**: Robust mechanisms have been implemented to efficiently manage errors and maintain consistent reporting throughout the service mesh.

These standards can serve as a foundation for designing and implementing a robust service mesh architecture that meets the needs of your microservices-based applications.

# Applicable Standards

We went through the relevant standards and determined which standards we need to take into account. We list standards here that are applicable to more OMD use cases and not specific to a single domain.

## ISO/IEC 27001

**ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.** This international standard for an information security management system (ISMS), aims to protect the confidentiality, integrity, and availability of information by applying a risk management process. This standard is used by all of our companies, so we adhere to this one.

While ISO 27001 and demand management are distinct processes, they share common ground in the areas of risk management, continual improvement, asset management, and security management. Implementing both effectively within an organization can ensure that both information security and resource demand are managed. ISO 27001 standards can enhance the effectiveness of demand management processes in organizations where information security is critical.

Overlaps with OMD

Context of the organization: understanding the business environment and stakeholders needs can help aligning IT service demand with business capabilities and security requirements.

* **Leadership:** ensures that demand management policies align with information security objectives, ensuring secure provision of services.
* **Planning**: In “risk management”; identifying risks related to fluctuations in demand and their impact on information security. In “opportunities”; planning to leverage opportunities that enhance demand management while maintaining security.
* **Support**: In “Resources and competence”; ensuring enough skilled resources are available to meet demand securely. In “Communication”; regular communication regarding demand forecasts and potential security implications.
* **Operation**: Implementing controls to manage demand changes securely. Ensuring operational resilience to fluctuations in demand.
* **Performance** **Evaluation**: In “continuous improvement”; regular evaluation of how well demand is managed in terms of security. In “risk and performance metrics”; monitoring demand against key security performance indicators.
* **Improvement**: Learning from demand-related security incidents to improve processes. Implementing feedback loops to continuously adapt demand management practices to security needs.
* **Asset** **management**: Making sure demand for IT services aligns with asset availability and protection measures, thus managing asset utilization securely.
* **Operations** **security**: Overlaps are in change management, capacity management, incident management.

## ISO/IEC 20000

**ISO/IEC 20000: Information Technology — Service Management.** This is an international standard (a family of standards, it has several parts) for IT Service Management (ITSM) that defines the requirements for establishing, implementing, maintaining, and continually improving a service management system (SMS). It is an important standard to the OMD project because of the following reasons:

* **Service Quality Improvement:** OMD aims to optimize demand management across various domains such as justice, healthcare, and software support. ISO/IEC 20000 ensures that all service management processes are well-defined, consistently executed, and continuously improved, which is crucial for achieving high service quality and meeting customer expectations across these sectors.
* **Risk and Incident Management:** In the OMD project, especially in domains like healthcare and justice, the ability to manage risks and respond to incidents efficiently is critical. ISO/IEC 20000 provides a framework for incident management, helping to minimize the impact of incidents on the business, thereby ensuring continuity of service.
* **Alignment with Business Objectives:** For domains like telemarketing and e-commerce, where customer satisfaction and service reliability are key, ISO/IEC 20000 helps align IT services with business needs, ensuring that the technology effectively supports business processes.
* **SLA Management:** In software support (Tickota) and software development (OSMTA), Service Level Agreements (SLAs) are important. ISO/IEC 20000 helps in managing and monitoring SLAs, ensuring that service performance meets the agreed standards, and reducing the risk of SLA breaches.

By aligning the OMD project with the requirements of ISO/IEC 20000, the project can ensure that its IT systems are robust, reliable, and capable of delivering high-quality services across all its use cases. This alignment improves operational efficiency and service quality but.

## ISO/IEC 42001

**ISO/IEC 42001:2023: Information technology — Artificial intelligence — Management system.** This standard provides a systematic approach to managing AI systems. It ensures that AI systems are developed, deployed, and maintained in a way that is ethical, transparent, and reliable. This standard is aligned with the OMD project, as follows:

* **AI Ethics and Compliance:** OMD use cases, such as the justice sector (EqualityInJustice) and healthcare, involve sensitive data and decision-making processes. ISO/IEC 42001 ensures that AI systems are developed with a focus on ethics, fairness, and legal compliance, which is essential in these domains to avoid biases and ensure trustworthiness.
* **AI System Performance:** In use cases like SmartFix (consumer electronics) and Recommend4You (e-commerce), the performance of AI models is critical to delivering accurate and timely results. ISO/IEC 42001 emphasizes the need for continuous monitoring and optimization of AI systems, ensuring that they perform as intended and adapt to changing conditions.
* **Data Management and Security:** For AI-based use cases in OMD, such as telemarketing (Omniticket) and software development, effective data management is crucial. ISO/IEC 42001 provides guidelines for handling data securely and ensuring that AI models are trained on high-quality data, thereby improving the reliability and security of the outcomes.
* **Risk Management in AI Systems:** The standard provides a framework for identifying and mitigating risks associated with AI systems, which is particularly important in domains like healthcare and justice, where decisions made by AI systems can have significant consequences.

By aligning the OMD project with the requirements of ISO/IEC 42001, the project can ensure that its IT and AI systems are robust, reliable, and capable of delivering high-quality services across all its use cases. This alignment also ensures that the AI-driven solutions developed within OMD are ethically sound and legally compliant.

## ISO/IEC 23894

**ISO/IEC 23894:2023: Information technology — Artificial intelligence — Guidance on risk management.** This standard provides guidance on how the risks associated with the use of AI solutions should be handled. As OMD builds on AI technologies, this standard applies to it. However, it is more important for some specific use cases of the project.

* **Risk of Wrong/Biased Training Data:** If the underlying AI model is trained on wrong data, the recommendations will also be wrong. In all use cases of the project this risk has to be understood and mitigated by the owner or provider of the service. However, in use cases where the customer/user of the service also provides sensitive data (e.g. Healthcare, Optimal Software Maintenance Task Assignment), the customer/user has to be also aware of the risk.
* **Risk of Unconditional Trust in the Recommendations:** The recommendations provided by the AI solutions must be evaluated by humans. It is always a risk that this evaluation gets more and more lightweight over time, and customers blindly trust in the system. For some use cases the inadequate filtering and unconditional acceptance of the recommendation may only cause inconvenience and loss of confidence in the system, or even cost money. However in some cases (e.g. Equality in Justice, Healthcare) it might have more serious consequences.

Thus, this standard should be applied by the service providers of the use cases, and for some of them, actions should also be taken to inform their customers about the risks of using the service.

## ISO/IEC 24027

**ISO/IEC 24027:2021: Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making.** This standard is strongly related to the previous one that concerns general risk management in AI related systems, but it focuses on the use, more precisely the potential misuse of these systems. As the use cases and the developed solutions will help the customers to make their decision, it is very important both for them and the service providers to be aware of the possible biases in both such systems and in the ways how they are used. This could help them to set up adequate processes and risk management.

## ISO/IEC 24028

**ISO/IEC 24028:2020: Information technology — Artificial intelligence (AI) — Overview of trustworthiness in artificial intelligence.** This standard is also strongly related to the various nonfunctional characteristics of the AIs. It proposes approaches to establish trust through transparency, explainability and controllability. It also lists typical threats and risks of AI-based systems, and proposes different methods to mitigate these risks, and will help, by proposing different approaches, to assess and establish (among others) the safety, security and privacy. Trustworthiness is very crucial for the effective exploitation of the OMD results.

## ISO/IEC 20546

**ISO/IEC 20546:2019: Information technology — Big data — Overview and vocabulary.** This document provides a terminological foundation for big data-related activities by defining a set of terms of the domain, and also provides a conceptual overview of the field, its relationship to other technical areas. As most of the OMD use cases will work with big data, this standard is important for them.

## ITIL PRACTICES

By integrating ITIL practices with demand management, organizations can more effectively align their IT services with business needs, ensuring that resources are used efficiently and that customer expectations are consistently met.

DT has developed an action plan considering ITIL framework practices for managing and ensuring access to IT support services for potential customers. Within the ITIL framework, they implement the following practices:

* **Service Desk and Request Management**: In coordination with the company's user support desk, we will manage and route requests through a single point of contact using the supported communication channels (request portal, email, WhatsApp, and phone).
* **Information Security and Incident Management**: The company’s information security team will provide support for services such as access security, the use of Data Loss Prevention (DLP) to monitor if transmitted data contains sensitive information, virtual network management, and incident monitoring and visualization.
* **Change Management**: The Azure DevOps infrastructure is utilized for the planning, evaluation, approval, implementation, and review of changes.

There are several other ITIL practices related to demand management that complement these:

* **Capacity and Performance Management**: By understanding current usage patterns and forecasting future demands, this practice helps ensure that sufficient capacity is available to meet demand without overprovisioning resources.
* **Service Level Management**: Demand management often works hand-in-hand with service level management to ensure that services are provided at the right levels, meeting agreed-upon SLAs even as demand fluctuates.
* **Financial Management for IT Services:** Understanding the financial implications of demand fluctuations is critical. This practice helps in making informed decisions about resource allocation based on cost and demand projections.
* **Service Catalog Management**: The service catalog provides transparency on what services are available, helping customers understand their options and thereby influencing demand.
* **Supplier Management**: Managing demand often involves coordinating with external suppliers, especially when services are outsourced or when third-party products are a critical part of the service delivery.
* **Business Relationship Management**: By understanding the business’s needs and strategic objectives, this practice helps in aligning demand with available services, ensuring that IT services are relevant and responsive to business needs.
* **Availability Management**: Ensuring that services are available to meet demand is a key part of maintaining customer satisfaction and meeting SLAs.
* **Service Continuity Management**: Service continuity management supports demand management by ensuring that services can continue to meet demand even during disruptions.

## GDPR

**GDPR - General Data Protection Regulation** is an EU regulation concerning the protection of personal data of natural persons. This regulation applies to all systems and services within the EU market. All services that require or process sensitive personal data (e.g. medical data, legal data) must adhere to this regulation.