Macedonian Interoperability Building Block: **IOP-T**

(Technical Interoperability)

Johann Höchtl, Bernd Zwattendorfer, Peter Reichstädter, Igor Crvenov, Filip Manevski, Nadica Josifovski

Delivery: 15.05.2015
Version: V1.0 FINAL

This project is funded by the European Union

TABLE OF CONTENTS

This project is funded by the European Union

This project is funded by the European Union


1 Executive Summary

This document deals with the aspects of technical interoperability in the Macedonian Government.

Interoperability is the ability of heterogeneous systems to exchange information in a meaningful way. In this regard meaningfulness means that two parties participating in electronic data exchange have a mutual understanding on technical requirements, the semantics of data and services, and the organisational procedures involved. In order for these three levels of interoperability to seamlessly work together, a set of governing principles is required, partly expressed by legal regulations as well as applied good practice.
Generally, successful interoperability frameworks are characterized by having those minimum interoperability elements in place which are required that parties can exchange data and information without exposing the inner workings of procedures or details about technical infrastructure. Additionally non-functional requirements have to be met, like services are allowed to be called only after successful authorization or exchanged messages to be encrypted.
The Macedonian Government is facing increasing pressure for collaboration, e.g. new services have to be provided with decreasing budgets. Technically this can be fulfilled by more efficient organisation of work, enabled by technology. However, employing technology in government is more but paper-based work carried out electronically. Embracing the possibilities enabled by technology will result in more efficient organisational patterns which may be disruptive to existing arcane procedures, requiring novel interaction patterns and new ways of thinking about openness and transparency.

Data and information are a valuable good. Citizens, the economy, and external stakeholders such as the EU are demanding services where data is being exchanged between government institutions instead of persons being forced to repeatedly present their documents in front of officials. Additionally, emerging trends like open data or improved decisions enabled by big data analytics require a wealth of data typically not available within a single ministry. Thus, the ability to exchange data and information in a frictionless, usable and secure way is in the spotlight of government considerations worldwide as well as in Macedonia.

The exchange of data and information is enabled by using different technologies and connection patterns, such as E-Mail, end-to-end connecting two parties, or by using a mediating intermediary infrastructure layer. In recent years, interaction patterns have emerged, which favours the concept of a centralized message broker, exposing a set of administrative services, providing core characteristics like authenticity and encryption. Such a system requires higher level services like identity management.

Technology is and ever was moving at a fast pace. The challenge thus is to define standards and draft agreements that are both specific enough to be technically implementable and in the same time generic enough to cause only reasonable efforts required by adapting to technological advancement. This document focuses on architectural design patterns of an IOP system enabling the interoperable interconnection of Macedonian government bodies while keeping future requirements like the connection with economic stakeholders and the European Community on the radar.

This project is funded by the European Union

2 Interoperability Assessment

Within the LAW ON ELECTRONIC MANAGEMENT (Official Gazette of RM, no. 105, 21.08.2009) Macedonia has, amongst others, laid down the foundations for electronic data exchange between entities. Herein a term, the "Unique Environment", is coined, which, according to the definition of Art. 3, *is a managed environment for standardized document and data exchange between organs*. Throughout the remainder of this document, whenever IOP system is mentioned, it is synonymous to "Unique Environment", which means *the ability of information systems to process, exchange and store documents and data by electronic means, using unique technological standards and processes*.

Each authority that needs to exchange electronic information is obliged to register in the unique environment. In those cases where an authority wants to provide a service, it is obliged to use a communication client (CC) defined in the "Guidelines on the technical requirements, manner of operation and functioning of the communication client and recommendations for use of the interoperability system" as *a hardware device with an adequate software which shall provide the interface for electronic documents and data exchange, whereby the documents and data are exchanged among information systems of authorities taking part in the exchange process*.

If an authority doesn't provide services, it still can participate in electronic data exchange by means of a web portal, which facilitates access to services other authorities have granted access to. Every system which participates on electronic data exchange is required to be certified, as laid out in Art. 36 of the aforementioned law. Certification therein is described as *a confirmation of the fulfilment of the terms of functioning of information systems*.

The Unique Environment (i.e. the IOP system) has a role of a bus for information transfer. The bus enabling the transfer is called Macedonian Information Bus - MIB. From a technical perspective, the protocol used for information transfer through the bus is called MIB protocol. This is somewhat unfortunate, as it causes confusion whether MIB refers to the technical appliance or the implementation of the software stack enabling interoperability. This document thus introduces the term MKIL (Macedonian interoperability layer) to unambiguously refer to the metaservices, enabling interoperability. Authorities participating on the MIB are required to establish security mechanisms by means of user authentication and an access control mechanisms.

For providing security and integrity of the information, according to the Guidelines on the technical requirements, manner of operation and functioning of the communication client, as well as recommendations on the usage of the interoperability system, the following shall be used:

- HTTPS protocol;
- authentication, authorization;
- connection in domain structure;
- use of digital signatures;
- encryption of the messages being exchanged;
- physical protection of the space; as well as
- other measures in accordance with the generally accepted recommendations and security standards, ISO 27000 for security and W3C standards.

This project is funded by the European Union

According to the Rulebook on the manner of recognizing the unique environment and electronic communication between authorities via the unique environment for electronic documents and data exchange, the "Unique Environment" is required to keep logs about the following information:

- a unique document identifier;
- a unique identifier of the user-sender;
- a unique identifier of the user-receiver;
- time of receipt of the data and the document on the communication server;
- basis of the request;
- manner of sending the data and the document;
- a unique transfer identifier.

Currently, if a service user wants to provide a service, he is required to do so using a communication client, which transparently provides transport layer security and provides a unified interface towards the MIB.

The communication client (C-client) is required to pose these technical features:

- C-client shall be able to communicate through web services with the institution's information system and the communication server of the interoperability system
- Whenever a web service has been invoked according to certain parameters, apart from the relevant parameters, the web service must also contain the parameters upon which it has been invoked.
- Each service provided by the authorities within the interoperability system shall be accompanied by the following service characteristics:
    - Service response time (minimum, maximum, average);
    - - Error rate;
    - - Flow (measured in bytes, representing the quantity of information which the virtual users receive from the server per second);
    - - Requests per second (how many requests per second can the service respond to);
    - - Simultaneous users

Concerning communication using web services, the following technical standards have to be met:

- SOAP 1.1: basic, widely used standard for message exchange through different transport protocols, including HTTP;
- SOAP 1.2: an improved version of the basic standard
- WS-Addressing, WS-ReliableMessaging, WS-TransmissionControl, and WS-EndpointResolution for reliable and improved SOAP message exchange.
- For purposes of performing a secured message exchange TSL 1.2 shall be used.

In those cases where a service consumer doesn't want to or is technically incapable of consuming services through the communication client, the authority may consume services using a dedicated web portal. In this case, the consuming authority is required to implement organizational and physical security measures that would guarantee the safe handling of information acquired through the MIB portal, and they need to appoint a user manager (institution administrator) responsible for setting up the user rights for the MIB portal.


Both parties will have to sign a mutual agreement which, among others, regulates the granted rights and service usage requirements as well as service level agreements.

Concerning auditing and clearance, each authority should be obliged to keep encrypted logs of entries of data and documents being exchanged with other authorities centrally or decentrally.

According to the current operator, the MIB-system exposes the following shortcomings:

- The current MIB implementation has been implemented with the requirements of the participating institutions in mind and is not easily adaptable to further parties.
- The metaservices enabling the functionality of an IOP system are tailored towards this particular implementation, poorly documented and challenging to extend. In particular this means that the functionality of Enterprise Application Integration (EAI) cannot be fulfilled.
- The current IOP architecture implements a point-to-point architecture, which misses the point of central administration and leaves ample space for solutions circumventing the IOP system altogether, further diminishing the goals of centralized message dispatching.
- The source code of the current implementation is not available
- The current implementation results in vendor lock-in.

Addressing these shortcomings resulted in two tenders, which both pursue the goal to implement an improved IOP system. The following sections describe the identified differences between these two tenders in more details and based on document analysis, interviews with tender issuing authorities, and European good practice on technical interoperability recommendations are drafted.


This project is funded by the European Union

3 Problem Description

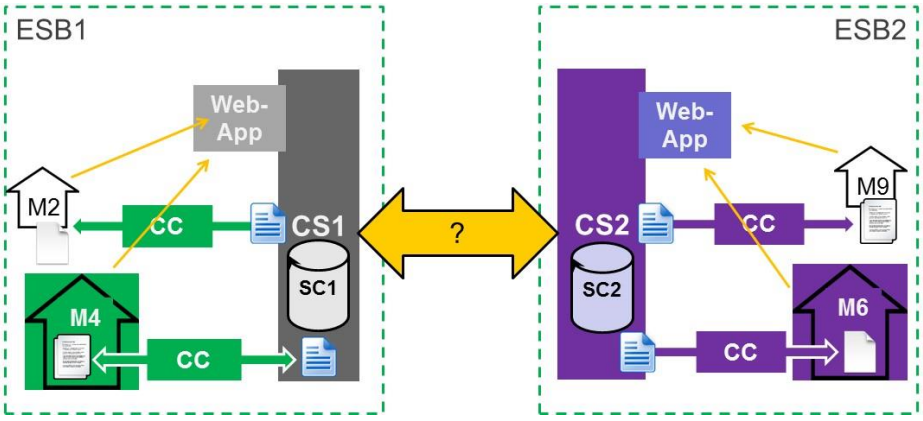
The Macedonian Administration commissioned two tenders implementing an information system to connect ministries, cities and entities charged to fulfil core administrative activities. The two tenders describe a common, largely overlapping set of requirements, for example, Service Orientation, using Web Services over SOAP, Authenticity of messages, and Encryption of messages.

While the transport layer (WS-*) and routing layer are well defined and overlap between these two tenders, the crucial metaservice protocol layer, henceforth abbreviated MIM, is undefined. The national tender even declares *"The standard and form of the structure of these web-services shall be defined in a separate document"*. However, having a standardized set of metaservices is an essential requirement for the functioning of an IOP system.

Furthermore, having two (or in the future even more) IOP systems requires to identify services, which should be provided at a higher level (i.e. outside the tenders scope), as otherwise interoperability (IOP) would be compromised. The challenging task is twofold:

1. To draft an architecture which fulfils the requirements of both tenders while
2. requiring minimum changes to these tenders in order not to delay their implementation.

The following figure tries to illustrate the problem description. On the one hand, different IOP systems should be interoperable to exchange messages and retrieve services also across IOP domains. On the other hand, the format and protocol of exchanged messages should be unified.



This project is funded by the European Union

4 Methodology

The STEs addressed that challenge by analysing the existing tenders, having meetings with the implementation teams of the tenders, and exchanging questions and answers with the partners. The following Figure 1 illustrates the underlying methodology extracting requirements for arguing subsequent recommendations.

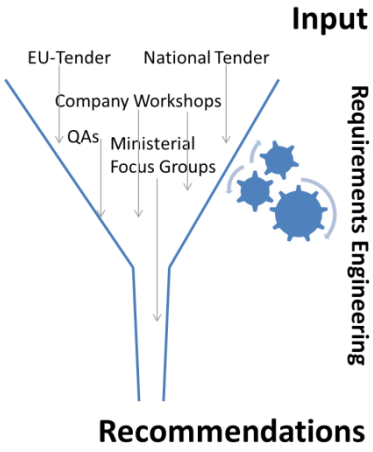


Figure 1- Methodology

The obtained input was and will be analyzed to formulate recommendations addressing the companies implementing the tenders as well as a generic output of the IOP-T document.

In more detail, the following process steps for deriving recommendations were followed:

1. *Information Gathering*
   In the information gathering phase the two available tenders (EU and national tender on information system implementation) were deeply analyzed. In addition, the contractors of the tenders were interviewed during workshop meetings to get a better understanding on the intended implementation of both IOP systems. In this phase, mainly information was gathered.
2. *Requirements engineering*
   Based on the information retrieved in the first phase, the two individual tenders were compared to find out synergies and differences, respectively. For both tenders a common set of requirements could be identified. In addition, synergies and differences could be found on how those two tenders are going to fulfill the identified requirements.
3. *Identify requirements important for IOP-T*
   Not all of the common identified requirements are important to achieve interoperability on technical level. Some of the identified requirements even relate more to organizational aspects. Hence, the list of common requirements was filtered which resulted in a list of requirements that are important for both IOP systems to achieve technical interoperability.
4. *Evaluate possible options*
   To fulfill the selected requirements, different options may exist. In a first step, different options for meeting individual requirements were identified. In a second step, the different options for fulfilling a particular requirement were thoroughly discussed and evaluated.
5. *Give recommendations*

This project is funded by the European Union

Based on the evaluation results recommendations were derived. The recommendations target the most important aspects/requirements for achieving interoperability on technical level,

This project is funded by the European Union

5 IOP System Requirements Elicitation

5.1 Common Requirements

According to the proposed methodology, the aim was to compare the two different enterprise service bus proposals and to extract synergies and differences. Based on this comparison, common requirements can be defined which need to be fulfilled by both IOP systems. The identification of common requirements build the basis for setting up an interoperability layer, as it is essential to meet these common requirements by both information system implementations (or even further implementations) and to achieve interoperability on technical level.
Based on the comparison between the two information system proposals, the following 13 common requirements could be identified:

- Deployment/operational requirements
- Implementation Requirements
- Architectural Requirements
- Requirements for service management
- Requirements for message transport
- Requirements for error handling
- Requirements for logging/record-keeping/auditing
- Requirements for security
- Requirements for payment
- Requirements for user/web interface
- Requirements for user/identity management
- Requirements for Licenses
- Requirements for maintenance/support

These requirements are further described in detail and tables illustrate the differences and synergies between the two IOP solutions. In other words, these tables describe how the common requirements are met by each individual IOP solution or how they will be met, respectively. Differences and synergies have been extracted out of the two tenders for IOP systems in Macedonia.

5.2 Deployment and Operational Requirements

This section describes the requirements that an IOP system should fulfil regarding deployment and operation of IOP systems. This requirement mainly affects the central server component (communication server), as high load can be expected on this central routing instance. Deployment or operation requirements are, for instance, hardware and server software selection, measures ensuring high availability (e.g. clustering or load balancing), or quality of service control (QoS).

5.2.1 Comparison between IOP SYSTEM 1 and IOP SYSTEM 2

The following Table 1 - IOP system 1 vs. IOP system 2: Deployment illustrates requirements regarding the operation and deployment extracted out of both IOP System tenders and how they should be fulfilled.

This project is funded by the European Union

Table 1 - IOP system 1 vs. IOP system 2: Deployment and Operational Requirements

IOP system 1 (EU)	IOP system 2 (MK)
• Active/Passive clustering configuration on two virtual servers. • Shall control quality of service (QoS). • High availability • Adequate performance • Concrete hardware for RDBMS	• two nodes, active/passive cluster (virtual environment) • limiting the use of network connection QoS • High availability (99,7%) • High performance • Automatic Load balancing • BizTalk Server 2009 (64-bit Microsoft Windows server) • Microsoft SQL Server 2008 is used for data storage

Discussion

Both tenders require the setup of powerful hardware to cope with possible high loads. Within the national tender explicit hardware requirements are listed. However, both implementations should be highly available, ready for clustering, and support load balancing. The national tender does not dictate the use of Microsoft BizTalk Server and Microsoft SQL Server, however, the implementing company intends to do so. In the EU tender the use of software components is more open (e.g. the use of database servers).

5.3 Implementation Requirements

This section describes the requirements for implementing an IOP system or its components (communication client, communication server), respectively. These requirements are related to the use of software products and the programming language for implementing components.

5.3.1 Comparison between IOP system 1 and IOP system 2

The following Table 2 illustrates requirements regarding the implementation extracted out of both IOP system tenders and how they should be fulfilled.

Table 2 - IOP system 1 vs. IOP system 2: Implementation Requirements

IOP system 1 (EU)	IOP system 2 (MK)
• .NET Framework technology and uses Microsoft Visual Studio with the program language C# • Commercial-Off-The-Shelves (COTS) software application • Detailed message processing • Symantec based automatic backup • High availability based on COTS (Vertitas) based replication	• .NET Framework technology and uses Microsoft Visual Studio with the program language C# • Integration of new tools and products, regardless of the platform for their development • Automatic back-ups (detailed Backup Copy Strategy) • shall contain DNS service • deliver the software source code

This project is funded by the European Union

5.3.2 Discussion

The EU tender is more open on the use of software implementations but requires the take up of Commercial-Off-The-Shelves (COTS) software. In contrast, the national tender explicitly requires .NET Framework and C# as programming language. New tools and workflows should be easily integrate able in both tenders, whereas the EU tender is more concrete on using UML.

5.4 Architectural Requirements for IOP system server

This section describes the requirements for the software architecture of an IOP system. The requirement affects the overall IOP system architecture but also the central software component for internal architectural design decisions. For instance, this requirement details whether the IOP system architecture should be centralized or loosely coupled or if the internal component architecture should be open and modular or closed.

5.4.1 Comparison between IOP system 1 and IOP system 2

The following Table 3 illustrates requirements regarding the IOP system and internal component architecture extracted out of both IOP system tenders and how they should be fulfilled.

Table 3 - IOP system 1 vs. IOP system 2: Architectural Requirements

IOP system 1 (EU)	IOP system 2 (MK)
• Single, secure point of access • SOA-based • Modular • Enterprise (Government) Application integration • Easy maintainability	• Central communications server acts solely as a mediator for exchange of the messages among the communication clients, but must not have insight into the content of the messages. • SOA architecture • Modular and open architecture • Easy changes without affecting the rest of the modules and solution functionalities

5.4.2 Discussion

Both IOP systems should rely on a centralized architecture, having a central communication server acting as mediator for various communication clients. The overall architecture should be SOA-based. The internal architecture of the components should be – according both tenders – modular and open, thus that new applications or components can be easily integrated and changes do not affect the rest of the solution.

5.5 Requirements for service management

This section describes the requirements for service management of an IOP system implementation. These requirements consider the registration, the discovery, and composition of services in an IOP system infrastructure.

5.5.1 Comparison between IOP system 1 and IOP system 2

5.5.1.1 Service registration

The following Table 4 illustrates requirements regarding the service registration out of both IOP system tenders and how they should be fulfilled.


This project is funded by the European Union

Table 4 - IOP system 1 vs. IOP system 2: Service registration

IOP system 1 (EU)	IOP system 2 (MK)
• Via Web Portal	• Via Web Portal

5.5.1.2 Service discovery

The following Table 5 illustrates requirements regarding the service discovery out of both IOP system tenders and how they should be fulfilled.

Table 5 - IOP system 1 vs. IOP system 2: Service discovery

IOP system 1 (EU)	IOP system 2 (MK)
• Metadata service catalogue on central server	• catalogue of services is located on the central communications server • list of all the services at disposal (including technical details)

5.5.1.3 Service composition

The following Table 6 illustrates requirements regarding the service composition out of both IOP system tenders and how they should be fulfilled.

Table 6 - IOP system 1 vs. IOP system 2: Service composition

IOP system 1 (EU)	IOP system 2 (MK)
• service provider and service consumer will not have to be aware of service interaction style	• Orchestration is performed on the central communication service

5.5.2 Discussion

Only a few details on service registration are provided in both tenders. The EU tender mainly speaks about service management, which includes also service registration. In the national tender service registration will be done via a web portal.
Service discovery in the national IOP system will be done via a catalogue of services.

5.6 Requirements for message transport

This section describes the requirements for transporting messages between components (i.e. between communication client and communication server) in an IOP system. The requirements are related to the format of the messages exchanged, the protocol to be used for exchanging messages, or the routing procedures for message exchange.

5.6.1 Comparison between IOP system 1 and IOP system 2

5.6.1.1 Routing

This requirement specifies the methods and communication channels for routing messages in an IOP system. The following Table 7 illustrates requirements regarding the routing of messages out of both IOP system tenders and how they should be fulfilled.


This project is funded by the European Union

Table 7 - IOP system 1 vs. IOP system 2: Routing

IOP system 1 (EU)	IOP system 2 (MK)
• dynamic routing: run-time content-based, itinerary-based, or context based message routing • Synchronous Communications, Asynchronous Communications	• communications between the communications clients may solely take place via the central communication server • Web Services Description Language (WSDL) for a description of its interface

5.6.1.2 Transport protocol

This requirement corresponds to the transport protocol to be used for exchanging messages. The following Table 8 illustrates requirements regarding the transport protocol out of both IOP system tenders and how they should be fulfilled.

Table 8 - IOP system 1 vs. IOP system 2: Transport protocol

IOP system 1 (EU)	IOP system 2 (MK)
• SOAP v1.2 • Web Service (WS*) Standard • SOAP/XML reliable and secure messaging • alternative communication way like HTTP Post • ESB shall provide protocol transformation	• SOAP versions 1.1 and 1.2 • provide a steady internet connection and VPN connection to the central communications server

5.6.1.3 Message format

This requirement affects the format of the exchange messages including metadata to be transferred between entities. The following Table 9 illustrates requirements regarding the message format out of both IOP system tenders and how they should be fulfilled.

Table 9 - IOP system 1 vs. IOP system 2: Message format

IOP system 1 (EU)	IOP system 2 (MK)
• dynamic message transformation and translation (structure and semantics) • Messages shall follow an "envelope" format, enabling message meta-data to be stored alongside the payload (the request data). The format includes a header that contains the meta-data and a body that contains the payload. Examples of the metadata that would be made available in the header are: ○ the identity of the sender, the originating application or service ○ the date of submission	• The standard and form of the structure of these web-services shall be defined in a separate document. • header composed of the following parameters: ○ username ○ password ○ service request basis ○ timestamp ○ at least one search parameter ○ digital signature

This project is funded by the European Union

○ the type of document contained within the message • XML Schema Definitions (XSDs) shall be designed to specify the format of the specific messages, requests and responses • Multi-linguality	

5.6.2 Discussion

Comparing both IOP system tenders, routing should take place via the central instance (communication server). The communication should be either synchronous or asynchronous. For describing endpoints the Web Services Description Language (WSDL) should be used, which is explicitly mentioned in the national tender. In contrast to that, dynamic routing functionality is only expected by the IOP system 1 implementation.
The requirements on the transport protocol are very similar in both solutions. Both IOP systems should rely on SOAP Web Services. However, the EU tender is more concrete and requires the use of WS-* technology. Finally, the IOP system 1 implementation shall also provide the capability of transforming different protocols.
Finally, the message format is not clearly defined in both tenders. They should follow an enveloped structure and should include certain meta information. Emphasizing, the form of the structure of the web services and messages is not given in the tenders and need to be defined in the IOP system.

5.7 Requirements for error handling

This section describes the requirements for error handling, e.g. where errors will be handled and who will be informed in case of failures.

5.7.1 Comparison between IOP system 1 and IOP system 2

The following Table 10 illustrates requirements regarding the error handling out of both IOP system tenders and how they should be fulfilled.

Table 10 - IOP system 1 vs. IOP system 2: Error Handling

IOP system 1 (EU)	IOP system 2 (MK)
• centralized exception management	• send notifications via e-mail or other means of communication in case of possible failure and error in its work

5.7.2 Discussion

There are only a few details given on error handling in both tenders. In IOP system 1 exception handling should be made centralized. For IOP system 2, no exception handling details are specified in the tender except that in case of failure responsible persons should get notified.

5.8 Requirements for logging/record-keeping/auditing

This section describes the requirements for logging/record-keeping/auditing extracted out of both tenders. In more detail, this requirement targets the record-keeping on technical details (logging) as well as on organizational/legal level (auditing).


This project is funded by the European Union

5.8.1 Comparison between IOP system 1 and IOP system 2

The following Table 11 illustrates requirements regarding error handling out of both IOP system tenders and how they should be fulfilled.

Table 11 - IOP system 1 vs. IOP system 2: Record-Keeping

IOP system 1 (EU)	IOP system 2 (MK)
• All messages from the IOP system shall be stored in a single, unified storage space (RDBMS) • track the status of messages to determine their state (delivered, responded to, error conditions, etc.), appropriate authentication/authorisation of messages, audit and so on • Detailed audit trail	• Keeps records of the transactions between institutions as XML files • communications server contains a built-in monitoring system for the business processes whereby it enables tracking of the operations in the system • Detailed records (audit trail) for all system transactions and events must also be kept on the central communications server and clients • each record must also contain corresponding timestamp issued by an authorized issuer (TSA) • each institutions may only have insight solely in the records referring to transactions that the institutions participated in • solution shall contain a central system for constant supervision, notification and alert over the work of all the system parts, the status of their workload, the use of resources

5.8.2 Discussion

Record-keeping is an important requirement in both tenders. All transported messages should be stored. In the EU tender the storage space is prescribed using a RDBMS, whereas in the national tender transactions should be recorded as XML files. Both IOP systems require a detailed audit trail, whereas the national tender requires the time stamping of records. Monitoring and status checking is also required in both IOP systems. Finally, the national tender requires more confidentiality with respect to the communication server concerning record-keeping.

5.9 Requirements for security

This section describes the security requirements in an IOP system. Security in an IOP system has several aspects, targeting the security of the component architecture (e.g. communication server) or the security on message level. In the following, security aspects on different levels (e.g. application level, transport level, etc.) are combined.

5.9.1 Comparison between IOP system 1 and IOP system 2

The following Table 12 illustrates requirements regarding security out of both IOP system tenders and how they should be fulfilled.


This project is funded by the European Union

Table 12 - IOP system 1 vs. IOP system 2: Security

IOP system 1 (EU)	IOP system 2 (MK)
• Secure messaging • SSL for transport security • Code Signing • Automated certificate discovery • User identification, authentication and authorisation •	• Message signature • Message encryption • HTTPS protocol (Secure Socket Layer v3 or Transport Layer Security 1.0 or more recent versions) • built-in monitoring system for the business processes whereby it enables tracking of the operations in the system, and also performs authentication and authorization of each system transaction. • solely the sender and receiver shall see the messages they mutually exchange. Other persons may see these messages only in cases defined by law • build a new PKI infrastructure or obtain the appropriate certificates from an authorized certificate issuer on the territory of the Republic of Macedonia. • Trusted TimeStamp Authority needs to be implemented within the system (in accordance with the RFC 3161 and the ANSI ASC X9.95 standards) - a new TSA infrastructure or obtain an adequate package of services from an authorized timestamp issuer located on the territory of the Republic of Macedonia • advanced digital signatures according to the current standards of ETSI (such as: PAdES, PAdES-T, XAdES, XAdES-T, CAdES, CAdES-T and other profiles)

5.9.2 Discussion

Security is an essential part when designing and implementing an IOP system. Both tenders require the use of several security features, most important the use of SSL/TLS for transport layer security as well as the signing and encryption of messages. The set-up or re-use of a PKI is clearly stated in the national tender, whereas the EU tender is more open in this respect. The use of time stamps is also explicitly required in the national tender. However, in comparison the EU tender requires certificates for code singing. The requirements for a user/identification, authentication and authorization management are also more detailed in the EU tender.

5.10 Requirements for Payment

This section describes the requirements for payment.

This project is funded by the European Union

5.10.1 Comparison between IOP system 1 and IOP system 2

The following Table 13 illustrates requirements regarding payment out of both IOP system tenders and how they should be fulfilled.

Table 13 - IOP system 1 vs. IOP system 2: Payment

IOP system 1 (EU)	IOP system 2 (MK)
• Payment processing	

5.10.2 Discussion

In fact, payment requirements are nearly neglected in both tenders. Payment is just mentioned once in the EU tender.

5.11 Requirements for User/Web interface

This section describes the requirements for a user/web interface in an IOP system.

5.11.1 Comparison between IOP system 1 and IOP system 2

The following Table 14 illustrates requirements regarding a user/web interface out of both IOP system tenders and how they should be fulfilled.

Table 14 - IOP system 1 vs. IOP system 2: User/Web interface

IOP system 1 (EU)	IOP system 2 (MK)
• A series of online web-based user interfaces to support Registration-Authentication-Authorisation	• A web portal has been built for the institutions which are still not able to incorporate the service in their own information systems, where the users can register and retrieve/order a service, and the results shall be displayed in a format understandable to them. The portal is supported by the Internet Explorer, Firefox, Chrome and Safari web-browsers. • The portal shall provide visual display of reports and transactions, logins etc.

5.11.2 Discussion

In both tenders details on user interfaces are nearly not given. However, user interfaces should be developed to support e.g. the registration of services or the identity/user management. In the national tender the user interface should be supported by most common web browsers.

5.12 Requirements for User/Identity management

This section describes the requirements for user/identity management such das the management of authorization roles and access rights.

5.12.1 Comparison between IOP system 1 and IOP system 2

The following Table 15 illustrates requirements regarding a user/user identity management out of both IOP system tenders and how they should be fulfilled.


This project is funded by the European Union

Table 15 - IOP system 1 vs. IOP system 2: User/Identity Management

IOP system 1 (EU)	IOP system 2 (MK)
• Different credentials • Different roles • User registration • WS-Trust and WS-Federation with SAML (Security Assertion Markup Language) 1.1 or above • provide federated authentication • Support authorization • Centralized authentication and authorisation based on Single Token Service STS	• user name and a password, as well as a digital certificate to sign the request with • Different roles • Different institutions

5.12.2 Discussion

A sophisticated user and identity management is required in both tenders. There, different institutions, users, and corresponding roles should be managed. The national tender specifies only two different credentials, whereas the EU tender requires the identity management to be more flexible in this respect. Explicit protocols are only mentioned in the EU tender.

5.13 Requirements for Licenses

This section describes the requirements for licenses.

5.13.1 Comparison between IOP system 1 and IOP system 2

The following Table 16 illustrates requirements regarding licenses out of both IOP system tenders and how they should be fulfilled.

Table 16 - IOP system 1 vs. IOP system 2: Licenses

IOP system 1 (EU)	IOP system 2 (MK)
• provide all the licenses	• provide all the licences

5.13.2 Discussion

All licenses should be offered to the contracting authority.

5.14 Requirements for Maintenance/Support

This section describes the requirements for maintenance/support.

5.14.1 Comparison between IOP system 1 and IOP system 2

The following Table 17 illustrates requirements regarding maintenance/support out of both IOP system tenders and how they should be fulfilled.

Table 17 - IOP system 1 vs. IOP system 2: Maintenance/Support

IOP system 1 (EU)	IOP system 2 (MK)
• 12 months warranty	• Provide maintenance and support

5.14.2 Discussion

Maintenance and support is only mentioned in the national tender, the EU tender mentions 12 months warranty.

This project is funded by the European Union

6 General requirements to consider for MKIL

Based on the requirements elicitation of Section IOP System Requirements Elicitation, not all requirements, which are essential for one individual IOP system, are also important for a common interoperability layer. For instance, licensing or support requirements for individual software components have no influence on a common interoperability interface, whereas the alignment on message transport level is important to achieve in interoperability between different service buses on technical level.
In this section, the requirements which are important for an interoperability layer between different IOP systems are filtered out from the complete list of requirements. Based on the analysis of the two different IOP system tenders and the results out of the discussions/workshops with the two information system contractors as well MISA, the following requirements are considered as important for achieving interoperability on technical level:

- Architectural Requirements
- Requirements for User/Identity management
- Requirements for service management
- Requirements for message transport
- Requirements for security

The following Figure 2: Macedonian Interoperability Layers illustrates interoperability requirements for a common interface between two IOP systems (IOP system 1 and IOP system 2). In this figure, the requirement for message transport is split into the requirements for routing, transport, protocol and data.

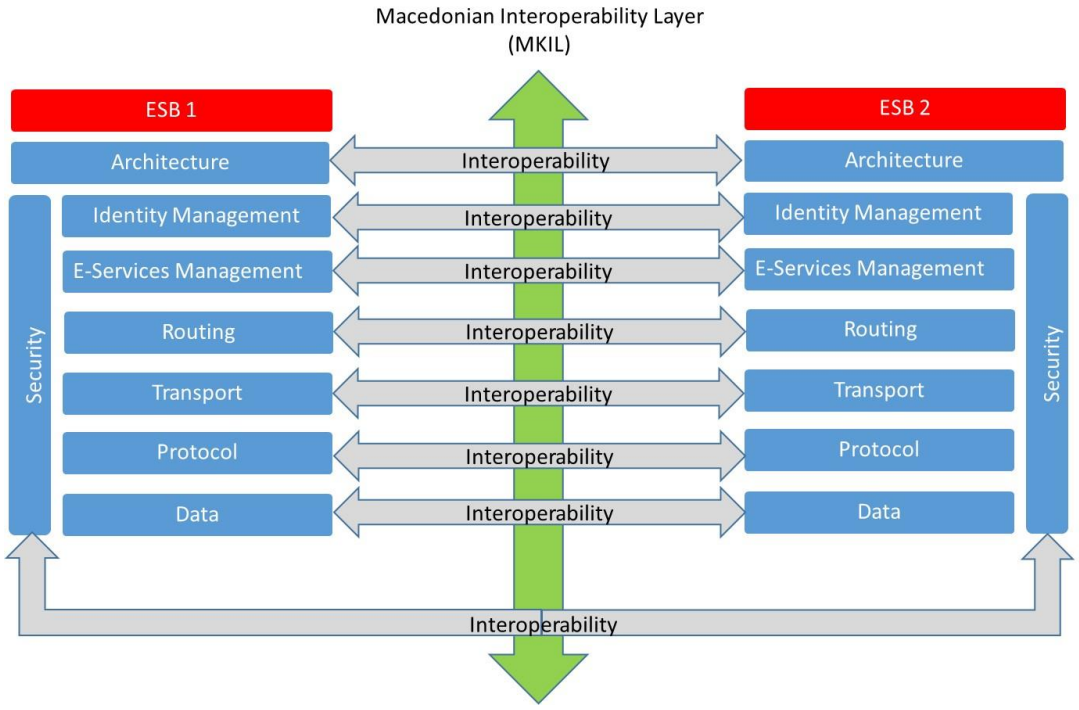


Figure 2: Macedonian Interoperability Layers

This project is funded by the European Union

To achieve interoperability between two or more IOP systems, architectural and conceptual modifications are necessary. Based on the information gathering phase, where the two different tenders for the implementation of a Macedonian IOP system were analyzed and interviews/workshops with the contracting companies were carried out, two conceptual interoperability models have emerged. The first interoperability model relies on a centralized approach, where metadata information is managed on a central instance for two or more IOP systems. The second interoperability model uses the concept of federation, where metadata is federated between the different IOP systems. However, the agreement of a common interoperability layer for message exchange is crucial for both models. In the following, the two different interoperability models are elaborated in more detail.

Central Interoperability Model

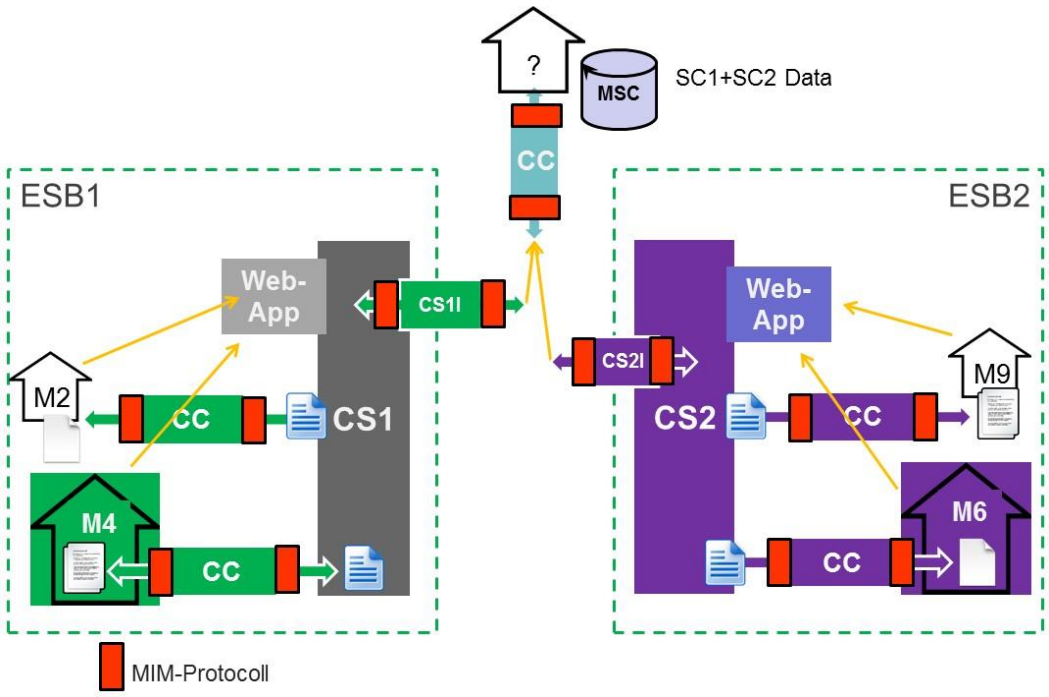


Figure 4 - Central Interoperability Model

Figure 4 illustrates the central interoperability model between two different interoperability systems. In this model, both IOP systems rely on a central instance for managing metadata of services or authorization information. This so-called metadata service catalogue (MSC) includes e-Service information from both IOP systems.

Different approaches exist for this MSC. As assumed in Figure 4 (for simplicity and better illustration of the concept of a central approach), all metadata and service information is managed in the MSC for both IOP systems. In that case, there is no need for each individual IOP system to maintain their (own) metadata service catalogue (MSC) within their IOP system domain. However, a more practical and realistic approach would be that each individual IOP system has its own SC but the MSC is just a virtualized SC combining the individual SCs. Another approach might be that the MSC just manages the location information of the SCs of other IOP systems, and then the SCs are queried directly by the service calling IOP system. Nevertheless, for all approaches a central MSC is required.

Who will operate this MSC still needs to defined, but probably the best solution is to run it by MISA, which has already been proposed. Another important thing is that querying must be done using a common interoperability protocol (MIM protocol as illustrated in Figure 4) used by both IOP system

This project is funded by the European Union

implementations. Otherwise service exchanged might be accompanied by complex protocol mappings.

Federated Interoperability Model

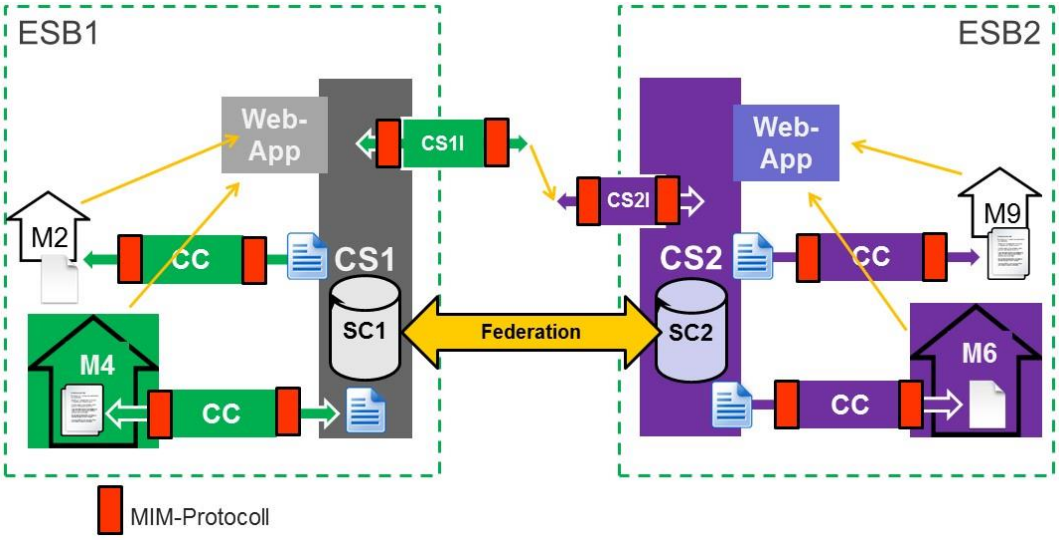


Figure 5 - Federated Interoperability Model

Figure 5 illustrates the federated interoperability model where no common central component is required. In that model, metadata for service and authorization management are federated. This means, for instance, that parts of the metadata information of SC2 needs to be federated into SC1, thus that IOP system1 is aware of the existence of services of IOP system 2.
Also here different approaches exist. One possibility would be to synchronize both SCs amongst each other. However, a more feasible approach is that only necessary information for data exchange is federated into the other SC and vice versa.
Nevertheless, that both IOP systems are able to communicate with each other the implementation of a common interoperability protocol (MIM protocol as illustrated in Figure 5) is crucial also in this architectural approach.

For a common interoperability layer (called Macedonian Interoperability Layer) between two different IOP systems, agreements for fulfilling the requirements on all individual layers/levels as illustrated in Figure 3 needs to be achieved. The figure illustrates the requirements in a layered/levelled architecture, starting from an architectural and more high-level view from the top down to a more detailed view defining exchanged data packets. In the following, we give a more detailed explanation on these requirements and levels, respectively.

6.1 Architectural Requirements

For achieving interoperability, an agreement on the overall interoperability architecture is essential as it may affect also lower levels. In fact, a decision needs to be made whether common interoperability architecture relies on common central components or if components and data of components of the individual IOP systems can be federated. Nevertheless, for achieving interoperability the common agreement on a SOA-based architecture is crucial.

This project is funded by the European Union

6.2 Requirements for User/Identity management

A common understanding on identity, authentication, and authorization information is required for achieving interoperability. Both IOP systems need to have somehow a common understanding on the amount of data stored in an identity management system and what kind of data is stored there. Examples are authorization information for accessing services. Important is also the granularity of the authorization data, e.g. the level of authorization (authorization is based on institutional level or on person level). Furthermore, used protocols are important in case of identity federation is considered.

6.3 Requirements for service management

Again, a common understanding on the metadata describing e-Services is important. An interoperability layer needs to know common details how e-Services are described and how they can be accessed. Will this be done via a Web Services Description Language (WSDL) or some other means? In addition, the interface for querying an e-Service register needs to be interoperable. How can web services be discovered? Is UDDI used? Security information required and supported by e-Services to ensure authenticity will be also stored in such a register. It is essential to know the kind of and the data format of such information for ensuring trust relationships.

6.4 Requirements for Routing

To communicate between two IOP systems, a common understanding on routing information is required to address communication endpoints and exchange messages. Common standard protocols should be used for routing messages. The questions that arise for this requirement are e.g. if this information is based on WSDLs, on WS-* specifications, or something similar?

According to the prescribed architecture of the tender, all communication between one IOP system domain should run through a central instance, which is called communication server. In an interoperability framework exchange of messages and routing between IOP systems is required. The requirement in this case will be that cross-IOP system message exchange needs to run between the individual communication servers of the individual IOP systems.

6.5 Requirements for the Transport

Web Service messages need to be transported between different endpoints and thus also between different IOP systems. In both tenders it has been agreed to use SOAP-based web services for transporting messages. The requirement is to use SOAP also for an interoperability transport protocol

6.6 Requirements for the Protocol

Even if the web services are defined by ministries/endpoint entities, there is a need for having some kind of meta services (e.g. for service discovering, checking authentication information or security, etc.). In both tenders specifications for this kind of protocol have been left open. Hence, there is a need to align this kind of protocol between both IOP systems if different protocols are specified in the implementation of each individual IOP system.


6.7 Requirements for Data

Of course, data that literally can be exchanged by using web service technologies are simply text or XML data. However, in fact arbitrary data can be exchanged, just a common agreement on the data format is required. Hence, also complex data such as images, documents, or containers can be exchanged. Nevertheless, the endpoints communicating with each other need at least have a common understanding on the data to be exchanged.

6.8 Requirements for Security

Especially in a governmental context security plays an important part as sensitive or personal data might be exchanged between endpoints or between IOP systems. Security is not important on one level only but affects several levels. In more detail, security functions need to be considered on application level (e.g. within identity management), transport, or even on data level. Both tenders specify the use of a lot of security functions such as using secure messaging (signing and encrypting of messages), using SSL/TLS for transport, or the specification of authentication and authorization mechanisms with respect to identity management.
In fact, an interoperability layer needs to agree on common security functions, such as on the specification for securing messages, algorithms used for signing or encrypting messages, etc.

This project is funded by the European Union

7 Recommendations

7.1 Recommendation: Use a centralized interoperability model

Problem: Currently, two similar projects have been commissioned to implement an IOP system. At the moment they are connecting different ministries/institutions amongst each other. In other words, as an example, IOP system 1 connects ministries M1…M4 and IOP system 2 connects to ministries M5…M9. Hence, M1…M4 can communicate with each other via IOP system 1 and M5…M9 via IOP system 2. However, in the current situation, the communication across the two different IOP systems is not required. This means, for instance, that at the present time it is not possible that ministry M1 is able to communicate and exchange services with ministry M9, since both ministries are interconnected on different IOP systems. To bypass this issue and to achieve interoperability between different IOP systems, architectural and conceptual modifications are necessary.

Verdict: The recommendation is to define means to interconnect the different IOP systems using a virtual centralized service.

Rationale: The recommendation for relying on a virtual central approach has the following reasons:

- No need for *n to m* connections when querying a service
- Accessing metadata information from a single point through a common interface
- Service information consistent over all IOP systems
- No need for metadata distribution between different CSs
- Lower maintenance effort (only one organization is responsible) and less error sources

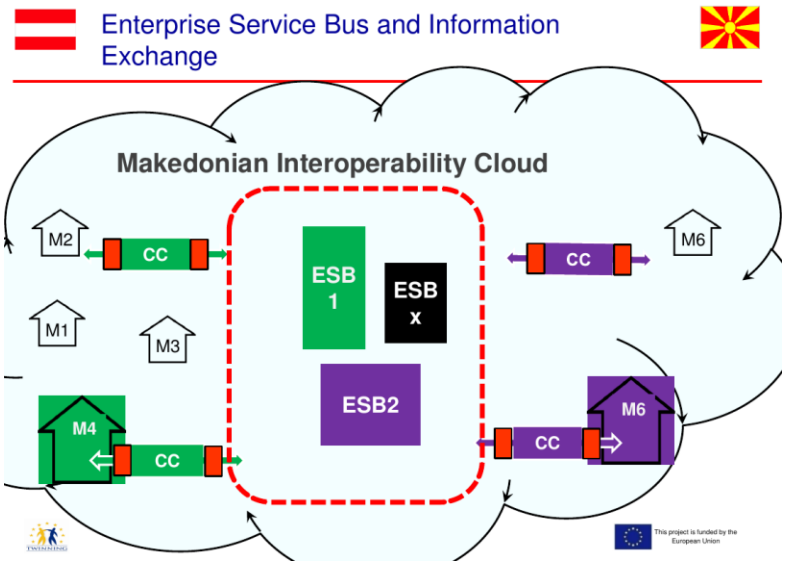


Figure 6: conceptional view on the virtual central IOP system implementation

Required action:

- Assure that the two tendering parties cooperate in crucial aspects of the implementation phase, that is: IOP system metaservices (MIM metaservices), MIM message container and routing specification (WS-*), security semantics (certificates, nounces), identification of

This project is funded by the European Union

participating parties (organization catalogue), identification of users (source of authentication and authorization).

7.2 Recommendation: Define metadata service catalogue architecture

Problem: In the current situation both IOP system implementations have to manage and maintain their own and separate metadata service catalogue MSC. Such a MSC holds – for instance – meta information (e.g. location, security requirements, etc.) of provided and offered services by the individual ministries. This information is necessary for being able to interconnect web services within an IOP system. However, in the current situation the MSC of an IOP system holds only the information of services accessible within one IOP system domain, meta information of other services from other IOP systems is not accessible.

Verdict: No clear recommendation can be given. The most promising solution is to balance pros and cons in respect to project risk (time and money) as well as mid- and long term stability of the system, maintainability, stability and failure resilience.

Rationale:
Both a centralized and a decentralized MSC approach are feasible, with respective pros and cons. A central MSC stores all meta information of web services of different IOP systems. Hence, one IOP system has easy access to other IOP system services beyond its domain. One IOP system just needs to query one central MSC instead of multiple. Services can be maintained at one central point, complex federation (e.g. distributing or synchronizing meta information of other IOP systems into the local domain's MSC) can be avoided. A central MSC also facilitates a possible connection to European services, as only one central instance needs to be accessed by European services instead of multiple national MSCs.
On the other hand, requiring the tendering parties to query a centralized MSC leaves the question open who is in charge to implement and operate the central MSC. Additionally, both administrative web sites to be implemented by the tendering parties (where services and the pre-requisites to call services are configured) would be required to store their information into this central system, opening questions of who is authorized with write privileges, again leading to the question of a centralized authorisation system.

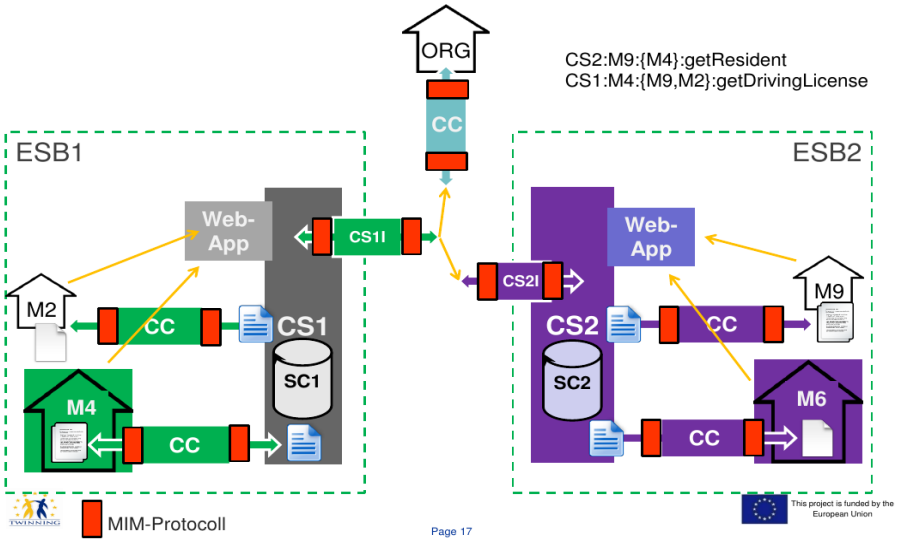


Figure 7: Decentralized, virtual higher level MSC

This project is funded by the European Union

An elegant solution, which also leaves to door open to implement a future central MSC, would be that CS1, once it receives a request to call a service which it cannot resolve within its own system, calls the other IOP system. From the viewpoint of CS1, this call could as well be perceived as it would go to a higher level infrastructure service (i.e. a higher level MSC). As long as there are only two IOP system implementations, a call for service discovery which cannot be resolved within the own system, would always go to the other system. Once there is a third IOP system implementation, a higher level service discovery service will be required though. In Figure 7: Decentralized, virtual higher level given above, the organisation information is centralized, schematically depicted by ORG (returning organisations) whereas the MSC information is federated across the two IOP systems.

Viewpoint of the experts:
In the short run, calling to the other IOP system, in cases where a call to a service cannot be resolved within the own system, using the MIM protocol, is the most promising solution, as it requires very little additional effort. In the long run a centralized MSC is more feasible as it results in an easier architectural layout. Increased failure vulnerability can be circumvented by load balancing and redundancy. A centralized approach eases discovery of and interconnection between services of different IOP systems.

Required action:

Clarify with both parties the necessity to resolve service calls, which cannot be handled by the own IOP system, to be delegated / resolved to one another service discovery instance.

7.3 Recommendation: Define authorization architecture

Problem: Besides meta information for administering and invoking metaservices, each individual IOP system needs to store and maintain authorization information in an authorization system. This authorization system manages who (e.g. ministry, institution, person, etc.) is in fact allowed to access a certain service within the communication client the administrative entity is connected to or in another IOP system. Similar to the meta information of services, currently authorization information is also managed separately in each individual IOP system domain. Creating a centralized authorization system would allow the configuration of access rights across IOP system implementations. However, this requires additional coordination between entities and increases the complexity and vulnerability of the system.

Verdict: No clear recommendation can be given. The most promising solution is to balance pros and cons in respect to project risk (time and money) as well as mid- and long term stability of the system, maintainability, stability and failure resilience.

Rationale:
Both a centralized and a decentralized authorization approach are feasible, with respective pros and cons.

Decentralized authorization

Pros:

- Reduced complexity: No additional service which is required to operate the IOP system.
- System more resilient to failure (no single point of failure)

Cons:

- Increased complexity: The gains of a simpler architecture are lost when the requirement has to be met to unambiguously identify and authorize users across IOP system borders as this logic has to repeatedly be re-implemented in backend systems.
- No single source of truth

Centralized authorization:

Pros:

- Single source of truth
- No trust relationships necessary
- Simpler architectural model

Cons:

- Less failure resilient architecture.
- Increaser complexity for tendering parties as requiring using (a) centralized authorization architecture is outside their scope.

Viewpoint of the experts:
When calling a service located in another IOP system domain, the local IOP authorization system is not aware who is actually allowed to call that service. A central authorization system facilitates this requirement and avoids a burdensome inclusion of authorization information of all other IOP systems into the local IOP system. However this requires a common understanding and format of the identities, attributes, and roles to be used in the central authorization system.

Required Action:

- Decide in a workshop within MISA whether a centralized or decentralized authorization infrastructure should be erected.

7.4 Recommendation: Specify a metaservice protocol MIM

Problem: The role of a metaservice protocol is to provide a generic set of methods which help to provide services, discover services including details of service invocation, auditing, logging, provisioning, etc. Besides the functional requirements of message exchange, additional services are required which are necessary for the clearing of data, such as organizational information. In total, the role of an IOP system metaservice protocol is to hide complexity, simplify access, allow developers to use generic, canonical forms of query, access and interaction, or handling the complex details in the background.

Verdict: After investigation of the semantics of the X-Road metaservice specification we recommend to consider basing the Macedonian Interoperability Protocol MIM on X-Road.


This project is funded by the European Union

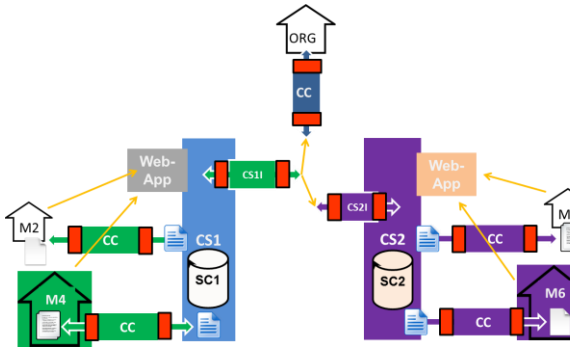
Figure 8: IOP Interoperability Layers

Rationale: X-Road is the Estonian implementation of a government IOP service layer, with the first implementation in 2001. As of today, millions of messages are sent over X-Road and X-Road has been successfully exported to Finland.
While the overall X-Road Architecture (c.f. https://www.x-road.eu/about.html) is not compatible with the Macedonian specification of IOP system tenders, as communication happens *n:m*, it provides a specification of metaservice methods, which can be useful for a Macedonian IOP system.

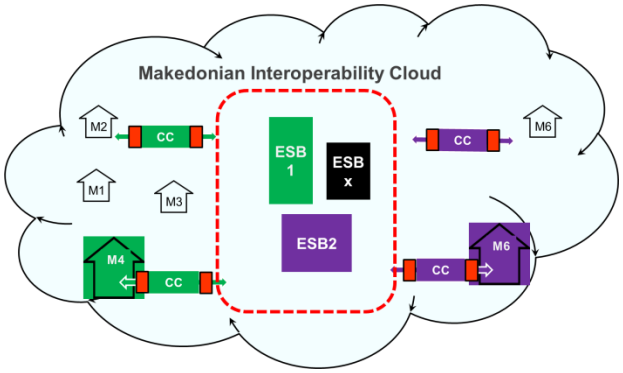
7.5 Recommendation: Use the MIM protocol as the only IOP system layer

Problem: Whenever an entity wants to provide a service in an interoperable manner, it has to do so using the unique information system. There may be services provided outside the IOP-layer for legacy reasons, however those services must not be called interoperable services according to the law. Given the current situation, two service busses are about to be implemented, varying in technical details yet without the requirement of being inter-interoperable (providing interoperability between entities connected within the domain of a respective service bus, but not in between service buses). This ties entities participating in an IOP system to their respective implementation, which must be avoided in order to prevent vendor lock-in.

Verdict: Every communication of services participating in the IOP system has to use the MIM protocol. This involves, in particular, the interfaces on both sides of Communication Clients (CCs) as well as, if deemed necessary, between service buses.



The MIM-Protocol (depicted in red) must be used throughout as the only communication interface.



From the Macedonian perspective, the fact that more but one service bus participates in the government IOP system cloud must be totally transparent.

Figure 9: Requirement of MIM as singular communication protocol and conceptional view on the IOP system cloud

This project is funded by the European Union

Rationale: From the Macedonian point of view, neither service provision nor service consumption must be tied to the implementation of a specific service bus. If one service bus goes offline, other service busses should be capable to take over discovery, invocation, routing, clearing and so on, as laid out in the MIM.

Required action:

Clarify with both tendering parties that every call to a service, in the moment the communication client is involved and when the required functionality is covered by the tendering requirements, has to be made using the MIM protocol.

7.6 Recommendation: Decide / Specify a Document Container Format

Problem: The current specification of the MIM is designed with machine-to-machine communication in mind. The entities participating on the MIM declared it as non-desirable to expose the actual user, who is calling a service. Instead, from the callee's perspective, it should be the ministry who is initiating the call and not an actual user. From a privacy perspective this requirement is understandable, however, in cases where privacy is not an issue or where the actual originator of a request has to be able to be traced down to the individual, a different approach is required. As the user information cannot be sensibly encoded in the MIM header as this information may be subject to data protection, a different approach has to be pursued.
Another use-case, which is sensibly covered at the semantics layer, is the transport of compound data like records including attachments or requirements of electronic records management, where the authenticity of the document has to be verified, for example, if the document has not been altered within the sphere of the originator instead during transport.

Verdict: Identify and use a standardized document container format.

Rationale: The IOP system specification of the two tenders at hand specifies the requirement that the Communication Server (CS) must not know about the data being exchanged, and in the case of end-to-end encryption, it is also technically impossible to inspect the information payload. The ASiC container, for instance, is a specification of a container covering these requirements:

- Associating advanced electronic signatures with any type of data
- Non-detached signing of data
- Standardized container bearing metadata information
- Support for timestamp tokens
- Standardized container format

While the actual structure of data exchanged will always be required to be mutually agreed, a common set of metadata (object creation time or change time, originator, provenance, etc.) is sensible to know about what kind of data ever, independent of the needs of any particular document or data type. ASiC is a container format specified by ETSI TS 102 918 (http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf) fulfilling the above mentioned requirements.

Another container format, which may be applicable in governmental data exchange scenarios, is the so-called OCD container. The SPOCS large scale EU pilot (http://www.eu-spocs-


This project is funded by the European Union


starterkit.eu/images/files/D2.1_List_of_standard_documents_and_relations_to_open_specifications.pdf) specifies and provides an implementation of a versatile container for documents, the Omnifarious Container for e-Documents (OCD). OCD is a multi-layered interoperability framework for the exchange of electronic documents. An OCD represents an electronic document container supporting any kind of electronic data as payload, provides semantic interoperability and authenticity.

ASiC and OCD are closely related: During the design of the OCD, the ASiC specification informed the OCD specification and development of the OCD container is happening further in the e-SENS large scale pilot project (http://www.esens.eu/technical-solutions/e-sens-competence-clusters/e-documents/).

However, ASiC and OCD might not be the only data format exchanged by IOP systems. Simply but well-established XML data structures such as ADMS (https://joinup.ec.europa.eu/asset/adms/home) might be another option. However, details on such data structures are elaborated in the activities related to IOP-S, the semantic interoperability layer.

Document container in relation to the MIM.
OCD is a container for payload realizing processing, authentication of the payload and extraction, whereas the MIM specifies core services required for the functioning of an IOP system. As such, OCD and the functionality provided by an IOP system (which is in part realized by using e.g. the X-Road specification) are orthogonal.
Document container in relation to the tenders. From the point of view of the IOP system tenders, the payload of data and information exchanged is irrelevant. As such, deciding on and specifying such a document container format will increase inter-ministerial IOP outside the scope of the IOP system tenders and will not cause any additional efforts on any tendering party.

This project is funded by the European Union