Модул за македонска интероперабилност:
ИОП-Т
(Техничка интероперабилност)

Јохан Хохтл, Бернд Цватендорфер, Петер Рајхштедтер, Игор Црвенов, Филип Маневски, Надица Јосифовски

Доставено на: 15.05.2015 г.
Верзија: V1.0 FINAL

СОДРЖИНА

1 Извршно резиме

Во рамките на овој документ се елаборирани аспектите на техничка интероперабилност во македонската влада.

Интероперабилноста претставува капацитет на хетерогени системи за размена на информации на разбирлив начин. Во овој контекст, под „разбирлив начин“ се подразбира дека две страни што учествуваат во електронска размена на податоци подеднакво ги разбираат техничките барања, семантиката на податоците и на услугите, како и засегнатите организациски процедури. Со цел овие три нивоа на интероперабилност да функционираат беспрекорно, неопходна е серија на управувачки принципи делумно изразена преку законски регулативи како и преку применети добри практики.
Општо земено, успешните рамки за интероперабилност се карактеризираат со воспоставени минимални елементи за интероперабилност коишто се неопходни со цел страните да бидат во можност да разменуваат податоци и информации, без притоа да го откриваат внатрешното функционирање на процедурите или деталите за техничката инфраструктура. Во продолжение на тоа, неопходно е да се исполнат и нефункционалните барања како на пример услуги за коишто е дозволено да се повикаат само по успешна авторизација, или пак шифрирање на разменетите пораки.
Македонската влада се соочува со растечки притисок за соработка, на пр. неопходно е да се обезбедат нови услуги со помали буџети. Технички ова може да се реализира преку поефикасно организирање на работата, потпомогнато од технологијата. Но сепак, користењето на технологијата во владата е нешто повеќе од работа заснована на хартија што се извршува по електронски пат. Искористувањето на можностите што ги нуди технологијата ќе резултира со поефикасни организациски модели коишто може да ги нарушат постојните затворени процедури, но затоа пак ќе поттикнат модели за нова интеракција и нови начини на размислување за отвореноста и транспарентноста.

Податоците и информациите се вреден производ. Граѓаните, економијата и надворешните засегнати страни како што се ЕУ бараат услуги во рамките на коишто податоците ќе се разменуваат помеѓу владините институции, наместо поединците да бидат приморани постојано да ги собираат своите документи и да ги доставуваат на државните службеници. Во продолжение на тоа, новите трендови како што се отворените податоци или подобрените одлуки овозможени поради сеопфатни анализи на податоци, подразбираат огромен опсег на податоци што вообичаено едно министерство не ги ни поседува. Токму затоа, способноста за размена на податоци и информации на непречен, корисен и безбеден начин е во центарот на дискусиите на владино ниво ширум светот, но и во Македонија.

Размената на податоците и информациите е овозможено преку примена на различни технологии и шеми за конекција како што се E-Mail, врска крај со крај помеѓу две страни, или пак преку користење на посреднички слој на инфраструктура. Во текот на последните неколку години се појавија шеми за интеракција коишто го претпочитаат концептот на централизиран брокер за пораки, откривање група на административни услуги, и обезбедување основни карактеристики како што се автентичност и шифрирање. Таквиот систем подразбира услуги на повисоко ниво како што е управување со идентитетот.

Технологијата се движи и отсекогаш се движела со забрзано темпо. Според тоа, предизвикот се однесува на дефинирање на стандарди и нацрт-договори што се и доволно конкретни за да можат технички да се спроведат, но и истовремено доволно општи за да подразбираат само

разумни напори за прилагодување кон технолошкиот напредок. Овој документ се фокусира на архитектонскиот дизајн на шемите на еден систем за ИОП што ќе ја овозможи интероперабилната интерконекција на македонските владини органи, притоа постојано имајќи ги предвид и идните барања како што се врската со економските засегнати страни и Европската заедница.

2 Проценка на интероперабилноста

Во рамките на ЗАКОНОТ ЗА ЕЛЕКТРОНСКО УПРАВУВАЊЕ (Службен весник на РМ бр. 105, 21.08.2009 г.), Македонија меѓу другото ги постави основите за електронска размена на податоци помеѓу субјекти. Тука е дефиниран поимот „единствена околина“ којшто според дефиницијата од член 3 *претставува управувана околина за стандардизирана размена на документи и податоци меѓу органите*. Во рамките на остатокот од овој документ, секаде каде што е споменат системот за ИОП повлечена е паралела со „единствената околина“, што подразбира *капацитет на информациските системи да обработуваат, разменуваат и зачувуваат документи и податоци по електронски пат, со примена на уникатни технолошки стандарди и процеси*.

Секој орган што има потреба од размена на информации во електронска форма е обврзан да се регистрира во единствената околина. Во случаи кога одреден орган сака да обезбеди услуга, тој е обврзан да користи комуникациски клиент (К-Клиент) дефиниран во „Насоки за техничките барања, начин на работа и функционирање на комуникацискиот клиент и препораки за користење на системот за интероперабилност“ како *хардверски уред со соодветен софтвер којшто обезбедува интерфејс за размена на документи и податоци во електронска форма коишто се разменуваат меѓу информациските системи на органите што учествуваат во размената*.

Доколку некој орган не обезбедува услуги, тој сепак може да учествува во размената на податоци во електронска форма преку веб-портал којшто го олеснува пристапот до услуги до коишто обезбедиле пристап други органи. Неопходно е секој систем којшто учествува во размена на податоци во електронска форма да биде сертифициран, како што е прецизирано во член 36 од гореспоменатиот закон. Сертифицирањето таму е опишано како *потврда на исполнувањето на условите за функционалност на информациските системи*.

Единствената околина (т.е. системот за ИОП) има улога на магистрала за пренос на информации. Магистралата што го овозможува преносот е наречена Македонска информациска магистрала - МИМ. Од технички аспект, протоколот што се користи за пренос на информации преку магистралата е наречен МИМ протокол. За жал, ова предизвикува конфузија во однос на тоа дали МИМ се однесува на техничката примена или на спроведувањето на софтверскиот сет (software stack) што ја овозможува интероперабилноста. Според тоа, овој документ го воведува поимот МКИЛ (Слој за интероперабилност во Македонија) којшто недвосмислено се однесува на метауслугите што ја овозможуваат интероперабилноста. Органите коишто учествуваат во МИМ се должни да воспостават безбедносни механизми преку автентикацијата на корисници и механизмите за контрола на пристапот.

Со цел гарантирање на заштитата и интегритетот на информациите, според „Насоките за техничките барања, начин на работа и функционирање на комуникацискиот клиент и препораки за користење на системот за интероперабилност“, ќе се применува следното:

- HTTPS протокол;
- автентикација, авторизација;
- конекција во доменската структура;
- користење на дигитални потписи;

- шифрирање на пораките што се разменуваат;
- физичка заштита на просторот; како и
- други мерки во согласност со општо прифатените препораки и безбедносни стандарди, ISO 27000 за безбедност и W3C стандарди.

Според „Правилникот за начинот на препознавање на единствената околина и за начинот на комуникацијата меѓу органите по електронски пат преку единствената околина за размена на документи и податоци по електронски пат“, неопходно е „единствената околина“ да има логови за следните информации:

- уникатен идентификатор на документ;
- уникатен идентификатор на корисникот-испраќач;
- уникатен идентификатор на корисникот-примач;
- време на прием на податоците и на документот на комуникацискиот сервер;
- основа за барањето;
- начин на испраќање на податоците и на документот;
- уникатен идентификатор на преносот.

Во моментов, доколку некој корисник на услуги сака да обезбеди услуга, тоа може да го направи со користење на комуникацискиот клиент којшто транспарентно обезбедува заштита на слојот за пренос, и обезбедува унифициран интерфејс кон МИМ.

Неопходно е комуникацискиот клиент (К-клиент) да ги поседува следните технички карактеристики:

- К-клиентот треба да може да комуницира преку веб-услугите со информацискиот систем на институцијата и со комуникацискиот сервер на системот за интероперабилност;
- Секогаш кога одредена веб-услуга се повикува според одредени параметри, покрај релевантните параметри, веб-услугата мора да ги содржи и параметрите според коишто била повикана;
- Неопходно е секоја услуга што органите ќе ја обезбедуваат во системот за интероперабилност да биде придружена од следните карактеристики:
    - време на одговор на услугата (минимално, максимално, просечно);
    - - стапка на грешки;
    - - тек (измерено во бајти, го претставува квантитетот на информациите што го добиваат виртуелните корисници од серверот по секунда);
    - - барања по секунда (на колку барања по секунда може да одговори услугата);
    - - симултани корисници.

Што се однесува пак до комуникацијата со користење на веб-услугите, потребно е да се исполнат следните технички стандарди:

- SOAP 1.1: основен, често користен стандард за размена на пораки преку различни транспортни протоколи, вклучително и HTTP;
- SOAP 1.2: подобрена верзија на основниот стандард;
- WS-Addressing, WS-ReliableMessaging, WS-TransmissionControl, и WS-EndpointResolution за доверлива и подобрена размена на SOAP порака;

- За цели поврзани со вршење на сигурна размена на пораки, неопходно е да се користи TSL 1.2.

Во случаи кога одреден корисник на услуги не сака или технички не е во можност да ги користи услугите преку комуникацискиот клиент, органот може да ги користи услугите преку посебен веб-портал. Во таков случај неопходно е органот-корисник да спроведе организациски мерки и мерки за физичка заштита, коишто ќе го гарантираат безбедното управување со информациите добиени преку МИМ порталот, и воедно потребно е да се назначи и менаџер на корисници (институционален администратор) одговорен за воспоставување на корисничките права за МИМ порталот.

И двете страни ќе мора да потпишат заеднички договор којшто меѓу другото ќе ги регулира и доделените права и барањата за користење на услугата, како и договори за нивото на услугите.

Што се однесува пак до ревизијата и одобрувањето, секој орган треба да биде обврзан да чува шифрирани логови на запишаните податоци и документи коишто се разменуваат со други органи на централно ниво или децентрализирано.

Според тековниот оператор, МИМ системот ги покажува следните недостатоци:

- Начинот на којшто МИМ е моментално спроведена е според барањата на институциите што учествуваат, и не може лесно да се прилагоди кон потребите на дополнителни страни;
- Метауслугите што ја овозможуваат функционалноста на системот за ИОП се скроени според тоа конкретно спроведување, се несоодветно документирани и нивното проширување се смета за предизвик. Поконкретно ова значи дека функционалноста за Интеграција на процесни апликации (EAI - Enterprise Application Integration) не може да се постигне;
- Моменталната архитектура за ИОП е архитектура од точка до точка, што ја промашува поентата за централна администрација и остава доволен простор за решенија што потполно можат да го заобиколат системот за ИОП, со што дополнително се промашува целта за централизирано диспечирање на пораките;
- Изворниот код на тековното спроведување не е достапен;
- Моменталниот начин на спроведување резултира со зависност од еден снабдувач.

Желбата за надминување на овие недостатоци резултирала со два тендери чијашто цел е да се спроведе подобрен систем за ИОП. Главите што следат подетално ги опишуваат воочените разлики помеѓу овие два тендери, и врз основа на анализа на документите, интервјуа со органите што се носители на тендерите, како и европските најдобри практики во однос на техничката интероперабилност, изработени се препораки.

3 Опис на проблемот

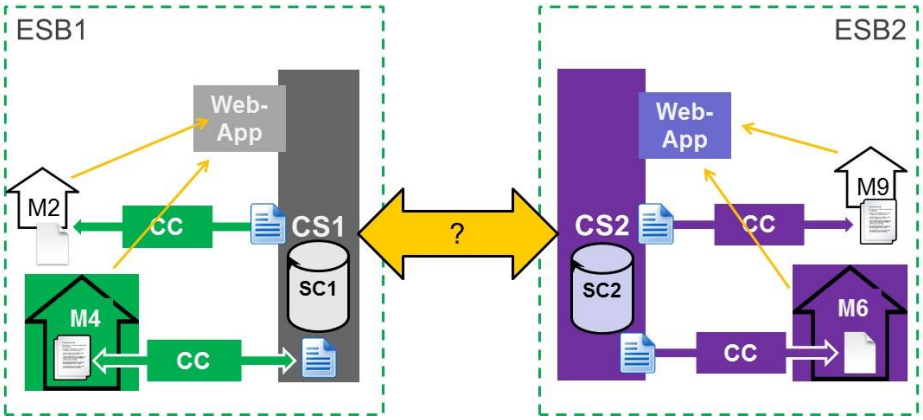
Македонската администрација објавила два тендери за спроведување на информациски систем за поврзување на министерства, градови и субјекти со надлежности за извршување на основни административни активности. Двата тендери опишуваат заедничка низа барања којашто во голем дел и се поклопува - на пр. ориентираност кон услуги, користење на веб-услуги преку SOAP, автентичност на пораките и шифрирање на пораките.

И покрај тоа што нивото за пренос (WS-*) и нивото за рутирање се добро дефинирани и се јавува поклопување кај двата тендери, суштинскиот слој за протокол на метауслуги (во понатамошниот текст се користи кратенката ММИ) не е дефиниран. Во националниот тендер дури и стои дека: *„Стандардот и формата на структурата на овие веб-услуги се дефинира во посебен документ“*. Меѓутоа, постоењето на стандардизиран сет на метауслуги е суштински предуслов за функционирање на системот за ИОП.

Во продолжение на тоа, постоењето на два (или во иднина и повеќе) системи за ИОП подразбира потреба од идентификување на услугите, што треба да се реализира на повисоко ниво (т.е. надвор од опсегот на тендерите), бидејќи во спротивно може да биде компромитирана интероперабилноста (ИОП). Предизвикот што претстои е двостран:

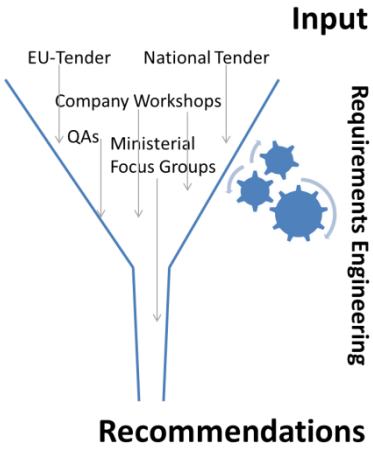
1. Да се изработи архитектура што ги исполнува барањата од двата тендери додека истовремено
2. потребни се минимални промени кај тие тендери со цел да не се одолговлечи нивното спроведување.

Сликата што следи е обид да се илустрира описот на проблемот. Од една страна, различни системи за ИОП треба да бидат интероперабилни за размена на пораки и за повлекување услуги и преку ИОП домени. Од друга страна пак, форматот и протоколот на разменетите пораки треба да бидат унифицирани.



4 Методологија

Експертите од земјата-членка го разгледаа тој предизвик и ги анализираа постоечките тендери, одржаа состаноци со тимовите за спроведување на тендерите, и разменија прашања и одговори со партнерите. Следната Слика 1 ја илустрира основната методологија за извлекување на барањата коишто ќе служат како основа за подоцнежните препораки.



Слика 1- Методологија

Собраниот инпут се анализираше и ќе се анализира за да се формулираат препораки коишто ги засегаат компаниите што ги спроведуваат тендерите, како и за да се формулира општиот исход од документот ИОП-Т.

Подетално, се работеше според следните чекори од процесот со цел да се извлечат препораки:

1. *Собирање информации*
   Во рамките на фазата за собирање информации темелно се анализираа двата достапни тендери (ЕУ тендерот и националниот тендер за спроведување на информациски систем). Во продолжение на тоа се интервјуираа и изведувачите од тендерите во рамките на организирани состаноци, со цел подобро да се сфати планираното спроведување на двата системи за ИОП. Во рамките на оваа фаза во главно се собираа информации.
2. *Прилагодување на барањата*
   Врз основа на собраните информации во рамките на првата фаза се изврши споредба на двата поединечни тендери, со цел да се откријат синергиите и разликите. За двата тендера можеше да се извлече заедничка серија на барања. Во продолжение на тоа можеа да се откријат и синергиите и разликите во однос на тоа како двата тендери ќе ги исполнат утврдените барања.
3. *Издвојување на барањата што се важни за ИОП-Т*
   Не сите од заеднички утврдените барања се важни за да се постигне интероперабилност на техничко ниво. Некои од утврдените барања дури и се повеќе поврзани со организациски аспекти. Токму поради тоа се пречисти списокот на заеднички барања, што резултираше со список на барања што се важни со цел двата системи за ИОП да постигнат техничка интероперабилност.
4. *Проценување на можните опции*
   Можно е да постојат различни опции за исполнување на избраните барања. Во рамките на првиот чекор се идентификуваа различните опции за исполнување на поединечните

барања. Во рамките на вториот чекор детално се дискутираше за различните опции за исполнување на некое одредено барање, а воедно и се проценуваа тие опции.

5. *Давање препораки*

   Врз основа на резултатите од евалуацијата се извлекуваат препораки. Препораките се фокусирани на најважните аспекти/барања за постигнување интероперабилност на техничко ниво.

5 Идентификување на барања за системот за ИОП

5.1 Заеднички барања

Во согласност со предложената методологија, целта беше да се споредат двата различни предлози за магистрали за интегрирање на услугите на организацијата со цел да се извлечат синергиите и разликите. Врз основа на оваа споредба може да се дефинираат заеднички барања што треба да ги исполнат и двата системи за ИОП. Идентификувањето на заедничките барања ја изгради основата за воспоставување на слојот за интероперабилност, бидејќи од суштинска важност е двата информациски системи што ќе се спроведат (или дури и идните системи) да ги задоволуваат овие заеднички барања, и со тоа да се постигне интероперабилност на техничко ниво.

Врз основа на споредбата на двата предлози за информациски системи може да се издвојат следните 13 заеднички барања:

- Стартни/оперативни барања
- Барања за спроведување
- Барања во однос на архитектурата
- Барања за управување со услуги
- Барања за пренос на пораки
- Барања за управување со грешки
- Барања за евидентирање/чување записи/ревизија
- Барања за безбедност
- Барања за плаќање
- Барања за кориснички интерфејс/ веб-интерфејс
- Барања за управување со корисници/идентитет
- Барања за лиценци
- Барања за одржување/поддршка

Овие барања се подетално опишани во деловите што следат, и табелите таму ги илустрираат разликите и синергиите што постојат помеѓу двете решенија за ИОП. Со други зборови, тие табели покажуваат како секое поединечно решение за ИОП ги исполнува или ќе ги исполнува заедничките барања. Од двата тендери за системи за ИОП во Македонија извлечени се разликите и синергиите.

5.2 Стартни и оперативни барања

Во рамките на овој дел опишани се барањата што треба да ги исполни еден систем за ИОП за да се овозможи негов старт и функционирање. Ова барање во главно ја засега централната серверска компонента (комуникацискиот сервер), бидејќи на оваа централна рутирачка инстанца може да се очекува големо оптоварување. Стартните или оперативни барања се однесуваат на пример на изборот на хардвер и серверски софтвер, мерки за гарантирање на голема достапност (на пр. кластер или баланс на оптоварувањето) или контрола на квалитетот на услугата.

5.2.1 Споредба на СИСТЕМОТ ЗА ИОП 1 и СИСТЕМОТ ЗА ИОП 2

Табелата Табела 1 - Систем за ИОП 1 наспроти систем за ИОП 2: Стартни ги илустрира барањата поврзани со оперативноста и стартот извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 1 - Систем за ИОП 1 наспроти систем за ИОП 2: Стартни и оперативни барања

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Активна/пасивна конфигурација на кластери на два виртуелни сервери • Контрола на квалитетот на услугата • Голема достапност • Соодветни перформанси • Конкретен хардвер за RDBMS (систем за управување со релациона база на податоци)	• Два јазли, активен/пасивен кластер (виртуелна средина) • Ограничување на користењето мрежна конекција (квалитет на услугата) • Голема достапност (99,7%) • Високи перформанси • Автоматско балансирање на оптоварувањето • BizTalk сервер 2009 (64-битен Microsoft Windows сервер) • За архива на податоци се користи Microsoft SQL сервер 2008

Дискусија

И двата тендери подразбираат воспоставување на моќен хардвер којшто ќе може да се справи со можни големи оптоварувања. Во рамките на националниот тендер набројани се јасни услови за хардверот. Но сепак и кај двете спроведувања треба да станува збор за голема достапност, подготвеност за кластери и поддршка на балансирањето на оптоварувањето. Националниот тендер не го наметнува користењето на Microsoft BizTalk сервер и Microsoft SQL сервер, но сепак компанијата што го врши спроведувањето планира да ги искористи. Во тендерот на ЕУ користењето на софтверските компоненти е поотворено (на пр. користење сервери за бази на податоци).

5.3 Барања за спроведување

Во рамките на овој дел се опишани барањата за спроведување на систем за ИОП или на неговите компоненти (комуникациски клиент, комуникациски сервер). Овие барања се однесуваат на користењето софтверски производи и програмски јазик за спроведување на компонентите.

5.3.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 2 ги илустрира барањата поврзани со спроведувањето извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 2 - Систем за ИОП 1 наспроти систем за ИОП 2: Барања за спроведување

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• .NET Framework технологија и користи Microsoft Visual Studio со програмскиот	• .NET Framework технологија и користи Microsoft Visual Studio со програмскиот

јазик C# • Комерцијална готова софтверска апликација (COTS - Commercial-Off-The-Shelves) • Детална обработка на порака • Автоматски бекап заснован на Symantec • Голема достапност врз основа на репликација заснована на COTS (Vertitas)	јазик C# • Интегрирање на нови алатки и производи, без оглед на платформата за нивен развој • Автоматски бекапи (детална стратегија за резервни копии) • Ќе содржи услуга за Доменски именски систем (DNS) • Испорака на софтверскиот изворен код

5.3.2 Дискусија

ЕУ тендерот е поотворен за примената на спроведениот софтвер, но подразбира користење на комерцијален готов софтвер (COTS). Спротивно на тоа, националниот тендер експлицитно наведува користење на .NET Framework и C# како програмски јазик. Нови алатки и работни текови би требало да можат лесно да се интегрираат кај двата тендери, но сепак ЕУ тендерот е поконкретен за примената на Унифицираниот јазик за моделирање (UML).

5.4 Барања во однос на архитектурата на серверот за системот за ИОП

Во рамките на овој дел опишани се барањата во однос на софтверската архитектура на системот за ИОП. Барањето влијае на целокупната архитектура на системот за ИОП, но и на централната софтверска компонента за внатрешни одлуки за дизајнот на архитектурата. На пример, ова барање ќе прецизира дали архитектурата на системот за ИОП треба да биде централизирана или лабаво поврзана, или пак, дали архитектурата на внатрешните компоненти треба да биде отворена и модуларна, или затворена.

5.4.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 3 ги илустрира барањата поврзани со архитектурата на системот за ИОП и на внатрешните компоненти извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 3 - Систем за ИОП 1 наспроти систем за ИОП 2: Барања во однос на архитектурата

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Единствена, безбедна точка за пристап • Засновано на архитектура ориентирана кон услуги (SOA) • Модуларно • Интеграција на процесни (владини) апликации • Лесно одржување	• Централниот комуникациски сервер функционира само како посредник за размена на пораки помеѓу комуникациските клиенти, но не смее да има увид во содржината на пораките • SOA архитектура • Модуларна и отворена архитектура • Лесни промени без притоа да се влијае на остатокот од модулите и на функционалностите на решението

5.4.2 Дискусија

И двата системи за ИОП треба да се засноваат на централизирана архитектура со централен комуникациски сервер што ќе функционира како посредник за различните комуникациски клиенти. Целокупната архитектура треба да се заснова на SOA. Внатрешната архитектура на компонентите треба да биде - според двата тендери - модуларна и отворена, со што новите апликации или компоненти лесно би се интегрирале, а промените не би влијаеле кај остатокот од решението.

5.5 Барања за управување со услуги

Во рамките на овој дел опишани се барањата за управување со услуги при спроведувањето систем за ИОП. Овие барања опфаќаат регистрирање, откривање и состав на услугите во рамките на инфраструктурата на системот за ИОП.

5.5.1 Споредба на системот за ИОП 1 и системот за ИОП 2

5.5.1.1 Регистрирање на услуги

Следната Табела 4 ги илустрира барањата поврзани со регистрирањето услуги извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 4 - Систем за ИОП 1 наспроти систем за ИОП 2: Регистрирање на услуги

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Преку веб-портал	• Преку веб-портал

5.5.1.2 Откривање на услуги

Следната Табела 5 ги илустрира барањата поврзани со откривањето услуги извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 5 - Систем за ИОП 1 наспроти систем за ИОП 2: Откривање на услуги

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Сервисен каталог на метаподатоци на централен сервер	• Каталогот на услугите е лоциран на централниот комуникациски сервер • Достапен список на сите услуги (вклучително и техничките детали)

5.5.1.3 Состав на услугите

Следната Табела 6 ги илустрира барањата поврзани со составот на услугите извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 6 - Систем за ИОП 1 наспроти систем за ИОП 2: Состав на услугите

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Обезбедувачот на услугата и нејзиниот корисник не мора да бидат запознаени со стилот на интеракција на услугите	• Оркестрацијата се врши на централната комуникациска услуга


5.5.2 Дискусија

Во двата тендери се наоѓаат само неколку детали во однос на регистрирањето услуги. ЕУ тендерот во главно го опфаќа управувањето со услуги, што воедно го вклучува и регистрирањето на услугите. Во националниот тендер пак, регистрирањето на услугите ќе се врши преку веб-портал.
Откривањето на услугите во националниот систем за ИОП ќе се врши преку каталогот на услуги.

5.6 Барања за пренос на пораки

Во рамките на овој дел опишани се барањата за пренос на пораки помеѓу компонентите (т.е. помеѓу комуникацискиот клиент и комуникацискиот сервер) во системот за ИОП. Барањата се поврзани со форматот на пораките што се разменуваат, протоколот што се користи за размена на пораки, или пак со процедурите за рутирање неопходни за размена на пораки.

5.6.1 Споредба на системот за ИОП 1 и системот за ИОП 2

5.6.1.1 Рутирање

Ова барање ги прецизира методите и комуникациските канали за рутирање пораки во рамките на еден систем за ИОП. Следната Табела 7 ги илустрира барањата поврзани со рутирањето пораки извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 7 - Систем за ИОП 1 наспроти систем за ИОП 2: Рутирање

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Динамично рутирање: рутирање на пораки засновано на содржина во рамките на рантајм (run-time), засновано на правец (itinerary), или засновано на контекст • Синхрони комуникации, асинхрони комуникации	• Комуникациите помеѓу комуникациските клиенти може да се одвиваат единствено преку централниот комуникациски сервер • WSDL (Web Services Description Language) за опис на интерфејсот

5.6.1.2 Протокол за пренос

Ова барање се однесува на протоколот за пренос којшто би се користел за размена на пораки. Следната Табела 8 ги илустрира барањата поврзани со протоколот за пренос извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 8 - Систем за ИОП 1 наспроти систем за ИОП 2: Протокол за пренос

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• SOAP v1.2 • Web Service (WS*) Standard • SOAP/XML доверливо и безбедно испраќање пораки • Алтернативен начин на комуникација како што е HTTP Post • Магистралата за интегрирање на	• SOAP верзии 1.1 и 1.2 • Се обезбедува сигурна интернет конекција и VPN (Виртуелна приватна мрежа) конекција со централниот комуникациски сервер

услугите на организацијата (ESB) ќе обезбеди трансформација на протоколот	

5.6.1.3 Формат на пораки

Ова барање влијае на форматот на пораките што се разменуваат, како и на метаподатоците што ќе се пренесат помеѓу субјектите. Следната Табела 9 ги илустрира барањата поврзани со форматот на пораки извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 9 - Систем за ИОП 1 наспроти систем за ИОП 2: Формат на пораки

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Динамична трансформација и превод на пораки (структура и семантика) • Пораките го следат форматот „плик“, со што се овозможува метаподатоците на пораката да се зачувуваат покрај основниот пакет на податоци за пренос (payload) (податоците за барањето). Форматот опфаќа заглавие (header) што ги содржи метаподатоците и тело што го содржи основниот пакет на податоци за пренос. Како примери на метаподатоци што би биле достапни во заглавието може да се наведат: ○ идентитет на испраќачот, почетната апликација или услуга; ○ датум на доставувањето; ○ тип на документот што го содржи пораката. • Ќе се дизајнираат XML шема дефиниции (XSDs) со цел да се прецизира форматот на специфичните пораки, барања и одговори • Повеќејазичност	• Стандардот и формата на структурата на овие веб-услуги се дефинира во посебен документ • Заглавието (header) се состои од следните параметри: ○ корисничко име; ○ лозинка; ○ основа за барање на услугата; ○ временски печат (timestamp); ○ најмалку еден параметар за пребарување; ○ дигитален потпис.

5.6.2 Дискусија

Доколку се споредат двата тендери за систем за ИОП, рутирањето треба да се одвива преку централна инстанца (комуникациски сервер). Комуникацијата треба да биде или синхрона или асинхрона. За опис на крајните точки треба да се користи WSDL (Web Services Description Language), што всушност е експлицитно наведено во националниот тендер. Спротивно на тоа, функционалноста за динамично рутирање се очекува само кај спроведувањето на системот за ИОП 1.

Барањата во однос на протоколот за пренос се мошне слични кај двете решенија. И двата системи за ИОП треба да се потпрат на SOAP веб-услуги. Меѓутоа, ЕУ тендерот е поконкретен и

го пропишува користењето на WS-* технологијата. Во продолжение на тоа, спроведувањето на системот за ИОП 1 ќе ја обезбеди и можноста за трансформирање различни протоколи.
На крајот, форматот на пораките не е јасно дефиниран во двата тендери. Тие треба да ја следат структурата „плик“ и треба да вклучуваат одредени метаподатоци. Неопходно е да се истакне дека формата на структурата на веб-услугите и на пораките не е прецизирана во тендерите, и потребно е да се дефинира во системот за ИОП.

5.7 Барања за управување со грешки

Во рамките на овој дел опишани се барањата во однос на управувањето со грешки, на пр. каде ќе се исправаат грешките и кој ќе треба да се информира доколку настанат одредени превиди.

5.7.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 10 ги илустрира барањата поврзани со управувањето со грешки извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 10 - Систем за ИОП 1 наспроти систем за ИОП 2: Управување со грешки

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Централизирана обработка на исклучоци	• Испраќање известувања преку е-мејл или други начини на комуникација во случај на можни недостатоци или грешки при работата

5.7.2 Дискусија

Кај двата тендери има само неколку детали во однос на управувањето со грешки. Во системот за ИОП 1 обработката на исклучоците треба да биде централизирана. Кај системот за ИОП 2 не се прецизирани никакви детали во тендерот во однос на обработката на исклучоците, освен дека во случај на пад треба да се известат одговорните лица.

5.8 Барања за евидентирање/чување записи/ревизија

Во рамките на овој дел опишани се барањата за евидентирање/чување записи/ревизија извлечени од двата тендери. Подетално, ова барање е фокусирано на чувањето записи за техничките детали (евидентирање), како и на организациско/правно ниво (ревизија).

5.8.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 11 ги илустрира барањата поврзани со евидентирање/чување записи/ревизија извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 11 - Систем за ИОП 1 наспроти систем за ИОП 2: Чување записи

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Сите пораки од системот за ИОП се зачувуваат во единствен, унифициран архивски простор (RDBMS - систем за управување со релациона база на податоци) • Следење на статусот на пораките за да се утврди нивната состојба	• Содржи записи од трансакциите меѓу институциите како XML датотеки • Комуникацискиот сервер содржи вграден мониторинг систем за бизнис процесите, со што се овозможува следење на операциите во системот • Детални записи (ревизорска трага) за сите

(испорачани, одговорени, услови за грешки, итн.), соодветна автентикација/авторизација на пораки, ревизија, итн. • Детална ревизорска трага	системски трансакции и настани мора исто така да се зачувуваат и кај централниот комуникациски сервер и клиенти • Секој запис мора да содржи и соодветен временски печат издаден од страна на авторизиран издавач (TSA - Орган за издавање временски печат) • Секоја институција може да има увид единствено во записите што се однесуваат на трансакции во коишто учествувала релевантната институција • Решението ќе содржи централен систем за постојан надзор, известување и предупредување за работата на сите делови од системот, за статусот на нивната работна оптовареност, користењето на ресурсите

5.8.2 Дискусија

Чувањето записи е важно барање и кај двата тендери. Сите пренесени пораки треба да се зачувани. Кај ЕУ тендерот за архивскиот простор се препорачува примена на RDBMS, додека пак, кај националниот тендер трансакциите треба да се зачувуваат како XML датотеки. И двата системи за ИОП подразбираат детална ревизорска трага, додека пак, националниот тендер наложува и временски печат на записите. Мониторингот и проверката на статусот се исто така предвидени и кај двата системи за ИОП. На крајот, националниот тендер предвидува поголема доверливост кај комуникацискиот сервер во однос на чувањето записи.

5.9 Барања за безбедност

Во рамките на овој дел опишани се барањата за безбедност во рамките на системот за ИОП. Безбедноста во системот за ИОП има неколку аспекти чијашто цел е безбедноста на архитектурата на компонентите (на пр. комуникацискиот сервер) или безбедноста на ниво на пораки. Подолу следи комбинација на безбедносните аспекти на различни нивоа (на пр. апликациско ниво, преносно ниво, итн.).

5.9.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 12 ги илустрира барањата поврзани со безбедноста извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 12 - Систем за ИОП 1 наспроти систем за ИОП 2: Безбедност

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Безбедно испраќање пораки • SSL за безбедност на преносот • Потпишување на код • Автоматско откривање на сертификат • Идентификација, автентикација и авторизација на корисник	• Потпис на пораки • Шифрирање на пораки • HTTPS протокол (Secure Socket Layer v3 или Transport Layer Security 1.0 или поактуелни верзии) • Вграден систем за мониторинг на бизнис процесите со што се обезбедува следење

•	на операциите во системот, а воедно се врши и автентикација и авторизација на секоја трансакција во системот • Единствено испраќачот и примачот ќе може да ги гледаат пораките што меѓусебно ги разменуваат. Други субјекти ќе може да ги видат овие пораки единствено во случаи прецизирани во законодавството • Развој на нова инфраструктура на јавниот клуч или стекнување соодветни сертификати од авторизиран издавач на сертификати на територијата на Република Македонија • Во рамките на системот е неопходно да се воспостави доверлив орган за издавање временски печат (TSA) (во согласност со RFC 3161 и ANSI ASC X9.95 стандардите) - нова инфраструктура за TSA или да се обезбеди соодветен пакет на услуги од авторизиран издавач на временски печат лоциран на територијата на Република Македонија • Напредни дигитални потписи според актуелните стандарди на Европскиот институт за телекомуникациски стандарди (ETSI) (како на пример: PAdES, PAdES-T, XAdES, XAdES-T, CAdES, CAdES-T, како и други профили)

5.9.2 Дискусија

Безбедноста е од суштинско значење кога се дизајнира и спроведува еден систем за ИОП. И двата тендери наложуваат спроведување на неколку безбедносни карактеристики, од кои како најважна може да се издвои примената на SSL/TLS за безбедност на нивото за пренос, како и потпишувањето и шифрирањето на пораките. Воспоставувањето или многукратното користење на инфраструктурата на јавниот клуч е јасно искажано во националниот тендер, додека пак, ЕУ тендерот е поотворен во однос на ова прашање. Користењето временски печати е исто така експлицитно наведено во националниот тендер. Но сепак за споредба, ЕУ тендерот подразбира сертификати за потпишување со код. Барањата за идентификација на корисник, како и за управување со автентикацијата и авторизацијата се подетално прецизирани во ЕУ тендерот.

5.10 Барања за плаќање

Во рамките на овој дел опишани се барањата за плаќање.

5.10.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 13 ги илустрира барањата поврзани плаќањето извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 13 - Систем за ИОП 1 наспроти систем за ИОП 2: Плаќање

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Обработка на плаќањата	

5.10.2 Дискусија

Барањата за плаќање се всушност речиси и занемарени кај двата тендери. Плаќањето е споменато само еднаш во ЕУ тендерот.

5.11 Барања за кориснички интерфејс/ веб-интерфејс

Во рамките на овој дел опишани се барањата за кориснички интерфејс/ веб-интерфејс во рамките на системот за ИОП.

5.11.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 14 ги илустрира барањата поврзани со кориснички интерфејс/ веб-интерфејс извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 14 - Систем за ИОП 1 наспроти систем за ИОП 2: Кориснички интерфејс/ веб-интерфејс

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Серија на онлајн кориснички интерфејси засновани на веб за поддршка на регистрацијата – автентикацијата - авторизацијата	• Развиен е веб-портал за институциите коишто сè уште не се во можност да ја инкорпорираат услугата кај своите информациски системи, каде што корисниците може да се регистрираат и да добијат/нарачаат услуга, а резултатите ќе бидат прикажани во формат што е разбирлив за нив. Порталот го поддржуваат Internet Explorer, Firefox, Chrome и Safari веб-прегледувачите • Порталот ќе обезбеди визуелен приказ на извештаите и на трансакциите, логинот, итн.

5.11.2 Дискусија

И кај двата тендери речиси и нема никакви детали во однос на корисничките интерфејси. Но сепак, корисничките интерфејси треба да се развијат за поддршка на пример на регистрацијата на услугите или на управувањето со идентитетот/корисниците. Кај националниот тендер корисничкиот интерфејс треба да го поддржат повеќето познати веб-прегледувачи.

5.12 Барања за управување со корисници/идентитет

Во рамките на овој дел опишани се барањата за управување со корисници/идентитет како на пример управувањето со улогите за авторизација и правата на пристап.


5.12.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 15 ги илустрира барањата поврзани со управувањето со корисници/кориснички идентитети извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 15 - Систем за ИОП 1 наспроти систем за ИОП 2: Управување со корисници/идентитети

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Различни акредитиви • Различни улоги • Регистрација на корисници • WS-Trust и WS-Federation со SAML (Security Assertion Markup Language) 1.1 или следно • Обезбедување на збирна автентикација • Поддршка на авторизацијата • Централизирана автентикација и авторизација заснована на услуга со единечен токен (STS - Single Token Service)	• Корисничко име и лозинка, како и дигитален сертификат за потпишување на барањето • Различни улоги • Различни институции

5.12.2 Дискусија

И кај двата тендери се бара софистицирано управување со корисниците и со идентитетот. Таму треба да се управуваат различните институции, корисници и релевантните улоги. Националниот тендер прецизира само две различни акредитиви, додека пак, ЕУ тендерот налага управувањето со идентитетот да биде пофлексибилно во тој поглед. Експлицитни протоколи се споменати само во ЕУ тендерот.

5.13 Барања за лиценци

Во рамките на овој дел опишани се барањата за лиценци.

5.13.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 16 ги илустрира барањата поврзани со лиценците извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 16 - Систем за ИОП 1 наспроти систем за ИОП 2: Лиценци

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• Обезбедување на сите лиценци	• Обезбедување на сите лиценци

5.13.2 Дискусија

Сите лиценци треба да се достават до договорниот орган.

5.14 Барања за одржување/поддршка

Во рамките на овој дел опишани се барањата за одржување/поддршка.

5.14.1 Споредба на системот за ИОП 1 и системот за ИОП 2

Следната Табела 17 ги илустрира барањата поврзани со одржување/поддршка извлечени од двата тендери за систем за ИОП, како и начинот на којшто тие треба да се исполнат.

Табела 17 - Систем за ИОП 1 наспроти систем за ИОП 2: Одржување/поддршка

Систем за ИОП 1 (ЕУ)	Систем за ИОП 2 (МК)
• 12 месечна гаранција	• Обезбедување одржување и поддршка

5.14.2 Дискусија

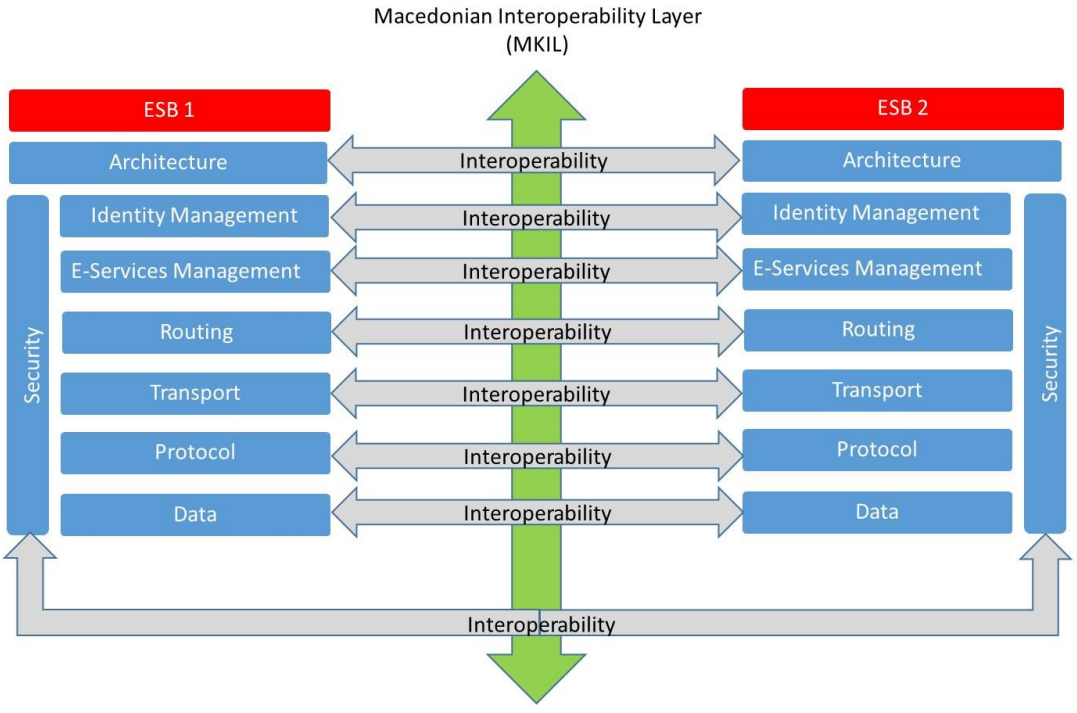
Одржувањето и поддршката се споменати само во националниот тендер, додека пак, во ЕУ тендерот спомената е само 12 месечната гаранција.

6 Општи барања што треба да се имаат предвид за МКИЛ

Врз основа на списокот со барања елаборирани во делот Идентификување на барања за системот за ИОП, не сите барања што се важни за еден одреден систем за ИОП се важни и за заедничкиот слој за интероперабилност. На пример, барањата за лиценцирање или за поддршка на поединечни софтверски компоненти немаат влијание на заедничкиот интерфејс за интероперабилност, додека пак прилагодувањето на нивото за пренос на пораки е важно за постигнување интероперабилност меѓу различните сервисни магистрали на техничко ниво.
Во рамките на овој дел, од комплетниот список на барања издвоени се барањата што се важни за слојот за интероперабилност меѓу различните системи за ИОП. Врз основа на анализата на двата различни тендери за систем за ИОП, како и на резултатите од дискусиите/работилниците со изведувачите на двата тендери за информациски систем и со МИОА, за постигнување интероперабилност на техничко ниво важни се следните барања:

- барања во однос на архитектурата;
- барања за управување со корисници/идентитет;
- барања за управување со услуги;
- барања за пренос на пораки;
- барања за безбедност.

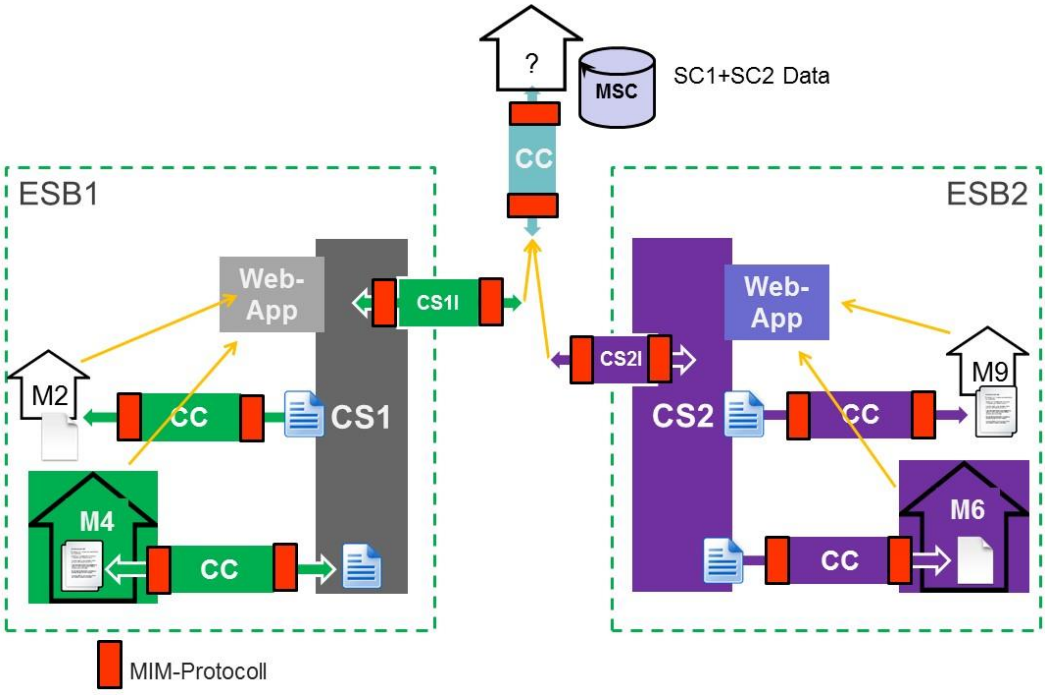
На следната Слика 2: Македонски слоеви на интероперабилност прикажани се барањата за интероперабилност за заедничкиот интерфејс меѓу двата системи за ИОП (систем за ИОП 1 и систем за ИОП 2). Кај оваа слика барањето за пренос на пораки е поделено на барањата за рутирање, пренос, протокол и податоци.



Слика 2: Македонски слоеви на интероперабилност

За да се постигне интероперабилност меѓу два или повеќе системи за ИОП неопходни се промени во однос на архитектурата и концептот. Врз основа на фазата за собирање информации во рамките на којашто се анализираа двата различни тендери за спроведување на македонски систем за ИОП, а се реализираа и интервјуа/работилници со изведувачите, се јавија два концептуални модели на интероперабилност. Првиот модел на интероперабилност е заснован на централизиран пристап, во рамките на којшто на централна инстанца се управува со информациите за метаподатоците за два или повеќе системи за ИОП. Вториот модел на интероперабилност го применува збирниот концепт (федерација), во рамките на којшто метаподатоците се собираат кај различните системи за ИОП. Но сепак, договорот за заеднички слој за интероперабилност за размена на пораки е од суштинска важност за двата модели. Во делот што следи детално се елаборирани двата различни модели на интероперабилност.

Централен модел за интероперабилност



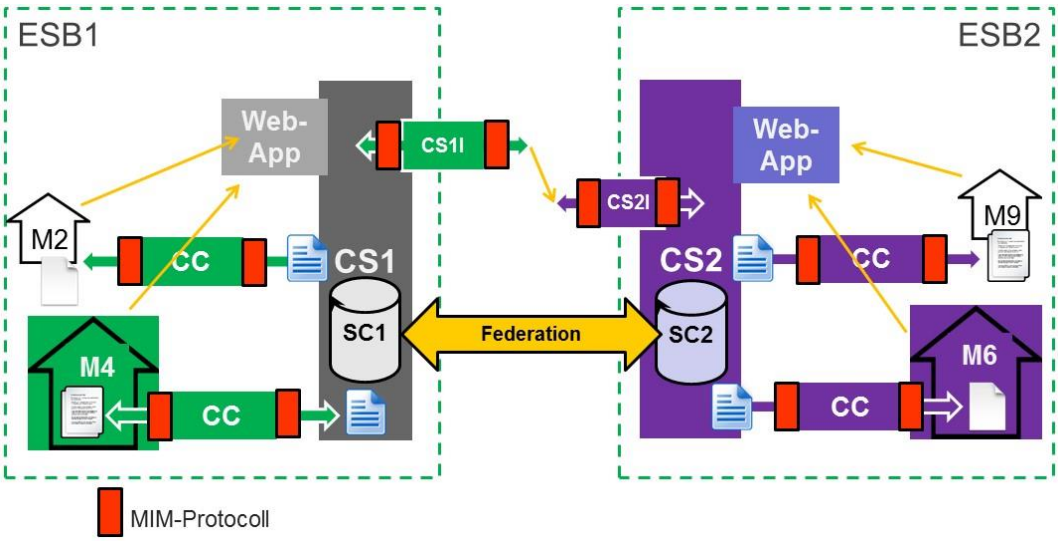
Слика 4 - Централен модел за интероперабилност

Слика 4 прикажан е централниот модел за интероперабилност меѓу двата различни системи за интероперабилност. Кај овој модел и двата системи за ИОП се потпираат на централната инстанца за управување со метаподатоците на услугите или информациите за авторизација. Овој таканаречен Сервисен каталог на метаподатоци (СКМ) опфаќа информации за е-услуги од двата системи за ИОП.

За овој СКМ постојат различни пристапи. Како што е претпоставено на Слика 4 (со цел поедноставување и подобра илустрација на концептот на централен пристап), сите метаподатоци и информации за услугите се управуваат во СКМ за двата системи за ИОП. Во таков случај секој поединечен систем за ИОП нема потреба да одржува свој (посебен) Сервисен каталог на метаподатоци (СКМ) во рамките на својот домен на системот за ИОП. Но сепак, како попрактичен и пореалистичен пристап би можело да се смета доколку секој поединечен систем за ИОП има свој СК, со оглед на тоа што СКМ е само виртуелизиран СК што комбинира поединечни СК. Како друг пристап би можел СКМ само да управува со локациските

информации на СК на други системи за ИОП, а потоа СК да бидат директно повикани од услугата што го повикува системот за ИОП. Но сепак, кај сите пристапи неопходен е централен СКМ.
Прашањето кој ќе управува со СКМ сè уште не е дефинирано, но веројатно најдоброто решение би било да го води МИОА, што веќе постои како предлог. Уште еден важен аспект е што повикувањето мора да се врши со користење на заеднички протокол за интероперабилност (протокол ММИ како што е прикажано на Слика 4), што го користат двата спроведени системи за ИОП. Во спротивно размената на услугите може да биде проследена со сложени мапирања на протоколот.

Збирен модел за интероперабилност



Слика 5 - Збирен модел за интероперабилност

Слика 5 прикажан е збирниот модел за интероперабилност каде што не е потребна никаква заедничка централна компонента. Во рамките на тој модел, метаподатоците за услугите и за управување со авторизацијата се здружени. Ова на пример значи дека делови од информациите за метаподатоци од СК2 треба да се здружат со СК1, со што системот за ИОП 1 би го препознал постоењето на услугите на системот за ИОП 2.
И овде исто така се јавуваат различни пристапи. Една можност би била да се синхронизираат и двата СК еден со друг. Меѓутоа поизведлив пристап би бил да се здружат само неопходните информации за размена на податоци кај другиот СК, и обратно.
Но сепак, и кај овој пристап за архитектурата е важно двата системи за ИОП да можат меѓусебно да комуницираат во однос на спроведувањето на заедничкиот протокол за интероперабилност (ММИ протоколот како што е прикажано на Слика 5).

За целите на заедничкиот слој за интероперабилност (наречен македонски слој за интероперабилност) помеѓу два различни системи за ИОП, неопходно е да се постигнат договори за исполнување на барањата за сите поединечни слоеви/нивоа, како што е прикажано на Слика 3. Графиконот ги прикажува барањата според поделената архитектура, почнувајќи од повисок преглед на архитектурата од врвот надолу, па се до подетален приказ

што ги дефинира разменетите податочни пакети. Во делот што следи прикажани се подетални објаснувања во однос на овие барања според нивоата.

6.1 Барања во однос на архитектурата

Со цел постигнување интероперабилност неопходно е да се постигне договор за целосната архитектура за интероперабилност, бидејќи тоа може да има влијание врз пониските делови. Всушност неопходно е да се донесе одлука дали заедничката архитектура за интероперабилност ќе се потпира на заеднички централни компоненти, или пак, ќе се здружат компоненти или податоци на компоненти од поединечните системи за ИОП. Но сепак, за да се постигне интероперабилност од суштинска важност е да се постигне договор за архитектура заснована на SOA.

6.2 Барања за управување со корисници/идентитет

За да се постигне интероперабилност потребно е заедничко сфаќање на идентитетот, автентикацијата и информациите за авторизација. И двата системи за ИОП е потребно некако подеднакво да ги разбираат количините на податоци зачувани во системот за управување со идентитет, како и типот на податоците што се зачувани таму. Како примери може да се наведат информациите за авторизација за пристап до услуги. Важна е и грануларноста на податоците за авторизација, како на пр. нивото на авторизација (дали авторизацијата е заснована на ниво на институција или на ниво на лица). Во продолжение на тоа важни се и користените протоколи доколку се размислува и за здружување на идентитетот.

6.3 Барања за управување со услуги

Повторно од суштинска важност е подеднаквото разбирање на метаподатоците што ги опишуваат е-услугите. Неопходно е слојот за интероперабилност да е запознаен со општите детали во однос на тоа како се опишани е-услугите, и начинот на којшто може да им се пристапи. Дали ова ќе се врши преку WSDL (Web Services Description Language) или на друг начин? Во продолжение на тоа, неопходно е и интерфејсот за повикување на регистар на е-услуги да биде интероперабилен. Како може да се откриваат веб-услугите? Дали се користи UDDI (Universal Description Discovery and Integration)? Во еден таков регистар би се зачувувале и безбедносните информации коишто се потребни и поддржани од е-услугите за да се гарантира автентичноста. Од суштинска важност е да се знае типот и податочниот формат на таквите информации, со цел да се воспостават доверливи односи.

6.4 Барања за рутирање

Со цел да се воспостави комуникација помеѓу два системи за ИОП потребно е подеднакво сфаќање на рутирачките информации, за да се адресираат комуникациските крајни точки и да се разменуваат пораки. За рутирање пораки треба да се користат заеднички стандардни протоколи. Прашањата што се јавуваат во однос на ова барање се однесуваат на пример на следното: дали тие информации се засновани на WSDLs, на WS-* спецификациите, или пак на нешто слично?

Во согласност со предвидената архитектура во тендерот, сета комуникација помеѓу еден домен на системот за ИОП треба да тече преку централна инстанца што се нарекува комуникациски сервер. Кај рамката за интероперабилност неопходна е размена на пораки и рутирање помеѓу системите за ИОП. Барањето во овој случај се однесува на тоа дека размената на пораки меѓу системите за ИОП треба да се одвива помеѓу поединечните комуникациски сервери на поединечните системи за ИОП.

6.5 Барања за пренос

Пораките на веб-услугите треба да се пренесуваат помеѓу различни крајни точки, а според тоа и помеѓу различни системи за ИОП. И кај двата тендери е договорено за пренос на пораките да се користат веб-услуги засновани на SOAP. Барањето се однесува на користење на SOAP и за интероперабилниот протокол за пренос.

6.6 Барања во однос на протоколот

Дури и ако веб-услугите се дефинирани од страна на министерствата/ субјектите од крајните точки, сепак се јавува потреба од некакви метауслуги (на пр. за откривање услуги, за проверка на информациите за автентикација или на безбедноста, итн.). И кај двата тендери спецификациите за овој тип на протокол се оставени отворени. Според тоа, неопходно е да се прилагоди овој тип на протокол кај двата системи за ИОП доколку при спроведувањето на секој поединечен систем за ИОП се прецизирани различни протоколи.

6.7 Барања за податоци

Се разбира дека податоците коишто може буквално да се разменат со користење на технологиите на веб-услуги, се едноставно текст или XML податоци. Но сепак може да се разменуваат и арбитрарни податоци, со тоа што ќе се обезбеди меѓусебен договор за форматот на податоците. Според тоа, може да се разменуваат и сложени податоци како што се слики, документи или контејнери. Но сепак, крајните точки што комуницираат меѓусебно треба барем да имаат подеднакво сфаќање на податоците што ќе се разменуваат.

6.8 Барања за безбедност

Особено кога станува збор за владин контекст, безбедноста игра значајна улога бидејќи помеѓу крајните точки или помеѓу системите за ИОП може да се разменуваат чувствителни или лични податоци. Безбедноста не е важна само на едно ниво, туку напротив, таа има влијание кај неколку нивоа. Подетално, безбедносните функции треба да се земат предвид на ниво на апликација (на пр. во рамките на управувањето со идентитетот), пренос, па дури и на податочно ниво. И кај двата тендери прецизирани се многубројни безбедносни функции како што се спроведување на безбедно испраќање пораки (потпишување и кодирање на пораките), користење SSL/TLS за пренос, или пак, специфицирање на механизмите за автентикација и авторизација во однос на управувањето со идентитетот.
Всушност, кај слојот за интероперабилност мора да се постигне согласност во однос на заедничките безбедносни функции како што е спецификацијата за обезбедување на пораките, алгоритмите за потпишување или кодирање на пораките, итн.

7 Препораки

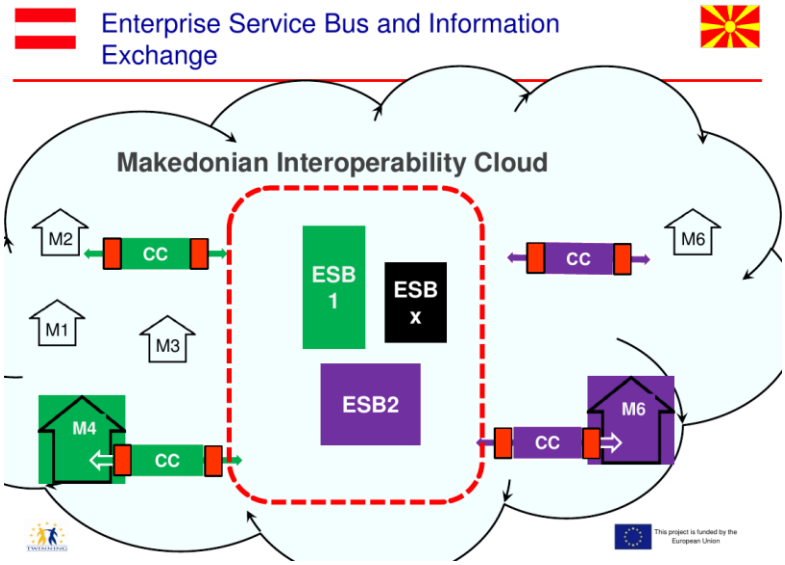
7.1 Препорака: Примена на централизиран модел за интероперабилност

Проблем: Во моментот два слични проекти ја имаат добиено задачата да спроведат систем за ИОП. Моментално меѓусебно се поврзуваат различни министерства/институции. Со други зборови и како пример, системот за ИОП 1 ги поврзува министерствата М1 ... М4, а пак системот за ИОП 2 ги поврзува министерствата М5 ... М9. Според тоа, М1 ... М4 може меѓусебно да комуницираат преку системот за ИОП 1, а М5 ... М9 преку системот за ИОП 2. Меѓутоа, според тековната ситуација не е побарана комуникација помеѓу двата различни системи за ИОП. Ова значи на пример дека моментално министерството М1 не може да воспостави комуникација и да размени услуги со министерството М9, бидејќи двете министерства се поврзани на различни системи за ИОП. Со цел да се заобиколи ова прашање и да се воспостави интероперабилност помеѓу различните системи за ИОП, неопходни се модификации на архитектурата и на концептот.

Решение: Препораката ќе дефинира начин за поврзување на различните системи за ИОП со користење на виртуелна централизирана услуга.

Објаснување: Препораката за потпирање на виртуелен централен пристап е донесена врз основа на следното:

- Нема потреба од *n до m* конекции при повикување на услуга
- Пристап до информациите за метаподатоците од една точка преку заеднички интерфејс
- Информациите за услугите се конзистентни кај сите системи за ИОП
- Нема потреба од дистрибуција на метаподатоците помеѓу различните КС
- Помали напори за одржување (само една организација ја има одговорноста) и помалку извори на грешки



Слика 6: концептуален преглед на спроведувањето на виртуелен централен систем за ИОП

Активности за спроведување:

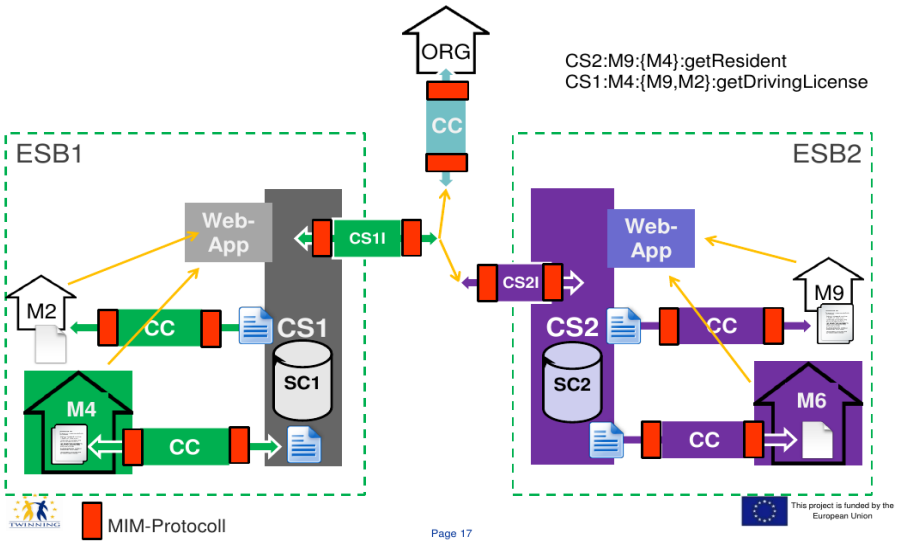
- Да се гарантира дека двата субјекти што учествуваат во тендерите соработуваат во однос на клучни аспекти од фазата на спроведување, односно: метауслуги на системот за ИОП (ММИ метауслуги), ММИ контејнер за пораки и спецификација за рутирање (WS-*), безбедносна семантика (сертификати, арбитрарни броеви (nounces)), идентификување на страните што учествуваат (организациски каталог), идентификување корисници (извор на автентикација и авторизација).

7.2 Препорака: Дефинирање на архитектурата на сервисниот каталог на метаподатоци

Проблем: Според тековната ситуација, и двата спроведени системи за ИОП треба да одржуваат и да управуваат со свој сопствен сервисен каталог на метаподатоци (СКМ). Таквиот СКМ содржи - на пример - метаинформации (на пр. локација, безбедносни барања, итн.) за обезбедените и понудени услуги од страна на поединечните министерства. Тие информации се неопходни за да може да се поврзат веб-услугите во рамките на системот за ИОП. Меѓутоа, според тековната ситуација СКМ на еден систем за ИОП содржи информации само за достапните услуги во рамките на еден домен на системот за ИОП, додека пак метаинформациите за други услуги од други системи за ИОП не се достапни.

Решение: Не може да се даде јасна препорака. Најповолно решение би било да се избалансираат предностите и недостатоците во однос на проектните ризици (време и пари), како и среднорочната и долгорочната стабилност на системот, одржливоста, стабилноста и отпорноста на падови.

Објаснување:
Можен е и централизиран и децентрализиран пристап за СКМ, со тоа што и двата пристапи имаат предности и недостатоци. Централниот СКМ ги зачувува сите метаинформации за веб-услугите на различни системи за ИОП. Според тоа, еден систем за ИОП има лесен пристап до услугите на другиот систем за ИОП дури и да се надвор од неговиот домен. Еден систем за ИОП само треба да повика еден централен СКМ наместо неколку други. Услугите може да се одржуваат кај една централна точка, а сложеното здружување (на пр. дистрибуција или синхронизација на метаинформации за други системи за ИОП кај локалниот домен на СКМ) може да се избегне. Централен СКМ исто така ја олеснува и можната конекција со европските услуги, бидејќи европските услуги треба да имаат пристап само до една централна инстанца, а не до повеќе национални СКМ.
Од друга страна пак, штом од субјектите што учествуваат во тендерот се бара да повикаат централизиран СКМ, останува отворено прашањето кој е одговорен за спроведување на централниот СКМ и за управување со него. Во продолжение на тоа, и двете административни веб-страници што ќе ги воспостават субјектите што учествуваат во тендерот (каде што ќе се конфигурираат услугите и предусловите за повикување на услугите) ќе треба да ги зачувуваат своите информации во тој централен систем, со што повторно се отвораат прашања од типот на тоа кој има овластувања за запишување, што повторно води кон прашањето за централизиран систем за авторизација.



Слика 7: Децентрализирано, виртуелно повисоко ниво на СКМ

Елегантно решение што воедно и остава простор за спроведување на иден централен СКМ би било следното: штом КС1 добие барање да повика услуга што не може да ја реши во рамките на својот систем, да го повика другиот систем за ИОП. Од аспект на КС1, за овој повик може да се смета како да ќе се проследи кај услуга од инфраструктурата на повисоко ниво (на пр. СКМ на повисоко ниво). Сè додека постојат само два спроведени системи за ИОП, повик за откривање услуги којшто не може да реши во рамките на матичниот систем секогаш ќе се препраќа кај другиот систем. Но сепак штом се спроведе и трет систем за ИОП, ќе биде потребно откривање на услуги на повисоко ниво. На Слика 7: Децентрализирано, виртуелно повисоко ниво на, информациите на организацијата се централизирани, шематски прикажани преку ORG (повратни организации), додека пак информациите од СКМ се здружени кај двата системи за ИОП.

Став на експертите:
На краткорочен план, повикувањето на другиот систем за ИОП во случаи кога повик до некоја услуга не може да се реши во рамките на матичниот систем, со користење на ММИ протоколот, е решение коешто најмногу ветува бидејќи подразбира многу мал дополнителен напор. На долгорочен план пак, централизиран СКМ е подобар бидејќи резултира со поедноставен распоред на архитектурата. Зголемената подложност на падови може да се избегне преку балансирање на оптоварувањето и редунданција. Централизираниот пристап го олеснува откривањето на услугите и нивната интерконекција кај различните системи за ИОП.

Активности за спроведување:

Да се разјасни со двете страни потребата од управување со повиците на услугата со коишто не може да управува матичниот систем за ИОП, и да се делегираат на друга инстанца за откривање услуги.

7.3 Препорака: Дефинирање на архитектура за авторизација

Проблем: Покрај метаинформациите за администрирање и повикување на метауслугите, секој поединечен систем за ИОП треба да зачувува и одржува информации за авторизација во

систем за авторизација. Овој систем за авторизација одлучува кој (на пр. министерство, институција, лице, итн.) всушност има право на пристап до одредена услуга во рамките на комуникацискиот клиент со којшто е поврзан административниот субјект, или на друг систем за ИОП. Слично на метаинформациите за услугите, со информациите за авторизација во моментот исто така се управува посебно, во рамките на секој поединечен домен на системот за ИОП. Воспоставувањето централизиран систем за авторизација би овозможило конфигурација на правата за пристап кај двата спроведени системи за ИОП. Меѓутоа, ова подразбира дополнителна координација помеѓу субјектите, а воедно и ја зголемува сложеноста и ранливоста на системот.

Решение: Не може да се даде јасна препорака. Најповолно решение би било да се избалансираат предностите и недостатоците во однос на проектните ризици (време и пари), како и среднорочната и долгорочната стабилност на системот, одржливоста, стабилноста и отпорноста на падови.

Објаснување:
Можен е и централизиран и децентрализиран пристап за авторизација, со тоа што и двата пристапи имаат предности и недостатоци.

Децентрализирана авторизација

Предности:

- Намалување на сложеноста: Нема дополнителна услуга потребна за управување со системот за ИОП
- Системот е поотпорен на падови (нема единствена точка на пад)

Недостатоци:

- Зголемување на сложеноста: Се губат придобивките од едноставната архитектура бидејќи мора да се исполни барањето за недвосмислено да се идентификуваат и авторизираат корисниците преку границите на системот за ИОП, имајќи предвид дека оваа логика мора постојано одново да се спроведува кај подредените (back end) системи.
- Нема единствен верен извор

Централизирана авторизација:

Предности:

- Единствен верен извор
- Не се неопходни доверливи односи
- Поедноставен модел на архитектурата

Недостатоци:

- Архитектура којашто е помалку отпорна на падови
- Повисок степен на сложеност за страните што учествуваат во тендерот бидејќи барањето да се користи архитектура за централизирана авторизација е надвор од нивниот опсег.

Став на експертите:

При повикувањето услуга што е лоцирана кај друг домен на системот за ИОП, локалниот систем за авторизација не знае кој има дозвола за повикување на таа услуга. Централниот систем за авторизација го олеснува ова барање и го избегнува оптоварувачкото вклучување на информации за авторизација за сите други системи за ИОП во локалниот систем за ИОП. Но сепак, ова подразбира подеднакво сфаќање и заеднички формат на идентитетите, атрибутите, и улогите што би се користеле во централниот систем за авторизација.

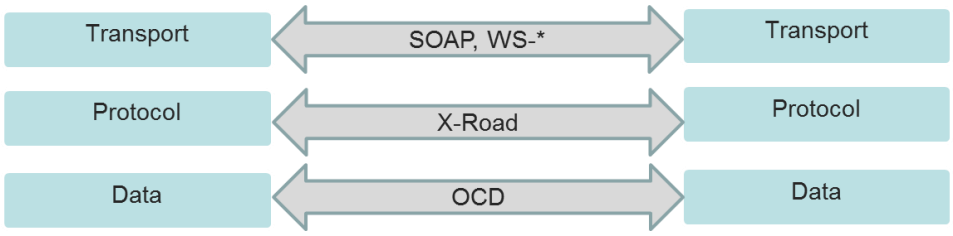
Активности за спроведување:

- Во рамките на една работилница за МИОА треба да се донесе одлука за тоа дали да се развие централизирана или децентрализирана инфраструктура за авторизација.

7.4 Препорака: Специфицирање на протокол за метауслуги ММИ

Проблем: Улогата на протоколот за метауслуги е да обезбеди генерички сет на методи коишто помагаат во обезбедувањето услуги, откривањето услуги вклучително и детали за повикување на услугата, нејзино ревидирање, евидентирање, обезбедување, итн. Покрај функционалните барања за размена на пораки, потребни се и дополнителни услуги неопходни за пречистување на податоците, како што се организациски информации. Општо земено, улогата на протоколот за метауслуги на системот за ИОП е да се сокрие сложеноста, да се поедностави пристапот, да им се овозможи на развивачите да користат генерички, канонски форми на повик, пристап и интеракција, или пак управување со сложените детали во позадината.

Решение: По анализата на семантиката на X-Road спецификациите за метауслуги, препорачуваме да се размисли за засновање на македонскиот протокол за интероперабилност ММИ на X-Road.



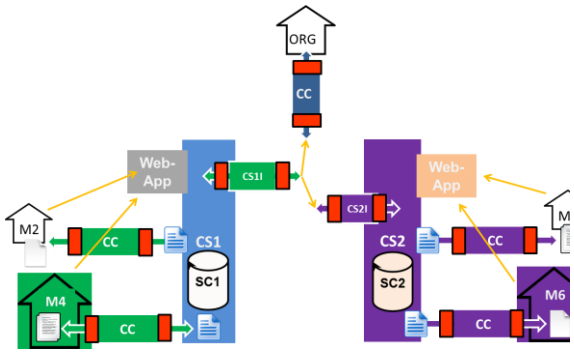
Слика 8: Нивоа на интероперабилност

Објаснување: X-Road претставува спроведен ИОП слој на услуги на естонската влада, прв пат воспоставен во 2001 г. До денес преку X-Road се испратени милиони пораки, а воедно тој е и успешно експортиран во Финска.
И покрај тоа што целокупната архитектура на X-Road (спореди https://www.x-road.eu/about.html) не е компатибилна со македонската спецификација за тендерите за системот за ИОП, со оглед на тоа што комуникацијата се случува како *n:m*, се обезбедува спецификација за методите на метауслуги, што може да е од корист за македонскиот систем за ИОП.

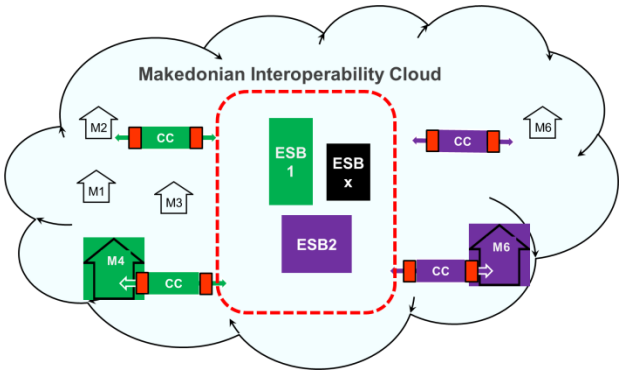
7.5 Препорака: Користење на ММИ протоколот како единствен слој на системот за ИОП

Проблем: Секогаш кога одреден субјект сака да обезбеди услуга на интероперабилен начин, тоа треба да го направи со користење на единствениот информациски систем. Можно е да се обезбедат услуги и надвор од слојот за интероперабилност поради причини поврзани со наследените системи, но тие услуги според законодавството не смеат да се нарекуваат интероперабилни услуги. Според тековната ситуација, во моментот треба да се воспостават две сервисни магистрали со различни технички карактеристики, но сепак без барање за интероперабилност (се обезбедува интероперабилност помеѓу субјектите поврзани во рамките на доменот на одредена сервисна магистрала, но не и помеѓу сервисните магистрали). Ова ги врзува субјектите што учествуваат во системот за ИОП со нивното спроведување, што мора да се избегне за да се спречи зависност од одреден продавач.

Решение: За секоја комуникација помеѓу услугите што учествуваат во системот за ИОП мора да се користи ММИ протоколот. Ова особено ги вклучува интерфејсите на двете страни на комуникациските клиенти (КК), како и помеѓу сервисните магистрали - доколку се смета за неопходно.



ММИ протоколот (претставен со црвена боја) мора да се користи постојано како единствен комуникациски интерфејс.



Од македонска перспектива, фактот дека во владиниот облак-систем за ИОП учествува повеќе од една сервисна магистрала мора да биде потполно транспарентен.

Слика 9: Барање за ММИ како единствен комуникациски протокол и концептуален преглед на облак-системот за ИОП

Објаснување: Од македонска перспектива, ниту обезбедувањето на услугите ниту користењето на услугите не мора да е врзано со спроведувањето на конкретна сервисна магистрала. Доколку една сервисна магистрала е офлајн, другите сервисни магистрали треба да се во можност да го преземат откривањето, повикувањето, рутирањето, пречистувањето итн., како што е прецизирано во ММИ.

Активности за спроведување:

Страните што учествуваат во двата тендери треба да бидат запознаени со фактот дека секој повик на услуга од моментот кога комуникациското клиент е вклучен и кога бараната функционалност е покриена со тендерските барања, мора да се реализира со примена на ММИ протоколот.

7.6 Препорака: Да се донесе одлука за / да се прецизира форматот на контејнерот за документи

Проблем: Моменталната спецификација на ММИ е дизајнирана имајќи ја предвид комуникацијата машина-машина. Страните што учествуваат во ММИ изјавија дека не би било пожелно да се открива фактичкиот корисник, оној којшто повикува услуга. Односно, од перспектива на повиканата страна, како страна што го иницира повикот треба да се јави министерство, а не фактички корисник. Од аспект на приватноста ова барање е јасно, меѓутоа, во случаи кога приватноста не е ставена на маса, или во случаи кога мора да има можност да се лоцира фактичкиот иницијатор на барањето (поединец), потребен е друг пристап. Со оглед на тоа што корисничките информации не може разумно да се кодираат во ММИ заглавието (header) бидејќи тие информации може да се предмет на заштита на податоци, неопходно е да се пронајде друг пристап.
Друг случај на примена којшто е релативно покриен во слојот за семантика, е преносот на сложени податоци како што се записи, вклучително и прилози или барања за управување со електронски записи, каде што треба да се верифицира автентичноста на документот, на пример доколку документот не бил изменет во рамките на областа на иницијаторот туку во текот на преносот.

Решение: Да се идентификува и примени стандардизиран формат на контејнерот за документи.

Објаснување: Спецификациите за системот за ИОП кај двата достапни тендери го прецизираат барањето комуникацискиот сервер (КС) да не е запознаен со податоците што се разменуваат, и во случај на шифрирање од крај до крај, всушност е технички невозможно да се провери основниот пакет на податоци за пренос (payload). ASiC контејнерот на пример претставува спецификација на контејнер што ги покрива следните барања:

- Поврзување на напредни електронски потписи со секаков тип на податоци;
- Нераздвоено потпишување податоци;
- Стандардизиран контејнер што носи информации за метаподатоците;
- Поддршка за токени за временски печат;
- Стандардизиран формат на контејнер.

Со оглед на тоа што за фактичката структура на разменетите податоци секогаш ќе има потреба да биде заеднички договорена, реално е да се познава и заедничкиот сет на метаподатоци (време на креирање на објектот или време на промена, иницијатор, потекло, итн.) за какви било податоци, независно од потребите на некој конкретен документ или тип на податок. ASiC претставува формат на контејнер специфициран од ETSI TS 102 918 (http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf) , којшто ги исполнува претходно споменатите барања.

Друг формат на контејнер што може да е применлив кај вакви сценарија за размена на владини податоци е т.н. OCD контејнер. Пилотот на ЕУ од голем размер, SPOCS (http://www.eu-spocs-starterkit.eu/images/files/D2.1_List_of_standard_documents_and_relations_to_open_specifications.pdf), го прецизира и обезбедува спроведувањето на прилагодлив контејнер за документи - OCD (Omnifarious Container for e-Documents - Разноврсен контејнер за е-документи). OCD

претставува повеќеслојна рамка за интероперабилност за размена на електронски документи. OCD претставува контејнер за електронски документи којшто ги поддржува сите видови електронски податоци како основен пакет на податоци за пренос, а обезбедува и семантичка интероперабилност и автентичност.

ASiC и OCD се тесно поврзани: во текот на дизајнирањето на OCD, ASiC спецификацијата ја информираше OCD спецификацијата, а развојот на OCD контејнерот се реализира и понатаму во рамките на e-SENS пилот проектот од голем размер (http://www.esens.eu/technical-solutions/e-sens-competence-clusters/e-documents/).

Меѓутоа, ASiC и OCD може да не се единствениот формат на податоци што ги разменуваат системите за ИОП. Едноставни, но добро воспоставени XML структури на податоци како што е ADMS (https://joinup.ec.europa.eu/asset/adms/home), може да се смета како друга опција. Но сепак, деталите за таквите податочни структури се елаборирани во рамките на активностите поврзани со ИОП-С, слојот за семантичка интероперабилност.

Контејнер за документи во однос на ММИ.
OCD претставува контејнер за обработка на основниот пакет на податоци за пренос, автентикација и екстракција, додека пак ММИ ги прецизира основните услуги што се потребни за функционирање на системот за ИОП. Како такви, OCD и функционалностите што ги обезбедува системот за ИОП (што делумно се реализирани со примена на пр. на X-Road спецификацијата) се ортогонални.
Контејнер за документи во однос на тендерите. Од перспектива на тендерите за системот за ИОП, основниот пакет на податоци и информации за пренос не е релевантен. Според тоа, донесувањето одлука за таквиот формат на контејнер за документи и неговото прецизирање ќе ја зголеми ИОП меѓу институциите неоптоварувајќи го опсегот на тендерите за систем за ИОП, и нема да предизвика никакви дополнителни напори за никој учесник во тендерот.