Модул за македонска интероперабилност: **ИОП-Т**

(Техничка интероперабилност)

АНЕКС: МИМ протокол

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

Доставено на: 13.08.2015
Верзија: V1.0

Овој проект е финансиран од Европската унија

СОДРЖИНА

Овој проект е финансиран од Европската унија

1 Историјат на верзијата

Верзија	Забелешки
2015-05-15, 1.0	**Финална**
2015-07-15, 1.0	Промени според инпутот од спроведувањето на системот за ИОП Појаснување на автентикацијата и авторизацијата **Финална**
2015-07-27, 1.0	Промени според инпутот од спроведувањето на системот за ИОП и заедничката дискусија на 2015-07-24 **Финална**
2015-08-12, 1.0	Промени според појаснувањата МК-ТК и KING-ICT: XSD шема, примери на SOAP плик **Финална**

Овој проект е финансиран од Европската унија

2 Апстракт

Овој документ го прецизира македонскиот протокол за интероперабилност - МИМ.

МИМ претставува:

- спецификација на протокол за пораки со минимална семантика специфична за еден домен;
- сет на услуги што ќе се спроведат преку систем за интероперабилност, со што ќе се овозможи соработката на информациските системи на интероперабилен начин;
- опис на текот на пораките помеѓу дефинирани услуги со примена на специфициран протокол.

Со оглед на тоа што семантиката на МИМ е независна од спроведувањето, со цел да се олесни читливоста и примената на оваа спецификација се претпоставува дека МИМ услугите ќе се спроведат како веб-услуги, а размената на пораките ќе се одвива со примена на SOAP.

Овој проект е финансиран од Европската унија

3 Дефинирање поими

Кратенка	Значење
МИМ	Македонска рамка за интероперабилност, Македонска информациска магистрала
СООУ	Сервис за организации што обезбедуваат услуги
СКМ	Сервисен каталог на метаподатоци

Овој проект е финансиран од Европската унија

4 Претставување на проблемот

Со цел информациските системи да можат да си разменуваат информации на разбирлив начин, неопходно е да се дефинира минимален сет на договорени компоненти, формати и процедури, имено:

1. Формати на пораки;
2. Метауслуги коишто изведуваат недвосмислени операции кај овие пораки; и
3. Интеракција на потребните инфраструктурни услуги.

Форматот на пораките, метауслугите и инфраструктурните компоненти, коишто го овозможуваат администрирањето на фактичките услуги што ги обезбедуваат страните коишто учествуваат во системот за интероперабилност, мора да ги исполнат следните општи барања:

1. Тие мора да се добро дефинирани;
2. Тие мора да се технолошки независни;
3. Тие мора да се доверливи;
4. Тие мора да се сигурни;
5. Тие мора да користат добро дефинирани стандарди коишто се широко распространети и познати.

Услугите мора да оформат модули коишто ќе му овозможат на еко-системот за интероперабилност да стане отпорен, толерантен кон грешки, лесен за спроведување и едноставен за администрирање.

Резултирачката архитектура на системот мора јасно да ја подели апликациската логика и комуникациската логика, како и да направи разлика помеѓу нив, а воедно и да ги охрабри субјектите што учествуваат во интероперабилноста да продолжат да ги сметаат своите услуги како „свој свет“, притоа задржувајќи ја сувереноста.

Овој проект е финансиран од Европската унија

5 Целна група

Овој документ е наменет за субјектите што сакаат да учествуваат во МИМ и што се засегнати со деталните технички аспекти на системот за интероперабилност. Вообичаено станува збор за следните функции/позиции:

- ИТ Директори коишто се соочуваат со растечки барања што треба да се исполнат со помали буџети, и коишто го сфаќаат концептот дека соработката на среднорочен или долгорочен план е поевтина и посоодветна за иднината отколку изолираното работење;
- Системски интегратори: тие ќе мора да ги проверат потребните компоненти коишто ја оформуваат МИМ архитектурата, да ги идентификуваат веќе постоечките, како и да ги дефинираат потребните напори за прилагодување на постоечките компоненти или за стекнување нови;
- Системски развивачи: тие ќе треба да ги прилагодат интерфејсите или да воспостават нови кон генеричките сервисни крајни точки дефинирани во МИМ;
- Офицер за безбедност: тие ќе треба да ја проверат спецификацијата во однос на безбедноста, како и дали крајниот систем ги исполнува дефинираните барања во однос на безбедноста.

Овој проект е финансиран од Европската унија


6 Карактеристики

МИМ обезбедува одредени нивоа со карактеристики. Карактеристиките од првото ниво ја опфаќаат синхроната комуникација. Карактеристиките од второто ниво ја опфаќаат синхроната и асинхроната комуникација.
Секој систем за ИОП мора да ги спроведе барем карактеристиките од првото ниво.

Карактеристика	Опис	Ниво
Вградена безбедност	Податоци: Врз основа на X.509 V3 сертификатите. Потпис и шифрирање на пораките Порака: Верификација на подобноста на повикувачот да повика услуга на одреден обезбедувач	1
Рутирање	На пораките до сите субјекти коишто се регистрирани (познати) во организацијата што обезбедува услуга	1
Евидентирање	Пораки: Фактот кога субјектот А му испратил порака на субјектот Б Грешки:	1
Архивирање на пораки	Во рамките на првото ниво, кај системот за ИОП нема да се складираат пораки (вклучувајќи го и КК и КС). Во рамките на второто ниво ќе се складираат пораки што може подоцна да ги повлече повикувач (асинхрона комуникација), или ќе се складираат пораки што ќе се достават доколку паднат системите за ИОП (КК до КС или КС до КК).	1
Управување со грешки	Управувањето со грешки го врши МИМ кај комуникацискиот слој, и се пријавуваат техничките грешки во однос на комуникацијата на пораки кај системот за ИОП, како што е недостапноста на услугата или обидите за прекршување на правилата за пристап до услугата.	1
Различни шеми на комуникација	Синхрона и асинхрона	2

Овој проект е финансиран од Европската унија

7 Одговорности

И покрај тоа што МИМ претставува техничка спецификација за интероперабилност во македонската администрација, сепак треба да се исполнат одредени организациски обврски со цел да се воспостави доверба помеѓу учесниците.

- МИОА е одговорно за администрирање и воспоставување на сервисот за организации што обезбедуваат услуги - СООУ.
- Обезбедувачот на магистралата за интероперабилност е одговорен за спроведување на комуникацискиот сервер (КС) според МИМ спецификацијата.
- МИОА е одговорно за сертифицирање на обезбедувачите на магистралата за интероперабилност што спровеле информациски систем за интероперабилност.

Овој проект е финансиран од Европската унија

8 МИМ Компоненти на архитектурата

8.1 Предуслови за МИМ

Со цел да функционира МИМ архитектурата неопходно е да се воспостават следните компоненти:

- Сервис за организации што обезбедуваат услуги - СООУ: Оваа услуга обезбедува список на организации. Неопходно е да се обезбеди барем јасниот назив на организацијата и уникатната идентификација. Овие информации вообичаено доаѓаат од датотека или од централна услуга (на пр. LDAP-услуга (Лесен протокол за пристап до директориум)). Деталите во однос на тоа како се обезбедуваат овие информации се надвор од опсегот на МИМ архитектурата.

8.2 Компоненти на МИМ

МИМ архитектурата се состои од следниве компоненти:

Акроним	Опис	Опис
КС	Комуникациски сервер	Комуникацискиот сервер е одговорен за: • Рутирање: пораки од сервисните клиенти до обезбедувачите на услуги и обратно; • Евидентирање: фактичката размена на пораки и кој/ која организација учествувале во размената на пораките • Безбедност: се пренесуваат само пораките што се во согласност со МИМ спецификацијата • Архивирање на пораки: ○ На првото ниво на МИМ не се зачувуваат пораки на КС освен кога станува збор за непосредно доставување на пораката. ○ На второто ниво на МИМ пораките се зачувуваат или на КК или на КС заради асинхроната комуникација, или доколку одредена услуга што учествува во системот за ИОП не е во можност навремено да ја добие пораката. Секој КС мора да воспостави крајна точка на КК, до којашто пристап мора да има само друг КС. Со цел одреден субјект да учествува во МИМ, неопходно е да склучи договор со овластен обезбедувач на услуги во МИМ.

Овој проект е финансиран од Европската унија

		За да се стане овластен обезбедувач на услуги во МИМ неопходен е сертификат од МИОА.
КК	Комуникациски клиент	Комуникацискиот клиент е одговорен за: • Интероперабилност: Неопходно е сите пораки на одреден субјект што учествува во МИМ да поминуваат преку КК. • Метауслуги: КК открива сет на метауслуги коишто го овозможуваат администрирањето на услугите што еден субјект сака или да ги искористи или да ги обезбеди во архитектурата на МИМ. • Безбедност: КК ја потпишува МИМ пораката и го шифрира корпусот на пораката. Со оглед на тоа дека сите пораки што се разменуваат во рамките на МИМ системот мора да поминат преку КК, тој има улога и на клиент и на обезбедувач на услугите. Субјект којшто сака да учествува во МИМ системот може или самостојно да воспостави комуникациски клиент, или да добие комуникациски клиент од одреден овластен и сертифициран обезбедувач на услуги во МИМ.
CCext	„Надворешен“ комуникациски клиент	За една сервисна магистрала постои само по еден надворешен КК. Станува збор за виртуелни комуникациски клиенти (или апликации) на (централниот) комуникациски сервер (КС), коишто се интерфејси за другата (или впрочем за која било друга) сервисна магистрала. Двете сервисни магистрали меѓусебно ќе комуницираат само преку тие надворешни КК.
ПУ	Подредена (back end) услуга	Услуга којашто учествува во интероперабилноста со користење на МИМ, или како корисник на услугата (клиент) или како обезбедувач на услугата. • Услугата ќе треба да комуницира со КК. • Услугата не смее да комуницира со КС. • Доколку ПУ има потреба да комуницира со други подредени системи, според техничките и организациските можности обезбедувачот на ПУ е одговорен да обезбеди пристап до ПУ и нејзино користење само на овластени лица, како и да гарантира дека сите зависни системи ги исполнуваат барем безбедносните барања наметнати од МИМ, како и законските

Овој проект е финансиран од Европската унија

	обврски (принцип на минимална безбедност[1]).

Обезбедувачот на системот за МИМ може да понуди дополнителни компоненти покрај споменатите, меѓутоа тие компоненти зависат од спроведувањето и би биле надвор од опсегот на МИМ спецификацијата[2].

[1]Максималното ниво на безбедност на поединечните системи што учествуваат во системот за интероперабилност мора да биде минимално ниво на безбедност на резултирачкиот виртуелен систем.

[2] На пример, веб-апликација за конфигурација на услуга и отповикување на услуга, услуга за евидентирање и ревизија, итн.

Овој проект е финансиран од Европската унија

8.3 Параметри на МИМ

Со цел да функционираат МИМ протоколот и МИМ метауслугите неопходен е сет од параметри. Станува збор за следните параметри:

Параметар	Опис
Корисник	Идентификатор на корисникот на услугата.
Обезбедувач	Идентификатор на обезбедувачот на услугата. Разликата помеѓу обезбедувачот и корисникот е валидна во рамките на контекстот на комуникацијата, и има логика ако се има предвид правецот на комуникацијата. Доколку не се реализира никаква комуникација во рамките на МИМ системот, и обезбедувачот и корисникот се еднакви и се класифицираат како учесници во МИМ.
РутирачкиТокен	Претставува идентификатор на обезбедувачот; во случај обезбедувачот да е лоциран кај друга ESB, пред него се наоѓа идентификаторот на ESB, по којшто следи $$ (= 2 знаци за долар).
УслугаИд	Идентификатор на услуга (на соодветен обезбедувач). УслугаИд претставува уникатен идентификатор на услугата, без целиот URL и методите. УслугаИд може недвосмислено да ја идентификува бизнис услугата на обезбедувачот во случаи кога УслугаМетод е празен или незастапен.
УслугаМетод	Идентификатор на метод обезбеден од УслугаИд. Ова поле е опционално и се користи во случаи кога клиентот може да ги поседува сите потребни информации за да адресира крајна точка што обезбедува бизнис услуга.
ТрансакцијаИд	Уникатен идентификатор за трансакција. ТрансакцијаИд е GUIDv4 генериран од КК на корисникот.
КорелацијаИд	Идентификатор што зависи од спроведувањето, издаден од ПУ за корелација на пораките кај подредениот систем.
Dir	Го претставува правецот на текот на пораката - или „барање“ или „одговор“.
повикТип	Тип на повик на метод. Вредностите се „синхрони“ или „асинхрони“. Првото ниво на МИМ спроведува само синхрони повици кај комуникацискиот слој, додека пак, второто ниво на МИМ ги поддржува асинхроните повици до услуги коишто ПУ ги обезбедува само на асинхрон начин.
јавенКлуч	Јавен клуч на субјект што повикува услуга во base64 кодирање што потекнува од x.509. Овој јавен клуч може да се издаде или на институција, на организациска единица или на лице.
Статус	Статус на комуникацијата. Се користат стандардни HTTP статусни кодови[3] со значење коешто е подолу опишано.

[3] http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

Овој проект е финансиран од Европската унија

СтатусПорака	Список на пораки на системот за ИОП. Толкувањето на пораката може да зависи од вредноста на полето за статус. Шифрирањето и серијализацијата на СтатусПорака е зависно од системот за ИОП.
Порака	Основниот пакет на податоци за пренос (payload) во пораката, секогаш шифриран.
Потпис	Вредноста на потписот на МИМ пораката.
МимеТип	Mime (Multipurpose Internet Mail Extensions) тип на основниот пакет на податоци за пренос во пораката. На пр. апликација/soap+xml или апликација/OCD[4]. Целосен список на дефинирани mime типови е достапен кај IANA (Internet Assigned Numbers Authority)[5].
ВременскиПечат	Временски печат издаден од системот за интероперабилност. Се претпочитаат потпишани временски печати издадени од орган за издавање временски печат (TSA).
Екстензија	Варијабла за понатамошна употреба.

Статусните идентификатори се стандардни HTTP кодови на грешка со повеќе детали (како што се истечени сертификати за инфраструктурата на јавен клуч) обезбедени во пораката за грешка во корпусот и опционално во полето на МИМ заглавието за СтатусПорака.

МИМ ги дефинира следните статусни кодови со следното значење:

Статус	Значење	МИМ ниво
102	Трансакција во тек. Барањето не може да се изврши бидејќи системот сè уште обработува барање (се користи како сигнал за повикувачот дека асинхрон повик е сè уште во тек).	2
200	Успешен пренос на порака	1
400	Повикувањето на еден од обезбедените сервисни методи од МИМ содржи невалидна комбинација на параметри. Корпусот ќе содржи дополнителни информации.	1
401	Повикувањето бизнис услуга изложена од КК не може да се изврши бидејќи КК којшто ја издава не може да се овласти.	1
402	Повикувањето бизнис услуга откриена од КК не може да се изврши бидејќи КК-примател одлучил дека деловните предуслови за исполнување на барањето не се задоволени. Ова може да опфаќа, но притоа не е ограничено само на необработени плаќања за користење на услугата.	1
403	Повикувањето бизнис услуга изложена од КК не може да се изврши	1

[4]Спецификација на OmnifariousContainerforeDocuments (OCD) http://www.gov2u.org/projects/spocs_starter_kit/images/files/D2.2_Standard_document_and_validation_common_specifications.pdf

[5]http://www.iana.org/assignments/media-types/media-types.xhtml

Овој проект е финансиран од Европската унија

	бидејќи системот за ИОП не може да пронајде валиден пат до КК којшто ја обезбедува услугата.	
429	Овој статусен код **може** да се испрати од КК доколку се препознаат измамнички активности како што се DoS (Denial of service) напади.	1
500	Системот за ИОП бил подлежен на внатрешна серверска грешка	1
503	Делови од системот за ИОП не се достапни, како на пример КК не е во можност да воспостави контакт со КС	1

Списокот на статусни кодови може да се прошири во подоцнежна фаза имајќи ги предвид организациските аспекти прецизирани во ИОП-О.

8.4 МИМ метауслуги

Метауслугите се дел од МИМ и го овозможуваат поставувањето и отповикувањето на услугите, повратот на пораките и управувањето со грешки. Следниот список на услуги им овозможува на субјектите да учествуваат во МИМ[6]:

Назив на услугата	Опис, вклучувајќи и влезни параметри и повратни вредности	МИМ ниво
РегистрирајУслуга (RegisterService)	Се користи за регистрирање услуга кај МИМ. Инпут: • УслугаИд: Уникатен идентификатор на услугата во рамките на средината на обезбедувачот. • WSDL – XML документ во WSDL стандард којшто содржи дефиниции за методите зад обезбеденатa УслугаИд. EndPoint адресите на услугите поставени во WSDL укажуваат на локална мрежа. Повратни вредности: нема	1
ДерегистрирајУслуга (UnRegisterService)	Се користи за дерегистрација на услуга кај МИМ. Инпут: • УслугаИд - Уникатен идентификатор на услуга. Повратни вредности: нема	1
ДобијОбезбедувачи (GetProviders)	Список на обезбедувачи за повик на метауслуги што го повикува корисникот, коишто откриваат најмалку една услуга за тој	1

[6]Во случај кога повратната порака е „None“, заглавието на повикот на пораката сè уште ќе биде според спецификацијата, а корпусот може да содржи податоци во случаи кога ќе мора да се врати грешка.

Овој проект е финансиран од Европската унија

	корисник. Инпут: нема Повратни вредности: • Списокот на обезбедувачи на услуга содржи: ○ идентификатори како РутирачкиТокен; ○ јавен клуч на организацијата што обезбедува услуга, за да се користи за шифрирање на порака од крај до крајна точка, олеснето од КК.	
ДобијУслуги (GetServices)	Враќа список на обезбедени услуги за конкретен обезбедувач. Инпут: • ОбезбедувачИд - Уникатен идентификатор на обезбедувач. Станува збор за ИД на организацијата којашто добила пристап до услуга од страна на друга организација, и којшто се поврзува со ИД што се користи за уникатно идентификување на организациите во рамките на МИМ системот. Повратни вредности: • Список на идентификатори на услуги што уникатно идентификуваат одредена услуга. Во случаи кога услугите се враќаат од друг МИМ систем, насочувачот на услугата содржи рутирачки информации за уникатно идентификување на услугите поставени кај друг МИМ систем (поставувањето РутирачкиТокен и интерпретацијата се дефинирани подолу).	1
ДобијУслуга (GetService)	Враќа сервисни дефиниции (WSDL документ) за конкретна услуга. Инпут: • ОбезбедувачИд - Уникатен идентификатор на обезбедувач. • УслугаИд - Уникатен идентификатор на услугата на обезбедувачот. • повикТип: Овој параметар влијае на	1,2

Овој проект е финансиран од Европската унија

	тоа како ќе реагира одреден повик на услугата, штом е повикана кај КК. Имплементацијата на првото ниво на МИМ може безбедно да го игнорира овој параметар, и секогаш ќе одговори со стандарден WSDL на побараната бизнис услуга. Повратни вредности: • Повратната вредност е XML документ според WSDL стандардот.	
СписокКорисници (ListConsumers)	Враќа список на сите регистрирани корисници. Инпут: • УслугаИд - Уникатен идентификатор на услугата на обезбедувачот. Повратни вредности: • Список на идентификатори на корисници.	1
ПроверкаСтатуспрекуТрансакцијаИд (CheckStateByTransactionId)	Дознавање на статусот на трансакцијата, корисно кај сценариото со асинхрон повик. Инпут: • ТрансакцијаИд - Уникатен идентификатор на трансакцијата. Повратни вредности: • Нумерички ИД којшто го прецизира статусот на барањето; Како можни вредности може да се јават: ○ Се обработува; ○ Непознато; ○ Исход.	2
ДобијПоракапрекуТрансакцијаИд (GetMessageByTransactionId)	Се добива порака преку ТрансакцијаИд од КК којшто се повикува во асинхрон режим. Повик до овој метод ќе ја избрише пораката од архивата на пораки. Овој метод го повикува подредениот систем ПУ за повраток на пораки што се вратени преку асинхрон повик на услуга. Инпут: • ТрансакцијаИд - Идентификација на трансакција Повратни вредности: • Порака со одговор	2

Овој проект е финансиран од Европската унија

ОбјавиПорака (PostMessage)	Се објавува порака во МИМ системот. Овој метод може да се повика за да се објави порака во МИМ системот, којашто ќе се зачува во редот со пораки и може да се повлече преку ДобијПоракапрекуТрансакцијаИд во случаи кога услугата што се нуди не се враќа навремено за да одговори на повикот на КК. Инпут: • ТрансакцијаИд на асинхрон повик на услуга за којшто ќе биде објавен одговорот; • Правец како параметар „dir“: правец на пораката - или „барање“ или „одговор“; • Пораката што ќе се објави По повикувањето на ОбјавиПорака следи повик на ПроверкаСтатуспрекуТрансакцијаИд со соодветна ТрансакцијаИд, со што ќе се добие статусот „Исход“, и пораката може да се поврати преку ДобијПоракапрекуТрансакцијаИд.	2

И покрај тоа што МИМ метауслугите се независни во поглед на технологијата и во теорија би можеле да се обезбедат со користење на JSON-API, RPC или Websocket протокол, често применето сценарио е користењето веб-услуги. Според тоа, претходно споменатите МИМ параметри ќе бидат подетално разработени во контекст на SOAP.

8.5 Управување со грешки

Управувањето со комуникациски грешки е интегрален дел од МИМ. Доколку одредено барање не може успешно да се обработи, претходно споменатите метауслуги ќе вратат статусен код во полето за заглавието на статус на пораката, со што ќе се укаже на неуспешниот обид за комуникација или на пр. на внатрешна серверска грешка. Во случај на внатрешни грешки кај системот за интероперабилност, потребно е да се пренесат стандардни SOAP грешки. Како опција, со цел да се олесни централизираниот преглед на статусот на системот, полето СтатусПорака може да содржи дополнителни информации коишто може да се толкуваат како специфични за спроведувањето на системот за ИОП.

Корпусот на Soap пораката за грешка ќе содржи детални информации за грешката, т.е. најмалку:

- ДатумВреме: печат за датум и време според ISO 8601;
- Локација: локацијата на грешката треба уникатно да се протолкува во рамките на доменот каде што се јавила грешката;
- Порака: порака за грешка;

Овој проект е финансиран од Европската унија

- ПоракаИД: ИД на пораката, специфично за имплементацијата[7].

Структурата на SOAP 1.2 пораката за грешка е следната:

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
              xmlns:m="http://www.example.org/timeouts"
              xmlns:xml="http://www.w3.org/XML/1998/namespace">
  <env:Body>
    <env:Fault>
      <env:Code>
        <env:Value>env:Sender</env:Value>
        <env:Subcode>
          <env:Value>m:MessageTimeout</env:Value>
        </env:Subcode>
      </env:Code>
      <env:Reason>
        <env:Text xml:lang="en">Sender Timeout</env:Text>
      </env:Reason>
      <env:Detail>
        <m:MaxTime>P5M</m:MaxTime>
      </env:Detail>
    </env:Fault>
  </env:Body>
</env:Envelope>
```

Шифрирањето на пораката за грешка ќе го дефинира MimeType.

[7]Треба да се има предвид дека во заглавието се определува специфициран Статус на ниво на целиот систем, и ќе се користи за да се одделат успешните повикувања на методот од погрешните враќања.

Овој проект е финансиран од Европската унија

8.6 SOAP контејнер за МИМ метауслуги

Во рамките на SOAP контекстот, именскиот простор на МИМ протоколот ќе биде поставен на: http://mioa.gov.mk/interop/mim/v1.

SOAP плик се состои од SOAP заглавие што содржи МИМ заглавие (Header) „Н“, МИМдополнителноЗаглавие „А“ и криптоЗаглавие „С“ и SOAP корпус што содржи МИМ корпус на порака „В“.

SOAP пораката треба да го следи следниот пример:

```
<?xmlversion="1.0"?>
<soap:Envelopexmlns:soap="http://www.w3.org/2003/05/soap-
envelope"xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:mioa="http://mioa.gov.mk/interop/mim/v1">
<soap:Header>
<mioa:MIMHeader/>
<mioa:MIMadditionalHeader/>
<mioa:CryptoHeader/>
</soap:Header>
<soap:Body>
<mioa:MIMbody>
            <Message/>
      <mioa:MIMbody>
</soap:Body>
</soap:Envelope>
```

МИМ корпусот може да содржи шифриран корпус на порака или корпус на порака со обичен текст, но не и двете истовремено.
Доколку пораката е шифрирана мора да се користи КриптоЗаглавие- елементот (CryptoHeader-Element).

Опис на параметар на МИМЗаглавие/МИМКорпус

Појавата на „М“ значи дека полето мора задолжително да се обезбеди, во зависност од контекстот на повикот (барање наспроти одговор). „О“ означува опционално појавување.

Параметар	Заглавие „З“ / Корпус „К“	Појава	xsd Тип на податок	Примена / Потекло
Корисник	З	М	низа	Утврдено од КК во моментот кога ќе се добие повикот за пораката, притоа идентификувајќи го оригиналниот повикувач на пораката
Обезбедувач	З	М	низа	Утврдено од КК во моментот кога ќе се

Овој проект е финансиран од Европската унија

				испрати одговор на пораката, притоа идентификувајќи го потеклото на организацијата што обезбедува услуги (обезбедувачот се пополнува само за одговорот (КК на страната на обезбедувачот)).
РутирачкиТокен	З	М	низа	РутирачкиотТокен се добива преку методот ДобијОбезбедувачи. Детален опис на значењето на РутирачкиТокен е претставен во 9.2.1
Услуга	З	М	низа	Називот на услугата е внесен од страна на КК кога ќе се добие барање за повик на бизнис услуга, и не го опфаќа називот на методот(-ите). Услугата може да биде и недвосмислено идентификувана со ИД (УслугаИд), што може да го реши само КС што е во улога на обезбедувач.
УслугаМетод	З	О	низа	Назив на методот што го обезбедува услугата. Ова поле е опционално. Доколку постои, комбинацијата на услуга и метод ја дефинира бизнис функционалноста што недвосмислено ја нуди обезбедувачот.

Овој проект е финансиран од Европската унија

ТрансакцијаИд	3	M	низа, содржи UUIDv4, се валидира според xsd:шема вредност="[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}"	КК вметнува трансакцијаИд кај МИМ заглавието во моментот кога ќе се добие повик за услуга.
Dir	3	M	низа	Правец на порака. Идентификаторот на правецот се извлекува од контекстот на пораката - дали станува збор за барање услуга или за одговор. Доколку комуникацискиот клиент оформи SOAP/МИМ барање, правецот се поставува на „Барање“. Доколку комуникацискиот клиент оформи порака со одговор, правецот се поставува на „Одговор“. Доколку станува збор за асинхрона комуникација, повикот до ДобијПоракапрекуТрансакцијаИд ќе го постави правецот на „Одговор“. Повик до ОбјавиПорака ќе го постави правецот во зависност од: • добиената вредност на Dir во МИМ заглавието; • параметарот за повик „Dir“.

Овој проект е финансиран од Европската унија

повикТип	З	М	набројување што содржи „асинхрон“, „синхрон“	Првото ниво на МИМ ќе ја поддржи само синхроната комуникација на комуникацискиот слој.
јавенКлуч	З	О	низа	КК мора да вметне јавен клуч на субјект којшто повикува некаква услуга.
Статус	А	М	низа	Статусот на преносот треба да се добие од основната технологија за пренос. Во случај на https-Пренос ова е http статусниот код.
Порака	К	О	xml	Корпусот на одговорот со основниот пакет на податоци за пренос (payload). Одговорот на КК е да изврши потпишување и шифрирање на корпусот.
MimeType	З	О	низа според http://www.iana.org/assignments/media-types/media-types.xhtml	Mime тип на пораката. Поставувањето на mime типот зависи од спроведувањето и може да се изврши на неколку начини: 1. Буквално копирање од прилагоденото MimeType поле за МИМ заглавие, штом пораката за одговор ќе

Овој проект е финансиран од Европската унија

				се пренесе преку КК; 2. Примена на евристика којашто ќе го утврди Mime типот од корпусот на пораката[8]; 3. Со поставување од URL параметарот „MimeType“ пренесен кај бизнис услугата конфигурирана кај крајната точка на КК; 4. Добивање од средината.
Временски печат (TimeStamp)	3	M	xsd:dateTime	Временскиот печат TS во полето за МИМ заглавието е поставен на КК. Се препорачува да се поставува TS по логичното финализирање на МИМ пораката, т.е. пред потпишувањето и шифрирањето. Временскиот печат не треба да се поставува според времето на фактичката достава, туку според времето кога се

[8] http://stackoverflow.com/questions/58510/using-net-how-can-you-find-the-mime-type-of-a-file-based-on-the-file-signature

Овој проект е финансиран од Европската унија

				реализирал првиот обид за достава[9].
СтатусПорака	А	О	xsd:anyType	Види погоре. СтатусПорака не смее да биде дел од потписот на пораката.
КорелацијаИд	З	О	xsd:string	Подреден идентификатор (backend-specific identifier) за корелација на статусот на подредениот повик со повикот на системот за ИОП. Вредноста ќе биде утврдена кај КК: 1. Преку поставување на прилагоденото поле за заглавие кај ПУ, при повикување на бизнис услугата изложена кај КК; 2. Од URL параметарот „КорелацијаИд“; 3. Добивање од средината.
Потпис	З	М	xsd:string	Го содржи потписот на МИМ пораката XMLDSigserialized.

Овие полиња за МИМ заглавија мора да се вметнат кај SOAP заглавието од страна на КК што добива барање што треба да се препрати кај КС:

[9]Доколку одредена услуга кешира порака бидејќи системот-примач не одговара навремено на барањето, TS се поставува според времето кога МИМ пораката била логички склопена и зачувана кај архивата за пораки за подоцнежно доставување, а не според датумот на фактичката достава. Фактичкото време на достава ќе се регистрира кај делот за евидентирање на системот за ИОП.

Овој проект е финансиран од Европската унија

- Корисник - Идентификатор на институцијата извлечен од СООУ
- Услуга - УслугаИд како што е регистрирана во СКМ
- јавенКлуч - опционално
- ТрансакцијаИд
- Dir – за првото ниво на МИМ секогаш ќе биде „Барање“
- Временски печат
- Потпис на организацијата-барател
- Порака

Следните МИМ заглавија може веќе да се поставени кај прилагоденото МИМ заглавие по приемот кај КК, или вметнати кај МИМ заглавијата специфични за SOAP, преку копирање од параметрите за повик на веб-услуги како што ги добиле крајните точки на веб-услугите, притоа откривајќи бизнис услуги контролирани кај МИМ:

- КорелацијаИд

Следните параметри на МИМ заглавието мора да ги вметне КК по исполнувањето на барањето за услуга:

- Обезбедувач (Обезбедувачот се пополнува само на барање (КК на страната на обезбедувачот))
- Статус
- MimeType
- Dir – за првото ниво на МИМ секогаш ќе биде „Одговор“
- Временски печат
- Порака
- Потпис на организацијата што одговара

По одговорот на пораката, следните полиња за заглавија буквално ќе се копираат од оригиналното барање за порака:

- Корисник - Идентификатор на институцијата што повикува, извлечен од СООУ
- Услуга - УслугаИд како што е регистрирана во СКМ
- јавенКлуч - опционално
- ТрансакцијаИд

По конечното составување на МИМ пораката неопходно е да се калкулира потписот на пораката, и да се стави во полето на заглавието за потпис.

Параметрите за заглавија мора да се дел од потпишаната порака, освен во случаи кога станува збор за опционалниот параметар СтатусПорака којшто може динамички да се додаде надвор од МИМ заглавието (МИМдополнителноЗаглавие) (не е дел од потписот) од страна на инфраструктурата за ИОП, како што пораката поминува низ системот (спореди и со горенаведениот пример).

КриптоЗаглавие- елемент

Овој проект е финансиран од Европската унија

Во моментот, за потребите поврзани со шифрирање и дешифрирање на телото на секоја порака што содржи барање/одговор, се користи симетрично шифрирање. Со цел да се разменат клучеви за симетрично шифрирање помеѓу корисникот и обезбедувачот и обратно, се воведува КриптоЗаглавие-елемент со два елементи:

Клуч: Шифриран симетричен клуч којшто се користи за симетрично шифрирање на телото на барањето/одговорот. Оваа вредност се генерира по случаен избор за секое барање, и потоа се шифрира со користење на Јавен Клуч на примачот на пораката со RSA алгоритам. На овој начин само сопственикот на поврзаниот приватен клуч е во можност да ја дешифрира оваа вредност, и да ја искористи за дешифрирање на телото.

Иницијализирачки вектор:

За одреден таен клуч „к“, едноставна блок шифра што не користи иницијализирачки вектор го шифрира истиот влезен блок на обичен текст во истиот излезен блок на шифриран текст. Доколку постојат дупликат блокови во рамките на текот на обичниот текст, ќе се јават дупликат блокови и кај текот на шифрираниот текст. Доколку неовластени корисници имаат какви било информации во однос на структурата на блокот на обичниот текст, тие може да ги искористат тие информации да го дешифрираат познатиот блок со шифриран текст, и дури и да го добијат клучот. За да се спречи овој проблем, информациите од претходниот блок се мешаат во рамките на процесот на шифрирање на следниот блок. Според тоа, аутпутот од два идентични блокови на обичен текст е различен. Со оглед на тоа што оваа техника го користи претходниот блок за да го шифрира следниот блок, неопходен е иницијализирачки вектор за да се шифрира првиот блок на податоци.

Корпусот на барањето/одговорот е шифриран со AES (Advanced Encryption Standard - Напреден стандард за шифрирање), познат и како Rijndael.

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Воведувањето на овој механизам гарантира дека се оптимални и перформансите и големината на шифрираниот резултат.

Следи пример на КриптоЗаглавие-елементот во рамките на следната XSD шема.

МИМдополнителноЗаглавие-елемент

Следните параметри: Статус, Статус Порака, ОбезбедувачКрајнаточкаУрл, НадворешнаКрајнаточкаУрл и ВебуслугаУрл се групирани во посебна структура наречена МИМдополнителноЗаглавие. Ова се должи на фактот дека вредноста на овие полиња може да се промени додека пораката поминува низ системите за интероперабилност, и според тоа тие не се дел од дигитално потпишаната порака.

XSD шема (http://mioa.gov.mk/interop/mim/v1**)**

```
<?xmlversion="1.0"encoding="utf-8"?>
<xs:schemaxmlns="http://mioa.gov.mk/interop/mim/v1"xmlns:xs="http://www.w3.org/2001/XM
LSchema"targetNamespace="http://mioa.gov.mk/interop/mim/v1"elementFormDefault="qualifi
ed">

<xs:complexTypename="MIMHeader">
<xs:sequence>
<xs:element minOccurs="1" maxOccurs="1"name="Consumer"type="xs:string">
              <xs:simpleType>
                     <xs:restriction base="xs:string">
                            <xs:maxLength value="50" />
```


Овој проект е финансиран од Европската унија


```
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="0"name="Provider"type="xs:string">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="50" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1"name="RoutingToken"type="xs:string">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="100" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1"name="Service"type="xs:string">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="100" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1"name="ServiceMethod"type="xs:string">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:maxLength value="100" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1"name="TransactionId">
            <xs:simpleType>
                <xs:restrictionbase="xs:string">
                    <xs:patternvalue="[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-
        f0-9]{4}-[a-f0-9]{12}"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1" name="Dir">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Request" />
                    <xs:enumeration value="Response" />
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:elementname="CallType" minOccurs="1" maxOccurs="1">
            <xs:simpleType>
                <xs:restrictionbase="xs:string">
                    <xs:enumerationvalue="synchronous"/>
                    <xs:enumerationvalue="asynchronous"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
<xs:elementname="PublicKey"type="xs:string"minOccurs="0"/>

<xs:elementname="MimeType"type="xs:string"minOccurs="0">
        <xs:annotation>
        <xs:documentationxml:lang="en">
```



Овој проект е финансиран од Европската унија

```
        according to http://www.iana.org/assignments/media-types/media-types.xhtml
        </xs:documentation>
        </xs:annotation>
        </xs:element>
<xs:element minOccurs="1" maxOccurs="1"name="TimeStamp"type="xs:dateTime"/>
<xs:elementname="CorrelationId"type="xs:string"minOccurs="0"/>
<xs:element minOccurs="1" maxOccurs="1"name="Signature"type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

<xs:elementname="MIMadditionalHeader">
<xs:complexType>
<xs:sequence>
<xs:elementname="Status"type="xs:string"minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                                <xs:maxLength value="50" />
                        </xs:restriction>
                </xs:simpleType>
        </xs:element>
<xs:elementname="StatusMessage"type="xs:string"minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                                <xs:maxLength value="255" />
                        </xs:restriction>
                </xs:simpleType>
        </xs:element>

<xs:elementname="ProviderEndpointUrl"type="xs:string"minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                                <xs:maxLength value="255" />
                        </xs:restriction>
                </xs:simpleType>
        </xs:element>

<xs:elementname="ExternalEndpointUrl"type="xs:string"minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                                <xs:maxLength value="255" />
                        </xs:restriction>
                </xs:simpleType>
        </xs:element>
<xs:elementname="WebServiceUrl"type="xs:string"minOccurs="0">
                <xs:simpleType>
                        <xs:restriction base="xs:string">
                                <xs:maxLength value="255" />
                        </xs:restriction>
                </xs:simpleType>
        </xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:elementname="CryptoHeader">
<xs:complexType>
<xs:sequence>
<xs:elementname="Key"type="xs:string" minOccurs="1" maxOccurs="1" />
<xs:elementname="InitializationVector"type="xs:string" minOccurs="1" maxOccurs="1" />
```


```
<xs:elementname="FormatValue"type="xs:string" minOccurs="1" maxOccurs="1">
            <xs:simpleType>
                  <xs:restriction base="xs:string">
                        <xs:enumeration value="AES" />
                  </xs:restriction>
            </xs:simpleType>
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:elementname="MIMBody"id="MIMBody">
<xs:complexType>
<xs:sequence>
<xs:elementname="Message"type="xs:anyType"/>
</xs:sequence>
</xs:complexType>
</xs:element>
```



Овој проект е финансиран од Европската унија

9 МИМ пораки и конфигурација

9.1 Принципи и стандарди

1. МИМ корисниците на услуги и МИМ обезбедувачите на услуги мора да комуницираат преку КК.
2. КК може слободно да комуницира со КС преку примена на протокол специфичен за имплементацијата.
3. Доколку МИМ се спроведува преку SOAP, рутирањето ќе се изврши со примена на WS-Addressing (спецификација за адресирање на веб-услуги).
4. КК ќе комуницира со КС со користење на https.
5. Со цел да се заштити комуникацијата помеѓу комуникацискиот клиент и внатрешните подредени системи (ПС), се препорачува да се применат безбедносни шеми крај до крај (end-to-end). Може да се користи или шифрирање од крај до крај помеѓу КК и внатрешниот систем, или барем клиентски сертификати, со цел да се гарантира дека само сертифицирани и овластени подредени системи имаат право да го повикаат КК[10].

9.2 Контрола на пристап до услуга

Контролата на пристапот се врши преку мапирање кај организациите; кои организации се овластени да повикаат услуга обезбедена од страна на друга организација.

- Автентикацијата се врши преку потпишување на МИМ пораката со користење на приватен сертификат доделен на организацијата. Според тоа, овластениот пристап до обезбедените услуги може да се верификува преку проверка на валидноста на потписот.
- Авторизацијата опционално се поддржува и со јавен клуч. Во таков случај SOAP заглавието ќе содржи јавен клуч што опфаќа кориснички информации. Доколку е присутен, системот за ИОП ќе го логира корисникот од сертификатот. Меѓутоа, авторизацијата мора да се реализира во рамките на доменот на обезбедувачот на услугата.

Овие два механизма го опишуваат минималното ниво на автентикација и авторизација што треба да го обезбеди МИМ. За внатрешна автентикација и авторизација во рамките на системот за интероперабилност може да се поддржат дополнителни механизми.

9.2.1 Мапирање на пристапот до услугите на обезбедувачите и корисниците

Дозволите за пристап помеѓу корисникот и обезбедувачот на услугите се дефинирани кај КС. Начинот на којшто е дефинирано тоа мапирање е надвор од опсегот на МИМ, но обезбедувачите во системот за МИМ најверојатно ќе обезбедат веб-интерфејс за конфигурирање.

Пример на мапирање:

Корисник	Обезбедувач	Услуга
Институција А	Институција Б	*ДобијКомпании*
Институција А	Институција Б	*ДобијВработени*
Институција А	Институција В	*ДобијВозила*
Институција В	ExtSys1$$InstitutionX	*ДобијПодатоци*

[10] http://tools.ietf.org/rfc/rfc3280.txt

Овој проект е финансиран од Европската унија

Откако КС ќе ја добие пораката, рутирачката логика на КС ќе ја евалуира валидноста на повикот на услугата. Доколку нема конфигурирана патека помеѓу корисникот и обезбедувачот повикот ќе биде неуспешен, во спротивно тој ќе се препрати до обезбедувачот, евидентирајќи ги рутирачките параметри и МИМ параметрите за заглавие.

Рутирачките информации внатрешно се зачувуваат кај КС и индиректно се анализираат кај КК каде што се конфигурирани крајните точки на услугата, врз основа на одговор од ДобијУслуги.

За одговори на ДобијУслуги оформени од локален КС, РутирачкиТокен се состои од шема за пристап (вообичаено https) и хост називот на комуникациските клиенти за којшто било направено барањето за ДобијУслуга. Првиот дел од URL патеката го идентификува комуникацискиот клиент што е обезбедувач, којшто хостира услуга.

Пример РутирачкиТокен: cc_min5
Објаснување: Овие информации се добиваат преку повик за ДобијУслуги до КК на министерството 1. Повикот ќе ја врати адресата на локалниот КК каде што ќе се спроведат услугите како крајни точки на услугата, и содржи исто така и информации дека услугата добијАдреса ја обезбедува КК на министерството 5 (cc_min5).

Пример РутирачкиТокен: cc_ext2$$cc_min8
Објаснување: Овие информации се добиваат преку повик за ДобијУслуги до КК на министерството 1. Повикот ќе врати информации за адресата на локалниот КК каде што услугите наменети за користење ќе се спроведат како крајни точки на услугата, и содржи исто така и информации дека услугата добијАдреса ја обезбедува КК cc_ext2. Ова cc_ext2 е КК на друг систем за интероперабилност каде што во случај на повикување услуга со користење на овој РутирачкиТокен, дополнителниот токен cc_min8 може да се толкува, така што една порака може да биде уникатно идентификувана и рутирана до конечната дестинација.

9.2.2 Авторизација

МИМ архитектурата се потпира на концептот на организациска доверба, но сепак преку авторизацијата на корисници се поддржани пософистицирани нивоа на грануларност. Во таков случај SOAP заглавието ќе содржи јавен клуч што опфаќа кориснички информации. Доколку е присутен, системот за ИОП ќе го логира корисникот од сертификатот. Меѓутоа, авторизацијата мора да се реализира во рамките на доменот на обезбедувачот на услугата.

9.3 Обезбедување услуга

Обезбедувањето услуги според МИМ подразбира инсталација на КК.

- До овој КК пристап мора да има КС.
- Овој КК мора да биде во можност физички да им пристапи на откриените бизнис услуги.

Обезбедувачот може да регистрира нова услуга кај КС преку повикување на метауслугата *РегистрирајУслуга* кај КК, којшто ќе го конфигурира тоа мапирање кај КС. WSDL се објавува со адресите на крајните точки кај локалната средина (средината на обезбедувачот).

Обезбедувачот на КС на МИМ може да понуди и други начини на конфигурирање на услугите, меѓутоа ова зависи од спроведувањето и е надвор од опсегот на МИМ спецификацијата.

Овој проект е финансиран од Европската унија

9.4 Откривање на услуги

Откривањето на услугите е олеснето со метауслугите*ДобијОбезбедувачи*, *ДобијУслуги* и *ДобијУслуга*.

- *ДобијОбезбедувачи* нуди список на идентификатори што обезбедуваат барем една услуга за корисникот којшто повикува, вклучително и јавниот клуч што мора да се користи за шифрирање.
- *ДобијУслуги* ги нуди сите РутирачкиТокени за одредени обезбедувачи што се достапни за корисникот којшто повикува.

  По добивањето на повикот за ДобијУслуги на КС, тој мора да го направи следното:

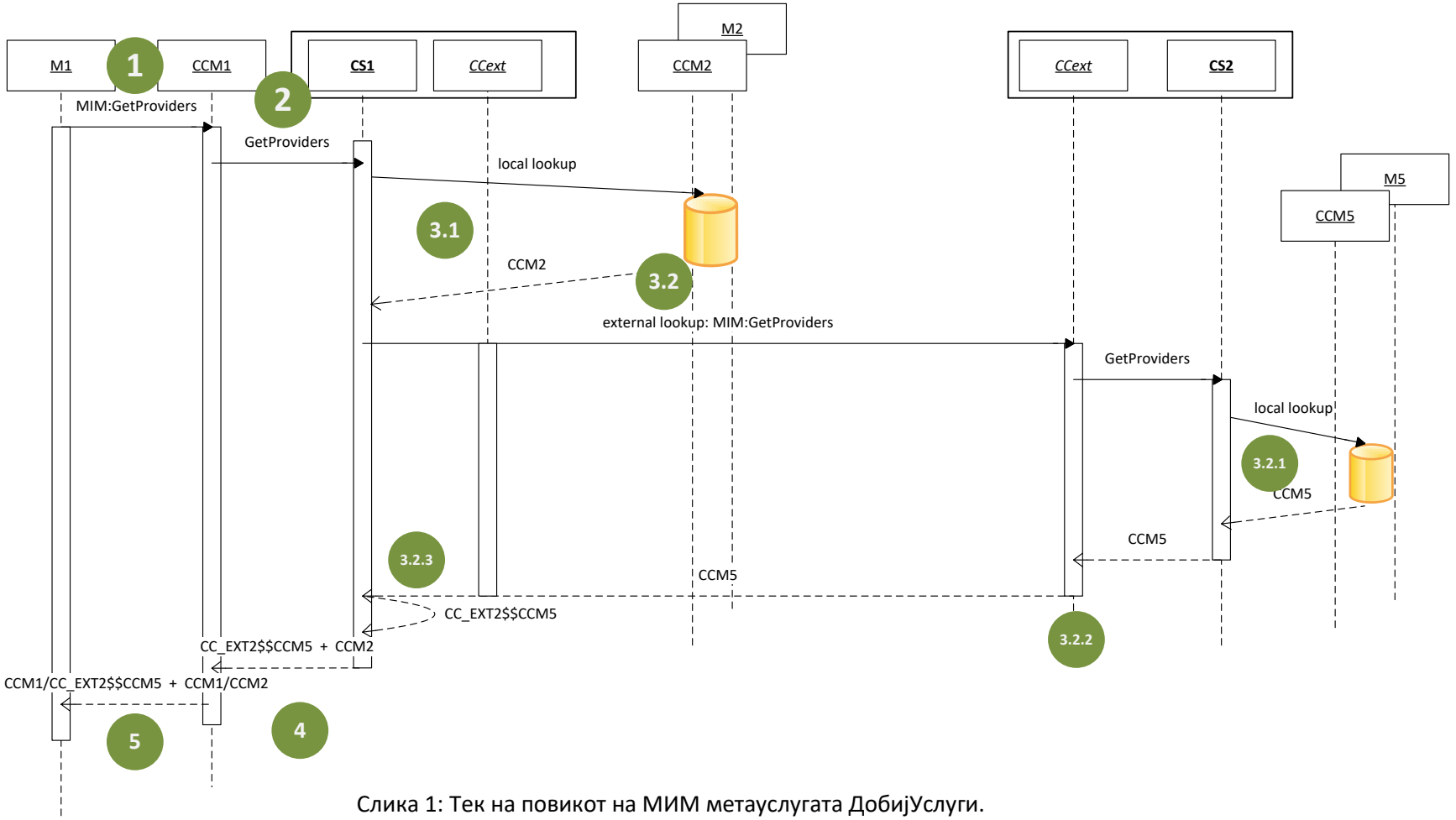
1. Да побара мапирање на услугата кај локалниот список за контрола на пристапот до услугата (СКМ); и
2. Да се повика истиот метод со којшто бил повикан и КС кај друг конфигурациски КК „CCext“ на синхрон начин. Доколку овој надворешен повик е успешен, информациите што се добиени од локалниот список за контрола на пристапот до услугата мора да се комбинираат со добиените информации од одговорот на надворешниот КК, а РутирачкиТокен до КК којшто повикува „CCorig“ мора да се спојат на следниот начин:

   a) CCorig/cc_min5/Service за информациите добиени од локалниот список за контрола на пристапот до услугата;
   b) CCorig/CCext/[InstiutionX]/Service за информациите добиени по повик за ДобијУслуги на CCext.
   Овие информации ги собира КС откако ќе ги добие одговорите на надворешниот систем за ИОП, и ќе бидат собрани за понатаму да му се одговори на КК којшто повикува. Детален опис на текот на повикот, на улогата на КС, како и на локалните и далечинските КК е претставен на Слика 1: Тек на повикот на МИМ метауслугата ДобијУслуги.

- *ДобијУслуги*ги нуди сите РутирачкиТокени за одредени обезбедувачи што се достапни за корисникот којшто повикува.
- ДобијУслуга нуди WSDL за конкретен обезбедувач и услуга.

Понудениот WSDL има адреси на крајните точки коишто укажуваат на локалниот КК, па според тоа повикувањето на тие услуги од перспектива на корисникот се реализира кај локалниот КК.

Овој проект е финансиран од Европската унија



Слика 1: Тек на повикот на МИМ метауслугата ДобијУслуги.

Овој проект е финансиран од Европската унија

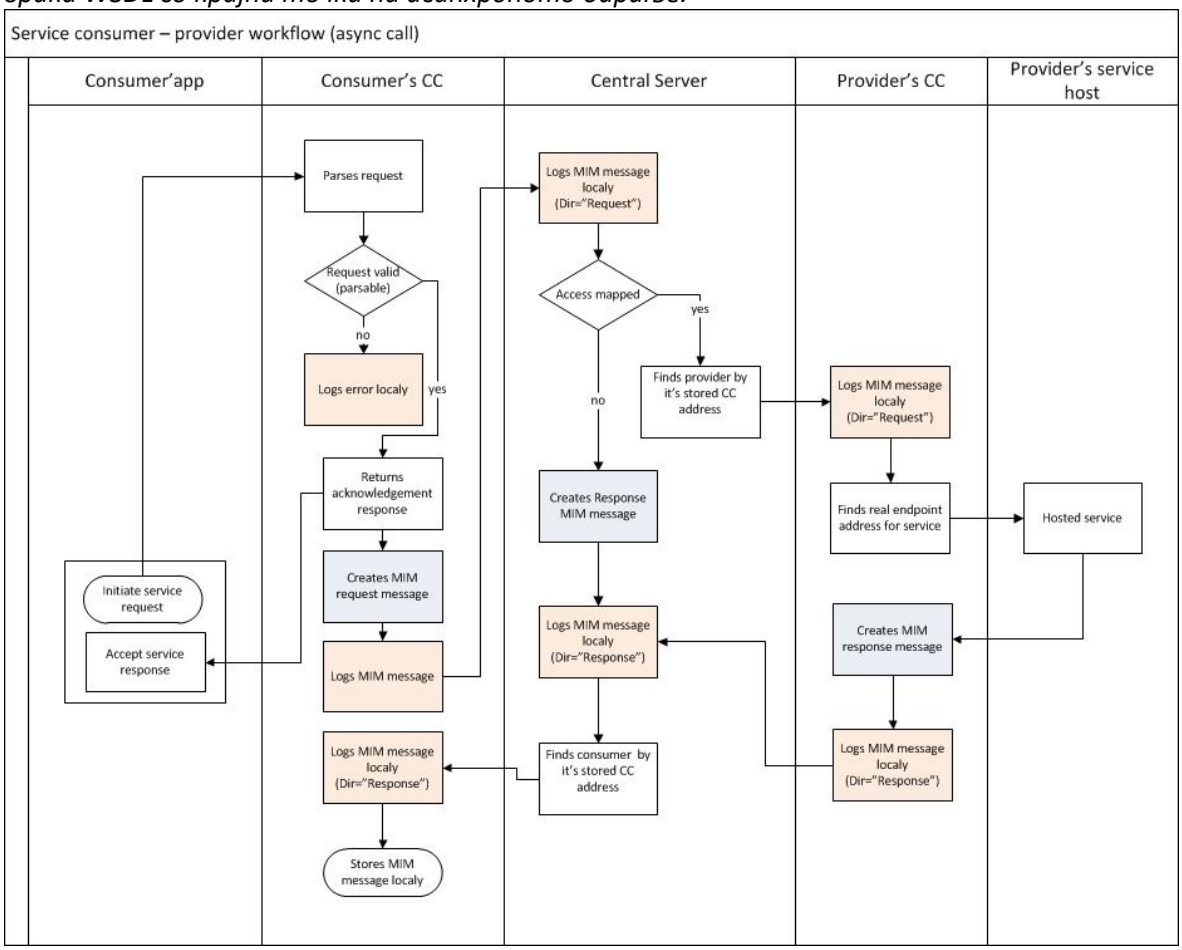
1. Институцијата М1 кај локалниот комуникациски клиент ССМ1 ја повикува метауслугата ДобијОбезбедувачи, со примена на МИМ протоколот.
2. ССМ1 ќе го повика соодветниот метод кај локалниот комуникациски сервер CS1.
3.
   3.1. CS1 ќе изврши преглед низ својата локална база на податоци. Кај претставениот пример, услугата добијЛице се обезбедува преку ССМ2 на институцијата М2. Оваа услуга се конфигурира кај CS1 со примена на панелот за конфигурација на административна услуга.
   3.2. CS1 ќе го повика методот ДобијОбезбедувачи кај својот „надворешен“ КК (*CCext*), со користење на МИМ протоколот преку *CCext* на CS2 (КС и КК од една сервисна магистрала не комуницираат директно со КС или КК на другата сервисна магистрала. Комуникацијата помеѓу двете сервисни магистрали се одвива само преку „надворешни“ КК (*CCext*) кај двете сервисни магистрали (по еден кај секоја сервисна магистрала), со што се оформува некаков вид на „мост“ помеѓу двете магистрали. *CCext* на секоја страна е „виртуелен КК“ хостиран кај КС (или апликација што работи кај КС), којшто служи како интерфејс за другата(-ите) сервисна(-и) магистрала(-и)).
      3.2.1. „Надворешниот“ CCext кај CS2 во рамките на својот комуникациски сервер CS2 ќе повика услуги коишто М1 има право да ги користи. CS2 мора да преземе мерки на претпазливост за да не го повика одново оригиналниот повикувач со повик за ДобијОбезбедувачи.
      3.2.2. Кај овој илустриран пример, „надворешниот“ комуникациски клиент *CCext* на CS2 ги враќа информациите дека комуникацискиот клиент (ССМ5) обезбедува услуга за институцијата М5.
      3.2.3. Бидејќи CS1 знае кој одговара, тој ја додава адресата на CCext пред добиените рутирачки информации.
4. Информациите на CCext/ССМ5 и ССМ2 се враќаат кај комуникацискиот клиент на М1 што повикува.
5. Добиените информации ќе се искористат за поставување на крајните точки на услугата преку повикување на ДобијУслуги (CCext/ССМ5) и ДобијУслуги (ССМ2) кај М1 за добијЛице и ДобијЛокација, што ќе пренасочи на локалниот ССМ1.

Овој проект е финансиран од Европската унија

9.5 Тек на пораките

9.5.1 Асинхрона размена на пораки (Применливо само за второто ниво на МИМ)

Кога се повикува метауслугата *ДобијУслуга* со параметар *повикТип* поставен на *асинхрон, се враќа WSDL со крајни точки на асинхроното барање.*



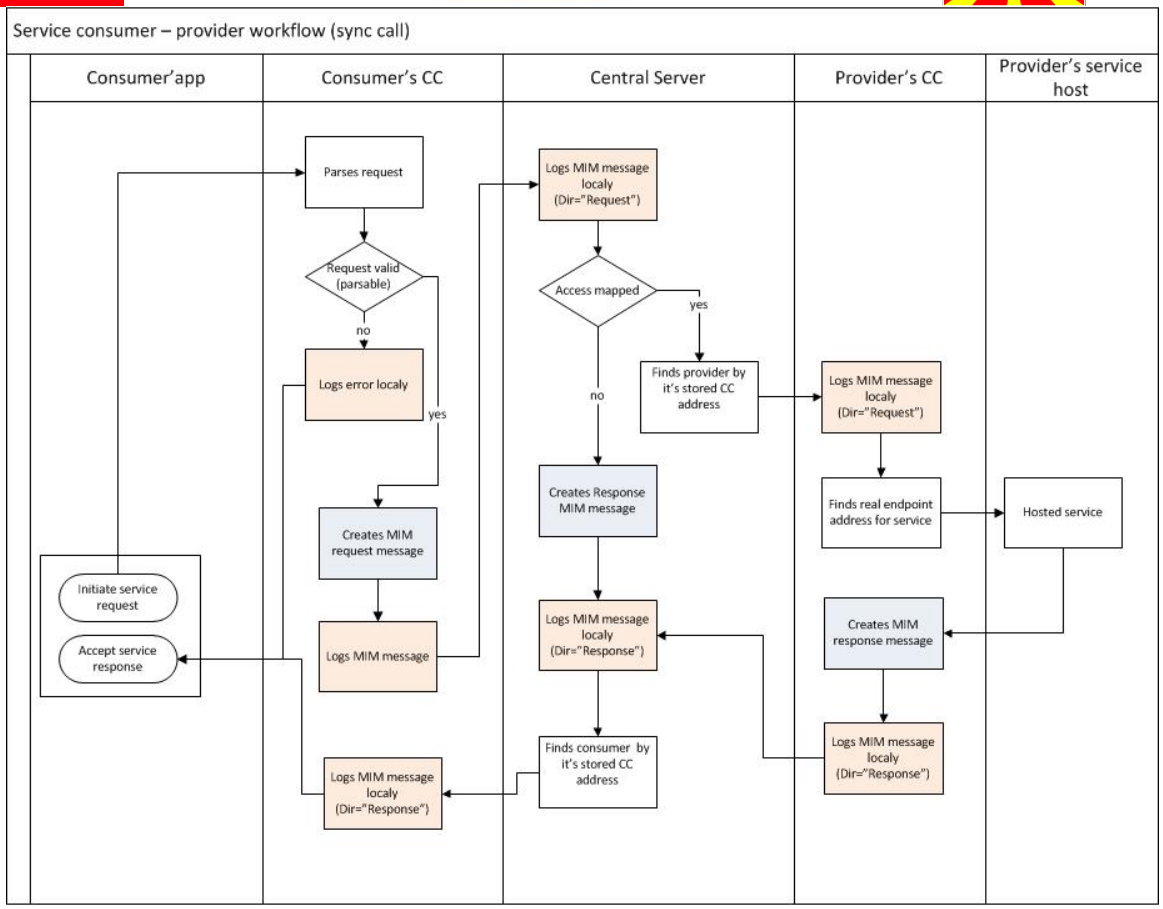
Слика 2 Тек на услугата корисник - обезбедувач кај асинхрон повик

Кога ќе се повика асинхрона услуга, КК веднаш одговара потврдувајќи го барањето со ТрансакцијаИд кај SOAP заглавието.

Кај КК на корисникот, сите пораки од асинхрони повици се собираат и зачувуваат во МИМ формат. Собраните пораки може да се искористат од МетауслугиДобијПорака и ДобијПоракаПрекуТрансакцијаИд. Овие МИМ услуги вообичаено ги повикува подреден (backend) систем (ПС).

9.5.2 Синхрона размена на пораки помеѓу институции

Овој проект е финансиран од Европската унија



Слика 3 Тек на услугата корисник - обезбедувач кај синхрон повик

9.5.3 Пример: Институција А има намера да повика сервисен метод добијКомпании што го обезбедува институција Б

Апликација којашто е хостирана кај институцијата А ја повикува услугата *КомпанијаУслуга/добијКомпании* кај својот КК (WSDL бил добиен преку метауслугата *ДобијУслуга*). Услугата се повикува во следниот формат:

https://institutionA/institutionB/CompanyService/getCompanies

каде што првиот сегмент е URL на хост називот на локалниот КК, (вториот сегмент е РутирачкиТокен што ја содржи барем локалната дестинација на КК на примателите, а третиот сегмент е УслугаИд - коишто се опционални).
SOAP пораката се објавува како HTTP корпус на барањето кај таа крајна точка на КК.

КК може да ја шифрира објавената XML порака и воедно создава структура на МИМ пораката каде што го додава следното:

- Корисник - Идентификатор на институцијата извлечен од СООУ
- Услуга - УслугаИд како што е регистрирана во СКМ
- јавенКлуч - опционално
- Корпус на пораката од фактичкото барање, доколку е потребно

Овој проект е финансиран од Европската унија

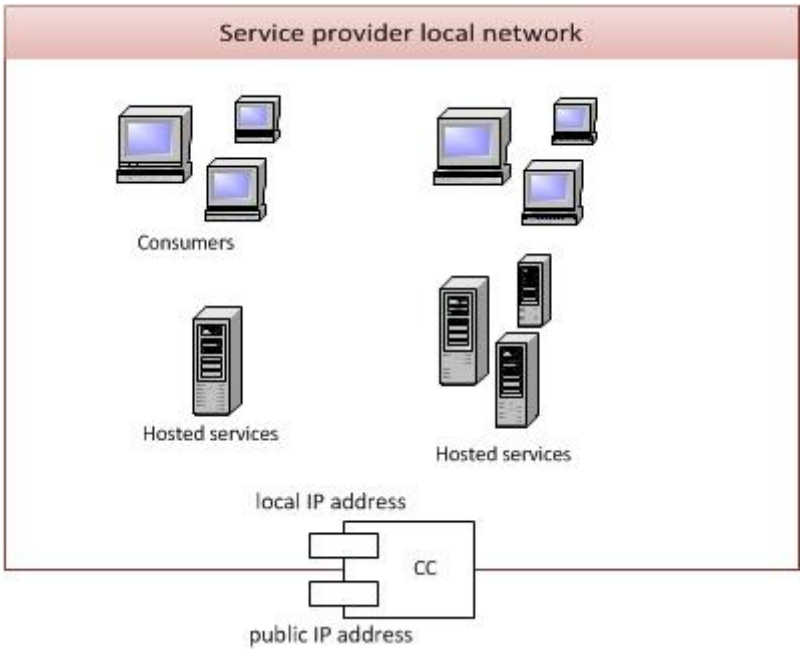
- ТрансакцијаИд
- Dir – за првото ниво на МИМ секогаш ќе биде „Барање“
- Временски печат

како и кој било друг параметар на МИМ заглавието, дефиниран како задолжителен. Потписот се пресметува и се поставува кај соодветното поле на МИМ заглавието.

МИМ пораката се препраќа кај КС којшто го евидентира барањето.

КС поседува информации за правата на пристап до услугата.

- Доколку повикот ги прекршува постоечките права на пристап од институцијата А кон институцијата Б за услугата КомпанијаУслуга/добијКомпании, обидот се евидентира како невалиден и се генерира одговор 403 во полето за МИМ Статус, корпусот на пораката содржи стандарден SOAP исклучок, а опционално дадени се и некои дополнителни информации поставени кај СтатусПорака на МИМ заглавието.
- Доколку повикот не ги прекршува правата на пристап, КС ја повикува услугата преку SOAP протоколот кај КК на институцијата Б. КК на институцијата Б добива порака од корпусот на МИМ SOAP пораката, го проверува потписот, го дешифрира корпусот на пораката, и ја објавува пораката кај внатрешниот систем што ја хостира услугата.



Слика 4: Комуникациски клиент од перспектива на обезбедувачот

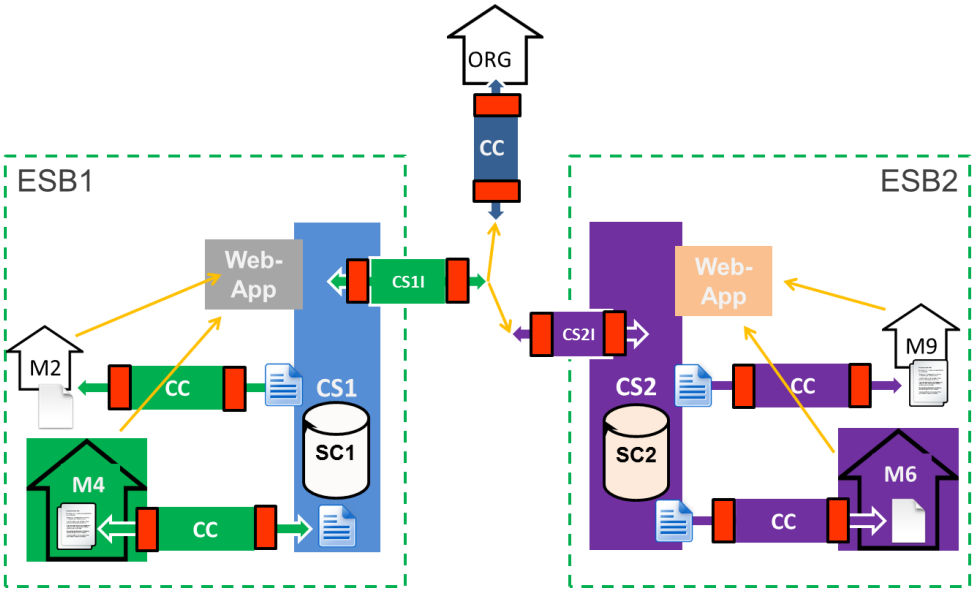
Гледано од аспект на институцијата, КК претставува единствена точка за комуникација со КС. КК пак има директен пристап до сите подредени услуги коишто или обезбедуваат или користат услуги кај МИМ системот.

Овој проект е финансиран од Европската унија

9.5.4 Пример: Интеграција со надворешни системи

Обезбедувањето и повикувањето услуги кај различни МИМ системи е овозможено поради фактот што секој КС мора да ги слуша метауслугите како што се опишани погоре, со докажување на крајната точка на КК.

Сите услуги што ги обезбедува надворешен МИМ систем ќе им бидат достапни на учесниците во рамките на една локална МИМ платформа преку РутирачкиТокен[11] којшто уникатно го идентификува далечинскиот КС, којшто пак ја проверува валидноста на мапирањето на повикот на услугата, и му ја препраќа пораката на конечниот КК во улога на корисник или обезбедувач.



Слика 5: Комуникација помеѓу различни МИМ системи

Информативно: КК како корисник и како обезбедувач на услугите

Во улога на корисник на услуга, КК хостира WSDL документи на други обезбедувачи на услуги, со цел да можат да ги користат апликации од локалната мрежа на КК. Сите WSDL крајни точки на услугата посочуваат на самиот КК.

WSDL URLs се формираат на следниот начин: https://Consumer/RoutingToken/ServiceId

1. КК управува со сите барања за својот домен и ги разложува со цел да го открие дестинацискиот КК. РутирачкиТокен се состои од ОбезбедувачИД или во случаи кога обезбедувачот е надвор од локалниот МИМ систем, го означува КК на дестинацискиот КС, а содржи и дополнителни рутирачки информации што ќе се пренесат преку КК на надворешниот систем за ИОП којшто ќе го користи надворешниот КС, со цел да ја открие патеката до конечниот КК во својот домен.
2. КК генерира *ТрансакцијаИд*
3. КК евидентира информации од МИМ заглавието

[11]Овој РутирачкиТокен се добива преку повик до ДобијОбезбедувачи.

Овој проект е финансиран од Европската унија

4. КК ја шифрира добиената SOAP порака (корпусот на барањето) со јавниот клуч на конечниот, дестинациски КК
5. КК ги создава / прикачува следните податоци кон МИМ пораката:

- Корисник - Идентификатор на институцијата извлечен од СООУ
- Услуга - УслугаИд како што е регистрирана во СКМ
- јавенКлуч - опционално
- Корпус на пораката од фактичкото барање, доколку е потребно
- ТрансакцијаИд
- Dir – за првото ниво на МИМ секогаш ќе биде „Барање“
- Временски печат
- КК го пресметува Потписот и го поставува кај соодветното поле на МИМ заглавието

6. КК ја препраќа пораката до КС
7. КК чека одговор и го препраќа тој одговор до испраќачот на барањето (од точка 1).

Во случај кога КК самиот ја зачувал оригиналната крајна точка за да обезбеди услуга од својата мрежа, повикот како обезбедувач на услуга би го имал следниот тек на информациите:

1. КК го проверува потписот на добиената порака и го дешифрира корпусот на пораката.
2. КК ги евидентира параметрите од МИМ заглавието.
3. КК ја добива оригиналната крајна точка од локална архива за извлечена услуга.
4. КК го испраќа POST барањето до оригиналната крајна точка.
5. Одговорот е шифриран со јавниот клуч на КК на корисникот.
6. Откако апликацијата успешно ќе одговори, КК создава нова МИМ порака и кај неа ги копира параметрите за барање на оригиналното заглавие, го додава mime типот на одговорот, го менува Dir во „Одговор“, и го шифрира одговорот на пораката. Потоа КК ја враќа направената МИМ порака кај КС.

Овој проект е финансиран од Европската унија