Постапки при оспособување нов сервер во улога на институција во Интероп

Во случај на потреба од оспособување на нова машина како учесник во Интероп, потребно е да се направат соодветни подготовки и подесувања пред да се стартува и да се очекува функционалност на системот.

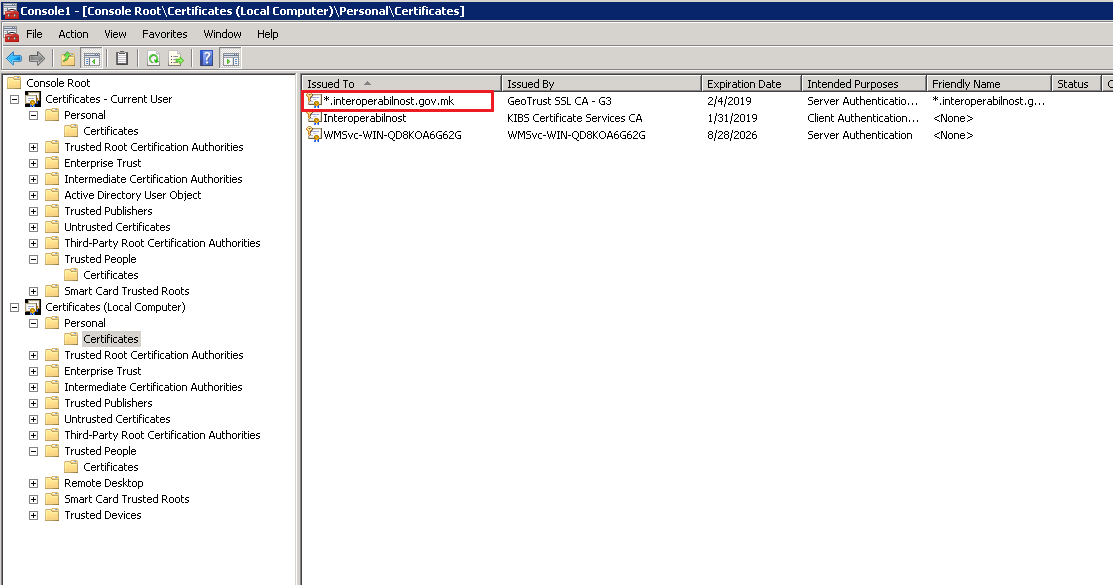
## IIS, .NET Framework, SQL Server

1. Инсталирање на IIS со сите features комплетно
2. Инсталирање на Features .NET Frameword 3.5.1 заедно со Features WCF Activation(full) на самата машина
3. Инсталирање на .NET 4.5.2
4. Инсталирање на SQL Server 2008 R2 SP2 Express

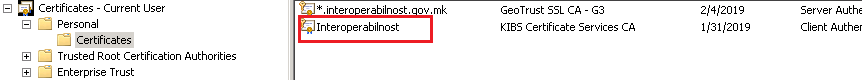
## Серверски и клиентски сертификати

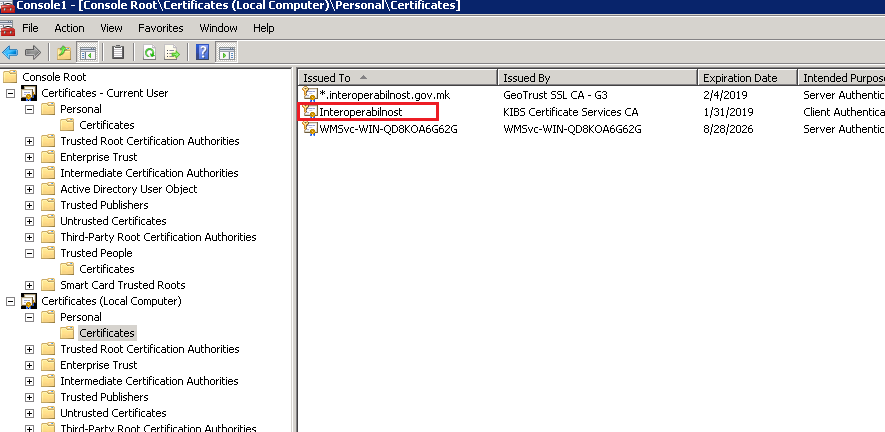
1. Тестната и продукциската околина во Интероп, во однос на порталот и апликацијата која е поврзана со порталот (WebApi), се поставени на https binding во IIS и истите користат Trusted SSL сертификат \*.interoperabilnost.gov.mk.

SSL - от \*.interoperabilnost.gov.mk треба да го има во Manage certificates (mmc), во Local computer -> Personal



1. Поставување на EPotpis2.crl CRL листата на самата машина. Десен клик на фајлот->Install CRL
2. Поставување на сертификатот UserCU.pfx на C://
3. Постојат Verba S1 сертификати за потпишување на MIM пораката која патува низ Интероп и истите треба да се постават во Manage certificates (mmc), Local computer->Personal и во Current User->Personal

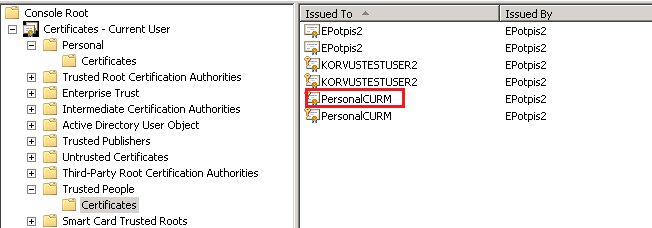


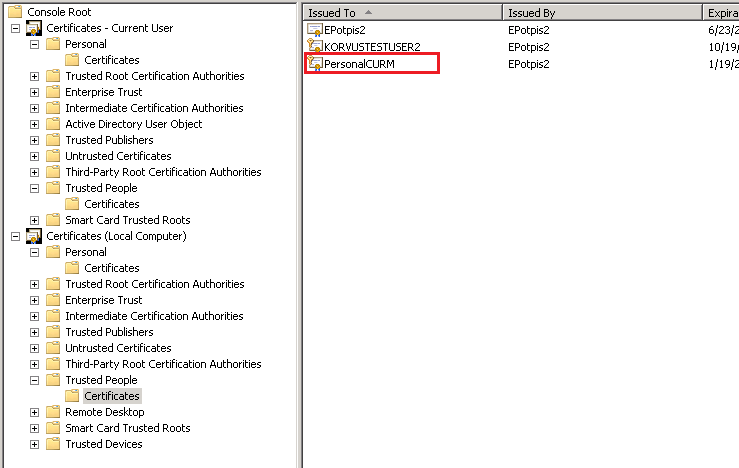


Притоа во Local computer->Personal на сертификатот десен клик->Manage private keys, и постави сите корисници да ги имаат сите привилегии и додади го IIS user-от (името на машината\IIS\_IUSRS) да ги има сите привилегии.

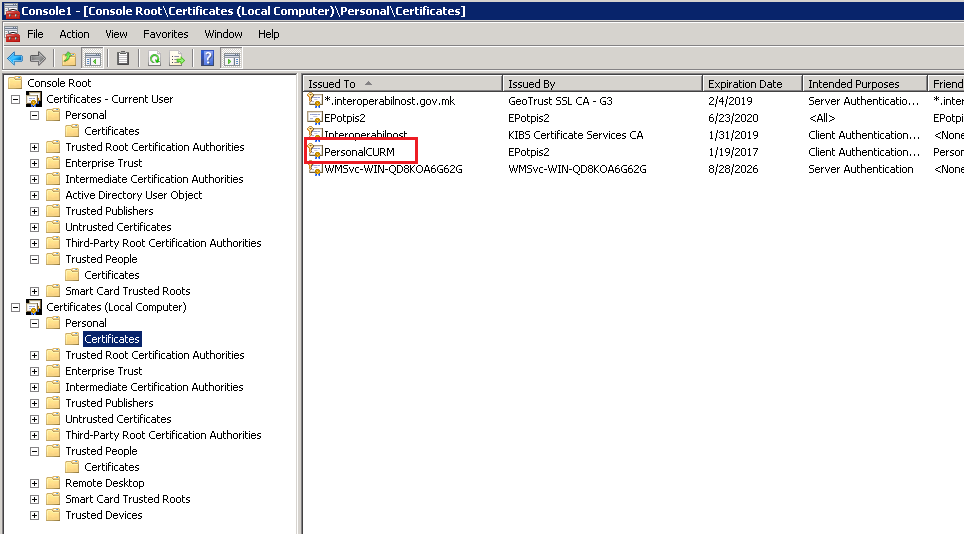
1. Постојат и Verba S1 сертификати за најавување на порталот и тие ги нарекуваме Personal Verba S1. Секоја институција си има свој Personal Verba S1 сертификат.

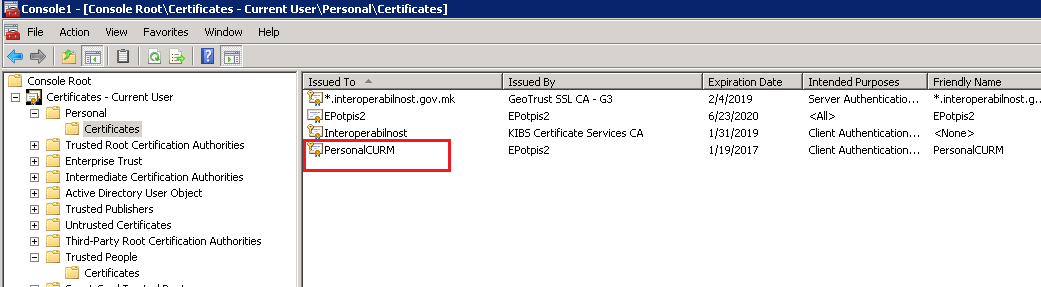
Тие треба да бидат поставени во Local computer->Trusted People и во Current User-> Trusted People





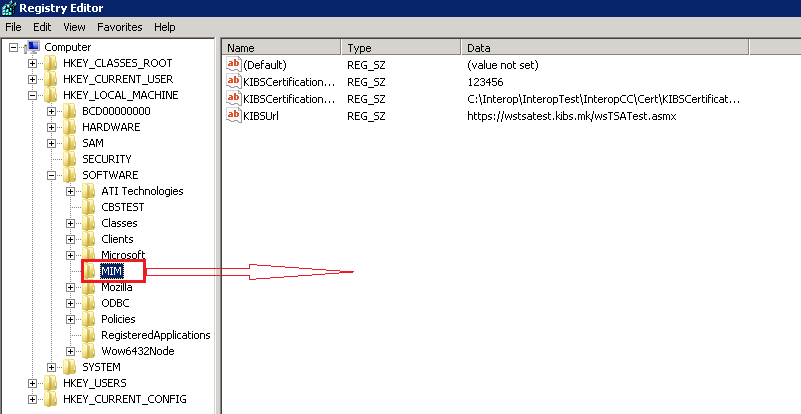
Personal Verba S1 сертификатот за најава треба да биде поставен и во Local computer->Personal и во Current User->Personal





## Сетирање поставки за читање на сертификат кој ќе биде користен за КИБС сервисот

1. Се отвара regedit.exe
2. Во HKEY\_LOCAL\_MACHINE -> SOFTWARE се креира нов KEY со назив MIM



Во него се креираат три String Value и тоа:

* Со назив KIBSUrl и вредност <https://wstsatest.kibs.mk/wsTSATest.asmx>
* Со назив KIBSCertificationPath и вредност на пат до Верба С1 сертификатот кој ќе се користи за потпишување на МИМ пораката (пример: C:\Interop\InteropTest\InteropCC\Cert\KIBSCertificate\TestServise1\_VerbaS1MK\_IE10.pfx) и за автентицирање пред сервисот на КИБС
* Со назив KIBSCertificationPassword и вредност на лозинка на самиот сертификат кој ќе се користи за потпишување на МИМ пораката и за автентицирање пред сервисот на КИБС

1. Во HKEY\_LOCAL\_MACHINE ->Wow6432Node се креира нов KEY со назив MIM

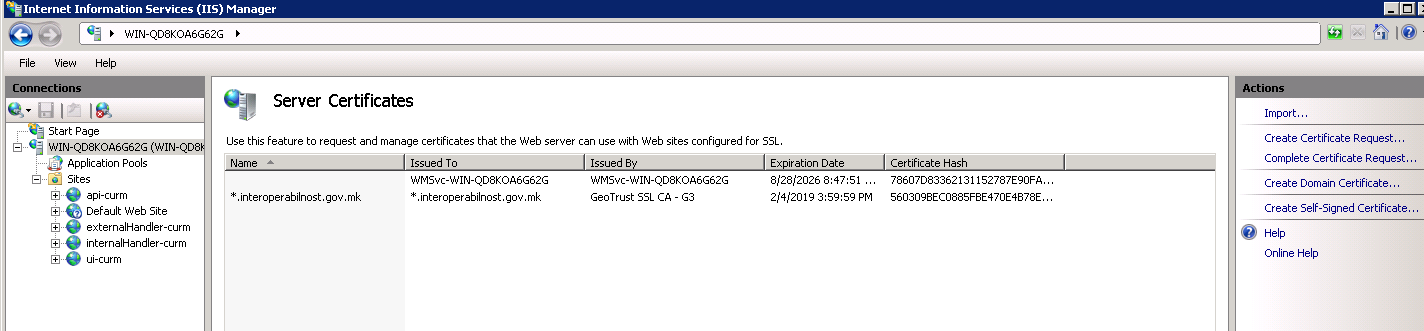
Во него се креираат три String Value и тоа:

* Со назив KIBSUrl и вредност <https://wstsatest.kibs.mk/wsTSATest.asmx>
* Со назив KIBSCertificationPath и вредност на пат до Верба С1 сертификатот кој ќе се користи за потпишување на МИМ пораката (пример: C:\Interop\InteropTest\InteropCC\Cert\KIBSCertificate\TestServise1\_VerbaS1MK\_IE10.pfx) и за автентицирање пред сервисот на КИБС
* Со назив KIBSCertificationPassword и вредност на лозинка на самиот сертификат кој ќе се користи за потпишување на МИМ пораката и за автентицирање пред сервисот на КИБС

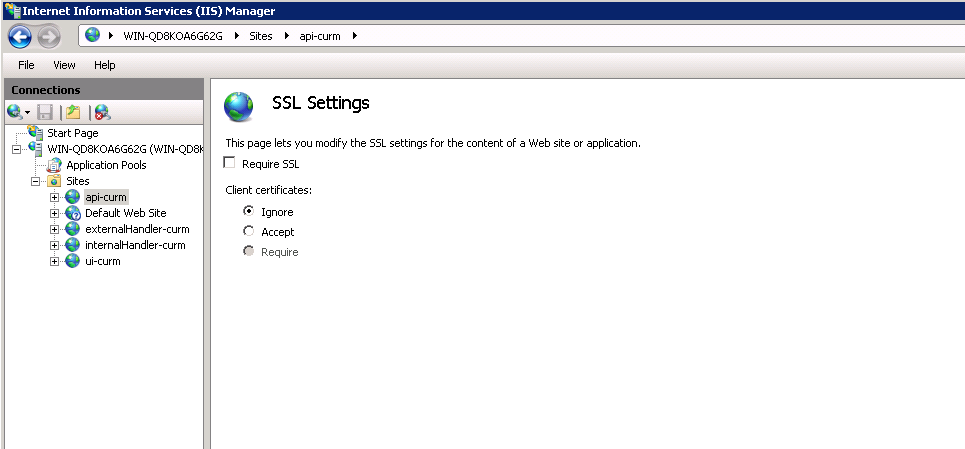
Притоа може да се провери дали автентикацијата пред сервисот на КИБС е успешна со тоа што во пребарувач се импортира сертификатот кој ќе се користи, се отвара линкот на КИБС <https://wstsatest.kibs.mk/wsTSATest.asmx> и би требало доколку сертификатот е во ред, да ги видиме методите од сервисот кои ни се достапни за користење.

## Креирање на потребните апликации во IIS и сетирање серверски сертификат SSL во IIS

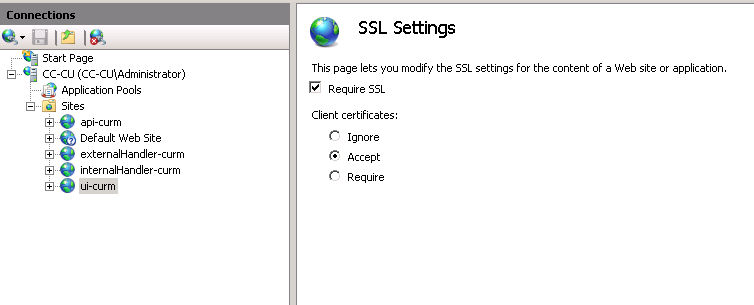
1. Поставување на SSL-от \*.interoperabilnost.gov.mk во IIS, во делот Server Certificates, за да може потоа истиот да се постави во Bindings на апликациите api и ui во IIS



1. При креирање на апликациите во IIS, апликацијата api треба да има binding на https со соодветна порта, и избран SSL \*.interoperabilnost.gov.mk, како и треба да има SSL поставки во делот на IIS -> SSL Settings, Client certificates->Ignore



1. При креирање на апликациите во IIS, апликацијата ui треба да има binding на https со соодветна порта, и избран SSL \*.interoperabilnost.gov.mk , како и треба да има SSL поставки во делот SSL Settings->Require SSL, Client certificates->Accept



1. При креирање на апликациите во IIS, апликацијата externalHandler треба да има binding на http
2. При креирање на апликациите во IIS, апликацијата internalHandler треба да има binding на http
3. Сите application pools во IIS треба да се на .NET Framework v4.0.30319. При креирање на апликацијата секој pool во IIS автоматски се креира со име исто како и самата апликација, но by default се поставува на .NET Framework v2.0
4. Постави ги сите application pools во IIS да имаат сетирано Load User Profile -> True
5. На самата машина, во host фајлот постави ги апликациите api и ui со соодветно IP на самата машина на која се хостирани апликациите