УПАТСТВО

ЗА АКТИВИРАЊЕ И ИНСТАЛАЦИЈА НА ДИГИТАЛЕН СЕРТИФИКАТ НА GEMALTO IDPRIME.NET ТОКЕН СО КОРИСТЕЊЕ НА INTERNET EXPLORER

СПОДЕЛИ ДОЖИВУВАЊА

СОДРЖИНА

Воведни препораки 3
Активирање на дигитален сертификат 4
Нагодување на ActiveX контроли и Trusted Sites 4
Поставување на коренската (root) датотека на Trusted сертификати 8
Активирање на Вашиот сертификат на десктоп компјутер /лаптоп 11
Експортирање на дигиталниот сертификат во фајл 16
Импортирање дигитален сертификат од фајл на токен од тип GEMALTO IDPRIME.NET .. 21
Инсталирање драјвери за токен Gemalto.NET – за Windows 7 и понови верзии на оперативен систем 21
Инсталирање на vSEC:SMC апликацијата 22
Импортирање на сертификатот на токен со vSEC:SMC апликацијата 24
Инсталација на PKCS11 (за апликација на УЈП) 26

ВОВЕДНИ ПРЕПОРАКИ

Ова упатство е наменето за сите корисници на квалификуван дигитален сертификат, **Доверливост KS+** и/или **Доверливост KSN+.**

Ги опишува чекорите за активирање и инсталација на сертификатот на десктоп компјутер и/или лаптоп и негово импортирање на Gemalto IDPRIME.NET токен, во понатамошниот текст референциран како Gemalto.NET токен.

Ова упатство претставува комбинација од:
А. Упатство за активирање на сертификат на десктоп компјутер/ лаптоп за Internet Explorer
Б. Упатство за импорт на активиран сертификат на токен

Можете редоследно да ги следите тие 2 упатства, наместо ова упатство.

Препораката за активирање на сертификатот на компјутер/лаптоп, а потоа негово префрлање на токен од тип Gemalto.NET, доаѓа од препораките на производителот на Gemalto IDPRIME.NET токен од 19.10.2017 година **Gemalto Bulletin Number** - [20171018].

Македонски Телеком препорачува чување на сертификатот исклучиво на токен, односно бришење на сертификатот од компјутерот по неговото префрлање на токен, од безбедносни причини и спречување евентуална злоупотреба на сертификатот.

ПРЕДУСЛОВ :

За инсталација и активирање на дигиталниот сертификат, со склучување на договорот за користење на дигитален сертификат, Македонски Телеком ви доставува авторизацискиот код и референтниот број. Референтниот број го добивате преку е-пошта, додека авторизацискиот код го добивате по SMS.

ВАЖНО!

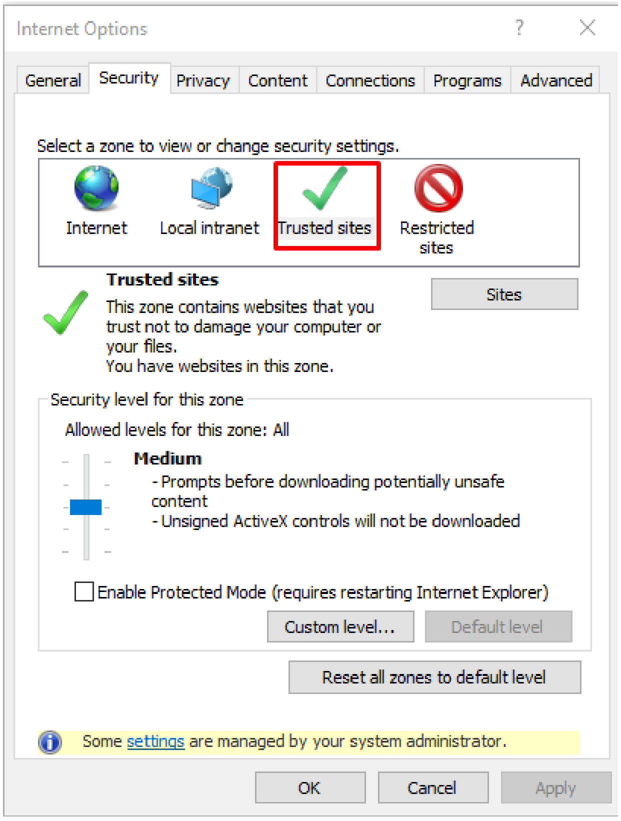
1. Времетрањето на авторизацискиот код и референтниот број е 30 дена од издавањето.
2. За инсталација и активирање потребно е да го користите **исклучиво Internet Explorer прелистувачот**
3. **Запомнете ја лозинката** потребна при користење на сертифкатот, а која ја креирате при повлекување на Вашиот сертификат.
4. Експортираниот сертификат зачувајте го на безбеден медиум (токен), во случај на дефект на компјутерот или форматирање.

АКТИВИРАЊЕ НА ДИГИТАЛЕН СЕРТИФИКАТ

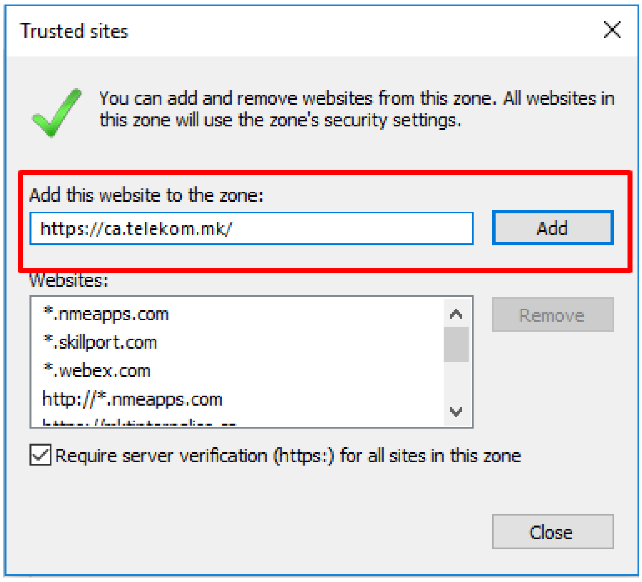
За да започнете со процесот на активирање на дигиталниот сертификат, отворете го **Internet Explorer** прелистувачот и внесете ја адресата: https://ca.telekom.mk. За успешно активирање на сертификатот, потребно е https://ca.telekom.mk да биде ставен во Trusted Sites и сите ActiveX контроли да бидат поставени на Enable.

НАГОДУВАЊЕ НА ACTIVEX КОНТРОЛИ И TRUSTED SITES

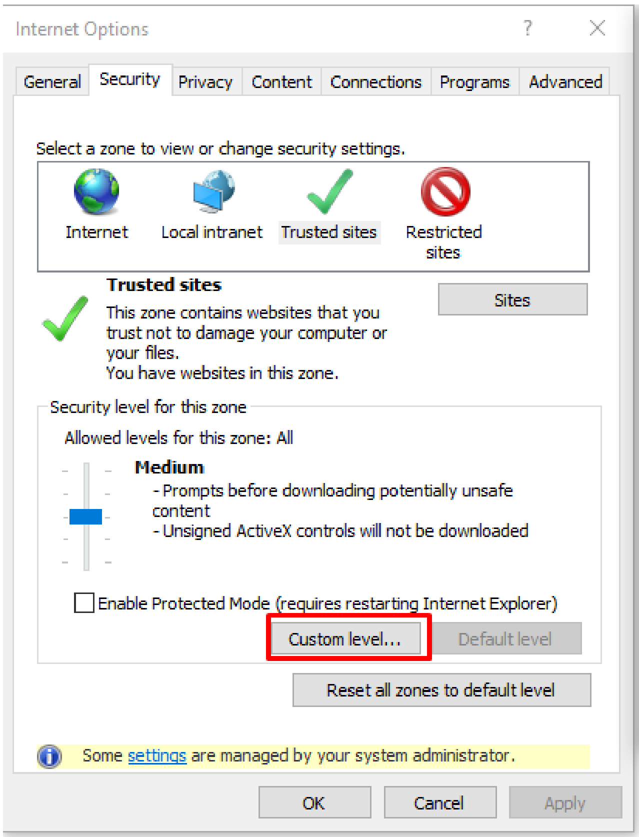
А. За да ја додадете веб-страницата https://ca.telekom.mk во Trusted Sites на Internet Explorer, во горниот десен агол од прелистувачот, кликнете на копчето што означува Алатки за подесување- Tools ( ), изберете Internet options, и кликнете на табот Security.

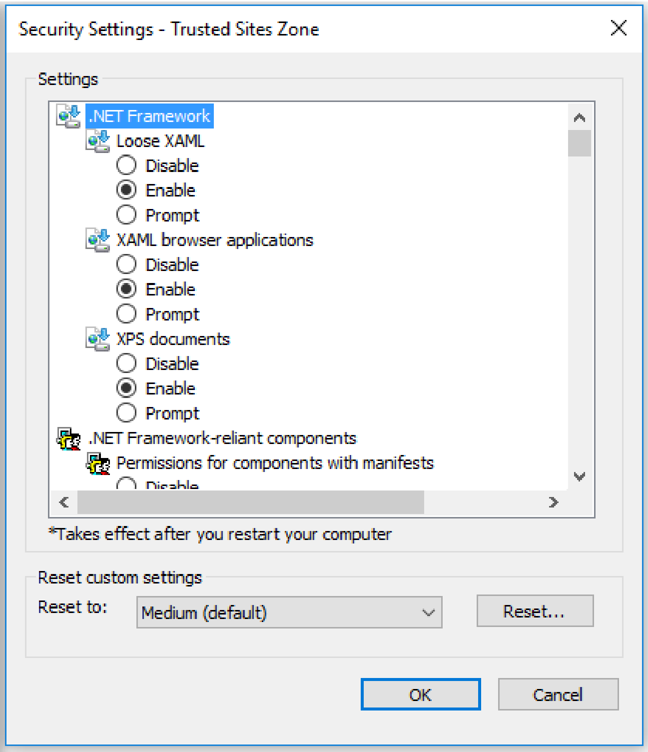


Б. Изберете Trusted sites и кликнете на копчето Sites. Во новоотворениот прозор во полето Add this website to the zone, внесете https://ca.telekom.mk и кликнете Add. По додавањето на адресата кликенете Close.



В. Продолжете со работа во прозорот Internet Options и под табот Security кликнете на Custom Level во долниот дел од прозорот (Trusted sites треба да остане избрано). Ќе се отвори прозорецот Security Settings – Trusted Sites Zone со листа на опции.

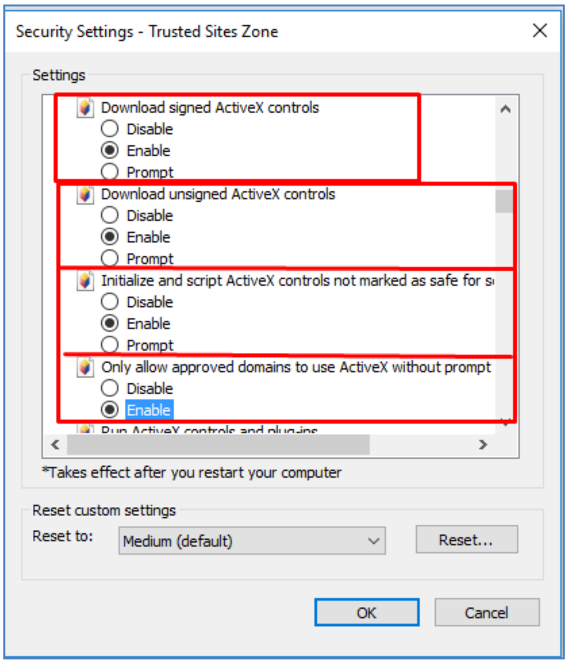


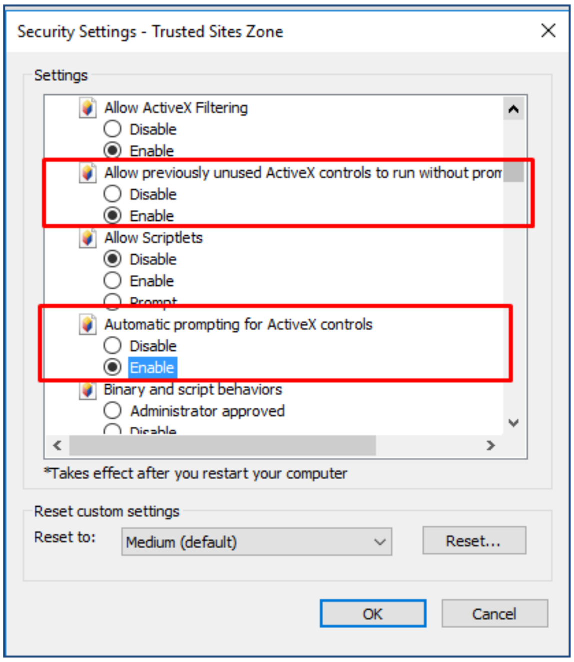


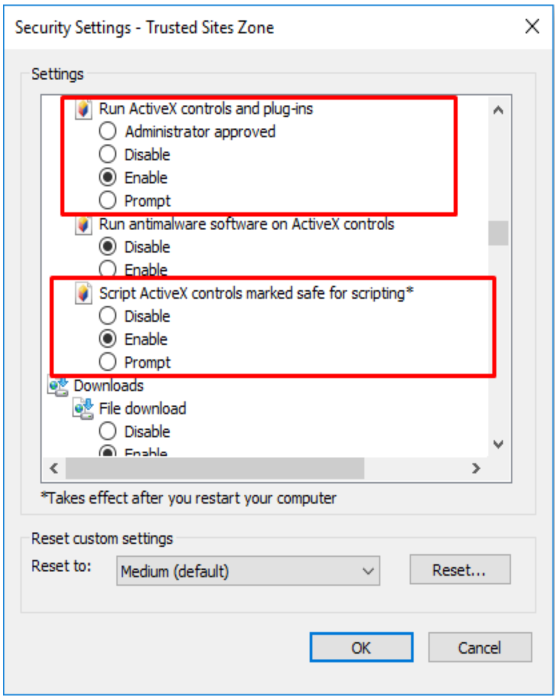
Г. Од дадената листа, следниве ставки поставете ги на Enable:

- ActiveX controls an plug-ins, Allow previously unused ActiveX controls to run without prompt

- Automatic prompting for ActiveX controls
- Download signed ActiveX controls
- Download unsigned ActiveX controls
- Initialize and script ActiveX controls not marked as safe for scripting
- Only allow approved domains to use ActiveX without prompt
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting



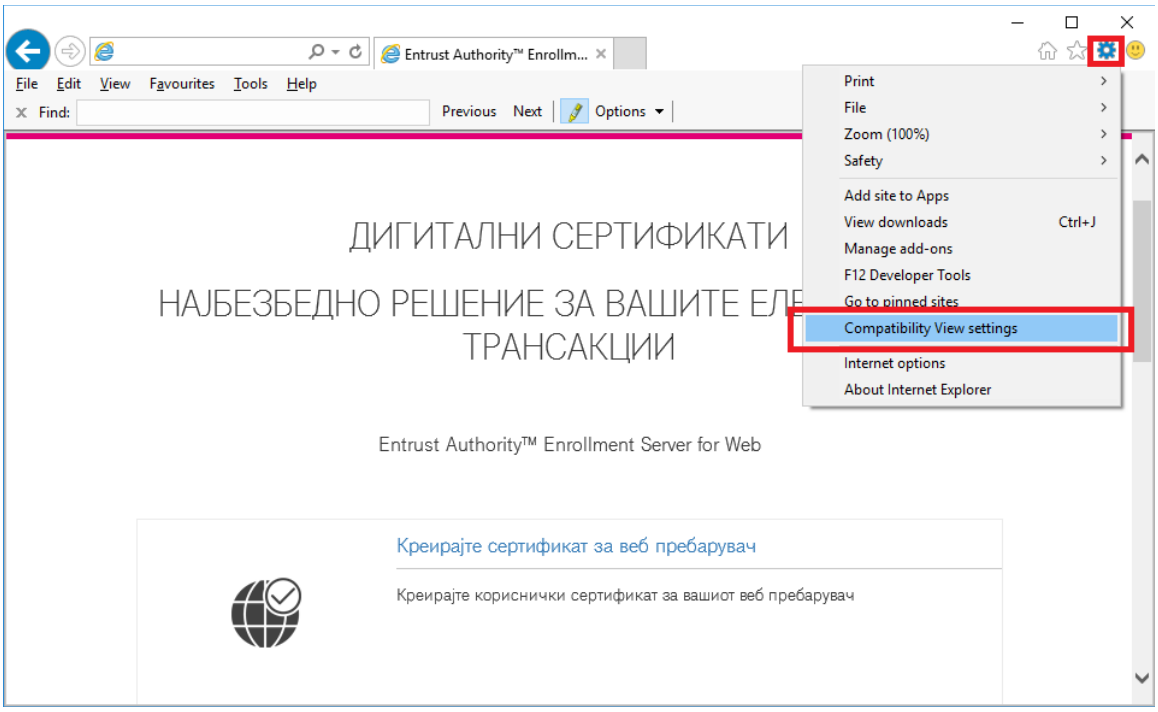




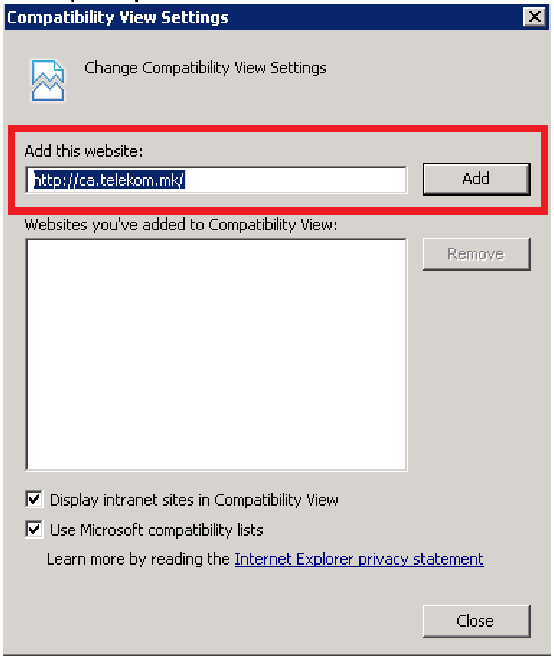
Д. Кликнете двапати на OK за да се затворат прозорите.

Следните два чекора (Ѓ и Е) направите ги само доколку го користите прелистувачот Internet Explorer верзија 11.

Ѓ. Во горниот десен агол од прозорецот во прелистувачот Internet Explorer 11, кликнете на копчето што означува Алатки за подесување (Tools) и одберете: Compatibility View settings:



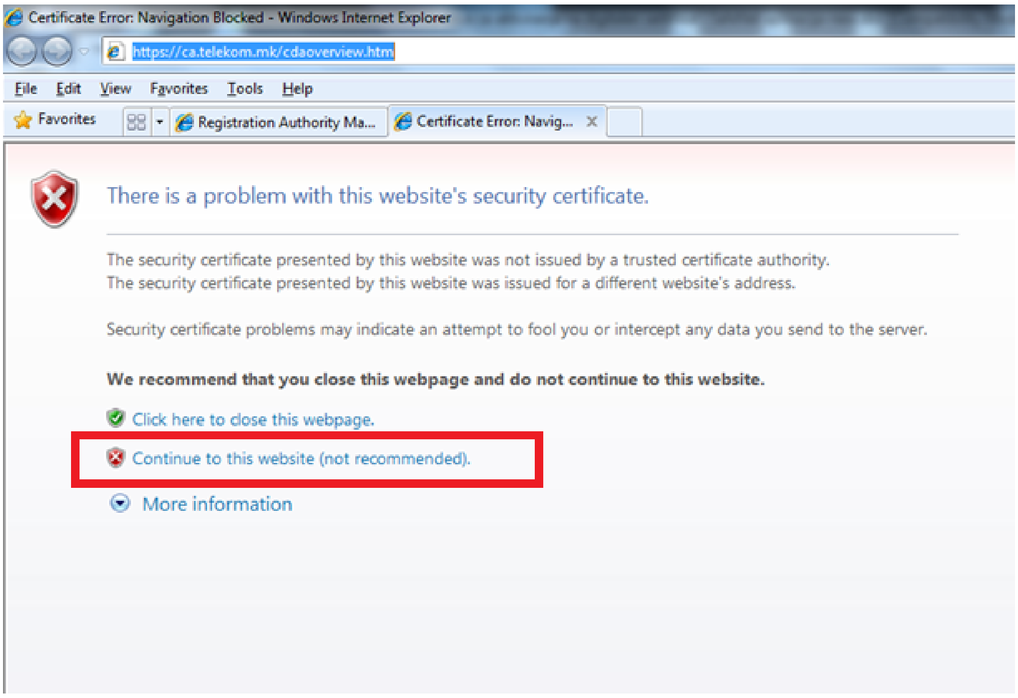
Е. страната https://ca.telekom.mkДодадете ја во празното поле со притискање на копчето **Add**, а потоа затворетего прозорот со кликање на копчето **Close.**



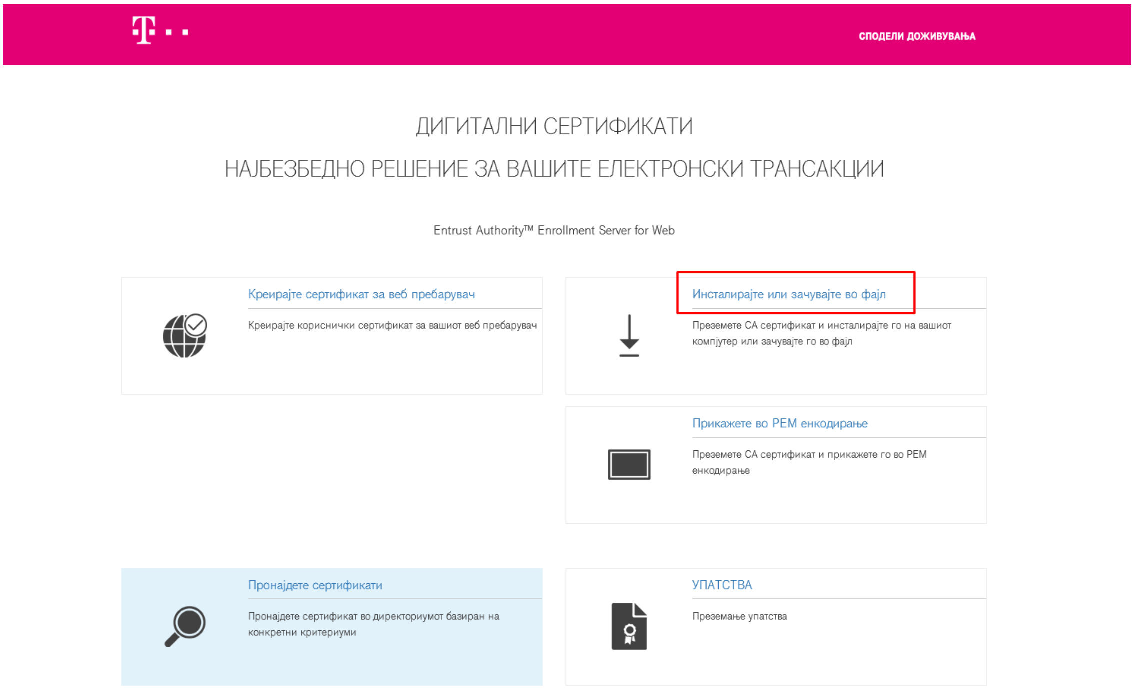
ПОСТАВУВАЊЕ НА КОРЕНСКАТА (ROOT) ДАТОТЕКА НА TRUSTED СЕРТИФИКАТИ

А. Отворете го прелистувачот Internet Explorer и внесете ја адресата: https://ca.telekom.mk.

Б. Изберете ја опцијата Continue to this website (not recommended).

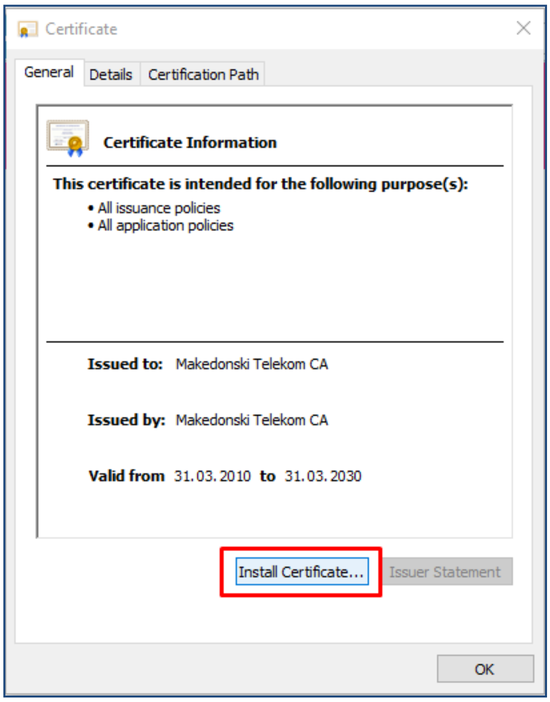


В. Од десната страна на прозорот изберете Инсталирај или Зачувајте во фајл.

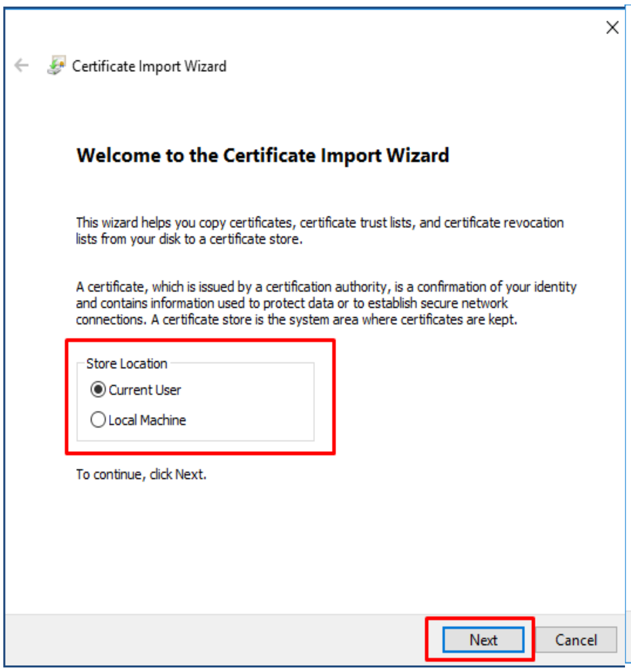


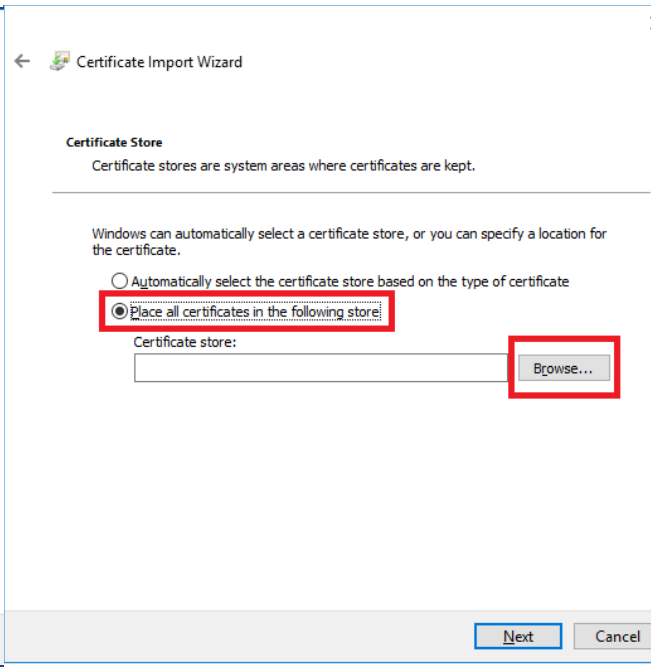
Г. Симнатиот фајл (сертификат) отворете го со кликање на копчето Open.

Д. Инсталирајте го сертификатот со избор на Instal Certificate.

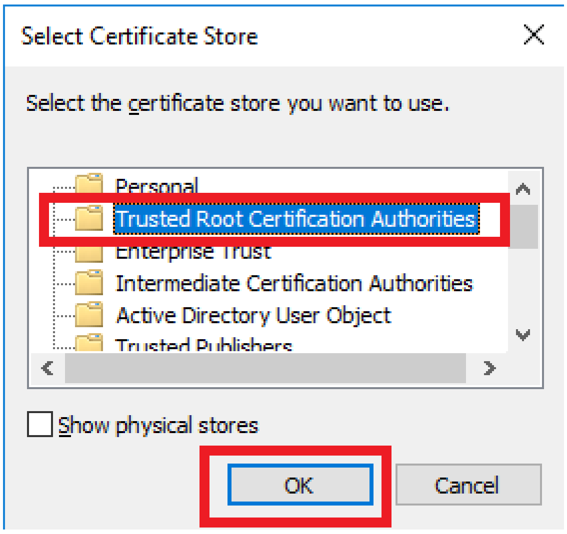


Ѓ. Одберете „Current User“, а на следниот чекор „Place all certificates in the following store“ .

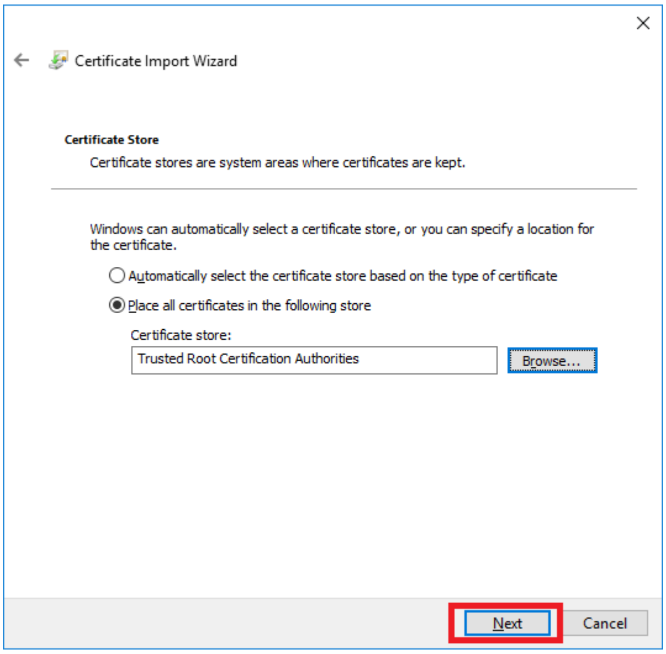


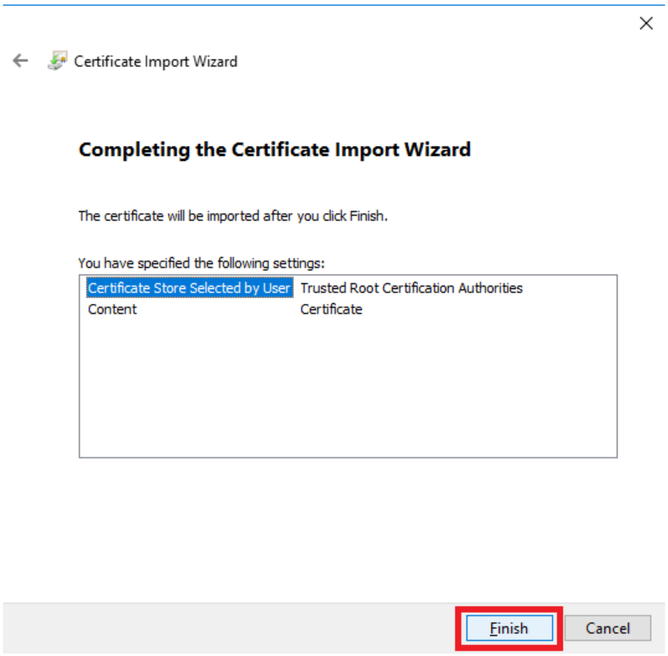


Е. Одберете „Trusted Root Certification Authorities“ и кликнете „ОК“

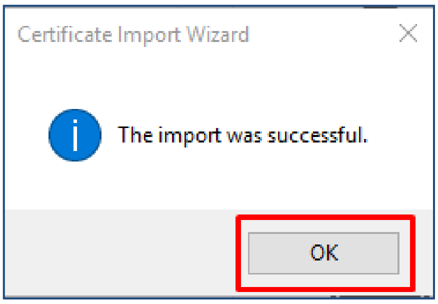


Ж. Кликнете на „Next“ па „Finish“



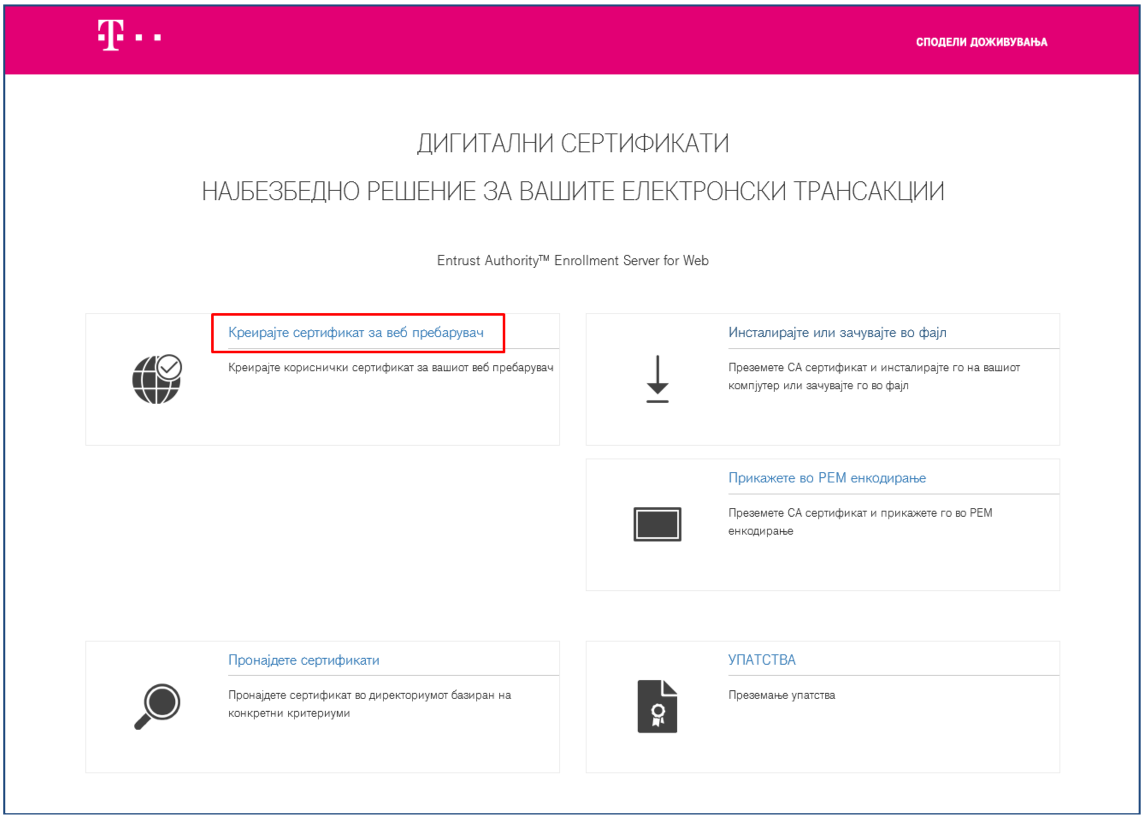


З. По успешно импортирање на root сертификатот, кликнете Finish па OK.

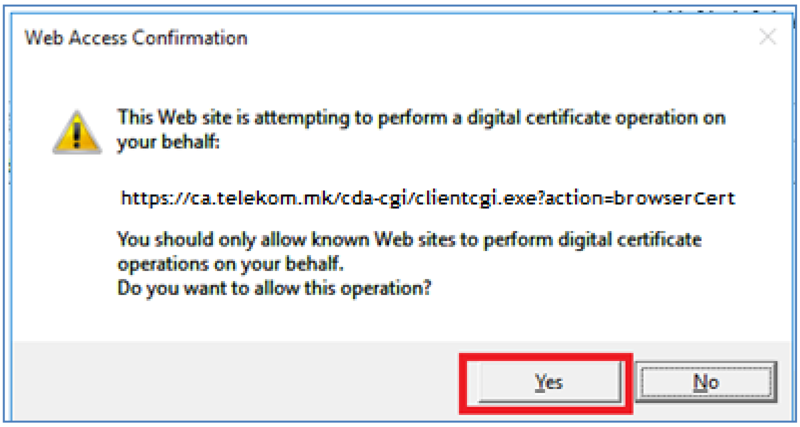


АКТИВИРАЊЕ НА ВАШИОТ СЕРТИФИКАТ НА ДЕСКТОП КОМПЈУТЕР /ЛАПТОП

Внесете ја адресата https://ca.telekom.mk во веб прелистувач. Од дадените опции изберете ја опцијата “Креирај сертификат за веб пребарувач”.



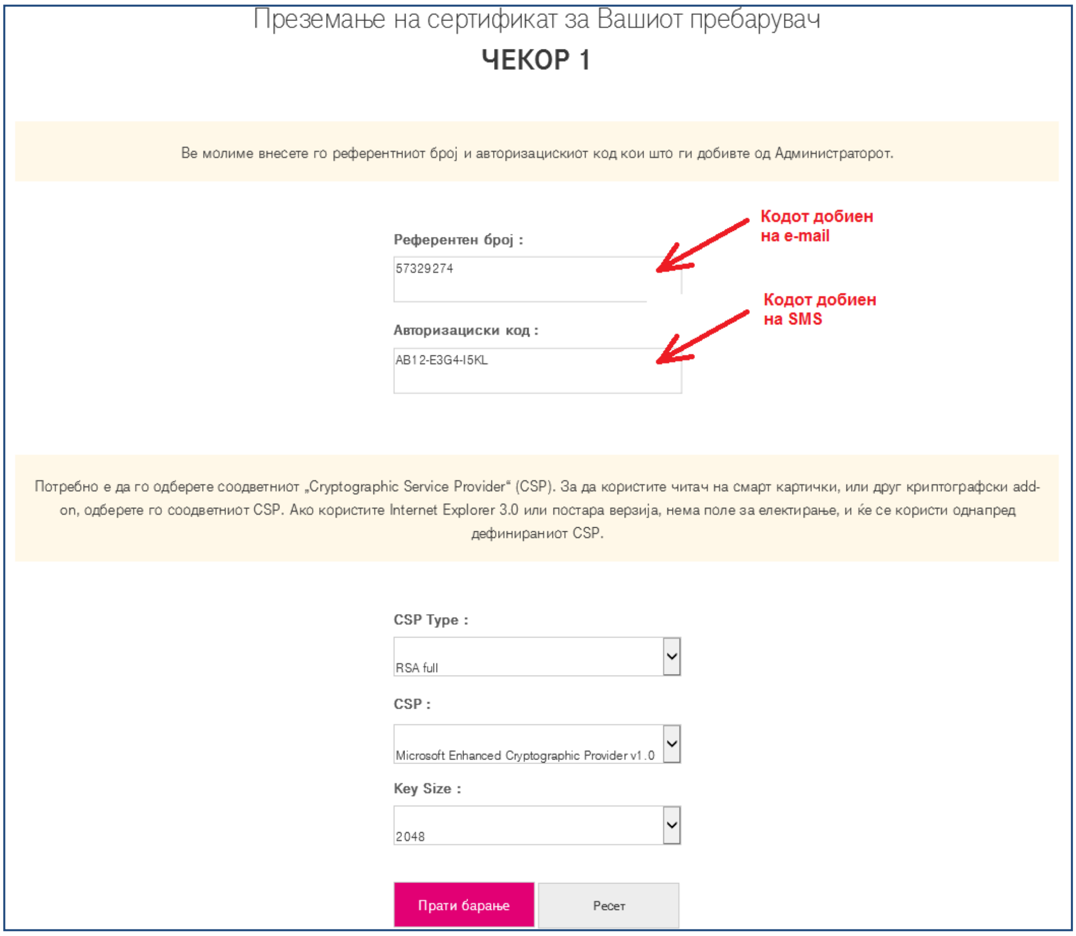
Б. Кликнете на Yes за да дозволите креирање на сертификат



В. Во полето за референтен број го внесувате бројот што го добивате по електронска пошта, додека пак во полето за авторизациски код го внесувате бројот што го добивате по СМС порака.

Во полето за CSP Provider-от задолжително изберете ги следниве опции:

- CSP type: RSA full
- CSP: Microsoft Enhanced Cryptographic Provider v1.0
- Key size: 2048

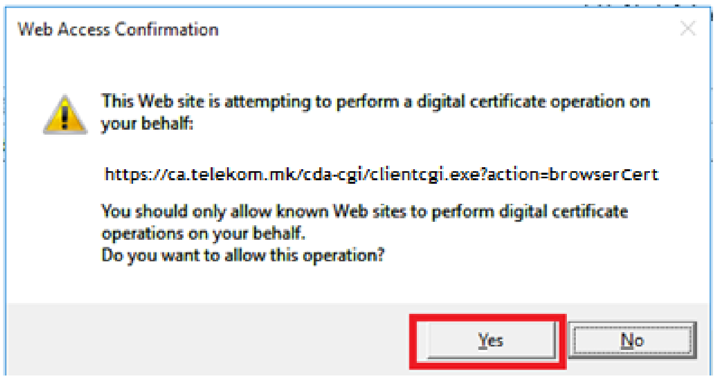


НАПОМЕНА:

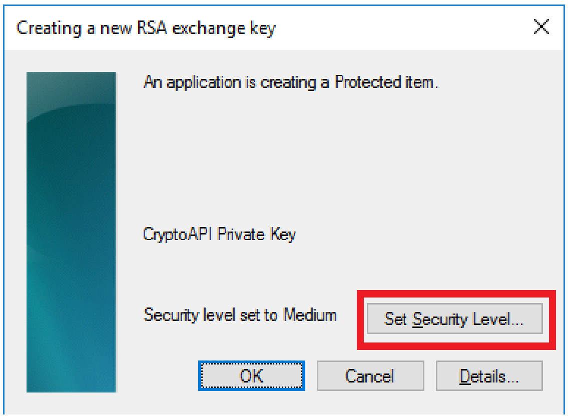
Во случај да изберете друг CSP, ризикувате губење на сертификатот по што ќе треба да доставите ново барање за нов дигитален сертификат.

Доколку во полето за избор го нема Microsoft Enhanced Cryptographic Provider v1.0, ќе треба да се направи Run на ActiveX контролата која се појавува како предупредување во Information bar-от на Browser-от.

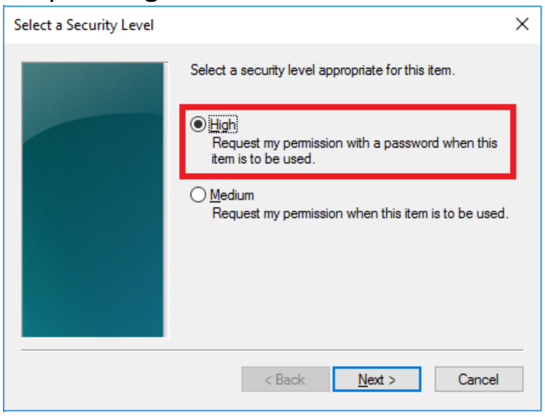
Г. Кликнете YES за потврда дека го повлекувате сертификатот.



Д. Кликнете на копчето Set Security Level.



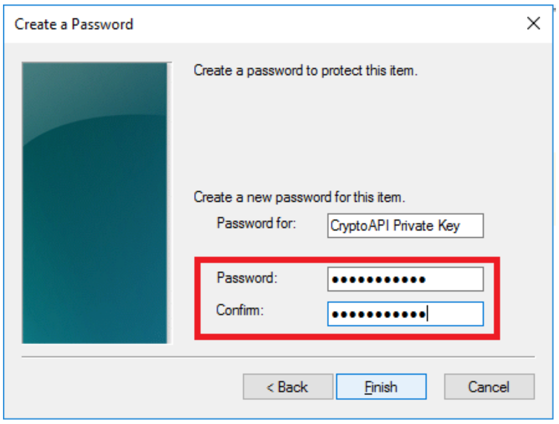
Ѓ. Во новиот прозорец изберете High и кликнете на Next.



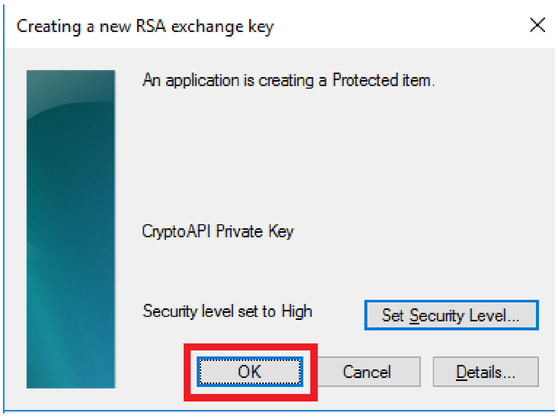
Е. Во полето Password и Confirm **внесете лозинка која подоцна ќе ја користите при потпишување со сертификатот** (лозинката треба да има најмалку 8 карактери и да содржи голема буква и барем една бројка или специјален карактер). Процесот завршете го со кликање на копчето “Finish”.

ВАЖНО!

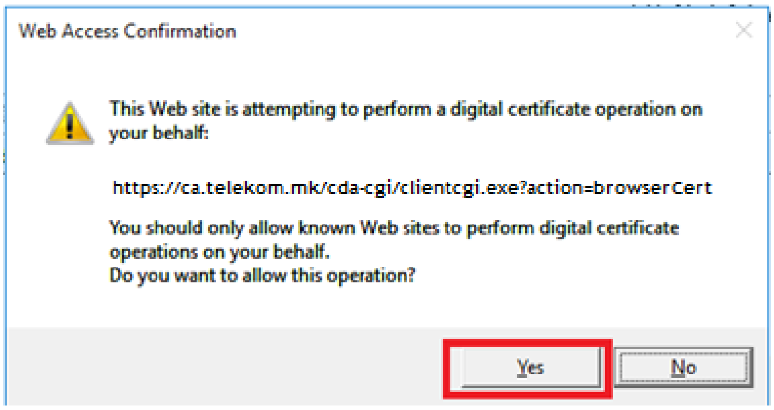
Ова е ВАШАТА лозинка. Запомнете ја оваа лозинка. Без неа сертификатот кој сте го повлекле на компјутерот нема да функционира.



Ж. Завршете со креирање на вашиот приватен клуч со избирање на ОК.

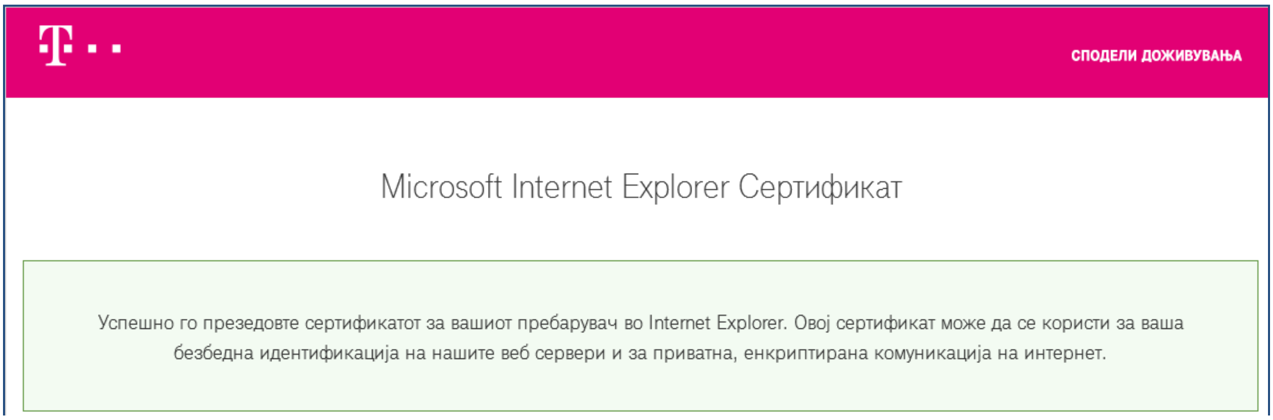


З. Кликнете на Yes за да дозволите креирање на сертификат



ВАЖНО!

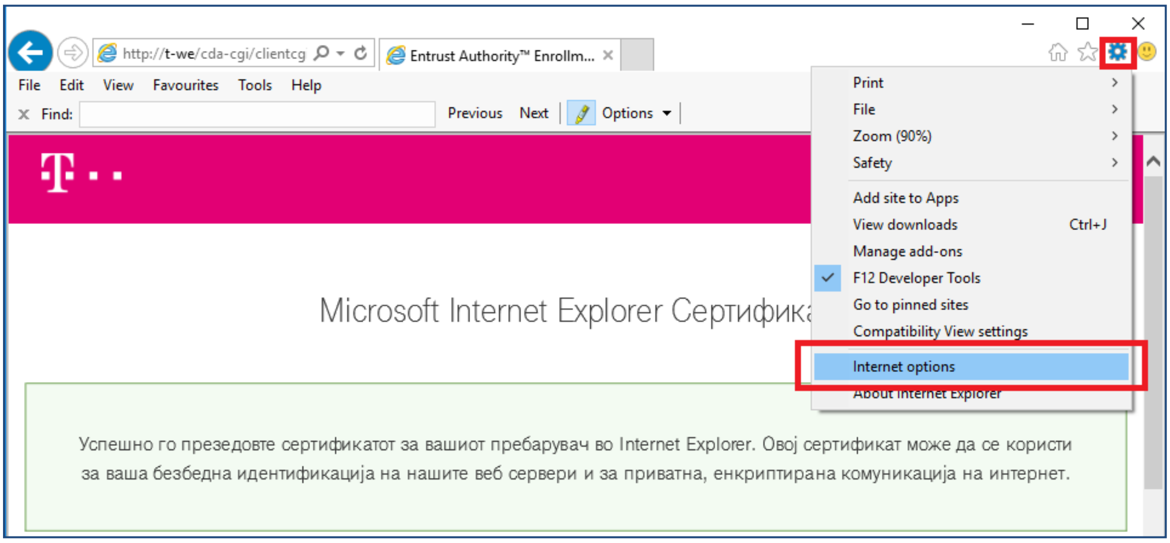
Почекајте да се креира дигиталниот сертификат. Траењето може да биде од дваесетина секунди до неколку минути. НЕ КЛИКАЈТЕ REFRESH, RESTART или BACK за време на креирањето на сертификатот. Системот ќе ве извести со порака за успешно или неуспешно креирање на сертификат. При успешно креирање ќе ја добиете следнава порака:



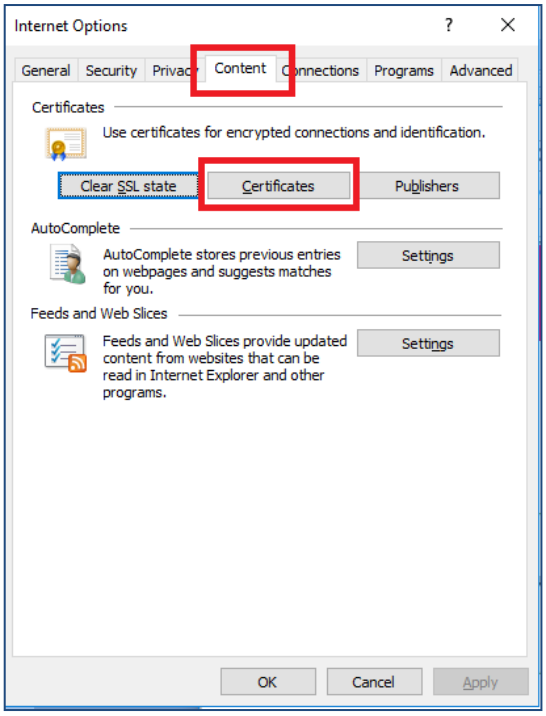
ЕКСПОРТИРАЊЕ НА ДИГИТАЛНИОТ СЕРТИФИКАТ ВО ФАЈЛ

Експортирање на дигиталниот сертификат може да се направи само на компјутерот кој веќе го има Вашиот сертификат. Тоа е компјутерот на кој сте го повлекле сертификатот, под услов во меѓувреме да не сте го избришале.

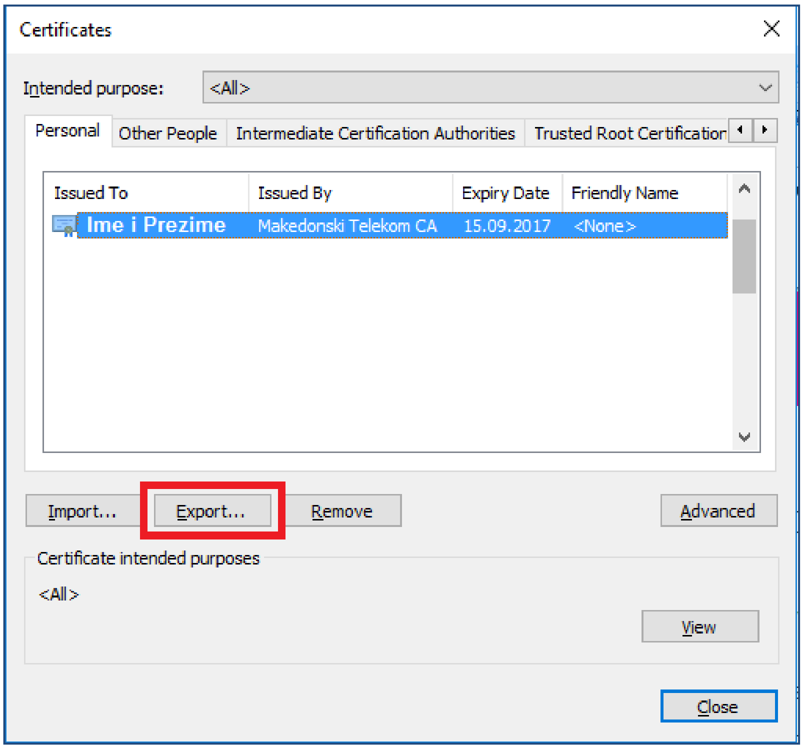
А. Во горниот десен агол од прелистувачот Internet Explorer, кликнете на копчето што означува Алатки за подесување (Tools) и одберете **Internet options**.



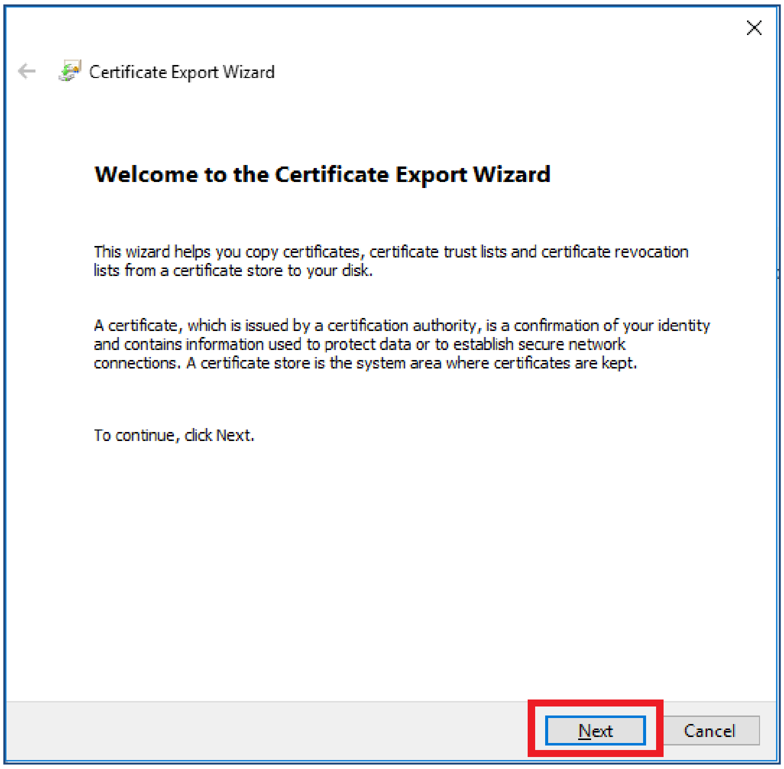
Б. Во табот **Content** избирете **Certificates.**



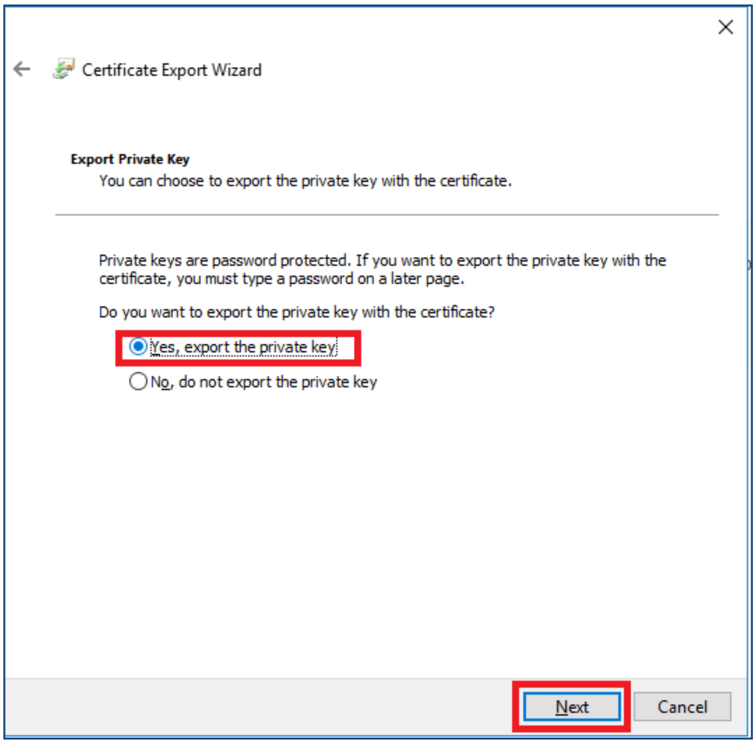
В. Селектирајте го вашиот персонален сертификат и кликнете **Export**



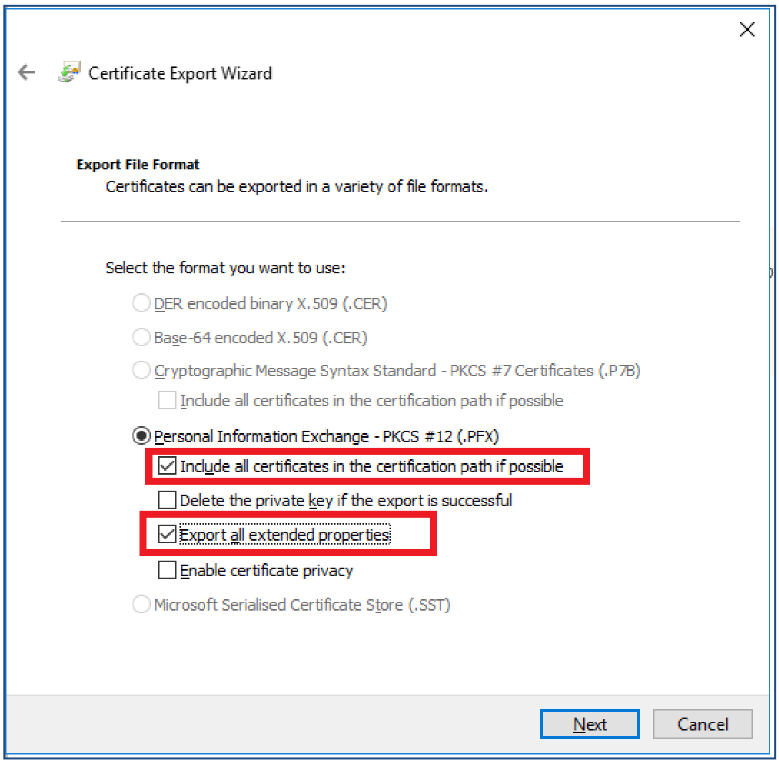
Г. Кликнете NEXT…



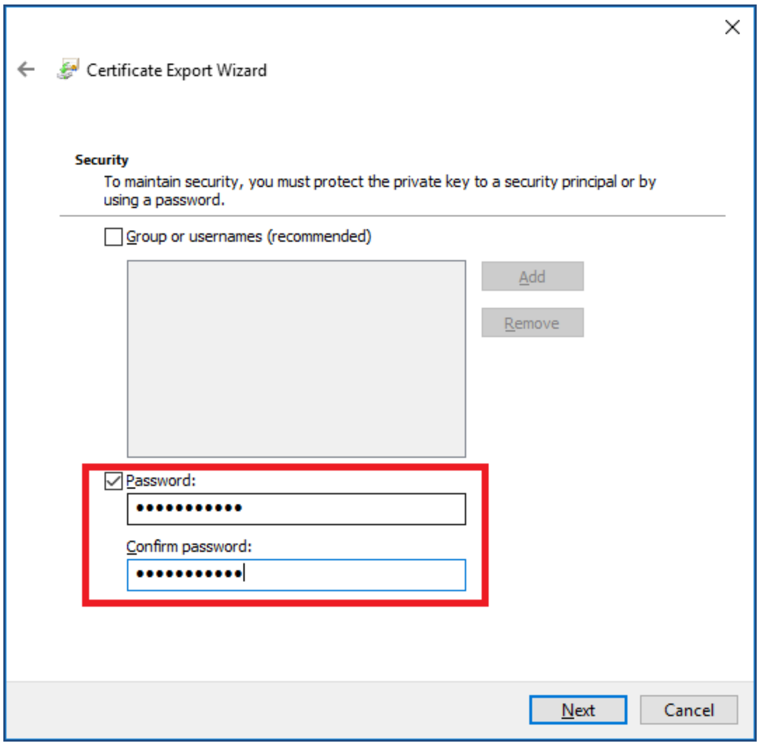
Д. Во следниот чекор, селектирајте ја опцијата **Yes, export the private key, со што ќе овозможите** правилно функционирање на сертификатот.



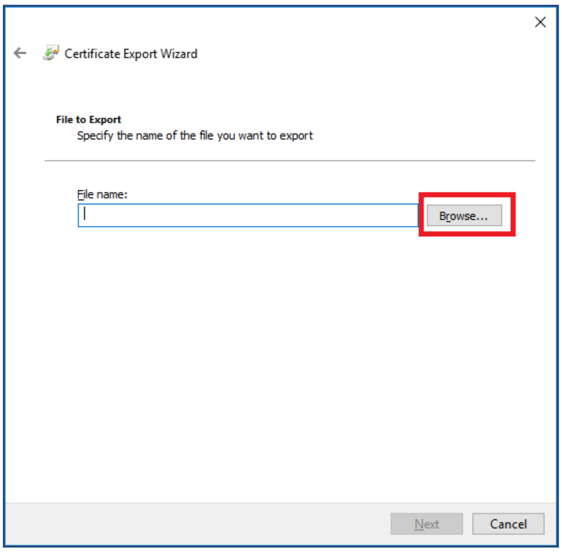
Ѓ. Во следниот прозорец задолжително изберете ги посочените опции:

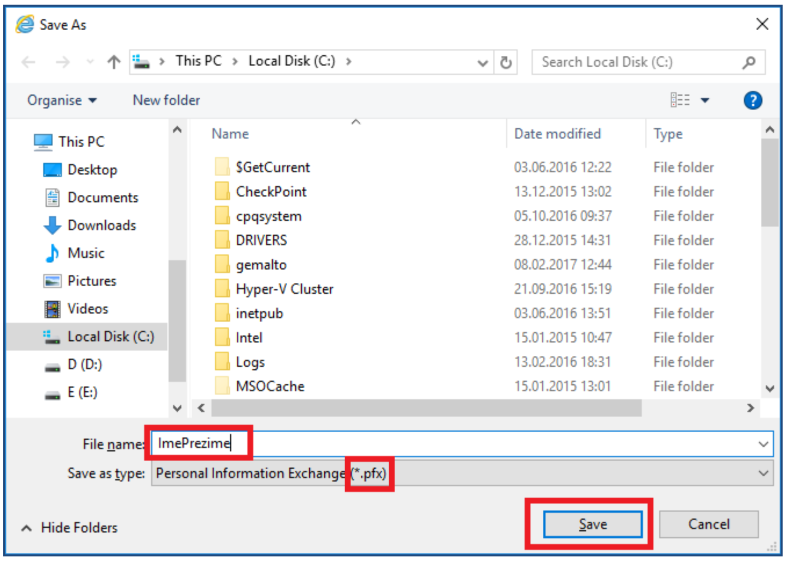


Е. По кликање на копчето Next од претходниот чекор, постапката води до внесување на лозинка. Ја внесувате истата лозинка која ја внесовте за дигиталниот сертификат при процесот на Активирање на Вашиот сертификат на десктоп компјутер/лаптоп (без употреба на токен) [(страница 13, точка Е во ова упатство)].

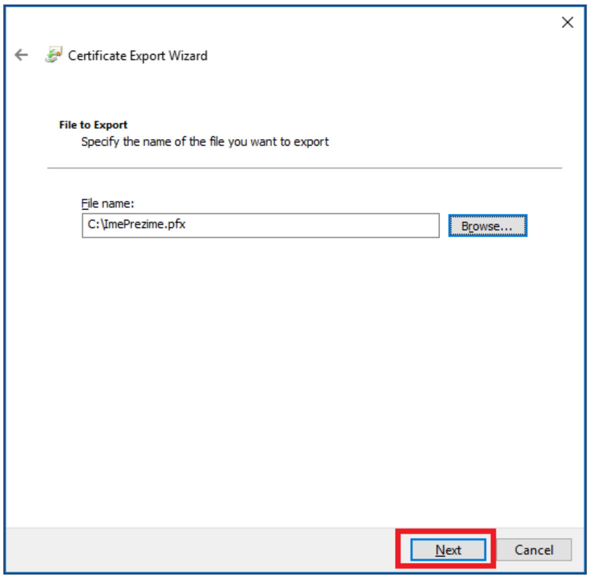


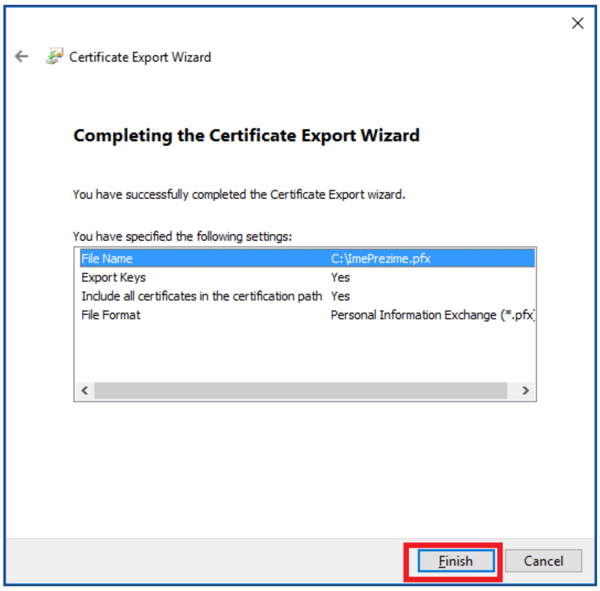
Ж. Во следниот чекор го бирате името на фајлот и локацијата каде што сакате да го зачувате сертификатот.



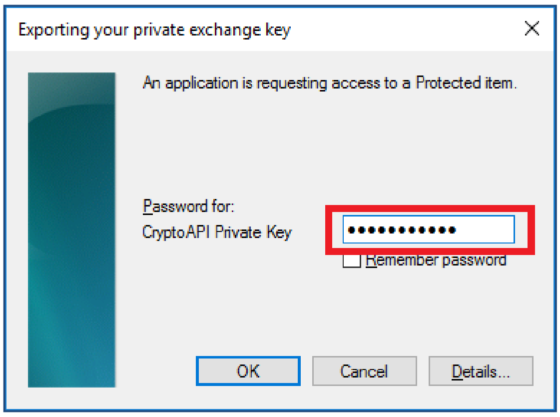


Типот на фајлот треба да е .pfx

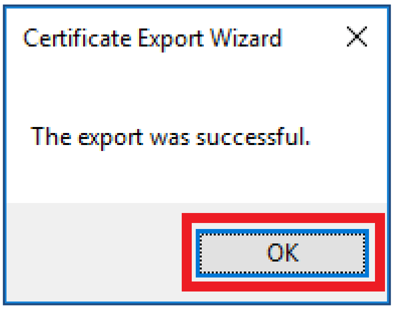




Внесете ја лозинката која ја ставивте при повлекувањето на сертификатот:



На крајниот преглед за експортирање на дигиталниот сертификат изберете OK.



НАПОМЕНА:

⚠ **Направете експортирање на сертификатот и зачувајте го на безбедносен медиум (токен) за во случај на дефект на компјутерот или потребно форматирање.**

⚠ **Лозинката креирана при активирање на дигиталниот сертификат Ви е неопходна за користење на сертификатот, запомнете ја.**

ИМПОРТИРАЊЕ ДИГИТАЛЕН СЕРТИФИКАТ ОД ФАЈЛ НА ТОКЕН ОД ТИП GEMALTO IDPRIME.NET

За да направите импортирање, потребно е да го имате сертификатот, зачуван во фајл со наставка .PFX.

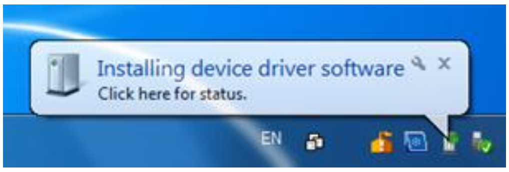
ИНСТАЛИРАЊЕ ДРАЈВЕРИ ЗА ТОКЕН GEMALTO.NET – ЗА WINDOWS 7 И ПОНОВИ ВЕРЗИИ НА ОПЕРАТИВЕН СИСТЕМ

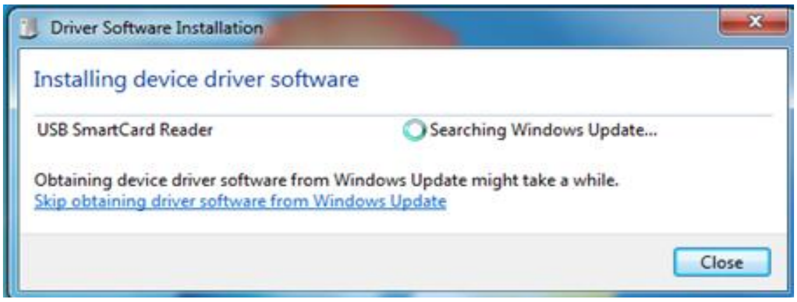
НАПОМЕНА:

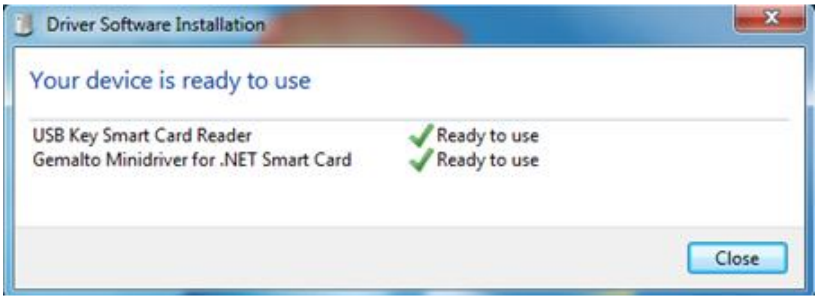
За овој чекор потребно е да бидете најавени со корисник кој има администраторски привилегии на вашиот компјутер (доколку го користат повеќе корисници).

За токенот од тип Gemalto.NET нема потреба инсталација на драјвери, доволно е само да го ставите токенот во USB портата, по што инсталацијата ќе се изврши сама.

А. Ставете го токенот во една од USB портите на десктоп компјутерот/лаптопот. Почекајте 2-3 минути да заврши инсталацијата.







Во случај на проблем со инсталација на драјверите, можете да ги преземете од следнава локација:

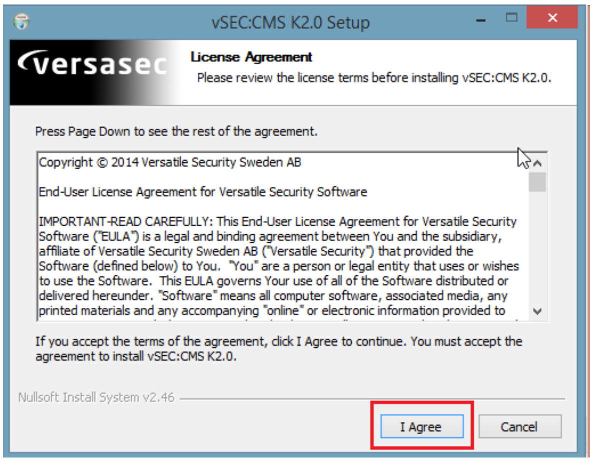
- За 32-bit OS: https://ca.telekom.mk/Gemalto/GemaltoNETDriver_32bit.zip
- За 64-bit OS: https://ca.telekom.mk/Gemalto/GemaltoNETDriver_64bit.zip

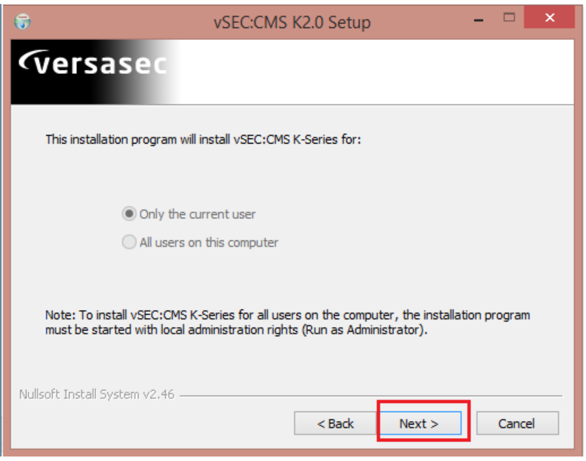
ИНСТАЛИРАЊЕ НА VSEC:SMC АПЛИКАЦИЈАТА

А. На следниов ЛИНК можете да ја спуштите најновата верзија на апликацијата **vSEC:CMS® K-Series.**

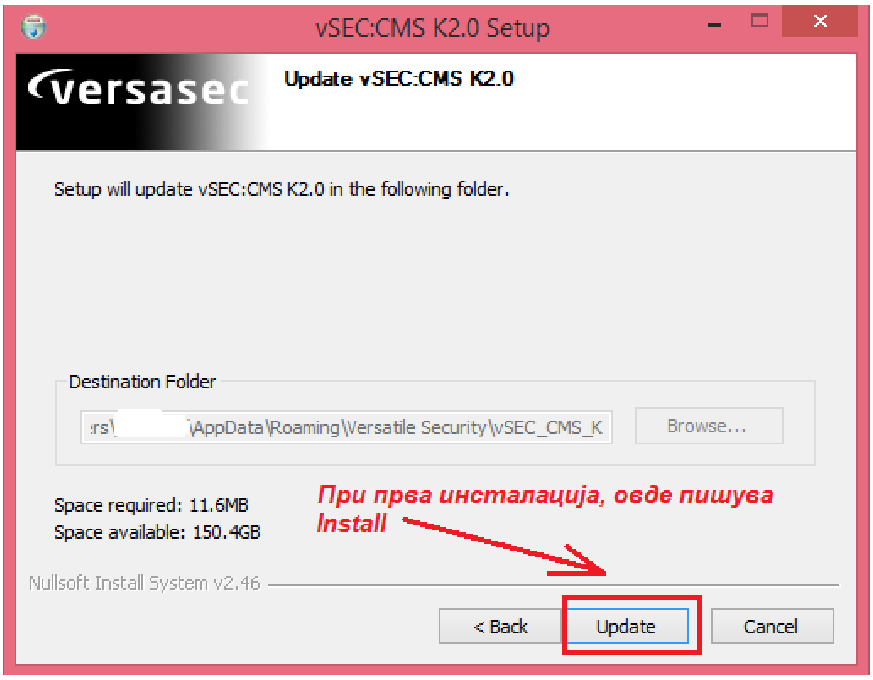
Б. Стартувајте со двоклик или со кликање на RUN: **vSEC_CMS_K2.0.exe**

В. Кликнете на: **I Agree.**

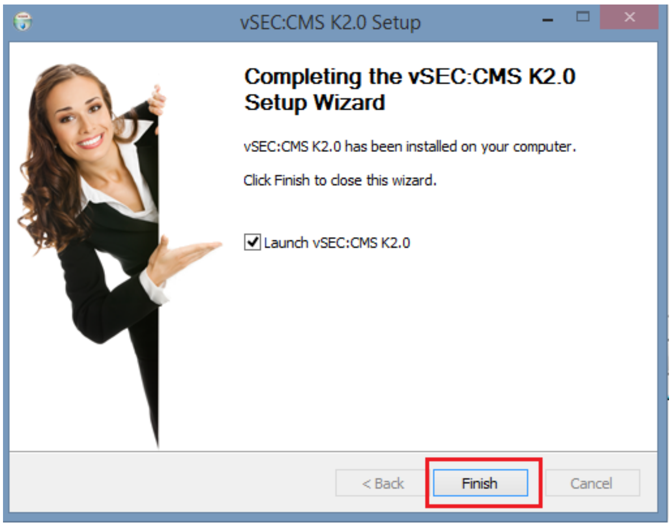




В. Кликнете на Install. Доколку веќе имате инсталирано пониска верзија, кликнете на Update



Г. Кликнете Finish, по што апликацијата ќе се стартува автоматски.

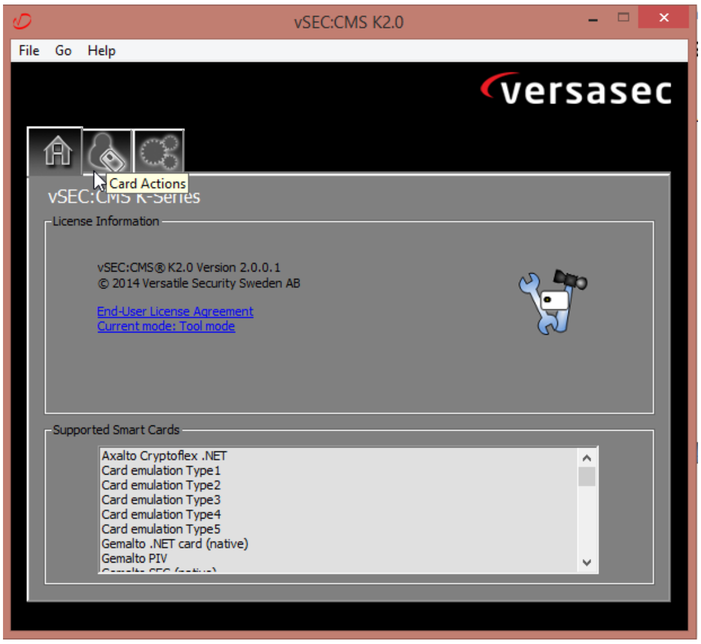


Д. Апликацијата можете да ја стартувате од Вашиот десктоп преку подолната иконка:

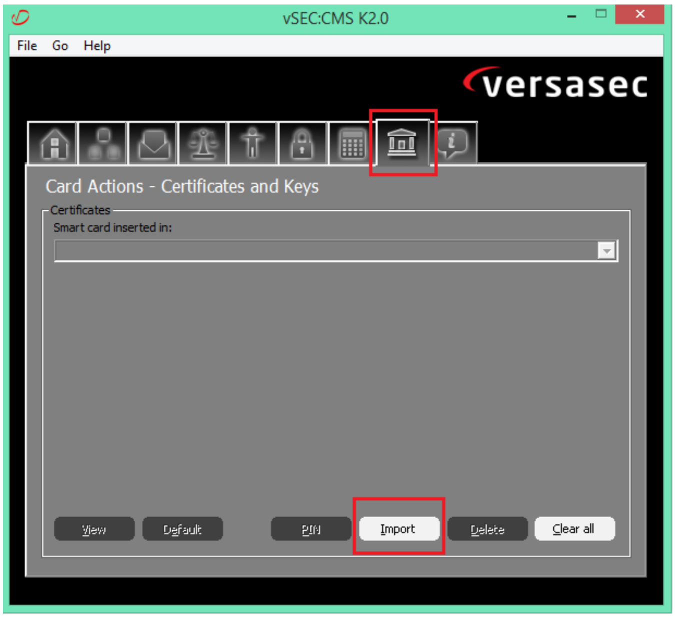
ИМПОРТИРАЊЕ НА СЕРТИФИКАТОТ НА ТОКЕН СО VSEC:SMC АПЛИКАЦИЈАТА

А. Ставете го Gemalto.NET токенот во компјутерот/лаптопот и стартувајте ја апликацијата vSEC:CMS од посочената иконка:

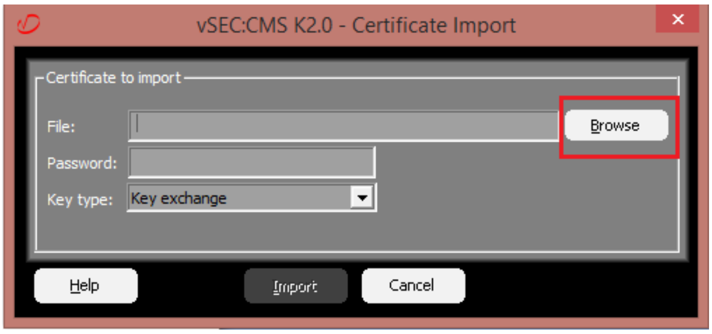
Б. Кликнете на табот: **Card Actions.**



В. Одберете го табот: **Certificates**, и кликнете на копчето **Import.**

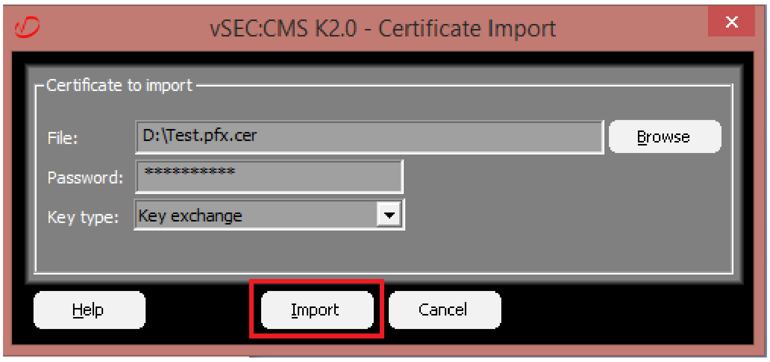


Г. Кликнете на копчето Browse, за да го одберете претходно добиениот сертификат со екстензија .PFX кој е добиен согласно упатството: „Упатство за активирање и инсталација на дигитален сертификат на десктоп компјутер и/или лаптоп“.

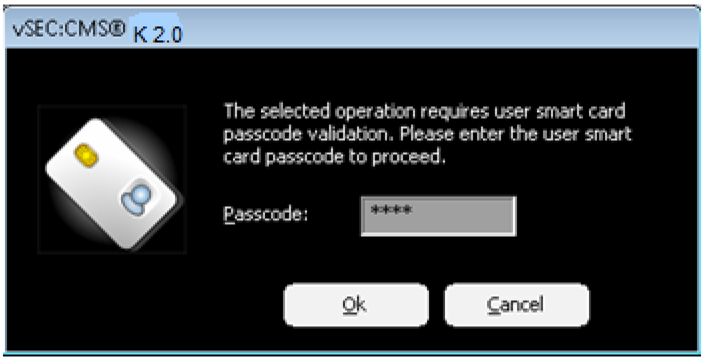


Во полето Password се внесува лозинката за фајлот која ја внесовте при негово креирање.

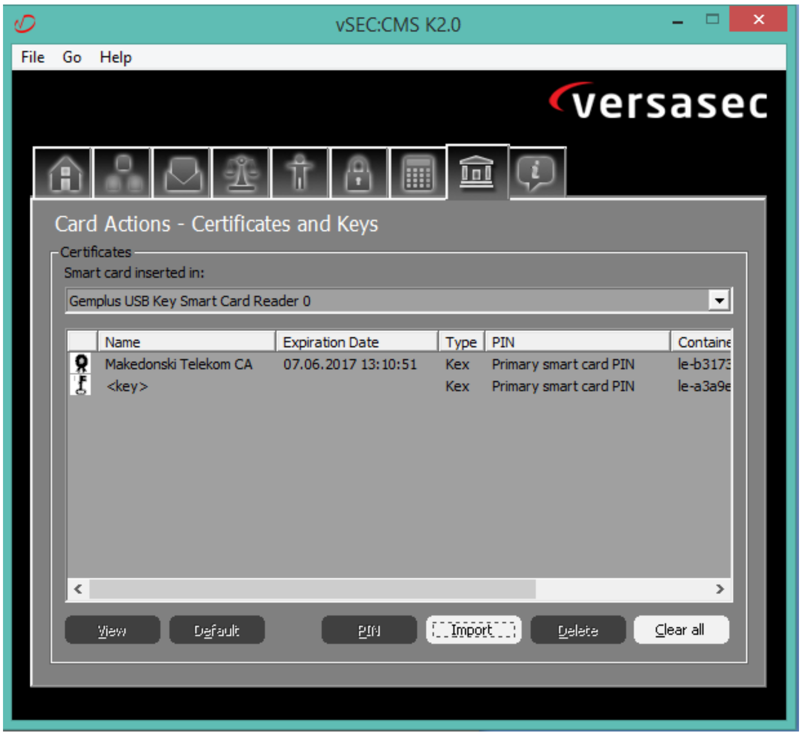
Д. Кликнете на копчето Import.



Ѓ. Внесете го ПИН-от за токенот (0000 – четири нули, доколку го немате променето со некој Ваш)., и кликнете ОК.



Е. Во апликацијата се појавува Вашиот сертификат, со Вашето корисничко име.



Ж. Кликнете Close.

Можете да го користите токенот со импортираниот сертификат.

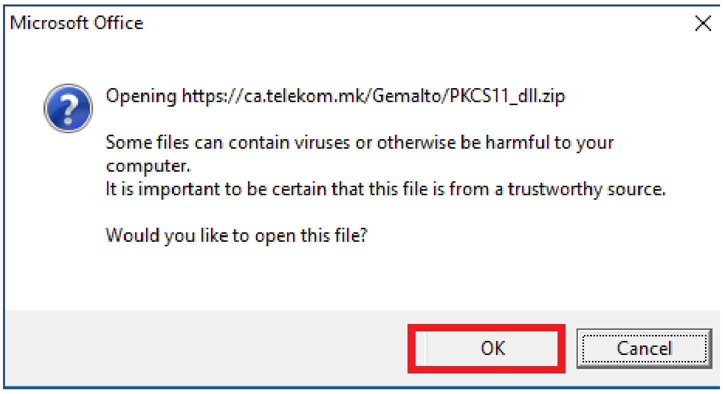
Употреба на токенот во апликација на УЈП

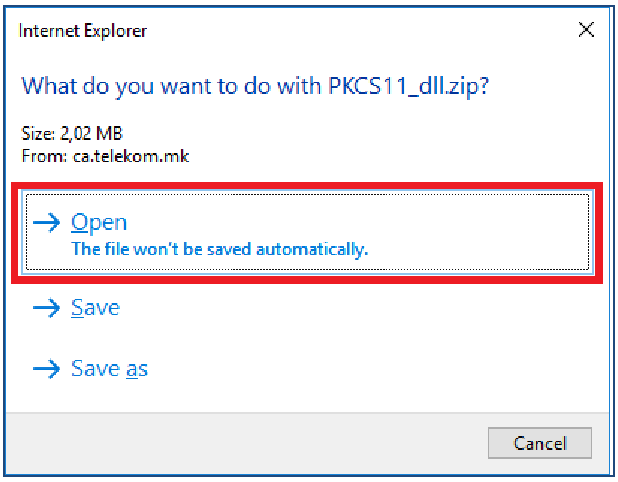
За да можете да го користите дигиталниот сертификат во апликацијата на Управа за Јавни Приходи (УЈП), претходно направете инсталација на PKCS11 од наредната точка.

ИНСТАЛАЦИЈА НА PKCS11 (ЗА АПЛИКАЦИЈА НА УЈП)

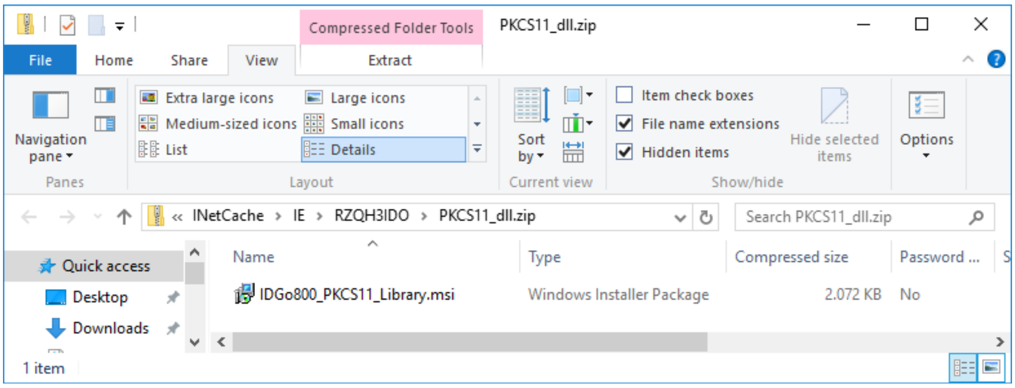
А. Кликнете на следниов линк: https://ca.telekom.mk/Gemalto/PKCS11_dll.zip

Б. Одберете ОК, а потоа Open;

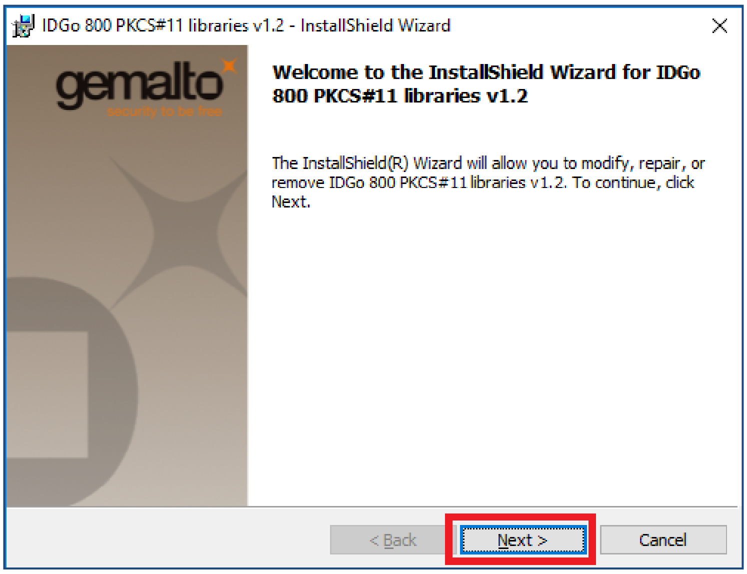




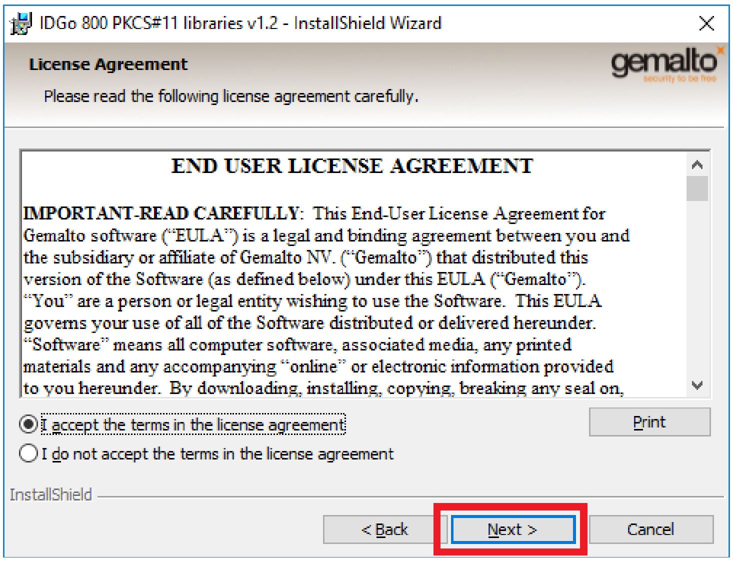
В. Со двоклик стартувајте го IDGo800_PKCS11_Library.msi



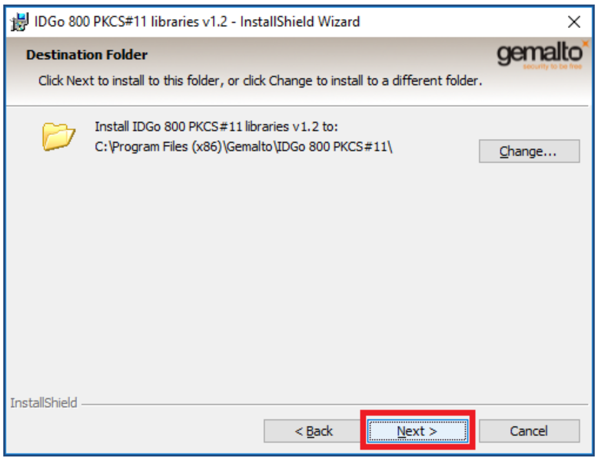
Г. Кликнете NEXT;



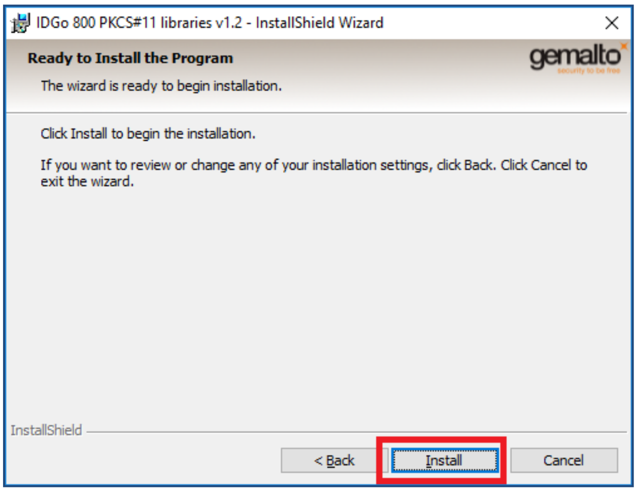
Д. Кликнете NEXT:

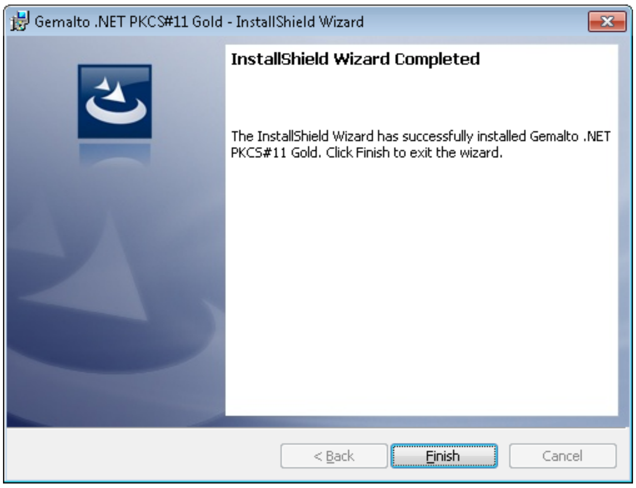


Ѓ. Кликнете NEXT;



Е. Кликнете Install па Finish;





Инсталацијата на потребните фајлови е на локација: **C:\Program Files\Gemalto\IDGo 800 PKCS#11**

Овде се наоѓаат потребните DLL фајлови за работа на Gemalto.NET токенот со апликацијата на УЈП:

- IDPrimePKCS11.dll – за 32-bit оперативен систем;
- IDPrimePKCS1164.dll– за 64-bit оперативен систем.

ДОКОЛКУ АПЛИКАЦИЈАТА КОЈА ЈА КОРИСТИТЕ БАРА НАВЕДЕНИТЕ ФАЈЛОВИ ДА БИДАТ НА ДРУГА ЛОКАЦИЈА, КОПИРАЈТЕ ГИ ВО СОГЛАСНОСТ СО УПАТСТВОТО ЗА ТАА АПЛИКАЦИЈА.

Ж. Овој чекор е важен за корисниците на апликацијата на УЈП:
Доколку имате 64-bit оперативен систем, одете во C:\Program Files (x86)\Gemalto и копирајте го целиот фолдер „DotNet PKCS11“ во новокреиран фолдер C:\Gemalto.