

Búnaðarskilríki – Leiðbeiningar.

Leiðbeiningar fyrir Windows notendur.

Efnisyfirlit

Formáli:.....	1
Svona er umsóknarferlið fyrir búnaðarskilríki - Yfirlit:	1
1. CSR útbúið (og einkalykill verður til):	2
2. Umsókn fyllt út á vef Auðkennis:.....	11
3. Íslandsrót og milliskilríkið Fullgilt auðkenni sett upp á tölvunni:	11
4. Búnaðarskilríkið sett upp á tölvunni:.....	13
5. Flytja búnaðarskilríkið út í pfx skrá:.....	16
Bókhaldskerfi og bankar:.....	18
Innskráning með rafrænum skilríkjum á vefsvæði	18
Aðstoð:	18

Formáli:

Rafræn skilríki samanstanda af Einkalykli (Privat key) og Dreifilykli (Public key)

Einkalykillinn er búinn til af eiganda skilríkisins og er hjartað í skilríkinu. Hann má aldrei senda öðrum en þeim sem eiga að sýsla með skilríkið fyrir hönd fyrirtækisins.

Dreifilykillinn er gefinn út af Auðkenni með milliskilríkinu Fullgilt audkenni og hann má senda hverjum sem er eins og t.d. bönkunum.

Þegar sótt er um Búnaðarskilríki þarf umsækjandinn fyrst að útbúa svokallað CSR (Certificate Signing Request). CSR er svo notað við framleiðslu á Dreifilyklinum. Þegar CSR er útbúið verður einkalykill til á sömu tölvu í leiðinni.

Svona er umsóknarferlið fyrir búnaðarskilríki - Yfirlit:

Ferlið gengur þannig fyrir sig að umsækjandi búnaðarskilríkis útbýr CRS á sinni tölvu eða server. Um leið verður til einkalykill á þeirri tölvu.

Því næst er umsókn fyllt út á vefsíðu Auðkennis og CSR sent með henni.

<https://umsoknir.audkenni.is/bunadarskilriki/bunadarskilrikiFG.cfm>

í umsókninni þarf að skilgreina tæknilega tengilið og forráðamann/prókúruhafa fyrirtækis.

Ef umsókn er samþykkt framleiðir Auðkenni dreifilykilinn fyrir skilríkið. Auðkenni sendir umsækjanda cer skrá sem inniheldur dreifilykilinn. Ef milliskilríkið Fullgilt audkenni og rötarskilríkið Íslandsrót eru ekki þegar til staðar á tölvunni þarf umsækjandi að setja þau inn. Umsækjandi keyrir cer skrána með dreifilyklinum **Á SÖMU TÖLVU** og hann bjó til CSR skrána. Wisard leiðir keyrsluna áfram og bindur dreifilykilinn við einkalykilinn og setur skilríkið í skilríkjageymslu tölvunnar.

Nú er skilríkin uppsett á tölvunni.

Hægt að flytja (export) skilríkið út í pfx skrá og setja upp á fleiri vélum.

1. CSR útbúið (og einkalykill verður til):

Notast er við **Microsoft Management Console (mmc)** til að útbúa CSR skrána, einkalykillinn verður til sjálfkrafa í því ferli.

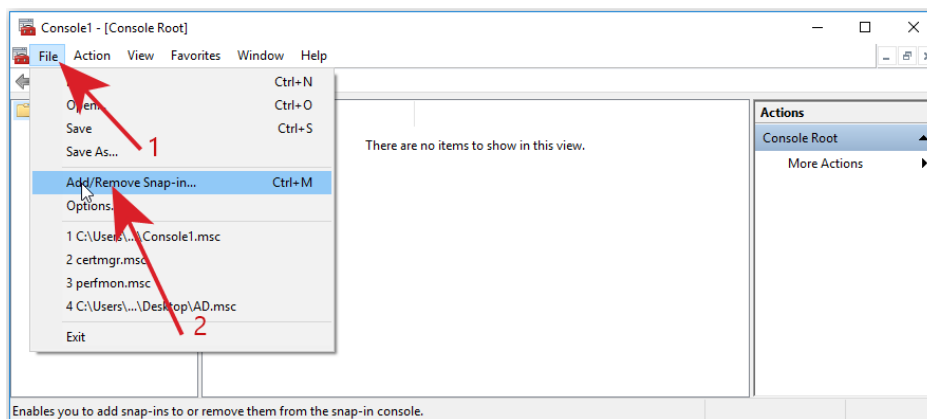
1. Til ræsa **mmc** skal smella á **start** hnappinn eða **Windows** hnappinn neðst í horninu vinstramegin á skjánum.
2. Sláðu inn **mmc** á lyklaborðið án þess að velja neitt.
3. **mmc** táknið ætti að sjást, smelltu á það.
4. **mmc** ætti að ræsa sig og opna **Console** glugga.



Console gluggi:

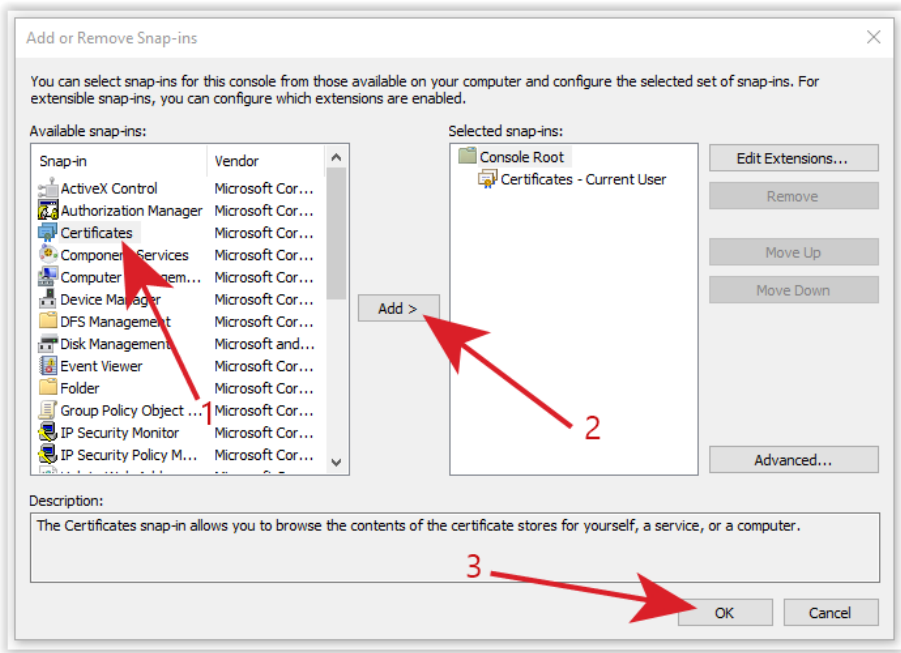
1. Veldu **File**.
2. Veldu **Add/Remove Snap-in...**

Add or Remove Snap-ins gluggi opnast



Add or Remove Snap-ins gluggi:

1. Veldu **Certificates**.
2. Veldu **Add >**
3. Smelltu á **OK** hnapp

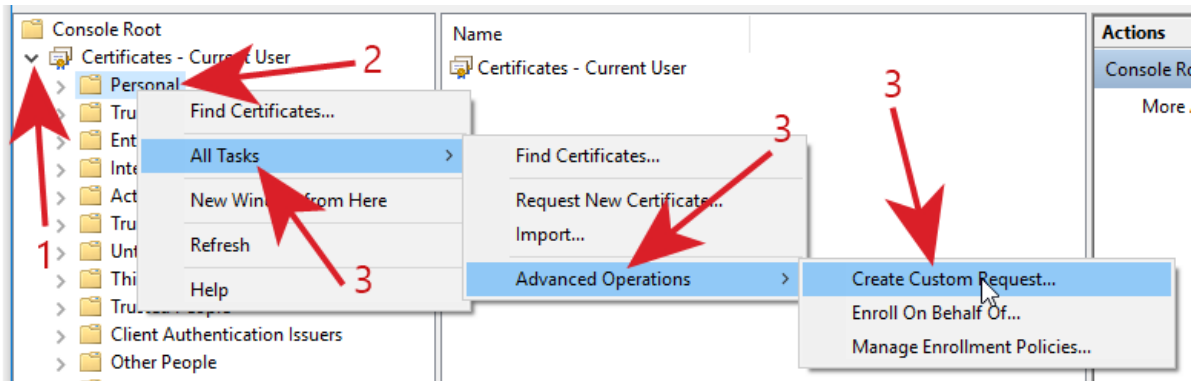


Add or Remove Snap-ins gluggi hverfur og nú er Certificates komið í Console gluggann.



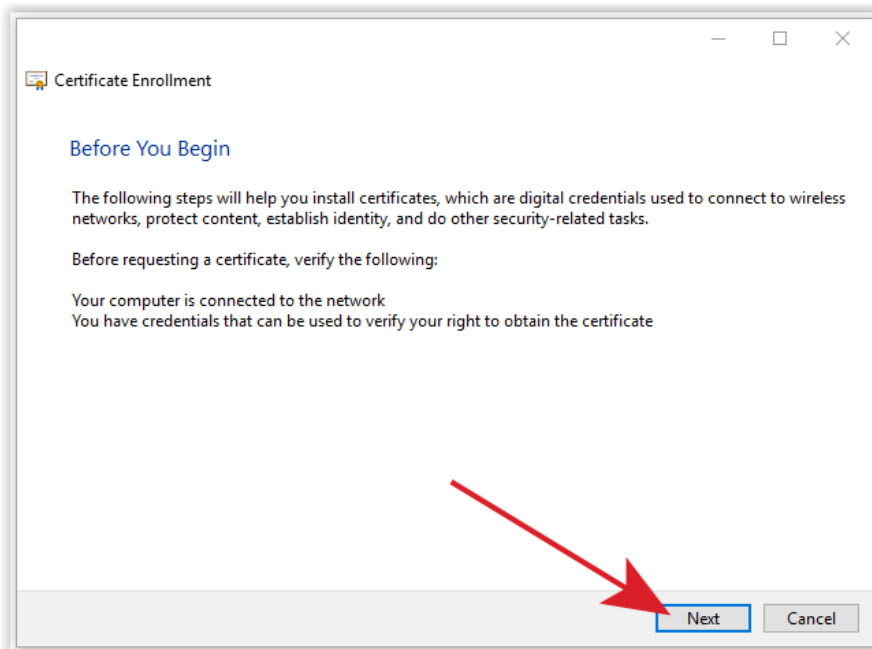
1. Smelltu á **píluna** við **Certificate** táknið. **2.** Hægri smelltu á **Personal** möppuna
3. Veldu **All Task / Advanced Operations / Create Custom Request...**

Certificate Enrollment gluggi opnast

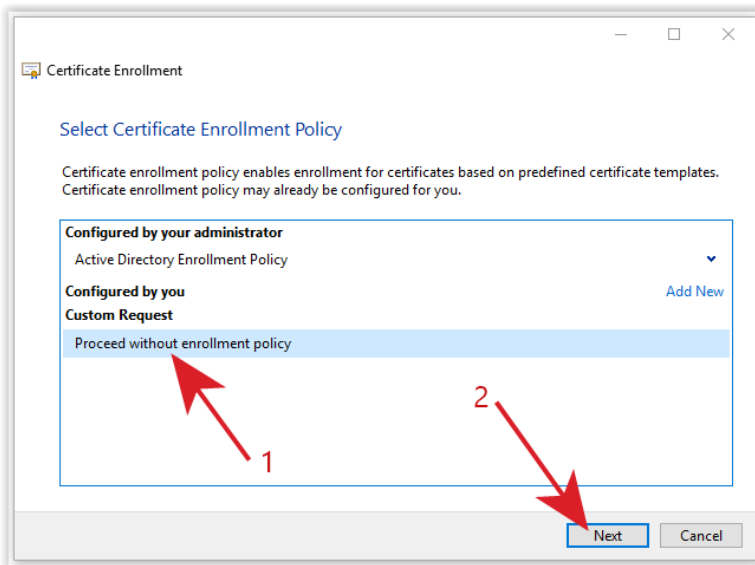


Certificate Enrollment gluggi:

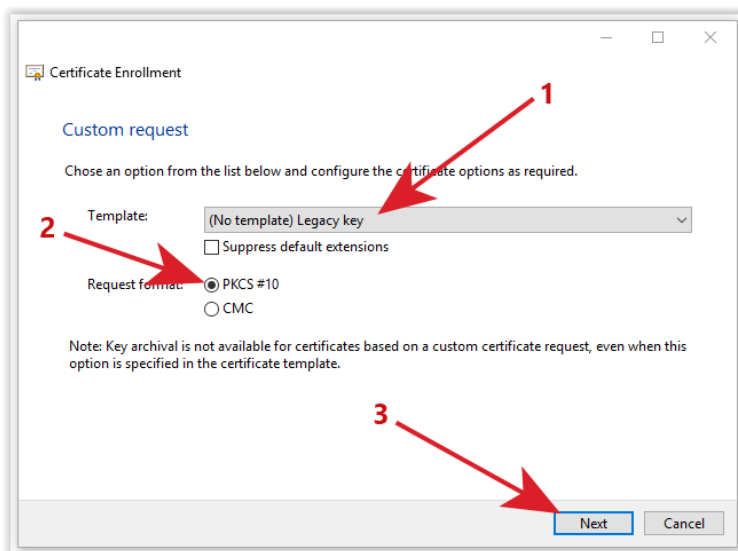
Smelltu á **Next**.



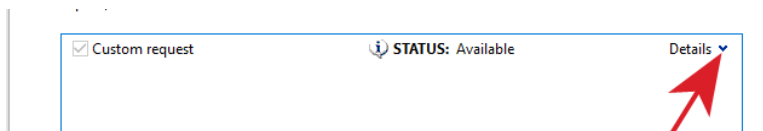
1. Veldu **Procced without enrollment policy**. 2. Smelltu á **Next**



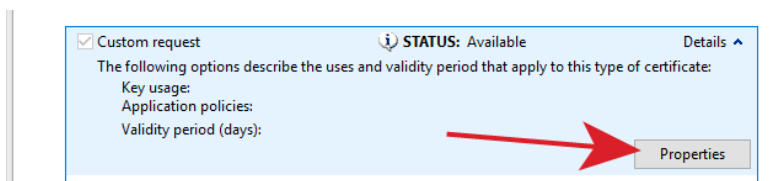
ATH. Mikilvægt: 1. Veldu **(No template) Legacy key**. 2. Veldu **PKCS#10**. 3. Smelltu á **Next**.



Smelltu á píluna við hliðina á **Details** til að kalla fram **Properties** hnappinn.



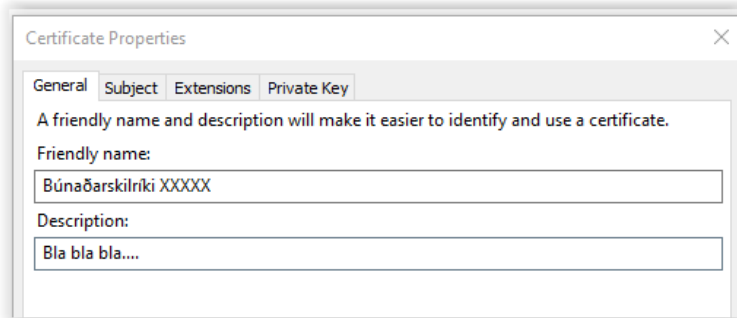
Smelltu á **Properties** hnappinn og þá opnast Certificate Properties glugginn.



Certificate Properties glugginn:

Undir **General** flípanum er hægt að skrá Friendly name og Description.

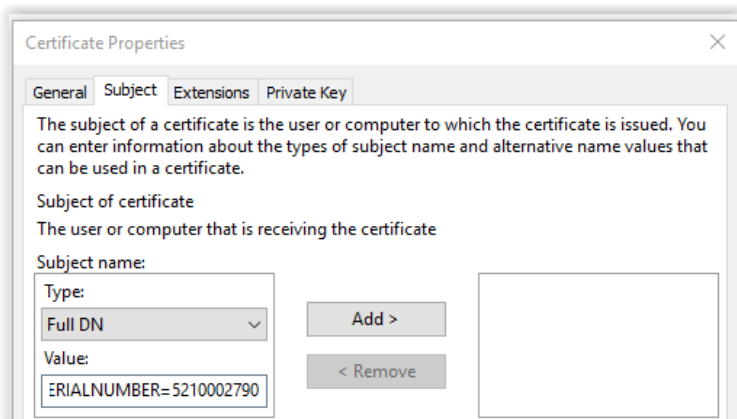
Það þarf ekki nauðsynlega en getur verið gott til aðgreiningar ef mörg skilríki eru á vélinni.



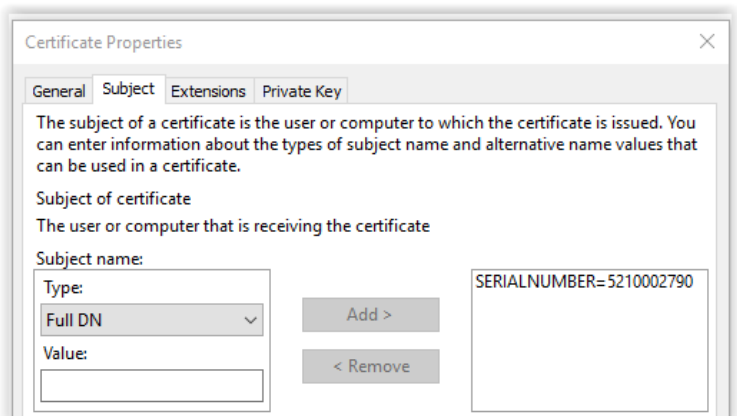
Veldu **Subject** flípann.

Undir Subject name þarf að setja inn nokkur gildi undir Type:

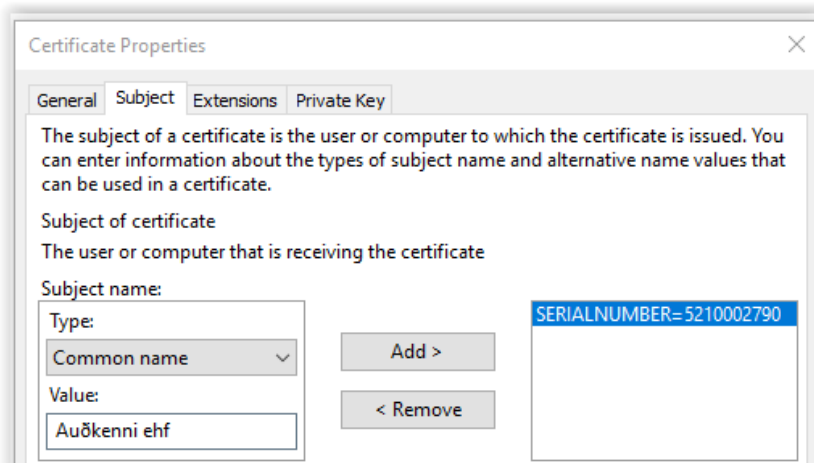
1. Veldu **Full DN** og í **Value** setur þú SERIALNUMBER=Kennitala fyrirtækis (Mikilvægt að hafa SERIALNUMBER í hástöfum)
2. Smelltu á **Add >** hnappinn



Þá á þetta að líta út eins og á myndinni hér fyrir neðan nema kennitalan er önnur.



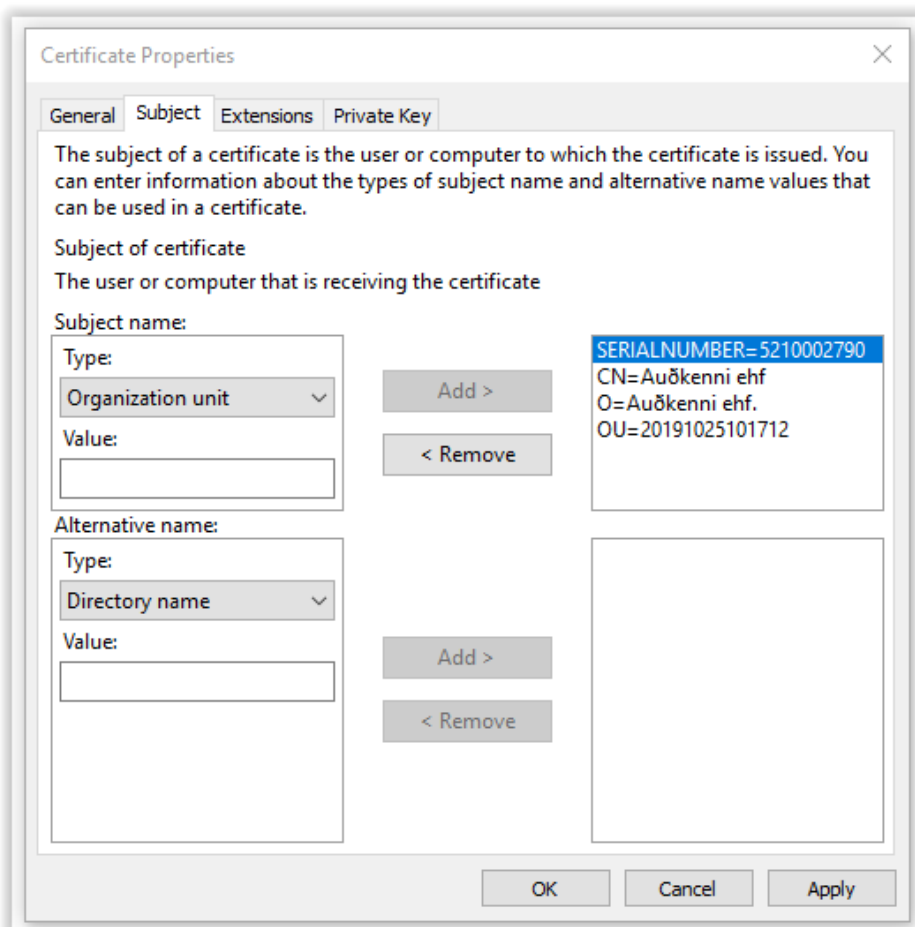
Næst skaltu velja **Common name** undir **Type** og setja þar nafn skilríkis. Reglan er sú að það sé nafn fyrirtækis eða tengt því. (Auðkenni áskilur sér rétt að hafna umsókn ef Common Name er vafasamt). Smelltu svo á **Add >** hnappinn



Veldu næst **Organization** og settu þar nafn fyrirtækis eins og það er skráð í Þjóðskrá, smelltu á **Add >**
Veldu **Organization Unit** og settu þar núverandi dagsetningu og tíma svona: **20191025101712**
(2019 er árið, 10 er mánuður, 25 er dagurinn, 10 er klukkustundir, 17 er mínútur og 12 sekúndur)
Smelltu á **Add >** hnappinn.

Þetta er gert til að fá einkvætt gildi í CSR, ekki hægt að nota kennitölu þar sem fleiri en ein búnaðarskilríki geta verið á hverri kennitölu.

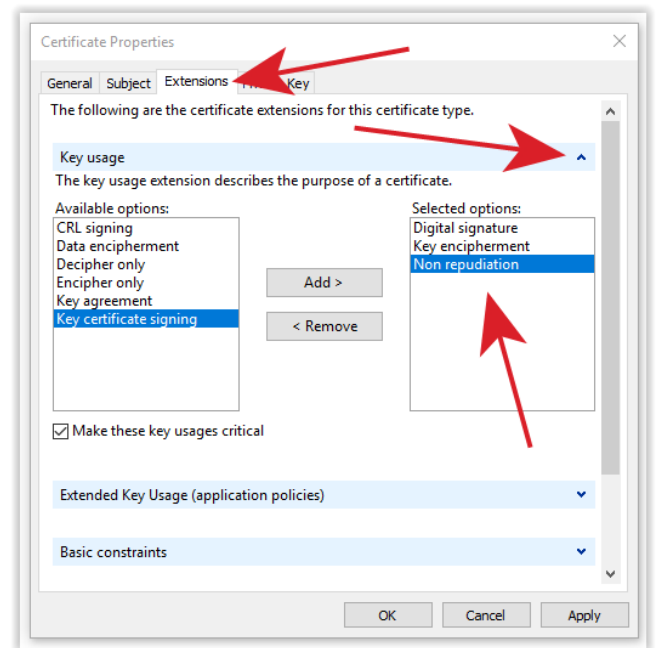
Nú eiga að vera komnar **4 línur** í gluggann hægra megin eins og á myndinni hér fyrir neðan.



Veldu **Extensions** flipann

Veldu **Key usage** og bættu við þessum gildum:

- Digital signature
- Key encipherment
- Non repudiation

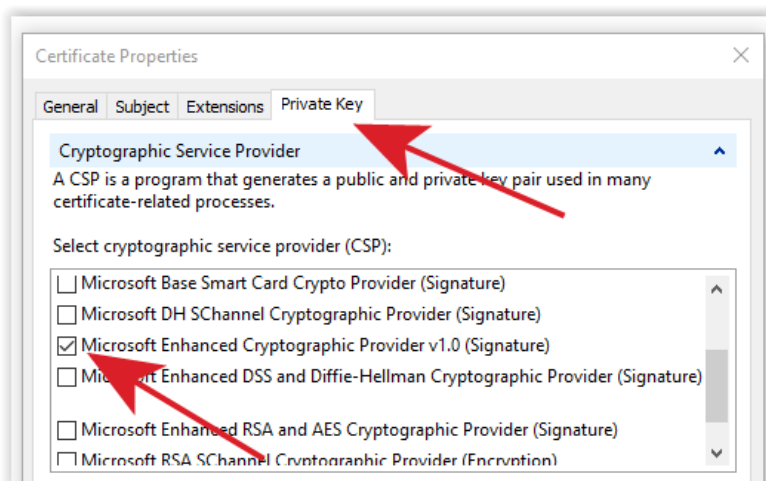


Veldu næst **Private Key** flipann

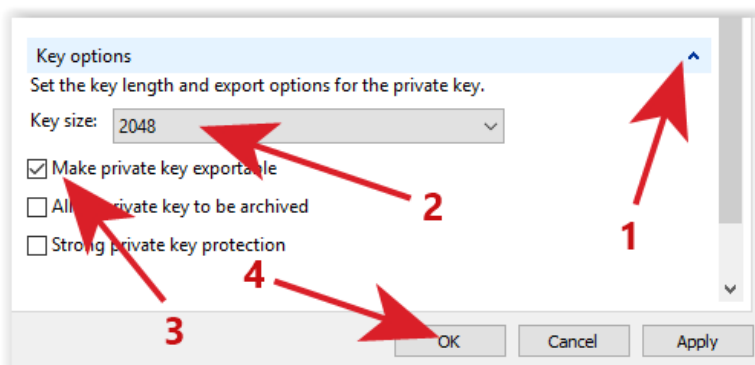
Veldu **Cryptographic Service Provider**

Taktu út efsta hakið við **Microsoft Strong Cryptographic Provider (Signature)**

Skrollaðu niður og hakaðu við **Microsoft Enhanced Cryptographic Provider v1.0 (Signature)**

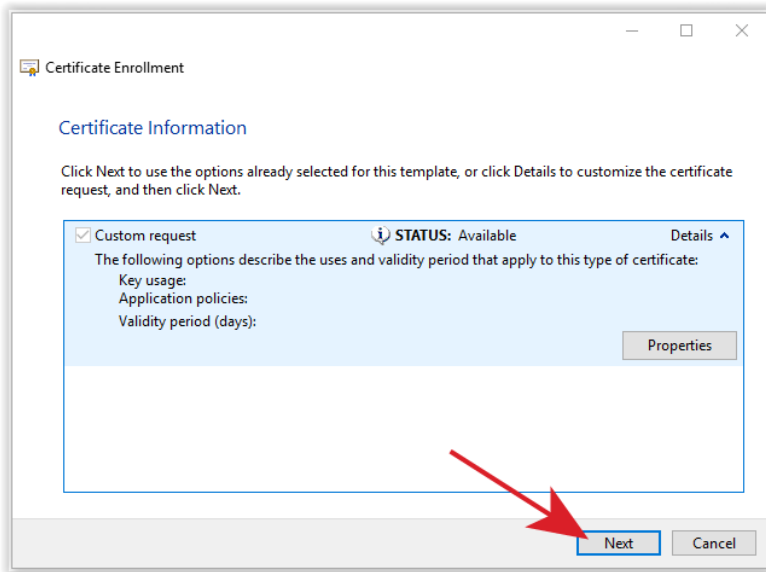


1. Veldu: **Key options**. **2.** Veldu: **Key size: 2048**. **3.** Hakaðu við: **Make private key exportable**.

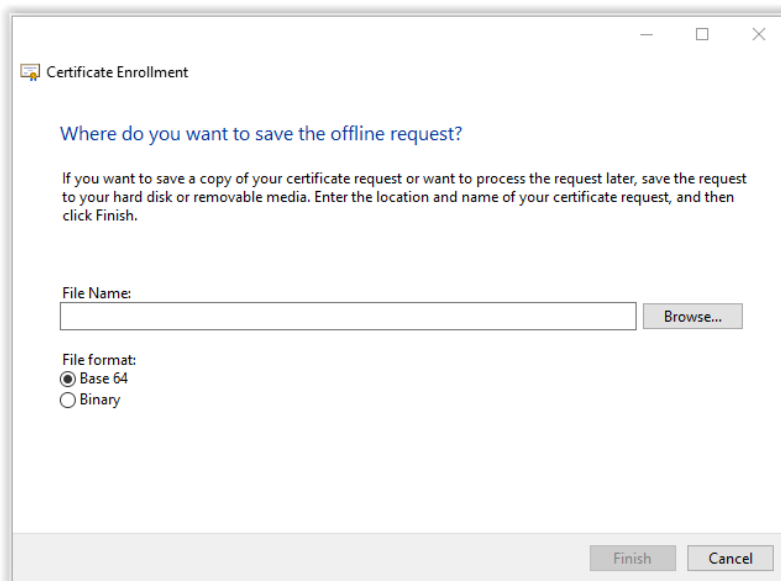


4. Smelltu svo á **OK**

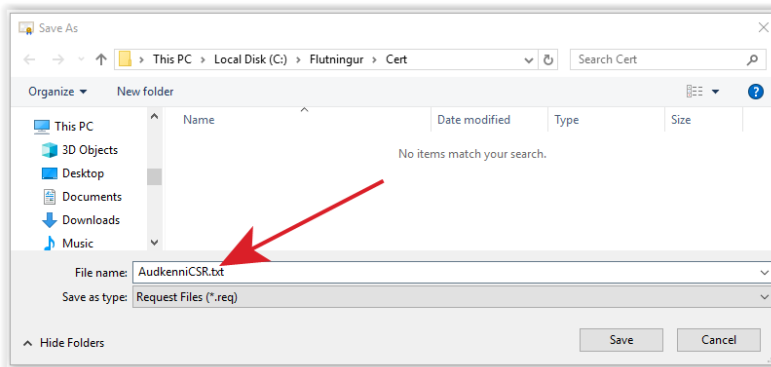
Þá hverfur Certificate Properties glugginn.
Smelltu á **Next** í Certificate Enrollment glugganum.



File format á að vera **Base 64**
Smelltu á **Browse** til að velja hvar þú vilt vista CSR skrána.

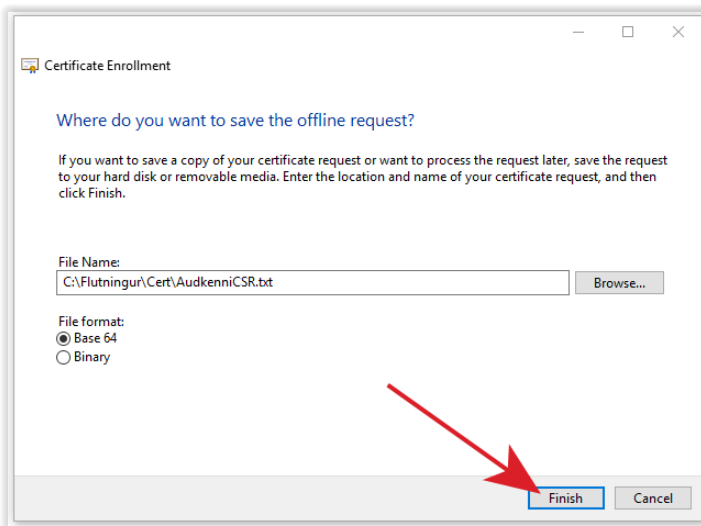


Þú velur hvar þú vistar skrána og hvaða nafn þú setur á hana. Gott er að **setja .txt** í endann á nafninu, smelltu svo á **Save**.

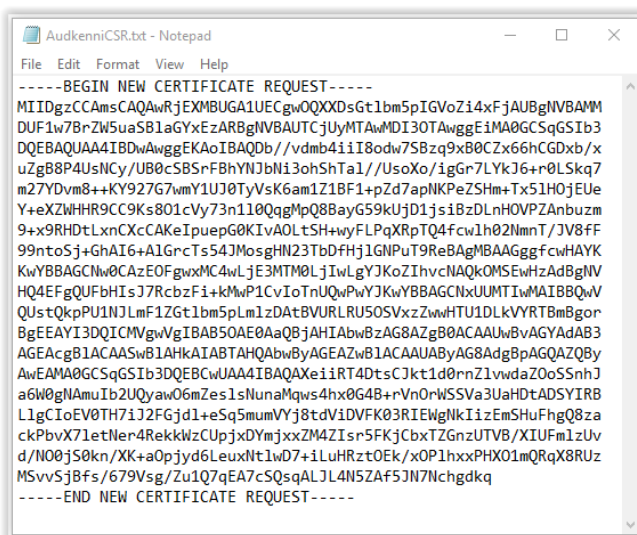


Þá hverfur Save As glugginn.

Smelltu á **Finish** í Certificate Enrollment glugganum og þá vistast CSR skráin á þeim stað sem þú valdir og einkalykill hefur verið búinn til.



Ef skráin er opnuð t.d. í Notepad ætti hún að líta svipað út og á myndinni hér fyrir neðan.



2. Umsókn fyllt út á vef Auðkennis:

Umsóknin er á þessari slóð:

<https://umsoknir.audkenni.is/bunadarskilriki/bunadarskilrikiFG.cfm>

Fylla þarf í alla reyti nema Athugasemdir.

Forráðamaður þarf að hafa prókúru á fyrirtækið eða umboð frá slíkum.

Tæknilegur tengiliður er sá sem Auðkennis sendir dreifilykilinn.

Í CSR reitinn þarf að setja innihald CSR skrár sem umsækjandi bjó til.

Best að opna CSR skrá í Notepad og afrita (copy) allt innihaldið og líma (paste) þarna inn.

Ef ekki er þegar til áskriftarsamningur milli fyrirtækis og Auðkennis mun forráðamaður fá samninginn sendan rafrænt til rafrænnar undirritunnar.

Þegar búið er að fylla út umsóknina eru tölvupóstar sendir á netföng forráðamanns og tæknilegs tengiliðs. Forráðamaður þarf að smella á hlekkinn „SAMÞYKKJA UMSÓKN“ og tæknilegur tengiliður þarf að smella á hlekkinn „STAÐFESTA NETFANG“.

Auðkenni kannar prókúru forráðamanns.

Ef prókúra er til staðar, áskriftarsamningur undirritaður, forráðamaður og tæknilegur tengiliður búnir að smella á hlekkina í tölvupóstunum er umsóknin samþykkt og dreifilykill framleiddur og skrá sem inniheldur dreifilykil, milliskilríki og rót send á tæknilegan tengilið.

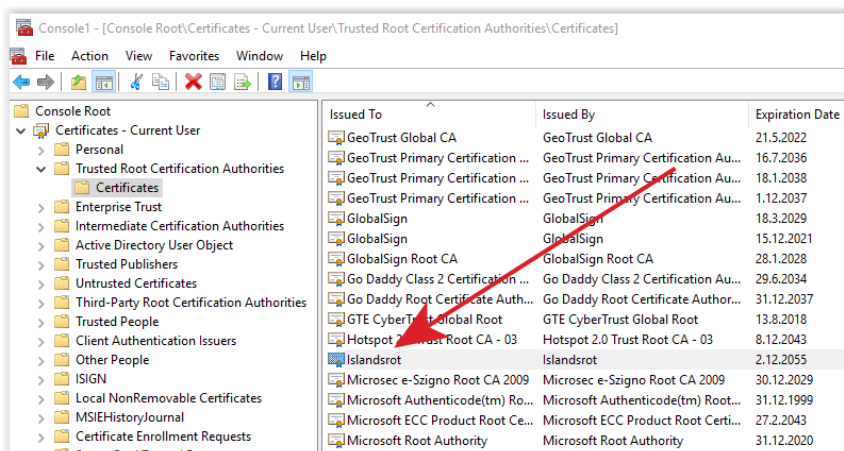
3. Íslandsrót og milliskilríkið Fullgilt auðkenni sett upp á tölvunni:

Til að búnaðarskilríkin virki þarf rötarskilríkið Íslandsrót og milliskilríkið Fullgilt auðkenni að vera til staðar á tölvunni.

Hér getur þú séð hvort þau eru á tölvunni:

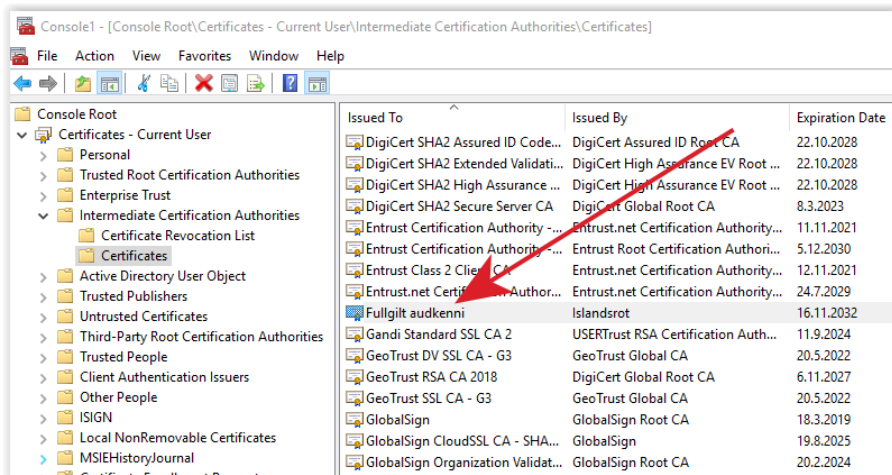
(Til að opna **MMC Console** aftur getur þú farið eftir **leiðbeiningunum á bls. 2)**

Rótin **Íslandsrót** á að vera undir **Trusted Root Certification Authorities/Certificates**:



Ath. það er eðlilegt að þarna sé fullt af öðrum skilríkjum.

Milliskilríkið **Fullgilt audkenni** á að vera undir **Intermediate Certification Authorities/Certificates**:



Ef skilríki hafa verið notuð á tölvunni áður eru miklar líkur á að þessi skilríki séu þegar til staðar en ef þú ert ekki viss borgar sig að setja þau upp, það gerir ekkert til þó þau séu til staðar nú þegar.

Hér getur þú sótt skilríkin:

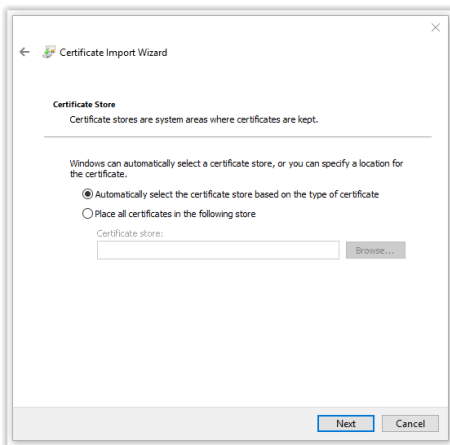
<https://www.audkenni.is/fyrirtaeki/skilriki-fyrirtaekja/bunadarskilriki/skilrikjakedjabunadarskilrikja/>

Þú þarft að setja upp bæði skilríkin og það er sama aðferðin við að setja þau upp.

Þú vistar .cer skrána á tölvunni og hægrismellir á hana og velur: **Install Certificate**

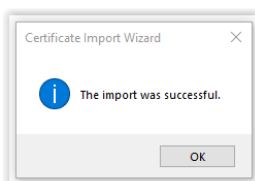
Þá opnast **Certificate Import Wizard** glugginn og þú smellir á **Next**.

Veldu: **Automatically select the certificate store...** og smelltu á **Next**

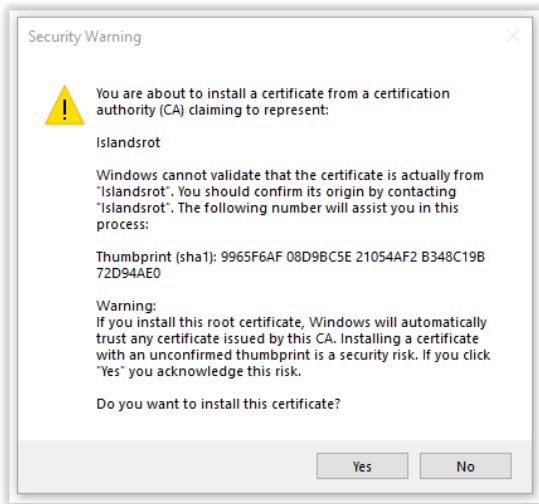


Þá kemur **Completing the Certificate Import Wizard** og þú smellir á **Finish**.

Glugginn hverfur og eftir stutta stund kemur minni gluggi sem segir: **The import was successful.**



Ef verið er að setja upp Íslandsrótin í fyrsta skipti kemur viðvörunargluggi upp sem í stuttu máli er að spyrja hvort þú viljir treysta rótinni. Smelltu á **Yes** til að segja tölvunni að treysta rótinni. Ef ekki er smellt á **Yes** treystir tölvan ekki Íslandsrót og þá munbúnaðarskilríkið ekki virka á þessari tölvu.

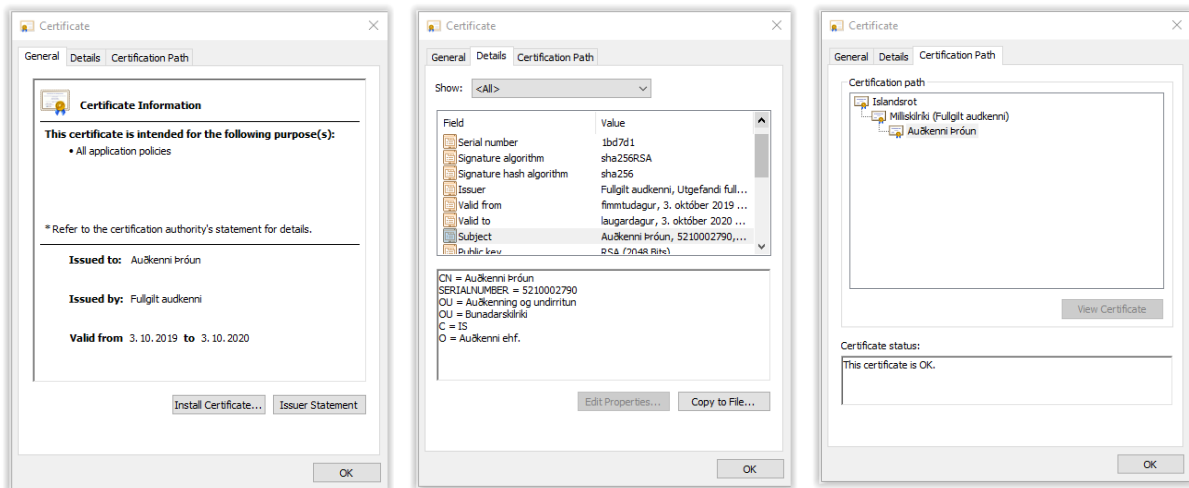


4. Búnaðarskilríkið sett upp á tölvunni:

Tæknilegur tengiliður ætti að vera búinn að fá .cer skrá senda frá Auðkenni. Þessa skrá má alveg senda bönkum og fleirum þar sem hún inniheldur ekki einkalykil skilríkisins. Sumir bankar vilja fá þessa skrá senda þegar verið er að setja upp ný búnaðarskilríki.

Skráin er keyrð á sömu vél og CSR var útbúið á. Dreifilykillinn finnur einkalykilinn sem er þegar á tölvunni og saman mynda þeir nýtt búnaðarskilríki.

Hægt er að skoða skrána með því að tvísmella á hana. Hún að líta svipað út og hér fyrir neðan.

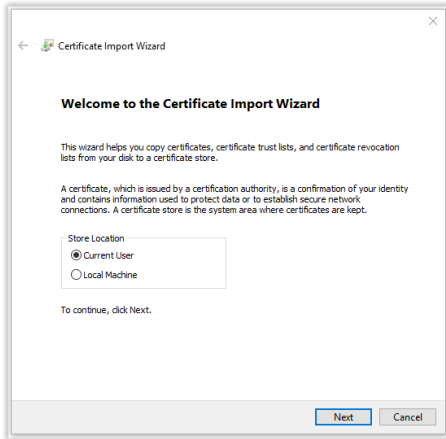


Til að keyra skrána skal hægri smella á hana og velja **Install Certificate**. Þá opnast **Certificate Import Wizard** glugginn.

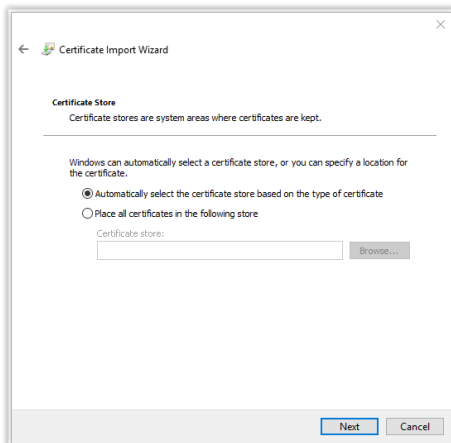
Certificate Import Wizard glugginn:

Hægt er að velja milli **Current User** eða **Local Machine** skilríkjageymslu. Í leiðbeiningunum fyrir CSR var notast við **Current User**. Það verður að vera það sama svo við höldum okkur áfram við það hér.

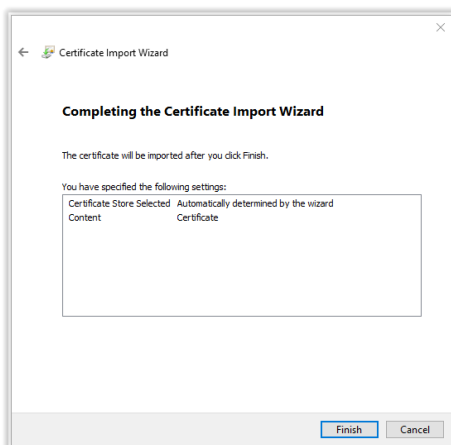
Smelltu á **Next**.



Veldu **Automatically select the certificate store based on the type of certificate** og smelltu á **Next**



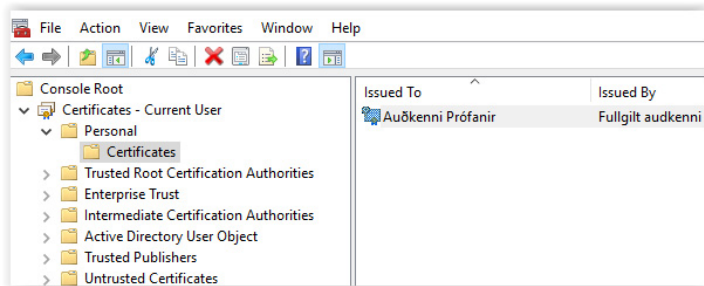
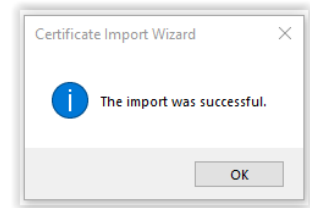
Þá kemur síðasti glugginn og þú smellir á **Finish**.



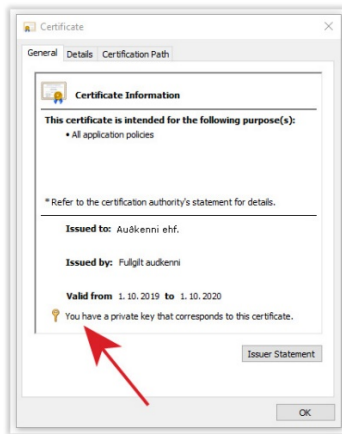
Glugginn hverfur og ef allt er eðlilegt birtist þessi gluggi eftir nokkrar sekúndur. Smelltu á **OK** og hann hverfur.

Skilríkið ætti nú að vera uppsett á þessari tölvu.

Til að gulltryggja að allt sé eins og það á að vera borgar sig að skoða skilríkið. Það á að vera undir **Personal/Certificates**.



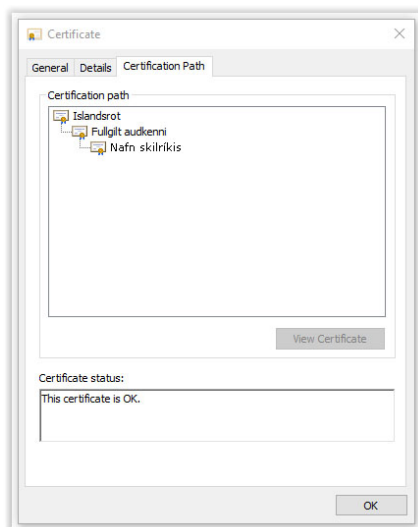
Tvísmelltu á skilríkið og þá færðu þessa mynd:



Það verður að standa: **You have a private key tha corresponds to this certificate**

Næst skaltu velja **Certification Path** flippann

Þá á þetta að líta út eins og hér á myndinni, Islandsrot – Fullgilt audkenni – Þitt skilríki



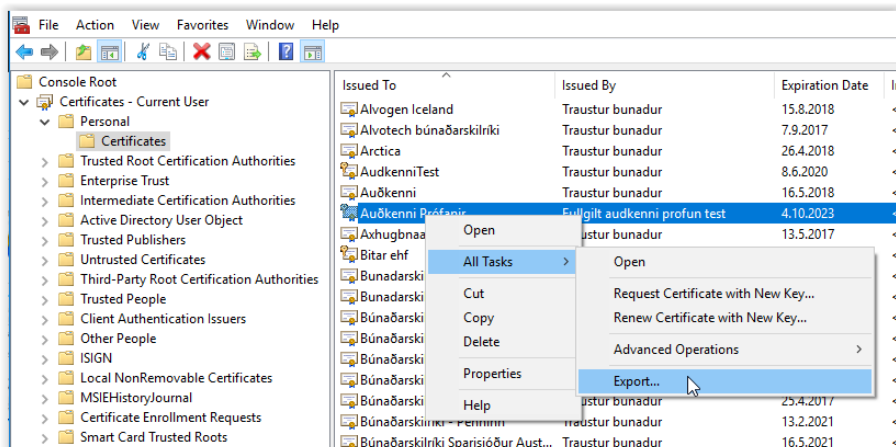
Ef það er rauður cross yfir Islandsrot eða Fullgilt audkenni þarf að setja þau skilríki á tölvuna.

Ef allt lítur eðlilega út er hægt er að flytja út skilríkið út í pfx skrá og setja upp á fleiri tölvur. Sjá leiðbeiningar um það hér fyrir neðan.

5. Flytja búnaðarskilríkið út í pfx skrá:

Ef setja þarf upp skilríkið á fleiri tölvur er hægt að flytja það út í pfx skrá með einkalyklinum, dreifilyklinum, milliskilríki og rót á einfaldan hátt.

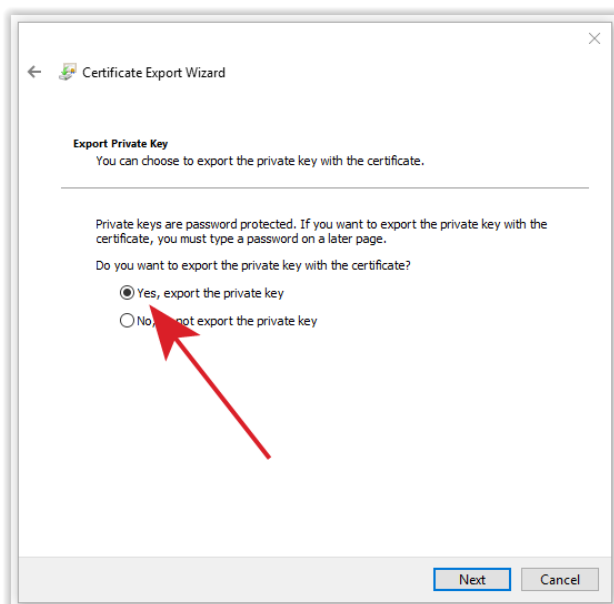
Í **mmc Console** skaltu hægrismella á búnaðarskilríkið og velja: **All Tasks > Export...**



Þá opnast **Certificate Export Wizard** glugginn:

Smelltu á **Next**

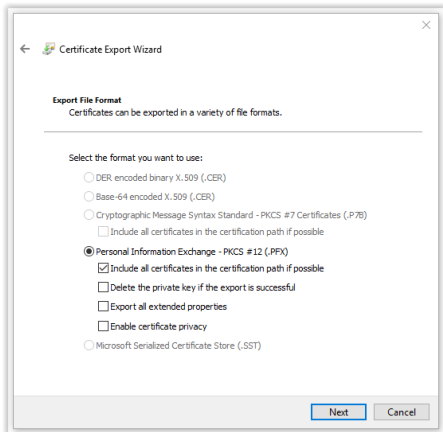
Veldu: **Yes, export the private key**



Smelltu á **Next**

Personal Information Exchange á að vera valið.

Hafðu hakað í **Include all certificates – PKCS #12 (.PFX)** Annað þarf ekki að haka í.

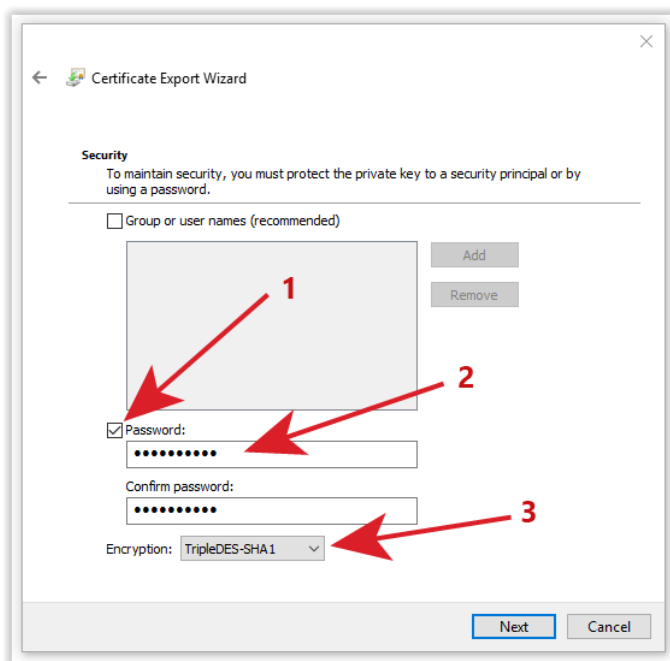


Smelltu á **Next**

1. Hakaðu í Password:

2. Veldu traust lykilorð. Það verndar skrána og notast þegar skilríkin eru sett upp á annarri tölvu.

3. Í Encryption: skaltu hafa það sem er sjálfgefið, **TripleDES-SHA1**



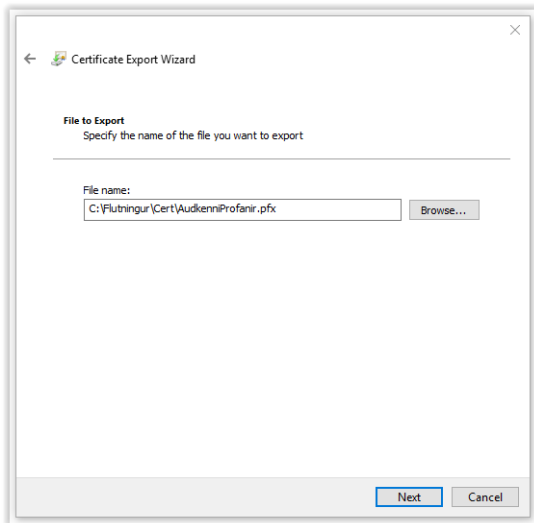
Smelltu á **Next**

Þá er komið að því að velja hvar skilríkið er vistað á tölvunni.

Smelltu á **Browse**, þá opnast annar gluggi. Veldu hvar skilríkið er vistað og nafn á skrána.

Smelltu á **Save** og þá lokast glugginn.

Slóðin og nafnið á pfx skránni er í File name: svæðinu í Certificate Export Wizard glugganum.



Smelltu á **Next** og svo **Finish**.

Lítill gluggi birtist með: **The export was successful**, smelltu á **OK**, báðir gluggar lokast og þá á skilríkið ásamt skilríkjakleðju að vera vistað í pfx skrá þar sem þú valdir að vista hana.

Til að setja skilríkin upp á annarri tölvu er tvísmellt á pfx skránni og þá opnast **Certificate Import Wizard**. Allir valmöguleikar eru hafðir sjálfgefdir (default) og einfaldlega smellt á Next 2x, lykilorð sem búið var til þegar pfx skráin var útbúin slegið inn. Smellt á Next 2x og svo Finish. Þá eru skilríkin uppsett með Íslandsrót og milliskilríkinu Fullgilt audkenni á tölvunni.

Bókhaldskerfi og bankar:

Ef þú ert að nota búnaðarskilríkin í samskiptum milli bókhaldskerfis og banka borgar sig að hafa samband við þá banka sem þú ert að tengjast við. Sumir þeirra þurfa að vita af því ef komin eru ný búnaðarskilríki og sumir vilja fá sendan dreifilykilinn fyrir skilríkið, .cer skránni sem er í lagi að senda þeim.

Innskráning með rafrænum skilríkjum á vefsvæði

Þjónustuveitendur sem nýta rafræn skilríki til innskráningar á sín vefsvæði þurfa að setja upp búnaðarskilríki og Auðkenni þarf að skrá dreifilykil þess í sín kerfi. Innskráning **VIRKAR EKKI** nema þjónustuveitandi sendi Auðkenni afrit af dreiflykli skilríkisins.

Ef þjónustuveitandi setur upp nýtt búnaðarskilríki **VERÐUR** að senda Auðkenni afrit af nýja dreifilyklinum.

Aðstoð:

Ef þú lendir í vandræðum og þessar leiðbeiningar eru ekki að duga þá getur þú haft samband við Auðkenni í síma 530-0000 eða í tölvupósti audkenni@audkenni.is