ELEKTRONIKUS TANÚSÍTVÁNY HASZNÁLATA

A REGIONAL BOOKING PLATFORMON,

A KERESKEDÉSI PLATFORMON ÉS

AZ FGSZ ZRT. INFROMARTIKAI PLATFORMJÁN

2018. 10. 01.

VERZIÓ 2.4.

Készítette: FGSZ Zrt.
Értékesítés és Ügyféltámogatás

Az FGSZ Zrt. elkötelezett az informatikai biztonság fejlesztése és magas színvonalon tartása mellett. A Regional Booking Platform, Informatikai Platform és Kereskedési Platform korszerű és kényelmes műszaki megoldások bázisán támogatja a Rendszerhasználók jogosultság alapú hozzáférését a webes technológiával megvalósított szolgáltatásokhoz.

A megfelelő módon kibocsátott és használt elektronikus tanúsítvány elemi feltétele annak, hogy Önt informatikai rendszereink aktív felhasználói között tudhassuk.

1. Az elektronikus tanúsítvány fogalma

Az elektronikus tanúsítvány olyan „elektronikus dokumentum", melyet elektronikus tanúsítvány kibocsátására felhatalmazott, (minősített) bizalmi szolgáltató bocsát ki abból a célból, hogy a nem biztonságos hálózatokon az elektronikus tanúsítvány tulajdonosa által küldött dokumentum valódiságát tanúsítsa, illetve őt magát az általa kezdeményezett adatforgalmazás ideje alatt hitelt érdemlően igazolja.

2. Általános ismeretek

Az elektronikus tanúsítvány egy elektronikus kódpár (kulcspár), amely egy titkos (privát, vagy aláíró) és egy nyilvános (publikus) kulcsból áll. A titkos kulcs az elektronikus tanúsítvány alanyának kizárólagos birtokában van, azzal senki más nem rendelkezhet (nem adható át), míg a nyilvános kulcs bárki számára hozzáférhető.

Az elektronikus tanúsítványhoz tartozó titkos és nyilvános kulcspár segítségével létrehozható elektronikus aláírás, dokumentumok és üzenetek, illetve a hálózati adatforgalom titkosító segítségével. Ezt a típusú kódolási eljárást nyilvános kulcsú kódolási technológiának nevezzük, míg a technológiához tartozó különböző eljárásrendeket, szervezeteket, illetve eszközöket együttesen Nyilvános Kulcsú Infrastruktúrának (PKI – Public Key Infrastructure).

Ha az aláíró (titkos) kulccsal kódolunk egy dokumentumot, adatkapcsolatot, akkor az csak és kizárólag a titkos kulcshoz tartozó nyilvános kulccsal dekódolható, fejthető vissza, mialatt biztosak lehetünk a küldő fél kilétében.

3. Elektronikus tanúsítvánnyal szemben támasztott követelmények

Az elektronikus tanúsítványoknak több típusa létezik. A Regional Booking Platform, Informatikai Platform és Kereskedési Platform eléréséhez használandó elektronikus tanúsítványnak a következő feltételeknek kell megfelelnie:

- Külső, minősített bizalmi szolgáltató állítja ki.
- A minősített bizalmi szolgáltató az igénylő személyazonosságának ellenőrzése után bocsátja ki az elektronikus tanúsítványt, amely az igénylő természetes személy vagy szervezeti tanúsítvány esetén az igénylő jogi személy felhasználó azonosítására alkalmas.
- Tanúsítvány regisztrálása a Platformokon létrehozott profilon belül
- Az elektronikus tanúsítvánnyal kapcsolatos technikai követelmény, hogy az alábbi feltételek teljesülésével alkalmas legyen ügyfél hitelesítésre (autentikáció céljára):
    - **Version**: v3
    - **Signature algorithm:** sha256RSA
    - **Signature hash algorithm:** sha256 (SHA1 nem támogatott)
    - **Public key:** RSA és minimum (2048 Bits) (pl. ECC (384 Bits) nem támogatott)
    - **Issuer:** publikusan elérhető CRL lista, harmadik fél által hitelesített tanúsítvány kiállító (belső PKI szolgáltatásból származó tanúsítványt nem támogatott)
    - **Valid:** javasoljuk, hogy legalább egy év érvényességi ideje legyen (de lehet több is)
    - **Key Usage:** Smart Card Logon, Client Authentication képes legyen a tanúsítvány (pl. Digital Signature (80))
    - Subject E mező és/vagy a Subject Alternative Name (RFC822 Name): tartalmazza az emailcímet melyre a tanúsítvány ki lett állítva (ha mindkettőt akkor ezeknek egyeznie kell)
    - Rendelkezésre kell állnia a teljes tanúsítványláncot felépítő root és intermediate tanúsítványoknak

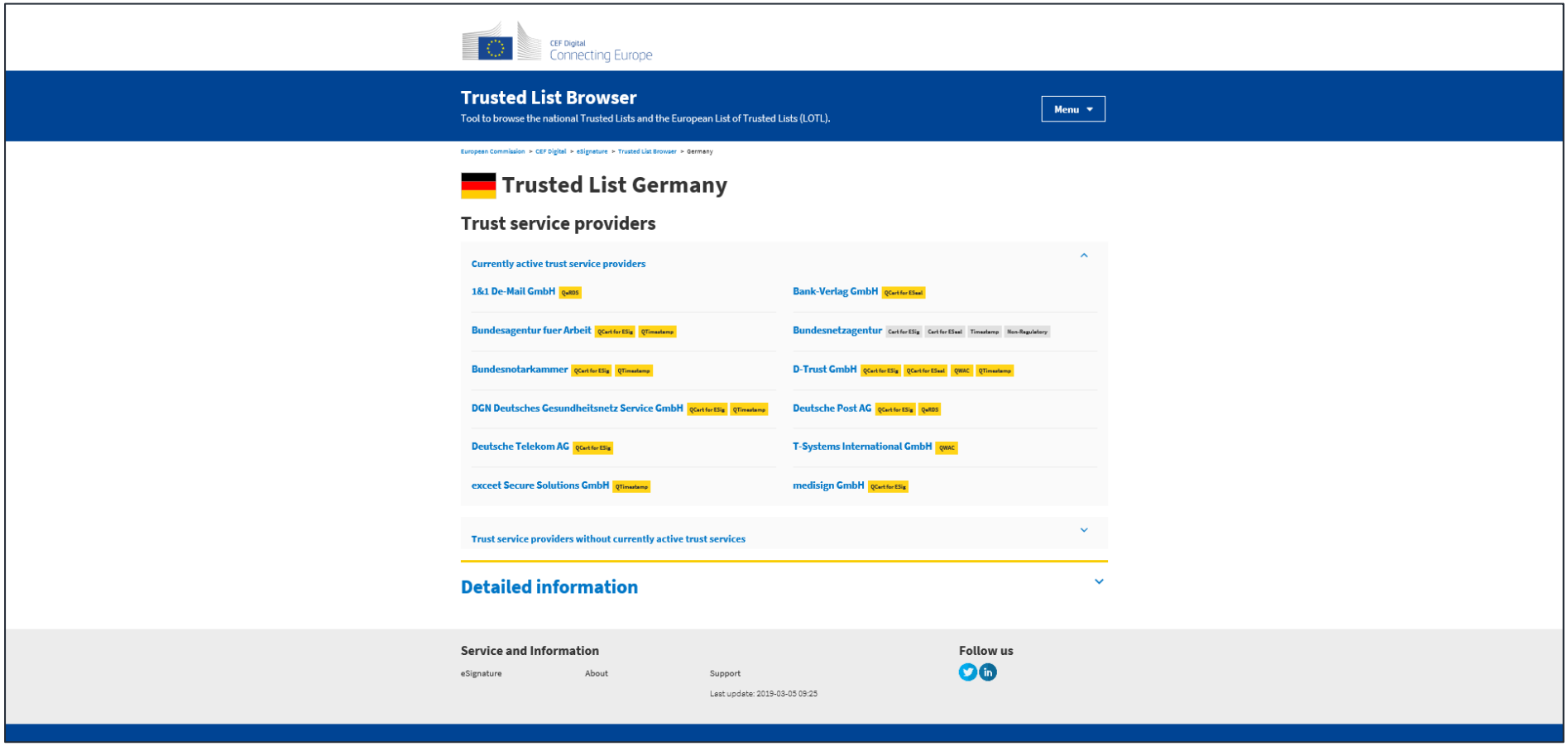
Fontos megjegyzés:

Kötelező megadni a tényleges e-mail címet a tanúsítvány „Tulajdonos" mező „E" attribútumában vagy az alternatív név mezőben. A rendszer biztonságának fenntartása érdekében a Regional Booking Platform, Informatikai Platform és Kereskedési Platform nem támogatja az azonos e-mail címmel rendelkező tanúsítványok használatát. Az alkalmazás üzemeltető jogosult visszautasítani olyan új tanúsítvány befogadását melynek e-mail címe a rendszerben már rögzítésre került.

Szervezeti tanúsítványt a tulajdonos jogi személy képviseletében felhasználó természetes személy(ek) felelősségét a tulajdonos jogi személyre, valamint a jogi személy és a tanúsítványt felhasználó természetes személy közötti jogviszonyra irányadó jogszabályok, és az irányadó belső szabályzatok szabályozzák. Az ilyen jogviszony tekintetében az FGSZ Zrt. minden felelősséget kizár a szervezeti tanúsítványok használatát illetően.

4. Elektronikus tanúsítvány beszerzése

Az elektronikus tanúsítvány olyan szervezettől szerezhető be, amely elektronikus tanúsítvány kiállítására felhatalmazott, minősített bizalmi szolgáltató (Trusted Service Provider - TSP), szerepel a 910/2014/EU Rendelet szerinti, az Európai Unió tagállamai által összeállított minősített bizalmi szolgáltatókat tartalmazó nemzeti listák valamelyikén. A nemzeti listákat tartalmazó európai uniós lista az „EU Trusted Lists of Certification Service Providers” az alábbi címen található: https://webgate.ec.europa.eu/tl-browser/#/



Az ezen nemzeti listákon kívüli szolgáltatók által kibocsátott tanúsítványokat az RBP Üzemeltető a 2016. július 1-je után regisztráló felhasználók esetében már nem fogadja el.

A korábban csatlakozott felhasználók a meglévő tanúsítványuk lejárta után kötelesek a nemzeti listák valamelyikén szereplő szolgáltatók által kibocsátott tanúsítványt beszerezni az RBP további használata érdekében.

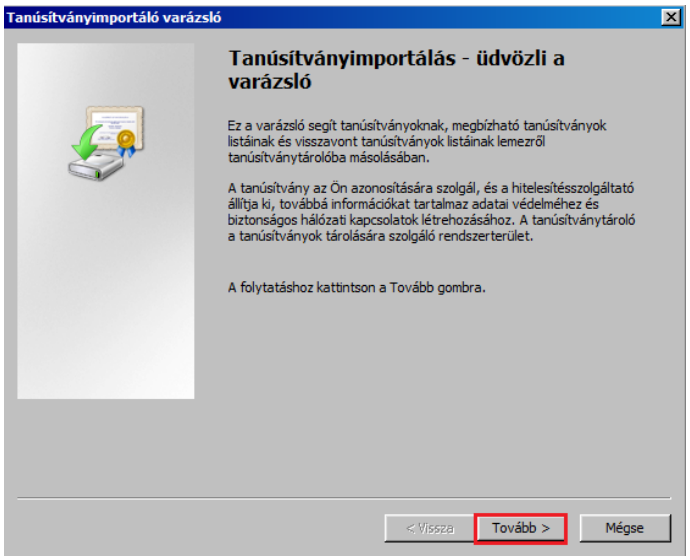
Az elektronikus tanúsítvány titkos kulcsa nem ruházható át, nem adható ki.

5. Elektronikus tanúsítvány telepítése

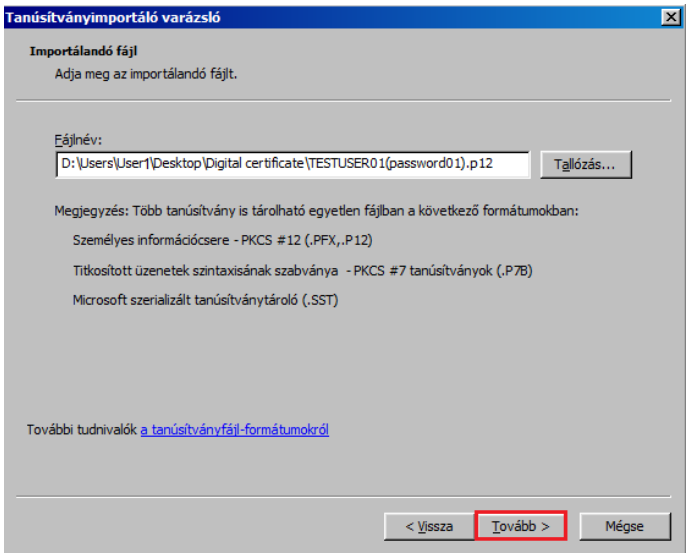
Az elektronikus tanúsítványt a használatba vétel előtt telepíteni kell saját számítógépünkre.

a. Internet Explorer esetében

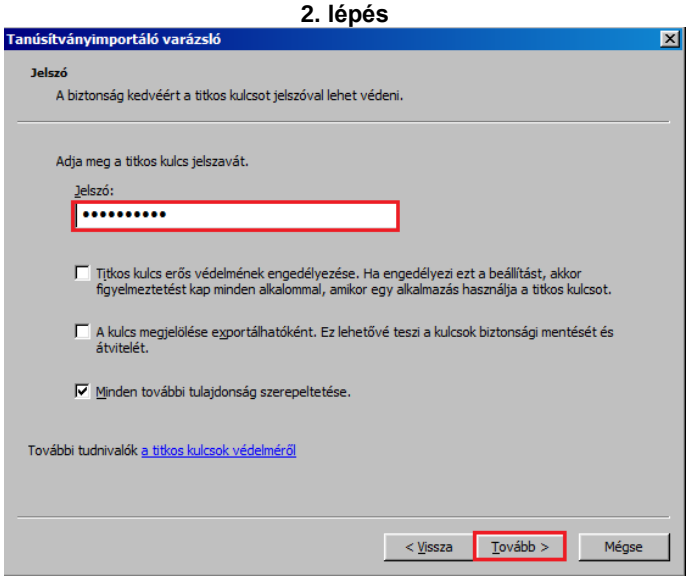
- egy tetszőleges fájlkezelő alkalmazással (Windows Intéző, stb.) meg kell keresni a tanúsítvány tárolóját, ami legtöbb esetben egy p12 (PKCS #12) kiterjesztésű fájl, amely jelszóval védett titkosított formában tartalmazza a tanúsítványt és a titkos kulcsot
- a tanúsítvány tárolóra történő dupla kattintással kezdeményezni kell a telepítést
- Tovább nyomógomb (1. lépés)
- Tovább nyomógomb (2. lépés)
- Jelszó megadása (3. lépés)
- Tovább nyomógomb (4. lépés)
- Személyes tároló választása (alapértelmezett) (5. lépés)
- Tovább nyomógomb (6. lépés)
- Befejezés nyomógomb (7. lépés)



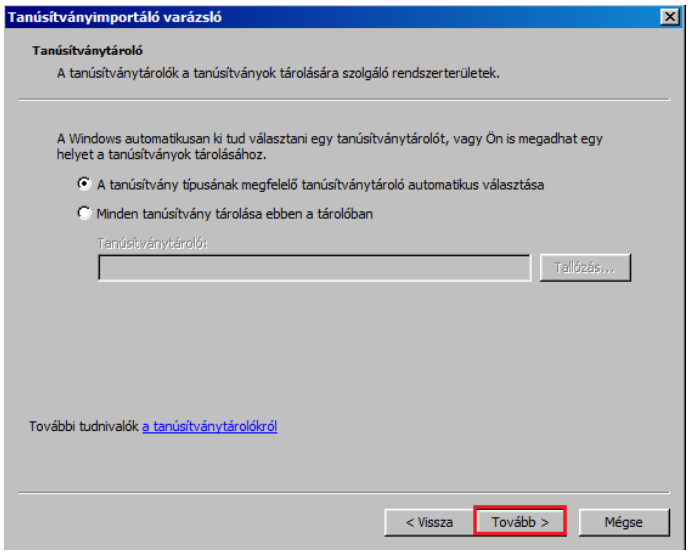
1. lépés



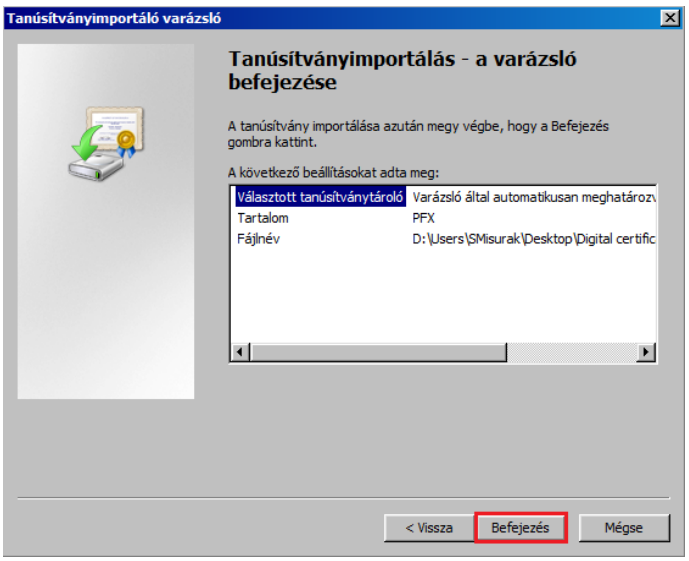
2. lépés



3-4. lépés



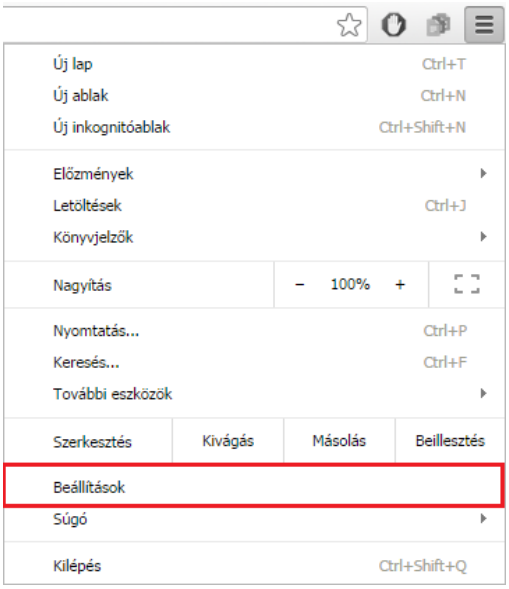
5-6. lépés



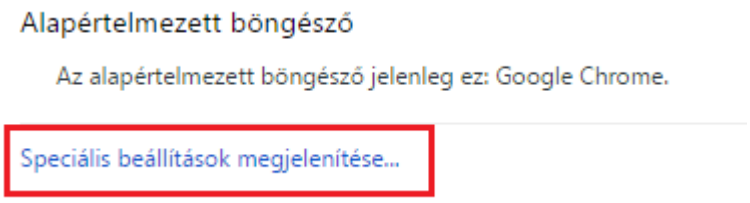
7. lépés

b. Google Chrome esetében:

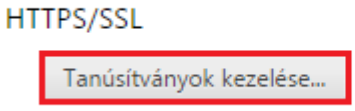
- Beállítások menü (1. lépés)
- Speciális beállítások megjelenítése (2. lépés)
- Tanúsítványok kezelése (3. lépés)
- Importálás nyomógomb (4. lépés)
- Tovább nyomógomb (5. lépés)
- Tanúsítvány tallózása, majd Tovább nyomógomb (6. lépés)
- Jelszó megadása, majd Tovább nyomógomb (7. lépés)
- Személyes tároló választása (alapértelmezett), majd Tovább nyomógomb (8. lépés)
- Befejezés nyomógomb (9. lépés)



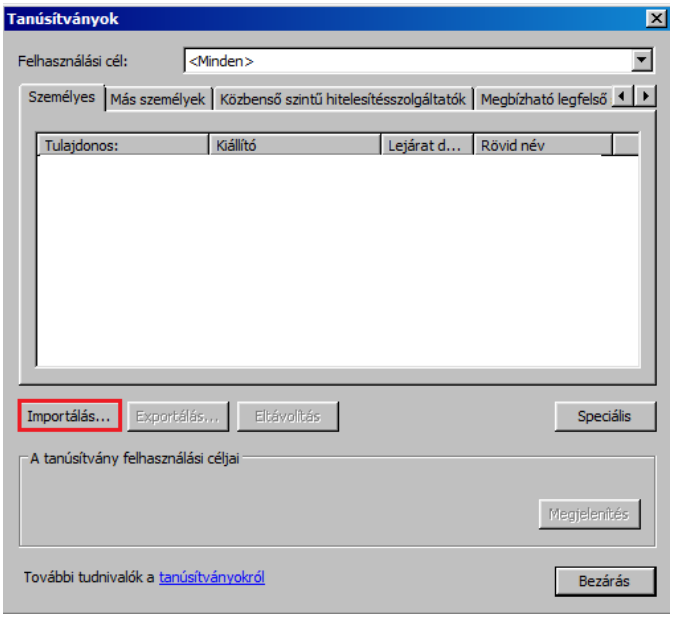
1. lépés



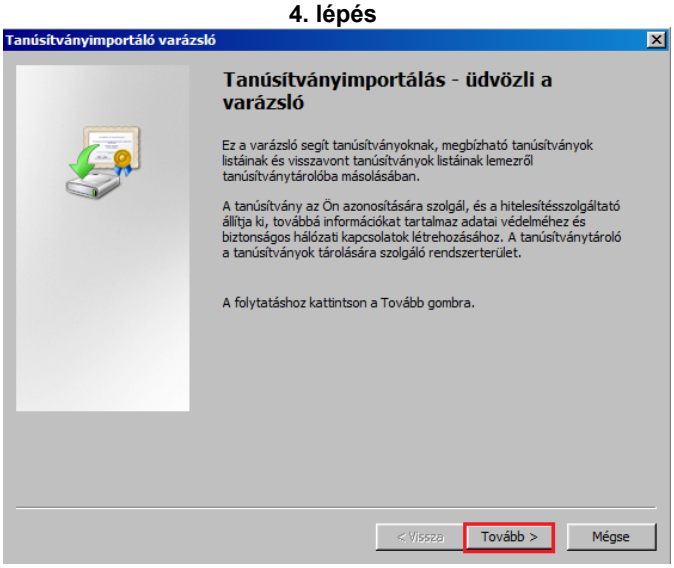
2. lépés



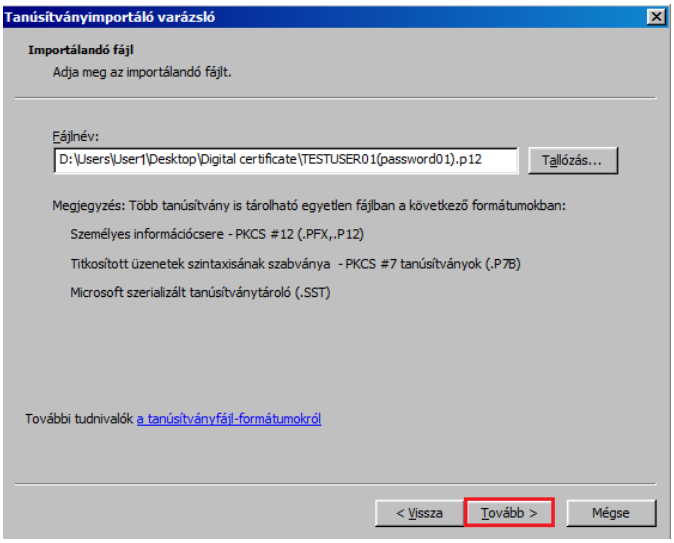
3. lépés



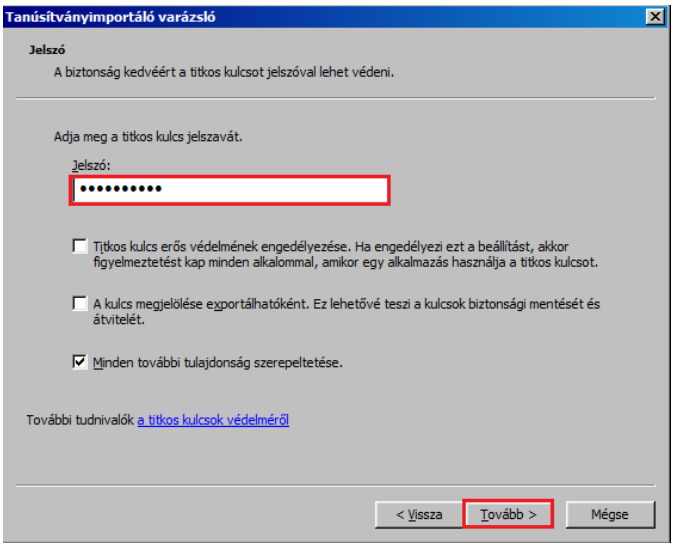
4. lépés



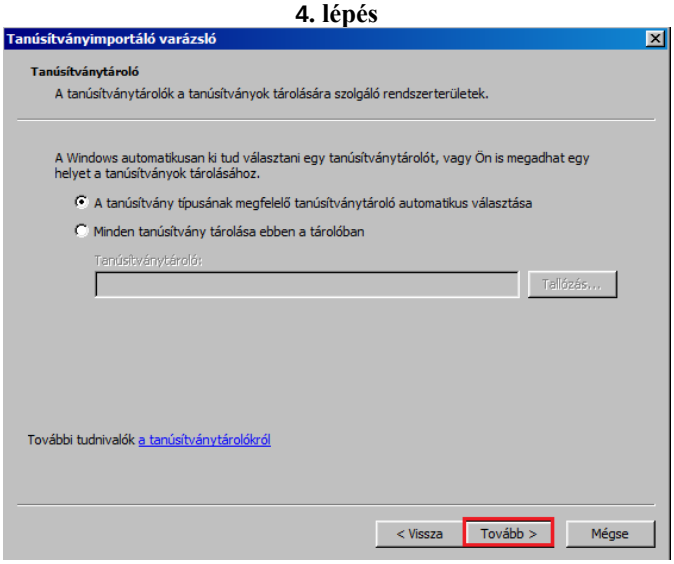
5. lépés



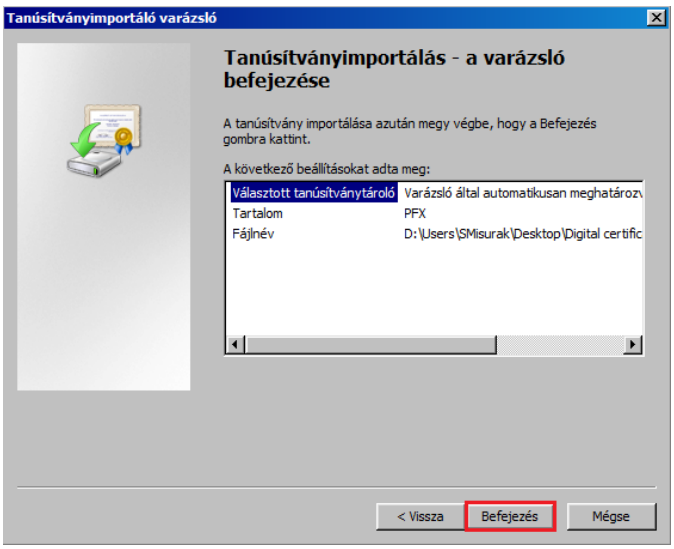
6. lépés



4. lépés



5. lépés



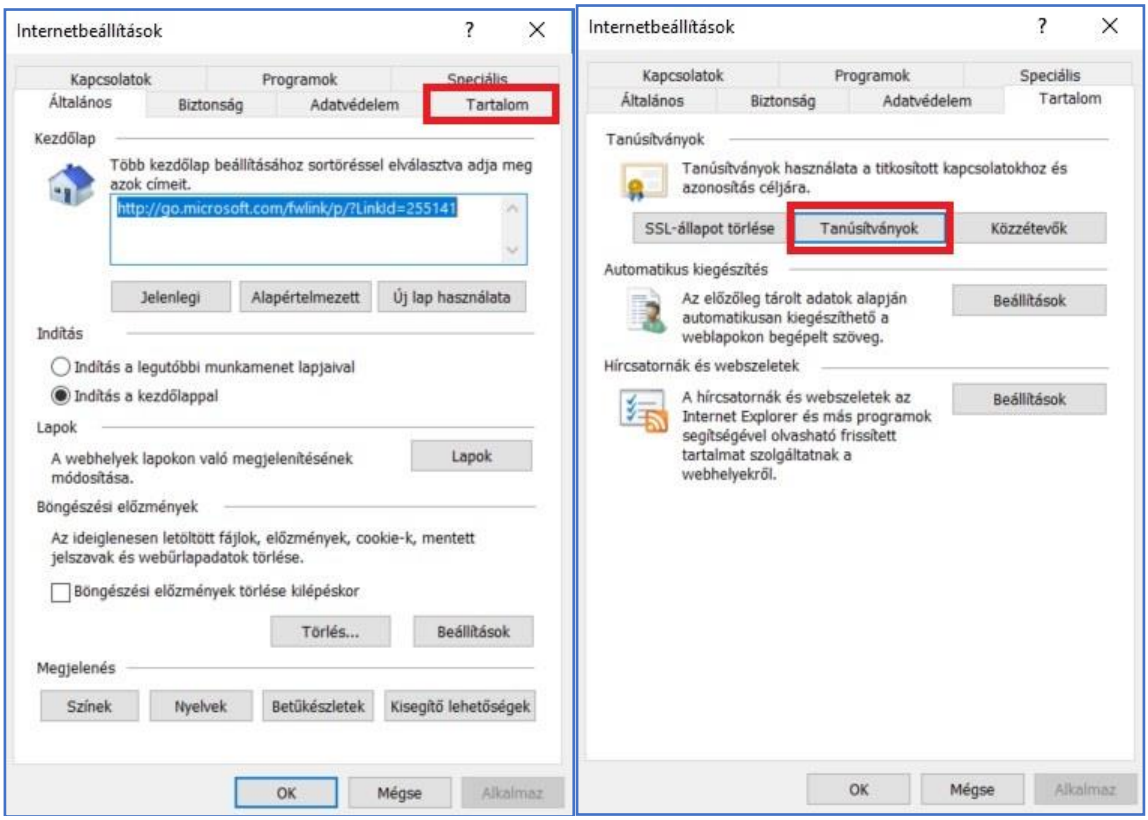
6. lépés

6. Elektronikus tanúsítvány nyilvános részének (.cer) kinyerése böngészőből

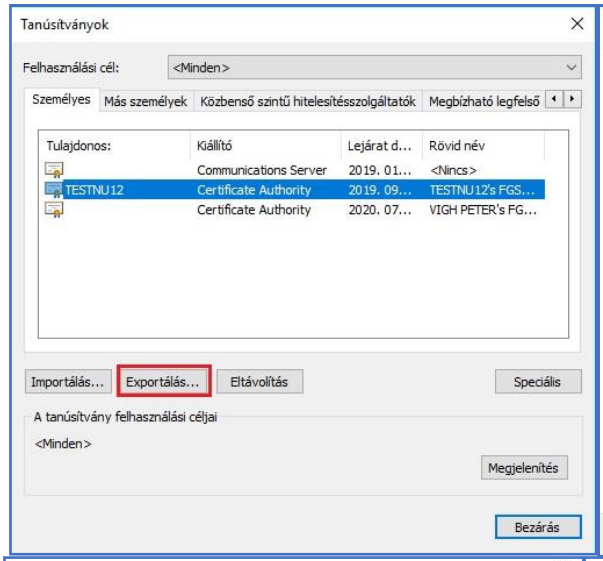
A felhasználók által használt elektronikus tanúsítványok nyilvánosa része (.cer) az alábbi módon nyerhető ki. Az letöltés lépései a következők:

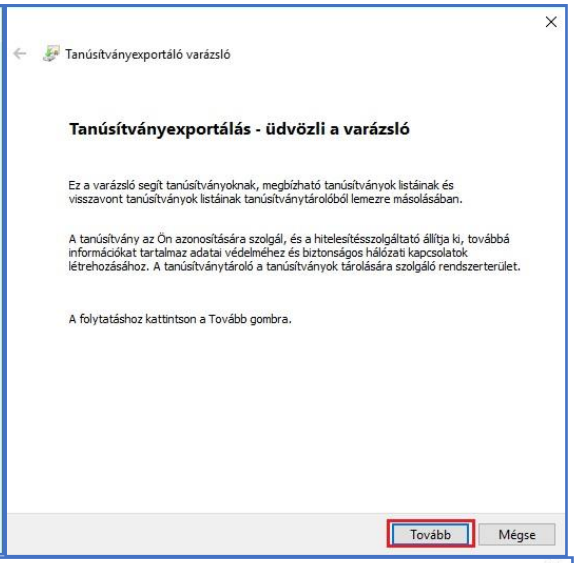
- „Eszközök” gombon belül, legördülő menüből az „Internetbeállítások” kiválasztása (1. lépés)
- Tartalom fül kiválasztása. Kattintás a „Tanúsítványok” gombra (2. lépés)
- A kívánt tanúsítvány kiválasztása, kattintás az „Exportálás” gombra. (3. lépés)
- Tanúsítványexportáló varázsló elindul. Kattintás a „Tovább” gombra. (4. lépés)
- „Nem, nem akarom exportálni a titkos kulcsomat.” lehetőség választása. (5. lépés)
- „Base64 kódolású X.509(.CER)” lehetőség választása (6. lépés)

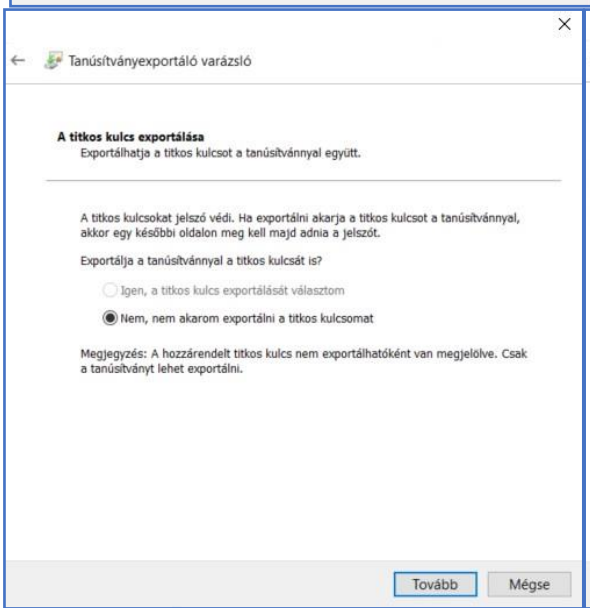
1. **és 2. lépés**

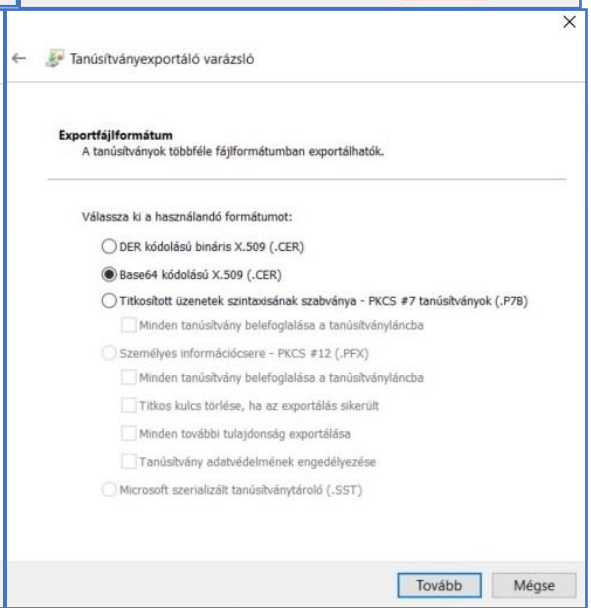


3. -6. lépés


Tanúsítványok
Felhasználási cél:
<Minden>
Személyes
Más személyek
Közbenső szintű hitelesítésszolgáltatók
Megbízható legfelső
Tulajdonos:
Kiállító
Lejárat d...
Rövid név
Communications Server
2019. 01...
<Nincs>
TESTNU12
Certificate Authority
2019. 09...
TESTNU12's FGS...
Certificate Authority
2020. 07...
VIGH PETER's FG...
Importálás...
Exportálás...
Eltávolítás
Speciális
A tanúsítvány felhasználási céljai
<Minden>
Megjelenítés
Bezárás


Tanúsítványexportáló varázsló
Tanúsítványexportálás - üdvözli a varázsló
Ez a varázsló segít tanúsítványoknak, megbízható tanúsítványok listáinak és visszavont tanúsítványok listáinak tanúsítványtárolóból lemezre másolásában.
A tanúsítvány az Ön azonosítására szolgál, és a hitelesítésszolgáltató állítja ki, továbbá információkat tartalmaz adatai védelméhez és biztonságos hálózati kapcsolatok létrehozásához. A tanúsítványtároló a tanúsítványok tárolására szolgáló rendszerterület.
A folytatáshoz kattintson a Tovább gombra.
Tovább
Mégse


Tanúsítványexportáló varázsló
A titkos kulcs exportálása
Exportálhatja a titkos kulcsot a tanúsítvánnyal együtt.
A titkos kulcsokat jelszó védi. Ha exportálni akarja a titkos kulcsot a tanúsítvánnyal, akkor egy későbbi oldalon meg kell majd adnia a jelszót.
Exportálja a tanúsítvánnyal a titkos kulcsát is?
Igen, a titkos kulcs exportálását választom
Nem, nem akarom exportálni a titkos kulcsomat
Megjegyzés: A hozzárendelt titkos kulcs nem exportálhatóként van megjelölve. Csak a tanúsítványt lehet exportálni.
Tovább
Mégse

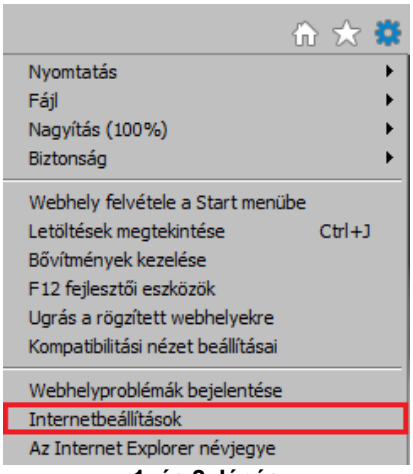

Tanúsítványexportáló varázsló
Exportfájlformátum
A tanúsítványok többféle fájlformátumban exportálhatók.
Válassza ki a használandó formátumot:
DER kódolású bináris X.509 (.CER)
Base64 kódolású X.509 (.CER)
Titkosított üzenetek szintaxisának szabványa - PKCS #7 tanúsítványok (.P7B)
Minden tanúsítvány belefoglalása a tanúsítványláncba
Személyes információcsere - PKCS #12 (.PFX)
Minden tanúsítvány belefoglalása a tanúsítványláncba
Titkos kulcs törlése, ha az exportálás sikerült
Minden további tulajdonság exportálása
Tanúsítvány adatvédelmének engedélyezése
Microsoft szerializált tanúsítványtároló (.SST)
Tovább
Mégse

7. Elektronikus tanúsítvány eltávolítása

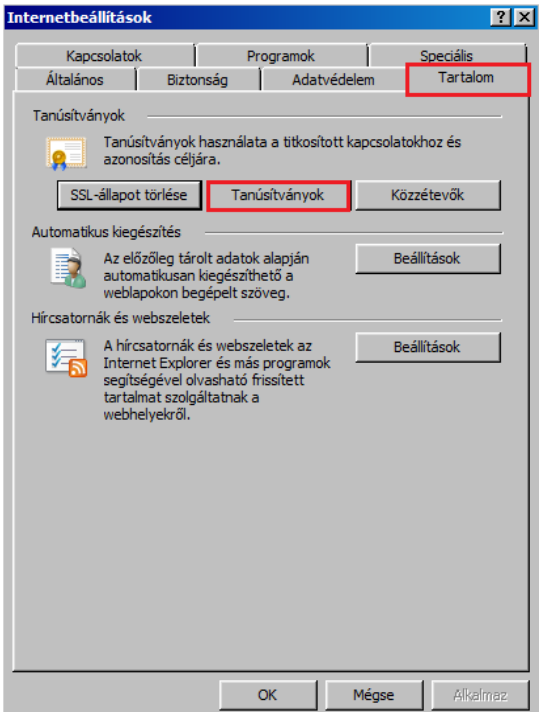
Az elektronikus tanúsítvánnyal történő visszaélések elkerülése végett a telepített tanúsítványt el kell távolítani, amennyiben azt már nem kívánja használni (pl.: munkakör-változás, gépcsere, stb.). Szintén célszerű a tanúsítvány eltávolítása olyan számítógépről, amelyre csak ideiglenes jelleggel telepítette azt.

a. Az eltávolításhoz a következőket kell végrehajtani Internet Explorer használata esetén:

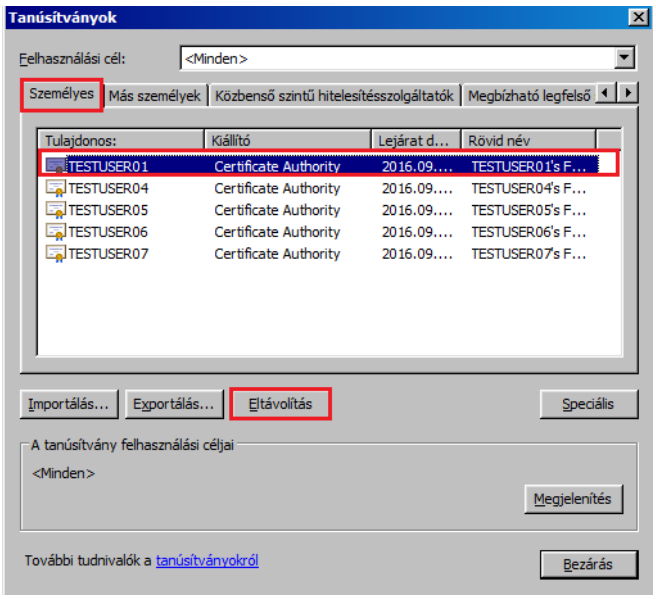
- Eszközök menü (1. lépés)
- Internet beállítások menü (2. lépés)
- Tartalom fül (3. lépés)
- Tanúsítványok nyomógomb (4. lépés)
- Személyes fül (alapértelmezett) (5. lépés)
- Tanúsítvány kiválasztása (6. lépés)
- Eltávolítás nyomógomb (7. lépés)
- Figyelmeztető ablakban „Igen” választása (8. lépés)



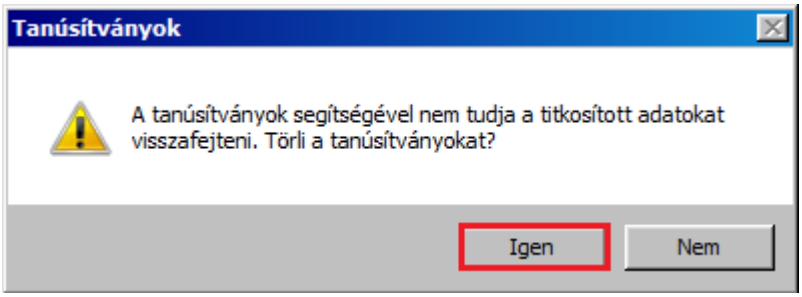
1. és 2. lépés



3. és 4. lépés



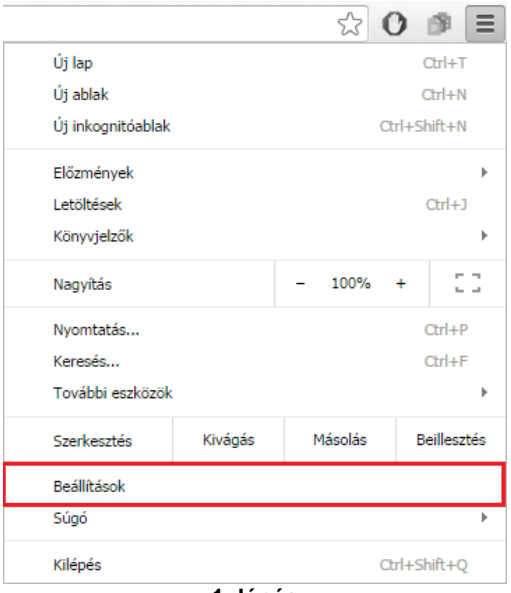
5.-6.-7. lépés



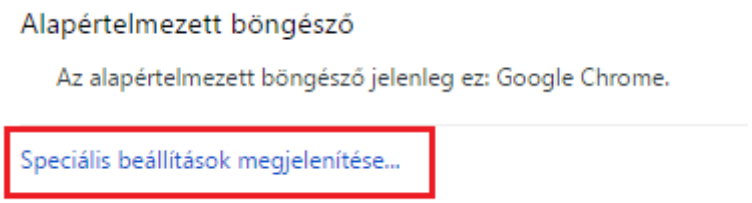
8. lépés

b. Az eltávolításhoz a következőket kell végrehajtani Google Chrome használata esetén:

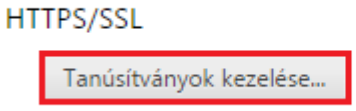
- Beállítások menü (1. lépés)
- Speciális beállítások megjelenítése (2. lépés)
- Tanúsítványok kezelése (3. lépés)
- Személyes fül (alapértelmezett) (4. lépés)
- Tanúsítvány kiválasztása (5.lépés)
- Eltávolítás nyomógomb (6. lépés)
- Figyelmeztető ablakban „Igen” választása (7. lépés)



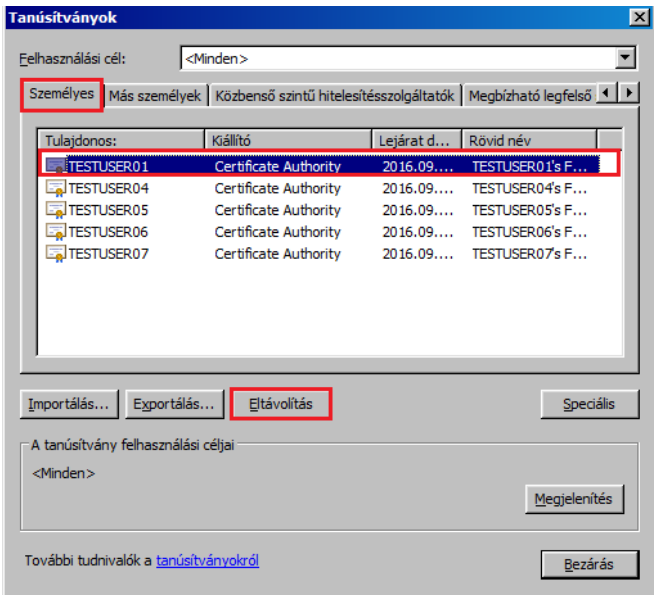
1. lépés



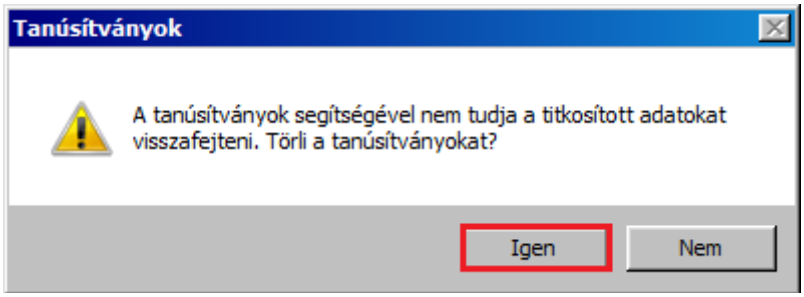
2. lépés



3. lépés



4.-5.-6. lépés



7. lépés

8. Elektronikus tanúsítvány használata

A Regionális Booking Platformra történő belépés során egy telepített elektronikus tanúsítvány esetén a rendszer azonnal belépteti a felhasználót, a munka megkezdhető.

Amennyiben több elektronikus tanúsítvány került telepítésre a felhasználó számítógépén, úgy megjelenik a tanúsítvány kiválasztó ablak, melyben valamennyi telepített tanúsítvány láthatóvá válik. Ebből a listából kiválasztható a Regionális Booking Platformon használni kívánt tanúsítvány.

9. Teendők számítógép elvesztése, ellopása esetén

Amennyiben számítógépét elveszti, vagy ellopják azt, kérjük, szíveskedjen haladéktalanul jelezni munkaidőben az rbp@fgsz.hu e-mail címen, munkaidőn túl a készenlétes kollégának, illetve a Regionális Booking Platform Felhasználói Megállapodásban rögzített kapcsolattartók egyikének, megakadályozandó az esetleges visszaélést.

10. Gyakori hibák és kezelésük módja

A gyakorlatban négyféle hiba szokott előfordulni, melyek a következők:

- az elektronikus tanúsítvány vagy a titkos kulcs nincs megfelelően telepítve a felhasználó számítógépére

Hibajelenség:	Egy tanúsítvány esetén nem jelenik meg a tanúsítvány kiválasztó ablak, illetve több tanúsítvány esetén megjelenik, de a kívánt tanúsítvány nincs a listában a Regionális Booking Platformra történő belépéskor, a belépés sikertelen.
Teendők:	A tanúsítvány állapotát 11. pont szerint ellenőrizni kell. Ha a tanúsítvány nincs telepítve, az 5. pont szerint telepíteni kell, melynek befejeztével célszerű ellenőrizni a 11. pont alapján annak sikerességét. Amennyiben a tanúsítvány szerepel a telepített tanúsítványok listájában, ellenőrizni kell annak érvényességét, ld. „elektronikus tanúsítvány lejárt” bekezdés.

- az elektronikus tanúsítvány nem tartalmaz e-mail címet az elvárt mezőben

  Hibajelenség: A tanúsítvány kiválasztó ablak a Regionális Booking Platformra történő belépéskor megjelenik, de ennek ellenére nem lehet belépni a rendszerbe a kiválasztott tanúsítvánnyal.

  Teendők: A tanúsítvány-telepítés sikerességét a 11. pont szerint ellenőrizni kell, különös tekintettel az e-mail címre.

- az e-mail cím pontatlanul szerepel az elvárt mezőben

  Hibajelenség: A tanúsítvány kiválasztó ablak a Regionális Booking Platformra történő belépéskor megjelenik, de ennek ellenére nem lehet belépni a rendszerbe a kiválasztott tanúsítvánnyal.

  Teendők: A tanúsítványban szereplő adatokat a 11. pont szerint ellenőrizni kell, különös tekintettel az e-mail címre. Amennyiben ez nem egyezik a tanúsítványt kibocsátó bizalmi szolgáltatóhoz benyújtott tanúsítvány iránti kérelemben foglalt e-mail címmel, a szolgáltatóval módosíttatni kell azt.

- a nyilvános kulcs nincs feltelepítve az FGSZ Zrt. szervereire

  Hibajelenség: A Regionális Booking Platformra történő belépéskor hibaüzenet utal a kapcsolat sikertelenségére, a belépés sikertelen.

  Teendők: A sikertelen belépésről tájékoztatni kell a 8. pontban feltüntetett kapcsolattartók egyikét, aki ellenőrzi az FGSZ Zrt. szerverein az adott nyilvános kulcs meglétét, majd segít a további teendőket illetően.

- az elektronikus tanúsítvány lejárt

  Hibajelenség: Egy tanúsítvány esetén nem jelenik meg a tanúsítvány kiválasztó ablak, illetve több tanúsítvány esetén megjelenik, de a kívánt tanúsítvány nincs a listában a Regionális Booking Platformra történő belépéskor, a belépés sikertelen.

  Teendők: A tanúsítványban szereplő adatokat a 11. pont szerint ellenőrizni kell, különös tekintettel a tanúsítvány érvényességére. Amennyiben lejárt az érvényessége, a tanúsítványt a kibocsátó bizalmi szolgáltatónál meghosszabbítható, vagy másik szolgáltatónál új tanúsítvány igényelhető.

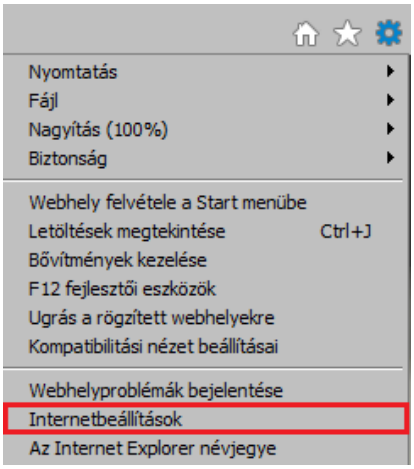
11. Elektronikus tanúsítvány ellenőrzése

A feltelepített elektronikus tanúsítványok adatainak ellenőrzése lehetőséget biztosít számos probléma kiküszöbölésében. Amennyiben igénybe veszi FGSZ Zrt. munkavállaló segítségét, ezen adatok szükségesek lehetnek a felmerült probléma elhárításában.

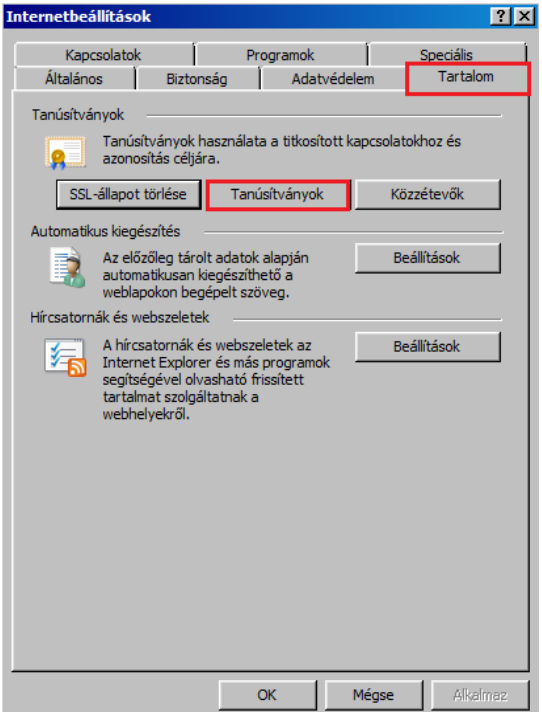
Az ellenőrzés lépései a következők:

a. Internet Explorer esetében

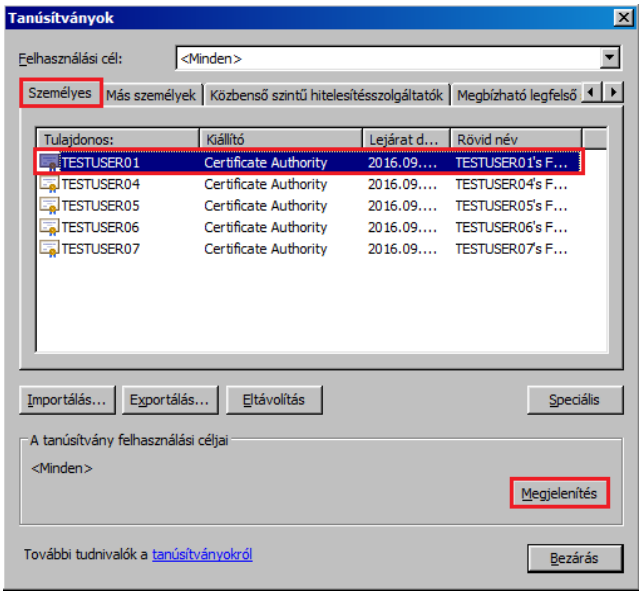
- Eszközök menü (1. lépés)
- Internetbeállítások menü (2. lépés)
- Tartalom fül (3. lépés)
- Tanúsítványok nyomógomb (4. lépés)
- Személyes fül (alapértelmezett) (5. lépés)
- Tanúsítvány kiválasztása (6. lépés)
- Megjelenítés nyomógomb (7. lépés)
- Általános fül (alapértelmezett): Érvényesség és érvényesség vége tekinthető meg
- Részletek fül: Kiállító szervezet, Érvényesség kezdete, Érvényesség vége, Tulajdonos, e-mail cím („E” mező), Nyilvános kulcs mező tekinthető meg



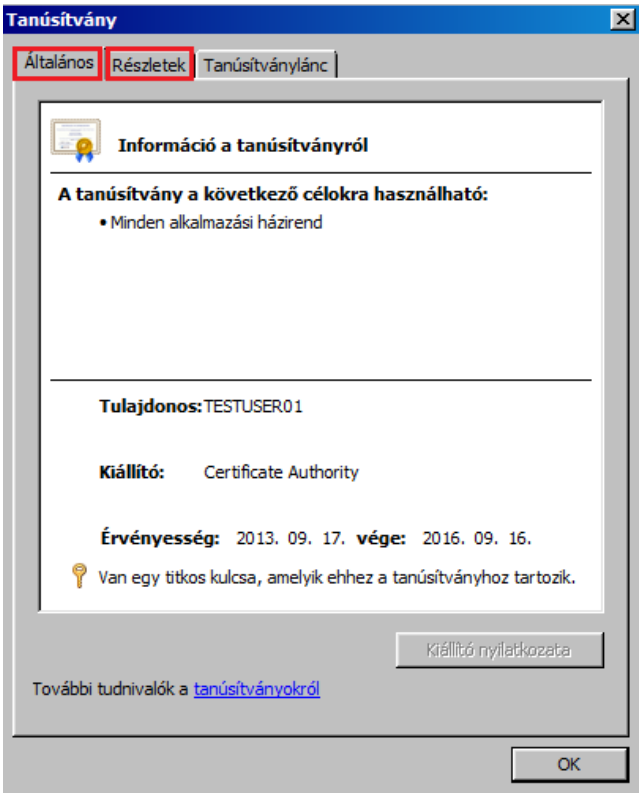
1. és 2. lépés



3. és 4. lépés



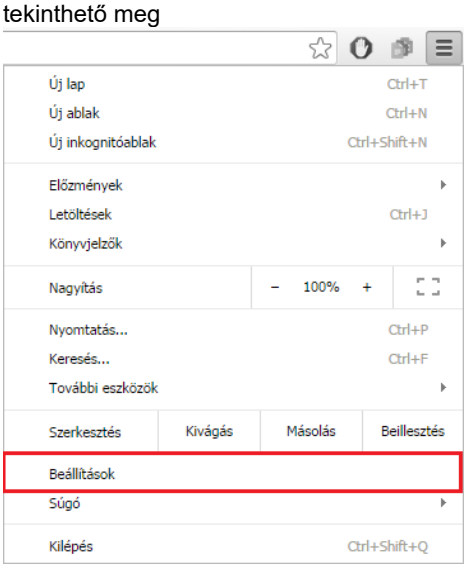
5.-6.-7. lépés



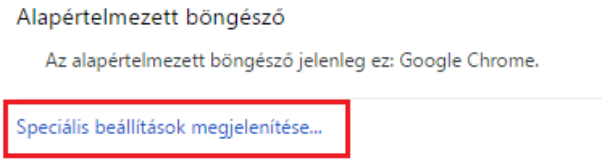
b. Google Chrome esetében

- Beállítások menü (1. lépés)
- Speciális beállítások megjelenítése (2. lépés)
- Tanúsítványok kezelése (3. lépés)
- Személyes fül (alapértelmezett) (4. lépés)
- Tanúsítvány kiválasztása (5. lépés)
- Megjelenítés nyomógomb (6. lépés)
- Általános fül: Tulajdonos, Kiállító szervezet, Érvényesség kezdete, Érvényesség vége tekinthető meg

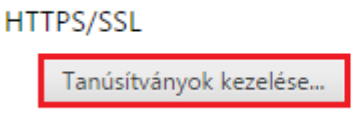
- Részletek fül: Kiállító szervezet, Érvényesség kezdete, Érvényesség vége, Tulajdonos, e-mail cím („E” mező), Nyilvános kulcs mező tekinthető meg



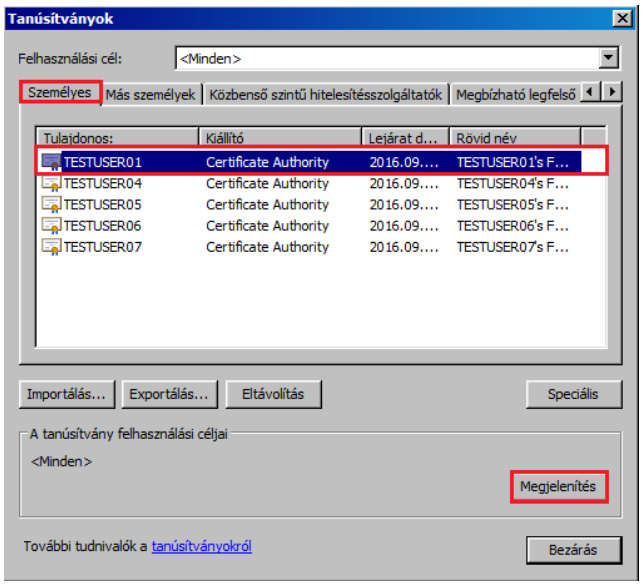
1. lépés



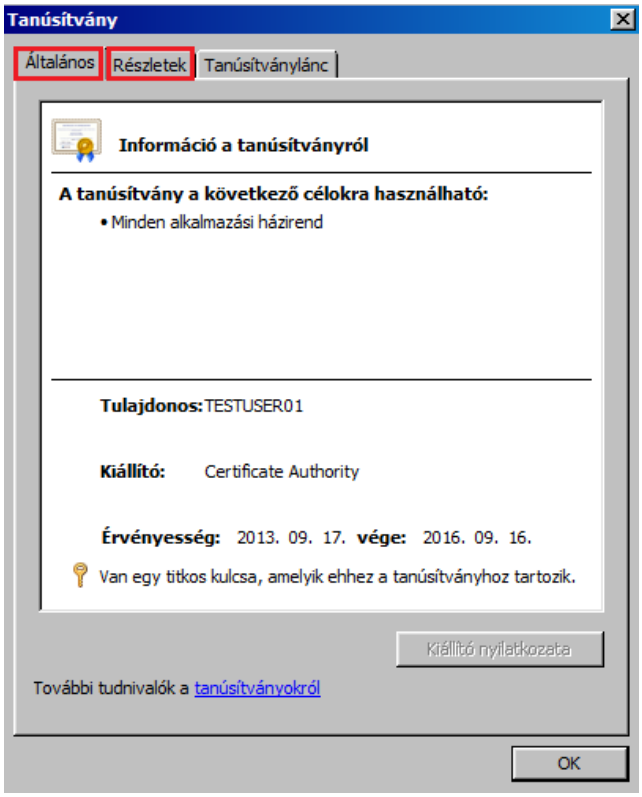
2. lépés



3. lépés



4.-5.-6. lépés


Tanúsítvány
Általános
Részletek
Tanúsítványlánc
Információ a tanúsítványról
A tanúsítvány a következő célokra használható:
• Minden alkalmazási házirend
Tulajdonos: TESTUSER01
Kiállító: Certificate Authority
Érvényesség: 2013. 09. 17. vége: 2016. 09. 16.
Van egy titkos kulcsa, amelyik ehhez a tanúsítványhoz tartozik.
Kiállító nyilatkozata
További tudnivalók a tanúsítványokról
OK

7. lépés