Import certifikátů a vytvoření keystore

Verze dokumentu 1.0 červenec 2021

Obsah

Seznam zkratek a pojmů uvedených v dokumentu

Pojem/zkratka	Text
E166/iszrAutentizaceAis	eGON služba pro ověření přistupujícího AIS k systému základních registrů
eGON služby	Služby poskytované přes vnější rozhraní ISZR a evidované v katalogu eGON služeb. Informace uvedené v Katalogu eGON služeb jsou určené implementátorům (programátorům) AIS pro jejich přípravu ke komunikaci se základními registry. Více informací na http://www.szrcr.cz/vyvojari.
GML	Značkovací jazyk geografie (GML), který stanoví gramatiku rozšiřitelného značkovacího jazyka (XML) napsanou ve Schématu XML pro popis aplikačních schémat geografické informace.
ID	Unikátní identifikátor prvku nebo operace.
ISÚI	**Informační systém územní identifikace** Editační agendový systém, jehož prostřednictvím jsou zapisována data do RÚIAN.
ISZR	**Informační systém základních registrů** Informační systém veřejné správy poskytující prostřednictvím eGON služeb referenční údaje ze základních registrů a vybrané nereferenční údaje ze spolupublikujících agendových informačních systémů s vazbou na referenční údaje.
keystore	Úložiště certifikátů pro Javu
OVM	**Orgán veřejné moci** Státní orgán, územní samosprávní celek a fyzická nebo právnická osoba, které byla svěřena působnost v oblasti veřejné správy, v souladu s definicí podle zákona o základních registrech.
request	Žádost ve formátu XML zaslaná na rozhraní webové služby.
RÚIAN	**Registr územní identifikace, adres a nemovitostí** Jeden ze čtyř základních registrů veřejné správy, který obsahuje údaje o územních prvcích, územně evidenčních jednotkách a adresy.
SoapUI	Volně dostupná (open source) aplikace pro testování webových služeb
truststore	Úložiště certifikátů certifikačních autorit pro Javu
validace	Proces porovnání žádosti XML oproti definici webové služby (WSDL, XSD)
WS	Webové služby
WSDL	Web Service Description Language – popisuje rozhraní webové služby
XML	eXtensible Markup Language
XSD	Definice struktury XML (XML Schema Definition)

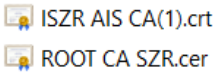
1. Certifikáty pro přístup k ISZR

Editační i informační služby na vnějším rozhraní ISZR jsou dostupné pouze s certifikátem (pro testovací nebo produkční prostředí), který vystaví na žádost SZR. Certifikát je tedy nezbytný pro úspěšnou autentifikaci a autorizaci OVM. Na základě žádosti dostanete sdělení o vydání certifikátu a certifikát, který je zabezpečený heslem.

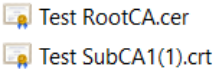
Ověření přistupujícího OVM probíhá přes eGON službu E166/iszrAutentizaceAis, jejíž specifikaci lze získat ve volně dostupném katalogu služeb.

Certifikáty pro přístup na rozhraní ISZR jsou k dispozici pro testovací nebo produkční prostředí ISZR, ke stažení jsou dostupné na webové stránce SZR: RAZR - Registrační autorita základních registrů. Stáhneme **Platné certifikáty CA** (soubor *certifikaty.zip)*, tento soubor obsahuje certifikáty do produkčního i testovacího prostředí ISZR.

Složka obsahuje certifikáty do produkčního prostředí:



A certifikáty do testovacího prostředí:



V případě, že chcete přistupovat na testovací prostředí ISZR, je potřeba přistupovat s certifikátem OVM vytvořeným pro testovací prostředí. Analogicky toto platí i pro produkční prostředí.

V dalších krocích se budeme věnovat importu certifikátů a zprovoznění na testovacím prostředí ISZR.

Certifikáty jsou nezbytné z hlediska bezpečnosti. Postup se provádí jako nezbytná příprava pro práci s certifikáty v prostředí softwaru SoapUI, ze stejného důvodu je také potřeba vytvořit závěrečný keystore a truststore, které SoapUI používá při práci s certifikáty. Je potřeba stáhnout kořenové soubory certifikační autority, která certifikáty vytvořila. Tímto postupem získáme certifikát včetně certifikačních autorit (CA).

2. Instalace pro zprovoznění služeb na testovacím ISZR

2.1 Instalace certifikátů v prohlížeči Microsoft Edge

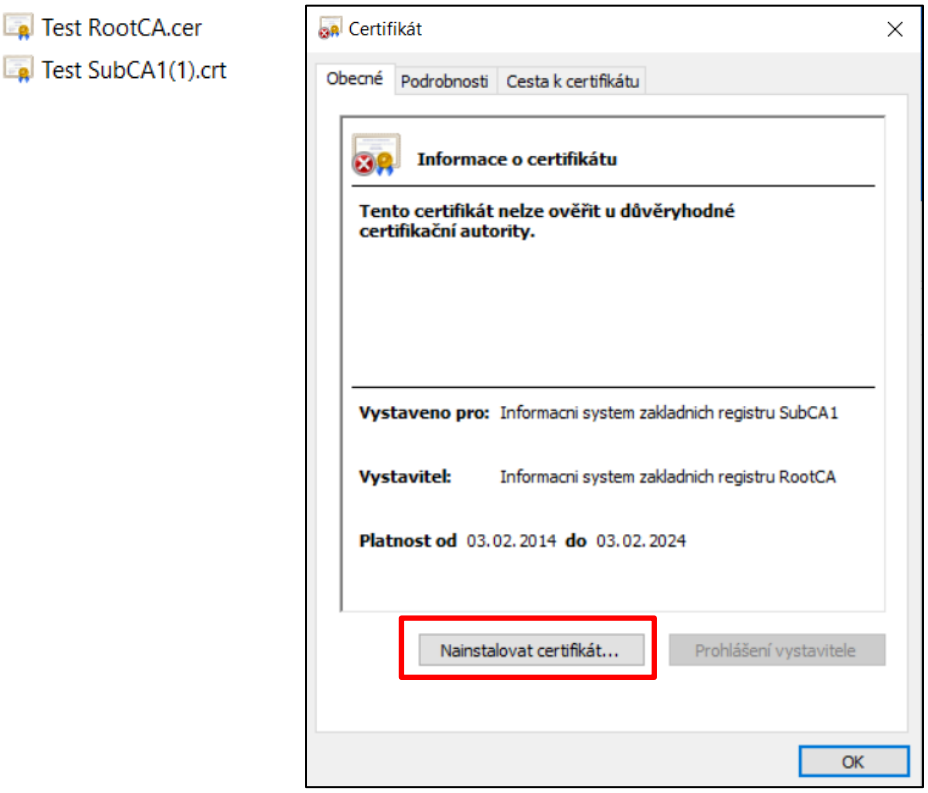
Instalaci certifikátů provedeme např. v prohlížeči Microsoft Edge (ME) nebo v jiném nástroji, který podporuje práci s certifikáty a jejich načtení.

2.1.1 Instalace certifikátů ISZR

Při instalaci certifikátů začneme instalací certifikátů pro testovací prostředí ISZR.

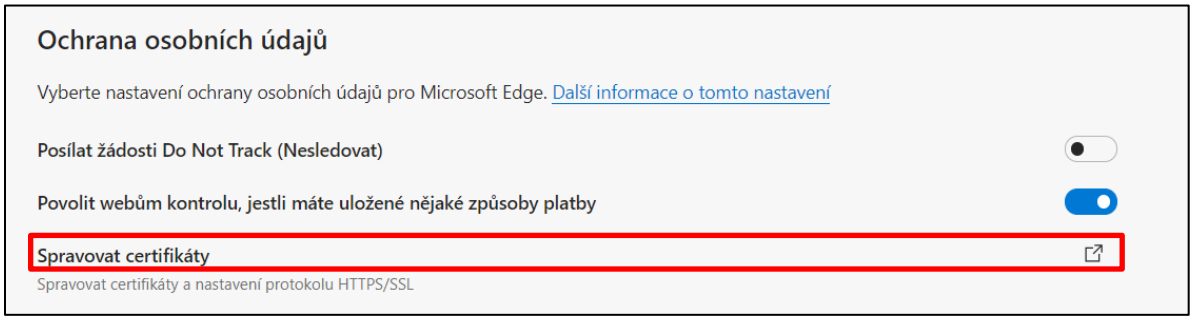
Certifikáty lze nainstalovat dvojím způsobem: Přímým dvojklikem na soubor – rovnou se spustí *Průvodce importem certifikátu* nebo v nastavení prohlížeče ME.

Postupně nainstalujeme oba certifikáty pro testovací ISZR:

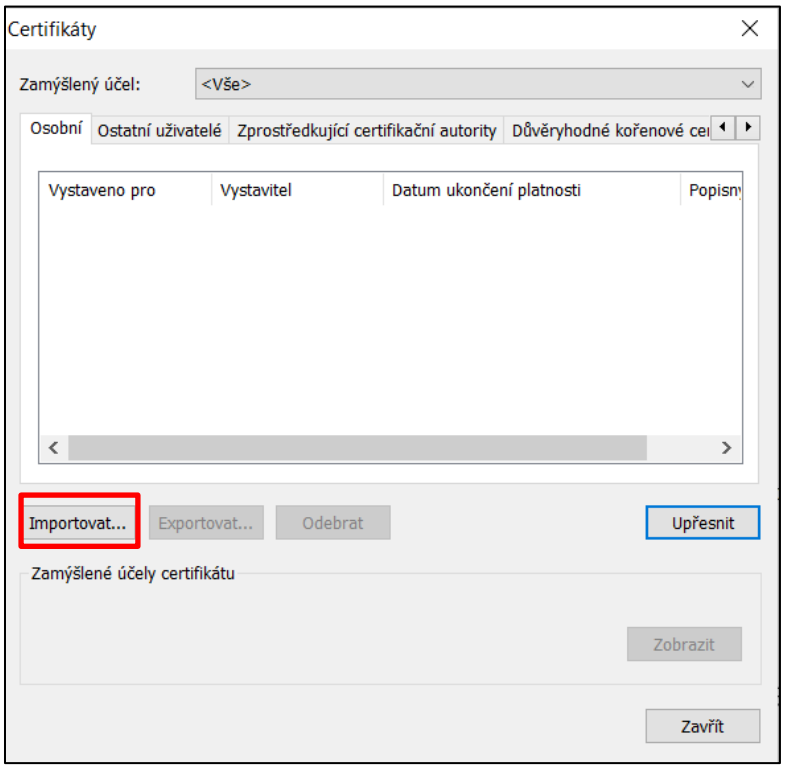


Instalace v ME → *Nastavení → Ochrana osobních údajů a služby → Spravovat certifikáty*.

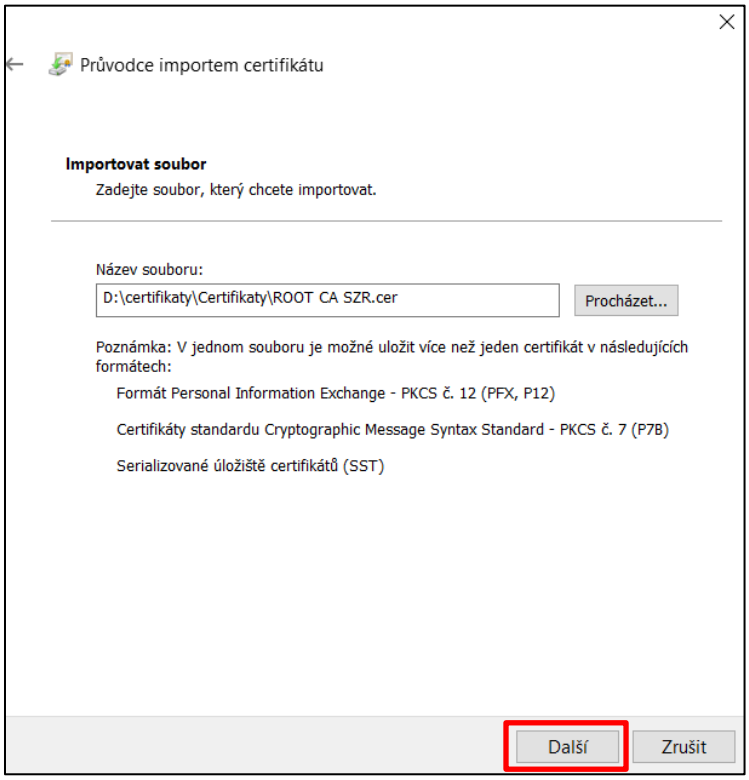
Zvolíme možnost *Spravovat certifikáty*



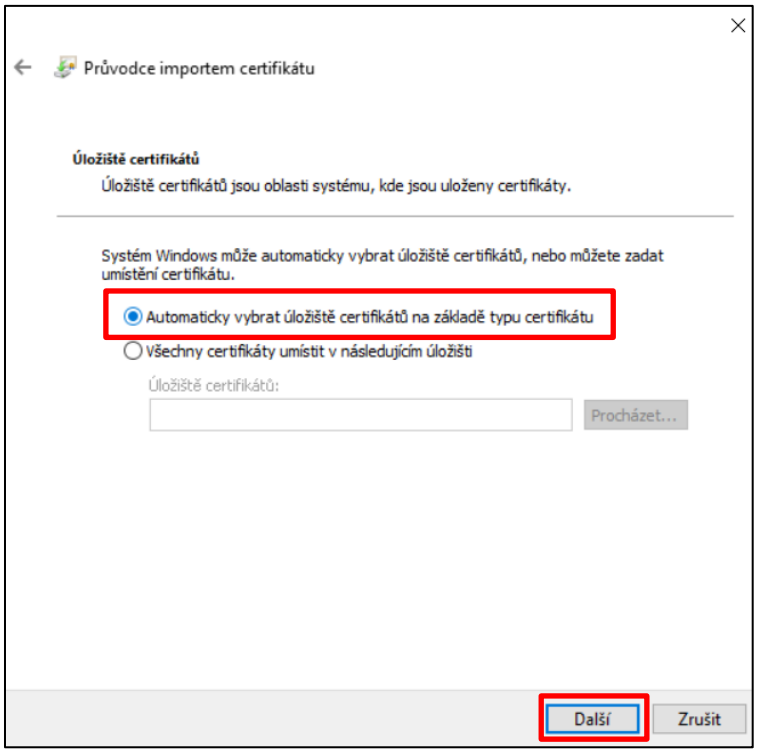
V okně Certifikáty stiskneme tlačítko *Importovat*

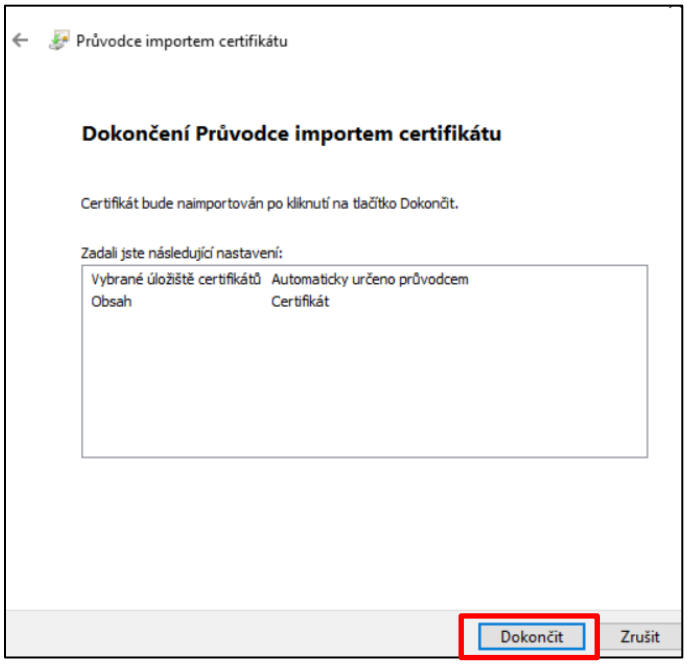


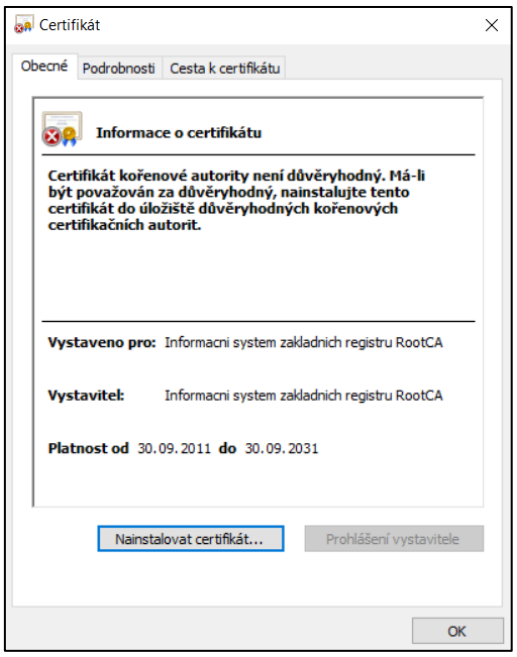
Vyhledáme uložený certifikát, který chceme importovat:

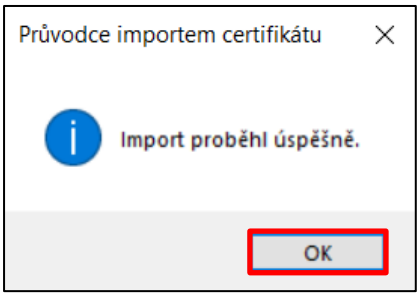


V průvodci importem certifikátu zvolíme výběr automatického úložiště na základě typu certifikátu:





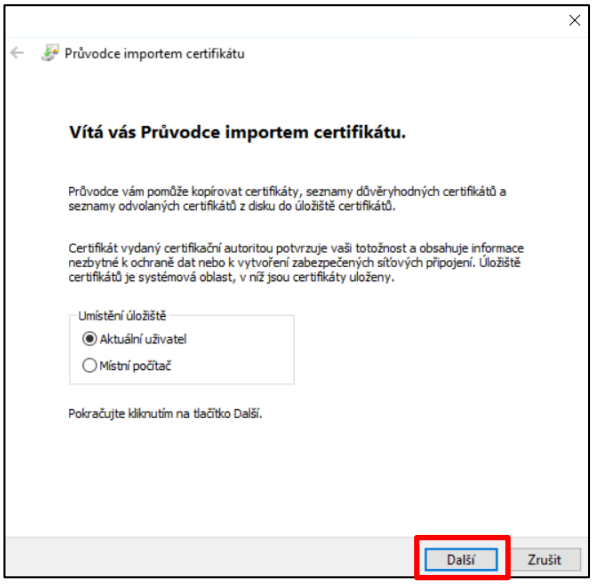


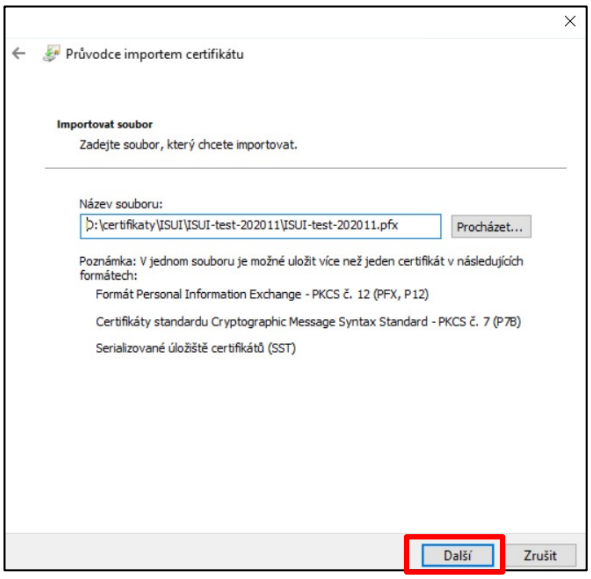


Instalaci provedeme stejným způsobem pro oba testovací certifikáty ISZR.

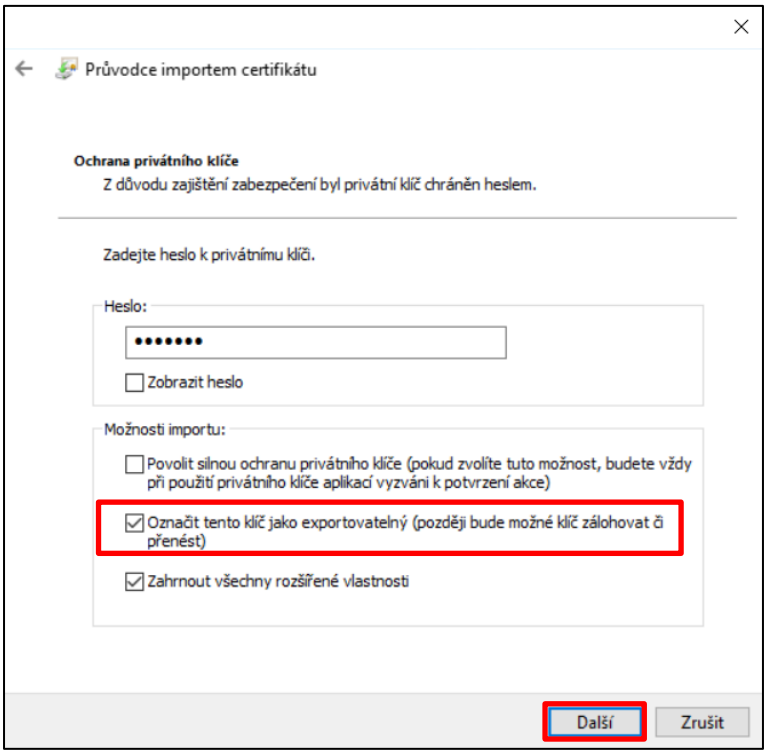
2.1.2 Instalace certifikátu OVM

Dále nainstalujeme vlastní certifikát, tedy certifikát vydaný SZR pro konkrétní OVM (v našem případě soubor ISUI-test-202011.pfx) a to také dvojklikem na soubor. Žádost o certifikát na testovacím i produkčním prostředí je potřeba zaslat přes Registrační autoritu základních registrů (RAZR), podrobnější informace jsou uvedené na adrese: https://razr.egon.gov.cz/.

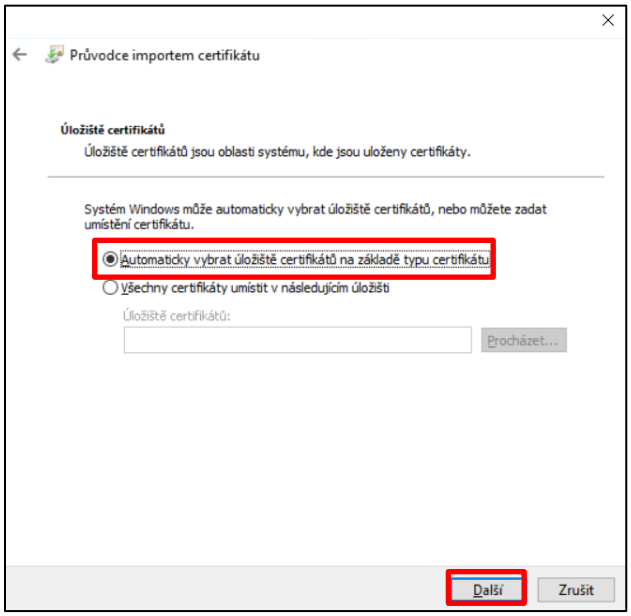


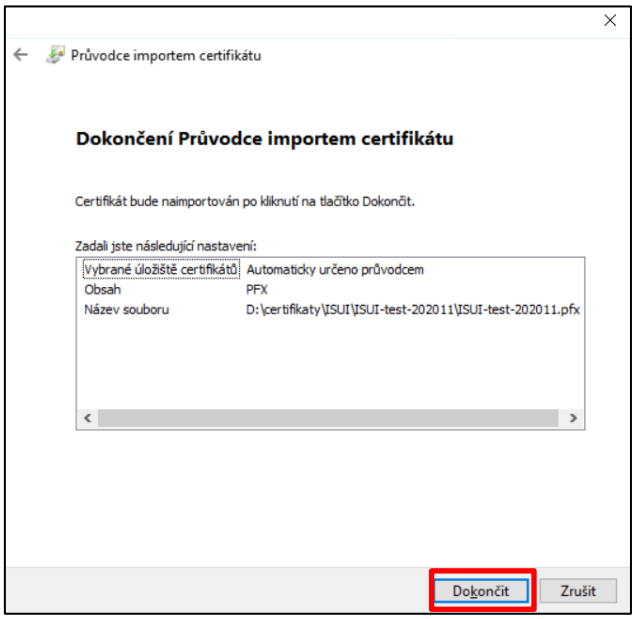


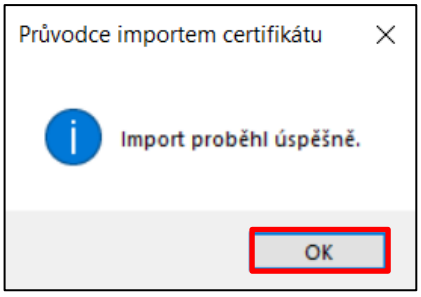
V průvodci necháváme přednastavené hodnoty kromě tohoto dialogu, kde musíme zaškrtnout jednu volbu (aby klíč byl exportovatelný) a zadat heslo k certifikátu, které jsme od SZR dostali spolu s certifikátem.



Zvolíme úložiště certifikátu





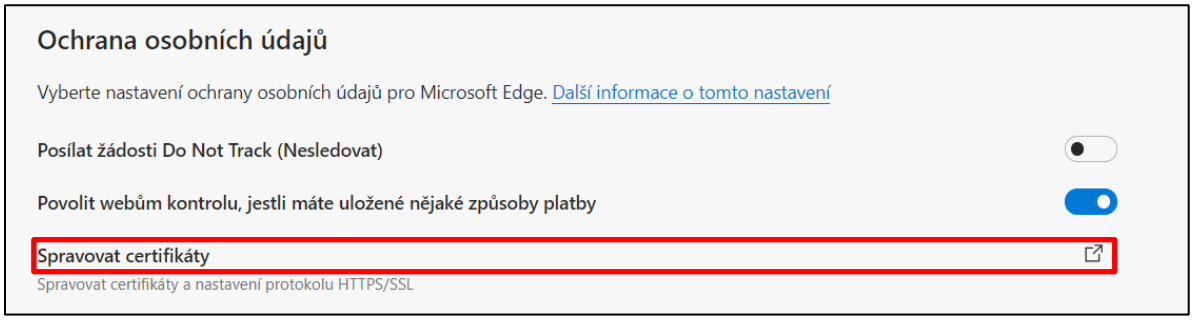


Pro ověření správnosti instalace certifikátu lze zobrazit tuto stránku z testovacího prostředí: https://isuiref.cuzk.cz:8445/isui_ws/IsuiNavrhZmenyObec?wsdl.

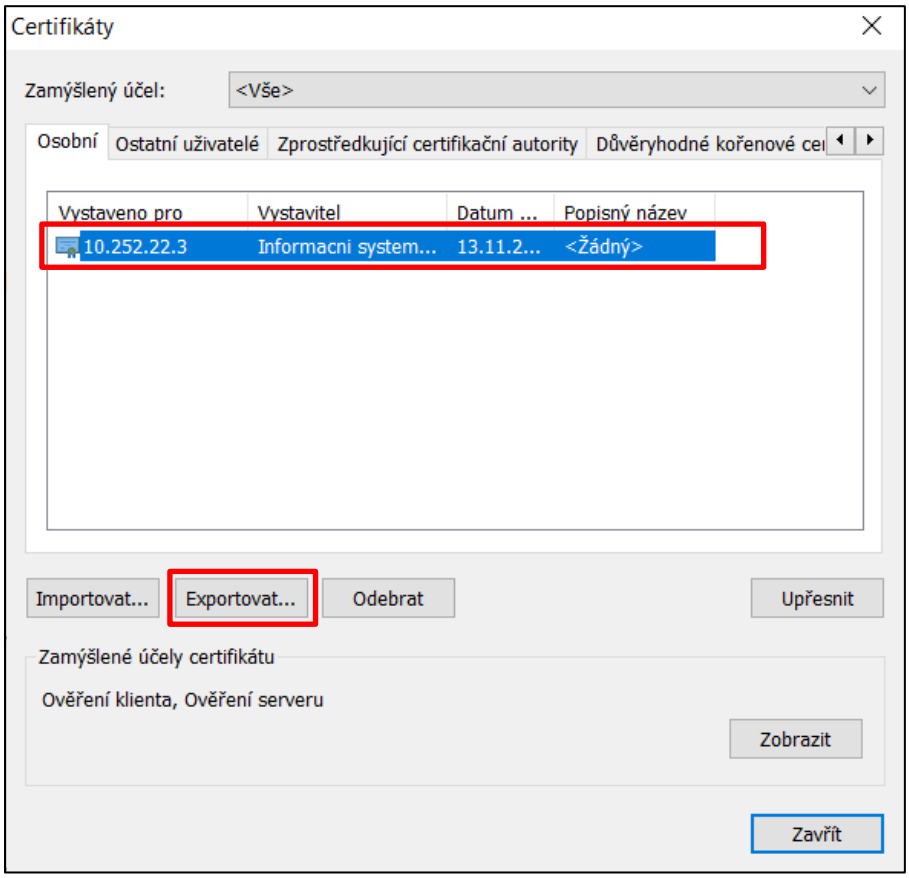
Pokud se stránka zobrazí dobře, byl certifikát správně nainstalován.

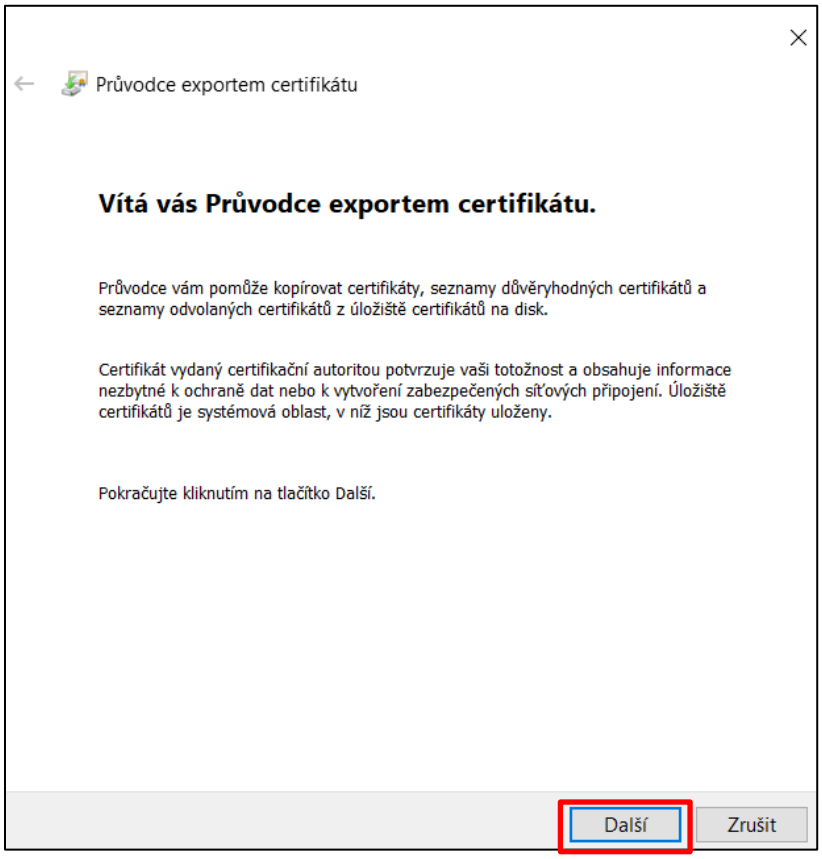
2.2 Export vytvořeného klíče z ME

Nastavení → Ochrana osobních údajů a služby → Spravovat certifikáty.

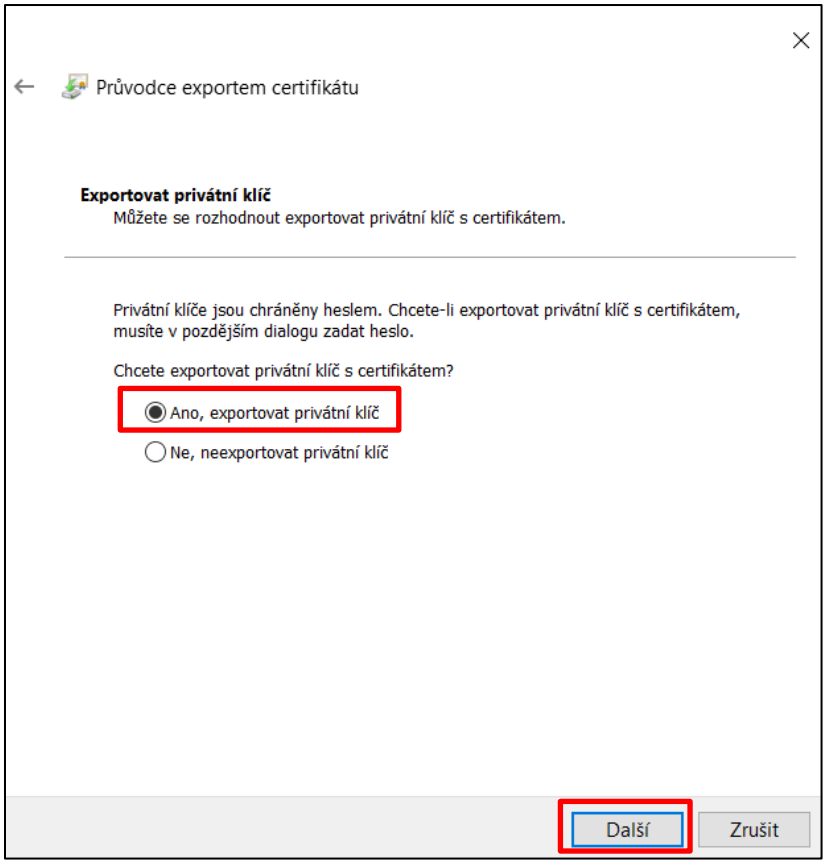


Zde vybereme příslušný certifikát a dáme *Exportovat*:

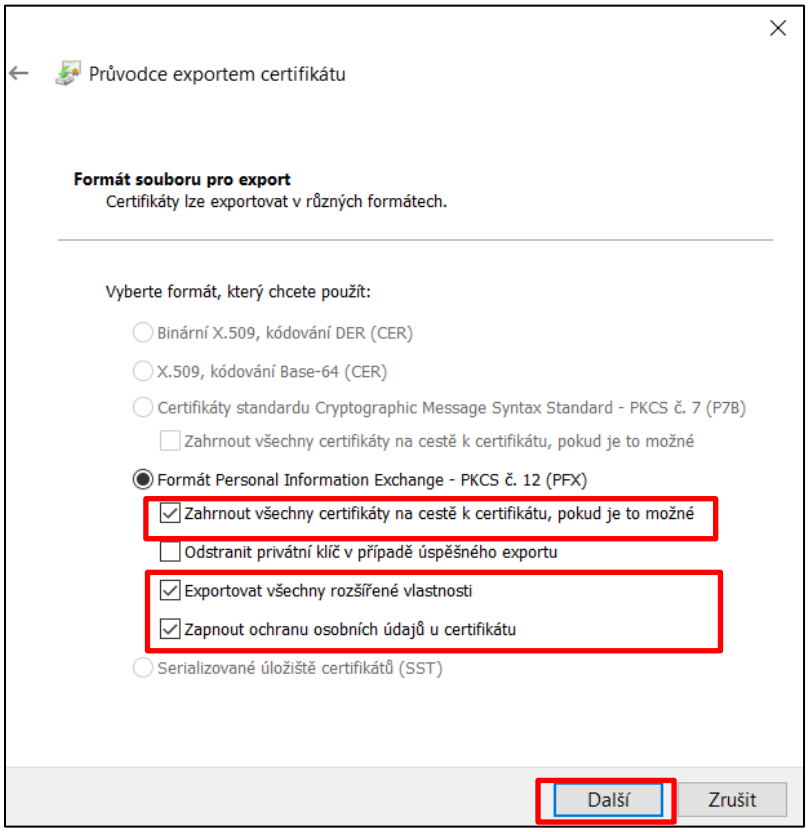




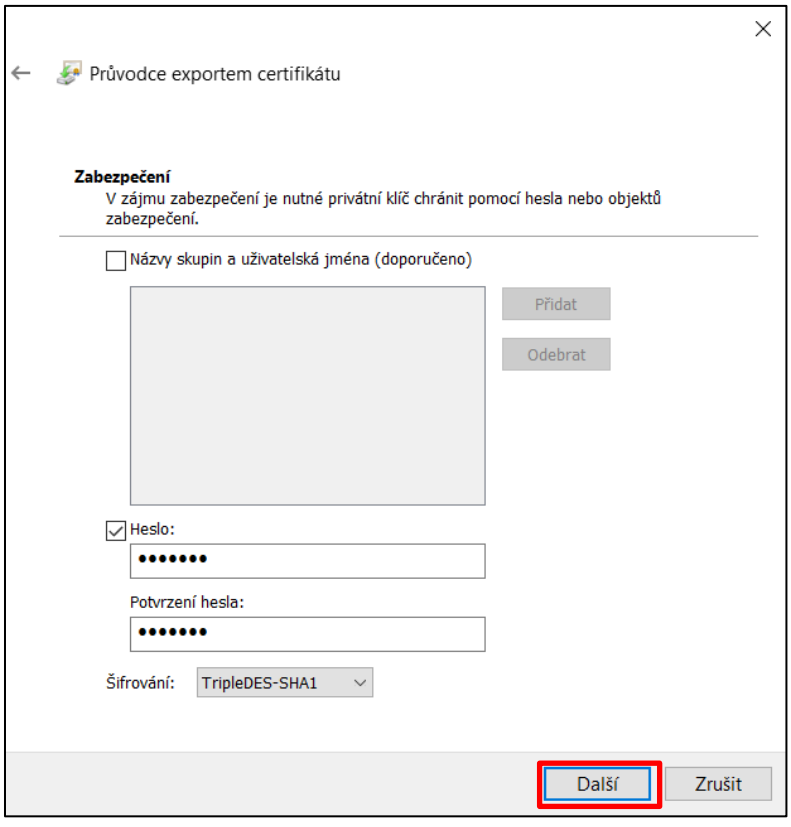
V exportu privátního klíče zvolíme možnost *Ano, exportovat privátní klíč*:



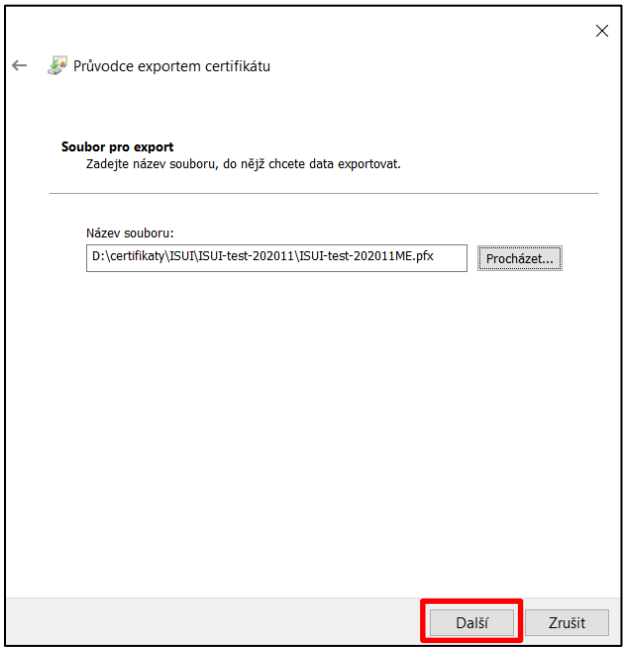
Vybereme formát, ve kterém chceme certifikát exportovat dle níže uvedených variant:

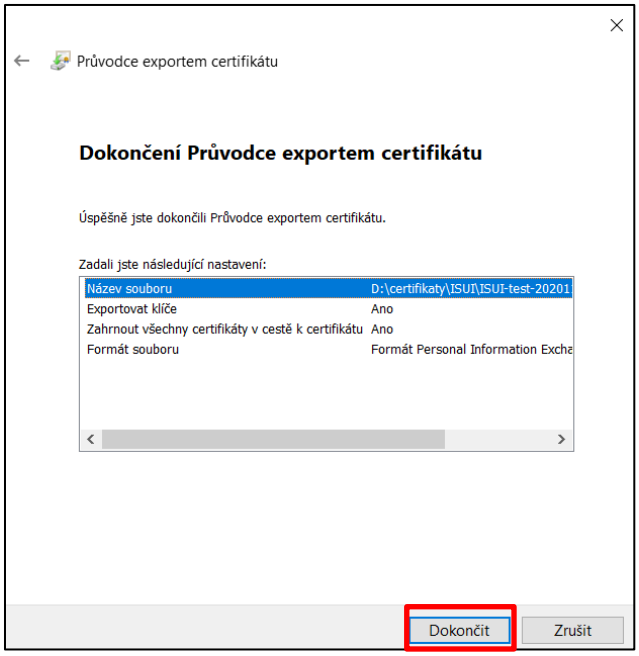


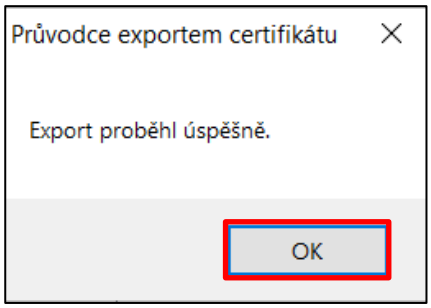
Nastavíme heslo pro přístup k privátnímu klíči, který jsme obdrželi spolu s certifikátem:



Následně zvolíme název souboru, do něhož budeme chtít certifikát exportovat.







Tímto postupem získáme certifikát včetně certifikačních autorit (CA).

Certifikát byl úspěšně exportován i se všemi soubory certifikační autority. Nyní máme k dispozici certifikát pro naše OVM, který splňuje všechny požadavky a lze jej použít k importu do souborů keystore a truststore.

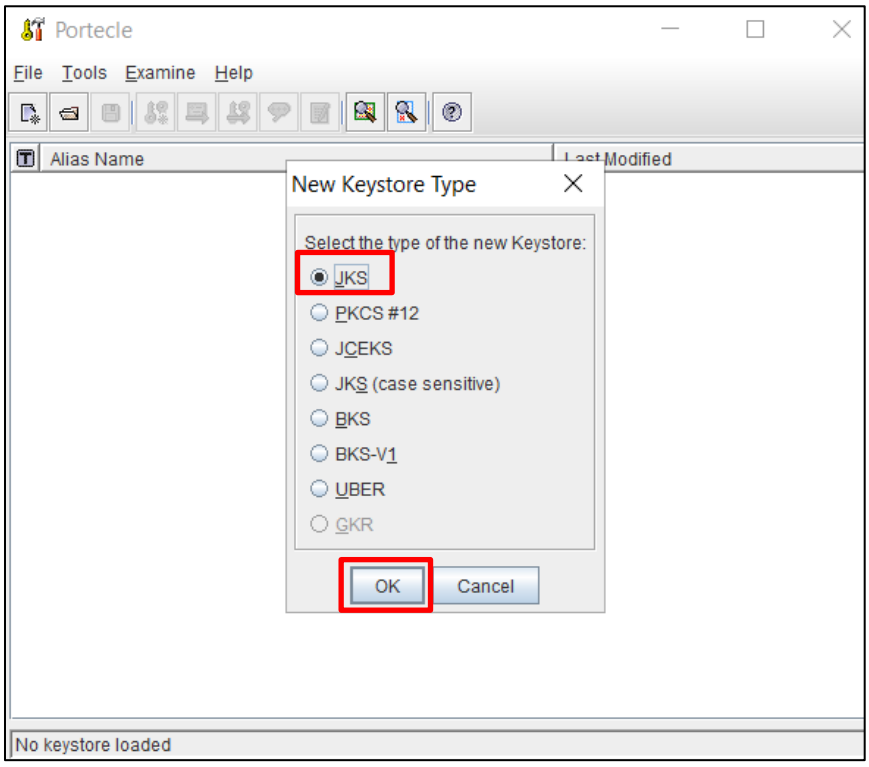
2.3 Vytvoření keystore.jks

Keystore je nezbytný pro načtení do SoapUI, protože se jedná o úložiště certifikátů pro Javu.

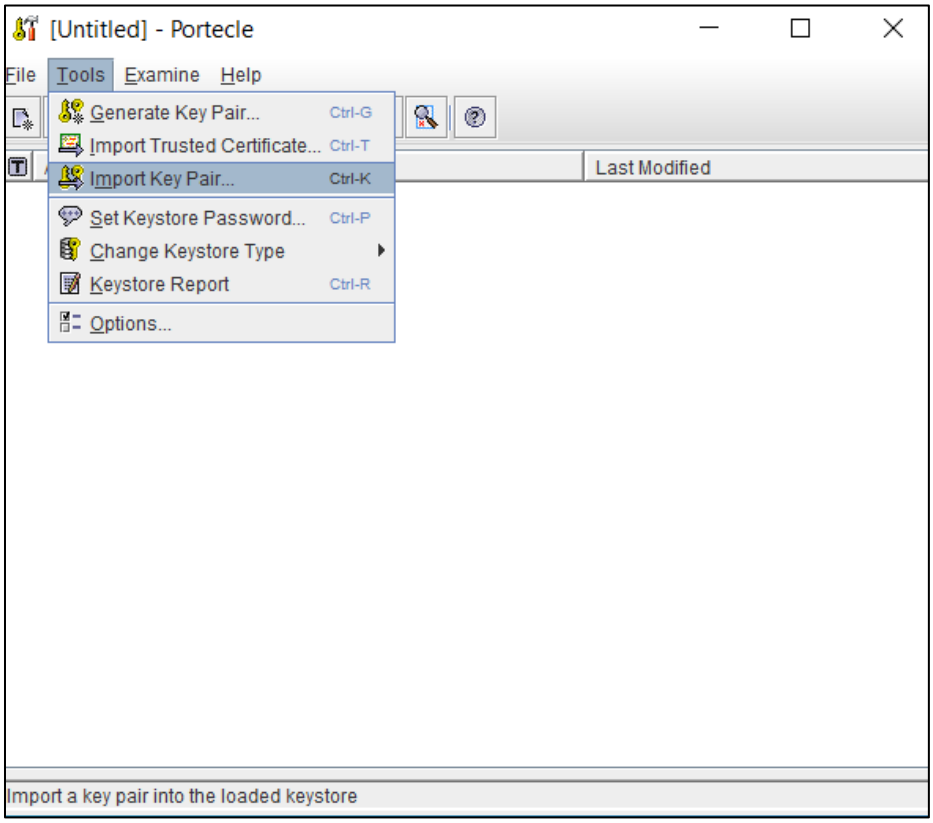
V tomto postupu si ukážeme vytvoření prostřednictvím programu Portecle. Vytvoření je možné i jinými nástroji, které zde nebudou popisovány.

Spustíme program Portecle, který je dostupný ke stažení na adrese: (http://sourceforge.net/projects/portecle/).

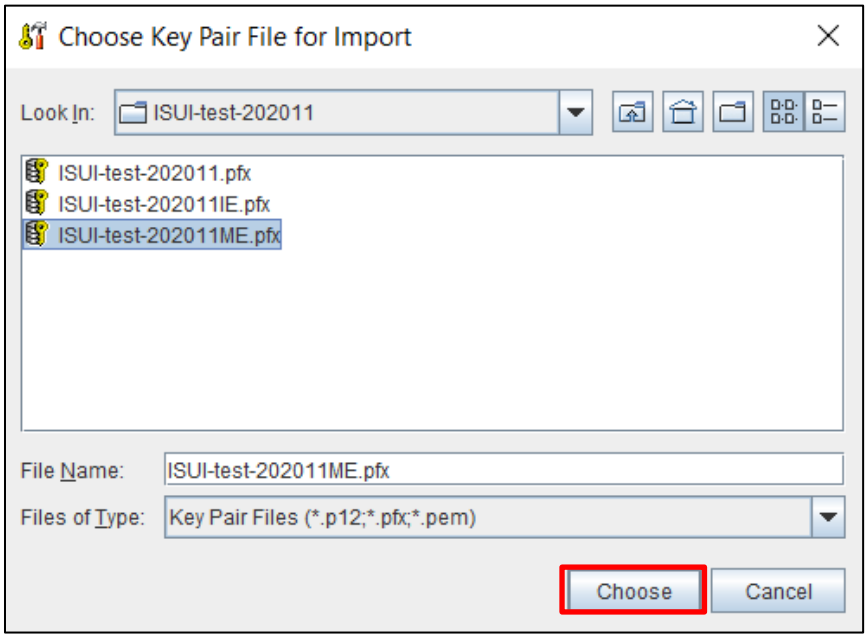
Zvolíme *File* → *New Keystore* → vybereme typ *JKS*



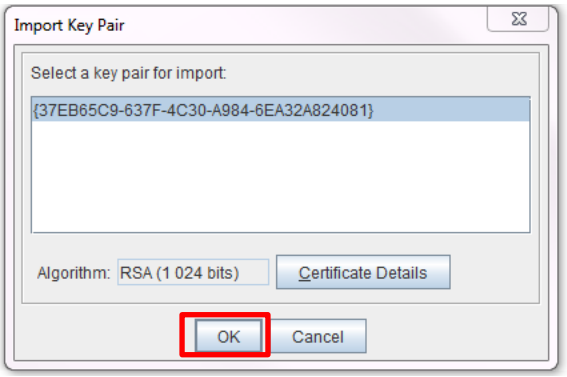
Dále zvolíme *Tools → Import Key Pair*



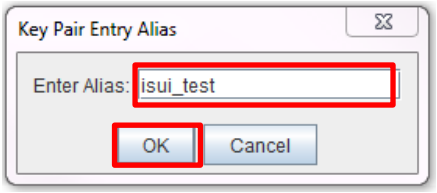
Vybereme vytvořený certifikát z ME (jehož součástí jsou i CA) a zvolíme *Import*.

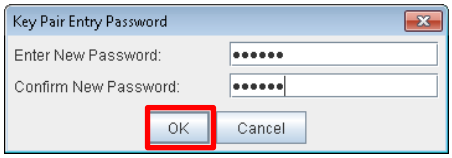


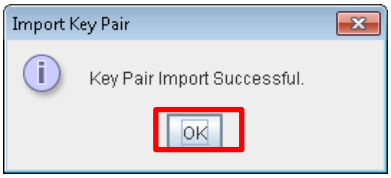
Po vyzvání vložíme heslo k vygenerovanému certifikátu a potvrdíme *OK*.



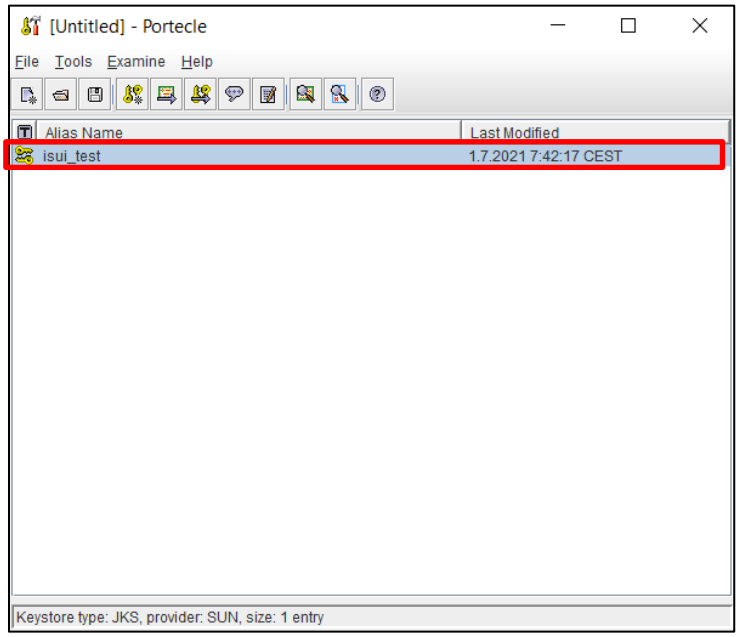
Po vyzvání vložíme alias k tomuto certifikátu např. „isui_test“ a zvolíme heslo (např. aaaaaa).

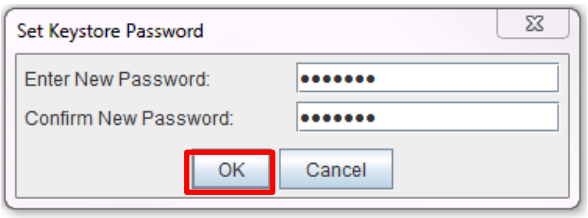


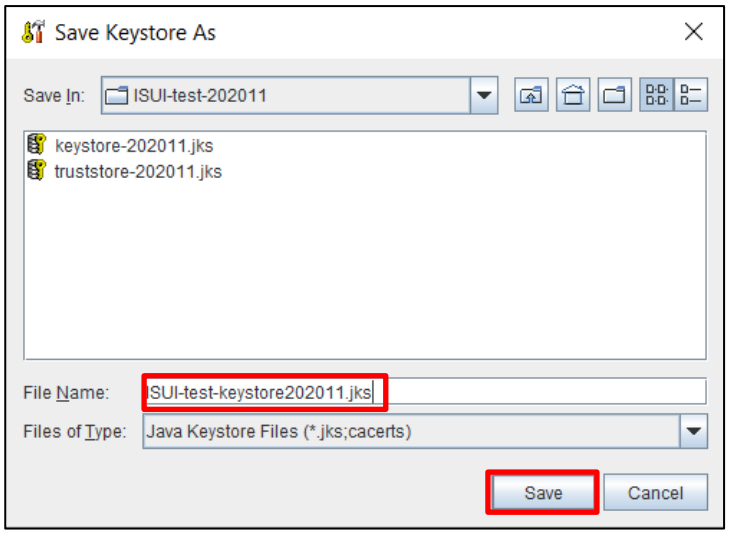




Zvolíme *File → Save Keystore As* a nový keystore uložíme do souboru keystore.jks (s heslem aaaaaa).

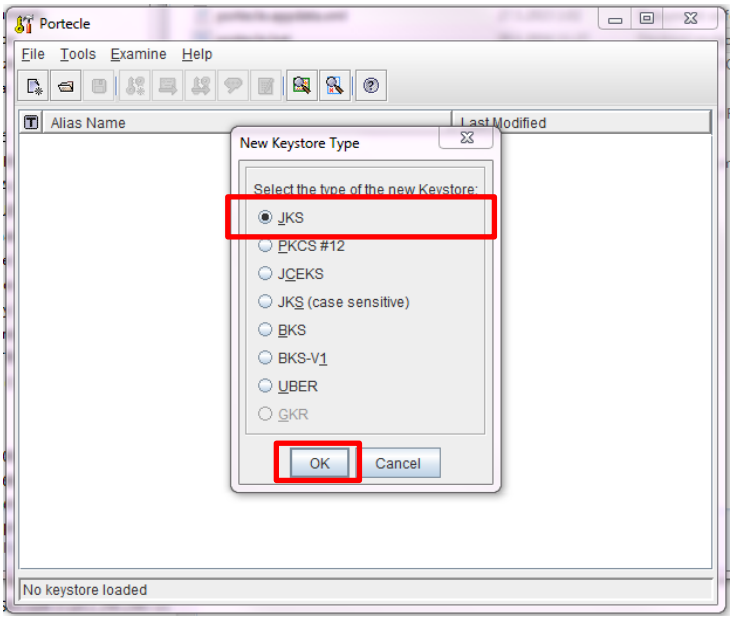






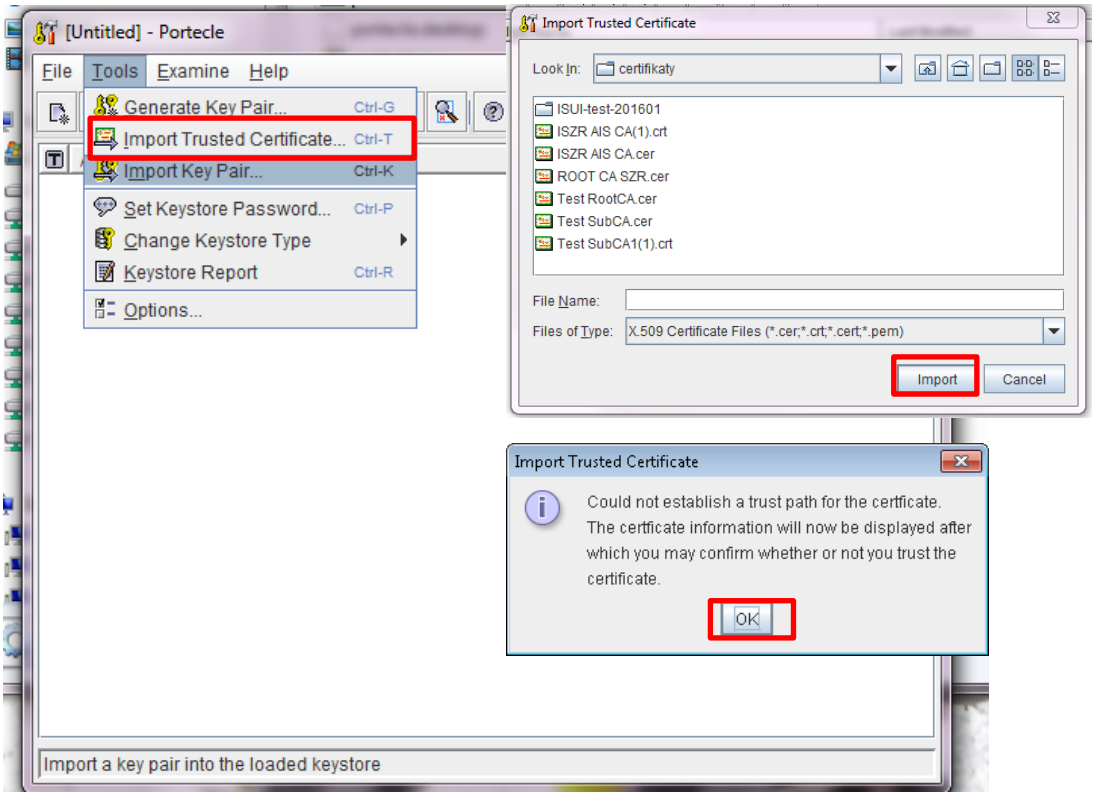
2.4 Vytvoření truststore.jks

Spustíme program Portecle a zvolíme *File* → *New Keystore* → vybereme typ *JKS*

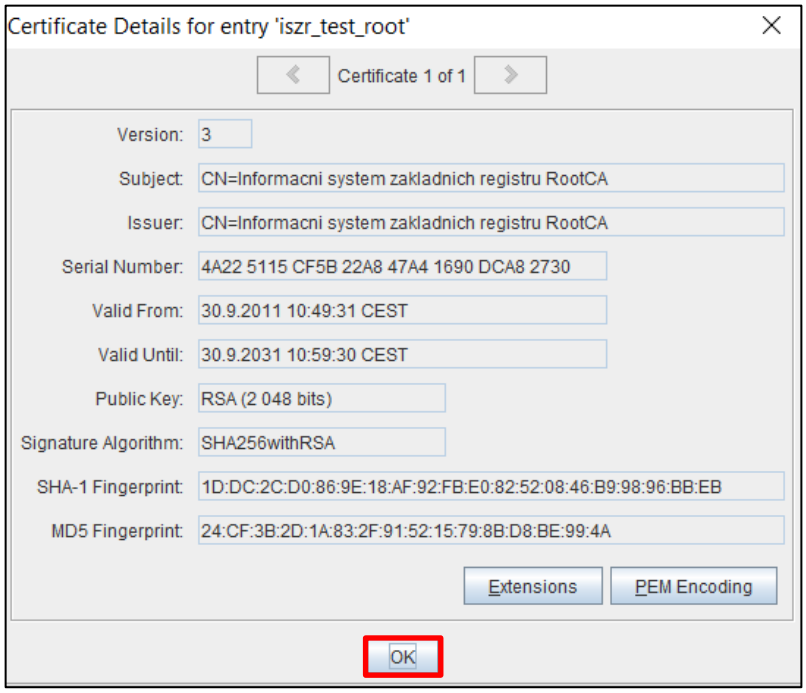


Zvolíme *Tools* → *Import Trusted Certificate*

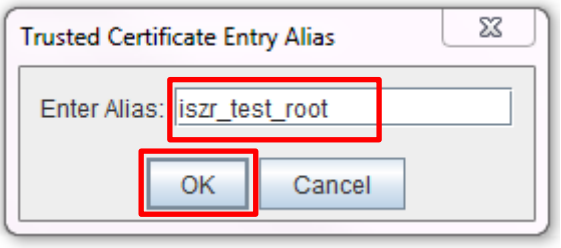
Postupně vložíme oba testovací certifikáty SZR (Test RootCA.cer, Test SubCA.cer).

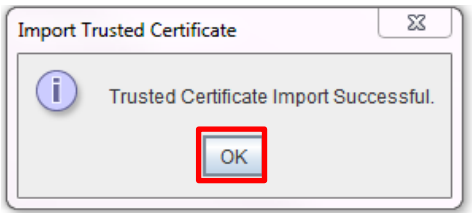


Po importu se zobrazí detail certifikátu.

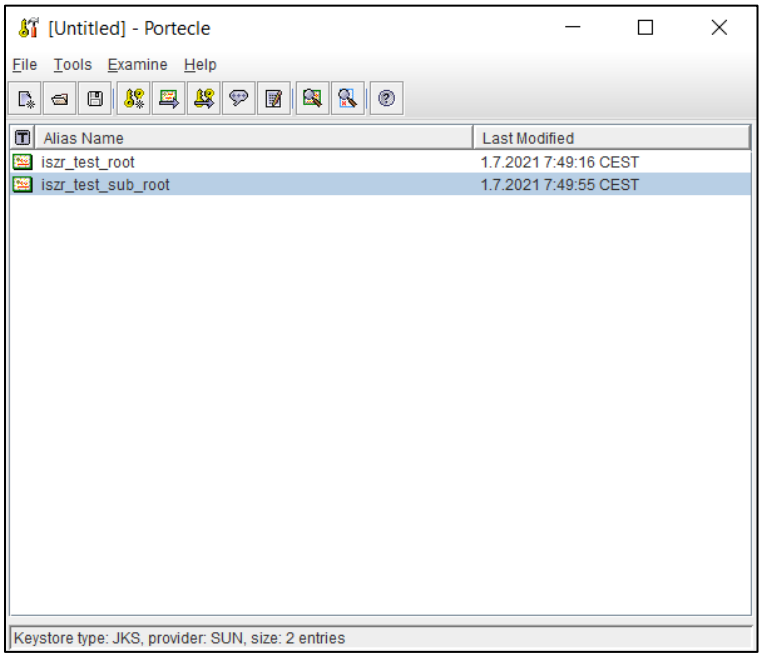


Zadáme příslušný alias pro oba testovací certifikáty ISZR, např. „iszr_test_root“, „iszr_test_sub_root“.

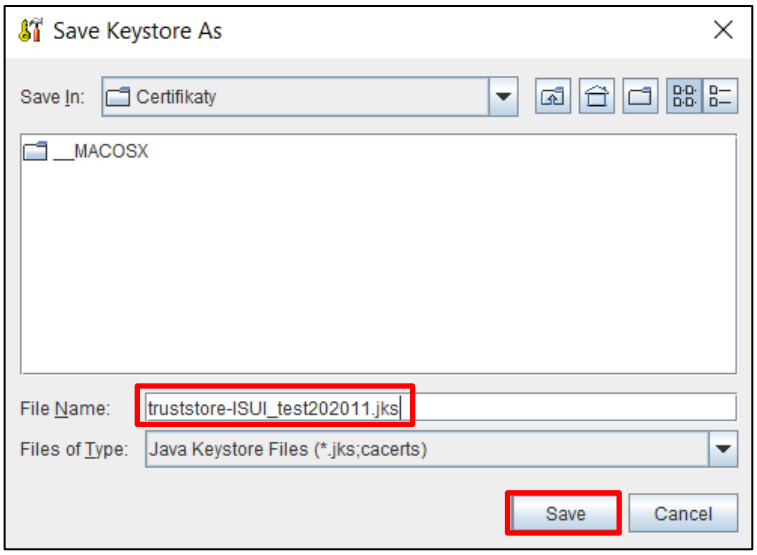




Následně získáme dva certifikáty:



Keystore uložíme do souboru: *File → Save Keystore*, nastavíme heslo (např. aaaaaa) a uložíme do souboru „truststore.jks“.



Zda se vytvoření povedlo, zjistíte při úspěšném spuštění projektu v SoapUI. Zprovoznění SoapUI pro účely testování je uvedeno v samostatném dokumentu Testování v SoapUI.