Vygenerování certifikátu

https://it.muni.cz/sluzby/osobni-certifikaty/navody/vydani-osobniho-certifikatu

Návod byl vytvořen využitím Internet Exploreru. Věnujte prosím pozornost poznámce o kompatibilitě webových prohlížečů na stránkách CESNETu v prvním bodě návodu.

- 1. Do prohlížeče zadejte adresu https://pki.cesnet.cz/cs/tcs-personal-user.html.
- 2. Klikněte na Žádost o nový certifikát.

Vydání Osobního certifikátu TCS

Vydání osobního TCS certifikátu je pro uživatele plně samoobslužné. Pro zpřístupnění této služby ale musí být splněny následující podmínky:

- domácí organizace musí být připojena k edulD.cz jako poskytovatel identity
- domácí organizace musí uživateli udělit oprávnění žádat o Osobní certifikáty TCS

Podporované prohlížeče

Jsou podporovány prohlížeče Firefox do verze 68 včetně, Safari a Internet Explorer (nikoliv Edge). Prohlížeč Chrome již nelze k vydání osobního certifikátu použít z důvodu odstranění přístupu k úložišti klíčů výrobcem aplikace, firmou Google. Stejný problém je i u prohlížečů Mozilla Firefox verze 69 a novějších.

Postup vydání nového osobního certifikátu

V menu aplikace klikněte na "Žádost o nový certifikát". Budete vyzvání k přihlášení pomocí účtu na IdP vaší organizace, po úspěšném přihlášení vám TCS portál zobrazí náhled parametrů certifikátu.

3. Ze seznamu institucí vyberte Masaryk Univerity/Masarykova univerzita.

Log in with	muni ×
Masaryk University	MUNI
Municipal Library and Informa Hradec nad Moravicí	tion centre of $\begin{bmatrix} M & \varepsilon & s & \tau & s & \kappa & A \\ \hline & K & N & H & O & V & N & A \\ H & R & A & D & \varepsilon & C^{0} \\ \hline \end{bmatrix}$
Municipal Library Česká Třebo	vá MĚSTSKÁ KNIHOVNA Česká Třebová
Municipal Library Chodov	Městská knihovna Chodov

4. Klikněte na tlačítko **Pokračovat/Continue**.

UNIVERSITAS. SISNER	MASARYKOVA UNIVERZITA Česká republika
	Poskytovatel identit MU Aplikace, ke které přistupujete, vyžaduje ověření pomocí hesla do ISu. Heslo, prosím, zadejte na následující stránce do systému INET.
	You are accessing an application requiring authentication with your IS password. You will be requested to present the password to the INET authentication service.

5. Vyplňte přihlašovací údaje a klikněte na **Přihlási**t.

M	н	Λ	Т	Unified
V	U	V	T.	Login

433479	
Primary password	
•••••	<u>م</u>
Remember me	
LOG IN	

 Klikněte na tlačítko Accept/Přijmout. Tímto umožníte využití Vašich údajů pro vygenerování certifikátu.



You are about to access the service: TCS certificates of <u>CESNET</u>

Description as provided by this service: Personal, server, robot, code and document certificates

Additional information about the service.

Data Re	quested by Service
UČO	433479
ID	433479@muni.cz
Given name	David
Surname	Štencel
Full Name	David Štencel
Full Name	David Stencel
E-mail	433479@mail.muni.cz 433479@muni.cz stencel@ics.muni.cz
Organization	Masarykova univerzita
Organization	muni.cz
Special permissions	
User's unique ID	
Consent to pe	ersonal data processing
o the service w	is requested to access the service. Do you accept that this data about you is se henever you access it?
Don't show m	e this page again.
	Reject Accept

7. Zatrhněte, se kterými e-mailovými adresami má být nový certifikát svázán (zpravidla všechny nabízené). Klikněte na Vydat certifikát.

Hodláte požádat o osobní certifikát s předmětem cn=David Stencel 433479,o=Masaryk University,c=CZ,dc=tcs,dc=terena,dc=org

Kliknutím na tlačítko Vydat certifikát souhlasíte s podmínkami služby. Informace o ochraně osobních údajů naleznete na stránkách CESNET CA.

V tomto certifikátu budou obsaženy emailové adresy, které jsou uvedeny níže. Seznam adres v certifikátu můžete upravovat, v certifikátu ale vždy musí být alespoň jedna emailová adresa.

Upozornění: Seznam Vašich autorizovaných emailových adres obsahuje jednu nebo více adres z domén, které nejsou autorizovány pro Vaši organizaci. Tyto adresy byly odškrtnuty. Pokud je v certifikátu opravdu potřebujete, zaškrtněte je a počítejte prosím se složitějším procesem vydání certifikátu (vlastnictví adres musí DigiCert ověřit autorizačními emaily).

Emaily v certifikátu: 🗹 433479@mail.muni.cz

433479@muni.cz
 stencel@ics.muni.cz
 Vydat certifikát

8. Potvrďte vydání certifikátu kliknutím na tlačítko Ano.

Osobní certifikát TCS

Hodláte požádat o osobní certifikát s předmětem cn=David Stencel 433479,o=Masaryk University,c=CZ,dc=tcs,dc=terena,dc=org.

Kliknutím na tlačítko Vydat certifikát souhlasíte s podmínkami služby. Informace o ochraně osobních údajů naleznete na stránkách CESNET CA.

V tomto certifikátu budou obsaženy emailové adresy, které jsou uvedeny níže. Seznam adres v certifikátu můžete upravovat, v certifikátu ale vždy musí být alespoň jedna emailová adresa.

Upozornění: Seznam Vašich autorizovaných emailových adres obsahuje jednu nebo více adres z domén, které nejsou autorizovány pro Vaši organizaci. Tyto adresy byly odškrtnuty. Pokud je v certifikátu opravdu potřebujete, zaškrtněte je a počítejte prosím se složitějším procesem vydání certifikátu (vlastnictví adres musí DigiCert ověřit autorizačními emaily).

Emaily v certifikátu:	✓ 433479@mail.muni.cz	Potvrzení přístupu k webu		
	✓ 433479@muni.cz			
	✓ stencel@ics.muni.cz	Tento web se pokouší provést vaším jménem operaci s digitálním certifikátem:		
	Vydat certifikát	https://tcs.cesnet.cz/clientrequestform/form		
		Provádět vaším jménem operace s digitálním certifikátem byste měli povolit pouze známým webům. Chcete tuto operaci povolit?		
		Ano Ne		

9. Zobrazí se potvrzení o vytvoření certifikátu.

Osobní certifikát TCS

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

Nyní je certifikát uložený ve Vašem prohlížeči (díky IE zároveň i v Certificate Store).

10. Pro export certifikátu z prohlížeče klikněte na tlačítko "ozubené kolo" ³³ v pravém horním rohu a zvolte **Možnosti internetu**.



11. V záložce Obsah klikněte na tlačítko Certifikáty.

Vyberte Váš nový certifikát (s roční platností od aktuálního dne vydaný TERENA eScience Personal) a klikněte na tlačítko **Exportovat**.

Osobní certifikát TCS

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

Možnosti internetu	? ×					
Připojení Programy Obecné Zabezpečení Osobní údaje	Upřesnit Obsah	Certifikáty				×
Certifikáty Pro šifrovaná připojení a identifikaci používejte c	ertifikáty.	Zamýšlený účel: Osobní Ostatní už	<vše></vše>	kační autority Dův	věryhodné kořenové	~ CE 1 •
Vymazat stav protokolu SSL Certifikáty V Automatické dokončování Funkce automatického dokončování uchovává předchozí zadané položky na webových stránkách a navrhuje odpovídajíc položky. Informační kanály a oblasti Web Slice Informační kanály a oblasti Web Slice Informační kanály a oblasti Web Slice Explorer a dalších aplikacích.	/ydavatelé Nastavení Nastavení	Vystaveno pro	Vystavitel 433479 TERENA eSdence Po	Datum uk er 10/25/2020	Popisný název <Žádný>	~
		Importovat Exp Zamýšlené účely ce Ověření klienta, Zal	oortovat Odebrat rtifikátu pezpečení e-mailu		Upi Zobra Za	esnit izit
OK Zrušit	Použít					

12. Klikněte na tlačítko **Další**.

🔶 🛿 Průvodce exportem certifikátu	×
Vítá vás Průvodce exportem certifikátu.	
Průvodce vám pomůže kopírovat certifikáty, seznamy důvěryhodných certifikátů a seznamy odvolaných certifikátů z úložiště certifikátů na disk.	
Certifikát vydaný certifikační autoritou potvrzuje vaši totožnost a obsahuje informace nezbytné k ochraně dat nebo k vytvoření zabezpečených síťových připojení. Úložiště certifikátů je systémová oblast, v níž jsou certifikáty uloženy.	
Pokračujte kliknutím na tlačítko Další.	
Další Z	rušit

13. Zatrhněte "Ano, exportovat privátní klíč" a klikněte na tlačítko Další.

		×
~	嵾 Průvodce exportem certifikátu	
	Exportovat privátní klíč	
	Můžete se rozhodnout exportovat privátní klíč s certifikátem.	
	Privátní klíče jsou chráněny heslem. Chcete-li exportovat privátní klíč s certifikátem, musíte v pozdějším dialogu zadat heslo.	
	Chcete exportovat privátní klíč s certifikátem?	
	Ano, exportovat privátní klíč	
	🔿 Ne, neexportovat privátní klíč	
	Další Zruš	iit
		_

14. Zvolte formát PFX dle obrázku a klikněte na tlačítko Další.

🖌 🦉 De ^s wadza avnastan catifikitu	×
Formát souboru pro export Certifikáty lze exportovat v různých formátech.	
Vyberte formát, který chcete použít:	
Binární X.509, kódování DER (CER)	
🔿 X.509, kódování Base-64 (CER)	
 Certifikáty standardu Cryptographic Message Syntax Standard - PKCS č. 7 (P7B) Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné 	
Formát Personal Information Exchange - PKCS č. 12 (PFX) Zahrnout všechny certifikáty na cestě k certifikátu, pokud je to možné	
Odstranit privátní klíč v případě úspěšného exportu	
Exportovat všechny rozšířené vlastnosti	
🗹 Zapnout ochranu osobních údajů u certifikátu	
🔵 Serializované úložiště certifikátů (SST)	
Další Zruši	t

15. Zatrhněte políčko Heslo a vložte své jedinečné heslo pro ochranu certifikátu. Klikněte na tlačítko **Další**.

Heslo si dobře zapamatujte nebo lépe jej uložte na bezpečné místo jako např. do správce hesel KeePass.

🗧 🐓 Průvodce exportem certifikátu	×
Zabezpečení V zájmu zabezpečení je nutné privátní klíč chránit pomocí hesla nebo objektů zabezpečení.	
Názvy skupin a uživatelská jména (doporučeno)	
Přidat	
Odebrat	
Heslo:	
•••••	
Potvrzení hesla:	
•••••	
Šifrování: AES256-SHA256 🗸	
Další Z	rušit

16. Po kliknutí na tlačítko Procházet... vyberte místo, kam se má certifikát uložit, zadejte název certifikátu a klikněte na Uložit.

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

← <i> </i>	e exportem certifikátu	×
Soubor pro Zadeji	o export te název souboru, do nějž chcete data exportovat.	_
	Procházet	x
	← → ~ ↑ ↓ → Tento p → Stažené soubory ~ ♂	Prohledat: Stažené soubory 🛛 🔎
	Uspořádat 🔻 Nová složka	III 🔹 🔹 😮
	 Rychlý přístup Plocha Stažené soub # Dokumenty # Git PS_skripts # Documents V 	Datum
	Název souboru: cert_433479_exp251020 Uložit jako typ: Formát Personal Information Exchange (*.pfx)	~
	∧ Skrýt složky	Uložit Zrušit

17. Klikněte na tlačítko **Další**.

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

	\times
🔶 🐓 Průvodce exportem certifikátu	
Soubor pro export	
Zadejte název souboru, do nějž chcete data exportovat.	
Název souboru:	
D:\Users\433479\Downloads\cert_433479_exp251020.pfx Procházet	
Další Zruš	it

18. Klikněte na tlačítko Dokončit.

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

🔶 😺 Průvodce exportem certifikátu	X
Dokončení Průvodce exportem certi	fikátu
Úspěšně jste dokončili Průvodce exportem certifikátu.	
Zadali jste následující nastavení:	
Název souboru D:\Us	ers\433479\Downloads\cert_
Exportovat klíče Ano	
Zahrnout všechny certifikáty v cestě k certifikátu Ano	
Formát souboru Forma	it Personal Information Excha
<	>
	Dokončit Zrušit

19. Klikněte na tlačítko OK. Váš certifikát byl úspěšně uložen.

Své certifikáty si bezpečně archivujte. Opět můžete využít např. správců hesel jako je KeePass, které umožnují uchovávat i soubory tedy i certifikáty. Certifikát si můžete uložit ve vašem OneDrive.

Váš osobní certifikát by nyní měl být úspěšně nainstalován do Vašeho prohlížeče.

← 😺 Průvodce expo	ortem certifikátu			
Dokonče	ní Průvodce exportem (certi	ifikátu	
Úspěšně jste d	okončili Průvodce exportem certifiká	tu.		
Zauali jste nasi	euujici nastaveni:	Dalu	\422470\D	
Nazev soubo	ru	0:10	sers (433479 (Downloads (cert_	
Zabroout vše	uce vchov certifikáty v cestě k certifikátu	Ano		
Formát soubo	oru	Form	nát Personal Information Excha	
	Průvodce exportem certifikátu	×		
<	Export proběhl úspěšně.		>	
	ОК]	