

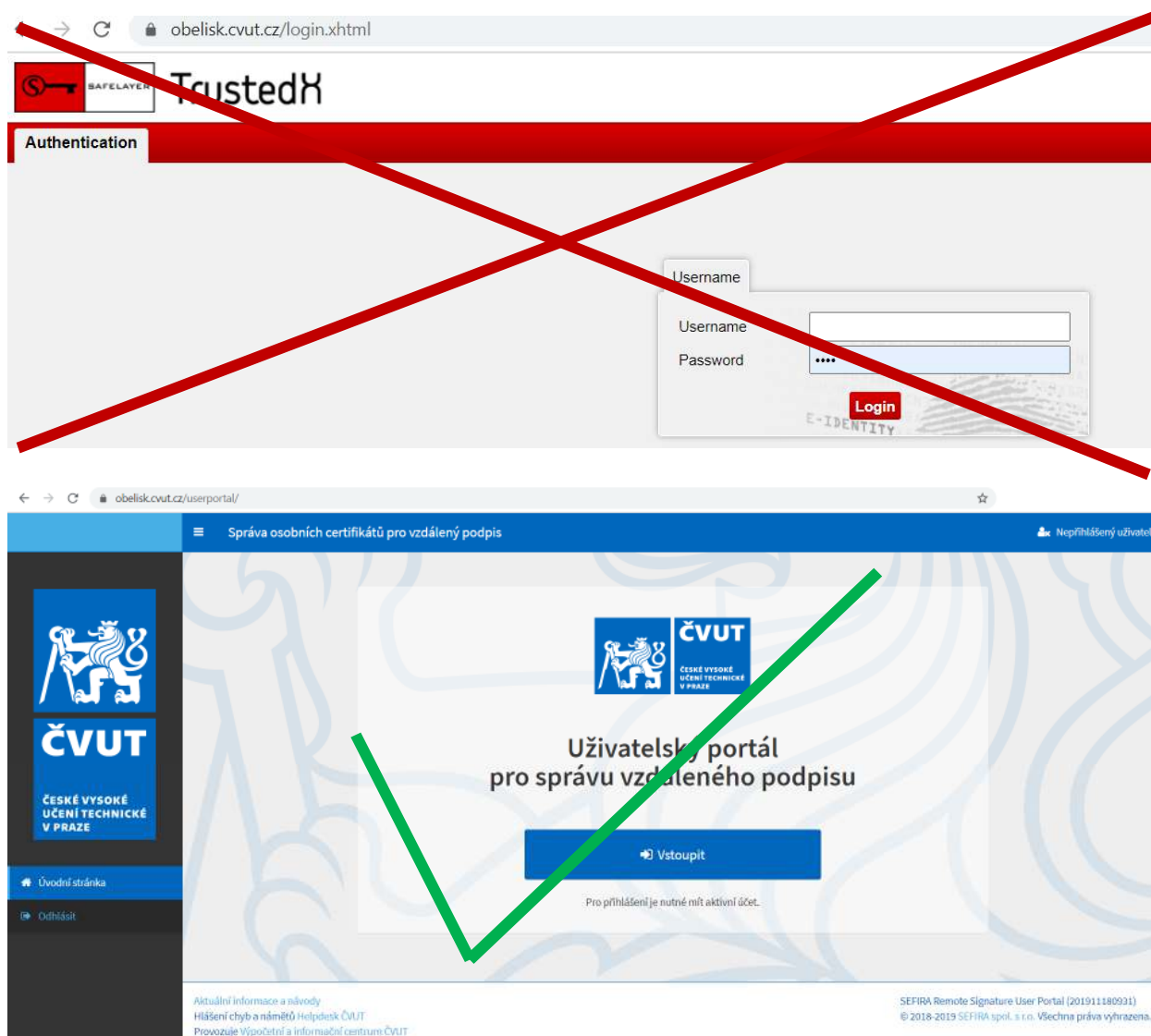
Manuál „Uživatelského portálu pro správu vzdáleného podpisu“ systému OBELISK (OBELISK USERPORTAL)

– nová politika podpisových identit (od 9.10.2020)

1. Přihlášení do uživatelského portálu

Do Uživatelského portálu má přístup každý zaměstnanec. O přihlašování se stará systém ČVUT Shibboleth SSO (Single-Sign-On), který znáte i z dalších systémů ČVUT např. KOS, AEDO... Přihlásit se můžete z vašeho uživatelského profilu na USERMAP – <https://usermap.cvut.cz> → Uživatelský profil → karta „Nastavení“ → odkaz „Správa osobních certifikátů“.

Nebo přímým odkazem <https://obelisk.cvut.cz/userportal> Pozor, protože systém OBELISK slouží k vytváření celé platformy digitální důvěry, nestačí zadat pouze <https://obelisk.cvut.cz> tím byste se dostali do části, do které nemáte umožněn přístup, ale musíte zadat adresu celou.



Obr. 1 Chybná a správná přihlašovací obrazovka do uživatelského portálu

Pokud vaše přihlašování není úspěšné a končí např. chybou „Chyba přesměrování (access_denied) popis: UnknownSubjectException“, bývá problém v údajích zadaných v systému USERMAP, zejména nevyplněná e-mailová adresa, což je pro práci v Uživatelském portálu podmínka nezbytná.

Kontrolu zda máte vyplněný e-mail provedte přihlášením na <https://usermap.cvut.cz> po rozkliknutí „Uživatelský profil“ → v části „kontaktní údaje“. Pro maximální důvěryhodnost doporučujeme používat email z domén cvut.cz

USERMAP

Lidé na ČVUT Pracoviště Čselníky - Role - Zelenka, Jan - CZ/EN

Uživatelský profil Odhlásit

Ing. Jan Zelenka

Profil uživatele Nastavení

Role na ČVUT

Posice na ČVUT: zaměstnanec / oddělení IS ekonomických a správních agend / Výpočetní a informační centrum
zaměstnanec / ústav aplikované informatiky v dopravě / Fakulta dopravní
student / ústav aplikované informatiky v dopravě / Fakulta dopravní
student / Fakulta dopravní

Popis: 16114 - odborný asistent, B1313 - uložiste CUL, certifikaty OBELISK

Kontaktní údaje

Místnost: Praha, Jugoslávských partyzánů 1580, místnost: B-336
Telefon: +420-22435-8432
E-mail: **Jan.Zelenka@cvut.cz**
zelenkj3@fd.cvut.cz

Údaje o identitě

Osobní číslo: 101658
Uživatelské jméno: zelenkj3
Rodné číslo (typ státní): [redacted]
Pohlaví: muž
Datum narození: [redacted]
Místo narození: Praha
Stát narození: Česko
Rodné příjmení: Zelenka
Státní příslušnost: Česko
Identifikátor ORCID: <https://orcid.org/0000-0002-9927-3636>
Kvalita identity: A - Identita plně identifikována, údaje ověřené
Žtotožnění - provedl: 27.11.2018 18:09, Příbramský, Stanislav, Mgr. (252261)
Žtotožnění - na základě dokladu: Občanský průkaz (Česko) - [redacted]

Heslo ČVUT — Aktuální stav: **Heslo je platné** (do 27.09.2021 07:20:02)

Heslo eduroam (WiFi)

Osobní certifikáty

Číslo certifikátu	Typ certifikátu	Stav certifikátu	Datum expirace
5B26DCE27A586600	Certifikát vydaný prostřednictvím systému Obelisk	Platný	30.11.2021 21:16:00

Obr. 2 Kontrola údajů v systému USERMAP, důležité položky: E-mail, Kvalita identity

2. Vydání nového certifikátu

2.1. Nutné podmínky pro vydání certifikátu.

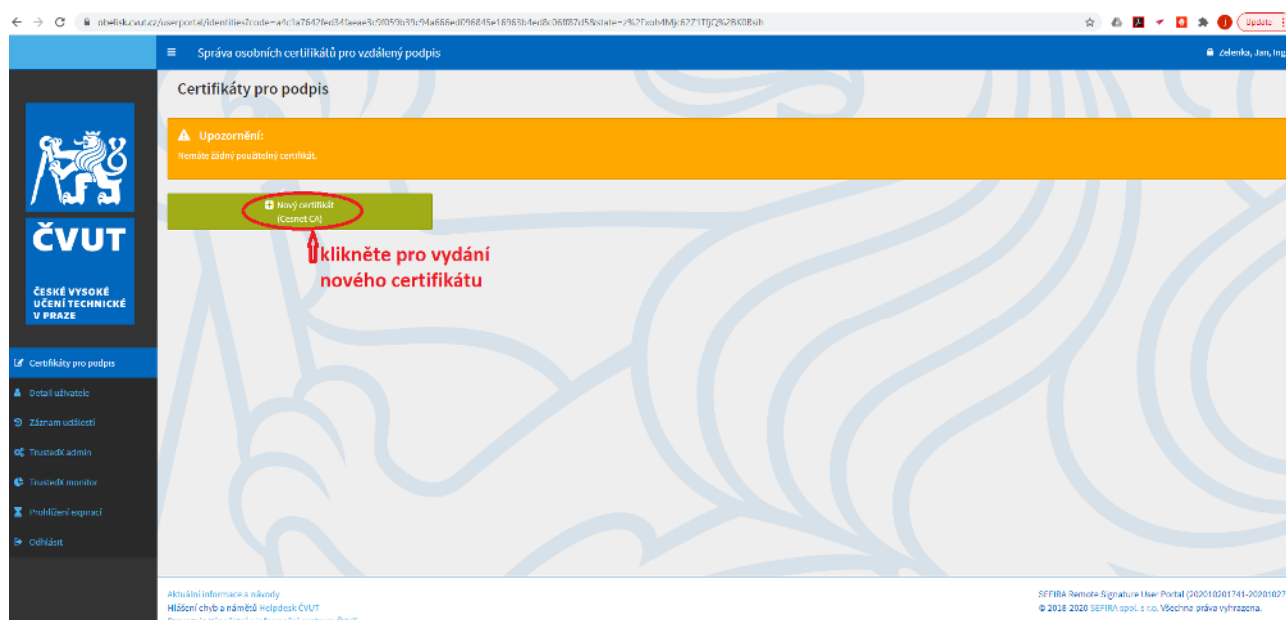
Pro vlastnictví certifikátu je nutná ověřená identita tzv. kvality A „Identita plně identifikovaná, údaje ověřené“. Toto ověření údajů, tzv. ztotožnění uživatele, provádí pověřené lidi na součástech ČVUT, většinou personální oddělení, nebo Vydavatelství průkazů ČVUT. Kontrolu kvality identity provedete přihlášením na <https://usermap.cvut.cz> po rozkliknutí „Uživatelský profil“ → v části „údaje o identitě“, viz Obr. 2.

Nárok na podpisový certifikát certifikační autority CESNET CA pro vzdálené podepisování pro interní oběhy ČVUT má každý zaměstnanec s platným pracovněprávním vztahem k ČVUT. V budoucnu nárok na podpisové certifikáty dalších CA závisí na konkrétní business roli zaměstnance.

2.2. Proces vydání certifikátu

2.2.1. CESNET CA

Po přihlášení je jako první otevřena stránka „Certifikáty pro podpis“ se seznamem certifikátů, pokud máte nárok na vydání certifikátu, uvidíte dostupné tlačítko „+ Nový certifikát (CESNET CA)“. Kliknutím na toto tlačítko zahájíte proces vydávání. Pokud nemáte identitu kvality A, není možné certifikát vydat, tlačítko nebude dostupné nebo proces skončí chybou.



Obr. 3 Nový certifikát – první krok

Pokud máte nárok i na jiný certifikát, např. kvalifikovaný, uvidíte zde i tlačítko pro další certifikační autoritu (např. PostSignum CA)

Tato operace je ověřována pomocí kódu, který je systémem zaslán na uživatelskou primární adresu.

User Portal vyžaduje přihlášení.

Ověřovací kód byl odeslán na Vaši emailovou adresu zelenkj3@fd.cvut.cz. První část kódu je 5474. Prosím, zadejte druhou část kódu (posledních 16 znaků).

vložte druhou část kódu, který vám přijde na email a stisknete "Ověřit kód"

Kód

Ověřit kód Storno

Powered by TrustedX from Safelayer Secure Communications, S.A.

Obr. 4 Nový certifikát – ověření operace ověřovacím kódem

Po ověření tímto kódem, budete vyzváni k zadání nového PIN pro použití tohoto certifikátu. Tento PIN je svázán pevně s vydávaným certifikátem, pokud v budoucnu PIN zapomenete, nebo zadáte opakovaně PIN nesprávně a dojde tak k uzamčení certifikátu, musíte certifikát zneplatnit a vydat si certifikát nový.

User Portal vyžaduje od uživatele Zelenka, Jan, Ing. povolení k:

Žádost o certifikát

Zadejte nový PIN k vašim podpisovým klíčům:

Nový PIN

Potvrdit PIN

Autorizovat Storno

Obr. 5 Nový certifikát – zadání PIN k novému certifikátu a autorizace žádosti o certifikát

Po stisknutí tlačítka autorizovat, je žádost o certifikát (tzv. request) obsahující informace o organizaci (ČVUT) a osobě (jméno, příjmení, osobní číslo, primární e-mail) odeslána na certifikační autoritu a certifikát je vydán. Certifikační autorita si po vygenerování uchovává pouze sériové číslo certifikátu.

Detaily certifikátu si můžete prohlédnout po rozkliknutí ikonky „=“ u tohoto certifikátu.

The screenshot shows the 'Správa osobních certifikátů pro vzdálený podpis' (Management of personal certificates for remote signing) interface. A green banner at the top indicates 'Úspěch: Certifikát byl vydán.' (Success: Certificate issued). Below, a red arrow points to a button labeled 'Zde můžete rozkliknout pro detaily certifikátu' (Here you can click for certificate details). The main content is divided into two sections: 'Atribut' (Attribute) and 'Hodnota' (Value).

Atribut	Hodnota
Popis	Remote signature HSM
CÁ schématu	Cesnet CA
Certifikát	Stáhnout
Labels	user_id:101858 non_qualified x509keyUsage:contentCommitment CesnetCA HSM x509keyUsage:digitalSignature creation_date:2020-11-05 21:41:27 server_HSM
Aktivace podpisu	hsm-pvud Zneplatnit PIN
Status	enabled
ID	984bshohku11ne19h7ku508g@
GID	rpbm7na46q4c40j35cjrbmpj55cd1us

Atribut	Hodnota
Seriové číslo (HEX)	5a311691cfbb5204
Seriové číslo (DEC)	6499000552783565316
Identifikační klíče subjektu (SKI SHA1)	829668CAFDC609E211F60E29182321A28FF47043
Použití klíče	digitalSignature nonRepudiation keyEncipherment
Vydatel	DC: cz DC: cesnet-ca O: CESNET CA CN: Personal Signing 2
Subjekt	CN: Zelenka, Jan, Ing. SERIALNUMBER: 101858@cvut.cz O: CTU in Prague DC: personal-signing DC: cesnet-ca DC: cz
Alternativní jména	rfc822Name: Jan.Zelenka@cvut.cz
Začátek platnosti	Čtvrtek, 5. listopad 2020 21:31:35 CET
Konec platnosti	Úterý, 30. listopad 2021 21:31:35 CET

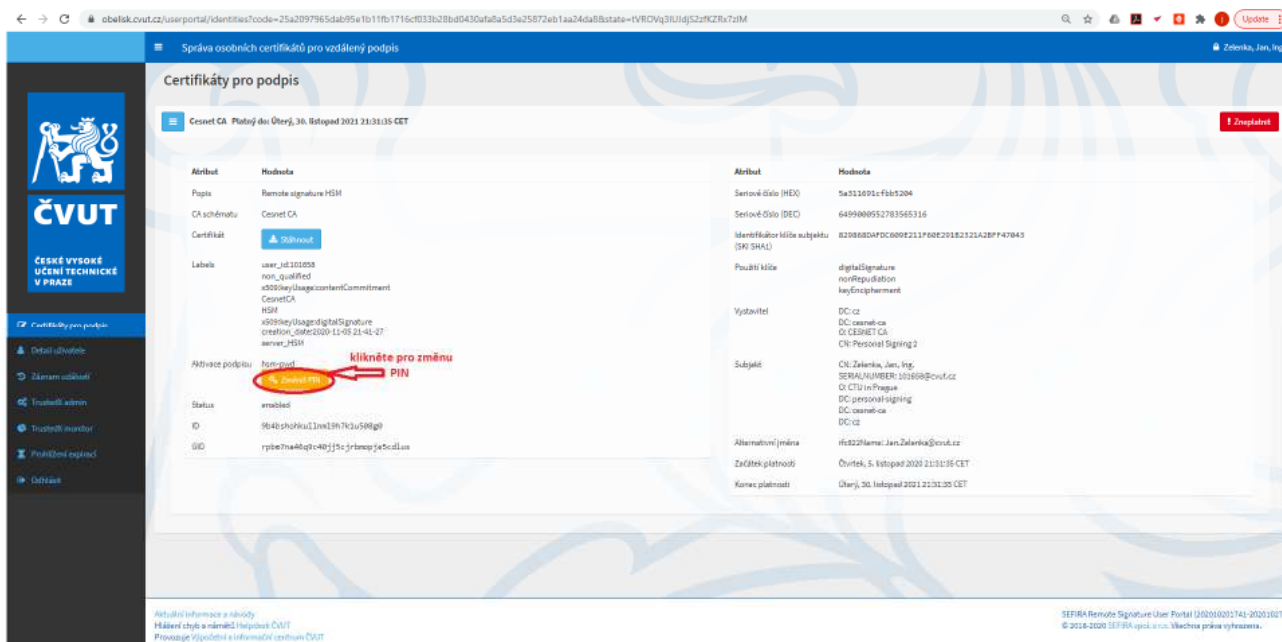
Obr. 6 Nový certifikát – úspěšné vydání a detail certifikátu

- Platnost tohoto certifikátu je 390 dní, poté si musíte stejným způsobem požádat o certifikát nový.
- Certifikát můžete sami zneplatnit v záložce „Certifikáty pro podpis“ tlačítkem „Zneplatnit“ po provedení autorizace operace.
- automaticky jsou certifikáty zneplatňovány v případě, že přijdete o identitu typu A nebo o vztah k ČVUT
- U certifikační autority CESNET CA je vydáván v tomto případě certifikát, sloužící pouze pro vnitřní oběh elektronických dokumentů v systému AEDO a pouze pro tento interní systém je uznávaný a důvěryhodný, jiné dokumenty není možné podepsat ani certifikát používat jiným způsobem např. pro šifrování e-mailů.

3. Změna PIN


3.1. CESNET CA

Pokud máte dojem, že došlo k vyrazení Vašeho PIN, můžete PIN změnit. V detailech certifikátu (viz výše) uvidíte u položky Aktivace podpisu: hsm-pwd tlačítko „Změnit PIN“. Předpokladem je, že si PIN pamatujete.



Obr. 7 Změna PIN – detail certifikátu a tlačítka pro změnu PIN

User Portal vyžaduje od uživatele Zelenka, Jan, Ing. povolení k:

 **Manage the password of your server signing identities**

Zadejte PIN k vašim podpisovým klíčům:

PIN

Zadejte nový PIN k vašim podpisovým klíčům:

Nový PIN

Potvrdit PIN

Obr. 8 Změna PIN – zadání stávajícího a nového PIN

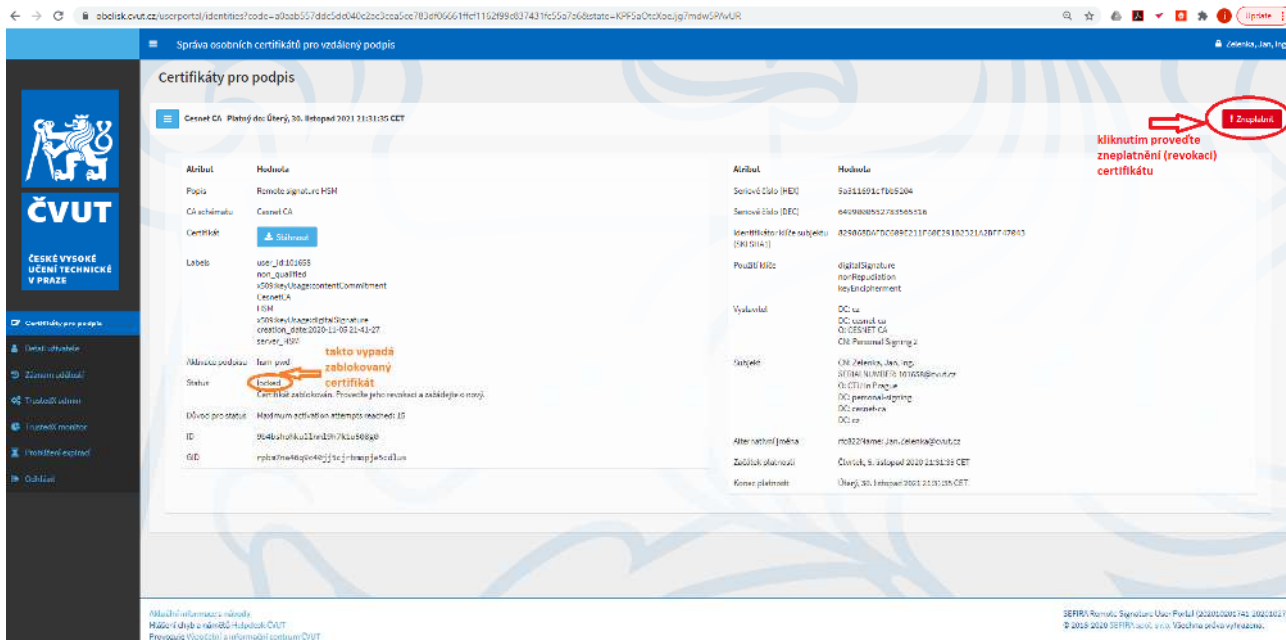
Po zadání platného PIN a nového do obou dvou políček (Nový PIN, Potvrzení PIN) a stisknutí tlačítka „Autorizovat“ bude PIN změněn.



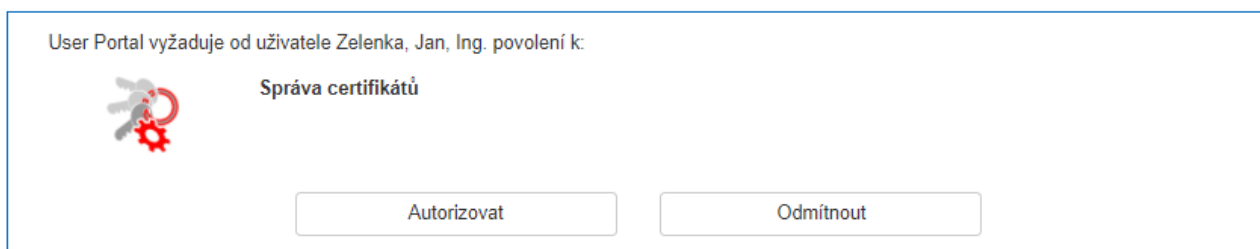
Obr. 9 Změna PIN – úspěšná změna

4. Zneplatnění certifikátu, zablokovaný certifikát, zapomenutý PIN

Pokud máte dojem, že došlo ke kompromitování důvěryhodnosti Vašeho certifikátu, můžete certifikát zneplatnit a stejným postupem výše uvedeným si vydat certifikát nový. Stejně tak, v případě že certifikát nemůžete používat, z důvodu zapomenutého PIN nebo kvůli zablokování certifikátu po opakovaně nesprávně zadaném PIN. To, že je certifikát blokový, se nepropisuje do systému USERMAP a je tedy vidět, na Obr. 2 jako platný, i když níže na Obr. 10 je vidět, že je blokový. Proto v případě potíží s podepisováním je na místě kontrola i zde.



Obr. 10 Zneplatnění certifikátu – detail certifikátu a tlačítka pro zneplatnění certifikátu



Obr. 11 Zneplatnění certifikátu – autorizace zneplatnění certifikátu



Obr. 12 Zneplatnění certifikátu – úspěšné zneplatnění

Certifikáty certifikační autority CESNET pro interní oběhy ČVUT jsou zdarma a nemusíte se tedy obávat, ale certifikáty jiných certifikačních autorit bývají zpoplatněny, u nich je na místě opatrnost.

5. Obnova certifikátu

5.1. CESNET CA

CESNET nevydává tzv. následný certifikát, tedy takový, kde by se žádost o další certifikát podepisovala současným platným certifikátem, ale v principu se jedná o vydání nového certifikátu.

Protože můžete vlastnit pouze jeden certifikát CESNET, není vidět tlačítko „+ Nový certifikát (CESNET CA)“ pokud máte stávající certifikát ještě platný.

Postup obnovení certifikátu je tedy dvoufázový.

- nejprve musíte současný certifikát zneplatnit (tlačítkem „! Zneplatnit“ vpravo na certifikátu).
- Po tomto zneplatnění se vám již na stránce certifikátů objeví tlačítko „+ Nový certifikát (CESNET CA)“ jehož stisknutím si požádáte o nový certifikát.

Oboje podle postupů uvedených výše.

V případě vypršení platnosti původního certifikátu odpadá bod a) a jedná se o stejný postup jako pro nový certifikát.

6. Použití certifikátu


6.1. CESNET CA – interní oběh dokumentů ČVUT

Pro úspěšné podepsání dokumentu je nutné mít platný certifikát. Zkontrolovat zda máte certifikát platný, můžete přihlášením do systému USERMAP na <https://usermap.cvut.cz> po rozkliknutí „Uživatelský profil“ → v části „osobní certifikáty“, viz Obr. 2.


Certifikát je uložen v zabezpečeném úložišti tzv. HSM modulu, které je mezinárodně certifikováno pro použití v systému eIDAS.

Uživatel se přihlásí do aplikace, která podporuje systém vzdáleného podepisování (např. AEDO). Tím je provedeno ověření uživatele. Aplikace dále v případě potřeby podepsání dokumentu odešle požadavek na použití certifikátu a uživatel je přesměrován na podpisovou aplikaci.

← → ↻ obelisk.cvut.cz/trustedx-resources/esignsp/v2/ui



AEDO TEST vyžaduje, aby uživatel Zelenka, Jan, Ing. podepsal následující dokument:

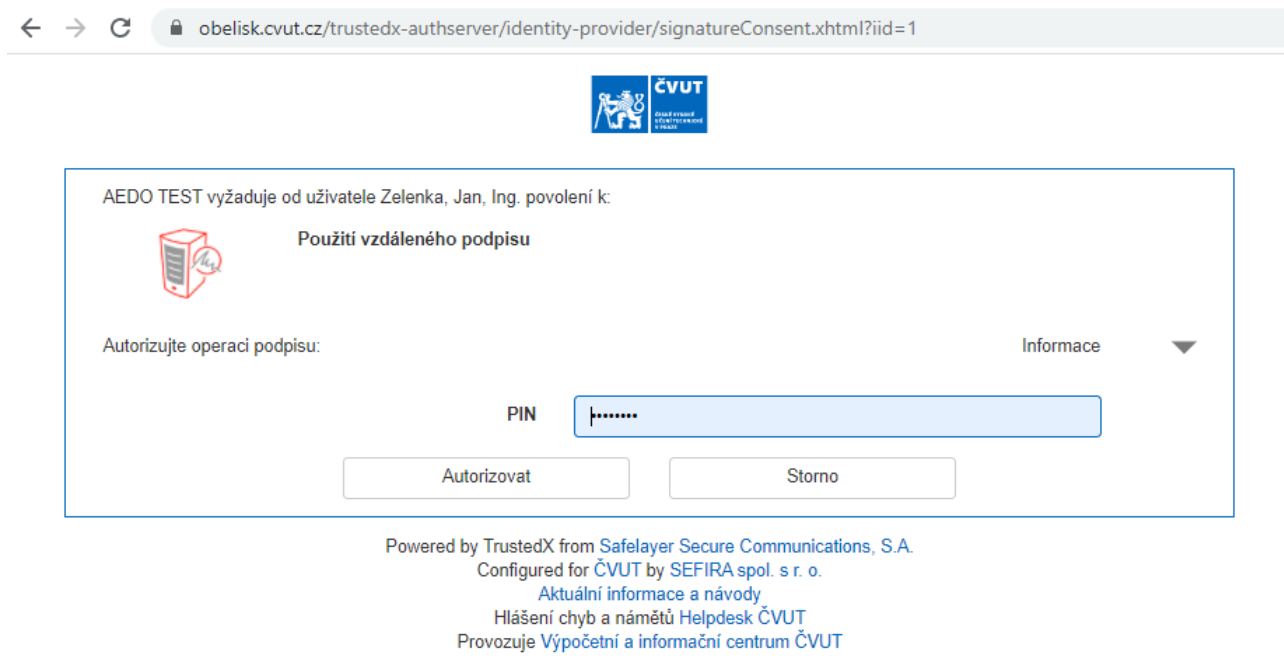
[nepritomnost-895583374.pdf](#) 

Dokument jsem přečetl(a)

Powered by TrustedX from Safelayer Secure Communications, S.A.
Configured for ČVUT by SEFIRA spol. s r. o.
[Aktuální informace a návody](#)
[Hlášení chyb a námětů Helpdesk ČVUT](#)
Provozuje Výpočetní a informační centrum ČVUT

Obr. 13 odeslán požadavek na podpis a uživatel byl přesměrován na podpisovou aplikaci

Tento požadavek na použití certifikátu je potřeba autorizovat pomocí PIN patřící k tomuto certifikátu.

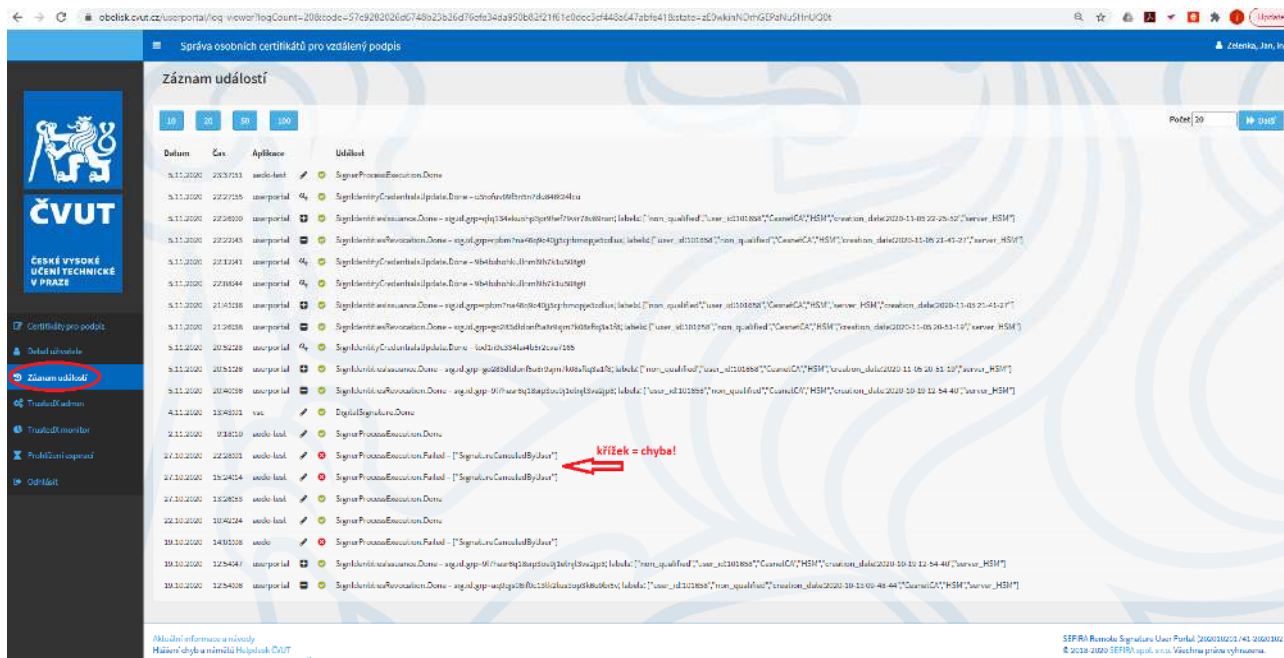


Obr. 14 Autorizace použití certifikátu pomocí PIN

Po autorizaci je výsledek podepisování vrácen podpisovou aplikací zpět do aplikace ze které požadavek na podpis vzešel (AEDO...)

7. Záznam událostí

Záznam událostí je možností, jak zjistit případné chyby při použití vzdáleného podpisu. Pokud jste vyloučili běžné chyby, jako je zapomenutý PIN, žádný, neplatný, nebo zablokovaný certifikát, podívejte se do „Záznam událostí“ opište událost nebo udělejte screenshot a kontaktujte přes helpdesk ČVUT podporu VIC.



Obr. 15 Záznam událostí uživatelského portálu systému OBELISK

8. Certifikáty vydané do 9.10.2020

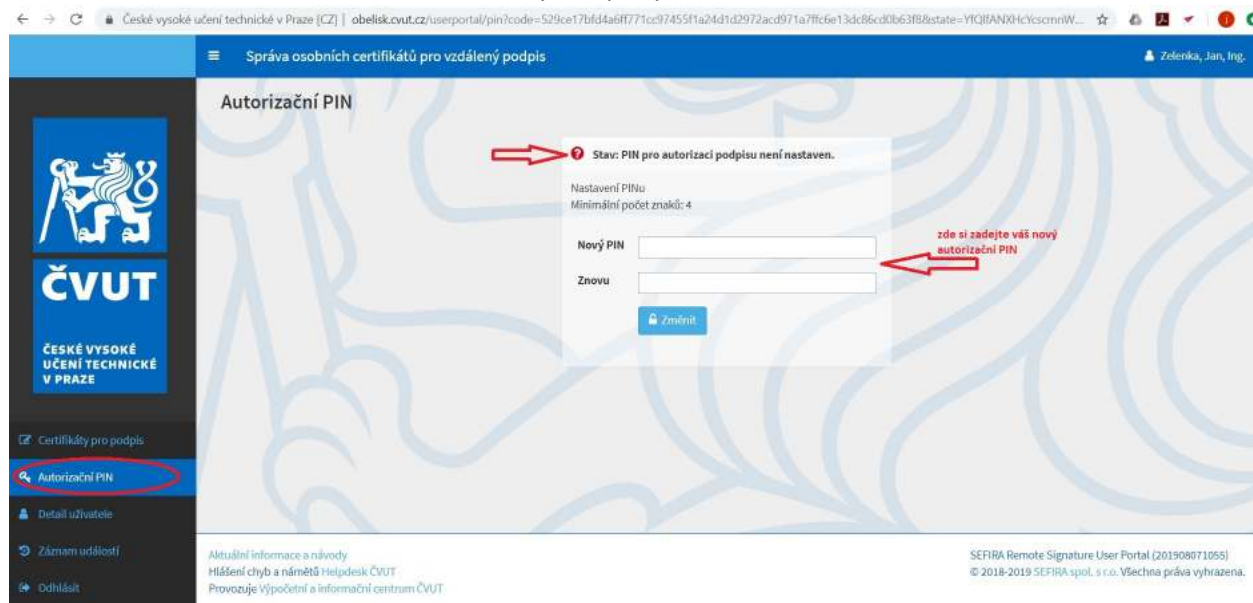
V nové politice podpisových identit je PIN svázan s konkrétním certifikátem. Pokud máte vydaný ještě certifikát podle staré politiky, můžete globálně nastavovat PIN níže uvedeným způsobem. Doporučujeme však raději stávající certifikát zneplatnit a vydat si certifikát nový.

8.1. Změna PIN

8.1.1. CESNET CA

Pokud máte dojem, že došlo k vyzrazení Vašeho PIN, nebo jste PIN zapomněli, můžete PIN změnit.

V záložce „Autorizační PIN“ nastavte váš nový PIN pro použití certifikátu.



The screenshot shows a web browser window with the URL `obelisk.cvut.cz/userportal/pin?code=529ce17bfd4a6ff71cc97455f1a24d1d2972acd971a7ffc6e13dc86cd0b63f9&state=YIQIIFANXhCycsmniW...`. The page title is "Správa osobních certifikátů pro vzdálený podpis" and the user is logged in as "Zelenka, Jan, Ing.". The main content area is titled "Autorizační PIN" and contains a form with the following elements:

- A red arrow points to a message: "Stav: PIN pro autorizaci podpisu není nastaven."
- Text: "Nastavení PINu. Minimální počet znaků: 4"
- Input field: "Nový PIN" (with a red arrow pointing to it and the text "zde si zadejte váš nový autorizační PIN")
- Input field: "Znovu"
- Button: "změnit"

The left sidebar contains a menu with "Autorizační PIN" highlighted in blue. At the bottom of the page, there is a footer with "Aktuální informace a návody", "Hlášení chyb a námětů Helpdesk ČVUT", "Provozuje Výpočetní a informační centrum ČVUT", and "SEFIRA Remote Signature User Portal (201908071055) © 2018-2019 SEFIRA spol. s r.o. Všechna práva vyhrazena."

Obr. 16 Změna PIN u certifikátů do 9.10.2020

Tato operace je ověřována pomocí kódu, který je systémem zaslán na uživateluva primární adresu.



The screenshot shows a verification screen with the following text:

User Portal vyžaduje přihlášení.

Ověřovací kód byl odeslán na Vaši emailovou adresu zelenkj3@fd.cvut.cz. První část kódu je 5474. Prosím, zadejte druhou část kódu (posledních 16 znaků).

A red arrow points to the "Kód" input field with the text "vlozte druhou část kódu, který vám přijde na email a stiskněte "Ověřit kód"". The "Ověřit kód" button is circled in red.

Powered by TrustedX from Safelayer Secure Communications, S.A.

Obr. 17 Ověření operace ověřovacím kódem

Po ověření tímto kódem a autorizací operace



User Portal vyžaduje od uživatele Zelenka, Jan, Ing. povolení k:



Správa hesel

Autorizovat

Odmítnout

Powered by TrustedX from Safelayer Secure Communications, S.A.
Configured for ČVUT by SEFIRA spol. s r. o.

Obr. 18 Autorizace operace

je PIN nastaven.