

## Instructions for obtaining a PostSignum (CA) certificate for users with qualified signature rights

### INTRODUCTION

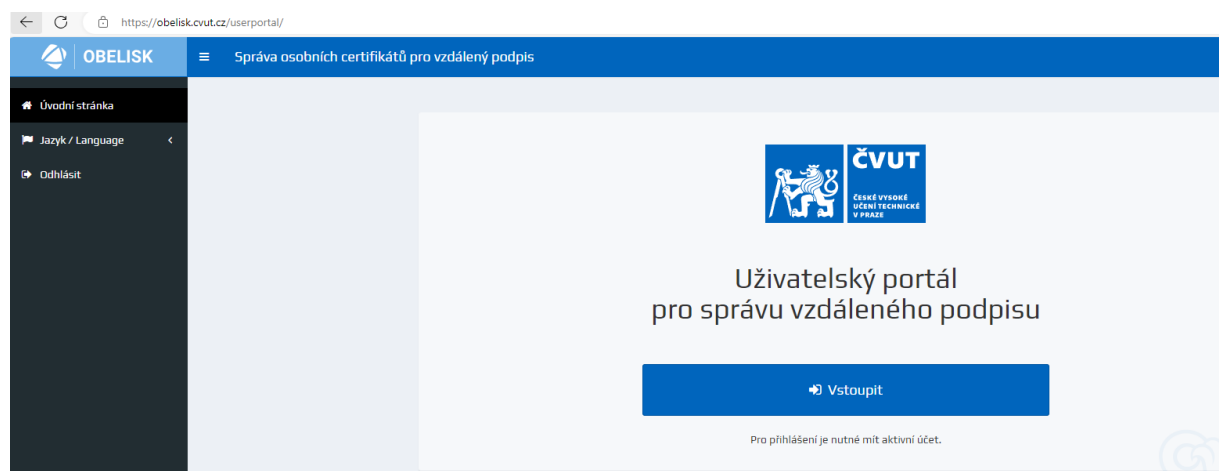
On October 7, 2024, all certificates from the certification authority PostSignum were invalidated in the CTU system. They now need to be migrated from the old system to the new one, or persons entitled to a qualified signature can establish it anew.

From 7 October 2024, users **must set up a new PIN**.

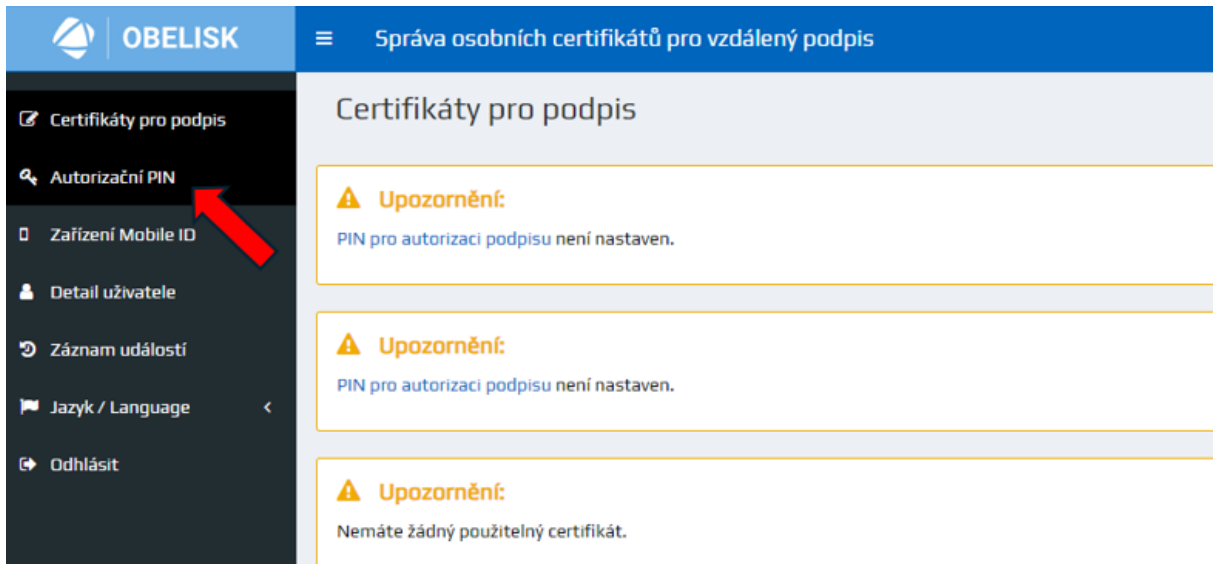
The change compared to the previous system consists in the absence of the need to use a separate PIN for each certificate. **Now one PIN permanently covers all certificates**. Compared to the past, the PIN must contain 2 or more character sets (a-z, A-Z, 0-9 and others).

If we **forget** or enter the PIN **incorrectly** (there are 5 attempts in total) - we will generate a new one. Since we are logged into the CTU system via SSO, the system knows which certificates are ours and matches us. Forgetting or entering it incorrectly does not affect the validity of the certificate.

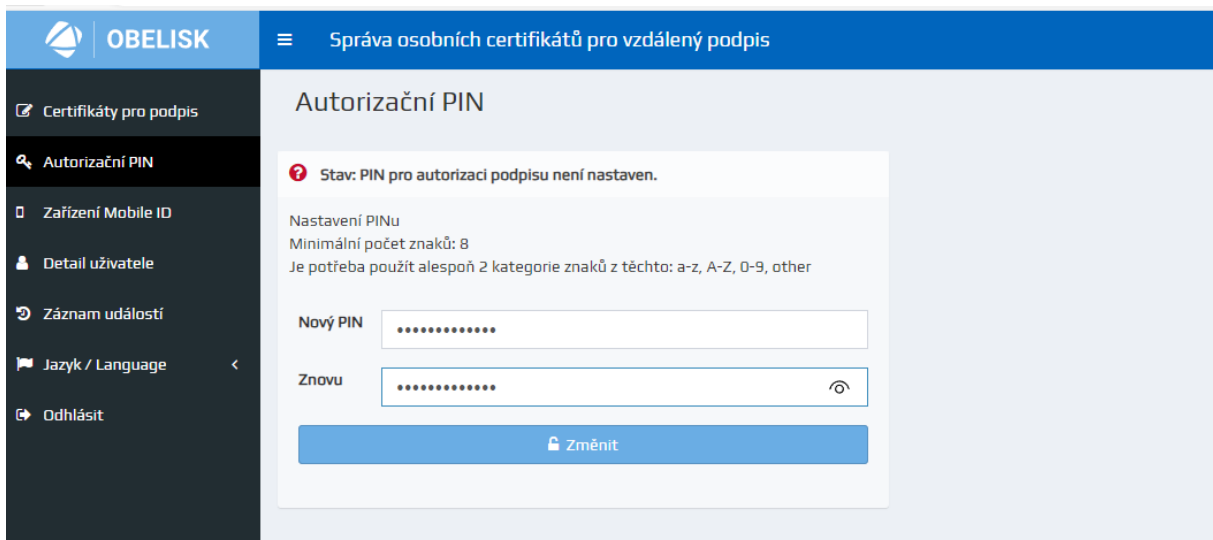
1. Enter the address <https://obelisk.cvut.cz/> in the browser. The page Management of personal certificates for remote signature will be loaded.



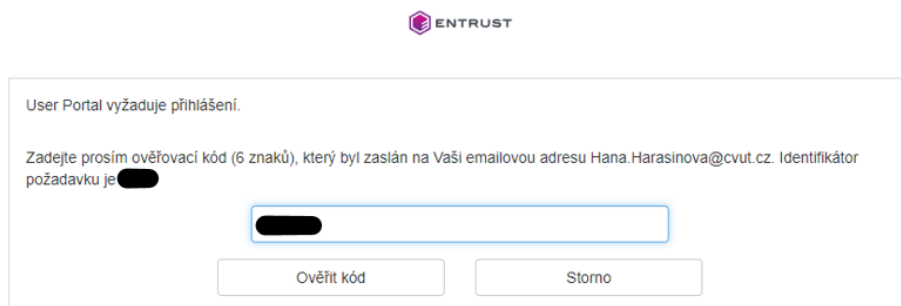
2. Log in to the CTU system via the Enter button with the CTU universal password, the page will look like this. **Attention - before obtaining the New PostSignum certificate itself, you need to obtain an Authorization PIN!**



3. After clicking, the following page will appear. Enter the new authorization PIN and confirm.



4. Security verification will redirect us to the next page, a confirmation code will be sent to the preferred email in Usermap. We'll put it in.



5. After successful verification, we get to the original page, where we now click on the Signing Certificates button.

The screenshot shows the OBELISK administration interface. The top header is blue with the OBELISK logo and the text 'Administration of personal certificates for remote signature'. The left sidebar is dark grey with a search icon and several menu items: 'Signing certificates' (highlighted with a red arrow), 'Authorization PIN', 'Mobile ID device', 'User detail', 'Event log', 'Mobile ID operator', 'Language / Jazyk', and 'Logout'. The main content area is white and titled 'Authorization PIN'. It features a green success message: 'Success: PIN was changed.' Below this is a 'Status: OK' indicator with a 'Remove' button. A 'Change PIN' section follows, with instructions: 'Enter at least 8 characters. You have to use at least 2 character categories out of these: a-z, A-Z, 0-9, other'. There are two input fields: 'New PIN' and 'Repeat'. At the bottom is a blue 'Change' button.

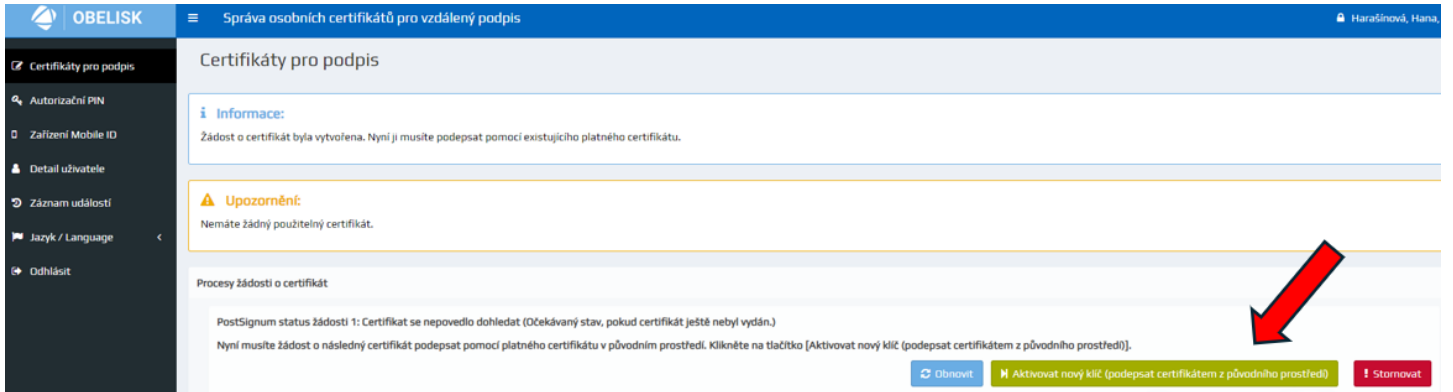
6. On the next page, select Certificate migration (PostSignum OCA).

The screenshot shows the OBELISK administration interface. The top header is blue with the OBELISK logo and the text 'Správa osobních certifikátů pro vzdálený podpis'. The left sidebar is dark grey with a search icon and several menu items: 'Certifikáty pro podpis' (highlighted), 'Autorizační PIN', 'Zařízení Mobile ID', 'Detail uživatele', 'Záznam událostí', 'Jazyk / Language', and 'Odhlásit'. The main content area is white and titled 'Certifikáty pro podpis'. It features a yellow warning message: 'Upozornění: Nemáte žádný použitelný certifikát.' Below this are three green buttons: 'Nový certifikát (Cesnet CA)', 'Nový certifikát (PostSignum OCA)', and 'Migrace certifikátu (PostSignum OCA)' (highlighted with a red arrow).

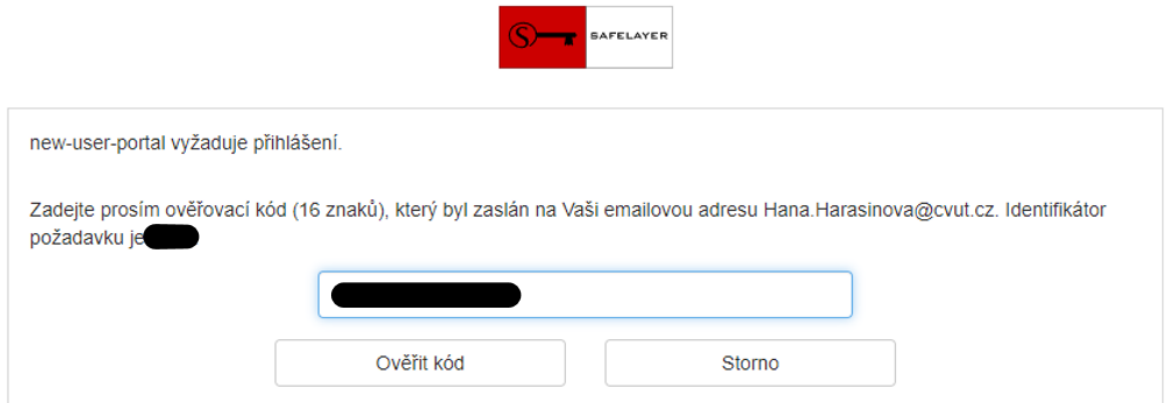
7. The window for entering a new PIN will open again. We will insert.

The screenshot shows the OBELISK login window. The title is 'OBELISK' and the subtitle is 'Zadejte PIN kód'. There are two input fields: 'Uživatelské jméno' (username) with the value 'psenijan' and 'PIN kód' (PIN code) with a masked input. Below the fields are two blue buttons: 'Pokračovat' (Continue) and 'Storno' (Cancel).

8. The following window will appear, click Activate new key

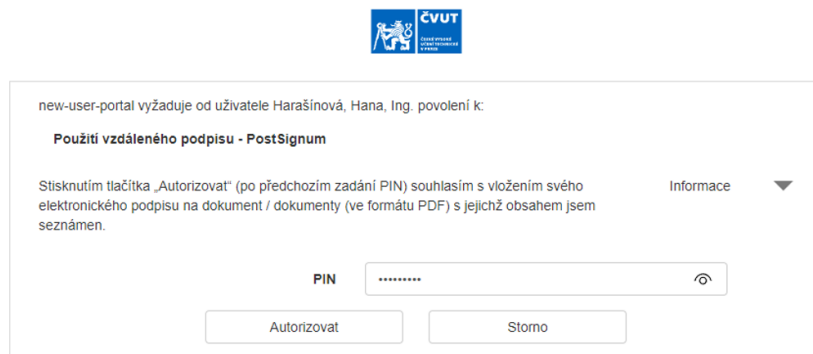


9. Now we will again fill in the verification code that came to us by email.



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

10. Now we enter the **ORIGINAL PIN** with which we confirmed the original certificate.



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

11. We will wait for 2 emails. **Attention, the waiting time can be up to several minutes.** The first one just tells us that PostSignum has accepted the request (we don't show it here). In the second, we have a link to the PostSignum page of the Czech Post, see below.

Upozornění na přípravu certifikát

info.postsignum@cpost.cz  
Komu: Harašínová, Hana; Harašínová, Hana  
Podpisné užívatelem: info.postsignum@cpost.cz

Vážená zákaznice, vážený zákazník,  
na základě Vaší žádosti Vám byl vydán certifikát.

Vydání certifikát stahnete z uvedené webové stránky:  
[https://www.postsignum.cz/nabidka\\_vydaneho\\_certifikatu.html?id=4253099&fingerprint=92F12FD270475AAEF8BCDC35CC594ADEECEF06F](https://www.postsignum.cz/nabidka_vydaneho_certifikatu.html?id=4253099&fingerprint=92F12FD270475AAEF8BCDC35CC594ADEECEF06F)

Pokud je výše uvedený odkaz rozdělen na více řádků, zkopírujte jej do libovolného textového editoru (Poznámkový blok, Word) a ručně spojte. Upozorňujeme, že vydání certifikát je nutné vyzvednout z výše uvedené adresy do 59 dní. Po překročení této doby budeme automaticky předpokládat, že certifikát nepřijímáte a bude zneplatněn. Vydání certifikátu je i v tomto případě zpoplatněno.

Protokol o vydání certifikátu lze stáhnout z výše uvedené webové stránky.

[TIP]  
Certifikát nainstalujte (nainportujte) pomocí aplikace, kde jste generovali elektronickou žádost.

[TIP]  
Po instalaci Vašeho certifikátu nezapomenejte provést jeho zálohu (zálohu nelze provést, pokud máte klíč uloženy na bezpečném prostředku - token/cipova karta).  
[https://www.postsignum.cz/faq/navody/zaloha\\_crt\\_p12/index.html](https://www.postsignum.cz/faq/navody/zaloha_crt_p12/index.html)

S jakýmkoliv problémem či dotazem se, prosím, obraťte na HelpDesk České pošty  
e-mail: [helpdesk-ca@cpost.cz](mailto:helpdesk-ca@cpost.cz), tel: 210 123 456 (linka je zpoplatněna dle bezneho tarifu). Pracovní doba HelpDesku je v pracovní dny od 8 do 18 hod.

12. After clicking, the Czech Post – PostSignum page will appear, click on Accept and that's all on this page. We can close it.

PostSignum

Úvodní stránka | Certifikát Online | Zákaznický portál | Zákaznická podpora | Kontakty

Vyhledat >> Veřejná správa >> Firmy a organizace >> Podnikatelé (OSVČ) >> Fyzické osoby

Navigace PostSignum

- Popis služeb PostSignum
- Postup pro získání certifikátu
- Ceník služeb
- Dokumenty, návody a jiné soubory
- Pobočky
- Certifikáty uživatelů
- Certifikáty a CRL autorit
- Generování žádosti o certifikát
- Instalace vydaného certifikátu
- Další služby PostSignum
- Programy ke stažení
- FAQ

» Generování žádosti o certifikát

» Stažení formulářů smluv

» Certifikát Online

» Programy ke stažení

» Obnova certifikátu

» Časové razítko TSA

» Objednávky produktů

» Úvodní stránka » Nabídka vydaného certifikátu

### Nabídka vydaného certifikátu

|                       |  |
|-----------------------|--|
| Vystavitel            | QCA  |
| Subjekt               | T=referent - oddělení personální a mzdové,serialNumber=P573562,G=Hana,SN=Harašínová,CN=Ing. Hana Harašínová,OU=506164,OU=Správa účelových zařízení,O=České vysoké učení technické v Praze,OrganizationIdentifier=NTRCZ-68407700,C=CZ |
| E-mail                | hana.harasinova@cvut.cz  |
| Sériové číslo         | 23486364   |
| Certifikát vydán      | 9.10.2024  |
| Kryptografický otisk  | 92F12FD270475AAEF8BCDC35CC594ADEECEF06F  |
| Certifikační politika | Kvalifikované osobní certifikáty   |

Protokol o vydání Podrobné informace o certifikátu naleznete v Protokolu o vydání. Stiskněte tlačítko **Přijmout** pro akceptaci certifikátu. Stiskněte tlačítko **Nepřijmout** pro odmítnutí následného certifikátu.

Prohlášení:  
Akceptováním certifikátu žadatel přebírá certifikát s výše uvedenými údaji, čímž se zákazník stává držitelem certifikátu.  
Žadatel stvrzuje:

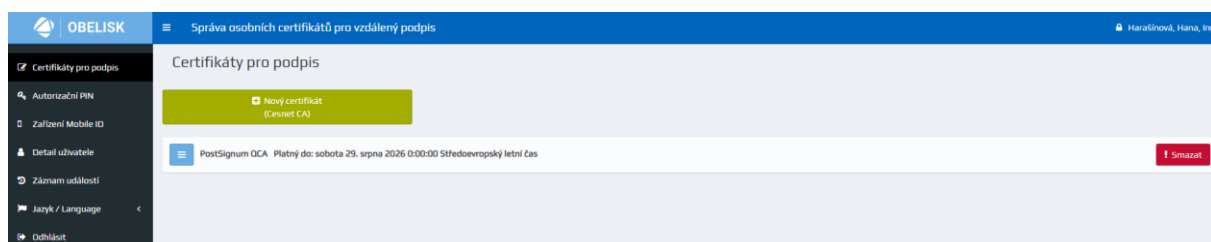
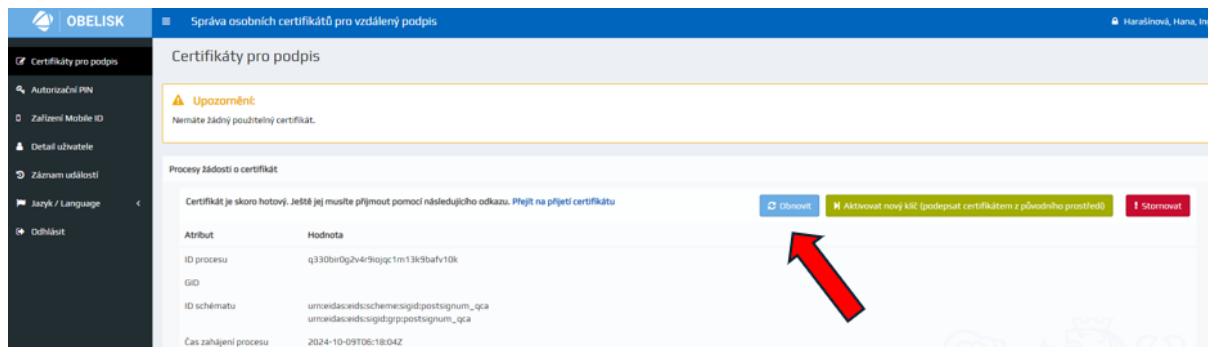
- že na sebe bere závazky vyplývající z certifikační politiky, podle níž byl certifikát vydán;
- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že soukromý klíč odpovídající veřejnému klíči v certifikátu vlastní jiná osoba;
- že je povoleno v příslušné certifikační politice;
- že výše uvedené údaje popisující certifikát jsou správné a úplné.

**Přijmout** Přijetím certifikátu žadatel přebírá certifikát s výše uvedenými údaji, čímž se zákazník stává držitelem certifikátu.

**Nepřijmout** Pokud nechcete vydaný certifikát přijmout, tak stiskněte tlačítko **Nepřijmout**. Akceptaci nebo odmítnutí certifikátu je nutné provést do 7.12.2024. Po uplynutí této doby bude certifikát automaticky považován za odmítnutý a bude zneplatněn.

[Informace o zobrazeném Hash kódu \(algoritmu\) ve formátu SHA 1](#)

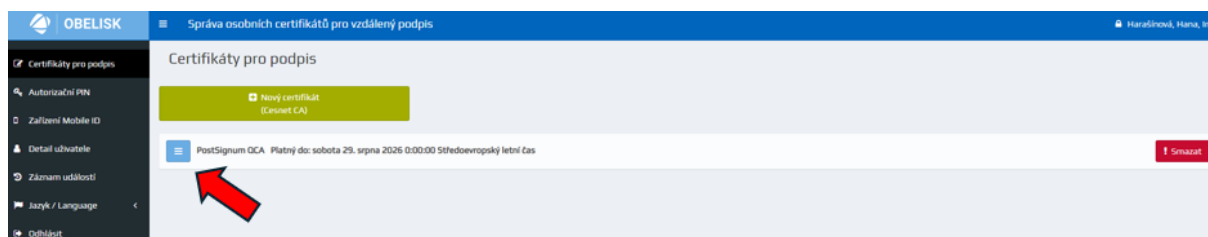
13. We return to the Obelisk User Portal. We can continuously click on the Restore button, but here again we have to wait, usually within 4 minutes. A final window with an overview of all our certificates will then appear and THAT'S IT.



### ALSO optional – for PMSV employees.

It is necessary to report the change of the certificate to the relevant authorities, usually to the CSSS (tel. 800 050 248, option 3), where after our verification (mostly they want the ID number of the CTU organization (68407700) or birth number) we will dictate a new serial number. This can be found by clicking on the three lines on the left.

Anyone who uses the PARTNERLINK application to transfer data must change the certificate in it as well, or in another Gate.



**OBELISK** Správa osobních certifikátů pro vzdálený podpis

**Certifikáty pro podpis**

Nový certifikát (Cesnet CA)

PostSignum OCA Platný do: sobota 29. srpna 2026 0:00:00 Středoevropský letní čas

| Atribut     | Hodnota                                | Atribut                                 | Hodnota                                  |
|-------------|--|---|--|
| Popis       | Remote signature - PostSignum          | Algoritmus klíče                        | RSA                                      |
| CA schémátu | PostSignum OCA                         | Algoritmus podpisu certifikátu          | SHA256withRSA                            |
| Certifikát  | <a href="#">Stáhnout</a>               | Seriové číslo (HEX)                     | 01665F9c                                 |
| Labels      | env_2024<br>server<br>qualified<br>HSM | Seriové číslo (DEC)                     | 23486364                                 |
|             |  | Identifikátor klíče subjektu (SKI SHA1) | 980B963467E484B1C47B0FB526094DC93780A804 |

