Instructions for obtaining a PostSignum (CA) certificate

for users with qualified signature rights

INTRODUCTION

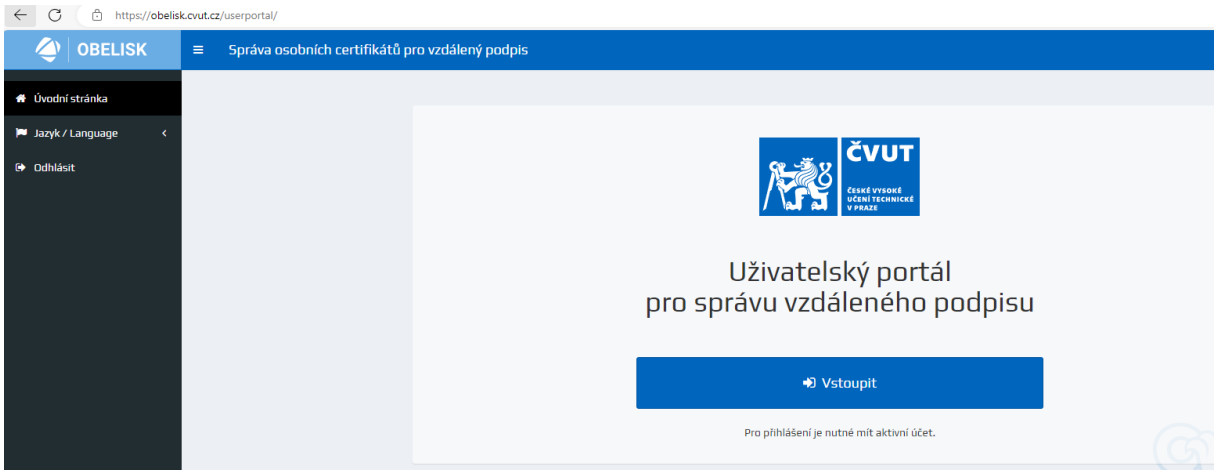
On October 7, 2024, all certificates from the certification authority PostSignum were invalidated in the CTU system. They now need to be migrated from the old system to the new one, or persons entitled to a qualified signature can establish it anew.

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

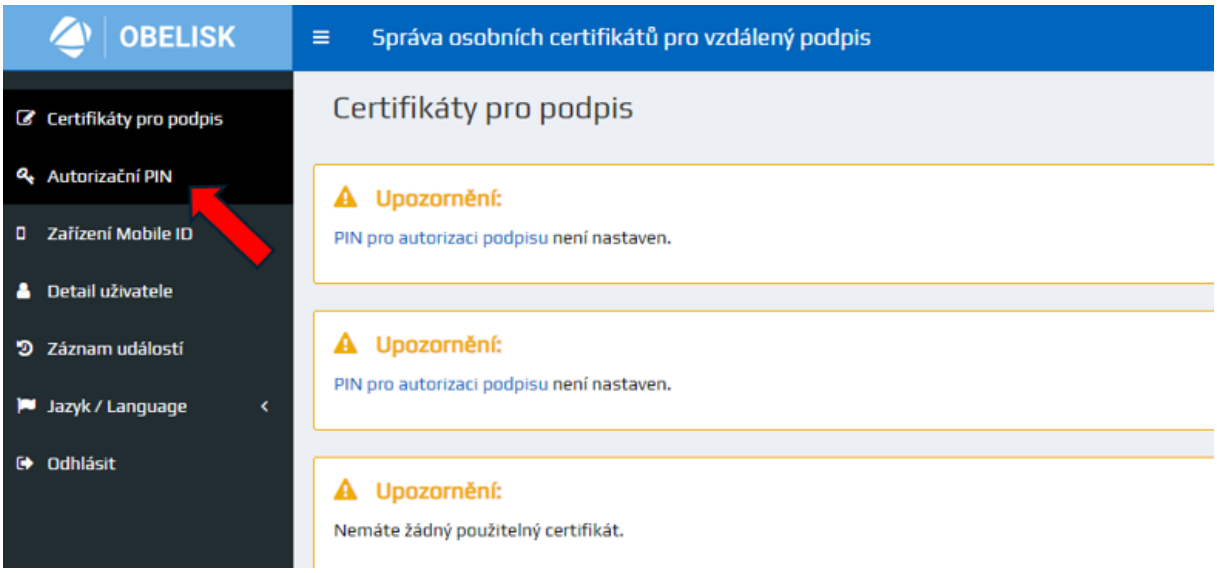
The change compared to the previous system consists in the absence of the need to use a separate PIN for each certificate. **Now one PIN permanently covers all certificates.** Compared to the past, the PIN must contain 2 or more character sets (a-z, A-Z, 0-9 and others).

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.

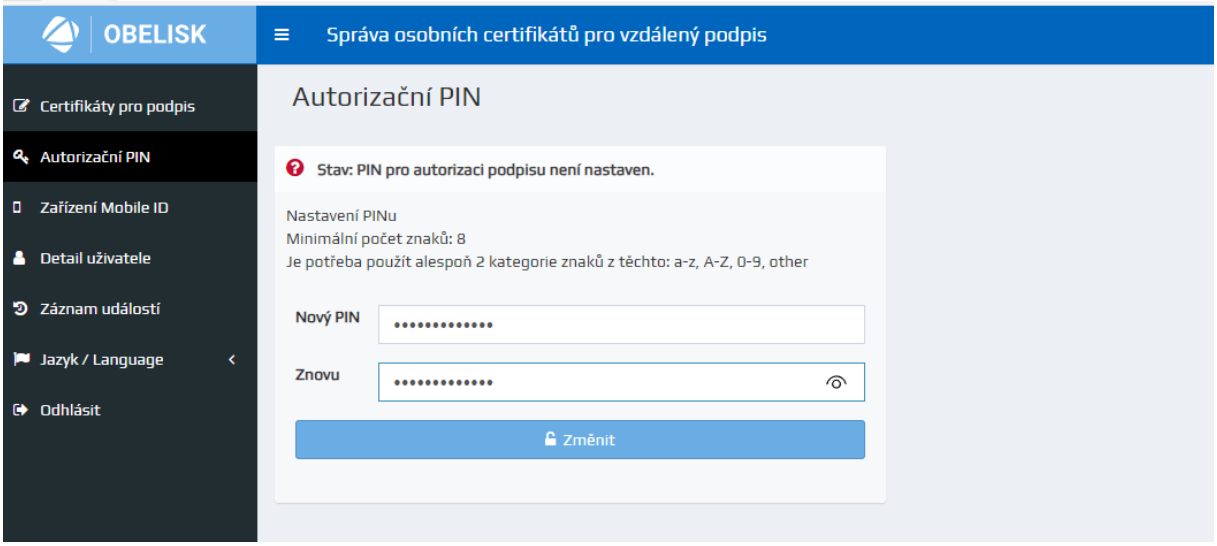
1. Enter the address https://obelisk.cvut.cz/ in the browser. The page Management of personal certificates for remote signature will be loaded.



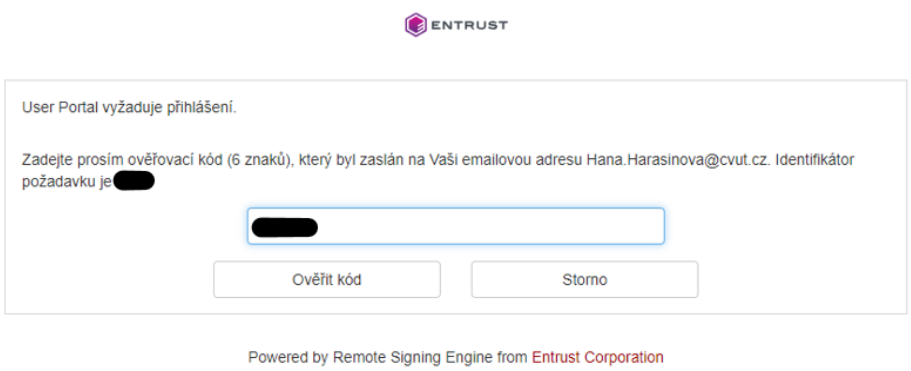
2. Log in to the CTU system via the Enter button with the CTU universal password, the page will look like this. **Attention - before obtaining the New PostSignum certificate itself, you need to obtain an Authorization PIN!**



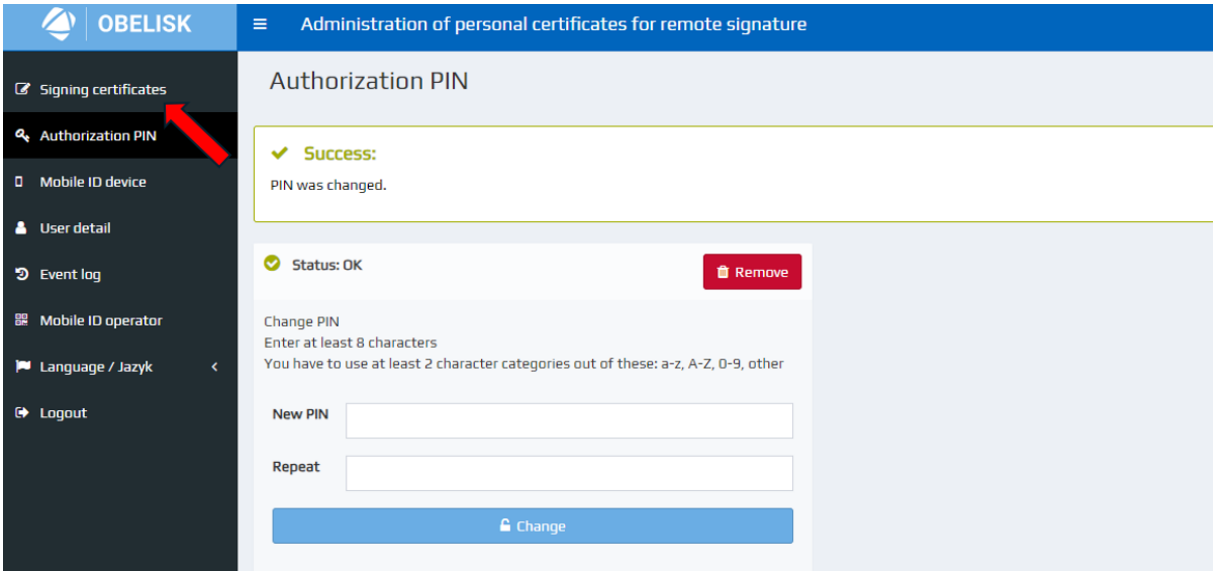
3. After clicking, the following page will appear. Enter the new authorization PIN and confirm.



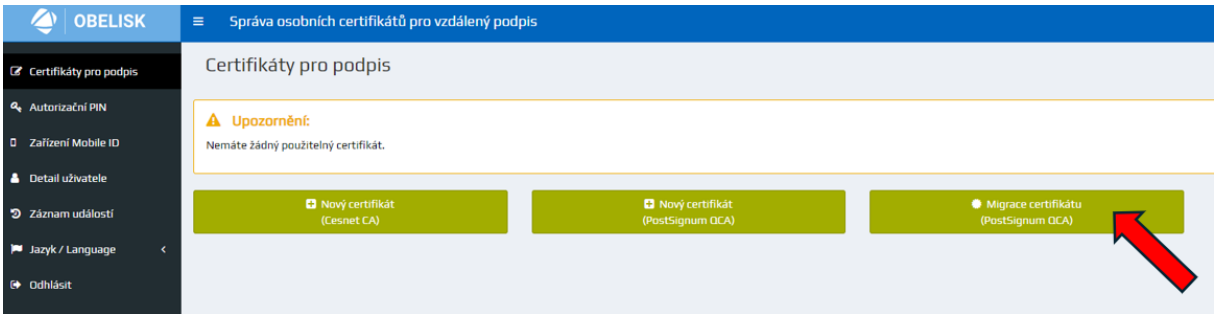
4. Security verification will redirect us to the next page, a confirmation code will be sent to the preferred email in Usermap. We'll put it in.



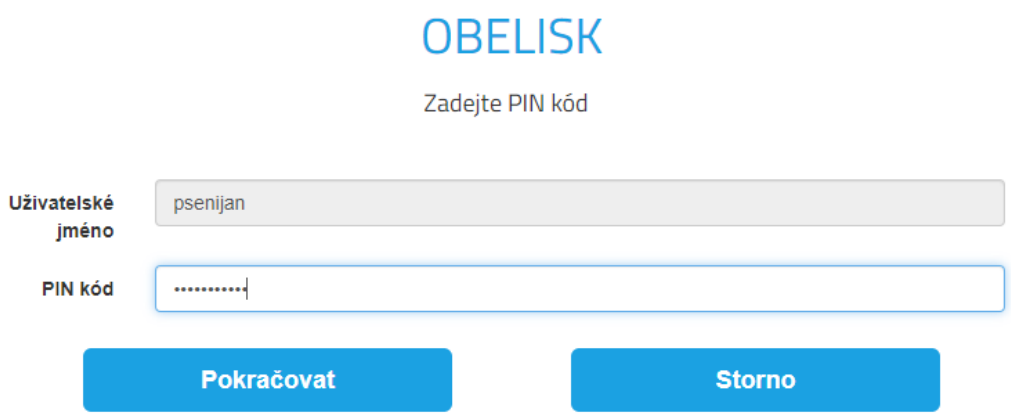
5. After successful verification, we get to the original page, where we now click on the Signing Certificates button.



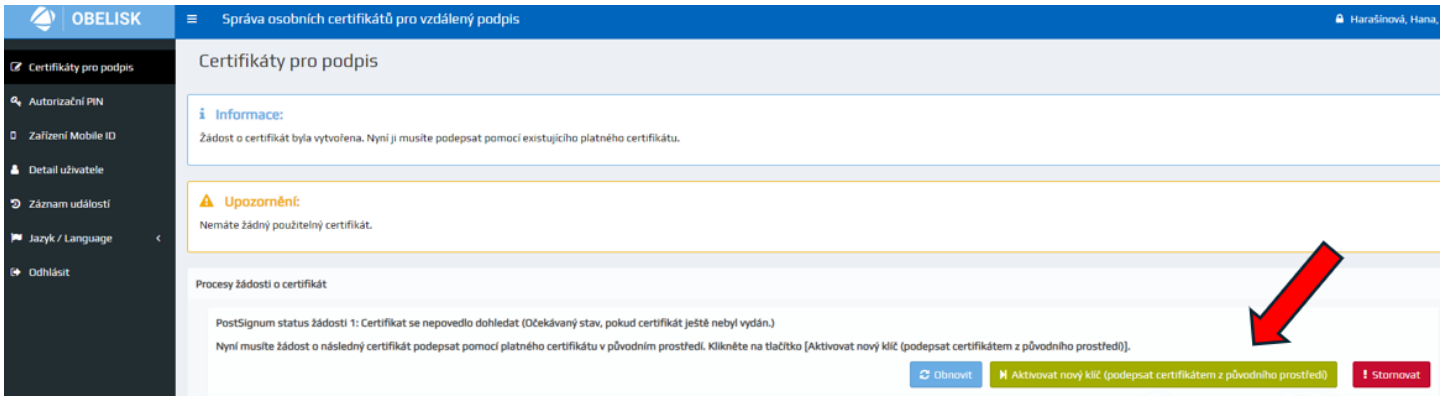
6. On the next page, select Certificate migration (PostSignum OCA).



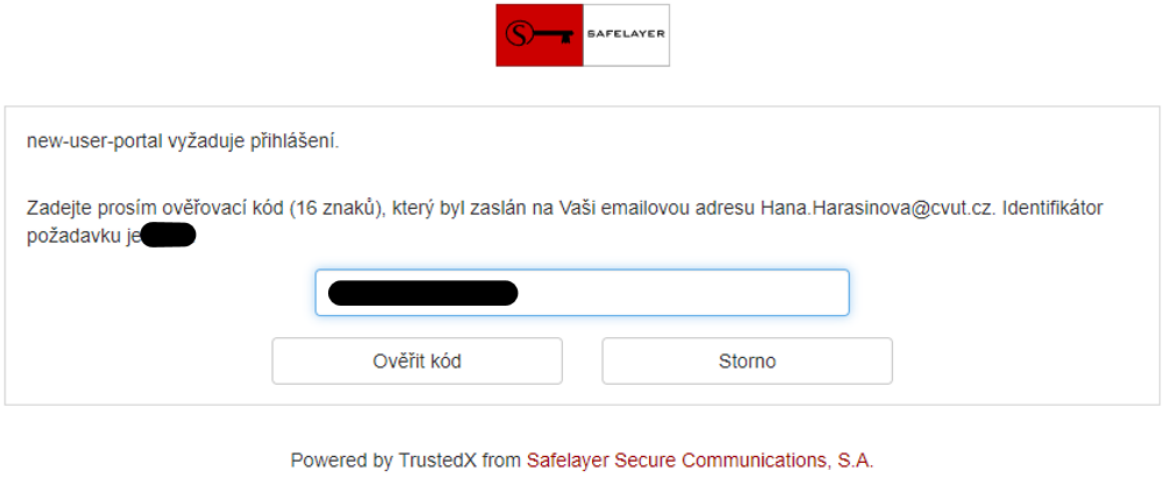
7. The window for entering a new PIN will open again. We will insert.



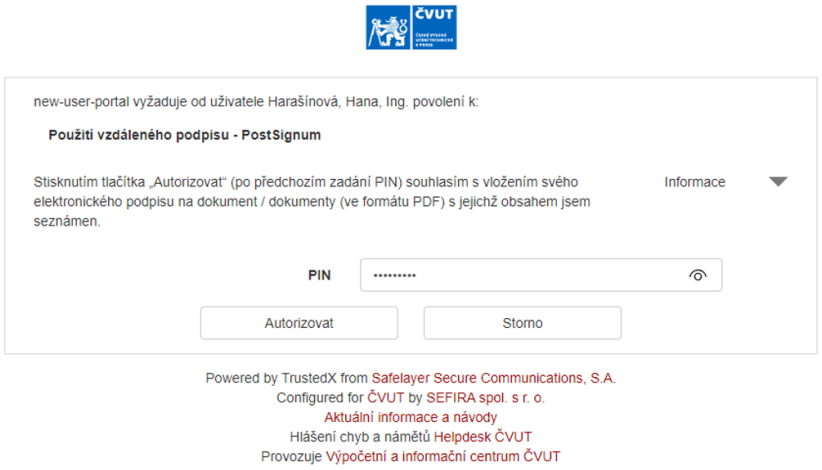
8. The following window will appear, click Activate new key



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

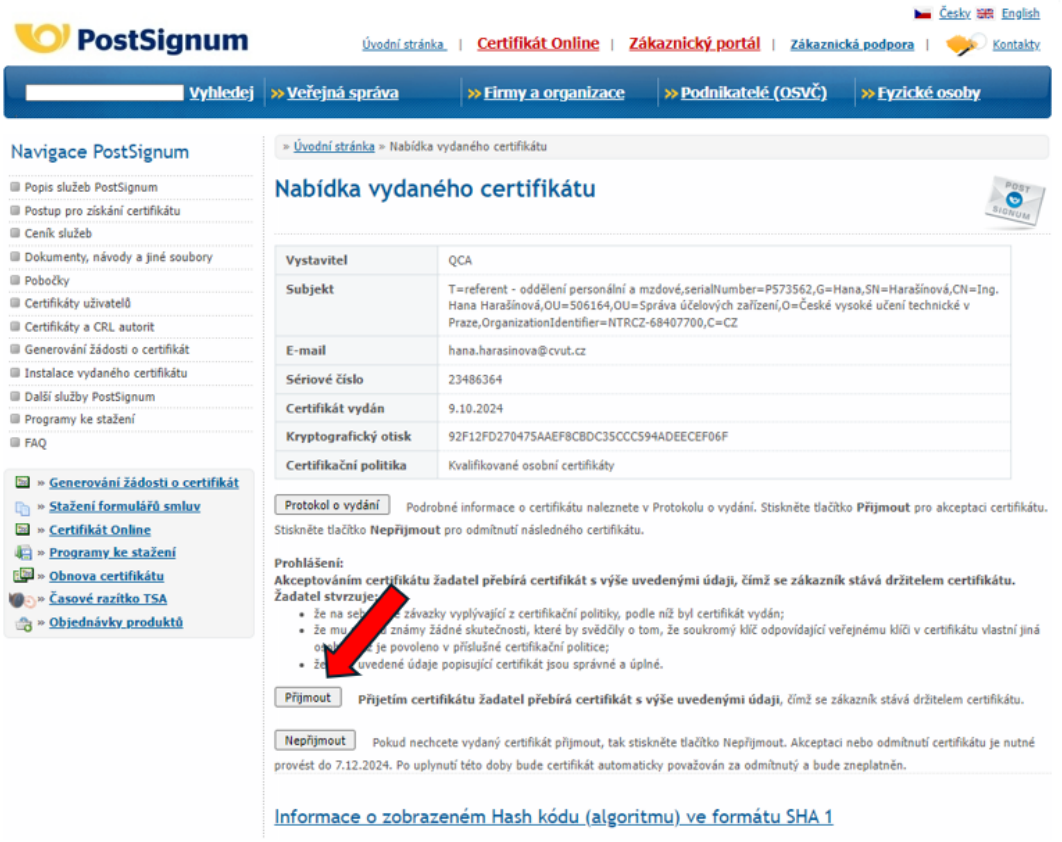


10. Now we enter the **ORIGINAL PIN** with which we confirmed the original certificate.

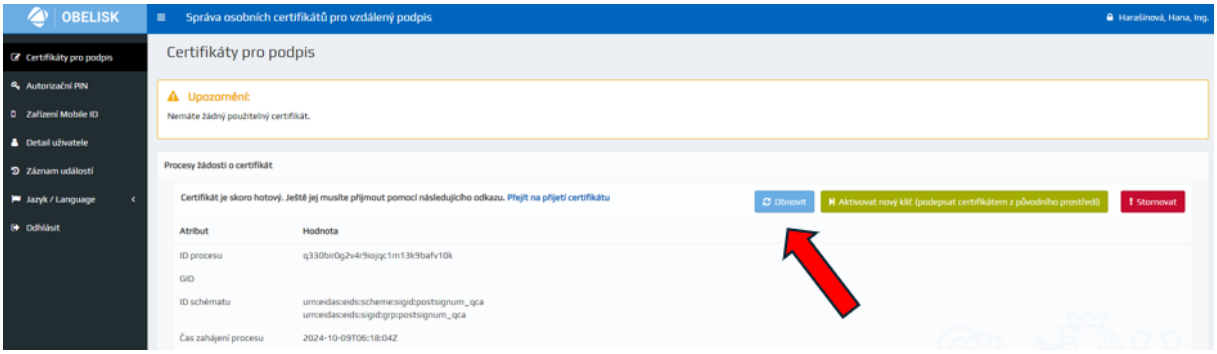


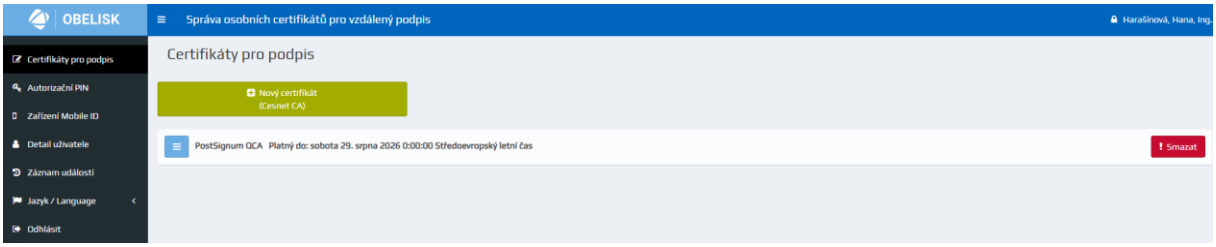
11. We will wait for 2 emails. **Attention, the waiting time can be up to several minutes**. The first one just tells us that PostSignum has accepted the request (we don't show it here). In the second, we have a link to the PostSignum page of the Czech Post, see below.

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



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.

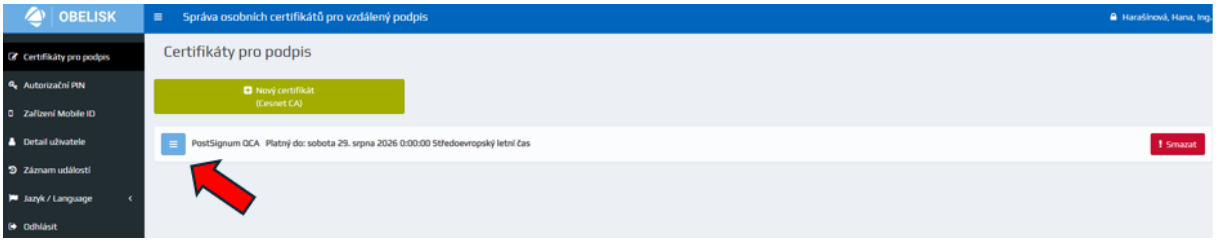


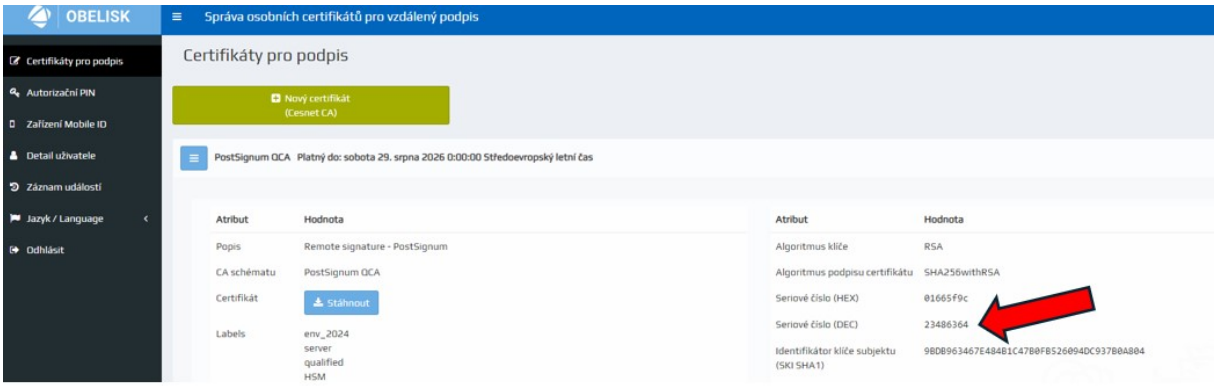


ALSO optional – for PMSV employees.

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
Autorizační PIN
Zařízení Mobile ID
Detail uživatele
Záznam událostí
Jazyk / Language
Odhlásit
Certifikáty pro podpis
Nový certifikát
(Cesnet CA)
PostSignum QCA Platný do: sobota 29. srpna 2026 0:00:00 Středoevropský letní čas
Atribut
Hodnota
Popis
Remote signature - PostSignum
CA schématu
PostSignum QCA
Certifikát
Stáhnout
Labels
env_2024
server
qualified
HSM
Atribut
Hodnota
Algoritmus klíče
RSA
Algoritmus podpisu certifikátu
SHA256withRSA
Seriové číslo (HEX)
01665f9c
Seriové číslo (DEC)
23486364
Identifikátor klíče subjektu (SKI SHA1)
9BDB963467E484B1C47B0FB526094DC937B0A804