ProID

PEČETĚNÍ PROID+QSEAL

INSTALAČNÍ PŘÍRUČKA A PROVOZNÍ DOKUMENTACE ŘEŠENÍ

Předkládá MONET+,a.s.
Za Dvorem 505, Zlín - Štípa

Zpracování: 25. 3. 2021
Verze číslo: 1.3

1 PROHLÁŠENÍ O AUTORSTVÍ

Informace v tomto dokumentu obsažené (tj. včetně nákresů, plánků, obrázků atd.) jsou předmětem obchodního tajemství (dle §504 Zákona č. 89/2012 Sb. v platném znění) společnosti MONET+,a.s. IČO 26217783 a dispozice s nimi podléhá právnímu řádu České republiky.
Společnost MONET+,a.s. IČO 26217783 je dle zákona č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, vykonavatelem majetkových práv k příslušným částem tohoto dokumentu.

2 OBSAH

1 Prohlášení o autorství 2
2 Obsah 3
3 Úvod 4
4 Architektura systému 5
4.1 Vlastnosti karet ProID+QSeal 6
4.1.1 Kapacita karty ProID+QSeal 6
4.1.2 Bezpečnostní kódy PIN/QPIN/PUK 6
5 Instalace 8
5.1 Před započetím instalace 8
5.2 Instalace Webového serveru a klientské aplikace QPin starter remote 8
5.2.1 Instalace ovladačů čipové karty 9
5.2.2 Instalační balíček ProID+QSeal 9
5.2.3 Instalační balíček QPinStarterRemote 14
5.3 Konfigurace služby ProId+QSeal 18
5.3.1 Dodatečná změna konfigurace 23
5.4 Zadání bezpečnostního kódu QPIN 23
5.4.1 Postup zadání hodnoty QPIN 24
5.5 Ověření instalace 25
5.5.1 IIS server, Webová služba 25
5.5.2 Ověření z klientského počítače 25
6 Vzdálená instalace společností Monet+ 27
7 PROVOZ ŘEŠENÍ PROID+QSEAL 28
7.1 API služby ProID+QSeal 28
7.2 Opakované Zadávání bezpečnostního kódu QPIN 28
7.2.1 Emailová notifikace chyby QPIN nezadán 29

3 ÚVOD

Tento dokument slouží jako návod, jak krok po kroku ve Vašem prostředí zprovoznit službu elektronického pečetění pomocí čipových karet a řešení ProID+QSeal. Instalace se skládá z několika návazných kroků, které bude provádět správce systému v klientské organizaci:

- Zakoupení licence produktu ProID+QSeal a kartu ProID+QSeal.
- Nastavení PINových hodnot na kartě ProID+QSeal.
- Vytvoření žádosti o certifikát + vydání certifikátu pro kvalifikované pečetění (postup podle dané CA).
- Instalace operačního systému a IIS.
- Připojení čtečky a karty.
- Instalace a konfigurace software ProID+QSeal.
- Spuštění služby *ProID+Qseal Service*.
- Zavedení QPIN do cache pomocí *QPIN Initializer* nebo vzdáleného zadávání pomocí aplikace *QPIN Initializer (QPIN Starter Remote)*.
- Test fungování.

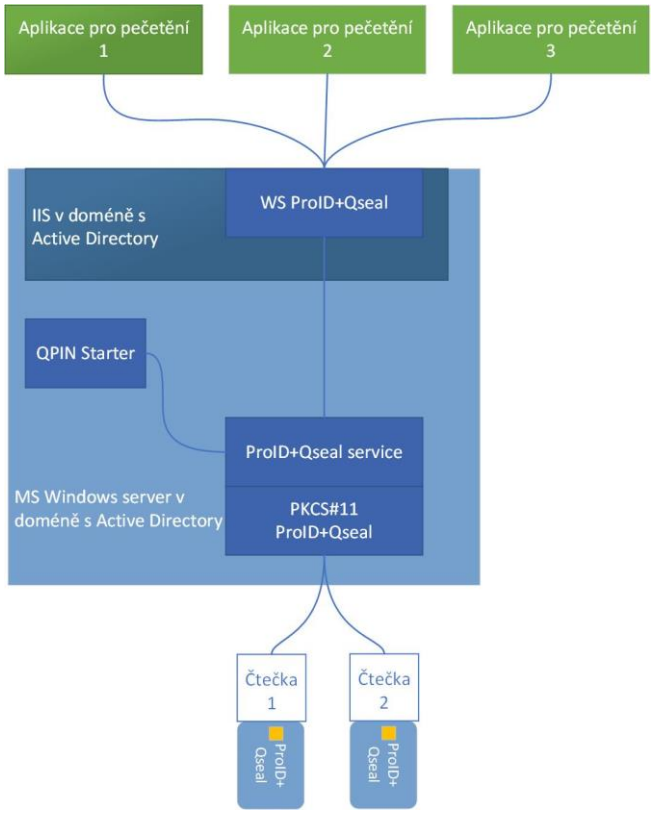
4 ARCHITEKTURA SYSTÉMU

Požadavky na vytváření kvalifikovaných pečetí budou zasílány z klientských stanic. Tyto požadavky budou přijímány na serverové straně pomocí webové služby ProID+QSeal. Tato webová služba bude komunikovat s čipovými kartami připojenými k serveru a bude zajišťovat pečetění dokumentů.

Kompletní podpora pečetění může být hostována na MS Windows Server (2012 R2 nebo vyšší) nebo Windows 10 (Professional nebo vyšší) v doméně s Active Directory. V rámci serveru bude instalováno:

- IIS, hostující webové služby.
- služba pro pečetění (WS ProID+QSeal).
- služba ProID+QSeal Service pro zajištění perzistence QPIN cache v knihovně PKCS#11.
- knihovna PKCS#11 ProID+QSeal.
- aplikace pro zavedení QPIN (QPIN Initializer) do cache v knihovně PKCS#11, prostřednictvím služby ProID+QSeal Service.

K serveru bude fyzicky připojena jedna čí více čteček čipových karet, do nichž budou vloženy karty ProID+QSeal.



Obrázek 1: Architektura řešení ProID+QSeal

QPIN cache je implementována na úrovni PKCS#11. Pověřený uživatel musí vždy "po startu" zavést QPIN do cache, pomocí uživatelské aplikace QPIN Initializer.

Služba ProID+QSeal Service běží trvale (bez ohledu na stav webové služby) a udržuje v paměti knihovnu PKCS#11. Díky trvalé přítomnosti v paměti je zajištěna perzistence QPIN v cache knihovny PKCS#11.

Schopnost vytvářet kvalifikované pečetě, vůči aplikacím třetích stran, bude serverem propagována prostřednictvím webové služby WS ProID+QSeal.

4.1 VLASTNOSTI KARET PROID+QSEAL

- Kontaktní čip Gemalto MAV4 s appletem IAS Classic a profilem ProID+QSeal, karty určené pro elektronické pečetění.
- Do těla karty není integrován bezkontaktní čip.
- Karty jsou dodány s náhodnou hodnotou bezpečnostního kódu PUK, který je vytištěný na PIN formuláři v dolní části v diskrétní zóně.
- Karty jsou dodány s výchozí hodnotou bezpečnostních kódů PIN a QPIN. Před prvním použitím je vynucena jejich změna. Změnu hodnot kódů PIN a QPIN lze provést v aplikaci Správce karty, která je součástí instalačního balíčku ProID+.
- Na karty bude vydán certifikát pro elektronické pečetění.

4.1.1 Kapacita karty ProID+QSeal

Kapacitní rozložení paměti kontaktního čipu:

- 6x RSA komerční kontejner.
- 4x RSA kvalifikovaný kontejner.
- 3x ECC komerční kontejner.
- 3x ECC kvalifikovaný kontejner.

4.1.2 Bezpečnostní kódy PIN/QPIN/PUK

Karty ProID+QSeal jsou dodávány se třemi autorizačními objekty:

- PIN pro autorizaci práce s klíči komerčních certifikátů. (dále pro rozlišení jen **PIN**).
  - PIN má povoleno využití PIN cache, v rámci jednoho spuštění aplikace postačí zadání hodnoty PIN jen jedenkrát.
  - Po zadání PIN ovladač karty udržuje čip v autorizovaném stavu, dokud se aplikace neukončí, anebo není karta vyjmuta ze čtečky.
  - Při dodání je hodnota PIN nastavena na výchozí hodnotu 11111.
  - Hodnotu PIN karty bude znát pouze právoplatný držitel karty.
  - Držitel si může hodnotu PIN kdykoli změnit na jinou hodnotu, v rozsahu 5- 15 číslic.
  - Po 3 neúspěšných pokusech zadání se hodnota PIN zablokuje.
- PIN pro autorizaci práce s klíči kvalifikovaných certifikátů. (dále pro rozlišení jen **QPIN**).
  - QPIN má povoleno konfigurační nastavení QPIN cache. Toto nastavení se provádí pomocí aplikace QPIN Initializer, viz: 5.3..
  - Při dodání je hodnota QPIN nastavena na výchozí hodnotu 11111.
  - Politika čipové karty vynucuje změnu QPIN před jejím prvním použitím.
  - Držitel si může hodnotu QPIN kdykoli změnit na jinou hodnotu, v rozsahu 5-15 číslic.
  - Po 3 neúspěšných pokusech zadání se hodnota QPIN zablokuje.
- PUK pro odblokování hodnot PIN a QPIN

- PUK má z důvodu bezpečnostní certifikace vynucenu politiku zadávání hodnoty PUK pro každou operaci odblokování. Není možné využít PUK cache.
- Při dodání je hodnota PUK vytištěna v PIN formuláři.
- Hodnotu PUK bude znát pouze právoplatný držitel karty.
- Držitel si může hodnotu PUK kdykoli změnit na jinou hodnotu, v rozsahu 8-15 číslic.
- Po 5 neúspěšných pokusech se hodnota PUK zablokuje.

5 INSTALACE

Tato kapitola slouží jako průvodce, jak krok po kroku v organizaci zprovoznit službu pečetění pomocí čipových karet ProID+QSeal.

5.1 PŘED ZAPOČETÍM INSTALACE

Před započetím instalace je třeba zkontrolovat dostupnost následujících komponent a zařízení.

- Dostupný IIS server na platformě MS Windows.
  - Windows Server (2012 R2 nebo vyšší), zařazený do domény AD.
  - Windows 10 Professional (nebo vyšší), zařazený do domény AD.
  - Minimální požadavky vycházejí z doporučených hodnot pro daný operační systém.
  - 4 GB RAM, CPU s 2x core/vcore, 30 GB diskového prostoru.
  - Na tomto serveru musí být funkční PC/SC vrstva, která zajišťuje komunikaci s čipovými kartami.
- Dostupné pečetící zařízení – karta, popřípadě karty ProID+Qseal.
  - Karta musí být pomocí čtečky, popřípadě pomocí čtečky a virtualizačního zařízení přístupná z IIS serveru.
- Na pečetícím zařízení dostupné certifikáty pro pečetění a inicializovaná hodnota bezpečnostního kódu QPIN.
  - Tento krok je podrobně popsán v návodu od poskytovatele certifikátů.
  - Je možné využívat kvalifikované pečetící certifikáty PostSignum, nebo eIdentity.
- Možnosti virtualizace.
  - Ověřena správná funkčnost s VMWare ESXi.
  - Microsoft HyperV nepodporuje možnost propagace karty/tokenu připojené k virtualizátoru do virtuálního stroje, službu tedy s touto technologií nelze provozovat.

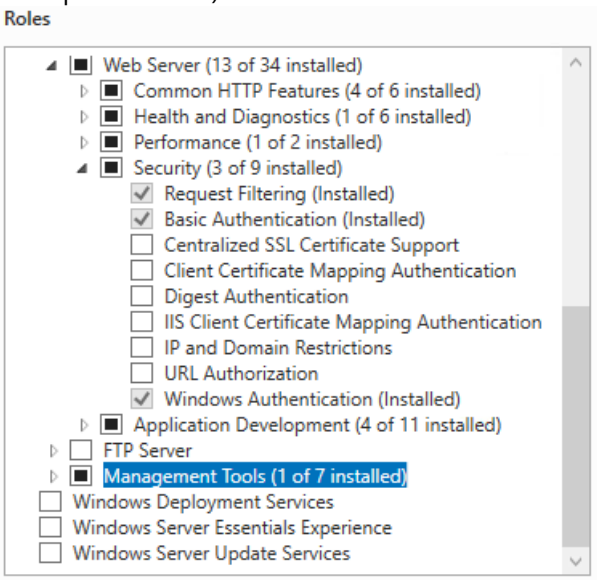
Jakmile budou tyto předpoklady připraveny, můžete přejít k instalaci IIS serveru popsané v kapitole 5.2.

5.2 INSTALACE WEBOVÉHO SERVERU A KLIENTSKÉ APLIKACE QPIN STARTER REMOTE

Na webovém serveru, kde bude provozováno řešení ProID+QSeal pro podporu pečetění bude třeba zprovoznit:

- Zajistit prostup k čipové kartě s certifikátem pro pečetění.
- Požadované SW vybavení:
  - IIS s podporou HTTPS a Windows Autentizace.

» Vydaný HTTPS certifikát pro IIS server (instalace ProID+QSeal vyžaduje připravenou HTTPS website viz. kapitola 5.2.2.3)



» ASP .NET Core Hosting Bundle verze 3.1.3 nebo vyšší dostupný zde: https://dotnet.microsoft.com/download/dotnet-core/3.1.

» .NET Core verze 3.1.3 nebo vyšší dostupný zde: https://dotnet.microsoft.com/download/dotnet-core/3.1.

» .NET Core Desktop verze 3.1.3 nebo vyšší dostupný zde: https://dotnet.microsoft.com/download/dotnet-core/3.1.

» PowerShell 2.0 nebo vyšší.

5.2.1 Instalace ovladačů čipové karty

Na straně IIS serveru není třeba instalovat balíček s ovladači čipové karty. Všechny potřebné ovladače jsou obsaženy v balíčku ProID+QSeal viz. kapitola 5.2.2.

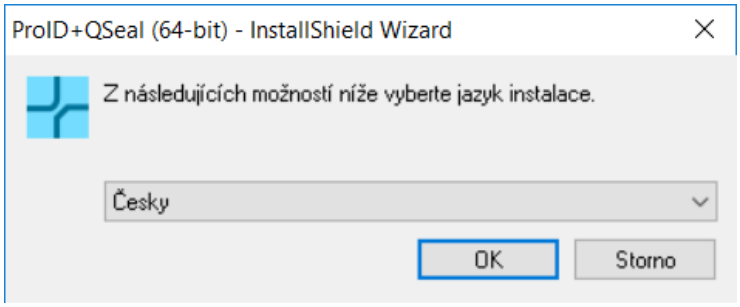
5.2.2 Instalační balíček ProID+QSeal

Instalace aplikace ProID+QSeal se provádí pomocí instalačního programu typu EXE.

Po spuštění řídí instalaci grafický průvodce – kroky instalace jsou popsány v následujících podkapitolách.

5.2.2.1 Spuštění instalace

Po spuštění instalačního průvodce proběhne příprava instalace a po její dokončení se zobrazí výběr jazyka. Aplikace nabízí možnost instalace v českém a anglickém jazyce. V tomto kroku vyberte jazyk instalace a potvrďte tlačítkem OK.



Obrázek 2: Výběr jazyka

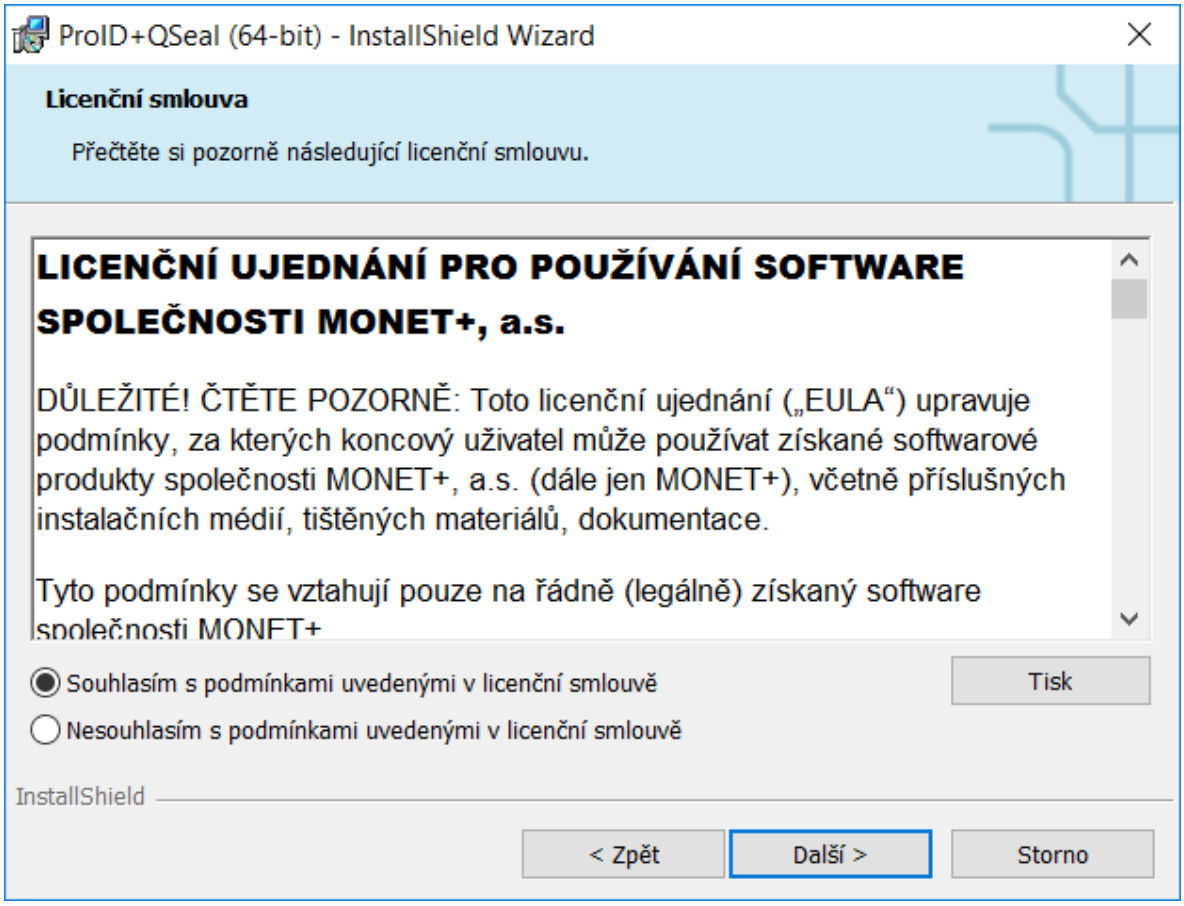
Po volbě jazyka instalačního průvodce se zobrazí uvítací okno instalace:

Obrázek 3: Uvítací okno instalace

Pro pokračování procesu instalace je třeba stisknout tlačítko *Další*.

5.2.2.2 Licenční ujednání

V dalším okně se zobrazí text licenčního ujednání.



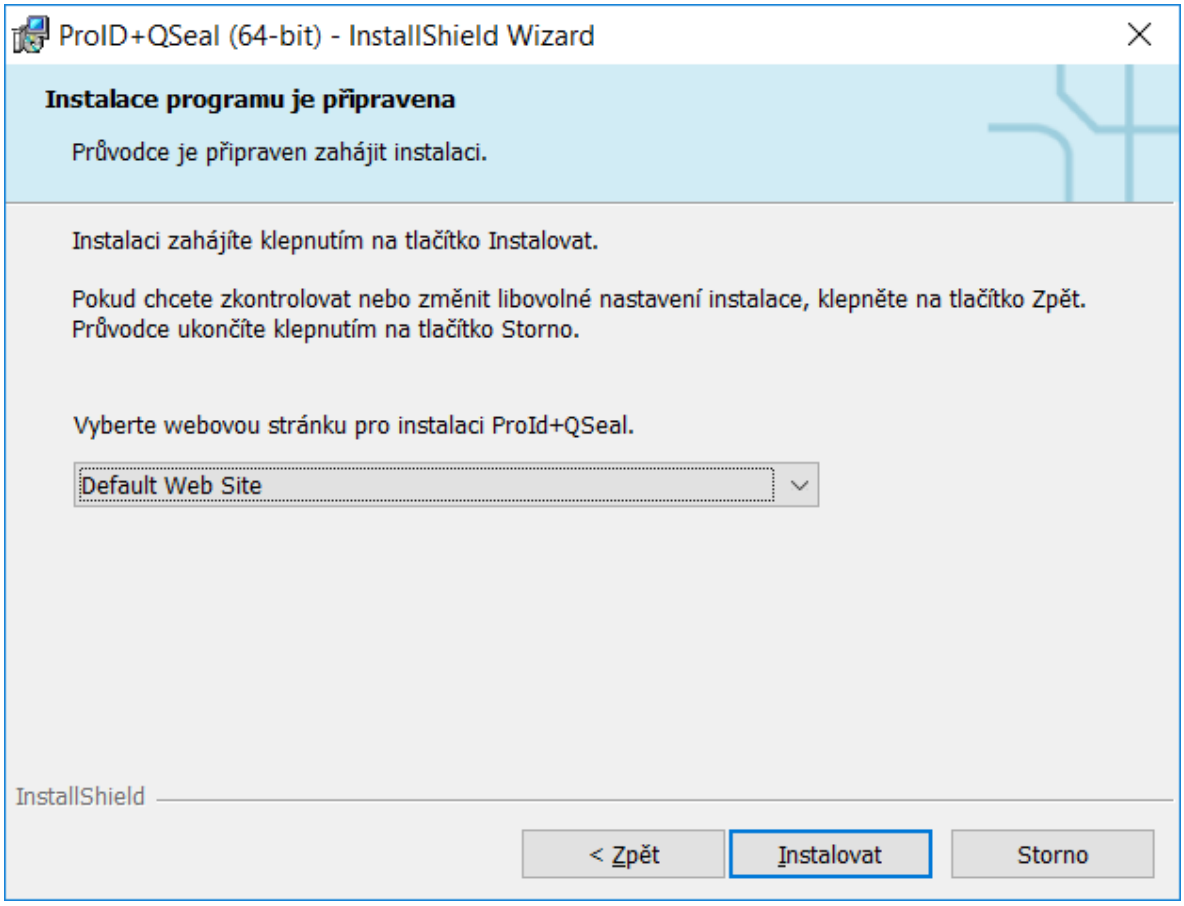
Obrázek 4: Licenční ujednání

Text je třeba pozorně prostudovat a v případě nesouhlasu předčasně ukončit instalaci tlačítkem Storno. Pro pokračování instalace je třeba:

- Udělit souhlas se zněním licenčního ujednání – zaškrtnutím pole Souhlasím s podmínkami uvedenými v licenční smlouvě.
- Stisknout tlačítko Další.

5.2.2.3 Výběr webové stránky pro instalaci ProID+QSeal

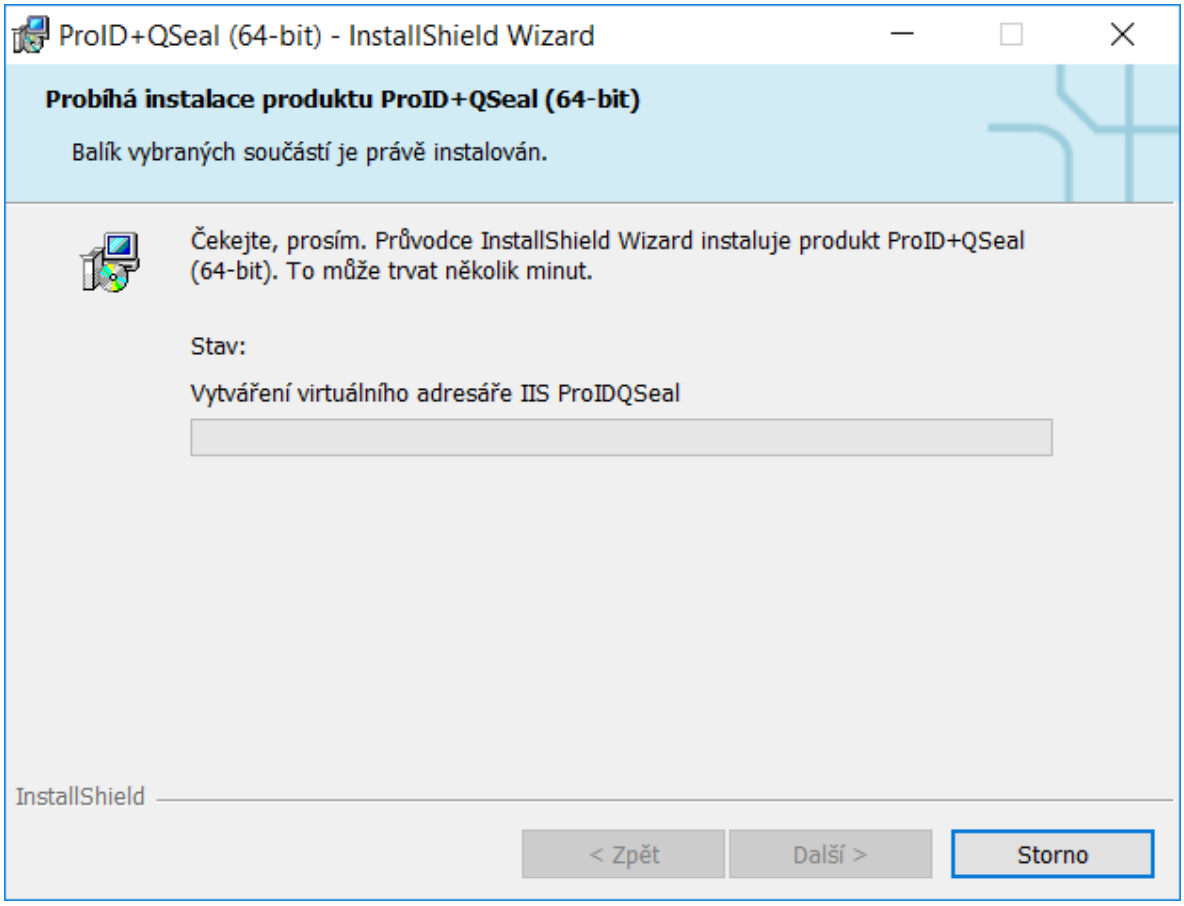
V dalším okně je nutné zvolit webovou stránku, do které bude instalována aplikace ProID+QSeal. Instalační balíček zobrazí všechny dostupné webové stránky provazované v režimu HTTPS. Pomocí comboboxu vyberte stránku, do které bude aplikace přiřazena. Instalaci zahájíte tlačítkem Instalovat.



Obrázek 5: Volba webové stránky pro instalaci

5.2.2.4 Průběh instalace

V průběhu instalace informuje instalační průvodce o prováděných operacích:



Obrázek 6: Průběh instalace

Proces instalace probíhá automaticky a je třeba počkat na dokončení procesu.

Po dokončení instalace se zobrazí okno s informací o výsledku a nabídkou spuštění průvodce s konfigurací:

Obrázek 7: Dokončení instalace

Uvedeným krokem je instalace software ProID+QSeal dokončena. Okno instalačního průvodce lze zavřít tlačítkem Dokončit.

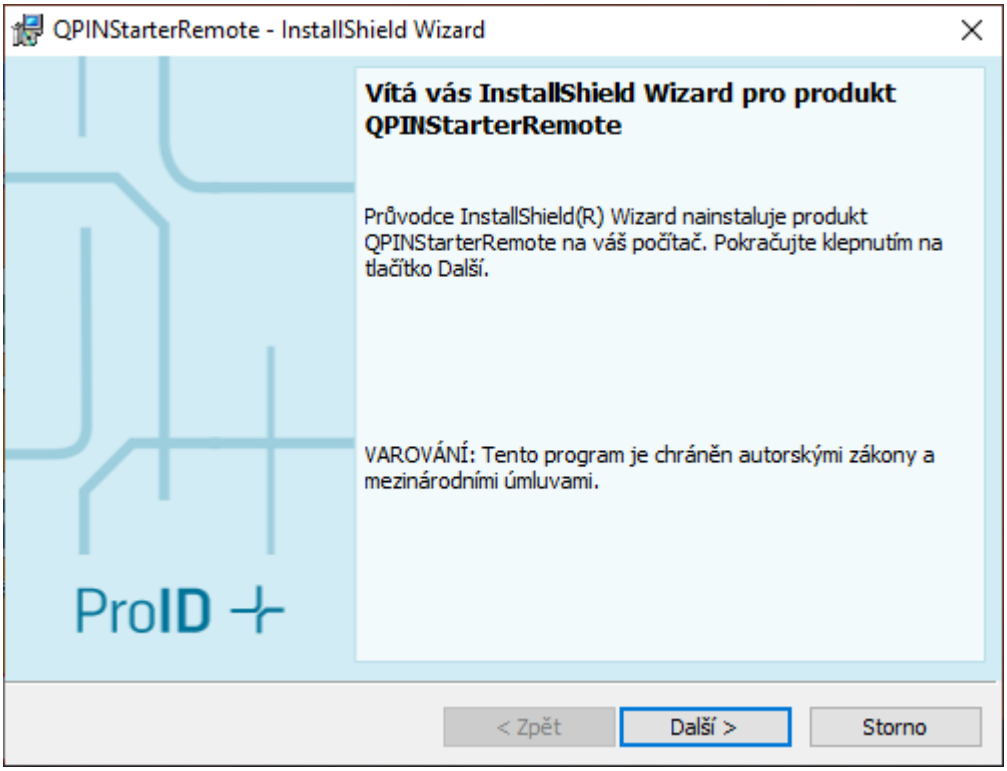
5.2.3 Instalační balíček QPinStarterRemote

Volitelnou součástí dodávaného řešení ProID+Qseal je instalace aplikace QPINStarterRemote. Jedná se o klientskou aplikaci, která uživateli umožní vzdálené zadání hodnoty QPIN bez nutnosti přihlašování na webový server, kde bude provozováno řešení ProID+QSeal. Aplikace má stejné grafické rozhraní jako aplikace QPIN Initializer. Balíček je ve formátu MSI, tak aby byla možná instalace pomocí prostředků Active Directory (GroupPolicy).

Po spuštění řídí instalaci grafický průvodce – kroky instalace jsou popsány v následujících podkapitolách.

5.2.3.1 Spuštění instalace

Po spuštění instalačního průvodce proběhne příprava instalace a po její dokončení se zobrazí uvítací okno průvodce.

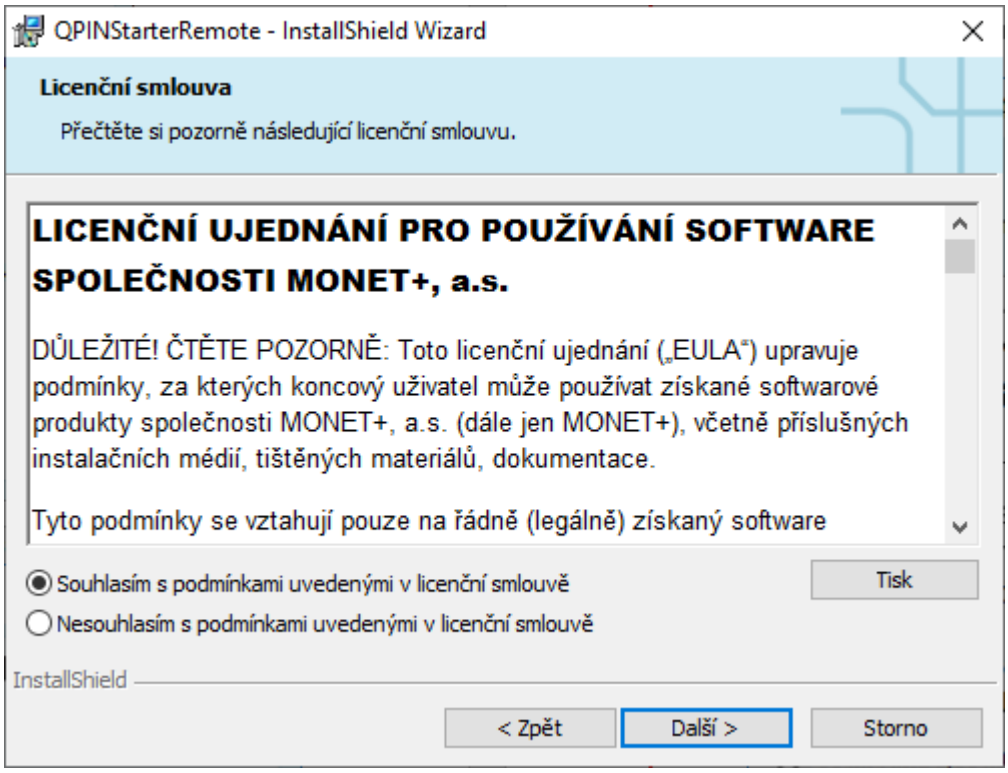


Obrázek 8: Uvítací okno instalace

Pro pokračování procesu instalace je třeba stisknout tlačítko *Další*.

5.2.3.2 Licenční ujednání

V dalším okně se zobrazí text licenčního ujednání.



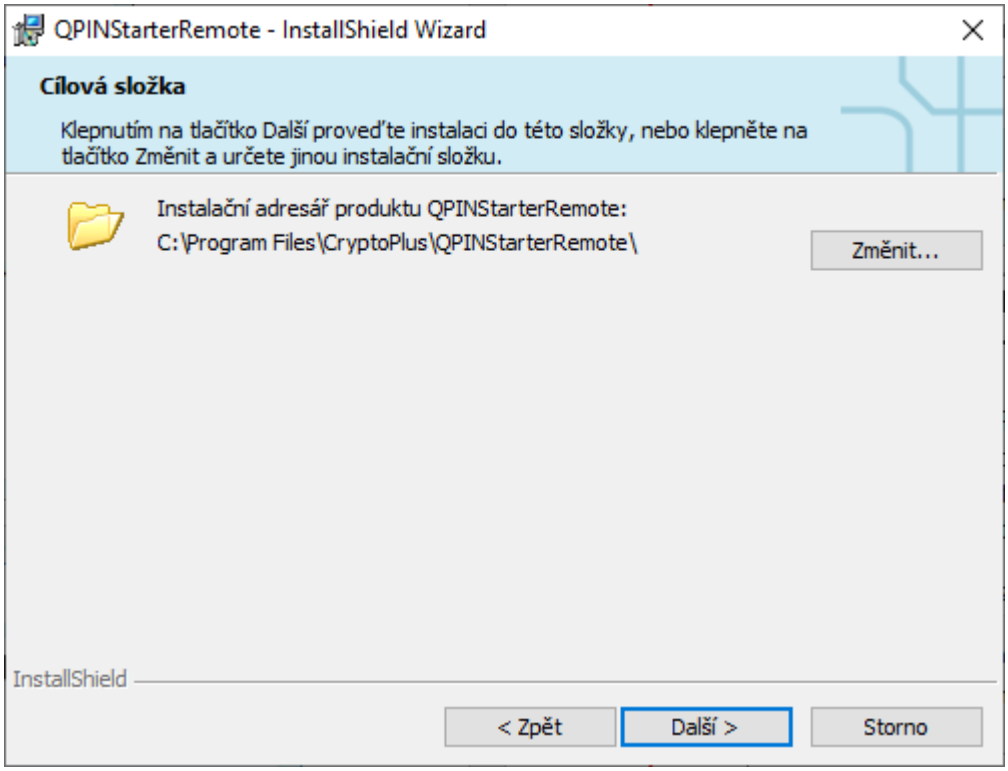
Obrázek 9: Licenční ujednání

Text je třeba pozorně prostudovat a v případě nesouhlasu předčasně ukončit instalaci tlačítkem Storno. Pro pokračování instalace je třeba:

- Udělit souhlas se zněním licenčního ujednání – zaškrtnutím pole Souhlasím s podmínkami uvedenými v licenční smlouvě
- Stisknout tlačítko Další

5.2.3.3 *Výběr adresáře pro instalaci aplikace QPINStarterRemote*

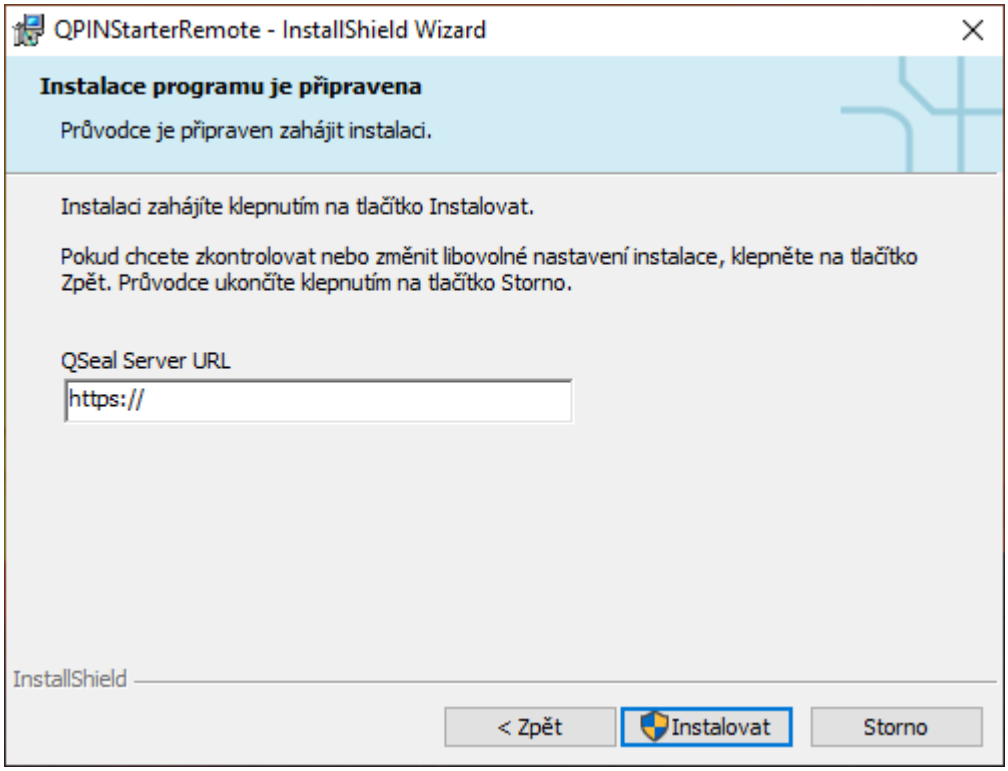
V dalším okně je možné změnit cílový adresář, do kterého bude aplikace QPIStarterRemote instalována. Pomocí tlačítka Změnit je možné vybrat jiné než předvolený adresář.



Obrázek 10: Volba adresáře

5.2.3.4 *Výběr webové stránky ProID+QSeal serveru*

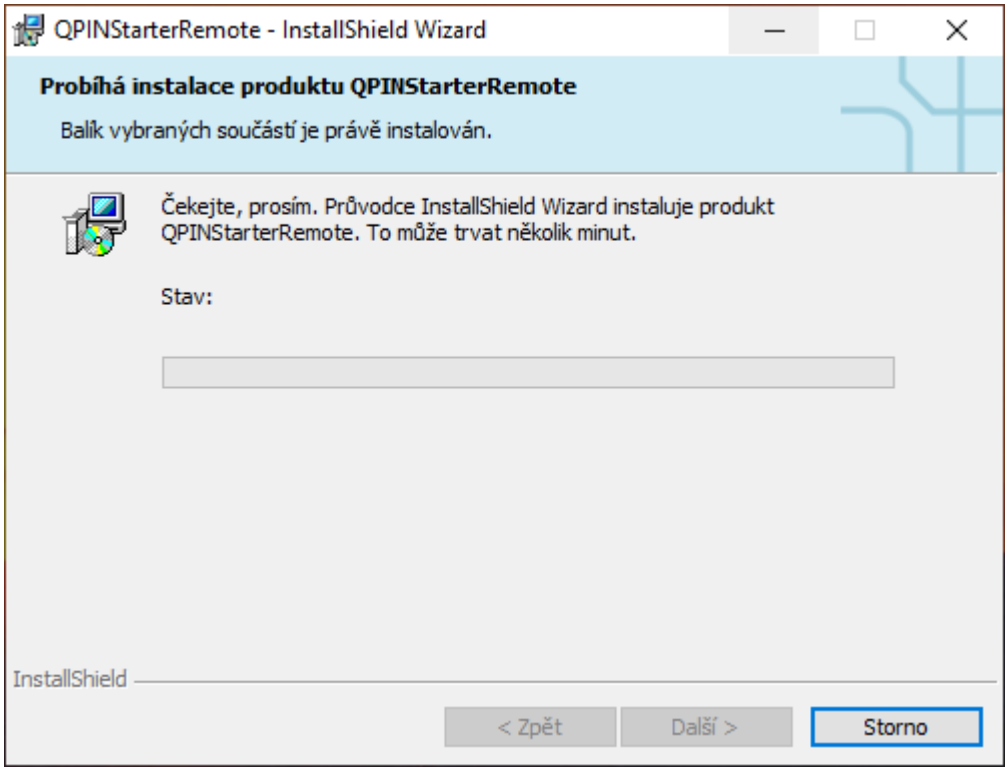
V dalším okně je nutné zvolit webovou stránku, na které běží aplikace ProID+QSeal server. Instalaci zahájíte tlačítkem Instalovat.



Obrázek 11: Volba webové stránky pro instalaci

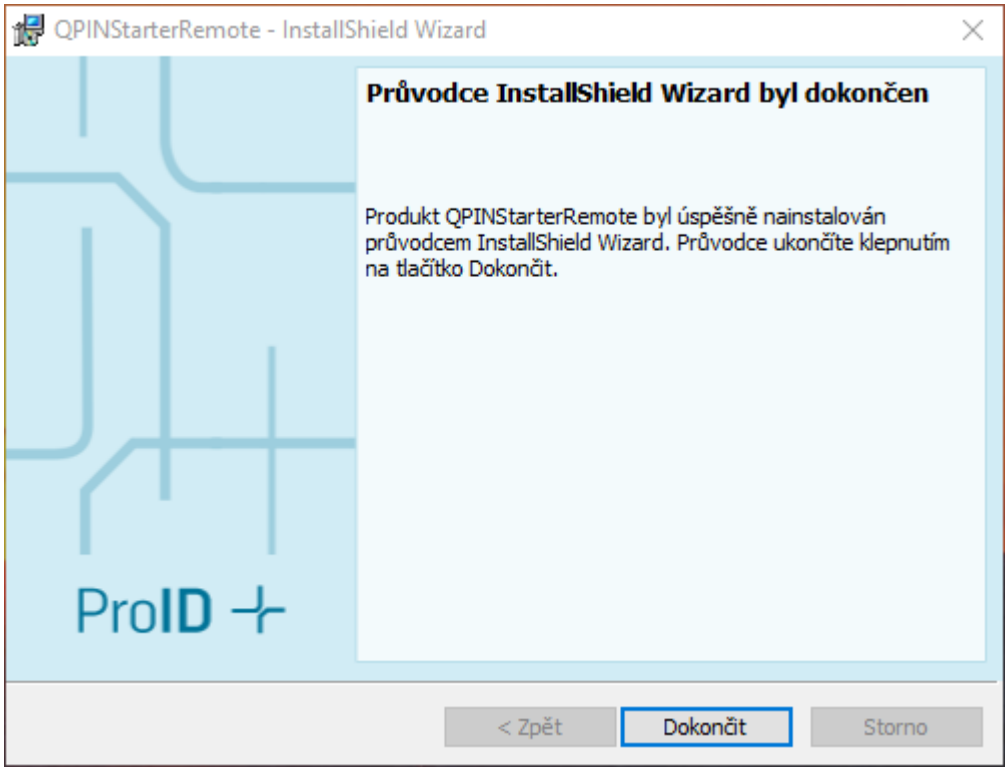
5.2.3.5 Průběh instalace

V průběhu instalace informuje instalační průvodce o prováděných operacích:



Obrázek 12: Průběh instalace

Proces instalace probíhá automaticky a je třeba počkat na dokončení procesu.



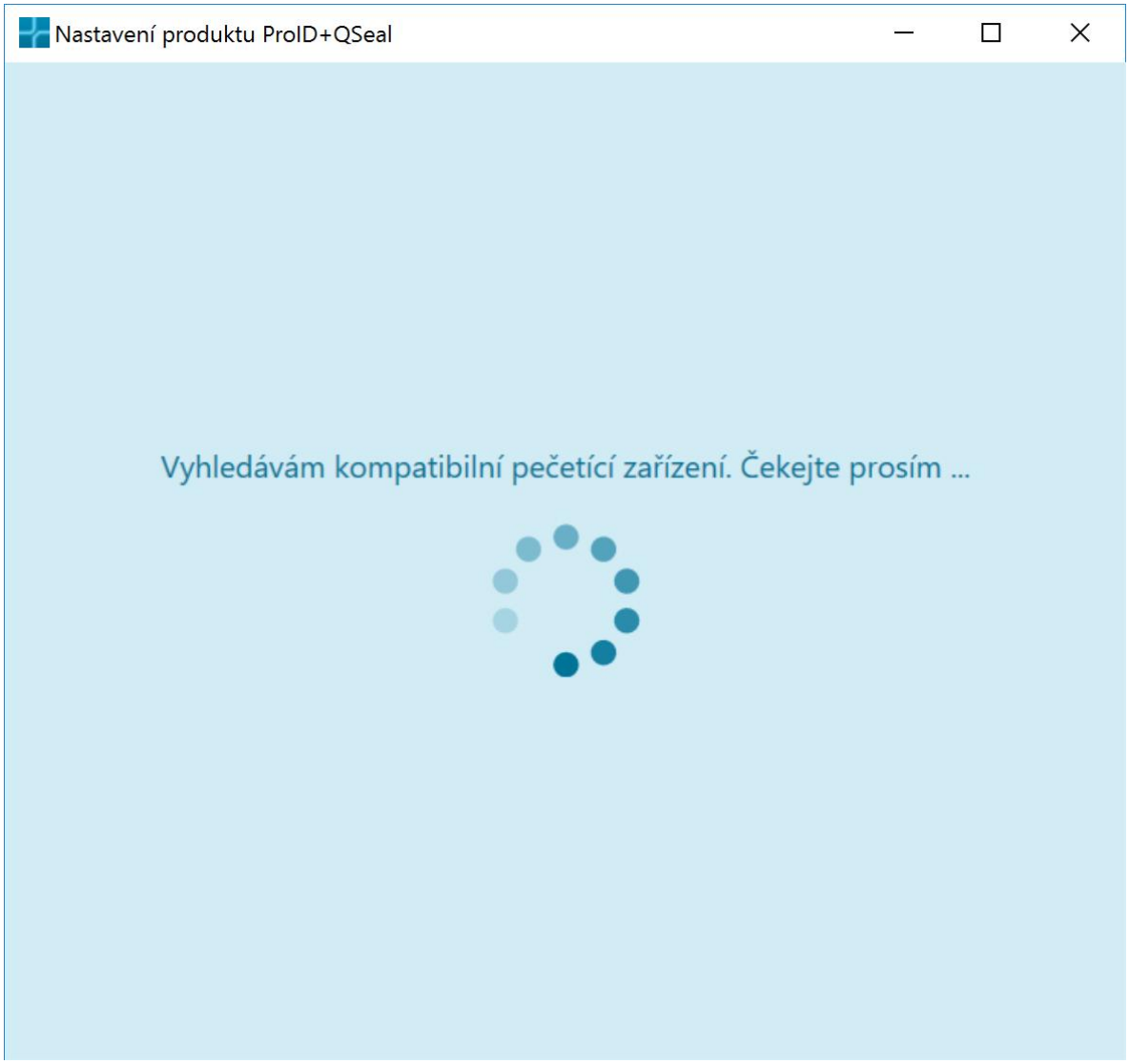
Obrázek 13: Dokončení instalace

Uvedeným krokem je instalace software QPINStarterRemote dokončena. Okno instalačního průvodce lze zavřít tlačítkem Dokončit.

5.3 KONFIGURACE SLUŽBY PROID+QSEAL

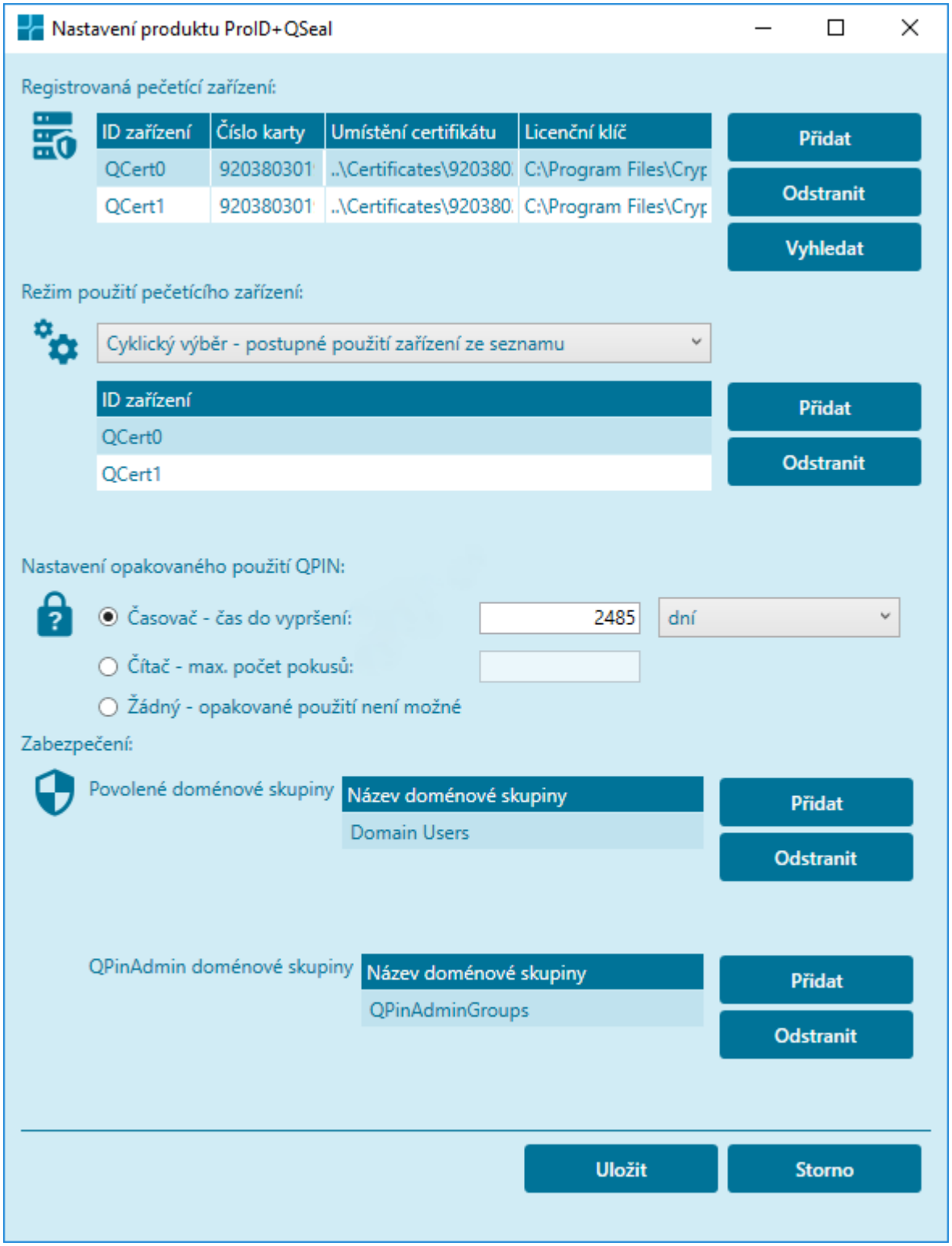
Po dokončení instalace je služba *zastavená* a je nutné provést její konfiguraci. Konfigurace se provádí formou integrovaného průvodce. Průvodce je možné spustit automaticky po dokončení instalace pomocí zatržení této volby v instalátoru, nebo kdykoli později z instalačního adresáře služby ProID+QSeal, typicky z cesty: *C:\ProID+QSeal\Configurator\Configurator.exe*

Prvním krokem průvodce je automatické vyhledání kompatibilních pečetících zařízení.



Obrázek 14: Vyhledání pečetících zařízení

Po dokončení vyhledávání je zobrazeno okno průvodce.

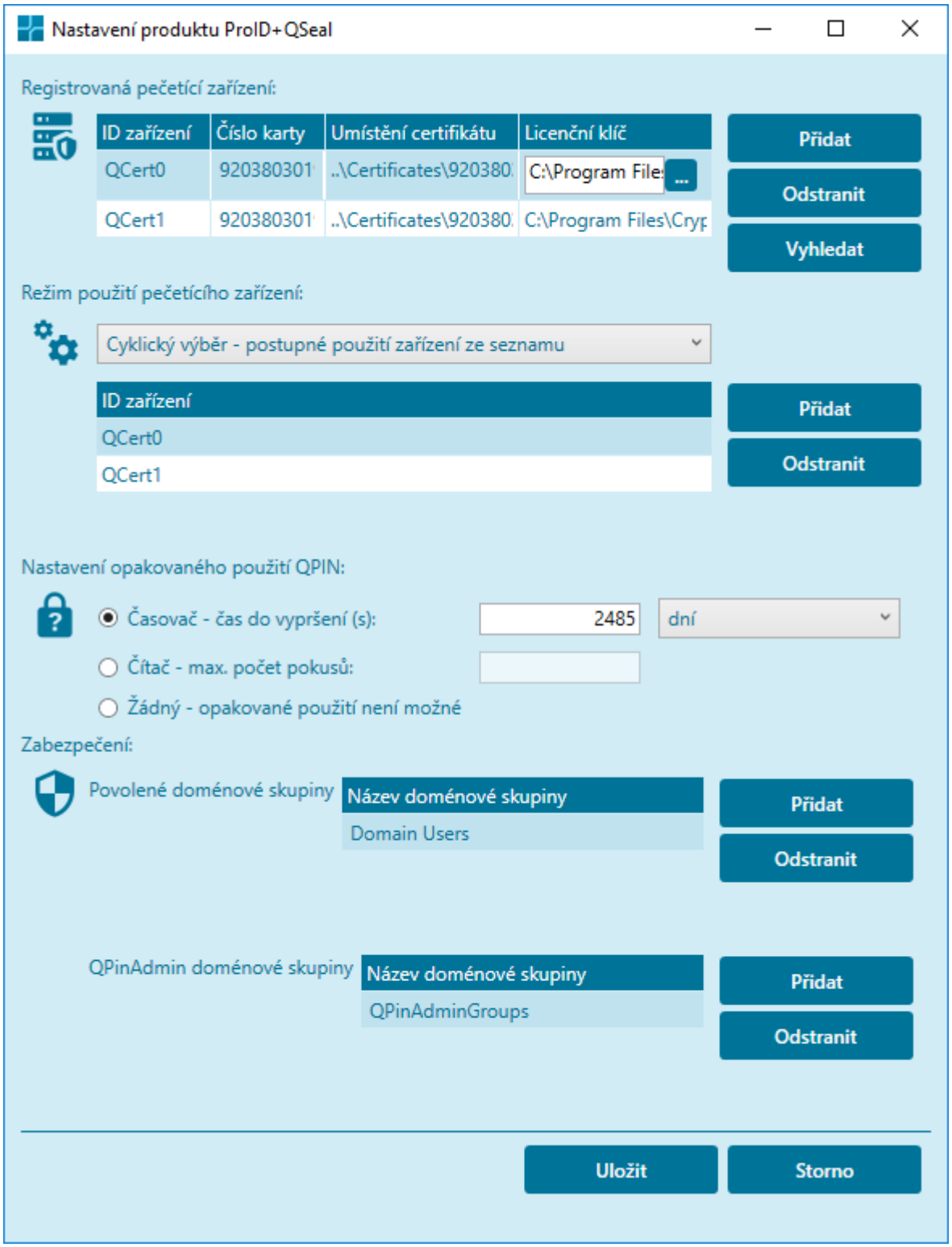


Obrázek 15: Nastavení ProID+QSeal

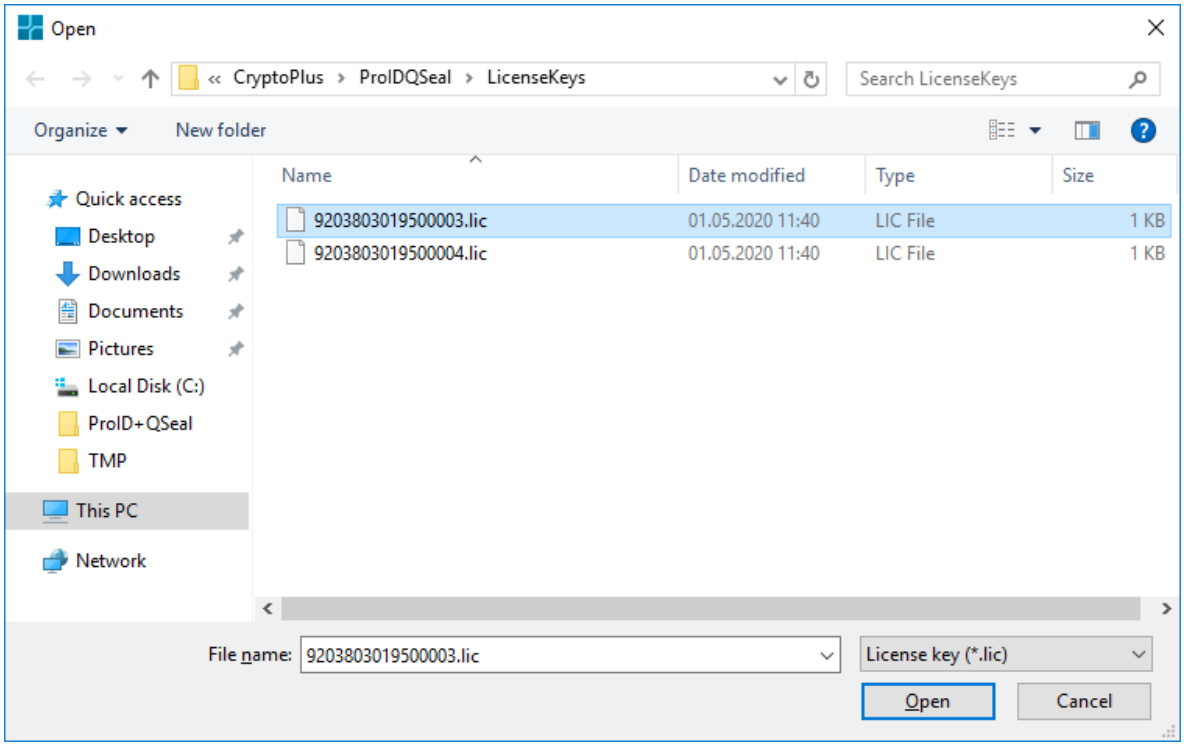
V sekci *Registrovaná pečetící zařízení* je zobrazen seznam aktuálně dostupných pečetících zařízení připojených k serveru. Tento seznam se dá spravovat pomocí tlačítek *Přidat Odstranit* a *Vyhledat*. Pro další pokračování konfigurace je nutné v tomto seznamu mít dostupné alespoň jedno pečetící zařízení.

Dalším krokem je doplnění licence k dodanému pečetícímu zařízení. Licenční kód je svázán s CLN pečetícího zařízení. CLN je uvedeno na dodaném PIN formuláři. Pro správnou funkčnost řešení ProID+Qseal je podmínkou

zadání licenčního čísla minimálně pro jedno pečetící zařízení. Postup pro získání licenčního čísla je popsán na PIN formuláři, který je součástí dodaného pečetícího zařízení.



Obrázek 16: Doplnění licence



Obrázek 17: Výběr licenčního klíče

V sekci Režim použití pečetícího zařízení se dá zvolit možnost, jakým způsobem se bude přistupovat k jednotlivým připojeným pečetícím zařízením.

- Statický – permanentní použití vybraného zařízení.
  - Pro pečetění bude použito pouze jedno konkrétní zařízení, bez ohledu na připojení dalších zařízení.
  - S možností výběru použitého zařízení.
- Cyklický výběr – postupné použití zařízení ze seznamu.
  - Zařízení budou používána pro pečetění postupně, tak jak je definováno jejich pořadí v seznamu.
  - Pořadí zařízení v seznamu je možné definovat pomocí tlačítek Přidat a Odstranit.
  - V rámci seznamu je možné použít jedno zařízení vícekrát, nebo naopak některé zařízení nepoužívat vůbec.
- Mapa doména – zařízení mapování domény na konkrétní zařízení.
  - Tuto možnost je možné zvolit v případě, kdy je třeba podle domény klienta volajícího službu pečetění rozhodnout, které pečetící zařízení využít.
  - Správa seznamu se provádí pomocí tlačítek Přidat a Odstranit.

V sekci Nastavení opakovaného použití QPIN se dá zvolit možnost uložení hodnoty bezpečnostního kódu QPIN a díky tomu také možnost nemuset zadávat tento bezpečnostní kód při každém pokusu o pečetění. Volba obsahuje možnosti:

- Časovač – čas do vypršení

- V rámci této možnosti je umožněno nastavit časový limit, počet sekund, minut, hodin, dní, jak dlouho bude hodnota QPIN uložena. Po uplynutí této doby bude třeba hodnotu QPIN znova zadat.
- Je možné zadat hodnotu v rozmezí od 0 do 24855 dnů.
- Pokud uživatel zadá hodnotu vyšší jak 10 dnů je následně zobrazen potvrzovací dialog. V něm je zobrazena aktuálně uživatelem zadaná hodnota a informace o doporučované maximální době (10 dní). Uživatel je vyzván, zda chce pokračovat. Potvrzením Ano dojde k zobrazení dialogu na restart služby. Následným potvrzením Ano je služba restartována a jsou použity nové hodnoty.

- Čítač – max. počet pokusů.
  - V rámci této možnosti je umožněno nastavit maximální počet provedených pečetí, do doby, než bude znovu vyžadováno zadání bezpečnostního kódu QPIN.
  - Je možné zadat hodnotu v rozmezí od 0 do 1000 opakovaných použití.
- Žádný – opakované použití není možné.
  - V rámci této možnosti není hodnota bezpečnostního kódu QPIN uložena a při každém pokusu o provedení pečetění bude třeba ji znovu zadat.

V sekci Zabezpečení je umožněno pomocí tlačítek přidat a odebrat přidat seznam doménových skupin, které mají oprávnění k provádění elektronického pečetění. Pokud v této sekci není uvedena žádná doménová skupina, všechny žádosti od všech uživatelů o elektronické pečeti budou serverem vyřízeny. Volba obsahuje možnosti:

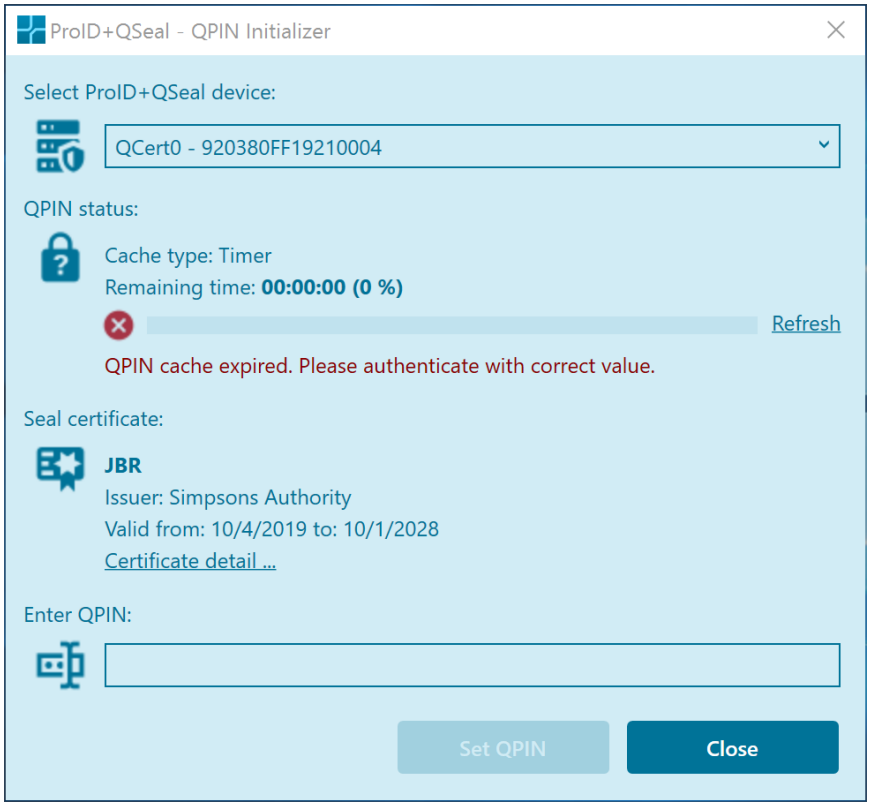
- Povolené doménové skupiny.
  - Seznam doménových skupin, které mají oprávnění k provádění elektronického pečetění.
- QPinAdmin doménové skupiny.
  - Seznam doménových skupin, které mají oprávnění k spuštění aplikace QPIN Starter Remote.

5.3.1 Dodatečná změna konfigurace

Všechny konfigurace popsané v kapitole 5.3 se dají změnit i kdykoli po dokončení instalace pomocí konfigurační aplikace *Nastavení produktu ProID+QSeal* dostupné v cestě: *C:\Program Files\CryptoPlus\ProIDQSeal\Configurator\Configurator.exe* vzhled a chování aplikace je stejné jako u konfigurátoru spouštěného na konci instalátoru popsaného výše.

5.4 ZADÁNÍ BEZPEČNOSTNÍHO KÓDU QPIN

Před začátkem pečetění, je třeba pomocí aplikace QPIN Initializer dostupné v cestě: *C:\Program Files\CryptoPlus\ProIDQSeal\QPINStarter\QPINStarter.exe* zadat hodnotu bezpečnostního kódu QPIN.



Obrázek 18: QPIN Initializer

5.4.1 Postup zadání hodnoty QPIN

- Na webovém serveru spustit aplikaci *C:\Program Files\CryptoPlus\ProIDQSeal\QPINStarter\QPINStarter.exe*.
- Variantně pokud je na klientském PC nainstalována aplikace QPinStarterRemote spustit aplikaci *C:\Program Files\CryptoPlus\QPINStarterRemote\QPINStarter.exe*.
- V sekci *Select ProID+QSeal device*: vybrat správnou čipovou kartu ProID+QSeal, ke které se bude zadávat QPIN.
- V sekci *QPIN Status*: zkontrolovat aktuální nastavení *Režimu použití bezpečnostního zařízení*. Tato hodnota je vyčtena z konfigurace. Nastavení konfiguračních parametrů je popsáno v kapitolách: 5.3 a 5.3.1.
- V sekci *Seal Certificate* zkontrolovat, zda je vybrán správný certifikát pro pečetění. Certifikát je vyčten z konfigurace. Nastavení konfiguračních parametrů je popsáno v kapitolách: 5.3 a 5.3.1.
- V sekci Enter QPIN potom zadat správnou hodnotu bezpečnostního kódu QPIN. Na zadání správné hodnoty QPIN jsou dostupné 3 pokusy. Vlastnosti bezpečnostních kódů čipové karty ProIDQ+Seal jsou uvedeny v kapitole 4.1.2.
- Zadání potvrdit pomocí tlačítka *Set QPIN*.

Takto inicializovanou kartu je možné začít používat pro pečetění. Protože délka cache bezpečnostního kódu QPIN není z bezpečnostních důvodů neomezená. Je třeba bezpečnostní kód QPIN zadávat pravidelně, tak jak je popsáno v kapitole: 7.2.

5.5 OVĚŘENÍ INSTALACE

Po dokončení instalace je možné volitelně také ověřit její výsledek a otestovat funkci pečetění.

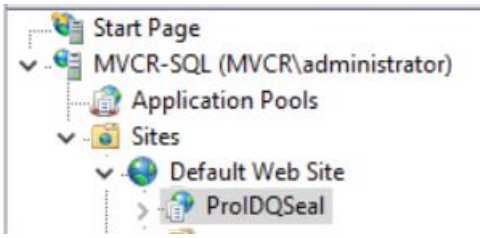
Ověření instalace probíhá v několika krocích, jak je popsáno v kapitolách 5.5.1 a 5.5.2.

5.5.1 IIS server, Webová služba

Prvním krokem je ověření správného provedení instalace na straně IIS serveru.

Pomocí konzole IIS Manager se ověří, že:

» Pod vybranou Web Site je nainstalována webová služba:

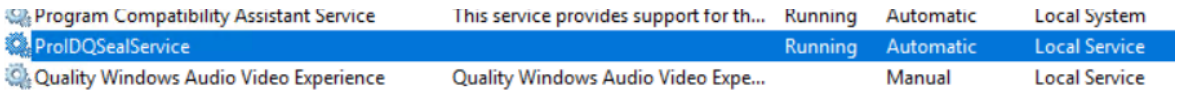


Obrázek 19: Webová služba

» Je instalovaný a běžící aplikační pool.

Obrázek 20: Aplikační pool

» Přes konzoli *services.msc* se zkontroluje běžící Windows služba:



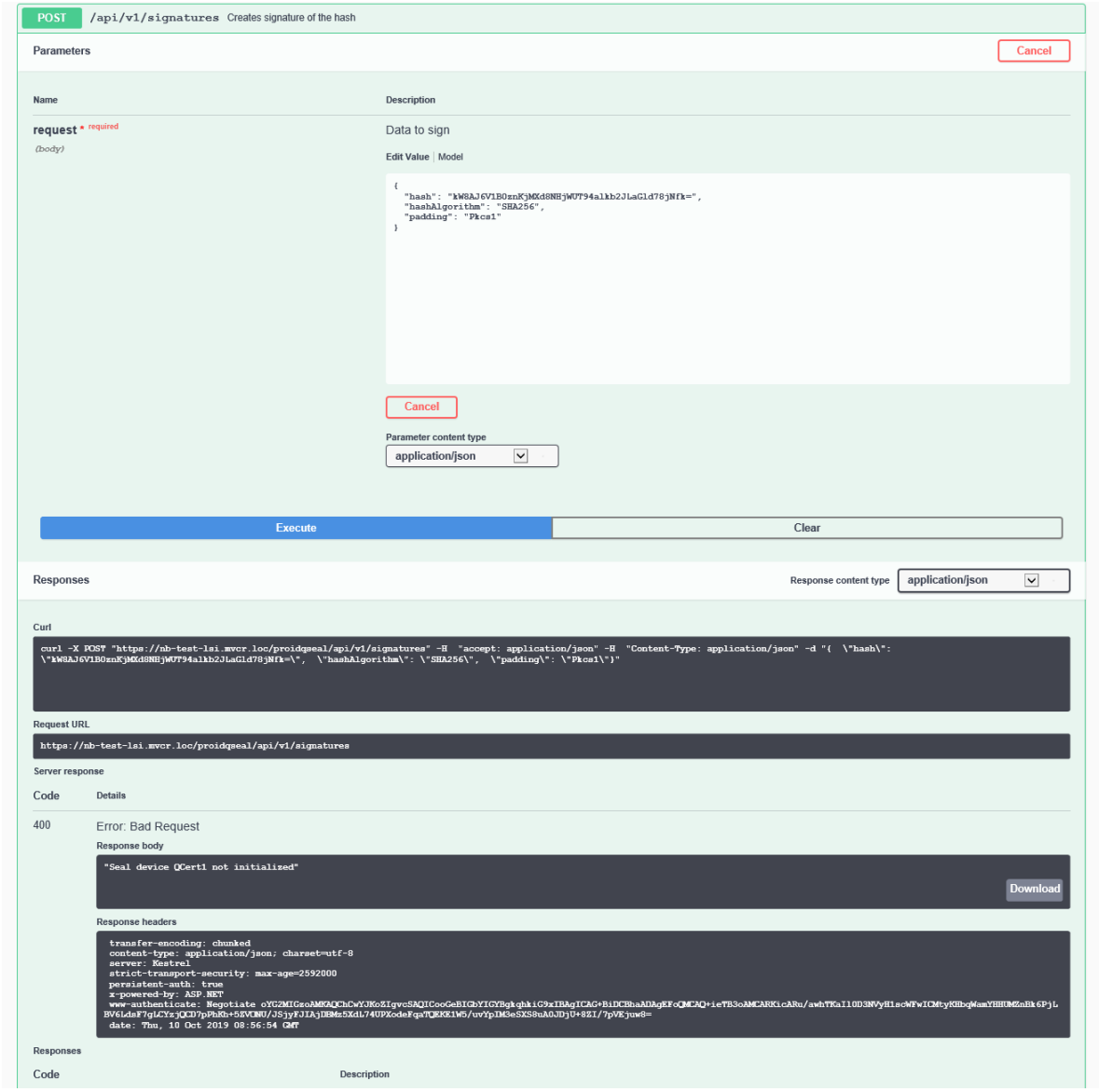
Obrázek 21: Windows služba

5.5.2 Ověření z klientského počítače

Po dokončení ověření na straně IIS serveru je možné vyzkoušet provolat službu pečetění z klientského počítače pomocí testovací aplikace.

» Na klientském počítači ve webovém prohlížeči otevřít adresu pečetící webové služby */swagger/index.html*, např: https://qseal.domain.loc/proidqseal/swagger/index.html.

- Na této stránce je dostupná webová aplikace Swagger, pomocí které lze provolat webovou službu a požádat o testovací pečeť.
- V sekci *Signatures* stisknout tlačítko *Post*.
- V sekci *Post* stisknout tlačítko *Execute*.
- Po provedení dotazu a získání odpovědi by měla webová služba vrátit kód *200, Success*.
- Jsou zde také uvedeny případné hodnoty chových kódů, na základě, kterých lze chyby ve službě opravit.



Obrázek 22: Swagger, ukázka chyby, neinicializovaná hodnota QPIN

Po úspěšném provedení těchto testů je služba pečetění připravena k provozu.

6 VZDÁLENÁ INSTALACE SPOLEČNOSTÍ MONET+

V případě potřeby společnost Monet+ dokáže provést na žádost zákazníka vzdálenou instalaci a poskytnout asistenci při zprovoznění pečetění. Tento postup je zpoplatněn a skládá se z následujících kroků.

- Asistence s vydáním pečetících certifikátů na čipovou kartu ProID+QSeal z klientské stanice.
- Zřízení vzdáleného připojení do prostředí zákazníka pro pracovníka Monet+.
  - Přístup na IIS server, kde budou instalovány webové služby.
  - Přístup na klientský počítač, odkud bude ověřena funkčnost pečetění.
- Vzdálená instalace všech komponent IIS serveru.
- Zprovoznění řešení pečetění, asistence se zadáním bezpečnostních kódů.
- Vzdálené ověření funkce pečetění z klientské stanice v prostředí zákazníka.
- Předání a prezentace kompletního řešení.

Společnost Monet+ může provést kompletní výše popsaný postup, nebo pouze jeho vybranou část.

V případě zájmu o vzdálenou instalaci a asistenci při zprovoznění řešení pečetění nás prosím kontaktujte na emailové adrese: info@proid.cz

7 PROVOZ ŘEŠENÍ PROID+QSEAL

Aplikace ProID+QSeal kombinuje několik komponent a služeb. Jedná se o

- IIS, hostující webové služby (WS ProID+QSeal).
  - Webová aplikace (WS ProID+QSeal) běží beze změn v provozu na protokolu https. Pravidelně je potřeba obnovovat certifikát webového serveru.
- Služba pečetění ProID+QSeal Service (Windows Service) pro zajištění perzistence QPIN cache v knihovně PKCS#11.
  - Služba pečetění pomocí ProIDQSeal vyžaduje pravidelné zadávání bezpečnostního kódu QPIN. Nastavení úrovně využití QPIN cache je popsáno v kapitole 5.3.
- knihovna PKCS#11 ProID+QSeal.
  - Nejsou potřeba pravidelné zásahy.
- aplikace pro zavedení QPIN (QPIN Initializer) do cache v knihovně PKCS#11, prostřednictvím služby ProID+QSeal Service.
  - Nejsou potřeba pravidelné zásahy.

7.1 API SLUŽBY PROID+QSEAL

Služba vystavuje API vytvořené v architektuře REST. Detaily rozhraní je možné zobrazit pomocí integrované aplikace Swagger viz. kapitola 5.5.2.

Příklad volání REST API:

- Request url pro pečetění:

```
"https://qseal.domain.loc/proidqseal/api/v1/signatures"
```

- Request body:

```
{  "Hash": "kW8AJ6V1B0znKjMXd8NHjWUT94alkb2JLaGld78jNfk=",
  "HashAlgorithm": "SHA256"}
```

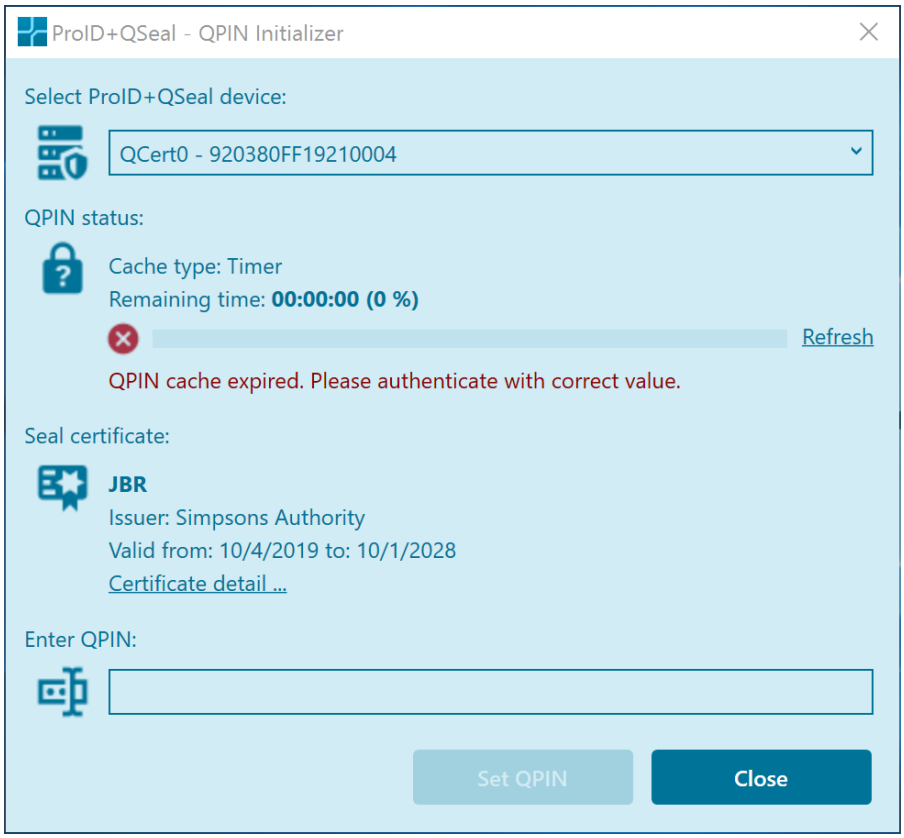
- Responses:

```
curl -X POST "https://qseal.domain.loc/proidqseal/api/v1/signatures" -H "accept: application/json" -H "Content-Type: application/json" -d "{\"Hash\":\"kW8AJ6V1B0znKjMXd8NHjWUT94alkb2JLaGld78jNfk=\",\"HashAlgorithm\":\"SHA256\"}"
```

7.2 OPAKOVANÉ ZADÁVÁNÍ BEZPEČNOSTNÍHO KÓDU QPIN

Protože z bezpečnostních důvodů není možné hodnotu bezpečnostního kódu QPIN držet v QPIN cache neomezenou dobu, je dle konfiguračních parametrů tuto hodnotu třeba pravidelně zadávat. Zadávání této hodnoty se provádí přímo na IIS serveru, pomocí aplikace *C:\Program*

Files\CryptoPlus\ProIDQSeal\QPINStarter\QPINStarter.exe Postup zadání je stejný jako při prvním zadání popsaném v kapitole 5.4.1



Obrázek 23:QPIN Initializer

Hodnotu QPIN lze zadat pomocí aplikace QPIN Initializer kdykoli, jak v období, kdy ještě platí původní zadání (hodnota QPIN je uložena v PIN cache) tak později, kdy původní zadání vyprší a hodnota již není uvedena v QPIN cache.

Protože potřeba opakovaného zadávání hodnoty QPIN je manuální činnost, je možné, že občas bude docházet k situacím, kdy hodnota QPIN nebude z nějakého důvodu zadána včas. Díky tomu dojde k pozastavení funkce pečetění. Pečetící server bude vracet volajícím aplikacím chybovou hlášku, že hodnota QPIN není zadána.

Aby se tuto situaci dalo co nejlépe eliminovat, je možné aktivovat zasílání varovných emailových zpráv na email, právě v případě, kdy se na serveru budou vyskytovat chyby související s nezadáním hodnoty QPIN. Na základě těchto zpráv potom může obsluha zareagovat a QPIN znova zadat.

7.2.1 Emailová notifikace chyby QPIN nezadán

Emailovou notifikaci, která zajistí upozornění v případech, kdy QPIN není zadán, je možné povolit pomocí logovacího nástroje NLog, který je v rámci aplikace standardně využíván.

» Na IIS serveru v rámci souboru s konfigurací aplikace NLog pro webovou službu: *C:\Program Files\CryptoPlus\ProIDQSeal\WebService\NLog.config*.

V sekci *Targets* odkomentovat element *target name="Mail" a v sekci rules odkomentovat element logger name="Monet.ProIdSeal.BackendServices.Client.SignatureServiceClient"*.

» V rámci elementu „Mail" potom editovat jednotlivé položky, které slouží ke konfiguraci zasílaných emailových zpráv.

» Např:

```
<?xml version="1.0" encoding="utf-8" ?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.nlog-project.org/schemas/NLog.xsd NLog.xsd"
      autoReload="true"
      throwExceptions="false"
      internalLogLevel="Off" internalLogFile="C:/Logs/ProID+QSeal/webservice-
nlog-internal.log">
  <targets>
    <target name="file" xsi:type="BufferingWrapper" flushTimeout="3000">
      <target xsi:type="File" name="fileDebugInner"
fileName="${specialfolder:folder=CommonApplicationData}/ProID+QSeal/webservice.l
og"
              layout="${longdate} ${activityId} [${threadid}] ${pad:padding=-
5:inner=${level:uppercase=true}} ${logger} - ${message}
${exception:format=tostring}"
              archiveEvery="Day"

archiveFileName="${specialfolder:folder=CommonApplicationData}/ProID+QSeal/webse
rvice_{#}.log"
              archiveNumbering="Date"
              archiveDateFormat="yyyy-MM-dd"
              maxArchiveFiles="10"
              encoding="utf-8" />
    </target>
<!--Vzor konfigurace odeslani emailu. (https://github.com/nlog/NLog/wiki/Mail-
target) -->
    <target name="Mail" xsi:type="Mail"
            smtpServer="smtp.domena.loc"
            smtpPort="25"
            enableSsl="false"
            smtpAuthentication="Basic"
            smtpUserName="Username"
            smtpPassword="Password"
                  encoding="UTF-8"
            from="podporaQSeal@organizace.loc"
            to="administrator@organizace.loc;admin@organizace.loc"
            subject="ProID+QSeal QPIN Error"
            subject="ProID+QSeal QPIN Error"
            body="ProID+QSeal QPIN Error: QPIN není inicializován
${newline}${newline}Chybové hlášení:${newline}${message:truncate=500}"
```

```
    />
  </targets>
  <rules>
    <logger name="*" minlevel="Info" writeTo="file" />
<!--Vzor konfigurace odeslani emailu.-->
   <logger name="Monet.ProIdSeal.BackendServices.Client.SignatureServiceClient"
minlevel="Error" writeTo="Mail" defaultAction="Ignore"/>
</rules>
</nlog>
```

Na základě této konfigurace budou potom na vybrané emailové adresy zasílány v případě chyby definované emailové notifikace.

Pozn. Pro odesílání mailových zpráv je podporována pouze Basic autentizace (jménem a heslem).