

Uživatelská dokumentace

iQ Signer



Zpracovatel: InQool, a.s.
Svatopetrská 35/7, 617 00 Brno
IČ: 29222389

1 OBSAH

1	OBSAH	2
2	ÚČEL	3
3	POPIS APLIKACE	4
4	INSTALAČNÍ BALÍČKY	5
5	INSTALACE	6
5.1	MACOS	7
6	SPUŠTĚNÍ A BĚH APLIKACE	10
6.1	PRVNÍ SPUŠTĚNÍ	10
6.2	AUTOMATICKÉ SPUŠTĚNÍ	10
6.3	BĚH APLIKACE	10
7	NASTAVENÍ	11
7.1	FILTRACE CERTIFIKÁTŮ	11
7.2	ČASOVÁ RAZÍTKA	11
7.3	PKCS#11 ZAŘÍZENÍ	11
7.4	PODPISOVÉ POLE	12
7.5	VÝBĚR FORMÁTU	12
7.6	PROXY	12
7.7	EXPERTNÍ FUNKCE	13
7.7.1	<i>Podpisová služba</i>	13
7.7.2	<i>Předvolba</i>	13
7.7.3	<i>Hash funkce</i>	13
8	POUŽITÍ	14
8.1	NÁHLED A STAŽENÍ	16
8.2	RESET APLIKACE	16

2 ÚČEL

Účelem tohoto dokumentu je seznámit koncové uživatele s instalačním procesem a užíváním aplikace iQ Signer.

3 POPIS APLIKACE

iQ Signer je aplikace pro koncové uživatele, která umožňuje podepisovat dokumenty kvalifikovaným elektronickým podpisem dle směrnice eIDAS.

Aplikace má dvojí využití:

1. Dá se použít samostatně pro podepisování dokumentů.
2. Poskytuje komunikační rozhraní pro jiné aplikace.

Pro komunikaci s kvalifikovaným zařízením (QSCD) využívá dva způsoby:

1. Komunikace s využitím PKCS#11 ovládače od dodavatele QSCD zařízení.
2. Komunikace s využitím Microsoft CryptoAPI.

Aplikace podporuje tyto formáty podpisu dle eIDAS:

1. PAdES
2. XAdES
 - Oddělený (Detached)
 - Obalující (Enveloping)
 - Obalený (Enveloped)
3. CAdES
 - Oddělený (Detached)
 - Obalující (Enveloping)
4. ASiC
 - ASiC-S s XAdES
 - ASiC-S s CAdES
 - ASiC-E s XAdES
 - ASiC-E s CAdES

4 INSTALAČNÍ BALÍČKY

Aplikace iQ Signer je dostupná pro 64bitové operační systémy Windows a MacOS. Je distribuovaná formou instalačních balíčků.

SOUBOR	POPIS
iQSigner-x.y.z.pkg	Instalační balíček pro systém MacOS

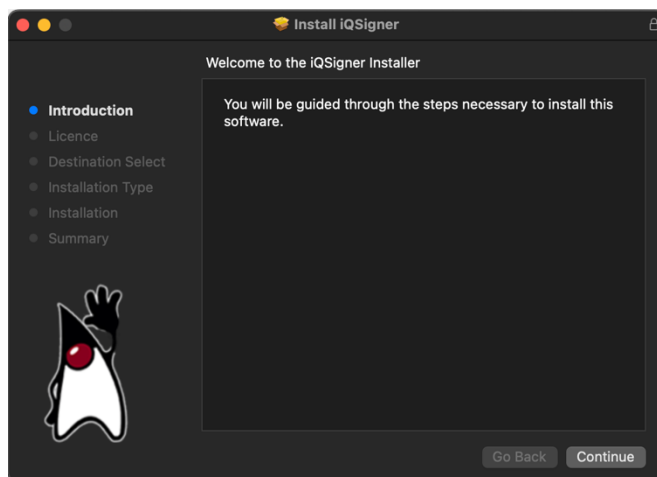
Kde x.y.z je číslo aktuální verze aplikace.

5 INSTALACE

Instalace je zahájena spuštěním instalačního balíčku. Instalátor následně provede uživatele celým procesem instalace.

5.1 MACOS

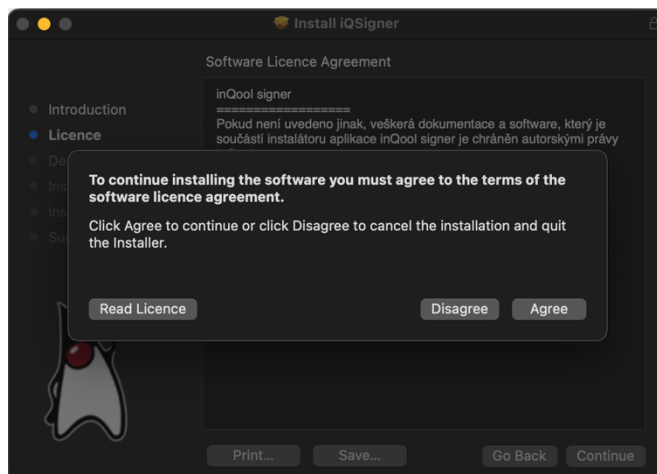
1. Po spuštění instalátoru se zobrazí uvítací zpráva. Uživatel pokračuje kliknutím na tlačítko **Continue**.



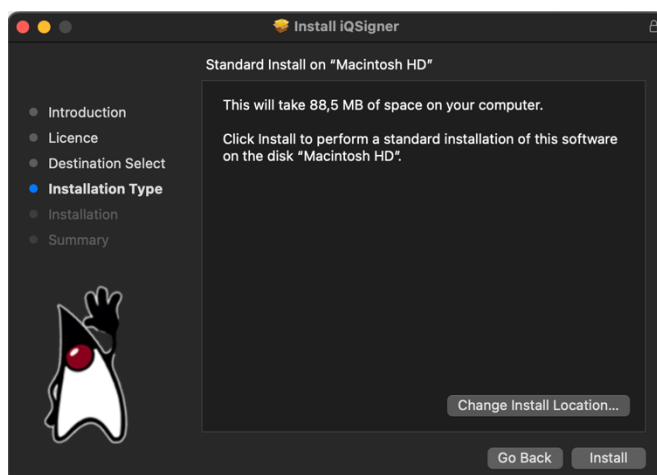
2. Následně je uživatel seznámen s licenčním ujednáním ohledně užívání aplikace iQ Signer.



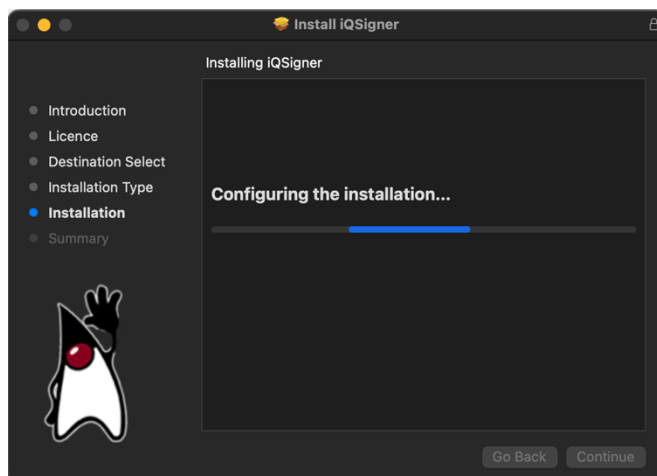
3. Pro pokračování musí uživatel s licencí souhlasit a kliknout na tlačítko **Agree**.



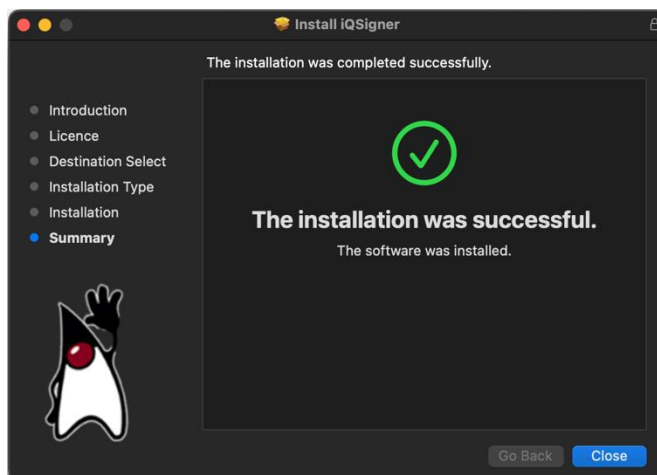
4. Uživateli je prezentována informace o velikosti instalované aplikace a možnost změnit umístění aplikace do jiného adresáře. Doporučuje se **ponechat** předvolenou hodnotu.



5. Probíhá automatická instalace.



6. Operační systém může informovat uživatele o zařazení iQ Signer mezi automaticky spouštěné aplikace po startu.
7. Instalace je u konce a uživatel uzavře instalátor kliknutím na tlačítko **Close**.



6 SPUŠTĚNÍ A BĚH APLIKACE

6.1 PRVNÍ SPUŠTĚNÍ

Po instalaci je nutné poprvé spustit aplikaci manuálně. Uživatel tak učiní vyhledáním aplikace iQ Signer v nabídce aplikací operačního systému. Případně může restartovat systém a aplikace se následně spustí automaticky.

6.2 AUTOMATICKÉ SPUŠTĚNÍ

iQ Signer se po instalaci zařadí mezi aplikace, které se spouštějí po přihlášení uživatele do systému. Tuto volbu může uživatel změnit pomocí standardních nástrojů operačního systému.

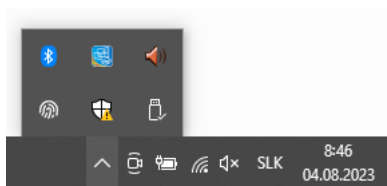
6.3 BĚH APLIKACE

Skutečnost, že aplikace běží, se dá zjistit podle přítomnosti ikony iQ Signer (otisk prstu) v systémové liště. Pozor, může se nacházet i mezi skrytými ikonami.

1. Windows systémová lišta



2. Windows systémová lišta skrytá

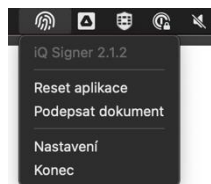


3. MacOS systémová lišta



7 NASTAVENÍ

Změna nastavení aplikace probíhá přes samostatný dialog, který uživatel vyvolá kliknutím na volbu **Nastavení**.



7.1 FILTRACE CERTIFIKÁTŮ

Aplikace umožňuje podepsat dokument libovolným podporovaným certifikátem, ke kterému má uživatel privátní klíč. Pro vytvoření kvalifikovaného podpisu dle směrnice eIDAS je zapotřebí použít kvalifikovaný certifikát na kvalifikovaném zařízení. Takový certifikát vydává zásadně kvalifikovaná certifikační autorita na USB tokenu nebo kartě.

Aby nebyl uživatel zbytečně zahlcen všemi certifikáty, které není možné využít na vytvoření kvalifikovaného podpisu, existuje v nastavení možnost filtrovat:

- kvalifikované certifikáty,
- certifikáty na kvalifikovaném zařízení.

Pro běžné potřeby doporučujeme obě možnosti zapnout.

7.2 ČASOVÁ RAZÍTKA

Časové razítko slouží k nezávislému prokázání existence dokumentu s elektronickým podpisem. Aplikace disponuje možností opatřit podepisovaný dokument časovým razítkem přímo v době podepisování.

Pro využití této možnosti je nutné vložit adresu a přístupové údaje o poskytovateli časových razítek do nastavení aplikace. Poskytovatel musí pro tuto službu využívat protokol RFC3161.

V případě, že poskytovatel nedisponuje validním HTTPS certifikátem pro zabezpečení komunikace (zpravidla testovací prostředí), existuje možnost **Důvěřovat SSL**, která vypne kontrolu tohoto certifikátu. Pro běžnou práci doporučujeme tuto možnost nezapínat.

7.3 PKCS#11 ZAŘÍZENÍ

V případě, že je k podpisu použit kvalifikovaný prostředek (token nebo karta) a poskytovatel tohoto prostředku neumožňuje uložit (propagovat) certifikát do prostředí operačního systému, je možné použít přímo knihovnu PKCS#11 od daného poskytovatele.

V nastavení aplikace je možnost uložit nastavení až pro tři různá zařízení.

Nastavení **Název** slouží pro jednoduchou uživatelskou identifikaci zařízení.

Nejdůležitějším nastavením je **Knihovna**. Zde se uvede cesta k souboru ovladače (.dll, .so, .dylib). Tato cesta je specifická pro daného poskytovatele a daný operační systém. S velkou pravděpodobností je možné ji najít v dokumentaci ke kvalifikovanému prostředku.

Nastavení **Slot index** určuje, ze kterého slotu (logického oddílu) kvalifikovaného zařízení se mají načítat certifikáty. Ve většině případů je správnou hodnotou **0**. V případě potíží s načtením certifikátů je doporučeno zkusit další hodnoty.

Někteří poskytovatelé zařízení implementují PKCS#11 protokol mírně odlišně a načtení certifikátů skončí chybou. V takovém případě je možné zapnout možnost **Vlastní PIN okno**, kdy se použije dialog aplikace pro zadání PIN místo dialogu od poskytovatele zařízení.

Ze stejného důvodu je někdy vyžadován QPIN, který ale není automaticky vyžádán přes dialog poskytovatele a podpis skončí chybou. V takovém případě je možné zapnout možnost **Vyžadovat QPIN**.

7.4 PODPISOVÉ POLE

Nastavení slouží pro vkládání viditelné vizualizace podpisu do dokumentu. Přítomnost nebo nepřítomnost vizualizace nemá vliv na pravost elektronického podpisu.

Toto nastavení není přítomno ve všech verzích aplikace.

7.5 VÝBĚR FORMÁTU

Pomocí tohoto nastavení lze povolit uživatelský výběr typu podpisu (PAdES, CAdES, XAdES, ASiC). Pokud je nastavení vypnuto, je zvolen předvolený formát.

7.6 PROXY

Pokud je nutné veškerou komunikaci z klientské stanice směřovat přes proxy server, je potřeba vyplnit nastavení **Proxy**.

Podporované jsou režimy HTTP a HTTPS. Rovněž je podporovaná autentizace jménem a heslem.

7.7 EXPERTNÍ FUNKCE

Funkce, které jsou popsány v této kapitole, nejsou nezbytné pro běh aplikace. Jejich neodborná změna může vést ke znefunkčnění samotné aplikace a nutnosti reinstalace, případně až k ručnímu smazání uložených nastavení ze systému.

7.7.1 PODPISOVÁ SLUŽBA

Aplikace iQSigner je určena pro integraci s jinými aplikacemi (i webovými) pomocí protokolu HTTP. Pro tuto komunikaci aplikace vystavuje vlastní rozhraní na dané IP/Hostname a portu. Toto nastavení je možné změnit pomocí hodnot v nastavení **Server** a **Port**.

Pokud má být aplikace použita pro pečetění místo podepisování v serverovém prostředí, je možné zvolit možnost **Headless**. Výsledkem je vypnutí jakéhokoli využití grafického rozhraní aplikace, včetně přístupu k Nastavení. **Proto se nedoporučuje toto nastavení měnit.**

7.7.2 PŘEDVOLBA

V případě použití aplikace pro pečetění se v nastavení **Předvolba** určí **Zařízení**, **certifikát** a **PIN**, který se použije pro vytvoření pečeti. Certifikát se zvolí pomocí uvedení jeho **Otisku** (SHA1Fingerprint).

7.7.3 HASH FUNKCE

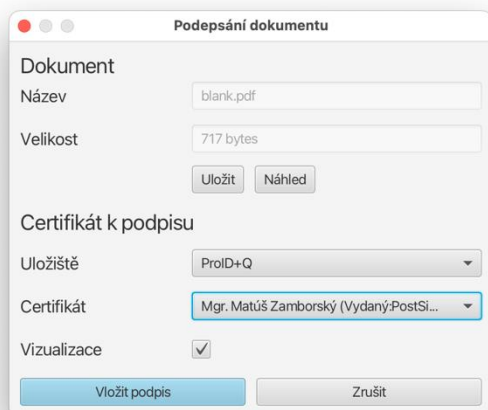
Součástí procesu podepisování je vytvoření HASH podepisovaného dokumentu. Běžně se používá algoritmus SHA256. Pokud to okolnosti vyžadují, dají se použít i jiné podporované algoritmy. Kvalifikované zařízení nemusí podporovat všechny tyto algoritmy.

8 POUŽITÍ

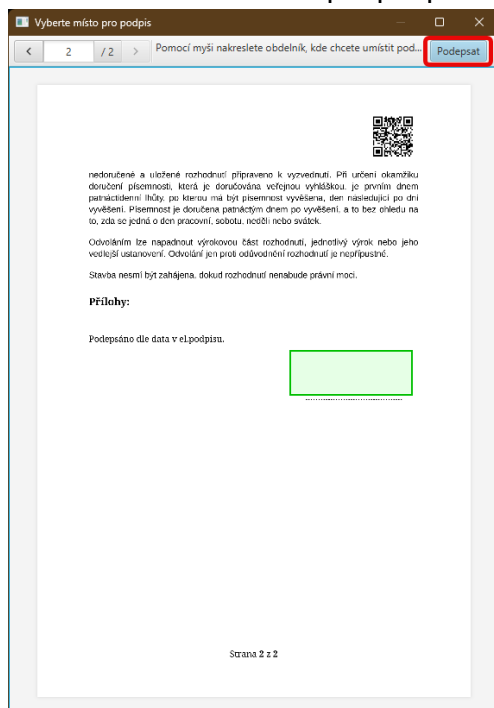
Tato kapitola pojednává o využití iQ Signer pro samostatné podepisování dokumentů. Využití iQ Signer jinou aplikací pomocí komunikačního rozhraní není předmětem této dokumentace.

Proces podepisování probíhá následovně:

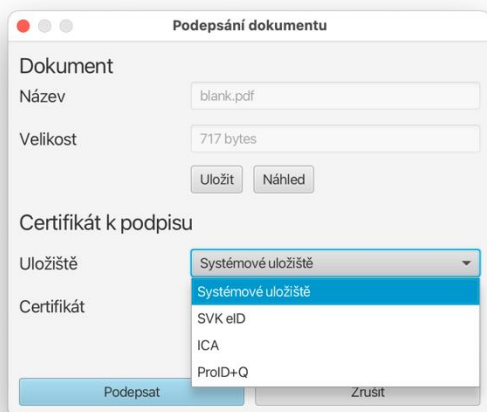
1. Uživatel klikne na tlačítko **Vložit podpis**



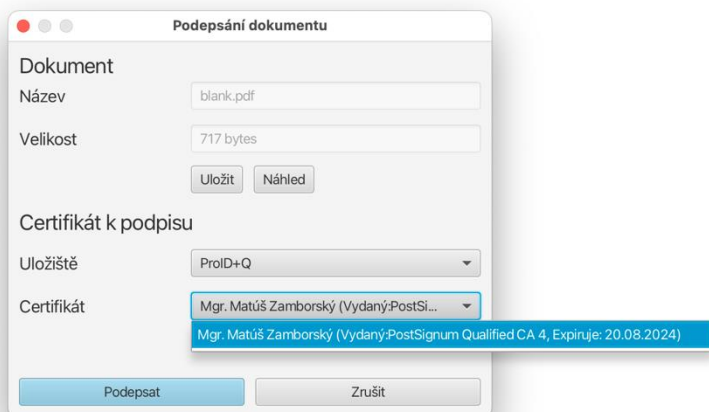
2. V náhledovém okně podepisovaného dokumentu vybere uživatel nakreslením obdélníku oblast pro podpis a klikne na tlačítko podepsat.



3. Uživatel vybere uložiště certifikátů. K výběru jsou systémová uložiště a všechna nakonfigurovaná PKCS#11 zařízení.



4. Uživatel zvolí konkrétní certifikát



5. Aplikace se může uživatele dotázat na zadání hodnoty PIN k zařízení. Podoba dialogu pro zadání PIN může být různá, dle zvoleného zařízení a nastavení aplikace.



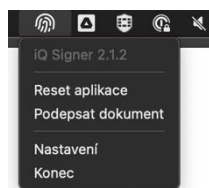
6. Aplikace se může uživatele dotázat na zadání hodnoty QPIN k certifikátu. Opět podoba dialogu pro zadání QPIN může být různá, dle zvoleného zařízení a nastavení aplikace.
7. Na pozadí probíhá podpis a případně komunikace se serverem poskytovatele časových razítek.

8.1 NÁHLED A STAŽENÍ

V procesu podepisování si uživatel může zobrazit podepisovaný dokument, případně si jej uložit (v nepodepsané podobě). Slouží k tomu tlačítka Uložit a Náhled v hlavním dialogu aplikace.

8.2 RESET APLIKACE

V případě, že aplikace vykazuje problémy se seznamem certifikátů nebo zařízení, je možné aplikaci resetovat přímo z jejího menu.



Pokud to nepomůže, doporučuje se aplikaci ukončit přes správce spuštěných procesů a znovu ji spustit.