

			\checkmark
Identifikace		Číslo jednací	
Nahrazuje		Klasifikace	veřejné
Platnost	16. 2. 2023	Účinnost	16. 2. 2023

Uživatelská příručka

eToken 5110 CC eToken 5110 CC (940) eToken 5110 CC (940B) IDPrime MD3840 IDPrime MD840 IDPrime MD841 IDPrime 3940 IDPrime 941 IDPrime 3940B IDPrime 941B

Verze 1.6



Obsah dokumentu

1.	Přehled	4
2.	Co potřebuji?	6
3.	Instalace softwaru	7
4.	Příprava tokenu pro generování klíčů	
4.1.	Používání hesel na tokenu	
4.2.	Změna Hesla k tokenu (PIN)	
4.3.	Změna Hesla správce (PUK)	
4.4.	Změna Digital Signature PIN (QPIN)	14
4.5.	Změna Digital Signature PUK (QPUK)	14
4.6.	Kontrola servisního klíče	15
4.7.	Podpora klíčů o velikosti 4096 bitů	15
4.8.	Expertní mód aplikace iSignum	16
5.	Generování žádosti o prvotní certifikát	
5.1.	Vygenerování žádosti o certifikát	
5.2.	Instalace certifikátu v iSignum	20
5.3.	Instalace certifikátu ze staženého souboru	23
6.	Generování žádosti o následný certifikát	25
7.	Další funkce softwaru SafeNet Authentication Client	27
7.1.	Import certifikátu z PKCS#12	27
7.2.	Odhlásit z tokenu	
7.3.	Aktualizovat	
7.4.	Exportovat certifikát	
7.5.	Nastavení (odblokování) hesla k tokenu (PIN)	29
7.6.	Nastavení (odblokování) Digital Signature PIN (QPIN)	29
7.7.	Odstranění dat	
7.7.	1. Odstranění certifikátu	
7.7.	2. Odstranění klíče	
7.8.	Změnit název tokenu	
7.9.	Náhled certifikátu	
7.10). Nastavení klienta	
8.	Reinicializace tokenu	
8.1.	Výmaz servisního klíče	
8.2.	Předání tokenu jiné osobě	
9.	Reklamace	

Česká pošta, s.p., se sídlem Politických vězňů 909/4, 225 99 Praha 1, IČ: 471 14 983, zapsaný v Obchodním rejstříku u Městského soudu v Praze, spisová značka A7565



Evidence revizí a změn				
Verze	Datum revize	Důvod a popis změny	Autor	Schválil
0.9	10. 6. 2017	první verze	Česká pošta, s.p.	
1.0	5. 6. 2018	finální verze	Česká pošta, s.p.	Manažer CA
1.1	29. 8. 2018	upřesněna kontrola servisního klíče	Česká pošta, s.p.	Manažer CA
1.2	1. 12. 2019	změna postupu rušení vazby prostředku na osobu	Česká pošta, s.p.	Manažer CA
1.3	28. 1. 2020	přidán postup na výmaz klíčů a certifikátů	Česká pošta, s.p.	Manažer CA
1.4	13. 8. 2020	přidán postup pro získání certifikátu pro el. pečeť	Česká pošta, s.p.	Manažer CA
1.5	25. 10. 2022	přidán nový typ tokenu a čipové karty s označením B	Česká pošta, s.p.	Manažer CA
1.6	16. 2. 2023	změna v souvislosti s novou verzí iSignum	Česká pošta, s.p.	Manažer CA



1. Přehled

Veškeré níže popsané postupy pro token eToken 5110 CC jsou platné také pro token eToken 5110 CC (940), eToken 5110 CC (940B) a pro čipové karty IDPrime MD3840, MD840, MD841, 3940, 940, 941, 3940B, 940B, 940B, 941B.

eToken (dále také jen token) je prakticky malé zařízení, které **je schválené jako kvalifikovaný prostředek pro vytváření elektronických podpisů** (všechny uvedené typy) **a pro vytváření elektronických pečetí** (pouze zařízení s označením 940, 941, 940B, 941B) **v souladu s nařízením eIDAS**. Je to PKI token postavený na kryptografickém mikroprocesoru s certifikací Common Criteria EAL4+ a FIPS 140-2 level 3.

eToken obsahuje oblast pro uložení kvalifikovaného certifikátu. Tuto oblast chrání **podpisový PIN** tzv. **QPIN**, který je vyžadován vždy při přístupu do této oblasti, tzn. při generování žádosti o kvalifikovaný certifikát nebo při použití kvalifikovaného certifikátu.

Informace k certifikaci prostředků:

Každý prostředek má certifikaci časově omezenou. Po skončení certifikace přestává být kvalifikovaným prostředkem. K datu skončení certifikace budou zneplatněné všechny platné kvalifikované certifikáty, které jsou na prostředku uloženy.

Po ukončení certifikace již nebude možné na prostředek uložit kvalifikovaný certifikát s příznakem QESCD.

O platnosti certifikace konkrétního prostředku se můžete přesvědčit na webových stránkách PostSignum: <u>https://www.postsignum.cz/certifikace_prostredku.html</u>

Upozornění: Aplikace iSignum bude i v případě ukončené certifikace označovat prostředek jako kvalifikovaný, nicméně funkce prostředku pro kvalifikované certifikáty budou omezeny. Ukončená certifikace se nedotkne komerčních certifikátů.

eToken je personalizován již z výroby, tzn., je na něm přednastaven PIN a QPIN (12345678) a PUK a QPUK (87654321).

Z bezpečnostních důvodů je při prvním použití nutné změnit PIN, QPIN, PUK a QPUK.

Před dodáním tokenu zákazníkovi je v prostředí České pošty provedena příprava tokenu pro bezpečné a průkazné předávání žádostí o certifikát. Příprava spočívá ve vygenerování páru klíčů, tzv. "servisní klíč", v tokenu označen "SERVICE KEY". Tento klíč se používá k zabezpečení komunikace mezi tokenem a systémem certifikační autority. Je nutné dbát na to, aby nedošlo ke smazání tohoto klíče z tokenu. Pokud dojde k výmazu servisního klíče, nebude možné vytvořit žádost o certifikát pomocí aplikace iSignum.

Při vydání prvotního certifikátu dochází k vytvoření vazby **prostředek–žadatel o certifikát**, která je evidována v systému certifikační autority a kontrolována při vydávání dalších (následných) certifikátů do zařízení. Technicky tedy není možné mít na prostředku více certifikátů různých žadatelů s příznakem QESCD (kvalifikované) nebo NCP+ (komerční). Toto platí jak pro osobní kvalifikované a komerční certifikáty, tak pro certifikáty pro el. pečeť.



Pokud dojde k situaci, že je nutné token předat jinému žadateli (např. z důvodu ukončení pracovního poměru) je nutné postupovat dle kapitoly 8.2.



Obrázek zařízení eToken



2. Co potřebuji?

1. PC s operačním systémem Windows



2. eToken 5110



3. Software



Software stáhnete z webové stránky: https://www.postsignum.cz/etoken_5110_cc.html



3. Instalace softwaru



Jernallo security to be free				
Setup has detected existing configuration settings				
✓ Use the existing configuration settings				











Knihovna PKCS#11

V případě použití tokenu v aplikacích, které nevyužívají systémové úložiště certifikátů ve Windows (např. Mozilla Firefox nebo Thunderbird), lze ke komunikaci s tokenem využít (pokud to aplikace podporuje) DLL knihovnu PKCS#11 *eTPKCS11.DLL*, která se nachází v adresáři *C:\WINDOWS\SYSTEM32*.



4. Příprava tokenu pro generování klíčů

Před prvním použití tokenu **je nutné změnit PIN, QPIN, PUK a QPUK** a přesvědčit se, zda je na tokenu přítomen "servisní klíč". Veškeré popsané činnosti se provádějí v programu **SafeNet Authentication Client**, který je možné otevřít například z nabídky START.

Pro podrobné zobrazení je nutné kliknout na úvodní obrazovce v SafeNet Authentication Client na volbu



SafeNet Authentication Client Tools			
		ge	
SafeNet Authen	iticatior	n Client 🛛 🧔 👩	2 🔒
*	1	Přejmenovat token	
	****	Změnit PIN tokenu	
		Odemknout token	
	\otimes	Odstranit obsah tokenu	
	Q	Zobrazit informace o tokenu	
		Disconnect SafeNet Virtual Token	
		⊖ gemai	то.сом

Okno programu **SafeNet Authentication Client** je rozděleno do tří částí. Levá část zobrazuje připojené tokeny a objekty na tokenu (klíče, certifikáty). Pravá horní část zobrazuje příkazy a funkce, pravá spodní část informace o vybraném tokenu či objektu.

Při práci s daným tokenem je vždy nutné příslušný token vybrat v levé části, tzn. kliknout na něj. To platí především v případě, je-li připojeno více kryptografických zařízení.



@		
SafeNet Authentication Client Tools		
		gemalto security to be free
SafeNet Authen	tication Client	a 😳 🤹 🕈 🔿
SafeNet Authentication Client Tools	🥺 🖡 🗊 🔪 🖊 🖡 🔛 👘 🎒	⊖ î ± ★
 Certifikáty CC Certifikáty CC Servisní klíč P 11#424d3aef2388006 Nastavení Nastavení Nastavení klienta 	Název tokenu Kategorie tokenu Název čtečky Sériové číslo (PKCS#11) Volné místo na čipové kartě (minimum estimated) Verze hardwaru Verze firmwaru ID karty (Minidriver) Název produktu Model Typ karty Applet Version Verze masky Barva Podporovaná velikost klíče Haela k tokenu	AKS ifdh 0 25213 25213 12.0 12.0 0x6A00002258693C746A00002258693C SafeNet e Token 5110 CC Token 12.0.0.0 12.0.13 ID Prime MD IDPrime Java Applet 4.0.2.K G260/Filt17 Nen í k dispozici 2048 bits la k dispozici la k dispozici
۰ (III) ا	Počet zbývaiících pokusů o zadání Heslo k toke ∢ [III	5
		⊖ GEMALTO.COM

Před dalšími kroky je potřeba se k tokenu přihlásit tlačítkem *Přihlášení* **b**a zadat přednastavený PIN: **12345678**

SafeNet Auth	hentication Client Tools 🥥 🖟 🗊 🔝 🔪 🎼 🔛 🔐 😂	1 1 1 *	
→	SafeNet Authentication Client	gemalto [×]	
	Zadejte Heslo k tokenu. Název tokenu:		■ A00002258693C C
	Heslo k tokenu: Aktuální jazyk: CS	D. Cancel	2.К
	Pocet zbyvalicich pokusů o zadani Heslo k toke 5		-

1



4.1. Používání hesel na tokenu

Token má po zakoupení od PostSignum tato iniciální nastavení hesel:

Heslo	Nastavená
	hodnota
Heslo k tokenu (PIN)	12345678
Heslo správce (PUK)	87654321
Digital Signature PIN (QPIN)	12345678
Digital Signature PUK (QPUK)	87654321

Všechna 4 hesla lze nastavit v programu SAC v Podrobném zobrazení - zapne se ikonkou 🥨

Význam a funkce hesel:

Heslo	Minimální délka	Max. počet pokusů	Význam a využití hesla
Heslo k tokenu (PIN)	4 znaky (lze nastavit)	5 pokusů	 přihlášení k tokenu, vytvoření podpisu certifikátem, který není kvalifikovaný
Heslo správce (PUK)	8 znaků (lze nastavit)	není omezeno	 nastavení nového hesla k tokenu PINu po opakovaném špatném zadání PINu, nutný k inicializaci tokenu do výchozího stavu (POZOR! – inicializací dojde ke smazání obsahu tokenu včetně certifikátů a Servisního klíče PostSignum)
Digital Signature PIN (QPIN)	6 znaků	3 pokusy	 vytváření kvalifikovaného podpisu pomocí kvalifikovaného certifikátu PostSignum
Digital Signature PUK (QPUK)	6 znaků	3 pokusy	 slouží k nastavení nového Digital Signature PINu (QPINu), nutný k inicializaci tokenu do výchozího stavu (POZOR! – inicializací dojde ke smazání obsahu tokenu včetně certifikátů a Servisního klíče PostSignum)

Upozornění:

Neprovádějte inicializaci tokenu! Inicializací dojde ke smazání obsahu tokenu včetně Servisního klíče a token bude nepoužitelný pro vytvoření žádosti o kvalifikovaný certifikát!

V případě zablokování QPUK i QPIN nebude možné token používat pro kvalifikované certifikáty.

V případě zapomenutí PUK a zablokování PIN nebude token použitelný pro další práci.



4.2. Změna Hesla k tokenu (PIN)

- 1. V SafeNet Authentication Client kliknout na volbu Změnit heslo (nutná znalost aktuálního Hesla k tokenu)
- 2. Do políčka Aktuální heslo k tokenu zadat: 12345678.
- 3. Do políčka Nové Heslo k tokenu zapsat nové heslo, které musí odpovídat kvalitě hesla definované na tokenu (viz tabulka výše).
- 4. Do políčka Potvrdit Heslo zopakovat nové heslo.
- 5. Změnu hesla potvrdit tlačítkem OK.

S Změnit Heslo:	×
SafeNet Authentication Client	gemalto*
Aktuální Heslo k tokenu:]
Nové Heslo k tokenu:	
Potvrdit Heslo:]
Nové heslo musí odpovídat nastavení kvality definované na tokenu.	
Bezpečné heslo má aspoň 8 znaků a obsahuje veľká písmena, malá písm (například !, \$, #, %).	ena, číslice a zvláštní znaky
Aktuální jazyk: CS	
Zadejte současné heslo.	
	OK Cancel

4.3. Změna Hesla správce (PUK)

- 1. V SafeNet Authentication Client kliknout na volbu Změnit heslo správce (nutná znalost aktuálního Hesla správce)
- 2. Do políčka Aktuální Heslo správce zadat: 87654321.
- 3. Do políčka Nové Heslo k tokenu zapsat nové heslo.
- 4. Do políčka Potvrdit Heslo zopakovat nové heslo.
- 5. Změnu Hesla správce potvrdit tlačítkem OK.

S Změnit Heslo správce:	×
SafeNet Authentication Client	gemalto [×]
Aktuální Heslo správce:]
Nové Heslo správce:	
Bezpečné heslo má aspoň 8 znaků a obsahuje veľká písmena, malá písm (například IS # %).	ena, číslice a zvláštní znaky
Aktuální jazyk: CS Zadeite současné heslo.	
	OK Cancel



4.4. Změna Digital Signature PIN (QPIN)

1. V SafeNet Authentication Client kliknout na volbu Změnit Digital Signatrue PIN (nutná znalost

aktuálního Digital Signature PINu)

- 2. Do políčka Aktuální Digital Signature PIN zadat: 12345678.
- 3. Do políčka Nový Digital Signature PIN zaspat nové heslo.
- 4. Do políčka potvrdit PIN zopakovat nové heslo.
- 5. Změnu Digital Signature PIN potvrdit tlačítkem OK.

S Change Digital Signature PIN:	-	×
SafeNet Authenticati	on Client	gemalto [×]
Current Digital Signature PIN:]
New Digital Signature PIN:]
Potvrdit PIN:		
Nové PIN musí odpovídat nastaveni	í kvality definované na tokenu.	
Bezpečné PIN má aspoň 8 znaků a o (například !, \$, #, %).	obsahuje velká písmena, malá písme	na, číslice a zvláštní znaky
Aktuální jazyk: CS		
Zadejte současné heslo.		
		OK Cancel

4.5. Změna Digital Signature PUK (QPUK)

- 1. V SafeNet Authentication Client kliknout na volbu Změnit Digital Signature PUK (nutná znalost aktuálního Digital Signature PUKu)
- 2. Do políčka Aktuální Digital Signature PUK zadat: 87654321.
- 3. Do políčka Nový Digital Signature PUK zaspat nové heslo.
- 4. Do políčka potvrdit PUK zopakovat nové heslo.
- 5. Změnu Digital Signature PUK potvrdit tlačítkem OK.

S Change Digital Signature PUK:	×
SafeNet Authentication Client	gemalto [×]
Current Digital Signature PUK:	
New Digital Signature PUK:	
Potvrdit PUK:	
Nové PUK musí odpovídat nastavení kvality definované na	tokenu.
Bezpečné PUK má aspoň 8 znaků a obsahuje velká písmen (například !, \$, #, %).	a, malá písmena, číslice a zvláštní znaky
Aktuální jazyk: CS	
Zadejte současné heslo.	
	OK Cancel



4.6. Kontrola servisního klíče

Servisní klíč je nutný pro zajištění identifikace tokenu v systému certifikační autority a využívá se pro zabezpečení komunikace při předávání žádosti o certifikát. Pokud servisní klíč na tokenu není přítomen, není možné token použít pro vytvoření žádosti o certifikát.

V SafeNet Authentication Client rozbalit volbu Osamocené objekty, kde se musí nacházet položka s názvem **Servisní klíč**, viz obrázek.

Na volbu Osamocené objekty nestačí pouze kliknout, ale je nutné volbu rozbalit kliknutím na 🕨 nebo 🖽.

- - X SafeNet Authentication Client Tools aemai SafeNet Authentication Client 1. SafeNet Authentication Client Tools r i 🦽 Tokeny Vydán pro Vydal Konec Účely Uživatelské certifikáty Certifikáty CC Osamocené objekty Servisní klíč 🚺 Nastavení 🔅 Nastaven í klienta • 4 111 → GEMALTO.COM

Pokud Servisní klíč chybí, je nutné postupovat dle kapitoly 8.1.

4.7. Podpora klíčů o velikosti 4096 bitů

Velikost 4096 bitů podporují pouze tokeny s označením 940, 941, 940B, 941B. Maximální možná velikost klíče je zobrazena v aplikaci iSignum při generování žádosti o nový certifikát nebo o obnovu certifikátu. Výběr velikosti klíče lze ovlivnit v expertním módu, viz kapitola 4.8.

Upozorňujeme, že generování klíče o velikosti 4096 bitů může trvat až 5 minut.

Česká pošta, s.p., se sídlem Politických vězňů 909/4, 225 99 Praha 1, 1Č: 471 14 983, zapsaný v Obchodním rejstříku u Městského soudu v Praze, spisová značka A7565



4.8. Expertní mód aplikace iSignum

Expertní mód aplikace iSignum umožňuje:

- Zvolit si velikost klíče při generování nového ID žádosti nebo v případě obnovy certifikátu. V nabídce je vždy velikost klíče 2048 bitů a pokud to vybrané úložiště umožňuje, tak i 4096 bitů.
- Možnost smazat vygenerovaný klíč z kvalifikovaného prostředku, pokud není spárovaný s vydaným certifikátem, viz kap. 7.7.2.
 POZOR! Tato operace může zapříčinit chybnou instalaci certifikátu, provádějte ji vždy s

POZOR! Tato operace může zapříčinit chybnou instalaci certifikátu, provádějte ji vždy s rozmyslem a až po instalaci všech vydaných certifikátů. Výmaz klíčů z prostředku může trvat až 5 minut.

Rozšíření funkcí aplikace iSignum provedete přepnutím aplikace do expertního módu stisknutím tlačítka Nápověda a o aplikaci. Expertní mód bude signalizovat červená barva horní lišty.





Změna velikosti klíče v expertním módu:

Průvodce	vygenerováním žád	osti o certifikát Pos	tSignum	
	Tento průvodce Vás pro Průvodce nejprve vyge žádost o vystavení cer PostSignum. Je vyžado Krok 1: Vyplnění zál	ovede procesem vygen eneruje klíčový pár ve z tifikátu pro tento pár. I vváno připojení k intern kladních informací	erování žádosti o cer zvoleném úložisti a vy Následně žádost ode etu.	tifikát PostSignum /generuje šle na server
	Typ certifikátu:	Kvalifikovaný certifiká	t (QCA)	~
	Jméno:			
	Email:			
	Mobilní telefonní číslo:	+420		
	Tyto informace jsou n žadatelem o certifikát. prostřednictvím SMS r	epovinné a slouží pro ověř Informace o generované ž na mobilní telefonní číslo.	ení uložené žádosti před žádosti o certifikát je zas	vydáním certifikátu sílána výhradně
	Po odeslání vytis Zálohovat privát	knout souhrnné inform ní klíč (pokud to umožňu	ace uje vybrané úložistě))
	Krok 2: Výběr úložiš	tě pro generování k	díčů	
	8A5E30B	42AEC53AC		~
	Bude gene	erován klíč o velikosti:	RSA 4096	~
	Byl vybra	án kvalifikovaný prostře	RSA 2048 RSA 4096	_
	Krok 3: Generování	a odeslání žádosti r	ia server PostSigi	num
	Souhrn:			
	Odeslat žádost	Zkopírovat II) do schránky	Zavřít



5. Generování žádosti o prvotní certifikát

Generování klíčů na token a žádosti o kvalifikovaný certifikát, který bude obsahovat příznak QESCD (kvalifikované cert.) nebo NCP+ (komerční cert.), je možné pouze v programu **iSignum**, který zajistí vytvoření správné žádosti o certifikát. Pokud bude ke generování žádosti využit jiný program, není možné do certifikátu uvedené příznaky vložit.

Program iSignum je ke stažení z webových stránek PostSignum:

https://www.postsignum.cz/isignum.html

Spustit lze poklikáním na stažený soubor iSignum.exe.

Program iSignum rozpozná vložení prostředku, záložka s prostředkem je indikována zelenou ikonou.

🜖 iSignum	
Νονý	Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení eIDAS č. 910/2014 (Příloha II).
Obnovit	Přehled Certifikáty 💭 Windows
Importovat	Obsazené místo: 4 z 32 KB (15%) Vyčistit Stažení certifikátu
Nápověda a o aplikaci	Jméno Sériové č. Platnost Zbývá Vydavatel Typ
V	
Česká pošta ► d i g n i t a	Detail

5.1. Vygenerování žádosti o certifikát

- 1. Vložit token do USB portu počítače.
- 2. V programu iSignum stisknout tlačítko Nový. Spustí se průvodce vygenerováním žádosti.
- 3. Úložiště pro generování klíčů bude přednastaveno na hodnotu **eToken** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek. (Zda je prostředek kvalifikovaný se můžete přesvědčit na webové stránce <u>https://www.postsignum.cz/certifikace_prostredku.html</u>.)
- 4. **Vybrat typ certifikátu**. Příznak QESCD lze vložit **pouze** do **Kvalifikovaného certifikátu (QCA)**. Pokud bude vybrán komerční certifikát, bude v certifikátu příznak NCP+.
- 5. Dále můžete vyplnit své jméno a e-mailovou adresu, případně tel. č. a stisknout tlačítko *Odeslat* žádost.
- 6. Velikost generovaného klíče (kap. 4.7) lze ovlivnit v expertním módu aplikace iSignum (kap. 4.8).
- 7. Před generováním klíčů a žádosti bude vyžadován PIN i QPIN.



Průvodce	vygenerováním žá	dosti o certifikát Pos	tSignum	×
	Tento průvodce Vás p	rovede procesem vygen	erování žádosti o ce	rtifikát PostSignum
	Průvodce nejprve vy žádost o vystavení ce PostSignum. Je vyžac Krok 1: Vyplnění za	generuje klíčový pár ve : rtifikátu pro tento pár. lováno připojení k intern ikladních informací	zvoleném úložisti a v Následně žádost ode etu.	/generuje šle na server
	Typ certifikátu:	Kvalifikovaný certifiká	t (QCA)	~
	Jméno:			
	Email:			
	Mobilní telefonní číslo:	+420		
	Tyto informace jsou žadatelem o certifiká prostřednictvím SMS	nepovinné a slouží pro ověl t. Informace o generované na mobilní telefonní číslo.	ení uložené žádosti před žádosti o certifikát je za:	vydáním certifikátu sílána výhradně
	Po odeslání vyt	sknout souhrnné inform tní klíč (pokud to umožň	ace uie vybrané úložistě	
		4	· · ·	
	Krok 2: Výběr úlož	iště pro generování	díčů	
	Krok 2: Výběr úlož 8A5E30	i ště pro generování B42AEC53AC	klíčů	~
	Krok 2: Výběr úlož 8A5E30 Bude ger	i ště pro generování l B42AEC53AC nerován klíč o velikosti:	klíčů RSA 4096	*
	Krok 2: Výběr úlož 8A5E30 Bude ger Bvl vyb	i ště pro generování l B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř	klíčů RSA 4096 edek	~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár	i ště pro generování B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti i	klíčů RSA 4096 edek na server PostSig	~ ~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár Souhrn:	iště pro generování 842AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti i	k líčů RSA 4096 edek na server PostSig	~ ~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár Souhrn:	iště pro generování B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti n	RSA 4096 edek na server PostSig	~ ~
	Krok 2: Výběr úlož 8A5E30 Bude gei Byl vyb Krok 3: Generovár Souhrn:	i ště pro generování i B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti i	klíčů RSA 4096 edek na server PostSig	~ ~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár Souhrn:	i ště pro generování B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti i	klíčů RSA 4096 edek na server PostSig	~ ~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár Souhrn:	iště pro generování 842AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti i	klíčů RSA 4096 edek na server PostSig	~
	Krok 2: Výběr úlož 8A5E30 Bude ger Byl vyb Krok 3: Generovár Souhrn:	iště pro generování l B42AEC53AC nerován klíč o velikosti: rán kvalifikovaný prostř í a odeslání žádosti n	klíčů RSA 4096 edek na server PostSig	~ ~

- 8. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a za pomoci servisního klíče dojde k autentizaci tokenu do systému a bezpečnému předání žádosti o certifikát.
- Při generování žádosti o Kvalifikovaný certifikát budete vyzvání k zadání Digital Signature PIN (QPIN).

S Digital Signature PIN Logon			X
SafeNet Authentication	n Client		gemalto
Enter the Digital Signature PIN: Název tokenu: Digital Signature PIN:	l Aktuální jazyk:	CS	OK Cancel

10. Pokud vše proběhne v pořádku, bude uživateli vráceno ID žádosti s prefixem BP (kvalifikovaný certifikát) nebo KC (komerční certifikát) následováno 10timístným číslem. Na základě tohoto ID bude vystaven kvalifikovaný nebo komerční certifikát s příznakem, že byl klíč vygenerován na prostředku.

Krok 3: Ge	nerování a odeslání žádosti na server PostSignum
Souhrn:	ID žádosti o certifikát: BP5638412975
nebo	



Krok 3: Generování a odeslání žádosti na server PostSignum

Souhrn: ID žádosti o certifikát : KC5765039450

Toto ID předložíte spolu s dalšími náležitostmi na pobočce České pošty. Postup, jak získat certifikát naleznete na webových stránkách PostSignum:

https://www.postsignum.cz/postup_pro_ziskani_certifikatu.html

Poznámka (certifikát pro el. pečeť):

Kvalifikovaný certifikát pro elektronickou pečeť není vydáván na pobočkách České pošty. V případě žádosti o tento typ certifikátu postupujte dle pokynů na webových stránkách PostSignum:

https://www.postsignum.cz/vydani_certifikatu_elektronicky.html

Platí pouze pro zařízení s označením 940, 941, 940B, 941B

5.2. Instalace certifikátu v iSignum

Instalaci přímo do tokenu lze provést pouze v programu iSignum:

- 1. Vložit token do USB portu počítače nebo do čtečky.
- 2. V programu iSignum stisknout tlačítko Stažení certifikátu.

🜖 iSignum	
Nový	Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti). Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení eIDAS č. 910/2014 (Příloha II).
Obnovit	Přehled Certifikáty 💭 Windows
Importovat	Obsazené místo: 4 z 32 KB (12%) Vyčistit Stažení certifikátu
Nápověda a o aplikaci	Jméno Sériové č. Platnost Zbývá Vydavatel Typ
Česká pošta	
► d i g n i t a	Detail

3. Stiskem tlačítka Zkontrolovat vydané certifikáty ověřit, zda je již certifikát připraven k instalaci.



Průvodce stažením certifikátu	X
Token:	
Zkontrolovat vydané certifikáty	Zavřít

4. Pokud byl certifikát nalezen, bude zobrazeno toto okno:

Byl nalezen certifikát
Byl nalezen certifikát
Stáhnout protokol o vydání certifikátu
Instalovat certifikát
Přeskočit

- 5. Dále je možné zkontrolovat údaje ve vydaném certifikátu v protokolu o vydání certifikátu, který lze stáhnout stiskem tlačítka *Stáhnout protokol o vydání certifikátu*.
- 6. Protokol lze uložit stiskem tlačítka Uložit jako nebo vytisknout tlačítkem Tisk.
- 7. Okno s protokolem lze zavřít stiskem tlačítka Zavřít.

Jložit jako Tisk	69%	•	1	🐑 z 2	Zavi
			ć	Číslo smlouvy	
Česká pošta	Protokol	o vydání (certifikát	u	
Udaje o zákaznikovi					1
Nazev / Obchodni firma / Jn příjmení:	neno a				
IČ:	in the second second				-
					1
Údaje o žadateli o certif	ikát:				1
Údaje o žadateli o certif Jméno a příjmení:	ikát:]
Údaje o žadateli o certif Jméno a příjmení: Údaje o certifikátu	ikát:]
Údaje o žadateli o certif Jméno a příjmeni: Údaje o certifikátu Základní údaje	ikát:]
Údaje o žadateli o certif Jméno a příjmení: Údaje o certifikátu Základní údaje Vydán autoritou:	ikát:]
Údaje o žadateli o certif Jméno a příjmení: Údaje o certifikátu Základní údaje Vydán autoritou: Certifikační politika:	ikát:]
Údaje o žadateli o certif Jméno a příjmení: Údaje o certifikátu Základní údaje Vydán autoritou: Certifikační politika: Sériové číslo:]
Údaje o žadateli o certif Jméno a příjmení: Údaje o certifikátu Základní údaje Vydán autoritou: Certifikační politika: Sériové číslo: Platnost od:]

8. Přijmout certifikát - pokud jsou údaje v certifikátu v pořádku.





9. Zadat PIN

Zadejte PIN	×
	Přístup k úložišti je chráněn PINem. Zadeite PIN
2	Aktivní jazyk klávesnice:
~	Ok

10. Pokud operace proběhne úspěšně, bude zobrazena hláška:



11. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce eToken.

🜖 iSignum	
Nový	Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení eIDAS č. 910/2014 (Přiloha II).
Obnovit	Přehled Certifikáty 🔘 Windows
Importovat	Obsazené místo: 6 z 32 KB (20%) Vyčistit Stažení certifikátu
Nápověda a o aplikaci	Jméno Sériové č. Platnost Zbývá Vydavatel Typ Osoba Testovací 566511 17.04.2019 364 dní DEMO PostSignum Qu Kvalifikovaný osobní
V	
Ceská pošta	Detail

12. Po instalaci doporučujeme token vyjmout a znovu vložit do USB portu nebo do čtečky.



5.3. Instalace certifikátu ze staženého souboru

Instalaci certifikátu doporučujeme provést taktéž v programu iSignum:

- 1. Vložit token do USB portu počítače.
- 2. V programu iSignum stisknout tlačítko Importovat.
- 3. Vybrat certifikát

 Otevřít 		×
	• i j	Prohledat: Token 🔎
Uspořádat 🔻 Nová složka		:= - 1 🔞
🚖 Oblíbené položky	 Název položky 	Datum změny
Naposledy navštívené	E QCAxxxxx.crt	10.10.2016 15:30
Plocha		
Počítač		
🏭 Místní disk (C:)		
	▼ • [4
Název souboru	u: QCAxxxxxx.crt 👻	Kryptografické soubory (*.crt;*, 🔻
		Otevřít 🔻 Storno

4. Ponechat přednastavené úložiště eToken

Volba úložiště		×
Vyberte úlo	ožiště, do kterého chcete	balíček importovat
		_
Storno	,	Ok

5. Pro import certifikátu bude vyžadován PIN

Zadejte PIN		×
	Přístup k úložišti chráněn PINem.	je
	Zadejte PIN	
	I	
$ \langle \zeta \rangle$	Aktivní jazyk klávesnice:	CS
	Ok	Storno

6. Pokud operace proběhne úspěšně, bude zobrazena hláška:





- 7. Po úspěšném importu bude certifikát vidět v programu iSignum na záložce eToken.
- 8. Po instalaci doporučujeme token vyjmout a znovu vložit do USB portu.

🜖 iSignum	
Nový	Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení eIDAS č. 910/2014 (Příloha II).
Obnovit	Přehled Certifikáty 💭 Windows
Importovat	Obsazené místo: 7 z 32 KB (23%) Vyčistit Stažení certifikátu
Nápověda a o aplikaci	Jméno Sériové č. Platnost Zbývá Vydavatel Typ Osoba Testovací 565895 10.04.2019 364 dní DEMO PostSignum Qu Kvalifikovaný osobní
V	
Ceská pošta ▶ d i g n i t a	Detail



6. Generování žádosti o následný certifikát

Před provedením obnovy kvalifikovaného certifikátu se přesvědčte, že je na tokenu dostatek místa pro vygenerování nového klíče. Na token do CC části lze uložit maximálně dva kvalifikované certifikáty. Odstranění dat z tokenu je popsáno v kapitole 7.7

- 1. Vložit token do USB portu počítače.
- 2. V programu iSignum stisknout tlačítko *Obnovit*. Spustí se průvodce vygenerováním žádosti o následný certifikát.
- 3. Vybrat certifikát, který chcete obnovit.
- 4. Úložiště pro generování klíčů bude přednastaveno na hodnotu **eToken** a zároveň bude zobrazeno upozornění: Byl vybrán kvalifikovaný prostředek. (Zda je prostředek kvalifikovaný se můžete přesvědčit na webové stránce <u>https://www.postsignum.cz/certifikace_prostredku.html</u>.)
- 5. Velikost generované klíče (kap. 4.7) lze ovlivnit v expertním módu aplikace iSignum (kap. 4.8).
- 6. Stisknout tlačítko Odeslat žádost případně Odeslat žádost o víceletý certifikát.

Pruvodce vygenerovanim zadosti o certifikat PostSignum				
	Tento průvodce Vás provede procesem vygenerování žádosti o následný certifikát. Průvodce nejprve vygeneruje klíčový pár v systémovém úložisti a vygeneruje žádost o vystavení certifikátu pro tento pár. Následně žádost odešle na server PostSignum. Je vyžadováno připojení k internetu. Krok 1: Volba aktuálního certifikátu, který chcete obnovit			
	Zálohovat privátní klíč (pokud to umožňuje vybrané úložistě) Kód slevové poukázky:			
	Krok 2: Výběr úložiště pro generování klíčů			
	8A5E30B42AEC53AC 8A5E30B42AEC53AC			
	Byl vybrán kvalifikovaný prostředek			
	Bude generován klíč o velikosti: RSA 4096 ~			
	Krok 3: Generování a odeslání žádosti na server PostSignum			
	Souhrn:			
	Odeslat žádost ovíceletý certifikát Zavřít			



7. Před generováním klíčů a žádosti bude vyžadován PIN.

Zadejte PIN		×
	Přístup k úložišti chráněn PINem. Zadejte PIN Aktivní jazyk klávesnice: Ok	je CS Storno

- 8. Po vygenerování klíčů a žádosti o certifikát bude navázána komunikace se systémem certifikační autority a za pomoci servisního klíče dojde k autentizaci tokenu do systému a bezpečnému předání žádosti o certifikát. Při zpracování žádosti o následný certifikát je navíc provedena kontrola vazby *token-žadatel*.
- 9. Při generování žádosti o Kvalifikovaný certifikát budete vyzvání k zadání Digital Signature PIN (QPIN).

🤶 Digital Signature PIN Logon			×
SafeNet Authenticatior	n Client		gemalto [×]
Enter the Digital Signature PIN: Název tokenu: Digital Signature PIN:	l Aktuální jazyk:	CS	OK Cancel

- 10. Pokud vše proběhne v pořádku, bude žádost o následný certifikát zařazena do systému PostSignum ke zpracování. O vydaném certifikátu budete informováni e-mailem, který bude odeslán na e-mailovou adresu uvedenou v certifikátu.
- 11. Instalace následného certifikátu probíhá totožným způsobem jako instalace prvotního certifikátu, viz kapitola 5.2.

Poznámka (certifikát pro el. pečeť):

Vygenerování žádosti o obnovu kvalifikovaného certifikátu pro elektronickou pečeť probíhá stejně jako generování žádosti o prvotní certifikát, viz kapitola *Generování žádosti o prvotní certifikát*, následný postup žádosti o obnovu certifikátu je popsán na webových stránkách PostSignum:

https://www.postsignum.cz/obnova_certifikatu.html

Platí pouze pro zařízení s označením 940, 941, 940B, 941B



7. Další funkce softwaru SafeNet Authentication Client

7.1. Import certifikátu z PKCS#12

Vložení certifikátů ze zálohy (PFX nebo P12) do tokenu se provede kliknutím na tlačítko Import certifikátu.

- 1. Zadat PIN k tokenu
- 2. Vybrat soubor se zálohou, kde je uložený certifikát ve formátu .pfx či .p12.

S Importovat certifikát:	×
SafeNet Authentication Client	gemalto [×]
 Importovat certifikát z mého osobního úložiště certifikátů Importovat certifikát ze souboru) 	
	OK Stomo
3. Zadat heslo k záloze certifikátu.	
S Heslo PFX nebo P12	
SafeNet Authentication Client	
Zadejte heslo k souboru PFX nebo P12:	
Aktuální jazyk: CS	
	OK Stomo
4. Potvrdit OK.	
SafeNet Authentication Client Tools	
Certifikát byl úspěšně importován.	
ОК	

Po úspěšném vložení certifikátu se zobrazí v horní části programu vybraný certifikát.



S SafeNet Authentication Client Tools				
				gemalto security to be free
SafeNet Authen ⁻	tication	Client		🏶 😳 i ? 🚖
⊿ ⊹SS SafeNet Authentication Client Tools	"			
	Vydán pro	Vydal	Konec	Účely
 Image: Sign of the state of th	SIPO CENTRUM	Post Signum Public CA 2	19-Jan-2020	Zásady všech aplikací
				⊖ GEMALTO.COM

Upozorňujeme, že takto importovaný kvalifikovaný certifikát nebude považován za kvalifikovaný certifikát uložený na bezpečném prostředku QESCD a nebude obsahovat příznak QESCD. Totéž platí i v případě importovaného komerčního certifikátu a příznaku NCP+.

7.2. Odhlásit z tokenu

Po stisku tlačítka dojde k odhlášení tokenu z aplikace.

7.3. Aktualizovat

Po stisku tlačítka dojde k obnovení zobrazených informací na tokenu. 🧐

7.4. Exportovat certifikát

Vyexportuje samotný certifikát ve formátu DER bez privátního klíče, který je uložen na tokenu.



7.5. Nastavení (odblokování) hesla k tokenu (PIN)

1. V SafeNet Authentication Client kliknout na volbu Nastavit heslo k tokenu (nutná znalost aktuálního

hesla správce - PUK)

- 2. Do políčka heslo správce zadat Vaše heslo správce PUK.
- 3. Do políčka Heslo k tokenu (PIN) zapsat nové heslo, které musí odpovídat kvalitě hesla definované na tokenu (viz kapitola 4.1).
- 4. Do políčka Potvrdit heslo zopakovat nové heslo.
- 5. Změnu hesla potvrdit tlačítkem OK.

S Nastavení hesla:	×
SafeNet Authentication Client	gemalto [×]
Heslo k tokenu:	
Potvrdit Heslo:	
Nastavte maximální počet neúspěšných přihlášení:	
Bezpečné heslo má aspoň 8 znaků a obsahuje velká písmena, malá písmer (například !, \$, #, %).	na, číslice a zvláštní znaky
Aktuální jazyk: CS	
Zadejte nové heslo.	
	OK Cancel

7.6. Nastavení (odblokování) Digital Signature PIN (QPIN)

1. V SafeNet Authentication Client kliknout na volbu Set Digital Signature PIN (nutná znalost aktuálního Digital Signature PUK)

2. Do políčka Digital Signature PUK zadat Vaše heslo Digital Signature PUK (QPUK) a stisknout tlačítko OK

- 3. Do políčka New Digital Signature PIN (QPIN) zapsat nové heslo, které musí odpovídat kvalitě hesla definované na tokenu (viz kapitola 4.1).
- 4. Do políčka Potvrdit PIN zopakovat nové heslo.
- 5. Změnu hesla potvrdit tlačítkem OK.

S Nastavení hesla:	×
SafeNet Authentication Client	gemalto [×]
New Digital Signature PIN:	
Nové PIN musí odpovídat nastavením kvality definovaným na tokenu. Bezpečné PIN má aspoň 8 znaků a obsahuje velká písmena, malá písmena, (například !, \$, #, %).	číslice a zvláštní znaky
Aktuální jazyk: CS Zadeite nové PIN.	
	DK Cancel



7.7. Odstranění dat

7.7.1. Odstranění certifikátu

Při obnově certifikátu může dojít k chybě 622. Tato chyba může znamenat, že na tokenu již není místo pro další certifikát. Na tokenu mohou být uložené maximálně 2 kvalifikované certifikáty v CC úložišti a 2 certifikáty s klíčem o velikosti 4096 bitů v běžném úložišti.

Pro vyčištění spusť te program iSignum, vyberte záložku s tokenem a stiskněte tlačítko Vyčistit.

🌖 iSignum		– 🗆 X
Νονý	Na této záložce máte k dispozici přehled všech certifikátů PostSignum, které jsou nainstalovány v úložišti Token Jedná se o kvalifikovaný prostředek pro vytváření elektronických podpisů odpovídající nařízení EIDAS č. 910/2014 (Příloha II).	ignum
Obnovit	Přehled Certifikáty 🔘 Windows 🔵 Token	
Importovat	Obsazené místo: 9 z 32 KB (30%)	Vyöstit Stažení certifikátu
Nápověda a o aplikaci	Jméno Sériové č. Platnost Zbývá Vydavatel 11.08.2020 197 dní PostSignum Qua 08.10.2020 255 dní PostSignum Publ	Typ lified Kvalifikovaný osobní lic CA 3 Komerční osobní
Česká pošta		
► d i g n i t a	Detail	

Vyberte certifikát, který chcete odstranit a stiskněte tlačítko Odstranit.

Průvodce vyčištěním token	L		×
	Tento průvodce Vás provede pro Na tokenu jsou nyní tyto certifika	ocesem vymazání neplatných certi áty, které je možno odstranit:	fikátů z USB tokenu.
	Odstranit: Jméno: Vydavatel: PostSignum Qualifie	Sériové č: Typ: ed CA 3 Kvalifikovan	Platnost: 11.08.2020 10:07 ý osobní
	Odstranit: Jméno: Vydavatel: PostSignum Public (Sériové č: Typ: CA 3 Komerční os	Platnost: 08.10.2020 10:27 obní
		Odstranit	Zavřít

Pokud se na tokenu již nenachází žádný certifikát k odstranění a chyba 622 přetrvává, můžete zkusit odstranit nepřiřazené klíče, viz následující kapitola.



7.7.2. Odstranění klíče

Chyba 622 může být rovněž způsobena tím, že na tokenu jsou uloženy klíče, které nebyly spárovány s certifikátem. Tyto klíče lze odstranit v programu iSignum v expertním módu (přepnutí do tohoto módu viz kapitola 4.8).

POZOR! Tato operace může zapříčinit chybnou instalaci certifikátu, provádějte ji vždy s rozmyslem a až po instalaci všech vydaných certifikátů.

Pro vyčištění stiskněte tlačítko Vyčistit.

Nepřiřazené klíče budou označené jako *Klíč bez certifikátu.* Tyto klíče můžete označit k odstranění a stisknout tlačítko **Odstranit**.

	Průvodce vyčištěním	tokenu	×
Tento prů V úložišti které je m	vodce Vás provede proc ožno odstranit.	esem vymazání certifikátů a klíčů uložených v úl	ožišti 7 a klíče,
Odstranit:	^{Jméno:} Testovací Žadatel ^{Vydavatel:} PostSignum Qua lifi	Sériové č.: Platnost: 22836314 13.02.2026 15: Typ: Kvalifikovaný osobní	^
Odstranit:	Jméno: iSiqnum 2022082 Vydavatel:	Sériové č.: Platnost: Typ: Klíč bez certifikátu	
		Odstranit	~
			Zavřít

Následně budete vyzvání k potvrzení operace a k zadání PINu k tokenu.

Upozorňujeme, že odstranění klíčů může trvat až 5 minut.



7.8. Změnit název tokenu

Touto volbou lze změnit jmenovku tokenu, kterou se bude token identifikovat. Do názvu doporučujeme zadávat text bez diakritiky, mezer a speciálních znaků.

Přejmenování tokenu				
SafeNet Authenticatior	n Client			gemalto
Nový název tokenu:	 Aktuální jazyk:	CS		
Tento název použijte k identifikaci tokenu.				
			OK	Cancel

7.9. Náhled certifikátu

Dojde k zobrazení detailu vybraného certifikátu.

7.10. Nastavení klienta

SafeNet Authentication Client Tools			
		genalto security to be free	
SafeNet Authen	tication Client	🏶 😳 i ? 💼	
SafeNet Authentication Client Tools SafeNet Authentication Client	Kvalita hesla Upřesnit Minimální délka (znaky): Maximální délka (znaky): Maximální doba používání (dny): Maximální doba používání (dny): Doba varování ohledně vypršení (dny): Doba varování ohledně vypršení (dny): Velikost historie: Maximální počet následných opakování: Musí splňovat požadavky na složitost: Ruční nastavení složitosti Velká písmena: Povolit	6 ★ 16 ★ 0 ★ 0 ★ 0 ★ 10 ★ 3 ★ Alespoň 3 typy ★ Hožit Zrušit	
⊖ GEMALTO.COM			



SafeNet Authentication Client Tools		
		gemalto security to be free
SafeNet Authent	ication Client	🏶 💁 i ? 🔒
 SafeNet Authentication Client Tools Token Diguzatelské certifikáty Certifikáty CA Osamocené objekty Nastavení Digital Signature PIN Digital Signature PUK Nastavení klienta 	Kvalita hesla Upřesnit V Kopírovat uživatelské certifikáty do místního úložiště) Správa certifikátů CA. Povolit jednotné přihlášení. V Umožnit nastavení kvality heslo po inicializaci tokenu Umožnit nastavení kvality heslo pouze správci Zobrazit ikonu aplikace na hlavním panelu Automaticky odhlásit po nečinnosti tokenu v délce (minuty)	Vždy
		→ GEMALTO.COM

Zde je možné nastavit pravidla pro vytváření PINu, povinné znaky, atp. Nastavení musí být v souladu s kapitolou 4.1.



8. Reinicializace tokenu

8.1. Výmaz servisního klíče

V případě, že dojde k výmazu servisního klíče, je nutné na token nahrát nový servisní klíč, což lze provést pouze na specializovaném pracovišti České pošty. V tomto případě, je nutné postupovat jako při reklamaci, viz kapitola 9. Servisní klíč není potřeba v případě ukončené certifikace nebo v případě generování žádosti o komerční certifikát.

8.2. Předání tokenu jiné osobě

Při vydání prvního certifikátu, jehož soukromý klíč je na tokenu, dochází k vytvoření vazby **osobabezpečný prostředek**, která je evidována v systému certifikační autority a kontrolována při vydávání dalších (následných) certifikátů do zařízení.

Pokud je nutné tuto vazbu změnit (např. z důvodu předání tokenu jinému žadateli), je nutné postupovat následovně:

- 1. Zneplatnit certifikáty původního žadatele uložené na tokenu.
- 2. Provést zrušení vazby osoba- bezpečný prostředek, to lze provést dvěma způsoby.
- a. Pověřená osoba v Zákaznickém portálu PostSignum v sekci Certifikáty → Správa žadatelů → Zrušení vazby osoba- bezpečný prostředek provede zrušení vazby.

Vyplňte jeden z údajů a stiskněte tlačítko **Vyhledat žadatele**. Následně bude zobrazen výsledek vyhledávání.

Přihlášená osoba	» <u>Úvodní stránka</u> » <u>Certifikáty</u> » <u>Správa žadatelů</u> » Zrušení vazby osoba-kvalifikovaný prostředek		
Jméno: Číslo smlouvy:	Zrušení vazby osoba/kvalifikovaný prostředek	POST SIGNUA	
Codhlásit Přístupové údaje			
Navigace	Jméno žadatele:	0	
•	Číslo zaměstnance:		
Casová razítka			
Balíčky časových razítek	prostředku:		
Certifikáty	Vyhledat žadatele		
Statistiky certifikátů			
Přehledy			
🔲 Správa žadatelů			
Zneplatnění certifikátu			
Zavedení nového žadatele o certifikát			
Nové údaje pro vydání certifikátu již zavedeného žadatele			
Změna údajů zavedeného žadatele o certifikát			
Blokace zavedeného žadatele			
Zrušení vazby osoba-kvalifikovaný prostředek			
Komerční doménový certifikát			
Ověření identity osoby			



Pokud byly všechny certifikáty původního žadatele uložené na tokenu zneplatněny, zobrazí se tlačítko **Odeslat požadavek na zrušení vazby**.

Přihlášená osoba	» <u>Úvodní stránka</u> » <u>Certi</u>	fikáty » <u>Správa žadatelů</u> » Zrušení vazby osoba-kvalifikovaný prostředek	
Jméno: Číslo smlouvy:	Zrušení vazby	POST SIGNUM	
<u>Odhlásit</u> <u>Přístupové údaje</u>			~
Navigace	Jméno žadatele:		Θ
	Číslo zaměstnance:		
Casová razitka	Číslo bezpečného		
Balíčky časových razítek	prostředku:		
Certifikáty	Vyhledat žadatele		
Statistiky certifikátů			
Přehledy	Detail žadatele o cert	ifikát – číslo smlouvy:	
🔲 Správa žadatelů			
Zneplatnění certifikátu	Jméno		
Zavedení nového žadatele o certifikát	Číslo zaměstnance	11192	
Nové údaje pro vydání certifikátu již zavedeného žadatele	Číslo bezpečného prostředku		
Změna údajů zavedeného žadatele o			
certifikát	Odeslat požadavek na z	rušení vazby	
Blokace zavedeného žadatele			
Zrušení vazby osoba-kvalifikovaný prostředek	✓ <u>Zpět</u>		
Komerční doménový certifikát			

Po stisku tlačítka se zobrazí: Požadavek na zrušení vazby byl úspěšně odeslán.

b. V případě, že nemá zákazník zřízen přístup do Zákaznického portálu, nebo se jedná o nepodnikající fyzickou osobu, je nutné oznámit zrušení vazby osoba- bezpečný prostředek certifikační autoritě elektronicky podepsaným e-mailem (elektronický podpis musí být založený na osobním certifikátu PostSignum)

Před odesláním e-mailu se ujistěte, že jsou zneplatněny certifikáty žadatele, kterému má být vazba zrušena.

Vzor e-mailu:

Adresát: certifikaty.postsignum@cpost.cz

Předmět: Zrušení vazby osoba-bezpečný prostředek

Tělo: Oznamuji zrušení vazby osoba-bezpečný prostředek. Jméno osoby: xxx Sériová čísla certifikátů uložených na prostředku: xxx (nebo výrobní číslo prostředku):



9. Reklamace

V případě reklamace je nutné provést níže uvedené kroky:

- 1. Vymazat z tokenu veškeré uživatelské certifikáty, aby nemohlo dojít k jejich zneužití.
- 2. Nastavit na tokenu tovární hodnoty PIN, QPIN, PUK a QPUK, aby bylo možné na tokenu vygenerovat nový servisní klíč.

PIN: 12345678

QPIN: 12345678

PUK: 87654321

QPUK: 87654321

3. Token spolu s reklamačním listem (ke stažení na webových stránkách PostShopu České pošty – www.postshop.cz) zaslat na adresu:

Česká pošta, s.p. Postshop ČP Ortenovo nám. 542/16 211 11 Praha 7

Pokud nebudou provedeny kroky 1 a 2, nebude možné na token vygenerovat nový servisní klíč.