

JAK A KDE ZÍSKÁM OVLÁDACÍ SOFTWARE KARTY KB QSCD?

Instalační balíčky pro všechny podporované platformy operačních systémů jsou dostupné na https://www.kb.cz/karta. Pro OS Windows jsou k dispozici jazykové lokalizace (v současné době čeština [CZ] anebo angličtina [EN]).

JE MOŽNÉ UKLÁDAT NA KARTU KB QSCD CERTIFIKÁTY RŮZNÝCH CERTIFIKAČNÍCH AUTORIT?

Na kartu nelze ukládat certifikáty různých certifikačních autorit, je vyhrazena a použitelná pouze pro certifikáty vydávané Komerční bankou, a.s. Kapacita karty KB QSCD je dostatečná, takže držitel může mít na své kartě uloženy všechny své klíče s certifikáty. Klíče jsou chráněny hodnotou PIN, klíče spojené s kvalifikovaným certifikátm v QSCD režimu pak QPINem

KOLIK CERTIFIKÁTŮ JE MOŽNÉ NA KARTU ULOŽIT?

Karty KB QSCD dodávány s úložnou kapacitou pro

• RSA klíčů 2048 bitů 10x

Karty KB QSCD dodávány s úložnou kapacitou pro

- RSA klíčů/kvalifikovaných max 4096 bitů 2x
- RSA klíčů/komerčních max 4096 bitů 2x
- ECC klíčů/kvalifikovaných max 521 bitů 2x
- ECC klíčů/komerčních max 521 bitů 2x

Správce karty ProID+		- 0	×
Gemplus US8 Smart Card Reader 0 9203803017350008 9- & 41349ec7-15a2-4c23-8eaa-a00a91 9- & te-Spri00e1vcecentifiki00e1ti016f	SPRÁVCE KARTY © čipová karta	Pro ID +	^
ellee8b6-4a09-4eef-b09b-51dfd	Číslo karty:	9203803017350008	
	Počet pokusů zadání PINu akt./nast.[max. nast]: Počet pokusů zadání PUKu akt./nast. [max. nast]:	3/3 [3] 5/5 [5]	
	Počet pokusů zadání podpisového PINu akt./nast. [max. nast]:	3/3 (3) (změnit) (odblokovat)	
	Počet kontejnerů použitých/celkem:	6/16	
	Počet RSA 4096b. klíčů (použitých/celkem):	0/4	
	Počet RSA 2048b. klíčů (použitých/celkem):	6/6	
	Počet EC 521b. klíčů (použitých/celkem):	0/6	
	Volný prostor:	> 32 k8	
	CPIN ZMÉNA PINU CPUK ZMÉNA PUKI	U ODBLOKOVÁNÍ 🚔 IMPORT KLÍČE PINU	
< >>			~

Detailní informace o zaplnění karty lze zobrazit pomocí aplikace Správce karty, kde se po označení karty ve stromové struktuře levého panelu zobrazí v pravém panelu příslušné informace.



JAK MOHU ZJISTIT, CO JE NA KARTĚ ULOŽENO?

Obsah karty KB QSCD lze zobrazit pomocí aplikace Správce karty. Po spuštění aplikace je třeba načíst obsah karty tlačítkem Obnovit, popř. funkční klávesou F5. Karta musí být po celou dobu načítání informací zasunuta ve čtečce.

V levém panelu Správce karty se zobrazí v přehledné stromové struktuře důležité objekty:

- Čtečka čipových karet identifikovaná jejím názvem a pořadovým číslem
- Karta KB QSCD identifikovaná číselným označením karty
- Uživatelské objekty na kartě se vážící certifikát

Správce karty ProID+		- 🗆 ×
<u>S</u> oubor <u>Z</u> obrazení <u>N</u> ápověda		
Gemplus USB Smart Card Reader 0 9203803018460193 ProID+ Q9203803018460193-0-5965-9609dd3f ProID+ Q9203803018460193-3-06b0-6942e741 Q Certifikat ProID+ Q9203803018460193-2-7th5-cef7a94d	SPRÁVCE KARTY ())))))))))))))))))))))))))))))))))))	^ ProID →
Certifikát	Počet pokusů zadání PINu akt./nast.[max. nast]: Počet pokusů zadání PUKu akt./nast. [max. nast]:	3/3 [3] 5/5 [5]
Certifikát	Počet pokusů zadání podpisového PINu akt./nast. [max. nast]:	3/3 [3] (<u>zménit) (odblokovat)</u>
PS-VCA-20190128130822	Počet kontejnerů použitých/celkem: Počet RSA 2048b. klíčů (použitých/celkem):	7/16 7/7
PS-QCA-20190131095835	Počet RSA 4096b. klíčů (použitých/celkem): Počet EC 521b. klíčů (použitých/celkem):	0/3 0/6
	Volný prostor:	> 32 k8
	CPIN ZMÉNA PINU CPUK ZMĚNA PUK	U ODBLOKOVÁNÍ 🚔 IMPORT KLÍČE PINU
	ⓒ MONET+ , a.s. všechna práva vyhrazena ProID+ ® je reg	istrovanou ochrannou známkou produktu. <u>proid.cz/podpora</u>

Jednotlivé objekty lze zvolit pomocí myši a získat tak detailnější informace, které jsou zobrazeny v pravém panelu aplikace.

Aplikaci Správce karty najdete v adresáři c:\Program files\Cryptoplus\KB QSCD. Na operačním systému MacOS najdete správce karty pod názvem "Správce karty".

JE MOŽNÉ CERTIFIKÁT Z KARTY VYMAZAT?

Aplikace KB spravují certifikáty na kartě samy. Neměli byste mít potřebu manuálně zasahovat do karty a nedoporučujeme jakkoliv zasahovat do obsahu karty bez konzultace nebo přímého pokynu od bankovního poradce nebo Kontaktního centra.

LZE Z KARTY EXPORTOVAT KLÍČ S CERTIFIKÁTEM?

Soukromý klíč nelze z karty exportovat ani kopírovat; to je základní bezpečnostní vlastnost karty KB QSCD.



Certifikát (s veřejným klíčem) lze z karty exportovat pomocí aplikace Správce karty. V levé části okna se zvolí certifikát k exportu a v pravé části se použije volba Export do souboru.

Správce karty ProID+		- 🗆 ×
Soubor Zobrazení <u>N</u> ápověda		
Soubor Zobrazeni Nápovéda Gemplus USB Smart Card Reader 0 9203903016161004 Gemplus USB Smart Card Reader 0 9203903016161004 Gemplus Les-Spri00e Ivecentifiki00e1ti011 9 Certifikát 1 e-Spri00e Ivecentifiki00e1ti011 9 Certifikát 1 e-Spri00e Ivecentifiki00e1ti011 9 Certifikát 1 e-Spri00e Ivecentifikát 1 e-Spri00e Ivecentifikát 1 e-Spri00e Ivecentifikát 1 e-Spri00e Ivecentifikát 1 e-CardManageStart-995b4f15	SPRÁVCE KARTY © CERTIFIKÁT Sériové číslo: 2200000433D362DEA30FD27A82000 Platnost: 15:59, 31,10,2018 - 15:59, 30,10,202 Vydavatek CZ, MVCR, MVCR-CA Subjekt: Ioc, mvcr, PKJ, Libor User Verze: 3	ProID →
Certifikát	SHA1: 683E31B3 C7A27573 D3D417AA 7E5	54CEF8 FB1DDDEE
	 Cesta k certifikátu ovéřena. Certifikát je zaregistrován v systému, lze ho odregistrovat. Certifikát je zaregistrován v systému, lze ho odregistrovat. Rozšíření certifikátu: Použit kliče Digitalní podpis, Neodvolatelnost, Šifrování kliče Rozšířené použit kliče Smartzard logon Enrollment agent VÍCE INFORMACÍ VÍCE INFORMACÍ VÍCE INFORMACÍ MONET-, s.s. všechna práva vyhrazena 	ODREGISTROVÁNÍ CERTIFIKÁTU
<	⑥ MONET+ , a.s. všechna práva vyhrazena ProlD+® je registrovanou ochrannou známkou produktu. g	proid.cz/podpora

V dalším kroku se zvolí umístění a název souboru a export se provede použitím tlačítka Uložit.

JE MOŽNÉ Z KARTY VYMAZAT KLÍČ S CERTIFIKÁTEM?

Viz dotaz JE MOŽNÉ CERTIFIKÁT Z KARTY VYMAZAT?

JE MOŽNÉ NA KARTU IMPORTOVAT CERTIFIKÁT ULOŽENÝ V SOUBORU?

Pomocí aplikace Správce karty je možné na kartu KB QSCD nelze importovat certifikát společně ani soukromým klíč.

JE MOŽNÉ ZMĚNIT KÓD PIN, QPIN A PUK KARTY?

Změna kódu PIN pomocí aplikace Správce Karty

Změnu kódu PIN je možné provést pomocí aplikace Správce karty. Změna PINu je podmíněna znalostí současné (původní) hodnoty.

V levém panelu se zvolí objekt karty a v pravém panelu se použije tlačítko Změna PINu.



ProiD+		– 🗆 X
<u>S</u> oubor <u>Z</u> obrazení <u>N</u> ápověda		
Gemplus USB Smart Card Reader 0 9203803018460193 ProlD+ Q9203803018460193-0-1 ProlD+ Q9203803018460193-3-1 ProlD+ Q9203803018460193-3-1 ProlD+ Q9203803018460193-2-1	SPRÁVCE KARTY ()) ČIPOVÁ KARTA	Pro ID ≁
	Číslo karty:	9203803018460193
	Počet pokusů zadání PINu akt./nast.[max. nast]: Počet pokusů zadání PUKu akt./nast. [max. nast]:	3/3 [3] 5/5 [5]
PS-VCA-20190131095835	Počet pokusů zadání podpisového PINu akt./nast. [max. nast]:	3/3 (3) (změnit) (odblokovat)
	Počet kontejnerů použitých/celkem:	7/16
	Počet RSA 2048b. klíčů (použitých/celkem):	7/7
	Počet RSA 4096b. klíčů (použitých/celkem):	0/3
	Počet EC 521b. klíčů (použitých/celkem):	0/6
	Volný prostor:	> 32 kB
	CPIN ZMÉNA PINU CPUK ZMÉNA PUK	KU ODBLOKOVÁNÍ 🚔 IMPORT KLÍČE PINU
<	(○ MONET+ , a.s. všechna práva vyhrazena ProID+ [®] je regi	strovanou ochrannou známkou produktu. <u>proid.cz/podpora</u>

Dále se zobrazí dialog Změna uživatelského PINU.

Do pole PIN se zadá původní hodnota PINu, do pole Nový PIN se zadá nová hodnota PINu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PIN.

Správce karty ProID+		- 🗆 ×
Soubor Zobrazení <u>N</u> ápověda		
Source karly ProU- Source karly ProU- Source karly ProU- Source karly ProU- ProU-	SPRÁVCE KARTY © ZMĚNA UŽIVATELSKÉHO PINU ••••• PIN ••••• Nový PIN ••••• Nový PIN zopakovaný	ProID +
	Cardenit maximální počet pokusů Composition Nový maximální počet pokusů Cardenit Composition Composit	



Změna kódu QPIN (podpisový PIN) pomocí aplikace Správce Karty

Změnu kódu QPIN je možné provést pomocí aplikace Správce karty. Změna QPINu je podmíněna znalostí současné (původní) hodnoty.

- 1. V levém panelu se zvolí objekt karty
- 2. Po kliknutí na tlačítko Více informací se zpřístupní Informace o Počtu pokusů zadání podpisového pinu. Je zde k dispozici tlačítko Změnit
- 3. Tlačítko Změnit vyvolá dialog Změna podpisového pinu (QPINu).

Frain Správce karty ProlD+	-	
<u>Soubor</u> Zobrazení <u>N</u> ápověda		
Soubor Zobrazni Niyovéda Gemplus USB Smart Card Reader 0 9203803018460193 1. ProID+ Q9203803018460193-0-! ProID- Q9203803018460193-0-! ProID- Q9203803018460193-0-! ProID- Q9203803018460193-2-: ProID- Q92038000-2-: ProID- Q9203800-2-: ProID- Q9203800-2-: ProID- Q9204	SPRÁVCE KARTY ProID →	
< >>	ZMÉNA PINU CPUR ZMÉNA PUKU ODBLOKOVÁNÍ IMPORT KLÍČE VÍCE INFORMACÍ 2. MONET+ , a.s. všechna práva vyhrazena ProID+® je registrovanou ochrannou známkou produktu. <u>proid.cz/podpora</u>	v

Dále se zobrazí dialog Změna podpisového PINU

Do pole PIN se zadá původní hodnota PINu, do pole Nový PIN se zadá nová hodnota PINu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PIN.



Správce karty ProID+		- 0	×
<u>S</u> oubor <u>Z</u> obrazení <u>N</u> ápověda			
Soubor Zobrazeni Nápovéda Gemplus USB Smart Card Reader 0 9203803018460193 ProlD - Q9203803018460193-0-1 ProlD - Q9203803018460193-0-1 ProlD - Q9203803018460193-0-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-2-1 ProlD - Q9203803018460193-10254 ProlD - Q920380301846019310822 ProlD - Q9201281012810822 ProlD - Q920280030184601931095835 ProlD - Q920280030184601931095835 ProlD - Q92038030184601931095835	Správce karty Demonstrative produktov poločeho pinu Demonstrative pin Demon	ID ≁	
< >			~

Změna maximálního počtu pokusů zadání hodnoty kódu Podpisového PINu (QPIN) není u karet KB QSCD možná.

Změna kódu PUK pomocí aplikace Správce Karty

Změnu kódu PUK je možné provést pomocí aplikace Správce karty. Změna PUKu je podmíněna znalostí současné (původní) hodnoty.

V levém panelu se zvolí objekt karty a v pravém panelu se použije tlačítko Změna PUKu.





Dále se zobrazí dialog Změna PUKU.

Do pole PUK se zadá původní hodnota PUKu, do pole Nový PUK se zadá nová hodnota PUKu. Novou hodnotu je nutné – pro kontrolu – zopakovat v poli Nový PUK zopakovaný. Po stisku tlačítka Změnit se provede požadovaná změna hodnoty PUK.

ProiD+	- 0	×
<u>S</u> oubor <u>Z</u> obrazení <u>N</u> ápověda		
Gemplus USB Smart Card Reader 0		^
<u>9203803018460193</u>		
ProID+Q9203803018460193-0-5	SPRAVCE KARTY ProID +	
⊞ E ProID+Q9203803018460193-3-(ZMĚNA UŽIVATELSKÉHO PUKU	
ProID+Q9203803018460193-2-2		
B	PUK	
	Nový PUK	
PS-QCA-20190131095835	Nový PUK zopakovaný	
PS-VCA-20190131095835	Změnit maximální počet pokusů	
	0 Nový maximální počet pokusů	
	Změnit	
	🕞 Zpět na kartu	
< >		~



ZTRATIL/ZAPOMNĚL JSEM PIN K ČIPOVÉ KARTĚ KB QSCD

PIN (Personal Identification Number) je sada alfanumerických znaků, která autorizuje přístup k chráněným objektům na kartě (soukromých klíčů). Bez znalosti PINu nelze kartu použít (ani zneužít).

V případě ztráty nebo zablokování PINu lze na kartě nastavit novou hodnotu kódu PIN. Tuto operaci je však nutné autorizovat. Autorizaci lze provést:

1. Kódem PUK (Pin Unblocked Key) – dodaným uživateli spolu s kartou KB QSCD

Nový PIN lze nastavit např. v aplikaci Správce karty.

Odblokování kódu PIN – nastavení nové hodnoty kódu PIN pomocí kódu PUK ve Správci karty

Po načtení karty ve Správci karty (tlačítko Obnovit/F5)se v levém panelu označí karta. V pravém panelu se stiskne tlačítko Odblokování PINu. Do pole **PUK** se zadá hodnota kódu PUK, dodaného k čipové kartě. Do pole **Nový PIN** se zadá nová hodnota kódu PIN. Novou hodnotu je nutné pro kontrolu zopakovat v poli **Nový PIN zopakovaný.**





Správce karty ProID+			- 0	×
Soubor Zobrazení Nápověda				
Soubor Zobrazeni Nápovéda Gemplus USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 92030017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 920300017350008 920300017350008 Image: Complex USB Smart Card Reader 0 92030017350008 92030017350008 Image: Complex USB Smart Card Reader 0 92030017350008 92030017350008 Image: Complex USB Smart Card Reader 0 92030017350008 9203001735008 Image: Complex USB Smart Card Reader 0 9203001735008 9203001735008 Image: Complex USB Smart Card Reader 0 9203001735008 9203001735008 Image: Complex USB Smart Card Reader 0 9203001725008 9203001735008	SPRÁVCE KA DOBLOKOVÁNÍ Odblokování podpisového PlNu pom PlN můžete odblokovat. Pro změnu ji jednoduchou posloupností - např. D 	RTY nori PUKu je třeba znát PUK a zadat novou bezpečnou hodnotu PINu. PIN t 000°. 1234°, apod. PUK Nový PIN Nový PIN Nový PIN zopakovaný usů počet pokusů	ProID +	~
٤				~

ZTRATIL/ZAPOMNĚL JSEM PODPISOVÝ PIN (QPIN) K ČIPOVÉ KARTĚ KB QSCD

PIN (Personal Identification Number) je sada alfanumerických znaků, která autorizuje přístup k chráněným objektům na kartě (soukromých klíčů). Bez znalosti PINu nelze kartu použít (ani zneužít).

Podpisový PIN pro kvalifikované elektronické podpisy (QPIN) – slouží ke schvalování kvalifikovaného elektronického podpisu.

Používá se při každém vytváření kvalifikovaného elektronického podpisu.

V případě ztráty nebo zablokování QPINu lze na kartě nastavit novou hodnotu kódu QPIN. Tuto operaci je však nutné autorizovat. Autorizaci lze provést:

• Kódem PUK (Pin Unblocked Key) – dodaným uživateli spolu s kartou KB QSCD

Nový QPIN lze nastavit např. v aplikaci Správce karty.

Odblokování kódu QPIN – nastavení nové hodnoty kódu QPIN pomocí kódu PUK ve Správci karty

Odblokování kódu QPIN je možné provést pomocí aplikace Správce karty.

- 1. V levém panelu se zvolí objekt karty
- 2. Po kliknutí na tlačítko Více informací se zpřístupní Informace o Počtu pokusů zadání podpisového pinu. Je zde k dispozici tlačítko Odblokovat
- 3. Tlačítko Odblokovat vyvolá dialog Odblokování podpisového PINU.

- KB

I

ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

France karty ProID+		– 🗆 X
Soubor Zobrazení Nápověda		
Gemplus USB Smart Card Reader 0 9208803017350000 1 0 0 0 0 0 0 0 0 0 0 0 0 0	SPRÁVCE KARTY (1) ČIPOVÁ KARTA	^ Pro ID ≁
	Císlo karty:	9203803017350008
6cf09736-face-4225-989f-687817	Počet pokusů zadání PINu akt./nast.[max. nast]:	2/3 [3]
cc348733-d2ee-4fb2-83a0-ce3ed	Počet pokusů zadání PUKu akt./nast. [max. nast]:	5/5 [5]
	3 Počet pokusů zadání podpisového PINu akt./nast. [max. nast]:	3/3 (3) (změnit) odbiokovat)
	Počet kontejnerů použitých/celkem:	6/16
	Počet RSA 4096b. klíčů (použitých/celkem):	0/4
	Počet RSA 2048b. klíčů (použitých/celkem):	6/6
	Počet EC 521b. klíčů (použitých/celkem):	0/6
	Volný prostor:	> 32 kB
	CPUN ZMÉNA PINU CPUK ZMÉNA PUI	KU ODBLOKOVÁNÍ 🚔 IMPORT KLÍČE
	2 VÍCE INFORMACÍ	
	O MONET+ , a.s. všechna práva vyhrazena ProID+ [®] je reg	jistrovanou ochrannou známkou produktu. proid.cz/podpora
<		~

Dále se zobrazí dialog Odblokování podpisového PINU

Do pole PUK se zadá hodnota PUKu, do pole Nový PIN se zadá nová hodnota QPIN

Novou hodnotu QPIN je nutné – pro kontrolu – zopakovat v poli Nový PIN zopakovaný. Po stisku tlačítka Odblokovat se provede požadovaná změna hodnoty QPIN.

Správce karty ProID+	- 0	×
Soubor Zobrazeni Napovéda		^
	SPRÁVCE KARTY Pro D +	
æ— ∰ cc348733-d2ee-41b2-83a0-ce3ed	••••••• PUK ••••• Nový PIN ••••• Nový PIN zopakovaný Změnit maximální počet pokusů Ø Nový maximální počet pokusů Odblokovat	
< >		Ŷ



JAK MOHU POUŽÍT KARTU KB QSCD V APLIKACÍCH MOZILLA FIREFOX NEBO THUNDERBIRD?

Webový prohlížeč Mozilla Firefox i poštovní klient Thunderbird mají zabudovanou podporu pro práci s bezpečnostními certifikáty. Jako úložiště klíčů a certifikátů umožňují použít čipovou kartu KB QSCD prostřednictvím standardizovaného modulu PKCS#11 (též nazývaný Cryptoki). Tento modul je součástí standardního instalačního balíčku a má formu dynamicky linkované knihovny (DLL). Jeho jméno je proidcm11.dll a je instalován do systémového adresáře.

Modul přidaný v aplikaci Mozilla Firefox není automaticky dostupný v Thunderbird a naopak. Pro každou aplikaci je nutné registrovat modul samostatně.

Před použitím je nutné modul zaregistrovat. To lze provést v menu příslušné aplikace.

- Firefox: Nástroje Možnosti Soukromí a zabezpečení Certifikáty Bezpečnostní zařízení.
- Thunderbird: Nástroje Možnosti Rozšířené Certifikáty Bezpečnostní zařízení.



Správce bezpečnostních zařízení zobrazuje seznam všech registrovaných modulů. Další modul lze přidat stiskem tlačítka **Načíst**. Do pole **Jméno modulu** se vyplní libovolný název (např. KBQSCD). Do pole **Název souboru modulu** se zapíše proidcm11.dll. V případě použití karty KB QSCD použijte soubor proidqcm11.dll.

Načíst ovladač PKCS#11 zařízení –		□ ×	
Zadejte informace o moo	dulu, který chcete přidat.		
Název modulu Nový modul PKCS#11			
<u>N</u> ázev souboru modulu	System32\proidqcm11	Procházet	
	ОК	Zrušit	

Alternativně lze modul vybrat pomocí tlačítka Procházet v systémovém adresáři (standardně C:\Windows\System32).

Po stisku tlačítka OK aplikace zobrazí modul KB QSCD P11 ve stromu informuje o výsledku přidání modulu.



	Správce bezpečnostních zařízení			×
			_	
Bezpečnostní moduly a zařízení	Podrobnosti	Hodnota	<u>P</u> řihlásit	
 NSS Internal PKCS #11 Module 	Stav	Nepřihlášeno	Odhlásit	
Obecné šifrovací služby	Popis	Gemplus USB Smart Card Reader 0	Oumasic	
Softwarové bezp. zařízení	Výrobce	Gemplus	Změnit <u>h</u> eslo	
∽ eOP PKCS#11	Verze HW	0.0	<u>N</u> ačíst	
Gemplus USB Smart Card Reader 0	Verze FW	0.0	Uvolnit	
v EOP DLL eopczep11.dll Nový modul PKCS#11	Označení	ProID+Q 9203803017350008	Ovonint	
Gemplus USB Smart Card Reader 0	Výrobce	Monet+,a.s.	Povolit <u>F</u> IPS	
 Vestavěný kořenový modul 	Sériové číslo	9203803017350008		
NSS Builtin Objects	Verze HW	1.0		
∽ ProID+Q	Verze FW	4.4		
Gemplus USB Smart Card Reader 0				
			ОК	

Použitím volby Přihlásit a vložením kódu PIN se stav modulu změní na Přihlášen.

I

Bezpečnostní moduly a zařízení	Podrobnosti	Hodnota	<u>P</u> řihlásit
 NSS Internal PKCS #11 Module 	Stav	Přihlášeno	Odblásit
Obecné šifrovací služby	Popis	Gemplus USB Smart Card Reader 0	Outliasit
Softwarové bezp. zařízení	Výrobce	Gemplus	Změnit <u>h</u> eslo
✓ eOP PKCS#11	Verze HW	0.0	Načíst
Gemplus USB Smart Card Reader 0	Verze FW	0.0	Uvolnit
EOP DLL eopczep11.dll Nový modul PKCS#11	Označení	ProID+Q 9203803017350008	Ovonint
Gemplus USB Smart Card Reader 0	Výrobce	Monet+,a.s.	Povolit <u>F</u> IPS
 Vestavěný kořenový modul 	Sériové číslo	9203803017350008	
NSS Builtin Objects	Verze HW	1.0	
✓ ProID+Q	Verze FW	4.4	
Gemplus USB Smart Card Reader 0			

Správce bezpečnostních zařízení se uzavře stiskem tlačítka OK. Tímto je aplikace připravena k používání karty KB QSCD.

FIREFOX/THUNDERBIRD HLÁSÍ, ŽE CERTIFIKÁT NENÍ DŮVĚRYHODNÝ

Zjednodušeně lze říci, že certifikát je pro danou aplikaci důvěryhodný, pokud je certifikát certifikační autority uveden v seznamu důvěryhodných certifikátů a nastaven příznak důvěryhodnosti pro danou množinu použití. Mozilla Firefox ani Thunderbird nepoužívají úložiště certifikátů Windows, proto je nutné importovat certifikáty certifikačních autorit do



jejich lokálních úložišť. Každá z aplikací si spravuje tato úložiště samostatně. Import certifikátu do úložiště Firefox neovlivní obsah úložiště Thunderbird a naopak.

JAK NAIMPORTUJI CERTIFIKÁT CERTIFIKAČNÍ AUTORITY DO ÚLOŽIŠTĚ APLIKACÍ MOZILLA FIREFOX NEBO THUNDERBIRD?

Import certifikátů certifikační autority lze provést v menu příslušné aplikace:

- Firefox: Nabídka Nástroje Možnosti Rozšířené Certifikáty
- Thunderbird: Nabídka Úpravy Předvolby Rozšířené Certifikáty Certifikáty

Zobrazí se okno s názvem Správce certifikátů. Vybere se záložka Autority a stiskněte tlačítko Importovat.

				Správce ce	rtifikátů	
Osobní	Lidé	Servery	Autority			
Pro identifikaci	certifikad	čních autorit	jsou dostupné t	yto certifikáty		
Jméno certifik	cátu				Bezpečnostní zařízení	E.
✓ AC Camerfir	ma S.A.					^
Chambers	of Com	merce Root -	2008	B	uiltin Object Token	
Global Ch	ambersig	n Root - 200	8	B	uiltin Object Token	
Camerfirm	na Corpo	rate Server II	- 2015	S	oftwarové bezp. zařízení	
✓ AC Camerfir	ma SA CI	F A82743287	,			
Camerfirm	na Chaml	pers of Comr	nerce Root	B	uiltin Object Token	
Camerfirm	na Global	Chambersig	n Root	B	uiltin Object Token	
~ ACCV						~
Zo <u>b</u> razit	Upr <u>a</u> vi	t důvěru	lmportovat	E <u>x</u> portovat	Smazat nebo ne <u>d</u> ůvěřovat	
						OK
						UK

V počítači vyhledejte soubor obsahující certifikát vydávající certifikační autority, označte jej a stiskněte tlačítko Otevřít.

Vyberte soubor obsahující certifikát(y) CA pro import	×
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \ll PKI \Rightarrow Certifikaty \Rightarrow \checkmark \Diamond	ව Prohledat: Certifikaty ා
Uspořádat 🔻 Nová složka	III 🔹 🕶 🔲 😲
 ConeDrive Tento počítač 3D objekty Dokumenty Hudba Obrázky Plocha Stažené soubory Videa Místní disk (C:) 	Datum změny Typ 30.10.2018 14:21 Složka soub 04.02.2019 12:39 Složka soub 04.02.2019 12:39 Certifikát za
➡ Temp (\\mbox.n ➡ jdalecky (\\mbo:	
Síť V K <u>N</u> ázev souboru: root3	 ✓ Soubory s certifikáty ✓ <u>O</u>tevřít Zrušit

Před potvrzením importu certifikátu se současně zvolí účel, pro který je certifikát důvěryhodný.

Stažení certifikátu	×
Byli jste požádáni o uznání nové Certifikační Autority (CA).	
Chcete důvěřovat "ACAelD3 - Root Certificate" pro následující účely?	
🗌 Uznat tuto CA pro identifikaci serverů.	
🗹 Uznat tuto CA pro identifikaci uživatelů pošty.	
Před uznáním této CA, a to pro jakýkoliv účel, byste měli prozkoumat její certifikát, její pravidla a podmínky (pokud jsou dostupné).	
Zobrazit Zobrazit certifikát CA	
OK Zrušit	



Import se dokončí stiskem tlačítka OK a opět OK. Pokud se používají certifikáty více certifikačních autorit, je nutné postup opakovat pro každou certifikační autoritu zvlášť.

CHCI POUŽÍT KARTU KB QSCD V APLIKACI ADOBE READER

Koncepce použití karty KB QSCD a bezpečnostních certifikátů v Adobe Reader do značné míry kopíruje koncept použití ve Firefox nebo Thunderbird.

Jednotlivé kroky vedoucí ke zprovoznění podpory KB QSCD v Adobe Readeru jsou však mírně odlišné.

Zpřístupnit certifikát lze buď v operačním systému Windows jeho registrací mezi osobní certifikáty prostřednictvím aplikace Správce karty, volnou registrovat certifikát do Windows.

Druhá možnost je registrací PKCS11 modulu.

Ve výchozím nastavení má Adobe Reader zapnut tzv. Chráněný režim. Tento režim omezuje přístup souborů PDF do systému, čímž chrání Windows před škodlivými kódy, které by mohly modifikovat součásti operačního systému. Toto omezení však znemožňuje přístup aplikace k modulu PKCS#11. Pro správnou funkčnost modulu je tedy nutné Chráněný režim deaktivovat. Deaktivace Chráněného režimu může zvýšit riziko infikace systému škodlivým kódem!

V hlavní nabídce se zvolí menu Úpravy – Předvolby – Zabezpečení (Rozšířené) a zruší se zatržení u pole Zapnout po spuštění chráněný režim. Deaktivace se potvrdí stiskem tlačítka Ano. Proces se dokončí stiskem tlačítka OK a restartem aplikace.

ategorie:	Ochrany prostoru zabezpečení (sandbox)	
Dokumenty Na celou obrazovku Přídávání poznámek Všeobecné Zobrazení stránky	Zapnout po spuštění chráněný režim Spustit v konte Chráněné zobrazení © Vypnuto Soubory pocházející z potenciálně nebe Všechny soubory	ejneru (Beta) Uytvořít soubor záznamu <u>c</u> hráněného režimu Zobrazit zázna
D a multimédia Štení Jůvěryhodnost multimédií (starší) - mailové účty ormuláře	Rozšířené zabezpečení 🗹 Povolit rozšířené zabezpečení	<u>Mezidoménový soubor protokolu</u> <u>Zobr</u>
Iledaní dentita nternet avaŠcript azyk controla pravopisu déření (2D) děření (2D) děření (3D) Měření (geoprostorové) Multimédia (starši) Dnline služby Adobe Podpisy Recenzování Jedování právce práv Jsnadnění přístupu Zabezpečení (rozšířené)	Oprávněna umístění Pokud nastavení zabezpečení negativně ovlivňuje vaše pracovní Oprávněná umístění vyberte důvěryhodné soubory, složky a host nastavení zabezpečení obežil. Oprávněná umístění umožňují bez povolení přístupu k pol Automaticky povačo Automaticky důvěro Automaticky důvěro Opravdu chráněného režimu r a kontejnet. Aby se změny pro aplikaci. Opravdu chcete pokračovat? Přídat soubor Přídat cestu ke složce Přídat ho	postupy, pomocí možnosti titele, abyte omezení trzečnou práci a zároveň ovměž vypne chráněné zobrazení ojevity, musite ručně restartovat Amo Ne ostitele Odstranit



I

ČIPOVÁ KARTA QSCD – NÁVODY A NEJČASTĚJI KLADENÉ DOTAZY

Po opětovném spuštění se zvolí v hlavní nabídce Úpravy – Předvolby – Podpisy – Identity a důvěryhodné certifikáty – tl. Další. Zobrazí se okno Nastavení digitálních identifikátorů a důvěryhodných certifikátů. Označí se položka Moduly a tokeny PKCS#11 a stiskne se tlačítko Připojit modul.

<u></u>	Vastavení digitálních identifikátorů a důvěry	nodných certifikátů	×
\sim	Digitální identifikátory	Připojit modul Odpojit modul 🧯	🕑 Obnovit
	Účty cestovních identifikátorů	ldentifikátor výrobce modulu Cesta knihovny	
	Soubory digitálních identifikátorů		
	Digitální identifikátory Windows		
	Moduly a tokeny PKCS#11		
	Důvěryhodné certifikáty	Správa modulů PKCS#11 Toto je seznam načtených modulů PKCS#11. M ziskali přistup k novým šifrovacím zařizením	fůžete načíst další moduly, abyste
			~

V případě karty KB QSCD se v počítači vyhledá soubor mopkcs11.dll. Pokud používáte kartu KB QSCD tak vyhledejte soubor mopkcs11.dll (instaluje se do systémového adresáře, standardně v C:\Windows\System32\) a stiskne se tlačítko Otevřít.

Najît modul PKCS#11						
\leftarrow \rightarrow \checkmark \uparrow Tento počítač \Rightarrow Místní disk (C:) \Rightarrow Windows \Rightarrow System32 \Rightarrow \checkmark \circlearrowright Prohledat: System32						
Uspořádat 🔻 Nová slož	ka			•== •		
System32	Název	Datum změny	Тур	Velikost	^	
a OneDrive	0409	15.09.2018 19:39	Složka souborů			
_	1033	03.10.2018 18:24	Složka souborů			
💻 Tento počítač	AdvancedInstallers	15.09.2018 9:34	Složka souborů			
🧊 3D objekty	af-ZA	19.06.2018 21:54	Složka souborů			
Dokumenty	am-ET	19.06.2018 21:54	Složka souborů			
👌 Hudba	AppLocker	15.09.2018 9:33	Složka souborů			
Obrázky	ar-SA	15.09.2018 19:40	Složka souborů			
Plocha	as-IN	19.06.2018 21:54	Složka souborů			
Ctažané saubany	az-Latn-AZ	14.09.2018 14:40	Složka souborů			
Stazene soubory	be-BY	19.06.2018 21:54	Složka souborů			
Videa	🚽 bg-BG	15.09.2018 19:40	Složka souborů			
🏪 Místní disk (C:)	bn-BD	19.06.2018 21:54	Složka souborů			
🛖 Temp (\\mbox.n	bn-IN	19.06.2018 21:54	Složka souborů			
🛖 jdalecky (\\mbo:	bs-Latn-BA	14.09.2018 14:40	Složka souborů			
×	Bthprops	15.09.2018 9:34	Složka souborů		~	
<u>N</u> ázev s	souboru: proidqcm11.dll		~ Modu	ly PKCS#11 (*.DLI	L) ~	
	<u>O</u> tevřít Zru					

KB

I

Po uzavření okna Nastavení digitálních identifikátorů se stiskne tlačítko OK. Restartuje se aplikace Adobe Reader a poté je třeba znovu otevřít okno Nastavení digitálních identifikátorů, zvolit modul Monet+ MiniDriver PKCS#11 a použít tlačítko Přihlásit se.

🔒 Nastavení digitálních identifikátorů a důvěrył	nodných certifikátů			×
 Digitální identifikátory 	Připojit modul	Odpojit modul	🔁 Obnovit	
Účty cestovních identifikátorů	Identifikátor výrobce mo	dulu Cesta knihovn	y ivstem32\proidacm11.dll	
Soubory digitálních identifikátorů	Monet+,a.s.	C. (Windows)	ystemszyprologenn nan	
Digitální identifikátory Windows				
Moduly a tokeny PKCS#11				
Důvěryhodné certifikáty	Identifikátor vy V V C	ýrobce modulu: Monet Popis modulu: ProID- ferze knihovny: 2.20 7erze Cryptoki: 2.20 festa knihovny: C:\Win	+,a.s. +Q PKCS#11 library ndows\System32\proidqcr	m11.dll
				~



Na vyžádání je třeba přihlásit se k čipové kartě: zadat PIN. Stav tokenu KB QSCD by se pak měl změnit na Přihlášený.

🔒 Nastavení digitálních identifikátorů a důvěry	hodných certifikátů				×
 Digitální identifikátory 	Změnit heslo	Přihlásit se	Odhlásit se	🔁 Obnovit	
Účty cestovních identifikátorů	Popis tokenu	Stav			
Soubory digitálních identifikátorů	ProID+Q 9203803017350	008 Přihláš	iený		
Digitální identifikátory Windows					
Moduly a tokeny PKCS#11			(
> ProID+Q PKCS#11 library		Popis toko	nu: ProID+0 920	3803017350008	~
Důvěryhodné certifikáty	Identifikát	or výrobce modu	l u: Monet+,a.s.	3803017330008	
		Mod	lel: MultiAppID		
		Sériové čís	lo: 92038030173	50008	
					~

Stejně jako v aplikacích Firefox a Thunderbird je nutné provést import certifikátu CA; ve stejném okně je třeba zvolit položku Důvěryhodné certifikáty a provést import certifikátu CA tlačítkem Importovat.

PŘI POKUSU O VLOŽENÍ KVALIFIKOVANÉHO PODPISU NA MACOS SE ZOBRAZÍ CHYBA LIBRARY NOT LOADED: /USR/LOCAL/OPT/LIBPNG/LIB/LIBPNG16.16.DYLIB

Operační systém neobsahuje knihovnu libpng a je nutné ji doinstalovat.

Instalaci je možné provést pomocí správce balíků Homebrew https://brew.sh/index_cs

Příkaz pro instalaci repozitáře Homebrew:

/bin/bash -c "\$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

Příkaz pro instalaci knihovny:

brew install libpng