



# Šifrovanie elektronickej pošty

Príručka používateľa

(AN101011)

December 2011

# Obsah

1 Systémové požiadavky	3
2 Zavedenie bezpečnostného modulu SIPKCS	3
3 Nastavenie dôvery v certifikát koreňovej autority	5
4 Voľba certifikátov pre šifrovanie a podpisovanie správ	8
5 Distribúcia certifikátov	11
6 Zabezpečenie elektronickej pošty	11
6.1 Odoslanie zabezpečenej správy	11
6.2 Príjem zabezpečenej správy	12
7 Zmena prístupového hesla k Tokenu	14
8 Dokumentácia	15

Táto príručka popisuje nastavenie poštového klienta *Thunderbird* pre zabezpečenie dôvernosti a zaručenie integrity elektronickej poštovej komunikácie s využitím hardvérového kryptografického zariadenia *GNT USB Token* od spoločnosti *SoftIdea*. Nastavenie poštového klienta podľa tejto príručky umožní šifrovať a digitálne podpisovať správy elektronickej pošty.

#### 1 Systémové požiadavky

- 1. Operačný systém: Microsoft Windows XP, Vista, 7, 8.
- 2. *GNT USB Token* inicializovaný administrátorom pre funkciu zabezpečenia poštového klienta Thunderbird. Takýto Token obsahuje kľúče užívateľa, certifikáty užívateľa a certifikačnej autority.
- 3. Poštový klient Mozilla Thunderbird
- **4.** Bezpečnostný modul SIPKCS vo forme dynamickej knižnice "*sipkcs.dll*". Modul SIPKCS je typicky umiestnený v systémovom adresáry.

#### 2 Zavedenie bezpečnostného modulu SIPKCS

Bezpečnostný modul SIPKCS umožňuje poštovému klientovi Thunderbird komunikovať s hardvérovým kryptografickým zariadením.

Doručená pošta - Zoskupené	priečinky - Mozilla Thunderbir	đ			
<u>S</u> úbor <u>U</u> praviť <u>Z</u> obraziť P <u>r</u> ejsť	na Správ <u>a</u> U <u>d</u> alosti a úlohy	Nástroje Pomocník			
🖄 Prijať 🔹 🃝 Nová 🔹 🧾 Adresá	ár 🔊 Popis - 🏼 🖉 ThunderNc	Adresár	Ctrl+Shift+B	<ctrl+k></ctrl+k>	$\mathcal{P}$
📄 🖄 Doručená pošta - Zoskupen.	📑 Kalendár	Key Manager Tool Box Uložené súbory	Ctrl+1		• 🖻 🔍 •
Neprečítané priečinky 🛛 🔺 🕨	🛠 Rýchly filter: 🔹 😂 🔒	<u>D</u> oplnky	ieto	správy <ctrl+< th=""><th>-F&gt; 🔎</th></ctrl+<>	-F> 🔎
	🕲 🖉 Predmet	Sprá <u>v</u> ca činností			miestnenie 🛤
		<b>Elitre správ</b> Spustiť fitre na tento priečinok Spus <u>t</u> iť fitre na správu			
		Sp <u>u</u> stiť rozpoznávanie nevyžiadanej pošty pre tento <u>O</u> dstrániť z priečinka správy označené ako nevyžiada	priečinok né (Spam)		
		Impo <u>r</u> t <u>C</u> hybová konzola [2] ThunderNote			4
		<u>N</u> astavenie účtov <u>M</u> ožnosti			
					3
Žiadne správy na prevzatie	1		Neprečítaných: 0	Celkovo: 0	31 Panel Dnes 🗸

1. Otvorte Thunderbird a zvolte "Nástroje->Možnosti"



2. Zvoľte kartu "Spresnenie, Certifikáty" a zvoľte tlačidlo "Zariadenia"

Možnosti							×
방 Všeobecné Z	obrazenie	Písanie správ	Bezpečnosť	<i>O</i> Pr <b>i</b> ohy	Spresnenie	Lightning	
Všeobecné Č Pokiaľ stránk	ítanie a zob a požaduje	razenie Sieť a r môj osobný cel	niesto na disku rtifikát:	Aktualizácie	Certifikáty		
O Vybra	ť auto <u>m</u> atio	cky ⊙ <u>V</u> ždy sa	a opýtať				
<u>C</u> ertifikáty	Zr <u>u</u> šene	é certifikáty	<u>O</u> verenie	<u>Z</u> ariadenia			
					OK	Zn	

3. V nasledujúcom okne zvoľte tlačidlo "Načítať"

Správca bezpečnostných zariaden	Í		
Bezpečnostné moduly a zariadenia ■ NSS Internal PKCS #11 Module Všeobecné šifrovacie služby Softvérové bezp. zariadenie ■ Vstavaný modul Roots Builtin Object Token	Podrobnosti	Hodnota	Prihlásiť Odhlásiť Zmeniť heslo Načítať Uvoľniť Povoliť EIPS
			ОК

SOFTIDEA-

**4.** Zadajte názov modulu "*SoftIdea PKCS #11 modul*" a s pomocou tlačidla "Prehľadávať" zvoľte názov súboru modulu. Typický názov súboru je "*C:\Windows\System32\sipkcs.dll*". Stlačte tlačidlo OK. Vložte Token.



**5.** Správca bezpečnostných zariadení teraz zobrazuje načítaný modul SIPKCS a podrobnosti o vloženom Tokene. V tomto okamihu je vhodné zmeniť užívateľské heslo postupom podľa kapitoly 7. Stlačte OK.



# 3 Nastavenie dôvery v certifikát koreňovej autority

 Otvorte okno "Nástroje->Možnosti", zvoľte kartu "Spresnenie, Certifikáty" a zvoľte tlačidlo "Certifikáty". V nasledujúcom okne zadajte užívateľské heslo pre prihlásenie k Tokenu.





2. V okne "Správca certifikátov"zvoľte kartu "Autority" a zvoľte certifikát koreňovej autority uložený na zariadení "GNT USB TOKEN". Názov certifikátu koreňovej autority Vám oznámi administrátor. V príklade na nasledujúcom obrázku sa jedná o certifikát s názvom "Moja koreňová autorita" vydaný organizáciou "Moja organizácia".

Poznámka: v okne "Správca certifikátov" sa dá vyhľadávať vkladaním začiatočných písmen názvu koreňovej autority.

Vaše certifikáty   Ľudia   Servery Autority   Iné		
Máte uložené certifikáty, ktoré identifikujú tieto certifikačn	é autority:	
Názov certifikátu	Bezpečnostné zariadenie	E\$
Microsec e-Szigno Root CA 2009 Microsec e-Szigno Root CA	Builtin Object Token Builtin Object Token	
Microsoft Secure Server Authority Moja organizácia	Softvérové bezp. zariadenie	
Moja koreňová autorita ■ NetLock Halozatbiztonsagi Kft. NetLock Minositett Kozjegyzoi (Class QA) Tanusitvar NetLock Expressz (Class C) Tanusitvanykiado NetLock Kozjegyzoi (Class A) Tanusitvanykiado NetLock Uzleti (Class B) Tanusitvanykiado	GNT USB TOKEN n Builtin Object Token Builtin Object Token Builtin Object Token Builtin Object Token	-
Zobraziť Upraviť Importovať Export	tovať O <u>d</u> strániť	
		ОК

**3.** Zvoľte tlačidlo "Upraviť" a nastavte dôveru certifikačnej autorite pre všetky identifikácie podľa nasledujúceho obrázka. Stlačte tlačidlo OK.





4. V okne "Správca certifikátov" zvoľte kartu "Vaše certifikáty" a overte že vaše certifikáty uložené na zariadení "GNT USB TOKEN" sú zobrazené.

Správca certifikáto	v			
Vaše certifikáty Ľudia	Servery Autority Iné			
Máte certifikáty od tý	chto organizácií, ktoré vás ic	lentifikujú:		
Názov certifikátu	Bezpečnostné zariadenie	Sériové číslo	Dátum vydania	Platnosť vyprší 🖽
Moja organizácia				
Peter Novák	GNT USB TOKEN	02	18. 10. 2011	18. 10. 2012
Z <u>o</u> braziť Zálo	hov <u>a</u> ť Zá <u>l</u> ohovať všetk	xy I <u>m</u> porto	ovať O <u>d</u> strá	niť
				OK

V závislosti od spôsobu, akým administrátor implementoval systém zabezpečenia, môže Váš Token obsahovať jeden, alebo dva vaše certifikáty. V prvom prípade sa ten istý certifikát použije na podpisovanie i šifrovanie správ. V druhom prípade je jeden z certifikátov určený na podpisovanie a druhý na šifrovanie správ.



# 4 Voľba certifikátov pre šifrovanie a podpisovanie správ

1. Zvoľte "Nástroje->Nastavenie účtov..."





2. Zvoľte účet elektronickej pošty ktorý chcete zabezpečiť. E-mailová adresa účtu by sa mala zhodovať s adresou na vašom certifikáte uloženom na Tokene. Zvoľte kartu "Bezpečnosť".

astavenie účtov	
peter.novak@moja.sk Nastavene servera	Bezpečnosť
Kópie a priečinky Pisanie a adresovanie Nevyžiadaná pošta Miesto na disku Potvrdenia o prečítaní Bezpečnosť	Ak chcete posielať a prijímať podpísané alebo šifrované správy, mali by ste zadať certifikát pre         Šifrovanie a certifikát pre digitálne podpisovanie.         Digitálne podpisovanie         Na digitálne podpisovanie správ používať tento osobný certifikát:         Vybrať         Vybrať         Úgitálne podpisovatí správy (predvolene)         Create Cert ·       □ Enable cert for encryption too
	Šifrovanie Na šifrovanie a dešifrovanie správ posielaných vám používať tento osobný certifikát:
	Vybr <u>a</u> ť Vy <u>m</u> azať
	Prednastavené šifrovanie pri posielaní správ: <ul> <li>Mikdy (nepoužívať šifrovanie)</li> <li>Vž<u>dy</u> (neumožní odoslanie, ak všetci adresáti nemajú certifikát)</li> </ul> Create Cert •              Enable cert for signing too
	Certifikáty
	Zobraziť certifikáty Bezpečnostné zariadenia
Akcie s účtami	•
	OK Zrušiť

**3.** V poli "Digitálne podpisovanie" zvoľte tlačidlo "Vybrať". Systém Vám ponúkne vhodný certifikát uložený na bezpečnostnom zariadení GNT USB TOKEN. Potvrďte výber tlačidlom OK.

Certifikát:	GNT USB TOKE	N:peter_novak [02				
Podrobno	osti vybraného ce	tifikátu:				
Vydaný j Sériové Platný o Účely: H Použitie E-mailo Vydal: Cl Uložené v	pre: E=peter.nov. • číslo: 02 od 18. 10. 2011 9 Klient,Podpísať,Šif • kľúča certifikátu: vá adresa: peter.: N=Moja koreňová v: GNT USB TOKE	ak@moja.sk,CN=Pe :35:00 pre 18. 10. ovať Podpisovanie,Zašifr iovak@moja.sk autorita,O=Moja o N	rter Novák,O=Moja orgai 2012 9:35:00 rovanie kľúča,Šifrovanie i rganizácia,L=Bratislava,C	nizácia,L=Novál údajov =SK	⟨y,C=SK	
				0	ОК	Zrušiť

SoftIdea-

4. Poštový klient Vám ponúkne možnosť nastaviť ten istý certifikát i pre šifrovanie správ. Ak máte jeden certifikát pre podpisovanie i šifrovanie, zvoľte v nasledujúcom okne "Áno". Ak máte samostatné certifikáty pre podpisovanie a pre šifrovanie, zvoľte "Nie" a nastavte certifikát pre šifrovanie podľa bodu 5.

Thund	erbird	×
?	Mali by ste tiež určiť certifikát, ktorý budú používať iní ľudia, keď vám budú posielať šifrované správy. Chcete na to použiť ten istý certifikát?	
	Án <u>o</u> <u>N</u> ie	

- 5. V poli "Šifrovanie" v okne "Nastavenie účtov" zvoľte tlačidlo "Vybrať". Systém Vám ponúkne vhodný certifikát uložený na bezpečnostnom zariadení GNT USB TOKEN. Potvrďte výber tlačidlom OK.
- 6. Úspešne ste zvolili certifikáty pre šifrovanie a podpisovanie správ. Tlačidlom "OK" zatvorte okno "Nastavenie účtov".

Nastavenie účtov		×
peter.novak@moja.sk Nastavenie servera	Bezpečnosť	
Nastavenie servera Kópie a priečinky Písanie a adresovanie Nevyžiadaná pošta Miesto na disku Potvrdenia o prečítaní Bezpečnosť	Ak chcete posielať a prijímať podpísané alebo šifrované správy, mal šifrovanie a certifikát pre digitálne podpisovanie. Digitálne podpisovanie Na digitálne podpisovanie správ používať tento osobný certifikát: GNT USB TOKEN:peter_novak Digitálne podpisovať správy (predvolene) Create Cert  Enable cert for encryption too Šifrovanie Na šifrovanie a dešifrovanie správ posielaných vám používať tento GNT USB TOKEN:peter_novak Prednastavené šifrovanie pri posielaní správ: Nikdy (nepoužívať šifrovanie) Vždy (neumožní odoslanie, ak všetci adresáti nemajú certifikát) Create Cert  Enable cert for signing too Certifikáty Zobraziť certifikáty Bezpečnostné zariadenia	l by ste zadať certifikát pre
Ak <u>c</u> ie s účtami 🔹		
		OK Zrušiť



#### 5 Distribúcia certifikátov

Pre zabezpečenie poštovej komunikácie s inými účastníkmi poštovej siete je potrebné, aby každý účastník vlastnil certifikáty svojich partnerov. Jednoduchý spôsob vzájomnej výmeny bezpečnostných certifikátov medzi dvoma účastníkmi je popísaný v nasledujúcom texte.

1. Vytvorte novú správu pre účastníka, s ktorým si chcete vymeniť certifikáty. Pred odoslaním správy kliknite na tlačidlo "Bezpečnosť" a označte voľbu "Digitálne podpísať túto správu" pre podpísanie správy (kapitola 6.1). Zašlite správu.

Poznámka: Túto úvodnú správu považujte za nezabezpečenú ! Keďže v tomto okamihu ešte nevlastníte certifikát Vášho partnera, nemôžete správu zašifrovať.

- 2. Partner príjme vami podpísanú správu. Keďže správa je podpísaná certifikátom vydaným dôverihodnou certifikačnou autoritou, poštový klient potvrdí, že správa je podpísaná a jej integrita nebola narušená. Zároveň poštový klient partnera automaticky uloží Váš certifikát do svojej databázy. Od tohoto okamihu Vám môže partner posielať zabezpečené správy.
- **3.** Partner vytvorí pre Vás správu, zašifruje ju a podpíše. Váš poštový klient správu dešifruje a potvrdí, že je podpísaná a jej integrita nebola narušená. Zároveň Váš poštový klient automaticky uloží certifikát partnera do svojej databázy. Od tohoto okamihu je prevádzka zabezpečenej poštovej komunikácie s vaším partnerom automatická.

# 6 Zabezpečenie elektronickej pošty

#### 6.1 Odoslanie zabezpečenej správy

1. Pred odoslaním správy kliknite na tlačidlo "Bezpečnosť" a označte voliče "Zašifrovať túto správu" pre zašifrovanie obsahu správy a "Digitálne podpísať túto správu" pre podpísanie správy.

🗣 Nová správa: zabezpecena sprava - Stredoeurópske (Windows-1250)	<u> </u>
<u>S</u> úbor <u>U</u> praviť <u>Z</u> obraziť <u>M</u> ožiť <u>F</u> ormát <u>M</u> ožnosti <u>N</u> ástroje <u>P</u> omocník	
🖳 Odoslať 👋 Pravopis • 🖉 Príložiť • 💾 Bezpečnosť • 🔚 Uložiť •	
Qd:       peter.novak@moja.sk       ✓ Zašífrovať túto správu         •       Komu:	<b>•</b>
Pregmet: Zabezpecena sprava	
Text tela 🔽 Premenivá šírka 🔍 🖛 🎢 🎢 🎢 🏔 🦂 🥖 🔚 🗄 🖶 🐨 🚇 🛛	
telo spravy	
	• 🖻 //.

AN101011

SOFTIDEA-

2. Po kliknutí na "Zobraziť informácie o zabezpečení" sa zobrazia informácie o zabezpečení odchádzajúcej správy. Overte, že správa bude podpísaná a zašifrovaná.

Zabezpečenie správy				×				
Poznámka: Pamätajte, že riadky s p	Poznámka: Pamätajte, že riadky s predmetom správy nie sú nikdy šifrované.							
Obsah správy bude odoslaný nasled Digitálne podpísaný: Áno Zašifrovaný: Áno	lovne:							
Certifikáty:								
Adresát:	Stav:	Vydaný:	Platný do:					
novakova@moja.sk	Platný	18. 10. 2011	18. 10. 2012					
<u>Z</u> obraziť			OK					

#### 6.2 Príjem zabezpečenej správy

Dešifrovanie prijatej zabezpečenej správy a overenie jej integrity je automatické. O stave zabezpečenia informujú ikony v pravej hornej časti okna zobrazujúceho správu (na nasledujúcich dvoch obrázkoch označené šipkou).







Po kliknutí na niektorú z týchto ikon sa zobrazí podrobný výpis o stave zabezpečenia správy. Ak správu nemožno dešifrovať a/alebo nieje možné overiť jej integritu, výpis má obsah ako na nasledujúcom obrázku.

Zabezpečenie správy	×
Správa neobsahuje elektronický podpis Táto správa neobsahuje digitálny podpis odosielateľa. Keďže tento podpis chýba, mohol túto správu odoslať ktokoľvek, kto pozná danú e-mailovú adresu. Je tiež možné, že správa bola pozmenená počas cesty v sieti. Nie je ale zrejmé, že sa niečo takéto stalo.	
Správu nie je možné dešifrovať Správa bola pred odoslaním zašifrovaná, ale teraz ju nemožno dešifrovať. So zašifrovanou správou nastali neznáme problémy. OK	

SOFTIDEA-

Ak bola správa úspešne dešifrovaná a jej integritu bola overená, výpis má obsah ako na nasledujúcom obrázku.



Poznámka: Pre správne dešifrovanie a overenie integrity prijatej zabezpečenej správy je potrebné, aby bol Váš Token pripojený k počítaču.

### 7 Zmena prístupového hesla k Tokenu

1. Otvorte okno "Správca bezpečnostných zariadení", zvoľte Váš GNT USB Token a stlačte tlačidlo "Zmeniť heslo". Vyplňte aktuálne a nové heslo. Stlačte OK.

Zmena hlavného hesk	a	×
Bezpečnostné zariader	nie: GNT USB TOKEN	
Aktuálne heslo:	••••	
Nové heslo:	•••••	
Nové heslo (znova):	•••••	
-Ukazovateľ kvality be	sla:	
	okti	
	OK Zručiť	

2. O úspešnej zmene hesla budete informovaný nasledujúcim oknom.



SoftIdea

#### 8 Dokumentácia

1 GNT USB Token - dátový list, SoftIdea, s.r.o., Máj 2011, http://www.softidea.sk/gnt\_datasheet\_sk.pdf

> SoftIdea s.r.o. Sliačska 10, 831 02 Bratislava tel.: +421 2 444 60 444 fax.: +421 2 446 40 441 http://www.softidea.sk info@softidea.sk

Tento dokument je intelektuálnym vlastníctvom spoločnosti SoftIdea s.r.o. Všetky práva vyhradené.