Odesílání citlivých dat prostřednictvím šifrovaného emailu s elektronickým podpisem standardem S/MIME

Je dostupnou možností, jak lze zaslat lékařskou dokumentaci elektronicky.

Co je třeba k odeslání šifrovaného emailu?

- Emailový klient s podporou šifrování
- Certifikát příjemce s veřejným klíčem určený k šifrování (mnohdy označován jako komerční či standardní) běžně dostupný automaticky z komunikace elektronicky podepsané příjemcem, někdy dostupný ke stažení z webových stránek příjemce ve formě souboru k importu.

Co je třeba k elektronickému podepsání emailu?

- Emailový klient s podporou elektronického podpisu
- Osobní certifikát s privátním klíčem, vzhledem k současné legislativě ideálně kvalifikovaný, a emailový účet s tímto certifikátem provázaný

Jaký je princip šifrování S/MIME v elektronické poště?

Odesilatel potřebuje k odeslání veřejný klíč příjemce, kterým zprávu zašifruje. Vše se děje zcela automaticky v poštovním klientu po příslušném nastavení. Šifrovaná zpráva následně putuje internetem jako každý jiný email. K jejímu přečtení je však potřeba privátní klíč příjemce. Příjemce, který tento klíč, má zobrazí zprávu dešifrovanou jako kterýkoli jiný email, pokud má správně nastavený poštovní klient.



Instalace a nastavení poštovního klienta Thunderbird

Thunderbird je zdarma dostupný poštovní klient, který má veškerou potřebnou funkcionalitu pro elektronický podpis a šifrování standardem S/MIME.

• Poslední verze je ke stažení na adrese: <u>http://thunderbird.mozilla.cz/</u>



Při instalaci je zcela dostačující zvolit *Standardní* typ a postupně po projití průvodce instalaci dokončit.



Po instalaci se systém zeptá, zda mý být Thunderbird výchozím poštovním klientem. Pokud chcete, aby vyhledávání ve Windows prohledávalo zprávy, zvolte *Povolit službě Windows Search prohledávat zprávy*

Nastavení systému ×
Použít aplikaci Thunderbird jako výchozí pro:
🗹 E-mail
🗌 Diskusní skupiny
🗹 Kanály
Povolit službě Windows Search prohledávat zprávy
✓ Vždy kontrolovat při startu aplikace Thunderbird
OK Zrušit

Následně se objeví průvodce nastavením účtu, vyberte Přeskočit průvodce a použít existující e-mail.

Chtěli byste novou e-mailovou adresu?			
Vaše jméno nebo přezdívl	ka		Hledat
Ve spolupráci s řadou poskytovatelů vám Thunderbird umožní založit si vlastní poštovní účet. Do pole výše vložte prosím vaše křesní jméno a příjmení nebo jakéholiv jiné slovo, které se vám líbí.			
🗹 😵 gandi.net 🕢 🌊 Hover.com			
Zadané výrazy jsou odesílány r pošty gandi.net (<u>Zásady ochrar</u> soukromí, <u>Podmínky služby</u>) za	a servery Mozilly 1 <u>y soukromí, Podn</u> účelem nelezení	(<u>Zásady ochrany soukromí</u> í <u>nky služby</u>) a Hover.com (dostupných adres.) a poskytovatelům (Zásady ochrany

V okně, které se zobrazí, zadejte Vaše jméno, které bude zobrazeno v emailové zprávě v kolonce odesilatel a následně zadejte Váš email a heslo. V případě většiny obecně dostupných emailových služeb proběhne nastavení Vašeho účtu zcela automaticky.

Pokud se tak nestane, obraťte se na provozovatele Vašeho emailového účtu s prosbou o nastavení poštovního klienta ideálně na protokol **IMAP**. Většinou mají poskytovatelé emailových služeb podrobné návody pro nastavení jednotlivých klientů na svých webových stránkách.

Založení poštovního účtu			×
<u>V</u> aše jméno:	Jméno Příjmení	Vaše jméno tak, jak se bude zobrazovat ostatním.	
E-mai <u>l</u> :	email@example.com]	
<u>H</u> eslo:	Heslo]	
	✓ Pamatovat si heslo		
Získat <u>n</u> ový (účet	Pokračovat Zrušit	

Založení poštovního účtu
Vaše jméno: E-mail: Heslo: Pamatovat si heslo
Mezi poskytovateli v databázi Mozilly bylo nalezeno následující nastavení
 IMAP (vzdálené složky) POP3 (místní uložiště pošty)
Příchozí IMAP, imap.googlemail.com, SSL
Odchozí SMTP, smtp.googlemail.com, SSL
Uživatelské jméno mudr.tomas.nosek@gmail.com
Získat <u>n</u> ový účet R <u>u</u> ční nastavení <u>H</u> otovo <u>Z</u> rušit

Pokud se Vám po potvrzení nastavení objeví výzva ke schválení bezpečností výjimky, tuto klidně schvalte a zvolte *Uložit tuto výjimku trvale*. Znamená to pouze, že certifikát či certifikační autorita Vašeho poskytovatele emailových služeb není v emailovém klientovi označena jako důvěryhodná (více viz níže).

	Přidání bezpečnostní výjimky	×
	Chystáte se změnit způsob, jakým aplikace Thunderbird identifikuje tento Legitimní banky, obchody a ostatní veřejné servery vás o toto žádat nebudou.	server.
Server		
Adresa:	Získat <u>c</u> erti	fikát
Stav cer	rtifikátu	
Tento s	erver se prokazuje neplatnými informacemi. Zobraz	zit
Neznán	má identita	
Certifika bezpečr	át je nedůvěryhodný, protože nebyl ověřen důvěryhodnou autoritou pomo ného podpisu.	νcí
⊻ <u>U</u> lo:	vžit tuto výjimku trvale Schválit bezpečnostní výjimku Zru	šit

Nyní, když máte účet nastaven, je třeba přidat nastavit elektronický podpis a šifrování. Menu klienta (tlačítko se třemi čárkami vedle vyhledávacího okna) vyberte volbu *Možnosti* \rightarrow *Nastavení účtu*.



V menu *Nastavení účtu* vyberte účet, který jste vytvořili a zvolte *Zabezpečení*. Jelikož Thunderbird není propojen s centrálním úložištěm certifikátů ve Windows, bude třeba nejdříve importovat osobní certifikáty s privátním klíčem pro podpis a šifrování. V našem ukázkovém případě nastavíme pro podpis certifikát kvalifikovaný a pro šifrování certifikát komerční. Zvolte tedy v menu *Zabezpečení* tlačítko *Zobrazit certifikáty*, čímž se dostanete do *Správce certifikát*ů.

Nastavení účtu ×				
	Zabezpečení			
Nastavení serveru Kopie a složky Vytváření zpráv a adresová Nevyžádaná pošta Synchronizace a úložiště Potvrzení o přečtení Zabezpečení Místní složky Nevyžádaná pošta Místo na disku Server odchozí pošty (SMTP)	Pro příjem a odesílání podepsaných nebo zašifrovaných zpráv musíte zadat jak certifikát pro elektronický podpis tak i certifikát pro šifrování. Elektronický podpis Používat tento certifikát pro elektronický podpis odesílaných zpráv: Vy <u>b</u> rat Vy <u>m</u> azat Elektronicky podepsat zprávy (výchozí) Šifrování Použít tento certifikát pro zašifrování a dešifrování obdržených zpráv: Vyb <u>r</u> at Vym <u>a</u> zat Výchozí nastavení šifrování při odesílání zpráv: Nikdy (nepoužívat šifrování) Vyžadováno (nelze odeslat zprávy, pokud všichni příjemci nemají certifikáty Zobrazit certifikáty B <u>e</u> zpečnostní zařízení			
<u>A</u> kce účtu •				
	OK Zrušit			

Ve *Správci certifikátů* jsou jednotlivé certifikáty rozděleny podle typu. V našem případě jsou důležité záložky *Osobní*, kde jsou uloženy certifikáty s privátním klíčem určené k podpisu. Záložka *Lidé* obsahuje certifikáty s veřejným klíčem od ostatních korespondenčních partnerů. V případě, že je příchozí email podepsán, a příslušný certifikát od korespondenčního partnera je platný, tak je automaticky uložen, alternativně je možnost certifikáty korespondenčních partnerů naimportovat. Poslední záložkou, která je v souvislosti s elektronickým podepisováním a šifrováním emailů zajímavá, je záložka *Autority*. Zde se nacházejí **kořenové certifikáty** certifikačních autorit. V případě, že přijde email podepsaný elektronickým podpisem vydaným danou autoritou, musí být certifikát této autority dostupný v záložce *Autority* a musí být označen jako důvěryhodný, jinak emailový klient hlásí problém s elektronickým podpisem.

Aby bylo možné emaily elektronicky podepisovat a šifrovat, je třeba importovat **kvalifikovaný** certifikát s privátním klíčem pro podpis a komerční certifikát s osobním klíčem pro šifrování (kvalifikovaný certifikát nelze k zašifrování zprávy použít).

Import certifikátu se provede po stištění tlačítka *Importovat* v dolní části příslušné záložky v okně *Správce certifikátů*.

8	Správce certif	ïkátů	-		
Osobní Lidé Servery Autority Ostatní					
Tyto certifikáty jsou dostup	Tyto certifikáty jsou dostupné pro vaši osobní identifikaci:				
Jméno certifikátu	Bezpečnostní zařízení	Sériové číslo	Platný do	E\$	
Zo <u>b</u> razit Zá <u>l</u> ohovat	t Zál <u>o</u> hovat vše Impo	ortovat <u>S</u> mazat			
				OK	

Poslední věcí k úspěšnému nastavení certifikátů pro podpis a šifrování je kontrola, zda jsou dostupné **kořenové certifikáty certifikační autority**, která vydala importované osobní certifikáty. Zároveň musí být tento certifikát nastaven jako **důvěryhodný**. **Všechny certifikační autority mají kořenové certifikáty běžně dostupné ke stažení na svých webových stránkách**.

V záložce *Autority* zkontrolujte, zda jsou dostupné kořenové certifikáty autority, která vydala importované osobní certifikáty. V případě, že dostupné nejsou, což v případě lokálních českých certifikačních autorit není výjimkou, je třeba je naimportovat. V dolní části záložky *Autority* je opět umístěno tlačítko *Importovat.* Po importu pro jistotu zkontrolujte nastavení důvěryhodnosti tlačítkem *Upravit důvěru.* V okně, které se objeví, zkontrolujte, zda je zaškrtnuto *Tento certifikát může identifikovat uživatele emailu* a případně zaškrtněte i ostatní volby dle potřeby a potvrďte stištěním tlačítka *OK.* Nyní můžete *Správce certifikátů* ukončit s potvrzením změn stištěním tlačítka *OK.*

Tyto certifikáty jsou dostupné pro identifikaci ce	rtifikačních autorit:	
Jméno certifikátu	Bezpečnostní zařízení	₽₽
Network Solutions L.L.C.		
Network Solutions Certificate Authority PM/SGDN	Builtin Object Token	
IGC/A	Builtin Object Token	
První certifikační autorita, a.s.	-	
I.CA - Qualified Certification Authority, 09/	. Softw. bezp. zařízení	
I.CA - Standard Certification Authority, 09/	. Softw. bezp. zařízení	
Upravit nastavení důvěryhodnosti CA	×)	
Certifikát "I.CA - Standard Certification Aut	hority, 09/2009" představuje Certifikační autoritu.	-
Upravit pastavení důvěrvhodnosti:		
	er.	
Tento certifikát může identifikovat uživa	atele e-mailu.	NV.
Tento certifikát může identifikovat výro	bce software.	IK.

V nastavení poštovního účtu ve volbě *Zabezpečení* vyberte **kvalifikovaný certifikát pro elektronický podpis a komerční pro šifrování.** Email lze podepsat i komerčním certifikátem, ale aby elektronický podpis splňoval požadavky současné legislativy pro zaručený elektronický podpis, je třeba použít certifikát kvalifikovaný. Při výběru certifikátu se Vám zobrazí okno s výběrem dostupných informací v jehož dolní části jsou veškeré podrobnosti o certifikátu včetně toho zda jde o certifikát komerční či kvalifikovaný.

Dále můžete nastavit, zda chcete implicitně elektronicky podepisovat všechny zprávy, což vřele doporučuji, protože na to nebude třeba myslet při odesílání každého emailu, a zda je chcete šifrovat. V případě nastavení šifrování emailu však implicitní nastavení nedoporučuji, protože minimálně z počátku zcela jistě nebudete mít certifikáty s veřejným klíčem od korespondenčních partnerů.

	Nastavení účtu		×		
	Zabezpečení				
Nastavení serveru Kopie a složky Vytváření zpráv a adresová…	Pro příjem a odesílání podepsaných nebo zašifrovaných zpráv musíte zadat jak certifikát pro elektronický podpis tak i certifikát pro šifrování.				
Nevyžádaná pošta Synchronizace a úložiště	Elektronický podpis Používat tento certifikát pro elektronický podpis odesílaných zpráv:				
Potvrzení o přečtení Zabezpečení	Softw. bezp. zařízení:TwinsQD				
 Místní složky Nevyžádaná pošta 	Šifrování]			
Místo na disku Server odchozí pošty (SMTP)	Použít tento certifikát pro zašifrování a dešifrov Softw. bezp. zařízení:TwinsSD	/ání obdržených Vyb <u>r</u> at	n zpráv: Vym <u>a</u> zat		
	Výchozí nastavení šifrování při odesílání zpráv:				
	 <u>N</u>ikdy (nepoužívat šifrování) <u>V</u>yžadováno (nelze odeslat zprávy, pokud v certifikáty) 	·šichni příjemci	nemají		
	Certifikáty				
	Zobrazit certifikáty B <u>e</u> zpečnostní zařízení				
<u>A</u> kce účtu •	<u>A</u> kce účtu •				
		ОК	Zrušit		
			×		
	Vyber certifikatu				
Certifikát: Softw. bezp. zařízen	í:TwinsQD	•			
Podrobnosti o vybraném certifikátu: Použití klíče certifikátu: Podpisování,Nepopiratelnost E-mail: Vydal: OU=I.CA - Accredited Provider of Certification Services,O="První certifikační autorita, a.s.",CN="I.CA - Qualified Certification Authority, 09/2009",C=CZ Uskladněno v: Softw. bezp. zařízení					
	[ОК	Zrušit		

Při odesílání emailu můžete nastavení podpisu a šifrování nastavit a měnit v okně odesílané zprávy po stištění šipky dolů u tlačítka zabezpečení.

🕞 Psaní zprávy: (bez předmětu)				
<u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obra	zení V <u>l</u> ožit <u>F</u> ormát <u>N</u>	<u>M</u> ožnosti <u>N</u> ástroje Nápo <u>v</u> ěda		
🗱 Odeslat 🛛 🗹 Pravo	opis 👻 🛛 Připojit 🔻	r 🕒 Zabezpečení 🔽 🔚 Uložit 🔻 Priorita		
<u>O</u> d:	MUDr. Tomáš Nosek <	< Zašifrovat zprávu		
▼ Komu:	8	<u>E</u> lektronicky podepsat zprávu		
		Zobrazit informace o zabezpečení		
Pře <u>d</u> mět:				

V případě, že Vám přijde email opatřený elektronickým podpisem, Thunderbird informaci zobrazí ikonou zapečetěné obálky v pravé části záhlaví zprávy. Pokud byl navíc email šifrován, zobrazí se vedle ikony dopisu navíc ještě ikona zámku.

🔦 Odpovědět 🌩 Přeposlat 🗟 Archivovat 🕚	Nevyžádaná pošta 🚫 Smazat
Od Tomáš Nosek 😭	
Předmět Šifrovaná zpráva Komu Tomáš Nosek	Další akce +
Tento text byl při odeslání zašifrován	

V emailovém klientu, který neobsahuje certifikát pro dešifrování je obsah zprávy viditelný pouze jako soubor přílohy *smime.p7m*, stejně tak je zobrazen i ve webovém rozhraní většiny emailových služeb.

