

Elektronický podpis praktické aspektu používania epodpisu

Šifrovanie a podpisovanie emailov Šifrovanie a podpisovanie súborov Podpisovanie a zabezpečenie pdf eID – použitie, portál Slovensko

Katedra aplikovanej matematiky a hospodárskej informatiky Ekonomická fakulta Technickej univerzity 2019

# Elektronický podpis emailu

### Bezpečná elektronická emailová komunikácia

- Nutnosť použiť email klienta
- Thunderbird od Mozily, ale aj iné aplikácie
- Ukážky, návody http://ca.ekf.tuke.sk

📝 Česká 530/26 - Mapy Go 🗙 Y 💾 Testovacia stránka certifi 🗶 Nová karta 🛛 🗶 🚺
$\leftarrow \rightarrow$ C $\bigtriangleup$ (i) ca.ekf.tuke.sk/index.html $\Rightarrow$ is G :
Certifikačná autorita CAEKFTUKE (neoficiálna testovacia stránka a verzia)
home Certifikačná autorita Ekon.fakulta TU Projekt Tatrabanka On-Line Banka Lab e-podnikania E-podpis Kontakt Seminár EP
<u>Certifikačná autorita Ekonomickej fakulty TU v Košiciach - web rozhranie</u>
Návody na prácu s certifikačnou autoritou:
1. <u>Ako získať certifikát CAEKFTUKE</u> (Návody)
Alternativa ziskania certifikátu:
<u>Thawte</u> - stránka spoločnosti Thawte už od r. 1995 vydáva zdarma osobné certifikáty
C.O.M.O.D.O - alternatíva získania free osobného certifikátu
2. Ako zrušiť svoj certifikát (v prípade krádeže, straty, zneužitia)
3. Ako exportovať certifikát z Internet explorera
4. Ako importovaľ certifikát do Internet explorera
5. Ako importovať certifikát do MS Outlook
<ol> <li>6. Ako importovať certifikát inej osoby do adresára MS Outlook a vytvoriť šifrovaný a podpísaný email</li> </ol>
7. Ako importovať certifikát a súkromný kľúč do PGP
8. <u>Ako exportovať verejný kľúč z PGP (pre ostatných užívateľov)</u>
<ol> <li><u>Ako podpísať dokument a overiť platnosť obsahu dokumentu a platnosť podpisu</u> dokumentu v PGP.</li> </ol>
10. Ako zašifrovať obsah dokumentu a následne rozšifrovať v PGP.
11. <u>Ako podpísať a zašifrovať dokument a následne ho rozšifrovať a overiť platnosť</u> podpisu súčasne jednou akciou v PGP
12. Nastavenie PGP servra pre upload vereiných kľúčov



#### TU Košice Ekonomická fakulta

# Praktická ukážka a postup

- Import certifikátu do email klienta
- Nastavenie priradenie certifikátu k poštovému kontu
- Podpisovanie a šifrovanie emailov

🔗 Nová správa: (bez predn	netu)		<u> </u>
<u>S</u> úbor <u>U</u> praviť <u>Z</u> obraziť	<u>V</u> ložiť <u>F</u> ormát <u>M</u> ožn	iosti <u>N</u> ástroje <u>P</u> omocník	
🙀 Odoslať 🛛 🖌 Pravopi	is 🔻 関 Priložiť 🔻	🖀 Bezpečnosť 🔻 🖶 Uložiť 🔻	
<u>O</u> d: d	loc. RNDr. Jozef Bucko, I	Zašifrovať túto správu	•
▼ Odpovedať na: jo	ozef.bucko@tuke.sk	Digitálne podpísať túto správu	
▼ Komu:		Z <u>o</u> braziť informácie o zabezpečení	٦
Pre <u>d</u> met:			
Odstavec 🔻 P	Premenlivá šírka	▼ ■ A-A'A'A A A A ∷ 12 55 55 E = • ■ • ◎ •	
			*
•			
•			
*****	*****		Ξ
doc. RNDr. Jozef B	Bucko, PhD.		
Katedra aplikovane	ej matematiky Formatiky		
Ekonomická fakulta	a TU,		
Nemcovej 32, 040 0	01 Košice,		
c.d. 222	Otuko sk		-
Email: Jozef.Bucko	JWCUKE.SK		

812qn@tuke.sk	^	Bezpečnosť
Vastavenie servera ćópie a priečinky Pisanie a adresovanie Nevziňadaná pošta Synchronizácia a úložný priestor Potvrdenia o prečítaní Bezpečnosť wekko@gmail.com		bezpecnost Ak chcete posielať a prijímať podpisané alebo šifrované správy, mali by ste zadať certifikát pre šifrovanie a certifikát pre digitálne podpisovanie. Digitálne podpisovanie správ používať tento osobný certifikát: Jozef Bucko Technicka univerzita v Kosiciach ID Ugitálne podpisovať správy (predvolene) Sjítrovanie
Nastavenie servera Kópie a priečinky Yisanie a adresovanie Vevyžiadaná pošta Synchronižácia a úložný priestor Potvrdenia o prečitaní Bezpečnosť b@tuke.sk Nastavenie servera Kópie a priečinky Pisanie a adresovanie Nevyžiadaná pošta Synchronižácia a úložný priestor Potvrdenia o prečitaní Bezpečnosť vetf@tuke.sk	E	Na šířrovanie a dešiřrovanie správ posielaných vám používať tento osobný cetrifikát: Jozef Bucko Technicka univerzita v Kosiciach ID Vybrgť Vymazať Prednastavené šířrovanie pri posielaní správ: <ul> <li>Nikdy (nepoužívať šířrovanie)</li> <li>Vždy (neumožní odoslanie, ak všetci adresáti nemajú cetrifikát)</li> </ul> <li>Cetrifikáty <ul> <li>Zobraziť certifikáty</li> <li>Bgzpečnostné zariadenia</li> </ul> </li>
Ak <u>c</u> ie s účtami	•	

## Podpisovanie a šifrovanie súborov

- Nutnosť použiť softvér problém!!!
- Kleopatra GNU GP, alebo GPG
- PGP komerčná verzia, do 8.1 zdarma
- PGP alternatíva k CA
  - Roztrúsená dôvera nie centrálna
  - Certifikáty si navzájom vydávajú účastníci krížovým podpisom
  - Nadšenci, rebeli, snaha o bežné využitie zdarma

# GPG – GnuPG - Kleopatra

Stiahnúť -

https://www.gpg4win.org/

- Nainštalovať
- Naimportovať certifikát (zo zálohy)
- Podpisovať súbory
- Šifrovať súbory
- Rozšifrovať súbory
- Overovať podpisy

$\mathbf{p}_{\mathbf{G}}$		$C_{ii}$		x
s <u>T</u> ools <u>S</u> ettin	igs <u>W</u> indo	w <u>H</u> elp		
Export Ce	rtificates	C Redisp	lay	**
<mark>ificates</mark>	M	y Certificate	s	•
Trusted Certific	ates <u>O</u> t	her Certifica	tes	×
E-Mail	Valid F	rom	Valid Until	
	2011-11-2	27 20	21-11-27	Х.
zef.bucko@t	2016-02-0	08 20	18-02-07	X.
				•
	Is <u>T</u> ools <u>S</u> ettin Export Centificates Trusted Certific E-Mail zef.bucko@t	is <u>Tools Settings Windo</u> Export Certificates ificates Trusted Certificates <u>Ott</u> E-Mail Valid Fr 2011-11-2 zef.bucko@t 2016-02-0	Is <u>Tools Settings Window H</u> elp Export Certificates My Certificates Trusted Certificates Other Certificate E-Mail Valid From 2011-11-27 20 zef.bucko@t 2016-02-08 20	s <u>Tools Settings Window H</u> elp Export Certificates My Certificates <u>Trusted Certificates</u> <u>Other Certificates</u> E-Mail Valid From Valid Until 2011-11-27 2021-11-27 zef.bucko@t 2016-02-08 2018-02-07





# Praktická ukážka

g:\Predmety-vyucba\den	faktura.txt	cba\denne\Eis\eis2016_2017
Meno	Tlačiť	Ext Veľkosť ↓Dá
<b>≜</b> []	Harry 20	<dir> 21.</dir>
MartinVejacka	Opravit	ppt 1 506 816 21.
faktura	Zobraziť (Lister)	panka2016 pdf 3 191 475 10.
	7	panka2016 ppt 6 012 416 10.
		ppt 3 /89 312 26.
1	Encrypt	ppt 522 /52 15.
		pui 1005 040 25.
1	Shred	pdf 810 867 22
	Rename with date	ppt 2 915 840 22.
	Rename with date	pdf 286 327 21.
	Skontrolovať pomocou ESET Endpoint Antivirus	o gif 120 485 21.0
	Ďalšie možnosti	▶ em_cr_popdf 158 567 07.0
		tup pdf 501 144 09.
	Convert to lower case	
	Convert to upper case	
	Capitalica	
	Capitalise	
	Touch now	
	Sign and encrypt	
1 k B / 1 k B x 1 / 2 súbo	Touch	B x 0 / 13 súborach
	More GpgEX options	Decrypt
ty-vyucba \denne \EB_pr		Verif.
F3 / Zobrazit' F4	Convert to PDF/A	venty
	🗶 Sign	Decrypt and verify
	a	Encrypt
1 - 1	Otvorit v programe	Sign
	Read-only	or in the second s
	Read only	Sign and encrypt
	Copy path(s) to clipboard	Import keys
	Ododať kam	Create checksums
	o doside kum	Verify checksums
	Vystrihnúť	Verity checksuns
	Konírovať	Help on GpgEX
		About GraEX
	Skomprimovat subory	About opger
	EkF TU Košice	



## **Podpisovanie PDF**

Jednoduché prostredníctvom Acrobat reader
Nástroje – certifikáty – digitálne podpísať

Podepsat pomocí digitálního ID	×		Konfigurovat digitální	ID pro	podepisování ×
Vyberte digitální ID, který chcete použít k podpisu:	Obnovit				
Jozef Bucko (Digitální identifikátor systému Window Vydal:Certifikacna autorita Ekonomickej fakul ,Konec platn	vs) iosti: 2017.02.07 Zobrazit podrobnosti		Digitální ID je vyžadován pro vytvoření digitálního podpisu. Nejbezpečnější digitální identříkátory jsou vydávány důvěryhodnými certifikačními autoritami a jsou založeny na zabeznečených zdříženích	()	<ul> <li>Použít zařízení pro vytváření podpisů</li> <li>Konfigurovat čipovou kartu nebo token připojený k počítači</li> </ul>
<b>Jozef Bucko</b> (Soubor digitálního identifikátoru) Vydal:Certifikacna autorita Ekonomickej fakul ,Konec platnosti: 2018.	02.07		jako jsou čipové karty a tokeny. Některé jsou založeny na souborech. Můžete také vytvořít nový	$\bigcirc$	Použít digitální ID ze souboru Importovat existující digitální ID, který jste obdrželi jako soubor
	Zobrazit podrobnosti		digitalni ID, ale takovy identifikátor poskytuje nízkou úroveň ochrany identity.	$\bigcirc$	Vytvořit nový digitální ID           Vytvořit digitální ID s vlastním podpisem
(? Konfigurace nového digitálního ID	Zrušit Pokračovat		3		Zrušit Pokračovat
		ELE TI	IVačiaa		

# Tvorba vlastného vzhľadu podpisu



Automa 🚞

Formát číslic

0123456789

=

Uložit

Zrušit





Rozlišující název

Logo

Popisy

Verze Adobe Acrobat

Název

Datum

Důvod

Umístění

Přednastavit název

# Overenie podpisu

- nastavenie root certifikátu podateľne CAEKFTUKE na stav dôveryhodný
- Použijeme panel podpisu v Acrobat Reader XI
- nájdeme root certifikát CAEKTUKE a nastavíme jeho dôveryhodnosť
- je možné nastaviť aj dôveryhodnosť priamo certifikátu používateľa (ale dôveryhodnosť sa dedí)

# Dedičnosť dôveryhodnosti



## **Overenie** podpisu

🔁 harmo	onogram_	hi.pdf - Adol	be Read	er					
Soubor	Úpravy	Zobrazení	Okna	Nápověda					

Nejméně jeden podpis má problém	ny.
---------------------------------	-----

🔁 harmonogram

🕖 Panel podpisu

🔁 harmonogram\_hi.pdf - Adobe Reader

#### HARMONOGRAM A HODNOTENIE PREDMETU EIS - HI

HARMONOGRAM PREDNÁŠOK (PC6

PREDNÁŠAJÚCI

Soubo

4

### Zvolíme podrobnosti podpisu

### Následne podrobnosti certifikátu

Pedméné jeden podpis má problémy.       Image: Comparison de la politica de la politi	Úpravy <u>Z</u> obrazení O <u>k</u> na <u>N</u> ápověda	×
Podpisy       (*)       >         □       Ověřit vše       Ověřit vše         □       Sev. 1: Podepsal(a): Jozef Bucko sjozef.bucko@tuke.sk>         Platnost podpisu je neznámá:       Dokument se od aplikování tohoto podpisu nezměnil       Identita podepisujícího není známá, protože jeho certifikát není v seznamu důvěryhodných c       C         □       Podrobnosti podpisu       Naposledy kontrolováno: 2015.09.29 10:20:23 + 02'00'       Naposledy kontrolováno: 2015.09.29 10:20:23 + 02'00'         Pole: Signature2 na stránce 2       Klepnutím zobrazite tuto verzi.       Na	lejméné jeden podpis má problémy.	💋 Panel podpisu
<ul> <li>Pratrios podpisu je Heininia.</li> <li>Dokument se od aplikování tohoto podpisu nezměnil</li> <li>Lidentita podepisujícího není známá, protože jeho certifikát není v seznamu důvěryhodných cí</li> <li>Čas podepisání pochází z hodin na počítači autora podpisu.</li> <li>Podrobnosti podpisu</li> <li>Naposledy kontrolováno: 2015.09.29 10:20:23 +02'00'</li> <li>Pole: Signature2 na stránce 2</li> <li><u>Klepnutím zobrazite tuto verzi</u>.</li> <li>Militaria podražite <u>tuto verzi</u>.</li> <li>Militaria podražite <u>verzi</u>.</li> <li>Militaria verzi</li> <l< th=""><th>Podpisy (4 ) □ - Ověřit vše □ <sup>2</sup> Rev. 1: Podepsal(a): Jozef Bucko <jozef.bucko@tuke.sk> Platosť nodpisu je neznámá:</jozef.bucko@tuke.sk></th><th>LADARNOCELMA A RODOTINE PEZMETU ES- AU</th></l<></ul>	Podpisy (4 ) □ - Ověřit vše □ <sup>2</sup> Rev. 1: Podepsal(a): Jozef Bucko <jozef.bucko@tuke.sk> Platosť nodpisu je neznámá:</jozef.bucko@tuke.sk>	LADARNOCELMA A RODOTINE PEZMETU ES- AU
11111 Thermal Research of the second	Platnost podpisu je neznama: Dokument se od aplikování tohoto podpisu nezměnil Identita podepisujícího není známá, protože jeho certifikát není v seznamu důvěryhodných co Čas podepsání pochází z hodin na počítači autora podpisu. ⊡ Podrobnosti podpisu Naposledy kontrolováno: 2015.09.29 10:20:23 +02'00' Pole: Signature2 na stránce 2 <u>Klepnutím zobrazíte tuto verzi.</u>	1000     Formulation for the second sec
		1100     Sector Se

11

Použijeme panel podpisu

# Nastavenie dôveryhodnosti certifikátu CAEKFTUKE

 Použijeme záložku "Dôveryhodnosť"

 Zvolíme "Pridať k dôveryhodným certifikátom"



Kontroly ověření platnosti cesty byly provedeny k času podepsání: 2015/09/28 16:41:43 +02'00' Model ověřování: shell

## Nastavenie dôveryhodnosti II

- Dôveryhodnosť
   Certifikačnej autority
   CAEkFTU
- Dôveryhodnosť pre certifikované dokumenty v rozsahu
  - Dynamický obsah
  - Vložený JavaScript
  - Systémové operácie

Importovat nastavení kontaktu
Podrobnosti certifikátu
Předmět: Certifikacna autorita Ekonomickej fakulty TU v Kosiciach
Vydavatel: Certifikacna autorita Ekonomickej fakulty TU v Kosiciach
Použití: Digitální podpis, Certifikát podpisu (CA), Podepisování CRL
Konec platnosti: 27.11.2021 19:07:58
Důvěryhodnost
Certifikát použitý k podepsání dokumentu musí být buď určen jako kotva důvěryhodnosti nebo být zřetězený ke kotvě důvěryhodnosti, aby bylo ověření podpisu úspěšné. Kontrola odvolání se neprovádí na kotvě důvěryhodnosti ani nad ní.
Použít tento certifikát jako důvěryhodný kořen
Pokud je ověření podpisu úspěšné, důvěřujte tomuto certifikátu pro:
✓ Podepsané dokumenty nebo data
Certifikované dokumenty
☑ Dynamický obsah
Vložený JavaScript s vysokou prioritou
Privilegované systémové operace (práce v síti, tisk, přístup k souborům atd.)
Nápověda OK Zrušit

# Nastavenie dôveryhodnosti III

- Dôveryhodnosť osoby (podpisujúceho)
- Dôveryhodnosť pre certifikované dokumenty v rozsahu
  - Dynamický obsah
  - Vložený JavaScript
  - Systémové operácie

tovat nastavení kontak	ctu
odrobnosti certifikátu	
Předmět: Jozef Bucko	o <jozef.bucko@tuke.sk></jozef.bucko@tuke.sk>
Vydavatel: Certifikacı	na autorita Ekonomickej fakulty TU v Kosiciach
Použití: Digitální pod	lpis, Neodvolatelnost, Zašifrovat klíče, Zašifrovat dokument
Konec platnosti: 7.2.	2016 15:21:06
Důvěrvhodnost	
ni. V Použít tento cer Pokud je ověření p pro:	tifikát jako důvěryhodný <u>k</u> ořen odpisu úspěšné, důvěřujte tomuto certifikátu
✓ Podepsané d	lokumenty nebo data
Cer <u>t</u> ifikovan	é dokumenty
<b>☑</b> <u>D</u> ynami	cký obsah
📝 Vložený	JavaScript s vysokou prioritou
<mark></mark> Privilego souborů	ované systémové operace (práce v síti, tisk, přístup k im atd.)

# Znovuoverenie podpisu

### Po potvrdení nastavenia možnosť znovuoverenia podpisu – klik na obrázok

podpisu 🗕

### Výsledok-Podpis PLATNÝ

Vlastnosti podpisu...

Zavřít

#### Stav ověření podpisu

Podpis je PLATNÝ, podepsaný uživatelem Jozef Bucko <jozef.bucko@tuke.sk>. - Tento Dokument se od aplikování tohoto podpisu nezměnil. - Identita autora podpisu byla při vydání platná, ale nyní nelze zkontrolovat, zda nebyla zrušena a zde její platnost trvá.

\_ 0 23 🔁 harmonogram\_hi.pdf - Adobe Reader Soubor Úpravy Zobrazení Okna Nápověda Podepsáno a všechny podpisy jsou platné. 🥖 Panel podpisu 13.12.2013 Zaverecne nodnotenie, uderovanie zapoc icite HOLNOTENIE MINIMUM Web-stránka 10 b Eshop (vvtvorenie, naplnenie) 15 b Digitálně Legislatíva 20 b podepsal Jozef 15 b Podnikateľský zámer Bucko Strategická štúdia 10 b Datum: Účtovníctvo 20 b 2015.09.28 Analýza, dolaďovanie, 10 b 16:41:43 +02'00' Spolu 100 h Minimálny počet bodov na udelenie zápočtu 51 b Stav ověření podpisu Podpis je PLATNÝ, podepsaný uživatelem Jozef Bucko <jozef.bucko@tuke.sk>. - Tento Dokument se od aplikování tohoto podpisu nezměnil. - Identita autora podpisu byla při vydání platná, ale nyní nelze zkontrolovat, zda nebyla zrušena a zde její platnost trvá. Vlastnosti podpisu.. Zavřít

# Podpisovanie pdf - alternatívy

### Množstvo aplikácií, komerčných aj freeware

- Web online portály
- Disig kvalifi kovaný elektro nický podpis pdfka

### https://zep.disig.sk/Portal





Súhlasím so všeobecnými podmienkami používania služieb zep.disig.sk.

VYBRAŤ/ZMENIŤ SÚBOR...

🖋 PODPÍSAŤ 🛛 🛇 OVERIŤ

ΙU

# Pdf dokumenty a epodpis SK

 Rovnakým spôsobom je možné podpisovať pdf dokumenty prostredníctvom elektronickej ID karty (občianský preukaz)

 Potrebný je aktivovaný čip, čítačka čipových kariet a príslušný driver a softvér pre prácu s e-ID (občianským preukazom)

- https://www.slovensko.sk/sk/titulna-stranka
- http://www.opis.gov.sk/

## Podpis a šifrovanie v SmartPhone



)	per)	۱Key	chai	in: E	Easy	PGP

Sufficiently Secure Komunikácia

\*\*\*\*\*\* 2 078 👤

Nainštalované

Ponúka nákupy v aplikácii

3 PEGI 3

Táto aplikácia je kompatibilná so všetkými vašimi zariadeniami.



https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain&hl=sk

# Postupy – v Moodle

- Video Pridanie novej identity do OpenKeychainSúbor
- Video Importovanie verejného kľúča kontaktu cez QR kód v OpenKeychainSúbor
- Video Zašifrovanie a odoslanie súboru v OpenKeychain
- Video Pridanie kontaktu v OpenKeychainSúbor
- Video Potvrdenie kľúča QR kódom v OpenKeyChainSúbor
- Video Rozšifrovanie súboru v OpenKeychain