

Elektronický podpis

praktické aspektu používania e- podpisu



Šifrovanie a podpisovanie emailov

Šifrovanie a podpisovanie súborov

Podpisovanie a zabezpečenie pdf

eID – použitie, portál Slovensko

Katedra aplikovanej matematiky a hospodárskej informatiky

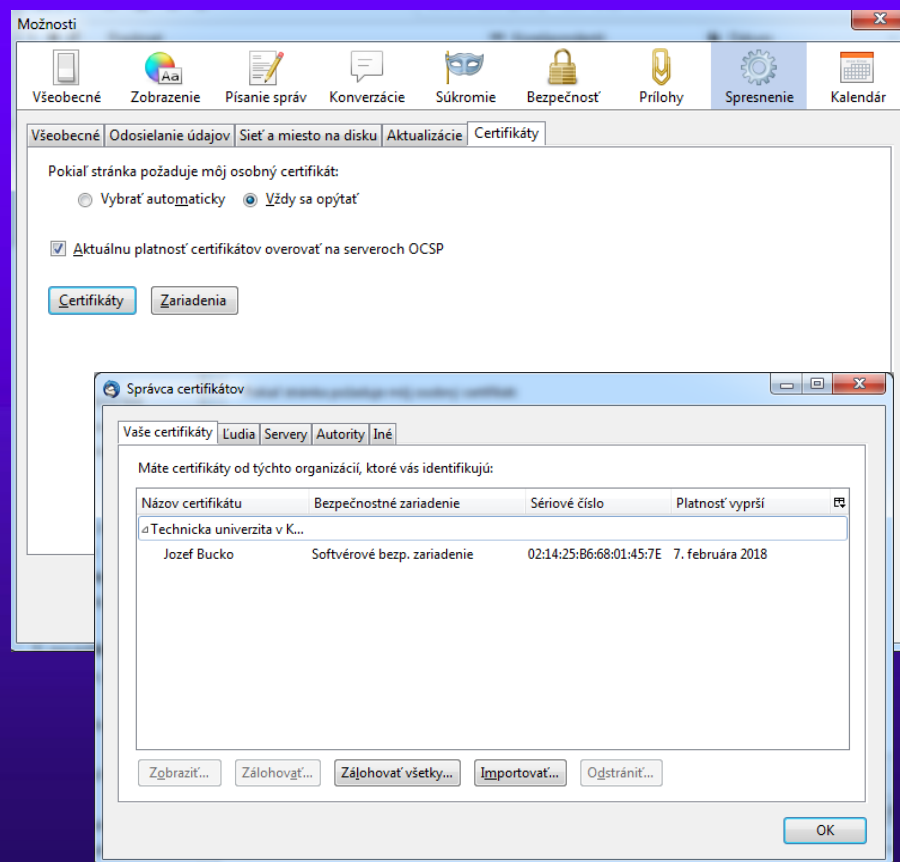
Ekonomická fakulta Technickej univerzity

2019

Elektronický podpis emailu

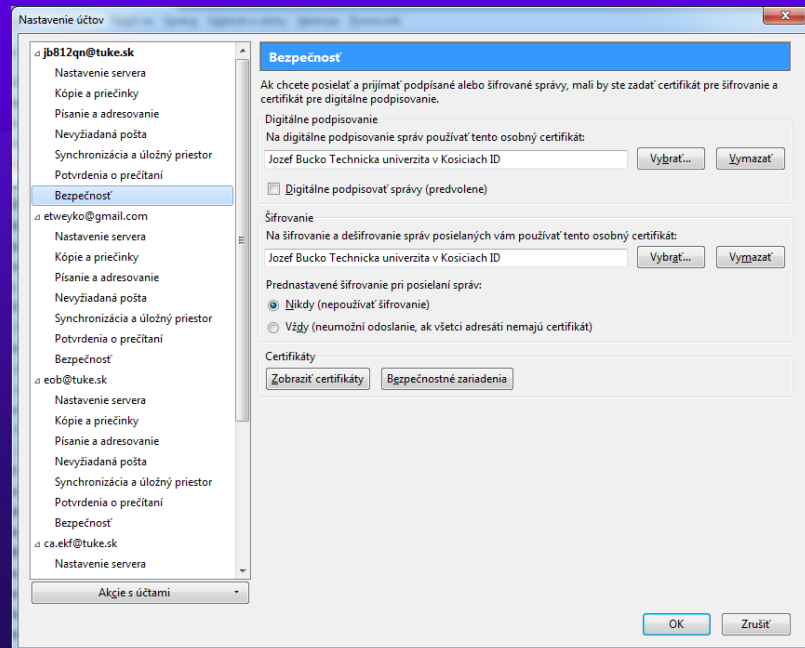
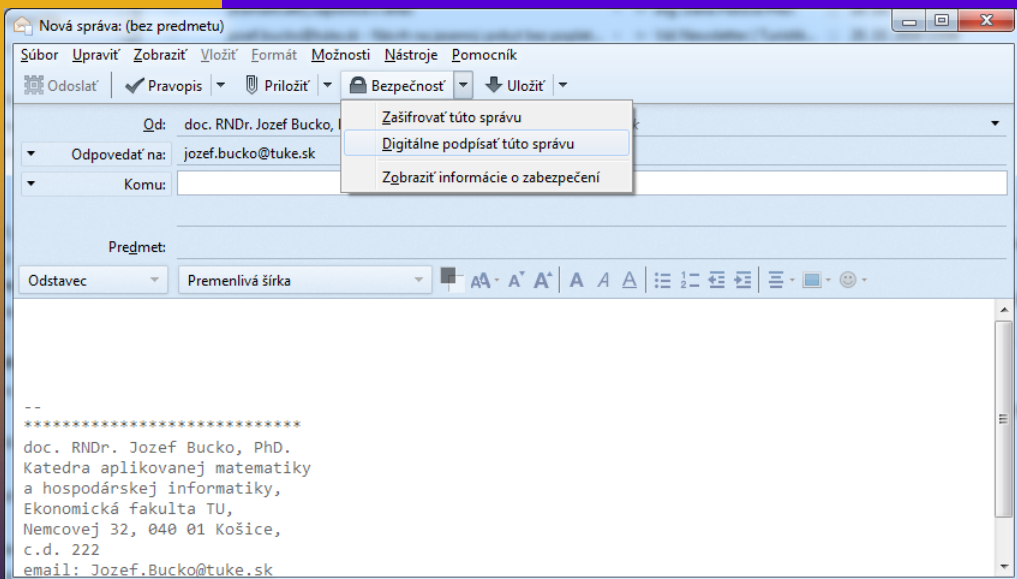
Bezpečná elektronická emailová komunikácia

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



Praktická ukážka a postup

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



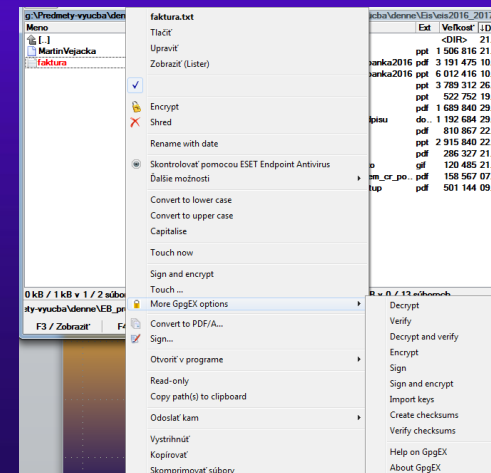
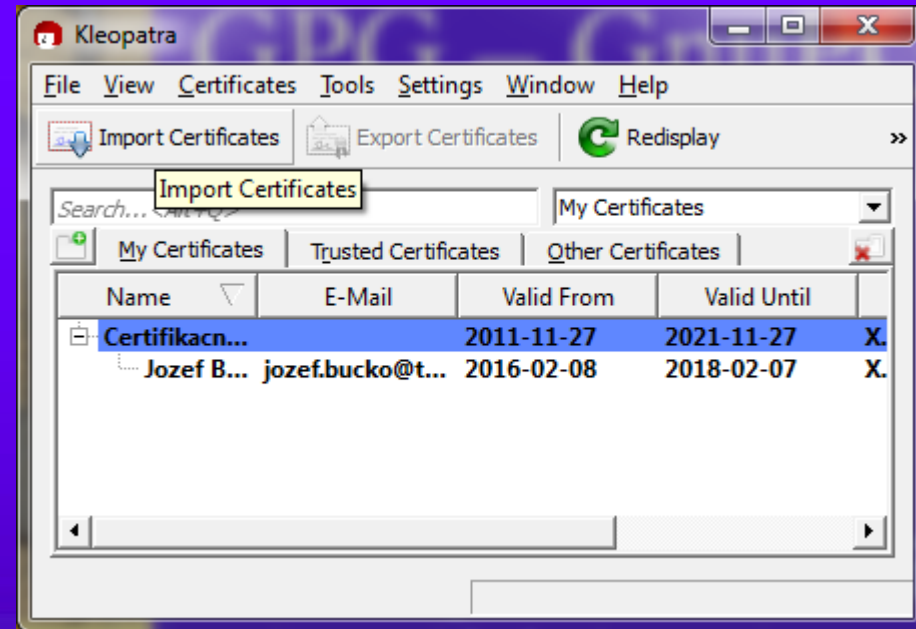


Podpisovanie a šifrovanie súborov

- ◆ 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
- ◆ Nainportovať certifikát (zo zálohy)
- ◆ Podpisovať súbory
- ◆ Šifrovať súbory
- ◆ Rozšifrovať súbory
- ◆ Overovať podpisy



Praktická ukážka

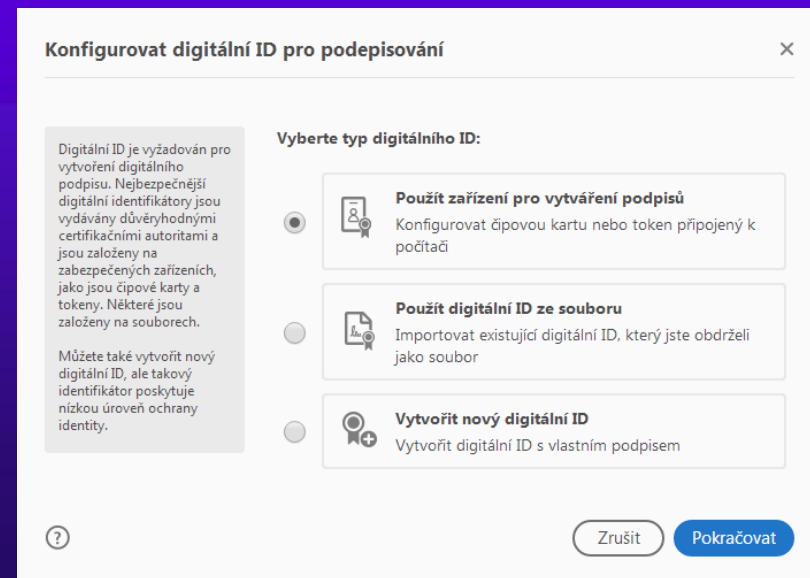
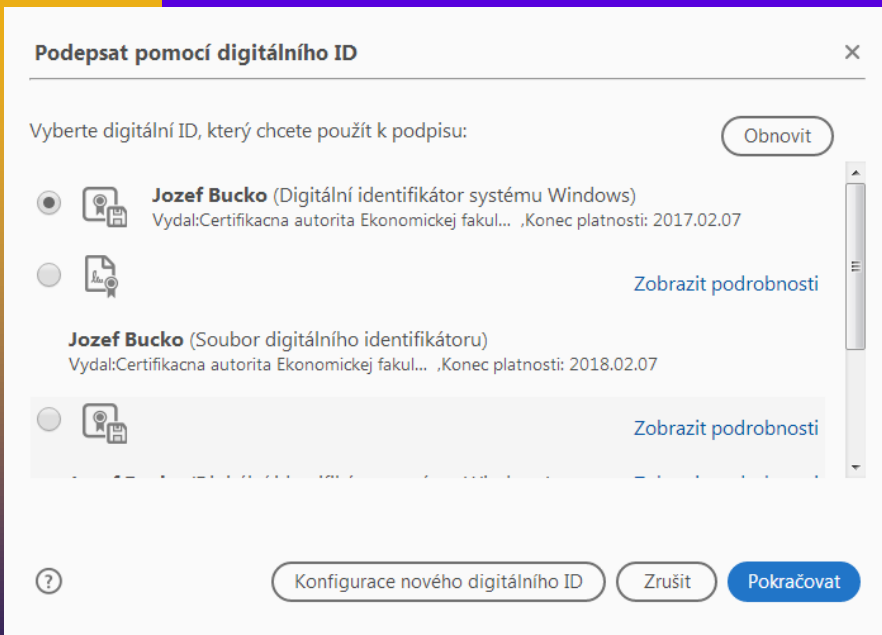


The screenshot shows a Windows file explorer window with a context menu open over a file named 'faktura.txt'. The menu includes various actions such as printing, editing, listing, encrypting, shredding, renaming, and signing. The 'More GpgEX options' sub-menu is currently selected and open, displaying a list of cryptographic operations.

Ext	Veľkosť	↓Dá
<DIR>	21.	
ppt	1 506 816	21.
banka2016 pdf	3 191 475	10.
banka2016 ppt	6 012 416	10.
ppt	3 789 312	26.
ppt	522 752	19.
pdf	1 689 840	29.
pisu do..	1 192 684	29.
pdf	810 867	22.
ppt	2 915 840	22.
pdf	286 327	21.
gif	120 485	21.
em_cr_po.. pdf	158 567	07.
tup pdf	501 144	09.

Podpisovanie PDF

- ◆ Jednoduché prostredníctvom Acrobat reader
- ◆ Nástroje – certifikáty – digitálne podpísať

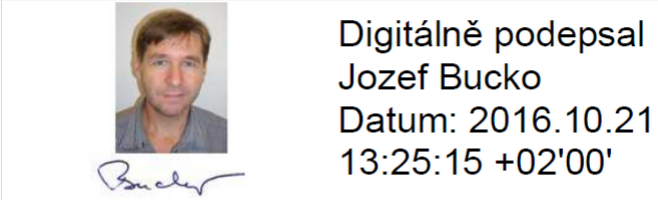


Tvorba vlastného vzhľadu podpisu

Podepsat jako "Jozef Bucko"

Vzhľad esig_foto

Vytvořit Upravit



Zamknout dokument po podepsání [Zobrazit detaily certifikátu](#)

Recenze obsah dokumentu, který může ovlivnit podepsání [Recenze](#)

Zpět **Podepsat**

Prizpůsobit vzhled podpisu

Text Obraz Žádný

<sem patří vaše skutečné jméno> Digitálně podepsal <sem patří vaše skutečné jméno>
Datum: 2016.10.21 13:27:04 +02'00'

Vložit text

Název Rozlišující název
 Datum Verze Adobe Acrobat
 Umístění Logo
 Důvod Popisy

Směr textu

Automa

Formát číslíc

0123456789

Přednastavit název

Zrušit **Uložit**

Prizpůsobit vzhled podpisu

Text Obraz Žádný

Digitálně podepsal <sem patří vaše skutečné jméno>
Datum: 2016.10.21 13:26:07 +02'00'

[Procházet](#) [Odstranit](#)

Vložit text

Název Rozlišující název
 Datum Verze Adobe Acrobat
 Umístění Logo
 Důvod Popisy

Směr textu

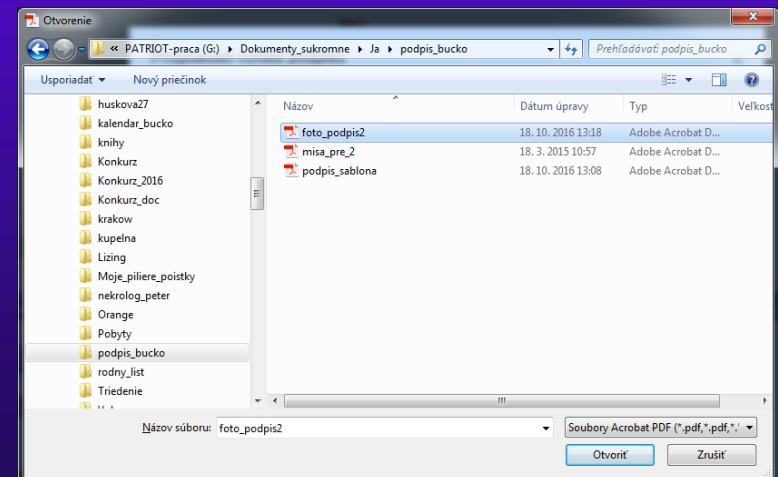
Automa

Formát číslíc

0123456789

Přednastavit název

Zrušit **Uložit**

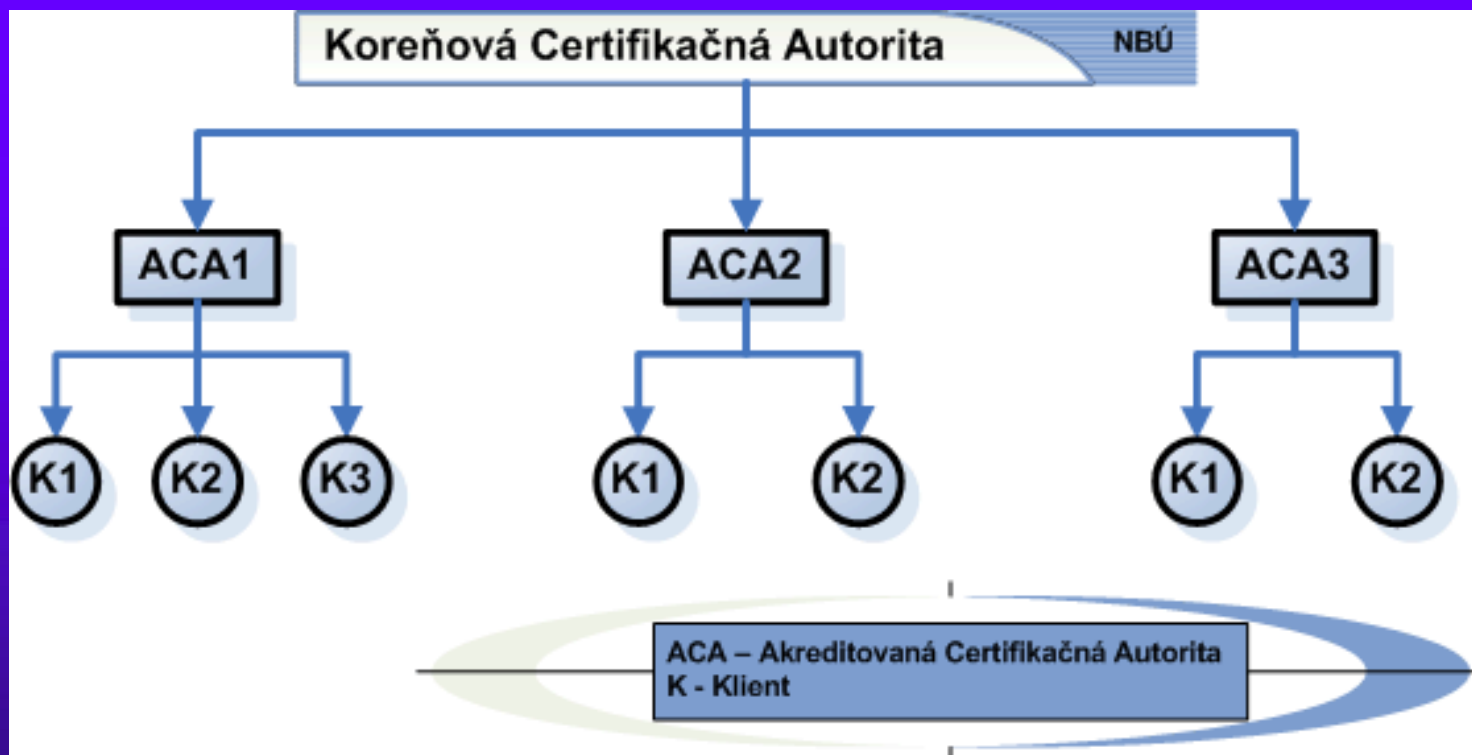




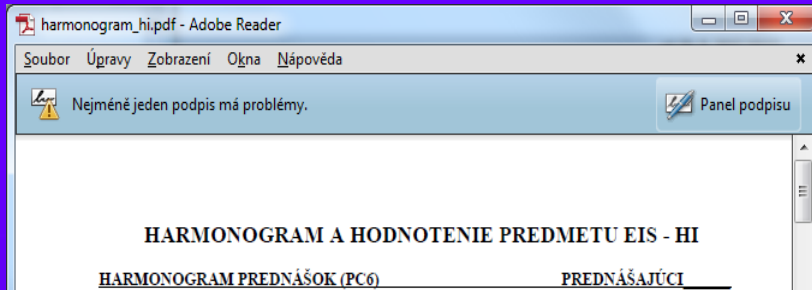
Overenie podpisu

- ◆ 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

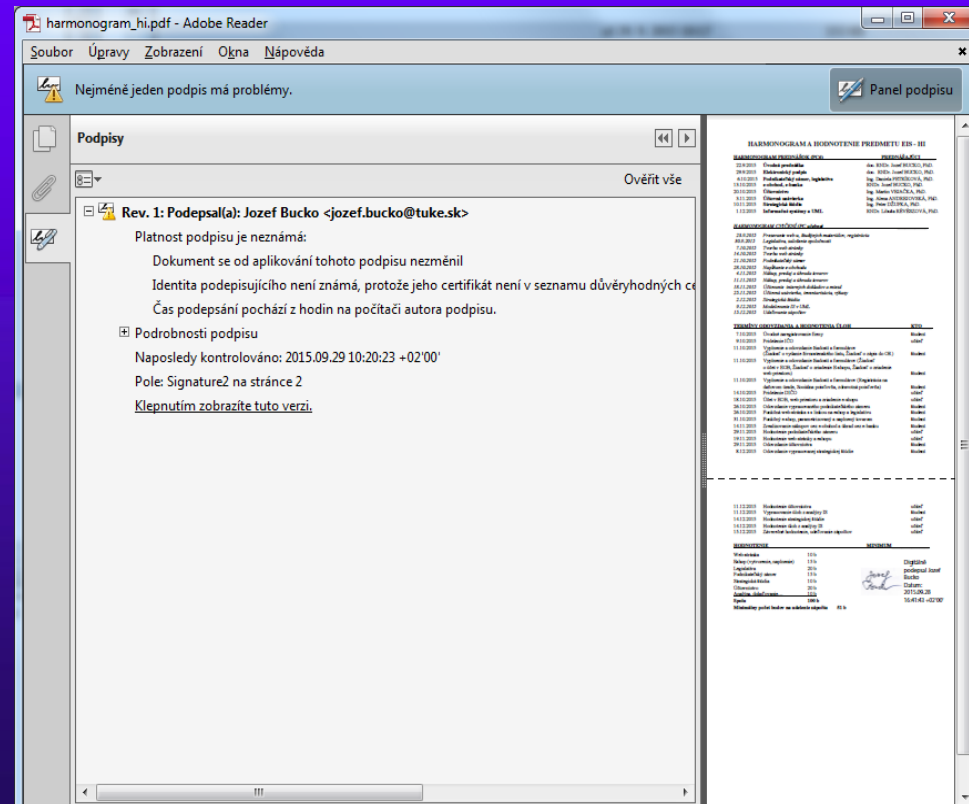


Overenie podpisu



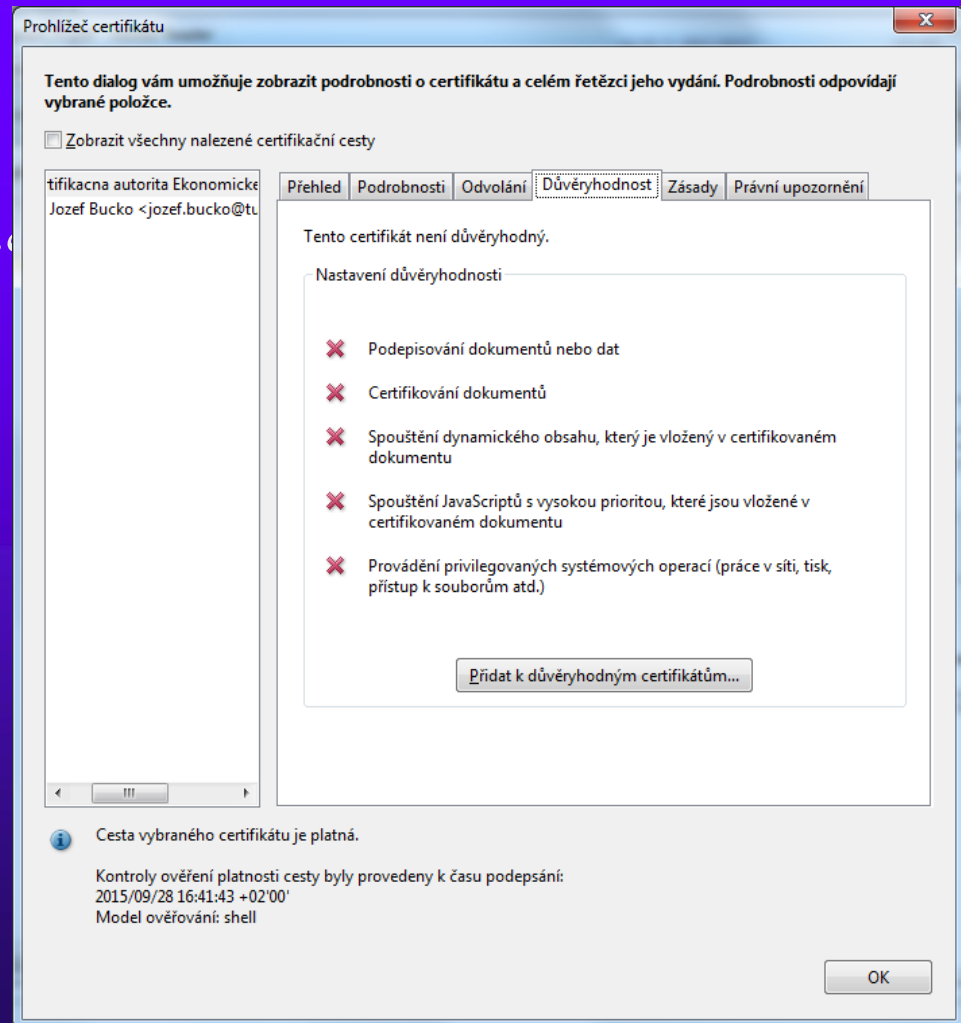
Použijeme panel podpisu

- ◆ Zvolíme podrobnosti podpisu
- ◆ Následne podrobnosti certifikátu



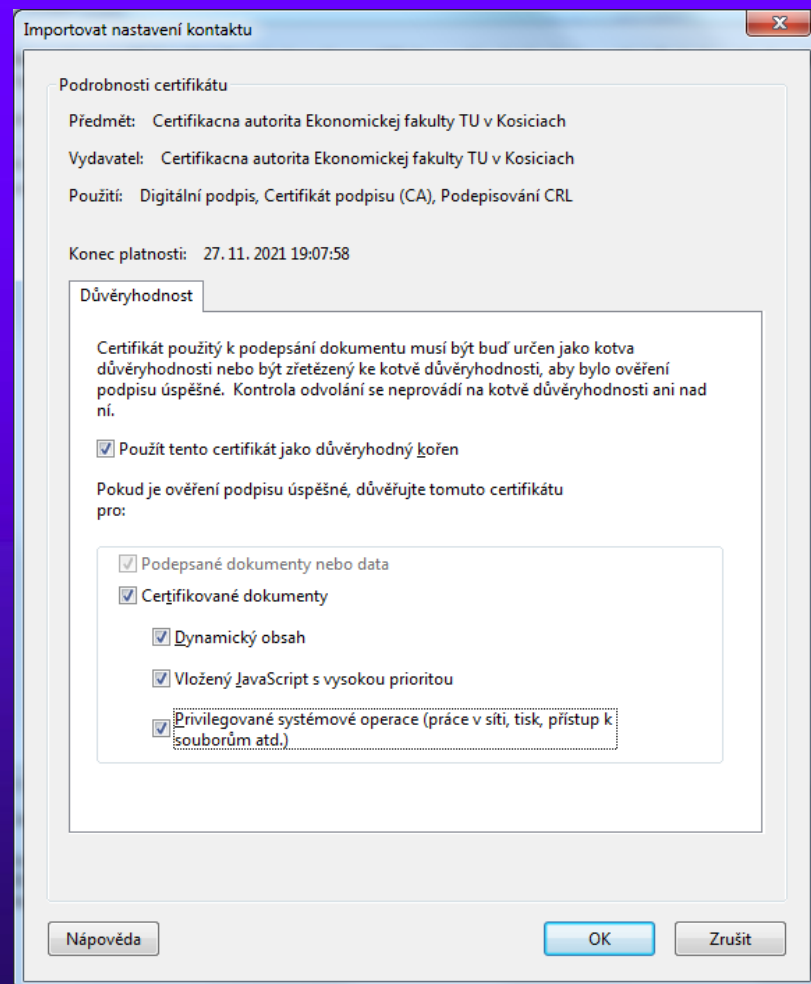
Nastavenie dôveryhodnosti certifikátu CAEKFTUKE

- ◆ Použijeme záložku „Dôveryhodnosť“
- ◆ Zvolíme „Pridať k dôveryhodným certifikátom“



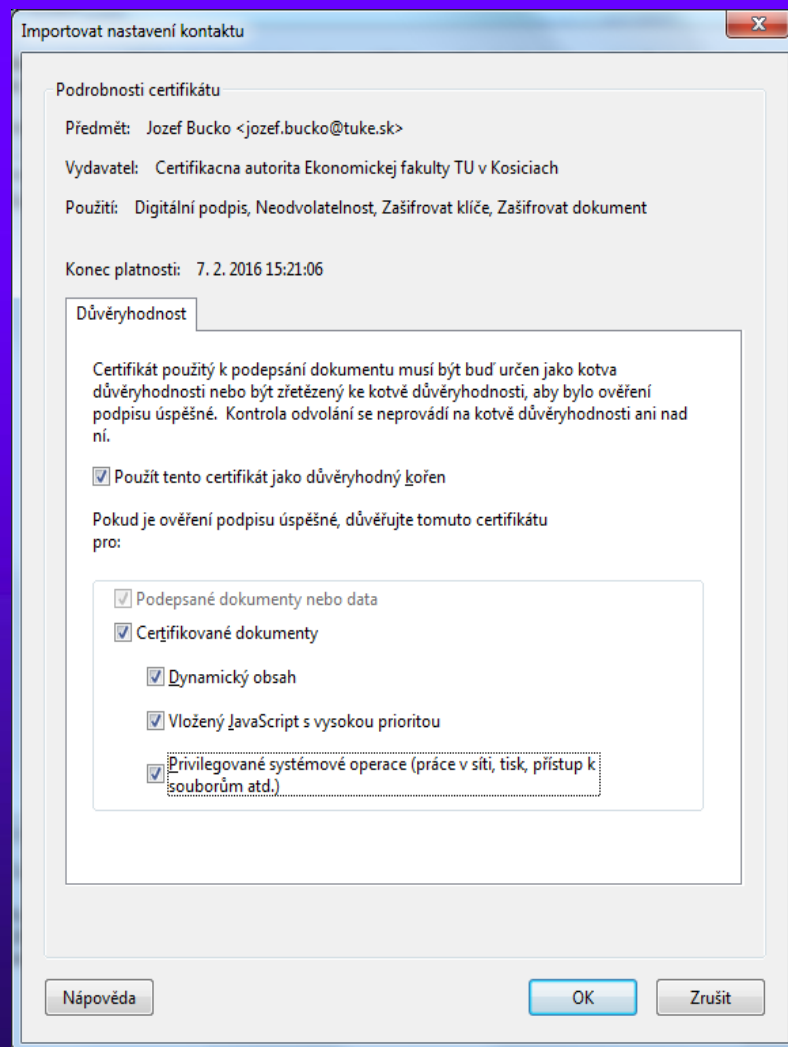
Nastavenie dôveryhodnosti II

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



Nastavenie dôveryhodnosti III

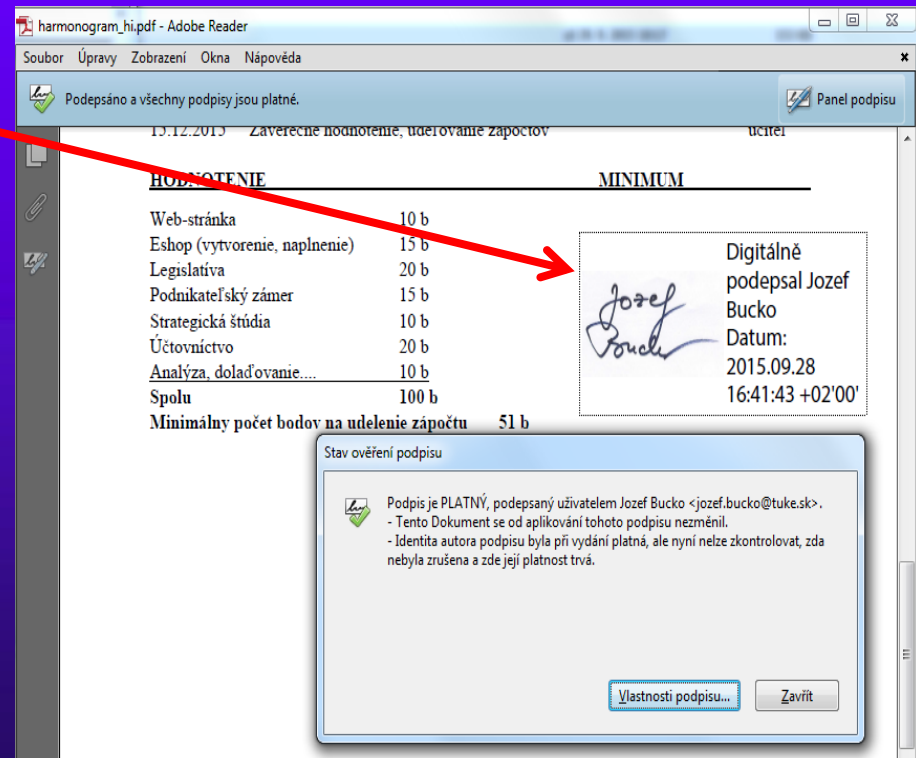
- ◆ Dôveryhodnosť osoby (podpisujúceho)
- ◆ Dôveryhodnosť pre certifikované dokumenty v rozsahu
 - Dynamický obsah
 - Vložený JavaScript
 - Systémové operácie



Znovuoverenie podpisu

- ◆ Po potvrdení nastavenia možnosť znovuoverenia podpisu – klik na obrázok podpisu

- ◆ Výsledok-
Podpis PLATNÝ



harmonogram_hi.pdf - Adobe Reader

Soubor Úpravy Zobrazení Okna nápověda

Podepsáno a všechny podpisy jsou platné. Panel podpisu

13.12.2013 Zaverenie rozhodnutie, udeľovanie započtov učitel

HODNOTENIE	MINIMUM
Web-stránka	10 b
Eshop (vytvorenie, naplnenie)	15 b
Legislativa	20 b
Podnikateľský zámer	15 b
Strategická štúdia	10 b
Účtovníctvo	20 b
Analýza, doľad'ovanie...	10 b
Spolu	100 b

Minimálny počet bodov na udeľenie zápočtu 51 b

Digitálne podepsal Jozef Bucko
Datum: 2015.09.28
16:41:43 +02'00'

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

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 – kvalifikovaný elektronický podpis pdfka

<https://zep.disig.sk/Portal>

The screenshot shows the website interface for ZEP.DISIG.SK. At the top right, there are language selection buttons for 'ZEP.DISIG.SK' and 'SK'. The main navigation menu includes 'Domov', 'Novinky', 'Podpora', 'Legislatíva', 'O portáli', and 'Kontakt'. A yellow banner below the navigation states: 'Spustili sme nový portál ZEP.DISIG.SK! Viac informácií nájdete v sekcii Novinky.' The main content area features a blue background with the heading 'Elektronický podpis bez hraníc' and the text: 'Vytvorte kvalifikovaný elektronický podpis jednoducho, bez nudnej registrácie, či zložitej konfigurácie.' Below this, there is a large red button with a white checkmark icon and the text 'Podpísať alebo overiť dokument'. Underneath the button is a checkbox labeled 'Súhlasím so všeobecnými podmienkami používania služieb zep.disig.sk.' At the bottom, there are three buttons: a green button 'VYBRAŤ/ZMENIŤ SÚBOR...', a red button 'PODPÍSAŤ', and a red button 'OVERIŤ'.



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



OpenKeychain: Easy PGP

Sufficiently Secure Komunikácia ★★★★★ 2 078

3 PEGI 3

Ponúka nákupy v aplikácii

Táto aplikácia je kompatibilná so všetkými vašimi zariadeniami.

Nainštalované

The screenshots show the app's main interface. The first shows a menu with options: Keys, Encrypt/Decrypt, Apps, Settings, and Help. The second shows a list of keys under 'My Keys' with entries for Alice (alice@example.com), Bob (bob@example.com), and Eve (eve@example.com). The third shows a detailed view of a key with options: Scan QR Code, Search Cloud, and Import from File.

<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](#)