

AKADEMICKÝ INFORMAČNÝ SYSTÉM AiS2

Príručka používateľa

Elektronický podpis

© Univerzita Pavla Jozefa Šafárika v Košiciach 2008



OBSAH

1	GENEROVANIE ŽIADOSTI O VYDANIE OSOBNÉHO CERTIFIKÁTU
1.1	GENEROVANIE ŽIADOSTI O VYDANIE OSOBNÉHO CERTIFIKÁTU V INTERNETOVOM PREHLIADAČI INTERNET EXPLORER
1.2	GENEROVANIE ŽIADOSTI O VYDANIE OSOBNÉHO CERTIFIKÁTU V INTERNETOVOM PREHLIADAČI Mozilla Firefox
2	INŠTALÁCIA OSOBNÉHO CERTIFIKÁTU 13
2.1	INŠTALÁCIA OSOBNÉHO CERTIFIKÁTU DO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MS Windows
2.2	INŠTALÁCIA OSOBNÉHO CERTIFIKÁTU DO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MOZILLA Firefox
3	ZÁLOHOVANIE A OBNOVA OSOBNÉHO CERTIFIKÁTU
3.1	ZÁLOHOVANIE (EXPORT) OSOBNÉHO CERTIFIKÁTU ZO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MS WINDOWS
3.2	ZÁLOHOVANIE (EXPORT) OSOBNÉHO CERTIFIKÁTU ZO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MOZILLA
3.3	Obnova (import) osobného certifikátu do systémového úložiska certifikátov MS Windows
3.4	Obnova (import) osobného certifikátu do systémového úložiska certifikátov Mozilla
4	VYUŽÍVANIE OSOBNÉHO CERTIFIKÁTU 49
4.1	IMPORT CERTIFIKÁTOV INÝCH OSÔB DO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MS WINDOWS
4.2	IMPORT CERTIFIKÁTOV INÝCH OSÔB DO SYSTÉMOVÉHO ÚLOŽISKA CERTIFIKÁTOV MOZILLA53
4.3	ELEKTRONICKÉ PODPÍSANIE TEXTOVÉHO DOKUMENTU MS WORDU57
4.4	ELEKTRONICKÉ PODPÍSANIE TEXTOVÉHO DOKUMENTU Z KANCELÁRSKEHO BALÍKU OPEN OFFICE
4.5	VYUŽÍVANIE OSOBNÉHO CERTIFIKÁTU S POŠTOVÝM KLIENTOM OUTLOOK EXPRESS60
4.6	VYUŽÍVANIE OSOBNÉHO CERTIFIKÁTU S POŠTOVÝM KLIENTOM MOZILLA THUNDERBIRD63
5	VYSVETLENIE POJMOV

V prípade problémov a otázok súvisiacich s elektronickým podpisom sa obráťte na: Radovana Engela, CIIT – TIP, Jesenná 5 <u>radovan.engel@upjs.sk</u>, VOIP: 2456

Poznámka: Zobrazenie okien a znenie textov závisí od konkrétnej inštalácie operačného systému a ďalších aplikácii. V jednotlivých jazykových mutáciách a verziách sa môžu líšiť.

1 GENEROVANIE ŽIADOSTI O VYDANIE OSOBNÉHO CERTIFIKÁTU

Dôležité upozornenie: Pri generovaní žiadosti majte na zreteli, že Váš osobný certifikát musí byť nainštalovaný **na tom istom počítači (a v tom istom prehliadači)**, na ktorom bola generovaná žiadosť. Po vyexportovaní už nainštalovaného osobného certifikátu ho však budete môcť používať aj na iných počítačoch.

1.1 Generovanie žiadosti o vydanie osobného certifikátu v internetovom prehliadači Internet Explorer

Pre užívateľov operačného systému Windows Vista: Pred samotným generovaním žiadosti o vydanie osobného certifikátu je potrebné urobiť nasledovné nastavenia Internet Exploreru:

I. Z hlavnej ponuky programu vyberte "Nástroje" a potom "Možnosti siete Internet". V tomto dialógovom okne zvoľte kartu "Zabezpečenie" a kliknite na "Dôveryhodné lokality":

žnosti siete l	nternet		?
Obsah	Pripojenia	Programy	Spresnenie
Všeobecné	Zabezpečenie	e Ochrana	osobných údajov
Vyberte webovú	zó <u>n</u> u a zadajte jej nast	avenie zabezpečeni.	a.
Internet	Lokálna sieť Dôver intranet lok	yhodné Vymedzei ality lokality	né
Táto zór lokality, l nepoško Úroveň <u>z</u> abez	na obsahuje webové ktorým dôverujete, že dia údaje alebo počítač pečenia pre túto zónu-	V tejto zóne s žiadne lokality	Lokality a nenachádzajú
Vlas Vla - A úrc - A tla	tná astné nastavenie. k chcete zmeniť nastav oveň. k chcete použiť odporú čidlo Predvolená úrovei	venie, kliknite na tlač čané nastavenia, kli ň.	idlo Vlastná knite na
		oveň	olená úroveň
		OK Zruš	šit P <u>o</u> užit

II. Kliknite na tlačidlo "Lokality" a urobte nastavenia podľa obrázku nižšie (nezabudnite zrušiť možnosť "Žiadať overenie servera (https:) pre všetky lokality v zóne"), potom kliknite na "Pridať" a napokon na "OK". Stránka <u>http://www.disig.sk</u> sa pridá medzi "Webové lokality":

Trusted sites	? 🛛
Môžete pridávať alebo odstraňovať webo tejto zóny. Všetky webové lokality v tejto jej nastavenie zabezpečenia. Pridať túto webovú lokalitu do zóny:	vé lokality patriace do zóne budú používať
http://www.disig.sk	<u>P</u> ridať
<u>W</u> ebové lokality:	
	O <u>d</u> strániť
Ziadať overenie <u>s</u> ervera (https:) pre všetky lok	ality v zóne
ОК	Zrušiť

III. Na karte "Zabezpečenie" dialógového okna "Možnosti siete Internet" kliknite na tlačidlo "Vlastná úroveň" (ako webová zóna musia byť stále označené "Dôveryhodné lokality"). V otvorenom dialógovom okne zabezpečte, aby bolo "Inicializovanie a skriptovanie ovládacích prvkov Active, ktoré nie sú označené ako bezpečné" povolené (viď obrázok nižšie). Nastavenia ukončíte kliknutím na "OK" a zatvorením dialógového okna "Možnosti siete Internet".

lastavenie zabezpečenia 🛛 🛜 🛛
Nastavenie:
 Prihlásiť automaticky s aktuálnym menom a heslom použív Sobraziť výzvu na zadanie mena používateľa a hesla Ovládacie prvky ActiveX a doplnky Automatické zobrazovanie výziev pre ovládacie prvky Active Povoliť Zakázať
Inicializácia a skriptovanie ovládacích prvkov Active, ktoré nie sú označené ako bezpečí
Zakázať Zobraziť výzvu
Preberanie nepodpísaných ovládacích prvkov ActiveX Povoliť Zakázať
Obnoviť predvolené nastavenie
Obnoviť na úroveň: Nízka Nastaviť
ОК Ζгиšiť

Postup pri generovaní žiadosti o vydanie o osobného certifikátu

Poznámka pre užívateľov operačného systému Windows Vista: Pri generovaní žiadosti o vydanie osobného certifikátu po 2. bode nižšie uvedeného postupu automaticky nasleduje 5.bod.

1. Kliknite na https://eidas.disig.sk/sk/genrequest/:



2. Ako typ certifikátu zvoľte "**Osobný – Fyzická osoba - zamestnanec**". Zobrazí sa Vám nasledujúci formulár, do ktorého je potrebné zadať údaje, ktoré požadujete mať v certifikáte:

Položky žiadosti prosím vypĺňajte bez diakritiky. Položky vyznačené červenou farbou sú povinné.			
Typ certifikátu:	Osobný - FO - zamestnanec 🛛 🔻 🛞		
Typ kľúča:	Microsoft Enhanced Cryptograp 👻 🛞		
	🗹 Zvýšená ochrana privátneho kľúča		
Meno a Priezvisko:			
Organizácia:			
Organizačný útvar:			
Mesto:			
Štát:	sк		
E-mail:			
Generova	ať žiadosť		

Všetky údaje sa vypisujú bez diakritiky!

- Typ certifikátu: zvoľte možnosť "Osobný FO zamestnanec"
- Políčko Zvýšená ochrana privátneho kľúča nechajte zaškrtnuté
- Typ kl'úča: zvoľte možnosť " Microsoft Enhanced Cryptographic vs 1.0. "
- Meno a priezvisko (POVINNÝ ÚDAJ): zadajte údaje z občianskeho preukazu, pokiaľ máte titul zapísaný v OP a požadujete ho mať uvedený aj v certifikáte, zapíšte ho pred Vaše krstné meno
- Organizácia UPJS v Kosiciach, položka musí byť vyplnená touto hodnotou!!!
- Organizačný útvar (NEPOVINNÝ ÚDAJ)
- Mesto (NEPOVINNÝ ÚDAJ): vypisuje sa podľa trvalého bydliska
- Štát (POVINNÝ ÚDAJ): položku nemeňte, jej hodnota je SK
- *E-mail (POVINNÝ ÚDAJ)*: (školský e-mail, NIE súkromný)
- 3. Zapísané hodnoty si ešte raz skontrolujte, ak s týmito hodnotami súhlasíte, zvoľte možnosť "Generovať žiadosť". Po kliknutí na túto možnosť sa Vám zobrazí nasledovná informácia:

Potentia	al Scripting Violation
♪	This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?
	Ano Nie

- Webové rozhranie Vás týmto oznamom upozorňuje, že webová stránka žiada o generovanie novej žiadosti o certifikát. Na pokračovanie zvoľte možnosť "Áno".
- 4. Následne budete vyzvaní, aby ste si zvolili úroveň zabezpečenia Vášho súkromného kľúča. V ponúknutom okne kliknite na možnosť "Nastaviť úroveň zabezpečenia...":

Vytvára sa no	ový výmenný kľúč RSA 🛛 🛛 🔯
	Aplikácia vytvára chránenú položku.
	Súkromný kľúč CryptoAPI Úroveň zabeznečenia je nastavená na bodnotu Stredná
Ca)。 汉王	Nastaviť úroveň zabezpečenia OK Zrušiť Podrobnosti

- Predvolené nastavenie je hodnota "**Stredná**". Znamená to, že Váš súkromný kľúč nebude chránený žiadnym heslom, takže práca s certifikátom prebehne automaticky:

Vytvára sa nový výmenný kľúč RSA 🛛 🔀		
	 Zvoľte úroveň zabezpečenia zodpovedajúcu tejto položke. Vysoká Na použitie položky vyžiadať moje povolenie spolu s heslom. Stredná Na použitie položky vyžiadať povolenie. 	
	< Naspäť Dalej > Zrušiť	

Dôležité upozornenie: V prípade, že sa rozhodnete úroveň zabezpečenia súkromného kľúča nastaviť na najvyššiu hodnotu (použitie súkromného kľúča bude zabezpečené heslom), zvoľte si možnosť "**Vysoká**". Heslo zapíšete do ponúknutého okna "**Heslo**", a následne zvolené heslo potvrďte zápisom do okna "**Potvrdiť**". Pri každej práci s certifikátom budete musieť zadávať Vami zvolené heslo.

- Pre pokračovanie generovania žiadosti kliknite na "Ďalej >" a následne na "Dokončiť":

Vytvára sa nový výmer	iný kľúč RSA	×
	Nastavili ste strednú úroveň zabezpečenia. Pred použitím položky sa zobrazí dialógové okno so žiadosťou o vaše povolenie.	
	< Naspäť Dokončiť Zrušiť	

- Proces nastavenia hesla ukončíte kliknutím na "OK":

Vytvára sa ne	ový výmenný kľúč RSA 🛛 🛛 🔀
	Aplikácia vytvára chránenú položku.
ai	Súkromný kľúč CryptoAPI Úroveň zabezpečenia je nastavená na hodnotu Stredná
	Nastaviť úroveň zabezpečenia OK Zrušiť Podrobnosti

5. Po vygenerovaní žiadosti uvidíte upozornenie, že žiadosť bola vygenerovaná:

Pre uloženie žiao	Josti na zvolené médium (HDD, USB, disketa) kliknite	na tlačidlo
	Uložiť žiadosť o certifikát	

6. Kliknite na možnosť "Uložiť žiadosť o certifikáť", po zobrazení ďalšieho okna kliknite na "Uložiť":



7. Zobrazí sa Vám nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Zvoľte si cestu a kliknite na možnosť "**Uložiť**". Zvolenú cestu si zapamätajte, pretože túto žiadosť je potrebné doručiť na príslušnú registračnú autoritu:

Uložiť ako			? 🔀
Uložiť do:	🞯 Pracovná ploc	cha 🔽 🧿 🗇 📴 🛄 🗸	
Naposledy použité Pracovná plocha	(⊟ Moje dokument	У	
Tento počítač	Nézaszékese		
	Nazov suboru:	asig-10112008144334-26/46.req	
Miesta v sieti	Uloźiť vo formáte:	Text Document	Zrušiť J

8. Kliknite na "Zavrieť", tým sa proces generovania žiadosti končí:

Preberanie dokončené	
Preberanie doko Uložené: g-10112008144756-75938	ončené 3.req z www.disig.sk
Descent Calu	1.271.0 2 1
Prevzatých:	1,27 KB za 2 sek.
Liel ove umlestnenie:	\disig-10112008144756-75938.req.txt
Prenosová rýchlosť:	651 bajtov/sek
📃 Po dokončení preberani	a zavrieť dialógové okno
	Otvoriť Otvoriť priečinok Zavrieť

1.2 Generovanie žiadosti o vydanie osobného certifikátu v internetovom prehliadači Mozilla Firefox

1. Kliknite na https://eidas.disig.sk/sk/genrequest/:

ETTER ARCON	Generovanie žiadosti o certifikát disig.sk » Certifikačná autorita » Generovanie žiadosti o certifikát
Certifikáty CA Disig Zoznamy zrušených certifikátov (CRL) Vyhľadávanie certifikátov Dokumenty Cenník produktov a služieb Generovanie žiadosti o certifikát Následný certifikát - zmluvní partneri	Na tejto stránke si môžete pomocou prehliadača Internet Explorer (Maxthon), Netscape alebo vygenerovať žiadost o vydanie osobného certifikátu. Na základe tejto žiadosti, po overení Va autorite, Vám certifikát vydá certifikačná autorita CA Disig. Položky žiadosti prosím vyplňajte bez diakritiky. Položky vyznačené červenou farbou sú povinné. Typ certifikátu: Prosím zvďrte typ certifikátu. 💌 🛞
Informácie a návody	

2. Ako typ certifikátu zvoľte "**Osobný – Fyzická osoba - zamestnanec**". Zobrazí sa Vám nasledujúci formulár, do ktorého je potrebné zadať údaje, ktoré požadujete mať v certifikáte:

yp certifikátu:	Osobný - FO - zamestnanec
eľkosť kľúča:	High Grade
eno a Priezvisko:	
rganizácia:	
rganizačný útvar:	
esto:	
át:	sk
nail:	

Všetky údaje sa vypisujú bez diakritiky!

- Typ certifikátu: zvoľte možnosť "Osobný FO zamestnanec"
- *Typ kľúča*: zvoľte možnosť "High Grade", prípadne dĺžku (veľkosť) kľúča 2048 bitov.
- Meno a priezvisko (POVINNÝ ÚDAJ): zadajte údaje z občianskeho preukazu, pokiaľ máte titul zapísaný v OP a požadujete ho mať uvedený aj v certifikáte, zapíšte ho pred Vaše krstné meno
- Organizácia UPJS v Kosiciach, položka musí byť vyplnená touto hodnotou!!!
- Organizačný útvar (NEPOVINNÝ ÚDAJ)
- *Mesto (NEPOVINNÝ ÚDAJ)*: vypisuje sa podľa trvalého bydliska
- *Štát (POVINNÝ ÚDAJ)*: položku nemeňte, jej hodnota je SK
- *E-mail (POVINNÝ ÚDAJ)*: (školský e-mail, NIE súkromný)
- 3. Zapísané hodnoty si ešte raz skontrolujte, ak s týmito hodnotami súhlasíte, zvoľte možnosť "Generovať žiadosť". Po kliknutí na túto možnosť sa Vám zobrazí upozornenie, že žiadosť bola vygenerovaná:

Bola vygenerovaná žiadosť vo formáte SPKAC

Pre uloženie žiadosti na zvolené médium (HDD, USB, disketa) kliknite na tlačidlo

Uložiť žiadosť o certifikát

Súbor s vygenerovanou žiadosťou je potrebné doručiť v súlade s certifikačným poriadkom na registračnú autoritu CA Disig za účelom vydania certifikátu. Obsah žiadosti si môžete prezrieť otvorením uloženého súboru v ľubovoľnom textovom editore.

4. Kliknite na možnosť "Uložiť žiadosť o certifikáť", po zobrazení ďalšieho okna kliknite na "Uložiť súbor":

Generovanie žiadosti o vydanie osobného certifikátu	• • •
Ot v ára sa disig-02022009092623-27979.req 🔀	
Vybrali ste akciu otvoriť súbor alebo odkaz	
🗐 disig-02022009092623-27979.req	
ktorý je typu: Text Document	
umiestnený na serveri: http://www.disig.sk	
Čo má Firefox vykonať s týmto súborom?	
O Otvoriť pomocou Notepad (predvolené)	
© ∐ložiť súbor	
Odteraz to robiť automaticky so všetkými súbormi ako je teoto	
OK Zrušiť	

5. V závislosti od nastavenia programu Mozilla Firefox sa Vám môže zobraziť nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Prípadne sa súbor uloží na vopred nastavené miesto a pokračujete hneď bodom 6 tohto návodu. Zvoľte si cestu a kliknite na možnosť "Uložiť". Zvolenú cestu si zapamätajte, pretože túto žiadosť je potrebné doručiť na príslušnú registračnú autoritu:

Zadajte názov s	úboru na uloženie	? ×
Save jn:	🞯 Desktop 💽 🕤 😥 📰 🗸	
My Recent Documents Desktop My Documents My Computer	My Documents My Computer My Network Places New Folder disig-02022009092623-27979.req	
My Network	File <u>n</u> ame: disig-02022009092834-30153	<u>S</u> ave
Places	Save as type: Text Document	Cancel

6. Zatvorte okno "Správcu preberania súborov", tým sa proces generovania žiadosti končí:

😻 Spi	ávca preberania súborov	
	disig-02022009092623-27979.req 875 bajtov — disig.sk	10:27
Vym <u>a</u>	zať zoznam	Hl'adat'

 Ak vám už aspoň raz bol vydaný certifikát od Disigu, tak stačí odoslať vygenerovanú žiadosť mailom z emailovej adresy uvedenej v žiadosti na adresu aio@upjs.sk (tel. kontakty s ďalšími informáciami 055/2341512 alebo 055/2341514)

V prípade, že sa **zmenili** vaše osobné údaje, je **nutná** vaša **osobná návšteva registračnej autority** (Správa AIO) na Šrobárovej 2, Ing. Ondrejová, p. Sedláková) a predloženie dokladov (OP + ďalší doklad (zamestnanecký preukaz, cestovný pas, vodičský preukaz, preukaz zdravotného poistenia, ...)) s aktuálnymi osobnými údajmi spolu s vygenerovanou žiadosťou na USB kľúči (prípadne inom nosiči). Rovnako je nutná osobná návšteva ak je Vám certifikát vydávaný prvý krát, alebo ak sa ukáže, že Vaše údaje **nie sú v aplikačnej databáze prístupné** (včas budete v takom prípade vyrozumený).



2 INŠTALÁCIA OSOBNÉHO CERTIFIKÁTU

2.1 Inštalácia osobného certifikátu do systémového úložiska certifikátov MS Windows

Inštalácia osobného certifikátu vydaného certifikačnou autoritou CA Disig do systémového úložiska certifikátov MS Windows sa vykonáva v dvoch krokoch.

V prvom kroku sa vykoná inštalácia certifikátu samotnej certifikačnej autority CA Disig, čím táto bude pridaná medzi "**Dôveryhodné úrady pre vydávanie základných certifikátov**". V druhom kroku sa vykoná vlastná inštalácia osobného certifikátu.

Pre užívateľov operačného systému Windows Vista: Pretože certifikát certifikačnej autority CA Disig je súčasťou operačného systému Windows Vista, môžete v uvedenom postupe automaticky prejsť na druhý krok. Podľa návodu na stranách 2-3 tejto príručky si medzi dôveryhodné lokality musíte pridať aj stránku <u>https://www.disig.sk</u> (teda **zabezpečenú** stránku, nezabezpečenú stránku <u>http://www.disig.sk</u> ste medzi dôveryhodné lokality museli pridať už pri generovaní žiadosti).

Prvý krok - Inštalácia certifikátu certifikačnej autority CA Disig

- 1. Kliknite na https://eidas.disig.sk/sk/cacert/.
- 2. Po zobrazení stránky s aktuálnym certifikátom CA Disig kliknite na text "**DER**" v spodnej časti tabuľky "**Certifikačná autorita CA Disig**" v časti "**Formáty na stiahnutie**":

Certifikačná autorita CA Disi	g		
Sériové číslo:	01		
Platný od:	22.marca 2006 1:39:34 G	MT	
Platný do:	22.marca 2016 1:39:34 G	MT	
SHA 1 (DER):	2a c8 d5 8b 57 ce bf 2f 4	9 af f2 fc 76 8f 51 14 62 90 7	7a 41
Formáty na stiahnutie:	DER	PEM	TXT

V prípade potreby inštalácie tohto certifikátu CA Disig do prehliadača typu Netscape (Mozilla Firefox ap.) resp. MSIE verzie 4.0 a nižšej, prípadne iného softvéru kliknite SEM.

3. Po zobrazení okna s ponukou na výber akcie zvoľte "Otvoriť":



4. Otvorí sa okno s informáciami o certifikáte. Zvoľte "Inštalovať certifikát":

Certifikát 🛛 💽 🔀
Všeobecné Podrobnosti Certifikačná cesta
Informácie o certifikáte Tento základný certifikát CA nie je dôveryhodný. Ak ho chcete zaradiť medzi dôveryhodné, nainštalujte tento certifikát do priestoru na uloženie certifikátov dôveryhodných hlavných certifikačných úradov.
Vydané pre: CA Disig
Vydavateľ: CA Disig
Platný od 22.3.2006 do 22.3.2016
Inštalovať certifikát
ОК

5. Pokračujte voľbou "Ďalej >":





6. Skontrolujte, či je zvolená možnosť "Umiestniť všetky certifikáty v nasledovnom priestore" a stlačte tlačidlo "Prehľadávať":

v sú systémové oblasti, do ktorých sa ukladajú certifikáty
icky vybrať priestor na uloženie certifikátu alebo
tor na uloženie certifikátov podľa typov
ty v nasledovnom priestore
fikátov:
Prehľadávať

7. Ako priestor na uloženie certifikátov použite "Dôveryhodné úrady pre vydávanie základných certifikátov". Svoju voľbu potvrďte stlačením tlačidla "OK":

Sobné		
Dôveryhodné úrady pre vydávanie základ	dných	certifik
Dôveryhodné podnikové zdroje	Ē	
📄 Sprostredkovateľské certifikačné úrady		
📄 Dôveryhodní vydavatelia		
🦳 Nedôvervbodné certifikáty	\mathbf{x}	

- 8. Pokračujte voľbou "Ďalej >".
- 9. Kliknite na tlačidlo "Dokončiť":



Sprievodca importom certif	ikátov 🛛 🔀
	Dokončenie práce Sprievodcu importom certifikátov Sprievodca importom certifikátov úspešne dokončil prácu. Určili ste nasledovné nastavenie:
	Vybraty priestor na ulozenie certifikatov Automaticky vy Obsah Certifikát
	< <u>N</u> aspäť Dokončiť Zrušiť

10. Zobrazí sa upozornenie, že sa chystáte nainštalovať certifikát certifikačnej autority CA Disig. Na potvrdenie zvoľte "Áno":

Upozorn	ienie zabezpečenia 🛛 🔀
	Touto akciou nainštalujete certifikát od certifikačného úradu, ktorý by mal reprezentovať:
	CA Disig
	Systém Windows nemôže overiť, či certifikát skutočne pochádza od CA Disig . Pôvod certifikátu by ste mali overiť kontaktovaním certifikačného úradu CA Disig . Pri tomto postupe budete môcť použiť nasledovné číslo:
	Odtlačok (sha1): 2AC8D58B 57CEBF2F 49AFF2FC 768F5114 62907A41
	Upozornenie: Ak nainštalujete tento základný certifikát, systém Windows bude automaticky považovať za dôveryhodné všetky certifikáty vydané týmto certifikačným úradom. Inštalovanie certifikátu bez overeného odtlačku predstavuje riziko pre zabezpečenie. Ak kliknete na tlačidlo Áno, vyjadríte tým, že akceptujete toto riziko.
	Chcete nainštalovať certifikát?
	[] Nie

11. Zobrazí sa informácia o úspešnom nainštalovaní certifikátu. Inštaláciu certifikátu CA Disig ukončíte stlačením "**OK**":

Sprievo	dca importom certifikátov	×
(į)	Import úspešne prebehol.	
	ОК	

Týmto je ukončená inštalácia certifikátu certifikačnej autority CA Disig. Ďalej nasleduje inštalácia Vášho osobného certifikátu.

Druhý krok - Inštalácia osobného certifikátu

Po vydaní osobného certifikátu Vám certifikačná autorita CA Disig odošle automaticky e-mail s upozornením, že Vám bol vydaný certifikát a zároveň v ňom dostanete linku, prostredníctvom ktorej si certifikát môžete nainštalovať.

1. Kliknite na linku v e-maile, ktorá má tvar (linka sa musí otvoriť v tom webovom prehliadači, ktorý ste použili pri generovaní žiadosti o vydanie certifikátu):

https://www.disig.sk/cgi-bin/get_cert?serial=\$eSerial

(**\$eSerial** je 7 miestne sériové číslo Vášho osobného certifikátu)

2. Po kliknutí na linku sa v závislosti od nastavenie Vášho internetového prehliadača môže otvoriť okno s informáciou, že stránka, ktorá sa ide otvárať, obsahuje zabezpečené aj nezabezpečené položky. Na pokračovanie zvoľte "Áno":



3. Po stlačení "Áno" sa otvorí okno s bezpečnostným upozornením o tom, že webová stránka ide pridať nový certifikát do Vášho počítača. Na otázku, či chcete pridať tento nový certifikát do Vášho úložiska certifikátov musíte odpovedať "Áno":

Inšt

Potenti	al Scripting Violation
⚠	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	Án <u>o N</u> ie

4. V prípade, že sú splnené všetky predpoklady na úspešnú inštaláciu certifikátu, je certifikát nainštalovaný a Vám sa zobrazí nasledovné okno s oznamom o úspešnej inštalácii certifikátu:

🖉 Inštalácia certifikátu - Windows Inter	rnet Explorer	
G + ttps://www.disig.sk/cgi-bin/g	*	
Eile Edit Yiew Favorites Iools Help		
😤 🔹 🕼 Inštalácia certifikátu		
Inštalácia používateľského cert Váš certifikát bol úspešne nainšta Ďakujeme za využtie služieb CA Disig.	tifikátu alovaný.	

- 5. V prípade, že sa Vám nepodarilo nainštalovať Váš osobný certifikát prostredníctvom zaslanej linky, je ho možné nainštalovať po jeho vyhľadaní na stránkach Disig-u. Kliknite na tento odkaz a v otvorenom okne vpíšte do položky "CN" bez diakritiky celé Vaše meno, (je uvedené v bode 4. protokolu o prevzatí certifikátu). Identifikujte certifikát, ktorý hodláte nainštalovať (spravidla prvý v poradí) a následne v stĺpčeku "Inštalácia" kliknite na hrubo vytlačený nápis "Explorer". Ďalej postupujte ako je popísané v bodoch 2 až 4.
- 6. Po inštalácii je potrebné overiť nainštalovanie certifikátu. V prehliadači Internet Explorer zvoľte "Nástroje -> Možnosti siete Internet...-> Obsah -> Certifikáty":

ertifikátu	•
Možnosti siete Internet ?	×
Všeobecné Zabezpečenie Ochrana osobných údajov Obsah Pripojenia Programy Spresnenie Poradca pre obsah Hodnotenia pomáhajú regulovať internetový obsah, ktorý sa dá zobraziť na tomto počítači. Zapnúť Nastavgnie Certifikáty Zapnúť Nastavgnie Nastavgnie Vyčistiť stav SEL Certifikáty Vydavatelia Osobné údaje Osobné údaje Mutomatické dokončovanie uchováva predchádzajúce položky a navrhuje zhodné záznamy. Automatické dokončovanie Profilový asistent uchováva vaše osobné údaje. Môj profil	
OK Zrušiť P <u>o</u> užiť	

7. Správne nainštalovaný certifikát (užívateľ vlastní zodpovedajúci privátny kľúč) sa po inštalácii nachádza v záložke "**Ósobné**":



jovaný účel:	(Všetky>		
sobné Ostatní Spro	ostredkovateľské certifikačné	úrady Dôveryh	odné úrady pre vydá [.]
Vydané pre	Vydavateľ	Platnosť do	Popisný názov
🕮 Michal Dur	CA Disig	28.3.2007	
portovať) <u>E</u> xporto	vať) Odstrániť		Spresn
portovať) (<u>E</u> xporto ánované účely certifika	wať) Odstrániť		Spresn
portovať) (Exporto ánované účely certifika verenie klienta, Zabez)	vať) <u>O</u> dstrániť átu pečený e-mail		<u>Spresn</u> <u>Z</u> obraziť

8. Po označení certifikátu kliknutím na Vaše meno a zvolením možnosti "Zobraziť" sa certifikát otvorí. Ak je všetko v poriadku, tak sa v záložke "Všeobecné" nachádza pod vyznačením platnosti text "Máte súkromný kľúč, ktorý zodpovedá tomuto certifikátu", v záložke "Certifikačná cesta " sú zobrazené oba inštalované certifikáty a v spodnej časti je vypísané "Tento certifikát je v poriadku":



Certifikát	? 🛛
Všeobecné Podrobnosti Certifikačná cesta	
<u>C</u> ertifikačná cesta	
CA Disig - Disig a.s.	
	Zobraziť certifikát
Stav certifikátu:	
Tento certifikát je v poriadku.	
	ОК

9. Týmto je ukončená inštalácia Vášho osobného certifikátu.

V prípade úspešného overenia funkčnosti ako ďalší krok jednoznačne odporúčame vykonať zálohu nainštalovaného certifikátu podľa postupu, ktorý je popísaný v kapitole "Zálohovanie a obnova osobného certifikátu".

Poznámka: V prípade, že sa Váš certifikát po inštalácii nenachádza v záložke "**Osobné**", ale je uložený napríklad v záložke "**Ostatní**", je pravdepodobné, že Váš systém nie je schopný zistiť umiestnenie Vášho privátneho kľúča a tým úspešne nainštalovať certifikát. Skôr ako sa pokúsite o opakovanú inštaláciu, kontaktujte podporu CA Disig.

2.2 Inštalácia osobného certifikátu do systémového úložiska certifikátov Mozilla Firefox

Dôležité upozornenie: Webový prehliadač Mozilla Firefox **zvyčajne nezdieľa systémové úložisko certifikátov** s ďalším softvérom (ani typu Mozilla, ako je napr. poštový klient Thunderbird, ...). Z toho dôvodu je potrebné ešte importovať certifikáty aj do ďalších programov (popisujú to nasledujúce kapitoly 3.1 až 3.4).

Inštalácia osobného certifikátu vydaného certifikačnou autoritou CA Disig do systémového úložiska Mozilla sa vykonáva v dvoch krokoch.

V prvom kroku sa vykoná inštalácia osobného certifikátu. V druhom kroku sa vykoná inštalácia certifikátu vydávajúcej certifikačnej CA Disig do úložiska dôveryhodných certifikačných autorít.

2.2.1 Prvý krok - Inštalácia osobného certifikátu

Po vydaní osobného certifikátu Vám certifikačná autorita CA Disig odošle automaticky e-mail s upozornením, že Vám bol vydaný certifikát a zároveň v ňom dostanete linku, prostredníctvom ktorej si certifikát môžete nainštalovať.

1. Kliknite na linku v e-maile, ktorá má tvar (linka sa musí otvoriť v tom webovom prehliadači, ktorý ste použili pri generovaní žiadosti o vydanie certifikátu):

https://www.disig.sk/cgi-bin/get_cert?serial=\$eSerial

(**\$eSerial** je 7 miestne sériové číslo Vášho certifikátu)

2. V prípade, že sa objaví výzva na zadanie hlavného hesla, zadajte heslo a pokračujte kliknutím na "OK".

Poznámka: Hlavné heslo je heslo, ktorým je chránený prístup k súkromným kľúčom daného užívateľa. Toto heslo, pokiaľ je aktivované, si zvolil samotný užívateľ už predtým v nastaveniach príslušného programu Mozilla:

Výzva	
?	Zadajte prosím hlavné heslo pre Softvérové bezpečnostné zari.
	OK Zrušiť

3. Podľa použitej verzie prehliadača sa Vám zobrazí okno s oznamom o úspešnej inštalácii osobného certifikátu. U starších verzii sa toto okno nemusí zobraziť. Zároveň ste upozornený aj na potrebu vytvorenia zálohy práve nainštalovaného certifikátu (pozrite kapitolu "Zálohovanie a obnova osobného certifikátu"):

Alert	
	Your personal certificate has been installed. You should keep a backup copy of this certificate.
	ОК

4. Na overenie, či inštalácia skutočne prebehla kliknite na "Nástroje" v hlavnom menu príslušného programu Mozilla a zvoľte "Možnosti". Potom zvoľte "Pokročilé" (prípadne "Rozšírené") (pre staršie verzie programov "Ostatné"), ďalej zvoľte záložku "Šifrovanie" (prípadne "Zabezpečenie") a nakoniec tlačidlo "Certifikáty" (alebo tlačidlo "Správa certifikátov"):

[©] Univerzita Pavla Jozefa Šafárika v Košiciach 2008

•	ţ,	ė	i	•)	•	•••	•

Certifika	.tu						
ožnosti							
<u>†</u>			3	9		Ô	
Hlavné	Karty	Obsah	Kanály	Súkromie	Bezpečnosť	Pokročilé	
/šeobecné	Sieť Akł	tualizácie	Šifrovanie				
Protok	ioly ——						
P	oužiť SSL 3	<u>)</u> .0		🗹 Použ	iť TLS <u>1</u> .0		
c Certifi	kátv —						\leq
Pokiaľ	stránka po	ožaduje cer	tifikát:				
💿 V;	ybrať auto	<u>m</u> aticky	🔿 Vždy sa	a opý <u>t</u> ať			
				<u> </u>			
<u>C</u> ert	itikáty	Z <u>r</u> ušené o	ertifikáty	Overenie	platnosti Z	ariadenia	
				ОК	Zrušiť	Pomo	cník

5. Otvorí sa okno "**Správca certifikátov**". Po úspešnej inštalácii musí byť certifikát uložený v okne "**Správca certifikátov**" v záložke "**Vaše certifikáty** (prípadne **Osobné certifikáty**)":

e E
007
007

Poznámka: V prípade, že sa Váš certifikát po inštalácii nenachádza v záložke "**Osobné**", ale je uložený napríklad v záložke "**Certifikáty iných ľudí**", je pravdepodobné, že Váš systém nie je schopný zistiť umiestnenie Vášho privátneho kľúča a tým úspešne nainštalovať certifikát. Skôr ako sa pokúsite o opakovanú inštaláciu, kontaktujte podporu CA Disig.

6. V prípade, že sa Vám nepodarilo nainštalovať Váš osobný certifikát prostredníctvom zaslanej linky, je ho možné nainštalovať po jeho vyhľadaní na stránkach Disig-u. Kliknite na tento odkaz a v otvorenom okne vpíšte do položky "CN" bez diakritiky celé Vaše meno, (je uvedené v bode 4. protokolu o prevzatí certifikátu). Identifikujte certifikát, ktorý hodláte nainštalovať (spravidla prvý v poradí) a následne v stĺpčeku "Inštalácia" kliknite na hrubo vytlačený nápis "Mozilla". Ďalej postupujte ako je popísané v bodoch 2 až 5.

Druhý krok - Inštalácia certifikátu certifikačnej autority CA Disig

- 1. Kliknite na https://eidas.disig.sk/sk/cacert/.
- 2. Po zobrazení stránky s aktuálnym certifikátom CA Disig kliknite na text "**DER**" v časti Formáty na stiahnutie:



Certifikačná autorita CA Disi	g		
Sériové číslo:	01		
Platný od:	22.marca 2006 1:39:34 G	ИT	
Platný do:	22.marca 2016 1:39:34 G	МΤ	
SHA 1 (DER):	2a c8 d5 8b 57 ce bf 2f 49	af f2 fc 76 8f 51 14 62 90 7	7a 41
Formáty na stiahnutie:	DER	PEM	тхт

V prípade potreby inštalácie tohto certifikátu CA Disig do prehliadača typu Netscape (Mozilla Firefox ap.) resp. MSIE verzie 4.0 a nižšej, prípadne iného softvéru kliknite SEM.

3. Po kliknutí na text "**DER**" sa Vám otvorí nasledovné okno. Zvoľte možnosť "**Uložiť súbor**" a potvrďte ju stlačením tlačidla "**OK**". Ďalej uložte súbor do Vami určeného (prípadne preddefinovaného) priečinku.

Otvára sa ca_disig. der	\mathbf{X}
Vybrali ste akciu otvoriť súbor alebo odkaz	
🔤 ca_disig.der	
ktorý je typu: Súbor DER	
umiestnený na serveri: http://www.disig.sk	
CČo má Firefox vykonať s týmto súborom?	_
O Otvoriť pomocou Prehľadávať	
⊙ ∐ložiť súbor	
Odterat to robiť sutomaticku so učetkými súborni ako je tento	

4. Kliknite na "Nástroje" v hlavnom menu príslušného programu Mozilla a zvoľte "Možnosti". Potom zvoľte "Pokročilé" (prípadne "Rozšírené") (pre staršie verzie programov "Ostatné"), d'alej zvoľte záložku "Šifrovanie" (prípadne "Zabezpečenie") a nakoniec tlačidlo "Certifikáty" (alebo tlačidlo "Správa certifikátov"). V otvorenom okne "Správcu certifikátov" vyberte záložku "Autority":



aše certifikáty Ľudia Servery Autority	Iné	
Máte uložené certifikáty, ktoré identifikuj	jú tieto certifikačné autority:	
Názov certifikátu	Bezpečnostné zariadenie	C.
🖃 (c) 2005 TÜRKTRUST Bilgi İletişim ve B	3ilişi	^
TÜRKTRUST Elektronik Sertifika Hi:	zme Builtin Object Token	
E ABA.ECOM, INC.		
ABA.ECOM Root CA	Builtin Object Token	
🖃 AC Camerfirma SA CIF A82743287		
Chambers of Commerce Root	Builtin Object Token	
Global Chambersign Root	Builtin Object Token	
🖃 AddTrust AB		
AddTrust Class 1 CA Root	Builtin Object Token	
AddTrust External CA Root	Builtin Object Token	~
Zobraziť	tovať Exportovať O <u>d</u> strániť	

- 5. Kliknite na "Importovat'...", vyhľadajte a otvorte súbor, ktorý ste uložili bode 3.
- 6. Otvorí sa Vám okno "**Sťahuje sa certifikát**", kde je potrebné zaškrtnúť všetky možnosti a pokračovať kliknutím na "**OK**":

Sťahuje sa certifikát				
Ste požiadaní dôverovať novej certifikačnej autorite.				
Chcete dôverovať "CA Disig" pre nasledujúce účely:				
🗹 Dôverovať tejto certifikačnej autorite pri identifikácii serverov.				
Dôverovať tejto certifikačnej autorite pri identifikácii poštových užívateľov.				
Dôverovať tejto certifikačnej autorite pri identifikácii výrobcov softvéru.				
Predtým ako sa rozhodnete dôverovať tejto CA pre akýkoľvek účel, mali by ste preveriť jej certifikát, jeho politiku a procedúry (ak sú prítomné).				
Zobraziť Preskúšať certifikát certifikačnej agentúry				
OK Zrušiť				

7. Po úspešnej inštalácii musí byť certifikát certifikačnej autority CA Disig umiestnený v záložke "**Autority**" v okne "**Správca certifikátov**":



secercinicaty Cercinicaty information Servery	PROVINCY	
Máte uložené certiřikáty, ktoré identiřikujú tieto	o certifikačné autority:	
Meno certifikátu	Bezpečnostné zariadenie	C.
Comodo CA Limited		^
-AAA Certificate Services	Builtin Object Token	
-Secure Certificate Services	Builtin Object Token	(B)
Trusted Certificate Services	Builtin Object Token	
Digital Signature Trust Co.		
Digital Signature Trust Co. Global CA 1	Builtin Object Token	
-Digital Signature Trust Co. Global CA 3	Builtin Object Token	
DST RootCA X1	Builtin Object Token	
DST RootCA X2	Builtin Object Token	
Disig a.s.		
	Softvérové bezpečnostné zari	
Entrust.net		~
Zobraziť Upraviť Importovať	Vymazať	

8. Týmto je ukončená inštalácia certifikátu certifikačnej autority CA Disig.

3 ZÁLOHOVANIE A OBNOVA OSOBNÉHO CERTIFIKÁTU

3.1 Zálohovanie (export) osobného certifikátu zo systémového úložiska certifikátov MS Windows

Zálohu užívateľského certifikátu zo systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

- 1. Otvorte program Internet Explorer. V hlavnom menu programu kliknite na "**Nástroje**". Zobrazí sa roletové menu. V ňom kliknite na "**Možnosti siete Internet...**".
- 2. V zobrazenom okne vyberte záložku "Obsah" a potom kliknite na tlačidlo "Certifikáty...":

Možnosti siete Internet 🛛 🖓 🔀				
Všeobecné Zabezpečenie Ochrana osobných údajov Obsah Pripojenia Programy Spresnenie				
Poradca pre obsah Hodnotenia pomáhajú regulovať internetový obsah, ktorý sa dá zobraziť na tomto počítači. Zapnúť				
Certifikáty Certifikáty umožňujú, aby ste mohli bezpečne identifikovať seba, certifikačné úrady a vydavateľov.				
Osobné údaje Funkcia Automatické dokončovanie uchováva predchádzajúce položky a navrhuje zhodné záznamy.				
<u>Automatické dokončovanie</u> Profilový asistent uchováva vaše osobné údaje. Môj pro <u>f</u> il				

3. Zobrazí sa okno s certifikátmi. Overte, či je zobrazená záložka "**Osobné**". Zvoľte certifikát, ktorý chcete zálohovať. Stlačte tlačidlo "**Exportovať...**":

Certifikáty			? 🗙
Plánovaný účel: <vše Osobné Ostatní Sprostre</vše 	tky> :dkovateľské certifikaj	čné úrady 🛛 Dôveryhodné úrady pre vyd	↓ á• ↓
Vydané pre 🔛 🖼 Michal Dur	Vydavateľ CA Disig	Platnosť do Popisný názov 28.3.2007	
Importovať) Exportovať Plánované účely certifikátu Overenie klienta, Zabezpeče) <u>O</u> dstrániť	Spres Zobraz	miť

κ.

Т

4. Pokračujte voľbou "**Ďalej** >":

Sprievodca exportom cert	ifikātov	X
	Víta vás Sprievodca exportom certifikátov Tento sprievodca vám pomôže skopírovať certifikáty, zoznamy dôveryhodných certifikátov a zoznamy zrušených certifikátov z priestoru na uloženie certifikát vydaný certifikačným úradom je potvrdením vašej totožnosti a obsahuje informácie potrebné na ochranu údajov alebo na vytvorenie zabezpečených sieťových pripojení. Priestor na uloženie certifikátov je systémová oblasť, v ktorej sú certifikáty uložené. Pokračujte kliknutím na tlačidlo Ďalej.	
	< <u>N</u> aspäť <mark>Ďalej > Zruši</mark>	ť

5. Zvoľte položku "Áno, exportovať privátny kľúč". Pokračujte voľbou "Ďalej >":

S	prievodca exportom certifikátov	×			
	Export súkromného kľúča Môžete zvoliť export súkromného kľúča spolu s certifikátom.				
	Súkromné kľúče sú chránené heslom. Ak chcete s certifikátom exportovať aj súkromné kľúče, musíte na niektorej z ďalších strán zadať heslo.				
	Chcete s certifikátom exportovať aj súkromný kľúč?				
	Áno, exportovať súkromný kľúč				
	🚫 <u>N</u> ie, neexportovať súkromný kľúč				
	< <u>N</u> aspäť Ď <u>a</u> lej > Zrušiť				

6. Zvoľte nastavenia podľa obrázku a pokračujte voľbou "Ďalej >":

Sp	rievodca exportom certifikátov 🛛 🔀				
	Formát exportného súboru Certifikáty je možné exportovať v rôznych formátoch.				
	Vyberte formát, ktorý chcete použiť:				
	O Binárny X.509 s kódovaním <u>D</u> ER (.CER)				
	🔿 X509 s kódovaním Ba <u>s</u> e-64 (.CER)				
	🔘 <u>C</u> ertifikáty štandardu Cryptographic Message Syntax - PKCS #7 (.P7B)				
	Zahrnúť všetky certifikáty v rámci certifikačnej cesty, ak je to možné				
	Standard Personal Information Exchange - PKCS #12 (.PFX)				
	Za <u>h</u> rnúť všetky certifikáty v rámci certifikačnej cesty, ak je to možné				
	🗹 Zapnúť vysoký stupeň ochrany (vyžaduje sa IE 5.0, NT 4.0 SP4 alebo vyššie verzie)				
	🔲 V prípade úspešného exportu odstrániť súkromný 🖞 úč				
	< <u>N</u> aspäť Ď <u>a</u> lej > Zrušiť				

 Napíšte heslo, ktorým bude chránený Váš privátny kľúč do poľa "Heslo" a zopakujte ho v poli "Potvrdiť heslo". Pokračujte voľbou "Ďalej >":

Sprievodca exportom certifikátov 🛛 🔀
Heslo Na zaistenie bezpečnosti musíte súkromné kľúče chrániť heslom.
Zadajte a potvrďte heslo. <u>H</u> eslo: P <u>o</u> tvrdiť heslo:
< <u>N</u> aspäť D <u>a</u> lej > Zrušiť

8. Napíšte meno, pod akým sa má súbor uložiť a cestu k nemu alebo kliknite na tlačidlo "**Prehľadávať…**", vyberte adresár, do ktorého sa má súbor uložiť a napíšte meno súboru. Pokračujte voľbou "Ďalej >":

Sprievodca exp	ortom certifikátov		×
Súbor na expo Zadajte náz	rt ov súboru, ktorý chcete ex	portovať	
Ná <u>z</u> ov súbo	ru:		
E:\zaloha_	cert\DurDisig.pf×		Prehľadávať
		< <u>N</u> aspäť Ď <u>s</u>	alej > Zrušiť

9. Kliknite na tlačidlo "Dokončiť":



10. Ak je privátny kľúč chránený heslom, otvorí sa okno, kde ho môžete zadať. Pokračujte voľbou "**OK**":

Exportuje sa	váš súkromný výmenný kľúč	×
	Aplikácia požaduje prístup k chránenej položke. Súkromný kľúč CryptoAPI	
	OK Zrušiť Po <u>d</u> robnosti.	

11. Zobrazí sa okno oznamujúce, že export certifikátu bol úspešný. Export ukončite voľbou "OK":



3.2 Zálohovanie (export) osobného certifikátu zo systémového úložiska certifikátov Mozilla

Zálohu užívateľského certifikátu zo systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

 Otvorte program Mozilla Thunderbird alebo Mozilla Firefox. V hlavnom menu programu kliknite na "Nástroje". Zobrazí sa roletové menu. V ňom kliknite na "Možnosti... ". Potom zvoľte "Rozšírené" (prípadne "Pokročilé") (pre staršie verzie programov "Ostatné") a ďalej zvoľte záložku "Certifikáty" (prípadne "Šifrovanie "):

Aa Zobrazení	Vytváření	Soukromí	Přílohy	Rozšířené
ní a místo na dis rtifikáty, seznar	ku Aktualizovat ny zneplatnění, ov	Certifikáty věřování platnos	ti a bezpečnostní	zařízení
áty Znep	olatnění	věřování	<u>B</u> ezpečnostní zai	řízení
			ОК	Zrušit
	Aa Zobrazení sní a místo na dis rtifikáty, seznam áty Znep	Aa Zobrazení Vytváření ní a místo na disku Aktualizovat rtifikáty, seznamy zneplatnění, o áty Zneplatnění C	Aa Vytváření Soukromí sní a místo na disku Aktualizovat Certifikáty rtifikáty, seznamy zneplatnění, ověřování platnos áty Zneplatnění Qvěřování	Ad Vytváření Soukromí Přilohy sní a místo na disku Aktualizovat Certifikáty rtifikáty, seznamy zneplatnění, ověřování platnosti a bezpečnostní áty Zneplatnění Qvěřování Bezpečnostní zai

2. Stlačte tlačidlo "Certifikáty" (prípadne "Správa certifikátov"). Týmto sa otvorí okno "Správca certifikátov". Vyberte záložku "Osobné certifikáty":

sprawce certi	íikátů					
sobní certifikáty	Ostatní certifikáty	Servery Certif	ikační autority			
Pro vaši osobní i	dentifikaci máte dos	tupné následujíc	í certifikáty:			
Jméno certifiká	tu Bezpečn	ostní zařízení	Účel	Sériové číslo	Platný do	EŞ.
🗆 Disig a.s.						
Michal Dur	Bezpečno	stní zařízení SW	Klient,Po	50:6A:3A	30,10,2009	

- 3. Kliknite na vaše meno a potom na tlačidlo "Zálohovať".
- 4. Prostredníctvom dialógového okna určte názov súbor s vašim osobným certifikátom a jeho umiestnenie vo Vašom počítači. Vaše nastavenie potvrď te stlačením tlačidla "Uložiť":

Název souboru	pro zálohu				? 🔀
Uložjť do:	🞯 Pracovná plo	cha 💌	GØØ	• •	
Naposledy použité Pracovná plocha Moje dokumenty	Moje dokument Tento počitač	Υ			
	<u>N</u> ázov súboru:	michaldur		~	<u>U</u> ložíť
Miesta v sieti	Uložiť vo formá <u>t</u> e:	PKCS12 Soubory		~	Zrušiť

5. Otvorí sa okno, kde musíte hlavné heslo, ktorým sú v programe Mozilla chránené Vaše osobné údaje. Pokračujte voľbou "**OK**":

Požado	váno heslo 🛛 🔀
?	Prosím zadejte hlavní heslo pro Bezpečnostní zařízení SW.

	OK Zrušit

6. Napíšte heslo, ktorým bude chránená záloha Vášho osobného certifikátu do poľa "Heslo zálohy certifikátu" a zopakujte ho v poli "Heslo zálohy certifikátu (znovu)". Pokračujte voľbou "OK":

Heslo zálohy certifikátu, které si z Abyste mohli pokračovat dále, mu	de nastavíte, chrání vaše soubory zál síte toto heslo zadat.	ohy, kterou se chystáte vytvořit.
Heslo zálohy certifikátu:	****	
Heslo zálohy certifikátu (znovu):	****	
Důležité: Pokud zapomenete svoje	heslo zálohy certifikátu, nebude poz	ději možno tuto zálohu obnovit.
Heslo si poznamenejte na BEZPEČ	NE misto.	
Heslo si poznamenejte na BEZPEČ Kvalita hesla	NE misto.	
Heslo si poznamenejte na BEZPEČ Kvalita hesla	NE misto.	

7. Zobrazí sa okno oznamujúce, že export certifikátu bol úspešný. Export ukončíte voľbou "OK":

Výstrah	ia 🛛 🛛
<u>.</u>	Váš(e) bezpečnostní certifikát(y) a privátní klíč(e) byly úspěšně zálohovány.

3.3 Obnova (import) osobného certifikátu do systémového úložiska certifikátov MS Windows

Obnovu užívateľského certifikátu do systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

 Najskôr je potrebné použiť médium s uloženou zálohou (HDD, disketa, USB kľúč) a prejsť do adresára, kde je uložená záloha Vášho certifikátu (napr. E:\zaloha_cert). Potom dvakrát rýchlo kliknite na súbor so zálohou certifikátu, alebo kliknite na súbor so zálohou certifikátu a stlačte Enter:

E:\zaloha_cert			
Súbor Úpr <u>a</u> vy Zobraziť <u>O</u> bľúbené j	położky Nástroje Bomocnik		
🌏 Dozadu 🔹 🌍 - 🍺 🔎	Hľadať 🏀 Priečinky 🛄 -		
gresa 🎃 E:\zaloha_cert\			Prejsl
	Názov 🗢	Veľkosť Typ	Dátum zmeny
Súbory a priečinky – úlohy 😤	DurDisig.pfx	3 kB Výmena oso	bných i 25.3.2006 12:54
Dremenovať súbor			
Premiestnit' súbor			
Kopírovať súbor			
Publikovať súbor na webe			
🙆 Odoslať súbor e-mailom			
X Odstrániť súbor			
Ďalšie miesta			
Removable Disk (E:)			
Moje dokumenty			
Into poctac			
S Miesta v seti			
Podrobnosti 🛞			
DuvDicia ofu			
Výmena osobných informácií			
Dátum zmeny: 25. marca 2006, 12:5	4		
Velkost: 2,02 kB			
	Co.		

2. Otvorí sa úvodné okno sprievodcu importom certifikátu. Kliknite na tlačidlo "Ďalej >":

Sprievodca importom cert	ifikátov	×
	Víta vás Sprievodca importom certifikátov Tento sprievodca vám pomôže skopírovať certifikáty, zoznamy dôveryhodných certifikátov a zoznamy zrušených certifikátov z pevného disku do priestoru na uloženie certifikátov. Certifikát vydaný certifikačným úradom je potvrdením vašej totožnosti a obsahuje informácie potrebné na ochranu údajov alebo na vytvorenie zabezpečených sieťových pripojení. Priestor na uloženie certifikátov je systémová oblasť, v ktorej sú certifikáty uložené. Pokračujte kliknutím na tlačidlo Ďalej.	
	< <u>N</u> aspäť <mark>Ďalej > Zrušit</mark>	·

3. Pokračujte voľbou "**Ďalej** >":

Sprievodca importom certifikátov
Súbor na import Zadajte súbor, ktorý chcete importovať.
Ná <u>z</u> ov súboru: E:\zaloha_cert\DurDisig.pfx Prehľadávať
Poznámka. V jednom súbore v nasledovných formátoch môže byť uložených viacero certifikátov:
Štandard Personal Information Exchange- PKCS #12 (.PFX,.P12)
Certifikáty štandardu Cryptographic Message Syntax - PKCS #7 (.P7B)
Priestor certifikátov Microsoft Serialized Certificate Store (*.SST)
< <u>N</u> aspäť Ď <u>a</u> lej > Zrušiť

4. Napíšte heslo, ktorým je chránený Váš privátny kľúč. Zaškrtnite prvú možnosť ak chcete zvýšenú ochranu privátneho kľúča. Zaškrtnite druhú možnosť ak chcete, aby sa certifikát dal znovu zálohovať (Odporúčame zaškrtnúť obe možnosti). Pokračovať voľbou "Ďalej >":

Sprievodca importom certifikátov	×
Heslo Na zaistenie bezpečnosti bol súkromný kľúč ochránený heslom.	
Zadajte heslo pre súkromný kľúč.	
Heslo:	
☑ Zapnúť vysokú úroveň ochrany súkromného kľúča. (Pri každom použití kľúča nejakou aplikáciou sa zobrazí upozornenie.)	
Označiť tento kľuč ako exportovateľný. Toto vám neskôr umožní zálohovať alebo prenášať vaše kľúče.	
< <u>N</u> aspäť Ď <u>a</u> lej > Zrušiť	

5. Skontrolujte, či je zvolená možnosť "Umiestniť všetky certifikáty v nasledovnom priestore" a stlačte tlačidlo "**Prehľadávať**":

prievodca importom certifikáto	v 🛛 🛛
Priestor na uloženie certifikátov	
Priestory na uloženie certifikátov :	sú systémové oblasti, do ktorých sa ukladajú certifikáty.
Systém Windows môže automatick môžete zadať jeho umiestnenie.	vy vybrať priestor na uloženie certifikátu alebo
🚫 Automaticky vybrať priesto	r na uloženie certifikátov podľa typov
💿 Umiestniť všetky certifikáty	v nasledovnom priestore
Priestor na uloženie certifik	átov:
	Prehľadávať

6. Ako priestor na uloženie certifikátov použite "**Osobné**". Svoju voľbu potvrďte stlačením tlačidla "**OK**":



- 7. Pokračujte voľbou "**Ďalej** >":
- 8. Importovanie ukončite voľbou "Dokončiť":

Sprievodca importom certifikátov 🛛 🔀					
	Dokončenie práce Sprievo importom certifikátov Sprievodca importom certifikátov úspešne o Určili ste nasledovné nastavenie: Vybratý priestor na uloženie certifikátov Obsah Názov súboru	Jokončil prácu. Automaticky vy PFX E:\zaloha_cert\			
	< <u>N</u> aspäť Dokončiť	Zrušiť			

- Ak ste zvolili zvýšenú ochranu privátneho kľúča, pokračujte bodom 10, inak pokračujte bodom 14.
- 10. Kliknite na tlačidlo "Nastaviť úroveň zabezpečenia...":



11. Zvoľte "Vysoká" a pokračujte voľbou "Ďalej >":



12. Napíšte heslo ktorým chcete chrániť Váš privátny kľúč do poľa "**Heslo**" a zopakujte ho v poli "**Potvrdiť**". Pokračujte voľbou "**Dokončiť**":

Importuje sa nový sú	cromný výmenný	kľúč 🛛 🔀
	Vytvoriť heslo na (ochranu tejto položky.
	Vytvoriť nové hesl Heslo pre: Heslo: Potvrdiť:	o pre túto položku. Súkromný kľúč CryptoAP
	< Nası	uäř <u>D</u> okončíť Zrušíť

13. Pokračujte voľbou "OK":

Importuje sa	nový súkromný výmenný kľúč 🛛 🔀
	Aplikácia vytvára chránenú položku.
	Súkromný kľúč CryptoAPI
R	Úroveň zabezpečenia je nastavená na hodnotu Vysoká
	Na <u>s</u> taviť úroveň zabezpečenia
	OK Zrušiť Po <u>d</u> robnosti

14. Po úspešnom importovaní certifikátu za zobrazí okno oznamujúce, že import certifikátu bol úspešný. Importovanie ukončíte voľbou "**OK**":

Sprievo	dca importom certifikátov 🔀
٩	Import úspešne prebehol.
	ОК

3.4 Obnova (import) osobného certifikátu do systémového úložiska certifikátov Mozilla

Obnovu užívateľského certifikátu do systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

 Otvorte program Mozilla Thunderbird alebo Mozilla Firefox. V hlavnom menu kliknite na "Nástroje". Zobrazí sa roletové menu. V ňom kliknite na "Možnosti ...". Potom zvoľte " Rozšírené" (prípadne "Pokročilé") (pre staršie verzie programov "Ostatné") a ďalej zvoľte záložku "Certifikáty" (prípadne "Šifrovanie"):

Možnosti					
Dbecné	Aa Zobrazení	Vytváření	Soukromí	Přilohy	Rozšířené
Obecné Připo	ojení a místo na dis	iku Aktualizovat	Certifikáty		
Spravovat o	ertifikáty, seznam	ny zneplatnění, ov platnění	věřování platnos věřování	sti a bezpečnostní Bezpečnostní zaj	zařízení řízení
					_

2. Stlačte tlačidlo "Certifikáty" (alebo "Správa certifikátov"). Týmto sa otvorí okno "Správca certifikátov". Vyberte tu záložku "Osobné certifikáty":

Pro vaši osobní identifik	aci máte dostupné následu	ující certifikáty:			
Jméno certifikátu	Bezpečnostní zařízení	Účel	Sériové číslo	Platný do	Ę
Zobrazit Zálol	novat Zálohovat vše	Importovat	Smazat		

- 3. Zvoľte tlačidlo "Importovať".
- 4. Otvorí sa dialógové okno, prostredníctvom ktorého nájdite súbor so zálohou Vášho osobného certifikátu. Výber potvrďte tlačidlo "**Otvoriť**":

Název souboru	pro obnovení				? 🛛
<u>K</u> de hľadať:	🞯 Pracovná plo	ocha 💌	GØP	•	
Naposledy použité	Moje dokumer Tento počítač Miesta v sieti michaldur;	nty p12			
Pracovná plocha					
Moje dokumenty					
Tento počítač					
	<u>N</u> ázov súboru:	michaldurp12		~	<u>O</u> tvoriť
Miesta v sieti	Súbory <u>t</u> ypu:	PKCS12 Soubory		~	Zrušiť

8. Zadajte hlavné heslo, ktorým sú v programe Mozilla chránené Vaše osobné údaje. Pokračujte voľbou "**OK**":

Požado	váno heslo 🛛 🛛 🕅
?	Prosím zadejte hlavní heslo pro Bezpečnostní zařízení SW.
2	*******
	OK Zrušit

5. Zadajte heslo, ktorým je chránená záloha Vášho osobného certifikátu. Pokračujte voľbou "OK":

Dialog z	adání hesla			
Prosím z certifiká	adejte heslo, kte tu.	eré bylo použi	to pro za	šifrování zálohy
Heslo:	****		ок	7ručit

6. Po úspešnom importovaní certifikátu za zobrazí okno oznamujúce, že import certifikátu bol úspešný. Importovanie ukončíte voľbou "**OK**":





4 VYUŽÍVANIE OSOBNÉHO CERTIFIKÁTU

Osobný certifikát je možné využiť na podpisovanie e-mailových správ a dokumentov a taktiež na šifrovanú komunikáciu prostredníctvom e-mailov. Na odoslanie šifrovanej správy je však potrebné mať nainštalovaný aj certifikát adresáta.

4.1 Import certifikátov iných osôb do systémového úložiska certifikátov MS Windows

Import certifikátu inej osoby (a tým zároveň jej verejného kľúča) do systémového úložiska certifikátov MS Windows vykonáte podľa nasledovného postupu:

- 1. Kliknite na https://eidas.disig.sk/sk/crtsearch/.
- V otvorenom okne vpíšte do položky "CN" bez diakritiky celé meno osoby, ktorej bol certifikát vydaný. Identifikujte certifikát, ktorý hodláte nainštalovať a následne kliknite na text "DER" v časti "Stiahnutie":

Údaje na vyhľadá	vanie zadávajte	prosím bez d	liakritiky.	
Typ certifikátu: CN:	Obyčajný certifiká	t 🧕		
E-mail:	Hľadať		0	
CN a E-mail	Sériové číslo	Stiahnutie	Inštalácia	
Michal Dur michal.dur@upjs.sk Certikát je platný	507c67 hex 5380643 dec	DER PEM TXT	Explorer Outlook	

3. Po zobrazení okna s ponukou na výber akcie zvoľte "Otvoriť":

Preberani	e súboru - upozornenie zabezpečenia	×
Chcete o	otvoriť alebo uložiť tento súbor?	
	Meno: Michal Durder Typ: Certifikát zabezpečenia, 1,01 KB Od: www.disig.sk Otvorit Uložit Zrušit	
	Súbory z internetu sú obyčajne užitočné, ale tento typ súboru mô: syť pre počítač škodlivý. Ak nedôverujete zdroju tohto súboru, neotvárajte ani neukladajte tento softvér. <u>Aké sú riziká?</u>	že

4. Otvorí sa okno s informáciami o certifikáte. Zvoľte "Inštalovať certifikát":

rtifikát		?
šeobecné	Podrobnosti Certifikačná cesta	
	Informácie o certifikáte	
Tento •	certifikát sa bude používať na nasledovné účely: Dokazuje vašu identitu vzdialenému počitaču Chráni e-mailové správy	_
2 v	ydané pre: Michal Dur	
v	ydavateľ: CA Disig	
Р	latný od 11.11.2008 do 11.11.2009	
1	Inštalovať certifikát Vyhlásenie vydava	ateľa
		ок

5. Pokračujte voľbou "**Ďalej** >":

Sprievodca importom certi	fikátov	×
	Víta vás Sprievodca importom certifikátov Tento sprievodca vám pomôže skopírovať certifikáty, zoznamy dôveryhodných certifikátov a zoznamy zrušených certifikátov z pevného disku do priestoru na uloženie certifikátov. Certifikát vydaný certifikačným úradom je potvrdením vašej totožnosti a obsahuje informácie potrebné na ochranu údajov alebo na vytvorenie zabezpečených sieťových pripojení. Priestor na uloženie certifikátov je systémová oblasť, v ktorej sú certifikáty uložené. Pokračujte kliknutím na tlačidlo Ďalej.	
	< <u>N</u> aspäť Ď <u>a</u> lej > Zrušiť	

6. Skontrolujte, či je zvolená možnosť "Umiestniť všetky certifikáty v nasledovnom priestore" a stlačte tlačidlo "Prehľadávať":

Sprievodca importom certifikátov
Priestor na uloženie certifikátov
Priestory na uloženie certifikátov sú systémové oblasti, do ktorých sa ukladajú certifikáty.
Systém Windows môže automaticky vybrať priestor na uloženie certifikátu alebo môžete zadať jeho umiestnenie.
O Automaticky vybrať priestor na uloženie certifikátov podľa typov
💿 Umiestniť všetky certifikáty v nasledovnom priestore
Priestor na uloženie certifikátov:
Prehľadávať
<pre>< Naspäť Ďalej > Zrušiť</pre>

7. Ako priestor na uloženie certifikátov použite "**Ostatní**". Svoju voľbu potvrďte stlačením tlačidla "**OK**":

Vyberte pr chcete pou	riestor na uloženie užiť.	certifikátov,	ktorý
)ôveryhodní vyda: Jedôveryhodné ce Jezávislé úrady pr Dôveryhodní Ostatní	vatelia rtifikáty e vydávanie	základný 📲
<)	>
Zobraz	iť fyzické priestory	/ na uloženie	700 211

- 8. Pokračujte voľbou "Ďalej >".
- 9. Kliknite na tlačidlo "Dokončiť":

Sprievodca importom cert	tifikátov 🛛 🛛
	Dokončenie práce Sprievodcu importom certifikátov Sprievodca importom certifikátov úspešne dokončil prácu. Určili ste nasledovné nastavenie:
	Priestor na uloženie certifikátov vybratý používateľom O: Obsah C¢
	< Naspäť Dokončiť Zrušiť

10. Zobrazí sa informácia o úspešnom nainštalovaní certifikátu. Inštaláciu certifikátu CA Disig ukončíte stlačením "**OK**":



Poznámka: Prijatím a akceptovaním digitálne podpísanej správy sa automaticky importuje certifikát odosielateľa.

4.2 Import certifikátov iných osôb do systémového úložiska certifikátov Mozilla

Import certifikátu inej osoby (a tým zároveň jej verejného kľúča) do systémového úložiska certifikátov Mozilla vykonáte podľa nasledovného postupu:

- 1. Kliknite na https://eidas.disig.sk/sk/crtsearch/.
- 2. V otvorenom okne vpíšte do položky "CN" bez diakritiky celé meno osoby, ktorej bol certifikát vydaný. Identifikujte certifikát, ktorý hodláte nainštalovať a následne kliknite na text "DER" v časti "Stiahnutie":

Údaje na vyhľadá	vanie zadávajte	prosím bez d	liakritiky.
Typ certifikátu: CN:	Obyčajný certifiká	t _	
E-mail:	Hľadať		0
CN a E-mail	Sériové číslo	Stiahnutie	Inštalácia
Michal Dur michal.dur@upjs.sk Certikát je platný	507c67 hex 5380643 dec	DER PEM TXT	Explorer Outlook

3. Po zobrazení okna s ponukou na výber akcie zvoľte "Uložiť":

Preberani	e súboru - upozornenie zabezpečenia	×
Chcete o	otvoriť alebo uložiť tento súbor?	
	Meno: Michal Dur ,der Typ: Certifikát zabezpečenia, 1,01 KB Od: www.disig.sk Otvoriť Uložiť Zrušiť	
)úbory z internetu sú obyčajne užitočné, ale tento typ súboru môž syť pre počítač škodlivý. Ak nedôverujete zdroju tohto súboru, neotvárajte ani neukladajte tento softvér. <u>Aké sú riziká?</u>	e

4. Zobrazí sa Vám nasledujúce okno, v ktorom je potrebné určiť si cestu uloženia žiadosti. Zvoľte si cestu a kliknite na možnosť "Uložit". Zvolenú cestu si zapamätajte:

Illožiť ako	IIIKatu			
		Anet.		
Uložiť do:	🕼 Pracovná ploc	ha	▶	
Naposledy použité Pracovná plocha	Aoje dokument: Tento počítač Miesta v sieti	Y		
Tento počítač	_			
	Názov súboru:	Michal Durder		Uložiť
Miesta v sieti	Uložiť vo formáte:	System certificate	v [Zrušiť

5. V hlavnom menu programu Mozilla zvoľte "**Nástroje -> Možnosti …**". Vyberte " **Rozšírené**" (prípadne "**Pokročilé**") a ďalej zvoľte záložku "**Certifikáty**" (prípadne "**Šifrovanie**"):

Aa				
Zobrazeni jení a místo na dis	vytvareni iku Aktualizovat	Certifikáty	Prilohy	Rozsirene
ertifikáty, seznam	ny zneplatnění, o	věřování platno	sti a bezpečnostní :	zařízení
káty Znep	olatnění	2věřování	<u>B</u> ezpečnostní zař	izení
			ОК	Zrušit
	Zobrazení ení a místo na dis ertifikáty, seznan káty Znep	Zobrazení Vytváření ení a místo na disku Aktualizovat ertifikáty, seznamy zneplatnění, o káty Zneplatnění (Yvytváření Soukromí ení a místo na disku Aktualizovat Certifikáty ertifikáty, seznamy zneplatnění, ověřování platno káty Zneplatnění Qvěřování	Vytváření Soukromí Přilohy ení a místo na disku Aktualizovat Certifikáty ertifikáty, seznamy zneplatnění, ověřování platnosti a bezpečnostní : káty Zneplatnění Qvěřování Bezpečnostní zař

6. Kliknite na tlačidlo "Certifikáty... " a potom zvoľte kartu "Ostatné certifikáty":

	tifikaty Servery Certifikační	autority	
Pro identifikaci lidí máte dosti	upné následující certifikáty:		
Jméno certifikátu	Účel	E-mailová adresa	Ę
🖃 Disig a.s.			
Zobrazit	Importovat Smaz	at	

7. Zvoľte možnosť "**Importovať**". Otvorí sa dialógové okno, prostredníctvom ktorého nájdite súbor uložený v bode 4. Výber potvrďte tlačidlo "**Otvoriť**":

<u>K</u> de hľadať:	🞯 Pracovná pl	locha	×	O Ø	• 🛄 🥙	
Naposledy použité Pracovná plocha	Moje dokumer Tento počitač Miesta v sieti Michal Dur	nty E				
Moje dokumenty						
Moje dokumenty						
Moje dokumenty	Názov súboru:	Michal Durder				<u>tvoriť</u>

8. Import ukončíte voľbou tlačidla "**OK**":

Osobní certifikáty 🛛 Ostatní o	ertifikáty Servery Certifikační	autority	
Pro identifikaci lidí máte do	stupné následující certifikáty:		
Jméno certifikátu	Účel	E-mailová adresa	Ę
🖃 Disig a.s.			
Michal Dur	Klient,Podepsat,Z	ašifrovat michal.dur@upjs.sk	
Zobrazit	it Importovat Smaz	at	

4.3 Elektronické podpísanie textového dokumentu MS Wordu

Predpokladá sa, že máte svoj osobný certifikát nainštalovaný v systémovom úložisku certifikátov MS Windows.

Textový dokument MS Wordu elektronicky podpíšete podľa nasledovného postupu:

- 1. Textový dokument musí byť vo svojej finálnej podobe a musí byť uložený. Elektronické podpisovanie vykonávame ako posledný krok.
- 2. Z hlavnej ponuky programu vyberte "Nástroje" a potom "Možnosti...". V dialógovom okne "Možnosti" zvoľte kartu "Zabezpečenie":

Sledovať zmeny 📔 🛙	informácie o používateľovi 📗 Kompatibilita	Umiestnenie súborov
Zobraziť Všeobecné	Úpravy Tlačiť Uložiť Zabezp	ečenie 🛛 Kontrola pravopisu
Možnosti šifrovania súborov	pre tento dokument	
Heslo na otvorenie:		Spresniť
Možnosti zdieľania súborov	pre tento dokument	
Heslo na úpravy:		
Divition and the second second		
	Zabezpecit dokument	
Možnosti ochrany osobných	údajov	
🦵 Pri ukladaní odstrániť :	z tohto súboru osobné in <u>f</u> ormácie	
Komentáre	uložením alebo odoslaním súboru obsahujúceho	sledované zmeny alebo
Výšiť presnosť zlúčer	nia ul <u>o</u> žením náhodného čísla	
Zabezpečenie makra		
Upravte úroveň zabezpeč obsahovať makrovírusy, a	énia pre otváranie súborov, ktoré môžu a zadajte mená dôveryhodných vývojárov makie	rZabezpečenie <u>m</u> akra

3. Pokračujte voľbou tlačidla "Digitálne podpisy...":

dpisy		
igitálny podpis vy rávne záväzný. Ď ánkoch o digitálny	generovaný programom alšie informácie nájdete vch podpisoch.	Office nemusí byť v Pomocníkovi v
ento dokument di Podpisovateľ	gitálne podpisali nasledo Vydavateľ digitál	vni podpisovatelia: , Dátum
<		
Pripojiť certifiká	liii ity k novým pridaným p	odpisom
< 7 Pripojiť certifiká Zobraziť certifiká	الله ity k novým pridaným pr t Pridať	odpisom Odstrániť

- 4. Kliknite na tlačidlo "Pridat'...".
- 5. Na pokračovanie zvoľte "Áno:

Microso	ft Word			
?	Tento dokument môže obsahovať text alebo obrá zobrazil celý text a všetky obrázky. Chcete pokra	izky, ktoré v danom ; čovať v podpisovaní Áno	zobrazení nie sú vidil í dokumentu bez jeho Nie	teľné. Program Word zmení možnosti zobrazenia tak, aby sa o revízie?

6. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "OK":

ýber certifikátu		?
/yberte certifikát, ktor	ý chcete použiť.	
Vudaná pre		Platnosť do
Michael Dur	CA Disia	30 10 2009
🥮 Michal Dur	CA Disig	30, 10, 2009
Michal Dur	CA Disig	30, 10, 2009
2	CA Disig	30, 10, 2009
<		>
		ušiť Zobraziť certifikát

7. Postupne zatvorte dialógové okná "**Digitálny podpis**" a "**Možnosti**" kliknutím na tlačidlo "**OK**". Podpísanie dokumentu indikuje ikona v stavovom riadku programu:



Poznámka: Analogickým spôsobom možno digitálne podpísať aj iné typy dokumentov z kancelárske balíka MS Office.

4.4 Elektronické podpísanie textového dokumentu z kancelárskeho balíku Open Office

Predpokladá sa, že máte svoj osobný certifikát nainštalovaný v systémovom úložisku certifikátov MS Windows. V operačnom systéme Windows totiž kancelársky balík OpenOffice zdieľa systémové úložisko certifikátov s Windows.

Poznámka: V OpenOffice možno elektronicky podpisovať len dokumenty formátu OpenDokument. Súbory typu doc nemožno v OpenOffice elektronicky podpísať.

Textový dokument OpenOffice elektronicky podpíšete podľa nasledovného postupu:

- 8. Textový dokument musí byť vo svojej finálnej podobe a musí byť uložený. Elektronické podpisovanie vykonávame ako posledný krok.
- 9. Z hlavnej ponuky programu vyberte "Súbor" a potom "Digitálne podpisy...":

Di	gitál	ne podpisy		×
	Obsał	h dokumentu bol podp	saný:	
		Podpísané	Digitálna ID vydaná	Dátum
	<u>Z</u> (obraziť certifikát	Pridat'	<u>O</u> dstrániť
			OK Zrušiť	Pomocník

- 10. Kliknite na tlačidlo "Pridat'...".
- 11. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "OK":

oany komu	Vydaný kým	Dátum platnosti
ichal Dur	CA Disig	30.10.2009

12. Zatvorte dialógové okno "**Digitálne podpisy**" kliknutím na tlačidlo "**OK**". Podpísanie dokumentu indikuje ikona v stavovom riadku programu:

		Digitálny podpis: Podpis dokumentu je OK.	
slovenčina	INSRT STD	@	

Poznámka: Analogickým spôsobom možno digitálne podpísať aj iné typy dokumentov z kancelárske balíka OpenOffice.

4.5 Využívanie osobného certifikátu s poštovým klientom Outlook Express

Dôležité upozornenie: Pre správne fungovanie poštového klienta Outlook Express s Vašim osobným certifikátom je nutné, aby emailová adresa vo Vašom osobnom certifikáte odpovedala emailovej adrese v nastaveniach Vášho poštového konta.

Predpokladá sa, že máte svoj osobný certifikát a certifikáty osôb, s ktorými si chcete vymieňať zašifrované správy nainštalované v systémovom úložisku certifikátov MS Windows.

Nastavenie účtu elektronickej pošty v programe Outlook Express vykonáte podľa nasledovného postupu:

1. V hlavnom okne programu vyberte "Nástroje", potom "Kontá..." a napokon kartu "Pošta":



šetky Pošta [Diskusné skupiny	Adresárová služba	Pridat
Konto	Тур	Pripojenie	Odstrániť
pop3.upjs.sk	pošta (predvol	ené) Všetky dostupné	Vlastnosti
			Predvoliť
			Importovať
			Exportovať
			Nastaviť poradie.

2. Označte účet univerzitnej elektronickej pošty a stlačte tlačidlo Vlastnosti. V otvorenom dialógovom okno aktivujte kartu "Zabezpečenie". Pomocou tlačidiel "Vybrať..." môžete nastaviť certifikát používaný na podpisovanie elektronickej pošty a taktiež na jej šifrovanie. Na obe účely môže byť použitý ten istý certifikát:

Podpisový certifikát Vyberte podpisový certifikát. Týmto sa určí digitálna identifikácia ktorá sa má používať pri podpisovaní správ na tomto konte. Certifikát: Vybrať Vastavenie šifrovania Vyberte certifikát a algoritmus šifrovania, ktoré sa pridajú do digitálne podpísaných správ, aby vám ostatní mohli posielať zašifrovanú poštu s rovnakými nastaveniami.	eobecné	Servery	Pripojenie	Zabezpečenie	Spresnenie
Vyberte podpisový certifikát. Týmto sa určí digitálna identifikácia ktorá sa má používať pri podpisovaní správ na tomto konte. Certifikát: Vybrať Vastavenie šifrovania Vyberte certifikát a algoritmus šifrovania, ktoré sa pridajú do digitálne podpísaných správ, aby vám ostatní mohli posielať zašifrovanú poštu s rovnakými nastaveniami.	odpisový r	certifikát			
Certifikát: Vybrať astavenie šifrovania Vyberte certifikát a algoritmus šifrovania, ktoré sa pridajú do digitálne podpísaných správ, aby vám ostatní mohli posielať zašifrovanú poštu s rovnakými nastaveniami.	Vyberte p ktorá sa	odpisový má použív	certifikát. Tý /ať pri podpis	mto sa určí digitá sovaní správ na t	ilna identifikácia, omto konte.
lastavenie šifrovania Vyberte certifikát a algoritmus šifrovania, ktoré sa pridajú do digitálne podpísaných správ, aby vám ostatní mohli posielať zašifrovanú poštu s rovnakými nastaveniami.	Certifikát	: [Vybrať
Vyberte certifikát a algoritmus šifrovania, ktoré sa pridajú do digitálne podpísaných správ, aby vám ostatní mohli posielať zašifrovanú poštu s rovnakými nastaveniami.	astavenie	šifrovania			
Certifikát: Vybrať	Vyberte o digitálne zašifrova Certifikát	certifikát a podpísaný nú poštu s	algoritmus ši joh správ, at ; rovnakými r	ífrovania, ktoré sa oy vám ostatní mo nastaveniami.	a pridajú do ohli posielať Vybrať
Algoritmus: 3DES 🗸		is:	3DES	~	

3. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "OK":





- 4. Postupne zatvorte dialógové okná "Vlastnosti" a "Internetové kontá" kliknutím na tlačidlo "OK" a "Zavriet'".
- 5. Pri tvorbe novej správy sa tlačidlá na podpísanie, prípadne šifrovanie správy (na to je potrebné mať nainštalovaný certifikát adresáta, pozrite 4.1) nachádzajú priamo v paneli nástrojov:



prípadne v ponuke "Nástroje":

lástroje	Správa	Pomocník	
Pravopi	s	F7	
Vyžiadať potvrdenie o prečítaní		nie o prečítaní	
Kontrolovať mená Vybrať príjemcov…		ı Ctrl+K	Ctrl+K
Adresá	(Ctrl+Sh	ift+B
Zašifrov	/ať		
Digitáln	y podpis		
Vyžiada	iť potvrdei	nie o zabezpečení	

6. Podpísanie emailu indikuje ikona pečate a zašifrovanie ikona zámky:

139 Kópia:	A
Predmet:	

4.6 Využívanie osobného certifikátu s poštovým klientom Mozilla Thunderbird

Dôležité upozornenia:

- Pre správne fungovanie poštového klienta Mozilla Thunderbird s Vašim osobným certifikátom je nutné, aby emailová adresa vo Vašom osobnom certifikáte odpovedala emailovej adrese v nastaveniach Vášho poštového konta.
- Predpokladá sa, že máte svoj osobný certifikát a certifikáty osôb, s ktorými si chcete vymieňať zašifrované správy nainštalované v systémovom úložisku certifikátov programu Mozilla Thunderbird (Firefox a Thunderbird zvyčajne svoje úložiská certifikátov nezdieľajú!).

Nastavenie účtu elektronickej pošty v programe Mozilla Thunderbird vykonáte podľa nasledovného postupu:

 V hlavnom okne programu vyberte "Nástroje" a potom "Nastavenia účtu...". Kliknite na text "Zabezpečenie" v ľavej časti dialógového okna účtu univerzitnej elektronickej pošty. Pomocou tlačidiel "Vybrať..." môžete nastaviť certifikát používaný na podpisovanie elektronickej pošty a taktiež na jej šifrovanie. Na obe účely môže byť použitý ten istý certifikát:

Nastavení účtu	
 Michal Dur Nastavení serveru Kopie a složky Vytváření zpráv a adresování Místo na disku Nevyžádaná pošta Potvrzení o přečtení Zabezpečení Gmail - Michal Dur Nastavení serveru Kopie a složky Vytváření zpráv a adresování Místo na disku Nevyžádaná pošta Potvrzení o přečtení Zabezpečení Michal Dur Místo na disku Nevyžádaná pošta Potvrzení o přečtení Zabezpečení Michal Dur Místo na disku Nevyžádaná pošta Server odchozí pošty (SMTP) 	Zabezpečení Pro příjem a odesílání podepsaných nebo zašifrovaných zpráv musíte zadat jak certifikát pro digitální podpis tak i certifikát pro šifrování. Digitální podpis Používat tento certifikát pro digitální podpis odesílaných zpráv: 2c32578d93d7f6f2d3dac5781d22a91e_f3b459fa-c9 Vybrat Digitálně podepsat zprávy (výchozí) Šifrování Použít tento certifikát pro zašifrování a dešifrování obdržených zpráv: 2c32578d93d7f6f2d3dac5781d22a91e_f3b459fa-c9 Vybrat Šifrování Použít tento certifikát pro zašifrování a dešifrování obdržených zpráv: 2c32578d93d7f6f2d3dac5781d22a91e_f3b459fa-c9 Vybrat Výchozí nastavení šifrování při odesílání zpráv: Výchozí nastavení šifrování při odesílání zpráv: Mikdy (nepoužívat šifrování) Vyžadováno (nelze odeslat zprávy, pokud všichni příjemci nemají certifikáty) Certifikáty Bezpečnostní zařízení
Přidat účet	
Nastavit jako výchozí	
Odeb <u>r</u> at účet	
	OK Zrušit

2. Vyberte certifikát, ktorý chcete použiť. Svoj výber potvrďte voľbou "OK":

Výběr cert	ifikátu 🛛 🛛
Certifikát: Podrobnost	2222 78d93d7f6f2d3dac5781d22a91e_f3b459fa-c983-40da-b723-6f9800503a9e [50:6A:3A]
Vydáno pri Sériové č Platný od Účel: Kliei Vydal: CN= Uskladněn	o: E= michal.dur@upjs.sk,CN= Michal Dur,OU=UPJS v Kosiciach,C=SK (slo: 50:6A:3A 130.10.2008 15:39:29 do 30.10.2009 15:39:29 nt,Podepsat,Zašifrovat =CA Disig,O=Disig a.s.,L=Bratislava,C=SK o v: Bezpečnostní zařízení SW
	OK Zrušit

- 3. Zatvorte dialógové okno "Nastavenia účtu" kliknutím na tlačidlo "OK".
- 4. Pri tvorbe novej správy sa tlačidlá na podpísanie, prípadne šifrovanie správy (na to je potrebné mať nainštalovaný certifikát adresáta, pozrite 4.2) nachádzajú priamo v paneli nástrojov:

🚔 Psaní zprávy: (bez předmětu)		
<u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obrazit Vložit <u>F</u> or	mát <u>M</u> ožnosti <u>N</u> ástroje Nápo <u>v</u> ěda	
Odeslat Adresář Pravopis Připojit	- Zabezpečení - Uložit -	
Od: Michal Dur <michal.dur@upjs.sk></michal.dur@upjs.sk>	• <u>N</u> ešifrovat zprávu	~
Komu: 💷	Zašifrovat zprávu	
	Digitálně podepsat zprávu	
	Z <u>o</u> brazit informace o zabezpečení	
Před <u>m</u> ět:		
Tělo 🗸 Proporcionální	→ A [*] A [*] B I U	$\underset{2^{-}}{\vDash} \underbrace{1^{-}}_{2^{-}} \underbrace{1^{-}}_$

prípadne v ponuke "Možnosti":



Psaní zprávy: (bez předmětu)		
<u>S</u> oubor Úpr <u>a</u> vy <u>Z</u> obrazit Vložit <u>F</u> ormát	Možnosti <u>N</u> ástroje Nápo <u>v</u> ěda	
Odeslat Adresář Pravopis Připojit Za	Kontrola pravopisu Ctrl+K <u>A</u> utomatická kontrola pravopisu Citovat zprávu	
Dd: Michal Dur <michal.dur@upjs.sk></michal.dur@upjs.sk>		
Komu: 💻	Po <u>t</u> vrzení o přečtení	
	Zna <u>k</u> ová sada	
	Eormát 🕨	
	Priorita	
vřed <u>m</u> ět:	Poslat kopij	
Tělo 🛛 Proporcionální	Za <u>b</u> ezpečení •	• <u>N</u> ešifrovat zprávu
		Zašitrovat zprávu
		Digitálně podepsat zprávu

5. Podpísanie emailu indikuje ikona obálky a zašifrovanie ikona zámky v okne správy vpravo dole:





5 VYSVETLENIE POJMOV

Certifikačná autorita

Certifikačná autorita je "dôveryhodná tretia strana", ktorá sprostredkúva dôveru medzi komunikujúcimi stranami. Vydáva certifikáty verejného kľúča, ktoré umožňujú komunikujúcim stranám dôveryhodne doložiť svoju identitu.

Elektronický podpis

Elektronický podpis predstavuje elektronickú obdobu klasického podpisu. Obidva typy podpisov (klasický aj elektronický) slúžia na potvrdenie autenticity podpisovaného dokumentu a na identifikáciu autora podpisu. Elektronický podpis (EP) je informácia pripojená k podpisovanému dokumentu, pomocou ktorej je možné overiť autenticitu a integritu podpísaného dokumentu (Zákon č. 215/2002 Z.z. o elektronickom podpise a o zmene a doplnení niektorých zákonov v platnom znení). Na jeho vytvorenie je potrebné, aby autor vlastnil súkromný kľúč a k nemu prislúchajúci certifikát, pričom identitu autora podpisu potvrdzuje dôveryhodná tretia strana - certifikačná autorita. Pomocou kryptografických algoritmov a súkromného kľúča je vytvorená štruktúra, ktorá je následne spolu s certifikátom prislúchajúcim k použitému súkromnému kľúču pripojená k elektronickému dokumentu. Prostredníctvom tejto štruktúry s použitím pripojeného certifikátu je možné kedykoľvek neskôr zistiť, či elektronický dokument je autentický alebo v ňom boli vykonané zmeny.

Súkromný kľúč

Súkromným kľúčom je tajná informácia, ktorá slúži na vyhotovenie elektronického podpisu elektronického dokumentu.

Verejný kľúč

Verejným kľúčom je informácia dostupná adresátovi (overovateľovi) podpísaného elektronického dokumentu, ktorá slúži na overenie pravosti elektronického podpisu vyhotoveného pomocou odpovedajúceho súkromného kľúča.

Certifikát

Certifikát (inak aj certifikát verejného kľúča) je elektronický dokument, ktorým vydavateľ certifikátu (certifikačná autorita) potvrdzuje, že v certifikáte uvedený verejný kľúč patrí osobe, ktorej je certifikát vydaný. Certifikát je určený na overovanie správnosti elektronického podpisu vyhotoveného pomocou súkromného kľúča patriaceho k danému verejnému kľúču.



© Univerzita Pavla Jozefa Šafárika v Košiciach 2008