

Nastavení formátu kvalifikovaného/zaručeného elektronického podpisu, vložení kvalifikovaného elektronického časového razítka a vložení kvalifikovaného/zaručeného elektronického podpisu dle nařízení eIDAS.

Následující řádky se věnují nastavení formátu kvalifikovaného/zaručeného elektronického podpisu, postupu přidání kvalifikovaného elektronického časového razítka a postupu vložení kvalifikovaného/zaručeného elektronického podpisu ve volně dostupné softwarové aplikaci Acrobat Reader DC. Zobrazení se může v systémech lišit. Tento dokument je zamýšlen pouze jako návod.

1. Nastavení požadovaného formátu podepisování
2. Nastavení vložení kvalifikovaného elektronického časového razítka
3. Vložení elektronického podpisu dle eIDAS
4. Ověření vloženého elektronického podpisu dle eIDAS.

1. Nastavení požadovaného formátu podepisování (Ekvivalent rozšíření CADES):

Pro správné nastavení formátu podepisování je potřeba u elektronického podpisu nastavit ekvivalent rozšíření CADES. Postup je následující - v programu Acrobat Reader DC je volba dostupná přes Úpravy -> Předvolby -> Podpisy -> Vytvoření a vzhled -> Další... -> Výchozí formát podepisování = **Ekvivalent rozšíření CADES** -> OK.

The screenshot shows the Adobe Acrobat Reader DC interface with several red arrows and numbers indicating the steps to set the signature format:

- 1**: Points to the 'Úpravy' (Edit) menu in the top bar.
- 2**: Points to the 'Podpisy' (Signatures) option in the 'Úpravy' dropdown menu.
- 3**: Points to the 'Další...' (More) button in the 'Vytvoření a vzhled' (Creation and Appearance) section of the 'Digitální podpisy' (Digital Signatures) panel.
- 4**: Points to the 'Výchozí formát podepisování' (Default signature format) dropdown menu in the 'Předvolby vytvoření a vzhledu' (Creation and Appearance Preferences) dialog box, which is set to 'Ekvivalent rozšíření CADES'.
- 5**: Points to the 'OK' button at the bottom of the dialog box.

2. Nastavení vložení kvalifikovaného elektronického časového razítka

Veřejnoprávní podepisující jsou povinni označit podepsaný dokument kvalifikovaným elektronickým časovým razítkem. Postup vložení kvalifikovaného elektronického časového razítka je následující - v Acrobat Reader DC je volba dostupná přes Úpravy -> Předvolby -> Podpisy -> Přidání časového razítka do dokumentu -> Další... -> Nový -> OK.

Kategorie:

- Dokumenty
- Na celou obrazovku
- Přidávání poznámek
- Všeobecné
- Zobrazení stránky
- 3D a multimédia
- Čtení
- Důvěryhodnost multimédií (starší)
- E-mailové účty
- Formuláře
- Hledání
- Identita
- Internet
- JavaScript
- Jazyk
- Jednotky
- Kontrola pravopisu
- Měření (2D)
- Měření (3D)
- Měření (geoprostorové)
- Multimédia (starší)
- Online služby Adobe
- Podpisy
- Recenzování
- Sledování
- Správce práv
- Uspřádání přístupu
- Zabezpečení
- Zabezpečení (rozšířené)

Digitální podpisy

- Vytvoření a vzhled
 - Volby pro vytvoření podpisu
 - Nastavení vzhledu podpisů v rámci dokumentu
- Ověření
 - Volba, jak a kdy se podpis ověřuje
- Identity a důvěryhodné certifikáty
 - Vytvoření a správa identit pro podepisování
 - Správa přihlašovacích údajů používaných k nastavení dokumentů jako důvěryhodných
- Přidání časového razítka do dokumentu
 - Nastavení konfigurace serveru časových razítek

Nastavení serveru

Adresářové servery	Nový	Upravit	Importovat	Exportovat	Odstranit
Servery časových razítek	Jméno	URL			
	ICA HTTPS	https://tsabase.ica.cz/cgi-bin/razi...			
	ICA IP	http://tsabase.ica.cz/cgi-bin/razit...			

Konfigurovat servery časových razítek

Nastavte výchozí server časových razítek. Pokud jste v pracovní skupině, můžete sdílet správu vašeho počítače.

Vyberte jednu z položek nahoře na Nový a přidejte a konfigurujte. Pokud vyberete výchozí server, klepněte na Exportovat, chcete-li.

Nový server časových razítek

Název: TSA

Nastavení serveru

URL serveru: tsabase.ica.cz/cgi-bin/razitko_base2.cgi

Tento server vyžaduje přihlášení

Jméno uživatele: login

Heslo: *****

Zadání hesla nebude nikdy vyžadováno. Heslo bude uloženo na tomto počítači a chráněno přihlašovací službou Windows. Jestliže se někdy později rozhodnete odhlásit, vyberte si pak jiné pravidlo pro dobu platnosti hesla.

OK Zrušit

Nastavení serveru

Adresářové servery

Servery časových razítek

Importovat Exportovat Odstranit Nastavit výchozí

Jméno	URL
★ ICA HTTPS	https://tsabase.ica.cz/cgi-bin/razi...
ICA IP	http://tsabase.ica.cz/cgi-bin/razit...
TSA	https://tsabase.ica.cz/cgi-bin/razi...

Konfigurovat servery časových razítek

3. Vložení elektronického podpisu dle eIDAS

Po dokončení nastavení je možno do dokumentu přidat elektronický podpis. Veřejnoprávní původce používá kvalifikovaný elektronický podpis (tzn. použit kvalifikovaný certifikát a kvalifikovaný prostředek) včetně připojení kvalifikovaného elektronického časového razítka. Kliknutím na tlačítko „Digitálně podepsat“ dojde k zobrazení výběru oblasti pro vložení podpisu, výběru podpisového certifikátu a uložení nového dokumentu s kvalifikovaným/zaručeným podpisem a současně vloženým kvalifikovaným elektronickým časovým razítkem. V rámci prvotní konfigurace může být nutno nastavit „Konfiguraci digitálního ID“.

zuct_8.pdf - Adobe Acrobat Reader DC

Soubor Úpravy Zobrazení Okna Nápověda

Domovská stránka Nástroje zuct_8.pdf x Přihlásit se

1 / 1 100%

Certifikáty Digitálně podepsat Časové razítko Ověřit všechny podpisy Zavřít

2. U projektů financovaných z prostředků Komunitárních programů na projekt RIS COMEX, Crocodile 3 – investiční část a C-ROADS – investiční část předložení podrobného přehledu aktivit, na které byly finanční prostředky použity:

Spustí proces podepsání

Zpracoval:		Zodpovídá (statut. zástupce):	
jméno a příjmení:		jméno a příjmení:	
funkce:		funkce:	
tel.:		tel.:	
e-mail:		e-mail:	

Digitálně podepsat Časové razítko Ověřit všechny podpisy

2. U projektů financovaných z prostředků Komunitárních programů na projekt RIS COMEX, Crocodile 3 – investiční část a C-ROADS – investiční část předložení podrobného přehledu aktivit, na které byly finanční prostředky po

Podepsat pomocí digitálního ID x

Vyberte digitální ID, který chcete použít k podpisu: Obnovit

- Karel [redacted]** (Digitální identifikátor systému Windows)
Vydal: I.CA Qualified 2 CA/RSA 02/2016. Konec platnosti: 2020.07.03
-

Zobrazit podrobnosti

4. Ověření vloženého kvalifikovaného/zaručeného elektronického podpisu dle eIDAS

U veřejnoprávního podepisujícího po otevření a rozkliknutí „Panelu podpisů“, kliknutím na podpis osoby pravým tlačítkem myši, vyberete volbu „Zobrazit vlastnosti podpisu...“ a dále pak v nově zobrazeném okně kliknete na tlačítko „Další vlastnosti...“.

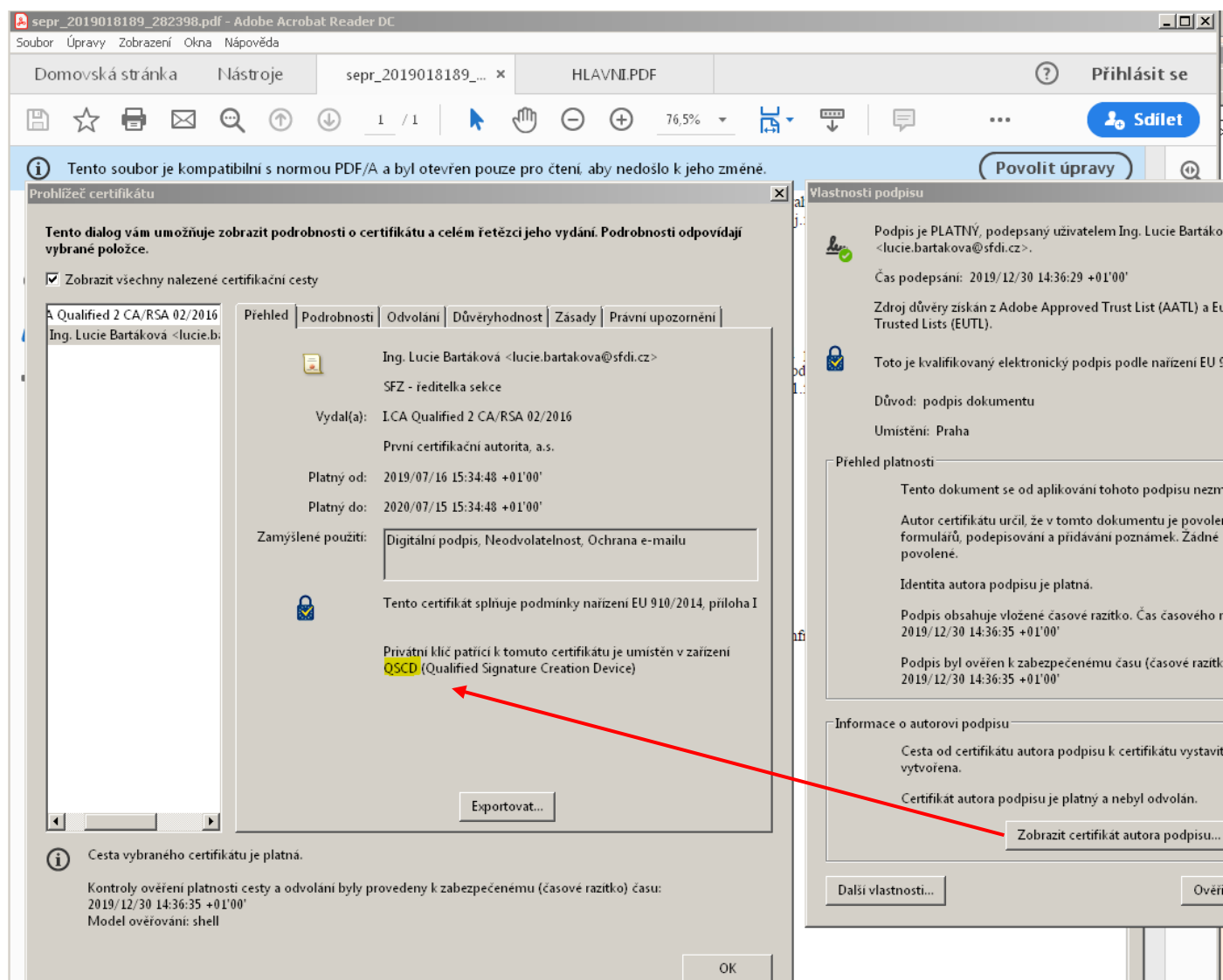
Kvalifikovaný elektronický podpis dle eIDAS musí mít formát **PAdES: B-T** nebo **PAdES: B-LT** (tzn. že **elektronický podpis** obsahuje vnořené časové razítko) a informaci o použití kvalifikovaného prostředku.

The screenshot shows the Adobe Acrobat Reader DC interface. The main window displays the document 'HLAVNI.PDF' with a signature by Ing. Lucie Bartáková. Two dialog boxes are open:

- Další vlastnosti podpisu (Further signature properties):**
 - Detaily podpisu: Podpis byl vytvořen s použitím Není k dispozici. Algoritmus hashSHA256. Algoritmus podpisu: RSA s PKCS#1 v.1.5. Úroveň podpisu: **PAdES: B-T**.
 - Podrobnosti časového razítka: **Časové razítko vloženo v podpisu**. Časová razítka se podepisují stejně jako dokumenty. Aby byl podpis časového razítka platný, musí být důvěryhodná autorita časového razítka, která časové razítko podepsala. Klepnutím na Zobrazit certifikát zobrazíte podrobnosti o ověření podpisu časového razítka. Autorita časového razítka: Zobrazit certifikát... Časová razítka se vytvářejí se specifickými zásadami, které jsou určeny autoritou časového razítka. Zásady mohou kromě jiných věcí také vyznačovat, jak spolehlivý je zdroj času. Zásady pro toto časové razítko jsou představovány identifikátorem 1.3.6.1.4.1.23624.10.1.50.2.0. Abyste porozuměli zásadám pro časová razítka, musíte kontaktovat autoritu časového razítka. Algoritmus hashSHA256. Zavřít
- Vlastnosti podpisu (Signature properties):**
 - Podpis je PLATNÝ, podepsaný uživatelem Ing. Lucie Bartáková <lucie.bartakova@sfdi.cz>.
 - Čas podepsání: 2019/12/30 14:36:29 +01'00'
 - Zdroj důvěry získán z Adobe Approved Trust List (AATL) a European Union Trusted Lists (EUTL).
 - Toto je kvalifikovaný elektronický podpis podle nařízení EU 910/2014.
 - Důvod: podpis dokumentu
 - Umístění: Praha
 - Přehled platnosti: Tento dokument se od aplikování tohoto podpisu nezměnil. Autor certifikátu určil, že v tomto dokumentu je povoleno vyplňování polí formulářů, podepisování a přidávání poznámek. Žádné další změny nejsou povolené. Identita autora podpisu je platná. **Podpis obsahuje vložené časové razítko.** Čas časového razítka: 2019/12/30 14:36:35 +01'00' Podpis byl ověřen k zabezpečenému času (časové razítko): 2019/12/30 14:36:35 +01'00'
 - Informace o autorovi podpisu: Cesta od certifikátu autora podpisu k certifikátu vystavitele byla úspěšně vytvořena. Certifikát autora podpisu je platný a nebyl odvolán. Zobrazit certifikát autora podpisu...

A red arrow points from the 'Další vlastnosti podpisu' dialog to the 'Vlastnosti podpisu' dialog.

Informaci, zda byl užit podpisový certifikát umístěný na kvalifikovaném postředku, lze vyčíst po rozkliknutí tlačítka „Zobrazit certifikát autora podpisu“. Kvalifikovaný prostředek odpovídá informaci „Privátní klíč patříci k tomuto certifikátu je umístěn v zařízení **QSCD**“.



V případě ostatních podepisujících – zaručený elektronický podpis dle eIDAS, musí mít formát **PADES: B-B** (tzn. že elektronický podpis neobsahuje vnořené časové razítko) a není vyžadováno použití podpisového certifikátu na kvalifikovaném prostředku (např. čipové kartě).

Shrnutí kontroly pro veřejnoprávní původce:

Pro elektronický podpis je použit kvalifikovaný podpisový certifikát, elektronický podpis byl umístěn na kvalifikovaném prostředku (např. čipové kartě) a elektronický podpis obsahuje vnořené kvalifikované elektronické časové razítko. Elektronický podpis je časově platný a není odvolán. Formát elektronického podpisu je standardu PADES: B-L nebo PADES: B-LT.

Shrnutí kontroly pro ostatní původce:

Pro elektronický podpis je použit kvalifikovaný podpisový certifikát. Elektronický podpis je časově platný a není odvolán. Formát elektronického podpisu je standardu PADES: B-B. Elektronický podpis v tomto případě může obsahovat prvky požadované pro veřejnoprávní původce, ale tyto nejsou vyžadovány.

Ve všech případech platí, že podpisový certifikát vystavil kvalifikovaný poskytovatel služeb vytvářejících důvěru v rámci EU.