



KB

Digitální podpis u výpisů v PDF

Jaký certifikát využívá KB pro digitální podpis?

Komerční banka využívá k zabezpečení svých elektronických výpisů ve formátu PDF předaných e-mailem nebo prostřednictvím internetového bankovníctví digitální podpis opatřený **Komerčním serverovým certifikátem** od společnosti **První certifikační autorita, a.s.** (dále jen I.CA).

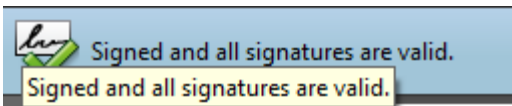
Digitální podpis zajistí výpisu „**autenticitu**“ (pravost výpisu, výstavce výpisu je KB) a „**integritu**“ (neporušenost výpisu, výpis nebyl na cestě pozměněn).

Jak poznáte zda je digitální podpis platný?

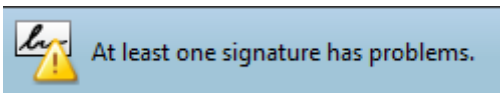
Následující návod platí pro nejčastěji používaný prohlížeč PDF dokumentů Adobe Reader. Většina dalších nástrojů digitální podpis nezobrazuje.

Zda je digitální podpis platný zjistíte na první pohled po otevření bankovního výpisu vlevo nahoře.

Platný digitální podpis:



Neplatný digitální podpis:



To, že se jeví digitální podpis jako neplatný může mít dvě příčiny:

- není povoleno „ověřování podpisů“ v Adobe Reader v rámci nastavení integrace s Windows
- Kořenový certifikát I.CA není umístěn mezi důvěryhodnými certifikáty

Jak umístit certifikát mezi důvěryhodné do Vašeho PC?

Kořenový serverový certifikát I.CA, který garantuje důvěryhodnost certifikátu KB, je umístěn mezi důvěryhodnými certifikáty OS Microsoft a od 11.4.2014 i v Apple Root Certificate Program.

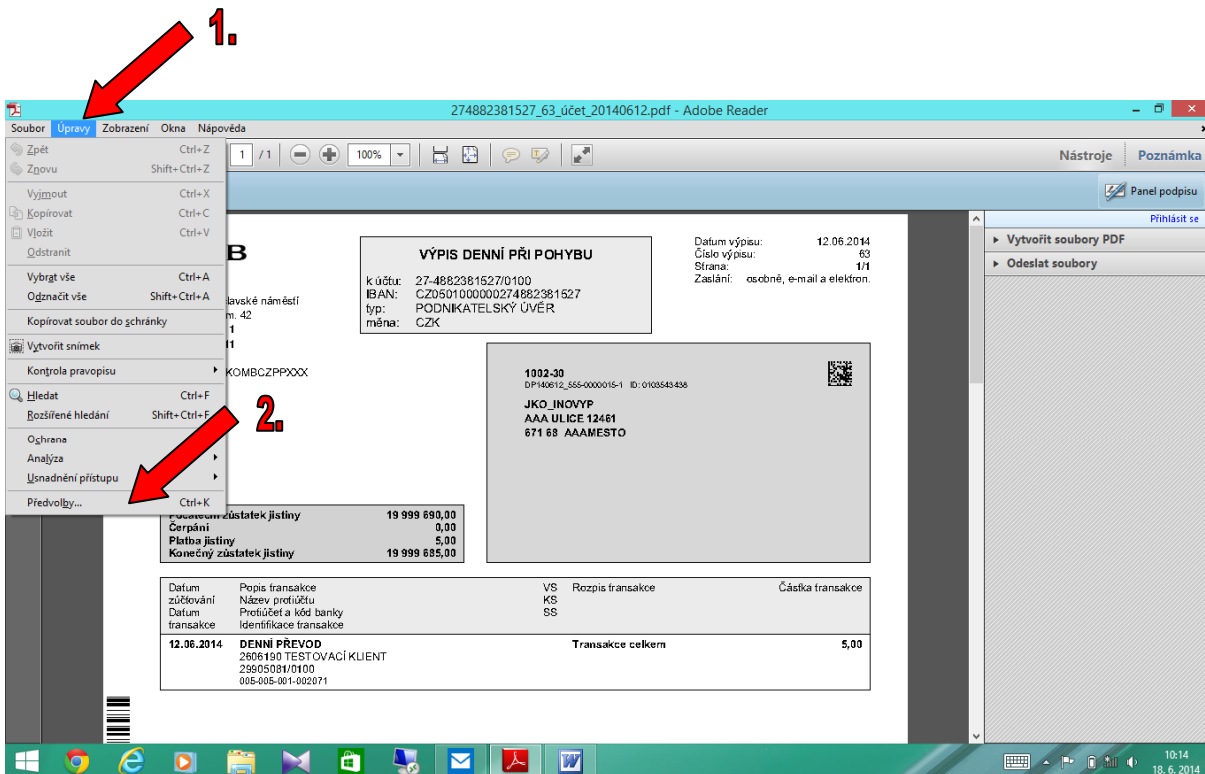
Pokud se Vám podpis nezobrazuje jako validní, proveďte prosím na svém PC následující kroky, které Vám zajistí umístění certifikátu mezi důvěryhodné.

KROK 1 - povolení „ověřování podpisů“ v Adobe Readeru

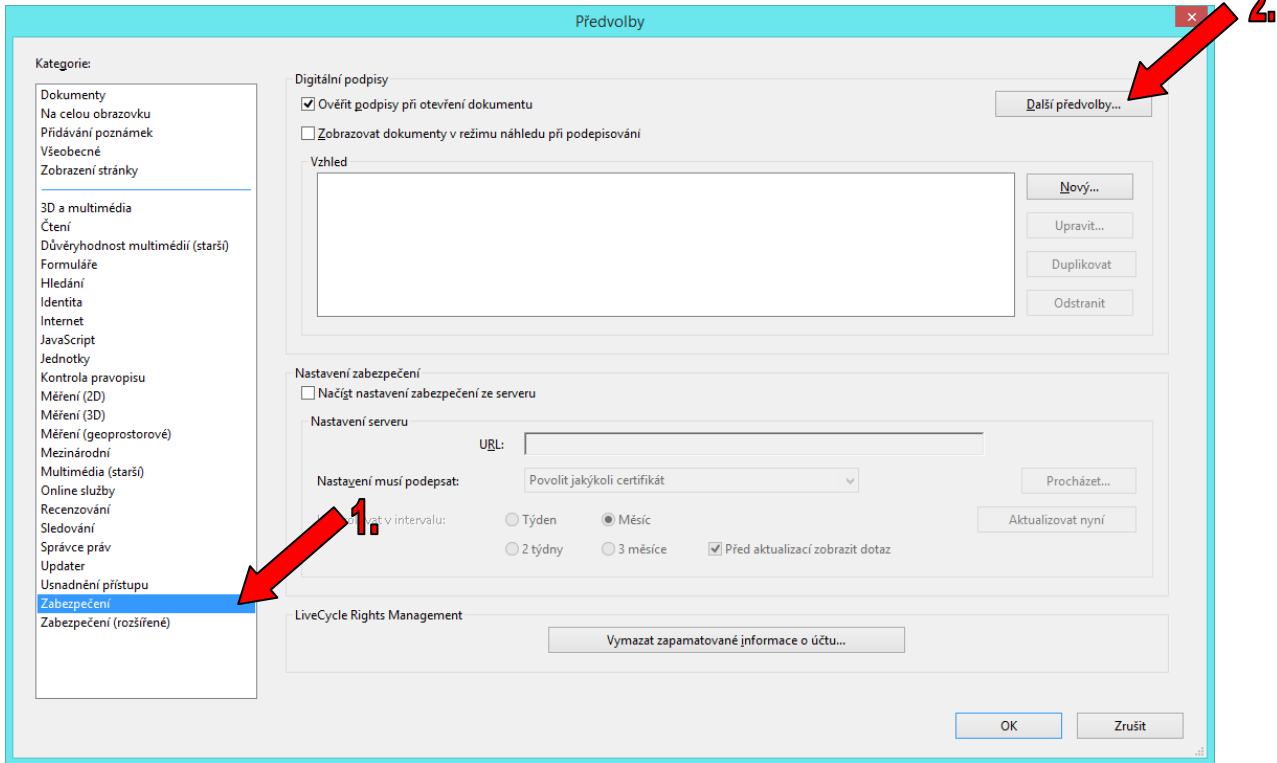
1. Postup pro Adobe reader verze 10 a nižší

Otevřete si prohlížeč Adobe Reader.

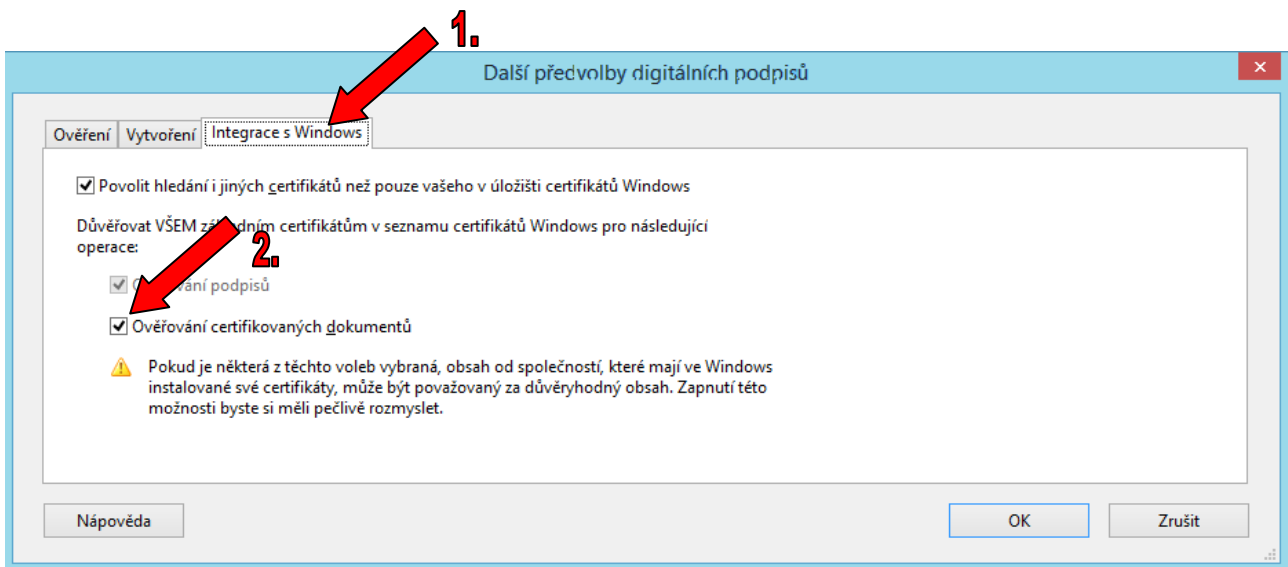
1. Na úvodní obrazovce prohlížeče klikněte na záložku **Úpravy** a poté vyberte volbu **Předvolby...**



2. Na záložce Předvolby zvolte kategorii **Zabezpečení** a poté klikněte na tlačítko **Další předvolby...**



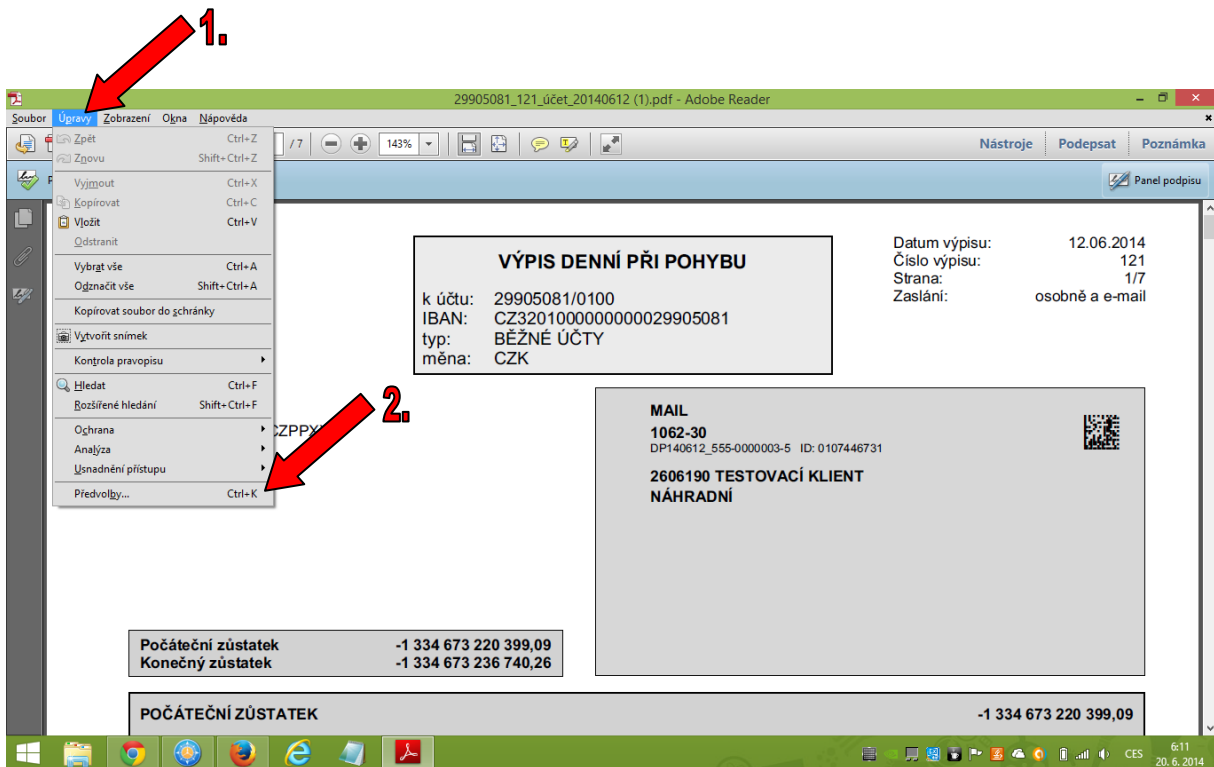
3. Zvolte záložku **Integrace s Windows** a povolte **Ověřování podpisů**, volby potvrďte tlačítkem **OK**.



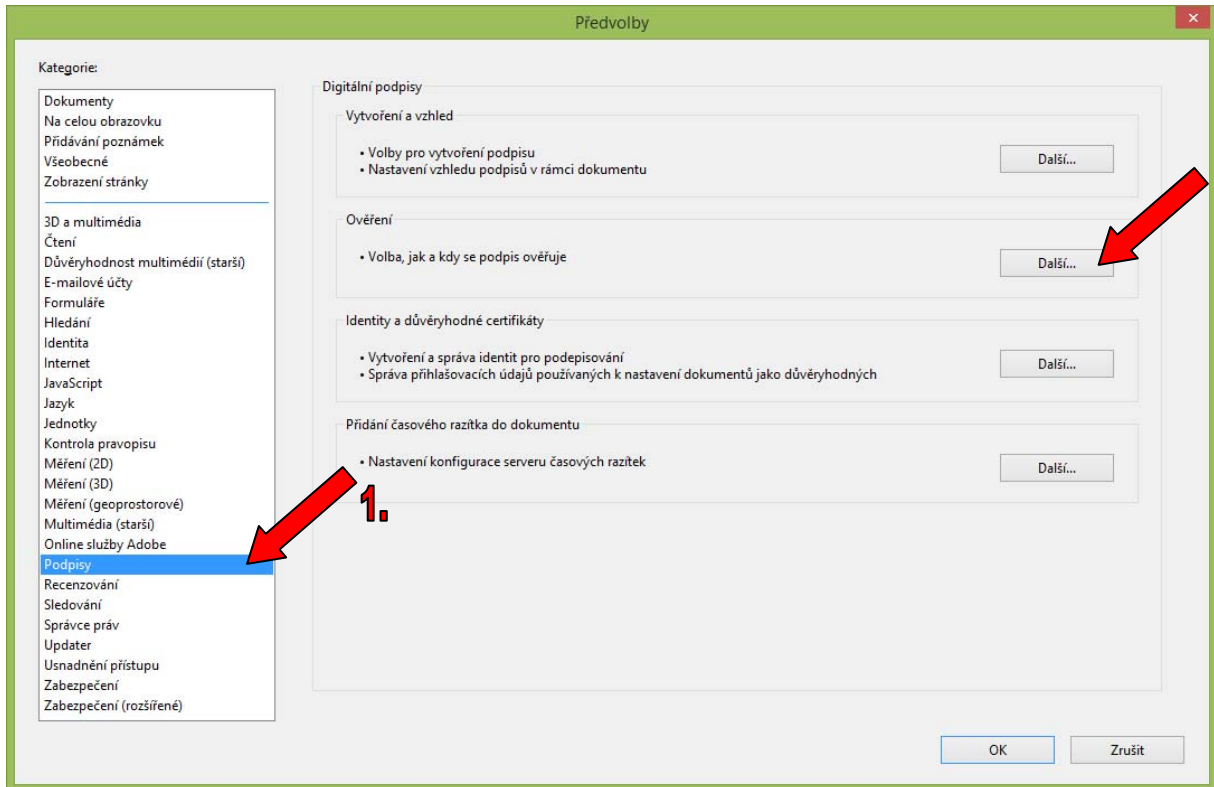
2. Postup pro Adobe reader verze 11

Otevřete si prohlížeč Adobe Reader.

1. Na úvodní obrazovce prohlížeče klikněte na záložku **Úpravy** a poté vyberte volbu **Předvolby...**



2. Na záložce Předvolby zvolte kategorii **Podpisy** a poté klikněte na tlačítko **Další...** u volby **Ověření**





3. Na záložce **Předvolby ověření podpisu** zaškrtněte v části **Integrace s Windows** volbu **Ověřování podpisů**, volby potvrďte tlačítkem **OK**

Předvolby ověření podpisu

Ověřit podpisy při otevření dokumentu

Pokud je dokument opatřen platnými podpisy, které však nebyly označeny jako důvěryhodné, zobrazí se výzva ke kontrole a k ověření důvěryhodnosti podpisů

Chování při ověřování

Při ověřování:

Použít metodu stanovenou v dokumentu; dotaz, pokud není k dispozici

Použít metodu stanovenou v dokumentu; pokud není k dispozici, použít výchozí metodu

Vždy použít výchozí metodu:

Vyžadovat, aby při ověřování podpisů byla kontrola odvolání certifikátu úspěšná, kdykoliv je to možné

Ignorovat informace o ověření dokumentu

Čas ověření

Ověřovat podpisy s použitím:

Čas vytvoření podpisu

Zabezpečený čas (časové razítko) vložené v podpisu

Aktuální čas

Použít časová razítka ukončené platnosti

Ověřovací informace

Automaticky přidávat ověřovací informace při ukládání podepsaného souboru PDF:

Zeptat se, když jsou ověřovací informace příliš velké

Vždy

Nikdy

Integrace s Windows

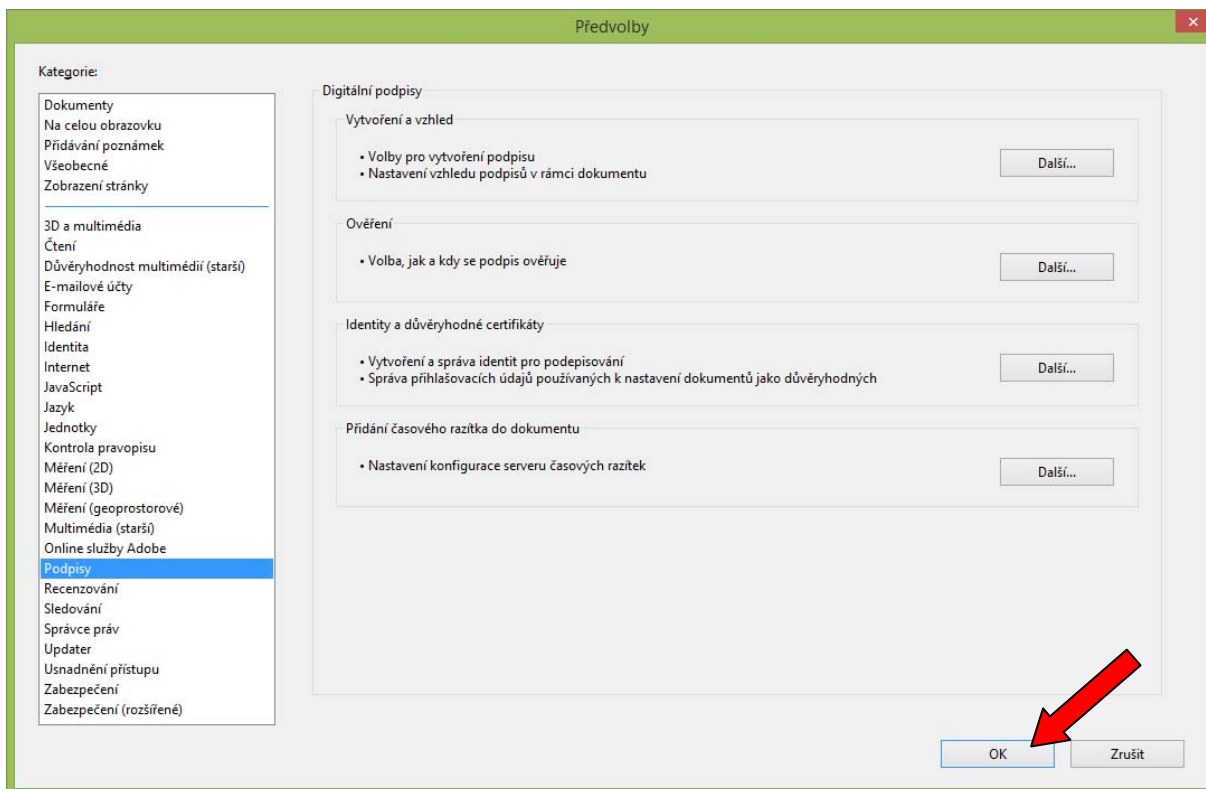
Důvěřovat certifikátům kořenovým certifikátům v seznamu certifikátů Windows pro:

Ověřování podpisů

Ověřování certifikovaných dokumentů

Volba kterékoliv z těchto voleb může vést k tomu, že za důvěryhodný obsah budou považovány libovolné materiály. Buďte opatrní před povolením těchto funkcí.

4. Na další obrazovce potvrďte tlačítkem **OK**.




Změny se promítnou do prohlížeče Adobe Reader po jeho zavření a opětovném otevření.

KROK 2 - Import certifikátu do PC

V některých ojedinělých případech je třeba pro správnou funkčnost ověření elektronického podpisu v pdf dokumentech nainstalovat platný certifikát. Pro instalaci certifikátu nejsou nutná administrátorská práva na Vašem počítači.

Platný certifikát od společnosti I.CA je umístěný ke stažení:


- na našich webových stránkách Komerční banky v sekci **Stáhněte si** <http://www.mojebanka.cz/cs/stahnete-si.shtml>, v část **Certifikační politika**, odkaz **Certifikát pro ověření elektronických výpisů**.
- přímo ze stránek 1. Certifikační autority <http://www.ica.cz/SHA2-Komerčni>
Otevře se vám stránka I.CA „Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2“
Klikněte na odkaz **DER 1070 byte**



První certifikační autorita, A.S.

SPOJENÍ S DŮVĚROU





O NÁS REGISTRAČNÍ AUTORITY PRODUKTY A SLUŽBY CENÍK PODPORA KONTAKTY



> [O nás](#) > [Rychlé odkazy](#) > [Kořenové certifikáty I.CA](#) > SHA2 Komerční

Kořenový certifikát certifikační autority pro vydávané komerční certifikáty SHA2

Kryptografický algoritmus: SHA-256
Délka kryptografického klíče pro algoritmus RSA: 2048 bitů
Doba platnosti: od 1.9.2009 do 1.9.2019

Odkaz	ZIP	Algoritmus otisku: otisk*
↓ DER 1070 byte		SHA-256: 6468bf8cf3cf688ebb2a6841bd70e97b5229b49df8690d7b74193e9ce3886141 SHA-1: 90dece77f8c825340e62ebd635e1be20cf7327dd MD-5: 86ef8e319d9f8569a2a41a127168ba1b
↓ PEM 1509 byte		SHA-256: 7449a917e246e5c336493d1eb877b95dee77c79666ff9ada1e3b5acea27a7bce SHA-1: 6472504137dd8cbb76a636382ac640225df1ff91 MD-5: c4bfa8052e15719e24e1b5cca623103d
↓ TXT 3301 byte		SHA-256: 701a78e0667442ba6d0d19702a0981fcfaa272a4dc3722305daa0a8f286c1697 SHA-1: 4e73ea0c1671fd1bfc25a5c380e5ec3fbb25b34a MD-5: 154fc80cb6ca05b0761d4e0a919658ad
↓ CMF 1336 byte		SHA-256: 0aa67e521ef20a4f2db1a496da46c8512dc0ca4350e19f8d00bc37830a45b396 SHA-1: 2a942921ac605bfa58e3db62f9cd45e9708e3b56 MD-5: c0f2cc806c6b51b439402ebc02d49e3b

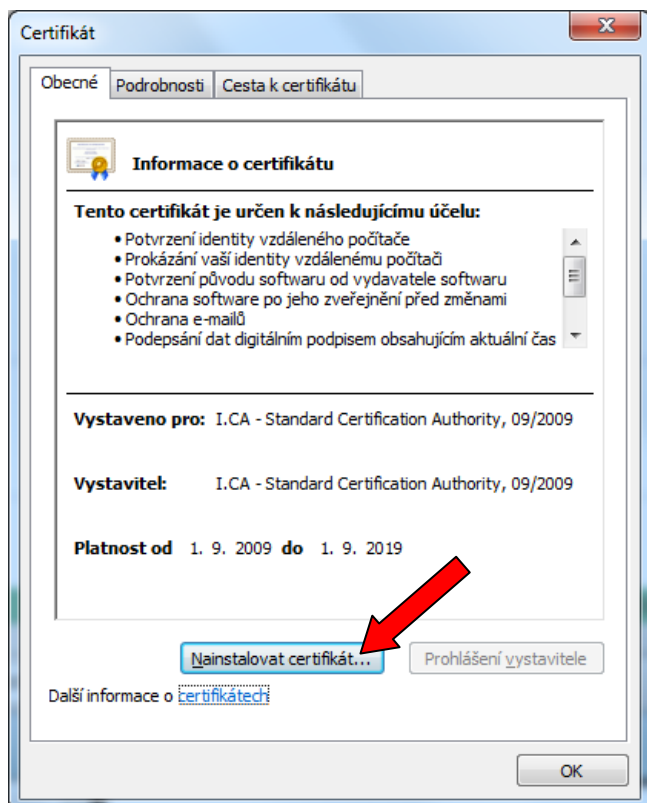
* Otisky jsou počítány z obsahu celého souboru.

Rychlé odkazy

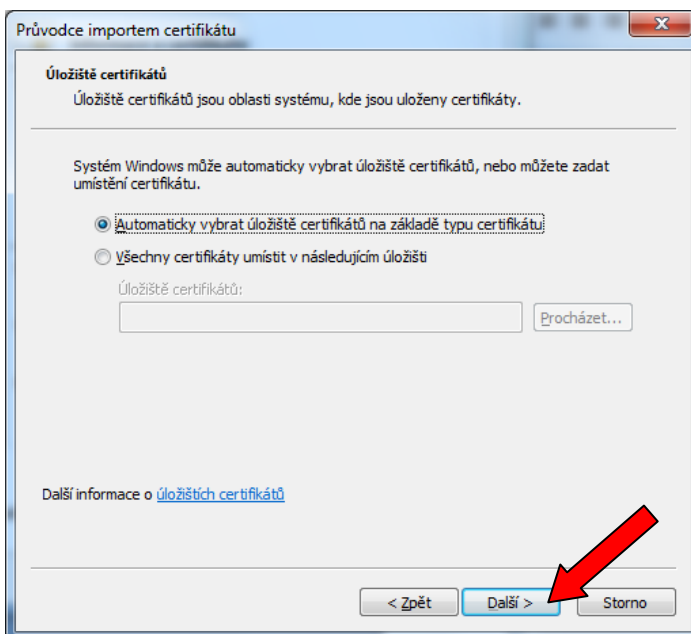
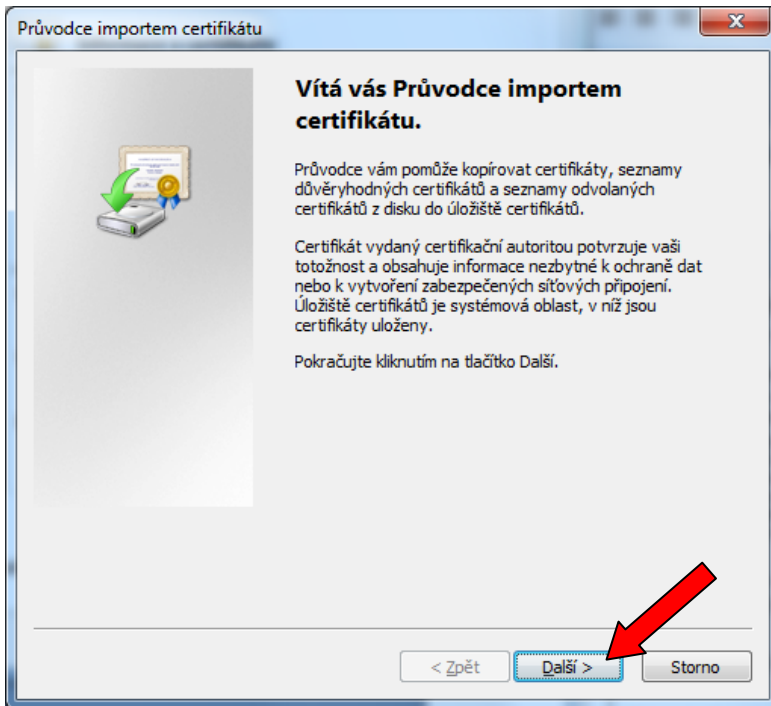
- ▶ [Objednávky produktů a služeb](#)
- ▶ [Získat elektronický podpis](#)
- ▶ [Dokumenty k získání certifikátů](#)
- ▶ [Žádost o zneplatnění certifikátů](#)
- ▶ [Certifikační politika](#)
- ▶ [Zprávy pro uživatele el. podpisu](#)
- ▶ [Kořenové certifikáty I.CA](#)
- ▶ [Certifikáty časové autority](#)
- ▶ [Seznamy veřejných certifikátů](#)
- ▶ [Seznamy zneplatněných certifikátů](#)

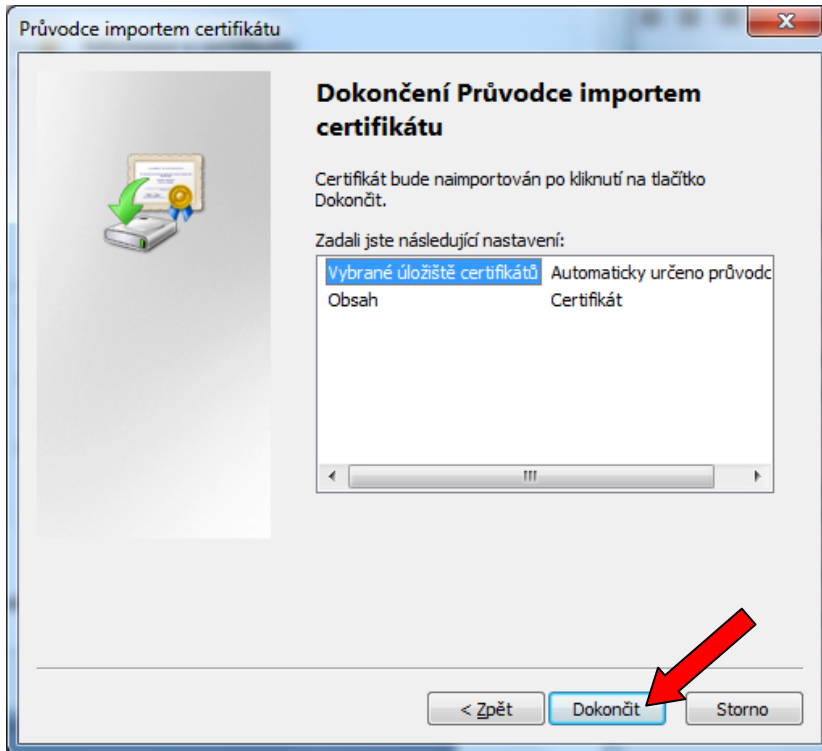
1. Postup pro import certifikátu v operačním systému WINDOWS 7

1. Klikněte 2x na certifikát a otevře se Vám okno **Certifikát**. Zvolte tlačítko **Nainstalovat certifikát...**

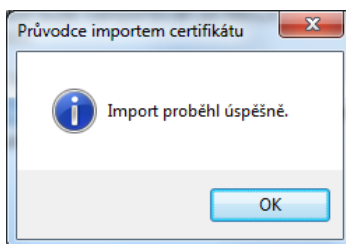


2. Otevře se Vám průvodce importem certifikátů, pomocí kterého provedete uložení certifikátu do Vašeho PC.



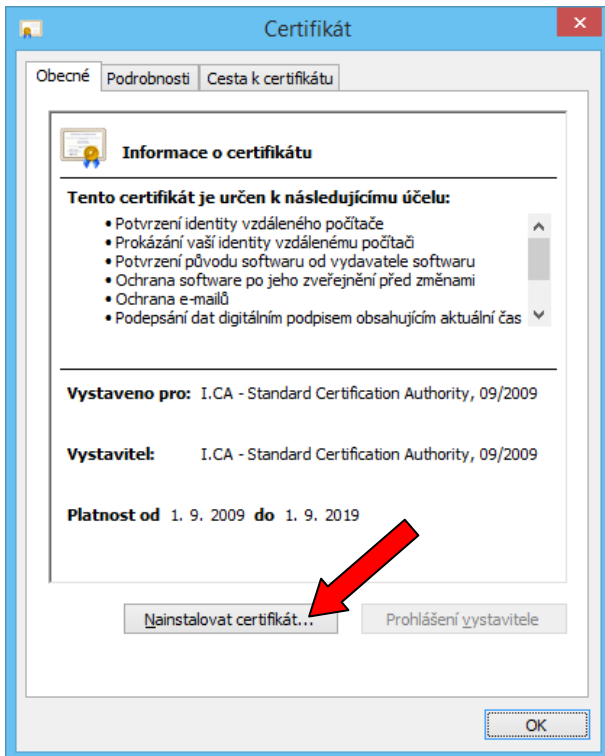


3. Po stisknutí tlačítka **Dokončit** se Vám zobrazí okno o úspěšném importu certifikátu.



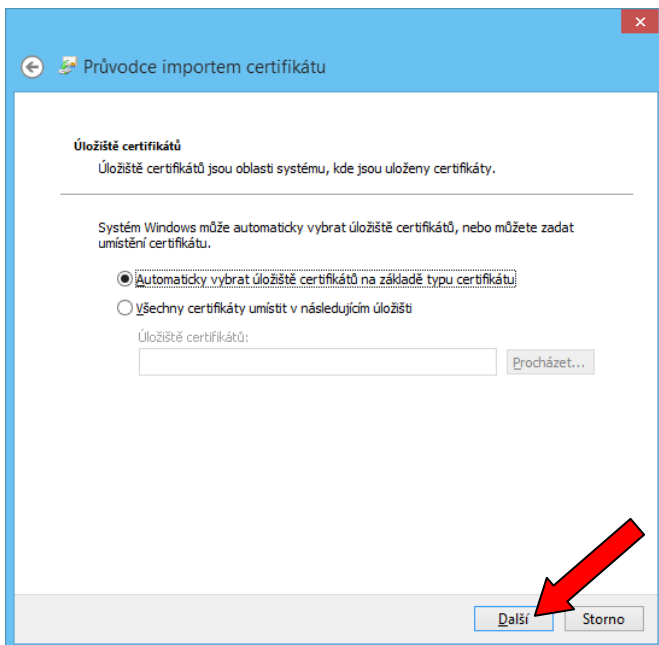
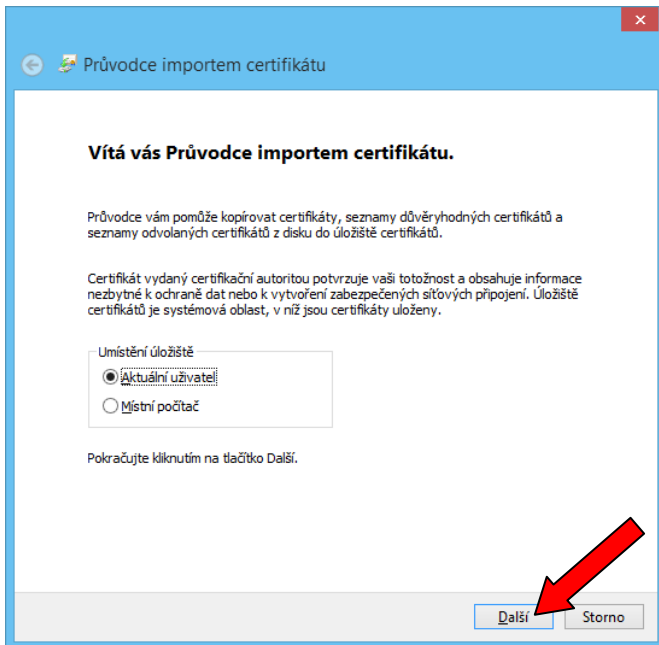
2. Postup pro import certifikátu v operačním systému WINDOWS 8

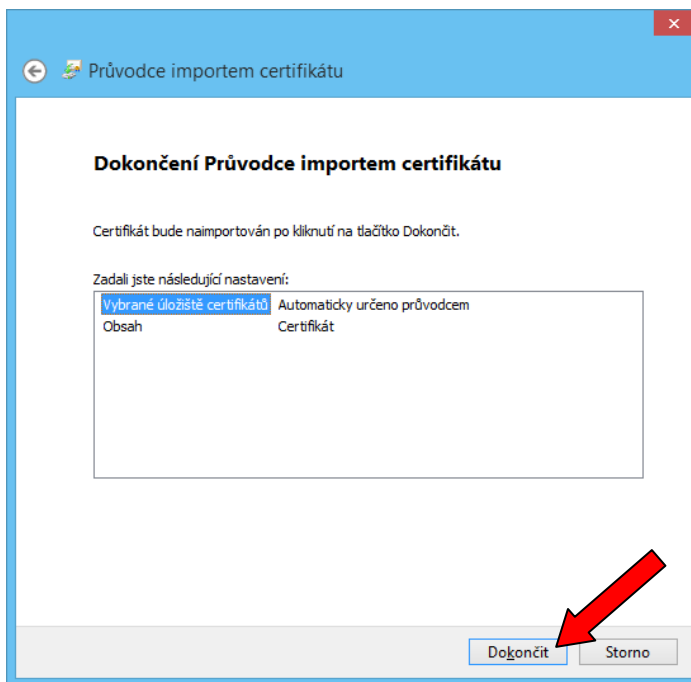
1. Klikněte 2x na certifikát a otevře se Vám okno **Certifikát**. Zvolte tlačítko **Nainstalovat certifikát...**





2. Otevře se Vám **průvodce importem certifikátů**, pomocí kterého provedete uložení certifikátu do Vašeho PC.





3. Po stisknutí tlačítka **Dokončit** se Vám zobrazí okno o úspěšném importu certifikátu.

