
# NÁPOVĚDA PRO VERISIGNIT

## PRO VERZI 2.0.6

## OBSAH

Úvod ..... 3
Vítejte v Nápovědě aplikace VerisignIT ..... 3
Certifikáty a Digitální podpis ..... 3
Instalace programu ..... 4
Systémové požadavky ..... 4
Kontaktní údaje ..... 5
Copyright ..... 5
Přihlášení do aplikace ..... 7
Licence ..... 7
Zadání jména a hesla ..... 7
Prostředí programu ..... 8
Navigace a způsob ovládání ..... 8
Hlavní okno aplikace ..... 8
Moduly ..... 9
Modul Podpisová kniha ..... 9
Modul Ověřovací kniha ..... 10
Modul Správa QCA ..... 12
Modul Správa CA ..... 13
Modul správa certifikátů ..... 13
Modul Konverze do PDF ..... 13
Modul Nastavení ..... 14
Doplňující funkce ..... 15

# ÚVOD

## VÍTEJTE V NÁPOVĚDĚ APLIKACE VERISIGNIT

Vítejte v nápovědě aplikace ***VerisignIT*** – aplikaci, která slouží k vytváření elektronických podpisů pomocí certifikátů (typu X509 v3) ke všem typům dokumentů a souborů.

Děkujeme, že používáte tento software. Děláme vše pro to, abychom splnili všechna vaše přání a očekávání od tohoto softwaru a věříme, že s ním budete maximálně spokojeni.

DIGNITA, s.r.o.

## CERTIFIKÁTY A DIGITÁLNÍ PODPIS

### POUŽITÍ CERTIFIKÁTŮ

Ověřování, kdy je třeba ověřit identitu osoby či objektu.

Ochrana soukromí zajišťující, že informace budou dostupné jen určeným osobám.

Šifrování, při kterém jsou informace skryty způsobem nerozluštitelným pro neoprávněné osoby.

Digitální podpisy zajišťující neodvolatelnost a integritu zprávy.

Tyto služby zabezpečení mohou být důležité pro zabezpečení komunikace. Kromě toho certifikáty používá mnoho aplikací systému Windows, například Internetová informační služba (IIS) společnosti Microsoft, aplikace Microsoft Outlook Express nebo aplikace Internet Explorer.

### DIGITÁLNÍ PODPIS

Digitální podpis je způsob, jak zajistit integritu a původ dat. Představuje přesvědčivý důkaz, že data nebyla po podepsání změněna, a potvrzuje identitu osoby nebo společnosti, která data podepsala. Jsou tak zajištěny důležité vlastnosti zabezpečení, integrita a neodvolatelnost, které jsou základním předpokladem bezpečných elektronických obchodních transakcí.

Digitální podpisy se při distribuci dat obvykle používají v textové neboli nezašifrované podobě. V případech, kdy samotný obsah zprávy nevyžaduje zašifrování, může existovat závažný důvod k zajištění toho, že data budou v původní podobě a že nebyla zaslána podvodně, protože data ve formátu prostého textu může v distribuovaném počítačovém prostředí číst a měnit kterýkoli uživatel sítě s příslušnými přístupovými právy, ať již je k tomu oprávněn, či nikoli.

### ZDROJE TÝKAJÍCÍ SE CERTIFIKÁTŮ

Technické informace o certifikátech, viz http://go.microsoft.com/fwlink/?LinkId=64035

Technické informace o certifikačních službách, viz http://go.microsoft.com/fwlink/?LinkId=64036

## INSTALACE PROGRAMU

Před instalací programu ***VerisignIT*** se nejdříve ujistěte, že máte **oprávnění instalovat program** v operačním systému, a že konfigurace vašeho počítače odpovídá uvedeným systémovým **požadavkům**, viz Systémové požadavky.

## SYSTÉMOVÉ POŽADAVKY

### MINIMÁLNÍ DOPORUČENÁ KONFIGURACE

- OS: Microsoft Windows XP, Windows Vista, Windows 7
- Procesor: kompatibilní s Intel Pentium® 800 MHz
- Paměť: 256 MB RAM[1]
- HDD: 300 MB volného místa na disku
- Připojení k Internetu[2]
- Instalace: Microsoft .NET Framework 4.0[3]
- Instalace: Microsoft Data Access Components (MDAC) 2.8 SP1[4]

[1] Pro komfortní práci s aplikací doporučujeme velikost operační paměti 1 GB RAM a více.

[2] Připojení k Internetu je nutné při ověřování elektronických podpisů k aktualizaci CRL, seznamu certifikátů důvěryhodných QCA a při používání časových razítek při vytváření podpisů.

[3] Ke stažení viz URL: http://www.microsoft.com/en-us/download/details.aspx?id=17851

[4] Ke stažení viz URL: http://www.microsoft.com/en-us/download/details.aspx?id=5793

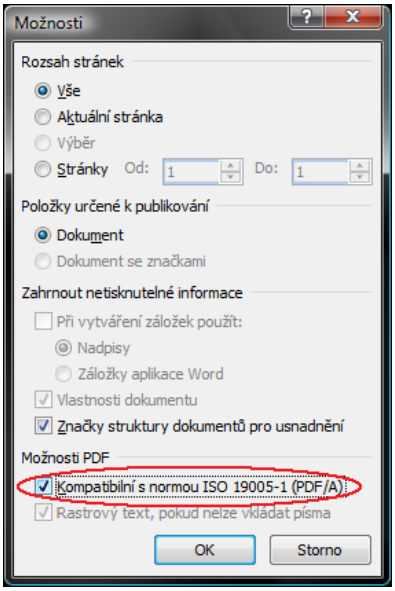
### PRO KONVERZI DO PDF JE VYŽADOVÁNA JEDNA Z NÁSLEDUJÍCÍCH MOŽNOSTÍ:

- **MS Office 2007** s instalací komponenty: ***2007 Microsoft Office Add-in: Microsoft Save as PDF*** [1]
- **MS Office 2010**

[1] Komponenta ***2007 Microsoft Office Add-in: Microsoft Save as PDF*** ke stažení viz URL: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=f1fc413c-6d89-4f15-991b-63b07ba5f2e5

## NASTAVENÍ PRO MS OFFICE 2007

Spusťte ***Microsoft Office Word 2007***. Přes tlačítko ***Office*** (kulaté tlačítko vlevo nahoře) najeďte myší na nabídku ***Uložit jako*** a vpravo vyberte možnost **PDF nebo XPS**. Zkontrolujte, že je v rolovací nabídce s názvem ***Uložit jako typ:*** (ve spodní části okna) správně nastaven formát **PDF**. Případně jej nastavte ručně. Dále klikněte na tlačítko ***Možnosti…*** a zaškrtněte volbu ***Kompatibilní s normou ISO 19005-1 (PDF/A)***. Nastavení potvrďte tlačítkem ***OK***.




## KONTAKTNÍ ÚDAJE

DIGNITA, s.r.o.,
Týnská 21,
110 00 Praha 1 - Staré Město

Fax: +420 224 808 206

E-mail: office@dignita.cz

http://www.dignita.cz

## COPYRIGHT

# PŘIHLÁŠENÍ DO APLIKACE

## LICENCE

Po prvotním spuštění aplikace se objeví licenční dialog s možností výběru licence. K načtení licenčního souboru slouží tlačítko ***Načíst licenci ze souboru***. Detaily o licenci jsou k dispozici přes tlačítko ***Informace o licenci*** (pouze pro komerční variantu). Pokud nemáte komerční licenci, můžete zvolit zkušební 30denní verzi (Trial). Po uplynutí této zkušební doby nebude možné aplikaci používat. Výběr licence potvrdíte tlačítkem ***OK***.

Pokud je použita zkušební verze (Trial), objevuje se licenční dialog po každém spuštění. Při použití platné komerční licence se po startu aplikace již licenční dialog znovu neobjevuje.

Aplikace ***VerisignIT*** obsahuje ochranu proti zpětnému posouvání systémového času počítače (obcházení 30denního limitu zkušební verze). Jakmile je taková manipulace s časem počítače zjištěna, zkušební licence se zablokuje a není nadále k dispozici. Jedinou možností jak ***VerisignIT*** dále používat je vložení platné komerční licence.

## ZADÁNÍ JMÉNA A HESLA

### PŘIHLAŠOVACÍ DIALOG

Po spuštění aplikace ***VerisignIT*** se jako první objeví přihlašovací dialog. Do pole s názvem ***Přihlašovací jméno*** zadejte své uživatelské jméno nebo jej vyberte ze seznamu, pokud obsahuje nějaké položky. Do pole s názvem ***Heslo*** zadejte heslo k vašemu uživatelskému účtu. Přihlášení proveďte pomocí tlačítka ***Přihlásit***.

Pokud je přihlašovací jméno nebo heslo zadáno chybně, aplikace na tuto skutečnost upozorní chybovým hlášením.

### PRVNÍ PŘIHLÁŠENÍ

Výchozí stav aplikace je stav, kdy ještě nedošlo k prvnímu přihlášení do aplikace a/nebo nebyly provedeny žádné uživatelské změny v nastavení. Ve výchozím stavu neexistují v konfiguraci některé hodnoty, které je nutné nastavit pro správné fungování aplikace. Více informací o nastavení najdete v sekci **Modul Nastavení**.

Po prvotním nainstalování aplikace do systému neexistuje žádný uživatelský účet. Při spuštění aplikace ***VerisignIT*** je tento stav detekován a uživatel je prostřednictvím automaticky otevřeného dialogu vyzván k založení nového účtu. Poté, co tak učiní, může se pod nově založeným účtem přihlásit.

Pokud z nějakého důvodu založení prvního účtu nedoběhne do konce, dialog je např. uživatelem uzavřen, běh aplikace ***VerisignIT*** je ukončen a při dalším spuštění se proces opakuje.

# PROSTŘEDÍ PROGRAMU

## NAVIGACE A ZPŮSOB OVLÁDÁNÍ

Základy navigace v aplikaci jsou popsány v sekci Hlavní okno aplikace. Zde je detailněji vysvětleno ovládání jednotlivých funkčních prvků, jež spolu s funkcemi horní lišty tvoří samotný obsah modulů.

## HLAVNÍ OKNO APLIKACE

Hlavní okno programu ***VerisignIT*** se skládá z několika modulů, viz Moduly, umístěnými v levé části okna. Mezi jednotlivými moduly lze přepínat kliknutím na příslušný modul. Část hlavního okna s přehledem modulů lze tažením pravého okraje pomocí myši zvětšovat či zmenšovat na libovolnou velikost, dle osobních preferencí. Po uvolnění tlačítka myši dojde k uložení aktuální pozice, takže při dalších startech aplikace už není potřeba si takto hlavní okno znovu přizpůsobovat.

Po aktivaci modulu v levé části se v horní liště objeví záložky s funkcemi k danému tématu. Současně dojde k automatickému výběru záložky, jejíž funkce jsou nejčastěji používané právě pro aktivní modul. Hlavní část hlavního okna tvoří samotný funkční obsah modulu.

# MODULY

Moduly jsou jednotlivé ucelené tematické celky aplikace, které spravují danou oblast.

## MODUL PODPISOVÁ KNIHA

Modul **Podpisová kniha** slouží k vytváření elektronických podpisů k dokumentům klientským certifikátem typu **X509 v3**. V hlavním panelu okna je přehled provedených podpisových akcí, které daný přihlášený uživatel provedl. Tyto záznamy jsou uloženy v šifrované podobě do databáze programu. Podpisová akce je taková akce uživatele, při níž jsou vybrány soubory na pevném disku nebo jiném nosiči a jsou k nim vytvořeny soubory s podpisem, popř. i soubory s časovými razítky. Kopie všech výše zmíněných souborů jsou v zašifrované podobě rovněž uloženy do databáze, to z důvodu pozdějšího prohlížení nebo zálohování podepsaných dokumentů.

Nová podpisová akce se provádí pomocí tlačítka ***Podepsat*** v horní liště modulu, v záložce ***Podpisová kniha*** (popř. přes kontextové menu). Spustí se průvodce, který uživatele provede dvěma kroky nutnými k provedení podpisové akce. Tento průvodce se spustí také automaticky v případě, že uživatel přetáhne (tzv. **Drag & Drop**) vybrané soubory a/nebo adresáře pomocí myši z Windows do okna aplikace ***VerisignIT***.

Soubory vybrané k podepsání lze libovolně přidávat a odebírat pomocí příslušných tlačítek napravo od okna seznamu souborů nebo pomocí kontextové nabídky seznamu souborů pomocí pravého tlačítka myši. Rovněž je možné soubory přidávat přetažením myší z Windows přímo do seznamu souborů.

**Tip:** Označené soubory lze snadno odebrat pomocí klávesy ***Delete***.

**V prvním** kroku průvodce je možné zadat také to, zda se má automaticky provádět **konverze** daného podepisovaného souboru do formátu PDF. Tato volba vyžaduje přítomnost alespoň jednoho podporovaného PDF konvertoru v systému a jeho nastavení (pro vice informací o nastavení PDF konverze viz sekci **Modul Nastavení**). Volba konvertoru se provádí v modulu Nastavení. Pokud je konverze dostupná a konvertor vybrán, je v seznamu souborů zobrazen sloupec ***Konverze***, který indikuje, zda je daný soubor možné do formátu PDF převést nebo nikoli. Podporovaný typ souboru je označen ikonou souboru typu PDF.

Další možností je zaškrtnutí položky ***Neukládat záznam o akci do Podpisové knihy***, což je v podstatě akce rychlého podepsání, která není zaznamenána do databáze a není tedy možné později prohlížet informace o této události nebo soubory, které byly podepsány ani jejich podpisy a časová razítka.

Do pole ***Popis podpisové akce*** může uživatel zadat popis dané akce, který bude zobrazen v přehledu v Podpisové knize. Pokud je vybrán alespoň jeden soubor k podepsání, lze přejít na druhý krok průvodce pomocí tlačítka ***Další>>>***.

**V druhém** kroku je možné změnit přednastavené parametry. Tato změna se týká pouze aktuální podpisové akce. Trvalá změna parametrů se provádí v modulu Nastavení. V případě, že nastavení podpisu měnit nechceme nebo jsme ho již provedli, spustíme akci tlačítkem ***Podepsat!***. Objeví se **indikátor průběhu** podepisování s informací o zpracovávaném souboru. Po **úspěšném** dokončení se průvodce ukončí a v Podpisové knize se objeví nový záznam.

## POLOŽKY PŘEHLEDU PODPISOVÁ KNIHA

***Datum podpisové akce:*** Slouží řazení záznamů v Podpisové knize a k snazšímu vyhledávání pomocí filtrování záznamů. Filtrování lze provádět v levém panelu Podpisové knihy.

***Zdroj času:*** Udává, jak byl získán čas pro danou ověřovací akci.

***Uživatel (login):*** Uživatel, resp. jeho uživatelské přihlašovací jméno, který akci provedl.

***Popis podpisové akce:*** Text s popisem akce zadaný uživatelem v průvodci.

***Konverze PDF:*** Příznak, zda byla v průvodci zatržena volba ***Konvertovat podporované typy souborů do formátu PDF***.

## POLOŽKY DETAILU ZÁZNAMU PODPISOVÉ AKCE

***Originální soubor:*** Soubor vybraný uživatelem k podepsání v průvodci.

***Podepisovaný soubor:*** Soubor, kterému byl vytvořen podpis. V případě volby konverze do PDF se liší od Originálního souboru, neboť podepisovaným souborem je ve skutečnosti až výstup konverze neboli soubor typu PDF. V opačném případě se Podepisovaný soubor rovná Originálnímu souboru.

***Soubor s podpisem:*** Je většinou nově vzniklý soubor podpisu (přípona **.p7s**). Může jím být ale PDF soubor, kterému byl vytvořen vnitřní podpis. Toto chování lze nastavit trvale v modulu Nastavení nebo pro každou podpisovou akci zvlášť v druhém kroku průvodce.

***Stav podepsání:*** Uvádí, jak proběhlo podepsání, resp. vytvoření souboru s podpisem.

***Soubor s časovým razítkem:*** Pokud je nastaveno vytváření časových razítek, obsahuje jméno souboru s tímto razítkem. Jedná se opět o soubor s příponou **.p7s**. Časové razítko může být rovněž vytvořeno jako interní časové razítko, neboli uvnitř souboru s podpisem.

***Stav časového razítka:*** Uvádí, jak proběhlo vytvoření časového razítka.

***Konverze PDF:*** Příznak, zda byl soubor konvertován do formátu PDF.

***Stav konverze:*** Uvádí, jak proběhla konverze daného souboru.

**Soubory** z podpisové akce lze kdykoli **prohlížet**, resp. otevírat v asociovaném programu nebo je **ukládat** na disk. A to jak pouze vybrané soubory nebo hromadně všechny soubory (daného typu) pro celou podpisovou akci. Tyto volby jsou dostupné přes **kontextové menu** v přehledu panelu Podpisová kniha a jsou vyvolány pravým tlačítkem myši.

# MODUL OVĚŘOVACÍ KNIHA

Modul **Ověřovací kniha** slouží k ověřování elektronických podpisů typu **.p7s** dokumentů. V hlavním panelu modulu Ověřovací kniha je přehled provedených ověřovacích akcí, které daný přihlášený uživatel provedl.

Tyto záznamy o ověřování podpisů jsou rovněž uloženy v šifrované podobě v databázi programu a v úložišti na disku. Ověřovací akce je taková akce uživatele, při níž jsou vybrány soubory na pevném disku nebo jiném nosiči, včetně souborů s podpisy a externími časovými razítky a tyto soubory jsou nejdříve aplikací párovány automaticky s každým zadaným dokumentem a ověřeny. Pokud aplikace **nemůže** některé zadané soubory automaticky spárovat na základě jejich unikátní miniatury (**hashe**) ani na základě jmen souborů, vyzve uživatele, aby provedl **párování** ručně.

Nová ověřovací akce se provádí pomocí tlačítka ***Ověřit*** v horní liště modulu, v záložce ***Ověřovací kniha***. Spustí se průvodce, který uživatele provede procesem ověřovací akce.

Soubory vybrané k ověření lze libovolně přidávat a odebírat pomocí příslušných tlačítek napravo od okna seznamu souborů nebo pomocí kontextové nabídky seznamu souborů pomocí pravého tlačítka myši. Rovněž je možné soubory přidávat přetažením myší z Windows přímo do seznamu souborů. Dále lze v průvodci zadat popis ověřovací akce. Další možností je zaškrtnutí položky ***Výsledek ověření do okna***, což způsobí zobrazení výsledku po skončení ověřování v samostatném okně pro lepší přehled uživatele o výsledku ověřovací akce.

Pokud jsou vybrány soubory, zpřístupní se tlačítko ***Ověřit!***. Kliknutím se spustí proces ověřování.

## DIALOG RUČNÍHO PÁROVÁNÍ

Plocha okna je rozdělena na tři seznamy s přehledem souborů. **Vlevo nahoře** je **seznam ověřovaných dokumentů**. **Napravo** od něj je **seznam uživatelem ručně připárovaných souborů** s podpisem nebo externím časovým razítkem k právě vybranému ověřovanému souboru. **Ve spodní části** je pak **seznam dosud nespárovaných** podpisů nebo externích časových razítek, ze kterých může uživatel vybírat a párovat je s libovolným ověřovaným souborem.

## POSTUP PÁROVANÍ

**Označíme ověřovaný soubor** (vlevo nahoře), ke kterému chceme připárovat podpis resp. externí časové razítko, v dolním seznamu dosud nespárovaných **označíme vybrané položky** a připárování provedeme pomocí tlačítka s ikonou  . Pokud chceme připárovanou položku **odebrat** (tzn. vrátit ji na seznam dosud nespárovaných), označíme ji v pravém horním seznamu a pomocí tlačítka s ikonou  tuto akci provedeme.

Pokud jsme s párováním hotovi, potvrdíme tlačítkem ***Potvrdit***. Jestliže v seznamu dosud nespárovaných podpisů resp. externích časových razítek zůstaly nějaké položky, aplikace se dotáže uživatele, zda si přeje v párování pokračovat nebo, zda je výsledek párování konečný a má se pokračovat v ověřovací akci.

## POLOŽKY PŘEHLEDU OVĚŘOVACÍ KNIHA

***Datum ověřovací akce:*** Slouží řazení záznamů v Ověřovací knize a k snazšímu vyhledávání pomocí filtrování záznamů. Filtrování lze provádět v levém panelu Ověřovací knihy.

***Zdroj času:*** Udává, jak byl získán čas pro danou ověřovací akci.

***Uživatel (login):*** Uživatel, resp. jeho uživatelské přihlašovací jméno, který akci provedl.

***Popis ověřovací akce:*** Text s popisem akce zadaný uživatelem v průvodci.

## POLOŽKY DETAILU ZÁZNAMU OVĚŘOVACÍ AKCE

***Originální soubor:*** Soubor, vůči kterému ověřujeme jeho podpis.

***Soubor s podpisem / Soubor s externím časovým razítkem:*** Je soubor typu **.p7s**. Může jím být ale PDF soubor, kterému byl vytvořen vnitřní podpis.

***Stav ověření:*** Uvádí, jak proběhlo ověření podpisu.

***Integrita zachována:*** Příznak, zda nedošlo k porušení integrity podpisu zásahem zvenčí.

***Ověřený čas vytvoření:*** Nejmenší možný čas, o kterém můžeme prohlásit, že podpis už existoval.

***Čas příštího ověření:*** Nejmenší možný čas, kdy už víme, že validace všech certifikátů použitých pro podpis bude úspěšná vzhledem k aktuálnosti stahovaných CRL souborů.

V okně s výsledkem ověření resp. pak v přehledu ověřovací knihy lze záznam rozbalit – symbol "**+**" vlevo na řádku – a prohlížet detailní výpis ověření.

Detail ověření je zobrazen jako strom, kdy každý soubor obsahuje informace o výsledku. Počet položek v stromu je závislý na výběru řádku v ověřovací knize. Pokud je označen řádek s originálním souborem, zobrazí se v detailu všechny informace o všech jeho podpisech a časových razítkách. Pokud je označen jeden konkrétní soubor s podpisem nebo časové razítko, zohlední panel s detailem tento výběr a zobrazí informace pouze pro něj.

**Soubory** z ověřovací akce lze kdykoli **prohlížet**, resp. otevírat v asociovaném programu nebo je **ukládat** na disk. A to jak pouze vybrané soubory nebo hromadně všechny soubory (daného typu) pro celou ověřovací akci. Tyto volby jsou dostupné přes **kontextové menu** v přehledu panelu Ověřovací kniha a jsou vyvolány pravým tlačítkem myši.

Pokud při ověřování zůstanou nějaké nespárované soubory zobrazí se jejich přehled. Pokud při ověřování všechny zadané soubory nespárovány (neobsahují podepsaná data a neexistuje k nim oddělený P7S podpis), může uživatel zvolit jestli se záznam o ověřovací akci uloží do ověřovací knihy nebo nikoli.

# MODUL SPRÁVA QCA

Modul **Správa QCA** slouží k přehledu o kořenových certifikátech **certifikačních autorit** ze všech členských zemí EU, které byly aplikací ***VerisignIT*** staženy za účelem ověření kvalifikovanosti certifikátu z nějakého podpisu. Aplikace udržuje tento seznam a aktualizuje jej dle potřeby, a to zejména při další ověřovací akci. Pro danou zemi se vždy stáhne kompletní seznam CA, které v dané zemi působí.

Záznamy v přehledu jsou seskupeny dle země, ve které byly certifikáty CA vydány. Tyto skupiny lze skrývat a rozbalovat dle potřeby. Nebo lze využít filtrování přes levý panel modulu **Správa QCA**.

Pro aktualizaci zobrazovaných dat použijte funkci ***Aktualizovat***, dostupnou přes kontextové menu nebo horní lištu na záložce ***Správa QCA***, čímž docílíte zobrazení aktuálního seznamu všech certifikátů QCA, které aplikace používá. Online aktualizaci není možné provádět na vyžádání uživatele, ale je zajištěna automaticky dle potřeb aplikace ***VerisignIT***.

Pro zobrazení detailu certifikátu slouží funkce ***Otevřít detail***, dostupná pro vybraný certifikát přes kontextové menu (nebo v horní liště na záložce ***Správa QCA***) po kliknutí pravého tlačítka myši. Akce vyvolá systémový dialog s informacemi o certifikátu.

## MODUL SPRÁVA CA

Modul **Správa CA** slouží k správě kořenových certifikátů **certifikačních autorit**, které si uživatel sám nadefinuje. Vlastní kořenové certifikáty CA se přidávají, resp. odebírají pomocí funkcí ***Přidat certifikát***, resp. ***Odebrat certifikát***. Zmíněné funkce jsou dostupné přes kontextové menu nebo horní lištu na záložce ***Správa CA***.

Pro zobrazení detailu certifikátu slouží funkce ***Otevřít detail***, dostupná pro vybraný certifikát přes kontextové menu (nebo v horní liště na záložce ***Správa CA***) po kliknutí pravého tlačítka myši. Akce vyvolá systémový dialog s informacemi o certifikátu.

Záznamy v přehledu jsou opět seskupeny dle země, ve které byly certifikáty CA vydány. Tyto skupiny lze skrývat a rozbalovat dle potřeby. Nebo lze využít filtrování přes levý panel modulu **Správa CA**.

## MODUL SPRÁVA CERTIFIKÁTŮ

Modul **Správa certifikátů** slouží ke správě osobních certifikátů, které jsou instalovány v úložišti certifikátů na uživatelově počítači. Zobrazuje základní údaje o certifikátu, kliknutím na tlačítko **Detail** lze zobrazit systémový dialog s kompletními informacemi o certifikátu. Některé údaje o certifikátech (Důvěryhodný, Typ, Specifikace a Revokovaný) nejsou ve výchozím zobrazení vyplněny, lze je získat kliknutím na tlačítko **Načíst podrobnosti**. Jejich načítání vyžaduje provést validaci certifikátu (vč. stažení CRL ze serveru), proto může trvat delší dobu.

V seznamu certifikátů je zvýrazněn certifikát nastavený aktuálně jako podpisový (tmavé podbarvení), certifikáty někdy v minulosti používané jako podpisové (světlé podbarvení), certifikáty s vypršenou dobou platnosti (tmavě červené podbarvení data) a certifikáty, jejichž doba platnosti vyprší v blízké době (světle červené podbarvení data). Tuto dobu lze nastavit v modulu **Nastavení**.

## MODUL KONVERZE DO PDF

Modul **Konverze PDF** slouží k rychlému převádění **podporovaných typů** souborů do formátu **PDF**. Množina podporovaných typů závisí na použitém PDF konvertoru v systému. Pro více informací o podporovaných konvertorech a jejich správném nastavení viz sekci Systémové požadavky.

Výběr souborů pro konverzi do PDF se provádí opět pomocí příslušných tlačítek (***Přidat***, ***Odebrat*** a ***Odebrat vše***) nalevo od seznamu souborů nebo přes kontextové menu seznamu souborů. Soubory můžeme pohodlně přidávat také tažením pomocí myši z prostředí Windows (tzv. **Drag & Drop**).

**Tip:** Označené soubory lze snadno odebrat pomocí klávesy **Delete**.

V levém panelu je přednastavena volba konvertoru, ovlivněno nastavením viz modul Nastavení. Pro každou akci můžeme buď ponechat přednastavený konvertor, nebo zvolit jiný (nainstalovaný v systému) dle libosti.

Podporované typy souborů jsou v seznamu označeny ikonou s typem souboru PDF, která se zobrazí ve sloupci ***Konverze***. Pokud jsme vybrali i soubory, jejichž typ podporován není, tato ikona se u nich nezobrazí a takový soubor je z konverze vyloučen a je aplikací ***VerisignIT*** ignorován.

Pokud chceme ihned vidět výsledek konverze, zatrhneme políčko vlevo na každém řádku v seznamu souborů, který chceme po konverzi otevřít a vlevo dole zaškrtneme volbu ***Po dokončení konverze otevřít zaškrtnuté soubory v asociovaném programu***.

Samotnou konverzi spustíme tlačítkem ***Konvertovat do PDF*** v horní liště na záložce **Konverze PDF**. Průběh konverze a informace o právě zpracovávaném souboru se zobrazí v dolní části panelu. Pokud byl soubor úspěšně konvertován a byl označen pro otevření, předá jej aplikace ***VerisignIT*** operačnímu systému Windows k otevření.

## MODUL NASTAVENÍ

Modul **Nastavení** slouží ke správě veškerých parametrů a nastavení aplikace ***VerisignIT***. V hlavním panelu modulu **Nastavení** je přehled nastavených parametrů zobrazen pouze v **režimu prohlížení**, tzn. hodnoty nelze nastavovat přímo. K editaci hodnot slouží funkce ***Změnit nastavení*** v horní liště na záložce ***Nastavení***.

Tato akce otevře okno s nastavením aplikace v **režimu editace**. Změny provedené v tomto okně jsou akceptovány a trvale uloženy až po kliknutí na tlačítko ***Uložit nastavení***. Zavřením okna jiným způsobem jsou veškeré změny provedené v okně nastavení ztraceny.

### POPIS ZÁLOŽEK OKNA NASTAVENÍ

***Obecné:*** Obecná nastavení týkající se chování okna aplikace ***VerisignIT*** po spuštění. Aplikace umožňuje, místo času lokálního počítače, pracovat s přesným časem získaným z Internetu z NTP serveru. Pokud jsou pracovní stanice, na kterých je ***VerisignIT***, v doméně, tedy je čas na lokálních stanicích důvěryhodný, není třeba používat čas z NTP serveru.

***Podpisy:*** Nastavuje parametry aplikované při vytváření elektronických podpisů. V horní části záložky je nutné vybrat certifikát, kterým se budou elektronické podpisy souborů vytvářet. Certifikát je třeba si nejdříve nainstalovat do systému. Tlačítko ***Vybrat certifikát*** zobrazí okno s nabídkou certifikátů uložených v systému Windows. Označíme vybraný certifikát a tlačítkem ***OK*** volbu potvrdíme. Bez vybraného certifikátu pro podepisování nelze nastavení uložit. Ve spodní části okna jsou **rozšiřující záložky** s nastavením **dle typu** podpisu, tzn., zda podepisujeme soubor typu PDF nebo obecně jakýkoli soubor.

**Rozšiřující záložky:**

- ***Obecné:*** Nastavení společných parametrů pro podepisování všech typů souborů. Volba typu **hash** algoritmu.
- ***Podpisy PDF:*** Volba, zda při podepisování souborů typu **PDF** podepisovat vnitřním podpisem či nikoli. Uživatel volí typ podpisu PDF souboru a položky ***Jméno autora*** a ***Důvod podpisu***, které se zobrazují uvnitř podepsaného PDF souboru v případě, že byla zvolena možnost vnitřního podpisu dokumentu.
- ***Podpisy XML:*** Volba, zda při podepisování souborů typu **XML** podepisovat vnitřním podpisem či nikoli. Existuje tzv. Enveloping (Obalující) a Enveloped (Obalený) typ, viz odkaz http://en.wikipedia.org/wiki/XML_Signature. Kanonizační metoda určuje z čeho se vytváří hash

podpisu (co z XML souboru se podepisuje), viz http://en.wikipedia.org/wiki/XML_Signature#XML_Canonicalization. Forma podpisu XAdES znamená, že podpis obsahuje jisté podepsané atributy. Tato forma vyhovuje směrnici 1999/93/EC Evropského Parlametu a umožňuje mj. pozdější snadnou archivaci podpisu (http://en.wikipedia.org/wiki/XAdES).

- ***Podpisy ZFO/FO:*** Vnitřní podpisy formulářů. Formát ZFO pro datové schránky není podporován. Podporován je Zipped FO, tj. zip archiv obsahující .fo formulář.
- ***Podpisy ISDOC/ISDOCX:*** Vnitřní podpisy pro formát elektronické fakturace (http://www.isdoc.cz)
- ***Podpisy OOXML:*** Jedná se o vnitřní podpisy některých dokumentů Microsoft Office, tzv. Office Open XML dokumentů (viz http://en.wikipedia.org/wiki/Office_Open_XML). Jsou to konkrétně dokumenty s příponou .docx, .xlsx a .pptx. Protože je to zaobalený XML podpis, lze u něj nastavit formu podpisu XAdES, viz předchozí Podpisy XML.
- ***Nastavení podpisu P7S:*** Uživatel volí, zda má být vytvářený podpis **oddělený** (tzn. k souboru se vytvoří nový soubor obsahující pouze podpis) nebo **začleněný** (tzn. do vytvořeného souboru s podpisem je začleněn celý původní podepisovaný soubor).
- ***Časová razítka:*** Volba ***Vyžadovat časové razítko od autority*** znamená, že při vytváření podpisu vznikne ještě časové razítko od nastavené autority. Případně lze zaškrtnout volbu ***Externí časové razítko***, čímž dojde k vytvoření samostatného souboru s časovým razítkem. Pokud chceme používat časová razítka, nastavíme adresu URL autority. Jestliže je vyžadována autentizace, máme na výběr ze dvou možností: **autentizace certifikátem** nebo autentizace **jménem a heslem**. Volba závisí na možnostech autentizace dané autority.

***Připojení:*** Umožňuje nastavit detaily internetového připojení.

***Konverze PDF:*** Definuje, který PDF konvertor má být použit při konverzi souborů do formátu PDF při podepisování. Tato volba rovněž ovlivňuje výchozí volbu konvertoru v modulu ***Konverze PDF***.

***Integrace:*** Umožňuje definovat typy souborů, které mají být asociovány s aplikací ***VerisignIT***. V kontextovém menu zaregistrovaných souborů se objeví položka ***Otevřít v aplikaci VerisignIT***. Kliknutím na tuto volbu se spustí aplikace a bezprostředně poté i průvodce podepisováním souborů s předdefinovaným souborem, přes jehož kontextové menu byla aplikace spuštěna. Kliknutím na tlačítko ***Nastavit přípony*** se otevře dialog se seznamem typů souborů, které mohou být aplikací zaregistrovány. Výběr se provádí **zaškrtnutím** vybraných položek a potvrzením pomocí tlačítka ***OK***. Integrace aplikace ***VerisignIT*** do Windows vyžaduje administrátorská oprávnění!

## DOPLŇUJÍCÍ FUNKCE

### SPRÁVA ÚČTŮ

K editaci aktivně přihlášeného účtu uživatele slouží tlačítko ***Editovat účet*** umístěné v horní liště na záložce ***Obecné***. Po kliknutí na tlačítko se objeví dialog s možností editace jména uživatele, hesla a textu s nápovědou pro případ zapomenutí hesla. Uložení změn provedeme tlačítkem ***Potvrdit***.

Předvyplněná maska u polí ***Heslo*** a ***Ověření hesla*** délkou neodpovídá skutečné délce hesla, které si uživatel nastavil. Pokud nechceme heslo měnit, ponecháme předvyplněné hodnoty.

V případě změny hesla rovněž nezapomeňte aktualizovat text v poli ***Nápověda pro případ zapomenutí hesla***. Tuto položku doporučujeme nastavit vždy, protože v případě zapomenutí hesla je pro Vás jedinou možností připomenutí nastaveného hesla. V opačném případě hrozí ztráta přístupu do aplikace pod daným uživatelským účtem a s tím spojená ztráta všech dat aplikace, která se účtu týkají.

K přidání dalších účtů pro přístup k aplikaci ***VerisignIT*** slouží tlačítko ***Přidat účet*** umístěné v horní liště na záložce ***Obecné***. Vyplnění všech polí, kromě pole ***Nápověda pro případ zapomenutí hesla***, je povinné. Uložení nového účtu provedeme opět tlačítkem ***Potvrdit***.

## LICENCE

Pro informace o používané licence a načtení nového licenčního souboru slouží tlačítko ***Licence*** na záložce ***Obecné*** v horní liště. Zobrazí se dialog, kde je aktuálně používaná licence. Detaily o komerční licenci jsou k dispozici přes tlačítko ***Informace o licenci***. K načtení licenčního souboru slouží tlačítko ***Načíst licenci ze souboru***. Výběr licence potvrdíte tlačítkem ***OK***.

## PROTOKOL O CHYBÁCH

Funkce slouží k zobrazení informací o chybách vzniklých při běhu aplikace. Tento výpis lze prohlížet, kopírovat do systémové schránky a především zasílat e-mailem k nám na analýzu problému. Tato zpětná vazba nám pomáhá při zlepšování aplikace ***VerisignIT***.