LongTermValidator

NÁPOVĚDA

PRO VERZI 1.1.0

OBSAH

ÚVOD

VÍTEJTE V NÁPOVĚDĚ APLIKACE LONGTERMVALIDATOR

Vítejte v nápovědě aplikace ***LongTermValidator*** – aplikaci, která slouží k archivaci elektronických podpisů přítomných v ZFO zprávách pocházejících z informačního systému datových datových schránek.

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.

ARCHIVACE DIGITÁLNÍCH PODPISŮ

SMYSL ARCHIVACE

Důvod, proč digitální podpisy archivujeme je ten, že chceme zachovat možnost jejich ověřování i ve velmi vzdálené době. V takové době už nemusí existovat certifikační autorita, která vydala certifikát použitý k vytvoření podpisu. To znamená, že už nebude možné dohledat řetězec vydávajících certifikátů včetně kořenového a nebude tak možné určit důvěryhodnost podepisujícího certifikátu. Navíc nepůjdou získat CRL soubory (popř. OCSP odpovědi), které by určili, zda byl nebo nebyl podepisující certifikát v době podpisu revokovaný. Také algoritmy pro tvorbu otisků zpráv a algoritmy pro šifrování otisků zpráv pomocí privátního klíče certifikátu mohou být v budoucnosti prolomeny. V takovém případě je informace o zachování integrity, ať už samotné podepsané zprávy nebo podepsaného certifikátu, zcela bezcenná. Právě tyto problémy řeší archivace podpisu.

ARCHIVAČNÍ KROKY

Princip archivace digitálního podpisu spočívá v postupném přidávání dodatečných informací k podpisu ve formě tzv. nepodepsaných atributů. Jsou to datové celky, které jsou k podpisu přidány až po jeho vytvoření, tedy až po vytvoření a zašifrování otisku. Hodnota otisku tedy není ovlivněna těmito atributy. Tyto atributy se k podpisu přidávají v jednotlivých krocích, které jsou od sebe časově různě vzdálené.

Následuje popis jednotlivých archivačních kroků, které se postupně aplikují na neorazítkovaný podpis.

1. Orazítkování podpisu. Pokud podpis ještě není orazítkován, je k němu, co nejdříve je to možné, přidáno běžné časové razítko. Tento krok se musí provést ještě před vypršením platnosti podpisového certifikátu, jinak podpis ztratí možnost být správně ověřen a tedy i archivován. Razítko by se mělo přidat co nejdříve, jelikož se musí počítat s tím, že podpisový certifikát může být kdykoli revokován.
2. Přidání referencí na validační data. Validační data tvoří řetězec certifikátů, která jsou nutná pro určení věrohodnosti podpisového certifikátu. Řetězec tedy obsahuje certifikáty od podpisového, přes vydávající, až po kořenový. Dále validační data obsahují informace o revokaci (CRL nebo OCSP) všech uvedených certifikátů v řetězci. Tento krok je nutné aplikovat ještě před vypršením certifikátu

časového razítka, ale současně až po uplynutí jisté doby od 1. kroku (tzv. grace period), kdy je už jisté, že validační data obsahují případnou informaci o revokaci.

3. Orazítkování referencí validačních dat tzv. validačním razítkem. Tímto se zachová možnost ověření certifikátů ve validačních datech i po jejich expiraci/revokaci.
4. Přidání samotných validačních dat.
5. Přidání archivačního razítka. Periodickým přidáváním archivačních razítek (vždy před vypršením certifikátu některého jiného časového razítka) se předchází kompromitaci podpisu z důvodu jeho oslabení v dlouhodobém časovém horizontu.

INSTALACE PROGRAMU

Před instalací programu ***LongTermValidator*** 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: 1 GB RAM
- HDD: 300 MB volného místa na disku
- Připojení k Internetu[1]
- Instalace: Microsoft .NET Framework 4 Client Profile[2]
- Instalace: Microsoft SQL Server Compact 4.0[3]

[1] Připojení k Internetu je nutné při archivování elektronických podpisů k aktualizaci CRL, seznamu certifikátů CA a při volání služeb časových autorit.

[2] Ke stažení viz URL: http://www.microsoft.com/download/en/details.aspx?id=17113

[3] Ke stažení viz URL: http://www.microsoft.com/download/en/details.aspx?id=17876

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***. Pokud nemáte komerční licenci, můžete zvolit zkušební (Trial). Ta je omezena na pět zpráv nebo na použití maximálně deseti časových razítek. 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.

PROSTŘEDÍ PROGRAMU

HLAVNÍ OKNO APLIKACE

Hlavní okno programu ***LongTermValidator*** se skládá z horní lišty s hlavními funkcemi, levého panelu pro statistiky a z panelů tabulek obsahující přehled ZFO zpráv.

TLAČÍTKO „NAČÍST“

Při stisku se do tabulek se ZFO zprávami načtou informace o těchto zprávách. Načtené zprávy reflektují zprávy umístěné v pracovních složkách (viz nastavení pracovních složek).

TLAČÍTKO „AUTORIZOVAT“

Při stisku se pustí aplikace pro autorizaci ZFO zpráv. Pokud tato aplikace během svého běhu autorizovala nějaké zprávy (vytvořila nové zprávy ve zdrojové složce), pak při ukončení této aplikace budou odpovídající staré neautorizované zprávy přesunuty do složky „Neautorizované zprávy“. Tato složka se automaticky vytvoří na úrovni zdrojové složky.

TLAČÍTKO „ARCHIVOVAT“

Při stisku se na vybraných zprávách (zaškrtnuté zprávy v tabulkách) provedou archivační kroky (viz fáze archivace podpisu).

PANEL S TABULKAMI S PŘEHLEDEM ZFO ZPRÁV

Tento panel obsahuje čtyři tabulky se ZFO zprávami. Rozlišují se podle toho, za jakou dobu dojde k exspiraci certifikátu užitého pro tvorbu časového razítka (normálního, validačního či archivního). Určí se tedy časové razítko s certifikátem s nejčasnějším vypršením certifikátu. (Datum a čas vypršení takového certifikátu je uveden ve sloupci „Vypršení cert. čas. razítka“, viz dále.)

- Validní – Certifikát exspiruje později než je jistá doba T.
- Brzy exspirují – Certifikát exspiruje dříve než doba T.
- Exspirované -Certifikát už exspiroval.
- Ostatní – Neobsahuje vůbec časové razítko nebo není možné určit čas v důsledku nějaké chyby.

Doba T se určuje v nastavení (viz dále).

V tabulce jsou přehledně na každém řádku zobrazeny některé informace o ZFO zprávách a informace o podpisu v této zprávě.

- Cesta k souboru – aktuální umístění souboru na disku včetně jeho jména
- Podepisovatel – jméno podepisovatele uvedené v certifikátu podepisovatele
- ISDS čas. razítko – čas orazítkování ZFO zprávy (ISDS razítkuje zprávy při jejich odesílání)
- ID zprávy – ID zprávy převzaté z obálky ZFO

- Odesílatel – odesílatel zprávy uvedený v obálce zprávy
- Příjemce – příjemce zprávy uvedený v obálce zprávy
- Do vlast. rukou – jméno příjemce do vlastních rukou
- Fáze archivace podpisu – viz Fáze archivace podpisu
- Vypršení cert. čas. razítka – čas vypršení certifikátu toho razítka, které vyprší nejdříve (normální, validační či archivační)
- Chybová hláška – pokud při čtení resp. archivaci ZFO zprávy dojde k nějaké chybě, která znemožní zobrazení všech informací resp. znemožní provést archivační krok, pak je zde zobrazen její popis.
- CAdES-BES/EPES – podpis ne/vyhovuje specifikaci CAdES-BES/EPES

FÁZE ARCHIVACE PODPISU

Aplikace rozlišuje čtyři fáze podpisu, se kterými dále pracuje, tzn. pokud může, aplikuje další krok archivace podpisu tím, že k němu přidá jisté informace ve formě nepodepsaných atributů. Pokud není důvod aplikovat další krok archivace, pak se tak neděje (závisí na nastavení aplikace a na aktuálním čase).

1. Basic – Běžný podpis, který zatím není opatřen časovým razítkem.
2. Timestamped – Podpis, který je už opatřen časovým razítkem.
3. ExtendedLongTerm – Podpis opatřený navíc orazítkovanými referencemi validačních dat i samotnými hodnotami validačních dat (všechny certifikáty z certifikační cesty a všechny potřebné CRL).
4. Archived – Podpis opatřený navíc jedním nebo více archivačními časovými razítky.

LEVÝ PANEL SE STATISTIKAMI

Levý panel obsahuje informace o počtu zpráv v jednotlivých tabulkách (viz výše). Dále obsahuje informace o počtu užití jednotlivých časových razítek. Lze vybrat konkrétní časové razítko podle URL adresy jeho služby, „datum od“ a „datum do“. Podle těchto tří parametrů se zobrazí počet užití daného razítka v daném časovém období.

OKNO NASTAVENÍ

V horní liště je tlačítko **Nastavení, které otevírá dialogové okno nastavení.** Obsahuje několik záložek, přičemž poslední tři záložky slouží k nastavení časových razítek.

POPIS OKNA NASTAVENÍ

Pracovní složky: Nastavují se tu cesty ke složkám, ve kterých se očekávají ZFO zprávy. **Zdrojová složka** je povinně nastavitelná. Čtou se z ní všechny ZFO zprávy, které jsou následně při archivaci přesunuty do **cílových složek**, pokud jsou nastaveny. Cílové složky jsou tři a odpovídají tabulkám s přehledem ZFO zpráv. Pokud ZFO zpráva neodpovídá ani jedné cílové složce, zůstává ve složce zdrojové (a zobrazí se v tabulce ZFO zpráv „Ostatní“). Pokud není některá cílová složka nastavena, pak se zpráva nemá kam přesunout a zůstává ve své současné složce.

Vypršení certifikátů: Nastavuje se zde kolik dní před exspirováním certifikátu je certifikát brán jako „brzy exspirovaný“, tj. určuje tu s jakým předstihem se má reagovat na exspiraci certifikátu. **Certifikát podepisovatele** se v současné verzi nebere v úvahu, rozlišuje se pouze stav certifikátu podepisovatele před a po exspiraci. Vypršení **certifikátu časového razítka** určuje, kdy se k podpisu přidá první/další archivační razítko.

Časová razítka, Validační časová razítka a Archivační časová razítka: U každého typu lze nastavit několik konfigurací časových razítek. Jedna konfigurace časového razítka obsahuje parametry nutné pro získání úspěšné odpovědi služby časové autority. Pokud je u jednoho typu časového razítka nastaveno více konfigurací, pak se tyto aplikují postupně za sebou u daného archivačního kroku.

Nastavení proxy - Lze přejmout nastavení proxy z prohlížeče Internet Explorer (defaultně nastaveno), nepoužívat proxy, nebo zadat vlastní přístupové údaje k proxy serveru. Tyto údaje zahrnuje hlavně **URL adresa proxy serveru**. Poté lze nastavit autentizaci k tomuto serveru. Lze se autentizovat jménem a heslem uživatele Windows, nepoužívat autentizaci, nebo zadat vlastní přihlašovací jméno a heslo k proxy serveru.

LICENCE

Pro informace o používané licence a načtení nového licenčního souboru slouží tlačítko ***Licence*** 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 A UDÁLOSTECH

Pro zobrazení logů aplikace slouží tlačítko ***Log*** v horní liště. Funkce slouží k zobrazení informací o chybách a událostech 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.