DITEC
Data Information Technology & Expert Consulting

Požiadavky na prevádzkové prostredie a SSCD

D.Signer/XAdES .NET

Copyright

Popisné charakteristiky dokumentu

Projekt	GOV_ZEP		A3019_002
Dokument	Požiadavky na prevádzkové prostredie a SSCD		
Podnázov	D.Signer/XAdES .NET		
Ref. číslo	GOV_ZEP.17	Verzia	6

Vypracoval	Vittek Róbert	Podpis	Dátum 25.3.2014
Preveril	Priezvisko Meno Preveril	Podpis	Dátum 31.12.2004
Schválil	Priezvisko Meno Schválil	Podpis	Dátum 30.12.2004

Formulár	Dokument		
Ref. číslo	Fo 11	Dátum poslednej aktualizácie	Dátum 13.10.2005

Akceptované dňa : <Dátum akceptácie>

Za <Objednávateľa>: Za <Dodávateľa>.:

<Meno zodpovednej osoby> < Meno zodpovednej osoby >

Projekt	GOV_ZEP		A3019_002
Dokument	Požiadavky na prevádzkové prostredie a SSCD		
Referencia	GOV_ZEP.17	Verzia	6

Záznamy o zmenách

Autor	Popis zmien	Dátum	Verzia

Pripomienkovanie a kontrola

Autor	Stanovisko	Dátum	Verzia

Rozdeľovník

	Priezvisko Meno	Firma, Funkcia
Originál		
Kópia		
Kópia		
Kópia		

Obsah

1. Úvod

Aplikácia D.Signer/XADES .NET predstavuje riešenie pre vytváranie zaručeného elektronického podpisu (ZEP) alebo tzv. obyčajného elektronického podpisu nad množinou rôznych formátov dokumentov, resp. typov dát (XML dokumenty, PDF dokumenty atď.), prípadne nad ľubovoľnou kombináciou podporovaných formátov dát, ktoré spolu vytvárajú tzv. *multipart* dokument. Aplikácia D.Signer/XADES .NET je koncipovaná ako sada knižníc, ktoré je možné integrovať do klientských Win32, .Net alebo webovských aplikácií.

Proces vytvorenia ZEP pomocou aplikácie D.Signer/XADES .NET prebieha v rámci prevádzkového prostredia aplikácie, a teda bezpečnosť tohto procesu je potrebné chápať a posudzovať v širšom kontexte tohto prevádzkového prostredia.

Prevádzkové prostredie aplikácie D.Signer/XADES .NET tvorí:

- hardware osobného počítača používateľa,
- operačný systém (a ďalší nainštalovaný software),
- sieťové pripojenie,
- klientská aplikácia,
- pripojené SSCD zariadenie.

Aplikácia D.Signer/XADES .NET nie je sama schopná podstatne znížiť úroveň rizík vyplývajúcich zo zámerného zneužitia oprávnení alebo z použitia sofistikovaných metód útoku.

Pre tieto dôvody je dôležité zadefinovať bezpečnostné požiadavky na prevádzku aplikácie D.Signer/XADES .NET a na operačné prostredie, v rámci ktorého bude aplikácia nasadená a používaná. Naplnenie týchto technických a procedurálnych požiadaviek tvorí nutný predpoklad korektnej a bezpečnej činnosti aplikácie D.Signer/XADES .NET.

Tieto bezpečnostné technické a procedurálne požiadavky je možné rozdeliť na:

- systémové požiadavky (operačný systém a iný požadovaný software),
- bezpečnostné požiadavky na prevádzkové prostredie,
- požiadavky na použité (podpisové) certifikáty,
- požiadavky na použité SSCD zariadenia,
- personálne požiadavky aplikácie.

2. Systémové požiadavky

Systémové požiadavky aplikácie D.Signer/XADES .NET definujú hardwarové a softwarové nároky aplikácie na inštaláciu aplikácie a na jej operačné prostredie, nezahŕňajú však systémové požiadavky na samotnú klientskú aplikáciu, ani požiadavky na bezpečnostný software, potrebný pre bezpečnú prevádzku aplikácie D.Signer/XADES .NET.

Systémové požiadavky aplikácie D.Signer/XADES .NET sú definované v rámci Používateľskej príručky aplikácie.

3. Bezpečnostné požiadavky

Používateľ (resp. prevádzkovateľ) aplikácie D.Signer/XADES .NET, musí pre bezpečnú prevádzku aplikácie zabezpečiť nasledujúce:

- korektne nainštalovaný a nakonfigurovaný operačný systém s doporučenými aktualizáciami, najmä bezpečnostnými,
- korektne nainštalovanú a nakonfigurovanú klientskú aplikáciu s doporučenými aktualizáciami,
- korektne nainštalovanú a nakonfigurovanú aplikáciu D.Signer/XADES .NET,
- korektne nainštalované a nakonfigurované SSCD zariadenie a jeho obslužný software, pričom zariadenie musí spĺňať bezpečnostné požiadavky na vytvorenie dôveryhodnej cesty pre prenos a spracovanie autentifikačných údajov podpisovateľa, podpisovaných dát a reprezentácie podpisovaných dát medzi aplikáciou D.Signer/XADES .NET a SSCD,
- nezavírené operačné prostredie tak, aby bolo možné vylúčiť hrozby trójskych koní, vírusov a iných druhov škodlivého kódu,
- v prípade klientských aplikácií, ktoré vyžadujú spojenie do Internetu, bezpečné pripojenie do Internetu tak, aby bolo možné vylúčiť hrozby útokov z prostredia Internetu,
- k aplikácii majú prístup len oprávnení používatelia. Autentifikáciu používateľov vykonáva operačný systém a/alebo klientská aplikácia,
- aplikácia D.Signer/XADES .NET nesmie byť prevádzkovaná ako verejná služba operátorom,
- aplikácia D.Signer/XADES .NET nesmie byť prevádzkovaná ako distribuovaná aplikácia (tj. ani autentifikačné údaje podpisovateľa, ani podpisované údaje alebo ich reprezentácia nebudú prenášané cez potenciálne nedôveryhodné komunikačné linky, resp. cez potenciálne nedôveryhodné systémové a aplikačné rozhrania),
- používateľ, resp. prevádzkovateľ aplikácie D.Signer/XADES .NET sa musí presvedčiť, že všetky komponenty (pluginy) aplikácie pre spracovanie jednotlivých formátov dokumentov za účelom vytvorenia ZEP sú certifikované NBÚ.

4. Požiadavky na certifikáty

Aplikácia D.Signer/XADES .NET umožňuje podpisovateľovi výber podpisového certifikátu z množiny jeho osobných certifikátov, ktoré sa nachádzajú v rámci jeho personálneho úložiska certifikátov (MS Personal Certificates Store).

Pre vytvorenie zaručeného elektronického podpisu musí podpisovateľ zvoliť zo svojho personálneho úložiska certifikátov kvalifikovaný certifikát, ktorý bol vydaný akreditovanou certifikačnou autoritou.

Pre vytvorenie obyčajného elektronického podpisu nie je potrebné použiť kvalifikovaný certifikát vydaný akreditovanou certifikačnou autoritou.

5. Požiadavky na SSCD

Pre vytváranie zaručeného elektronického podpisu pomocou aplikácie D.Signer/XADES .NET sa vyžaduje použitie SSCD zariadenia pre generovanie a uloženie privátneho kľúča a pre vytvorenie zaručeného elektronického podpisu, napr. čipová karta, USB token a pod., ktoré musí byť korektne nainštalované podľa požiadaviek výrobcu (dodávateľa). Dané zariadenie musí byť certifikované NBÚ a musí spĺňať požiadavky zákona č. 215/2002 Z.z. o elektronickom podpise a súvisiacich vyhlášok. Pre vytváranie obyčajného elektronického podpisu nie je potrebné použiť certifikované SSCD zariadenie.

Aplikácia D.Signer/XADES .NET je schopná spolupracovať len s takými zariadeniami, pre ktoré výrobca dodáva príslušnú implementáciu MS Cryptographic API – modul CSP (Cryptographic Service Provider). SSCD zariadenie pritom musí podporovať požadovanú podpisovú schému pre elektronický podpis (napr. RSA-SHA-1).

Aplikácia by mala byť primárne používaná s takými SSCD, ktoré sa pripájajú k PC pomocou sériového alebo paralelného rozhrania, USB rozhrania alebo PCMCIA rozhrania. V takomto prípade je možné zabezpečiť dôveryhodnú cestu pre prenos autentifikačných údajov, podpisovaných údajov a ich reprezentácie medzi aplikáciou D.Signer/XADES .NET a SSCD splnením bezpečnostných požiadaviek aplikácie, definovaných v kapitole 3.

V prípade použitia SSCD s rádiovým alebo infra rozhraním musí byť dôveryhodný komunikačný kanál medzi aplikáciou D.Signer/XADES .NET a SSCD zabezpečený splnením bezpečnostných požiadaviek, definovaných výrobcom takéhoto zariadenia. Výrobca takéhoto SSCD musí takisto poskytovať prostriedky pre zamedzenie odpočúvania alebo interferencie.

Keďže aplikácia D.Signer/XADES .NET neobsahuje funkcionalitu pre zadávanie autentifikačných údajov podpisovateľa (SAC komponent), ale spolieha v tomto prípade na dané SSCD zariadenie (resp. na príslušné CSP), ochrana integrity a dôvernosti autentifikačných údajov podpisovateľa, či už sú založené na vedomosti podpisovateľa alebo ide napr. o jeho biometrické údaje, je povinnosťou výrobcu príslušného SSCD zariadenia, prípadne dodávateľa CSP pre dané zariadenie.

Vyžiadanie autentifikácie podpisovateľa pre použitie privátneho kľúča je závislé na nastavení daného SSCD zariadenia a na príslušnom CSP. Aplikácia D.Signer/XADES .NET technicky nevyžaduje, aby príslušný CSP pre dané SSCD zariadenie požadoval opätovnú autentifikáciu používateľa pri každom prístupe k privátnemu kľúču, uloženému na SSCD, ale pre zvýšenie bezpečnosti SSCD a jeho obsahu odporúčame, aby SSCD (prípadne príslušný CSP) boli takto nakonfigurované, ak je to možné. Pri zadávaní PINu pre použitie privátneho kľúča je tiež vhodné, aby autentifikačné údaje (PIN, heslo ap.) neboli zobrazené, ale používateľovi musí byť vhodným symbolom alebo metódou poskytnutá spätná väzba pri stlačení klávesy tak, aby nebolo možné odhaliť zadávané autentifikačné údaje. V prípade biometrickej autentifikácie musia biometrické senzory chrániť

biometrické autentifikačné údaje podpisovateľa pred zneužitím pri "replay" útokoch.

V prípade zadania nesprávnych autentifikačných údajov podpisovateľa musí príslušná funkcia CSP vrátiť chybový kód. Aplikácia D.Signer/XADES .NET chybu spracuje, zobrazí chybovú hlášku a neumožní dokument podpísať. V prípade opakovaného zadania nesprávnych autentifikačných údajov podpisovateľa (hádanie autentifikačných údajov) musí SSCD zariadenie zablokovať ďalšie pokusy. Zároveň musí existovať spôsob, ako znovu odblokovať dané SSCD zariadenie (napr. PUK kód ap.)

Aplikácia D.Signer/XADES .NET takisto neobsahuje funkcionalitu pre manažment autentifikačných údajov. Výrobca (dodávateľ) daného zariadenia musí zabezpečovať túto funkcionalitu v rámci obslužného softwaru, ktorý sa s daným zariadením dodáva.

6. Personálne požiadavky aplikácie

Pre zabezpečenie správnej funkcionality aplikácie D.Signer/XADES .NET je potrebné naplniť takisto personálne požiadavky, súvisiace s:

- inštaláciou aplikácie,
- správou a prevádzkou aplikácie,
- používaním aplikácie.

Aplikáciu musí nainštalovať a spravovať kompetentný používateľ (administrátor) v súlade s požiadavkami a postupmi definovanými v používateľskej príručke. Pre inštaláciu aplikácie je potrebné zabezpečiť, aby používateľ, ktorý inštaluje aplikáciu D.Signer/XADES .NET mal počas inštalácie administrátorské práva.

Pri inštalácii aplikácie D.Signer/XADES .NET je potrebné zabezpečiť, aby k aplikácii mali prístup len oprávnení používatelia. Autentifikáciu oprávnených používateľov pritom vykonáva operačný systém a/alebo klientská aplikácia.

Úspešne autentifikovaní používatelia musia mať dostatočné vedomosti o povahe aplikácie, problematike PKI a elektronického podpisu a musia chápať potrebu bezpečného IT prostredia aplikácie. Používatelia sú povinní dodržiavať postupy a pokyny, uvedené v príručke používateľa, a nesmú vykonávať žiadnu činnosť, ktorá by bola v rozpore s bezpečnostnými požiadavkami aplikácie alebo by narušila bezpečnosť jej prevádzky.