

Deklarácia výrobcu aplikácie pre ZEP

Úvod

Formulár obsahuje základný prehľad vlastností aplikácie pre zaručený elektronický podpis. Formulár vyplní a podpisuje výrobca aplikácie.

Formulár je zverejnený na stránke Národného bezpečnostného úradu ako informácia výrobcu o vlastnostiach aplikácie pre zaručený elektronický podpis, ktorá je certifikovaná Národným bezpečnostným úradom (NBÚ).

Obsah formulára

1 Aplikácia pre zaručený elektronický podpis

Údaje o aplikácii:

Názov aplikácie:	Disig CA Signer
Verzia:	1.1
Hlavný modul aplikácie:	signer
SHA256 digitálny odtlačok:	Ubuntu: dd68faf243e6497b2316850f4ea3d589db7493ba7700935924e42049e243e566 RedHat: 17d95ff0c4913f53e53be65076f6bb515f20b206765af2ffaed23a4bebddeedc

Údaje o výrobcovi:

Obchodné meno:	Disig a.s.
Adresa:	Záhradnícka 151, 821 08 Bratislava 2
Web adresa:	www.disig.sk

2 Typy podpisu podporované aplikáciou – **nevzťahuje sa**

- CMS AdES (CAAdES) - RFC 5126, ETSI 101 733
- XML AdES (XAdES) - ETSI TS 101 903

2.1 Formáty podpisu podporované aplikáciou - **nevzťahuje sa**

- | | |
|--|---|
| <input type="checkbox"/> CAAdES - EPES | <input type="checkbox"/> XAdES - EPES |
| <input type="checkbox"/> CAAdES – EPES-T | <input type="checkbox"/> XAdES – EPES-T |
| <input type="checkbox"/> CAAdES – EPES-C-X | <input type="checkbox"/> XAdES – EPES-C-X |
| <input type="checkbox"/> CAAdES – EPES-A | <input type="checkbox"/> XAdES – EPES-A |
| <input type="checkbox"/> kombinácia horeuvedených formátov | |

EPES	podpis bez časovej pečiatky
EPES-T	podpis s časovou pečiatkou,
EPES-C-X	podpis s úplnou informáciou na overenie platnosti,
EPES-A	podpis archívny,

2.2 Atribúty alebo elementy chránené podpisom podpisovateľa v aplikácii - **nevzťahuje sa**

(s id- na začiatku sa označujú CMS atribúty) - (bez id- na začiatku sú XML elementy):

- | | |
|---|---|
| <input type="checkbox"/> (id-contentType) | <input type="checkbox"/> (DataObjektFormat) |
| <input type="checkbox"/> (id-messageDigest) | |
| <input type="checkbox"/> (id-signingTime) | <input type="checkbox"/> (SigningTime) |
| <input type="checkbox"/> (id-aa-ets-signingCertificateV2) | <input type="checkbox"/> (SigningCertificate) |
| <input type="checkbox"/> (id-aa-signingCertificate) | |
| <input type="checkbox"/> (id-aa-ets-sigPolicyId) | <input type="checkbox"/> (SignaturePolicyIdentifier) |
| <input type="checkbox"/> (id-aa-ets-contentTimestamp) | <input type="checkbox"/> (AllDataObjectsTimeStamp) |
| | <input type="checkbox"/> (IndividualDataObjectsTimeStamp) |
| <input type="checkbox"/> (id-aa-ets-signerLocation) | <input type="checkbox"/> (SignatureProductionPlace) |
| <input type="checkbox"/> (id-aa-ets-signerAttr) | <input type="checkbox"/> (SignerRole) |

2.2 Atribúty alebo elementy podpisu nechránené podpisom podpisovateľa v aplikácii - **nevzťahuje sa**

(s id- na začiatku sa označujú CMS atribúty) - (bez id- na začiatku sú XML elementy):

- | | |
|--|--|
| <input type="checkbox"/> (id-aa-ets-certificateRefs) | <input type="checkbox"/> (CompleteCertificateRefs) |
| <input type="checkbox"/> (id-aa-ets-revocationRefs) | <input type="checkbox"/> (CompleteRevocationRefs) |
| <input type="checkbox"/> (id-aa-signatureTimeStampToken) | <input type="checkbox"/> (SignatureTimeStamp) |
| <input type="checkbox"/> (id-aa-ets-escTimeStamp) | <input type="checkbox"/> (SigAndRefsTimeStamp) |
| <input type="checkbox"/> (id-aa-ets-certCRLTimestamp) | <input type="checkbox"/> (RefsOnlyTimeStamp) |
| <input type="checkbox"/> (id-aa-ets-archiveTimestamp) | <input type="checkbox"/> (ArchiveTimeStamp) |

Deklarácia výrobcu aplikácie pre ZEP

((id-aa-ets-certValues)

(CertificatesValues)

(id-aa-ets-revocationValues)

(RevocationValues)

3 Užívateľské rozhranie

- 3.1 Je užívateľské rozhranie aplikácie chránené proti zmene nastavení zobrazenia v systéme (farba, veľkosť okien a fontov, transparentnosť, názvy a veľkosť tlačidiel)?
 Áno Nie **nevzťahuje sa**
- 3.2 Aplikácia musí byť použitá len v bezpečnom prostredí, ktoré je plne pod kontrolou používateľa, nie je chránená proti útokom na operačný systém (zmena fontu, odchytenie PIN, podhodenie falošnej hodnoty pre SSCD na podpis alebo vytvorenie viacerých podpisov).
 Áno Nie
- 3.3 Zmena systémových fontov môže spôsobiť odlišné zobrazenie podpísaného obsahu pri podpisovaní na rôznych počítačoch a odlišné zobrazenie pri overovaní podpisu na rôznych počítačoch.
 Áno Nie **nevzťahuje sa**
- 3.4 Aplikácia komunikuje s bezpečným zariadením pre vytváranie podpisu cez bezpečný kanál, ktorý zabráni modifikácii a zmene údajov určených na podpis.
 Áno Nie
- 3.5 Aplikácia podporuje zadávanie PIN bezpečného zariadenia pre vytváranie podpisu cez klávesnicu na čítacom zariadení, ktoré zabráni odchyteniu PIN hodnoty.
 Áno Nie
- 3.6 Aplikácia upozorní na nebezpečenstvo zadávania PIN na klávesnici, ak nie je použité bezpečné zadávanie PIN hodnoty (3.5).
 Áno Nie
- 3.7 Aplikácia obsahuje úložisko dôveryhodných certifikátov.
 Áno Nie
- 3.8 Úložisko dôveryhodných certifikátov je chránené proti neautorizovanej zmene
 Áno Nie **nevzťahuje sa**

Ak áno-Úložisko dôveryhodných certifikátov je chránené:

- Podpisom overovateľa Podpisom autority (Admin) Podpisom TSL listu explicitnej autority
 Inak:

- 3.9 Aplikácia je chránená proti zmene svojho kódu:

Áno Nie

Ak áno- Spôsob ochrany proti zmene kódu je :

- Hash z komponent je podpísany a kontroluje sa pri štarte aplikácie.
 Je ho možné prekontrolovať aj externou aplikáciou.

Zverejnený je zoznam hash hodnôt komponent pre externé overenie externou aplikáciou.

Inak:

4. Overovanie platnosti certifikátu a vytvorenie a overenie podpisu

4.1 Pred podpísaním je umožnené zobrazit' certifikát podpisovateľa

Áno Nie

4.2 Pred podpísaním je overená platnosť certifikátu podpisovateľa

Áno Nie

Ak áno - informatívne overenie je pomocou CRL alebo OCSP.

Systémového času.

4.7 Overovanie platnosti certifikátu je zabezpečené pomocou:

CRL OCSP Nepriame CRL... Nepriame OCSP OCSP s pozitívnou odpoveďou - certHash:

Prevádzkovateľ zabezpečuje zastavenie aplikácie pri zrušení certifikátu.

4.8 . Aplikácia má pri overovaní certifikačnej cesty¹ implementovaný nasledovný postup:
nevzťahuje sa

1.Na základe explicitného zoznamu OID certifikačných politík vyžaduje ich prítomnosť vo všetkých certifikátoch certifikačnej cesty².

Áno Nie

2.Ak je v certifikáte cez policyConstraints vyžadované overovanie certifikačných politík cez policyMapping, aplikácia overuje certifikačné politiky na základe policyConstraints, certificatePolicy a policyMapping. Áno Nie

4.9 Aplikácia identifikuje kvalifikované certifikáty na základe rozšírenia QCStatement.

Áno Nie **nevzťahuje sa**

4.3 Do položiek chránených podpisom podpisovateľa je možné vloženie odkazu na podpisovú politiku

Áno Nie **nevzťahuje sa**

Ak áno, pravidlá z podpisovej politiky sú použité pri vytvorení podpisu: Áno Nie

4.4 Aplikácia umožňuje zobrazenie obsahu podpisovej politiky v čitateľnej podobe

Áno Nie **nevzťahuje sa**

4.5 Overovanie podpisu je realizované na základe podpisovej politiky, ktorej identifikátor je súčasťou podpisu (chránený podpisom podpisovateľa).

Áno Nie **nevzťahuje sa**

4.6 Overovanie podpisu je realizované na základe podpisovej politiky, ktorú si vyberie overovateľ, ak nie je identifikátor podpisovej politiky súčasťou podpisu.

Áno Nie **nevzťahuje sa**

4.10 Aplikácia umožňuje pri vytváraní podpisu vloženie časovej pečiatky.

Áno Nie **nevzťahuje sa**

4.11 Aplikácia umožňuje pri overovaní podpisu vloženie časovej pečiatky.

Áno Nie **nevzťahuje sa**

4.12 Aplikácia overuje vloženú časovú pečiatku pri overovaní podpisu.

Áno Nie **nevzťahuje sa**

4.13 Aplikácia pred vložením archívnej časovej pečiatky dopĺňa podpis na archívny (s aktuálnymi CRL, OCSP) pri overovaní podpisu.

¹ Odkaz na štandardizačný dokument ITU-T X.509, ISO, RFC + dokument Kontrola certifikačnej cesty

² NBÚ podpisová politika pre ZEP vyžaduje OID certifikačnej politiky QCP-SK (1 3 158 36061701 0 0 0 1 2 2)

Deklarácia výrobcu aplikácie pre ZEP

Áno Nie **nevzťahuje sa**

4.14 .Aplikácia overuje archívnu časovú pečiatku(s aktuálnymi CRL, OCSP) pri overovaní archívneho podpisu. Áno Nie **nevzťahuje sa**

5 Bezpečný prehliadač

- 5.1 Aplikácia pri podpísaní a overení dokumentu zabezpečuje pomocou údajov chránených podpisom podpisovateľa jednoznačné určenie formátu podpísaného dokumentu.

Áno Nie **nevzťahuje sa**

Ochrana formátu podpísaného dokumentu je pomocou:

MIME content-type v MIME hlavičke MIME MIMEType v DataObjectFormat

Iné:

- 5.2 Aplikácia podpisuje/overuje a zobrazuje formáty dokumentov vymenované vo vyhláške NBÚ č. 136/2009 Z. z. v bezpečnom prehliadači vo všetkých verziách aplikácie rovnako:

Áno Nie **nevzťahuje sa**

Ak nie – Aké iné formáty elektronických dokumentov podpisuje a zobrazuje:

- 5.3 Pri podpísaní/overení a zobrazení iného formátu dokumentu, než je uvedený vo vyhláške NBÚ č. 136/2009 Z. Z, sa zobrazí upozornenie:

Áno Nie **nevzťahuje sa**

- 5.4 Aplikácia v bezpečnom prehliadači zobrazuje nasledovné formáty³: **nevzťahuje sa**

ASCII v niektorom z kódovaní znakov podľa ISO.

Na jednoznačnú identifikáciu je použitý MIME typ (text/plain; charset=UTF-8) v podpísovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

³ Formáty sú definované v prílohe č.2 Vyhlášky NBÚ č. 136/2009 Z.z. o spôsobe a postupe používania elektronického podpisu v obchodnom a administratívnom styku s odkazmi na zahraničné normy.

Microsoft/Apple Rich Text Format (RTF) Verzia 1.5.

Na jednoznačnú identifikáciu je použitý MIME typ (text/rtf) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Adobe Portable Document Format (PDF) Verzia 1.3.

Na jednoznačnú identifikáciu je použitý MIME typ (application/pdf) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Adobe Portable Document Format (PDF) Verzia 1.4.

Na jednoznačnú identifikáciu je použitý MIME typ (application/pdf) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

HTML 4.01.

Na jednoznačnú identifikáciu je použitý MIME typ (text/html; charset=UTF-8) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Deklarácia výrobcu aplikácie pre ZEP

XML 1.0.

Na jednoznačnú identifikáciu je použitý MIME typ (text/xml; charset=UTF-8) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

XHTML 1.0.

Na jednoznačnú identifikáciu je použitý MIME typ (application/xhtml+xml; charset=UTF-8) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

XHTML 1.1

Na jednoznačnú identifikáciu je použitý MIME typ (application/xhtml+xml; charset=UTF-8) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Open Office.org XML File Format

Na jednoznačnú identifikáciu je použitý MIME typ (application/xml) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Deklarácia výrobcu aplikácie pre ZEP

Secure Hyper Text Transfer Protocol

Na jednoznačnú identifikáciu je použitý MIME typ (message/rfc822) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

S/MIME Verzia 3

Na jednoznačnú identifikáciu je použitý MIME typ (message/rfc822) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Security Services for S/MIME

Na jednoznačnú identifikáciu je použitý MIME typ (message/rfc822) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Tag Image File Format for image technology (TIFF)

Na jednoznačnú identifikáciu je použitý MIME typ (image/tiff) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Deklarácia výrobcu aplikácie pre ZEP

Portable Network Graphics (PNG)

Na jednoznačnú identifikáciu je použitý MIME typ (image/png) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

PDF/A-1

Na jednoznačnú identifikáciu je použitý MIME typ (application/pdf) v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

Open Document Format for Office Applications (OpenDocument) v.1.0 (ODF)

Na jednoznačnú identifikáciu je použitý MIME typ v podpisovaných údajoch. Áno Nie

Bezpečné zobrazenie je len s nasledovnými nastaveniami (znaková sada, font, veľkosť písma, zväčšenie, ...) alebo ďalšími obmedzeniami prehliadača pre bezpečné a jednotné zobrazenie:

6 Dopĺňujúce informácie

6.1 Aplikácia môže byť použitá len pri splnení nasledovných obmedzení:

Požiadavka [1] - Organizačne zabezpečiť ochranu prístupu k pracovisku aplikácie proti neautorizovanému prístupu, inštaláciám alebo iným útokom.

Požiadavka [2] - Hardvér, na ktorom bude systém nasadený, musí byť umiestnený v prostredí chránenom proti vplyvom prírodných katastrof (požiar, povodeň) a toto prostredie musí byť vhodné pre bezproblémový chod hardvéru (stála teplota, vlhkosť a pod.).

Požiadavka [3] - Na operačnom systéme, na ktorom je inštalovaná aplikácia, musia byť spustené iba služby nevyhnutné na poskytovanie certifikačných služieb.

Požiadavka [4] - Na operačnom systéme, na ktorom bude aplikácia spustená, je nainštalovaná a spravovaná aplikácia prostredníctvom kompetentného administrátora so stanovenými administrátorskými právami.

Požiadavka [5] - Hardware, na ktorom bude aplikácia nasadená musí mať korektné nainštalovaný operačný systém s odporúčanými aktualizáciami, najmä bezpečnostnými.

Požiadavka [6] - V prípade inštalačných a záložných médií musí byť zabezpečená ich integrita a dostupnosť v požadovanom čase. Z inštalačných médií sa vytvárajú ešte u výrobcu HASH-e, ktoré sa pri inštalácii musia kontrolovať.

Požiadavka [7] - Operačný systém hardvéru určeného na poskytovanie certifikačných služieb prostredníctvom aplikácie musí mať k dispozícii primeranú diskovú kapacitu pre potreby zaistenia bezpečnej prevádzky operačného systému vrátane spravovania auditných záznamov.

Požiadavka [8] - Na operačnom systéme hardvéru slúžiaceho na zhromažďovanie a správu auditných záznamov musia byť nastavené prístupové práva na ich čítanie a manipuláciu iba pre autorizované role (Systémový operátor, Systémový Audítor).

Požiadavka [9] - Pre potreby uchovávania auditných záznamov musí byť k dispozícii bezpečné úložisko (napr. trezor), aby sa zabránilo neautorizovanému prístupu k auditným záznamom v čase ich úschovy.

Požiadavka [10] - Auditné záznamy musia byť uchovávané na neprepisovateľných médiách, aby sa zabezpečila ochrana ich integrity.

Požiadavka [11] - Pre potreby zaznamenávania auditných záznamov musí mať aplikácia k dispozícii dôveryhodný zdroj presného času.

Požiadavka [12] - Pre potreby overovania identity žiadateľa o QC, a činností súvisiacich s vydávaním/rušením QC, musí existovať príslušná registračná autorita – pracovník registračnej autority, ktorý ma pridelený vlastný kľúčový pár, ktorým podpisuje žiadosti o vydanie/zrušenie QC.

Požiadavka [13] - Pre potreby zabezpečenia ochrany osobných údajov, musí byť spracovaný bezpečnostný projekt na ochranu osobných údajov v rozsahu požadovanom platnou legislatívou SR.

Požiadavka [14] - Korektne nainštalovať aplikáciu a používať ju s certifikovaným HSM a jeho obslužným softvérom.

Požiadavka [15] - Privátny kľúč certifikačnej autority môže byť použitý iba výhradne na podpisovanie QC, prípadne podpisovanie CRL a nesmie slúžiť na žiadne iné účely.

Požiadavka [16] - Pre prípad výskytu havárie alebo inej vážnej mimoriadnej udalosti, musí byť k dispozícii dokumentácia, popisujúca havarijné plánovanie.

Požiadavka [17] - Zabezpečiť nezavírené operačné prostredie pre vylúčenie hrozby trójskych koňov, vírusov a iných druhov škodlivého kódu.

Požiadavka [18] - V prípade spojenia do internetu, zabezpečiť bezpečné pripojenie do internetu tak, aby bolo možné vylúčiť hrozby útokov z tejto siete.

Požiadavka [19] - K aplikácii môžu pristupovať len používatelia, ktorí majú zadané roly, v zmysle dokumentu CA Signer Security Target, pričom autentifikáciu vykonáva vstavaná funkcionálna zvoleného operačného systému. Úspešne autentifikovaní používatelia nesmú vykonávať žiadnu činnosť, ktorá by bola v rozpore s bezpečnostnými požiadavkami aplikácie alebo by mohla narušiť bezpečnosť jej prevádzky.

6.2 Podporované certifikované bezpečné zariadenia pre vytváranie podpisu:

Všetky HSM moduly od Thales/nCipher Corporation Ltd. certifikované Národným bezpečnostným úradom.