

## 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 (NBU).

### Obsah formulára

#### 1 Aplikácia pre zaručený elektronický podpis

##### Údaje o aplikácii:

Názov aplikácie:

**ICASignZEP**

Verzia:

**3.0.0**

Hlavný modul aplikácie:

**ICASignZEP.dll**

SHA256 digitálny odtlačok:

**585E5997E5A6BC9FA6283D872BFBC7EAC43ECCF3C6BC2  
5ECD4CF98367EEFBFF1**

##### Údaje o výrobcovi:

Obchodné meno:

**První certifikační autorita, a.s.**

Adresa:

**Praha 9, Libeň, Podvinný mlýn 2178/6, PSČ: 19000**

Web adresa:

**<http://www.ica.cz>**

## Deklarácia výrobcu aplikácie pre ZEP

### 2 Typy podpisu podporované aplikáciou

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

#### 2.1 Formáty podpisu podporované aplikáciou

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> CAAdES - EPES           | <input type="checkbox"/> XAdES - EPES     |
| <input checked="" 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 hore uvedených formátov |   |

EPES                podpis bez časovej pečiatky  
EPES-T            podpis s časovej 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

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

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> (id-contentType)                 | <input type="checkbox"/> (DataObjektFormat)               |
| <input checked="" type="checkbox"/> (id-messageDigest)               |   |
| <input checked="" type="checkbox"/> (id-signingTime)                 | <input type="checkbox"/> (SigningTime)                    |
| <input checked="" type="checkbox"/> (id-aa-ets-signingCertificateV2) | <input type="checkbox"/> (SigningCertificate)             |
| <input checked="" type="checkbox"/> (id-aa-signingCertificate)       |   |
| <input checked="" 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

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

- |   |  |
|---|--|
| (id-aa-ets-certificateRefs)   | <input type="checkbox"/> (CompleteCertificateRefs) |
| <input type="checkbox"/> (id-aa-ets-revocationRefs)                 | <input type="checkbox"/> (CompleteRevocationRefs)  |
| <input checked="" 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)        |
| <input type="checkbox"/> ((id-aa-ets-certValues)                    | <input type="checkbox"/> (CertificatesValues)      |
| <input type="checkbox"/> (id-aa-ets-revocationValues)               | <input type="checkbox"/> (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
- 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 podpisovaného obsahu pri podpisovaní na rôznych počítačoch a odlišné zobrazenie pri overovaní podpisu na rôznych počítačoch.  
 Áno       Nie
- 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

Ak áno-Úložisko dôveryhodných certifikátov je chránené:

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

- 3.9 Aplikácia je chránená proti zmene svojho kódu:

Áno       Nie

Ak áno- Spôsob ochrany proti zmene kódu je :

- Hash z komponent je podpísaný 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 <sup>\*)</sup>.

\* v závislosti na použitých prostriedkoch

4.7 Overovanie platnosti certifikátu je zabezpečené pomocou:

CRL  OCSP <sup>\*)</sup>  Nepriame CRL...  Nepriame OCSP  OCSP s pozitívnou odpoveďou - certHash:

\* v závislosti na použitých prostriedkoch

4.8 Aplikácia má pri overovaní certifikačnej cesty<sup>1</sup> implementovaný nasledovný postup:

1. Na základe explicitného zoznamu OID certifikačných politík vyžaduje ich prítomnosť vo všetkých certifikátoch certifikačnej cesty<sup>2</sup>.

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

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

Áno  Nie

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

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

Áno  Nie

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

Áno  Nie

4.10 Aplikácia umožňuje pri vytváraní podpisu vloženie časovej pečiatky.

Áno  Nie

4.11 Aplikácia umožňuje pri overovaní podpisu vloženie časovej pečiatky.

Áno  Nie

4.12 Aplikácia overuje vloženú časovú pečiatku pri overovaní podpisu.

Áno  Nie

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

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

<sup>2</sup> 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

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

## 5 Bezpečný prehliadač

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

Áno       Nie

Ochrana formátu podpisovaného 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 vyhláske NBÚ č. 136/2009 Z. z. v bezpečnom prehliadači vo všetkých verziách aplikácie rovnako:

Áno       Nie

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

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

Áno       Nie

- 5.4 Aplikácia v bezpečnom prehliadači zobrazuje nasledovné formáty<sup>3</sup>:

**ASCII v niektorom z kódovaní znakov podľa ISO.**

Na jednoznačnú identifikáciu je použitý MIME typ (text/plain; 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:

S instalovaným certifikovaným pluginom ICATXTPluginZEP (který není součástí aplikace).

<sup>3</sup> 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.

## Deklarácia výrobcu aplikácie pre ZEP

### 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:

S instalovaným certifikovaným pluginom ICARTFPluginZEP (který není součástí aplikace).

Poznámka:

Při zpracování formátu DOC/DOCX instalovaným certifikovaným pluginem ICAOfficePluginZEP (který není součástí aplikace) se provede nejprve konverze z DOC/DOCX na RTF, a dále zobrazení a podpis RTF formátu.

### 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

## Deklarácia výrobcu aplikácie pre ZEP

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

### **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

## Deklarácia výrobcu aplikácie pre ZEP

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

### 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 Doplňujúce informácie

### 6.1 Aplikácia môže byť použitá len pri splnení nasledovných obmedzení:

Není povolen provoz aplikace ve veřejném nekontrolovaném prostředí jako např. internetové kiosky a kavárny. Aplikace je určena pro provoz na PC s jistou úrovní kontroly fyzického přístupu - PC v podnikovém prostředí nebo osobní PC. Aplikace je určena pro provoz v operačním systému Windows XP SP3 a vyšší. Další požadavky výrobce na prostředí jsou uvedeny v dokumentu "ICASignZEP - Referenční manuál aplikace".

Aplikaci lze použít jen při dodržení bezpečnostních požadavků ve smyslu podle platné legislativy SR a požadavků výrobce uvedených v dokumentu "ICASignZEP - Referenční manuál aplikace".

Výrobce nadřazené aplikace musí zajistit, že volání API rozhraní aplikace jsou v souladu s dokumentem "ICASignZEP - Referenční manuál aplikace" a zároveň jsou použita tak, aby nedošlo nesprávnou kombinací vstupních parametrů k vytvoření neplatného ZEP podpisu.

Aplikaci lze použít pouze se zásuvnými moduly pro jednotlivé typy dat, dodanými výrobcem aplikace a certifikovanými Národným bezpečnostným úradom SR.

### 6.2 Podporované certifikované bezpečné zariadenia pre vytváranie podpisu:

Aplikace je schopna spolupracovat se všemi certifikovanými bezpečnými zařízeními pro vytváření podpisu (SSCD), se kterými je dodáván modul CSP umožňující přístup k jejich funkcím prostřednictvím Microsoft CryptoAPI.

Na OS Windows XP musí výpočet SHA-2 otisku důvěryhodným (certifikovaným) kryptografickým modulem zajistit CSP dodávané spolu s NBÚ SR certifikovaným SSCD.

Konkrétní povolená SSCD jsou určována prostřednictvím konfiguračního souboru řízeného výrobcem, který je aplikaci předáván jako vstupní parametr.

Poznámky:

Výrobce ICASignZEP dodává SSCD s CSP používajícím pro výpočet SHA-2 otisku modul "*Enhanced RSA and AES Cryptographic Provider (Prototype)*" fy Microsoft obsažený ve Windows XP od SP3 a certifikovaný dle FIPS 140-2.

Testovací aplikace, která ICASignZEP předanou k certifikaci využívá, povoluje použití pouze čipové karty I.CA STARCOS SPK 3.0.