

## 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:

**QSign eSigner**

Verzia:

**1.0**

Hlavný modul aplikácie:

**ArdacoSignApplet.jar**

SHA256 digitálny odtlačok:

**E2EB1740D61FA11986F7A18BE04B38510A88F44662  
EEC27CE10BCC5972F0C8F2**

##### Údaje o výrobcovi:

Obchodné meno:

**Ardaco, a.s.**

Adresa:

**Polianky 5, 841 01 Bratislava**

Web adresa:

**<http://www.ardaco.com>**

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

- |  |  |
|--|--|
| <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)        |
| <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 autority (Admin)       Podpisom TSL listu explicitnej autority  
 Inak:

ako

- 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:

V používateľskej príručke sú definované bezpečnostné požiadavky na prevádzku aplikácie, ktorých cieľom je zabezpečenie ochrany integrity kódu aplikácie.

Aplikácia je podpísaná certifikátom výrobcu, pričom platnosť podpisu sa overuje

Deklarácia výrobcu aplikácie pre ZEP

prostriedkami operačného systému.

#### 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.
- 4.7 Overovanie platnosti certifikátu je zabezpečené pomocou:  
 CRL  OCSP  Nepriame CRL...  Nepriame OCSP  OCSP s pozitívnou odpoveďou - certHash:
- 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 vložení 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.  
 Áno  Nie
- 4.14 .Aplikácia overuje archívnu časovú pečiatku(s aktuálnymi CRL, OCSP) pri overovaní archívneho podpisu.  Áno  Nie

<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)

## 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:

aké
-----

- 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:

--

<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:

### 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:

Bezpečné zobrazenie je možné so štandardnými nastaveniami systému.

### 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:

Deklarácia výrobcu aplikácie pre ZEP

## 6 Doplňujúce informácie

6.1 Aplikácia môže byť použitá len pri splnení nasledovných obmedzení:

6.2 Podporované certifikované bezpečné zariadenia pre vytváranie podpisu:

Cryptoflex 32K e-Gate Smart Card by SchlumbergerSema  
Čipová karta STARCOS SPK 2.3  
Safenet iKey 2032 FIPS Hardware versions (A and 909-23002) and 909-25001 Firmware version 0.6  
Čipová karta STARCOS SPK 3.0  
Siemens CardOS Smartcard 32KB/64KB, verzia CardOS V4.3B - PKCS#15 SecAuth  
Siemens HiPath Scurity Smart Card 32KB, verzia SLE66CX322P, CardOS 4.3B  
Siemens HiPath Scurity Smart Card 64KB, verzia SLE66CX642P, CardOS 4.3B  
Čipová karta CryptoPlus XG ZEP/EP Profiles verzia CryptoPlus XG v1.14

Vo všeobecnosti ľubovoľné SSCD zariadenie s PKCS#11 rozhraním.