PRAVIDLÁ

poskytovania služby QES portal

Disig, a.s.
poskytovateľ služby

Vypracoval	**Ing. Jozef Cesnek**
Dátum platnosti	**10.6.2019**
Verzia	**1.0**
Typ	**PRAVIDLÁ**
Schválil	**Ing. Peter Miškovič**

Obsah

1. Úvod

Tento dokument definuje pravidlá (ďalej len „CPS“) poskytovania dôveryhodnej služby QES portál (ďalej len „QES portal“). Poskytovateľom tejto služby je spoločnosť Disig, a.s., so sídlom Záhradnícka 151, 821 08 Bratislava, IČO: 35975946, zapísaná v Obchodnom registri OS BA I, odd. Sa, vložka č. 3794/B (ďalej len „Poskytovateľ“), prostredníctvom svojho systému validačnej služby.

Tento dokument môže byť použitý tretími stranami na posúdenie, či poskytovaná služba QES portal je v súlade s ich požiadavkami a Všeobecnými podmienkami poskytovania a používania služby QES Portal.

1.1 Prehľad

Tieto CPS vychádzajú s požiadaviek štandardu ETSI TS 119 431-2 [1].

1.2 Názov dokumentu a jeho identifikácia

Názov:	**Pravidlá poskytovania služby QES portal**
Skratka názvu:	**CPS QES portal***
Verzia:	**1.0**
Schválené dňa:	**5.6.2019**
Platnosť od:	**10.6.2019**
Týmto CPS je priradený identifikátor objektu (OID):	**1.3.158.35975946.0.1.0.0.4**

* - v texte tohto dokumentu sa väčšinou používa pri odkaze len skrátená forma CPS QES

Popis použitého identifikátora objektu (OID):

1 – ISO assigned OIDs

1.**3** – ISO Identified Organization

1.3.**158** – Identifikačné číslo subjektu (IČO)

1.3.158.**35975946** – Disig

1.3.158.35975946.0.**1** – Dôveryhodné služby

1.3.158.35975946.0.1.0.0.2 – CPS QES portal

1.3 Účastníci Služby QES portal

V rámci poskytovania dôveryhodných služieb podpisovania a validácie sú účastníkmi PKI infraštruktúry entity uvedené v tejto časti.

1.3.1 Jednotka poskytujúca službu QES portal

Jednotka poskytujúcej služby QES portal :

- je entita, ktorá poskytuje dôveryhodné služby podpisovania a validácie elektronických podpisov a pečatí používateľom (Zákazníci, Spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie dôveryhodných služieb špecifikovaných v odstavci 1.1,

1.3.2 Zákazník

Zákazníkom sa rozumie fyzická osoba resp. právnická osoba, ktorej Poskytovateľ poskytuje službu a ten, na koho sa viažu záväzky odberateľa.

Podmienky, ktoré musí splniť Zákazník, definuje Všeobecné podmienky služby QES portal a tieto CPS (ďalej aj „VPaP QES portal“).

Ak je Zákazníkom právnická osoba, táto môže zahŕňať niekoľko koncových používateľov alebo jediného koncového používateľa. Niektoré povinnosti, ktoré sa vzťahujú na túto právnickú osobu, sa zároveň vzťahujú aj na týchto koncových používateľov. V každom prípade právnická osoba je plne zodpovedná ak povinnosti dané VPaP QES portal nie sú zo strany koncových používateľov správne splnené, a preto je takáto organizácia zodpovedná za vhodnú informovanosť svojich koncových používateľov.

Keď je Zákazník zároveň koncovým používateľom, tak je priamo zodpovedný, ak neplní svoje povinnosti v zmysle VPaP QES portal.

1.4 Správa pravidiel

1.4.1 Organizácia zodpovedná za správu dokumentu

Tabuľka č. 1 obsahuje údaje Poskytovateľa, ktorý je zodpovedný za prípravu, vytvorenie a udržiavanie tohto dokumentu.

Tabuľka č. 1: Kontaktné údaje Disig

Poskytovateľ	
spoločnosť:	**Disig, a.s.**
adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
IČO:	**359 75 946**
telefón	**+421 2 20850140**
e-mail:	**disig@disig.sk**
webové sídlo:	**http://www.disig.sk**

1.4.2 Kontaktná osoba

Na účel tvorby politík a pravidiel má Poskytovateľ vytvorenú autoritu pre správu politík (PMA) (pozri bod **Error! Reference source not found.**), ktorá plne zodpovedá za ich obsah, a ktorá je pripravená odpovedať na všetky otázky týkajúce sa politík a pravidiel Poskytovateľa.

Tabuľka č. 2 obsahuje kontaktné údaje na zložku zodpovednú za prevádzku služby

Tabuľka č. 2: Kontaktné údaje služby

Poskytovateľ	
adresa:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**spravaqes@disig.sk;**
telefón	**+421 2 20850140**
fax:	**+421 2 20850141**
webové sídlo:	**http://eidas.disig.sk**

1.5 Skratky a definície

1.5.1 Skratky a definície

CA — Certifikačná autorita, autorita vyhotovujúca certifikáty verejného kľúča (Certification Authority)

TSP — Poskytovateľ dôveryhodnej služby (Trust Service Provider (TSP)): entita, ktorá poskytuje jednu alebo viac dôveryhodných služieb

IT — Informačná technológia (Information Technology)

NBÚ — Národný bezpečnostný úrad

TSA	—	Autorita časovej pečiatky, vydavateľ časovej pečiatky (Time-Stamping Authority)
QSCD	—	Kvalifikované zariadenie na vyhotovovanie elektronického podpisu/pečate (Qualified electronic Signature/Seal Creation Device)
UTC	—	Univerzálny koordinovaný čas (Coordinated Universal Time (UTC)): časová škála založená na sekunde podľa definície v Recommendation ITU-R TF.460-6, „svetový čas“
VSU		Jednotka služby validácie (Validation Service Unit (VSU)): sústava technických a programových prostriedkov, ktorá je spravovaná ako jednotka a má v danom čase aktívny jeden kľúč na vytváranie správ z validácie

2. Úložiská

Úložiská musia byť umiestnené tak, aby boli prístupné Zákazníkom a v súlade s celkovými bezpečnostnými požiadavkami.

Funkciu úložiska Poskytovateľa bude zastávať jeho webové sídlo. Presná URL adresa je uvedené v kapitole 1 Webové sídlo Poskytovateľa je prostredníctvom internetu verejne prístupné Zákazníkom.

Verejne dostupné informácie uvedené na webovom sídle Poskytovateľa majú charakter riadeného prístupu.

2.1 Zverejňovanie informácií o službe

Poskytovateľ musí zverejňovať, v on-line režime, úložisko, ktoré je prístupné Zákazníkom, ktoré bude obsahovať minimálne tieto informácie:

- aktuálne stavy všetkých Európskych TSL,
- certifikáty jednotlivých VSU Poskytovateľa, ktoré patria k jej verejným kľúčom, ktorých zodpovedajúci súkromný kľúč je využívaný pri podpisovaní správ z validácie.

Poskytovateľ musí zverejňovať v on-line režime prostredníctvom svojho webového sídla tieto CPS ako aj ďalšie dokumenty súvisiace s poskytovaním dôveryhodných služieb.

2.2 Kontroly prístupu

Poskytovateľ musí chrániť ľubovoľnú informáciu uloženú v úložisku, ktorá nie je určená na verejné rozšírenie. Poskytovateľ musí vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát vyplývajúcich s poskytovaných dôveryhodných služieb. Taktiež musí vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje uložené v úložisku.

3. Technické parametre a obmedzenia služby QES portal

Služba QES portal pracuje v dvoch nezávislých módoch:

1. **eIDAS QES - v zmysle** [európskeho Nariadenia eIDAS](), vytvára podpisy použiteľné v členských krajinách EÚ a overuje podpisy vytvorené v členských krajinách EÚ

2. **SK ZEP - v zmysle** [Zákona o elektronickom podpise 215/2002 Z.z.](), platného do 1.7.2016, vytvára podpisy použiteľné informačnými systémami v Slovenskej republike a overuje podpisy vytvorené informačnými systémami v Slovenskej republike

Požadovaný mód si volí Zákazník pri výbere dokumentu na podpísanie alebo overenie. V oboch módoch práce sú využívané aj viaceré doplnkové technológie ako napríklad služba elektronickej časovej pečiatky, vďaka ktorej obsahuje každý podpísaný dokument dôveryhodné potvrdenie o svojej existencii v čase vytvorenia podpisu.

3.1 Technické parametre pre mód eIDAS QES

3.1.1 Zdroj informácií o dôveryhodnosti

Trusted list (TSL) publikovaný Európskou Komisiou (aktuálny stav)

3.1.2 Podporované formáty nepodpísaných dokumentov

- Dokumenty typu PDF, DOC, DOCX, ODT, TXT, XML (čisté XML, XMLDataContainer) a RTF
- Obrázky typu PNG, GIF, TIFF, BMP a JPG

3.1.3 Podporované formáty podpísaných dokumentov/kontajnerov

- PDF – dokument podľa špecifikácie PDF ISO-32000 [2], ktorý je zároveň aj kontajnerom,
- ASICS – ASiC kontajner podľa ETSI TS 103174 [3],
- ASICE – ASiC kontajner podľa ETSI TS 103174 [3],
- SCS – ASiC kontajner podľa ETSI TS 103174 [3],
- SCE – ASiC kontajner podľa ETSI TS 103174 [3],
- ZIP – ASiC kontajner podľa ETSI TS 103174 [3],

Služba predpokladá, že sa jedná o kontajnery podľa ich špecifikácií.

3.1.4 Podporované formáty elektronických podpisov

- CAdES (CMS Advanced Electronic Signatures) vo formátoch

- CAdES-B-B, CAdES-B-T, CAdES-B-LT a CAdES-B-LTA podľa štandardu ETSI TS 103 173
- XAdES (XML Advanced Electronic Signatures) vo formátoch
  - XAdES-B-B, XAdES-B-T, XAdES-B-LT a XAdES-B-LTA podľa štandardu ETSI TS 103 171
- PAdES (PDF Advanced Electronic Signatures) vo formátoch
  - PAdES-B-B, PAdES-B-T, PAdES-B-LT a PAdES-B-LTA podľa štandardu ETSI TS 103 172

3.1.5 Podporované podpisové certifikáty

- kvalifikované certifikáty pre elektronický podpis vydané kvalifikovaným poskytovateľom dôveryhodných služieb registrovaným v dôveryhodnom zozname publikovanom Európskou Komisiou
- kvalifikované certifikáty pre elektronickú pečať vydané kvalifikovaným poskytovateľom dôveryhodných služieb registrovaným v dôveryhodnom zozname publikovanom Európskou Komisiou

3.1.6 Podporované rozhrania pre prácu s QSCD zariadeniami

- PKCS #11: Cryptographic Token Interface Standard
- Microsoft Crypto API / Cryptographic Service Provider

3.1.7 Podporované kryptografické algoritmy

3.1.7.1. Hash algoritmy

Služba QES portal podporuje nasledovné hash algoritmy:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého QSCD zariadenia a klientskej podpisovej aplikácie.

3.1.7.2. Podpisové algoritmy

Aplikácia poskytovania služby QES portal podporuje nasledovné podpisové algoritmy:

- MD5withRSA
- SHA-1withRSA
- SHA-224withRSA
- SHA-256withRSA
- SHA-384withRSA
- SHA-512withRSA

Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého SSCD zariadenia a klientskej podpisovej aplikácie.

3.2 Technické parametre pre mód SK ZEP

3.2.1 Zdroj informácií o dôveryhodnosti

Dôveryhodný zoznam (DZ) publikovaný NBÚ SR (aktuálny stav)

3.2.2 Podporované formáty nepodpísaných dokumentov

- Dokumenty typu PDF, DOC, DOCX, ODT, TXT, XML (čisté XML, XMLDataContainer) a RTF
- Obrázky typu PNG, GIF, TIFF, BMP a JPG

3.2.3 Podporované formáty podpísaných dokumentov/kontajnerov

- PDF – dokument podľa špecifikácie PDF ISO-32000 [2], ktorý je zároveň aj kontajnerom,
- ASICS – ASiC kontajner podľa ETSI TS 103174 [3],
- CMS, ZEPf, xZEP / ZEPx

Služba predpokladá, že sa jedná o kontajnery podľa ich špecifikácií.

3.2.4 Podporované formáty elektronických podpisov

- CAdES (CMS Advanced Electronic Signatures) vo formátoch
  - CAdES-BES, CAdES-EPES, CAdES-T, CAdES-X a CAdES-A podľa štandardu ETSI TS 101 733
- XAdES (XML Advanced Electronic Signatures) vo formátoch
  - XAdES-BES, XAdES-EPES, XAdES-T, XAdES-X a XAdES-A podľa štandardu ETSI TS 101 903
  - XAdES_ZEP s dátovými objektmi typu XML, PDF a zložený elektronický podpis
- PAdES (PDF Advanced Electronic Signatures) vo formátoch

- PAdES-BES, PAdES-EPES, PAdES-T a PAdES-LTV podľa štandardu ETSI TS 102 778

3.2.5 Podporované podpisové certifikáty

- kvalifikované certifikáty vydané certifikačnou autoritou akreditovanou NBÚ SR
- kvalifikované systémové certifikáty vydané certifikačnou autoritou akreditovanou NBÚ SR

3.2.6 Podporované rozhrania pre prácu s QSCD zariadeniami

- PKCS #11: Cryptographic Token Interface Standard
- Microsoft Crypto API / Cryptographic Service Provider

3.2.7 Podporované kryptografické algoritmy

3.2.7.1. Hash algoritmy

Služba QES portal podporuje nasledovné hash algoritmy:

- MD5
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého SSCD zariadenia a klientskej podpisovej aplikácie.

3.2.7.2. Podpisové algoritmy

Aplikácia poskytovania služby QES portal podporuje nasledovné podpisové algoritmy:

- MD5withRSA
- SHA-1withRSA
- SHA-224withRSA
- SHA-256withRSA
- SHA-384withRSA
- SHA-512withRSA

Uvedená množina algoritmov môže byť zúžená alebo rozšírená v závislosti od použitého SSCD zariadenia a klientskej podpisovej aplikácie.

3.3 Zdroj času

V oboch módoch práce je využívaná aj služba elektronickej časovej pečiatky, vďaka ktorej obsahuje každý podpísaný dokument dôveryhodné potvrdenie o svojej existencii v čase vytvorenia podpisu.

Spoločnosť Disig je oprávnená vydávať elektronické časové pečiatky v základnej ako aj kvalifikovanej forme, a to v súlade s Nariadením eIDAS, zákonom č. 272/2016 Z. z. o dôveryhodných službách ako aj v súlade s požiadavkami RFC 3161 Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP).

Kvalifikovaná služba vydávania časových pečiatok využíva presný čas vysokej a zaručenej presnosti získaný prostredníctvom NTP servera napojeného na presný čas vysielaný prostredníctvom GPS satelitov. Súkromné kľúče sú uchovávané v HSM zariadení, ktoré spĺňa požiadavky FIPS 140-2 level 3 a je certifikované NBÚ SR. Všetky časy, ak nie je explicitne uvedené inak, sú uvádzané vo formáte UTC.

3.4 Obmedzenie na veľkosti súborov

Služba akceptuje z bezpečnostných dôvodov súbory do veľkosti 10 MB.

3.5 Vnorené kontajnery

Validácia vnorených kontajnerov nie je službou podporovaná. Vnorené kontajnery vo validovanom kontajneri sú vyhodnocované ako akékoľvek iné binárne súbory (nie sú už ďalej expandované).

História zmien

Verzia	Dátum	Popis revízie; revidoval
1.0	05.06.2019	Prvá verzia dokumentu; Cesnek