

KVALIFIKOVANÁ PEČEŤ

| Michal Hanzal |

| Solution Consultant |



DEFINICE ELEKTRONICKÉ PEČETI

V nařízení eIDAS



Preamble

§59



Článek 3

§25



Článek 3

§26



Článek 3

§27



Články
35 – 40

ÚČEL ELEKTRONICKÉ PEČETI



Prokázání původu

Vnáší do dokumentu nezměnitelné informace o původci dokumentu opatřeného elektronickou pečeti.



Zajištění integrity

Umožňuje detekci neautorizovaných změn v dokumentu opatřeného elektronickou pečeti.

TYPY ELEKTRONICKÝCH PEČETÍ



Zaručená pečeť

je založená na interním
nebo komerčním certifikátu



Uznávaná pečeť

je založená na
kvalifikovaném certifikátu
pro elektronickou pečeť



Kvalifikovaná pečeť

je založená na
kvalifikovaném certifikátu
pro elektronickou pečeť
a
vytvořena pomocí
kvalifikovaného prostředku
pro vytváření pečetí

POVINNOSTI POUŽITÍ EL. PEČETI A ČASOVÉHO RAZÍTKA

dle Zákona 297/2016 Sb. o službách vytvářejících důvěru

§8

„Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí. “

§11

„Veřejnoprávní podepisující, který zapečetil elektronický dokument, kterým právně jedná, způsobem podle § 8, ..., opatří zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem.“

TYPY ELEKTRONICKÝCH PEČETÍ

a povinnost jejich použití v praxi dle Zákona 297/2016 Sb.

Původce \ Příjemce	Příjemce	
	Veřejná správa	Komerční sektor
Veřejná správa	Kvalifikovaná	Kvalifikovaná
Komerční sektor	Uznávaná	Libovolný typ

PŘEDMĚT PEČETĚNÍ



Elektronické dokumenty

PDF
dokumenty

formát
PAeS



Emaily

MSG i EML
emaily

formát CAdES
v S/MIME



Data/Transakce

Audio, video,
obchodní transakce

formáty CAdES
a XAdES



**OBELISK
SEAL**



Automatizuje vytváření elektronických pečetí ve formátech
a úrovních stanovených nařízením eIDAS.



VÝHODY PRODUKTU



VÝHODY PRODUKTU



Neomezený počet
používaných pečetí



Nasazení v řádu dní



Univerzální použití
pro všechny typy pečetí



Cena nezávislá na počtu
pečetěných dokumentů



Přehled
o provedených operacích
pečetění

VÝHODY PRODUKTU



Neomezený počet
napojených IS



Napojení na více
časových autorit



Řízení oprávnění
k použití jednotlivých
pečetí



Škálovatelný
výkon i dostupnost



Snadná integrace služby
pečetění na další systémy



Konektory na QSCD
součástí produktu



**OBELISK
SEAL**

FUNKCE A VLASTNOSTI



FUNKCE A VLASTNOSTI



VYTVÁŘENÍ PEČETÍ

✓ Vytváření neviditelných i vizualizovaných pečetí v PDF dokumentech

- Vizualizovat lze textové informace nebo libovolnou grafiku

✓ Podporované formáty

- PAdES B-B a B-T
- XAdES B-B a B-T
- CAdES B-B a B-T
- S/MIME



PŘÍKLAD VIZUALIZOVANÉ PEČETI

Dolore non est a odio viverra sagittis. Nam quis lobortis metus lobortis id. Etiam at tellus laoreet tortor a dolor dapibus, in viverra Vestibulum pellentesque volutpat turpis, finibus accumsan. Nam commodo consectetur finibus.

Elektronicky opečetěno,
SEFIRA spol. s r. o.



Podpis je PLATNÝ, podepsaný uživatelem TEST - OB-A, AdES signing certificate - TEST.

Čas podepsání: 2020/02/28 13:38:07 +01'00'

Zdroj důvěry získán z European Union Trusted Lists (EUTL).

Důvod: Demonstrace elektronické pečeti

Umístění:

Přehled platnosti

Tento dokument se od aplikování tohoto podpisu nezměnil.

Autor certifikátu určil, že v tomto dokumentu je povoleno vyplňování polí formulářů, podepisování a přidávání poznámek. Žádné další změny nejsou povolené.

Identita autora podpisu je platná.

Čas podepsání pochází z hodin na počítači autora podpisu.

Podpis byl ověřen k času podepsání
2020/02/28 13:38:07 +01'00'

Informace o autorovi podpisu

Cesta od certifikátu autora podpisu k certifikátu vystavitele byla úspěšně vytvořena.

Certifikát autora podpisu je platný a nebyl odvolán.

[Zobrazit certifikát autora podpisu...](#)

[Další vlastnosti...](#)

[Ověřit podpis](#)

[Zavít](#)

SPRÁVA KLÍČŮ

- ✓ Sledování platnosti certifikátů zaregistrovaných klíčů včetně zasílání administrátorských notifikací
- ✓ Možnosti paralelního využití pečetících klíčů uložených jak v QSCD, tak lokálně v OBELISK Seal
- ✓ Řízení přístupu k registrovaným pečetícím klíčům na úrovni systémových účtů integrovaných informačních systémů



SPRÁVA KLÍČŮ

Administrace certifikátů a klíčů

Správa certifikátů

System > Administrace > Správa certifikátů

← Zpět

Výsledková sada záznamů (13)

	Typ	Název	Úložiště	Seriové číslo	Algoritmus	Platnost od	Platnost do
	X509Certificate	guildProvider			SHA256withRSA	30.10.2017	30.10.2027
	X509Certificate	certReviewTrustedCert	certReviewTruststore		SHA256withRSA	04.04.2017	04.04.2037
	X509Certificate	crtLOTLRootTrust1	Důvěryhodné certifikáty pro podpis TSL		SHA256withRSA	06.03.2015	05.03.2035
	X509Certificate	crtLOTLRootTrust2	Důvěryhodné certifikáty pro podpis TSL		SHA1withRSA	04.10.2007	15.12.2021
	X509Certificate	crtLOTLRootTrust3	Důvěryhodné certifikáty pro podpis TSL		SHA1withRSA	26.06.2013	28.01.2028
	LocalKeyPair	certReviewClient			SHA256withRSA	04.03.2019	03.03.2021
	X509Certificate	cert_PostSignumPublicCA2	OB-TA SSL TrustStore		SHA256withRSA	19.01.2010	19.01.2020
	X509Certificate	cert_PostSignumRootQCA4	OB-TA SSL TrustStore		SHA512withRSA	26.07.2018	26.07.2038
	Pkcs11KeyIdentifier	key_QSealKey01			SHA256/RSA	05.06.2019	04.06.2020

SPRÁVA KLÍČŮ

Podporovaná zařízení pro uložení a správu klíčů



Softwarové úložiště

Úložiště klíčů OBELISK



HSM

Kvalifikovaný prostředek pro
vytváření elektronických pečeti
QSealCD

PODPOROVANÁ QSealCD ZAŘÍZENÍ

HSM moduly

The logo for N CIPHER, featuring a blue circle with a white 'N' inside, followed by the word 'CIPHER' in blue capital letters with a trademark symbol.



The logo for utimaco, featuring the word 'utimaco' in black lowercase letters with a registered trademark symbol, and a small blue diamond icon above the 'i'.



CENTRÁLNÍ KONFIGURACE

- ✓ Zavádění a správa pečetících klíčů
- ✓ Napojení na úložiště klíčů resp. QSCD zařízení
- ✓ Definice pečetících politik
- ✓ Nastavení vizualizace pečetí (pouze v PDF)
- ✓ Správa oprávnění použití pečetících klíčů
- ✓ Napojení služby časových razítek (možnost využití několika poskytovatelů současně formou fail-over)



AUDIT A MONITORING SYSTÉMU

✓ Pro jednotlivé vytvářené pečeti se zaznamenává:

- Datum a čas provedeného pečeti
- Otisk pečetěných dat
- Identifikace pečetěcího klíče, který byl použit
- Technický uživatel (volající systém)





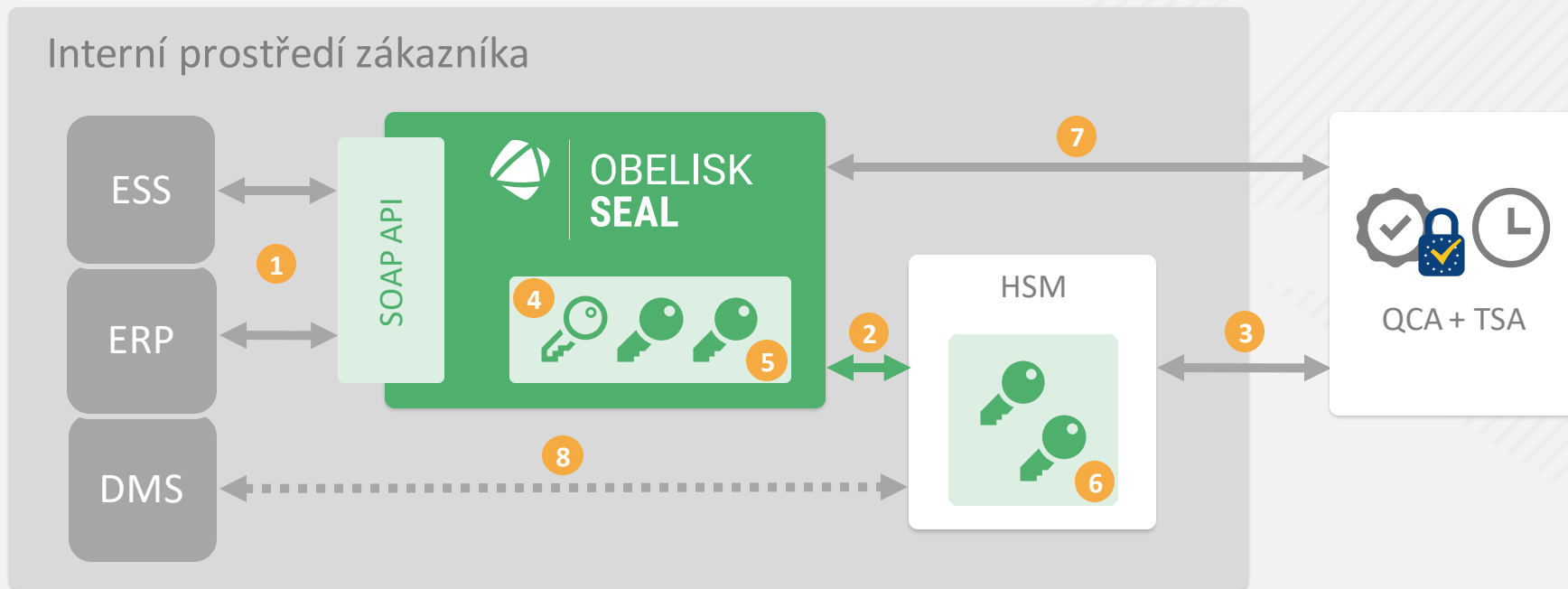
OBELISK
SEAL

MOŽNOSTI
NAsAZENÍ



KVALIFIKOVANÁ PEČEŤ

Single instalace s využitím HSM

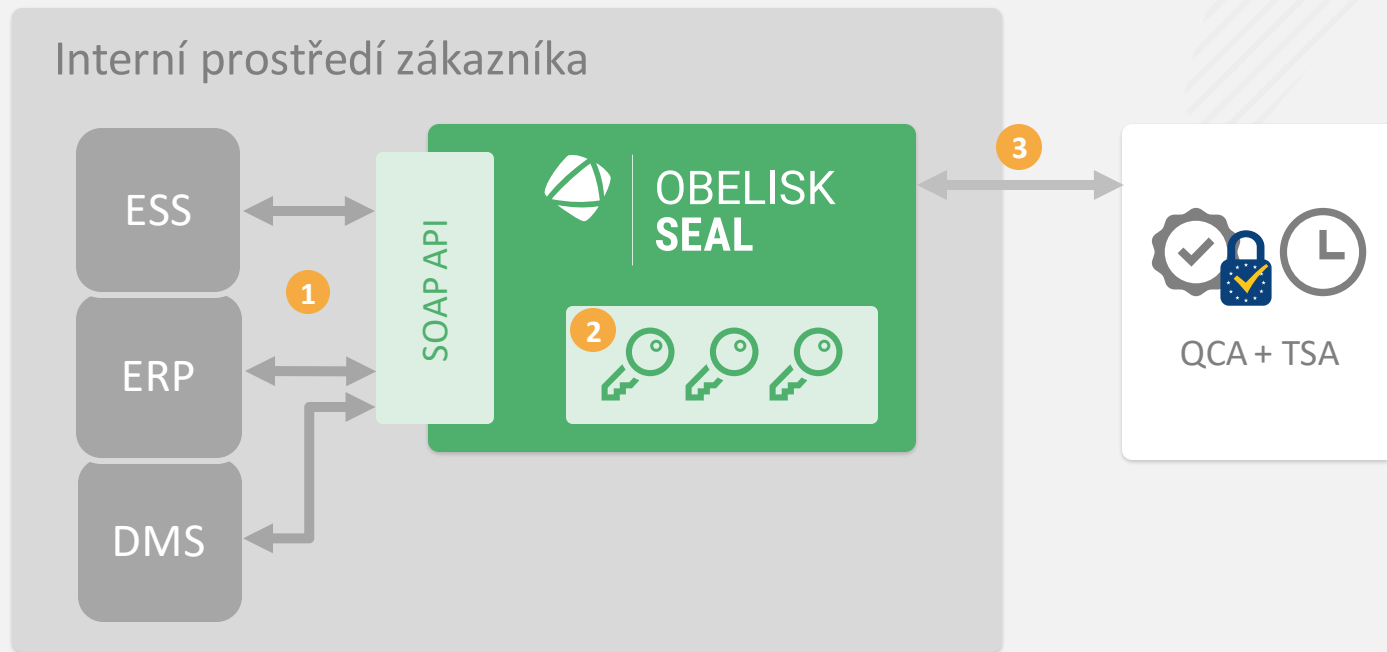


Legenda:

- 1 – požadavek na pečetění (dokument/hash + auth + výběr klíče) a odpověď s opečetěným dokumentem,
- 2 – vytvoření pečeti v HSM, 3 – žádost o certifikát a vystavení certifikátu autoritou, 4 – klíč v lokálním úložišti OBELISK,
- 5 – certifikáty dostupné pro pečetění klíči chráněnými v HSM, 6 – pečeti klíče vytvořené a chráněné v HSM,
- 7 – napojení na časovou autoritu, 8 – přímý přístup k HSM (PKCS#11 rozhraní)

ZARUČENÁ ELEKTRONICKÁ PEČEŤ

Single instalace s využitím SW úložiště

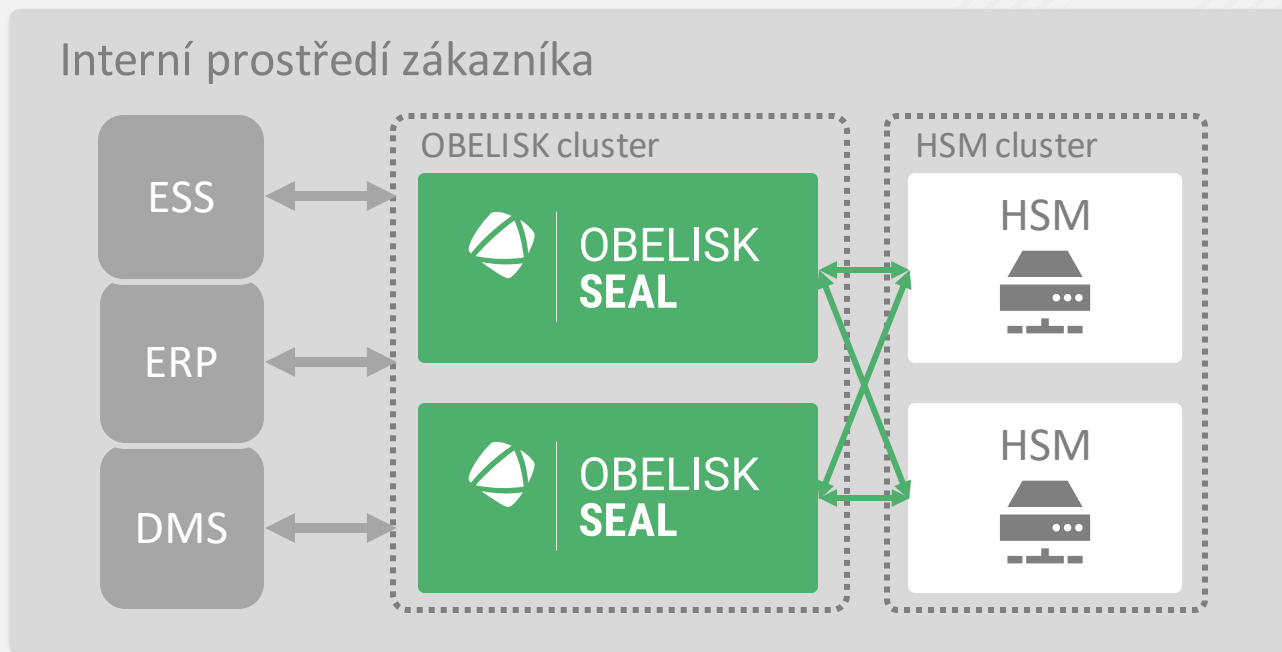


Legenda:

- 1 – požadavek na pečetění (dokument/hash + auth + výběr klíče) a odpověď s opečetěným dokumentem,
- 2 – klíče v lokálním úložišti OBELISK, 3 – napojení na časovou autoritu

KVALIFIKOVANÁ PEČEŤ

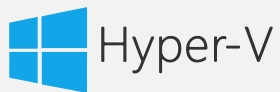
High Availability s využitím HSM – Active/Active i Active/Passive



TECHNICKÉ INFORMACE A SYSTÉMOVÉ POŽADAVKY

Virtuální appliance

vmware®



Podporované databáze

ORACLE®

PostgreSQL



Výpočetní nároky



min. 4 vCPU



min. 32 GB RAM

VÝKONNOST

až **12** pečetí
/ node / sekundu

Počet vytvořených pečetí závisí na velikosti dokumentů, síťové propustnosti a infrastruktuře.

INTEGRAČNÍ ROZHRANÍ (1)

Vstupy a výstupy

✓ Integrační API

- SOAP webové služby vybudované dle principů OASIS DSS

✓ Napojení na služby poskytující časová razítka

- OBELISK Seal je možné připojit na jakoukoli službu vydávající časová razítka prostřednictvím protokolu RFC 3161 Time-Stamp Protocol (TSP)

INTEGRAČNÍ ROZHRANÍ (2)

Detaily rozhraní

✓ Autentizace vůči webovým službám

- http basic
- autentizace certifikátem

✓ Výběr klíče k pečetění

- automaticky konfigurací vlastníka pečetícího klíče
- výběr v rámci volání pomocí elementu KeySelector

✓ Způsoby pečetění

- **předání celého dokumentu** – výsledkem pečetění je dokument s vloženou pečetí
- **předání hashe dokumentu** – výsledkem je elektronická pečeť, kterou volající systém s dokumentem sám spojí



**OBELISK
SEAL**

CERTIFIKACE



SOULAD S NORMAMI ETSI

Norma	Zaměření
ETSI EN 319 102	Creation and validation of AdES digital signatures
ETSI EN 319 122	CAdES digital signatures
ETSI EN 319 132	XAdES digital signatures
ETSI EN 319 142	PAdES digital signatures
ETSI EN 319 172	Signature Policies
ETSI EN 319 312	Cryptographic Suites

CERTIFIKACE A ATESTY

Atesty shody vydané Elektrotechnickým zkušebním ústavem

- ✓ Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce (články 26, 32, 33, 34, 36, 40)
- ✓ Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce (§5 - §12)



ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV



ELECTROTECHNICAL TESTING INSTITUTE - CZECH REPUBLIC
ELEKTROTECHNISCHE PRÜFANSTALT - TSCHIECHISCHE REPUBLIK
INSTITUT ELECTROTECHNIQUE D'ESSAIS - RÉPUBLIQUE TCHÈQUE
ЭЛЕКТРОТЕХНИЧЕСКИЙ ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ - ЧЕШСКАЯ РЕПУБЛИКА

Pod lísom 129/2, 171 02 Praha 8 - Troja

Elektrotechnický zkušební ústav, s.p. uděluje

ATEST SHODY

č.: AS180001

Předmět atestu: Produkt OBELISK, verze 2.1.x

Objednatel: SEFIRA spol. s r.o.
Antala Staška 2027/77, 140 00 Praha 4 - Krč, Česká republika

Datum posouzení: 29.03.2018

Výsledek posouzení: SPLNĚNO

Výsledky posouzení jsou uvedeny ve zprávě č.: 801204-02 ze dne 30.05.2018

Předmět atestu je ve shodě s požadavky:

- a) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- článek 26: Požadavky na zaručení elektronické podpisy
- článek 32: Požadavky na ověřování platnosti kvalifikovaných elektronických podpisů
- článek 33: Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů
- článek 34: Kvalifikovaná služba uchování kvalifikovaných elektronických podpisů
- článek 36: Požadavky na zaručení elektronické pečeti
- článek 40: Ověřování platnosti: a uchování kvalifikovaných elektronických pečeti
- b) Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce
- §5-7: Podpisování dokumentů
- §8-10: Pečetění dokumentů
- §11: Použití kvalifikovanosti elektronického časového razítka
- §12: Ověřování platnosti zaručeného elektronického podpisu a zaručení elektronické pečeti.

Atest shody byl vydán na základě splnění vybraných požadavků Nařízení Evropského parlamentu a Rady (EU) č. 910/2014, Zákon č. 297/2016 Sb. o službách vytvářejících důvěru a na základě smlouvy č. 801204 mezi objednatel, a Elektrotechnickým zkušebním ústavem, s.p. Atest shody vyjadřuje shodu s požadavky ke dni jeho posouzení.

11.06.2018

V Praze dne

Mgr. Miroslav Sedláček
Vedoucí certifikačního orgánu



razítko



801204-02

ELEKTROTECHNICKÝ ZKUŠEBNÍ ÚSTAV



ELECTROTECHNICAL TESTING INSTITUTE - CZECH REPUBLIC
ELEKTROTECHNISCHE PRÜFANSTALT - TSCHIECHISCHE REPUBLIK
INSTITUT ELECTROTECHNIQUE D'ESSAIS - RÉPUBLIQUE TCHÈQUE
ЭЛЕКТРОТЕХНИЧЕСКИЙ ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ - ЧЕШСКАЯ РЕПУБЛИКА

Pod lísom 129/2, 171 02 Praha 8 - Troja

Elektrotechnický zkušební ústav, certifikační orgán č. 3018 akreditovaný Českým institutem pro akreditaci, o.p.s. podle ČSN EN ISO/IEC 17065, uděluje

CERTIFIKÁT

č.: 1180424

Výrobek: Systém pro dlouhodobě důvěryhodné ukládání dokumentů

Typ: OBELISK, verze 2.1.x

Jmenovitě hodnoty: -

Objednatel: SEFIRA spol. s r.o.
Antala Staška 2027/77, 140 00 Praha 4 - Krč, Česká republika

Výrobce: SEFIRA spol. s r.o.
Antala Staška 2027/77, 140 00 Praha 4 - Krč, Česká republika

Obchodní značka:

Výsledky zkoušek jsou uvedeny v protokolu č.: 801204-01 ze dne 30.05.2018

Vzorček zkoušeného výrobku je ve shodě s požadavky:

- Zákon č. 499/2004 Sb. o archivnictví a spisové službě ve znění pozdějších předpisů (§3 bod 5; §8 bod 1, 2; §9 bod 1 a §69a), Vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby (§20 bod 1, 4, 5 a §21 bod 4, 7),
- Národní standard pro elektronické systémy spisové služby (NSESSS) (čl. 2.5, čl. 2.6, čl. 3.1 (body 3.1.1, 3.1.2, 3.1.4 - 3.1.6, 3.1.13, 3.1.16, 3.1.18, 3.1.20 - 3.1.22, 3.1.24 - 3.1.31, 3.1.33), čl. 5.1 (body 5.1.1 - 5.1.3, 5.1.6, 5.1.9, 5.1.11, 5.1.13 - 5.1.15, 5.1.17, 5.1.18), čl. 5.3 (bod 5.3.3), čl. 6.2, čl. 6.3 (body 6.3.1 - 6.3.3), čl. 7.2 (body 7.2.1 - 7.2.3, 7.2.5, 7.2.6, 7.2.8 - 7.2.10), čl. 7.3, čl. 11.1 (body 11.1.1 - 11.1.2, 11.1.5, 11.1.7, 11.1.12), čl. 11.2, čl. 11.3).

Jiné údaje:

Certifikát byl vydán na základě splnění požadavků certifikačního schématu „Certifikace SW“ a na základě smlouvy č. 801204 mezi objednavatelem a Elektrotechnickým zkušebním ústavem.

Platnost certifikátu je omezena do: 30.06.2021

11.06.2018

V Praze dne

Mgr. Miroslav Sedláček
Vedoucí certifikačního orgánu



razítko



801204-01



**OBELISK
SEAL**

REFERENCE



REFERENCE



GENERÁLNÍ FINANČNÍ
ŘEDITELSTVÍ

Kvalifikovaná elektronická
pečeť v odchozích emailech



Česká republika
Nejvyšší kontrolní úřad

Kvalifikovaná elektronická
pečeť v high availability

wüstenrot

Vizualizovaná pečeť jako
forma vzdáleného podpisu
klientských smluv



Ministerstvo spravedlnosti
České republiky

Centralizované řešení
kvalifikované elektronické
pečeti pro všech soudy

REFERENCE



Kvalifikovaná elektronická
pečet' v rámci projektu
nového mýta



Kvalifikovaná elektronická
pečet' v high availability

DALŠÍ PRODUKTY OBELISK



OBELISK
SIGNING PORTAL



OBELISK
VALIDATOR



OBELISK
TRUSTED ARCHIVE



OBELISK
STORAGE



25
LET

www.sefira.cz