CERTIFIKAČNÍ PROTOKOL

Posouzení provedl:	
ID protokolu:	PCEB 19/01/02
ID certifikátu:	PCEB 19/01/02
Datum uvolnění protokolu:	31.01.2019

Zpráva o posouzení shody

dle čl. 20 nařízení Evropského Parlamentu a Rady (EU) č. 910/2014.

Posouzení provedl:	Certifikační orgán TAYLLORCOX PCEB, zřízený TAYLLORCOX s.r.o.
Rozsah posouzení:	Posouzení shody kvalifikované služby vytvářející důvěru - vydávání kvalifikovaných certifikátů pro elektronické pečetě s Nařízením Evropského Parlamentu a Rady (EU) č. 910/2014.
Posuzovaná služba:	NCA – služba vydávání kvalifikovaných certifikátů pro elektronickou pečeť
Výsledek posouzení:	**Posuzovaná služba je VE SHODĚ s příslušnými požadavky Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014.**
Odůvodnění:	Předložené podklady k posouzení shody byly ověřeny v souladu s požadavky certifikačního schématu definovaného normou ČSN EN 319 403 v2.2.2, ve spojení s DKP verze 2, formou auditu, a vyhodnoceny dle stanovených metrik. Na základě výsledků posouzení nebyly shledány nedostatky bránící vystavení certifikátu, a proto bylo posouzení služby ukončeno s výše uvedeným výsledkem. Zjištění a podmínky platnosti certifikátu jsou uvedeny v kap. 1.2, 1.3 a v Příloze.

OBSAH

IDENTIFIKAČNÍ ÚDAJE

Identifikační údaje žadatele (TSP)	
Obchodní firma / Název společnosti nebo jméno a příjmení fyzické osoby	Česká republika – Správa základních registrů
Sídlo nebo místo podnikání/trvalého pobytu fyzické osoby	Na Vápence 14, 130 00 Praha 3
Zastoupený	Ing. Michalem Peškem, ředitelem
IČ (bylo-li přiděleno)	72054506

Identifikační údaje posuzované služby	
Název posuzované služby	NCA – služba vydávání kvalifikovaných certifikátů pro elektronickou pečeť
Verze posuzované služby	OID 1.2.203.72054506.10.1.31.1.0 (SZR_CP_Pecet_RSA) OID 1.2.203.72054506.10.1.32.1.0 (SZR_CP_TSA_RSA)

HLAVNÍ ZÁVĚRY AUDITU

Hlavní závěry auditu jsou uvedeny na úvodní straně této zprávy o posouzení shody, včetně výsledku certifikace. Důkazy, prokazující relevantnost a správnost rozhodnutí certifikačního orgánu dokládají následující kapitoly.

1.1 AUDITOVANÉ OBLASTI

Certifikační audit pokryl posuzovanou službu v rozsahu a míře požadavků definovaných certifikačním schématem. Výčet hlavních požadavků na službu je uveden v tabulce níže:

Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014
• článek 5 – Zpracování a ochrana údajů
• článek 13 – Odpovědnost za škodu a důkazní břemeno
• článek 15 – Přístupnost pro osoby se zdravotním postižením
• článek 19 – Bezpečnostní požadavky vztahující se na poskytovatele služeb vytvářejících důvěru
• článek 24 – Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru
• článek 38 – Kvalifikované certifikáty pro elektronické pečetě
• Příloha III – Požadavky na kvalifikované certifikáty pro elektronické pečetě

Detailní zjištění, která byla během auditu provedena, jsou zaznamenána v kapitole Kritéria auditu.

1.1.1 SOUPIS POUŽITÉ VSTUPNÍ DOKUMENTACE

TSP poskytl dále uvedený seznam řízené dokumentace, kterým dokládá shodu své kvalifikované služby s výše uvedenými požadavky na tuto službu.

ID	Název souboru (pdf)	Verze	Název dokumentu
1	SZR_Rozsah_ISMS_1v0.pdf	1.0	NCA - Rozsah ISMS (Návrh na doplnění stávajícího dokumentu SZR)
2	SZR_AR_Zaverecna_zprava_1v0	1.0	NCA - Analýza rizik - závěrečná zpráva
3	SZR_AR_Vyber_protio_1v1	1.1	NCA - Analýza rizik - výběr bezpečnostních opatření
4	SZR_Zbytkova_rizika_1v1 (dva dokumenty - PDF a XLS)	1.1	NCA - Zbytková rizika
5	SZR_ZR_Manazerske_shrnuti_1v1	1.1	NCA - Zbytková rizika - manažerské shrnutí
6	SZR_NCA-SBP_CA_TSA_1v0 SZR_NCA-SBP_Checklist_1v0	1.0	NCA - systémová bezpečnostní politika (CA a TSA) NCA - systémová bezpečnostní politika (CA a TSA) – checklist
7	SZR_Rizeni_kontinuity_1v0	1.0	NCA - Řízení kontinuity provozu
8	SZR_CP_Root_RSA_1v01	1.01	NCA - Certifikační politika kořenové certifikační autority (kryptografie RSA)
9	SZR_CP_Pecet_RSA_1v01	1.01	NCA - Certifikační politika vydávání kvalifikovaných certifikátů pro ověřování elektronických pečetí (kryptografie RSA)
10	SZR_CP_OCSP_RSA_1v01	1.01	NCA - Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA)
11	SZR_CPS_RSA_1v01	1.01	NCA Certifikační prováděcí Směrnice (kryptografie RSA)
12	SZR_CP_PDS_RSA_1v1	1.1	NCA Zpráva pro uživatele CA
13	SZR_CP_PDS_RSA_EN_1v1	1.1	NCA CA PKI Disclosure Statement
14	SZR_Rizeni_fyz_pristupu_1v1	1.1	NCA Řízení fyzického přístupu do provozních prostor (Návrh směrnice)

ID	Název souboru (pdf)	Verze	Název dokumentu
15	SZR_Smernice_prac_RA_1v1	1.1	NCA Směrnice pro pracovníky RA
16	SZR_Ukonceni_cinnosti_1v1	1.1	NCA Ukončení činnosti služeb CA, TSA
17	SZR_Pozarni_bezpecnost_1v0	1.0	NCA Požární bezpečnost (Návrh na doplnění stávající dokumentace SZR)
18	SZR_NCA-HSM_PrivateServer-1v0	1.0	NCA HSM PrivateServer Směrnice pro správu
19	SZR-NCA-HSM_Postupy_instalace_a_správy_1v00	1.0	HSM PrivateServer v.5 Postupy instalace a správy
20	SZR_NCA-HSM-Postupy_generování_klíčů_a_certifikátů_CA-1v00	1.0	NCA HSM PrivateServer Postupy generování klíčů a certifikátů CA
21	SZR_Uchovavani_dat_a_informaci_1v0	1.0	NCA Uchovávání dat a informací
22	SZR_Kontrolni_cinnost_1v0	1.0	NCA Kontrolní činnost, bezúhonnost a odbornost
23	SZR_Zmenove_rizeni_1v0	1.0	NCA Změnové řízení (Návrh na doplnění stávajícího dokumentu SZR)
24	SZR_Bezpecnostni_incidenty_1v0	1.0	NCA Bezpečnostní incidenty (Návrh na doplnění stávajícího dokumentu SZR)
25	SZR_Sitova_bezpecnost_NCA_1v0	1.0	NCA Síťová bezpečnost (Návrh na doplnění stávajícího dokumentu SZR)
26	SZR_Projekt_fyzicke_bezpecnosti_1v0	1.0	NCA Projekt fyzické bezpečnosti prostor (Návrh na doplnění stávající dokumentace SZR)
27	SZR_Dilci_spisovy_plan_1v0	1.0	NCA Spisový a skartační plán (Návrh na doplnění stávající dokumentace SZR)
28	SZR_Spisovy_a_skartacni_rad_1v0	1.0	NCA Spisový a skartační řád (Návrh na doplnění stávající dokumentace SZR)
29	SZR_Evidence_aktiv_1v0	1.0	NCA Evidence aktiv (Návrh na doplnění stávající dokumentace SZR)
30	SZR_Politika_vydavani_QSigCD_1v0	1.0	NCA Politika vydávání QSigCD
31	NCA - Premisteni systemu CA v.1.0	1.0	NCA Přemístnění systémů CA, TSA

ID	Název souboru (pdf)	Verze	Název dokumentu
32	NCA - Zaloha dat systemu v.1.0	1.0	NCA Záloha dat systémů
33	NCA -Obnova systemu CA v.1.1	1.1	NCA Obnova systémů CA
34	NCA - Prirucka_administratora_1v1	1.1	NCA Příručka administrátora systémů CA, TSA
35	SZR_CP_TSA_RSA_1v01.pdf	1.01	NCA - Certifikační politika vydávání certifikátů pro systém TSA (kryptografie RSA)

1.1.2 OBLASTI, V NICHŽ BYLA CERTIFIKACE PROVÁDĚNA

Oblasti, v nichž byla certifikace prováděna, vycházejí z typu certifikované služby, rizik spojených s realizací auditu na místě a dohod s TSP, jehož služba je certifikována. Výčet oblastí je uveden v tabulce.

Místo ověřování dokumentace	Provozovna certifikačního orgánu TAYLLORCOX PCEB
Místo auditu	1. Sídlo: Česká republika – Správa základních registrů, Na Vápence 915/14, Praha 3 2. Provozovna / Primární lokalita: Česká republika – Správa základních registrů, Na Vápence 915/14, Praha 3 3. Dislokované pracoviště: Ministerstvo obrany (zvláštní složka – typizované řešení)
Použitý HW TSP pro audit	HW operátora registrační autority (PC) HW administrátora certifikační autority a serverové části služby – provozní pracoviště (Na Vápence) HSM PSV 5.0 /5.0.3 (HSM podepisující certifikáty vydané TSP) HW serverové části služby QSealCD - HSM Thales nShield Connect 1500+ CC (Model Number: NH2061, SN: 36-NCxxxxA) Čtečka karet s PINpad (operátor RA) Tiskárna (tisk žádostí a smluv)
Použitý SW TSP pro audit	APP operátora registrační autority „NCA NewCert“ – identická pro všechny RA (Na Vápence i na RA zvláštních složek) Adobe Acrobat Reader DC APP operátora certifikační autority a serverové části služby – provozní pracoviště (Na Vápence) HSM Private Server 5.0 /5.0.3 – provozní pracoviště Na Vápence

1.1.3 POUŽITÝ ETALON A METRIKY

Pro posouzení jednotlivých požadavků na službu byl stanoven následující etalon a metriky.

Označení Etalonu	Definice Etalonu (popis)
eIDAS	Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 (eIDAS), v rozsahu požadavků na danou službu uvedených v kapitole 1.1 této zprávy DKP verze 2 (dokument vydaný MVČR a dostupný na jeho webu) Prováděcí rozhodnutí Komise (EU) 2016/650
Norma	Normy, na které se etalon eIDAS odvolává, v aktuálně platném znění: ČSN EN ISO/IEC 17065:2013 včetně specifických požadavků ČSN EN ISO/IEC 17021-1 a ČSN EN ISO/IEC 27006 ČSN ETSI EN 319 403 V2.2.2 (2015-08) ve spojení s DKP verze 2 ETSI EN 301 549 V2.1.2 (2018-08) ETSI EN 319 401 V2.1.1 (2016-02) / ETSI EN 319 401 V2.2.1 (2018-04) ETSI EN 319 411-1 V1.1.1 (2016-02) / ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-2 V2.1.1 (2016-02) / ETSI EN 319 411-2 V2.2.2 (2018-04) ETSI EN 319 412-1 V1.1.1 (2016-02) ETSI EN 319 412-2 V2.1.1 (2016-02) ETSI EN 319 412-3 V1.1.1 (2016-02) ETSI EN 319 412-4 V1.1.1 (2016-02) ETSI EN 319 412-5 V2.1.1 (2016-02) / ETSI EN 319 412-5 V2.2.1 (2017-11) Řada norem EN 419 2XX (Protection Profiles) Nařízení Evropského parlamentu a Rady (EU) 2016/679

Označení metriky	Definice metriky (popis)
EQUAL	Ověření splnění / nesplnění požadavku Etalonu z dokumentace Zjištění: S – Splňuje, V – splňuje s Výhradou, N-Nesplňuje, N/A-Neověřováno.
TEST	Ověření splnění / nesplnění požadavku Etalonu testem Zjištění: S – Splňuje, V – splňuje s Výhradou, N-Nesplňuje, N/A-Neověřováno.

1.2 PROVEDENÁ ZJIŠTĚNÍ

Souhrnná zjištění (dle zákazníkem stanovené funkcionality a etalonu)	Ano[1]	Ne[1]	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 5	☒	☐	V	EQUAL	Kritéria etalonu eIDAS byla naplněna Výhrady uvedeny v kap. 1.3
eIDAS, čl. 13	☒	☐	V	EQUAL	Kritéria etalonu eIDAS byla naplněna Výhrady uvedeny v kap. 1.3
eIDAS, čl. 15	☒	☐	S	EQUAL	Kritéria etalonu eIDAS byla naplněna
eIDAS, čl. 19	☒	☐	V	EQUAL	Kritéria etalonu eIDAS byla naplněna Výhrady uvedeny v kap. 1.3
eIDAS, čl. 24	☒	☐	V	EQUAL	Kritéria etalonu eIDAS byla naplněna Výhrady uvedeny v kap. 1.3
eIDAS, čl. 38	☒	☐	S	EQUAL	Kritéria etalonu eIDAS byla naplněna
Příloha III.	☒	☐	S	EQUAL, TEST	Kritéria etalonu eIDAS byla naplněna Ověřeno testem

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky v kap. 1.1.3, sloupci „Označení metriky“.*

1.3 POPIS NALEZENÝCH NESHOD

Během auditu nebyly shledány žádné neshody bránící řádnému poskytování kvalifikované služby vydávání kvalifikovaných certifikátů pro elektronické pečetě v rozsahu požadavků na kvalifikovanou službu a udělení certifikátu shody s požadavky na kvalifikovanou službu.

V následující tabulce je uveden seznam výhrad, které musí být vypořádány, a výčet opatření, která musí být zavedena, před spuštěním certifikované služby do provozu.

Nedoložení vypořádání výhrad a zavedení opatření před spuštěním služby do provozu je důvodem k pozastavení, případně ukončení platnosti certifikátu.

Vypořádání bude doloženo jak certifikačnímu orgánu, který certifikaci provedl, tak i dozorovému orgánu, který rozhoduje o schválení služby jako kvalifikované a zařazení služby na EU Trust list.

eIDAS	Výhrady
Řízená dokumentace Čl. 19	**Dokumenty obecně** - Zapracovat dokumenty označená jako „návrh na zapracování“ do stávající dokumentace SZR (dle vysvětlení se nejedná o návrhy, ale informace, které mají být zohledněny v již existující dokumentací SZR). Příkladem může být dokument „NCA Bezpečnostní incidenty (Návrh na doplnění stávajícího dokumentu SZR)“.
Smlouvy obecně Čl. 19, 24	**Finální verze smluv musí pokrývat minimálně** - postupy obnovy certifikátů ve správě NCA v dané lokalitě zvláštní složky a v prostředí NCA (každý rok) - pravidla do smlouvy (možno i jako samostatná příloha smlouvy), - pravidla pro činnost pracovníka RA v rámci jeho jmenovacího dekretu (vědomý a vymahatelný závazek dodržování pravidel a politik NCA) - pravidla obsazení do rolí a povinnost proškolení, ošetřit do smlouvy se zvláštními složkami - pravidla nakládání s dokumenty na RA i v serverovně zvláštní složky, ošetřit do smlouvy (pravidla spisovny, archivu) - na dislokovaném pracovišti (zvláštní složce) zavést docházkovou knihu a ukotvit do smlouvy nakládání s touto knihou (přístup, uchovávání, skartace atd.) - popsat plán kontinuity při výpadku primární lokality, aby nebyl překročen čas 24 hodin pro publikaci CRL – dle poskytnutých informací bude ošetřeno v provozní smlouvě s I.CA, než se vybuduje záložní lokalita - zavést plány kontinuity nejen pro primární lokalitu, ale zohlednit je i do smluv se zvláštními složkami - vymínit do smluv se zvláštními složkami právo NCA provést jejich kontrolu, včetně jimi provozovanými RA, alespoň 1x ročně - podchytit monitorování infrastruktury a běhu serverů a fungování RA na zvláštních složkách tak, aby mohlo NCA vždy garantovat důvěrnost poskytované služby - podchytit do smluv se zvláštními složkami požadavky kapitol 2.2 a 4 dokumentu SZR_Rizeni_fyz_pristupu_1v1, který se týká práva přístupu a nakládání s prostředky NCA v prostorech zvláštní složky - SZR_Ukonceni_cinnosti_1v1, kap. 2.5: NCA musí i na straně smluvního partnera nastavit pravidla tak, aby za všech okolností byly dodrženy lhůty, po které má NCA povinnost dokumentaci o svých službách uchovávat
Čl. 5	Předložené informace neobsahují plné pokrytí požadavků nařízení GDPR na informování subjektu údajů o jeho právech dle čl. 12 až 22 tohoto nařízení. Během auditu bylo deklarováno, že NCA využívá pro plnění tohoto bodu již zavedené procesy SZR jako celku. Je tedy nezbytné doložit provázání ochrany osobních údajů NCA s procesy SZR, např. odkazem z řízené dokumentace NCA na dokumenty SZR, kde jsou bližší informace o uplatnění práv SÚ a ochraně OÚ, včetně kontaktu na pověřence.
ČL. 13.2	Informace, které mají být dostupné neomezeným vzdáleným přístupem (certifikáty, CP, CPS, atd.) existují, ale zpřístupněny ještě nejsou. Web www.narodni-CA.cz nebyl ke dni auditu spuštěn, ani nebyl prezentován návrh jeho plánovaného obsahu.

1.4 DOPLŇUJÍCÍ KOMENTÁŘE A UPŘESNĚNÍ

Služba **NCA – služba vydávání kvalifikovaných certifikátů pro elektronickou pečeť** umožňuje vydávat kvalifikované certifikáty pro elektronické pečetě, využívané v procesech ověřování zaručených elektronických pečetí a kvalifikovaných elektronických pečetí.

Na základě provedeného auditu certifikační orgán identifikoval následující místa pro zlepšení, kterým by měl TSP věnovat zvýšenou pozornost v následujícím období.

eIDAS	Doporučení
Řízená dokumentace	Změna loga z I.CA na SZR na první straně některých dokumentů
Čl. 5	využít web SZR, kde již jsou bližší informace k GDPR, včetně pravidel pro uplatnění práv subjektu údajů
ČL. 13.2	Provázat web SZR a www.narodni-CA.cz pro efektivní zveřejňování informací NCA na jednom místě
Čl. 15	Projít v rámci systému řízení všechna doporučení z nové verze normy ETSI EN 301 549
Čl. 19	- Zpracovat záznamy z testů plánů kontinuity - Zavést vnitřní proces kontroly dodržování požadavků eIDAS v aktuálních verzích (Prováděcí rozhodnutí komise (EU), ETSI normy), včetně procesu změnového řízení při identifikaci takové změny
Čl. 38	Při spuštění služby do ostrého provozu vystavit kvalifikovaný certifikát pro elektronický podpis, kvalifikovaný certifikát pro elektronickou pečeť (kvalifikovanou a zaručenou) a kvalifikované elektronické časové razítko, u těchto provést kontrolu správnosti jejich struktury a vazby na root a mezilehlý certifikát. O ověření provést písemný záznam. Tyto výstupy následně uchovat pro kontrolu v rámci dozorového auditu.

SHRNUTÍ AUDITU ANALÝZY RIZIK

V průběhu auditu bylo provedeno posouzení rizik ve vazbě na posuzovanou službu i procesy TSP. Při posouzení byly zohledněny výsledky řízení rizik TSP, popsané v dokumentech SZR_AR_Zaverecna_zprava_1v0, SZR_AR_Vyber_protio_1v1, SZR_Zbytkova_rizika_1v1, SZR_ZR_Manazerske_shrnuti_1v1. Řízení rizik vychází a je členěno dle normy ISO/IEC 27001 s tím, že je prováděno v nástroji RAMSES, založeném na metodice CRAMM.

Auditní tým neshledal ve zprávě z analýzy rizik žádnou neshodu bránící fungování TSP a jeho služeb, ani diskontinuitu v TSP identifikovaných rizicích ani navržených a realizovaných opatřeních k ošetření těchto rizik a zajištění informační bezpečnosti služby i procesů TSP.

ČASOVÉ HLEDISKO AUDITU

Harmonogram provedeného posouzení služby proběhl v následujícím časovém rámci.

Datum	Činnost
12.12.2018 11.01.2019 14.01.2019	Převzetí dokumentace TSP k auditu
17.12.2018 – 18.01.2019	Posouzení dokumentace TSP
24.01.2019 – 25.01.2019	Audit služby na místě, v rozsahu vystavení kvalifikovaných elektronických pečetí
26.01.2019 – 30.01.2019	Zpracování zprávy o posouzení shody, zapracování předaných aktualizovaných dokumentů
31.01.2019	Schválení zprávy o posouzení shody

KRITÉRIA AUDITU

Kritéria auditu jsou jednoznačně dány certifikačním schématem pro danou službu a vymezením posuzované služby a požadavků na tuto službu. Kritéria a požadavky na jejich vyhodnocení vycházejí ze stanoveného etalonu. Audit je provádět postupem dle interní metodiky certifikačního orgánu Metodika_TCOX_eIDAS, která stanovuje pracovníkům certifikačního orgánu postup, jak službu TSP dle certifikačního schématu ověřit.

Dále jsou uvedeny konkrétní kritéria a zjištění, která byla provedena během certifikace služby.

EIDAS, ČL. 5

Zpracování a ochrana údajů

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 5.1	☒	ETSI EN 319 401, kap. 7.13 c)	S	EQUAL	Dodržování zákona č. 101/2000 Sb. je doloženo popisem v dokumentaci a certifikační politikou. Dokumentace: CP kap. 9.4, Ochrana osobních údajů v I.CA, CBP kap. 3.1.7, SBP 3.1.4, Sm 10 kap. 2, 4, 6, 7, 8
eIDAS, čl. 5.2	☒		S	EQUAL	Dokumentace: CP kap. 3.3, 3.2.4, 7.1

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.*

EIDAS, ČL. 13

Odpovědnost za škodu a důkazní břemeno

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 13.1	☒		S	EQUAL	Zákazník podpisem smluvního vztahu souhlasí s politikou služby Dokumentace: CP kap. 9.8 Omezení odpovědnosti CP kap. 9.9 Záruky a odškodnění
eIDAS, čl. 13.2	☒	ETSI EN 319 401, kap. 6.2	V	EQUAL	Dokumentace / Norma: Má být vystaveno na webu www.narodni-CA.cz ETSI EN 319 401, kap 6.2 a) CP kap. 7.1.6. b) Omezení CP kap. 1.4, platnost CP kap. 6.3.2. c) CP kap. 4.1.2, 4.5.1. d) CP kap. 4.5.2. e) CP kap. 5.4.3. f) CP kap. 9.8. g) CP kap. 9.9. h) CP kap. 9.14. i) CP kap. 9.13. j) CP kap. 8, podrobnosti ve Zprávě pro uživatele (PDS). k) CP kap. 2.2. l) Vydání CP kap. 4.2.3., Zneplatnění CP kap. 4.9. CRL a OCSP CP kap. 4.10.2.
eIDAS, čl. 13.3	☒		S	EQUAL	Dokumentace: CP 9.2 Finanční odpovědnost Případné škody jsou kryty z rozpočtu SZR a následně ze státního rozpočtu ČR

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.*

EIDAS, ČL. 15

Přístupnost pro osoby se zdravotním postižením

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 15	☒	ETSI EN 319 401, kapitola 7.13 b) ETSI EN 301 549	S	EQUAL	ETSI EN 319 401, kap 7.13 (REQ-7.13-03, REQ-7.13-04) b) CP kap. 1. (možnost využití mobilní RA), dále též eIDAS článek 19.1 ETSI EN 301 549 Ze zavedených opatření vyplývá, že oblast byla posouzena, ale není jednoznačně popsáno opatření nebo nebyl předložen záznam o zamítnutí opatření Pozn.: Použít, pokud poskytovaná služba nebo konečný uživatelský produkt má být přístupný pro osoby se zdravotním postižením, viz. ETSI EN 319 401

Pozn.:

1) Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.

2) Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.

EIDAS, ČL. 19

Bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 19.1	☒	ETSI EN 319 401: kapitola 5 (hodnocení rizik) kapitola 6.3 (politika bezpečnosti informací) kapitola 7 (řízení a provoz TSP s výjimkou 7.1.1 a 7.13) kap. 7.9 (zvládání incidentů)	V	EQUAL	Zjištění / Dokumentace: Rizika řízena v nástroji RAMSES, dokumentace zpracovávána v souladu s doporučeními ISO/IEC 27002 Zbytková rizika (celá dokumentace) schválena 22.1.2019 výborem kybernetické bezpečnosti (členy vrcholové vedení SZR) Norma: **ETSI EN 319 401 (REQ-5-01, REQ-5-05)** Kap. 5. Analýza rizik je součástí ISMS. Je prováděna každoročně, protiopatření jsou vybrána a implementována, zbytková rizika jsou spočtena a manažerské shrnutí schváleno vedením NCA. Prováděno v nástroji RAMSES. Kap. 6.3 (REQ-6.3-01, REQ-6.3-02, REQ-6.3-03, REQ-6. 3-04, REQ-6. 3-05, REQ-6. 3-06) a) Celková bezpečnostní politika je hotová, analýza rizik jako součást ISMS provedena, protiopatření vybrána a implementována. Sada bezpečnostních politik dle ISO 27002 kap. 5.1.1 zahrnuje SBP, která je do požadovaných oblastí rozpracována interními směrnicemi. SZR_NCA-SBP_CA_TSA_1v0 Promítání změn SZR_NCA-SBP_CA_TSA_1v0 b) CP kap. 5.3.7 c) Naplněno dokumenty: Rozsah ISMS, Analýza rizik ISMS, Rozsah ISMS, Analýza rizik , SZR_Zmenove_rizeni_1v0 kap. 2.1, NCA - Prirucka_administratora v.1.1, kap. 7.1, SZR_Evidence_aktiv_1v0

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap 7.1.2(REQ-7.1.2-01) CP kap. 5.2, CBP kap. 3.2.2 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap. 3.1.1, NCA - Prirucka_administratora v.1.1, kap.2 Kap 7.2 (REQ-7.2-01 až REQ-7.2-16) a) CP kap. 5.3, Politika bezpečnosti informací SZR SZR_Kontrolni_cinnost_1v0, kap. 3.2. b) CP kap. 5.3, Politika bezpečnosti informací SZR, SZR_Kontrolni_cinnost_1v0, kap. 3.2. c) CP kap. 5.3.6, Zákoník práce., CPS kap. 5.3.6 - Provozní řád SZR d) plněno zvláštním dokumentem podepsaným pracovníky, viz též EN 319 401 kap. 7.1.2 e) viz EN 319 401 kap. 7.1.2, Politika bezpečnosti informací , SZR-SZR_NCA-SBP_CA_TSA_1v0, NCA - Prirucka_administratora v.1.1, CP kap. 5.2. f) Politika bezpečnosti informací SZR CP kap. 6.5.2, 6.6.2, g) CP kap. 5.3 SZR_Kontrolni_cinnost_1v0, kap. 3 h) CP kap. 5.2.1. i) CP kap. 5.2.1, Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap. 3.1.1, NCA - Prirucka_administratora v.1.1, kap. 2. j) CP kap. 5.2.1, SZR_Kontrolni_cinnost_1v0, kap. 3.2, 3.3. k) SZR_Kontrolni_cinnost_1v0, kap. 3.1. Kap 7.3.1 Politika bezpečnosti informací SZR, SZR_Evidence_aktiv_1v0, SZR_Uchovavani_dat_a_informaci_1v0, NCA - Prirucka_administratora v.1.1, kap. 7.1 Kap 7.3.2 (REQ-7.3.2-01 Politika bezpečnosti informací SZR SZR_NCA-SBP_CA_TSA_1v0, kap 3.1.7, 3.2.2, SZR_Smernice_prac_RA_1v1 kap. 7, CP, kap 7, SZR_Uchovavani_dat_a_informaci_1v0, kap.4, SZR_Dilci_spisovy_plan_1v0,

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					NCA - Zaloha dat systemu v.1.0 kap. 3.1, 2.2, Prirucka_administratora v.1.0 kap. 6.8, skartovací stroje s certifikátem NBÚ. Naplnění ISO 27002 kap. 8.3 Kap 7.4 (REQ-7.4-01 až REQ-7.4-10) a) SZR_Sitova_bezpecnost_NCA_1v0 b) Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap. 3.1.3, Prirucka_administratora v.1.0, kap. 2, 3.4, 7.1.3 c) Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, 3.1.4, Prirucka_administratora v.1.0, kap. 2, 3, 5, 6, 7. d) Dvoufaktorová autentizace, CP kap. 6.5.1, Prirucka_administratora v.1.0, kap. 3, práce s logem kap. 7.1. e) CBP kap. 3.2.4 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap.3.1.6 (podepisování logů). f) parametry OS, které byly použity Kap 7.5 (REQ-7.5-01) RAMSES (Stav protiopatření dle ISO 27002 část 10) Kap 7.6 (REQ-7.6-01 až REQ-7.6-05) Naplnění ISO 27002 kap. 11 viz Výběr protiopatření a) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0 b) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0, Prirucka_administratora v.1.0, kap. 7, CP, Striktní politika prázdného stolu není vyžadována. c) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0 d) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1 SZR_Pozarni_bezpecnost_1v0.

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap 7.7 (REQ-7.7-01 až REQ-7.7-09) a) SZR_Zmenove_rizeni_1v0, kap. 2.1. b) SZR_Zmenove_rizeni_1v0, kap. 2 c) Prirucka_administratora v.1.0, kap. 6, 6.2, 7 (Kontrola integrity provozního SW) d) NCA - Zaloha dat systemu v.1.0, kap. 3.1, 3.2, 7. e) NCA - Zaloha dat systemu v.1.0, kap. 3.1, 3.2, 7. f) Prirucka_administratora v.1.0, kap. 3, 5, 6, 7, SZR_Smernice_prac_RA_1v1 g) SZR_Kontrolni_cinnost_1v0, kap. 3.2 Prirucka_administratora v.1.0, kap. 6, 6.1, 6.2, 6.7, 7. Kap 7.8 (REQ-7.8-01 až REQ-7.8-15) a) Rozdělení subsítí, SZR_Sitova_bezpecnost_NCA_1v0, kap. 2, bod 1. b) Definována pravidla, SZR_Sitova_bezpecnost_NCA_1v0, kap. 2, body 2, 5. c) Rozdělení subsítí, SZR_Sitova_bezpecnost_NCA_1v0, kap. 2, bod 1. d) Zvláštní síť pro administraci, rozdělení subsití na firewallu, oddělení vývojového a testovacího prostředí, SZR_Sitova_bezpecnost_NCA_1v0, kap. 2, bod 4. e) Komunikace s RA probíhá šifrovaně (certifikáty), komunikace mezi firewallem oddělenými interními částmi CA je rovněž šifrovaná (CIMC). f) přepínání na záložní linku. g) Zajištěno smluvně, provádí se definovaným postupem. Na FW provádí výrobce a dodává aktualizační patche. h) SZR_Sitova_bezpecnost_NCA_1v0, kap. 2, body 7 až 9. Kap 7.9 (REQ-7.9-01 až REQ-7.9-12) a) CP kap. 5.4, Prirucka_administratora v.1.0, kap. 7.1 b) Prirucka_administratora v.1.0, kap. 6.11 (NAGIOS) c) Prirucka_administratora v.1.0, kap. 6.11 d) SZR_Bezpecnostni_incidenty_1v0, kap. 2 e) SZR_Bezpecnostni_incidenty_1v0, kap. 2.2.2 - hlásit okamžitě po zjištění f) SZR _Bezpecnostni_incidenty_1v0.p kap 2.2.4 - informování subjektů

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					g) Prirucka_administratora v.1.0, kap. 6.11 (NAGIOS), příslušné osoby jsou v případě kritických bezpečnostních událostí informovány (ředitel SZR). SZR_Bezpecnostni_incidenty_1v0, kap. 2.2.2 h) Prirucka_administratora v.1.0, kap. 6.7. i) SZR_Bezpecnostni_incidenty_1v0, kap. 2.2.2, 2.2.4. Kap 7.10 (REQ-7.10-01 až REQ-7.10-08) a) Listinný archiv, auditní záznamy s el. podpisem, řízení přístupu na server s logy (role), řízení fyzického přístupu k archivním kopiím. b) Papírové dokumenty v archivu SZR, záloha elektronických logů v trezoru v místnosti SZR s řízeným přístupem - CP kap. 5.4.4. c) V souladu s aktuální legislativou, mj. CP kap. 9.4.7. d) Čas události je součástí logového záznamu - CPS kap. 5.4.1. , Prirucka_administratora v.1.0, kap. 7.1.4. Přesnost systémového času a frekvence kontroly synchronizace je řešena současně s požadavky na vydávání časových razítek. SZR_NCA-SBP_CA_TSA_1v0, kap. 3.4.2, Prirucka_administratora v.1.0, kap. 6 - čas se bere z NTP serveru (GPS, Galileo) e) CP kap. 5.4.3. f) Paralelní ukládání médií CP kap.5.1.6, Integrita chráněna elektronickými podpisy (Prirucka_administratora v.1.0, kap. 7.1.4). Kap 7.11 (REQ-7.11-01, REQ-7.11-02) SZR_Rizeni_kontinuity_1v0, NCA -Obnova systemu CA v.1.1, NCA - Premisteni systemu CA v.1.0 Kap 7.12 (REQ-7.12-01, REQ-7.12-11) a) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7. b) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7. c) CP kap. 9.2.1, 9.2.2 d) CPS kap. 5.8, SZR_Ukonceni_cinnosti_1v1, kap. 2.4, 2.6 e) _Ukonceni_cinnosti_1v0, kap. 2.6

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 19.2	☒	ETSI EN 319 401: kapitola 7.9 (zvládání incidentů, zejména písm. e) a f))	V	EQUAL	Kap 7.9 (REQ-7.09-01 až REQ-7.09-11) a) CP kap. 5.4 b) Prirucka_administratora v.1.0, kap. 6.11 (NAGIOS, program Monit), IPS na FW - logování a reportování c) Prirucka_administratora v.1.0, kap. 6.11 d) SZR_Bezpecnostni_incidenty_1v0, kap. 2 e) SZR_Bezpecnostni_incidenty_1v0, kap. 2.2.2 – má být nahlašováno okamžitě po zjištění f) SZR _Bezpecnostni_incidenty_1v0.p kap 2.2.4 - informování subjektů. g) Prirucka_administratora v.1.0, kap. 6.11 (SW NAGIOS), příslušné osoby jsou v případě kritických bezpečnostních událostí informovány ředitelem SZR. h) Prirucka_administratora v.1.0, kap. 6.7. i) SZR_Bezpecnostni_incidenty_1v0, kap. 2.2.2, 2.2.4. ***Pozn.: zejména písm. e), f)***
eIDAS, čl. 19.3	☐		N/A	EQUAL	Irelevantní.
eIDAS, čl. 19.4	☐		N/A	EQUAL	Irelevantní.

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.*

EIDAS, ČL. 24

Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 24.1	☒		S	EQUAL	Ověřováno na RA Ověřeno pomocí dvou dokladů totožnost (OP, ŘP, pas), plné moci a souhlasy podle oprávněných osob uvedených ve smlouvě Norma: ETSI EN 319 411-2, Kap 6.2.2 a) – e) Požadavky na ověření identity uvedeny v CP, kap. 3.2.3., ověřeno fyzickou přítomností žadatele, nebo notářsky ověřenou plnou mocí. f) – g) Požadavky na ověření identity právnické osoby uvedeny v kap. 3.2.2. h) – k) SSL certifikáty QCP-w se nevydávají – NERELEVANTNÍ l) Smlouva o vydání certifikátu je vždy tištěna a žadatelem podepsána m) CP kap. 3.2.3. n) Povinně zadávána adresa. o) - p) Pravidelně prováděné audity. q) SZR_Smernice_prac_RA_1v1 ETSI EN 319 411-2, Kap 6.2.3 Re-keying po zneplatnění certifikátu se neprovádí (vydává se nový certifikát). Výměna veřejného klíče jen před vypršením platnosti předchozího certifikátu viz CP kap. 4.7. a) Po zneplatnění certifikátu nelze provést. Žádost může být podepsána platným klíčem z původního certifikátu. Kontrolovat správnost údajů v certifikátu je povinen žadatel/držitel klíče – CP kap. 4.1.2. b) Po dobu platnosti certifikátu platí podmínky, za kterých byl certifikát vydán (CP platí minimálně po dobu platnosti posledního, podle ní vydaného, certifikátu, CP kap. 9.10.1). c) viz kap. 6.2.2 normy výše

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 24.2	☒	a) ETSI EN 319 401, kap. 6.1 g), h) b) ETSI EN 319 401, kap. 7.1.2 (oddělení povinností), 7.2 (lidské zdroje) c) ETSI EN 319 401, kap. 7.1.1c),d) (spolehlivost organizace) d) ETSI EN 319 401, kap. 6.2 (smluvní podmínky) e) CEN/TS 419 261 f) CEN/TS 419 261 g) ETSI EN 319 401: kap. 5 (posouzení rizik) kap. 6.3 (politika bezp.informací) kap. 7.4 d) e) (řízení přístupu) kap. 7.6 (fyzická bezpečnost) h) ETSI EN 319 401: kap. 7.10 (sběr důkazů) kap. 7.12 (ukončení činnosti TSP) i) ETSI EN 319 401 kap. 7.12 (ukončení činnosti TSP)	V	EQUAL	**Norma:** **a)** ETSI EN 319 401, kap 6.1. (REQ-6.01-01 až REQ-6.01-11) a) CPS bude vystavena na webu SZR (kap. 2.3), struktura dle RFC 3647. b) Využívány i smluvní RA, jejich činnost se řídí smlouvou (kap. 1.3.2). c) bude vystaveno na webu SZR, k dispozici veřejnosti 24/7 (kap. 2.4). d) Ředitel SZR (CP kap. 1.5.4). e) Ověřováno interním monitoringem a pravidelnými (minimálně jednou ročně) audity dle EN 319403 prováděnými subjektem posuzování shody (CAB) f) CP kap. 6.6.2, 6.6.3 a 8. g) CP kap. 2.3. h) CP kap. 5.8. **b)** ETSI EN 319 401, kap. 7.1.2 (REQ-7.1.2-01) CP kap. 5.2, SZR_NCA-SBP_CA_TSA_1v0, Prirucka_administratora v.1.0, kap.2 ETSI EN 319 401 kap. 7.2 (REQ-7.2-01 až REQ-7.2-17) a) CP kap. 5.3, SZR_Kontrolni_cinnost_1v0, kap. 3 b) CP kap. 5.3, SZR_Kontrolni_cinnost_1v0, kap. 3.2, 2.2.2 c) kap. 5.3.6, Zákoník práce., CPS kap. 5.3.6, Provozní řád SZR. d) splněno samostatným záznamem podepsaným pracovníky, viz též EN 319 401 kap. 7.1.2 e) viz EN 319 401 kap. 7.1.2, CBP 3.1.1 (politika přístupu - nejmenší privilegia), CBP 3.5 (popisy, znalosti) Politika bezpečnosti informací SZR, CP kap. 5.2. f) CBP kap. 2.4 Politika bezpečnosti informací SZR, CP kap. 6.6.2 g) kap. 5.3, SZR_Kontrolni_cinnost_1v0, kap. 3 h) CP kap. 5.2.1. i) CP kap. 5.2.1, CBP kap. 3.2.2 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap. 3.1.1, Prirucka_administratora v.1.0, kap. 2. j) kap. 5.2.1, SZR_Kontrolni_cinnost_1v0, kap.3. k) SZR_Kontrolni_cinnost_1v0 kap.3.3.

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					c) ETSI EN 319 401, kap. 7.1.1 (REQ-7.1.1-02 až REQ-7.1.1-07) a) CP kap. 1. b) CP kap. 1. c) CP kap. 9.2 d) CP kap. 9.2.2. e) kap. 9.13. f) CP kap. 5.3.7 **d)** Dokumentace / Norma: ETSI EN 319 401, Kap 6.2. (REQ-6.2-01) vystaveno na webu narodni-CA.cz (SZR) a) CP kap. 7.1.6. b) omezení CP kap. 1.4, platnost CP kap. 6.3.2. c) CP kap. 4.1.2, 4.5.1. d) CP kap. 4.5.2. e) CP kap. 5.4.3. f) CP kap. 9.8. g) CP kap. 9.14 h) CP kap. 9.13. i) CP kap. 8, podrobnosti ve Zprávě pro uživatele (PDS) j) CP kap. 2.2. k) CP kap. 4.2.3. lhůty pro vydání, CP kap. 4.9. pravidla pro zneplatnění, CP kap. 4.10.2. pravidla pro CRL a OCSP CP, SZR_CPS_RSA_1v01, SZR_CP_PDS_RSA_1v1, ZR_CP_PDS_RSA_EN_1v0 **e), f)** Pr CEN TS 419 261 **Popsáno a řešeno normou** ETSI EN 319 401, kap. 7, viz čl. 19 eIDAS

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					g) ETSI EN 319 401 Kap. 5. (REQ-5-01 až REQ-5 -05) Analýza rizik je součástí systému řízení NCA a SZR. Je prováděna každoročně, protiopatření jsou vybrána a implementována, zbytková rizika jsou spočtena a manažerské shrnutí schváleno vedením NCA (SZR). Analýza prováděna v nástroji RAMSES. Kap. 6.3 (REQ-6.3-01 až REQ-6. 3-10) SZR_NCA-SBP_CA_TSA_1v0 Změny SZR_NCA-SBP_CA_TSA_1v0 přenášeny do příslušné CP - zveřejňování na webu narodini-CA.cz (SZR) a) Celková bezpečnostní politika Politika bezpečnosti informací SZR je hotová SZR_NCA-SBP_CA_TSA_1v0, analýza rizik jako součást systému řízení provedena, protiopatření vybrána a implementována. Sada bezpečnostních politik dle ISO 27002 kap. 5.1.1 zahrnuje SZR_NCA-SBP_CA_TSA_1v0, která je dále rozpracována interními směrnicemi. b) CP kap. 5.3.7 c) Naplněno dokumenty: Rozsah ISMS, Analýza rizik , SZR_Zmenove_rizeni_1v0 kap. 2.1, NCA - Prirucka_administratora v.1.1, kap. 7.1, SZR_Evidence_aktiv_1v0 Kap 7.4 a) SZR_Sitova_bezpecnost_NCA_1v0 b) CBP kap. 3.1.5 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0, kap. 3.1.3, Prirucka_administratora v.1.0, kap. 2, 3.4, 7.1.3. c) CBP kap. 3.1.7, Politika bezpečnosti informací SZR, SBP_CA_TSA_1v0 kap. 3.1.4, Prirucka_administratora v.1.0 kap. 2, 3, 5, 6,78. d) Dvoufaktorová autentizace, CP kap. 6.5.1, Prirucka_administratora v.1.0 kap. 3, práce s logem kap. 7.1. e) CBP kap. 3.2.4 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA_1v0 kap. 3.1.6 - podepisování logů. f) vlastnosti OS, které byly použity

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap 7.6 (REQ-7.6-01 až REQ-7.6-05) Naplnění ISO 27002 kap. 11 viz Výběr protiopatření a) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0. b) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0, Prirucka_administratora v.1.0 kap. 7, CP, Politika prázdného stolu není vyžadována. c) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1, SZR_Pozarni_bezpecnost_1v0 d) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v1 SZR_Pozarni_bezpecnost_1v0. **h)** ETSI EN 319 401 Kap 7.10 (REQ-7.10-01 až REQ-7.10-08, REQ-7.13-05) a) Listinný archiv, auditní záznamy s el. podpisem, řízení přístupu na server s logy (role), řízení fyzického přístupu k archivním kopiím. b) Papírové dokumenty v archivu SZR, záloha elektronických logů v trezoru v místnosti SZR s řízeným přístupem - CP kap. 5.4.4. c) V souladu s aktuální legislativou, mj. CP kap. 9.4.7. d) Čas události je součástí logového záznamu - CPS kap. 5.4.1. , Prirucka_administratora v.1.0 kap. 7.1.4. Přesnost systémového času a frekvence kontroly synchronizace je spojena s postupy pro vydávání časových razítek. SZR_NCA-SBP_CA_TSA_1v0 kap. 3.4.2, čas se bere z NTP serveru (GPS, Galileo) e) CP kap. 5.4.3. f) Paralelní ukládání médií (CP kap.5.1.6). Integrita chráněna elektronickými podpisy (Prirucka_administratora v.1.0 kap. 7.1.4). Kap 7.12 (REQ-7.12-01 až REQ-7.10-11) a) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7.

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					b) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7. c) CP kap. 9.2.1, 9.2.2 d) CPS kap. 5.8, _Ukonceni_cinnosti_1v0 kap. 2.4, 2.6 e) _Ukonceni_cinnosti_1v0 - kap. 2.6 **i)** Kap 7.12 (REQ-7.12-01 až REQ-7.10-11) a) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7. b) SZR_Ukonceni_cinnosti_1v1 kap. 2.4, 2.5, 2.6, 2.7. c) CP kap. 9.2.1, 9.2.2 d) CPS kap. 5.8, _Ukonceni_cinnosti_1v0 kap. 2.4, 2.6 e) SZR _Ukonceni_cinnosti_1v0 - kap. 2.6 **j)** ETSI EN 319 401, kap 7.13 (REQ-7.13-01 až REQ-7.13-05) a) Požadavky právního systému zahrnuty v interních dokumentech, audit plnění prokazuje b) CP kap. 1. možnost využití mobilní RA). c) CP kap. 9.4, Ochrana osobních údajů v SZR, CBP kap. 3.1.7, SZR_NCA-SBP_CA_TSA_1v0 kap. 3.1.4, NCA - Prirucka_administratora v.1.1 kap. 2, 3, 5, 6, 7 **k)** ETSI EN 319 411-1, kap 6.1 a) CP kap. 4.3.2. b) CP kap. 4.4.2 a 4.4.3. c) Bude vystaveno na webu SZR d) Uvedeno v odpovídající politice. e) Bude vystaveno na webu SZR, dostupné 24x7. f) Nerelevantní, certifikáty jsou PTC. g) Informace (CP, CPS) budou vystaveny na webu SZR

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 24.3	☒		V	EQUAL	Norma: ETSI EN 319 411-1. Kap 6.2.4 a) CP kap. 4.9.3., potvrzování není vyžadováno (osobní přítomnost na RA, elektronický podpis, heslo pro zneplatnění). Pozastavení (CP kap 4.9) ani odklad doby zneplatnění (CP kap 4.9.4) nelze. Podmínky zneplatnění v CP kap. 4.9.1. CP kap. 4.9.5. CRL vydáván bezprostředně po zneplatnění certifikátu - CP kap. 4.9.7 Příručka administrátora kap. 6.13. b) CP kap. 4.9.3, 4.9.5. c) CP kap. 4.9.3.
eIDAS, čl. 24.4	☒		V	EQUAL	Norma: ETSI EN 319 411-1. Kap 6.3.10 a) CP kap 4.10.2., CPS 7.3. b) CP kap 4.10.2., CPS 7.3. c) Informace je uveřejňována po dobu platnosti certifikátu. d) CP kap. 4.10.1. e) CP kap. 4.10.1. f) CP kap. 4.9.7 - CRL vydáván po každém zneplatnění. g) Veřejně přístupné v Internetu
eIDAS, čl. 24.5	☒		S	EQUAL	-

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.*

EIDAS, ČL. 38, PŘÍLOHA III

Kvalifikované certifikáty pro elektronické pečetě

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 38.1, Příloha III	☒	ETSI EN 319 411-2	S	EQUAL TEST	Ověřeno vůči vystavené kvalifikované elektronické pečeti. Klíčový pár vygenerován na QSCD HSM Thales nShield Connect 1500+ CC Důkaz: Čestné prohlášení pracovníka SZR, že klíčový pár byl za jeho přítomnosti generován v daném HSM. Na základě čestného prohlášení (podepsaného pracovníkem SZR před operátorem RA) a přinesené žádosti pracovník RA, který ověří identitu pracovníka SZR, vystaví kvalifikovaný certifikát pro ověřování kvalifikovaných elektronických pečetí. Pracovník SZR nahraje vydaný certifikát do HSM. Kvalifikované certifikáty pro ověřování elektronické pečeti jsou ve shodě s certifikační politikou a naplňují požadavky Přílohy III eIDAS. **Informace o vydaném certifikátu:** Seriové číslo: 2B04 Číslo RA: AA Vydán: 23.01.2019 9.11:01 GMT Reg. číslo žádosti: AA00000017 Vystavitel: Test NCA SubCA1 CA/RSA 11/2018 Kořenová autorita: Test NCA Root CA/RSA 11/2018 V prosinci 2018 vygenerována sada klíčů a certifikáty pro provozní prostředí **Kořenová certifikační autorita SZR** (vydává certifikáty podřízeným CA a svému OCSP responderu)

Pole	Obsah
SerialNumber	1 (0x1)
Issuer	
commonName	NCA Root CA/RSA 12/2018
organizationName	Správa základních registrů

organizationIdentifier	NTRCZ-72054506
countryName	CZ
Subject	
commonName	NCA Root CA/RSA 12/2018
organizationName	Správa základních registrů
organizationIdentifier	NTRCZ-72054506
countryName	CZ

Podřízená certifikační autorita SZR
(vydává certifikáty koncovým klientům bezpečnostních složek, časovým serverům a svému OCSP responderu)

Pole	**Obsah**
SerialNumber	1001 (**0x3e9**)
Issuer	
commonName	NCA Root CA/RSA 12/2018
organizationName	Správa základních registrů
organizationIdentifier	NTRCZ-72054506
countryName	CZ
Subject	
commonName	NCA SubCA1/RSA 12/2018
organizationName	Správa základních registrů
organizationIdentifier	NTRCZ-72054506
countryName	CZ

					Ověření údajů z žádosti a údajů zadaných operátorem RA se provádí automatizovaně včetně schválení vystavení certifikátu. Dokumentace: CP Norma: ETSI EN 319 411-2 Kap. 6.2.1 V CP je deklarována shoda s RFC5280 a profilem (příslušná část ETSI EN 319 412). Shoda prokazována auditem. Kap. 6.2.2 a) CP kap. 3.2.3. b) CP kap. 3.2.3. c) CP kap. 3.2.3. d) CP kap. 3.2.3. e) CP kap. 3.2.3. f) CP kap. 3.2.2. g) CP kap. 3.2.2. h) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván. i) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván. j) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván. k) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván. l) Smlouva o vydání certifikátu. Kap. 6.3.9 a) CP kap 4.9.3 b) CP kap. 4.6 a 4.9., obnovení certifikátu ani pozastavení platnosti nejsou poskytovány. c) CP kap. 4.9.7., CP kap. 7.2 - profil CRL. d) Nerelevantní, není DVCP, OVCP e) Nerelevantní, není EVCP. f) CARL vydáváno jednou za půl roku, platnost je rok. CP kořenové CA (CP_Root_RSA_1v00.pdf), kap. 4.9.7. g) Není relevantní, křížové certifikáty nejsou vydávány.

					Kap. 6.6.1 a) CP kap. 7.1, X.509 v 3. b) CP kap. 7.1. c) CP kap. 7.1. d) CP kap. 7.1. e) CP kap. 7.1. f) CP kap. 7.1. g) CP kap. 7.1. h) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván i) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván j) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván k) Obsahuje OID dle ETSI EN 319 411-2 i OID SZR
eIDAS, čl. 38.2	☒		S	EQUAL	Splněno naplněním požadavků v čl. 38.1 a Příloze III.
eIDAS, čl. 38.3	☒	ETSI EN 319 411-2	S	EQUAL	Dokumentace: CP Norma: ETSI EN 319 411-2 Kap. 6.3.9 a) CP kap 4.9.3 b) CP kap. 4.6 a 4.9., obnovení certifikátu ani pozastavení platnosti nejsou poskytovány. c) CP kap. 4.9.7., CP kap. 7.2 - profil CRL. d) Nerelevantní, není DVCP, OVCP e) Nerelevantní, není EVCP. f) CARL vydáváno jednou za půl roku, platnost je rok. CP kořenové CA (SZR_CP_Root_RSA_1v01.pdf), kap. 4.9.7. g) Není relevantní, křížové certifikáty nejsou vydávány. Kap. 6.6.1 a) CP kap. 7.1, X.509 v 3. b) CP kap. 7.1. c) CP kap. 7.1.

					d) CP kap. 7.1. e) CP kap. 7.1. f) CP kap. 7.1. g) CP kap. 7.1. h) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván i) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván j) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván k) Obsahuje OID dle ETSI EN 319 411-2 i OID SZR
eIDAS, čl. 38.4	☒	ETSI EN 319 411-2	S	EQUAL	Certifikát kvalifikované elektronické pečeti může být pouze zneplatněn a to bez jakékoli možnosti jeho následného obnovení. Dokumentace: CP Norma: ETSI EN 319 411-2 Kap. 6.3.9 a) CP kap 4.9.3 b) CP kap. 4.6 a 4.9., obnovení certifikátu ani pozastavení platnosti nejsou poskytovány. c) CP kap. 4.9.7., CP kap. 7.2 - profil CRL. d) Nerelevantní, není DVCP, OVCP e) Nerelevantní, není EVCP. f) CARL je vydáván po každém zneplatnění certifikátu a dále v pravidelných intervalech, nejvýše jeden rok od vydání předchozího CARL. CP kořenové CA (CP_Root_RSA_1v00.pdf), kap. 4.9.7. g) Není relevantní, křížové certifikáty nejsou vydávány. Kap. 6.6.1 a) CP kap. 7.1, X.509 v 3. b) CP kap. 7.1. c) CP kap. 7.1. d) CP kap. 7.1. e) CP kap. 7.1. f) CP kap. 7.1. g) CP kap. 7.1.

					h) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván i) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván j) Nerelevantní, tento typ certifikátů (QCP-w) nevydáván k) Obsahuje OID dle ETSI EN 319 411-2 i OID SZR
eIDAS, čl. 38.5	☒	ETSI EN 319 411-2	S	EQUAL	Není aplikováno. Certifikát kvalifikované elektronické pečeti může být pouze zneplatněn a to bez jakékoli možnosti jeho následného obnovení. Dokumentace: CP
eIDAS, čl. 38.6	☒		S	EQUAL	Prováděcí rozhodnutí komise (EU) 2016/650 naplněno nastaveným systémem řízení a opatřeními a ISMS.

Pozn.:

1) *Sloupec Ano: zaškrtnout pokud hodnocená funkcionalita byla součástí posouzení, analogicky sloupec Ne pokud nebyla.*
2) *Sloupec Metrika: určuje metriku, která je stanovena k vyhodnocení daného kritéria. Uvádí se označení metriky dle tabulky „Výčet použitých metrik“.*

ZÁVĚREČNÁ ČÁST PROTOKOLU

Posouzení provedl *(hodnotitel)*:	
Datum předání zprávy k přezkoumání:	30.01.2019
Protokol přezkoumal *(přezkoumavatel)*:	
Datum přezkoumání:	31.01.2019
Podpis přezkoumavatele:	

METRIKA ROZHODNUTÍ

Rozhodnutí bylo provedeno na základě všech dílčích výsledků zjištění uvedených v kap. Kritéria auditu. Při výskytu výroku „NESHODA“ je celkový výsledek stanoven jako **„Posuzovaná služba NENÍ VE SHODĚ s příslušnými požadavky Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014“** a certifikát **NENÍ VYSTAVEN**. V ostatních případech je celkový výsledek stanoven jako **„Posuzovaná služba je VE SHODĚ s příslušnými požadavky Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014“** a certifikát **JE VYSTAVEN**.

POZNÁMKY

Záznamy o konkrétních testech (žádosti, certifikáty) nejsou součástí této zprávy z důvodu reálných osobních údajů v nich obsažených. Tyto záznamy jsou uloženy v certifikačním orgánu jako důkaz o správnosti výroků auditu a výsledku certifikace.

PŘÍLOHA CERTIFIKAČNÍHO PROTOKOLU – PODMÍNKY UŽÍVÁNÍ CERTIFIKÁTU SHODY

1.1 PODMÍNKY PRO UŽÍVÁNÍ CERTIFIKÁTU TAYLLORCOX PCEB

Tato kapitola upravuje podmínky pro užívání certifikátu shody vydaného certifikačním orgánem.

a) ***Certifikát*** je listina vydaná certifikačního orgánu **TAYLLORCOX PCEB** pro TSP, která potvrzuje, že specifikovaná služba vyhovuje normám a jiným normativním dokumentům v ní uvedených. Obsahuje:

1. Název a adresu objednatele
2. Rozsah udělené certifikace, který je vymezen:
    a) názvem (včetně verze) certifikované služby

b) specifikací norem, případně dalších normativních dokumentů, podle kterých byla služba certifikována

c) příslušným certifikačním systémem

3. Datum platnosti, popřípadě i datum účinnosti certifikátu, je-li pozdější.
4. Doba platnosti certifikátu
5. Datum a podpis oprávněné osoby k uvolňování výstupů z certifikace
6. Hologram

1.2 PODMÍNKY REPRODUKCE NEBO ZAČLEŇOVÁNÍ VÝSTUPNÍCH DOKUMENTŮ CERTIFIKAČNÍHO ORGÁNU DO MATERIÁLŮ TSP

1. Výstupním dokumentem certifikačního orgánu se v této příloze rozumí:
    - certifikát (je-li výsledek ověřování pozitivní)
    - certifikační protokol

2. Výstupní dokument nesmí objednatel používat ve svých materiálech (zejména propagačních) způsobem, který navozuje mylný dojem, že produkt byl certifikován v jiném certifikačním systému, podle jiných norem nebo v jiném rozsahu, než je uvedeno na certifikátu.

3. Výstupní dokument musí objednatel ve svém materiálu reprodukovat nebo začlenit vždy v úplném rozsahu. Výjimku tvoří certifikát, který může objednatel reprodukovat samostatně, při dodržení povinností podle odst. 2.

1.3 PODMÍNKY PRO UDĚLOVÁNÍ, UDRŽOVÁNÍ, POZASTAVOVÁNÍ, ROZŠIŘOVÁNÍ, OBNOVOVÁNÍ A ODNÍMÁNÍ CERTIFIKÁTU

Udělování: Certifikát může být udělen pouze za předpokladu splnění všech hodnocených kritérií.

Udržování: Udržování je prováděno v souladu s normativním/legislativním rámcem a s požadavky danými certifikačním schématem certifikačního orgánu pro daný předmět certifikace, které je uvedeno na certifikátu.

Pozastavování: Pozastavování platnosti certifikátu je prováděno na základě zjištění při kontrole, po upozornění certifikačního orgánu na neadekvátní užívání certifikátu nebo značky shody objednatelem nebo při porušení smluvních podmínek. O pozastavení je objednatel informován písemnou formou, kde je mu sdělen důvod pozastavení a termín na odstranění.

Rozšiřování: Rozšiřování certifikační orgán neprovádí. Každý požadavek na rozšíření rozsahu certifikace je řešen novým certifikačním případem.

Obnovování: Obnovování platnosti certifikátu je prováděno na základě odstranění všech důvodů pro pozastavení certifikátu v určené době.

Odnímání: Odnímání je prováděno při ukončení platnosti certifikátu nebo při nesplnění podmínek daných při pozastavení platnosti certifikátu nebo při závažném porušení smluvních podmínek.