CERTIFIKAČNÍ PROTOKOL

Posouzení provedl:	
ID protokolu:	PCEB 19/01/03
ID certifikátu:	PCEB 19/01/03
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 elektronických časových razítek s Nařízením Evropského Parlamentu a Rady (EU) č. 910/2014.
Posuzovaná služba:	NCA - služba vydávání kvalifikovaných elektronických časových razítek
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 elektronických časových razítek
Verze posuzované služby	OID 1.2.203.72054506.10.1.50.1.0

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 42 – Požadavky na kvalifikovaná elektronická časová razítka

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	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_OCSP_RSA_1v01	1.01	NCA - Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA)
10	SZR_CP_TSA_RSA_1v01	1.01	NCA - Certifikační politika vydávání certifikátů pro systém TSA (kryptografie RSA)
11	SZR_CPS_RSA_1v01	1.01	NCA Certifikační prováděcí Směrnice (kryptografie RSA)
12	SZR_PDS_TSA_1v1	1.1	NCA Zpráva pro uživatele TSA
13	SZR_Rizeni_fyz_pristupu_1v1	1.1	NCA Řízení fyzického přístupu do provozních prostor (Návrh směrnice)
14	SZR_Ukonceni_cinnosti_1v1	1.1	NCA Ukončení činnosti služeb CA, TSA
15	SZR_Pozarni_bezpecnost_1v0	1.0	NCA Požární bezpečnost (Návrh na doplnění stávající dokumentace SZR)
16	SZR_NCA-HSM_PrivateServer-1v0	1.0	NCA HSM PrivateServer Směrnice pro správu
17	SZR-NCA-HSM_Postupy_instalace_a_správy_1v00	1.0	HSM PrivateServer v.5 Postupy instalace a správy
18	SZR_NCA-HSM-	1.0	NCA HSM PrivateServer

ID	Název souboru (pdf)	Verze	Název dokumentu
	Postupy_generování_klíčů_a_certifikátů_CA-1v00		Postupy generování klíčů a certifikátů CA
19	SZR_Uchovavani_dat_a_informaci_1v0	1.0	NCA Uchovávání dat a informací
20	SZR_Kontrolni_cinnost_1v0	1.0	NCA Kontrolní činnost, bezúhonnost a odbornost
21	SZR_Zmenove_rizeni_1v0	1.0	NCA Změnové řízení (Návrh na doplnění stávajícího dokumentu SZR)
22	SZR_Bezpecnostni_incidenty_1v0	1.0	NCA Bezpečnostní incidenty (Návrh na doplnění stávajícího dokumentu SZR)
23	SZR_Sitova_bezpecnost_NCA_1v0	1.0	NCA Síťová bezpečnost (Návrh na doplnění stávajícího dokumentu SZR)
24	SZR_Projekt_fyzicke_bezpecnosti_1v0	1.0	NCA Projekt fyzické bezpečnosti prostor (Návrh na doplnění stávající dokumentace SZR)
25	SZR_Dilci_spisovy_plan_1v0	1.0	NCA Spisový a skartační plán (Návrh na doplnění stávající dokumentace SZR)
26	SZR_Spisovy_a_skartacni_rad_1v0	1.0	NCA Spisový a skartační řád (Návrh na doplnění stávající dokumentace SZR)
27	SZR_Evidence_aktiv_1v0	1.0	NCA Evidence aktiv (Návrh na doplnění stávající dokumentace SZR)
28	NCA - Premisteni systemu CA v.1.0	1.0	NCA Přemístnění systémů CA, TSA
29	NCA - Sprava TSS v.1.0	1.0	NCA - Správa TSS
30	NCA - Zaloha dat systemu v.1.0	1.0	NCA Záloha dat systémů
31	NCA -Obnova systemu CA v.1.1	1.1	NCA Obnova systémů CA
32	NCA - Prirucka_administratora_1v1	1.1	NCA Příručka administrátora systémů CA, TSA
33	SZR_Smernice_razitka_1v01	1.01	NCA - Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA (kryptografie RSA)
34	SZR_Politika_razitka_1v01	1.01	NCA - Politika vydávání kvalifikovaných elektronických časových razítek systémem TSA (kryptografie RSA)
35	SZR_CP_PDS_RSA_1v1	1.1	NCA Zpráva pro uživatele CA
36	SZR_CP_PDS_RSA_EN_1v1	1.1	NCA CA PKI Disclosure Statement
37	NCA - Sprava TSS v.1.0.pdf	1.0	NCA - Sprava TSS v.1.0.pdf

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	HSM PSV 5.0 /5.0.3 (HSM podepisující certifikáty vydané TSP) HPE ProLiant DL380 Gen10 8SFF CTO Server HSM – Thales nShield F3 500+ PCI Express (karta umístěna v časových serverech) HW administrátora systému TSA (PC) Meinberg M300/GPS NTP server Meinberg M300/GNS NTP server
Použitý SW TSP pro audit	APP serverové části služby – provozní pracoviště (Na Vápence i na lokality zvláštních složek) Adobe Acrobat Reader DC ASN.1 Editor

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 319 401 V2.1.1 (2016-02) / ETSI EN 319 401 V2.2.1 (2018-04) ETSI EN 319 421 V1.1.1 (2016-03) ETSI EN 319 422 V1.1.1 (2016-03) Řada norem EN 419 2XX (Protection Profiles) ANSSI DCSSI-PP 2008/7 (profil) CEN/TS 419261:2015 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) 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. 42	☒	☐	S	EQUAL, TEST	Kritéria etalonu eIDAS byla naplněna

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 elektronických časových razítek 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
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.
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

1.4 DOPLŇUJÍCÍ KOMENTÁŘE A UPŘESNĚNÍ

Služba **NCA - služba vydávání kvalifikovaných elektronických časových razítek** umožňuje vydávat kvalifikovaná elektronická časová razítka v souladu s eIDAS.

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. 13.2	Provázat web SZR a www.narodni-CA.cz pro efektivní zveřejňování informací NCA na jednom místě
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. 42	Při spuštění služby do ostrého provozu vystavit kvalifikovaný certifikát pro elektronickou pečeť časového serveru 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 30.01.2019	Převzetí dokumentace TSP k auditu
17.12.2018 – 18.01.2019 30.01.2019	Posouzení dokumentace TSP
24.01.2019 – 25.01.2019	Audit služby na místě, v rozsahu vydání časového razítka
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)	V	EQUAL	Dodržování zákona č. 101/2000 Sb. a GDPR je doloženo popisem v dokumentaci a certifikační politikou. Chybí provázání na GDPR procesy SZR. Dokumentace: SZR_POLITIKA_RAZITKA kap. 6.5.4 Norma: ETSI EN 319 401, kap. 7.13 c) c) TSU nepracuje s osobními daty
eIDAS, čl. 5.2	☒		S	EQUAL	Pseudonymy nejsou používány. Dokumentace: SZR_POLITIKA_RAZITKA kap. 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 souhlasí s riziky souhlasem s politikou služby při uzavírání smluvního vztahu. Škody jsou kryty z rozpočtu SZR, případně ze státního rozpočtu ČR. Dokumentace: SZR_POLITIKA_RAZITKA kap. 5.4
eIDAS, čl. 13.2	☒	ETSI EN 319 401, kap. 6.2	V	EQUAL	Zákazník je informován o pravidlech v politice TSA. Dokumentace: SZR_POLITIKA_RAZITKA kap. 5 SZR_POLITIKA_RAZITKA kap. 4.1 Norma: ETSI EN 319 401, Kap. 6.2 (REQ-6.2-01, REQ-6.2-02) Připraveno, bude vystaveno na webu SZR Omezení jsou součástí veřejné politiky TSA a info bude vystaveno na webu SZR a) OID TSA policy, b) SZR_POLITIKA_RAZITKA, kap.5.1.1, c) SZR_POLITIKA_RAZITKA, kap.5.2, d) SZR_POLITIKA_RAZITKA, kap.5.3, e) SZR_POLITIKA_RAZITKA, kap.6.4.13, SZR_SMERNICE_RAZITKA f) SZR_POLITIKA_RAZITKA, kap.5.4, g) omezení ručení za škody - kap.6.5.2, h) SZR_POLITIKA_RAZITKA, kap.6.5.10, i) SZR_POLITIKA_RAZITKA, kap.6.5.9, j) certifikát o shodě na webu SZR, k) kontakty budou na webu SZR, l) dostupnost - SZR_POLITIKA_RAZITKA, kap.5.1.1 (nepřetržitě až na poruchy a odstávky)

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 13.3	☒		S	EQUAL	Případné škody jsou kryty z rozpočtu SZR a následně ze státního rozpočtu ČR. Dokumentace: SZR_POLITIKA_RAZITKA kap. 5.4

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	Pro fyzické poskytování služby není bod relevantní. Dokumentace: SZR_POLITIKA_RAZITKA kap. 5 Norma: ETSI EN 319 401, kapitola 7.13 b) – nerelevantní, požadavek na službu je součástí klientské aplikace nebo je sestaven pomocí knihoven jako elektronický požadavek pro automatizované využití služby

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)	S	EQUAL	AR pro TSP služby SZR zpracována společně s ostatními službami. Norma: **ETSI EN 319 401** Kap. 5. (REQ-5-01 až REQ-5 -05) Analýza rizik je součástí ISMS. Je prováděna každoročně, protiopatření jsou vybrána a implementována, zbytková rizika jsou spočtena a manažerské shrnutí schváleno vedením SZR. Prováděno v nástroji RAMSES. Kap. 6.3 (REQ-6.3-01, REQ-6.3-02) SZR_NCA-SBP_CA_TSA Promítání změn SZR_NCA-SBP_CA_TSA do příslušné CP - zveřejňování na webu SZR Kap. 6.3 (REQ-6.3-03 až REQ-6. 3-06, REQ-6.3-07-10) a) Politika bezpečnosti informací SZR, analýza rizik jako součást ISMS provedena, protiopatření vybrána a implementována. Sada bezpečnostních politik dle ISO 27002 kap. 5.1.1 obsahuje SZR_NCA-SBP_CA_TSA, která je doplněna interními směrnicemi. b) CP_TSA kap. 5.3.7 c) Naplněno dokumenty: Rozsah ISMS, Analýza rizik , SZR_Zmenove_rizeni_1v0 kap. 2.1, NCA - Prirucka_administratora kap. 7.1, SZR_Evidence_aktiv_1v0 Kap 7.1.2 (REQ-7.1.2-01) CP_TSA kap. 5.2,Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA kap. 3.1.1, NCA - Prirucka_administratora kap.2

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap 7.2 (REQ-7.2-01 až REQ-7.2-17) a) ano, SZR_Kontrolni_cinnost kap. 3.2. b) ano, SZR_Kontrolni_cinnost kap. 3.2 c) SZR_POLITIKA_RAZITKA kap. 6.4.5, ZP, Provozní řád SZR. d) ano, SZR_NCA-SBP_CA_TSA, zvláštní dokument podepsaný pracovníky e) ano, dtto, CBP 3.1.1 (politika přístupu - nejmenší privilegia), CBP 3.5 (popisy, znalosti) viz EN 319 401 kap. 7.1.2, Politika bezpečnosti informací SZR SZR_NCA-SBP_CA_TSA , NCA - Prirucka_administratora. f) Politika bezpečnosti informací SZR g) ano, SZR_Kontrolni_cinnost kap. 3 h) ano - SZR_POLITIKA_RAZITKA kap. 6.4.5, i) ano, NCA - Prirucka_administratora kap. 2, SZR_NCA-SBP_CA_TSA 3.1.1 j) ano - SZR_Kontrolni_cinnost kap. 3.2, 3.3. k) SZR_Kontrolni_cinnost kap. 3.1. 7.3.1 Politika bezpečnosti informací SZR, SZR_Evidence_aktiv_1v0, SZR_Uchovavani_dat_a_informaci_1v0, NCA - Prirucka_administratora kap. 7.1 7.3.2 Politika bezpečnosti informací SZR, SZR_NCA-SBP_CA_TSA kap 3.1.7, 3.2.2, SZR_Smernice_prac_RA kap. 7, CP_TSA kap 7, SZR_Uchovavani_dat_a_informaci_1v0.pd kap.4, SZR_Dilci_spisovy_plan_1v0, NCA - Zaloha dat systemu v.1.0 kap. 3.1, 2.2, Prirucka_administratora kap. 6.8, skartovací stroje. Naplnění ISO 27002 kap. 8.3

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap 7.4 (REQ-7.4-01 až REQ-7.4-10) a) SZR_Sitova_bezpecnost_NCA b) SZR_NCA-SBP_CA_TSA kap. 3.1.3, Prirucka_administratora, kontrola účtů c) SZR_NCA-SBP_CA_TSA, Prirucka_administratora. d) Dvoufaktorová autentizace, CP_TSA kap. 6.5.1, Prirucka_administratora kap. 3, práce s logem kap. 7.1. e) ano - logy uchovávány f) ano - secure delete klíčů Kap 7.5 (REQ-7.5-01) TSU klíč generován/používán v HSM, mimo HSM a zálohy pouze šifrovaně 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_1v0, SZR_Pozarni_bezpecnost_1v0.. b) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v0, SZR_Pozarni_bezpecnost_1v0, Prirucka_administratora kap. 7, UPS, dieselagregát. c) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v0, SZR_Pozarni_bezpecnost_1v0 d) SZR_Projekt_fyzicke_bezpecnosti_1v0, SZR_Rizeni_fyz_pristupu_1v0 SZR_Pozarni_bezpecnost_1v0. 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 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 kap. 3, 5, 6, 7, SZR_Smernice_prac_RA. SZR_Pozarni_bezpecnost), SZR_Kontrolni_cinnost kap. 3.2,

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					NCA - Prirucka_administratora 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 kap. 2, bod 1. b) Definována pravidla, SZR_Sitova_bezpecnost_NCA kap. 2, body 2, 5. c) Rozdělení subsítí, SZR_Sitova_bezpecnost_NCA kap. 2, bod 1 d) Zvláštní síť pro administraci, rozdělení subsití na firewallu, oddělení vývojového a testovacího prostředí, SZR_Sitova_bezpecnost_NCA kap. 2, bod4. e) Komunikace TSAweb – TSS, řídí firewall f) přepínání na záložní linku g) Zajištěno smluvně, provádí se definovaným postupem. Na FW provádí výrobce a dodává patche, je-li třeba. h) SZR_Sitova_bezpecnost_NCA kap. 2, body 9,8,7. Kap 7.9 (REQ-7.9-01 až REQ-7.9-12) a) CP_TSA kap. 5.4,NCA - Prirucka_administratora kap. 7.1 b) NCA - Prirucka_administratora kap. 6.11 (NAGIOS, program Monit) c) NCA - Prirucka_administratora kap. 6.11 (program Monit) d) SZR_Bezpecnostni_incidenty kap. 2 e) SZR_Bezpecnostni_incidenty kap. 2.2.2 - hlásit okamžitě po zjištění f) SZR _Bezpecnostni_incidenty_1v0.p kap 2.2.4 - informování subjektů. g) NCA - Prirucka_administratora kap. 6.11 (NAGIOS), příslušné osoby jsou v případě kritických bezpečnostních událostí informovány (SZR_Bezpecnostni_incidenty kap. 2.2.2). h Prirucka_administratora kap. 6.7. i) SZR_Bezpecnostni_incidenty kap. 2.2.2, 2.2.4. 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

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					v místnosti SZR s řízeným přístupem - SZR_POLITIKA_RAZITKA kap. 6.4.13, SZR_Uchovavani_dat_a_informaci_1v0 kap. 2. c) V souladu s aktuální legislativou, mj. SZR_POLITIKA_RAZITKA kap. 6.4.13. d) Čas události je součástí logového záznamu - SZR_POLITIKA_RAZITKA kap. 6.3.7. Přesnost systémového času a frekvence synchronizace a kontroly je dána standardy pro vydávání časových razítek. SZR_NCA-SBP_CA_TSA kap. 3.4.2, NCA - Prirucka_administratora kap. 6 - čas se bere z NTP serveru (GPS, Galileo). e) SZR_POLITIKA_RAZITKA kap. 6.4.13 f) Paralelní ukládání médií CP_TSA kap.5.1.6). Integrita chráněna elektronickými podpisy (NCA - Prirucka_administratora kap. 7.1.4). Kap 7.11 (REQ-7.11-01, REQ-7.11-02) SZR_Rizeni_kontinuity_1v0, NCA -Obnova systemu CA , NCA - Premisteni systemu CA Kap 7.12 (REQ-7.12-01 až REQ-7.12-11) a) SZR_Ukonceni_cinnosti_1v0 kap. 2.4, 2.5, 2.6, 2.7. b) SZR_Ukonceni_cinnosti_1v0 kap. 2.4, 2.5, 2.6, 2.7. c) SZR_POLITIKA_RAZITKA, kap. 6.5.2 d) SZR_SMERNICE_RAZITKA kap.6.4.11, SZR_Ukonceni_cinnosti_1v0 kap. 2.4, 2.6 (vydané TST, logy), e) SZR_Ukonceni_cinnosti_1v0 - kap. 2.6
eIDAS, čl. 19.2	☒	ETSI EN 319 401: kapitola 7.9 (zvládání incidentů, zejména písm. e) a f))	S	EQUAL	Popsáno v předchozím bodu. Norma: ETSI EN 319 401, kap. 7.9 (REQ-7.09-01 až REQ-7.09-10) a) CP_TSA kap. 5.4, Sm 10 kap. 7.1 b) NCA - Prirucka_administratora kap. 6.11 (NAGIOS, program Monit), IPS na FW - logování a reportování c) NCA - Prirucka_administratora kap. 6.11 (program Monit)

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					d) SZR_Bezpecnostni_incidenty kap. 2 e) SZR_Bezpecnostni_incidenty kap. 2.2.2 - hlásit okamžitě po zjištění f) SZR _Bezpecnostni_incidenty_1v0.p kap 2.2.4 - informování subjektů. g) NCA - Prirucka_administratora kap. 6.11 (NAGIOS), příslušné osoby jsou v případě kritických bezpečnostních událostí informovány. h) NCA - Prirucka_administratora kap. 6.7. i) SZR_Bezpecnostni_incidenty kap. 2.2.2, 2.2.4.
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	Pro tuto službu není relevantní.
eIDAS, čl. 24.2	☒	a) ETSI EN 319 401, kap. 6.1 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)	S	EQUAL	Dokumentace: SZR_SMERNICE_RAZITKA **Norma:** **a)** ETSI EN 319 401, kap 6.1. SZR_SMERNICE_RAZITKA **b)** ETSI EN 319 401 Kap 7.1.1 (REQ-1.1.1-02 až REQ-7.1.1-07) a) SZR_POLITIKA_RAZITKA, kap. 1. b) SZR_POLITIKA_RAZITKA, kap. 1 c) SZR_POLITIKA_RAZITKA, kap. 6.5.2 d) SZR_POLITIKA_RAZITKA, kap. 6.5.2 e) SZR_POLITIKA_RAZITKA, kap. 6.5.9 f) SZR_POLITIKA_RAZITKA, kap. 6.4.5.11 kap. 7.1.2 ETSI EN 319 401, kap. 7.1.2 (REQ-7.1.2-01) SZR_POLITIKA_RAZITKA kap. 5.2, SZR_NCA-SBP_CA_TSA, NCA-Prirucka_administratora kap.2 Kap. 7.2 (REQ-7.2-03 až REQ-7.2-17) a) ano SZR_Kontrolni_cinnost kap. 3. b) ano, SZR_Kontrolni_cinnost kap. 3 c) SZR_SMERNICE_RAZITKA kap. 6.4.5, ZP, Provozní řád SZR

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					d) ano, splněno zvláštní dokument podepsaný pracovníky, viz též EN 319 401 kap. 7.1.2 e) ano, viz EN 319 401 kap. 7.1.2, CBP 3.1.1 (politika přístupu - minimální privilegia), CBP 3.5 (popisy, znalosti) Politika bezpečnosti informací SZR f) CBP kap. 2.4 Politika bezpečnosti informací SZR g) kap. 5.3, SZR_Kontrolni_cinnost kap. 3 h) ano – SZR_POLITIKA_RAZITKA kap. 6.4.5, i) ano - SZR_NCA-SBP_CA_TSA kap. 3.1.1, NCA - Prirucka_administratora kap. 2 j) kap. 5.2.1, SZR_Kontrolni_cinnost kap.3. k) SZR_Kontrolni_cinnost kap.3.3. **c)** ETSI EN 319 401 kap. 7.1.1 (REQ-7.1.1-02 až REQ-7.1.1-07) a) SZR_POLITIKA_RAZITKA, kap. 1. b) SZR_POLITIKA_RAZITKA, kap. 1 c) SZR_POLITIKA_RAZITKA, kap. 6.5.2 d) SZR_POLITIKA_RAZITKA, kap. 6.5.2 e) SZR_POLITIKA_RAZITKA, kap. 6.5.9 f) SZR_POLITIKA_RAZITKA, kap. 6.4.5.11 kap. 7.1.2 SBP_CA_TSA 3.1.2 **d)** Připraveno, bude vystaveno na webu SZR ETSI EN 319 401, Kap. 6.2 (REQ-6.2-01 až REQ-6.2-02) Omezení jsou součástí veřejné politiky TSA a info bude vystaveno na webu SZR a) OID TSA policy, b) SZR_POLITIKA_RAZITKA, kap.5.1.1, c) SZR_POLITIKA_RAZITKA, kap.5.2, d) SZR_POLITIKA_RAZITKA, kap.5.3, e) SZR_POLITIKA_RAZITKA, kap.6.4.13, prováděcí směrnice,

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					f) SZR_POLITIKA_RAZITKA, kap.5.4, g) omezení ručení za škody - kap.6.5.2, h) SZR_POLITIKA_RAZITKA, kap.6.5.10, i) SZR_POLITIKA_RAZITKA, kap.6.5.9, j) certifikát o shodě na webu I.CA, k) kontakty budou na webu SZR, l) dostupnost - SZR_POLITIKA_RAZITKA, kap.5.1.1 (nepřetržitě až na poruchy a odstávky) **e), f)** CEN TS 419 261 **Popsáno a řešeno normou** ETSI EN 319 401, kap. 7, viz čl. 19 eIDAS této zprávy **g)** ETSI EN 319 401 kap. 5., kap. 6. a kap. 7 – viz čl. 19.1 eIDAS této zprávy **h)** ETSI EN 319 421 Kap 7.6.5 Lifetime: sha256RSA2048 = dle algopaper 6let Kap 7.7.2 a) hodiny TSU dolaďovány pomocí NTP b) uzavřená appliance/systém v provozní místnosti c) pravidelná auditní kontrola - auditní "token" d) neplatný auditní token zastaví vydávání časových razítek e) manuálně (odstávka, problémy se SW/HW) kap. 7.8 SZR_Rizeni_fyz_pristupu, TSS na chráněném provozním pracovišti Viz též ETSI EN319 401, kap. 7.6 (popsáno výše)

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
					Kap. 7.12 a) vytvoření žádosti/zavedení TSU certifikátu logováno b) vytvoření žádosti/zavedení TSU certifikátu logováno c) NTPD loguje do systémového logu synchronizaci, kalibraci i chyby synchronizace d) dtto Viz též ETSI EN319 401, kap. 7.10 (popsáno výše) **i)** revokace certifikátů TSU - SZR_Ukonceni_cinnosti ETSI EN 319 401, kap 7.12. a) SZR_Ukonceni_cinnosti kap. 2.4, 2.5, 2.6, 2.7. b) SZR_Ukonceni_cinnosti kap. 2.4, 2.5, 2.6, 2.7. c) SZR_POLITIKA_RAZITKA kap. 6.5.2, d) SZR_SMERNICE_RAZITKA kap. 6.4.11, SZR_Ukonceni_cinnosti 2.6 (vydané TST, logy) e) SZR_Ukonceni_cinnosti kap. 2.6 **j)** ETSI EN 319 401, kap 7.13. a) Požadavky právního systému zahrnuty v interních dokumentech, plnění prokazováno auditem. b) nerelavantní c) TSU nepracuje s osobními daty
eIDAS, čl. 24.3	☒		S	EQUAL	Nerelevantní
eIDAS, čl. 24.4	☒		S	EQUAL	Nerelevantní

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
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. 42

Požadavky na kvalifikovaná elektronická časová razítka

Kritérium	Ověř[1]	Rozšíření ETSI	Zjištění	Metrika[2]	Zdůvodnění
eIDAS, čl. 42.1	☒	ETSI EN 319 411-2	S	EQUAL TEST	Ověřeno vůči vystavenému časovému razítku připojenému k dokumentu a kontrolou času vůči UTC. Časové razítko je ve shodě s politikou i s požadavkem chyby času do 1 sekundy. Dokumentace: SZR_POLITIKA_RAZITKA, SZR_NCA-SBP_CA_TSA, NCA - Sprava TSS Norma: ETSI EN 319 421 Kap. 7.7.1 a) NTP hodiny mají referenční UTC čas z GPS a Galieo b) čas TSS synchronizován s hodinami NTP c) neplatný "token" d) soukromý klíč TSU pouze pro tvorbu zaručené elektronické pečetě TST e) sledováno podle platnosti doby importovaného certifikátu TSU
eIDAS, čl. 42.2	☒	ETSI EN 319 421, ETSI EN 319 422	S	EQUAL	Splněno naplněním požadavků v čl. 42.1. Dle čl. 48, odst. 2 nejsou pro tuto službu předepsány další prováděcí akty.

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 (dokument s připojeným časovým razítkem) nejsou součástí této zprávy. 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.