ZPRÁVA

o posouzení vypořádání výhrad k důvěryhodným službám NCA

Posouzení provedl: [redacted]

Datum uvolnění zprávy: 26.04.2019

Zpráva o posouzení shody

Tato zpráva je vydána certifikačním orgánem na žádost TSP.

Posouzení provedl:	Certifikační orgán TAYLLORCOX PCEB, zřízený TAYLLORCOX s.r.o.
Rozsah posouzení:	Posouzení způsobu a dostatečnosti vypořádání výhrad k důvěryhodným službám NCA dle Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014., vzešlých z certifikačního auditu důvěryhodných služeb NCA, provedených certifikačním orgánem TAYLLORCOX PCEB, který byl ukončen k 31.1.2019.
Posuzované služby:	NCA – služba vydávání kvalifikovaných certifikátů pro elektronický podpis NCA – služba vydávání kvalifikovaných certifikátů pro elektronickou pečeť NCA - služba vydávání kvalifikovaných elektronických časových razítek
Výsledek posouzení:	**Posuzovaná vypořádání jsou VE SHODĚ s příslušnými požadavky Nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 a NCA naplňuje požadavky eIDAS pro poskytování výše uvedených důvěryhodných služeb, viz níže uvedené odůvodnění.**
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 řádnému poskytování důvěryhodných služeb. Kvalifikované služby může NCA začít poskytovat až po zalistování svých služeb na důvěryhodný seznam EU (EUTL).

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 elektronický podpis
Verze posuzované služby	Politika OID 1.2.203.72054506.10.1.30.1.0

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)

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

PŘEDMĚT ZPRÁVY

Hlavní závěry jsou uvedeny na straně 2 této zprávy. Důkazy, prokazující relevantnost a správnost posouzení a vyhodnocení předložených vypořádání certifikačním orgánem dokládají následující kapitoly.

POPIS NALEZENÝCH VÝHRAD BĚHEM AUDITU

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

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

Vypořádání výhrad má být 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 označené 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

eIDAS	Výhrady
	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, který se týká práva přístupu a nakládání s prostředky NCA v prostorech zvláštní složky - SZR_Ukonceni_cinnosti, 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

DOPLŇUJÍCÍ KOMENTÁŘE A UPŘESNĚNÍ

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. 28	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.
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.

DOPLŇUJÍCÍ KOMENTÁŘE A UPŘESNĚNÍ

Dne 23.4.2019 proběhla u TSP schůzka, kde TSP prezentoval způsob vypořádání výhrad a doporučení z provedeného lednového certifikačního auditu.

Dne 25.4.2019 poskytl TSP dokumentaci se zapracovanými změnami:

- POL019D-2013_Bezpečnostní politika ISMS_20190326
- Zápis_provozní_smlouva_návrh_v1.0
- Návrh ZÁPISU 25. 4. 19_v1
- Kořenový a mezilehlý certifikát NCA pro svou CA

Dále byly poskytnuty informace, že:

- Bezpečnostní politika SZR zohledňuje činnost NCA.
- Zaslaný návrh provozní smlouvy, resp. zápisu mezi SZR a bezpečnostní složkou je všemi zúčastněnými akceptovatelný a jsou svolní jej podepsat.
- Odkaz na web https://www.narodni-ca.cz/ je funkční a Certifikační prováděcí směrnice (CPS) a kořenový a mezilehlý certifikát bude zveřejněn až po obdržení stanoviska od MVCR, jako dohledového orgánu.
- Smlouvy, které jsou generovány na RA, jsou z pohledu GDPR ošetřeny a další ustanovení k ochraně osobních údajů je pak mezi SZR a bezpečnostní složkou v zápise k RA, viz výše uvedený dokument Návrh ZÁPISU 25. 4. 19_v1

Návrh ZÁPISU 25. 4. 19_v1 bude doplněn o řízený postup ukončení činnost RA, který bude separátní přílohou smlouvy na RA. Čeká se na oficiální potvrzení, ale od bezpečnostních složek má NCA informaci, že k Návrhu ZÁPISU 25. 4. 19_v1 nevnímají žádné nesoulady.

SHRNUTÍ A ZÁVĚR

Posouzením výše uvedených dokumentů a informací dospěl certifikační orgán k názoru, že při dodržení závazků NCA uvedených v předchozí kapitole (doplnění informací na web a uzavřením smlouvy (zápisu) s bezpečnostní složkou před spuštěním RA a služeb na této bezpečnostní složce), vypořádal TSP všechny výhrady certifikačního orgánu a naplnil požadavky stanovené pro získání statutu QTSP, které má certifikační orgán právo posoudit a vyjádřit se k nim.

ZÁVĚREČNÁ ČÁST ZPRÁVY

Posouzení provedl: 

Datum posouzení: 26.04.2019

Podpis posuzovatele: