Certifikačná politika pre službu OCSP (Online Certificate Status protocol)

Názov dokumentu:	Certifikačná politika pre službu OCSP (Online Certificate Status protocol)		
Označenie dokumentu:	cp_ocsp_snca.pdf		
Verzia:	1.2	Status:	*Finálna verzia*
Dátum vytvorenia:	20.5.2021	Platný do:	

História dokumentu

História revízií dokumentu

Verzia	Dátum	Popis zmeny	Autor / Autor zmien
0.9	18.11.2020	Úvodná verzia	Ing. Marián Štefánek
1.0	30.11.2020	Finálna verzia	Tibor Berešík
1.1	03.05.2021	Doplnenie SNCA4	Štefan Szilva
1.2	20.05.2021	Formálne úpravy	Štefan Szilva

Schválenia

Verzia	Funkcia	V zastúpení	Schválil dňa	Podpis

Distribúcia

Verzia	Spoločnosť	Meno	Počet výtlačkov

Referencie na legislatívne a normatívne dokumenty

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej aj „Nariadenie eIDAS“).
Nariadenie eIDAS

[2] RFC 6960 - Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.
RFC 6960

[3] Pravidlá na výkon certifikačných činností (CPS) SNCA.

[4] Certifikačná politika pre kvalifikovanú dôveryhodnú službu vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, ktorej kvalifikovaný štatút udelil NBÚ SR, OID: 1.3.158.42156424.0.1.2.

[5] Politika poskytovania dôveryhodných služieb NASES, OID: 1.3.158.42156424.0.1.1.

Zoznam tabuliek

Použité definície a skratky

Tabuľka 1 Použité definície

Definícia	Vysvetlenie definície
Žiadateľ	Ktokoľvek.
Spoliehajúca sa strana	Ľubovoľná právnická alebo fyzická osoba.
Univerzálny koordinovaný čas	Časový údaj v „svetovom čase“, odvodený od slnečného času nultého poludníka.

Tabuľka 2 Použité skratky

Skratka	Vysvetlenie skratky
UTC	Univerzálny koordinovaný čas.
OCSP responder	Vydavateľ OCSP odpovedí.
NASES	Národná agentúra pre sieťové a elektronické služby.
KCA	Koreňová certifikačná autorita NBÚ.
SNCA	Slovenská národná certifikačná autorita NASES.
CA	Certifikačná autorita SNCA.
RA	Registračná autorita SNCA.
TAC	Čas na dokončenie (Time At Completion).
PMA	Autorita pre riadenie politík (Policy Management Authority).

Obsah

1 Úvod

Tento dokument definuje politiku poskytovania služby OCSP (Online Cerificate Status Protocol ďalej aj „CP OCSP“) a bezpečnostné požiadavky, ktoré sa týkajú prevádzkovej praxe a postupov pri poskytovaní tejto služby.

Účelom tohto dokumentu je definovať a prezentovať metodiku, záväzné postupy a zodpovednosti prevádzkovateľa certifikačnej autority Slovenskej národnej certifikačnej autority (ďalej aj „SNCA“), prevádzkovanej v systéme IS KDS, pri poskytovaní služby OCSP, definovať úlohy, povinnosti a zodpovednosť zúčastnených strán pri používaní tejto služby.

Politika je záväzným dokumentom, slúžiacim ako štandard zásad, procedúr a postupov, ktoré musia dodržiavať všetky zúčastnené strany.

Poskytovateľom tejto dôveryhodnej služby je:

Názov poskytovateľa	**Národná agentúra pre sieťové a elektronické služby**
Sídlo / poštová adresa	Kollárova 8, 917 02 Trnava **Detašované pracovisko:** BC Omnipolis, Trnavská cesta 100/II, 821 01 Bratislava
IČO	42 156 424
Telefón	+421 2 3278 0700
E-mail	podatelna@nases.gov.sk
Webové sídlo	http://www.nases.gov.sk

(ďalej len „NASES“), prostredníctvom svojho systému OCSP (OCSP SNCA).

Tento dokument môže byť použitý nezávislými orgánmi ako základ pre potvrdenie, že NASES je dôveryhodný na poskytovanie služby OCSP.

Služba OCSP, identifikovaná v tomto dokumente, je využívaná v okruhu pôsobnosti SNCA, prevádzkovanej agentúrou NASES.

1.1 Prehľad

Táto CP OCSP sa týka poskytovania služby OCSP v zmysle ustanovení Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 3. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“).

Vyhotovované OCSP odpovede, sú podpisované s využitím súkromného kľúča jednotky, vyhotovujúcej OCSP odpovede (ďalej aj „OCSP responder“), ktorého certifikát môže byť vydaný výhradne touto certifikačnou autoritou SNCA:

Názov	Sériové číslo certifikátu	Vydavateľ	DigitalID v SK dôveryhodnom zozname
SNCA4	008179d0a5e8cff32a	SNCA4	
SNCA3	07 8e	KCA NBU SR 3	KaIHEeYMKI6axfcIS0LG1RwNvOI

1.2 Názov dokumentu a jeho identifikácia

Tomuto dokumentu je priradený identifikátor objektu (OID):

1.3.158.42156424.0.1.5

kde jednotlivé zložky OID majú nasledovný význam:

1	ISO
3	ISO Identified Organization
158	Slovakia
42156424	jedinečný identifikátor Národnej agentúry pre sieťové a elektronické služby priradený organizáciou ISO (IČO)
0	KCA (poskytovanie dôveryhodných služieb)
1	Certifikačné politiky
5	Certifikačná politika pre službu OCSP

1.3 Účastníci PKI

V rámci poskytovania služby OCSP, sú účastníci infraštruktúry verejného kľúča prevádzkovateľa, uvedení v tejto časti.

1.3.1 Jednotka vyhotovovania OCSP odpovede

Jednotka vyhotovovania OCSP odpovede:

- je entita, ktorá poskytuje službu vyhotovovania odpovede OCSP používateľom (klienti SNCA, spoliehajúce sa strany),
- má celkovú zodpovednosť za poskytovanie služby, špecifikovanej v odstavci 1.1,

- je uvádzaná vo vydaných OCSP odpovediach ako vydavateľ a jej súkromné kľúče sú používané pri vyhotovovaní podpisu týchto odpovedí,
- zaručuje, že všetky aspekty jej služieb, operácií a infraštruktúry, zviazanej s OCSP odpoveďami, vydanými podľa tejto politiky, sú vykonávané v súlade s jej požiadavkami a ustanoveniami a v súlade s pravidlami na výkon certifikačných činností SNCA.

OCSP responder SNCA je súčasťou hierarchickej PKI:

SNCA 4

- SNCA 4 -> OCSP responder

SNCA 3

- KCA NBÚ SR 3 -> SNCA 3 -> OCSP responder

1.3.2 Registračná autorita

Neuplatňuje sa.

1.3.3 Klient

O vyhotovenie OCSP odpovede môže žiadať:

1. neobmedzené

Žiadatelia o službu OCSP odpovede sú povinní:

- postupovať pri žiadosti o vydanie OCSP odpovede spôsobom, predpísaným v tomto dokumente,
- používať predpísaný formát a protokol žiadosti o OCSP odpoveď,
- žiadosť OCSP klienta musí byť v súlade s požiadavkami RFC 6960 a dokumentu SigG-profile (potvrdenie o dostupnosti certifikátu – „positive statement“),
- riešiť nezrovnalosti pri vydaní OCSP odpovede s kontaktnou osobou NASES bez zbytočných prieťahov.

1.3.4 Spoliehajúca sa strana

Spoliehajúca sa strana je ľubovoľná právnická alebo fyzická osoba so sídlom v SR alebo v zahraničí.

1.3.5 Iní účastníci

Žiadne ustanovenia.

1.4 Použiteľnosť časovej pečiatky

OCSP odpovede, vyhotovené v rámci poskytovania služby vyhotovovania OCSP odpovedí, popísanej v tejto politike, môžu účastníci a spoliehajúce sa strany používať bez obmedzenia všade.

1.5 Správa politiky

Táto politika spĺňa požiadavky RFC 6960.

1.5.1 Organizácia zodpovedná za správu dokumentu

Tento dokument je spravovaný sekciou Slovenskej národnej certifikačnej autority Národnej agentúry pre sieťové a elektronické služby.

Kontaktná adresa:

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

http://www.nases.gov.sk

1.5.2 Kontaktná osoba

Bezpečnostný správca SNCA.

Národná agentúra pre sieťové a elektronické služby

Detašované pracovisko:

BC Omnipolis,

Trnavská cesta 100/II,

821 01 Bratislava,

Slovenská republika,

Telefón: +421 2 3278 0700

e-mail: info@nases.gov.sk

1.5.3 Osoba rozhodujúca o súlade CP s certifikačnou politikou

Vo všetkých záležitostiach a aspektoch, týkajúcich sa poskytovateľa a jeho činnosti, s konečnou platnosťou rozhoduje riaditeľ sekcie Slovenskej národnej certifikačnej autority NASES.

1.5.4 Postupy schvaľovania CP a externej politiky

Je nevyhnutné, aby pred uvedením do prevádzky, mal poskytovateľ schválenú požadovanú dokumentáciu, svoje certifikačné politiky (ďalej aj „CP“) a pravidlá na výkon certifikačných činností (ďalej aj „CPS“) a zároveň, aby spĺňal všetky požiadavky, definované v týchto dokumentoch. Obsah CP a CPS schvaľuje riaditeľ sekcie Slovenskej národnej certifikačnej autority NASES.

Po schválení, je príslušný dokument publikovaný, v súlade s publikačnou a oznamovacou politikou.

2 Úložiská

2.1 Zverejňovanie informácií o OCSP

Zásady, pre poskytovanie služby OCSP odpovede, sú zverejnené na internetovej stránke SNCA SR:

SNCA 4

https://snca.gov.sk/cps/cp_ocsp_snca.pdf

SNCA 3

http://ep.nbusr.sk/snca/docs/cp_ocsp_snca.pdf

V listinnej podobe je dokumentácia k dispozícii aj na pracovisku prevádzkovateľa SNCA.

Verejný kľúč OCSP respondera, určený na overovanie OCSP odpovedí, je distribuovaný vo forme certifikátu vydaného SNCA, samostatne, na webovom sídle:

SNCA 4

https://www.nases.gov.sk/doveryhodne-sluzby/index.html

SNCA 3

http://ep.nbu.gov.sk/snca/ocsp.html

Aktuálny zoznam zrušených certifikátov, je publikovaný v súbore na internetovej stránke:

SNCA 4

http://cdp1.snca.gov.sk/snca4/crl/snca4.crl
http://cdp2.snca.gov.sk/snca4/crl/snca4.crl

SNCA 3

http://ep.nbu.gov.sk/snca/crls3/snca3.crl

2.2 Frekvencia zverejňovania informácií

Zoznam zrušených certifikátov (ďalej aj „CRL“), musí byť publikovaný v súlade s podmienkami, špecifikovanými v aktuálnej CP pre vyhotovovanie kvalifikovaných certifikátov. Informácie o zrušenom certifikáte OCSP respondera, musia byť dostupné na webovom sídle SNCA (pozri kapitola 2.1), ktorý slúži ako jeho úložisko.

CP OCSP sa musí zverejniť čo najskôr po jej schválení a vydaní.

Všetky ďalšie informácie, ktoré je povinný prevádzkovateľ publikovať v úložisku, je potrebné publikovať podľa možnosti čo najskôr.

2.3 Kontroly prístupu

V záujme ochrany informácií a dát, uložených v úložisku, ktoré nemajú byť verejne dostupné, musí prevádzkovateľ SNCA:

- vynaložiť maximálne úsilie na to, aby zaistil integritu, dôvernosť a dostupnosť dát, súvisiacich s poskytovanými dôveryhodnými službami,
- vykonať logické a bezpečnostné opatrenia, aby zabránil neautorizovanému prístupu k úložisku všetkým osobám, ktoré by mohli akýmkoľvek spôsobom zmeniť, poškodiť, pridať resp. vymazať údaje, uložené v úložisku.

3 Všeobecné ustanovenia

Služba OCSP odpovede, poskytuje žiadateľovi informácie o stave certifikátu.

Poskytnutím OCSP odpovede NASES, ako poskytovateľ OCSP odpovede prostredníctvom prevádzkovaného systému OCSP SNCA, vydáva potvrdenie o stave platnosti certifikátu.

3.1 Všeobecné ustanovenia politiky

Právne záruky a obmedzenia záruk, v rámci tohto dokumentu, vyplývajú zo zákonných predpisov, platných v SR.

Všetky spory budú riešené v zmysle platných zákonov a všeobecne záväzných predpisov SR.

V rámci tohto dokumentu nie je stanovená žiadna finančná zodpovednosť. V prípade jej vzniku, bude finančná zodpovednosť jednotlivých strán určená právnymi predpismi, platnými v Slovenskej republike.

3.2 Služby súvisiace s OCSP odpoveďou

Služby, súvisiace s OCSP odpoveďou, je možné z pohľadu naplnenia požiadaviek rozdeliť na dve samostatné služby, ktorými sú:

- poskytovanie OCSP odpovede – táto služba vytvára samotnú OCSP odpoveď,
- validátor platnosti údajov databázy – táto služba kontroluje funkčnosť mechanizmu prenášania záznamov databázy poskytovateľa služieb CA SNCA do databázy OCSP. Na základe pozitívnej validácie platnosti údajov z databázy, umožní OCSP responder samotné generovanie odpovedí o stave platnosti certifikátov klientom.

3.3 Vydavateľ OCSP odpovedí

Poskytovateľom služby vyhotovovania OCSP odpovedí pre potreby klientov v zmysle tejto CP OCSP je NASES prostredníctvom SNCA.

Za poskytovanie služieb, súvisiacich s OCSP odpoveďou podľa bodu 3.2, zodpovedá prevádzkovateľ SNCA.

Prevádzkovateľ SNCA zodpovedá za bezpečnú prevádzku systému OCSP SNCA a bezpečnosť poskytovanej služby vyhotovovania OCSP odpovedí v rozsahu bodu 6.7.

3.4 Používateľ OCSP odpovedí

Používateľom služby vyhotovovania OCSP odpovedí môže byť ktokoľvek.

Služba OCSP musí byť dostupná v režime 24 hodín denne, 7 dní v týždni, 365 dní v roku.

Služba OCSP je v zmysle nariadenia eIDAS poskytovaná bezodplatne.

4 Úvod do politiky OCSP odpovedí a plnenie všeobecných požiadaviek

4.1 Všeobecne

Tento dokument „Certifikačná politika pre službu OCSP (Online Certificate Status protocol)“ je verejným dokumentom.

Činnosť SNCA pri vydávaní OCSP odpovedí sa riadi prevádzkovými a bezpečnostnými smernicami SNCA.

4.2 Cieľoví používatelia a použitie

4.2.1 Správna prax uplatňovania politiky vyhotovovania OCSP odpovedí

Neuplatňuje sa.

5 Politiky a pravidlá

5.1 Ohodnotenie rizík

Pravidlá a zásady pre hodnotenie rizík, sú definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“, kap. 5. „Posúdenie rizík“.

5.2 Pravidlá pre praktický výkon dôveryhodných služieb

Všeobecné pravidlá pre praktický výkon dôveryhodných služieb sú uvedené v dokumente - „Politika poskytovania dôveryhodných služieb NASES“.

5.3 Všeobecné podmienky

Všeobecné podmienky, týkajúce sa služieb Poskytovateľa, sú uvedené v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 6.2.

5.4 Politika informačnej bezpečnosti

Politika informačnej bezpečnosti je uvedená a popísaná v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 6.3, pričom dôveryhodnosť systému je zabezpečená:

- zavedenými bezpečnostnými pravidlami a procedúrami,
- spôsobom riadenia bezpečnosti OCSP SNCA,
- dohľadom nad bezpečnosťou vykonávania obslužných činností a prevádzkových rutín,
- pravidelným vnútorným a externým auditom bezpečnosti,
- súladom so štandardami, definujúcimi požiadavky na bezpečnosť dôveryhodných systémov.

5.5 Záväzky Poskytovateľa

5.5.1 Všeobecne

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP sa zaväzuje:

- zabezpečiť plnenie požiadaviek v zmysle kapitoly 6 a 7 tejto CP OCSP;

- používať bezpečnostné systémy ktoré zaisťujú primeranú technickú úroveň ochrany, vrátane použitia kryptografických opatrení;
- vykonávať prijaté postupy bezpečným a spoľahlivým spôsobom;
- zabezpečiť súlad hodín servera OCSP s časom UTC v proklamovanej presnosti;
- zabezpečiť sledovateľnosť spracovania žiadostí o vydanie OCSP odpovede;
- zabezpečiť ochranu kľúčov, používaných na vydávanie OCSP odpovede;
- zabezpečiť zverejňovanie údajov, nutných na overovanie vydaných OCSP odpovedí v podobe certifikátov verejného kľúča, prislúchajúceho súkromnému kľúču, používanému pri podpisovaní OCSP odpovedí;
- zverejňovať informácie o:
  - spôsobe poskytovania služby OCSP,
  - spôsobe prijímania žiadostí o OCSP odpovede,
  - spôsobe overovania OCSP odpovedí.
- zabezpečiť, aby prax vyhotovovania OCSP odpovedí zodpovedala procedúram, popísaným v tejto CP OCSP a bola v súlade s CPS SNCA.

5.5.2 Záväzky SNCA k používateľom služby

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP, je povinný:

- zaistiť spracovanie žiadostí o vydanie OCSP odpovedí, doručených v predpísanom formáte;
- odpovedať na platnú žiadosť o vydanie OCSP odpovede vydaním OCSP odpovede (pokiaľ tomu nebránia technické problémy);
- zverejňovať údaje, nutné na overovanie vydaných OCSP odpovedí v podobe certifikátu verejného kľúča, prislúchajúceho súkromnému kľúču, používanému pri podpisovaní OCSP odpovedí.

5.6 Informácie pre spoliehajúce sa strany

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP, je vo vzťahu k Spoliehajúcim sa stranám povinný zaistiť podmienky na overenie OCSP odpovedí zverejňovaním údajov, nutných na overovanie vydaných OCSP odpovedí v podobe certifikátu verejného kľúča, prislúchajúceho k súkromnému kľúču, používanému pri podpisovaní OCSP odpovedí.

6 Riadenie a prevádzka OCSP Poskytovateľa

6.1 Úvod

Riadenie a prevádzka OCSP poskytovateľa sú vykonávané tak, aby prijaté bezpečnostné opatrenia a nástroje na kontrolu ich plnenia poskytli nevyhnutnú dôveru, že budú naplnené.

6.2 Vnútorná organizácia

NASES, ako prevádzkovateľ SNCA a poskytovateľ dôveryhodných služieb:

- sa pri plnení úloh riadi Ústavou Slovenskej republiky, ústavnými zákonmi, právne záväznými aktmi Európskej únie, medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, zákonmi, ďalšími všeobecne záväznými právnymi predpismi, uzneseniami vlády Slovenskej republiky, svojim štatútom a organizačným poriadkom ako aj ostatnými internými predpismi agentúry,
- riadi informačnú bezpečnosť primerane pre poskytovanú službu vyhotovovania OCSP odpovedí,
- zamestnáva dostatočný počet osôb, ktoré majú nevyhnutné vzdelanie, školenia, technické znalosti a skúsenosti vzhľadom na typ, rozsah a množstvo práce, nevyhnutnej na poskytovanie služieb vyhotovovania OCSP odpovedí.

OCSP SNCA je organizačnou súčasťou sekcie Slovenskej národnej certifikačnej autority Národnej agentúry pre sieťové a elektronické služby.

Organizačná štruktúra agentúry NASES je popísaná v organizačnej schéme, zverejnenej na webovom sídle www.nases.gov.sk.

6.3 Personálna bezpečnosť

Manažment kľúčov, môže vykonávať len k tomu poverený pracovník, v rámci svojej role. Tieto role pracovníkov sú jednoznačne definované dokumentáciou ku kvalifikovaným dôveryhodným službám SNCA. Každý pracovník, je preukázateľne poučený o svojich povinnostiach, pracovných a bezpečnostných postupoch požadovaných pri plnení úloh a vyplývajúcich z jeho role.

Osoby, zabezpečujúce činnosti v prevádzke SNCA, sú preverované v zmysle Vyhlášky NBÚ č. 331/2004 Z. z. o personálnej bezpečnosti.

Externé organizácie, ktoré vystupujú ako zmluvní dodávatelia činností pre poskytovateľa, sú preverované v zmysle Vyhlášky NBÚ č. 325/2004 Z. z. o priemyselnej bezpečnosti.

6.4 Správa aktív

Požiadavky pre oblasť správy aktív, sú uvedené a popísané v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.3.

6.5 Riadenie prístupu

Požiadavky pre oblasť riadenia prístupu, sú uvedené a popísané v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.4.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP, garantuje bezpečnú prevádzku systému OCSP SNCA a dostupnosť uvedenej služby naviac nasledovnými činnosťami:

- na vykonanie kritických činností na kryptografickom module (napr. generovanie, záloha súkromného kľúča SNCA, obnova kľúčov, obnova zariadení) je nutný prístup dvoch určených pracovníkov prevádzkovateľa SNCA (princíp štyroch očí),
- kľúče servera OCSP, určené na podpisovanie a overovanie OCSP odpovedí, sú generované v kryptografickom module SNCA. Procedúra generovania kľúčov sa vykonáva len pod dozorom komisie, na to poverenej.

6.6 OCSP odpovede

Žiadosť o OCSP odpoveď, musí byť záujemcom o službu OCSP, zaslaná v súlade s RFC 6960.

Služba OCSP je dostupná na adrese:

SNCA 4

http://snca4-ocsp.snca.gov.sk/ocsp/snca4

SNCA 3

http://snca3-ocsp.nbu.gov.sk/ocsp/snca3

6.6.1 Synchronizácia hodín s UTC

Hodiny OCSP respondera, používané ako zdroj času pre OCSP odpovede, sú synchronizované protokolom NTP od zdroja presného času služby Meinberg GPS.

6.7 Fyzická a objektová bezpečnosť

Pravidlá a zásady pre zaistenie fyzickej a objektovej bezpečnosti, sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.6.

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP, garantuje bezpečnú prevádzku OCSP SNCA a dostupnosť uvedenej služby, aplikovaním dodatočných opatrení, v rozsahu:

- Na kryptografický modul musí byť aplikované riadenie prístupu v súlade s bodom 6.5 tejto CP OCSP.
- Na správu služby OCSP, musia byť aplikované nasledovné dodatočné opatrenia:
  - Technické prostriedky na zabezpečenie služby OCSP, musia byť prevádzkované v prostredí, ktoré fyzicky a logicky chráni služby pred kompromitáciou, ktorá môže byť spôsobená neautorizovaným prístupom k systémom alebo údajom.
  - Každý vstup do fyzicky bezpečnej oblasti, musí podliehať nezávislému dohľadu a neautorizovaná osoba musí byť sprevádzaná autorizovanou osobou, pokiaľ sa nachádza v bezpečnej oblasti. Každý vstup a prítomnosť musia byť zaznamenané.
  - Fyzická ochrana musí byť dosiahnutá vytvorením jasne definovanej bezpečnostnej hranice (perimetrom, fyzickou bariérou) okolo správy služby OCSP. Akékoľvek časti objektu, zdieľané s inými organizáciami, musia byť mimo tohto perimetra.
  - Fyzické a objektové bezpečnostné opatrenia musia chrániť objekty, kde sú umiestnené systémy, samotné systémové zdroje a objekty, použité na podporu ich prevádzky. Bezpečnostné opatrenia, týkajúce sa fyzickej a objektovej bezpečnosti SNCA, musia pokrývať minimálne fyzické riadenie prístupu, ochranu pred prírodnými katastrofami, ochranu pred požiarom, výpadok podporných rozvodov (napr. elektrina, telekomunikácie), zrútenie štruktúry, úniky z potrubí, ochranu proti odcudzeniu, vlámaniu a obnovu po pohrome.
  - Prijaté opatrenia musia chrániť zariadenia, informácie, médiá a prevádzkované softvérové prostriedky, súvisiace so službou OCSP, pred vynesením bez autorizácie.

6.8 Prevádzková bezpečnosť

Bezpečnosť prevádzky OCSP SNCA je riadená v rámci manažmentu bezpečnosti SNCA.

Na zabezpečovanie akreditovaných certifikačných služieb, používa SNCA produkty na elektronický podpis s medzinárodne uznávanou certifikáciou ISO/IEC 15408 a FIPS 140-1. Na dosiahnutie certifikácie ISO/IEC 15408 a FIPS 140-1, museli produkty pre elektronický podpis splniť príslušné požiadavky na zabezpečenie vývoja, ktoré tieto štandardy stanovujú.

Pri vývoji špecializovaného programového vybavenia sa uplatňujú ustanovenia interných bezpečnostných smerníc, ktoré predpisujú zásady bezpečnosti vývoja programového vybavenia a riadenie bezpečnosti pri poskytovaní certifikačných služieb.

Kľúče servera OCSP, určené na podpisovanie OCSP odpovedí, sú generované v kryptografickom module SNCA. Generovanie kľúčov sa vykonáva v bezpečnom prostredí.

Procedúra generovania kľúčov sa vykonáva pod dozorom komisie, na to poverenej. Po ukončení platnosti certifikátu pre OCSP, bude záloha súkromného kľúča zničená.

Súkromné kľúče servera OCSP, určené na podpisovanie OCSP odpovedí, sú uchovávané v kryptografickom module servera SNCA a za žiadnych okolností neopúšťajú kryptografický modul.

Kryptografický modul servera SNCA zodpovedá požiadavkám štandardu FIPS 140-1 level 3.

6.9 Sieťová bezpečnosť

Systém a pravidlá na zaistenie sieťovej bezpečnosti, sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.8.

6.10 Riadenie bezpečnostných incidentov

Systém riadenia bezpečnostných incidentov je popísaný a definovaný v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.9.

6.11 Zber dôkazov

Všeobecné požiadavky na zber dôkazov sú popísané a definované v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.10.

V súvislosti s poskytovaním služby OCSP, je zber dôkazov zabezpečovaný zaznamenávaním a bezpečným uchovávaním informácií, súvisiacich s poskytovaním služby OCSP.

Procesy pri poskytovaní OCSP odpovedí zaznamenávajú auditné stopy, z ktorých je možné spätne analyzovať priebeh vydania OCSP odpovede.

6.12 Riadenie kontinuity činnosti organizácie

Pre prípad vzniku pohromy má poskytovateľ definovaný a udržiavaný plán kontinuity. V prípade pohromy (vrátanie kompromitácie súkromného kľúča alebo iných citlivých údajov SNCA), musí byť prevádzka SNCA obnovená v rámci oneskorenia, definovaného v pláne kontinuity.

6.13 Ukončenie činnosti SNCA a plány ukončenia činnosti

Postup ukončenia činnosti poskytovateľa je popísaný a definovaný v dokumente „Politika poskytovania dôveryhodných služieb NASES“, bod 7.12.

6.14 Zhoda

NASES, ako prevádzkovateľ SNCA a poskytovateľ služby OCSP, garantuje bezpečnú prevádzku systému OCSP SNCA a dostupnosť uvedenej služby. Poskytovanie služby vyhotovovania OCSP odpovedí sa riadi:

- Nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES, Zákonom č. 272/2016 Z. z. o dôveryhodných službách,
- Ostatnými, všeobecne platnými nariadeniami, platnými v SR, vzťahujúcimi sa k výkonu tejto činnosti.

7 Profil certifikátu OCSP

Certifikát OCSP musí byť vydaný v súlade so štandardom X.509 verzia 3.

OCSP odpovede musia byť v zmysle RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

7.1 Rozšírenie na použitie kľúča

Podpis protokolu OCSP – OCSP Signing (OID 1.3.6.1.5.5.7.3.9)