

VNESITE STOPNJO TAJNOSTI

Priloga 17: Vsebina dokumentacije za začetek postopka ugotavljanja ustreznosti kriptografske rešitve**DOKUMENTACIJA K PREDLOGU
ZA UVEDBO POSTOPKA UGOTAVLJANJA USTREZNOSTI KRIPTOGRAFSKE REŠITVE ZA
VAROVANJE TAJNIH PODATKOV****PROIZVAJALEC**

Ime podjetja: _____

Sedež podjetja: _____

Odgovorna oseba: _____

Kontaktna oseba (navedite osebo, s katero bo nacionalni varnostni organ v tem postopku sodeloval):

Ime in priimek kontaktne osebe: _____

Telefonska številka kontaktne osebe: _____

Elektronski naslov kontaktne osebe: _____

KRIPTOGRAFSKA REŠITEV

Ime kriptografske rešitve: _____

Kratek opis delovanja kriptografske rešitve, vključno s predvidenim namenom uporabe:

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

VRSTA POSTOPKA: (ustrezno označite)

[A] ugotavljanje varnostne ustreznosti nove kriptografske rešitve

[B] ugotavljanje varnostne ustreznosti nadgradnje varnostno ustrezne kriptografske rešitve

[C] ostalo: _____
(navedite)

Če ste označili točko **[A]**, priložite zahtevano dokumentacijo
(glej **[A] NOVA KRIPTOGRAFSKA REŠITVE; ZAHTEVANA DOKUMENTACIJA**).

Če ste označili točko **[B]**, priložite zahtevano dokumentacijo
(glej **[B] NADGRADNJA VARNOSTNO USTREZNE KRIPTOGRAFSKE REŠITVE; ZAHTEVANA DOKUMENTACIJA**)

in navedite številko in datum potrdila o varnostni ustreznosti že potrjene kriptografske rešitve:

datum potrdila: _____ številka potrdila: _____

Če ste označili točko **[C]**, priložite zahtevano dokumentacijo
(glej **[C] OSTALO; ZAHTEVANA DOKUMENTACIJA**).

V/Na _____ , dne _____

Ime in priimek odgovorne osebe

Podpis kontaktne osebe

Podpis odgovorne osebe

Žig

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

[A] NOVA KRIPTOGRAFSKA REŠITEV

ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti v slovenskem jeziku, celovitost in jasnost opisov imata neposredni vpliv na časovni potek postopka)

1. O
 pis kriptografske rešitve, in sicer:
 - a) p
 odroben opis delovanja kriptografske rešitve, vseh njenih načinov uporabe, vključno z njeno namembnostjo. V kolikor gre za kompleksnejšo rešitev lahko proizvajalec dodatno pripravi tudi osebno predstavitev;
 popis vseh kriptografskih mehanizmov, ki jih izvajajo varnostne funkcije, kot so kriptografski algoritmi, generatorji naključnih števil, razni kriptografski protokoli, kriptografski ključi (tajni in javni), podatki za overitev in drugi varnostno pomembni parametri, katerih razkritje bi lahko ogrozilo varnost kriptografske rešitve. Možna je uporaba drugih mehanizmov, ki zagotavljajo ustrezno zaščito tajnih podatkov. Pri kriptografskih mehanizmih, kjer se ocena varnosti presoja z dolžino ključa se le ta navede.
2. O
 pis vlog in funkcij pooblaščenih uporabnikov kriptografske rešitve ter opis mehanizmov overjanja, in sicer:
 - a) o
 pis vseh vlog, ki jih podpira kriptografska rešitev;
 - b) o
 pis vseh funkcij, servisov in operacij, ki jih lahko določene vloge opravljajo;
 - c) o
 pis mehanizmov overjanja, overitvenih podatkov in inicializacije.
3. O
 pis vseh stanj kriptografske rešitve:
 - a) o
 pis vseh stanj kriptografske rešitve;
 - b) o
 pis prehodov med različnimi stanji kriptografske rešitve.
4. O
 pis zaščite opreme:
 - a) o
 pis mehanske zaščite strojne opreme;
 - b) o
 pis zaščite pred nedovoljenimi posegi v kriptografsko rešitev (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
 - c) o
 pis okoliških parametrov (temperatura, vlažnost, napajanje, ...) delovanja.
5. O
 pis delovnega okolja:
 - a) o
 pis delovnega okolja glede na možnost spreminjanja in dostopa do delovnega okolja;

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

- b) pis delovnega okolja glede na možnost spreminjanja in dostopa do kriptografske rešitve; o
- c) p operacijskega sistema in razčlenitev neprizeto nastavljenih parametrov. ti
6. pis upravljanja s kriptografskimi ključi: O
- a) pis vseh kriptografskih ključev ali sestavnih delov, s pomočjo katerih ključi nastajajo; o
- b) pis načinov za generiranje kriptografskih ključev; o
- c) pis načinov za vzpostavljanje kriptografskih ključev; o
- d) pis postopka vnosa in iznosa kriptografskih ključev; o
- e) pis načinov shranjevanja kriptografskih ključev; o
- f) pis postopka brisanja/uničenja kriptografskih ključev. o
7. odroben opis vseh varnostnih funkcij (kriptografski protokoli, kriptografski mehanizmi,...): P
- a) pis vseh varnostnih funkcij, načinov uporabe, vhodnih parametrov, izhodnih parametrov, ...; o
- b) atančen opis kriptografskih prvin in protokolov, kateri zagotavljajo zaupnost, celovitost, pristnost, razpoložljivost in nezatajljivost. n
8. odroben opis delovanja generatorja naključnih števil: P
- a) pis delovanja, virov entropije, če obstajajo; o
- b) okaz statistične pravilnosti delovanja (opis izvedenih statističnih in ostalih testov); d
- c) pis mehanizmov zaščite pred možnimi kompromitacijami. o
9. pis samopreizkušanja: O
- a) pis postopka samopreizkušanja, vključno s preizkušanjem pri zagonu in vsemi pogojnimi preizkusi; o
- b) pis stanj, ko samopreizkušanje ni uspešno, in postopek za vzpostavitev ponovnega operativnega delovanja; o
- c) pis vseh varnostno kritičnih funkcij, ki se pri zagonu kriptografske rešitve preverijo; o

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

- d) o
pis mehanizma izključitve varnostnih funkcij kriptografske rešitve, če ta obstaja.
10. O
pis življenjskega cikla kriptografske rešitve:
- a) o
pis postopkov za varno generiranje, namestitvev in zagon kriptografske rešitve, vključno z morebitno nadgradnjo z novimi različicami;
- b) b
ločna predstavitev posameznih varnostno pomembnih programskih podsklopov z izvlečki izvirne programske kode (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
- c) i
zvorna programska koda (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
- d) o
pis strojne, programske in/ali strojno - programske opreme in bločna predstavitev posameznih varnostno pomembnih strojnih, programskih in/ali strojno – programskih podsklopov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);
- e) o
pis (za vse programske, strojne in strojno-programске sestavne dele) vhodnih parametrov, vseh funkcij, ki se izvedejo na podlagi vhodnih parametrov, ter pričakovanih rezultatov, ko se te funkcije izvedejo;
- f) o
pis fizičnih vhodov/izhodov in logičnih vmesnikov z določenimi vhodnimi/izhodnimi potmi;
- g) o
pis fizičnih in logičnih kontrol kriptografskih rešitev, opis fizičnih in logičnih kazalnikov stanja;
- h) o
pis postopka brisanja/uničenja varnostno pomembnih parametrov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).
11. N
avodila za skrbnike kriptografskega materiala:
- a) o
pis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal;
- b) p
ostopek za varno upravljanje kriptografske rešitve;
12. N
avodila za uporabnika: (Uporabniški priročnik)
- a) o
dobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;
- b) p
opis nalog, ki zagotavljajo varno delovanje kriptografske rešitve.
13. O
pis razvojnega okolja in razvojnih procesov (za kriptografske rešitve, ki se uporabljajo za

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):

- | | | |
|------|---|---|
| a) | pis razvojnega okolja; | o |
| b) | avedite in opišite teste, ki ste jih izvedli v fazah razvoja kriptografske rešitve za: | n |
| i. | reverjanje pravilnosti delovanja kriptografske rešitve; | p |
| ii. | ripravo varnostne analize izvirne programske kode kriptografske rešitve; | p |
| iii. | reverjanje robustnosti strojne opreme; | p |
| iv. | ripravo varnostne analize kriptografske rešitve kot celote; | p |
| v. | pis mehanizmov zaščite pred možnimi kompromitacijami. | o |
| c) | avedite načine testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji,...); | n |
| d) | ripravite testna orodja, ki jih bo nacionalni varnostni organ potreboval pri testiranju in morebitno dodatno opremo za izvedbo postopka. | p |
| 14. | pis dobavne verige varnostno pomembnih gradnikov kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna). | O |

[B] NADGRADNJA VARNOSTNO USTREZNE KRIPTOGRAFSKE REŠITVE

ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku, celovitost in jasnost opisov imata neposredni vpliv na časovni potek postopka)

- | | | |
|-----|---|---|
| 1. | atančen opis spremenjenih ali novih funkcionalnosti nadgradnje varnostno ustrezne kriptografske rešitve (v nadaljnjem besedilu: nadgradnja). | N |
| 2. | pis razvojnega okolja in razvojnih procesov nadgradnje (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna): | O |
| a) | pis razvojnega okolja; | o |
| b) | avedite in opišite teste, ki ste jih izvedli v fazah razvoja nadgradnje za: | n |
| i. | reverjanje pravilnosti delovanja nadgradnje; | p |
| ii. | ripravo varnostne analize izvirne programske kode nadgradnje; | p |

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

- | | | |
|------|--|---|
| iii. | reverjanje robustnosti strojne opreme; | p |
| iv. | ripravo varnostne analize nadgradnje kot celote; | p |
| v. | pis mehanizmov zaščite pred možnimi kompromitacijami. | o |
| c) | avedite načine testiranja varnosti (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji,...); | n |
| d) | ripravite testna orodja, ki jih bo nacionalni varnostni organ potreboval pri testiranju in morebitno dodatno opremo za izvedbo postopka. | p |
| 3. | pecifikacija navodil za uporabnika: (Uporabniški priročnik) | S |
| a) | dobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal; | o |
| b) | opis nalog, ki zagotavljajo varno delovanje nadgradnje. | p |
| 4. | pis postopka razdelitve nadgradnje avtoriziranim skrbnikom kriptografskega materiala: | O |
| a) | pis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal; | o |
| b) | ostopek za varno upravljanje nadgradnje; | p |
| c) | redpostavke, ki so varnostno pomembne pri ravnanju uporabnika z nadgradnjo. | p |
| 5. | pis dobavne verige varnostno pomembnih gradnikov nadgradnje (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna). | O |

[C] OSTALO

ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku, celovitost in jasnost opisov imata neposredni vpliv na časovni potek postopka)

- | | | |
|----|--|---|
| 1. | odroben opis delovanja rešitve (oz. sistema, sheme, mehanizma,...), vseh njenih načinov uporabe, vključno z njeno namembnostjo in dokazom pravilnosti delovanja. V kolikor gre za kompleksnejšo rešitev lahko proizvajalec pripravi osebno predstavitev. | P |
| 2. | pis razvojnega okolja in razvojnih procesov rešitve (za rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna): | O |
| a) | | o |

VNESITE STOPNJO TAJNOSTI

VNESITE STOPNJO TAJNOSTI

- pis razvojnega okolja;
- b) n
- avedite in opišite teste, ki ste jih izvedli v fazah razvoja rešitve za:
- i. p
- reverjanje pravilnosti delovanja;
- ii. p
- reverjanje robustnosti delovanja;
- iii. p
- ripravo varnostne analize rešitve;
- iv. o
- pis mehanizmov zaščite pred možnimi kompromitacijami.
- c) n
- avedite načine testiranja varnosti (testni vektorji, dokaz ekvivalentnosti s standardnimi protokoli, testni scenariji,...);
- d) p
- ripravite testna orodja, ki jih bo nacionalni varnostni organ potreboval pri testiranju in morebitno dodatno opremo za izvedbo postopka.
3. O
- pis dobavne verige varnostno pomembnih gradnikov rešitve (za rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

VNESITE STOPNJO TAJNOSTI