Priloga 17: Vsebina dokumentacije za začetek postopka ugotavljanja ustreznosti kriptografske rešitve

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

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 organ v tem postopku sodeloval):

Ime in priimek kontaktne osebe: _____

Delovno mesto 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:

_____

_____

_____

_____

IZPOLNI PROIZVAJALEC

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 REŠITEV; ZAHTEVANA DOKUMENTACIJA**).

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

ter 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

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

[A] NOVA KRIPTOGRAFSKA REŠITEV
ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Opis kriptografske rešitve (modula), in sicer:

a) podroben opis delovanja kriptografske rešitve, vseh njenih načinov uporabe, vključno z njeno namembnostjo. Če gre za bolj zapleteno rešitev, lahko proizvajalec pripravi osebno predstavitev;

b) podroben opis vseh kriptografskih mehanizmov, ki izvajajo varnostne funkcije. Običajno so to šifrirni 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.

2. Opis vlog in funkcij pooblaščenih uporabnikov kriptografske rešitve ter opis mehanizmov overjanja, in sicer:

a) opis vseh vlog, ki jih podpira kriptografska rešitev;

b) opis vseh funkcij, servisov in operacij, ki jih lahko določene vloge opravljajo;

c) opis mehanizmov overjanja, overitvenih podatkov in inicializacije.

3. Opis modela končnih stanj:

a) opis modela vseh končnih stanj kriptografskega modula;

b) opis prehodov med različnimi končnimi stanji kriptografskega modula.

4. Opis fizične varnosti:

a) opis fizične materialne zaščite;

b) poročilo o ustrezni zaščiti pred neželenim elektromagnetnim sevanjem (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);

c) opis postopka brisanja varnostno pomembnih parametrov;

d) opis okoliških parametrov (temperatura, vlažnost, napajanje ...) delovanja.

5. Opis delovnega okolja:

a) opis delovnega okolja glede na možnost spreminjanja in dostopa do delovnega okolja;

b) opis delovnega okolja glede na možnost spreminjanja in dostopa do že delujoče kriptografske rešitve;

c) tip operacijskega sistema in razčlenitev neprivzeto nastavljenih parametrov.

6. Opis upravljanja kriptografskih ključev:

a) opis vseh kriptografskih ključev ali sestavnih delov, s pomočjo katerih ključi nastajajo;

b) podroben opis vseh generatorjev naključnih števil;

c) opis načinov za generiranje kriptografskih ključev;

d) opis načinov za vzpostavljanje kriptografskih ključev;

e) opis postopka vnosa in iznosa kriptografskih ključev;

f) opis načinov shranjevanja kriptografskih ključev;

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

g) opis postopka brisanja kriptografskih ključev.

7. Opis samopreizkušanja:

a) opis postopka samopreizkušanja, vključno s preizkušanjem pri zagonu in vsemi pogojnimi preizkusi;

b) opis stanj, ko samopreizkušanje ni uspešno, in postopek za vzpostavitev ponovnega normalnega operativnega delovanja;

c) opis vseh varnostno kritičnih funkcij, ki se pri zagonu kriptografske rešitve preverijo;

d) opis mehanizma izključitve varnostnih funkcij kriptografske rešitve, če ta obstaja.

8. Opis življenjskega cikla kriptografske rešitve:

a) opis postopkov za varno generiranje, namestitev in zagon kriptografske rešitve, vključno z morebitno nadgradnjo z novimi različicami;

b) bločna predstavitev posameznih varnostno pomembnih programskih podsklopov z izvlečki izvorne programske kode (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);

c) izvorna programska koda (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);

d) opis strojne, programske oziroma strojno-programske opreme in bločna predstavitev posameznih varnostno pomembnih strojnih, programskih ali strojno-programskih podsklopov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna);

e) opis (za vse programske, strojne in strojno-programske sestavne dele) vhodnih parametrov, vseh funkcij, ki se izvedejo na podlagi vhodnih parametrov, ter pričakovanih rezultatov, ko se te funkcije izvedejo;

f) opis fizičnih vhodov/izhodov in logičnih vmesnikov z določenimi vhodnimi/izhodnimi potmi;

g) opis ročnih in logičnih kontrol kriptografskih rešitev, opis fizičnih in logičnih kazalnikov statusa.

9. Opis postopka razdelitve kriptografske rešitve avtoriziranim skrbnikom kriptografskega materiala:

a) opis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal;

b) postopek za varno upravljanje kriptografske rešitve;

c) varnostno pomembne domneve glede na ravnanje uporabnika kriptografske rešitve.

10. Navodila za uporabnika (uporabniški priročnik):

a) odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;

b) naloge, ki zagotavljajo varno delovanje kriptografske rešitve.

11. Opis razvojnega okolja in razvojnih procesov (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):

a) opis razvojnega okolja;

b) navedba in opis testov, ki ste jih izvedli v fazah razvoja kriptografske rešitve za:

   i. preverjanje pravilnosti delovanja kriptografske rešitve;

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

ii. preverjanje robustnosti strojne opreme;

iii. varnostno analizo kriptografske rešitve, možnosti kompromitacij;

c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);

d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.

12. Opis 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).

[B] NADGRADNJA VARNOSTNO USTREZNE KRIPTOGRAFSKE REŠITVE
ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Natančen opis spremenjenih ali novih funkcionalnosti nadgradnje kriptografske rešitve (modula).

2. Opis razvojnega okolja in razvojnih procesov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):

a) opis razvojnega okolja;

b) navedba in opis testov, ki so bili izvedeni v fazah razvoja nadgradnje kriptografske rešitve za:

i. preverjanje pravilnosti delovanja kriptografske rešitve;

ii. preverjanje robustnosti strojne opreme;

iii. varnostno analizo kriptografske rešitve, možnosti kompromitacij;

c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);

d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.

3. Specifikacija navodil za uporabnika (uporabniški priročnik):

a) odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;

b) naloge, ki zagotavljajo varno delovanje kriptografske rešitve.

4. Opis postopka razdelitve kriptografske rešitve avtoriziranim skrbnikom kriptografskega materiala:

a) opis administrativnih funkcij, varnostnih dogodkov, varnostnih parametrov, fizičnih in logičnih vmesnikov, ki jih bo uporabljal;

b) postopek za varno upravljanje kriptografske rešitve;

c) varnostno pomembne domneve glede na ravnanje uporabnika kriptografske rešitve.

VNESITE STOPNJO TAJNOSTI

IZPOLNI PROIZVAJALEC

VNESITE STOPNJO TAJNOSTI

5. Opis dobavne verige varnostno pomembnih gradnikov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

[C] OSTALO _____
ZAHTEVANA DOKUMENTACIJA (dokumentacija mora biti zapisana v slovenskem jeziku)

1. Podroben (matematični) opis delovanja nekriptografske rešitve (oz. sistema, sheme, mehanizma …) in dokaz pravilnosti delovanja nekriptografske rešitve (oz. sistema, sheme, mehanizma …).

2. Opis razvojnega okolja in razvojnih procesov nadgradnje kriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna):

a) opis razvojnega okolja;

b) navedba in opis testov, ki ste jih izvedli v fazah razvoja nekriptografske rešitve za:
   i. preverjanje pravilnosti delovanja;
   ii. preverjanje robustnosti delovanja;
   iii. varnostno analizo nekriptografske rešitve, možnosti kompromitacij;

c) navedba načinov testiranja varnosti tega protokola (testni vektorji, dokaz ekvivalentnosti s standardnim kriptografskim protokolom, testni scenariji ipd.);

d) priprava testnih orodij, ki jih bo nacionalni varnostni organ potreboval pri testiranju, in morebitne dodatne opreme za izvedbo postopka.

3. Opis dobavne verige varnostno pomembnih gradnikov nekriptografske rešitve (za kriptografske rešitve, ki se uporabljajo za varovanje tajnih podatkov stopnje tajnosti INTERNO, navedba te točke ni nujno potrebna).

VNESITE STOPNJO TAJNOSTI