Na podlagi četrtega odstavka 15. člena Uredbe o varovanju tajnih podatkov v komunikacijsko-informacijskih sistemih (Uradni list RS, št. 48/07) Komisija za informacijsko varnost izdaja

NAVODILO
o postopku odobritve uporabe šifrirnih rešitev

1. člen
(predmet urejanja)

Navodilo opredeljuje postopke odobritve uporabe šifrirnih rešitev v Republiki Sloveniji.

2. člen
(pomen izrazov)

(1) Šifrirne rešitve so šifrirna oprema (strojna in programska) in sistemi, ki se uporabljajo za šifrirno varovanje podatkov v komunikacijsko-informacijskih sistemih, v katerih se obravnavajo tajni podatki (v nadaljnjem besedilu: sistemi). Med šifrirne rešitve spadajo tudi vsi moduli (sklopi), ki so vgrajeni v posameznih delih sistemov in so namenjeni šifrirnemu varovanju podatkov.

(2) Potrdilo o varnostni ustreznosti je dokument, ki upravljavcem sistemov dovoljuje uporabo šifrirno ovrednotenih rešitev.

(3) Šifrirno ovrednotenje je postopek, v katerem se ugotovi primernost predlagane šifrirne rešitve za varovanje tajnih podatkov določene stopnje tajnosti.

3. člen
(uporaba šifrirnih rešitev)

V sistemih je za varovanje tajnih podatkov dovoljeno uporabljati le tiste šifrirne rešitve, za katere je izdano potrdilo o varnostni ustreznosti.

4. člen
(potrdilo o varnostni ustreznosti)

(1) Potrdilo o varnostni ustreznosti izda Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljnjem besedilu: UVTP) ali drug z zakonom določen organ, in sicer za vsako šifrirno rešitev posebej.

(2) Oblika potrdila je navedena v prilogi I.

(3) Potrdilo o varnostni ustreznosti se izda na podlagi ugotovitev šifrirnega ovrednotenja predložene šifrirne rešitve, ki ga opravi Komisija za informacijsko varnost (v nadaljnjem besedilu: komisija) ali drug z zakonom določen organ, ter odobrenih minimalnih varnostnih zahtev za označevanje, distribucijo in uporabo.

5. člen
(priznavanje potrdil o varnostni ustreznosti šifrirnih rešitev tujih držav in mednarodnih združenj)

(1) Urad ali drug z zakonom določen organ lahko na podlagi potrdila o varnostni ustreznosti šifrirnih rešitev, ki ga izda za to pooblaščen tuji nacionalni ali mednarodni varnostni organ,

izda enakovredno potrdilo o varnostni ustreznosti za uporabo teh rešitev v sistemih Republike Slovenije.

(2) Za šifrirne rešitve iz prvega odstavka tega člena se lahko pridobi potrdilo o varnostni ustreznosti brez izvedbe postopka varnostnega ovrednotenja, če se bodo uporabile v sistemih, ki obravnavajo tajne podatke stopnje INTERNO.

(3) Šifrirne rešitve iz prvega odstavka tega člena, namenjene uporabi v sistemih, ki obravnavajo tajne podatke stopnje ZAUPNO ali višje, morajo biti šifrirno ovrednotene.

(4) V sistemih, ki obravnavajo tajne podatke stopnje STROGO TAJNO, izključno tujih šifrirnih rešitev ni dovoljeno uporabljati.

6. člen
(postopek šifrirnega ovrednotenja)

(1) V postopku šifrirnega ovrednotenja se preverja stopnja varnosti arhitekture in izvedbe šifrirnih rešitev.

(2) Šifrirno ovrednotenje se opravi na podlagi zahtevane dokumentacije, ki je navedena v prilogi II.

(3) Pri šifrirnem ovrednotenju šifrirnih rešitev v sistemih, ki obravnavajo tajne podatke stopnje INTERNO, komisija pregleda zahtevano dokumentacijo.

(4) Pri šifrirnem ovrednotenju šifrirnih rešitev v sistemih, ki obravnavajo tajne podatke stopnje ZAUPNO, komisija poleg ovrednotenja, navedenega v tretjem odstavku tega člena, izvede še funkcionalni preizkus šifrirnih rešitve v celoti in posameznih šifrirnih mehanizmov.

(5) Pri šifrirnem ovrednotenju šifrirnih rešitev v sistemih, ki obravnavajo tajne podatke stopnje TAJNO ali STROGO TAJNO, komisija poleg ovrednotenja, navedenega v četrtem odstavku tega člena, izvede še analizo možnosti kompromitiranja varnostno pomembnih parametrov, ki vključuje penetracijske preizkuse.

(6) Komisija lahko prizna šifrirno vrednotenje drugega nacionalnega organa za komunikacijsko varnost države članice Evropske unije ali zveze NATO, če člani komisije tako mnenje sprejmejo soglasno.

7. člen
(splošne varnostne zahteve šifrirnih rešitev)

Šifrirna rešitev mora izpolnjevati naslednje pogoje:

- izvedeni morajo biti taki šifrirni primitivi, ki omogočajo zaščito tajnih podatkov,
- zaščitena mora biti pred nepooblaščenim ravnanjem ali uporabo,
- onemogočiti mora nepooblaščeno odkritje vsebine in varnostno pomembnih parametrov,
- onemogočiti mora nepooblaščeno in neugotovljivo spreminjanje šifrirnih modulov in algoritmov, vključno z nepooblaščenim spreminjanjem, nadomeščanjem, vrinjenjem ali izbrisom šifrirnih ključev in drugih varnostno pomembnih parametrov,
- med delovanjem mora biti vidno stanje,v katerem je,
- zagotovljeno mora biti pravilno delovanje varnostnih mehanizmov,
- zagotovljeno mora biti odkrivanje napak med delovanjem in vzpostavljen mehanizem, ki preprečuje kompromitiranje varnostno pomembnih parametrov.

8. člen
(šifrirne rešitve s programsko opremo)

(1) Šifrirne rešitve, ki so uresničene s programsko opremo, se kot samostojne rešitve lahko uporabljajo za varovanje podatkov stopnje tajnosti INTERNO.

(2) Šifrirne rešitve, ki so uresničene z namensko programsko opremo, razvito in izdelano v državnih organih, se kot samostojne rešitve lahko uporabljajo za varovanje podatkov vključno do stopnje tajnosti ZAUPNO.

9. člen
(zahteve za označevanje, distribucijo in uporabo)

(1) Za vsako šifrirno rešitev morajo biti izdelane minimalne varnostne zahteve za označevanje, distribucijo in uporabo, ki jih odobri komisija ali drug z zakonom določen organ, in sicer za vsako posamezno šifrirno rešitev posebej.

(2) Upoštevane morajo biti tudi varnostne zahteve, ki izhajajo iz članstva Republike Slovenije v mednarodnih organizacijah oziroma jih je Republika Slovenija sprejela s sklenitvijo drugih mednarodnih pogodb in sporazumov.

10. člen
(kombinacije šifrirnih rešitev)

(1) Kombinacije posameznih (samostojnih) šifrirnih rešitev je mogoče v posebnih primerih uporabljati tudi za varovanje podatkov višje stopnje tajnosti, kot to omogoča posamezna šifrirna rešitev.

(2) Taka kombinirana šifrirnih rešitev je obravnavana kot nova šifrirna rešitev in tudi zanjo velja to navodilo.

11. člen
(evidenca šifrirnih rešitev)

UVTP vodi evidenco šifrirnih rešitev, za katere je izdano potrdilo o varnostni ustreznosti.

12. člen
(veljavnost)

Navodilo začne veljati naslednji dan po podpisu.

Igor Eršte
PREDSEDNIK KOMISIJE

Številka: 0220-1/2010/61
Datum: 7.12.2010

PRILOGA:1

Vzorec potrdila o varnostni ustreznosti

Glava izdajatelja potrdila

Izdajatelj potrdila na podlagi prvega odstavka 4. člena Navodila o postopku odobritve uporabe šifrirnih rešitev izdaja

POTRDILO O VARNOSTNI USTREZNOSTI

za šifrirno napravo/sistem _____ _____

proizvajalca

_____,

ki se bo uporabljala v sistemu _____

_____

za prenos tajnih podatkov do stopnje tajnosti

STOPNJA TAJNOSTI

Potrdilo velja od _____

do/za dobo _____

Številka:
Datum:

Pečat podpis predstojnika

Številka dokumenta:

PRILOGA: 2

Zahtevana dokumentacija

1. Opis varnostnih funkcij, ki jih šifrirna rešitev izvaja.

2. Opis šifrirne rešitve (modula), in sicer:
   a. specifikacija strojnih, programskih in strojno-programskih sestavnih delov, specifikacija drugih sestavnih delov, ki niso varnostno pomembni, in opis materialnega videza;
   b. specifikacija fizičnih vhodov/izhodov in logičnih vmesnikov z določenimi vhodnimi/izhodnimi potmi;
   c. specifikacija ročnih in logičnih kontrol šifrirnih rešitev, specifikacija fizičnih in logičnih kazalnikov statusa;
   d. specifikacija vseh varnostnih funkcij in načinov delovanja;
   e. bločni diagram vseh pomembnejših strojnih ali/in programskih podsklopov s poudarkom na sestavinah, kjer so varnostno pomembni parametri;
   f. specifikacija vseh varnostno pomembnih parametrov, kot so šifrirni algoritmi, generatorji naključnih števil, razni šifrirni protokoli, šifrirni ključi (tajni in javni), avtentikacijski podatki (pin, geslo), in drugi varnostno pomembni parametri, katerih razkritje bi lahko ogrozilo varnost šifrirne rešitve;
   g. specifikacija varnostne politike uporabe in delovanja šifrirnega modula.

3. Opis vlog in funkcij pooblaščenih uporabnikov šifrirne rešitve ter opis avtentikacijskega mehanizma, in sicer:
   a. specifikacija vseh avtoriziranih vlog, ki jih podpira šifrirna rešitev;
   b. specifikacija vseh funkcij, servisov in operacij;
   c. specifikacija avtentikacijskih mehanizmov, opis avtentikacijskih podatkov in inicializacije.

4. Opis modela končnih stanj.

5. Opis fizične varnosti:
   a. specifikacija fizične materialne zaščite;
   b. specifikacija postopka brisanja varnostno pomembnih parametrov, če šifrirna rešitev omogoča vzdrževalni dostop;
   c. specifikacija okoljskih parametrov (temperatura, vlažnost, napajanje, ...) operativnega delovanja.

6. Opis operativnega okolja:
   a. specifikacija operativnega okolja glede na možnost spreminjanja funkcionalnosti že delujoče šifrirne rešitve;
   b. specifikacija operacijskega sistema.

7. Opis upravljanja šifrirnih ključev:
   a. specifikacija vseh šifrirnih ključev ali sestavnih delov, s pomočjo katerih ključi nastajajo;
   b. specifikacija vseh generatorjev naključnih števil;
   c. specifikacija načinov za generiranje šifrirnih ključev;
   d. specifikacija načinov za vzpostavljanje šifrirnih ključev;
   e. specifikacija postopka vnosa in iznosa šifrirnih ključev;
   f. specifikacija načinov shranjevanja šifrirnih ključev;
   g. specifikacija postopka brisanja šifrirnih ključev.

8. Opis samopreizkušanja:
    a. specifikacija postopka samopreizkušanja, vključno s preizkušanjem pri zagonu in vsemi pogojnimi preizkusi;
    b. specifikacija stanj, ko samopreizkušanje ni uspešno, in postopek za vzpostavitev ponovnega normalnega operativnega delovanja;
    c. specifikacija vseh varnostno kritičnih funkcij, ki se pri zagonu šifrirne rešitve preverijo;
    d. specifikacija mehanizma izključitve varnostnih funkcij šifrirne rešitve, če ta obstaja.

9. Opis varnostnega jamstva življenjskega cikla šifrirne rešitve:
    a. specifikacija postopkov za varno generiranje, namestitev in zagon šifrirne rešitve, vključno z morebitno nadgradnjo z novimi različicami;
    b. specifikacija, ki povezuje razvito šifrirno rešitev z navedenimi varnostnimi funkcijami;
    c. specifikacija izvorne programske kode in bločna predstavitev posameznih varnostno pomembnih programskih podsklopov;
    d. specifikacija strojne opreme in bločna predstavitev posameznih varnostno pomembnih strojnih podsklopov;
    e. specifikacija (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. specifikacija za navodila kriptoadministratorju:
        i. administrativne funkcije, varnostni dogodki, varnostni parametri, fizični in logični vmesniki, ki jih bo uporabljal;
        ii. postopek za varno upravljanje šifrirne rešitve;
        iii. predpostavke, ki so varnostno pomembne glede na ravnanje uporabnika šifrirne rešitve;
    g. specifikacija za navodila uporabniku:
        i. odobrene varnostne funkcije, fizični in logični vmesniki, ki jih bo uporabljal;
        ii. naloge, ki zagotavljajo varno delovanje šifrirne rešitve.