

VENDIM
Nr. 771, datë 19.12.2025

**PËR PROCEDURAT PËR PËRZGJEDHJEN, OPERIMIN, MIRËMBAJTJEN,
SHPËRNDARJEN DHE MENAXHIMIN E MATERIALEVE KRIPTOGRAFIKE¹**

Në mbështetje të nenit 100 të Kushtetutës dhe të pikave 3 e 4, të nenit 45, të ligjit nr. 10/2023, “Për informacionin e klasifikuar”, me propozimin e ministrit të Mbrojtjes, Këshilli i Ministrave

VENDOSI:

Neni 1
Objekti

Objekti i këtij vendimi është përcaktimi i procedurave për përzgjedhjen, operimin, mirëmbajtjen, shpërndarjen dhe menaxhimin e materialeve kriptografike.

Neni 2
Qëllimi

Qëllimi i këtij vendimi është garantimi i mbrojtjes kriptografike të informacionit të klasifikuar që prodhohet, përpunohet, ruhet dhe transmetohet në sistemet e komunikimit e të informacionit (në vijim SKI).

Neni 3
Fusha e veprimit

Ky vendim zbatohet për mbrojtjen kriptografike në SKI, që trajtojnë informacion të klasifikuar “Sekret shtetëror” të NATO-s, BE-së, shteteve dhe/ose organizatave të huaja, me të cilat Republika e Shqipërisë ka marrëveshje sigurie.

Neni 4
Përkufizime

Në këtë vendim, termat e mëposhtëm kanë këto kuptime:

1. “AKSIK”, Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar.
2. “Algoritëm kriptografik”, një ekuacion matematikor që, nëpërmjet ngatërimit të tekstit të hapur, e transformon informacionin në të palexueshëm (dhe anasjelltas).
3. “Autorizim kripto”, dokumenti që cakton personelin e institucionit shtetëror ose të operatorit ekonomik përgjegjës për sigurinë e “Pajisjes kriptografike të kontrolluar”.
4. “Pajisje kriptografike e kontrolluar”, pajisja kriptografike e specifikuar si e tillë nga vendi prodhues.
5. “Çelës kriptografik”, një informacion i ruajtur zakonisht në një skedar, i cili, nëpërmjet një algoritmi kriptografik mund të kriptojë ose të dekriptojë të dhëna.
6. “Dekriptim”, procesi që transformon informacionin e kriptuar në informacion të hapur.

¹Ky vendim është përafëruar pjesërisht me vendimin e Këshillit, datë 23 shtator 2013, “Për rregullat e sigurisë për mbrojtjen e informacionit të klasifikuar të BE-së”, numri CELEX 32013D0488, Fletorja Zyrtare e Bashkimit Evropian, seria L, nr. 274, datë 15.10.2013, f. 1–50.

7. “Incident kriptografik” konsiderohet çdo ngjarje që cenon sigurinë e pajisjeve, programeve apo materialeve kriptografike, duke komprometuar procesin kriptografik.
8. “Komprometim i informacionit kriptografik” nënkupton vënien në dispozicion në mënyrë të qëllimshme ose jo të materialit kriptografik personave të paaautorizuar, si rrjedhojë e humbjes, vjedhjes, spiunazhit, rikuperimit, defekteve të materialit kriptografik, shikimit, fotografimit etj. dhe që cenon konfidencialitetin, disponibilitetin dhe integritetin e informacionit të klasifikuar.
9. “Korrier”, personeli i autorizuar nga titullari i institucionit për të realizuar transportimin e materialeve kriptografike.
10. “Kriptim”, procesi i transformimit të informacionit, në mënyrë të tillë që të fshehë përmbajtjen e tij.
11. “Kriptografia”, disiplina që përfshin principet, mjetet dhe metodat për të ofruar sigurinë e informacionit nëpërmjet konfidencialitetit, integritetit, autenticitetit e të disponibilitetit.
12. “Material kriptografik” përfshin çelësat në të gjitha format e tyre, dokumentet, kodet, pajisjet, që përmbajnë informacion kriptografik e që janë të rëndësishëm në procesin e kriptimit/ dekriptimit.
13. “Mbrotjtja kriptografike”, aplikimi i metodave dhe i mjeteve kriptografike, me qëllim mbrojtjen e informacionit të klasifikuar nga akseset e paaautorizuara gjatë krijimit, përpunimit, ruajtjes ose transmetimit.
14. “Pajisje kriptografike” nënkupton pajisje teknike që përdoret për mbrojtjen kriptografike të informacionit.
15. “Program kriptografik”, një soft, i cili, nëpërmjet algoritmeve dhe çelësve kriptografikë, bën të mundur procesin e kriptimit/dekriptimit.
16. “Ruajtësi krypto”, personeli i institucionit shtetëror ose i operatorit ekonomik, përgjegjës për operimin e materialeve kriptografike, i pajisur me “Autorizim krypto”.
17. “Sisteme kriptografike” nënkupton tërësinë e softeve kriptografike, pajisjeve kriptografike dhe materialeve kriptografike të përdorura si një njësi e vetme për të realizuar procesin kriptografik sipas rregullave përkatëse.

Neni 5

Procedurat për përzgjedhjen e materialeve kriptografike

1. Përzgjedhja e materialeve kriptografike është procesi, nëpërmjet të cilit bëhet përcaktimi i materialeve kriptografike, që garantojnë sigurinë e informacionit të klasifikuar, që prodhohet, ruhet, transmetohet dhe trajtohet në SKI.
2. Përzgjedhja e materialeve kriptografike kryhet nga administratori i SKI-së.
3. Procedura e përzgjedhjes së materialeve kriptografike konsiston në:
 - a) vlerësimin e nevojave teknike për mbrojtjen kriptografike, në përputhje me kërkesat funksionale dhe sigurinë e operimit të SKI-së;
 - b) konsultimin me Drejtorinë e Shifrës për:
 - i. pajisjet dhe sistemet që janë të miratuara për mbrojtjen kriptografike të informacionit të klasifikuar;
 - ii. çelësat kriptografikë që mund të sigurohen nga Drejtoria e Shifrës;
 - c) verifikimin e pajtueshmërisë me kërkesat e sigurisë, të përcaktuara nga Drejtoria e Shifrës me anë të një udhëzimi të klasifikuar “Sekret”, në zbatim të shkronjës “a”, të nenit 13, të vendimit nr. 792, datë 28.12.2023, të Këshillit të Ministrave, “Për miratimin e rregullores ‘Për përcaktimin e rregullave dhe të procedurave për sigurinë e informacionit të klasifikuar, që trajtohet në Sistemet e Komunikimit dhe Informacionit (SKI)’”.

4. Në rastet kur Drejtoria e Shifrës nuk disponon infrastrukturën e përshtatshme për prodhimin e çelësit kriptografik për pajisjet dhe sistemet kriptografike të përzgjedhura, kjo infrastrukturë sigurohet nga institucioni shtetëror ose nga operatori ekonomik dhe i kalohet në administrim Drejtorisë së Shifrës.

5. Përzgjedhja e materialeve kriptografike për mbrojtjen e informacionit të klasifikuar të NATO-s, BE-së apo shteteve dhe organizatave të tjera ndërkombëtare bëhet në përputhje me marrëveshjet e sigurisë për mbrojtjen e ndërsjellë të informacionit të klasifikuar.

Neni 6

Procedurat për operimin dhe mirëmbajtjen e materialeve kriptografike

1. Operimi dhe mirëmbajtja e materialeve kriptografike është procesi që përfshin përdorimin, ruajtjen, konfigurimin dhe ndryshimin e çelësve kriptografikë, me qëllim garantimin e funksionalitetit e të sigurisë së vazhdueshme të materialeve kriptografike.

2. Drejtoria e Shifrës kryen konfigurimin fillestar të materialeve kriptografike, përpara vendosjes në përdorim.

3. Operimi dhe mirëmbajtja e materialeve kriptografike bëhet nga ruajtësi krypto.

4. Ruajtësi krypto pajiset me “Autorizim krypto” nga titullari i institucionit shtetëror ose nga operatori ekonomik.

5. Ruajtësi krypto ka këto detyra:

a) Merr masa që materialet kriptografike të ruhen në ambiente të sigurta fizike, që garantojnë mbrojtjen nga dëmtimet dhe nga akseset e paautorizuara;

b) Zbaton kontrolle të vazhdueshme teknike për të garantuar funksionimin e duhur të materialeve kriptografike;

c) Koordinon me Drejtorinë e Shifrës për probleme teknike për të cilat ka nevojë për asistencë më të specializuar;

ç) Koordinon me Drejtorinë e Shifrës për ndryshimin e çelësve kriptografikë, sipas afateve të vlefshmërisë së çelësve.

Neni 7

Procedurat për shpërndarjen e materialeve kriptografike

1. Shpërndarja e materialeve kriptografike është procesi që siguron dërgimin dhe marrjen e sigurt të tyre në institucione shtetërore ose në operatorët ekonomikë, brenda territorit të Republikës së Shqipërisë, në përfaqësitë diplomatike, konsullore dhe në struktura të tjera të institucioneve shtetërore jashtë vendit.

2. Shpërndarja elektronike e materialeve kriptografike bëhet nëpërmjet:

a) SKI-ve të akredituara përshtatshmërisht për shpërndarjen e materialeve kriptografike;

b) kanaleve të komunikimit masiv dhe publik, të kriptuar me çelësat kriptografikë paraardhës aktivë kur:

i. përdoren për mbrojtjen e informacionit të klasifikuar me nivel klasifikimi “I kufizuar”;

ii. shpërndarja fillestare e çelësve kriptografikë bëhet në kanale të tjera komunikimi (rrjete të klasifikuara ose media të lëvizshme);

iii. fjalëkalimi i instalimit dërgohet i ndarë nga materialet kriptografike;

c) mediave të lëvizshme të miratuara nga AKSIK-u;

ç) pajisjeve të sigurta ngarkuese.

3. Shpërndarja fizike e materialeve kriptografike sigurohet nga korrieri i materialeve kriptografike, i shoqëruar nga një person tjetër, i cili autorizohet si shoqërues i korrierit dhe instruktohet për përgjegjësitë gjatë transportimit të materialeve kriptografike.

4. Korrieri merr në dorëzim materialet kriptografike nëpërmjet një procesverbali, i cili nënshkruhet nga korrieri dhe nga ruajtësi krypto.

5. Për shpërndarjen fizike të materialeve kriptografike ndiqen procedurat e mëposhtme:

a) Institucionet shtetërore ose operatorët ekonomikë, kur sigurojnë materiale kriptografike nga vendet e NATO-s e të BE-së dhe nevojitet transportimi i tyre, njoftojnë Drejtorinë e Shifrës;

b) Drejtoria e Shifrës koordinon me shërbimin me korrier të NATO-s dhe të BE-së për sigurimin e transportit të materialeve kriptografike;

c) Gjatë transportit, pajisjet kriptografike janë në gjendjen fillestare, të pakonfiguruar dhe pa çelësa kriptografikë, përjashtuar rastet kur konfigurimi fizik i tyre e bën të pamundur kthimin në gjendjen fillestare.

6. Gjatë shpërndarjes fizike të materialeve kriptografike, për paketimin e tyre, merren masat e mëposhtme:

a) Materiali kriptografik mbyllet me dy mbështjellëse jotransparente:

i. në mbështjellësen e brendshme shënohet adresa e dërguesit, adresa e marrësit, niveli i klasifikimit, i shoqëruar me shenjëzimin “Kriptografik” dhe instruksionin “Hapet vetëm nga (emri dhe mbiemri i marrësit)”;

ii. në mbështjellësen e jashtme shënohet adresa e dërguesit, adresa e marrësit dhe numri i regjistrimit dhe ndalohet vendosja e shenjëzimeve të tjera mbi këtë mbështjellëse;

b) Autoritetet doganore dhe të sigurisë i ekzaminonjë pakot me material kriptografik pa i hapur ato;

c) Korrierët sigurohen që materiali ka mbrojtjen maksimale gjatë të gjitha fazave të transportit të tij;

ç) Për transportimin e pakove me material kriptografik, që nuk mbahen me vete, korrierët marrin masa që të shohin ngarkimin dhe shkarkimin e sigurt të tyre, sipas parimit “I fundit në hyrje – i pari në dalje”.

7. Përpara marrjes në dorëzim të pakos, korrieri verifikon rregullsinë e masave të përcaktuara në pikën 6, të këtij neni.

8. Shpërndarja e materialeve kriptografike për mbrojtjen e informacionit të klasifikuar të NATO-s, BE-së apo të shteteve dhe organizatave të tjera ndërkombëtare bëhet në përputhje me marrëveshjet e sigurisë për mbrojtjen e ndërsjellë të informacionit të klasifikuar.

Neni 8

Procedurat për menaxhimin e materialeve kriptografike

1. Menaxhimi i materialeve kriptografike është procesi i trajtimit dhe i dokumentimit të situatave emergjente dhe i incidenteve të sigurisë, që lidhen me komprometimin, humbjen ose përdorimin e paautorizuar të materialeve kriptografike.

2. Në kushtet e situatave emergjente, kur dëmi që shkakton mosdërgimi i informacionit është më i madh se dëmi që shkakton zbulimi i tij, informacioni i klasifikuar “Sekret shtetëror” transmetohet me anë të materialeve kriptografike me nivel më të ulët klasifikimi, me urdhër të titullarit të strukturës ku bën pjesë, në rast se:

a) dërguesi dhe marrësi nuk kanë të njëjtat materiale kriptografike;

b) kur nuk ka në dispozicion mënyra të tjera të sigurta komunikimi.

3. Në rastet e përcaktuara në pikën 2, të këtij neni:

a) përdoruesit i sigurohet minimumi i kushteve të sigurisë, në përputhje me nivelin e klasifikimit të sistemeve kriptografike që përdor;

b) përpilohet një raport, me anë të të cilit vihet në dijeni AKSIK-u dhe Drejtoria e Shifrës.

4. Incident kriptografik konsiderohet:

a) komprometimi, humbja apo kopjimi nga persona të paautorizuar i materialeve kriptografike;

b) përdorimi i materialeve kriptografike të pavlerësuar nga Drejtoria e Shifrës dhe të pamiratuara nga AKSIK-u;

c) përdorimi i sistemeve kriptografike nga persona të paautorizuar;

ç) transmetimi i informacionit të klasifikuar, duke përdorur materiale kriptografike me nivel klasifikimi më të ulët, përjashtuar rastet sipas pikës 2, të këtij neni;

d) transmetimi i informacionit të klasifikuar me materiale kriptografike të dëmtuara;

dh) administrimi, në kundërshtim me rregullat e përcaktuara të materialeve kriptografike;

e) modifikimi i paautorizuar i materialit kriptografik;

ë) konstatimi i parregullsive në paketim dhe/ose shenjëzime.

5. Në rastet kur konstatohen incidente kriptografike, merren masat e mëposhtme:

a) Ndërpritet procesi i kriptim–dekriptimit me materialet kriptografike në përdorim;

b) Ruajtësi krypto merr masa për shmangien ose kufizimin e pasojave negative dhe informon brenda 24 orëve Drejtorinë e Shifrës;

c) Për sqarimin e rrethanave të incidentit ngrihet një komision, në përbërje të të cilit janë specialistë nga Drejtoria e Shifrës, ruajtësi krypto dhe specialistë nga institucioni shtetëror ose nga operatori ekonomik, ku është konstatuar incidenti;

ç) Komisioni i ngritur harton, në dy kopje, raportin për incidentin kriptografik, një për institucionin ose operatorin ekonomik, ku ka ndodhur incidenti, dhe një për Drejtorinë e Shifrës;

d) Drejtoria e Shifrës njofton AKSIK-un për konkluzionet e nxjerra për incidentin kriptografik nga komisioni i ngritur dhe për masat e marra.

6. Raporti i incidentit kriptografik merr klasifikimin e materialit kriptografik të përfshirë në incident.

7. Raporti përmban një përshkrim të qartë të incidentit kriptografik, ku të përfshihen:

a) lloji i materialit kriptografik të përfshirë në incident;

b) sistemet e prekura nga incidenti;

c) struktura ku ka ndodhur incidenti;

ç) përdoruesit e sistemit dhe ruajtësi krypto përkatës.

8. Raporti i incidentit kriptografik përmban një nga deklaratat e mëposhtme:

a) “I komprometuar”: Në rast se materiali kriptografik ka humbur në mënyrë të pakthyeshme ose informacionet tregojnë në mënyrë të qartë që materialet kriptografike janë aksesuar nga një person i paautorizuar;

b) “Nuk përjashtohet komprometimi”: Informacioni në dispozicion tregon që materialet kriptografike janë aksesuar nga persona të paautorizuar, por nuk ka prova të qarta;

c) “Nuk ka komprometim”: Informacioni në dispozicion provon qartësisht që materiali kriptografik nuk është aksesuar nga persona të paautorizuar.

9. Raporti i incidentit kriptografik nënshkruhet nga të gjithë pjesëtarët e komisionit të ngritur sipas shkronjës “c”, të pikës 5, të këtij neni.

Neni 9

Dispozita kalimtare dhe të fundit

1. Vendimi nr. 690, datë 5.10.2011, i Këshillit të Ministrave, “Për miratimin e rregullores ‘Për mbrojtjen kriptografike të informacionit të klasifikuar ‘Sekret shtetëror’””, shfuqizohet, me përjashtim të neneve 6, 9 e 25, të cilat vazhdojnë të mbeten në fuqi deri në daljen e aktit nënligjor për organizimin dhe funksionimin e Drejtorisë së Shifrës, për sa kohë nuk bien ndesh me parashikimet e këtij vendimi.

2. Ngarkohen institucionet shtetërore dhe operatorët ekonomikë për zbatimin e kërkesave të këtij vendimi.

3. Ngarkohen Drejtoria e Shifrës dhe Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar për kontrollin e zbatimit të kërkesave të këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama