

FORMULARI I ANKESËS PRANË AUTORITETIT/ENTIT KONTRAKTOR DHE KOMISIONIT TË PROKURIMIT PUBLIK

Ankesë drejtuar: Autoriteti/Entit Kontraktor dhe Komisionit të Prokurimit Publik ☐

Seksioni I. Identifikimi i ankimuesit

Ankimuesi mund të jetë një ofertues ose ofertues i mundshëm (p.sh. individ, operator ekonomik, shoqatë, bashkim operatorësh ekonomikë) ☐

ABISSNET

Emri i plotë i ankimuesit (ju lutem shtypeni)

K01417001C

NUIS/NIPT

Njesia Bashkiake Nr.5, Rruga Ismail Qemali, Pallati 18, Kati II.

Adresa

Tiranë

Albania

1019

Qyteti

Shteti

Kodi Postar/Posta

0696879191

Numri i telefonit (përfshirë kodin e zonës)

Numri i faksit (përfshirë kodin e zonës)

rudina.cepi@abissnet.al

E-mail

Administrator Koço Kokëdhima

Emri dhe titulli i zyrtarit të autorizuar për lëshimin e ankesës (ju lutemi shkruani)

2025/06/03

Nënshkrimi i zyrtarit të autorizuar

Data (viti/muaji/dita)

+355692073999

Numri i telefonit (përfshirë kodin e zonës)

Numri i faksit (përfshirë kodin e zonës)

Seksioni II: Informacion mbi procedurën

Numri i referencës së procedurës/Lotit

Plotësoni numrin e referencës së kontratës në njoftimin e kontratës ose në dokumentin e tenderit.

REF-49365-05-28-2025

Tipi i procedurës për ankesën

Procedure Prokurimi Publik

Tipi i ankesës

Dokumenta Tenderi

Plotësoni llojin e procedurës së përdorur

Open Simple

Autoriteti/Enti Kontraktor

Emri i autoritetit/entit kontraktor që administrojnë procesin e prokurimit.

ILLYRIAN GUARD SH.A

Vlera e përllogaritur e prokurimit

Vlera e përllogaritur e kontratës/Marrëveshjes Kuadër (shuma në shifra dhe fjalë)

9360000

Objekti i kontratës/Marrëveshjes Kuadër

Përshkrimi i shkurtër i punëve/mallrave/shërbimeve objekt kontrate/marrëveshje kuadër.

“Shërbime Rrjeti data 2025 për nevojat e shoqërisë “Illyrian Guard Sha”.

Afati i fundit për paraqitjen e ofertës

Data (viti/muaji/dita)

2025/06/09

Data e publikimit të Njoftimit të Fituesit

(Data (viti/muaji/dita) nëse është e zbatueshme) ☐

Data e nënshkrimit të kontratës

(Data (viti/muaji/dita) në rastet e kërkesave për pavlefshmërinë e kontratës) ☐

Tipi i kontratës

Shërbime

Data e zhvillimit të procedurës

2025/06/09

Numri i njoftimit

CN/47928/05282025

Kodi CPV

98390000-3

Ankese mbi argument në KPP

Seksioni III: Përshkrimi i ankesës

1. Baza ligjore

(Shkelje/arsyetime ligjore, bazuar në vendime, akte, dokumente, etj.) ☐

1. Baza ligjore (Shkelje ligjore, bazuar në vendime, akte, dokumente, etj.)

? Ligji nr. 162, datë 23.12.2020 “Per prokurimin publik” i perditësuar;

? Ligji 54/2024 “Për komunikimet elektronike”;

? Ligji 25/2024 “Per sigurine kibernetike”;

? VKM nr. 285 datë 19.05.2021 “Për Miratimin e rregullave të Prokurimit Publik”;

? Dokumentet Standarde të Tenderit;

? Ekstrakti i shoqërisë Abissnet sha;

? Mandati i Pageses se tarifës së ankimit;

2. Objekti i ankesës ☐

- Modifikim i dokumentave të tenderit

☒

- Kundërshtim i vendimit të Komisionit të Vlerësimit të Ofertave lidhur me skualifikimin e ofertës tuaj.

☐

(Citoni këtu arsyet e skualifikimit)

- Kundërshtim i vendimit të Komisionit të Vlerësimit të Ofertave lidhur me kualifikimin e ofertës të një/disë operatori/ëve ekonomikë pjesëmarrës në procedurën e prokurimit.

☐

(Citoni operatorin/ët ekonomik për të cilin keni pretendime)

- Pavlefshmëri kontrate ☐

☐

(Citoni kontratën për të cilën kërkon pavallefshmërinë)

- Tjetër ☐

☐

(Citoni këtu objektin e ankesës që nuk përfshihet më sipër)

3. Rrethanat dhe faktet ☐

Përshkruani rrethanat e faktit. ☐

Autoriteti Kontraktor, Zyra e Prokurorit të Përgjithshëm (ne vijim AK), në datën 29.05.2025, në Sistemin e Prokurimeve Publike, administruar nga Agjencia e Prokurimeve Publike ka publikuar Dokumentet Standarde të Tenderit me REF-49365-05-28-2025, në të cilat janë parashikuar në mënyrë të detajuar, kushtet që duhet të plotësohen nga operatorët pjesëmarrës në prokurim. Më konkretisht, kriteri veçantë që kundërshtohet prej Ankuesit është si më poshtë:

? 2.3.6 Operatori Ekonomik duhet të paraqesë një propozim teknik të shoqëruar me skemat e rrjetit të ofertuesit, për zgjidhjen teknike për ofrimin e shërbimit si dhe planin e back-up për ofrimin e shërbimit, duke përfshirë edhe mbrojtjen nga sulmet DDoS. Mbrojtja nga sulmet DDoS do të ofrohet për linjën e internetit në site primar nëpërmjet monitorimit, njoftimit dhe pastrimit automatik të sulmeve DDoS që trafikohen në rrjetin e Institucionit duke ofruar kështu; mbrojtje të serverit, mbrojtje të infrastrukturës BGP (Border Gateway Protocol), mbrojtje në bazë volumetrike, rrugëzim (routing) të trafikut drejt një “Scrubbing Center” qëndërzim pastrimi, i cili duhet të ketë lidhje Intranet Layer 2 nga operatori ekonomik për të rrugëzuar të gjithë trafikun në rast sulmesh. Monitorim 24 orë / 7 ditë dhe suport nga specialistë me eksperiencë në këtë shërbim. Operatori ekonomik duhet të ofrojë mbrojtjen DDoS në disa perimetra sigurie (multi layer DDoS protection në të gjithë perimetrat e sigurisë, lokale, kombëtare dhe ndërkombëtare). Gjithashtu për platformën e përdorur për ofrimin e shërbimit DDoS, operatori ekonomik duhet ta provojë duke paraqitur kontratën e blerjes/suportit të platformës respektive.

Ky kriter plotësohet me dorëzimin e propozimit Teknik dhe kontratës së blerjes/suportit të platformës respektive për mbrojtjen DDoS.

4. Argumentime mbi shkeljet e pretenduara

Përshkruani në mënyrë koncize shkeljet e pretenduara, duke argumentuar qartë dhe saktë se përse pretendoni për paligjshmëri në veprimet e autoritetit/entit kontraktor.

Në pikën 2.3.6 tek “Kriteret e Veçanta të Kualifikimit” parashikohet se:

2.3.6 Operatori Ekonomik duhet të paraqesë një propozim teknik të shoqëruar me skemat e rrjetit të ofertuesit, për zgjidhjen teknike për ofrimin e shërbimit si dhe planin e back-up për ofrimin e shërbimit, duke përfshirë edhe mbrojtjen nga sulmet DDoS. Mbrojtja nga sulmet DDoS do të ofrohet për linjën e internetit në site primar nëpërmjet monitorimit, njoftimit dhe pastrimit automatik të sulmeve DDoS që trafikohen në rrjetin e Institucionit duke ofruar kështu; mbrojtje të serverit, mbrojtje të infrastrukturës BGP (Border Gateway Protocol), mbrojtje në bazë volumetrike, rrugëzim (routing) të trafikut drejt një “Scrubbing Center” qëndërzim pastrimi, i cili duhet të ketë lidhje Intranet Layer 2 nga operatori ekonomik për të rrugëzuar të gjithë trafikun në rast sulmesh. Monitorim 24 orë / 7 ditë dhe suport nga specialistë me eksperiencë në këtë shërbim. Operatori ekonomik duhet të ofrojë mbrojtjen DDoS në disa perimetra sigurie (multi layer DDoS protection

ne te gjithe perimetrat e sigurise, lokale, kombetare dhe nderkombetare). Gjithashtu per platformen e perdorur per ofrimin sherbimit DDoS, operatori ekonomik duhet ta provoje duke paraqitur kontraten e blerjes/suportit te platformes respektive.

Ky kriter plotësohet me dorëzimin e propozimit Teknik dhe kontrates se blerjes/suportit te platformes respektive per mbrojtjen DDoS.

Sulmi DDoS është një sulm në rrjet, synimi i të cilit është që një website ose rrjet të shkëputet për një periudhë kohore, duke e ngarkuar me trafik të tepërt dhe duke e bërë shërbimin e tij të padisponueshëm.

Abissnet sha ka rrjet dhe ofron shërbime të komunikimeve elektronike në Republikën e Shqipërisë nën regjimin e Autorizimit të Përgjithshëm të lëshuar nga AKEP Nr. 2022-AP-1.1 395 / datë 22.11.2022. Abissnet sha e ushtron veprimtarinë e vet mbi një sërë aktesh ligjore dhe nënligjore që përcaktojnë të drejtat, detyrimet dhe mënyrën e shtrimit të aktivitetit, por mbi të gjitha në bazë të ligjit “Për komunikimet elektronike në RSH” dhe ligjit 25/2024 “Për Sigurinë Kibernetike”.

Duke analizuar dispozitat e këtyre ligjeve nuk ekziston asnjë detyrim ligjor për ofruesit e shërbimit të internetit, që zgjidhjet e tyre teknologjike në fushën e sigurisë kibernetike – përfshirë sistemet mbrojtëse ndaj sulmeve DDoS – të jenë të blera nga subjekte të treta, ne baze te kontratave te caktuara. Përkundrazi, legjislacioni u njeh këtyre subjekteve te drejten e neutralitetit teknologjik, në mënyrën se si ato organizojnë dhe garantojnë sigurinë e rrjeteve që operojnë.

Më konkretisht në Ligjin 25/2024 “Për sigurinë kibernetike” ne nenin “Parime të përgjithshme të sigurisë Kibernetike” parashikohet se:

?

2. Në përputhje me përcaktimet e bëra në këtë ligj, zbatohet për aq sa është e mundur parimi i neutralitetit të teknologjisë, sipas të cilit subjektet e këtij ligji janë të lira për të zgjedhur teknologjinë më të përshtatshme për nevojat e tyre duke mos imponuar dhe as diskriminuar ndonjë lloj të veçantë teknologjie, duke inkurajuar përdorimin e standardeve evropiane dhe ndërkombëtare dhe specifikimeve teknike të rëndësishme për sigurinë e rrjetit dhe sistemeve të informacionit.

Pra, ky ligj, që është akti më i rëndësishëm normativ në vend për instalimin e masave nga operatorët, në lidhje me sigurinë kibernetike, i referohet parimit të neutralitetit të teknologjisë, pa i lidhur operatorët me detyrimin e krijimit të marrëdhënieve të zhvillimit të të tilla sistemeve, me skema të caktuara të blera apo të marra nga subjekte të tjerë.

Gjithashtu, në ligjin për “Për komunikimet elektronike në Republikën e Shqipërisë”, në nenin 54/1 parashikohet se:

“Ofruesit e rrjeteve publike të komunikimeve elektronike ose të shërbimeve të komunikimeve elektronike të disponueshme për publikun marrin masat e duhura teknike, organizative dhe proporcionale për të menaxhuar në mënyrë të përshtatshme rreziqet që vijnë për sigurinë e rrjeteve dhe shërbimeve. Duke pasur parasysh gjendjen e teknologjisë, këto masa duhet të sigurojnë një nivel të përshtatshëm sigurie për rrezikun e paraqitur. Në veçanti, masat, duke përfshirë aty ku është e përshtatshme enkriptimin, merren për të parandaluar dhe minimizuar ndikimin e incidenteve të sigurisë te përdoruesit, në rrjetet dhe shërbimet e tjera.

2. Ofruesit e shërbimit të aksesit në internet marrin masa për të siguruar mbrojtjen nga sulmet DDoS për të parandaluar dhe minimizuar ndikimin e incidenteve të sigurisë, që çojnë në mohimin e marrjes së shërbimit te përdoruesit.

Pra, edhe ligji i lartpërmendur vendos detyrimin e operatorëve për marrjen e masave nga sulmet DDoS, por nuk e lidh me sisteme apo mënyra të caktuara të përfitimit të tyre.

Sa më sipër, legjislacioni kërkon që operatorët të realizojnë rezultate konkrete në drejtim të parandalimit të sulmeve DDoS dhe ruajtjes së sigurisë, por nuk imponon asnjë detyrim për mënyrën teknike të realizimit të këtyre masave. Kësisoj, implementimi i një sistemi të zhvilluar nga vetë operatori është plotësisht i lejueshëm, pa e blere, nga subjekte të treta, për aq kohë sa përmbush detyrimet funksionale të parashikuara nga aktet ligjore. Organet rregullatore AKEP dhe AKSK, mbikëqyrin nivelin e efektshmërisë së masave të marra.

Kjo është praktikë e zakonshme edhe në nivel ndërkombëtar, ku shumë operatorë kanë infrastrukura të brendshme kundër DDoS të ndërtuara plotësisht në mënyrë in-house.

Nga ana tjetër, as ENISA, nuk imponon përdorimin ekskluziv të pajisjeve apo platformave të palëve të treta për mbrojtjen nga sulmet DDoS. ENISA është Agjencia e Specializuar e Bashkimit Evropian për Çështjet e Sigurisë Kibernetike. Kjo Agjenci e vendosur në krye të piramidës evropiane për çështjet e sigurisë kibernetike, nuk përcakton as llojin dhe as origjinën e zgjidhjeve teknike që operatorët duhet të përdorin për mbrojtjen nga sulmet kibernetike, duke përkrahur parimin e teknologjitit kibernetik.

Në “Udhëzuesin për Zbutjen e Sulmeve DDoS” (DDoS Mitigation Guidelines), ENISA ka rekomanduar që:

Operatorët duhet të zbatojnë masa teknike dhe organizative të përshtatshme dhe proporcionale për zbutjen e sulmeve DDoS, të bazuara në vlerësimin e rrezikut të rrjeteve dhe shërbimeve të tyre.

Ky udhëzim i ENISA përcakton zbatimin e një qasjeje të bazuar në rrezik (risk-based approach), lirinë e operatorëve për të vendosur masat teknike që ata konsiderojnë të përshtatshme dhe proporcionale dhe mungesën e çdo detyrimi për përdorimin e zgjidhjeve të gatshme nga palë të treta.

Gjithashtu, në ligjin nr. 162/2020 “Për prokurimin publik” i përditësuar në vijim (Ligji 162/2020), parashikohet se:

Neni 2

Qëllimi

Qëllim i këtij ligji është:

- a) të rrisë eficiencën dhe efikasitetin në procedurat e prokurimit publik;
- b) të sigurojë mirëpërdorim të fondeve publike dhe të ulë shpenzimet procedurale;
- c) të nxisë pjesëmarrjen e operatorëve ekonomikë në procedurat e prokurimit publik;
- ç) të nxisë konkurrencën ndërmjet operatorëve ekonomikë
- d) të sigurojë një trajtim të barabartë dhe jodiskriminues për të gjithë operatorët ekonomikë, pjesëmarrës në procedurat e prokurimit publik;
- dh) të sigurojë integritet, besim publik dhe transparencë në procedurat e prokurimit publik.

Neni 3

Parime të përgjithshme

1. Autoritetet dhe entet kontraktore garantojnë trajtim të barabartë dhe jodiskriminues për operatorët ekonomikë, si dhe veprojnë me transparencë e në mënyrë proporcionale.
2. Autoritetet dhe entet kontraktore nuk duhet të shmangin fushën e zbatimit të këtij ligji ose

të ngushtojnë në mënyrë artificiale konkurrencën. Konkurrenca konsiderohet se është ngushtuar artificialisht kur prokurimi përgatitet me qëllimin për të favorizuar ose dëmtuar në mënyrë të padrejtë operatorë ekonomikë të caktuar.

3. Autoritetet dhe entet kontraktore janë të detyruara të zbatojnë detyrimet e përcaktuara në legjislacionin mjedisor, social e të punës dhe në dispozitat e marrëveshjeve dhe konventat ndërkombëtare, të ratifikuara në përputhje me Kushtetutën.

Në nenin 36/2 të ligjit parashikohet se: 2. Specifikimet teknike duhet të mundësojnë trajtim të barabartë për të gjithë kandidatët dhe ofertuesit dhe të mos shërbejnë si pengesa për konkurrencën e hapur në prokurimin publik.

Në nenin 77/1 parashikohet se “Kërkesat kufizohen vetëm në ato që janë të përshtatshme për të garantuar që një kandidat ose ofertues të ketë kapacitetet juridike, financiare dhe aftësitë teknike e profesionale për të zbatuar kontratën që do të jepet. Të gjitha kërkesat duhet të kenë lidhje dhe të jenë proporcionale me objektin e kontratës.”

Kufizimi i vendosur në DST në pikën 2.3.6 për blerjen nga palë të treta të sistemeve anti DDoS, përbën kusht diskriminues, që ngushton në mënyrë artificiale konkurrencën, në kundërshtim me parimet dhe qëllimet e ligjit 162/2020.

Bazuar në sa më sipër, në bazë të parimit të proporcionalitetit dhe trajtimit të barabartë në vlerësimin e kriterëve teknike, kërkojmë që të hiqet nga DST-ja kushti që zgjidhjet mbrojtëse kundër DDoS të blihen/suportohen nga kontraktore, dhe të mos zhvillohen brenda strukturës së operatorit ekonomik.

5. Kërkesë për ekspertizë të posaçme ☐

Po ☐

Jo ☒

(Nëse po, specifikoni llojin e ekspertizës që kërkon)

6. Kërkesë për përjashtim të zyrtarëve që do të merren me shqyrtimin e ankesës:

Jo

7. Lista e informacionit konfidencial: ☐

Jo

Përcaktoni se cili informacion është konfidencial, nëse ka. Shpjegoni pse informacioni është ose një version i dokumenteve përkatëse me heqjen e pjesëve konfidenciale dhe një përmbledhje të përmbajtjes. ☐

Kujdes: Ankimuesi duhet t'i bashkëlidhë ankimit, që do të paraqesë në autoritetin/entin kontraktor dhe Komisionin e Prokurimit Publik, dokumentin bankar që vërteton pagesën e tarifës përkatëse për ankesën pranë Komisionit të Prokurimit Publik

Dërgojeni formularin e plotësuar të ankesës së prokurimit, të gjitha shtojcat e nevojshme dhe kopjet shtesë, pranë **Autoritetit/Enti Kontraktor dhe Komisionit të Prokurimit Publik**.

Shënim: Ankimuesi duhet ta dërgojë njëkohësisht ankesën në autoritetin/entin kontraktor dhe Komisionin e Prokurimit publik

Nr. i faksit:

E-mail:

rudina.cepi@abissnet.al

Nënshkrimi dhe vula e Ankuesit

Administratori/Përfaqësuesi i autorizuar

Koço Kokëdhima