REPUBLIKA E SHQIPËRISË
IDENTITEK SH.A

RELACION
PËR ARGUMENTIMIN E SPECIFIKIMEVE TEKNIKE

LËNDA: Argumentim për specifikimet teknike sipas Urdhrit të Brendshëm Nr.460 Prot., datë 28.08.2025, për procedurën e prokurimit me objekt: "Sistem mbrojtje nga sulmet "DDOS – Distributed Denial of Service "për shërbimet/aplikacionet dhe faqet e ekspozuara në internet (WAF –Web Application Firewall)".

Në zbatim të Urdhrit të Brendshëm nr. 146 Prot., datë 18.03.2026, me shkresën 428 Prot., datë 18.03.2026 "për ngritjen e grupit të punës për rishikimin e specifikimeve teknike/termave te referencës, përllogaritjen dhe argumentimin e fondit limit, për objektet e Sistemeve të Sigurisë së Informacionit"; dhe Urdhrit të Brendshëm nr. 199 Prot., datë 10.04.2026, me shkresën 428/2 Prot., datë 18.03.2026 "Për Shtyrjen e afatit të Përcaktuar me Urdhrin Nr 428…", grupi i punës ka hartuar specifikimet teknike për procedurën me objekt "Sistem mbrojtje nga sulmet "DDOS – Distributed Denial of Service "për shërbimet / aplikacionet dhe faqet e ekspozuara në internet (WAF –Web Application Firewall)", sipas procedurave të prokurimit referuar Ligjit nr. 162, datë 23.12.2020 "Për Prokurimin Publik",
i ndryshuar; VKM-së nr. 285, datë 19.05.2021, "Për Miratimin e Rregullave të Prokurimit Publik", e ndryshuar, dhe akteve të tjera nënligjore në fuqi.

Duke përfshirë një spektër të gjerë aplikimesh në sistemet aktuale, zgjidhje të mundshme që ofrojnë shërbimin e kërkuar për të evidentuar elementët dhe specifikat më aktuale të sistemit të mbrojtjes nga sulmet "DDOS – Distributed Denial of Service " për shërbimet/aplikacionet dhe faqet e ekspozuara në internet (WAF –Web Application Firewall), që i përshtaten dhe nevojave të Shoqërisë IdentiTek sh.a. dhe teknologjive më të fundit në treg, grupi i punës ka argumentuar zgjedhjen e këtyre specifikimeve si më poshtë:

Arsyet teknike që kërkojnë implementimin dhe përdorimin e një zgjidhjeje WAF

- **Mbrojtja ndaj sulmeve të zakonshme në aplikacionet web.** WAF ndihmon në mbrojtjen kundër sulmeve si SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), dhe të tjera që janë të listuara në OWASP Top 10.

- **Filtrimi i trafikut të padëshiruar dhe i keqdashës.** WAF monitoron dhe filtrin trafikun HTTP/HTTPS për të parandaluar qasje të paautorizuar apo trafik nga burime keqdashëse.

- **Mbrojtje për aplikacione të trashëguara (legacy).** Në mungesë të mundësisë për të përditësuar kodin e aplikacionit 'të vjetra' , WAF mund të përdoret si një shtresë mbrojtëse për të adresuar dobësitë.

identiTek
Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

- **Pajtueshmëri me standardet e sigurisë.** WAF kontribuon në përmbushjen e kërkesave të standardeve si ISO 27001 dhe rregulloreve të tjera të sigurisë së informacionit.

- **Monitorimi dhe auditimi i kërkesave web.** WAF ofron logim dhe gjurmim të kërkesave HTTP/HTTPS që ndihmojnë në hetimin e incidenteve dhe analizimin e trafikut në kohë reale.

Për të përmbushur kërkesat teknike të specifikuara për një Web Application Firewall (WAF) që ofrohet si një shërbim "Software as a Service" (SaaS), është e nevojshme të sigurohet një zgjidhje e avancuar e cila garanton mbrojtje të plotë për aplikacionet web nga një gamë e gjerë sulmesh kibernetike. Një zgjidhje e tillë duhet të operojë në modalitetin "Reverse Proxy," duke përdorur një infrastrukturë të mirëmbajtur dhe të menaxhuar nga vetë prodhuesi. Kjo ofron avantazhin e një menaxhimi qendror të sigurisë dhe një kornizë të mbrojtjes që është gjithmonë e përditësuar dhe e përshtatur ndaj kërcënimeve të fundit, duke garantuar që klientët të mbrohen në kohë reale.

Platforma duhet të sigurojë një ndërfaqe intuitive, të disponueshme përmes një GUI dhe API, duke mundësuar menaxhimin dhe konfigurimin e plotë të politikave të sigurisë në mënyrë të barabartë përmes të dyja metodave. Një sistem i tillë duhet të jetë në gjendje të mbrojë aplikacionet web nga një numër sulmesh të njohura, si: Backdoor, Cross Site Scripting (XSS), Illegal Resource Access, Remote File Inclusion (RFI), dhe SQL Injection. Për më tepër, duhet të përfshijë një mekanizëm për parandalimin automatik të sulmeve DDoS, i cili jo vetëm që duhet të zbulojë dhe zbusë sulmet në kohë reale, por gjithashtu duhet të jetë i aftë të dallojë trafikun legjitim nga trafiku i automatizuar ose keqdashës (bots) përmes sfidave si Cookie, JavaScript, dhe CAPTCHA.

Zgjidhja duhet të përputhet me standardet e fundit të sigurisë, si ISO 27001, dhe të jetë në gjendje të integrohet me sisteme të jashtme për menaxhimin e identiteteve për autentifikimin e administratorëve, duke mbështetur protokollet SAML për një menaxhim të sigurt të roleve dhe privilegjeve.

Një komponent tjetër kritik është mbështetja për teknologjitë e fundit të rrjetit, si IPv6 dhe HTTP/2, duke garantuar se komunikimi midis klientëve, infrastrukturës së prodhuesit, dhe serverëve të aplikacioneve është i sigurt dhe i përputhshëm me standardet moderne.

Për sa i përket mbrojtjes së DNS, sistemi duhet të ofrojë një shërbim të fortë për mbrojtjen nga sulmet DDoS, duke përfshirë opsione për proxy DNS dhe mbrojtje përmes zonave të pritjes. Zgjidhja duhet të mbështesë konfigurimin e serverave DNS sekondar dhe transferimin e zonave, duke ofruar një siguri të plotë në gjithë infrastrukturën DNS. Për më tepër, është e rëndësishme që sistemi të ofrojë mbështetje të avancuar për SSL/TLS, përfshirë mbështetjen për SNI, mTLS, dhe TLS Resumption, duke garantuar se të gjitha komunikimet janë të siguruara dhe të certifikuara siç duhet.

Një sistem i tillë duhet të ofrojë një motor fleksibël për krijimin e roleve të bazuara në një sërë

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

kriteresh të avancuara, duke përfshirë geolocation, headers, metoda HTTP, dhe më shumë. Në aspektin e raportimit dhe analizës, sistemi duhet të ofrojë një panel të detajuar dhe vizual për monitorimin e sulmeve dhe ngjarjeve, duke përfshirë sugjerime dinamike për përmirësimin e konfigurimeve të sigurisë. Ky sistem gjithashtu duhet të përfshijë një aplikacion për pajisjet mobile për të ofruar shikueshmëri të plotë dhe njoftime të menjëhershme mbi incidentet dhe ngjarjet kritike.

Në fund, për të përmbushur nevojat e biznesit, sistemi duhet të ofrojë licencim të përshtatshëm që mbulon një vit mbrojtje për trafik deri në 20 Mb bandwidth dhe tre aplikacione web, duke siguruar një mbrojtje të qëndrueshme dhe një performancë të lartë për klientët e tij. Ky kombinim i veçorive dhe kapaciteteve e bën këtë zgjidhje ideale për organizatat që kërkojnë të mbrojnë aplikacionet e tyre web nga kërcënimet më të fundit dhe më të sofistikuara kibernetike.

Specifikimet teknike të hartuara, për këtë objekt prokurimi të sistemit të mbrojtjes nga sulmet "***DDOS*** *– Distributed Denial of Service* " për shërbimet/aplikacionet dhe faqet e ekspozuara në internet (***WAF*** *–Web Application Firewall*), përshkruajnë minimumin ose tërësinë e elementeve më të rëndësishme përbërëse, që garantojnë cilësinë e kërkuar, dhe që i vlerëson mallrat si të pranueshme për funksionet e kërkuara, në përputhje me parashikimet e nenit 4, pika 38/b dhe nenit 36, të LPP, si dhe nenit 40, pika 2, të VKM nr. 285, datë 19.05.2021, "Për miratimin e rregullave të prokurimit publik", duke argumentuar çdo kërkesë funksionale ose performancë, apo/dhe çdo standard të kërkuar, ku çdo referencë duhet të shoqërohet nga fjalët "ose ekuivalenti i tij/saj".

<u>Arsyetim mbi domosdoshmërinë ligjore të Implementimit të projekteve të sigurisë.</u>

Duke qenë se IDENTITEK SHA është klasifikuar nga ana e Autoritetit Kombëtar për Sigurinë Kibernetike AKSK si Organizatë e Infrastrukturës Kritike të Informacionit (OIKI).
(*AKSK Ref. Nr. 2445 Prot. Dt. 26.08.2025/ Identitek Nr. 1343 Prot. Dt. 29.08.2025*),

Realizimi i këtyre projekteve përfaqëson detyrime të qarta ligjore dhe rregullatore, dhe më konkretisht:

1. ***LIGJ Nr. 25/2024 Për Sigurinë Kibernetike,*** Neni 31 - Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit**.**

2. ***VKM Nr. 531, datë 25.09.2025*** përcakton <u>masa të detyrueshme teknike</u> të sigurisë kibernetike për OIKI, duke përfshirë një listë masash te domosdoshme, mosrespektimi i të cilave përbën shkelje të detyrimeve ligjore dhe ekspozon institucionin ndaj sanksioneve administrative.

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

3. ***VKM Nr. 606, datë 23.10.2025,*** "Për Miratimin e Strategjisë Kombëtare Për Sigurinë Kibernetike 2025–2030 dhe të Planit të Veprimit 2025-2027".

   Përputhshmëria me të cilin ka këto qëllime kryesore:
   - Mbrojtja e infrastrukturës digjitale
   - Mbrojtja online e qytetarëve dhe nxitja e kulturës kibernetike
   - Forcimi i bashkëpunimit ndërkombëtar:
   - Mbrojtja ndaj kërcënimeve hibride

4. ***Certifikimi ISO/IEC 27001:2022*****.**
   IDENTITEK SHA mban certifikimin ISO/IEC 27001:2022 për Sistemin e Menaxhimit të Sigurisë së Informacionit (ISMS);

   Në përputhje me Kërkesat e ligjit 25/2024, për Sigurinë Kibernetike, ky certifikim, është i detyrueshëm për *Organizatat e Infrastrukturave Kritike të Informacionit OIKI***.**

   Ky standard i sigurisë së informacionit kërkon Specifikisht zbatimin e masave, (kontrolleve të Annex A), përfshirë:
   - A.5.37 - Menaxhimi i vulnerabiliteteve (Zgjidhja Vulnerability Scanner);
   - A.5.19 / A.5.29 - Siguria e rrjeteve (Zgjidhja WAF/DDoS);
   - A.5.15 - Menaxhimi i aksesit të privilegjuar (Zgjidhja PAM);
   - A.8.16 / A.5.30 - Monitorimi dhe parandalimi i rrjedhjeve (Zgjidhja EDR/DLP).

   Moszbatimi i këtyre masave brenda afateve të përcaktuara rrezikon certifikimin ISO/IEC 27001:2022, me impakt të drejtpërdrejtë në funksionimin ligjor të IDENTITEK si operator i infrastrukturës kritike kombëtare, pasi mungesa apo vonesa e implementimit të këtyre projekteve krijon ekspozim të drejtpërdrejtë ndaj:

   - Sulmeve kibernetike (DDoS, Web Application Attacks, Ransomware);
   - Rrjedhjeve të të dhënave personale (biometrike, te dhëna sensitive);
   - Kompromet imit të sistemeve nga vulnerabilitete të paidentifikuara;
   - Akseseve jo të autorizuara nga përdorues të brendshëm (insider threats).

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

DETAJET E KONTRATËS:

Sipas specifikimeve bashkëngjitur të hartuara, vendosur dhe përllogaritur nga struktura të posacme të specializuara, e konkretisht nga: "Grupi i punës për hartimin e specifikimeve teknike dhe përllogaritjen e fondit limit", mbështetur në Vendimit të Këshillit të Ministrave Nr.285, datë 19.05.2021 "Për miratimin e Rregullave të Prokurimit Publik":

Kohëzgjatja e kontratës: 5 muaj nga nënshkrimi i saj

Licensa aktive: 12 Muaj

Plani i implementimit

Ofertuesi duhet të instalojë zgjidhjen në ambientet e IdentiTek sipas kalendarit të mëposhtëm të dakordësuar në bashkëpunim me ekipin e IT. Shërbimi do të ndahet në faza dhe afati për secilën fazë është si në tabelën më poshtë:

Nr	Faza	Muaj 1	Muaj 2	Muaj 3	Muaj 4	Muaj 5
1	Marrja e të dhënave paraprake					
2	Implementimi					
3	Testimi i shërbimit					
4	UAC (User Acceptance)					
5	Dorëzimi i shërbimit					
6	Trajnimi për stafin					

GRUPI I PUNËS:

Z. Sadiol Ruka **Z. Gjergj Floqi** **Z. Xhulio Kurteshi**

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al