

ANUNȚ DE PARTICIPARE

privind Achiziționarea Session Border Controler (SBC)
prin procedura de achiziție Licităția deschisă

1. Denumirea autorității contractante: I.P. „Serviciul național unic pentru apelurile de urgență 112”, în continuare – Serviciul 112
2. IDNO: 1016600011534
3. Adresa: mun. Chișinău, bd. Dacia 58/C, com. Băcioi
4. Numărul de telefon: (022) 294 -813
5. Adresa de e-mail și de internet a autorității contractante: office@112.md
6. Adresa de e-mail sau de internet de la care se va putea obține accesul la documentația de atribuire, ion.lisnic@112.md
7. Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună): Serviciul 112 este structură organizațională și tehnologică care asigură preluarea, înregistrarea, prelucrarea apelurilor de urgență și transmiterea solicitărilor de intervenție procesate către serviciile specializate de urgență, precum și interacțiunea cu furnizorii de comunicații electronic.
8. Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea/prestarea/executarea următoarelor bunuri /servicii/lucrări:

Nr. d/o	Cod CPV	Denumirea bunurilor, serviciilor sau lucrărilor	Cantitate / Unitate de măsură	Descrierea achiziției	Valoarea estimată lei, (scutită de TVA) (pentru fiecare lot în parte)
1.	32420000-3	Achiziționare a Session Border Controler (SBC)	Buc.	• O instanță SBC pentru fiecare locație a sistemului. SBC trebuie să aibă o configurație de redundanță geografică cu standby la cald. • SBC va furniza următoarele funcții: • Criptarea comunicațiilor (TLS și IPsec) • SIP NAT • Interconectarea rețelelor SIP și SIP-I. • Transcodificare între trunchiuri SIP. • Funcții de rutare SIP bazate pe identitățile apelantului și ale apelatului. • Balansarea încărcării către serverele SIP țintă. • Menținerea conexiunilor SIP active (SIP OPTIONS) • Înregistrarea apelurilor și a calității apelurilor. • SBC va asigura o capacitate suficientă (cel puțin 240 de apeluri SIP simultane) în funcție de operațiunile sistemului, bazată pe statisticile apelurilor active și ale apelurilor în coadă în situații de vârf.	2,250,000.00

9. În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):
- 1) Pentru un singur lot
 - 2) Pentru mai multe loturi
10. Admiterea sau interzicerea ofertelor alternative: nu se admite.
11. Termenul pentru înaintarea clarificărilor conform SIA RSAP.
12. Termenul pentru depunere a ofertelor conform SIA RSAP.
13. Termenii și condițiile de livrare/prestare/executare solicități: Conform SIA RSAP.
14. Termenul de valabilitate a contractului: 12 de luni.
15. Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz): nu.
16. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina.
17. Eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAЕ, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/Obligativitatea
1.	DUAЕ	Semnat electronic	obligatoriu
2.	Scrisoare de garanție bancară de 1% sau virată în cont (Garanția pentru ofertă se va prezenta la depunerea ofertei)	Model (Anexa nr. 9) din documentația standard, aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021 al Republicii Moldova, semnat electronic	obligatoriu
3.	Specificația tehnică	Model (Anexa nr. 22), din documentația standard, aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021 al Republicii Moldova, semnat electronic	obligatoriu
4.	Specificația de preț	Model (Anexa nr. 23), din documentația standard, aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021 al Republicii Moldova, semnat electronic	obligatoriu
5.	Certificat de atribuire a contului bancar	copie - eliberat de banca detinatoare de cont, confirmata prin aplicarea semnăturii electronice	obligatoriu
6.	Garanția de bună execuție de 5% se va prezenta la momentul încheierii contractului	Model (Anexa nr. 10) din documentația standard aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021) al Republicii Moldova, semnat electronic	obligatoriu
7.	Dovada înregistrării persoanei juridice	Documente edificatoare cum ar fi certificate constatatoare eliberate de autoritatea competenta, în original sau copie legalizata din care sa rezulte adresa actuala și obiectul de activitate al societatii. • Certificat/decizie de înregistrare a întreprinderii sau extras. In cazul unei persoane juridice non-profit, se vor depune documente care sa ateste ca persoana semnatară este autorizată sa desfășoare activitățile ce fac	obligatoriu

		obiectul contractului, cum ar fi: • statutul cu modificările la zi. • procese verbale relevante, etc. Pentru a-i demonstra capacitatea de exercitare a activității profesionale, operatorul economic străin va prezenta documente din țara de origine care dovedesc forma de înregistrare/ atestare ori aparentă din punct de vedere profesional. • Extras din Registrul de Stat – semnat electronic	
8.	Dovada îndeplinirii obligațiilor de plată a impozitelor, taxelor și contribuțiilor de asigurări sociale în conformitate cu prevederile legale în vigoare în Republica Moldova sau în țara în care este stabilit operatorul economic	Original sau copie - eliberat de Inspectoratul Fiscal sau de organul competent în țara de reședință a operatorului economic (valabilitatea certificatului - conform cerințelor Inspectoratului Fiscal al Republicii Moldova sau al organului competent în țara de reședință a operatorului economic străin). Care confirmă lipsa restanțelor la buget, semnat electronic	obligatoriu
9.	Prezentarea actelor ce atestă dreptul de livrare a produsului/serviciului	Ofertantul trebuie să prezinte documente ce atestă relația participantului cu producătorul/dezvoltatorul (certificat de partener autorizat pentru livrarea soluției/ mentenanței aferente, solicitate al producătorului/dezvoltatorului sau contract de relație cu producătorul/dezvoltatorul, sau autorizație de livrare, în cazul în care ofertantul nu folosește soluția proprie, semnat electronic	obligatoriu
10.	Împuternicirile de a încheia contract de achiziții publice	În cazul în care se delegă împuterniciri de către director, administrator unei alte persoane, semnat electronic	obligatoriu
11.	Declarație privind valabilitatea ofertei	Model (Anexa nr. 8) din documentația standard, aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021 al Republicii Moldova, semnat electronic	obligatoriu
12.	Cerere de participare	Model (Anexa nr. 7), conform formularului din documentația standard aprobată prin Ordinul Ministerului Finanțelor nr. 115 din 15.09.2021, semnat electronic	obligatoriu
13.	Declarație privind conformarea identității beneficiarilor efectivi	În conformitate cu Ordinul Ministerului Finanțelor al Republicii Moldova Nr. 145 din 24-11-2020, semnat electronic	obligatoriu

Mențiune. În cazul apariției unor împrejurări, independente de voința părților, care vor determina necesitatea modificării termenelor de livrare/prestare a Bunurilor și/sau Serviciilor, acestea vor putea fi modificate prin încheierea unui acord adițional la prezentul Contract. În scop de clarificare, lipsa alocărilor bugetare sau insuficiența acestora care ar face imposibilă plata de către Cumpărător/Beneficiar a Bunurilor și/sau Serviciilor care urmează a fi livrate / prestate conform planului de facturare, în condițiile prezentului Contract, constituie împrejurări care pot determina modificarea termenelor de achitare a Serviciilor de către Beneficiar. Cumpărătorul/Beneficiar are obligația de a informa în scris pe Prestatorul despre insuficiența /lipsa alocărilor bugetare, în termen de 14 zile lucrătoare.

18. Evaluarea ofertelor

Raportul cel mai bun cost/beneficiu va fi luat în considerare. Produsul propus va fi, de asemenea, testat pentru a se asigura că îndeplinește cerințele solicitate. Toți licitatorii vor fi solicitați să pună soluția propusă la dispoziție pentru testare și să ofere suport complet pentru integrare și personalizare.

Propunerea va fi evaluată pe baza următoarelor criterii:

(O) Propunerea de preț - maximum 40 p. (puncte)

(Ex) Experiență anterioară în implementarea soluțiilor propuse pe rețelele unor operatori majori de telecomunicații sau servicii de intervenție de urgență - 10 p. (puncte). Feedback pozitiv din partea beneficiarului este binevenit.

(Ext) Conformitatea cu specificațiile tehnice conform tabelului de conformitate - maximum 20 p. (puncte). Nu îndeplinește 1-3 cerințe - 10 p. (puncte), până la 5 cerințe - 0 p. (puncte).

(P) Evaluare bazată pe rezultatele testelor pentru conformitatea cu funcționalitatea enunțată - maximum 20 p. (puncte).

(S) Conformitatea cu toate cerințele pentru ofertant conform punctului 2. Toate cerințele îndeplinite - 10 p. (puncte). Cel puțin o cerință nu este îndeplinită - 0 p. (puncte).

Formula de calcul: $N = O/Ob*40 + Ex + Ext + P + S$

Unde:

N - scorul cumulativ

O - oferta evaluată

Ob - cea mai bună ofertă

Ex - scorul cumulativ la evaluarea experienței anterioare de implementare a soluțiilor propuse

Ext - scorul obținut la evaluarea conformității cu specificațiile tehnice

P - scorul obținut pe baza rezultatelor testelor

S - scorul obținut la evaluarea conformității cu cerințele participantului.

19. Criteriul de evaluare aplicat pentru adjudecarea contractului: Cel mai bun raport calitate-cost

20. Termenul limită de depunere/deschidere a ofertelor – conform SIA RSAP

- e-mail: office@112.md
- tel.: 022-294-813.

21. Adresa la care trebuie transmise ofertele sau cererile de participare:

Ofertele sau cererile de participare vor fi depuse electronic – pe platforma SIA RSAP

22. Termenul de valabilitate a ofertelor: 60 de zile

23. Locul deschiderii ofertelor: mun. Chișinău, bd. Dacia 58/C, com. Băcioi

Ofertele întârziate vor fi respinse.

24. Persoanele autorizate să asiste la deschiderea ofertelor:

Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului când ofertele au fost depuse prin SIA "RSAP".

25. Termenul pentru încheierea contractului constituie 6 zile lucrătoare de la data desemnării a câștigătorului procedurii (Licitatie deschisă) cu respectarea, după caz a termenelor de așteptare în sensul prevederilor art. 32 alin. (1), lit. a) a Legii achizițiilor publice al Republicii Moldova.

26. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare: de stat a Republicii Moldova

27. Denumirea și adresa organismului competent de soluționare a contestațiilor:

Agenția Națională pentru Soluționarea Contestațiilor;
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/email: 022-820 652, 022 820-651, contestatii@ansc.md

28. Data publicării conform SIA RSAP

29. Data transmiterii spre publicare conform SIA RSAP

30. În cadrul procedurii de achiziție publică se va utiliza/accepta:

Denumirea instrumentului electronic	Se va utiliza/accepta sau nu
depunerea electronică a ofertelor sau a cererilor de participare	Se va utiliza
sistemul de comenzi electronice	Se va utiliza
facturarea electronică	Se va utiliza
plățile electronice	Se va utiliza

Conducătorul Grupului de lucru:

Constantin GORINCIOI

(Semnătura)

CAIET DE SARCINI **Bunuri/Servicii**

Obiectul: Achiziționarea Session Border Controler (SBC)

Autoritatea contractantă I.P. „Serviciul național unic pentru apelurile de urgență 112”, Adresa: mun. Chișinău, bd. Dacia 58/C, com. Băcioi

I. Cadrul Legal: Acte normative.

Sistemul Informațional Automatizat 112 (SIA112) este un sistem informatic destinat primirii, procesării și transmiterii apelurilor de urgență către serviciile specializate de urgență (SSU). SIA112 formează registrul de stat RS112 și păstrează înregistrările vocale a apelurilor și datele aferente cazurilor de urgență.

Baza juridico-normativă include legislația națională în vigoare, convențiile și tratatele internaționale, la care R. Moldova este parte și constă din:

- ✓ Constituție Republicii Moldova;
- ✓ Legea nr.174 din 25 iulie 2014 cu privire la organizarea și funcționarea Serviciului național unic pentru apelurile de urgență 112;
- ✓ Legea nr.241-XVI din 15 noiembrie 2007 cu privire la comunicațiile electronice;
- ✓ H.G. nr.241 din 3 martie 2016, cu privire la aprobarea Programului național privind implementarea Serviciului național unic pentru apelurile de urgență 112;
- ✓ H.G. nr.242 din 3 martie 2016 cu privire la aprobarea Regulamentului privind organizarea și funcționarea Comitetului coordonator interdepartamental pentru asigurarea interacțiunii dintre Serviciul național unic pentru apelurile de urgență 112 și serviciile specializate de urgență;
- ✓ H.G. nr.243 din 3 martie 2016 cu privire la crearea Serviciului național unic pentru apelurile de urgență 112;
- ✓ H.G. nr.244 din 3 martie 2016 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat al Serviciului național unic pentru apelurile de urgență 112;
- ✓ H.G. nr.1207 din 05.12.2018 pentru aprobarea Regulamentului privind modul de ținere a Registrului de stat format de Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112;
- ✓ Hotărâre nr.30 din 22.12.2016 privind aprobarea Condițiilor tehnice, juridice și organizatorico-economice referitoare la realizarea comunicațiilor electronice către/de la Serviciul 112;
- ✓ Hotărâre nr.31 din 22.12.2016 cu privire la aprobarea Condițiilor tehnice de transmitere a informației de localizare primară în cazul apelurilor la numărul unic de urgență 112;
- ✓ Hotărâre nr.32 din 22.12.2016 cu privire la aprobarea Procedurilor și limitelor tehnice pentru reducerea apelării abuzive, a alertării false și a apelurilor involuntare către Serviciul 112;
- ✓ Directiva 98/10/EC, care stipulează garantarea apelării gratuite a serviciilor de urgență prin intermediul numărului 112;
- ✓ Directiva 2002/22/EC (cunoscută ca Directiva Serviciului Universal), care oferă drepturi legate de utilizarea serviciului universal în rețelele de comunicații electronice și stipulează obligația statelor membre ale UE de a asigura localizarea apelurilor de urgență, pentru a permite găsirea în timp util a victimelor.

SBC Specificații tehnice

1. Configurație minimă de bază:

- O instanță SBC pentru fiecare locație a sistemului. SBC trebuie să aibă o configurație de redundanță geografică cu standby la cald.
- SBC va furniza următoarele funcții: • Criptarea comunicațiilor (TLS și IPsec) • SIP NAT • Interconectarea rețelelor SIP și SIP-I. • Transcodificare între trunchiuri SIP. • Funcții de rutare SIP bazate pe identitățile apelantului și ale apelatului. • Balansarea încărcării către serverele SIP țintă. • Menținerea conexiunilor SIP active (SIP OPTIONS) • Înregistrarea apelurilor și a calității apelurilor.
- SBC va asigura o capacitate suficientă (cel puțin 240 de apeluri SIP simultane) în funcție de operațiunile sistemului, bazată pe statisticile apelurilor active și ale apelurilor în coadă în situații de vârf.

2. Cerințe pentru furnizor:

2.1 Participantul trebuie să aibă statutul de Distribuitor sau Partener al Producătorului (în cazul în care Participantul și Producătorul sunt entități legale diferite). Acest statut trebuie confirmat printr-o scrisoare semnată de un reprezentant autorizat al Producătorului, care confirmă calificarea, sau alt document care atestă statutul de distribuitor sau partener al Producătorului respectiv. Dacă Participantul participă la selecția de calificare a Producătorului în mod independent, scrisoarea nu este necesară.

2.2 Participantul trebuie să aibă un istoric demonstrat de implementare a soluției propuse în condiții similare, cu o capacitate de cel puțin 10 mii de sesiuni în EMEA, conform unei scrisori din partea producătorului.

2.3 Participantul trebuie să aibă un specialist instruit și certificat de către producător pentru a întreține produsul software furnizat. Calificarea va fi confirmată printr-un certificat relevant sau de către producător (cu excepția cazurilor în care lucrările la proiect sunt realizate direct de către producător).

2.4 Participantul va confirma disponibilitatea unui serviciu de partener sau furnizor pe teritoriul Republicii Moldova, sau disponibilitatea de a organiza un astfel de serviciu (confirmat printr-o scrisoare din partea Participantului).

2.5 Participantul trebuie să organizeze formare pentru cel puțin doi specialiști ai clientului la propriul centru de formare sau la un centru de formare partener. Nivelul de formare - Avansat. Costul formării este inclus în costul pachetului de software livrat.

2.6 Complexul de controlere de frontieră pentru sesiunea propusă de Participant și sistemul său de control și monitorizare trebuie să îndeplinească pe deplin următoarele cerințe tehnice, pregătite având în vedere dezvoltarea viitoare a proiectului Clientului, precum și posibilitățile tehnologiilor și tendințelor moderne.

3. Cerințe arhitecturale pentru controlerul de frontieră pentru sesiuni.

No.	Name of evaluation criterion
3.1	SBC must be software-based and installed on a virtual machine
3.2	The SBC must be delivered as a ready-to-use image for a specific virtualization environment.
3.3	SBC must support the following virtualization environments: VMWare, Hyper-V, KVM, OpenStack.
3.4	SBC shall support SR-IOV technology on the virtualization environment
3.5	The SBC must be able to implement both geographic redundancy and 1+1 redundancy in a cluster with one passive and one redundant component. And this functionality should be provided by its own tools, not virtualization tools.
3.6	Switching time between active and standby SBC modules shall be no more than 50ms
3.7	SBC should be able to synchronize information about the state of established SIP sessions between nodes in the cluster (signaling, media traffic) when operating in fault-tolerant mode.
3.8	Minimum system requirements for the SBC Shall be no more than: 1 vCPU/2GB RAM/20 GB HDD
3.9	One SBC virtual machine shall support up to 24,000 concurrent sessions, together with RTP proxying on a single server.
3.10	The SBC shall support a distributed architecture in which all signaling traffic is handled on separate servers and voice traffic is handled on media servers. With this architecture, the virtual SBC shall support up to 48,000 simultaneous connections.
3.11	SBC in distributed architecture mode shall support dynamic switching on and off of media servers depending on the load on the media servers.
3.12	In case of failure of one of the media servers in distributed architecture mode, the SBC shall redistribute active calls to the remaining active media servers
3.13	SBC in distributed architecture mode shall be able to synchronize information about the status of established SIP sessions between nodes in a cluster of signaling components.
3.14	SBC shall have the ability to switch over to the backup node automatically or manually without disrupting established connections.
3.15	SBC must be able to synchronize information about registered subscribers between nodes in the cluster when operating in access mode (A-SBC)

3.16	SBC must be able to, when operating in failover mode, save all information about calls made (CDR or SDR) in case of emergency switching between cluster elements.
3.17	SBC must be able to virtualize DSP processors on a virtual machine and be able to allocate these resources for transcoding. The allocated DSP resources must be statically allocated and committed when the SBC boots and must not affect the performance of signaling messages and RTP proxying.
3.18	SBC in distributed architecture mode shall support at least up to 20 media nodes for transcoding and RTP proxying.
3.19	SBC shall support the following codecs for transcoding: Opus Wideband, Opus Narrowband, SILK Wideband, SILK Narrowband, G.722.2, G.722, G.729, G.711, AMR Wideband, AMR Narrowband, G.723.1, G.726.
3.20	SBC in distributed architecture mode shall support at least 600 simultaneous transcoding sessions from G.711 codec to Opus codec and vice versa on a single media node.
3.21	SBC shall support Interworking-SBC (I-SBC) and Access-SBC (A-SBC) functionality simultaneously on one hardware node, as well as be able to organize such functionality on one IP address, including on one port.
3.22	SBC must have a service availability of at least 99.999% for a standard configuration of a single hardware node
3.23	SBC shall have the ability to register at least 75,000 subscribers per device.
3.24	SBC must be able to handle at least 600 concurrent connection attempts (CAPS) per device (cluster)
3.25	SBC should be able to install software complex in geographically dispersed locations to provide fault tolerance (geo-distribution of the HA pair). With geographically dispersed pairs of SBCs, the solution should be managed as if it were a single device - without the need to configure each set separately.
3.26	SBC must ensure synchronization of geographically separated pairs of equipment with signal propagation delays of up to 15 ms (RTT).
3.27	SBC, when operating in geo-redundant pair mode, must support providing the same IP address to the network core and access equipment.
3.28	When operating in HA pair geo-redundant mode, the use of the SBC should not impose additional requirements on existing equipment in terms of setting up additional SBC IP addresses. Existing equipment should always communicate with the SBC over a single IP address without setting up a Layer 2 channel between the distributed equipment.
3.29	When operating in geo-redundancy mode with two different SBCs, each SBC must handle 50% of the network traffic, and in an emergency, each SBC must handle 100% of the traffic. In this case, the licenses from the emergency SBC

	node must be automatically transferred to the working SBC node (without any personnel administration or other action).
3.30	When two different SBCs are operating in georedundant mode, the allocation of the number of licenses to each individual SBC in a geo-distributed scheme is done dynamically depending on the load.
3.31	Operational changes to the SBC configuration must not be accompanied by SBC rebooting.

4. Cerințe funcționale pentru controlerul de frontieră pentru sesiuni

Toate cerințele listate în secțiunea 4 trebuie să fie îndeplinite într-un mod de cluster SBC rezervat geografic (membrii clusterului instalați în centre de date diferite).

No.	Name of evaluation criterion
4.1	SBC must support the SSH/HTTPS protocol for secure remote management of the SBC.
4.2	SBC shall support DSCP marking of the IP header field for SIP and RTP protocols in order to provide QoS on IP network equipment. (For example, marking application, audio, image, message, text, video traffic). It is possible to configure different DSCP values separately for signaling, media and control traffic.
4.3	SBC shall fully support the SIP signaling layer protocol in accordance with RFC3261.
4.4	SBC must support the SIP-I signaling layer protocol. The ability to analyze and modify message content.
4.5	SBC should provide interaction between PRACK and non-PRACK scenarios.
4.6	SBC must support the UDP transport layer protocol.
4.7	SBC must support the TCP transport layer protocol. (Support for SIP over TCP).
4.8	SBC must support the SCTP transport layer protocol, including SCTP multi-homing. (Support for SIP over SCTP).
4.9	SBC must support the TLS transport layer protocol.
4.10	SBC must support transport layer protocol conversion (i.e., the SBC input call uses TCP protocol and the output call uses UDP or SCTP or TLS).
4.11	SBC shall support dynamic transport layer protocol changes from the endpoint to the SBC and vice versa. For example, SIP user registration is done using UDP, but attempting to establish a session with TCP.
4.12	SBC shall have support for the IEEE 802.1Q specification, on all interfaces

4.13	SBC must have support for ACLs (Access Lists) on the SBC. Ability to create access lists based on various criteria, including dynamic ones.
4.14	SBC must have support for terminating signaling and RTP traffic to one IP address/to different IP addresses.
4.15	SBC must have support for mechanisms of SBC resistance to DOS, DDOS attacks, including from different IP addresses (correct processing of distorted signaling messages). DoS and overload attack filtering, etc., confirmed by tests. Attack detection, blacklisting of the attacker with the possibility of specifying the time of blacklisting, separate queues of parasitic traffic processing, etc.
4.16	SBC must have an architecture that ensures stable operation of the CPU in DoS and DDoS attack modes.
4.17	SBC must have support for SNMP v2C and SNMP v3 (SNMP encryption support).
4.18	SBC must be able to send events from the device as SNMP trap.
4.19	SBC should be able to log all commands entered by users, specify username who made an action.
4.20	SBC must be able to use syslog.
4.21	SBC must support NTP (Network Time Protocol) time synchronization.
4.22	SBC must be able to use RADIUS for online billing.
4.23	SBC must be able to set conditions for CDR and SDR generation on local data storage with subsequent unloading
4.24	SBC must be able to automatically transmit CDRs and SDRs via RADIUS/Syslog/HTTP protocols.
4.25	SBC must be able to customize CDR fields.
4.26	SBC must be able to collect statistics on the quality of voice connections and calculate R-Factor and MOS values (based on such parameters as Packet Loss, Jitter, Delay). Possibility of dynamic routing in real time based on these statistics. Sending statistical data to an external server for further analysis (via CDR).
4.27	SBC must be able to completely hide (spoof) user information such as IP addresses of communicating termination points, interfaces, etc. in all (any) SIP headers, thereby realizing complete concealment of the network topology. Network topology hiding should be provided for both signaling and media traffic.
4.28	SBC must be able to manipulate any SIP headers in the received SIP message. Moving values from one header to another (store and paste). Manipulation means: deleting a certain header, adding a new header, changing the content of the header in any part of it.
4.29	SBC must be able to manipulate any SIP headers in the received SIP message using regular expressions. Manipulation means: deleting a certain header, adding a new header, changing the content of the header in any part of it.

4.30	SBC must be able to manipulate ISUP headers in the received SIP message. Moving values from one header to another (store and paste). Manipulation means: deleting a certain header, adding a new header, changing the content of the header in any part of it.
4.31	SBC must be able to manipulate ISUP headers in a received SIP message using regular expressions. Manipulation means: deleting a certain header, adding a new header, changing the content of the header in any part of it.
4.32	SBC shall have the ability to manipulate SIP headers in a received SIP message on both the incoming and outgoing interfaces.
4.33	SBC shall have the ability to manipulate SIP headers in a received SIP message as text, prior to parsing the message to the SBC, to allow normalization of SIP messages that do not conform to RFC standards.
4.34	SBC must be able to manipulate ISUP headers in a received SIP message on both the incoming and outgoing interfaces.
4.35	SBC shall have support for different DTMF translation/transcoding methods from one to another: • SIP INFO • RFC 2833 • In-band (G711)
4.36	SBC must have support for voice transcoding features - provide a list of codecs available for transcoding. Minimum required set of codecs with transcoding support: G711(PCMA/PCMU), G729, OPUS, SILK, G.722, AMR, AMR-WB
4.37	SBC must have support for voice trans-rating features (changing the packetization time of media traffic) - provide a list of codecs available for trans-rating. Minimum required set of codecs with support for transrating in the range up to 100 msec: G711(PCMA/PCMU), G729, OPUS, SILK, G.722, AMR
4.38	SBC must be able to selectively enable (disable) RTP proxying for an individual direction.
4.39	SBC must be able to manipulate SDP headers. Manipulation means adding, deleting, manipulating any value of any SDP protocol field. Changing codecs priority.
4.40	SBC must be able to route based on trunk group information.
4.41	SBC must be able to route based on information about the codec being used.
4.42	SBC must be able to route based on priority. (Based on the posted destination cost or weight parameter).
4.43	SBC shall have the ability to route outgoing calls based on call establishment time. (Based on time of day and/or days of the week).
4.44	SBC must have policy-based routing capability. Policies refer to the ability to flexibly analyze several parameters simultaneously.

4.45	SBC Must have routing capability with the ability to use multiple policies to handle a single call.
4.46	SBC must be able to route a call based on any header (part of a header) in a SIP message.
4.47	SBC must be able to add up to 100 thousand unique routes (numbers or prefixes), without using third-party voice call routing systems.
4.48	SBC must be able to use LDAP/LDAPS protocols for call routing.
4.49	SBC must be able to combine the created SIP destination addresses into a group, and route calls towards this group.
4.50	SBC shall support re-routing based on unsuccessful response code (4xx, 5xx), using recursion. Recursion refers to rerouting to the next available destination address in the same group selected as a result of the initial routing rule analysis.
4.51	SBC shall support re-routing based on unsuccessful response code (4xx, 5xx), without using recursion. I.e. rerouting does not take place in the same address group, but on the basis of the next routing rule, e.g. in the direction of an alternative address group.
4.52	SBC Should support different call balancing strategies. For example, Hunt, Round robin, Proportional distribution.
4.53	SBC must be able to track the availability of the destination address and set the corresponding destination to the "not in use" status in the following cases (keep-alive): - in case of non-receipt of a response to SIP OPTIONS within a given time interval - receipt of a response code characterizing it as unavailable with the possibility of specifying these codes - in case the destination address is FQDN and is translated to several IP-addresses, availability check for all addresses from the list.
4.54	SBC must be able to route calls based on the availability of the destination address.
4.55	SBC must be able to set limits on the number of simultaneous incoming or outgoing sessions for a single destination, for a single registered user.
4.56	SBC must be able to re-route calls to an alternative direction when the thresholds for the number of simultaneous calls in a given direction are reached.
4.57	SBC must be able to set limits on the speed (number of calls per second) of incoming or outgoing sessions for an individual direction.
4.58	SBC must be able to control the bandwidth used for a particular direction.
4.59	SBC shall be able to control the absence of RTP packets separately for both directions of RTP transmission during a separate call. In case of absence of RTP activity in one of the directions, the ability to form a BYE with encapsulated ISUP part, with appropriate release.

4.60	SBC must be able to work only with destination addresses known to the SBC (SIP-trunks).
4.61	SBC must support the ability to replicate the conversation to the call recording system (SRS) using the SIPREC protocol (RFC 6341).
4.62	When working with Session Recording Server (SRS), the SBC must be able to replicate a SIPREC session simultaneously towards 3 SRSs with traffic balancing between them (Round Robin, Hunt).
4.63	SBC shall support the transfer of call metadata to the SRS in XML format, per RFC 7865 protocol
4.64	SBC must be able to work with SIP endpoints behind NAT.
4.65	SBC shall support dynamic detection of remote NAT port closure times, to optimize re-registration methods in the case of Hosted NAT traversal.
4.66	SBC must support working with SIP URIs and Tel URIs.
4.67	SBC must support generation of RTCP/RTCP-XR reports for calls that have RTP proxied through the SBC.
4.68	SBC Must support simultaneous encryption of media traffic (SRTP) and transcoding within a single call.
4.69	SBC must be able to locally terminate REFER (call forwarding) messages with the ability to route this call through the local routing table.
4.70	SBC should be able to decide on the method of processing the REFER message based on the values of the REFER message header (in accordance with RFC 3515). For example, for certain REFER messages, process locally, and for others skip transparently, for the same direction.
4.71	In the case of local REFER processing, the SBC shall be able to automatically transfer the User-To-User parameter/header from REFER to INVITE.
4.72	SBC must support T.38<-> G.711Passthrough <-> G.711 fax broadcasts (without VBD mode).
4.73	SBC must support the ability to register on a third-party SIP server on behalf of the IP PBX (surrogate registration)
4.74	SBC must be able to generate the dial tone independently.
4.75	SBC must be able to convert IPv4 protocols to IPv6 and vice versa for SIP calls.
4.76	SBC must be able to assign IPv4 and IPv6 addresses simultaneously on the same interface.
4.77	SBC must be able to authorize users through external systems using RADIUS protocols.
4.78	SBC must support HTTP/HTTPS proxy functionality with the ability to set the number of simultaneous HTTP(S) connections from a single sip client/phone.
4.79	SBC must support SIP protocol operation via WebSocket and HTTP/HTTPS protocol.
4.80	SBC must support the ICE (Interactive Connectivity Establishment) and ICE Lite protocols
4.81	SBC must support encryption of media information (RTP) using the DTLS protocol.

4.82	SBC must support RTCP Feedback (RFC 5124), which allows SIP devices to exchange information about the current bit rate of the media stream.
4.83	SBC shall support number modification using information obtained through the LDAP protocol.
4.84	SBC must support call routing based on information received through the Rest API protocol.
4.85	SBC shall support number modification based on information received through the Rest API protocol.
4.86	SBC must support call authorization using the OAuth 2.0 protocol.
4.87	SBC shall support call duplication to the recording system using the SIPREC protocol.
4.88	SBC must support simultaneous DTMF sending in SIP INFO and RFC2833 formats.
4.89	SBC must be able to split the call based on information obtained through the LDAP protocol.
4.90	SBC must support the DHCP server function.
4.91	In case of loss of connection to the telephone exchange in Access mode, the SBC must support base call functions for registered devices between each other and to an external SIP trunk.
4.92	SBC must support up to 5 alternate names (SAN) in a downloadable TLS certificate.
4.93	SBC must support playing an external audio file on hold.
4.94	SBC must be able to reroute a call based on the QoS value (e.g., MOS) if the average quality of calls in a given direction is lower than the specified value.
4.95	SBC must be able to snapshot the system with its own hardware, regardless of the snapshot of the virtualization system.

5. Cerințe de administrare pentru controlerul de frontieră pentru sesiuni.

Toate cerințele listate în secțiunea 5 trebuie să fie îndeplinite în modul de cluster SBC redundand geografic (elementele clusterului sunt instalate în centre de date diferite)

No.	Name of evaluation criterion
5.1	SBC must be configurable via a Graphical User Interface (GUI) as well as a Command Line Interface (CLI)
5.2	SBC should be able to display basic system KPIs (CAPS, memory/CPU utilization, number of sessions, etc.) in the form of graphs.
5.3	SBC should have a built-in capability to dump network (signaling, service traffic) traffic passing through SBC in pcap format
5.4	SBC must support viewing CDR records from the Web interface.
5.5	SBC must be able to connect securely to the GUI via https protocol.
5.6	SBC must be able to act as a source of information (sample) for the Monitoring System

5.7	SBC must support system management via external REST API interface
5.8	SBC must support system monitoring via external Rest API interface
5.9	SBC must support different access levels for different user groups.
5.10	SBC must support authentication to the SBC via corporate directory credentials (Active Directory)
5.11	SBC should provide syntax checking and auto-filling of fields in tables where internal variables, header names, internal parameters, regular expressions are required.

6. Cerințe pentru sistemul de management al controlerului de frontieră pentru sesiuni cu funcționalitate extinsă pentru monitorizarea rețelelor UC/VoIP

No.	Name of evaluation criterion
6.1	The system must support SIP protocol monitoring.
6.2	SBC as a source of information.
6.3	The system should be able to measure the call quality (R-Factor, MOS) using as a source of information: RTP, RTCP, RTCP - XR . And also using information from the devices themselves.
6.4	The system should be able to analyze and display the voice quality for each call individually.
6.5	The system should be able to display the average total quality by direction, device, VoIP network as a whole
6.6	The call information must contain information about all signaling messages (and their content) for the given call and the voice quality at all call segments monitored by the system.
6.7	The system should be able to filter calls by: call start/end time, call duration, voice quality, A/B numbers, call end code, etc.
6.8	The system must be able to display the call in graphical form (a diagram of the call flow through network devices) with detail down to each signaling message and its content.

6.9	The system must have the ability to control key traffic parameters (Key Performance Indicator) on VoIP network segments with the ability to customize them: • Basic parameters – number of call attempts, number of unsuccessful calls, etc. • Advanced parameters – ASR, average call duration, average connection establishment time, etc. • Quality control parameters at the network, device, and direction levels
6.10	The system must have the ability to set KPI threshold values, upon reaching which the system must inform the service personnel about this event using SNMP trap or by means of an e-mail message.
6.11	The system must be able to be installed on VMWare, Hyper – V media
6.12	The system should be able to import SBC configuration for automatic provisioning of monitoring functionality.
6.13	The system should be able to download call statistics. It should support up to 1,000,000 records per download.
6.14	The system must support backup and restore of the configuration.
6.15	The system must support mass configuration changes on a group or all SBCs.
6.16	The system must support monitoring of device performance (Performance monitoring). The system must support at least 500,000 different metrics
6.17	The management system must support monitoring of device performance (Performance monitoring). The system must support at least 500,000 different metrics
6.18	The system must support user authentication using information from the corporate directory (Active Directory)
6.19	The system must support the collection of connection quality information from end devices using the RFC 6035 protocol.
6.20	The system should provide the ability to download reports on various parameters. Downloading should be done either manually or on schedule.
6.21	The system must support integration with external monitoring systems to redirect SNMP system messages.

7. Condiții de service în garanție și suport tehnic extins.

7.1. Perioada de garanție

Perioada de garanție pentru Sistemul furnizat este de cel puțin 1 an.

7.2. Condiții de service în perioada de garanție

Perioada de întreținere este de 12 luni.

Suportul în perioada de garanție acoperă întregul complex al componentei de software-aplicație furnizată a Controlerului de Frontieră pentru Sesiuni (SBC).

Întreținerea în perioada de garanție/post-garanție a Produselor în perioada specificată include următoarele servicii:

- În cazul în care sunt descoperite defecte în funcționarea Produselor în perioada de garanție a pachetului software, Furnizorul se angajează să elimine defectele pe cont propriu și pe cheltuiala proprie, asigurând continuitatea procesului de afaceri.
- Furnizorul va începe lucrările de eliminare a defectelor produsului în ziua primirii solicitării, în termen de 4 ore de la primirea acesteia, în cazul unui incident critic care întrerupe procesele de afaceri ale Clientului – în termen de 1 oră de la primirea solicitării.
- În cazul în care Clientul efectuează lucrări planificate care au riscuri mari de influență asupra proceselor de afaceri, Contractorul va trimite un specialist pentru a sprijini aceste lucrări și pentru a minimiza riscurile acestora. În acest caz, Clientul va conveni cu Executorul asupra orei lucrărilor cu cel puțin 5 zile înainte de perioada planificată a executării lucrărilor.
- Solicitățile de service sunt gestionate 24 de ore pe zi, 7 zile pe săptămână, 365 de zile pe an.
- Dacă este necesar, Furnizorul va asigura prezența unui inginer la fața locului pentru a rezolva incidente critice sau pentru a sprijini lucrările cu risc înalt.
- Costurile suplimentare suportate de Furnizor pentru îndeplinirea obligațiilor de garanție nu vor implica costuri suplimentare pentru Client.
- Furnizorul va organiza pentru persoanele autorizate ale Clientului accesul la portalele electronice de informații ale producătorilor Produselor și Software-ului Sistemului (SW) inclus în Produse, cu posibilitatea de a monitoriza starea solicitărilor și apelurilor de service ale Clientului, pentru întreaga perioadă a Acordului de Suport al Serviciului.
- Furnizorul va organiza posibilitatea de a angaja specialiști din Centrul de Competență al Furnizorului și/sau al Producătorului pentru a evalua impactul lucrărilor de integrare cu echipamente de terți și modificările arhitecturii sistemului planificate pe echipamentele Clientului (prin acord preliminar separat).
- În cazul în care apare o problemă tehnică sau o întrebare în timpul operării, asigurându-se că solicitările sunt primite prin telefon, e-mail sau prin portalul de

înregistrare a aplicației, 24 de ore pe zi, 7 zile pe săptămână, iar timpul necesar pentru a răspunde solicitării este conform următoarelor priorități:

Critic:

Sistemul nu funcționează și nu poate îndeplini sarcinile de bază. Pierdere completă sau semnificativă a funcționalității software-ului, care are un impact critic asupra afacerii. Funcționalitatea rețelei nu poate fi restaurată de utilizator, nici măcar într-o măsură limitată.

- Timpul de răspuns la incident – 10 minute. Reprezintă timpul de la deschiderea incidentului până la intervenția specialistului echipei de suport asupra sistemului.
- Timpul de rezolvare – 1 oră. Reprezintă timpul de la deschiderea incidentului până la rezolvarea acestuia. Rezolvarea poate fi temporară, dar face funcțiile afectate disponibile.

Major:

Prezența defecțiunilor severe ale sistemului. Degradare semnificativă a performanței, păstrând funcționalitatea. Performanța normală nu poate fi restaurată de specialiștii Clientului.

- Timpul de răspuns la incident – 1 oră. Reprezintă timpul de la deschiderea incidentului până la intervenția specialistului echipei de suport asupra sistemului.
- Timpul de rezolvare – 4 ore. Reprezintă timpul de la deschiderea incidentului până la rezolvarea acestuia. Rezolvarea poate fi temporară, dar face funcțiile afectate disponibile.

Minor:

Prezența defecțiunilor minore în funcționarea complexului software. Operabilitatea s-a deteriorat, dar majoritatea funcțiilor sunt păstrate.

- Timpul de răspuns la incident – 8 ore.
- Timpul de rezolvare – 48 de ore. Acesta este timpul de la deschiderea incidentului până la rezolvarea acestuia sau furnizarea unei soluții temporare.

8. Criterii de evaluare a soluției SBC propuse pentru licitație.

Raportul cel mai bun cost/beneficiu va fi luat în considerare. Produsul propus va fi, de asemenea, testat pentru a se asigura că îndeplinește cerințele solicitate. Toți licitatorii vor fi solicitați să pună soluția propusă la dispoziție pentru testare și să ofere suport complet pentru integrare și personalizare.

Propunerea va fi evaluată pe baza următoarelor criterii:

(O) Propunerea de preț - maximum 40 p. (puncte)

(Ex) Experiență anterioară în implementarea soluțiilor propuse pe rețelele unor operatori majori de telecomunicații sau servicii de intervenție de urgență - 10 p. (puncte). Feedback pozitiv din partea beneficiarului este binevenit.

(Ext) Conformitatea cu specificațiile tehnice conform tabelului de conformitate - maximum 20 p. (puncte). Nu îndeplinește 1-3 cerințe - 10 p. (puncte), până la 5 cerințe - 0 p. (puncte).

(P) Evaluare bazată pe rezultatele testelor pentru conformitatea cu funcționalitatea enunțată - maximum 20 p. (puncte).

(S) Conformitatea cu toate cerințele pentru ofertant conform punctului 2. Toate cerințele îndeplinite - 10 p. (puncte). Cel puțin o cerință nu este îndeplinită - 0 p. (puncte).

Formula de calcul: $N = O/Ob*40 + Ex + Ext + P + S$

Unde:

N - scorul cumulativ

O - oferta evaluată

Ob - cea mai bună ofertă

Ex - scorul cumulativ la evaluarea experienței anterioare de implementare a soluțiilor propuse

Ext - scorul obținut la evaluarea conformității cu specificațiile tehnice

P - scorul obținut pe baza rezultatelor testelor

S - scorul obținut la evaluarea conformității cu cerințele participantului.

9. Informația suplimentară.

Conform HG nr.246/2010 cu privire la modul de aplicare a facilităților fiscale și vamale aferente realizării proiectelor de asistență tehnică și investițională în derulare, care cad sub incidența tratatelor internaționale la care Republica Moldova este parte sau a contractelor de stat, proiectul nr. 872112584881 X-HeERO-eCall Next Generation „eCall NG”, cade sub incidența tratatelor internaționale, pentru aplicarea scutirilor la impozitul pe venit, accize, taxe vamale, taxe pentru efectuarea procedurilor vamale, taxe pentru mărfurile care, în procesul utilizării, cauzează poluarea mediului, precum și aplicarea scutirii de TVA cu drept de deducere pentru mărfurile și serviciile destinate acestora.