MONITORUL OFICIAL AL ROMÂNIEI

Anul 179 (XXIII) — Nr. 491

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Luni, 11 iulie 2011

SUMAR

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL ADMINISTRAȚIEI ȘI INTERNELOR

ORDIN
pentru organizarea activităților privind accesul poliției locale la baze de date ale Ministerului Administrației și Internelor

Având în vedere dispozițiile art. 20 alin. (2) din Legea poliției locale nr. 155/2010,
în temeiul art. 7 alin. (4) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Administrației și Internelor nr. 30/2007, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare,

ministrul administrației și internelor emite următorul ordin:

Art. 1. — (1) Se abilitează Inspectoratul General al Poliției Române, prin Direcția Generală de Poliție a Municipiului București și inspectoratele județene de poliție, Direcția pentru evidența persoanelor și administrarea bazelor de date și Direcția regim permise de conducere și înmatriculare a vehiculelor, denumite în continuare *structuri abilitate*, să încheie protocoale de colaborare cu unitatea/subdiviziunea administrativ-teritorială în care se organizează și funcționează poliție locală, având ca obiect asigurarea accesului la baze de date ale Ministerului Administrației și Internelor, potrivit prevederilor art. 20 alin. (2) din Legea poliției locale nr. 155/2010.

(2) Direcția generală pentru comunicații și tehnologia informației din cadrul Ministerului Administrației și Internelor, împreună cu structurile abilitate, asigură condițiile tehnice necesare pentru realizarea accesului poliției locale la bazele de date menționate.

Art. 2. — Bazele de date ale Ministerului Administrației și Internelor la care se asigură accesul poliției locale, în condițiile legii, sunt prevăzute în anexa nr. 1.

Art. 3. — (1) Pentru aplicarea unitară a dispozițiilor legale, protocoalele de colaborare încheiate între structurile abilitate și unitățile/subdiviziunile administrativ-teritoriale în care se organizează și funcționează poliția locală trebuie să conțină cel puțin clauzele prevăzute în modelul Protocolului privind accesul poliției locale la baze de date ale Ministerului Administrației și Internelor, prevăzut în anexa nr. 2.

(2) Accesul poliției locale la bazele de date se realizează cu respectarea clauzelor tehnice și de securitate prevăzute în anexa nr. 3. Clauzele tehnice și de securitate se prevăd ca anexă la protocolul de colaborare încheiat potrivit alin. (1).

Art. 4. — Anexele nr. 1—3 fac parte integrantă din prezentul ordin.

Art. 5. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Ministrul administrației și internelor,
Constantin-Traian Igaș

București, 22 iunie 2011.
Nr. 128.

ANEXA Nr. 1

BAZE DE DATE
ale Ministerului Administrației și Internelor la care se asigură accesul poliției locale

Nr. crt.	Denumirea bazei de date	Structura abilitată care administrează baza de date
1.	Evidența informatică a persoanelor date în urmărire și a persoanelor dispărute — „Urmăriți”	Inspectoratul General al Poliției Române
2.	Evidența informatică a furturilor de autovehicule săvârșite în România și a celor săvârșite în alte state sesizate oficial Poliției Române — „Furt auto”	Inspectoratul General al Poliției Române
3.	Registrul național de evidență a permiselor de conducere și a vehiculelor înmatriculate	Direcția regim permise de conducere și înmatriculare a vehiculelor
4.	Registrul național de evidență a persoanelor	Direcția pentru evidența persoanelor și administrarea bazelor de date

ANEXA Nr. 2

— Model —

P R O T O C O L

privind accesul Poliției Locale a ….....

(municipiul/orașul/sectorul/comuna)

la baze de date ale Ministerului Administrației și Internelor

Primăria .....….
(municipiul/orașul/sectorul/comuna)
Poliția Locală a .....….
(municipiul/orașul/sectorul/comuna)
Nr. ..... din .....….

Inspectoratul de Poliție Județean
.....
sau
Direcția Generală de Poliție a Municipiului București
Nr. .....… din .....….

Direcția pentru evidența persoanelor
și administrarea bazelor de date
Nr. .....… din .....….

Direcția regim permise de conducere
și înmatriculare a vehiculelor
Nr. .....… din .....….

Având în vedere dispozițiile art. 3 din Legea nr. 218/2002 privind organizarea și funcționarea Poliției Române, cu modificările și completările ulterioare, ale art. 11^5 alin. (1) lit. e), f) și h) din Ordonanța Guvernului nr. 83/2001 privind înființarea, organizarea și funcționarea serviciilor publice comunitare pentru eliberarea și evidența pașapoartelor simple și serviciilor publice comunitare regim permise de conducere și înmatriculare a vehiculelor, aprobată cu modificări și completări prin Legea nr. 362/2002, cu modificările și completările ulterioare, și ale art. 2 alin. (1) lit. c) și art. 3 din Hotărârea Guvernului nr. 1.367/2009 privind înființarea, organizarea și funcționarea Direcției pentru Evidența Persoanelor și Administrarea Bazelor de Date,

ținând seama de dispozițiile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare, și ale Ordinului Avocatului Poporului nr. 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal,

având în vedere că Poliția Locală a …..... este înregistrată la Autoritatea Națională
(municipiul/orașul/sectorul/comuna)
de Supraveghere a Prelucrării Datelor cu Caracter Personal ca operator de date cu caracter personal, cu număr de notificare .....…,

în temeiul art. 20 alin. (2) din Legea poliției locale nr. 155/2010 și al art. 34 lit. a) din Regulamentul-cadru de organizare și funcționare a poliției locale, aprobat prin Hotărârea Guvernului nr. 1.332/2010,

se încheie prezentul protocol

între:

Unitatea administrativ-teritorială .....…, reprezentată de domnul .....…, în calitate de primar,
(municipiul/orașul/sectorul/comuna)

și

Inspectoratul de Poliție Județean …../Direcția Generală de Poliție a Municipiului București, cu sediul în .....…, reprezentat(ă) de …....., în calitate de .....…,

Direcția pentru evidența persoanelor și administrarea bazelor de date, cu sediul în .....…, reprezentată de …....., în calitate de director,

Direcția regim permise de conducere și înmatriculare a vehiculelor, cu sediul în .....…, reprezentată de ....., în calitate de director, denumite în continuare *structuri abilitate*.

Obiectul protocolului

Art. 1. — Prezentul protocol are ca obiect asigurarea accesului la baze de date ale Ministerului Administrației și Internelor, pentru îndeplinirea atribuțiilor legale ale poliției locale, în conformitate cu dispozițiile art. 20 alin. (2) din Legea poliției locale nr. 155/2010.

Baze de date

Art. 2. — Bazele de date la care se asigură accesul poliției locale, denumite în continuare *baze de date*, sunt[1)]:

a) .....…

b) .....… ș.a.m.d.

Accesul la bazele de date

Art. 3. — (1) Accesul la bazele de date se asigură în condițiile legii, cu respectarea clauzelor cuprinse în prezentul protocol, exclusiv pentru îndeplinirea atribuțiilor legale ale poliției locale.

(2) Condițiile tehnice și de securitate privind accesul la bazele de date sunt prevăzute în anexa nr. 1, respectiv în specificațiile tehnice stabilite de Serviciul de telecomunicații speciale, denumit în continuare *STS,* împreună cu Direcția generală comunicații și tehnologia informației, denumită în continuare *DGCTI*, din cadrul Ministerului Administrației și Internelor.

(3) Accesul la bazele de date se realizează exclusiv prin intermediul aplicațiilor informatice puse la dispoziție de structurile abilitate, pe suportul de comunicații asigurat de DGCTI și STS, de persoane anume desemnate, agreate de părți, denumite în continuare *utilizatori*. Datele de identificare ale utilizatorilor se transmit în timp util părții interesate.

[1)] Se nominalizează bazele de date prevăzute în anexa nr. 1 la Ordinul ministrului administrației și internelor nr. 128/2011 pentru organizarea activităților privind accesul poliției locale la baze de date ale Ministerului Administrației și Internelor, în raport de solicitările concrete formulate de poliția locală.

(4) Accesul la bazele de date se realizează numai prin dispeceratul poliției locale și se limitează la maximum două stații/dispecerat. Numărul maxim de utilizatori la nivelul poliției locale este de 5.

Condiții pentru utilizatori

Art. 4. — (1) Utilizatorii dobândesc drept de acces la bazele de date numai după semnarea unui angajament de confidențialitate, al cărui model este prevăzut în anexa nr. 2, și a unui instructaj cu privire la normele legale în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal, respectiv numai în condițiile deținerii unui certificat digital eliberat de STS.

(2) Se interzice utilizatorilor să transmită datele de autentificare altor persoane ori să utilizeze alte date de autentificare decât cele alocate.

Responsabilitățile structurilor abilitate

Art. 5. — În vederea realizării obiectului protocolului, structurilor abilitate le revin următoarele responsabilități:

a) să colaboreze cu structurile teritoriale ale STS pentru asigurarea accesului la bazele de date, potrivit solicitărilor adresate în scris de poliția locală;

b) să monitorizeze toate accesările și să țină o evidență a acestora, în condiții care să permită identificarea utilizatorului;

c) să pună la dispoziția poliției locale aplicațiile informatice prin care se asigură accesul la bazele de date, în condiții de securitate a prelucrării;

d) să urmărească respectarea de către poliția locală a condițiilor de accesare a bazelor de date și să revoce dreptul de acces, în cazul constatării unor încălcări ale acestor condiții;

e) să ofere expertiza necesară pentru realizarea obiectului protocolului, la solicitarea poliției locale.

Responsabilitățile poliției locale

Art. 6. — În vederea realizării obiectului protocolului, poliției locale îi revin următoarele responsabilități:

a) să solicite accesul la bazele de date și să comunice, în scris, Direcției Generale de Poliție a Municipiului București/inspectoratului de poliție județean competent teritorial informațiile prevăzute la pct. III din anexa nr. 1;

b) să stabilească sediile de la care se realizează accesul la bazele de date și să solicite evaluarea acestor sedii din punct de vedere tehnic;

c) în funcție de soluția tehnică identificată, să achiziționeze și să utilizeze echipamentele și serviciile prevăzute în proiectul tehnic propus/avizat de STS și Ministerul Administrației și Internelor, denumit în continuare *MAI*; să solicite asistență tehnică, pe durata procesului de operaționalizare a conexiunilor;

d) să consulte bazele de date numai prin intermediul aplicațiilor informatice puse la dispoziție de MAI;

e) să stabilească utilizatorii și să le distribuie certificatele digitale emise de STS, să asigure instruirea periodică a acestora și să comunice Direcției Generale de Poliție a Municipiului București/inspectoratului de poliție județean competent teritorial orice modificări intervenite în situația fiecărui utilizator, pentru care s-ar impune revocarea dreptului de acces;

f) să întocmească metodologii proprii de lucru privind protecția datelor cu caracter personal;

g) să sesizeze de îndată unitatea de poliție competentă teritorial în cazul identificării unor persoane sau autovehicule urmărite;

h) să nu conecteze echipamentele prin care se asigură accesul la bazele de date la alte rețele;

i) să constituie registre conținând cererile de interogare și motivațiile acestora, să le păstreze la sediul dispeceratului, pentru o perioadă de cel puțin 2 ani, împreună cu angajamentele de confidențialitate și instructajele periodice, și să le pună la dispoziția autorităților competente în domeniu;

j) să ia măsurile necesare pentru asigurarea confidențialității și securității prelucrărilor de date;

k) să nu dezvăluie către terți datele obținute din accesarea bazelor de date;

l) să ia măsurile legale ce se impun atunci când se constată că informațiile din bazele de date au fost utilizate cu încălcarea prevederilor legale în vigoare și ale prezentului protocol.

Respectarea drepturilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare

Art. 7. — (1) Pentru respectarea dreptului de acces prevăzut de Legea nr. 677/2001, cu modificările și completările ulterioare, în cazul unor cereri care vizează prelucrările efectuate de utilizatori din cadrul poliției locale, structurile abilitate vor transmite către poliția locală o solicitare scrisă, în termen de 48 de ore de la înregistrarea cererii.

(2) În termen de 5 zile lucrătoare de la data înregistrării solicitării prevăzute la alin. (1), poliția locală va formula răspuns către structura abilitată solicitantă, în care va menționa scopul în care a fost efectuată prelucrarea.

(3) Poliția locală va informa de îndată structurile abilitate atunci când, cu privire la datele cu caracter personal furnizate de Ministerul Administrației și Internelor, apare una din următoarele situații:

a) există o solicitare de dezvăluire a datelor cu caracter personal, adresată de o autoritate publică;

b) s-a produs o dezvăluire accidentală sau neautorizată a datelor cu caracter personal prelucrate;

c) s-a produs un incident tehnic de securitate care este de natură să conducă la dezvăluirea de date cu caracter personal;

d) există o solicitare primită direct de la persoanele vizate referitoare la datele cu caracter personal prelucrate.

Comunicarea între părți

Art. 8. — (1) Orice comunicare între părți în scopul realizării obiectului protocolului se realizează în scris.

(2) Comunicările între părți se pot realiza și prin telefon, fax sau e-mail, sub condiția confirmării în scris a primirii comunicării.

(3) Notificările transmise prin fax sau e-mail se consideră primite în prima zi lucrătoare următoare celei în care au fost expediate.

Intrarea în vigoare și amendamente

Art. 9. — (1) Prezentul protocol intră în vigoare la data semnării și înregistrării de către părți și este valabil un an de la această dată.

(2) Valabilitatea protocolului se prelungește de drept, pe perioade succesive de câte un an, dacă niciuna dintre părți nu notifică celeilalte, cu cel puțin 30 de zile înainte de expirarea termenului, voința de încetare a aplicabilității acestuia.

(3) Prezentul protocol poate fi modificat/completat prin acordul scris al ambelor părți, cu respectarea regulilor prevăzute la alin. (1) și (2).

(4) Protocoalele de colaborare încheiate până la data intrării în vigoare a prezentului protocol, având ca obiect accesul la bazele de date menționate la art. 2, își încetează aplicabilitatea[2)].

Eficientizarea cooperării

Art. 10. — Părțile vor analiza, ori de câte ori situația impune, modul de îndeplinire a obiectului protocolului și se vor informa reciproc cu privire la problemele constatate, în vederea luării măsurilor optime.

Anexele la protocol

Art. 11. — Anexele nr. 1 și 2 fac parte integrantă din prezentul protocol.

Prezentul protocol a fost întocmit în … exemplare, câte unul pentru fiecare parte semnatară.

Primar,
…….....……

Inspectorul șef al Inspectoratului de Poliție Județean,
…….....……
sau
Directorul general al Direcției Generale de Poliție a Municipiului București,
…….....……
Directorul Direcției pentru evidența persoanelor și administrarea bazelor de date,
…….....……
Directorul Direcției regim permise de conducere și înmatriculare a vehiculelor,
…….....……

[2)] Prevederea se înscrie în măsura în care la nivel local au fost încheiate cu structurile Ministerului Administrației și Internelor protocoale de colaborare având ca obiect accesul la bazele de date prevăzute în anexa nr. 1 la Ordinul ministrului administrației și internelor nr. 128/2011 pentru organizarea activităților privind accesul poliției locale la baze de date ale Ministerului Administrației și Internelor.

ANEXA Nr. 1
la protocol

CONDIȚII TEHNICE ȘI DE SECURITATE
privind accesul poliției locale la bazele de date ale Ministerului Administrației și Internelor

Se înscriu datele prevăzute în anexa nr. 3 la Ordinul ministrului administrației și internelor nr. 128/2011 pentru organizarea activităților privind accesul poliției locale la baze de date ale Ministerului Administrației și Internelor. La pct. I și II, se vor înscrie datele tehnice și de securitate rezultate după alegerea soluției tehnice care va fi implementată.

ANEXA Nr. 2
la protocol

ANGAJAMENT DE CONFIDENȚIALITATE

Subsemnatul/Subsemnata, ...…, născut(ă) în localitatea .....…, la data de …....., fiul(fiica) lui ….. și al(a) …..... angajat(ă) al(a) …....., în funcția de …....., cu domiciliul în …....,

declar pe propria răspundere că am luat cunoștință de prevederile legale privind protecția datelor cu caracter personal și consimt să păstrez confidențialitatea datelor cu caracter personal a căror prelucrare o efectuez în condițiile legii, în virtutea atribuțiilor de serviciu, inclusiv după încetarea activităților de prelucrare a acestor date.

Cunosc faptul că încălcarea prevederilor legale privind protecția datelor cu caracter personal atrage răspunderea administrativă, disciplinară, materială, civilă ori penală, în raport de gravitatea faptei, potrivit legii.

ANEXA Nr. 3

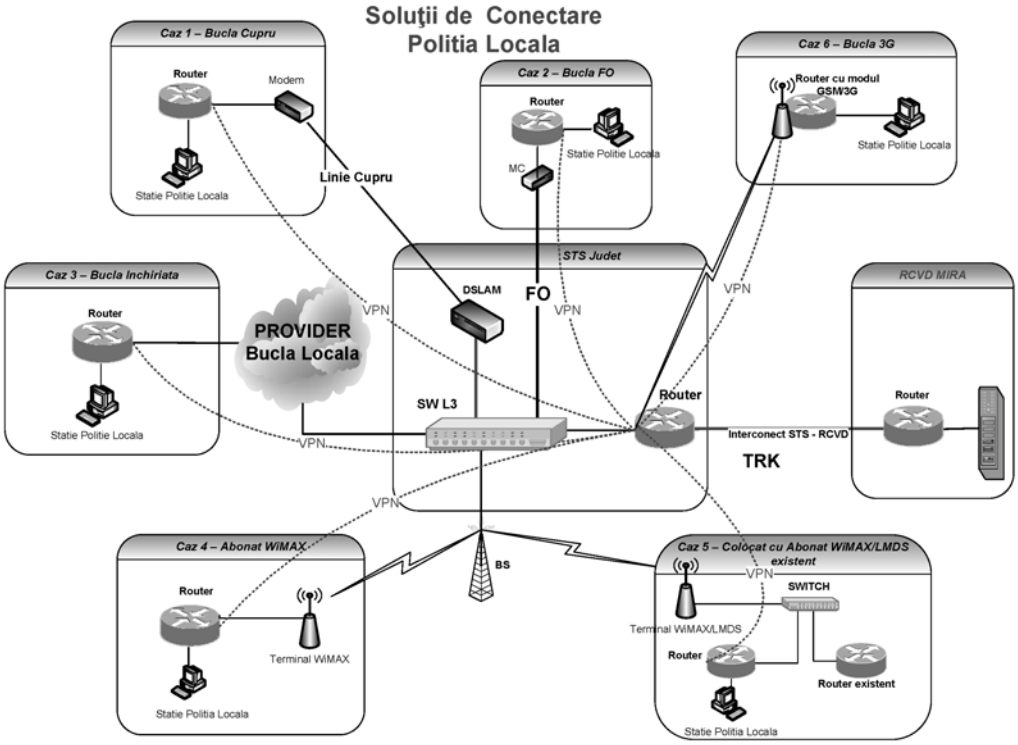
CLAUZE TEHNICE ȘI DE SECURITATE
privind accesul poliției locale la bazele de date ale Ministerului Administrației și Internelor

I. **Soluțiile tehnice posibile pentru conectarea la bazele de date ale Ministerului Administrației și Internelor**

Serviciul de Telecomunicații Speciale, *STS,* oferă servicii de transport pe suportul infrastructurii proprii administrate, soluțiile de buclă locală fiind propuse în funcție de locație și de furnizor, utilizându-se tehnologii radio, cupru și fibră optică.

Soluția de conectare va fi selectată în urma prospectării amplasamentului de către reprezentanții STS, propunându-se, prin proiectul tehnic pentru implementare, cea mai fiabilă soluție pentru fiecare locație în parte.

Soluțiile tehnice posibile pentru realizarea conectării sunt după cum urmează:



1. Buclă locală pe cablu cupru — necesar: router
2. Fibră optică — necesar: router, media convertoare (MC)
3. Buclă locală închiriată — necesar: router, închiriere buclă locală
4. Abonat nou WiMAX — necesar: terminal fix WiMAX, router
5. Colocat cu abonat WiMAX/LMDS existent — necesar: switch cu management, router
6. Buclă 3G — necesar: router cu modul 3G + SIM operatori de telefonie mobilă

Se vor realiza conexiuni VPN criptate între routerul din sediul poliției locale și routerul STS din OJTS, acestea fiind rutate către rețeaua RCVD MAI prin interconectul existent.

Pentru situațiile în care bunurile și serviciile nu pot fi asigurate din resurse proprii STS sau MAI, pentru implementarea soluției tehnice, acestea vor fi achiziționate de pe piața publică. Caracteristicile tehnice ale serviciilor sau/și produselor sunt cele de mai jos.

După instalare, echipamentele vor fi preluate în sistemul de management de către STS și vor fi monitorizate 7 x 24 pentru prevenirea și remedierea eventualelor deranjamente. Responsabilitatea STS pentru remedierea deranjamentelor se va extinde numai asupra elementelor de comunicații, aplicațiile și funcționarea rețelei RCVD fiind în responsabilitatea reprezentanților MAI.

Punctul de contact unic pentru remedierea deranjamentelor este NOC OJTS, urmând ca în funcție de domeniul în care se încadrează deranjamentul sesizat, acesta să fie eventual escaladat către NOC STS București, respectiv MAI.

STS configurează echipamentele aflate în fiecare locație a beneficiarului pentru criptarea capăt-la-capăt a canalului de transport folosind tehnologia IPSec cu algoritmi de schimbare chei și de criptare avansați. În acest mod se asigură transportul securizat al informațiilor ce tranzitează rețeaua de comunicații de date fixă și se garantează decriptarea informațiilor doar la capetele legăturii de comunicație.

STS pune la dispoziție un server de DNS care are rolul de a face forward la cererile stațiilor client către un server DNS MAI.

II. **Specificații tehnice și de securitate**

1. Specificații bucla locală

I. Suportul fizic pe care este asigurată legătura de date:

— conexiune permanentă instalată la sediul beneficiarului, pentru serviciul de buclă locală;

— se vor asigura echipamentele de media conversie pentru suportul fizic oferit, acestea asigurând cel puțin o interfață Ethernet/Fast Ethernet;

— serviciul de comunicații de buclă locală va trebui să permită dirijarea traficului între locația beneficiarului și PoP STS, în vederea rutării traficului către RCVD MAI.

II. Caracteristicile tehnice ale legăturilor de date (obligatorii):

— conexiuni permanente nivel 2 dedicate, VLAN Ethernet, EoMPLS, VPWS, VPLS, end-to-end (denumite generic *conexiuni nivel 2*);

— furnizorul are obligația să asigure separarea traficului asigurat pentru acest proiect de restul traficului transportat prin rețelele sale (VLAN dedicat).

III. Caracteristici generale de performanță:

— disponibilitatea accesului = 99,90%;

— latența pachetelor/1.000 pachete < 30 ms;

— procent de pachete pierdute < 1%;

— bandă garantată: 100%.

2. Specificații router

Carcasa	• Router rack-mount 19 inch de 1U sau kit de montare în rack (tavă, șuruburi, piulițe, alte accesorii)
Procesor	• Accelerator hardware VPN integrat (onboard)
Memorie instalată	• Flash minimum 32 MB • BOOT/NVRAM minimum 2MB • DRAM minimum 128 MB • Memoria instalată va trebui să asigure simultan toate funcționalitățile solicitate
Standarde	• IEEE 802.3 • IEEE 802.3u • IEEE 802.1q
Protocoale suportate	• Stiva TCP/IP • RIP v1 și v2 • OSPF • BGP • SNMPv3, SSHv2 • DMVPN sau echivalent • CDP sau echivalent
Switching protocol	• Ethernet și Fast Ethernet
Interfețe	• 2 x port 10/100 BaseT/TX Fast Ethernet RJ-45 integrate (onboard) • Switch de 8 porturi 10/100 BaseT/TX Fast Ethernet RJ-45, cu management și suport pentru VLAN-uri, integrat (onboard) • Modem analog V.92 integrat (onboard) • 1 X port management console (115.2 kbps) • 1 X port auxiliar (115.2 kbps) • 2 X port USB 2.0
Sistem de operare și caracteristici minimale incluse	• Configurabil de la consolă prin command line interface, via SSH și telnet, configurabil web • Suport pentru servicii integrate • Suport pentru „express forwarding” • Imagine sistem de operare cu suport pentru pachet de securitate și servicii IP avansate (a se specifica denumirea sistemului de operare furnizat) • Firewall (stateful, transparent, URL filtering), NAT, IPSec, VPN (DES, 3DES, AES128, AES192, AES256), QoS, AAA integrate în sistemul de operare • Licență 3DES și AES256 inclusă sau drepturi de configurare echivalente licențierii 3DES și AES256 • Criptare hardware integrată • Suport pentru maximum 50 de tunele IPSec • Throughput de până la 70000 pps • Până la 8 VLAN-uri 802.1q • Ceas intern în timp real
Temperatura de operare	• 0 la 40°C
Alimentare cu energie electrică	• Sursa de alimentare internă cu suport pentru standardele românești: 220 VAC/50 Hz internă
Certificare ISO	• Certificat ISO 9001 pentru producător
Accesorii	• 1 X cablu consolă • 1 X cablu de alimentare energie electrică tip șuco conform standardelor românești

	• Documentație cu manual de utilizare și configurare tipărit • Documentație cu manual de utilizare și configurare în format electronic pe mediu optic (CD) • 1 X kit de instalare cu toate cablurile de protecție (împământare), șuruburile și alte accesorii necesare instalării și punerii în funcțiune incluse

3. Specificații switch

Descriere generală	8 X 10/100 Ethernet 2 X 10/100/1000 Ethernet
Capacitate de comutație și transfer	• Minimum 4 milioane de pachete pe secundă (pachete de 64 octeți) • Capacitate de comutare (Gbps): 5,5
Caracteristici și performanțe	• Suport pentru cadrele Jumbo • Tabela MAC suportă până la 8000 de intrări • LLDP (Link Layer Discovery Protocol) (802.1ab) • CDP • Flash: 16MB; • Memorie procesor: 128 MB • Packet buffer: 4 MB
Protocoale suportate	• IEEE 802.1d STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP • GVRP (Generic Vlan Registration Protocol) • IEEE 802.3ad LACP (până la 8 grupuri) • IGMP (până la 256 de grupuri de multicast)
VLAN	• Suportă 256 vlan-uri (în sistemul 4096 VLAN ID) • Vlan-uri bazate pe tag-uri și porturi 802.1q • Vlan-uri bazate pe MAC • Vlan de management • Vlan voce (traficul de voce este asignat automat unui vlan de voce și tratat cu nivelele corespunzătoare de QOS) • PVE — Private Edge Vlan • Vlan Guest • Vlan neautentificat
Releu DHCP	• Retransmite traficul DHCP pentru un server DHCP din alt vlan (DHCP opțiunea 82)
Rutare IPv4	• Rutare la viteza cablului • Până la 32 de rute statice și 32 de interfețe IP • Suport pentru CIDR • Releu pentru traficul DHCP pe un domeniu IP
Securitate, acces distant	• SSH • SSL: criptează traficul HTTP pentru acces la interfața web a echipamentului • 802.1x • Izolare de nivel 3 (activează/dezactivează rutarea între rețele direct conectate) • PVE (Private Edge Vlan): izolare de nivel 2 între două dispozitive din același vlan și folosirea a mai multor legături de Uplink • Securitatea porturilor: blochează adresele MAC pe un port și limitează numărul de MAC-uri învățate • RADIUS/TACACS+: suport pentru autentificarea RADIUS și TACACS • Storm control • Prevenire atacuri DoS • ACL: până la 512 reguli; limitarea ratei de transfer sau drop pe baza adresei MAC, VLAN ID sau IP sursă și destinație, protocol, port, IP Precedence DSCP (Differentiated Services Code Point), port-sursă și destinație TCP/UDP, 802.1p priority, Ethernet type, ICMP (Internet Control Message Protocol) IGMP packets, TCP flag
QOS	• 4 cozi hardware • Strict priority și round-robin weighted • Asignarea cozilor se face pe baza DSCP și CoS (802.1p/CoS) • Clase de serviciu bazate pe: port, 802.1p VLAN priority, DSCP/ToS (type of service)/IP precedence IPv4/v6; Differentiated Services (DiffServ) clasificare și reclasificare a listelor de acces, QoS (QoS) trust • Rate control, VLAN, port and flow based

IPv6	• IPv6 host mode • IPv6 over Ethernet • Dual-stack IPv4 și IPV6 • Neighbor discovery și IPV6 routers (ND) • Automatic configuration of IPv6 Stateless Address • Path MTU discovery • Duplicate Address Detection (DAD) • ICMP Version 6 • Suport pentru ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) • Prioritizarea pachetelor Ipv6 în hardware • Rate limit sau drop a pachetelor Ipv6 în hardware • Aplicații Ipv6: Web/SSL, Telnet server/SSH, ping, traceroute, SNTP (Simple Network Time Protocol), TFTP (Trivial File Transfer Protocol), SNMP, RADIUS, syslog, DNS client, protocol-based VLANs
Management	• WEB, SNMP, MIB SNMP, RMON • Port mirroring, VLAN mirroring • Smartports • DHCP Options (66, 67, 82, 129 și 150)

4. Router cu modul 3G

Carcasa	• Router rack-mount 19 inch de 1U sau kit de montare în rack (tavă, șuruburi, piulițe, alte accesorii)
Procesor	• Accelerator hardware VPN integrat (onboard)
Memorie instalată	• Flash minimum 128 MB • BOOT/NVRAM minimum 2MB • DRAM minimum 256 MB • Memoria instalată va trebui să asigure simultan toate funcționalitățile solicitate
Standarde	• IEEE 802.3 • IEEE 802.3u • IEEE 802.1q • IEEE 802.11b • IEEE 802.11g • IEEE 802.11n • IEEE 802.1d
Protocoale suportate	• Stiva TCP/IP • RIP v1 și v2 • OSPF • EIGRP • BGP • NHRP • WCCP • BFD • GRE • SNMPv3, SSHv2 • DMVPN sau echivalent • CDP sau echivalent
Switching protocol	• Ethernet și Fast Ethernet
Interfețe	• 1 x port 10/100 BaseT/TX Fast Ethernet RJ-45 integrate (onboard) • Switch de 5 porturi 10/100 BaseT/TX Fast Ethernet RJ-45, cu management și suport pentru VLAN-uri, integrat (onboard) • 1 X port management console (115.2 kbps) • 1 X port auxiliar (115.2 kbps) • 2 X port USB 2.0 • Modul 3G
Rețele multiple mobile și standarde acceptate	• Modem multimode device pentru HSDPA/UMTS/EDGE/GPRS/GSM • Rețele mobile: GSM (2G) în benzile 900/1800/1900 MHz, GPRS/EDGE 900/1800 (2,5G) și • Rețele mobile 3G HSUPA/HSDPA/UMTS în benzile 850/1900/2100 MHz
Specificații antenă	• Benzi de frecvență: GSM 890—960 MHz, PCN 1710—1880 MHz, PCS 1850—1990 MHz, UMTS/HDSPA 1920—2170 MHz • Câștig antenă: minimum 0 dB • Polarizare verticală • Cablu: minimum 1,5 m

5. Specificații terminal fix WiMAX

Specificații tehnice generale	
	Rețeaua WiMAX existentă: — Rețeaua WiMAX este implementată și operată în concordanță cu standardele WiMAX. Deoarece rețeaua WiMAX este operațională, terminalele fixe WiMAX vor fi integrate în rețeaua existentă și operate conform condițiilor existente. — Rețeaua WiMAX este implementată cu următoarele tipuri de echipamente, produse și/sau integrate de către Airspan Networks Inc: • WiMAX BS: MacroMAXe (AIR 4G) • Arhitectura rețelei: Profile C (centralized ASN-GW) pentru servicii mobile • ASN-GW: AN1 WiMAX ASN-GW (Starent) • AAA: AAA Service Controller (Bridgewater) • RAN management: Netspan — EMS — Element Management System (Airspan) • CPE management: Friendly TR69 Management Server (Friendly Technologies) Se va preciza explicit posibilitatea terminalelor fixe WiMAX de a fi integrate în rețeaua WiMAX existentă.
	Norme și standarde aplicabile: — IEEE 802.16e-2005, wave 2 (MIMO matrix A și MIMO Matrix A) — ETSI EN 302 326-1-2-3 — Fixed Radio Systems; Multipoint Equipment and Antennas; Part 1 — Overview and Requirements for Digital Multipoint Radio Systems; Part 2 — Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive for Digital Multipoint Radio Equipment; Part 3 — Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive for Multipoint Radio Antennas — ETSI EN 302 623 — Broadband Wireless Access Systems (BWA) in the 3400 to 3800 MHz frequency band; Mobile Terminal Stations; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive — Directiva 2002/95/CE a Parlamentului European și a Consiliului din 27 ianuarie 2003 privind restricțiile de utilizare a anumitor substanțe periculoase în echipamentele electrice și electronice (RoHS) — alte standarde indicate în prezentele specificații NOTĂ: În situațiile în care prezentele specificații tehnice diferă sau sunt mai stricte decât standardele, vor prevala aceste specificații.
	Producătorul/furnizorul terminalelor fixe WiMAX trebuie să dovedească participarea la programul de certificare WiMAX Forum și că are cel puțin un terminal WiMAX certificat conform specificațiilor WiMAX Rev. E wave 2 în una dintre benzile de frecvență (2.5—2.7 GHz, 3.4—3.8 GHz). Va fi precizat tipul terminalului certificat, iar certificatul WiMAX Forum va fi atașat.
Specificații funcționale	
Distanța maximă față de stația de bază	Terminalul fix WiMAX va avea capabilități de conectare la stații de bază aflate la o distanță de aproximativ 20 km în condiții de vizibilitate directă LoS (Line-Of-Sight) sau aproape LoS (near Line-Of-Sight). Pentru obținerea acestor performanțe, stațiile de bază WiMAX existente (Airspan MacroMAXe) implementează parametrii TGG (Transmit Transition Gap) și IR (Initial Ranging) în mod diferit. Terminalele fixe WiMAX trebuie să suporte aceste modificări.
Suport MIMO și HARQ	Cerințele minime pentru MIMO și HARQ sunt: — Matrix A + MRC on DL pentru două antene — Matrix B on DL — HARQ va suportat împreună cu MIMO
Suportul pentru subnivelele de convergență și moduri de operare	Terminalele fixe WiMAX vor implementa subnivelele de convergență: IP CS și ETH CS. — Moduri de operare: • Bridge Mode: L2 ETH CS transparent VLAN services vor fi configurate în modul bridge; mai multe servicii de acces la nivelul terminalului vor fi separate între ele prin VLAN ID; • NAT Mode: L3 IP CS vor fi configurate în modul NAT (server DHCP pe interfața LAN și DHCP client pe interfața WAN).
Implementarea serviciilor de acces	L2 transparent VLAN services — operare în modul bridge — Ca urmare a înregistrării în rețea, bazată pe credențialele (username/password) de autentificare configurate în terminalul fix WiMAX,

	serverul AAA va proviziona numai fluxurile de servicii (service flows) de bază și primare, dar nu va permite traficul de date al utilizatorului. — Serviciile fixe L2 transparent VLAN vor fi provizionate în serverul existent WiMAX Element Management Server (NETSPAN furnizat de Airspan); aceste servicii sunt asociate cu adresa MAC a terminalului fix WiMAX. L3 IP CS services — operare în modul NAT — Ca urmare a înregistrării în rețea, bazată pe credențialele (username/pasword) de autentificare configurate în terminalul fix WiMAX, serviciile L3 vor fi provizionate în serverul AAA. — Serviciile L3 IP CS vor fi provizionate pentru modurile de acces nomadic și mobil.
Mobilitatea și rooamingul	— Terminalele WiMAX vor fi capabile să ofere servicii mobile în concordanță cu specificațiile IEEE 802.16e-2005 și WiMAX Forum (profile C architecture). Serviciile mobile vor fi provizionate de obicei în terminalul aflat în modul NAT. — Deoarece în cele mai multe situații terminalele fixe WiMAX vor oferi servicii L2 transparent VLAN, comutate la nivelul interfeței de trafic a BS, terminalele fixe WiMAX vor avea posibilitatea de a dezactiva modul de lucru — MS initiated handover.
Service flow scheduling and QoS	— Următoarele prioritizări ale traficului vor fi suportate de terminalele fixe WiMAX: BE, nrtPS, rtPS, ErtPS, UGS. — Toți parametrii obligatorii specificați de standardul IEEE 802.16e-2005 pentru tipurile de prioritizări de trafic de mai sus trebuie să fie implementate în terminalele fixe WiMAX. — Numărul minim service flows: 10 service flows (5 în uplink și 5 în downlink), cu diferiți parametri QoS. — Terminalele fixe WiMAX vor suporta minimum 4 VLAN pentru fiecare pereche de service flows (uplink/downlink). — Terminalele fixe WiMAX trebuie să suporte următoarele clasificări de pachete în UL: • 802.1Q • DSCP/IP TOS field • IP Protocol/Next Header field • IP masked Source Address • IP Destination Address • Protocol source port range • Protocol destination port range
Autentificarea și criptarea	— Nu va fi asignat terminalului fix WiMAX niciun serviciu de acces înainte de autentificare în serverul AAA. — Terminalele fixe WiMAX vor suporta următoarele metode de criptare și autentificare: • PKMv2 CMAC, security association • EAP-TLS, EAP-TTLS (MD5, MS-CHAPv2) authentication • X.509 certificate • Cryptographic Suites • CCM-Mode 128-bit AES, CCM Mode, AES Key Wrap with 128-bit key.
Managementul local	— Terminalele fixe WiMAX vor avea obligatoriu posibilitatea de administrare locală cu acces prin username și parolă. — Aplicația de administrare locală poate fi o aplicație proprietară (în acest caz va fi livrată fără restricții de licență) sau o aplicație de uz general (ssh, telnet, interfață web etc.). — Aplicația de administrare locală va avea un minim de posibilități de configurare astfel încât să asigure conectivitatea terminalului fix WiMAX la rețeaua de acces WiMAX și să fie luat în management de către NOC: • frecvențe de lucru • username/parolă pentru autentificare și metode de autentificare • parametri de networking și management • firmware upgrade/downgrade.
Managementul de la distanță	— Managementul de la distanță va fi implementat astfel: • adițional față de service flows provizionate pentru traficul utilizatorilor, vor fi provizionate două service flows (uplink/downlink) dedicate, având asignat același VLAN ID ca cel pentru managementul BS; • în configurația ETH-CS, pentru serviciile L2 fixe, adresa IP de management pentru WAN va fi configurabilă de către utilizator (nu asignată prin DHCP). — Terminalul fix WiMAX va implementa obligatoriu un agent TR-069 (în concordanță cu specificațiile CWMP — CPE WAN Management Protocol), oferind NOC-ului posibilități de management și supervizare. — Opțional pot fi oferite și alte posibilități de management (agent SNMP).

Soluția constructivă	Split type: IDU (indoor unit) și ODU (outdoor unit) cu antenă directivă integrată, conexiune IDU-ODU cu cablu ecranat Ethernet (POE)
Unitatea Indoor (IDU)	
Soluția constructivă	— Două porturi Ethernet (unul pentru conectarea la rețeaua utilizatorului — LAN, celălalt pentru conexiunea PoE cu ODU, un conector pentru alimentarea cu energie electrică (220 Vac) — Puterea maximă consumată de terminalul fix WiMAX < 15W — Cablul de alimentare va respecta specificațiile standardelor românești (împământarea este obligatorie)
Specificații de mediu	Conform standardului ETSI EN 300 019 class 3.2. vor fi specificați următorii parametri: • temperatura de funcționare • temperatura de stocare • umiditatea relativă maxim permisă
Interfețe de trafic	Minimum o interfață 10/100 Base T, conector RJ 45 utilizat pentru: — management local — obligatoriu restricționat cu username și parolă — traficul de date al utilizatorilor — conectat la rețeaua LAN — configurații posibile ale interfeței Ethernet a: • Mod Acces: în situațiile în care un singur serviciu de acces va fi oferit utilizatorului (bridge mode sau NAT mode). Când terminalul fix WiMAX este configurat în modul bridge cu un singur utilizator, tagarea VLAN a traficului se va face la nivelul BS. • Mod Trunk (IEEE 802.1q): în situațiile când sunt oferite utilizatorilor multiple servicii de acces (L2 VLAN transparent services). În acest caz se va instala la utilizator un switch cu management pentru gestionarea VLAN-urilor.
Unitatea outdoor (ODU) cu antenă directivă integrată	
Soluția constructivă	— Antena terminalului fix WiMAX va fi fizic integrată cu ODU. — ODU cu antena integrată va fi livrat cu toate accesoriile necesare pentru asamblare pe suportul de tip pipă, incluzând kitul pentru reglarea înclinării (tilt). Vor fi specificate grosimea minimă și maximă a suportului de antenă. — ODU va avea un conector integrat pentru conexiunea cu IDU (POE). — Întreaga construcție a ODU-lui, incluzând conectorii și accesoriile, vor fi impermeabilizate. — ODU trebuie sa aibă conector pentru împământare.
Specificații de mediu	— Conform ETSI EN 300 019 class 4.1E — ODU+ ansamblul antenă trebuie să respecte următorii parametri de mediu: • operare stabilă în condiții meteo: viteza maximă a vântului, încărcarea radială maximă cu gheață (densitatea 7 kN/m^3) • condiții meteo de supraviețuire: viteza maximă a vântului, încărcarea radială maximă cu gheață (densitatea 7 kN/m^3) • gama temperaturilor de lucru • gama temperaturilor de stocare • umiditatea relativă permisă • cotare IP/clasificare IEC 60529
Parametrii emițătorului	— Puterea de emisie: minimum 25 dBm — Masca emisiilor pentru ODU va fi atașată și suprapusă peste masca impusă de standardul ETSI EN 302 326-2 pentru clasa echipamentelor ofertate. — Nivelul de emisii parazite va fi specificat ținând cont de prevederile standardului ETSI EN 302 326-2.
Parametrii receptorului	— Sensibilitatea receptorului — sensibilitatea ODU-lui va fi indicată pentru toate tipurile de modulație și codificări, pentru toate lărgimile de canal pe care echipamentul ofertat le suportă. — Rezistența la interferențele C/I va fi specificată: Co-channel, Adiacent channel adiacent (+1 și +2) pentru toate tipurile de modulație, codare și pentru toate lărgimile de bandă pe care echipamentul ofertat le permite. — Zgomotul generat și pragul de zgomot vor fi specificate pentru ODU-ul ofertat, pentru fiecare lărgime de canal permisă. — Rata maximă de transfer în mod single user și rata de transfer care poate fi atinsă UL/DL pe un sector vor fi specificate pentru toate tipurile de modulație, codare și pentru toate lărgimile de bandă pe care echipamentul ofertat le permite.
Banda de frecvențe și parametrii canalului	Banda de frecvențe • Rețeaua WiMAX operează în 3 canale în sub-banda 3685-3700 MHz , metoda de duplexare fiind TDD

	— Lărgimile de bandă pentru canal impuse: 5, 7, 10 MHz — Metoda Duplex cerută: TDD — Acordul de frecvență: minimum 200 MHz (3600-3800 MHz)
Implementarea antenei	Două antene Rx/1 antenă Tx — cu scopul să permită MIMO B pe downlink Câștigul antenei: minimum 15 dBi Diagramele de radiație ale antenei în plan orizontal și vertical vor fi furnizate în fișier de tip text sau de tip excel.
	Pentru antena ofertată vor fi specificați cel puțin următorii parametri (datasheet): • fabricant • banda de frecvențe • polarizare • Half Power Beam Width (HPBW) — câștigul antenei în plan orizontal • Half Power Beam Width (HPBW) — câștigul antenei în plan vertical • separarea cros-polarizare (dB) • raportul față/spate • VSWR • dimensiunile • greutatea • intervalul de ajustare mecanică pentru azimut • intervalul de ajustare mecanică pentru elevație
Materiale de instalare	Următoarele materiale de instalare vor fi asigurate pentru fiecare terminal fix WiMAX: • cablu Ethernet autoportant Cat5e pentru exterior, lungime — 75 metri • conectori ecranati RJ-45 — 2 bucăți • Patch Ethernet Cat5e conectorizat cu RJ-45 minimum 3 metri — o bucată; • cablu împământare VLPY 16 mm^2 (înveliș exterior verde/galben) — 20 metri NOTĂ: Cablul Ethernet de exterior și cablul de împământare vor fi livrate bulk, pe tamburi, așa cum sunt împachetate de fabricant.
Cablu Ethernet autoportant Cat5e pentru exterior, instalare aeriană	
Aplicație	Instalarea exterioară în medii aspre, temperatură scăzută cu aplicabilitate în interior/exterior. Certificare pentru folosire în exterior
Construcția generală	— Corespunde cerințelor Cat 5e per ANSI/TIA/EIA-568-B.2 and IEC 61156-5; certificate care să ateste performanțele cablului Cat. 5e vor fi atașate ofertei tehnice. — Cablul este compus din 4 perechi de fire răsucite 24 AWG (0.52 mm) din cupru solid. — Ecranarea minimă: F/UTP (UTP cu folie) 24 AWG cu șufă; F/UTP ecranat este acceptat. — Compatibil cu conectori RJ-45 care să permită conectarea directă la echipamente fără patch-cord-uri. — Pentru autoportanță, cablul trebuie să includă în construcția sa șufă oțelită galvanizată sau protejată împotriva coroziunii. Șufa va fi dimensionată astfel încât să suporte greutatea sa și a cablului întins pe o distanță de minimum 50 metri între 2 suporți. — Pentru o mai bună înțelegere a cerințelor pe care cablul trebuie să le îndeplinească este prezentată figura următoare:  — Materialul din care este confecționat învelișul exterior al cablului și al șufei trebuie să fie rezistent la radiația UV și ignifug. Culoarea învelișului exterior trebuie să fie neagră (pentru protecție UV). Să respecte directiva RoHS 2002/95/EC.
Temperatura de funcționare	— Temperatura minimă de funcționare : –40°C — Temperatura maximă de funcționare: +70°C
Testarea terminalului fix WIMAX	Având în vedere că rețeaua WiMAX este pe deplin operațională, terminalul fix WiMAX va trebui să se integreze și să opereze în același fel în care rețeaua operează.

	În acest scop terminalul fix WiMAX va fi testat pentru a se determina dacă poate fi integrat în arhitectura rețelei operaționale existente.
Mențiuni și condiții pentru testare	Resurse puse la dispoziție de către ofertanți: — Terminale pentru testare (TPT): • Două terminale fixe WiMAX, incluzând toate accesoriile pentru instalare la locația clientului, excluzând suportul de antenă • Un terminal fix WiMAX customizat pentru teste de conformitate radio cu un conector N sau TNC pentru antena externă — Echipamentul terminal fix WiMAX trebuie să fie, în configurația specificată în oferta tehnică, corespunzător cerințelor tehnice prezentate aici. — Toate echipamentele/modulele/materialele de instalare vor fi asigurate de către ofertanți pentru instalarea și testarea în condiții reale de operare (outdoor), în locațiile de radiocomunicații indicate și puse la dispoziție de STS. — Ofertanții trebuie să asigure la sediul STS și în locațiile de radiocomunicații indicate și puse la dispozitie de către STS tot necesarul de personal tehnic calificat, capabil să instaleze și să configureze echipamentele de test, să ducă la bun sfârșit testele, în prezența și cu suportul tehnic al personalului STS . — Echipamentele puse la dispoziție de către ofertanți vor fi returnate către aceștia în cel mult 10 zile lucrătoare de la terminarea evaluării. Resurse puse la dispoziție de STS: — STS va pune la dispoziție și va asigura funcționalitatea tuturor echipamentelor de rețea (upstream incluzând stația de bază WiMAX) și a tuturor echipamentelor „clientului” (downstream terminalul fix WiMAX). Analizoarele de spectru necesare testelor de conformitate radio și pentru monitorizarea spectrului pe parcursul perioadei de testare vor fi puse la dispoziție de către STS. — STS va pune la dispoziție locațiile de test (incluzând locațiile pentru instalare și testare a terminalelor fixe WiMAX). — STS va asigura personal tehnic calificat pentru a efectua testele și pentru a asigura suport ofertanților în vederea instalării și configurării echipamentelor. Programul și locațiile testelor: — Alte echipamente și materiale care vor fi necesare testelor pot fi furnizate de către ofertanți la începutul perioadei de test alocate pentru fiecare ofertant (atunci când echipamentele fiecărui ofertant sunt testate). — Testele vor fi efectuate începând cu prima zi a perioadei de evaluare a ofertelor, în ordinea în care ofertanții vor furniza la sediul STS terminalele pentru testare care să îndeplinească condițiile de testare. Testele se vor efectua pe întreaga perioadă de timp alocată evaluării ofertelor. — O perioadă de maximum două zile va fi rezervată fiecărui ofertant, în care terminalele fixe WiMAX ale acestuia vor fi testate. Această perioadă nu poate fi mai mare. — Testele se vor efectua în aceleași condiții și în aceleași locații pentru fiecare ofertant. Locația de instalare a terminalelor fixe WiMAX va fi situată la 15-20 km distanță de stația de bază WiMAX, în condiții de vizibilitate directă. — Spectrul radio din sau în vecinătatea locației de test va fi permanent monitorizat de STS , pentru a detecta orice anomalie sau radiație neesențială care ar putea afecta rezultatele testelor. — Un plan detaliat pentru testarea echipamentelor va fi pus la dispoziție de către STS fiecărui ofertant în timpul sesiunii de deschidere a ofertelor. Excepții de la planul de teste: Dacă terminalul fix WiMAX al ofertantului a trecut cu success IOT (testele de interoperabilitate) cu stația de bază MacroMAXe, operând în banda de 3600-3800 MHz, nu va face subiectul testelor de echipamente. Interoperabilitatea trebuie să fie certificată de Airspan Inc., cu mențiunea expresă că terminalele fixe WiMAX pot opera în rețeaua WiMAX furnizată/ integrată de Airspan. Certificarea IOT trebuie de asemenea să existe. NOTĂ: — Un reprezentant împuternicit al ofertantului va semna documentul de rezultate ale testelor pentru echipamentul propriu, împreună cu reprezentanții tehnici ai STS. Șablonul acestui document va fi inclus în planul de test detaliat care va fi emis de cumpărător. — Nefinalizarea cu succes pentru orice test punctat cu PASS/FAIL sau eșecul în completarea testelor în perioada alocată va conduce la descalificarea ofertei respective. Descalificarea înseamnă ca oferta va fi considerată neconformă, din motive tehnice, cu toate consecințele specificate de lege. — Orice costuri sau cheltuieli pe care ofertanții le-ar putea avea, legate în orice fel de teste, nu vor avea efecte asupra cumpărătorului.

Descrierea generală a planului de testare	
Teste de conformitate radio (PASS/FAIL)	NOTĂ: Ofertanții vor asigura o aplicație software dedicată care să permită terminalului fix WiMAX să transmită cu putere maximă sau vor asigura un dispozitiv care să permită terminalului fix WiMAX să transmită cu putere maximă (dispozitiv similar cu cel specificat în clauza 5.4 a ETSI EN 302 623). Cablurile necesare și atenuatorii vor fi de asemenea furnizați. Testele de conformitate radio se vor desfășura pe terminalul fix WiMAX dedicat cu conector de tip N sau TNC pentru antena externă. Următoarele caracteristici vor fi testate: • puterea maximă de emisie minimum 25 dBm • banda de frecvență 3600—3800 MHz • lărgimea canalului 5, 7, 10 MHz • masca spectrală a emisiilor și emisiile neesențiale pentru canale de 5, 7, 10 MHz la putere maximă de emisie • funcția de control și monitorizare: terminalul fix WiMAX nu va emite în absența unei rețele valide.
Configurarea inițială a terminalului fix WiMAX, intrarea în rețea și autentificarea (PASS/FAIL)	— Configurarea inițială a terminalului fix WiMAX: • frecvențele de scanare (3 canale în banda 3685-3700 MHz) • lărgimea canalului: 5 MHz • credențialele de autentificare (utilizator și parolă) • metode de autentificare (EAP/TTLS cu MS-CHAPv2) • moduri de operare: Mod bridge și Mod NAT • setări IP: static IP în modul bridge, client DHCP în modul NAT • setări TR-69 • setarea de dezactivare a Handover-ului din terminalul fix WiMAX va fi selectată și testată • autentificarea și intrarea în rețea cu succes urmată de identificarea în EMS Netspan
Provizionarea serviciilor în modul bridge și modul NAT (PASS/FAIL)	— Modul Bridge • O pereche de service flow-uri vor fi provizionate pentru management (pe un VLAN ID distinct). • 4 perechi de service flow-uri vor fi provizionate pentru trafic (BE, NRTPS, RTPS, eRTPS); suma vitezelor de transfer a datelor UL/DL nu va depăși capacitatea maximă a unui singur utilizator UL/DL. • Capacitatea de transfer a datelor a unui singur utilizator UL/DL. • 4 VLAN ID-uri vor fi asignate fiecărei perechi de service flow-uri. • Terminalul fix WiMAX ar trebui să poată fi contactat din rețeaua de management (cu ping, telnet/ssh, interfața web) și din serverul de TR69. • Serviciile provizionate vor fi testate aleator cu IGMP între host-urile downstream terminalul fix WiMAX și upstream stația de bază. — Modul NAT • O pereche de service flow-uri va fi provizionată din serverul AAA. • Serviciile provizionate vor fi testate IGMP între host-urile downstream terminalul fix WiMAX și upstream ASN-GW. • Terminalele fixe WiMAX trebuie să poată fi contactate din ASN-GW cu ping, telnet/ssh, web.
Rata de transfer a unui singur utilizator aflat pe un sector dedicat al stației de bază (PASS/FAIL)	— Terminalul fix WIMAX va fi setat în modul bridge. — O pereche de service flow-uri vor fi provizionate pentru management (pe un VLAN ID distinct). — O pereche de service flow-uri va fi provizionată cu BE la o rată maximă realizabilă pe sector pentru un singur utilizator. — Rata de transfer va fi testată cu iperf în modul UDP și ar trebui să depășească 10 Mbps DL și 1.5 Mbps UL, pentru un canal cu o lărgime de 5 MHz.
Implementarea mecanismelor de QoS (PASS/FAIL)	—Terminalul fix WiMAX va fi setat în modul bridge. — O pereche de service flow-uri vor fi provizionate pentru management (pe un VLAN ID distinct). — 3 perechi de service flow-uri vor fi provizionate după cum urmează: • BE pentru date (rata maximă de transfer UL/DL) • RTPS pentru video (512 kbps UL/DL) • ERTPS pentru voice (512 kbps UL/DL). — Pe fiecare pereche de service flow-uri va fi provizionat câte un VLAN distinct. — Traficul va fi generat cu iperf în modul UDP pentru a umple banda pentru fiecare service flow. — Congestiile de trafic ar trebui să fie observate pe service flow-urile cu prioritate mai mică. — Testele vor rula de asemenea și cu echipamente dedicate pentru voce și VoIP.

6. Specificații stație de lucru completă
• Procesor: Intel Pentium 4 sau echivalent
• Memorie fizică instalată: 1GB
• Port USB 2.0 minimum 2
• Port NIC 10/100 MHz
• Mouse, tastatură, monitor
• Rezoluția video a ecranului minimum 1024x768
• Sistemul de operare: minimum Microsoft Windows XP, actualizat zilnic
• Antivirus cu posibilitate de update off-line, actualizat zilnic
• Browser Internet Explorer 6.0 sau echivalent
• Interfață Ethernet 10/100/1000 Mbps
7. Specificații certificate digitale

Accesul la nivelul de aplicație este realizat numai în urma certificării utilizatorului cu certificate digitale în format X509v3 emise de către o autoritate de certificare implementată de către STS în acest scop. Certificatele sunt emise, respectiv revocate ca urmare a solicitării IPJ/DGPMB, care va notifica STS ori de câte ori apar modificări în lista utilizatorilor cu drept de acces.

Certificatele vor fi instalate pe echipamente de tip token-usb, care vor fi achiziționate de către beneficiar. Este necesar ca dispozitivele criptografice să respecte următoarele caracteristici tehnice:

a) cerințe:

— sistem compact care să prevadă doi factori de autentificare în vederea furnizării securității pentru utilizatorul care îl folosește la autentificarea în rețea, criptarea de mesaje electronice, precum și semnarea digitală a documentelor;

— dispozitivul trebuie să poată genera chei private, precum și să stocheze chei private și certificate digitale. Protecția cheilor de pe dispozitiv se va face cu ajutorul unui cod pin;

b) caracteristici:

Sisteme de operare suportate:

Windows Server 2003/Windows Server 2008, Windows 2000/XP/2003/Vista

Linux, Mac OS X.

Standarde și APIs cryptografic
• PKCS #11 v2.01
• Microsoft CryptoAPI (CAPI) 2.0
• Microsoft PC/SC
• X.509 v3 certificate storage
• SSL v3
• IPsec/IKE

Certificări de securitate
• FIPS 140-2 L2&3 (full device)
• Common Criteria EAL4/EAL5 (smart card chip și OS)

Memorie
• 72 K

Conectivitate
• USB Type A (Universal Serial Bus)

Dimensiuni
• 52 x 16 x 8 mm (2.05 x 0.63 x 0.31 inches)

Suport pentru specificații ISO
• Suport pentru specificații ISO 7816-1 până la 4

Funcții criptografice
• generarea perechilor de chei asimetrice (RSA 1024-bit/2048-bit)
• generare chei simetrice (DES, 3DES)
• semnare digitală (RSA 1024-biti, RSA 2048-biti)
• algoritmi hash (SHA-1)
• Stocarea și generarea cheilor criptografice pe dispozitiv
• Realizarea semnăturii digitale pe dispozitiv.

Timpi de generare
• Generarea cheii: în mai puțin de 90 de secunde
• Semnare digitală: în mai puțin de o secundă

Caracteristici fizice

a) Hardware
• 8-bit processor
• 32K memory

b) Conectivitate
• USB 1.1/2.0 compliant
• 1.5 Mbits per second transfer

c) Regulatory Standards

FCC Part 15 - Class B CE

Limite de temperatură de funcționare
• 0°C to 70°C (32°F to 158°F)

Limite de temperatură de stocare
• –40°C to 85°C (–40°F to 185°F)

Certificare rezistență la umiditate
• IP X8 — IEC 529

Carcasă
• Carcasă din plastic, tamper evident

Retenția datelor în memorie
• Cel puțin 10 ani

III. **Informațiile utilizatorilor care vor fi comunicate la Inspectoratul poliției județene/Direcția Generală de Poliție a Municipiului București**

Nume = se completează cu prima literă mare urmată de celelalte litere mici

CNP = CNP-ul utilizatorului

Prenume = se completează cu prima literă mare urmată de celelalte litere mici

Inițiala tatălui

Județ/Sector = județul/sectorul din care face parte posesorul certificatului

Localitate = localitatea din care face parte posesorul certificatului

E-mail = adresa de e-mail a utilizatorului nu trebuie să cuprindă spații libere; se acceptă adrese de e-mail generice.

Organizația = poliția locală din care face parte utilizatorul.

N O T Ă:

Informațiile menționate mai sus se redau cu diacritice!

Georgeta N. Stoica

Motivul: Format electronic AUTENTIC, conform Legii nr. 202/1998, republicata.
Locatia:Bucuresti

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București
și IBAN: RO12TREZ7005069XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București
(alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro
Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,
bloc P33, parter, sectorul 5, tel. 021.401.00.70, fax 021.401.00.71 și 021.401.00.72
Tiparul: „Monitorul Oficial” R.A.

MONITORUL OFICIAL

5 948368 524521

Monitorul Oficial al României, Partea I, nr. 491/11.VII.2011 conține 16 pagini. Prețul: 3,20 lei **ISSN** 1453—4495