

...../...../.....

CAIET DE SARCINI

Servicii de Help-desk, mentenanță și suport tehnic aferente componentei aplicative a sistemului informatic Cardul Electronic de Asigurări de Sănătate

LISTA DE ACRONIME

Acronim	Explicatie
CNAS	Casa Nationala de Asigurari de Sanatate
CJAS	Casa Judeteana de Asigurari de Sanatate sau Casa de Asigurari de Sanatate a Municipiului Bucuresti
MS	Ministerul Sanatatii
FNUASS	Fondul national unic de asigurari de sanatate
SIUI	Sistemul informatic unic integrat al CNAS
SIPE	Sistemul informatic pentru prescriptia electronica
CEAS	Sistemul informatic pentru cardul electronic de asigurari de sanatate
TIC	Tehnologia informatiei si a comunicatiei
WSDL	Web Service Definition Language
XML	Extensible Markup Language
SSL	Secure Sockets Layer
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
TCP	Transmission Control Protocol
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
JSP	JavaServer Page
API	Application Programming Interface
SLA	Service Level Agreement

1. INTRODUCERE

Casa Nationala de Asigurari de Sanatate (CNAS) este institutie publica, autonoma, de interes national, cu personalitate juridica, al carei principal obiect de activitate il reprezinta asigurarea functionarii unitare si coordonate a sistemului asigurarilor sociale de sanatate din Romania.

CNAS s-a înființat în baza Legii Asigurărilor Sociale de Sănătate - Legea nr. 145/1997. Aceasta a urmărit modelul de asigurări tip Bismark, cu asigurare de sănătate obligatorie, bazat pe principiul solidarității și funcționând în cadrul unui sistem descentralizat. Legea a intrat în vigoare, cu toate prevederile, începând cu 1 ianuarie 1999 dar a existat o perioadă de tranziție în anul 1998 în care Direcțiile Sanitare Județene și Ministerul Sănătății au administrat fondurile de asigurare. În consecință, de la 1 ianuarie 1999, conform legii, casele de asigurări și Casa Națională de Asigurări de Sănătate au funcționat ca instituții publice autonome, conduse prin consiliile de administrație formate din reprezentanți ai asiguraților, sindicatelor, Guvernului României, Presedinției și patronatului.

CNAS funcționează pe baza statutului propriu, avizat de consiliul de administrație și aprobat prin HG nr. 972/2006 pentru aprobarea Statutului Casei Naționale de Asigurări de Sănătate, cu modificările și completările ulterioare, și are următoarele obligații principale:

- ✓ să asigure logistica functionarii unitare si coordonate a sistemului asigurarilor sociale de sanatate;
- ✓ să urmărească colectarea și folosirea cu eficiență a fondului;
- ✓ să folosească mijloace adecvate de mediatizare pentru reprezentarea, informarea și susținerea intereselor asiguraților pe care îi reprezintă;
- ✓ să acopere nevoile de servicii de sanatate ale persoanelor, în limita fondurilor disponibile.

CNAS are în subordine casele județene de asigurari de sanatate, Casa de Asigurari de Sanatate a Municipiului Bucuresti, Casa Asigurarilor de Sanatate a Apararii, Ordinii Publice, Sigurantei Nationale si Autoritatii Judecatoresti.

1.1. CADRUL LEGAL

Cadrul legal al desfasurarii serviciilor solicitate este constituit din:

- Acte normative specifice:
 - Legea nr. 95/2006 privind reforma in domeniul sanatatii, cu modificarile si completarile ulterioare
 - Legea nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, modificata si completata
 - Hotararea Guvernului Romaniei Nr. 900/2012 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la cardul național de asigurări sociale de sănătate din titlul IX "Cardul european și cardul național de asigurări sociale de sănătate" din Legea nr. 95/2006 privind reforma în domeniul sănătății
 - Ordinul Presedintelui CNAS Nr. 98/2015 pentru aprobarea procedurii de eliberare, a modalității de suportare a cheltuielilor aferente producerii și distribuției cardului duplicat către asigurat, precum și a modalității de acordare a serviciilor medicale, medicamentelor și dispozitivelor medicale până la eliberarea sau în cazul refuzului cardului național de asigurări sociale de sănătate
 - Contractul Cadru si Normele sale de aplicare
 - Alte Ordine sau acte normative specifice
 - Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal

Acte normative incidente procedurii de achizitie:

- OUG nr. 34/2006 privind atribuirea contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii, cu completarile si modificarile ulterioare
- HG nr. 925/2006 pentru aprobarea normelor de aplicare a prevederilor referitoare la atribuirea contractelor de achizitie publica din OUG nr. 34/2006 privind atribuirea contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii, cu completarile si modificarile ulterioare
- HG nr. 1660/2006 pentru aprobarea Normelor de aplicare a prevederilor referitoare la atribuirea contractelor de achizitie publica prin mijloace electronice din OUG nr. 34/2006 privind atribuirea

contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii, cu completarile si modificarile ulterioare

- OUG nr. 30/2006 privind functia de verificare a aspectelor procedurale aferente procesului de atribuire a contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii, cu modificarile si completarile ulterioare
- HG nr. 942/2006 pentru aprobarea Normelor de aplicare a OUG nr. 30/2006 privind functia de verificare a aspectelor procedurale aferente procesului de atribuire a contractelor de achizitie publica
- Ordin nr. 175/2007 privind aprobarea Manualului operational pentru activitatea de observare si verificare a atribuirii contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii - modelul si continutul formularelor si documentelor utilizate
- HG nr. 782/2006 pentru aprobarea Regulamentului de organizare si functionare al Consiliului National de Solutionare a Contestatiilor, cu modificarile si completarile ulterioare
- Ordin nr. 113/2008 pentru aprobarea Regulamentului privind supravegherea modului de atribuire a contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii. Supravegherea va viza inclusiv procedurile de achizitie publica impuse operatorilor economici de catre autoritatile de management pentru derularea proiectelor finantate din fondurile structurale acordate Romaniei de catre Uniunea Europeana.

Alte acte normative incidente procesului de achizitie:

- Legea contenciosului administrativ nr. 554/2004, cu modificarile si completarile ulterioare
- OG nr. 2/2001 privind regimul juridic al contravențiilor, cu modificarile si completarile ulterioare

2. OBIECTUL PROCEDURII

SERVICII CARE FAC OBIECTUL PROCEDURII:

2.1 SERVICII DE HELP-DESK, MENTENANȚĂ ȘI SUPORT TEHNIC AFERENTE COMPONENTEI APLICATIVE A SISTEMULUI INFORMATIC CARDUL ELECTRONIC DE ASIGURĂRI DE SĂNĂTATE, INCLUZAND:

- I.**
 1. Servicii de administrare, suport si mentenanta pentru componenta aplicativa specifica;
 2. Servicii de administrare suport si mentenanta pentru configurariile specifice modulului Autoritate de Certificare;
 3. Servicii de administrare suport si mentenanta pentru configurariile specifice modulului Zona de Transfer;
 4. Servicii de gestionare a tranzacțiilor cu cardul prin Unitatea de Managemnet;
 5. Actualizari pentru toate componentele software ale solutiei aplicative a CEAS
 6. Actualizarea documentatiei de instalare si configurare a sistemului;
 7. Restaurarea/reinstalarea si configurarea aplicatiilor;
- II.** Dezvoltari ale sistemului CEAS, ca urmare a unor modificari legislative altele decat cele de la Cap 8.2, care au ca impact necesitatea extinderii, sau la cererea CNAS, in limita unui nr de maxim 1.000 zile-om/an. Aceste dezvoltari vor intra in categoria „extindere a sistemului”, intelegandu-se prin aceasta adaugarea de noi functionalitati, suplimentar fata de cele actuale, cuprinse atat in documentatia de atribuire initiala de achizitie a sistemului cat si fata de cele reglementate si documentate pana la data prezentei achizitiei. Nu se considera extindere a functionalitatilor dezvoltarile ca rezultat al modificarilor legislative pentru imbunatatirea fluxurilor actuale.
- III.** Serviciile de Help-desk vor acoperi de la preluarea incidentului (solicitarii) si pana la confirmarea de catre solicitant a solutionarii acestuia.

Solicitarile de Help-desk vor fi solutionate pe baza documentatiei aplicatiilor, a procedurilor curente de lucru sau istoricului de cazuri similare. Solicitarile care exced acest nivel vor fi

solutionate prin interventia personalului din echipa de mentenanta software, a prestatorului care asigura serviciile de administrare, suport tehnic si mentenanta pentru componenta hardware, interventia altor furnizori, interventia personalului de specialitate al CNAS, etc.

3. CONDITII GENERALE

1. Prestatorul trebuie sa asigure functionarea in integralitate, la un nivel standard de performanta, astfel incat sa fie gestionate toate fluxurile de tranzactionare cu cardurile inrolate in sistem, prin interogarea si comunicarea bidirectionala cu SIUI – extensia eCard, unde sunt definite atat cardurile cat si asocierile intre carduri si persoanele asigurate; -
2. Oferta trebuie sa contina suficiente informatii si detalii, astfel incat, comisia de evaluare a ofertelor sa poata evalua capacitatea de furnizare a serviciilor pe baza cerintelor din prezentul Caiet de Sarcini.
3. Cu exceptia serviciilor prevazute la Cap 2.1 punctul II, serviciile care fac obiectul procedurii nu vor fi limitate, (ex. numar maxim de zile/om sau pe tipuri de solicitari).
4. Serviciile prevazute la Cap 2.1 pct. II vor fi prestate la solicitarea scrisa a Beneficiarului. Acestea vor fi facturate si achitate in functie de nr. efectiv de zile-om efectuate. Oferta financiara va cuprinde contravaloarea celor 1.000 zile-om/an cu evidentierea costului unitar (zi-om de prestare).
5. Oferta depusa va avea in vedere acoperirea tuturor cerintelor exprimate in Caietul de Sarcini. Acestea sunt minimale si obligatorii.
6. Autoritatea Contractanta isi rezerva dreptul de a suplimenta sau diminua, in limitele permise de reglementarile legale in vigoare, cantitatea de servicii solicitate prin prezenta documentatie de atribuire.
7. Autoritatea Contractanta isi rezerva dreptul de a solicita prelungirea cu maxim 4 luni a Acordului Cadru, in conditiile reglementarilor legale in vigoare.
8. CNAS va pune la dispozitia prestatorului codurile sursa ale aplicatiilor si intreaga documentatie tehnica aferenta sistemelor.

Procedura aplicabila: Licitatie deschisa – Acord cadru pentru o perioada de 36 de luni.

Criteriu de atribuire: Pretul cel mai scazut al ofertei.

4. COSTUL OFERTEI

Toate cheltuielile pentru pregătirea și depunerea ofertelor sunt suportate de către Ofertanți. CNAS nu poate fi făcută responsabilă pentru aceste costuri, indiferent de rezultatele procesului de selecție a ofertelor.

5. LIMBA FOLOSITA PENTRU PREZENTAREA OFERTEI

Toată corespondența va fi redactată în limba română, la fel ca și întocmirea ofertei de către Ofertant, precum și toate documentele care au legătură cu oferta.

6. PREZENTAREA FUNCTIONALA A SISTEMULUI INFORMATIC CEAS

Sistemul Informatic pentru Cardul Electronic de Asigurari de Sanatate (CEAS) este un sistem informatic centralizat compus dintr-o serie de module, care functioneaza in mod integrat si care sunt descrise in continuare.

6.1. MODULUL eCARD

Acest modul realizeaza gestiunea cardurilor pe intreg ciclul de viata al acestora. Este accesat de catre utilizatorii interni CNAS/CJAS pentru realizarea loturilor de carduri CEAS propuse pentru personalizare si transmiterea acestora catre Zona de Transfer in vederea personalizarii.

Modulu eCard asigura urmatoarele functionalitati:

- Preluarea datelor referitoare la productia si personalizarea cardurilor si transmiterea acestora in Zona de transfer,
- Determinarea din punct logic a eligibilitatii solicitantilor de a beneficia de acordarea serviciilor medicale,
- Verificarea validitatii certificatelor digitale, prin conectarea catre Unitatea de Management,
- Asigurarea evidentei individuale a cardurilor emise catre asigurati, precum si a istoricului modificarilor,
- Interactiunea in timp real cu Unitatea de Management in vederea gestionarii cu carduri cu chip catre sistemul SIUI,
- Asigura interogarea SIUI si extragerea fisierelor XML de import in cazul inrolarii initiale precum si in cazul inrolarii periodice,
- Asigura actualizarea statusurilor loturilor aferente, cu posibilitatea ulterioara de consultare, vizualizare, stergere fisiere generate,
- Managementul cardurilor, in toate starile acestuia

Pentru a facilita interfatarea aplicatiilor SIUI si de terta parte fara a afecta securitatea si integritatea sistemului, primitivele de acces la facilitatile cardului si cititorului sunt incapsulate intr-un Software Development Kit (SDK) eCard de interfatare cu cititorul/cardul de sanatate astfel incat se exclude eventuala folosire indirecta sau neautorizata.

6.2. UNITATEA DE MANAGEMENT

Este o componenta de procesare a tranzactiilor efectuate cu cardurile, gestionand toate interactiunile si toate starile prin care trece acesta de-a lungul perioadei sale de activitate. Inregistreaza date despre cardurile emise si starile lor, precum si despre tranzactiile efectuate cu cardurile la dispozitivele autorizate.

Unitatea de management asigura urmatoarele roluri principale:

- Autentificare, prin folosirea cheilor publice aferente cardurilor preluate de la Autoritatea de certificare,
- Suport pentru activarea de catre medici a cardurilor,
- Reinoirea cardurilor, atunci cand este necesar (distrugere, pierdere, blocare, etc),
- Managementul cardurilor in toate starile lui.

Unitatea de management comunica bidirectional cu SIUI pentru toate fluxurile ce presupun interactiunea cu carduri CEAS.

Cardurile emise in cadrul sistemului sunt urmarite de-a lungul utilizarii lor, de la emitere pana la dezactivare, starile prin care acestea trec fiind gestionate de UM. De asemenea, modificarile (trecherile dintr-o stare in alta) ce survin de-a lungul timpului sunt implementate sub forma de fluxuri de activitati ce pot fi invocate prin intermediul UM, sau automat, in cazul fluxurilor cu declansare temporala.

6.3. MODULUL AUTORITATE DE CERTIFICARE

Acest modul gestioneaza certificatele digitale ce sunt stocate pe cardurile CEAS, pe intreg ciclul de viata al acestora, permitand functionalitati de emitere, revocare si interogare a starii certificatului. Acest modul se gaseste in aceeasi locatie cu infrastructura ce realizeaza personalizarea cardurilor, fiind apelat de aceasta in procesul de personalizare.

Componenta utilizata pentru Autoritatea de certificare este certSAFE CA.

Pentru infrastructura cu chei publice care gestioneaza certificatele digitale stocate pe carduri este utilizata solutia certSAFE CA. Aceasta solutie include toate serviciile aferente gestionarii cheilor criptografice si a certificatelor digitale pe toata durata acestora de viata impreuna cu operarea unei infrastructuri de securitate bazata pe PKI:

- Autoritatea de Certificare Radacina (Root CA), care este off-line si care constituie punctul de incredere al infrastructurii de chei publice;

- Autoritatea de Certificare (CA - Certification Authority) - cu rolul de a emite si revoca certificatele digitale
- Autoritatea de Inregistrare (RA - Registration Authority) - cu rolul de a prelua cererile de emitere certificate si de a valida identitatea entitatilor finale
- Depozitul de Certificate (Repository) - asigura stocarea si distribuirea certificatelor digitale si a listelor de certificate revocate.
- Serviciul de validare online a starii certificatului prin protocolul OCSP (RFC 2560) Root CA, Autoritatea de certificare si Autoritatea de inregistrare sunt gazduite de catre DGP-CNUPPE. Serviciul de directoare (repository) si componenta de validare on-line a starii certificatelor prin OCSP sunt gazduite la Unitatea de management.

Infrastructura de chei publice este implementata pe doua niveluri: Root CA, offline, si SubCA, care emite certificatele digitale ale utilizatorilor.

certSAFE asigura un grad ridicat de securitate pentru operatiunile sistemului:

1. Emiterea certificatelor digitale care sunt stocate pe cardurile cetatenilor. Acestea sunt certificate digitale necalificate, fiind emise intr-o arhitectura PKI organizationala, gestionata in cadrul DGP-CNUPPE.
2. Schimbul de chei criptografice intre SIUI si Unitatea de management, asigura definirea si transmiterea intre cele doua entitati a Zone Master Key (ZMK). certSAFE CA este un produs folosind kit-ul de dezvoltare RSA BSAFE.

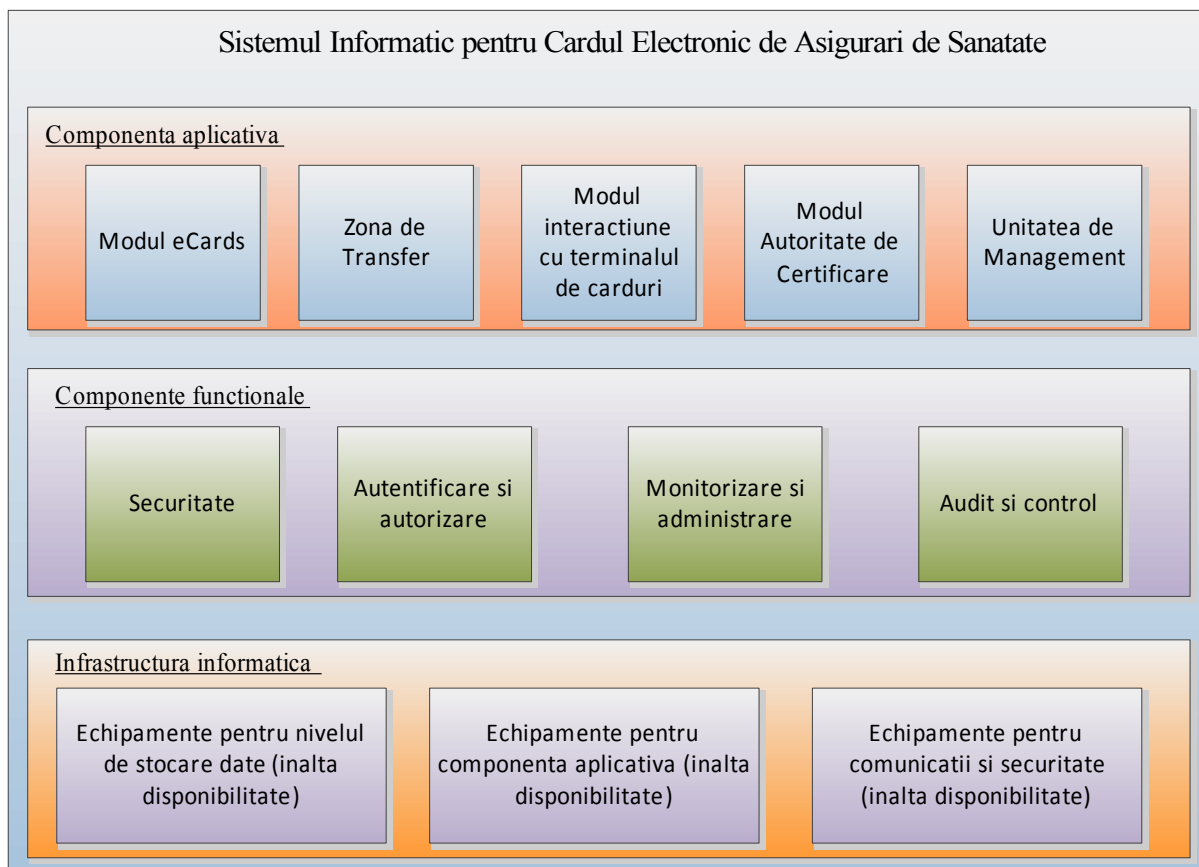
6.4. MODULUL ZONA DE TRANSFER

Acest modul realizeaza transferul loturilor de productie carduri catre infrastructura ce realizeaza personalizarea acestor carduri si transmiterea catre modulul eCard a starii de personalizare a acestor carduri.

Pentru transferul informatiei intre SIUI si DGP-CNUPE (zona de transfer) se utilizeaza o infrastructura tip SOA din cadrul sistemului (sunt configurate fluxuri utilizand modulele File Adaptor, Service Bus si BPEL)

Toate aceste module sunt inglobate intr-o aplicatie de tip compozita (composite application) ce este instalata pe clusterul SOA. Adaptorul de fisiere este configurat explicit ca si serviciu de tip singleton la nivelul platformei SOA cu capabilitati HA (migrarea serviciului de pe un nod pe altul). Solutia implementata este tranzactionala si permite modificarea parametrilor de functionare dinamic.

O privire de ansamblu asupra sistemului CEAS este redată în cadrul diagramei următoare:



7. PREZENTAREA TEHNOLOGICA A SISTEMULUI INFORMATIC CEAS

Din punct de vedere tehnologic, CEAS este un sistem informatic de tip multi-tier, cu urmatoarele elemente componente:

1. Nivelul de baza de date format din:

- Productie: un server HP SuperDome2, cu sistemul de operare HP-UX 11i v3 cluster ServiceGuard – Veritas CFS, ruland SGBD Oracle RAC 11g, ce utilizeaza pentru boot un echipament de stocare de tip HP MSA
- Dezvoltare: doua servere HP BL870c i2 cu sistemul de operare HP-UX 11i v3 cluster ServiceGuard – Veritas CFS, ruland SGBD Oracle RAC 11g
- Storage XP 24000 si 3PAR F400 ce stocheaza datele sistemului
- Switch-uri SAN HP

2. Nivelul de procesare format din:

- Productie: servere HP BL460c G7, cu sistemul de operare Redhat Enterprise Linux v5, server de aplicatie Java ce expune o aplicatie Web catre utilizatorii interni si servicii Web catre utilizatorii externi ai CEAS, gazduite intr-un HP Blade Enclosure c7000.
- Dezvoltare: server HP BL460c G7, cu sistemul de operare Redhat Enterprise Linux v5, server de aplicatie Java ce expune o aplicatie Web catre utilizatorii interni si servicii Web catre utilizatorii externi ai CEAS, gazduit intr-un Blade Enclosure c7000.

3. Nivelul de prezentare format dintr-o componenta software dezvoltata de contractantul initial:

- Pentru utilizatori interni (CNAS si CJAS): Aplicatie Web (Oracle Database 11g R2.04), bazata in principal pe urmatoarele tehnologii: Java, EJB, JSP, Servlets, Struts, Spring, Hibernate, Axis, JDBC, JasperReports, AndroMDA.
- Pentru utilizatori externi (furnizori de servicii medicale prescriptori de retete si furnizori de servicii farmaceutice): 16 aplicatii desktop individuale .NET cu baza de date locala SQL Server, pentru fiecare din tipurile de furnizori de servicii medicale si farmaceutice. Aplicatiile desktop realizate au un core comun si folosesc module reconfigurable.
- Informatii despre aplicatiile desktop se gasesc la urmatoarele adrese web:
 - o <http://www.cnas.ro/siui>

- http://siui.casan.ro/cnas/siui_3.7/versiuni
 - http://siui.casan.ro/cnas/siui_3.7/manuale
4. Nivelul de validare OCSP al certificatelor digitale emise de autoritatea de certificare din cadrul sistemului este reprezentat de servere HP DL380G7 cu sistem de operare Linux si echipamente Big-IP pentru echilibrarea incarcarii.
 5. Autoritatea de certificare si Zona de Transfer utilizeaza 8 servere HP DL380G7 cu sistem de operare Linux, un sistem de stocare HP P2000 G3, 4 switch-uri SAN HP, switch-uri Ethernet 1Gbps din seriile 6600 si 2600, un echipament HP S1400N IPS, firewall, un server de backup DL380 G7 si o biblioteca de benzi HP MSL2024.
 6. Solutia de monitorizare a infrastructurii IT consta dintr-o suita integrata de aplicatii, disponibile comercial ce ruleaza pe o infrastruktura de calcul formata din 4 servere BL460c G7 virtualizate cu tehnologie Vmware: HP WebInspect, HP Operations Manager, HP Quality Center+ Functional Testing, HP BAC+ TV+ uCMDB+ Site Scope, HP Service Manager
 7. Solutia de comunicatie interna se bazeaza pe folosirea a doua echipamente modulare HP 7500 Switch cu modulele firewall, IPS, load balancing, si a unor switch-uri Ethernet 1Gbps si 10Gbps din seriile HP 6120, 2600.
 8. Accesul in sistem prin intermediul HTTPS cu autentificare pe baza de certificat digital calificat precum si echilibrarea incărcării pe fermele de servere de aplicație ce deserveșc diversele servicii aplicative CEAS se realizează prin folosirea configurațiilor specifice de pe echipamente partajate CISCO ACE.
 9. Backup-ul pe banda si restaurarea bazei de date CEAS se realizează prin folosirea unei soluții de backup ce utilizează biblioteca de benzi partajata LTO-5 HP StorageWorks ESL712e precum si software specializat HP Data Protector.
 10. Pentru aplicatii sunt folosite .Net 4.0 si SQL Server 2008 R2, respectiv Java 2EE si Oracle Database 11g R2.04
 11. Tehnologiile folosite la realizarea modulelor sunt Java EE si .Net. iar pentru aplicatii sunt folosite tehnologiile .Net 4.0 si SQL Server 2008 R2, respectiv Java 2EE si Oracle Database 11g R2.04.

8. CERINTE GENERALE PRIVIND SERVICIILE

STANDARDE DE SERVICII - NIVELURILE DE SERVICII (SLA) A REZOLVARII INCIDENTELOR SEMNALATE:

Grad criticitate incident	Descriere	Timp maxim de raspuns	Timp maxim solutie provizorie/	Termen maxim de remediere
<i>Critic</i>	<p>Intreg sistemul este nefunctional.</p> <p>Problema impiedica desfasurarea activitatii, activitatea in cadrul sistemului este afectata si nu mai poate continua, pierderea functionalitatilor devenind critica.</p>	1 h	1 h	24 h
<i>Major</i>	<p>Impact asupra functionarii sistemului</p> <p>Problema impiedica desfasurarea in conditii normale a activitatii utilizatorilor.</p> <p>Nicio solutie alternativa nu este disponibila, dar activitatea utilizatorilor poate totusi continua, insa limitata la componentele neafectate.</p>	1 h	8 h	24 h
<i>Mediu</i>	<p>Problema afecteaza functionalitatile sistemului.</p> <p>Impactul reprezinta un inconvenient care necesita solutii alternative pentru refacerea functionalitatilor, exista cel putin o cale de a ocoli defectul.</p>	1 h	24 h	36 h
<i>Minor</i>	<p>Problema nu afecteaza functionalitatile sistemului.</p> <p>Rezultatul este o eroare minora, care nu impiedica desfasurarea in bune conditii a activitatii utilizatorilor.</p>	1 h	36 h	48 h

Depasirile timpilor de raspuns/solutie provizorie/remediere, respectiv penalizarile, sunt cuantificate in puncte de penalizare, acordate pe grade diferite de criticitate, conform tabelului urmator:

Grad criticitate	Punctaj penalizare
<i>Critic</i>	1h depasire=10 puncte penalizare
<i>Major</i>	1h depasire=8 puncte penalizare
<i>Mediu</i>	1h depasire=4 puncte penalizare
<i>Minor</i>	1h depasire=2 puncte penalizare

Se considera ***depasire*** orice depasire a timpilor de raspuns, pe fiecare componenta de timp (Timp de raspuns, Timp solutie provizorie, Termen de remediere)

Un punct de penalizare valoreaza 1% din factura lunara aferenta serviciilor ce fac obiectul contractului. Valoarea penalitatilor nu va putea depasi valoarea facturii.

Nefunctionarea sistemului pentru o perioada mai mare de 72 de ore, cauzata de nerespectarea SLA, conduce la executarea de catre Beneficiar a Scrisorii de garantie de buna executie a Contractului si da dreptul Beneficiarului la rezilierea Contractului/Acordului Cadru fara interventia instantei sau alte formalitati.

Definitii:

Timp de Răspuns: Timpul scurs de la contactul inițial dintre utilizatorii sistemului si HelpDesk si răspunsul primit de la echipa de suport tehnic. Aceasta acțiune se va desfășura prin Intermediul telefonului sau a mesageriei electronice si va fi auditata de catre Prestator. Prestatorul va asigura accesul Beneficiarului la aplicatia de auditare in vederea confirmarii nivelului serviciilor, realizarii de estimari cantitative etc.

Solutie provizorie: O modificare in cadrul procedurilor sau datelor care sa evite erorile fara folosirea defectuoasa a produselor.

Termen de Remediere: Durata de timp de la momentul finalizarii solutiei temporare pana la oferirea solutiei finale.

Pentru tratarea incidentelor care afecteaza functionalitatile sistemului serviciile vor fi asigurate 24/7.

9. CERINTE SPECIFICE PRIVIND SERVICIILE

Serviciile vor acoperi obligatoriu urmatoarele activitati:

- Activitatile vor fi derulate de personal specializat pe tehnologiile folosite;
- In cadrul serviciilor, se va asigura suport tehnic specializat in cadrul grupului de discutii al producatorilor de software specializati pe Cardul National. Operatorul economic desemnat castigator va asigura suport tehnic specializat in cadrul grupului de discutii al producatorilor de software specializati pe Cardul National ori de cate ori acestea se vor organiza prin decizia CNAS, cu scopul de a a oferi detalii despre modul în care se poate realiza compatibilizarea softurilor achizitionate de furnizori cu sistemul cardului de sănătate;
- La cererea CNAS vor fi intreprinse fara costuri suplimentare, activitati de testare a performantei sistemului, a incarcarii si capacitatii disponibile a acestuia si vor fi furnizate rapoarte cu acest continut. In prezent sistemul informatic detine functionalitati cu privire la testarea performantei, a incarcarii si a capacitatii disponibile a acestuia iar aplicarea concluziilor acestor activitati, vor fi incluse fara costuri in serviciile de administrare si mentenanta;
- Se va asigura administrare si suport pentru interfata de comunicare a sistemului CEAS cu mediului CAS AOPSNAJ, in baza documentatiei tehnice si functionale puse la dispozitie de CNAS;
- In cazul in care CNAS decide efectuarea unor audituri independente asupra SIUI, SIPE, CEAS, prestatorul va asigura, in cadrul contractului, suportul sau tehnic. Auditarea independenta va viza: auditul de performanta a sistemului si auditul de securitate; Numar anticipat anual de audituri: 1/sistem.
- In cazul unor modificari legislative aplicabile functionalitatilor curente ale proiectului CEAS si modificarilor de tip organizational impuse prin legislatie, sistemul va fi modificat corespunzator, fara costuri pentru Beneficiar;
- Se va asigura, fara costuri suplimentare pentru Beneficiar, suport specializat (analiza, documentare), in interconectarea CEAS cu proiectele existente din cadrul PIAS (SIUI, SIPE, DES).
- Se va asigura o monitorizare proactiva permanenta de functionare a elementelor sistemului incluse in prezenta procedura. CNAS detine in prezent o solutie de monitorizare licentiata Oracle. Solutia pentru monitorizarea calitatii serviciilor, prin intermediul componente pentru diagnostic, pune la dispozitie o abordare „top-down”, „end-to-end” privind monitorizarea, trierea si diagnosticare problemelor critice cu aplicatii .NET, SAP, Oracle, Siebel, J2EE, SOA si Java. Prin abordarea integrata, solutia pentru monitorizarea calitatii serviciilor este capabila sa prezinte CNAS o vedere completa asupra starii mediului IT si unelte pentru a putea identifica rapid cauza problemelor.

Ofertantul va beneficia de o perioada 30 de zile calendaristice pentru acomodare cu mediul specific de lucru al elementelor de detaliu ale sistemului informatic. Pentru aceasta perioada operatorul economic nu va fi raspunzator pentru derularea serviciilor.

Codul sursa este proprietatea Beneficiarului si va fi pus la dispozitia prestatorului dupa incheierea contractului. Modificarea codului sursa pe parcursul contractului nu presupune costuri suplimentare pentru prestator. Dezvoltarile software (codul sursa) rezultate din prestarea serviciilor in cadrul contractului sunt proprietatea beneficiarului.

Operatorul va asigura o copie actualizata permanent a codului sursa explicat al aplicatiilor, precum si a structurii bazelor de date si a procedurilor aplicate in sistem pe care o va pune la dispozitia CNAS dupa fiecare actualizare.

Serviciile vor fi furnizate sub incidenta clauzelor de confidentialitate.

Serviciile se vor realiza On site (la sediul central al beneficiarului).

Activitatile nu acopera:

- serviciile necesare ca urmare a interventiilor neautorizate efectuate de persoane care nu sunt certificate pentru aplicatiile CEAS, pentru administrare sau intretinere;
- efectuarea operatiilor de introducere/corectie de date necesare sistemului CEAS;
- rezolvarea incidentelor generate de aplicatii folosite de furnizorii de servicii medicale si farmaceutice, altele decat cele puse la dispozitie de CNAS, cu exceptia incidentelor generate de functionarea defectuoasa a web-service-urilor de interconectare;
- deplasarea specialistilor ofertantului la locatiile furnizorilor de servicii medicale si farmaceutice;
- rezolvarea problemelor de tipul urmator sau similare:
 - cauzate de utilizarea eronata (neconforma cu manualele de utilizare) a aplicatiei CEAS, sau aparute prin neglijenta utilizatorilor finali;
 - cauzate de utilizarea neconforma a suportului fizic al sistemului CEAS, de catre utilizatorii finali;
 - cauzate de erori de comunicatie
 - cauzate de virusi informatici
 - aparute in alte aplicatii folosite de utilizatorii finali, cu exceptia situatiei in care problemele sunt cauzate sau pot fi asociate unei functionari defectuase a interfetelor expuse de CEAS.

9.1 CERINTE SPECIFICE PENTRU SERVICIILE DE SUPORT SI MENTENANTA PENTRU COMPONENTA APLICATIVA SPECIFICA A CEAS (MODUL ECARD SI MODULE DESKTOP)

Serviciile de suport si mentenanta pentru componenta aplicativa specifica a CEAS (modul eCard si module desktop) vor consta in urmatoarele:

- Interventii in software-ul pentru componenta aplicativa specifica a CEAS respectiv in:
 - modul eCard
 - serviciile Web expuse de CEAS
- aplicatiile puse la dispozitie gratuit de CNAS pentru conectarea la SIUI si CEAS a diferitelor categorii de furnizori de servicii medicale (16 tipuri de aplicatii desktop). Rezolvarea incidentelor semnalate prin dezvoltarea de *update*-uri ale aplicatiilor de raportare și *patch*-uri de sistem central
- Ofertantul asigura servicii de verificare a sincronizarii nomenclatoarelor intre sistemele SIUI si CEAS la validarea unor versiuni noi în SIUI

9.2 CERINTE SPECIFICE PENTRU SERVICIILE DE SUPORT SI MENTENANTA PENTRU CONFIGURARILE SPECIFICE MODULULUI ZONA DE TRANSFER

Serviciile de suport si mentenanta pentru configurariile specifice modulului Zona de Transfer, vor fi asigurate conform cu urmatoarele cerinte:

- a. Analiza problemelor semnalate la nivel de modul Zona de Transfer
- b. Investigarea si rezolvarea problemelor semnalate la nivel de sincronizare loturi de carduri cu modulul eCard, transmise si receptionate de Zona de Transfer
- c. Mentinerea relatiei din punct de vedere al suportului tehnic cu producatorul aplicatiilor standard folosite
- d. Aplicarea de patch-uri si update-uri la nivel de aplicatie puse la dispozitie de producator pentru corectarea unor probleme, dupa analiza implicatiilor in cadrul sistemului

9.3 CERINTE SPECIFICE PENTRU CONFIGURARILE SPECIFICE MODULULUI AUTORITATE DE CERTIFICARE

Pentru modulul Autoritate de Certificare vor fi asigurate conform cu urmatoarele cerinte:

- a. Analiza problemelor semnalate la nivel de modul Autoritate de Certificare
- b. Investigarea si rezolvarea problemelor semnalate la nivel de interactiune cu echipamentele de personalizare carduri CEAS
- c. Investigarea si rezolvarea problemelor semnalate la nivel de interactiune cu echipamentele ce sustin serviciul OCSP

- d. Ajustarea configurațiilor la nivelul modulului, conform necesităților identificate

9.4 SERVICIILE DE GESTIONARE A TRANZACȚIILOR SI INTERACȚIUNILOR CU CARDUL NAȚIONAL DE ASIGURĂRI DE SĂNĂTATE SI TOATE STĂRILE PRIN CARE TRECE ACESTA

Ofertantul trebuie să asigure funcționarea CEAS, astfel încât să fie gestionate toate fluxurile de tranzacționare cu cardurile înrolate în sistem, prin interogarea și comunicarea bidirecțională cu SIUI – extensia eCard, unde sunt definite atât cardurile cât și asocierile între carduri și persoanele asigurate.

Trebuie asigurate următoarele funcționalități:

- Autentificare, prin folosirea cheilor publice aferente cardurilor preluate de la Autoritatea de Certificare;
- Suport pentru activarea de către medici a cardurilor, după ce acestea au fost livrate către utilizatorii finali;
- Suport pentru actualizarea informațiilor cu caracter medical, stocate pe card;
- Reînnoirea cardurilor, atunci când este necesar (distrugere, pierdere, defectiuni tehnice, etc);
- Managementul avertizărilor din SIUI
- Managementul cardurilor în toate stările lui;
- Suport privind operațiunile asupra stării cardurilor, inclusiv activități necesare deblocării cardurilor, respectiv investigarea și rezolvarea solicitărilor privind cardurile pentru care mesajul de eroare întors de operația de autentificare/validare este de tip “card invalid”

Aceste servicii sunt necesare asigurării accesului la date și automatizării proceselor de planificarea proceselor, personalizare, livrare, validare, activare, deblocare și utilizare a cardurilor.

Stările prin care trec cardurile CEAS de-a lungul ciclului de viață din sunt:

- Inactiv: starea inițială în care sunt livrate cardurile către cetățeni. Se aplică atât în cazul primei emiterii cât și în cazul re-emiterii.
- Înrolare în curs: cardul CEAS se află în această stare din momentul inițierii procesului de producție al cardului de către sistemul SIUI până în momentul în care acesta este personalizat.
- Transport: cardul CEAS se află în această stare din momentul din care este trimis către persoana asigurată până când trece în starea activ.

- Activ: este starea implicita. Cardurile pot fi utilizate pentru verificarea eligibilitatii solicitantilor in vederea acordarii serviciilor medicale.
- Actualizare in curs: cardul CEAS se afla in aceasta stare din momentul in care unitatea de management a initiat o cerere de actualizare a datelor de pe card pana in momentul in care operatiunea se incheie cu succes.
- Blocat: cardul poate ajunge in aceasta stare in urma introducerii unui cod PIN eronat, de cel putin de trei ori. Pentru deblocarea cardului se va folosi un serviciu de tip help-desk.
- Suspendat: cardul este trecut in aceasta stare in urma semnalarii, prin serviciul help-desk, a pierderii/deteriorarii acestuia. Cardul este mentinut in aceasta stare pana cand se genereaza o cerere de re-emitere a unui nou card.
- Dezactivat: aceasta stare marcheaza cardurile CEAS iesite din sistem.
- Expirat: aceasta stare marcheaza expirarea validitatii cardurilor CEAS si conditioneaza reluarea fluxurilor de productie in vederea emiterii unui nou card.

PREVEDERI DE SECURITATE APLICABILE

- i. standardul ISO/IEC 7816 pentru procesarea tranzactiilor cu carduri cu chip ce contin date cu caracter personal,
- ii. standardul PCI-DSS, care se aplica tuturor entitatilor care stocheaza, proceseaza sau transmit date referitoare la operatiunile cu carduri si care impune adoptarea proceselor si masurilor de securitate a informatiei care sa asigure integritatea datelor,
- iii. procedura de auditare a logurilor, integritatea datelor stocate in format electronic trebuie sa fie protejata si este necesar sa existe mecanisme de alertare in timp real care sa semnalizeze incercarile de alterare a integritatii datelor,
- iv. protejat de o solutie de detectie a intruziunii („IDS”),
- v. segmentele de retea separate prin firewall,
- vi. deruleaza cu periodicitate anuala teste de penetrare.

Pentru verificarea autenticitatii cardurilor se folosesc echipamente de tip HSM („Hardware Security Module”) conforme cu standardul FIPS 140-2 Level 3 si alimentate de la o sursa neintreruptibila de energie electrica.

9.5 SERVICIILE DE HELP-DESK AFERENTE SISTEMULUI INFORMATIC CEAS

CERINTE SPECIFICE PENTRU SERVICIILE DE HELP-DESK AFERENTE SISTEMULUI INFORMATIC AL CEAS

Ofertantul va asigura serviciul de Help-desk pentru toti utilizatorii interni si externi ai sistemului CEAS. Numarul utilizatorilor externi ai sistemului informatic al CEAS la nivelul asiguratilor este reprezentat de posesorii de card, asigurati in sistemul public al asigurarilor sociale de sanatate, la nivelul furnizorilor de

servicii medicale este estimat la peste 70.000, iar la nivelul CNAS/CAS numarul de utilizatori interni estimat este de 300.

Serviciile de help-desk pentru CEAS vor fi asigurate de ofertant avand in vedere urmatoarele cerinte:

1. Contractorul va utiliza pentru prestarea serviciului un numar de apel din categoria „telverde”, apelabil gratuit la nivel national.
2. In cadrul acestui serviciu, prestatorul va furniza (va face diponibila) o aplicatie licentiata de suport (HelpDesk) fara costuri pentru CNAS, atat pentru furnizare/instalare, cat si pentru mentenanta acesteia, prin intermediul careia vor fi inregistrate incidentele, prin care va urmari incadrarea in nivelurile de servicii (SLA) a rezolvarii incidentelor semnalate pe fiecare componenta (software, hardware), se va monitoriza rezolvarea lor si care sa calculeze si sa furnizeze si timpii de depasire inregistrati in rezolvarea incidentelor. Aplicatia de Help Desk va putea fi accesata cu drepturi de vizualizare si de catre personalul CNAS in vederea consultarii si extragerii de rapoarte.
3. Va receptiona, va analiza si in cazul in care nu poate formula un raspuns propriu sau nu poate oferi o solutie din istoricul de cazuri similare, va asigura dispecerizarea incidentelor catre nivelurile help-desk 2, asigurate pentru componenta software si pentru componenta hardware, respectiv Catre help-desk nivel 2 asigurat de CNAS/STS – pentru probleme de business/date CEAS si pentru probleme ce afecteaza tronsoanele de comunicatii de date folosite de CEAS.
4. Serviciul va fi furnizat in regim 24/7 in conditiile punctelor 5., 6. si 7. de mai jos
5. Serviciul va functiona cu minim 5 operatori pe intervalul orar 08:00 – 20:00, in zilele declarate lucratoare
6. Serviciul va functiona cu un operator pe intervalul orar 08:00 – 16:00, in zilele de repaos si in zilele declarate sarbatori legale.
7. In restul intervalului orar, serviciul va fi accesibil telefonic prin intermediul unui mecanism de tip Interactive Voice Response (IVR) cu posibilitatea de a se inregistra apelurile dupa informarea prealabila a apelantilor. Mecanismul de tip IVR va fi pus la dispozitie de catre Ofertant, gratuit, in cadrul acordului, incluzand mentenanta.
8. Acest nivel va supraveghea permanent adresa suport.ceas@casan.ro, va prelua de acolo incidentele si le va introduce in sistem, le va dispeceriza si va urmari rezolvarea solicitarilor primite pe aceasta cale. Ofertantul declarat castigator va fi inclus in grupul de suport care are acces la adresa suport.ceas@casan.ro .
9. Desfasurarea activitatii va prevedea generarea de rapoarte de activitate si calcul de penalitati periodice.
10. Vor fi asigurate cel putin urmatoarele rapoarte periodice (minim: lunar; maxim: saptamanal; la incident):

- Timpi medii de raspuns ai sistemului, calculat pe intervale orare, masurat dintr-o locatie externa sistemului dar care este prevazuta cu acces bun la retea Internet, pentru a elimina aceasta variabila,
- Numar de tranzactii efectuate cu cardul de sanatate (acceptate si respinse) pe intervale orare,
- Numarul de solicitari telefonice pentru suport utilizatori

Activitatile de suport vor fi derulate de personal specializat.

9.6 CERINTE PENTRU SERVICIILE DE ADMINISTRARE, SUPT SI MENTENANTA PENTRU CONFIGURARILE SPECIFICE LA NIVEL DE SISTEME DE OPERARE CEAS

Serviciile de administrare, suport si mentenanta la nivelul sistemului de operare vor fi asigurate pentru confirgurarile specifice la nivel de sistem de operare inclusiv pentru serverele de test si dezvoltare, conform urmatoarelor cerinte:

1. Asistență pentru problemele software critice și necritice.
2. Izolarea problemei si clasificarea unui incident, determinandu-se dacă acesta este de tip hardware sau software. Ofertantul serviciilor va informa Beneficiarul în situația în care o problemă percepută inițial ca fiind software este calificată ca fiind de natură hardware.
3. Suport în rezolvarea problemelor produselor software care pot fi identificate și reproduse de către Beneficiar.
4. Suport pentru a identifica problemele dificil de reprodus precum si diagnosticarea problemelor și determinarea unor parametri de configurare pentru configurațiile suportate.
5. Acces la anumite unelte proprietare electronice și accesibile pe Web cum ar fi:
 - Facilitățile disponibile utilizatorilor înregistrați care permit descărcarea patch-urilor de software și de firmware, abonarea la notificările de service proactive referitoare la hardware și participarea în forumuri electronice de suport care au drept scop rezolvarea problemelor prin schimbul de informații cu alți utilizatori înregistrați.
 - Acces extins la motoare web de căutare a documentelor tehnice de suport pentru a facilita rezolvarea mai rapidă a problemelor.
 - Acces la anumite unelte proprietare de diagnoză accesibile pe bază de parolă.

6. Suport la solutia software care monitorizează starea hardware-ului și generează notificări când sunt detectate anumite condiții predeterminate. Evenimentele de notificare vor fi recepționate și trimise direct Ofertantului pentru analiză și posibilă acțiune de suport inclusiv de la distanță pentru diagnosticarea și soluționarea rapidă a problemei.
7. Accesul, pe măsura apariției, la actualizări software pentru produsele software utilizate, ultimile revizii software și documentația aferentă
8. Aplicarea de patch-uri si update-uri puse la dispozitie de producator pentru corectarea unor probleme

9.7 CERINTE PENTRU SERVICIILE DE ADMINISTRARE, SUPORT SI MENTENANTA PENTRU COMPONENTA DE MONITORIZARE A INFRASTRUCTURII IT

Componenta de monitorizare infrastructura IT cuprinde: HP Quality Center+ Functional Testing – 1 licenta, HP Webinspect – 1 licenta, HP Operations Manager – 1 licenta, HP BAC+ TV+ uCMDB+ Site Scope – 1 licenta si HP Service Manager -15 licente

Serviciile de administrare, suport si mentenanta la nivelul componenta de monitorizare a infrastructurii IT vor fi asigurate conform urmatoarelor cerinte:

1. Servicii de suport si mentenanta la nivelul componentelor software standard, in intervalul orar 8--20
 - a. Acces pe site-ul producatorului la informatii tehnice (manuale, kit-uri de instalare, patch-uri, documente de tip “how-to”, etc)
 - b. Acces pe site-ul producatorului la forumuri de discutii si la instrument de tip chat
 - c. Managementul licentelor (se vor oferi facilitati de raportare, migrare si consolidare licente)
 - d. Abonare la buletine de securitate pentru aplicatiile achizitionate
 - e. Asistenta in deschiderea, urmarirea si rezolvarea cazurilor de suport pe site-ul producatorului
2. Servicii de suport si mentenanta la nivelul sistemului de virtualizare VMware vSphere in regim Subscription only:
 - a. Accesul la actualizarile pentru versiunea software si accesul la noi versiuni software
 - b. Raportarea incidentelor si acces la expertii de suport tehnic VMware
3. Servicii de suport si mentenanta la nivelul solutiei implementate vor include urmatoarele:
 - a. Analiza problemelor semnalate la nivel de solutie

- b. Aplicarea de patch-uri si update-uri la nivel de aplicatie puse la dispozitie de producator pentru corectarea unor probleme
- c. Mentinerea la zi a documentatiei de instalare si configurare a aplicatiei

Prestatorul este responsabil de functionarea componentei de monitorizare si va asigura accesul Beneficiarului la aplicatii.

Activitatile de administrare si suport vor fi derulate de personal specializat pe componentele software standard implementate.

Prestatorul va realiza si va pune la dispozitia beneficiarului, periodic, la intervalele convenite, rapoarte de monitorizare a infrastructurii, generate de aplicatiile de monitorizare. Frecventa minima a rapoartelor: lunar; frecventa maxima: saptamanal sau la aparitia unui incident (din toate cele 4 categorii de criticitate);

9.8 CERINTE PENTRU SERVICIILE DE ADMINISTRARE, SUPT SI MENTENANTA PENTRU CONFIGURARILE SPECIFICE LA NIVEL DE ECHIPAMENTE DE NETWORKING

Serviciile de administrare, suport si mentenanta pentru configurările specifice la nivel de echipamente de networking ce asigura traficul intern vor fi asigurate conform urmatoarelor cerinte:

1. Analiza incidentelor semnalate la nivel de mecanisme MSTP si LACP in cadrul echipamentelor de networking intern
2. Acces la suportul tehnic al producatorilor echipamentelor de networking intern
3. Aplicarea de patch-uri si update-uri la nivel de firmware pus la dispozitie de producatorul echipamentelor pentru corectarea unor probleme
4. Ajustarea configurarilor la nivelul solutiei, in urma recomandarilor de la producatorul echipamentelor
5. Restaurarea/reinstalarea si reconfigurarea echipamentelor de networking in caz de probleme hardware.
6. Prelevarea periodica a datelor relevante pentru incidentele de securitate semnalate.
7. Propuneri de actiuni in scopul prevenirii vulnerabilitatilor semnalate de comunitate.

Serviciile de administrare, suport si mentenanta pentru configurările specifice la nivel de echipamente de networking ce asigura traficul extern pentru sistemul CEAS vor fi asigurate conform urmatoarelor cerinte:

1. Reinnoirea valabilitatii certificatelor digital server SSL de la nivelul adresei ceas.siui.ro

2. Analiza incidentelor semnalate la nivel de functionalitati de degrevare SSL asistata hardware, echilibrare a incarcarii, firewall in cadrul echipamentelor de networking extern ce sustin functionarea CEAS
3. Acces la suportul tehnic al producatorilor echipamentelor de networking extern ce sustin functionarea CEAS
4. Aplicarea de patch-uri si update-uri la nivel de firmware pus la dispozitie de producatorul echipamentelor pentru corectarea unor probleme
5. Ajustarea configurarilor la nivelul solutiei, in urma recomandarilor de la producatorul echipamentelor
6. Restaurarea/reinstalarea si configurarea echipamentelor de networking in caz de probleme hardware.
7. Prelevarea periodica a datelor relevante pentru incidentele de securitate semnalate.
8. Propuneri de actiuni in scopul prevenirii vulnerabilitatilor semnalate de comunitate.

9.9 CERINTE PENTRU SERVICIILE DE ADMINISTRARE, SUPORT SI MENTENANTA PENTRU

CONFIGURARILE SPECIFICE LA NIVEL DE SOLUTIE DE BACKUP PE BANDA AL BAZEI DE DATE

CNAS dispune de o solutie profesionala de back-up pe banda a bazei de date, automatizata, "HP Data Protection".

Serviciile de administrare, suport si mentenanta pentru configurariile specifice la nivel de solutie de backup pe banda al bazei de date centrale vor fi asigurate conform urmatoarelor cerinte:

1. Analiza problemelor semnalate la nivel de solutie de backup
2. Acces la suportul tehnic al producatorului aplicatiei standard pentru backup si restaurare
3. Coordonarea rezolvarii problemelor aparute impreuna cu suportul ofertantului de hardware
4. Aplicarea de patch-uri si update-uri la nivel de aplicatie standard de backup si restaurare
5. Ajustarea configurărilor la nivelul soluției, in urma recomandărilor de la producător sau a modificării configurației hardware sau software
6. Restaurarea/reinstalarea si reconfigurarea aplicației standard pentru backup si restaurare, in caz de probleme hardware.

9.10 CANTITATEA SAU DURATA ACHIZIȚIEI:

- Cantitatea sau durata maxima estimata a Acordului Cadru – 36 de luni
- Cantitatea sau durata minima estimata a Acordului Cadru – 12 luni
- Cantitatea sau durata maxima estimata a unui singur Contract Subsecvent – 12 luni
- Cantitatea sau durata minima estimata a unui singur Contract Subsecvent – 3 luni