Caiet de sarcini

„Dezvoltare BRIDGE PKI”

Ministerul Comunicațiilor si Societății Informationale

Conținut

1 OBIECTIVELE PROIECTULUI

Strategia MCSI referitoare la informatizarea serviciilor publice la nivel central și local trebuie să urmărească cu precădere câteva direcții de acțiune:

Creșterea eficienței aparatului administrativ prin folosirea noilor tehnologii electronice de comunicare;
Orientarea serviciilor publice spre necesitățile cetățenilor și ale oamenilor de afaceri;
Asigurarea accesului liber la informațiile publice;
Transparența în exercitarea actului administrativ;
Îndeplinirea standardelor administrației europene, în vederea interconectării cu sistemele statelor din Uniunea Europeană;

În acest sens MCSI dorește să pună la dispoziția mediului de afaceri o infrastructura care să permită interoperabilitatea intre membrii participanți, precum și accesul securizat la aceasta infrastructura.

Interoperabilitatea este un factor critic în implementarea infrastructurilor de chei publice (Public Key Infrastructure). Interoperabilitatea permite efectuarea unor tranzacții sigure intre organizații ce folosesc tehnologii PKI provenind de la firme diferite, asigura o flexibilitate ridicată în alegerea tehnologiei PKI și reduce riscul de implementare a soluțiilor bazate pe PKI.

O infrastructura interoperabila presupune ca toate componentele din infrastructura de chei publice să fie conectate împreuna. Daca, un departament din cadrul unei instituții alege modelul de infrastructura de chei publice ale producătorului de software A, iar instituția alege ulterior modelul furnizat de producătorul B, este normal ca se va crea o oarecare suprapunere în acest caz.

Situația devine mai complexa atunci când instituțiile A și B vor dori ca extranet-urile lor, fiecare având propria infrastructură de securitate, să interopereze. Aceasta poate implica existenta unor autorități de certificare dedicate sau este posibil ca ambele infrastructuri să fie subordonate unei instituții guvernamentale. Complexitatea tehnică a unor astfel de situații vine din necesitatea de a asocia elementele de bază pentru realizarea încrederii, aceste aspecte nefiind specificate încă în nici un standard existent.

Astfel, interoperabilitatea intre infrastructurile de chei publice are semnificații diferite în funcție de contextul în care este folosita.

În concluzie, exista trei mari categorii de interoperabilitate specifice infrastructurii de chei publice:

interoperabilitatea la nivelul componentelor
interoperabilitatea la nivelul aplicațiilor

interoperabilitatea intre domenii diferite

1.1 Obiective pe termen scurt

Realizarea unui mediu de lucru care să asigure prin interoperabilitate:

capacitatea unei aplicații de chei publice de a interacționa cu alta aplicație de chei publice
posibilitatea mixării de componente provenind de la firme diferite pentru crearea unei infrastructuri de chei publice organizaționale
interacțiunea dintre domenii de chei publice aparținând unor organizații diferite, pentru a permite efectuarea unor tranzacții sigure intre aceste organizații

1.2 Obiective pe termen lung

Standardele în domeniul criptografiei cu chei publice au fost și încă sunt greu de adoptat și implica multe discuții, deoarece, pentru a crea o infrastructură bazată pe chei publice, este necesar un consens în ceea ce privește părțile fundamentale, anume:

formatul certificatelor digitale – care trebuie să fie cat mai apropiat de necesitățile fiecărei aplicații
clienții care fac cereri pentru astfel de certificate
server-ele care emit certificate
părțile ce verifica validitatea certificatelor

Toate aceste componente trebuie să funcționeze independent de implementare, dând astfel integratorilor de sisteme posibilitatea să realizeze modele complexe de securitate, având la bază tipuri de componente de chei publice realizate de diferiți producători software.

Informatizarea administrației publice este parte integrantă a "Strategiei naționale pentru promovarea noii economii și implementarea societății informaționale", așa cum este ea reglementată în legislația românească. Modelul ce se dorește a fi implementat este acela al unei administrații publice orientate spre deservirea cetățenilor, al unei administrații care să susțină un schimb intensiv de informații și date, atât în interiorul sistemului intre instituțiile publice, cat și în relația cu exteriorul, cu mediul de afaceri și organizațiile neguvernamentale.

Informatizarea administrației publice se înscrie intr-o suită de masuri guvernamentale ce vizează reformarea acestui sector de activitate din România. Strategia guvernamentala de informatizare a administrației publice urmărește atingerea indicatorilor stabiliți de către Consiliul European, definiți în anul 2002, sub conceptul de "procentaj al serviciilor publice de baza disponibile on-line", și redefiniți în 2005, ca "număr al serviciilor publice de baza disponibile integral on-line".

Printre obiectivele globale ale informatizării administrației publice din România regăsim următoarele:

Îmbunătățirea calității serviciilor publice având ca beneficiari cetățenii și agenții economici;

Accesul cetățenilor la informația de interes public va fi astfel asigurat evitându-se restricționările legate de spațiu și timp. Totodată, soluțiile de securitate implementate la nivelul instituțiilor publice vor asigura deplina confidențialitate și integritate a datelor și informațiilor transmise sistemului. Îndeplinirea unor criterii de excelență și calitate la nivelul instituțiilor publice va contribui decisiv la formarea unei imagini profesioniste a organizațiilor în rândul celor cu care acestea interacționează.

Modernizarea administrației publice;

Electronizarea instituțiilor publice se înscrie în tendința generala de a aduce administrația publica românească la standardele europene.

Dezvoltarea sectorului IT&C, prin lansarea de noi proiecte și implementarea de noi sisteme informatice integrate la nivelul instituțiilor publice.

Pentru punerea în aplicare a strategiei guvernamentale referitoare la reformarea administrației prin informatizare, este necesară derularea de proiecte specifice tehnologiilor informației și comunicațiilor. Pentru implementarea unor astfel proiecte, sectorul privat este stimulat să proiecteze și să realizeze sisteme competitive, integrate. Succesul acestor proiecte va aduce companiilor private IT&C recunoaștere și performante financiare importante, consolidându-le poziția în piața.

Creșterea calității vieții cetățenilor prin utilizarea noilor tehnologii

Prin promovarea la nivelul administrației publice a tehnologiilor informatice competitive, orientate spre Internet, se va asigura o creștere a satisfacției cetățenilor în ceea ce privește relația cu instituțiile statului. Toate aceste acțiuni vor putea fi derulate în spațiul virtual pe care Internetul îl oferă, în condiții de maxima siguranță și confidențialitate, fără alte limitări temporale, exceptându-le pe cele legale.

Menținerea și dezvoltarea unei capacitați de cercetare-dezvoltare-inovare susținută de un transfer tehnologic activ către producătorii de bunuri și servicii.

Ținând cont de dinamica instituțională, de liberă concurență din spațiul european precum și de noile principii ce vor guverna conducerea instituțiilor publice, furnizorii de soluții informatice în domeniul serviciilor publice, vor trebui să mențină un ritm alert de cercetare și dezvoltare pentru a putea veni în întâmpinarea solicitărilor pieței cu produse și servicii competitive, care să mențină și să crească calitatea serviciilor publice. Furnizarea de servicii complete intre unități ale administratei publice centrale și locale, diferite, implica îndeplinirea interoperabilității totale a sistemelor informaționale centrale cu cele ale administrațiilor publice locale, care sunt desemnate din ce în ce mai mult să asigure coordonarea directă a serviciilor furnizate către cetățeni sau agenți economici, devenind astfel interfața administratei publice centrale.

1.3 Beneficii şi beneficiari

Prin acest proiect se dorește comunicarea intr-un mod securizat intre Administrația Centrala și Autoritățile de Certificare. Fiecare entitate implicată în acest proiect va avea propria ei arhitectura PKI, deci este nevoie ca aceste ierarhii PKI să interacționeze.

Prin dezvoltarea acestei infrastructuri de interoperabilitate, entitățile ce aderă la acest sistem vor fi recunoscute în cadrul topologiei. În momentul în care enrollment-ul unității în cadrul acestui sistem reușește, va fi soluționată comunicarea sigura intre părți, nemaifiind necesară o autentificare auxiliara, deoarece unitatea este deja considerata de încredere în cadrul sistemului.

Prin aderarea marilor companii la acest sistem, costurile financiare dar și resursele privind timpul și efortul de implementare, vor scădea considerabil.

Schimbul de informații și cunoștințe intre entitățile implicate va fi facil și se va realiza în mod securizat.

2 CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1 Cerințe generale

Proiectul în cauza urmărește creșterea calității serviciilor publice ofe rite mediului de afaceri.

Sistemul rezultat trebuie să satisfacă următoarele cerințe:

trebuie să fie compatibil cu platforma J2EE;
trebuie să includă interfeţe administrative capabile web;
trebuie să ruleze ca un site web securizat;
trebuie să ofere capabilitatea de a detecta în timp real orice schimbare în informaţia referitoare la un utilizator (nume, prenume, parola, alte proprietăți) care apare în orice sursă care conţine respectiva informaţie și să propage în mod automat acea schimbare către orice alta sursă care conţine informaţii despre acel utilizator. Mecanismul de propagare trebuie să fie configurabil;
trebuie să poată prelua informaţiile despre utilizator din surse multiple: fişiere neformatate, fişiere XML, baze de date, servere de directoare;
trebuie să fie compatibil cu surse multiple care stochează informaţiile de identitate (precum un sistem HR, baze de date, fișiere, servere de directoare);
să ofere capabilitatea de a aloca / modifica drepturile de utilizator / privilegiile de acces la resursele organizaţiei în funcţie de politicile existente în organizaţie şi de rolul utilizatorului în organizaţie;
să ofere capabilitatea de a delega responsabilitatea de administrare către divizii, departamente sau alte unităţi ale organizaţiei;
trebuie să ofere capabilitatea de a permite utilizatorilor să își administreze parolele, incluzând schimbarea şi resetarea parolelor fără intervenția administratorilor;
să permită utilizatorilor să solicite crearea de noi conturi folosind un browser web (user self service);
trebuie să permită utilizatorului să își actualizeze informaţiile personale (adresă, telefon etc.) şi să propage în mod automat informaţia către toate resursele organizaţiei care conţin total sau parţial acele informaţii;
trebuie să conţină un motor pentru fluxul de lucru care direcţionează orice cerere către aprobatorul sau aprobatorii corespunzători; notificările trebuie făcute printr-un sistem email;
trebuie să ofere o interfaţă grafică pentru configurarea fluxului de lucru conform politicilor / procedurilor existente în organizaţie;
să poată simula orice schimbare referitoare la informaţiile despre utilizatori, politici înainte de efectuarea schimbării;
trebuie să ofere capabilitatea de a vizualiza solicitările oricărui utilizator sau cererile care privesc solicitările legate de modificarea informaţiei utilizatorului;

2.2 Prevederi de securitate generale

Sistemul va respecta următoarele prevederi de securitate generale:

trebuie să folosească un mecanism de autentificare LDAP cu nume de utilizator şi parolă pentru toate accesele, inclusiv GUI web şi cereri API
să se integreze (folosind plugin-uri sau agenţi) cu suport pentru soluţia de autentificare a utilizatorilor.
Sistemul trebuie să poată impune încetarea sesiunii din cauza inactivităţii pe o perioadă de timp configurabilă
Toate parolele vor fi mascate la introducere
Toate sesiunile de comunicare din soluţie trebuie securizate folosindu-se sesiuni de criptare SSL . Aceasta include toate sesiunile utilizatorilor finali cu browser web precum şi comunicarea între componenţii soluţiei precum Serverul şi agenţii săi.
Soluţia trebuie să ofere o politică de parolă care se poate aplica global tuturor conturilor ţintă sau care poate fi atribuită unuia sau mai multor servicii ţintă, şi are mai multe aspecte, incluzând:

- Lungime minimă şi maximă
- Numărul maxim de caractere repetabile
- Numărul minim de caractere alfa şi/sau numerice
- Definirea caracterelor invalide şi/sau a celor cerute
- Restricţionarea primului caracter şi/sau a întregii parole la un set de caractere declarat
- Numărul de parole precedente să nu fie permis (inclusiv cele scrise invers)
- Nepermiterea numelui de utilizator şi/sau a ID-ului de utilizator ca parolă
- Nepermiterea parolelor găsite în dicţionare

Valoarea iniţială a parolei trebuie să fie limitată la prima folosire
Soluţia trebuie să ofere posibilitatea de a genera parole aleatoare
Dacă statutul unui utilizator se schimbă (schimbarea rolului, schimbarea zonei de responsabilitate, concediu fără plată, terminare etc.) soluţia trebuie să ofere metodele de suspendare/terminare/modificare a contului în cauză conform politicii organizaţiei
Soluţia trebuie să ofere metode pentru prevenirea reutilizării identităţilor conturilor după ce acestea au fost retrase

3 DESCRIEREA TEHNICA A PROIECTULUI

Proiectul “Dezvoltarea infrastructurii în vederea interoperabilității și accesului securizat pentru Administrația Centrală” propune o soluție pentru realizarea unui mediu de lucru (framework) în care să fie posibilă interoperabilitatea intre diferite autorități de certificare (CA).

La nivelul unei autorități de certificare se identifică următoarele aspecte importante din punct de vedere al interoperabilității:

o autoritate de certificare emite și livrează certificate pentru entitățile subordonate și cele din alte structuri;
accepta cereri de revocare de la deținătorii de certificate, pentru certificatul emis;
publica certificatele și listele de revocare intr-un repository;
solicita certificate de CA de la alte autorități de certificare (CA).

Proiectul propune o soluție bazată pe liste cu autorități de certificare trust pentru asigurarea interoperabilității intre domenii de chei publice diferite.

Sistemul este simplu și ușor de gestionat și pentru a evita dezavantajele ce pot apare din punct de vedere al securității se introduc listele cu certificate de încredere (CTL – certificate Trust List).

O lista de încredere CTL este o structura de date PKCS#7 semnată de un digital terț , emitentul listei și conține o serie de autorități de certificare trust.

O autoritate de certificare trust este identificată în cadrul listei prin intermediul valorii hash a certificatului său digital.

Pentru a asigura interoperabilitatea intre domenii, în listele CTL se pot substitui certificatele reciproce. Prin declararea de încredere a emitentului listei CTL se pot valida toate certificatele digitale emise direct sau indirect de către autoritățile de certificare din listă.

3.1 Arhitectura sistemului informatic şi de comunicaţii

3.1.1 Arhitectura funcţională

Arhitectura sistemului “Dezvoltarea infrastructurii în vederea interoperabilității și accesului securizat pentru Administrația Centrală” furnizează membrilor participanți următoarele servicii:

distribuția certificatelor acreditate CA sub forma unei liste semnate, listă de încredere (TL)
certificarea cross-certification membrilor participanți ce nu doresc să folosească lista de încredere (TL).

Se va distribui o listă de încredere ce cuprinde autoritățile de certificare rădăcina, listă semnată de certificatul propriu sistemului.

Utilizatorii sistemului

pot accepta aceasta lista sau
pot crea liste proprii prin înlăturarea unor certificate și resemnarea listei actualizate cu certificatul propriu.

Stabilirea relației de încrede între autoritățile de certificare participante.

Un certificat electronic va conține, print altele, numele autorității de certificare inițiatoare, certificatul deținătorului și cheia publică și va fi semnat de către autoritatea de certificare emițătoare cu, cheia privată.

Oricine primește un certificat, îl poate autentifica verificând semnătura electronica a autorității de certificare emițătoare, apoi poate utiliza cheia publică pentru a verifica semnătura electronică creată cu ajutorul cheii private a deținătorului.

Când este prezentat un certificat , primitorul poate deasemenea accesa autoritatea de certificare inițiatoare pentru a stabili dacă certificatul a fost înlăturat.

Primitorul trebuie să cunoască și să aibă încredere în autoritatea de certificare ce a lansat certificatul.

Totuși când primitorului îi este prezentat un certificate semnat de o autoritate de certificare necunoscuta lui, este necesar un mecanism care să-i permită să stabilească încrederea cu autoritatea de certificare apărută.

Conform modelului standard al infrastructurii de chei publice, aceasta este realizata de către primitor, urmărind o cale de certificare.

Aceasta situație apare dacă certificatul CA a fost semnat de cheia privată a unei alte autorități de certificare (CA), care la rândul ei are semnat certificatul de o alta autoritate de certificare (CA).

Daca primitorul se încrede într-una din aceste autorități de certificare (CA) și îi cunoaște cheia publică, atunci poate verifica fiecare certificat aflat în calea de certificare până ajunge la autoritatea de certificare (CA) noua și o poate verifica.

Maniera în care autoritățile de certificare (CA) se certifica intre ele , stabilește arhitectura de chei publice.

Scopul proiectului “Dezvoltarea infrastructurii în vederea interoperabilității și accesului securizat pentru Administrația Centrală” este de a :

depăși dezavantajele altor modele PKI (simplu, ierarhic, mesh)

permite realizarea încrederii reciproce intre participanți, dar să-și mențină propria structură de încredere.

Funcționalitatea de bază

Sistemul va furniza:

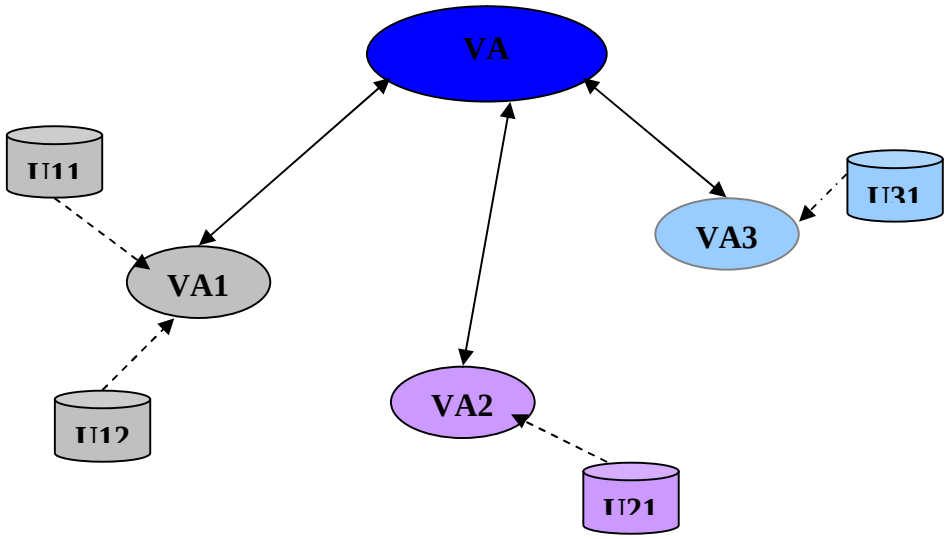
posibilitatea certificării cross-certification între participanți
lista semnată cu autoritățile de certificare acreditate
furnizează certificate cheie publică pentru fiecare membru PKI, precum și lista corespunzătoare de certificate revocate
specificațiile interfeței pentru fiecare membru PKI ce interacționează cu BCA
posibilitatea participanților de a testa, valida propria interfață la site-ul de referință.

Pentru a realiza o arhitectura funcțională care să asigure interoperabilitatea PKI, s-au evaluat modelele PKI actuale.

Modele de infrastructură chei publice

Modelul “autorității de validare” (VA)
Modelul “ierarhic”
Modelul “mesh”
Modelul “Web/Internet Trust”
Modelul “Bridge CA”

Modelul “autorității de validare” (VA)



Modelul “autorității de validare” se bazează pe utilizarea protocolului OCSP (Online Certificate Status Protocol) pentru a chestiona un server cu privire la statutul certificatelor.

Fiecare RP (Relying Party) trebuie să verifice starea unui certificat accesat prin intermediul unui canal on-line de autentificare, către un server de validare, ce returnează informația referitoare la starea certificatului în cauza.

Avantaje:

consultarea on-line furnizează întotdeauna informații actuale
validarea informației nu trebuie să fie diseminată pe toate stațiile de lucru
se poate implementa un software de validare eficient care să acopere toate situațiile complexe
utilizatorii ce aparțin unei ierarhii pot obține informația asupra certificatelor autorizate

Dezavantaje:

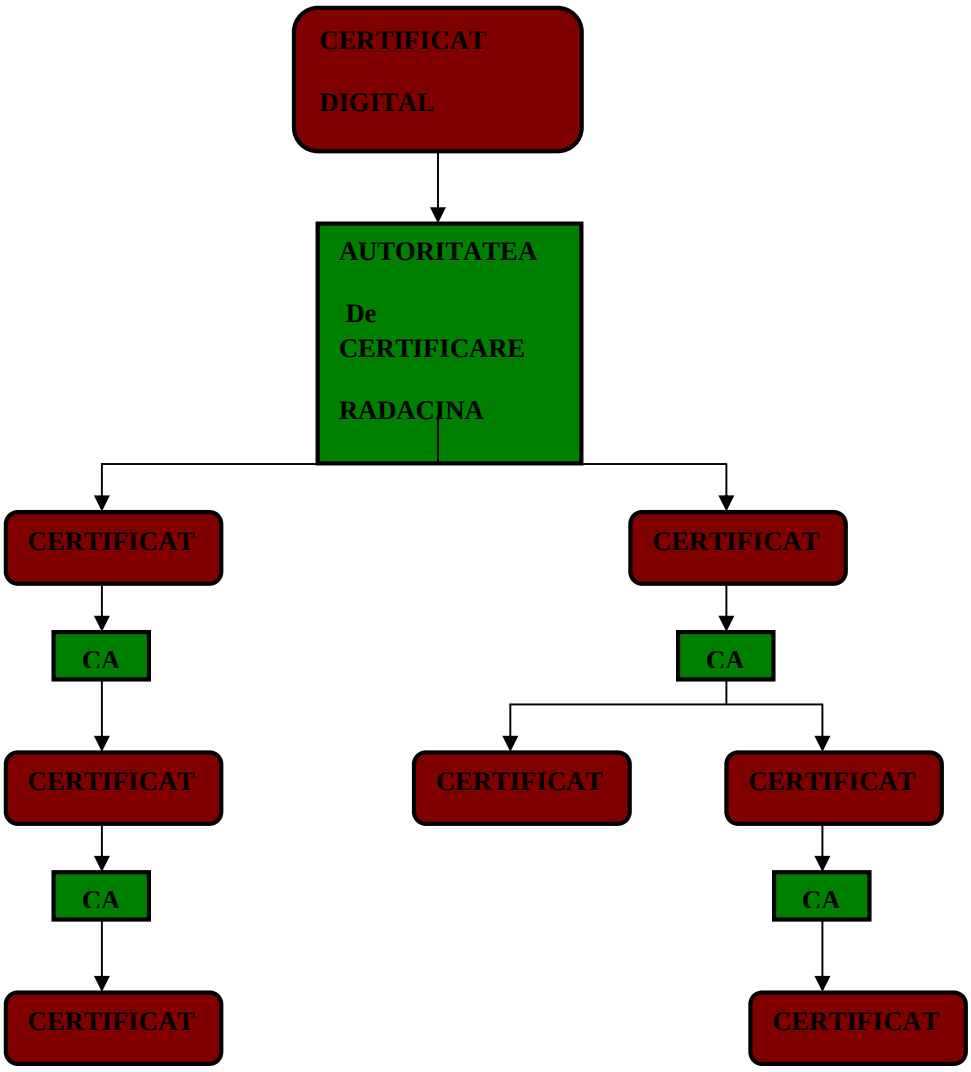
este obligatoriu folosirea de către utilizatori a instrumentelor software compliante OCSP
verificarea caii de validare este parțial delegată unei alte părți
necesită în permanență conexiune la rețea pentru a interoga server-ul de validare.

Modelul "ierarhic"

În cazul unei astfel de structuri, autoritățile de certificare sunt organizate ierarhic, fiecare dintre ele putând emite certificate autoritarilor subordonate sau utilizatorilor acesteia.

În topul ierarhiei se afla autoritatea de certificare root (Root CA) sub care sunt dispuse autoritățile de certificare subordonate, fiecare autoritate de certificare având un singur părinte.

În figura de mai jos este prezentat un caz de structura CA ierarhica.



Toate entitățile trebuie să aibă încredere în autoritatea de certificare din topul ierarhiei (root CA), validarea certificatelor din sistem facondu-se pe baza cheii publice a acesteia. Numele autorității de certificare rădăcina și cheia să publică sunt incluse intr-un certificat digital auto semnat. Un certificat digital auto semnat este un certificat emis de o autoritate de certificare pentru ea însăși, adică numele emitentului și numele subiectului din certificatul digital auto semnat sunt identice. Acest certificat se distribuie tuturor utilizatorilor din sistem folosind mecanisme sigure de distribuție. Pentru a se asigura securitatea sistemului, stocarea certificatului autorității din topul ierarhiei trebuie să se facă astfel încât să se evite substituirea sau modificarea neautorizata a acestuia.

Structurile PKI ierarhice oferă următoarele avantaje:

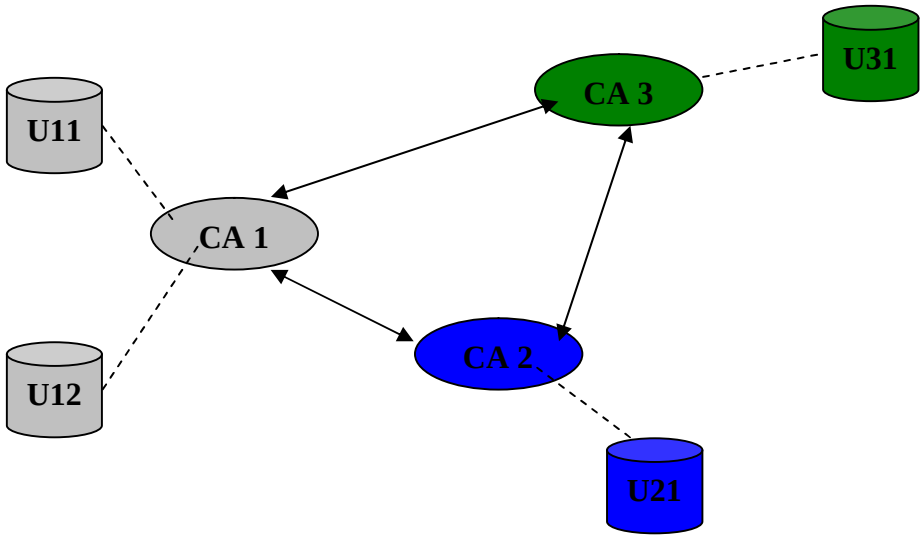
Structura multor organizații este de tip ierarhic (organizații guvernamentale, militare)
Căile de certificare sunt ușor de determinat, deoarece sunt unidirecționale. Pentru fiecare certificat există o cale de certificare unică spre autoritatea de certificare rădăcina.

Căile de certificare sunt relativ scurte și prin urmare timpul de validare al certificatelor este redus.
O arhitectura ierarhica oferă un grad ridicat de scalabilitate, adăugarea de noi autorități de certificare subordonate, care să permită gestionarea unui număr crescut de utilizatori, realizându-se astfel simplu.

Pe lângă aceste avantaje, o structura PKI ierarhica are însa și o serie de dezavantaje:

Compromiterea cheii private a autorității de certificare rădăcină are efecte catastrofale, necesitând revocarea tuturor certificatelor existente și recrearea ierarhiei.
Relațiile de încredere dintre organizații sau firme nu sunt neapărat ierarhice și prin urmare este foarte dificil să se găsească o singura autoritate în care să aibă toți încredere.

Modelul "mesh"



Toate autoritățile de certificare (CA) dintr-un model "mesh" sunt considerate puncte de încredere. Autoritățile de certificare (CA) emit certificate uneia alteia; perechea de certificate descriind relația de încredere bidirecțională .

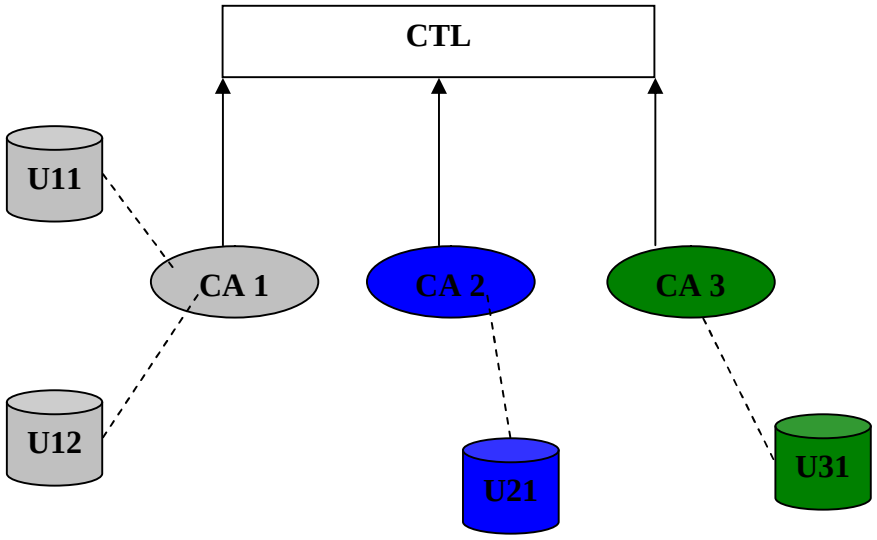
Avantaje:

utilizatorii noi pot fi cu ușurință incorporați
compromiterea unei autorități de certificare (CA) nu distruge întreaga structura de chei publice
recuperarea ca urmare a unei compromiteri este mai ușoară decât în cazul unei structuri ierarhice
o structura de chei publice "mesh" poate fi cu ușurință construită dintr-un set de autorități de certificare (CA) izolate

Dezavantaje:

dezvoltarea unei cai de certificare este mult mai complexa decât în cazul unei structuri ierarhice
se poate dezvolta un loop nesfârșit de certificate
conținutul unui certificat nu poate fi utilizat pentru recunoașterea drepturilor de acces.

Modelul "Web/Internet Trust "



Aceasta soluție se bazează pe liste de certificate de încredere CTL (Certificate Trust List).

Browse-ele Web actuale folosesc aceasta soluție, având pre-instalate zeci de autorități de certificare în aceasta listă. Adăugarea sau ștergerea unei autorități de certificare (CA) din listă se poate face de către fiecare utilizator în parte, sau centralizat, la nivelul unei organizații.

O listă CTL este o structura de date PKCS#7 semnată digital de un terț de încredere , ce conține o serie de autorități de certificare (CA) considerate a fi de încredere. O auto ritate de certificare (CA) de încredere este identificată în cadrul listei prin intermediul valorii hash a certificatului sau digital. De asemenea, o CTL poate conține identificatori de politici.

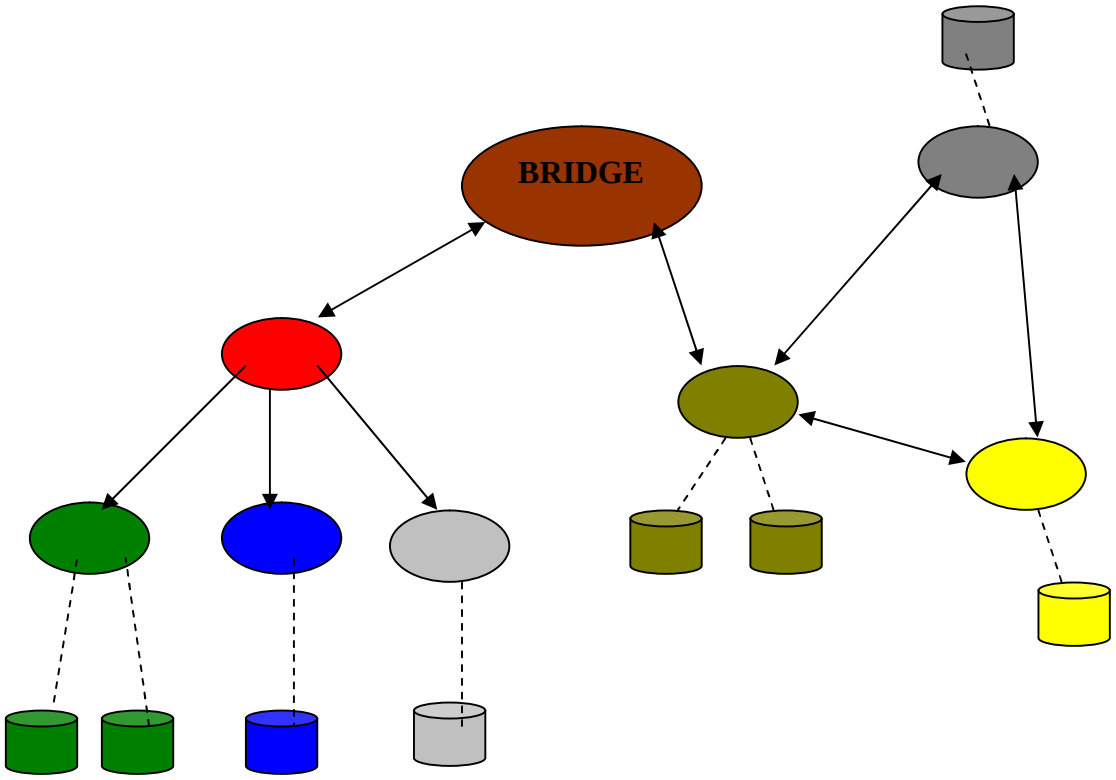
Avantaje :

acest model este deschis
compromiterea unei autorități de certificare (CA) nu distruge întreaga structură de chei publice
realizarea caii de certificare este mai simpla decât în cazul modelului "mesh"

Dezavantaje:

nu se procesează și revocările
nu asigură suport pentru folosirea politicilor de certificare multiple
nu dispune de mecanisme pentru protecția integrității datelor

Modelul “Bridge CA”



Arhitectură ierarhică PKI

Arhitectură ierarhică PKI

Acest model se bazează tot pe relații de certificare reciprocă, însă modelul de încredere folosit este de tip stea. Numărul de certificări în cazul unei structuri bridge creste liniar cu numărul domeniilor PKI.

“Bridge BCA” reprezintă o autoritate de certificare intermediară, având rolul de a crea o punte de legătura intre domenii de chei publice diferite.

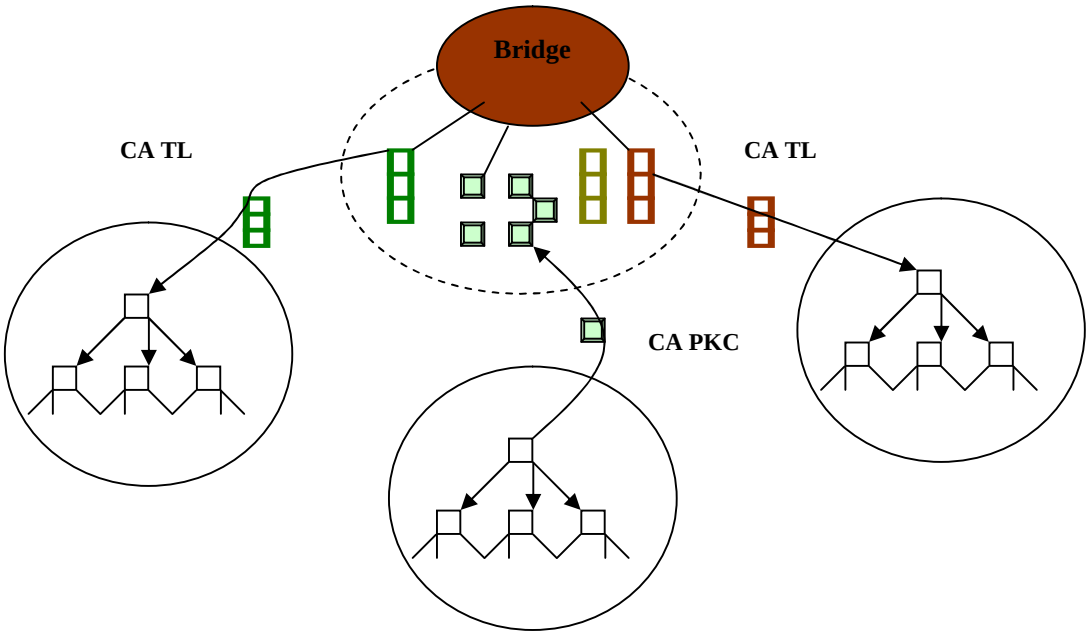
“BCA” permite interconectarea domeniilor de chei publice indiferent de arhitectura acestora.

Avantaje:

în comparație cu modelul de chei publice “mesh”, descoperirea caii de certificare devine mai ușoara
căile de certificare sunt mai scurte

Modelul proiectului

Modelul infrastructurii de chei publice al proiectului propus este o combinație intre modelul Web/Internet Trust și modelul bridge expuse mai sus.



Sistemul va furniza participanților:

certificate cheie publica
lista de autorități de certificare acreditate (CTL)

Sistemul va permite unui participant fie să descarce certificatele CA cross-certification, fie să aleagă lista de certificate trust CTL.

În cel din urma caz:

sistemul va distribui o lista de certificate rădăcină de încredere ce satisfac anumite cerințe; această listă este semnată de către certificatul sistemului.
participanții pot accepta pur și simplu aceasta lista sau
pot crea propria lista de CA prin eliminarea unor certificate și resemnarea listei actualizate cu certificatul propriu

Servicii oferite

Proiectul "Dezvoltarea infrastructurii în vederea interoperabilității și accesului securizat pentru Administrația Centrală" va asigura următoarele servicii:

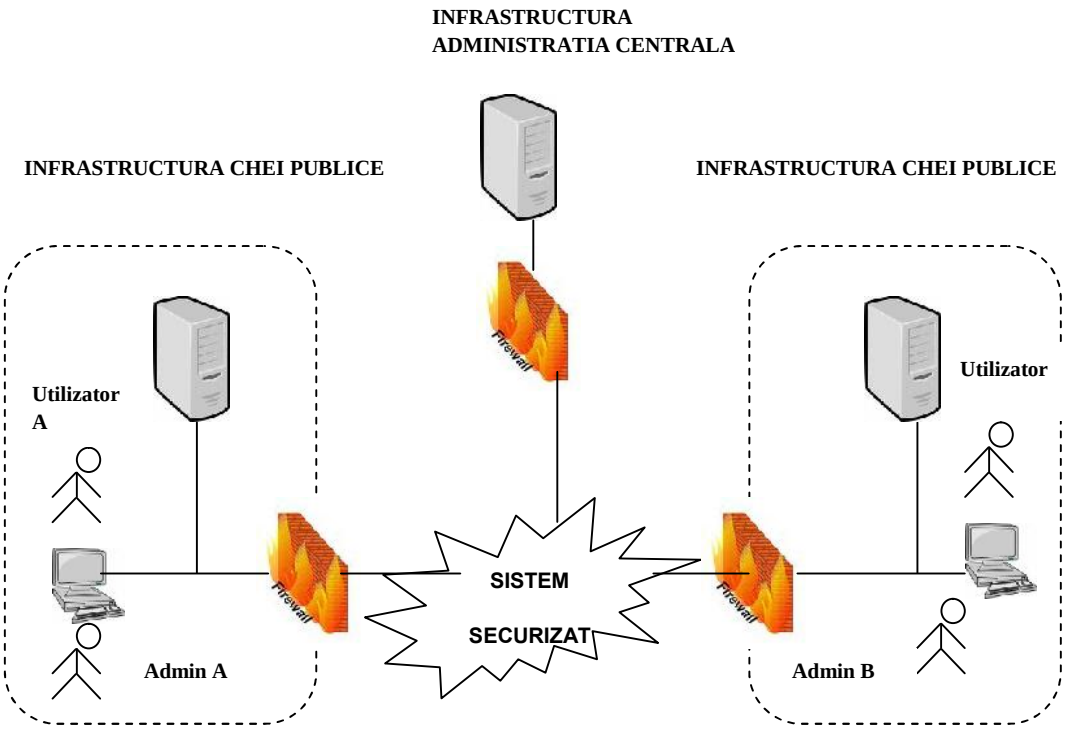
schimbul de certificate prin intermediul cross-certification
liste de certificate trust (CTL)

certificate cheie publica furnizate de sistem către fiecare membru participant, la fel ca și listele cu autorități de certificare revocate și listele cu certificate revocate
site web pentru publicarea listelor cu, certificate trust (CTL), a documentelor CP (certificate policy) și a memorandului de convenții

Arhitectura functionala a sistemului e intregita de componentele ale caror functionalitati sunt descrise in prezentul document in capitolul 3.3 – „Functionalitati ale sistemului”.

3.1.2 Arhitectura tehnică

Figura de mai jos reprezintă configurația sistemului propusă de proiectul “Dezvoltarea infrastructurii în vederea interoperabilității și accesului securizat pentru Administrația Centrală” cu două autorități de certificare CA.



Arhitectura tehnica a sistemului include totalitatea echipamentelor hardware descrise in prezentul document la capitolul 4 – “Infrastructura hardware”.

3.2 Cerinte privind serviciile de implementare a sistemului

3.2.1 Activitati

Implementarea (din punct de vedere tehnic a) sistemului vizeaza urmatoarele activitati distincte:

Numar Activitate	Denumire activitate proiect
1	Livrarea catre Beneficiar a echipamentelor hardware: • Instalarea infrastructurii hardware de suport a sistemului: o Punerea in functiune, configurarea si testarea echipamentelor; o Testarea integrata, acolo unde e cazul, a functionalitatii echipamentelor.
2	Livrarea catre Beneficiar a licentelor software aferente componentelor sistemului: • Instalarea a infrastructurii software a sistemului: o Instalarea si configurare componente; o Testarea componentelor.
3	Dezvoltarea sistemului, in cadrul componentelor software: • Analiza si proiectare: o Analiza (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 80 de zile-om pentru aceasta etapa); o Proiectare; o Elaborare specificatii de dezvoltare. • Instalare, configurare si dezvoltare in cadrul componentelor software: o Dezvoltare in cadrul componentelor software; o Integrarea componentelor in cadrul sistemului; o Deployment; o Documentare. • Testare functionala si integrata (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 70 de zile-om pentru aceasta etapa): o Integrarea sistemului cu aplicatiile/sistemele cu care acesta trebuie sa se integreze (lista completa a acestora se va definitiva in perioada de analiza aferenta implementarii sistemului); o Testare integrata; o Acceptanta.
4	Servicii de populare cu date a bazelor de date ale sistemului, care se constituie din preluarea (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 20 de zile-om pentru aceasta etapa): • datelor necesare din diverse aplicatii/baze de date (lista completa a acestora se va definitiva in perioada de analiza aferenta implementarii sistemului); • altor date necesare lansarii in folosinta a sistemului.

5	Instruire a utilizatorilor sistemului, care include (tinand cont de complexitatea activitatilor specifice beneficiarului si a calendarului incarcat al utilizatorilor acestuia implicati in etapa de analiza, ofertantii vor lua in calcul privind propriul efort un numar minim de 20 de zile-om pentru aceasta etapa): • Instruirea in clasa a utilizatorilor desemnati de Beneficiar cu ajutorul unui instructor; • Livrarea catre Beneficiar a materialelor aferente instruirii in clasa pe suport electronic.
6	Servicii de suport, care includ: • Suport acordat Beneficiarului in perioada de Go-Live a proiectului.
7	Garantie

3.2.2 Volumetrie servicii de dezvoltare

In perioada de analiza aferenta implementarii sistemului informatic sunt incluse minim urmatoarele:

Elaborarea documentelor de arhitectura functionala detaliata a sistemului (stabilire in detaliu a componentelor si sub-componentelor de lucru);
Stabilirea fluxurilor informationale intre componente/sub-componentele sistemului;
Definire tipuri de date, structuri de date, metadate;
Definirea schemelor de securitate (nivele de acces, roluri, etc,);
Definire si elaborare nomenclatoare de lucru (aproximativ 20 de nomenclatoare lucru);
Definirea fluxurilor de lucru necesare pentru operatiuni de tip aprobare, semnare, etc. (aproximativ 50 de fluxuri de lucru);
Elaborare interfete de lucru (vizualizare,aprobare, etc.);
Definire rapoarte (aproximativ 40 de rapoarte sistem);
Definirea schemelor de salvare regulata a datelor/informatiilor din punct de vedere business;
Definirea modalitatilor de indeplinire/aplicare a diverselor taskuri administrative;
Elaborare detaliata a specificatiilor de integrare ale sistemului (se va integra cu aproximativ 15 sisteme/aplicatii informatice);
Definirea specificatiilor de interfatare (se va interfata cu aproximativ 5 sisteme/aplicatii informatice);
Definirea specificatiilor pentru modulul „ajutor”;
Elaborarea detaliata a cerintelor de performanta ale sistemului;
Elaborarea detaliata a cerintelor non-functionale ale sistemului;
Definitivarea rapoartelor pentru evidentierea indicatorilor de performanta ai sistemului si a anumitor categorii de utilizatori ai acestuia;
Elaborarea propunerilor de optimizare (tuning) a sistemului;
Elaborarea specificatiilor de deployment;
Elaborarea specificatiilor scenariilor in vederea testarii;
Elaborarea specificatiilor privind documentatia aferenta sistemului, pentru toate categoriile de utilizatori ai acestuia.

3.3 Funcţionalităţi ale sistemului

3.3.1 Functionalitati software de bază

3.3.1.1 Cerințe tehnice tip server de aplicații

Cerinte generale:

Server-ul de aplicaţie trebuie să fie o platformă robustă şi agilă ce oferă suport pentru rularea de aplicaţii J2EE, simplificarea dezvoltării, performanţă ridicată şi administrare inteligentă.

Server-ul de aplicaţie trebuie să ofere suport pentru tehnologiile standard recente şi cadre de dezvoltare menite să simplifice modelul de programare.

Server-ul de aplicaţie trebuie să respecte standardul Java EE 6, să ofere suport pentru EJB 3.0, JPA (Java Persistence API) şi JDK 6.0.

Server-ul de aplicaţie trebuie să permită simplificare interoperabilităţii prin suport pentru servicii web incluzând JAX-WS, SOAP 1.2, MTOM, XOP, WS-Reliable Messaging, WS-Trust, WS-Secure Conversation, WS-Policy, şi Kerberos Token Profile.

Server-ul de aplicaţie trebuie să ofere suport WEB 2.0 .

Server-ul de aplicaţie trebuie să ofere suport pentru Session Initiation Protocol (SIP).

Server-ul de aplicaţie trebuie să permită comunicare prin mesaje asincrone utilizând un provider integrat de Java Message Service (JMS), care respectă standardul JMS 1.1.

Server-ul de aplicaţie trebuie să ofere suport pentru Java EE Connector Architecture (JCA) 1.5 pentru conectivitatea intre serverele de aplicaţii şi diferite Enterprise Information Systems (EIS).

Server-ul de aplicaţie trebuie să ofere suport pentru Java Transaction API (JTA) 1.1 pentru gestionarea tranzacţiilor.

Server-ul de aplicaţie trebuie să ofere acces autentificat şi autorizat pentru a securiza funcţii administrative şi aplicaţii.

Server-ul de aplicaţie trebuie să ofere suport pentru Resource Acces Control Facility (RACF) on z/OS, LDAP registry, Custom registry, file-based registry, sau federate registry.

Server-ul de aplicaţie trebuie ofere suport pentru Java Authorization Contract for Containers (JACC) 1.1, care să ofere securizarea resurselor gestionate de către server-ul de aplicaţie.

Server-ul de aplicaţie trebuie să ofere suport pentru dezvoltare bazată pe modele cum ar fi Spring.

Server-ul de aplicaţie trebuie să permită instalarea într-un singur pas.

Server-ul de aplicaţie trebuie să ofere integrare nativă cu o platforma de dezvoltare compatibilă.

Server-ul de aplicaţie trebuie să permită expunerea securizată a serviciilor intranet către utilizatorii de internet.

Server-ul de aplicaţie trebuie să permită utilizare securizată a serviciilor web externe de către sistemele localizate în intranet.
Server-ul de aplicaţie trebuie să permită structuri de cluster.
Server-ul de aplicaţie trebuie să poată funcţiona ca un server web, care să direcţioneze cereri din browser către aplicaţiile ce rulează pe server-ul de aplicaţii.
Server-ul de aplicaţie trebuie să permită distribuţie inteligentă a sarcinii de lucru în cluster.
Server-ul de aplicaţie trebuie să poată realiza balansarea traficului ce intră în sistem.
Server-ul de aplicaţie trebuie să ofere disponibilitate ridicată (high availability) şi rezervă (backup) în interiorul clusterului.
Server-ul de aplicaţie trebuie să ofere disponibilitate ridicată a tranzacţiilor şi backup pentru tranzacții prin replicarea informațiilor referitoare la tranzacțiile în lucru pe toate nodurile active.
Server-ul de aplicaţie trebuie să ofere mecanisme de reglare a performanţei de la nivelul serverelor până la nivelul cel mai detaliat al aplicaţiilor şi al componentelor utilizate de acestea.

Acces universal de date şi persistenţă:

Server-ul de aplicaţie trebuie să suporte standardul Java Data Base Connectivity (JDBC) API 4.0 pentru conectare la orice tip de bază de date.
Server-ul de aplicaţie trebuie să suporte Java Persistence API (JPA) pentru a asigura persistenţa şi reutilizarea obiectelor.
Server-ul de aplicaţie trebuie să suporte standardul Service Data Objects (SDO), pentru a accesa şi manipula în mod uniform date din sisteme heterogene, sub forma de obiecte de colecţii de structuri de tip arbore sau graph-uri.
Server-ul de aplicaţie trebuie să suporte Portlets conform standardului Java Specification Requests (JSR) 286 (Portlet 2.0) .
Server-ul de aplicaţie trebuie să suporte aplicaţii Session Initiation Protocol (SIP) conform standardului JSR 116.
Server-ul de aplicaţie trebuie să suporte standardele Java Servlet 2.5 (JSR 154) şi JavaServer™ Pages (JSR 245) .

Securitatea aplicaţiilor:

Server-ul de aplicaţie trebuie să ofere o granularitate ridicată.
Server-ul de aplicaţie trebuie să ofere flexibilitate de definire şi control al utilizatorilor.
Server-ul de aplicaţie trebuie să ofere capabilităţi de auditare pentru a asigura respectarea regulilor şi standardele existente în anumite domenii de activităţi.
Server-ul de aplicaţie trebuie să permită implementări de tip secure proxy pentru a putea configura mai uşor serverul de aplicaţii când acesta este utilizat în DMZ.
Server-ul de aplicaţie trebuie să ofere funcţionalităţi Single Sign-On pentru interoperabilitate îmbunătățită intre diferite aplicaţii şi medii.

Server-ul de aplicaţie trebuie să permită auditarea informaţiilor de securitate a acţiunilor administrative, cum ar fi modificări de configurări de securitate, gestionare de chei şi certificate , modificări de politici de control al accesului, etc.
Server-ul de aplicaţie trebuie să ofere administrare a securităţii îmbunătățită la nivelul consolei de administrare, cu acces pe bază de drepturile în funcţie de roluri la nivelul cell, node, cluster sau aplicaţie.

Administrare inteligentă:

Server-ul de aplicaţie trebuie să permită anticiparea şi ajustarea parametrilor critici pentru platformă.
Server-ul de aplicaţie trebuie să ofere infrastructură simplificată şi flexibilă pentru controlul eficienţei mediilor de rulare.
Server-ul de aplicaţie trebuie să ofere administrarea de la distanţă a mai multor servere de aplicaţii.
Server-ul de aplicaţie trebuie să ofere controlul mediilor complexe cu topologii complexe.
Server-ul de aplicaţie trebuie să ofere activităţi administrative simplificate pentru aplicaţiile de tip “multi-component”.
Server-ul de aplicaţie trebuie să ofere o consolă de administrare web-base pentru gestionarea centralizată a tuturor componentelor din topologii ce includ mai multe servere de aplicaţii şi/sau web.
Server-ul de aplicaţie trebuie să permită gestionare centralizată a transferului de informaţii intre medii cum ar fi: deploy, start, stop aplicaţii şi distribuirea fişierelor în topologii ce includ mai multe servere de aplicaţii şi/sau web.
Server-ul de aplicaţie trebuie să ofere capabilitatea de a realiza instalări centralizate către diferite medii remote.
Server-ul de aplicaţie trebuie să ofere posibilitatea de a grupa şi gestiona mai multe artefacte Java EE sub o singură definiţie de aplicaţie.
Server-ul de aplicaţie trebuie să ofere capabilităţi de a configura cu uşurinţă securitatea şi conectivitatea la baza de date şi un client stand-alone pentru administrarea eficientă a mediului de deployment.
Server-ul de aplicaţie trebuie să ofere scripturi avansate de administrare, care accelerează automatizarea implementărilor.
Server-ul de aplicaţie trebuie să ofere capabilităţi consolidate de administrare pentru dispozitive externe care pot fi integrate şi gestionate în mediul de servere de aplicaţii.
Server-ul de aplicaţie trebuie să ofere suport avansat de gestionare a resurselor ce constă în a alege doar funcţionalităţile necesare pentru memorie şi spaţiu, în mod dinamic, în funcţie de necesităţile aplicaţiilor care rulează, pornind doar componentele necesare aplicaţiilor ce rulează la un moment dat pe server şi astfel reducând timpul de pornire şi spaţiul alocat server-ului.
Server-ul de aplicaţie trebuie să ofere suport pentru noile standarde de Servicii Web cum ar fi:

- Web Services Interoperability Organization (WS-I) Basic Profile 1.2 şi 2.0;
- WS-I Reliable Secure Profile;
- Java API for XML Web Services (JAX-WS);
- SOAP 1.2;
- SOAP Message Transmission Optimization Mechanism (MTOM);
- XML-binary Optimized Packaging (XOP);
- WS-Reliable Messaging;
- WS-Trust;
- WS-Secure Conversation;
- WS-Policy.

3.3.1.2 Flux de lucru automatizat

Solutia trebuie sa ofere urmatoarele functionalitati:
Produsul trebuie să ofere capabilitatea ca anumiţi utilizatori să aibă privilegii de acces specifice pentru a crea, modifica şi/sau şterge un proces de flux de lucru.
Produsul trebuie să aibă capabilitatea de a iniţia procese de fluxuri de lucru bazate pe declanşatori veniţi din sisteme externe.
Produsul trebuie să aibă capabilitatea de a detecta noii angajaţi adăugaţi intr-un sistem HR sau în alte surse şi automatizează procesul de acordare a drepturilor pentru noul utilizator.
Produsul trebuie să aibă capabilitatea să automatizeze procesul de acordare sau luare a drepturilor cu sau fără un flux de lucru.
Componenta flux de lucru a produsului trebuie să fie o funcţionalitate integrată a produsului.
Componenta flux de lucru a produsului trebuie să ofere abilitatea să ridice nivelul sau să transmită acţiunile/cererile în funcţie de data la care au fost iniţiate.
Componenta flux de lucru trebuie să suporte cerinţe logice conţinute între diferite etape.
Componenta flux de lucru a produsului trebuie să permită participanţilor la fluxul de lucru să întreprindă acţiuni (aprobare / rejectare) prin intermediul unui browser web.
Componenta flux de lucru a produsului trebuie să suporte transmiterea solicitărilor folosind sisteme de mesagerie (e-mail).
Componenta flux de lucru a produsului trebuie să suporte bifurcaţii şi împreunări ale proceselor.
Componenta flux de lucru a produsului trebuie să suporte crearea unui flux de lucru cu etape multiple şi lansarea unui sub-flux de lucru.
Componenta flux de lucru a produsului trebuie să suporte procesele care pot avea sub-fluxuri de lucru sau fluxuri găzduite.
Componenta flux de lucru a produsului suportă reutilizarea proceselor/fluxurilor de lucru create.
Componenta flux de lucru a produsului trebuie să suporte transmiterea bazată pe rol către recipienţi.
Componenta flux de lucru a produsului trebuie să suporte roluri alternatoare (delegaţi)

Componenta flux de lucru a produsului trebuie să permită unei interfeţe să invoce aplicaţii externe ca să lege orice date relevante ale fluxului de lucru.
Componenta flux de lucru a produsului trebuie să ofere o interfaţă grafică pentru dezvoltarea proceselor/fluxului de lucru.

3.3.1.3 Raportare

Soluţia trebuie să ofere următoarele rapoarte standard (incluse cu soluţia):
Raport de operaţii – Raport ale tranzacţiilor operaţionale de un anumit tip (de ex. Adăugarea unui nou utilizator).
Raportul de serviciu – tranzacţiile trimise care afectează oferirea către resurse administrate (de ex server Unix).
Raport de utilizator – tranzacţiile trimise care afectează conturile utilizatorilor.
Raport de respingere – conturile respinse de către aprobatori în cadrul procesului fluxului de lucru.
Raport de reconciliere – rezultatele din reconcilierile recente ale unei resurse administrare.
Raportul conturilor inactive de către Resursa Administrativă (de ex Conturile în sisteme Unix).
Raportul conturilor – listează utilizatorii şi conturile asociate şi dacă contul se conformează politicilor curente sau nu.
Rapoartele trebuie să fie generate în timp real către utilizator/administrator.
Rapoartele trebuie redate în format pdf.
Soluţia trebuie să poată genera rapoarte configurabile.

3.3.1.4 Interfaţa cu utilizatorul

Interfaţa cu utilizatorul trebuie să fie configurabilă, permiţând: specificarea fonturilor, culorilor, localizarea tastelor de navigare, numele de afişare ale câmpurilor, amplasamentul siglelor etc.

3.3.1.5 Arhitectura de conectare

Soluţia trebuie să ofere conexiune fără agenţi, în afară de agenţii platformei locale către resurse de administrare.
Soluţia trebuie să ofere agenţi/conexiuni către următoarele resurse:

- Sistemul de operare;
- Servere de aplicaţii;
- Sisteme de Directoare;
- Baze de date;
- Acces mainframe (de ex RACF, ACF2 etc.);
- Produse de autentificare majore;
- Produse web SSO;

- Platforme de mesaje/email;
- Aplicaţii de tip help desk;
- Aplicaţii ERP;
- Aplicaţii HR.

Soluţia trebuie să includă un SDK pentru a extinde acoperirea platformelor administrate prin aplicaţii customizate şi proprietare (construite în companie).
Soluţia trebuie să permită sistemelor externe să acceseze sau să interogheze date din interiorul produsului (de ex LDAP, ODBC, JDBC etc.).
Soluţia trebuie să includă un „scheduler" pentru rularea sarcinilor programate.

3.3.1.6 Cerințe tehnice tip sistem de baza de date

Caracteristici generale:
Baza de date relaţională trebuie să suporte comunicarea cu aplicaţiile client folosind protocolul de transport pe reţea TCP/IP.
Baza de date relaţională trebuie să opereze pe sisteme incluzand cel putin Windows, Unix sau Linux.
Baza de date trebuie sa suporte aplicatii scrise in limbaje procedurale SQL caracteristice mai multor sisteme de gestiune a bazelor de date.
Baza de date trebuie să permită execuţia de instructiuni INSERT de tip multi-tabelă.
Baza de date trebuie să suporte tranzactii autonome.
Baza de date trebuie sa suporte nativ stocarea si gestiunea datelor de tip XML.
Baza de date trebuie sa ofere un mecanism inclus care sa permita interogarea istoricului modificarilor unei tabele fara a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvare periodica sau utilizarea functiei de audit.

Securitate:
Baza de date relaţională nu trebuie să permită executarea de operaţii asupra obiectelor bazei de date decât dacă utilizatorul este autorizat pentru operaţia în cauză.
Baza de date relaţională trebuie să ofere o listă cu operaţiile pe care un grup sau o clasă de utilizatori le poate executa.
Baza de date relaţională trebuie să ofere o facilitate care înregistrează informaţii despre modificări, inserări, ştergeri şi selectări ale obiectelor bazei de date de către utilizatori individuali,
Baza de date relaţională trebuie să ofere abilitatea de a se ajusta la gradul de detalii, capturate de către facilitatea de audit.
Baza de date trebuie sa ofere mecanisme incluse de restrictionare a accesului la date pe baza de etichete si politici de securitate.
Baza de date trebuie sa ofere mecanisme incluse de control granular al accesului la datele din tabele, la nivel de coloana, rand si la ambele niveluri.

Salvare şi recuperare date:

Baza de date relaţională trebuie să ofere o facilitate pentru salvarea întregii baze de date.

Baza de date relaţională trebuie să ofere o facilitate pentru restaurarea întregii baze de date.

Baza de date relaţională trebuie să ofere o facilitate pentru înregistrarea tuturor modificărilor bazei de date, pentru a permite recuperarea bazei de date (înregistrarea tranzacţiilor).

Baza de date relaţională trebuie să ofere o facilitate pentru recuperarea întregii baze de date la un moment din timp specificat de utilizator.

Baza de date relaţională trebuie să ofere abilitatea de a face salvări pentru unul sau mai multe spaţii alocate tabelelor aşa cum este specificat de către administratorul bazei de date.

Baza de date relaţională trebuie să scrie în mai multe fişiere pe disc simultan în timpul unei operaţii de salvare.

Baza de date relaţională trebuie să citească din mai multe fişiere pe disc simultan în timpul unei operaţii de restaurare.

Baza de date relaţională trebuie să permită citirea și scrierea paralelă în timpul unei operaţii de salvare.

Baza de date relaţională trebuie să permită citirea şi scrierea paralelă în timpul unei operaţii de restaurare.

Baza de date relaţională trebuie să permită o arhitectură de înaltă disponibilitate.

Performanţa şi scalabilitatea bazei de date.

Baza de date relaţională trebuie să permită folosirea ei în sisteme cluster.

Baza de date relaţională trebuie să ofere abilitatea să partiţioneze tabele si indecsi.

Baza de date relaţională trebuie să permită unui tabel să fie partiţionat bazându-se pe una sau mai multe valori specifice de date, aşa cum este hotărât de către administratorul bazei de date.

Baza de date relaţională trebuie să permită definirea cantităţii minime de date transferate între disc și memoria locală a bazei de date la o cerere.

Baza de date relaţională trebuie să ofere facilitatea să reţină date din tabele special indicate în memoria locală pentru o perioadă nedefinită de timp.

Baza de date relaţională trebuie să permită setarea mărimii unei zone din memoria locală, rezervată să reţină date din tabele special indicate, pentru o perioadă nedefinită de timp.

Baza de date relaţională trebuie să aibă un optimizator bazat pe cost pentru a optimiza interogările.

Instanţe multiple, izolate, şi complet funcţionale ale bazei de date trebuie să poată coexista pe un singur nod SMP.

Baza de date relaţională trebuie să suporte indecşi.

Baza de date trebuie sa permita reorganizarea, mutarea si redefinirea de tabele fara blocarea activitatii.

Baza de date trebuie să permita ajustarea automata, atat in plus cat si in minus, a memoriei alocate, in functie de cerintele din baza de date si de memoria disponibila in sistem.

Baza de date trebuie să se ajusteze automat in cazul suplimentarii spaţiului de stocare.

Baza de date trebuie sa permita gestionarea dinamica a stocarii datelor in functie de frecventa de acces la date, astfel incat datele frecvent accesate sa fie stocate pe discuri rapide, iar datele mai rar accesate pe discuri lente.
Baza de date trebuie să permita organizarea fizică a inregistrarilor din tabele in ordinea data de o coloană, mai multe coloane, si mai multe grupuri de coloane.

Integritate date:
Baza de date relaţională trebuie să identifice şi să rezolve situaţiile de blocaj (deadlock).
Baza de date relaţională trebuie să permită administratorului să impună constrângeri de tip cheie primara.
Baza de date relaţională trebuie să permită ca o coloană să nu accepte valori NULL.
Baza de date relaţională trebuie să ofere abilitatea de a impune constrângeri asupra valorilor datelor.

Dicţionar de date:
Baza de date relaţională trebuie să ofere o facilitate de catalog (sau dicţionar de date) care este modificată automat de fiecare dată când instrucţiuni de tipul Data Definition Language (DDL – Limbajul de definire a datelor) se aplică pe aceea bază de date.
Baza de date relaţională trebuie să ofere o facilitate pe platforma instalată pentru a accesa catalogul şi a obţine informaţii legate de obiectele bazei de date.

Administrare:
Baza de date relaţională trebuie să ofere o interfata de administrare si dezvoltare a bazei de date.
Baza de date relaţională trebuie să aibă implementată o soluţie internă bazei de date pentru comprimare în momentul execuţiei operaţiei de backup.
Baza de date relaţională trebuie să includa facilităţi de replicare între două baze de date de acelaşi tip.

3.3.1.7 Virtualizare

Solutia va include o platforma de virtualizare dedicata, bazata pe Hypervizor propriu, fara dependenta de un sistem de operare anume. Aceasta solutie va fi instalata direct in platforma de procesare si va beneficia de suportul acestei platforme atat la nivelul capacitatii de procesare cat si la nivelul optiunilor de conectica si integrare cu restul elementelor de infrastructura.

Platforma de virtualizare trebuie sa fie compatibila cu toti producatorii hardware recunoscuti: IBM, Dell, HP, Sun, Intel, iar hypervizorul pe care aceasta plaforma se bazeaza

trebuie sa fie independent de producatorul sau de metoda de stocare interna/externa disponibila in platforma de procesare si/sau stocare pe care ruleaza.

Platforma de virtualizare trebuie sa ofere suport pentru urmatoarele sisteme de operare instalabile in masina virtuala: Windows Xp/Vista/7/2003/2008/2008 R2, Linux Suse/Red Hat/CentOS, FreeBSD, Solaris, Netware si sa permita adaugarea de spatiu de stocare pentru masinile virtuale prin folosirea urmatoarelor protocoale : NAS – NFS/CIFS ; SAN – iSCSI/FCP si prin folosirea urmatoarelor sisteme de fisiere : FAT32, NTFS, EXT2, EXT3, asigurand astfel compatibilitate cu majoritatea tehnologiilor implementate in mod uzual atat in platformele de procesare cat si in platformele de stocare.

Componentele virtuale ale platformei sa poata fi modificate cu usurinta permitand astfel crearea de configuratii diferite pentru seturi comune de masini virtuale, precum si crearea de configuratii unitare la nivelul intregii infrastructure virtuale, atat din prisma elementelor virtuale de procesare si stocare (integrate nativ in platforma sau prin integrarea nativa cu componente terte ale respectivelor platforme de proceare si stocare), cat si din prisma elementelor de comunicatie (posibilitatea integrarii directe cu platforma de retea aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de retea si asigurarea crearii unei retele virtuale unificate la nivelul intregii infrastructuri virtuale).

Platforma de virtualizare trebuie sa ofere mecanisme proprietare pentru adaugarea de resurse de procesare si memorie fara restartarea sistemului de operare din masina virtuala, (in masura in care sistemul de operare suporta aceste facilitati), mecanisme ce pot fi independente de platformele de procesare/stocare/comunicatie sau prin intermediul unor conectori/componente comune respectivelor platforme.

Resursele virtuale (resurse de procesare, stocare si comunicatie) disponibile la nivelul intregii platforme de virtualizare (prin integrarea nativa cu platformele fizice de procesare, stocare si comunicatie) trebuie sa fie adresabile si configurabile in totalitatea lor prin intermediul unei singure interfete de management si nu prin configurarea separata pentru fiecare echipament disponibil in respectivele platforme.

Platforma trebuie sa permita gruparea si organizarea logica a resurselor de procesare in functie de necesitati, precum si izolarea acestor grupari de resurse, respectiv sa asigure flexibilitatea necesara maririi cantitatii de resurse disponibile intr-o grupare prin extragerea de resurse din alte grupari.Accesul masinilor virtuale si apartenenta la aceste grupari de resurse trebuie sa se faca atat in mod manual prin interventia unui operator cat si pe baza unor politici dinamice de acces.

Prin integrarea nativa cu platformele de procesare, masinile virtuale definite in platforma de virtualizare trebuie sa beneficieze concomitent de suportul a minim 8 procesoare logice, minim 256GB de RAM si acces la totalitatea porturilor I/O, resurse adresabile virtual prin abstractizarea resurselor fizice disponibile in infrastructura.

Platforma trebuie sa ofere mecanisme integrate de balansare a incarcarii resurselor fizice si virtuale disponibile in infrastructura si redistribuire a sarcinilor generate de utilizatori, servicii si aplicatii, prin integrarea nativa cu platformele hardware, indiferent de producatorul respectivelor elemente de infrastructura.Aceste mecanisme trebuie sa fie disponibile atat la comanda prin interventia unui operator cat si prin operatiuni automate definite in functie de necesitati, gradul de ocupare al resurselor si/sau pe baza unor reguli/politici prestabilite

Platforma de virtualizare trebuie sa ofere redundanta completa a arhitecturii, atat la nivelul elementelor virtuale distincte (procesoare, memorie, elemente de comunicatie, masini virtuale, etc) cat si la nivelul unor seturi intregi de echipamente de infrastructura (platforma de procesare, platforma de stocare, platform de comunicatie, etc) prin integrarea nativa cu mecanismele redundante existente in aceste platforme si prin folosirea unor tehnologii proprietare de redundanta, balansare si fail-over aplicabile intregului spectru de functionalitate asigurata (masini virtuale, servcii, aplicatii, platforme de procesare, platforme de stocare, platforme de comunicatie).

Platforma de virtualizare trebuie sa permita configurarea spatiului de stocare virtual prin integrarea directa cu platforma de stocare aleasa prin intermediul unor conectori/componente proprietare sau de la producatorul platformei de stocare, mecansim ce va permite extinderea discurilor virtuale fara a fi necesara oprirea masinilor virtuale ce au atasate aceste discuri.

Prin integrarea cu resursele de management, platforma de virtualizare trebuie sa permita mecanisme integrate de mutare a masinilor virtuale de pe un server pe altul sau dintr-un datacenter in altul fara oprirea sistemului de operare ce ruleaza in masina virtuala si fara intreruperea serviciului oferit de aplicatia/aplicatiile din masina virtuala.Aceleasi mecanisme trebuie sa permita atat mutarea intregului harddisk virtual concomitent pentru oricare masina virtuala in cadrul aceluiasi datacenter sau intre datacenter-e diferite, independent de platforma de stocare folosita si de mecanismele de replicare ale acesteia, precum si extinderea automata a harddisk-urilor virtuale pe masura ce sistemul de operare si aplicatiile din masinile virtuale o cer.In acest fel vor deveni posibile scenarii automate, prin politici pre-definite/definibile, de consolidare a masinilor virtuale pe un numar prestabilit de servere oprirea automata a serverele fara activitate sau cu subutilizare a resurselor de procesare.

Platforma trebuie sa includa o componenta de administrare si monitorizare dedicata, disponibila atat la nivelul echipamentelor fizice ce alcatuiesc platformele de procesare, stocare si comunicatie cat si la nivelul masinilor virtuale, ale resurselor virtualizate, aplicatiilor, serviciilor si protocoalelor insumate in infrastructura.In vederea accesului facil la functiile de administrare si monitorizare oferite, platforma trebuie sa permita acces atat prin consola locala/la distanta cat si prin browser web si prin platforma de management dedicata.

Componenta de management si monitorizare a infrastructurii trebuie sa permita autentificarea utilizatorilor bazata pe roluri si privilegii distincte de utilizare, prin integrarea cu un serviciu de tip director. Deasemenea trebuie sa permita crearea facila de politici dinamice de acces la resursele de procesare, precum si de disponibilitate ale acestora.

Separarea privilegiilor administrative trebuie sa se poata face pe orice element disponibil in interfata de administrare (server, utilizator, resursa de procesare, stocare, retea, etc), permitand astfel crearea de zone/domenii de securitate in functie de aplicatii si/sau roluri functionale, nu in functie de elementele disponibile in infrastructura de procesare, stocare si comunicatie.

Platforma de management trebuie sa asigure si mecanisme de definire si aplicare a profilelor standard de configuratie pentru serverele ce fac parte din infrastructura virtuala. Deasemenea sa permita configurarea de politici de aplicare a acestor profile in functie de necesitatile de moment sau in concordanta cu politica stabilita in prealabil.

Componenta de management trebuie sa se integreze nativ sau prin intermediul unor conectori/componente cu platforma de procesare si cu platforma de stocare in vederea realizarii operatiunilor de backup direct din aceste platforme, precum si pentru crearea rapida a unor zone izolate atat din punct de vedere al securitatii cat si al gruparilor de resurse de procesare, stocare si retea, in scopul testarii si dezvoltarii.

Se vor include licentele de folosire solutiei de virtualizare a resurselor de procesare, corelate cu modul de licentiere al producatorului, care sa ofere suport pentru toate procesoarele folosite in componentele de multi-procesare simetrica din infrastructura hardware a sistemului.

3.3.1.8 Salvare si restaurare date

Sistemul va include o componenta performanta pentru salvarea si datelor - produs software pentru protecţia continuă a datelor cu posibilitati de salvare în sistem de disaster recovery - care va indeplini urmatoarele cerinte minimale:

Soluţia trebuie să permita ca de pe aceeasi consola centrala să se poata administra mai multe locatii.
Soluţia trebuie să fie modulara, cu posibilitati de extindere.
Soluţia să fie certificata de producator.
Soluţia trebuie să detina o consola centralizata cu interfaţa grafică intuitivă.
Accesul la consola trebuie să fie securizat cu autentificare bazate pe nume utilizator şi parola.
Sa se adreseze afacerilor desfasurate în medii eterogene.

Consola centralizată trebuie să permita administrarea şi monitorizarea mai multor servere de backup într-o retea distribuită sau din locatii aflate la distanta, precum şi toate joburile şi dispozitivele fizice de stocare existente pe aceste servere.
Soluţia trebuie să ofere suport pentru:

- Sistemul de operare Microsoft Windows XP, Windows Server 2003 R2, Windows Server 2008 R2, 7 pe 32 de biţi şi 64 biţi - inclusiv registrii şi starea sistemului, precum şi în configuraţii cluster,
- Distribuţii Linux,
- UNIX.

Soluţia trebuie să permita instalarea remote a agenţilor şi optiunilor din consola de administrare.
Soluţia trebuie să permită administrarea dispozitivele de stocare din multiple locatii fizice, inclusiv librariile şi mediile de stocare decuplate.
Soluția sa permita backup de tip mirror, backup care sa poate fi realizat la locatii diferite simultan, pentru a asigura un nivel ridicat de protectie a datelor.

Soluţia trebuie să permita administrarea extinsa a erorilor hardware, să corecteze erorile pentru a realiza completarea backup-ului, să permita detectarea şi îndreptarea facilă a oricarui tip de eroare hardware.

Soluţia trebuie să permita utilizatorilor verificarea şi corectarea problemelor legate de securitate, disponibilitatea mediilor de stocare sau a conectarilor din retea, inainte de a rula operaţiunile de backup.
Soluţia trebuie să permita posibilitatea de a defini politici de filtrare şi sabloane care să defineasca atributele job-urilor ce vor fi executate.
Soluţia trebuie să permita asistenti (wizard) pentru operatiile importante:

- instalare,
- creare joburi de backup/recovery,
- formatare medii de stocare.

Soluţia trebuie să permita posibilitatea de a face backup pe o retea secundara.
Soluţia trebuie să permita reincercarea job-urilor esuate, cu rutarea lor catre medii alternative.
Soluţia trebuie să permita notificarea automata folosind Microsoft Exchange, SMTP, SNMP şi verificarea CRC („cyclic redundancy check”) a datelor.
Soluţia trebuie să permita stergerea automată a log-urilor şi cataloagelor vechi, cu posibilitatea de definire a perioadei de retinere pentru acestea.
Soluţia trebuie să permita posibilitatea de restaurare a sistemului de operare şi a aplicaţiilor deja instalate, inclusiv configurarile existente, utilizând banda sau CD (tape/cd boot).
Soluţia trebuie să permită posibilitatea de a realiza backup de pe clienţi (statiile de lucru).
Soluţia trebuie să permită capacitatea de multiplexing ce permite până la 32 de servicii de scriere simultană pe acelaşi support media.

Soluţia trebuie să permita utilizarea SAN-urilor Fibre Channel pentru backup şi recuperare.
Optiuni de Disaster Recovery - Soluţia trebuie să permita posibilitatea restaurării serverelor din reţea, fără a fi nevoie reinstalarea sistemul de operare sau softului de backup.
Optiunea de Open Files - Soluţia trebuie să permita cu ajutorul acestui agent ca aplicațiile să poată rula fară intrerupere în timpul salvării datelor.
Soluţia trebuie să permita administratorilor să faca operţtii de backup şi restore pentru device- urile de tip NAS. Soluţia de backup să permita efectuarea backup-ul pe tape-uri sau librarii atasate direct device-urilor NAS.
Soluţia trebuie să asigure protecţia continua a datelor şi care să restaureze datele corupte de virusi, erori software sau erori umane prin capabilitatea de a relua datele de la un moment imediat anterior inainte de coruperea acestora.
Instalarea şi mentenanţa acestui software se va face de personal tehnic de specialitate al prestatorului certificat de către producător - cel puţin 2 specialişti certificaţi de producator – (se vor prezenta diplome, acorduri si/sau atestari) astfel incât să poata fi urmarite eventualele defectiuni şi să fie remediate imediat ce au fost semnalate în sistem.
Se va prezenta de către Prestator atestare pentru abilitatea de a sustine traininguri cu personalul beneficiarului pentru produsele instalate în sistem.
Se va prezenta de catre Prestator o solutie demo care sa prezinta modul in care cerintele enuntate au fost indeplinite de solutia ofertata.

Se vor include licenţe dimensionate pentru nevoile sistemului, corelate cu modul de licentiere al producatorului, incluzandu-se totodata si şi subscriptii pentru actualizări software din partea producătorului aplicaţiei pentru minim 1 an fără costuri suplimentare din partea beneficiarului.

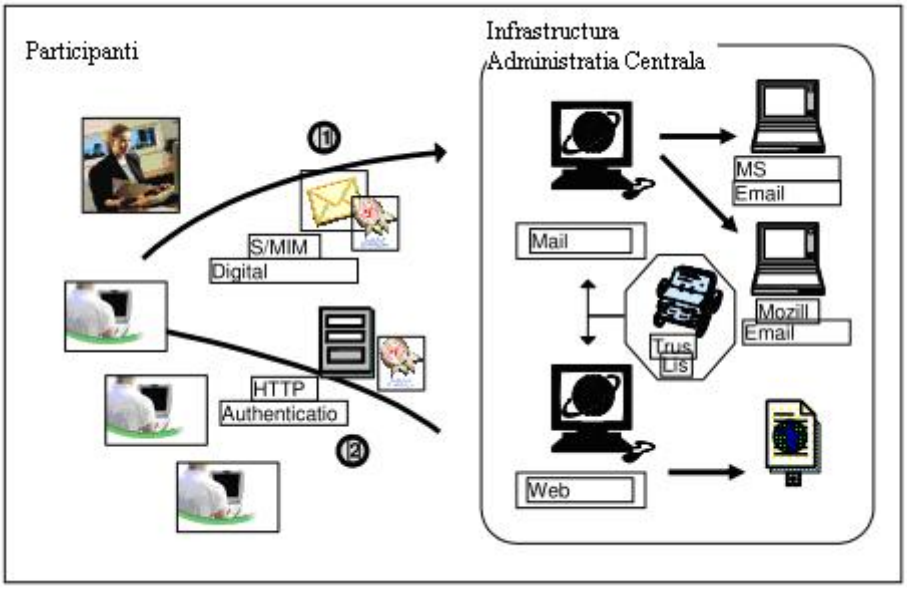
3.3.2 Funcţionalităţi front-office şi back-office

Funcționalități TL (Trust List) și acțiuni ale Administrației Centrale:

emiterea unei liste trust (TL)
listarea conținutului unei liste trust
adăugarea unui certificat al unei autorități de certificare la lista trust
eliminarea unui certificat al unei autorități de certificare din lista trust
validarea semnăturii listei trust

Etapele urmate de un participant CA în vederea realizării interoperabilității:

enrolmentul
importarea listei trust intr-o aplicație (Outlook, Mozilla)
transmiterea unui mesaj via S/MIME către sistemul Administrației Centrale
conectarea la sistem utilizând certificatul
resemnarea și publicarea listei trust



3.3.2.1 Validare

Validarea unui certificat necesită verificarea stării certificatului. Aceasta se poate realiza cu ajutorul listei CRL (Certificate Revocation List) sau/și prin serviciul on-line OCSP (Online Certificate Status Protocol).

Procedura exactă pentru verificarea certificatului, depinde totuși de autoritatea de certificare ce a emis certificatul și de certificatele corespunzătoare corespondente.

3.3.2.2 Functionalitati de baza

Abstractizarea / Translatarea Adresei de Reţea - Toate adresele interne trebuie să fie abstractizate, translatare sau ascunse utilizatorilor finali care accesează aplicaţii interne
Abstractizarea / Translatarea Namespace/URL - Serverul Reverse Proxy trebuie să abstractizeze, translateze și să ascundă numele de sistem şi url-urile interne. Este necesară capabilitatea de mapare între numele intern şi extern al URL-ului. Maparea trebuie să se aplice URL-ului tuturor cererilor, redirecţionărilor, linkurilor şi conţinutului afişat.
Suport pentru autentificare globală (SSO) - Mecanismul Reverse Proxy trebuie să ofere mecanisme pentru autentificare globală. Trebuie să ofere posibilitatea de efectuare a mai multor operaţii de autorizare pentru resurse sau aplicaţii diferite fără să fie necesară reautentificarea utilizatorului dacă noua resursă sau aplicaţie necesită un nivel mai ridicat de autentificare.
Suport pentru autentificare globală (SSO) - Mecanismul Reverse Proxy trebuie să ofere mecanisme pentru autentificare globală. Trebuie să ofere posibilitatea de efectuare a mai multor operaţii de autorizare pentru resurse sau aplicaţii diferite fără să fie necesară reautentificarea utilizatorului dacă noua resursă sau aplicaţie necesită un nivel mai ridicat de autentificare.

Accelerarea Criptării/Decriptării SSL - Mecanismul Reverse Proxy trebuie să suporte mecanisme de criptare/decriptare hardware pentru a îmbunătăţi performanţa SSL.
Accelerarea Criptării/Decriptării SSL - Mecanismul Reverse Proxy trebuie să suporte mecanisme de criptare/decriptare hardware pentru a îmbunătăţi performanţa SSL.
Suport pentru Split SSL Certificate - Mecanismul Reverse Proxy trebuie să ofere serverului suport pentru certificate SSL pentru sisteme client externe.
Mecanisme de criptare - Produsul trebuie să suporte următoarele mecanisme de criptare:

- 40-bit RC2
- 128-bit RC2
- 40-bit RC4
- 128-bit RC4
- 40-Data Encryption Standard (DES)
- 56-bit DES
- 168-bit triple DES

3.3.2.3 Scalabilitate

Mecanismul Reverse Proxy trebuie să fie scalabil pentru a suporta zeci de mii de sesiuni simultane.

3.3.2.4 Securitate

Legătură prin proxy - Toate conexiunile prin reţea către resurse şi aplicaţii din zona DMZ sau interne trebuie să fie iniţiate de la serverul reverse proxy. Adresele de reţea sau “namespace-urile” externe ale clienţilor nu vor fi permise în DMZ sau în serverele interne de web sau de aplicaţii. Serverul reverse proxy trebuie, în caz de eroare, să intre într-un mod de siguranţă sau de blocare a accesului, nu într-un mod “pass-thru.”
Metode de autentificare - Serverul reverse proxy trebuie să suporte următoarele metode de autentificare:

- Nume de utilizator/parolă;
- Certificate Client x.509 ;
- Autentificare RSA SecureID;
- Autentificare NTLM;
- LDAP.

Suport pentru autentificare cu doi actori de autentificare - Serverul reverse proxy trebuie să suporte autentificare cu doi factori prin RSA SecureID hardware tokens şi combinarea a două metode de autentificare cu factor singular precum certificatele X.509 şi nume de utilizator/parolă.

Impunerea criptării - Soluţia trebuie să permită definirea politicilor de securitate pentru a defini la orice nivel cerinţa criptării sesiunii.
Politici și Restricționări - Soluţia trebuie să includă politici de securitate configurabile care să permită impunerea de restricţii de acces în funcție de interval de timp, adresa IP sau clase de adrese pentru a limita accesul la resurse. Soluţia trebuie să includă politici care să permită accesul utilizatorilor doar la acele resurse protejate pe care au dreptul să le acceseze, în funcție de rolul lor în organizaţie.
Integrare LDAP și Server de aplicaţii - Soluţia trebuie să conţină un server de directoare LDAP pentru administrarea utilizatorilor şi să se integreze nativ cu serverul de aplicaţii.
Administrare centralizată - Soluţia trebuie să ofere administrare centralizată bazată pe tehnologie web pentru administrarea utilizatorilor, grupurilor, rolurilor, permisiunilor, politicilor, domeniilor, resurselor protejate etc.
Delegarea administrării - Soluţia trebuie să ofere un model administrativ flexibil care să permită mai multe niveluri de administrare precum şi delegarea administrării.

3.3.2.5 Disponibilitate

Integrare cu mecanisme de balansare a sarcinii - Serverul Reverse Proxy trebuie să coexiste şi să opereze în spatele oricărei soluţii de balansare a încărcării pentru a echilibra traficul şi a oferi disponibilitate ridicată a sistemului.
Suport pentru centre de date multiple - Serverul Reverse Proxy trebuie să suporte capabilitatea de a migra suportul pentru aplicaţie către alte servere proxy dintr-un centru de date alternativ sau dintr-un alt punct de conectivitate în eventualitatea unei probleme majore sau al unui eveniment de întreţinere.

3.3.2.6 Monitorizare/Raportare

Auditare şi Raportare - Soluţia trebuie să includă mecanisme de auditare pentru toate evenimentele de autentificare, autorizare şi administrare, precum şi avertizări legate de componentele soluției, incluzând:

- Logări reuşite;
- Logări nereuşite;
- Conturile blocate ;
- Mesaje de violare;
- Toate încercările de acces;
- Erorile de autorizare;
- Utilizatorii anonimi;
- Identificarea creării, modificării sau ştergerii ;
- Crearea, modificarea şi ştergerea politicii;
- Evenimente suspicioase;
- Urmărirea utilizatorilor anonimi;

- Înregistrările de audit vor fi scrise în format XML în fişiere ASCII neformatate.

Istoricul schimbării/ reconfigurării - Soluţia trebuie să păstreze istoricul modificărilor configuraţiei pentru administrarea configurării şi pentru scopuri de investigare a eventualelor evenimente de securitate.
Administrarea log-urilor - Soluţia trebuie să suporte arhivarea log-urilor de evenimente/alerte precum şi funcţionalităţi de export a acestora. Log-urile trebuie reținute pe termen lung şi informaţia din log-uri trebuie să fie exportabilă în formate pentru post-procesare şi analiză.

3.3.3 Managementul utilizatorilor și accesul la sistem

3.3.3.1 Administrarea conturilor de utilizator

Sistemul trebuie să aibă implementate următoarele facilități:

trebuie să asigure că fiecare cont de utilizator are un ID unic.
trebuie să ofere reguli configurabile pentru crearea identificatorilor unici.
să permită utilizarea unei date de expirare care poate fi utilizată pentru a urmări înnoirea / ştergerea / modificarea conturilor de utilizator.
să suporte expirarea conturilor de utilizator pentru diferite tipuri de utilizatori folosind o dată de expirare a contului sau o dată de terminare a contractului
trebuie să permită notificarea prin email a proprietarului oricărui cont care a fost inactiv pentru o perioadă configurabilă.
trebuie să ofere o politică de revocare/ştergere a conturilor inactive în cadrul unei perioade configurabile.
trebuie să ofere capabilitatea de a exporta/importa utilizatori.
trebuie să ofere capabilitatea de a aproba în mod automat orice solicitare printr-un set de reguli şi politici.
să ofere capabilitatea de a vizualiza o solicitare de cont care a fost trimisă şi datele asociate cu acea solicitare.
trebuie să permită ca grupurile de utilizatori să fie create dintr-o interfaţă web.

3.3.3.2 Crearea de reguli bazate pe rol

Sistemul trebuie să suporte crearea de „roluri” după cum urmează:

Suportarea atribuirii utilizatorilor către mai multe roluri.
Suportarea atribuirii utilizatorilor către roluri ierarhice.
Oferirea capabilităţii de a specifica roluri care exclud alte roluri pentru a preveni atribuirea de roluri care s-ar afla în conflict.

Soluţia permite utilizarea sistemelor de informaţii cheie din mediul organizaţiei ca sursă de informaţii de încredere despre informaţii de identitate pentru a genera crearea automată de conturi (de ex detectarea noilor angajaţi adăugaţi şi crearea automată de conturi pentru noii angajaţi în funcţie de rolul lor în organizaţie).
Poate atribui unor utilizatori drepturi de acces diferite de cele corespunzătoare rolurilor respectivilor utilizatori.
Atribuie utilizatorilor drepturi de acces individuale pe lângă cele definite în cadrul rolului.
Poate schimba dinamic şi automat drepturile de acces în funcţie de schimbările din rolurile utilizatorilor.
Generează ID-uri de utilizator unice, în conformitate cu politicile organizaţiei.
Suportă noţiunea de „roluri persistente” (adică schimbările făcute definiţiei unui rol sunt aplicate tuturor utilizatorilor sub acelaşi rol).
Suportă mutarea unui utilizator dintr-un rol în altul, impactul fiind modificarea drepturilor de acces corespunzătoare noului rol.
Suportă „roluri” flexibile.
Suportă introducerea drepturilor de utilizator arbitrare ca parte a procesului de oferire de drepturi.
trebuie să suporte opţiuni multiple de anulare a drepturilor (precum oprirea dar lăsarea conturilor intacte, ştergerea conturilor dar păstrarea identităţii utilizatorului, sau ştergerea cu totul a utilizatorului).
trebuie să suporte descoperirea automată şi rezolvarea inadvertenţelor de informaţii de identitate dispersate pe mai multe resurse (de exemplu, sincronizarea datelor între mai multe directoare, baze de date şi fişiere).

3.3.3.3 Delegarea administrării

Sistemul trebuie să ofere capabilităţi de administrare granulară delegată precum politici de informaţie internă de control al accesului (ACI) care limitează atât accesul utilizatorului cât şi al administratorului la rapoarte, informaţii ale utilizatorilor, şi funcţii operaţionale, cu rubrici specifice „Permis” şi „Nepermis” pentru toate atributele şi operaţiile de identitate (ştergere, transfer, căutare, recuperare, suspendare, adăugare şi modificare).
Trebuie să ofere abilitatea de a propaga utilizatorii desemnaţi (administratorii delegaţi) în funcţie de rol sau în funcţie de un set de atribute configurabile.
Trebuie să permită sarcinilor administrative n niveluri de profunzime.
Produsul trebuie să fie capabil să lucreze în medii izolate (reţele izolate prin firewall-uri etc.).
Produsul trebuie să utilizeze tehnologia internet (email şi pagini web) pentru a facilita fluxurile de lucru de aprobare.

3.3.3.4 Administrarea parolelor

Produsul trebuie să ofere funcţii de resetări de parole ale conturile pe platformele administrate.
Produsul sincronizează parolele pentru utilizatori imediat ce utilizatorul şi-a schimbat parola.
Pentru administrarea parolei (resetare şi sincronizare), produsul trebuie să includă o notificare de operație reuşite/nereuşită).
Produsul trebuie să trimită o notificare email către un utilizator într-o manieră configurabilă cu un număr de zile înainte ca parola/contul său să expire.
Produsul trebuie să poată să genereze în mod aleator parola iniţială a unui cont de utilizator.
Produsul trebuie să aibă abilitatea să genereze o parolă pentru utilizarea în accesul iniţial al sistemului.
Produsul trebuie să poată forţa utilizatorul să schimbe parola resetată după prima folosire.
Produsul trebuie să aibă abilitatea de a impune anumite combinaţii configurabile de caractere alfa şi numerice într-o parolă.
Atunci când utilizatorii schimbă sau sincronizează parole, produsul poate impune politica parolei (lungime, nr. caractere alfanumerice, caractere neacceptate etc.).
Produsul trebuie să suporte o listă de parole restricţionate pentru a nu permite utilizatorilor să selecteze cuvinte comune.
Produsul trebuie să poată menţine un istoric al parolelor configurabil pentru a evita reutilizarea parolei.
Produsul trebuie să ofere capabilitatea de a genera parole ca un set aleatoriu de numere şi caractere cu lungime configurabilă.
Produsul trebuie să suporte un număr configurabil de întrebări pentru recuperarea eventualitatea unei parole uitate. Numărul și conţinutul întrebărilor și răspunsurilor trebuie să poată fi configurat de către fiecare utilizator.

3.3.3.5 Controlul accesului

Soluţia de control al accesului utilizatorilor trebuie să ofere şi să suporte următoarele tehnologii fundamentale:

Suport pentru autentificare.
Autorizare: soluţia trebuie să asigure autorizarea prin utilizarea următoarelor mecanisme:

- Propriul serviciu de autorizare;
- Liste de control al accesului (ACL), politici de obiect protejat (POP) şi reguli de autorizare pentru control al accesului la nivel scăzut;
- Autorizarea API bazată pe standarde, folosind un API pentru aplicaţiile de limbaj C, şi Java Auhentication & Authorization Service (JAAS) pentru aplicaţiile Java;
- Capabilitate pentru serviciu de autorizare externă.

Calitatea protecţiei: este gradul în care soluţia protejează orice informaţia transferată între client şi server.
Calitatea protecţiei datelor este determinată de către efectul combinat al standardelor de criptare şi al algoritmilor de detectare a modificărilor:

- Comunicare prin folosirea protocolului de control al transmisiei (TCP) standard (nu oferă protecţie);
- Integritatea datelor – protejează mesajele (fluxurile de date) împotriva modificărilor din timpul comunicării pe reţea;
- Secretul datelor – protejează mesajele împotriva modificărilor sau inspecţiilor din timpul comunicării pe reţea).

Soluţia trebuie să suporte integritatea datelor şi secretul datelor oferite de către protocolul de comunicare Secure Sockets Layer (SSL). Tipurile de chei de criptare suportate sunt următoarele:

- 40-bit RC2;
- 128-bit RC2;
- 40-bit RC4;
- 128-bit RC4;
- 40-Data Encryption Standard (DES);
- 56-bit DES;
- 168-bit tribple DES.

Suport pentru scalabilitate.
Responsabilitate: soluţia trebuie să ofere capabilităţi puternice de logare şi auditare.
Suport pentru administrare centralizată.
Browser suportate - Produsul trebuie să funcţioneze cu browser-ele Mozilla Firefox şi Microsoft Internet Explorer.
Platforme suportate:

- Microsoft Windows Server;
- Red Hat Enterprise Linux ;
- Sun Solaris;

Certificare - Produsul trebuie să fie certificat conform Common Criteria Certification EAL3 pentru a îndeplini standarde de securitate riguroase, recunoscute la nivel internaţional.

3.3.4 Functionalitati de semnare centralizata de documente si de autentificare de tranzactii

- Arhitectura functionala interna flexibila bazata pe componente/module, care va permite deservirea de multiple instante de tip server de semnare digitala, cu certificate digitale X.509v3 si de validare a documentelor semnate, de pe aceeasi platforma hardware;

- Solutia va oferi servicii integrate de gestiune a cheilor, atat pentru algoritmi simetrici cat si pentru mecanisme de cifru asimetric, care vor putea arbitra accesul aplicatiilor beneficiare la materialul criptografic necesar;
- Va putea utiliza un sistem standard si performant de gestiune a bazelor de date, pentru stocarea datelor obiect certificate prin marcare temporala si semnatura digitala, precum si a datelor de context (meta-data) relevante;
- Solutia va include functionalitate interna de gestiune a bazelor de date, dar va putea fi configurata si sa lucreze cu sisteme externe standard, respectiv cel putin cu Oracle, MySQL, PostgreSQL;
- Va permite utilizarea de algoritm RSA, pana la cel putin 4096 bit, si va asigura suport pentru ECDSA (curbe standard, specific identificate);
- Va permite utlizarea a diversi algoritmi de hashing, respectiv cel putin MD5, SHA-1, SHA-2;
- Va oferi functionalitati interne integrate de marcare temporala, in conformitate cu RFC 3161, precum si de validare automata a valabilitatii certificatelor digitale de verificare relevante, atat prin metode de tip catalog (CRL si asimilate), cat si de tip tranzactional (OCSP si asimilate);
- Accesul la functiile specifice va putea fi configurat atat pe baza de Web Services, cat si in mod HTTP, pentru incarcare si semnare punctuala de documente;
- Va include sub-module pre-configurate pentru semnarea si marcarea temporala a formatelor de documente folosite in mod uzual pentru publicare si/sau pentru schimbul de informatie, respectiv cel putin pentru formate PDF, documente XML, formate deschise derivate, precum ODF, OOXML;
- Va permite semnarea de documente/fisiere generice prin mecanisme standardizate, respectiv cel putin PKCS#7;
- Va oferi, inclus in oferta, un API prin care sa se poata crea noi module specifice configurate pentru semnarea de alte formate de document;
- Va include, in configuratia oferita, module de validare a documentelor semnate, cu suport nativ de validare in format XML, precum si cu capacitatea de a crea module noi de validare;
- Va include mecanisme de instalare si configurare, precum si interfata grafica de administrare de pe statiile de management dedicate;
- Va include interfete standardizate pentru interactiune controlata programatic, in mod ne-asistat, inclusiv API Java, cu suport HTTP si Web Services, dar si in linie comanda;
- Va include module criptografice interne amovbile, de tip HSM (cel putin unul, pentru fiecare echipament / instanta), pentru suport criptografic hardware destinat procesarii rutinelor specifice, respectiv cel putin generarii cheilor si procesarii algoritmilor criptografici exclusiv in hardware;

- Modulul HSM inclus va avea implementare criptografica certficiata FIPS 140-2 Level 3 si va asigura suport nativ pentru generare numere aleatorii pentru material criptografic, si va asigura suport nativ pentru procesare de algoritmi criptografici
- Va procesa nativ in hardware rutine de cifru asimetric, respectiv pe baza de algoritmi standard:
    - Diffie-Helman;
    - DSA, cel putin 1024 bit;
    - RSA, cel putin 4096 bit;
    - ECDSA (pe curbe specific identificate), pana la cel putin 512bit.
- Va procesa nativ in hardware rutine de cifru simetric, respectiv pe baza algoritmilor standard:
    - AES 256;
    - 3DES.
- Va procesa nativ in hardware rutine de amprentare criptografica si de certificare de integritate, pe baza algoritmilor standard:
    - SHA-1;
    - SHA-2/256 ;
    - SHA-2/512 ;
    - RIPEMD160.
- Va asigura un nivel adecvat de performanta specifica:
    - (minim) 200 de operatii de executare de semnatura RSA cu chei de 1024bit pe secunda;
- Va permite controlul accesului la resurse atat pe baza de simpla autentificare HTTP, si/sau cu restrictii la nivel de identificator de retea (IP), cat si cu certificate client;
- Va permite, direct de pe platforma, reinnoirea automata a certificatelor de verificare, respectiv corespunzatoare cheilor provate de semnare folosite;
- Va permite arhivarea optionala a documentelor semnate;
- Va permite jurnalizarea si auditul operatiunilor adminsitrative si a celor specifice, de semnare / validare;
- Va putea fi integrat in fluxuri de solicitare si aprobare de documente certificate, respectiv prin semnare si marcare temporala, automata sau cu interventia operatorului uman;
- Va asigura interoperabilitate testata cu platforme de servere de aplicatie Java standard, respectiv cel putin cu JBoss si GlassFish;
- Va putea fi instalat in configuratii redundante, de tip cluster 1+1, pentru asigurarea unui nivel inalt de disponibilitate operationala;
- Atat configuratiile independente, cat si cele in mod custer, vor permite mecanisme de monitorizare si de verificare a starii generale si a disponibilitatii nodurilor de tip server de semnare digitala si de marcare temporala administrate;
- Solutia oferita va incliude toate reperele hardware si licentele software care vor permite implementarea pentru semnarea offline a documentelor obiect si a

documentelor martor de tranzactie generate, pe baza de schimb continuu de semnale de tip web-services si asimilate, la nivel de protocol de aplicatie, intre componenta care solicita semnarea si componenta care executa semnatura, dar fara a permite stabilirea de legatura de comunicatie la nivel de retea cu restul sistemului;

- In aceasta varianta de implementare asigurarea separatiei se va face, pe ambele sensuri, cu dispozitive de control al comunicatiei unidirectionale, certificate minimum CC EAL 7;
- Modulele oferite vor fi de tip appliance si vor fi dimensionate optim, inclusiv in ceea ce priveste puterea de calcul de care dispun pe functionalitatile specifice, si vor fi configurate pentru a putea opera, pentru asigurarea functionalitatilor specifice, in mod independent de alte module sau echipamente;
- In configuratia oferita, modulele vor putea fi instalate in rack standard de 19inch, si vor dispune de surse de alimentare redundante.

Ofertantii vor include in oferta cel putin urmatoarele:

- 2 componente integrate de tip server de semnare centralizata de documente si de autentificare de tranzactii, respectiv:
- fara restrictie de numar de identitati sistem sau utilizator certificate deservite, sau de tranzactii prelucrate.

3.3.5 Confidenţialitatea datelor

Soluția de securitate propusă trebuie să asigure confidențialitatea informațiilor, ceea ce reprezintă o misiune critică. Informația dintr-un astfel de sistem trebuie protejată împotriva amenințărilor în orice situație, fie când este stocată, fie când este transportată.

Pe lângă cerințele enunțate mai sus, platforma și instrumentele pentru asigurarea confidențialității datelor trebuie:

Una din soluțiile de securitate a Sistemului trebuie să asigure confidențialitatea informațiilor. Informația din acest sistem trebuie protejată împotriva amenințărilor în orice situație, fie când este stocată, fie când este transportată.

Principalele cerințe sunt:

Sa fie independentă de platformă – să ofere suport pentru majoritatea sistemelor de baze de date relaţionale.
Sa fie independenta de producătorul bazei de date: nu se va baza pe logurile si nici pe auditul nativ al bazei de date.
Sa fie accesibilă din locaţii multiple, în mod securizat, prin intermediul unei console web.

Sa ofere scalabilitate ridicata, mergând de la protecţia unei singure baze de date la protejarea a zeci de baze de date în centre distribuite.
Sa permită accesul la modulele soluţiei şi la date pe baza rolurilor.
Sa includă un modul de management al rolurilor.
Sa includă un singur repository centralizat la nivelul companiei pentru investigatii.
Sa centralizeze datele de audit in real-time, şi nu la momentul creării de rapoarte, sau la un anumit interval de timp.
Sa monitorizeze şi sa aplice politici de acces privitoare la date sensibile, acţiuni privilegiate ale utilizator, controlul modificărilor, cererilor şi activităţilor utilizatorilor precum şi excepţii de securitate, cum ar fi operaţiuni eşuate.
Sa permită crearea politicilor de acces la anumite tabele, pe baza userului cu care s-a autentificat utilizatorul la nivel de sistem de operare, pe baza adresei IP sau a adresei MAC, a protocolului de reţea, a momentului de timp în care a fost efectuată acţiunea, a aplicaţiei sursă sau a tipului de comandă SQL.
Sa trimită alerte în cazul violarii politicilor de securitate.
Să monitorizeze continuu toate operaţiile asupra bazei de date, în timp real, detectând acţiunile neautorizate pe baza informaţiei contextuale – “cine, ce, unde, când, cum” din fiecare tranzacţie SQL.
Politicile să poată fi adăugate facil prin intermediul unei interfeţe intuitive.
Soluţia trebuie să ofere vizibilitate de 100% şi granularitate a tranzacţiilor din bazele de date, prin monitorizarea urmatoarelor operatii:

- Excepţiile de securitate, cum ar fi erori SQL şi autentificări eşuate;
- Comenzi DDL gen Create/Drop/Alter Tables, care modifică structura bazelor de date;
- Interogări SELECT ce pot avea impact asupra confidenţialităţii datelor;
- Comenzi DML (Insert, Update, Delete) care includ variabile;
- Fraze XML executate de către baza de date.

Să permită corelarea evenimentelor si actualizarea politicilor pe bază de comportament.
Soluţia trebuie să ofere totodata si:

- Rapoarte predefinite.
- Rapoarte care să ofere facilitatea de drill-down pentru identificarea problemelor.
- O interfaţă grafică tip drag-and-drop cu ajutorul căreia să se construiască rapid rapoarte noi, sau să se modifice cele existente.
- Facilităţi pentru transmiterea rapoartelor în mod automat, prin email sau sub formă de linkuri către pagini HTML. Aceleaşi rapoarte să poată fi vizualizate şi online, prin consola web.
- Posibilitatea ca logurile de audit trebuie sa fie protejate fata de acces implicit la nivel "root".
- O funcţionalitate de arhivare/restaurare a logurilor, cu criptarea arhivelor de loguri.

- Integrare cu sisteme LDAP.
- Suport pentru următoarele standarde: SNMP, SMTP, Syslog, CEF.
- Integrarea cu sisteme de tip Security Information and Event Management (SIEM).
- Configuratie de inalta disponibilitate pentru toate componentele solutiei.

Se vor include licentele de folosire a solutiei pentru asigurarea confidentialitatii datelor care sa ofere suport pentru necesitatile sistemului, corelate cu modul de licentiere al producatorului, incluzandu-se totodata, daca e cazul, echipamentele tip appliance dedicate.

3.3.6 Integrarea componentelor

3.3.6.1 Infrastructura de integrare

Solutia oferita trebuie sa contina o infrastructura de conectivitate ce suporta servicii web şi mesagerie JMS, oferind o flexibilitate mare prin implementarea interfeţelor orientate pe servicii.

Aceasta infrastructura va reprezenta componenta de conectivitate dintr-o arhitectură orientată pe servicii, oferind soluţii de integrare bazate pe standarde deschise care sa permita implementarea de soluţii intr-un mod rapid, prin reducerea complexităţii şi numărului de interfeţe dezvoltate. Infrastructura software de conectivitate va respecta cerintele detaliate de mai jos.

Sistemul ce se va dezvolta in cadrul proiectului va trebui sa se interconecteze cu Sistemul Electronic National, prin integrarea cu Punctul Unic de Contact Electronic (parte integranta a SEN) conform legii 161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a fuctiilor publice in mediul de afaceri, prevenirea si sanctionarea coruptiei. Conditiile tehnice si de interoperabilitate prin care se poate realiza interconectarea vor fi puse la dispozitie de catre MCSI.

3.3.6.2 Server de integrare

Server-ul de integrare trebuie să permită conectivitate bazată pe servicii web şi mesagerie JMS, oferind o flexibilitate mare datorita interfeţelor orientate pe servicii.
Server-ul de integrare trebuie să reprezinte componenta de conectivitate dintr-o arhitectură orientată pe servicii, oferind soluţii de integrare bazate pe standarde deschise.
Server-ul de integrare trebuie să permită implementarea soluţiilor cu ajutorul uni instrument de dezvoltare compatibil, uşor de utilizat, care nu necesită cunoştinţe avansate de programare, instalarea, configurarea, dezvoltarea interfețelor făcându-se prin instrumente vizuale.

Server-ul de integrare trebuie să ofere suport pentru integrarea cu o gama largă de tehnologii şi aplicaţii.
Server-ul de integrare trebuie să ofere flexibilitate în administrarea şi configurarea de servicii.
Server-ul de integrare trebuie să ofere un set larg de medieri gestionate prin politici şi reguli.
Server-ul de integrare trebuie să permită integrare cu un catalog de servicii, pentru gestionare politici și guvernare.
Server-ul de integrare trebuie să permită selectarea în mod dinamic a End Point Web Service dintr-un catalog de servicii.
Server-ul de integrare trebuie să ofere un mediu integrat de test pentru integrarea cu un catalog de servicii.
Server-ul de integrare trebuie să ofere noduri native de jurnalizare a mesajelor primite dintr-o bază de date, oferind o interfaţă de configurare grafică, nefiind nevoie de programare.
Server-ul de integrare trebuie să ofere o interoperabilitate sporită, oferind suport pentru WS-I Reliable Secure Profile, SOAP 1.2, WS-Reliable Messaging şi standarde deschise.
Server-ul de integrare trebuie să ofere capabilităţi de administrare simplificată a Qualities of Service prin seturi de politici Web Services.
Server-ul de integrare trebuie să ofere un model de dezvoltare simplificată prin furnizarea unui nou mecanism de binding pentru Web Services bazat pe JAX-WS 2.0, JAXB 2.0, SAAJ 1.3 şi StAX 1.0.
Server-ul de integrare trebuie să ofere un model de dezvoltare simplificată bazat pe standardele SCA şi SDO.
Serverul de integrare trebuie să permită patern-uri de mesaje şi protocoale, cum ar fi publish/subscribe, synchronous/asynchronous şi topics/queues.
Serverul de integrare trebuie să ofere suport complet pentru persistenţa mesajelor.
Serverul de integrare trebuie să permită integrare la nivel de FTP, fişier şi bază de date, nativ sau cu adaptori.
Server-ul de integrare trebuie să ofere o flexibilitate sporită în scenariile service gateway.
Server-ul de integrare trebuie să ofere o performanţă sporită cu procesare paralelă pentru patern-uri de separare și agregare.
Server-ul de integrare trebuie să ofere o posibilitatea rapidă şi ușoară de upgrade la o platformă de Business Process Management.
Server-ul de integrare trebuie să ofere integrare cu orice provider de JMS şi o automatizare pentru resursele JMS care rulează pe server.
Server-ul de integrare trebuie să ofere posibilitatea de comunicare cu alte sisteme utilizând atât modele de programare bazate pe JMS cât şi MQI.
Server-ul de integrare trebuie să ofere suport pentru captarea şi tratarea evenimentelor.
Server-ul de integrare trebuie să ofere interacţiuni HTTP cu clienţi de servicii RESTful şi Servicii Web legacy.
Server-ul de integrare trebuie să suporte transformări universale pentru formate de date complexe şi standarde de industrie prin integrarea cu un motor specializat de transformare.

Server-ul de integrare trebuie să permită export-import de diferite formate de date.
Server-ul de integrare trebuie să suporte Web Services Notification pentru Servicii Web de tipul publish-and-subscribe.
Server-ul de integrare trebuie să ofere posibilități de scalare pentru a permite creşterea numărului de procese şi a utilizatorilor sistemului.
Server-ul de integrare trebuie să suporte o arhitectura de tip cluster.
Server-ul de integrare trebuie să suporte failover automat.
Server-ul de integrare trebuie să ofere o balansare a încărcării la nivel web şi aplicaţie.
Se vor include licentele de folosire ai Platformei de Integrare a Componentelor, corelate cu modul de licentiere al producatorului, insa nu mai putin de 2 procesoare folosite in componentele de multi-procesare simetrica din infrastructura hardware a sistemului.

3.3.7 Autentificare tip OTP

Suplimentar fata de autentificarea prin metoda « user name / password », sistemul informatic va trebui sa permita utilizatorilor-cheie (50 de persoane desemnate de catre Institutia Beneficiara), prin intermediul unui sistem specializat, autentificarea de tip « OTP – One-Time Password ». Aceasta metoda se bazeaza pe ideea ca parola folosita la autentificare este valabila pe perioada acelei sesiuni de lucru.

Sistemul de autentificare de tip OTP (« One-Time Password ») trebuie sa indeplineasca urmatoarele cerinte :

Generalitati :

Accesarea sistemului din locatia Beneficiarului se va realiza securizat prin intermediul Sistemului de autentificare tip OTP. Sistemul trebuie sa asigure autentificare de tip « two factor authentication », asigurand astfel protectie impotriva atacurilor de tip troieni, « man in the middle », « phishing », precum si pentru atacuri interne. Sistemul va prelua cererea de autentificare a utilizatorului, identitatea acestuia si parola dinamica, si o va trimite sistemului/serverului de autentificare OTP. Serverul de autentificare va verifica si va valida parola dinamica si va raspunde sistemului pentru continuarea interactiunii cu utilizatorul pe baza rezultatului procesului de autentificare. Validarea parolei dinamice de catre sistem asigura evidenta participarii utilizatorului respectiv, deoarece numai acesta cunoaste parola PIN precum si evidenta utilizarii echipamentului (token/card) asignat respectivului utilizator.

Avand in vedere numarul de utilizatori, cu niveluri de pregatire si profile eterogene, se va asigura o mare flexibilitate in configurarea solutiei, in conditii de performanta si costuri reduse. Pentru a asigura flexibilitatea solutiei, serverul de autentificare care valideaza parolele dinamice va trebui sa suporte echipamente si protocoale de autentificare multiple. Se solicita minim:

Token hardware (minim 2 producatori diferiti cum ar fi Vasco, ActivIdentity sau echivalent);
Carduri (ex. EMV CAP/DPA, Smartcard X.509 sau echivalent);
Aplicatie de tip token pentru telefon mobil pentru utilizator (mobile token) in limba romana;
SMS OTP;

Avand in vedere necesitatea de a proteja aplicatii cu caracter special, administratorii si utilizatorii care au acces la functionalitati de administrare si utilizare a Sistemului de autentificare tip OTP vor utiliza dispozitive de tip card, Sistemul de autentificare tip OTP asigurand totodata mecanismele tehnice necesare pentru a putea accepta mai multe tipuri de carduri.

Sistemul de autentificare tip OTP va asigura functionalitati/servicii de:

Autentificare;
Administrare.

Autentificare :

Avand in vedere drepturile de acces diferite la diverse resurse ale sistemului, solutia va asigura autentificarea diferentiata a administratorilor solutiei fata de autententificarea utilizatorilor.

Autentificarea utilizatorilor in sistemul informatic se va realiza pe baza cererii primite si a validarii parolei dinamice introduse de catre utilizator;
Fiecare tranzactie de autentificare (cerere si rezultat) va fi semnata digital si stocata in baza de date a serverului de autentificare;
Solutia trebuie sa contina un mecanism implementat de prevenire a atacurilor de tip „brute force attack”
Utilizatorilor li se permite accesul in sistem prin intermediul unui nume de utilizator si o parola dinamica OTP (One Time Password).
Se va realiza restrictionarea accesului la informatie si la functionalitati in functie de drepturile de acces acordate fiecarui utilizator in parte.

Autentificarea administratorilor Sistemului de autentificare tip OTP si a utilizatorilor beneficiari :

Autentificarea se va realiza prin utilizarea card-urilor de autentificare, in conformitate cu urmatorul flux de autentificare (dupa accesarea Sistemului de autentificare, utilizatorul va parcurge urmatorii pasi):

- Va apasa butonului de pe cardul personal de generare al parolelor OTP pentru generarea dinamica a „user name-ul” si ”OTP password” ;
- Va introduce « user name-ul » si « OTP password » generate anterior ;

- Serverul de autentificare va verifica cu ajutorul algoritmilor specifici daca parola este corecta;
- Daca parola OTP introdusa de utilizator este validata si acceptata de catre componenta tip server de autentificare, se va permite accesul utilizatorului la portal;
- In caz contrar, utilizatorul va trebui sa genereze o alta parola OTP si sa execute o noua incercare de autentificare.

Sistemul/serverul de autentificare va implementa metoda « Dynamic One-Time Password », metoda de generare a parolei OTP trebuie sa accepte atat versiunea « Event based » cat si versiunea « Time based » ;

Cardurile fizice utilizate pentru generarea parolelor OTP vor indeplini urmatoarele conditii :

Respecta formatul "slim form factor" (pentru a fi usor transportal, sa incapa intr-un portofel obisnuit);
Trebuie sa incorporeze un buton pentru comanda parolei OTP si un display luminos si cu contrast ridicat tip e-paper de 6-digit pentru afisarea acesteia (pentru utilizare facila in diverse locatii, in conditii de siguranta);
Trebuie sa se ofera posibilitati de personalizare grafica a cardului pentru autentificarea OTP (astfel incat sa fie usor depistabila orice incercare de insusire, imprumut sau schimbare de carduri intre utilizatori de tip administrator si cursant, evitand astfel orice incercare de frauda);
Trebuie sa respecte standardele ISO 7810, ISO 14443, OATH, RoHS;
Trebuie sa ofere o garantie de minim 3 ani sau 10.000 coduri generate.

Furnizorii vor asigura numarul necesar de carduri de autentificare pentru utilizatorii beneficiari ai MCSI, respectiv 50 de carduri de autentificare.

Sistemul de autentificare tip OTP trebuie sa includa un sub-modul de management al cardurilor pentru stocarea informatiile necesare referitoare la titularii cardurilor de autentificare, perioadele de valabilitate, statusuri, etc.

<u>Administrarea sistemului/serverului de autentificare</u>

Serviciile de administrare trebuie sa fie disponibile printr-o interfata Web si sa asigure minim:

Administrarea conturilor utilizatorilor si a proprietatilor de autentificare ale acestora :

Configurarea proprietatilor de autentificare ca de ex :

- Tipuri de autentificare;
- Configurare hsm;

- Managementul cheilor;
- Parametrii de autentificare.

Administrarea echipamentelor de autentificare:

- Initializarea acestora;
- Inrolare;
- Monitorizarea starii / blocare;
- Deblocare;
- Sincronizare.

Managementul conturilor utilizator:

- Inrolare;
- Asignarea echipamentului de autentificare;
- Tiparirea parolei pin initiale;
- Monitorizarea starii / blocare.

Managementul conturilor administrator:

- Roluri;
- Drepturi de acces.
- Statistici si rapoarte diverse:
- Modul de audit .

Audit :

Se va asigura auditarea tuturor operatiilor efectuate in cadrul sistemului de autentificare OTP.

Facilitati de integrare, standardizare si interoperabilitate

Sistemul de autentificare tip OTP trebuie sa functioneze pe baza unei arhitecturi orientata pe servicii iar serviciile de autentificare sa fie furnizate ca servicii Web XML/SOAP, astfel incat sa se asigure mecanime standardizate de integrare cu infrastructura software, interoperabilitatea cu aplicatiile existente, contribuind astfel la asigurarea sustenabilitatii proiectului.

Pentru integrarea cu alte aplicatii/componente software se solicita disponibilitatea unui API standard care sa permita integrare peste canale SSL.

Sistemul de autentificare tip OTP trebuie sa asigure si acces prin protocol standard RADIUS.

Sisteme de operare si servere de baze de date suportate

Sistemul de autentificare tip OTP trebuie sa asigure disponibilitate pentru multiple sisteme de operare, precum :

Microsoft Windows,
distributii Linux.

Sistemul de autentificare tip OTP trebuie sa asigure disponibilitate pentru multiple sisteme de baze de date relationale, precum :

Oracle Database,
IBM DB2 ,
Microsoft SQL Server.

Dispozitive hardware suportate

Pentru asigurarea flexibilitatii in implementare, compatibilitatea cu infrastructura hardware furnizata de beneficiar si minimizarea pe cat posibil a costurilor, solutia de autentificare va asigura disponibilitate pentru multiple echipamente HSM si telefoane mobile dupa cum urmeaza:

Suport pentru echipamente HSM de la minim 2 producatori diferiti.

Sistemul propus pentru autentificare tip OTP trebuie sa fie o solutie consacrata pe piata. In acest sens, furnizorii vor prezenta in oferta tehnica minim trei exemple de implementari similare ale solutiei.

Furnizorii trebuie sa includa in oferta licentele de utilizare a Sistemului de autentificare OTP, corelate cu modul de licentiere al producatorului, si care sa asigure necesitatile de autentificare tip OTP pentru Sistemul Informatic.

3.3.8 Autentificare pe baza recunoasterii semnaturii olografe

In vederea asigurarii unui grad ridicat de securitate al autentificarii administratorilor de sistem, se va implementa un sistem de autentificare si recunoastere a semnaturii olografe. Sistemul de recunoastere a semnaturii olografe trebuie sa indeplineasca urmatoarele cerinte :

Inregistrarea utilizatorului in sistemul informatic prin stocarea in sistem de la acesta a unui numar de specimene de semnatura efectuate cu un device de tip « pix electronic » ;
Recunoasterea semnaturii utilizatorului (semnatura originala) efectuata cu un echipament dedicat de tip pix electronic;
Respingerea incercarilor de frauda prin imitarea semnaturii corecte a utilizatorului (adica respingerea accesului la semnalarea semnaturilor false).
Nivelul de respingere a semnaturilor false sa fie de minimum 98 % ;

Modulul trebuie sa tina cont in procesul de recunoastere a semnaturilor nu numai de aspectul grafic ci si de caracteristicile (acceleratiile) gestului utilizatorului reprezentat de semnatura.

Se vor oferi licentele de utilizare a sistemului de recunoastere a semnaturii olografe cu suport pentru 4 administratori ai sistemului, incluzadu-se totodata si echipamentele hardware tip appliance dedicate.

Se vor oferi licentele de utilizare a sistemului de recunoastere a semnaturii olografe cu suport pentru 8 administratori ai sistemului, incluzadu-se totodata si echipamentele hardware tip pix electronic (dedicate). Pixul electronic trebuie sa indeplineasca urmatoarele cerinte tehnice :

Caracteristici fizice :

- Lungime pix: Minim 140 mm;
- Diametru pix: maxim 13 mm;
- Greutate: maxim 60 g;
- Formă ergonomică;
- Carcasă metalică;
- Tensiune de alimentare: 5V prin conexiune USB.

Componente incluse (minim) :

- Două microsisteme senzoriale de accelerație de tip MEMS (micro-electro-mecanical system) inerțiale, fiecare cu câte două axe ortogonale de sensibilitate;
- Microsistem senzorial autoreferențial de navigare optică pe suprafața de scriere;
- Microcontroler de tip AVR RISC pentru achiziția datelor captate de senzori.

Funcționalități :

- Captează semnale dinamice produse de mișcarea mâinii în timpul efectuării semnăturii olografe;
- Captează semnale dinamice produse de microvibrațiile de contact ale pixului cu suportul de hârtie pe care se semnează;
- Captează proiecția relativă a traiectoriei pixului, pe hârtia cu pattern de navigare imprimat;
- Comunicare cu sistemul de procesare și stocare a datelor prin conexiune USB 2.0;
- Odată cu achiziția datelor, se poate reține și semnătura în sens clasic, pe hârtie.

Funcționalități (oferite impreuna cu componenta software de recunoastere a semnaturii olografe) :

- Procesează semnalele dinamice produse de mișcarea mâinii în timpul semnăturii olografe
- Procesează microvibrațiile de contact ale pixului cu suportul pe care se semnează

- Oferă feed-back vizual, în timp real, către utilizator
- Stochează informațiile/semnalele asociate semnăturii într-o baza de date
- Procesează/compară semnalele asociate semnăturilor specimen inițial stocate în baza de date, cu semnalele asociate semnăturilor de intrare, stabilind în timp real, gradul de asemănare dintre acestea.

Uzabilitate :

- Semnătura se efectuează pe coli hârtie cu pattern pre-tipărit (se vor include minim 4000 de astfel de coli).

3.3.9 Parametri tehnici

Sistemul trebuie să fie foarte scalabil și cu o disponibilitate foarte mare astfel încât să susțină un număr de 5000 de utilizatori înregistrați.

4 INFRASTRUCTURA HARDWARE

În continuare, sunt prezentate specificațiile tehnice minimale ale platformelor si echipamentelor hardware de suport pentru sistem:

4.1 Platforma integrata de procesare

4.1.1 Suport fizic de tip rack pentru montarea şi poziţionarea echipamentelor (1 bucata)

Ansamblu modular standard de 19 inchi, cu 42U disponibili pentru pozitionarea echipamentelor. Se vor include reperele de montare necesare, inclusiv şine extensibile telescopic (sau soluţii similare) cel puţin pentru echipamentele complexe de natura nodurilor de procesare, în scopul de a permite accesul fizic facil la componentele interne de tip hot-plug / hot-swap (surse, ventilatoare, plăci de extensie etc.) şi deservirea acestora fără a fi necesară oprirea funcţionării şi/sau deconectarea echipamentului (ori de câte ori acest lucru este posibil din punct de vedere funcţional).

Structura internă a rack-ului va facilita poziţionarea cablurilor, pentru distribuirea echilibrată a bugetului de conexiuni, respectiv pentru a implementa o schemă de asigurare a redundanţei (la nivel de alimentare, interconectare SAN, LAN etc.) şi evitarea condiţiilor de tip single-point-of-failure.

4.1.2 Consolă de management general – (1 bucata)

Consolă locală KVM - unitate montată în rack, care va include:

- monitor TFT, de min. 17inch şi suport pentru afişare de rezoluţii native 1280x1024;
- tastatură USB cu dispozitive integrate de tip touch-pad şi track-point;
- porturi de acces la consolele KVM şi la porturile usb si video din nodurile de procesare astfel incat toate nodurile de procesare sa fie deservite de monitorul si tastatura incluse in consola (nu mai putin de 6 porturi de acces KVM).

Pliată, consola va ocupa un spaţiu optim de 1-2U în rack.

4.1.3 Surse neîntreruptibile (UPS) – (2 bucati)

Se va implementa o structură eficientă de alimentare de tip UPS compusă dintr-o unitate discreta independenta de tip on-line dublă conversie, monofazata (1/1) de 10KVA (8KW).

Aceasta structura trebuie sa ofere un timp de functionare in regim de avarie de minim 20 de minute la o incarcare preconizata de minim 50%.

Arhitectura preconizată este de natură sa aibă cost şi complexitate minime, precum şi un nivel optim de disponibilitate operaţională; capacitatea preconizată şi suportul de uptime vor permite acomodarea echipamentelor solicitate precum şi rezerva necesară pentru extensiile ulterioare previzibile, fără a pune probleme de implementare.

Unitatea UPS trebuie sa permita extinderea timpului de functionare in regim de avarie prin cel putin un modul discret de baterii, integrabil in structura fara necesitatea opririi alimentarii echipamentelor deservite.

Componentele interne ale unităţilor UPS, inclusiv bateriile, vor fi de tip hot-swap şi vor permite deservirea (inclusiv înlocuirea acestora) fără oprirea sarcinii.

Unitatea UPS va include modul de management pentru monitorizare la distanţă, inclusiv software de management si idicatori frontali pentru suprasarcina si nivel incarcare module de baterii.

4.1.4 Componente de distribuţie (PDU) – (4 bucati)

Pentru alimentarea echipamentelor se vor folosi unităţi de tip PDU cu ieşiri tipice de 6A şi conectorizare C13/C14.

Ansamblul va fi echipat cu numărul şi structura de unităţi PDU, precum şi cu cablurile aferente, necesare alimentării tuturor surselor echipamentelor instalate.

Interconectarea acestora se va realiza de aşa manieră încât sursele care formează un set redundant, pentru acelaşi echipament, nu se vor alimenta în acelaşi PDU.

Această organizare are ca scop echilibrarea implicită a sarcinii precum şi evitarea situaţiei în care oprirea, accidentală sau planificată, a oricărei unităţi PDU să provoace oprirea alimentării oricărei surse în echipamentele critice echipate cu două sau mai multe surse şi nici să nu necesite reorganizarea cablurilor pentru menţinerea stării operaţionale. Echipamentele critice echipate cu o singură sursă vor fi grupate în perechi redundante, oricare dintre ele capabil să preia sarcina sau să acopere funcţionalităţile echipamentului pereche.

4.1.5 Şasiu modular pentru suportul procesării centralizate – (1 bucata)

Soluţia/componentele oferite trebuie să îndeplinească următoarele cerinţe generale:

- Sistemele şi echipamentele livrate trebuie să fie noi, neutilizate şi de ultimă generaţie. Ele trebuie să asigure gradul solicitat de performanţă, fiabilitate şi flexibilitate fiind proiectate şi destinate pentru aplicaţii critice “enterprise level”.
- Dispozitivele hardware trebuie să fie astfel proiectate încât să poată asigura scalarea sistemului în cazul creşterii nevoii de putere de calcul.
- Dispozitivele hardware trebuie să fie compatibile cu caracteristicile reţelei electrice din România astfel încât să nu existe probleme la conectarea acestora la reţeaua electrică.

Arhitectura soluţiei propuse trebuie să includă următoarele caracteristici generale de fiabilitate, disponibilitate şi uşurinţă în efectuarea service-ului (Reliability Availability Serviceability-RAS) la nivel de servere sau şasiu:

- componente redundante în interiorul sistemului (surse de alimentare electrică).
- capabilităţi de auto-testare şi rezolvare a defectelor intermitente fără intervenţie umană .
- dealocarea “online” şi izolarea componentelor defecte ale sistemului (de exemplu discuri, ventilatoare, subsisteme de alimentare cu energie electrică, adaptoare PCI); în momentul reboot-ului componentele defecte vor fi deconfigurate
- diagnosticarea erorilor în timp real.
- capabilităţi arhitecturale de prevenire a erorilor .

Platforma de procesare reprezintă un ansamblu modular pentru suportul procesării, în arhitecturi mixte eterogene, format din şasiu modular şi module de procesare:

- Componenta de tip şasiu modular pentru suportul procesării centralizate, cu suport pentru integrarea modulelor de procesare, a extensiilor de I/O ale acestora, precum şi a modulelor de management.

- Şasiul trebuie configurat pentru instalarea de noduri de procesare de tip blade sau similare, optimizate pentru asigurarea densităţii si puterii de calcul necesare.

- Şasiul va fi echipat cu toate componentele redundante, hot-plug / hot-swap şi utilizabile în mod concurent, pentru alimentare şi ventilare, management (inclusiv procesoare de serviciu / management).

- Pentru asigurarea puterii de calcul necesare şi adaptării la cerinţele diverselor aplicaţii, fiecare şasiu va suporta configurarea şi echiparea cu module (noduri) de procesare de tip blade pe 64 biţi, în arhitectură CISC x 86 şi/sau RISC, EPIC (sau derivate din EPIC).

- Şasiu montabil în cabinet sistem, cu suport pentru cel puţin 14 module blade, cu posibilitatea intermixării acestor module blade în şasiu în orice mod.

- Midplane de înaltă disponibilitate care suportă funcţii de tip hot-swap la nivel de server blade individual, module de interconectare LAN, module de management, surse de alimentare.

- Suport pentru management de la distanta, redirectare interfata grafica, tastatura si mouse, posibilitate de pornire/oprire de la distanta pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer).

- Unitate optică DVD-RW internă, pe panoul frontal, accesibilă de fiecare din serverele blade instalate în şasiu.

- Minim patru surse hot-swap, instalate intern în şasiu, redundante n+n, alimentare la 200-240 Vac. Sistemul va permite alimentarea concurentă a fiecărui modul sursă prin cel puţin 2 componente (căi de alimentare) intermediare PDU sau similare.

- Minim doua porturi USB pe panoul frontal pentru unităţi media adiţionale, accesibile de oricare dintre serverele blade instalate în şasiu.

- Sistem de ventilaţie de tip hot-swap, redundant, instalat intern în şasiu.

- Suport pentru minim opt module I/O interne pentru interconectare în tehnologie 1Gbps Gigabit Ethernet, 10 Gbps Ethernet, 8 Gbps Fibre Channel.

- Se vor oferi module de interconectare externa capabile sa maximizeze disponibilitatea ansamblului prin operare cat mai facila in caz de defectare minimizand necesitatea de reconfigurari LAN efectuate de administrator. Se solicita configuratii care sa asigure redundanta la defectare si No Single Point Of Failure.

- Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 1 Gbps porturi Ethernet, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2.

- Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 10Gb porturi Ethernet fiecare, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2, echipate cu minim 6 module de conectare SFP+ fiecare.

Componenta	Specificaţia tehnică minimală
Şasiu modular pentru suportul procesării centralizate - 1 buc.	
Tip, format	- Şasiu cu suport pentru integrarea modulelor de procesare, a extensiilor de I/O ale acestora precum şi a modulelor de management. - Design modular, maxim 10U, montabil in cabinet de 19” cu toate accesoriile necesare montării incluse
Capacitate	Suport pentru minim 14 servere tip blade
Componente de acces la funcţiile de tip consola de management ale fiecărui modul de procesare	- Module de management centralizat pentru întregul şasiu, hot-swap, redundante 1+1, cu switch KVM încorporat pentru toate modulele de procesare de tip blade. - Suport pentru management de la distanţă, redirectare interfaţa grafică, tastatură şi mouse, posibilitate de pornire/oprire de la distanţă pentru fiecare server blade, switch instalat, suport pentru remote media (virtual CD si floppy), suport pentru SSL (Secure Socket Layer), integrare LDAP (Lightweight Directory Access Protocol). - Modulul de management trebuie să dispună de porturi USB pentru tastatură şi mouse, port VGA pentru conectare la monitor, port RJ-45 pentru management.
Consolă locală	Modul de tip KVM inclus, rack-mountable 1-2U, format din: - monitor TFT, de min. 17” şi suport pentru afişare de rezoluţii native 1280x1024

	- tastatură USB cu dispozitive integrate de tip touch-pad şi track-point. Consola va avea porturi de acces şi interconectare cu consolele KVM din componentele platformei de stocare: min. 8 x porturi locale KVM/Cat5 pentru acces local.
Subsistem de interconectare multi-path a componentelor de procesare şi de stocare, în cabinetul sistem şi în reţele locale LAN	- Subsistemul va include componente discrete, implementate pentru configurare şi operare independentă sau ca module în şasiul platformei de procesare - Atunci când acestea se vor implementa independent, porturile de comunicaţie individuale din fiecare modul de procesare de tip blade vor fi accesibile direct, din afara şasiului sub-sistemului de procesare, fără dispozitive intermediare de conectare, prin componenta neutră de tip pass-through. - Atunci când acestea se vor implementa ca module în şasiul sub-sistemului de procesare, vor dispune de cel puţin câte un port intern de conectare pentru fiecare modul de procesare blade pe care îl deservesc.
Surse de alimentare	2 module cu câte 2 surse de alimentare de minim 2200 W fiecare, hot-swap, instalate intern în şasiu, redundante n+n, alimentare la 200-240 Vac
Sistem de ventilaţie	Baterii de ventilatoare tip hot-swap, redundante, instalate intern în şasiu
Unitate optică	Internă, de tip DVD-RW, pe panoul frontal, accesibilă de fiecare din serverele blade instalate în şasiu
Porturi	Minim 2 porturi USB pe panoul frontal pentru unităţi media adiţionale, accesibile de oricare dintre serverele blade instalate în şasiu
Module de interconectare LAN	Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 1 Gbps porturi Ethernet, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2. Minim 2 module ce vor asigura conectivitate externa prin minim 14 x 10Gb porturi Ethernet fiecare, cu capabilitati VLAN tagging, port mirroring, IGMP snooping si urmatoarele protocoale suportate: 802.1Q, IEEE 802.3ae, SNMP v2, echipate cu minim 6 module de conectare SFP+ fiecare
Standarde respectate	CE Mark (EN55022 Class A, EN60950, EN55024) CISPR 22, Class A, FCC Part 15 Class A

4.1.6 Componente de multi-procesare simetrică – (6 + 1 bucati)

Se solicită componente de multi-procesare simetrică, echipate cu procesoare CISC x86 multi-core cu următoarele cerinţe:

- Modul de procesare de tip blade, compatibil cu şasiurile ofertate;

- Minim 2x Intel Xeon Hex-Core, frecvenţa minim 2 GHz, 15 MB L3 cache sau echivalent;
- 128 GB PC3-10600 1333MHz ECC DDR3, suport pentru ChipKill sau echivalent, respectiv pentru configurare în mod hot-spare şi pentru memory mirroring; fiecare modul va dispune de minim 16 sloturi de memorie în configuraţia oferită şi va putea scala la minim 256 GB RAM prin extindere ulterioară;
- Controller video integrat;
- Interfeţe de reţea dual 1 Gbps Gigabit Ethernet integrat, suport pentru failover şi load balancing, suport TCP/IP Offload Engine (TOE);
- Interfete de retea dual 10 Gbps Ethernet integrat, suport pentru failover şi load balancing, suport TCP/IP Offload Engine (TOE);
- Procesor de management integrat, capabilităţi de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local şi la distanţă;
- Să includă funcţii de diagnostic, reset, POST şi auto-recuperare;
- Serverul va fi livrat împreună cu aplicaţia de management realizată de producătorul echipamentului, aplicaţie ce trebuie să asigure cel puţin: inventarierea componentelor, monitorizarea stării de funcţionare, trimiterea de alerte prin e-mail;
- Modulul de procesare oferit trebuie să fie compatibil, certificat de producător şi să dispună de suport pentru următoarele sisteme de operare: Microsoft Windows Server 2003 şi 2008 Web/Standard/Enterprise, SUSE Linux Enterprise Server 11, Red Hat Enterprise 5 sau superior, VMware ESX 4.0 sau superior, Solaris 10.

Componenta	Specificaţia tehnică minimală
Componente de multi-procesare simetrică – 6 + 1 buc.	
Format	Modul de procesare de tip blade, compatibil cu şasiul ofertat
Procesor	Echipat cu minim 2 x Intel Xeon Hex-core cu frecvenţa minim 2 GHz, 15 MB L3 cache, sau echivalent
Memorie internă	128 GB PC3-10600 1333MHz ECC DDR3, suport pentru ChipKill sau echivalent, respectiv pentru configurare în mod hot-spare şi

	pentru memory mirroring; fiecare modul de procesare va putea scala la minim 256 GB RAM prin extindere ulterioară
Video	Controller video integrat
Interfeţe de reţea	Echipat cu: - Interfeţe de reţea Dual 1 Gbps Gigabit Ethernet, suport pentru failover şi load balancing, suport TCP/IP Offload Engine (TOE) - Interfeţe de reţea Dual 10 Gbps Ethernet integrate, suport pentru failover şi load balancing, suport TCP/IP Offload Engine (TOE)
Management	- Procesor de management integrat, capabilităţi de monitorizare a componentelor critice pe fiecare modul de procesare de tip blade, local şi la distanţă - Suport pentru funcţii de diagnostic, reset, POST şi auto-recuperare - Serverul va fi livrat împreună cu aplicaţia de management realizată de producătorul echipamentului, aplicaţie ce trebuie să asigure cel puţin: inventarierea componentelor, monitorizarea stării de funcţionare, trimiterea de alerte prin e-mail
Sisteme de operare compatibile, certificate de producător	Microsoft Windows Server 2003 şi 2008 Web/Standard/Enterprise, SUSE Linux Enterprise Server 11, Red Hat Enterprise 5 sau superior, VMware ESX 4.0 sau superior, Solaris 10
Garanţie şi suport	Minim 3 ani
Unul dintre modulele blade va fi pentru management si trebuie sa fie echipat cu 2 HDD-uri SAS 600G	

4.2 Platforma de stocare consolidata multi-protocol – (1 bucata dual-node)

Solutia trebuie sa includa un sistem de stocare cu arhitectură internă flexibilă, în care nodurile active de control vor fi simultan conectate la toate structurile de tip bus sau loop (SAS loops şi similare), pentru a face posibilă arondarea iniţială şi reconfigurarea ulterioară facilă a alocării discurilor între nodurile de control, între diferitele volume (sau structuri similare), precum şi între servicii diferite (SAN/NAS).

Platforma de stocare va indeplini urmatoarele caracteristici :

- Echipamentul trebuie sa fie echipat cu doua controller-e in acelasi spatiu din rack pentru a putea dispune de o configuratie redundanta de tip cluster la nivelul echipamentului
- Echipamentul trebuie sa permita scalarea la minim 130 de discuri cu conectare de tip Serial SCSI (SAS) sau SATA.

- Echipamentul trebuie sa permita utilizarea in paralel a discurilor de tip SAS 3Gb/s si SATA II 3Gb/s.
- Capacitatile pentru un HDD minim disponibile trebuie sa fie de 1TB pentru discurile SATA si 600GB pentru cele SAS.
- Minim 6 GB memorie instalati si utilizabili pe sistemul de stocare. Memoria trebuie sa fie protejata cel putin cu acumulatori (baterie). In configuratie dual controller capacitatea maxima de memorie trebuie sa fie de minim 12GB.
- Minim 1 procesoare pe fiecare controller.
- Sistemul trebuie sa permita conecatarea atat in standard File Access (NAS) cat si in standard Block Access (SAN).
- In configuratia livrata echipamentul trebuie sa fie echipat cu cel putin 8 porturi Ethernet cu o latime de banda de 1 Gb/s si minim 4 porturi Ethernet cu o latime de banda de 10 Gb/s.
- Echipamentul trebuie sa suporte utilizarea in paralel a urmatoarelor protocoale de acces si comunicatie: NFS, CIFS, iSCSI, FC.
- Sistemul trebuie sa suporte conectarea prin protocolul CIFS, NFS, iSCSI si FC la urmatoarele sisteme de operare: Microsoft Windows, Linux, SUN Solaris, in functie de suportul tehnologic oferit de fiecare sistem de operare in parte.
- Echipamentul trebuie sa suporte realizarea copiilor de tip Snapshot precum si replicarea datelor la distanta in mod sincron si asincron. Replicarea datelor la distanta trebuie sa fie suportata atata cu echipamentele din aceeasi clasa cat si cu cele din clasa diferite (inferioare sau superioare ca performanta) produse de acelasi producator.
- Unitatile de expansiune cu discuri trebuie sa fie compatibile cu sisteme de stocare din clasa superioara(scalabilitate si performanta) in asa fel incat in situatia unui upgrade/migrari inlocuirea acestora sa nu fie necesara.

In configuratia livrata echipamentul trebuie sa dispuna de urmatoarele functionalitati:

- Realizarea copiilor de tip instantanee - Snapshot, si posiiblitatea de restaurare foarte rapida a acestora fara mutarea datelor salvate in copia de tip Snapshot ci prin remaparea blocurilor de date.
- Licenta inclusa pentru deduplicarea datelor.
- Configurarea si optimizarea matricilor RAID de tip RAID 0, 1, 5 6 si combinații..
- Conectarea prin protocol iSCSI sa fie disponibila in configuratia initiala.
- Conectarea prin protocol NFS sa fie disponibila in configuratia initiala.
- Conectarea prin protocol CIFS sa fie disponibila in configuratia initiala.
- Sistemul trebuie sa fie echipat in configuratia livrata cu minim 24 de discuri SAS cu o capacitate de 600GB pentru fiecare disc. In aceste conditii spatiul ocupat in rack nu trebuie sa depaseasca 4U impreuna cu controller-ul sistemului de stocare.
- Licenta software care sa asigure monitorizarea performantei si capacitatii platformei de stocare atat la nivel fizic cat si la nivel virtual. Solutia software trebuie sa asigure functionalitatile respective atat pentru platforma existenta cat si pentru alte platforme de la acelasi producator sau de la producatori diferiti, platforme ce pot face obiectul unor achizitii ulterioare. Solutia trebuie sa indelineasca urmatoarele cerinte:

    1. Sa monitorizeze performanta platformelor de stocare existente si sa identifice blocajele de performanta atat la nivelul serverelor fizice si virtuale conectate la volumele de date cat si la nivelul volumelor de date exportate catre platformele de procesare

    2. Sa permita izolarea surselor de blocaj al performantei si oferirea de solutii alternative de acces la volumele de date si la capacitatea disponibila pe discuri, astfel incat aceste blocaje sa poata fi usor depasite

    3. Sa permita automatizarea proceselor de planificare a capacitatii de stocare prin mecanisme de colectare datelor relevante privind numarul de discuri, lun-uri, volume de date, cai de acces, grad de ocupare al resurselor de

procesare si al capacitatii de stocare, respectiv predictie pentru gradul viitor de ocupare al acestor resurse, prin analiza predictiva a tuturor parametrilor enumerati

4. Sa permita vizulizarea facila a tuturor parametrilor rezultati in urma proceselor de planificare si predictie
5. Sa permita procese automate de corelare a masinilor din platformele de virtualizare, a aplicatiilor si a conexiunilor logice cu spatiul fizic de stocare disponibil in platformele de stocare
6. Sa permita clasificarea datelor aflate in platforma de stocare, prin identificarea tipurilor de fisiere si a istoricului de acces catre aceste fisiere
7. Functionalitatile descrise trebuie sa fie disponibile atat pentru platforma existenta cat si pentru platforme SAN (incluzand echipamentele de comunicatie de tip fabric SAN si echipamente de conexiune de tip HBA) de la alti producatori majori de platforme de stocare, platforme ce pot face obiectul unor achizitii viitoare.
8. Sa permita agregarea datelor de la platforme eterogene (multi-vendor) de stocare intr-o singura interfata de administrare, vizualizare si raportare.
9. Sa permita vizualizarea si raportarea capacitatii de stocare, alocarii si utilizarii capacitatii de stocare la toate nivelele platformei de stocare (raw, RAID, LUN, volume de date si sisteme de fisiere).

- Grantie de minim 36 de luni inclusa in configuratia propusa. Suportul si garantia trebuie sa fie asigurate in Romania de producatorul echipamentului de stocare.

Componenta echipamentului	**Specificatia tehnica minimala solicitata**
Arhitectura	Cluster Activ-Activ de 2 noduri (controller-e)
Protocoale SAN	IP SAN (iSCSI)

Protocoale NAS	NFS V2/V3/V4 peste UDP sau TCP, PCNFSD V1/V2 pentru (PC) autentificarea clientilor NFS, Microsoft® CIFS, CIFS
Numar de LUN-uri	Minim 1000
Numar de volume	Minim 1000
Numar de servere host conectate direct	4 in conexiune directa, 256 in conexiuni prin mediu de comunicatie de tip fabric
Tip conectivitate pentru disk-uri	Minim Dual-Path/Multi-Path pentru asigurarea suportului de inalta disponibilitate
Interfata de management dedicata	Minim 1 port de consola integrat Full-duplex 10/100 Base-T Ethernet
Porturi Gigabit Ethernet	Minim 8 x Full-duplex 10/100/1000 Ethernet
Porturi 10 Gbps	Minim 4 x Full-duplex 10 Gbps Ethernet
Memorie totala	Minim 12 GB ECC
Disk-uri suportate	SAS : 300 GB, 600 GB SATA : 1 TB, 2 TB, 3 TB
Disk-uri echipate	24 x HDD SAS 600 GB la 10000 rpm
Capacitate utila de date	Minim 12 TB
Nivele RAID	RAID 0, 1, 5, 6 și combinații
Sistem de operare	Proprietar producatorului echipamentului de stocare
Sisteme de operare suportate	Windows® 2000, Windows Server 2003, Windows XP, Linux®, Sun™ Solaris™, Mac® OS, VMware ESX
Copii instantanee de date	Minim 100000
Functii de management al echipamentului	diagnostic LED, SNMP, telnet, SSH, HTTP, Web (SSL), host scripting, alerte pe e-mail

Functii de securitate	SecureAdmin, IPSec, autentificare CHAP, acces pe baza de roluri administrative (RBAC)
Sursa de alimentare	Minim 2 surse redundante cu alimentare 200 la 240VAC/1.9A cu un consum de maxim 600W
Ventilatoare	Ventilatoare redundante

4.3 Sistem securitate pentru controlul traficului

Sistemul de securitate pentru controlul traficului trebuie sa indeplineasca urmatoarele cerinte:

4.3.1 Control rețea

controlul traficului proxy și direct-internet.
inspectarea traficului de rețea, incluzând atașamente și fișiere compresate.
identificarea tuturor tipurilor de informații importante – informații de identificare, cod sursa, ePHI (electronic Protected Health Information), informații clasificate și alte tipuri de date.
traficul neautorizat de conținut, aplicații și/sau protocol să fie oprit.
e-mail-urile importante sau necriptate să fie dispuse în carantina înainte de a părăsi rețeaua.
administrarea și monitorizarea tuturor canalelor, incluzând e-mail, web, webmail, chat, transferului de fișiere, telnet și peer-to-peer.

4.3.2 Control intern

monitorizarea și impunerea de politici pentru traficul intern, prevenirea accesului neautorizat.
acceptarea bazelor de date Oracle și DB2, transferului de fișiere SMB/CIFS/SAMBA și a interogărilor LDAP.

4.3.3 Analiza conținutului

Monitorizarea și blocarea următoarelor tipuri de fișiere și documente:

suita Microsoft Office (toate versiunile incluzând versiunea 2007 și baza de date Access);

Open Office;
Zip;
TAR (Tape Archive Format);
PDF (Adobe Acrobat);
AutoCad;
PostScript;
Text/Flat;
bazse 64;
gzip;
HTML (Hypertext Markup Language);
Mail;
MIME;
MIME message;
Multipart MIME;
Quoted-printable (MIME);
Fișiere grafice (incluzând png, jpeg, gif, bmp, dcx);
RFC 822/SMTP;
URL encoded;
UU encoded;
RAR.

Toate documentele listate să fie suportate via unei transmisii directe și ca atașamente , indiferent de port.

Să fie suportate atașamente integrate/incluse (de exemplu, fișier codat PK ZIP conținând doua fișiere TAR, ce conține fișiere PowerPoint și PDF, vor fi procesate individual.

4.3.4 Prevenire

La descoperirea unei tentative de încălcare a unei politici va fi emisa o alerta și sesiunea va fi întreruptă, pentru a se preveni scurgerea de informații. Deasemenea se va preveni și depășirea benzii de transfer – oprind astfel scurgerea de informații fără impact asupra performantei rețelei.

4.3.5 Vizibilitate completa

Desfășurare la nivel de sesiune, nu la nivel de pachet, inspectarea traficului rețelei de-a lungul celor 65,535 porturi de rețea intr-un singur nivel 2 de rețea.

Furnizeze vizibilitatea în protocoale, canale și aplicațiile în uz în rețea incluzând, minimum următoarele canale: SMTP, POP, IMAP, FTP, HTTP, P2P, IRC, AIM, Jabber, Yahoo Messenger, MSN Messenger, Telnet, CIFS/SAMBA/SMB, DB2, Oracle, LDAP, servicii WEB, furnizori WEBMAIL și platforme de WEBMAIL.
Să realizeze inspectarea protocolului port-independent, care inspectează toate cele 65,535 porturi pentru toate protocoalele suportate.
Să extragă conținut ușor de citit și meta-data conținute în sesiune și în orice atașament și fișier compresat , pentru analiza.
Inspectarea sesiunii încriptate SSL via integrării cu un proxy server ICAP.
Înțelegerea bazelor de date și a aplicațiilor file sharing pentru a stabili zone de control, extinzând protecția rețelei interne dincolo de punctele de ieșire.
Să furnizeze tehnologii avansate de analiza a conținutului pentru a detecta informații importante și/sau protejate.

4.3.6 Control

Împiedicarea în canale neautorizate fără oprirea proceselor normale.
Împiedicarea transferurilor neautorizate pe cele 65,535 porturi incluzând traficul non-proxy, resetarea pachetelor out-of-band via TCP când este instalat out-of-band și prin pachetelor când este inline.

4.4 Alte componente hardware

4.4.1 Firewall

Descriere generala	Echipament integrat de protectie in retea cu capabilitati de scanare antivirus, scanare antispam si prevenirea intruziunilor destinat folosirii ca o solutie de securitate unificata.
Specificatii hardware	2 x interfete 10GbE SFP+ 8 x interfete 10/100/1000 Duale (RJ-45/SFP) 12 x interfete 10/100/1000 Ethernet 4 x interfete 10/100/1000 Ethernet cu bypass (functionare in pereche) 2 x interfete 10/100/1000 Ethernet pentru Management 2 x porturi USB 1 x modul stocare intern 128 GB
Performanta sistemului	Firewall Throughput(pachete UDP 1514 byte): 20 Gbps

	Firewall Throughput(pachete UDP 512 byte): 20 Gbps Firewall Throughput(pachete UDP 64 byte): 20 Gbps Firewall Throughput(pachete pe secunda): 31 Mpps IPSec VPN Throughput(pachete 512 byte): 8 Gbps IPS Throughput: 3.6 Gbps Antivirus Throughput(flow-based): 2.1 Gbps Antivirus Throughput(proxy-based): 1.7 Gbps Tunele IPSec VPN (gateway to gateway) concurente: 10000 Tunele IPSec VPN (client to gateway) concurente: 50000 Useri SSL-VPN: 3000 SSL-VPN Throughput: 350 Mbps Concurrent session(TCP): 7 Milioane New Session/Sec(TCP): 190000 Policies(Maxim): 100000 Domenii virtuale: 100 Configuratii redundante posibile: Activ/Activ, Activ/Pasiv, Cluster Unlimited Users Licences
Parametrii echipament	Alimentare alternativa 100-240V, 50-60Hz 2 x surse de alimentare redundante Hot-swappable
Protocoale si standarde	Servicii de Retea Rutare/Retea: Suport WAN multiplu Suport PPPoE Client/Server DHCP Policy-based routing Rutare dinamica IPv4/IPv6-RIP,OSPF,BGP,Multicast(IPv4) Suport multi-zone Rutare intre zonele de securitate

	VLAN Tagging(802.1q) Rutare intre VLAN-uri Multi-link aggregation(802.3ad) Suport IPv6 (Firewall,DNS,Transparent,SIP,rutare dinamica) Traffic Shaping: Policy-based Suport DiffServ Banda Garantata/Maxima/Prioritara Shaping per-IP,per-Account, per aplicatie Domenii Virtuale: Domenii Firewall/Rutare separate Politici de securitate per domeniu Interfete VLAN separate High Availability: Funcționare Activ/Activ, Activ/Pasiv Statefull Failover Link status monitor Link failover Server Load Balancing Servicii de Securitate Firewall: NAT,PAT,Transparent Rutare dinamica-RIP,OSPF,BGP,Multicast Policy-based NAT Domenii Virtuale (NAT/Transparent) VLAN Tagging(802.1q) SIP/H.323/SCCP NAT Traversal Profile granulare de protectie per-policy

	Suport proxy explicit, optimizare WAN, caching Suport IPv6 VPN: PPTP,IPSec,SSL Suport criptare DES,3DES,AES Autentificare SHA-1 / MD5 PPTP,L2TP,VPN Client pass through Suport VPN "Hub and Spoke" Autentificare IKE cu Certificate(v1 si v2) IPSec NAT Traversal Prevenirea Intruziunilor Suport Anomalii de protocoale Suport Semnaturi definite de utilizator Suport IPv6 Antivirus Protecție anti-malware (virus, troian, worm, spyware) Protocoale: HTTP/HTTPS; POP/POP3S; SMTP/SMTPS; IMAP/IMAPS, IM (AIM, ICQ, Yahoo, MSN) Blocare fisierelor in funtie de tip sau dimensiune Suport Ipv6 Antispam SMTP/SMTPS;IMAP/IMAPS;POP/POPS Suport RBL/ORDBL Inspecție header MIME, filtrare dupa cuvinte/expresii si black/white list Update-uri automate și în timp real.
Management	Administrare: Consola, Telnet, SSH, HTTP/HTTPS,CLI Utilizatori/Administratori cu drepturi configurabile Syslog,SNMP,log-uri interne,grafice,notificari email Autentificare: Baza de date locala

	Integrare Active Directory Integrare LDAP/Radius/TACACS+ IP/MAC address binding
Software	Echipamentul sa permita prin achizitia unor licente suplimentare activarea si actualizarea serviciilor Antivirus, Antispam, Prevenirea Intruziunilor,etc. Aceste functii trebuie sa fie asigurate de echipament fara a mai necesita vreun modul hardware suplimentar.
Service si garantie	Garantie: minim 3 ani Update software gratuit: minim 3 ani

4.4.2 Notebook – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Procesor	X_86 cu 4-core sau echivalent, frecventa minim 2.4 GHz
Memorie RAM	Minim 4GB
Placa Video	Dedicata, Minim 1GB
Hard disk	Minim 500GB
Unitate optica	DVD RW
Camera WEB	Da, Minim 1,3MP
Display	LCD LED, minim 15 inch
Audio	Difuzoare stereo incorporate
Comunicatii	Retea: 10/100/1000 Wireless:WiFi 802.11n; Bluetooth
I/O (Input/Output) Porturi si Sloturi	VGA: 1 Microfon: 1

	RJ-45: 1 USB 3.0: 2 Iesire audio: 1 HDMI: 1
Sistem de operare	Da
Garantie	Minim 2 ani, locala
Altele	Geanta notebook de dimensiuni adecvate produsului achizitionat Mouse fara fir conectivitate Bluetooth Alimentator notebook

4.4.3 Multifunctionala – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Format	A4
Functii disponibile	Copiere, imprimare, scanare, fax
Tehnologie	Laser
Mod tiparire	Color
Duplex	Da
Interfata	USB, retea
ADF	Da
Medii printare	A4, A5,
Viteza de copiere color	8 / minut
Viteza de copiere alb negru	18 / minut
Rezolutie copiere	Minim 600 dpi
Viteza de printare color	21 / minut

Viteza de printare alb negru	21 / minut
Rezolutie printare	Minim 600x600 dpi
Rezolutie scanner	Minim 600x600 dpi
Alimentare hartie	Minim 250 coli
Capacitate memorie	Minim 256 MB

4.4.4 Desktop "All in One" – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Tip ecran	LED
Diagonala	Minim 23 inch
Rezolutie	Minim 1920x1080
Frecventa Procesor	Minim 2.5 (GHz)
Sunet integrat	Da
Retea integrata	Da
Capacitate RAM	Minim 4GB
Capacitate HDD	Minim 500GB
Tip placa video	Dedicata
Capacitate memorie	Minim 1024 MB
Difuzoare	Da
Microfon	Da
Tip unitate optica	DVD-RW
Webcam	Da
Bluetooth	Da
Retea	Da

Wireless	Da
USB 2.0	Minim 4
Iesire audio	Da
Intrare microfon	Da
Sistem de operare	Da
Accesorii	Tastatura fara fir conectivitate Bluetooth Mouse Mouse fara fir conectivitate Bluetooth

4.4.5 Tabla interactiva – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Diagonala (cm)	Minim 190 cm; format 4:3
Facilitati minimale:	Functii Multiuser si Multitouch – trebuie sa permita utilizarea simultana a suprafetei interactive, cu degetele sau cu markerele speciale, de catre doi utizatori. Recunoastere obiecte - utilizatorul trebuie sa poata folosi degetele, palma sau markerul fara a mai fi necesara accesarea meniului sau reasezarea in tavita a instrumentelor de lucru. Recunoasterea avansata a gesturilor – trebuie sa poata fi folosite gesturi intuitive de aruncare, rotire, marire sau micsorare a obiectelor pe tabla cu ajutoru degetelor. Orice obiect trebuie sa poata fi transformat in instrument de scris pe tabla. Functia de corectare caligrafica a adnotarilor
Software	Trebuie sa permita crearea, transmiterea si managementul lectiilor sau al diverselor prezentari; Trebuie sa permita salvarea si editarea ulterioara a sesiunilor de lucru de pe tabla, adnotarilor pot fi salvate direct in alte aplicatii software - Word, Power Point, Excel, Acrobat, AutoCAD
Montare	pe perete sau stand mobil
Accesorii incluse	2 markere si burete care nu necesita baterii sau alte consumabile, cablu USB 5 m, kit montare pe perete, stand mobil ajustabil

4.4.6 Tableta electronica – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Frecventa Procesor	Minim 1Ghz
Tehnologie display	Capacitive Multi-Touch sau echivalent
Diagonala	Minim 9.7 inch
Rezolutie	Minim 1024 x 768
Memorie Flash integrata:	Minim 16 GB
Audio	Difuzor integrat
Camera WEB	In spate: Minim 3 MP In fata: Minim 0.3 MP
Iesire audio	Minim 1 x 3.5 mm
Bluetooth	Da
Wireless	802.11 b/g/n sau echivalent
3G	Da
Baterie	Li-Polymer sau echivalent
Autonomie de lucru	Minim 9 ore
Sistem de operare	Da

4.4.7 Router wireless – (1 bucata)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Standard Wi-Fi:	802.11 n
Porturi LAN:	4 x RJ-45

Porturi WAN:	1 x RJ-45
Rata de transfer Ethernet (Mbps):	10/100
Securitate	WEP 64/128 bit. WPA, WPA2. Layer 2 Isolation. SSL Administration. SSL Login Page. Session Limit. Secure Remote (PPTP Client). Firewall. Filtrare adrese MAC.
Antena:	Minim 3 x antena externe
Frecventa (GHz):	2.4
Rata de transfer WI-FI (Mbps):	300
Alimentare:	12 V, 1.5A

4.4.8 Hard Disk Drive Extern – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Capacitate:	Minim 2 TB
Interfata:	USB 2.0 USB 3.0
Altele	Plug-and-play

	Minim 5 Gb/sec in USB 3.0 Minim 480 Mb/sec in USB 2.0
Sisteme de operare suportate	Microsoft Windows 7 Microsoft Windows Vista Microsoft Windows XP
Format	Minim 2.5"

4.4.9 Memory Stick USB – (2 bucati)

Echipamentul trebuie sa indeplineasca urmatoarele cerinte minimale:

Capacitate (GB):	Minim 64
Interfata	USB 2.0 USB 3.0
Rata de transfer la citire (MB/s):	225 (USB 3.0) 30 (USB 2.0)
Rata de transfer la scriere (MB/s):	135 (USB 3.0) 30 (USB 2.0)
Culoare	Negru/Albastru
Altele	Carcasa din metal sau cauciuc

4.4.10 Echipamente birotica

Se vor livra urmatoarele echipamente de birotica:

- Aparat de spiralat: 1 bucata;
- Laminator: 1 bucata;
- Ghilotina: 1 bucata;
- Calculator de birou: 1 bucata;
- Aparat de indosariat: 1 bucata.

5 CERINTE PRIVIND SERVICIILE DE PROMOVARE SI PUBLICITATE

5.1 Plan de informare şi publicitate

Cerinte:

- Prestatorul va realiza un plan de informare si publicitate a proiectului ce va contine o metodologie de specialitate in ceea ce priveste diseminarea/comunicarea informatiilor cu privire la proiect
- Prestatorul va realiza un plan de informare si publicitate a proiectului ce va contine un grafic de realizare a activitatilor de informare si publicitate.
- Planul de informare si publicitate va fi livrat Autoritatii Contractante in termen de 7 zile lucratoare de la data semnarii contractului de prestari servicii.

5.2 Organizare evenimente de promovare a proiectului

Livrabile:

- organizare eveniment de lansare a proiectului
- organizare eveniment de diseminare a rezultatelor proiectului

Prestatorul va realiza urmatoarele activitati:

- **Elaborarea agendei evenimentului şi a invitaţiilor de participare**

Cerinte:

- Agenda evenimentului va cuprinde: discuţii asupra obiectivelor proiectului/rezultatele proiectului, sursele de finantare, beneficiile implementarii proiectului.
- Vorbitorii vor fi desemnati de autoritatea contractanta si vor fi comunicati prestatorului cu cel putin 10 zile lucratoare inainte de data de derulare a evenimentului.
- Agenda evenimentului si textul invitatiei de participare vor fi elaborate cu cel putin 10 zile lucratoare inainte de data de derulare a evenimentului si vor fi transmise spre aprobare autoritatii contractante.

- **Transmiterea invitatiilor**

Cerinte:

- Lista cu potentialii participanti va fi comunicata de autoritatea contractanta prestatorului cu cel putin 10 zile lucratoare inainte de data de derulare a evenimentului.
- Invitatiile de participare vor fi transmise potentialilor participanti cu cel putin 5 zile lucratoare inainte de data de derulare a evenimentului printr-o modalitate care sa asigure primirea acestora.
- Lista de invitati confirmati va fi transmisa de prestator autoritatii contractante cu cel putin 2 zile lucratoare inainte de data de derulare a evenimentului.

- **Desfăşurarea evenimentului**

Cerinte:

- Organizarea unei conferinte de lansare (luna 5 de desfasurare a proiectului) si a unei conferinte de incheiere a proiectului (luna 12 de desfasurare a proiectului) cu urmatoarele caracteristici:
    - locul de derulare: Bucuresti
    - durata: ½ zi
    - program: 10.00 – 15.00
    - numar de participanti: 50
    - sala de conferinte care sa permita prezenta a cel putin 50 de persoane, in format de aranjare a scaunelor amfiteatru sau sala de cinema, cu prezidiu la care sa poata sta 5 persoane
    - dotari: videoproiector cu ecran de proiectie, telecomanda, pointer laser, laptop, flipchart, foi de flipchart, markere – negru, verde, albastru, rosu
    - echipament de sonorizare care sa permita inregistrarea discutiilor
    - aer conditionat reglabil din sala
    - o pauza de cafea pentru 50 de persoane care sa contina cel putin: cafea, ceai, apa minerala, apa plata, sucuri naturale, patiserie dulce si sarata

- masa de pranz pentru 50 de persoane, in regim a la carte sau bufet suedez, care sa contina cel putin doua feluri principale calde, desert si/sau fructe, apa minerala, apa plata, suc natural si cafea
- o persoana cu atributii de asistent de eveniment care sa realizeze inregistrarea participantilor si distribuirea materialelor de prezentare precum si sa solutioneze de indata orice problema administrativa sau tehnica legata de sala de conferinte si dotarile acesteia, pauza de cafea, pauza de masa sau orice alte situatii legate de relatia cu administratorul salii de conferinta

Conferinta va fi vizibila prin afise pozitionate in cel putin urmatoarele locuri: unul la intrarea in cladirea ce gazduieste conferinta, unul pe parcursul drumului parcurs de participanti de la intrare in cladire pana la sala unde are loc conferinta si unul in apropierea intrarii in sala in care se deruleaza conferinta. In sala in care are loc conferinta va fi instalat banner-ul de tip roll-up, in apropierea prezidiului.

Prestatorul va realiza un raport al conferintei in cel mult 5 zile lucratoare de la finalizare, ce va contine cel putin:

- agenda
- lista de participanti semnata de fiecare dintre acestia
- fotografii de la conferinta, ce vor surprinde si elementele de identitate vizuala ale proiectului.

5.3 Editarea, producţia, tipărirea/multiplicarea, inscripţionarea şi distribuţia de materiale promoţionale

Prestatorul va realiza urmatoarele activitati:

- **Elaborarea continutului materialelor promotionale: pixuri, calendare, agende, afise, banner, autocolante**

Cerinte:

- Toate materialele vor fi elaborate in conformitate cu Manualul de identitate vizuală pentru instrumentele structurale 2007-2013 în România (obiectivul Convergenţă).
- Materialele tiparite vor contine date referitoare la obiectivele proiectului, sursele de finantare, beneficiile si rezultatele implementarii.
- Toate mostrele de materiale promotionale vor fi elaborate de catre prestator si transmise autoritatii contractante cu cel putin 10 zile lucratoare inainte de termenul

pentru trimiterea acestora in productie. Autoritatea contractanta va comunica observatiile in termen de cel mult 48 de ore de la primirea propunerilor de materiale. Textul materialelor tiparite (cum ar fi pliante, afise, calendare) va fi furnizat de catre autoritatea contractanta.

- Un numar de 5 exemplare din fiecare material vor fi transmise autoritatii contractante pentru a fi incluse in rapoartele catre finantator.
- Materialele promotionale vor fi livrate de catre prestator la sediul autoritatii contractante cu cel putin 5 zile lucratoare inainte de data desfasurarii conferintei de lansare a proiectului.

- **Tipărirea/multiplicarea, inscripţionarea si distributia materialelor promotionale**

Cerinte:

Nr.crt.	Denumire	UM	Numar de unitati
1.	**Pliante:** format inchis: 100 x 210 mm, format deschis: 200 x 210 mm, hârtie: dublucretat lucios 130g, culori: 4+4	buc	1000
2.	**Banner rollup**, format 0,8 x 2 m, 4+0 print + suport aluminiu.	buc	2
3.	**Afise format A3** cm, suport 150 g/mp lucios, print 4+0, autoadeziv pe spate, în colţuri.	buc	500
4.	**Pixuri** din plastic rezistent, personalizat. Mină pix: albastru.	buc	500
5.	**Agende format închis A5**, coperta 300 g/mp plastifiată mat față – verso, interior 135 g/mp mat, tipar copertă 4+4, tipar interior 4+4, 100 pag. interior, finisări: spirala.	buc	200
6.	**Calendar** format 50 x 70 cm, suport 150 g/mp lucios, print 4+0.	buc	200
7.	**Autocolante plastifiate** format 90 x 50 mm (lungime x latime), color.	buc	1000

5.4 Elaborare comunicate de presa

Cerinte:

- Prestatorul va elabora 2 comunicate de presa privind implementarea proiectului, astfel:
    - 1 comunicat de presa privind inceperea proiectului
    - 1 comunicat de presa la inchiderea proiectului cu mentionarea rezultatelor obtinute
- Comunicatele de presa vor fi formulate de catre prestator si transmise autoritatii contractante spre aprobare cu cel putin 3 zile lucratoare inainte de data la care sunt programate a fi distribuite. Autoritatea Contractanta va transmite aprobarea insotita de eventualele observatii in cel mult 1 zi lucratoare de la primirea propunerii de comunicat de presa.
- Prestatorul va suporta difuzarea celor 2 comunicate de presa catre minim 3 fluxuri de presa cu diseminare la nivel national.

5.5 Realizare pagina Web si publicare anunturi

Cerinte:

- Prestatorul va realiza o pagina web dedicata proiectului ce va contine informatii despre proiect, anunturi de presa, comunicate si legaturi utile catre website-ul Ministerului Comunicaţiilor şi Societăţii Informaţionale, www.fonduri-ue.ro, etc. Pagina Web va fi gazduita ca subdomeniu la adresa www.mcsi.ro.
- Prestatorul va redacta anunturi cuprinzand informatii despre proiect si le va trimite autoritatii contractante in vederea publicarii pe pagina web a proiectului respectiv pagina web www.mcsi.ro.
- Anunturile vor cuprinde informatii privind stadiul implementarii proiectului, beneficiile proiectului si despre sursa de finantare.
- Prestatorul va redacta si publica anunturi informative pe pagina web a proiectului, pagina web a MCSI astfel incat sa fie publicat cel putin unul in fiecare luna de implementare a contractului.

6 CERINTE PRIVIND SERVICIILE DE MANAGEMENT DE PROIECT

Ofertantul va asigura Ministerului Comunicaţiilor şi Societăţii Informaţionale suportul necesar în vederea implementării în bune condiţii a proiectului şi elaborarea tuturor documentelor de raportare solicitate de către OIPSI pe perioada implementării acestui proiect.

Activităţile principale ce urmeaza a fi prestate de catre Ofertant constau în:

1. Iniţializarea proiectului
    a. Organizarea şedinţelor pentru demararea proiectului
    b. Clarificarea rolurilor şi responsabilităţilor
2. Planificarea proiectului
3. Monitorizare şi control
    a. Colectarea, înregistrarea şi raportarea periodică a informaţiilor referitoare la progresul proiectului
    b. Analize trimestriale cu privire la starea implementării proiectului
    c. Determinarea riscurilor în realizarea proiectului şi realizarea de recomandări pentru tratarea acestora
    d. Realizarea managementului documentaţiei proiectului
    e. Monitorizarea şi controlul costurilor, raportare financiară
    f. Coordonarea implementării proiectului conform planului de lucru
    g. Verificarea realizării fiecărei subactivităţi şi activităţi în parte şi acordarea acceptanţelor parţiale către furnizori;
4. Comunicare
    a. Comunicarea permanentă cu echipa implementatorului proiectului în vederea monitorizării progreselor realizate;
    b. Raportarea periodică asupra progreselor realizate în implementarea proiectului, către responsabilul de proiect din partea Ministerului Comunicatiilor si Societatii Informationale;
    c. Menţinerea contactului permanent cu Organismul Intermediar pentru Promovarea Societăţii Informaţionale (OIPSI);

5. Managementul calităţii şi schimbării

    a. Monitorizarea calităţii serviciilor de implementare a proiectului;

    b. Validarea calităţii activităţilor de implementare a proiectului

    c. Managementul activităţilor de acceptanţă a livrabilelor proiectului

Aceste activităţi trebuie considerate ca fiind cerinţe minime, iar dacă alte activitaţi relaţionate sunt necesare în vederea realizării obiectivelor activitatii de management de proiect, acestea vor face parte din responsabilitatea Prestatorului.

Prestatorul va îndeplini toate sarcinile de raportare ale Beneficiarului faţă de Organismul Intermediar, în conformitate cu prevederile Contractului de Finanţare.

Prestatorul va fi responsabil din punct de vedere tehnic şi financiar faţă de Autoritatea Contractantă.

Următoarele activităţi de management al proiectului vor fi realizate de catre Ofertant:

- elaborarea rapoartelor de progres
- suport pentru fundamentarea și elaborarea Cererilor de rambursare
- suport pentru managementul financiar al proiectului
- asigurarea suportului privind informarea şi publicitatea pentru proiectul ce urmează a fi implementat
- elaborarea sistemului de arhivare a documentaţiei proiectului.

Prin personalul pus la dispoziţie de către furnizorul selecţionat în urma acestei proceduri de achiziţie, Ofertantul va realiza următoarele activităţi generale:

<u>Management de proiect</u>

- Monitorizare activitate management de proiect extern – derularea proiectului va fi monitorizată de către o echipă de monitorizare din cadrul Ministerului Comunicatiilor si Societatii Informationale.
- Întocmirea planului de lucru – echipa de management al proiectului va realiza şi agrea un plan de lucru cu toate părţile implicate în proiect
- Raportare – activitatea de întocmire a rapoartelor se întinde pe tot parcursul proiectului.
- Management financiar-contabil – toate cheltuielile aferente proiectului vor fi urmărite cu atenţie, pentru a se asigura respectarea tuturor obligaţiilor şi cerinţelor contractuale.

Activitatea de management reprezintă o activitate continuă pe tot parcursul proiectului

Totodată, managementul proiectului cuprinde activitățile:

- Planificarea activităţilor proiectului pentru încadrarea în graficul de implementare aprobat prin Contractul de Finanţare
- Monitorizarea tuturor activităţilor proiectului, derulate atât de către echipa de proiect a Beneficiarului cât şi de către Furnizor
- Monitorizarea respectării de către furnizorul tehnic a angajamentelor asumate prin contract
- Managementul riscurilor (identificare, analiză, planificare, urmărire) prin întreţinerea unui Registru de Riscuri şi planificarea măsurilor de prevenire şi reducere
- Managementul calităţii prin întreţinerea unui Registru de Calitate în care să se înscrie toate problemele apărute pe durata derulării proiectului (în cadrul testelor de acceptanţă) şi prin urmărirea rezolvării acestor probleme
- Managementul schimbării – pregătirea şi aplicarea unei proceduri de tratare a cererilor de schimbare prin care să se asigure introducerea controlată a schimbărilor în cadrul ciclului de analiză-proiectare-dezvoltare-implementare-testare-acceptanţă.

Management Financiar

- Consultantul va furniza suport în vederea înregistrării cheltuielilor proiectului
- Consultantul va întocmi cererile de rambursare către Finanţator, astfel:

Cerere de rambursare nr.	**Activitate/ subactivitate**	**Data depunerii (ziua x, luna y, anul z de la semnarea Contractului de Finanţare)**
Cerere de rambursare nr. 1	Managementul de proiect/ Implementarea soluţiei/ Instruirea utilizatorilor/Informare si publicitate/ Auditarea proiectului	Până la ultima zi, luna 6, anul 1 de la semnarea contractului
Cerere de rambursare nr. 2	Managementul de proiect/ Implementarea soluţiei/ Instruirea utilizatorilor/Informare si publicitate	Până la ultima zi, luna 9, anul 1 de la semnarea contractului

Cerere de rambursare nr. 3	Managementul de proiect/ Implementarea soluţiei/ Instruirea utilizatorilor/Informare si publicitate/Auditarea proiectului	Până la ultima zi, luna 12, anul 1 de la semnarea contractului
Total asistenţă financiară nerambursabilă		

Raportare către Finanţator

- Consultantul va elabora Rapoartele Tehnice periodice de progres
- Consultantul va elabora rapoartele lunare de stare cu privire la derularea activităţilor proiectului tehnic
- Arhivarea documentelor – are drept scop păstrarea și arhivarea documentelor generate în cadrul proiectului, pentru a asigura o pistă adecvată de audit.

Monitorizarea activităţilor de management al proiectului

Monitorizarea serviciilor de management al proiectului va fi realizată de o echipă de monitorizare din partea Ministerului Comunicatiilor si Societatii Informationale pe baza rapoartelor saptamanale transmise de catre Prestatorul serviciilor de management de proiect

7 RESURSE

7.1 Personal şi instruire

7.1.1 Managementul proiectului, personal si instruire

7.1.1.1 Managementul proiectului

Managementul de proiect reprezintă procesul de coordonare, organizare şi gestionare a activităţilor interdependente şi a resurselor alocate, pentru a asigura atingerea obiectivelor stabilite la standardele de calitate solicitate, în condiţiile existenţei unor constrângeri referitoare la timp, resurse şi costuri.

Metodologia de management de proiect care va fi folosită pentru finalizarea cu succes a tuturor activităților propuse în prezentul proiect are următoarele componente:

I. Activităţi generale de management de proiect

- Planificare si organizare
- Coordonare si monitorizare
- Control si raportare
- Activităţi specifice proiectelor europene:
    - management financiar
    - asigurarea vizibilităţii proiectului în conformitate cu regulile de identitate vizuală prevăzute de Manualul de identitate vizuală publicat pe website-ul O.I.P.S.I
    - asigurarea calității proiectului urmăreşte realizarea unor sisteme eficiente de verificare şi păstrare a documentaţiilor tehnice şi financiare ale proiectului, care să confere siguranţă şi un acces facil la aceste documentaţii, în cazul vizitelor de monitorizare sau al auditurilor parţiale și finale.

7.1.1.2 Personalul și echipa tehnică a proiectului

7.1.1.3 Necesitatea contractării managementului de proiect

Ministerul Comunicaţiilor şi Societăţii Informaţionale va contracta serviciile de management al proiectului, întrucât instituţia doreşte să beneficieze de o expertiză superioară în domeniul managementului proiectelor finanţate prin fonduri europene.

Astfel va fi asigurat suportul pentru Ministerul Comunicaţiilor şi Societăţii Informaţionale în vederea implementării în bune condiţii a proiectului şi elaborarea tuturor documentelor de raportare solicitate de către OIPSI pe perioada implementării acestui proiect. Implementarea în cele mai bune condiții va fi asigurată de către Ministerul Comunicaţiilor şi Societăţii Informaţionale prin furnizarea unei echipe de implementare, prezentată mai sus.

Activităţile de management de proiect ce urmează a fi contractate

Următoarele activităţi de management al proiectului vor fi contractate:

- elaborarea rapoartelor de progres
- suport pentru fundamentarea și elaborarea Cererilor de rambursare
- suport pentru managementul financiar al proiectului
- asigurarea suportului privind informarea şi publicitatea pentru proiectul ce urmează a fi implementat
- elaborarea sistemului de arhivare a documentaţiei proiectului.

Metodologia de management de proiect

Concret, activităţile specifice proiectelor finanţate din fonduri europene vor fi realizate astfel:

I. Achiziţii

În procesul de desfăşurare a procedurilor de achiziţii publice, echipa de achiziţii va utiliza următorul model:

<table>
<tr><th rowspan="2">Valoare Contract (exclusiv TVA)</th><th rowspan="2">Tip contract</th><th colspan="3">Proceduri de achiziţie</th><th>Referinţă legislativă</th></tr>
<tr><td>Achiziţie directă</td><td>Cerere de ofertă</td><td>Licitaţie deschisă</td><td rowspan="2">Art. 19, art.20(1) şi art.124 din O.U.G. nr. 34/2006, cu modificările şi completările ulterioare</td></tr>
<tr><td>Servicii (S) Bunuri (B)</td><td>< 15.000 Euro sau echivalent în lei</td><td>< 125.000 Euro sau echivalent în lei</td><td>≥125.000 Euro sau echivalent în lei</td></tr>
</table>

Procedurile menţionate mai sus se vor derula cu stricta respectare a legislaţiei în vigoare.

Input:

- informaţii privind sistemele informatice existente
- cerinţe de asistenţă tehnică
- analiza de nevoi şi studiu de fezabilitate
- caiete de sarcini şi documentaţii de atribuire pentru servicii şi bunuri

Output:

- Contracte de servicii şi bunuri.

II. Management financiar

Pentru o bună gestionare a bugetului alocat proiectului, până la rambursarea sumelor solicitate, echipa consultantului va elabora un registru de cheltuieli, pentru înscrierea cronologică a tuturor cheltuielilor făcute, defalcate în eligibile şi neeligibile, precum şi a detaliilor documentelor justificative şi a datelor plăţilor efective.

Etapa de verificare a cheltuielilor are ca scop asigurarea conformităţii tuturor cheltuielilor efectuate în cadrul proiectului cu prevederile Ghidului Solicitantului, contractului de finanţare şi legislaţiei în vigoare. Totodată vor fi elaborate cererile de rambursare, care vor însoți rapoartele de progres și care vor fi înaintate spre aprobare către O.I.P.S.I.

Input:

- Documente contabile (facturi, ordine de plată, etc.)
- Planul de cheltuieli
- Bugetul proiectului

Output:

- Registrul de cheltuieli
- Cererile de rambursare

III. Elaborarea rapoartelor de progres şi a cererilor de rambursare

Echipa Consultantului selectat va oferi suport pentru Ministerul Comunicaţiilor şi Societăţii Informaţionale în vederea realizării rapoartelor de progres stabilite prin contractul de finanţare. Astfel rapoartele de progres vor fi elaborate de către Managerul de proiect și înaintate către Coordonatorul de proiect din partea Ministerului Comunicaţiilor şi Societăţii Informaţionale, care va verifica și semna rapoartele mai sus-menţionate. Rapoartele de progres se vor baza pe informațiile din rapoartele de activitate transmise lunar de către Managerul de proiect şi discutate în cadrul întâlnirilor de monitorizare.

Aceste rapoarte vor respecta întocmai cerinţele specificate în Ghidul Solicitantului şi în contractul de finanţare semnat cu O.I.P.S.I. şi vor fi depuse la O.I.P.S.I. la termenele stabilite conform contractului, împreună cu toate celelalte documente solicitate în mod expres prin contractul de finanţare.

Cererile de rambursare, care vor fi ataşate rapoartelor de progres, vor fi elaborate de către Managerului de proiect cu sprijinul Responsabilului Financiar, iar dosarul de rambursare va fi pregătit în conformitate cu cerinţele specificate în contract şi va conţine toate documentele justificative necesare verificării eligibilităţii cheltuielilor efectuate şi efectuării plăţii.

Input:

- Bugetul proiectului, registrul de cheltuieli, documente contabile – în copie certificată
- Contractul de finanţare
- Rapoartele de activitate ale Furnizorilor de servicii şi bunuri

Output:

- Rapoarte de progres
- Cereri de rambursare

IV. Arhivarea documentelor

Conform regulamentelor comunitare circuitul auditului (pista de audit) reprezintă stabilirea fluxurilor informaţiilor, atribuţiile şi responsabilităţile referitoare la acestea, precum şi arhivarea documentaţiei justificative complete, pentru toate stadiile desfăşurării unei acţiuni, care să permită totodată reconstituirea operaţiunilor de la suma totală până la detalii individuale şi invers.

Pista de audit este deci o înregistrare cronologică a activităţilor din proiect pentru a permite reconstrucţia şi examinarea succesiunii de evenimente şi/sau schimbări.

Solicitantul va pregăti și asigura o pistă de audit adecvată prin măsuri de păstrare și arhivare a documentelor astfel încât acestea să nu fie alterate de factorul uman și de timp.

Astfel, cu sprijinul Consultantului, Ministerul Comunicaţiilor şi Societăţii Informaţionale va întreprinde următoarele măsuri:

- exemplarele originale ale facturilor şi documentelor care atestă efectuarea plăţilor vor fi păstrate de către Ministerul Comunicaţiilor şi Societăţii Informaţionale, la locaţia proiectului, împreună cu o copie certificată, atât pe suport de hârtie cât și electronic (CD/DVD etc.).
- documentele elaborate în cadrul proiectului vor fi păstrate astfel: 1 exemplar original şi 1 copie pe suport hârtie cât și în variantă electronică.
- rapoartele, cererile de rambursare şi alte documente oficiale solicitate de către O.I.P.S.I vor fi elaborate într-un exemplar original şi numărul de exemplare - copii stabilite prin contractul de finanţare, care vor fi predate O.I.P.S.I., câte o copie certificată a acestora păstrându-se la sediul proiectului.
- arhivarea se va face la finalizarea proiectului, dosarul complet cu documentele în original va fi păstrat într-un spațiu protejat, împreună cu un CD/DVD cuprinzând toate documentele scanate, acesta rămânând la locaţia proiectului pe perioada legală de arhivare şi păstrare (5 ani post-implementare).

Input:

- bugetul proiectului şi registrul de cheltuieli, documente contabile – în original şi în copie certificată
- contractul de finanţare
- rapoarte de progres şi cereri de rambursare, alte documente realizate în cadrul proiectului
- procedura de arhivare

Output:

- dosarele / cutia de arhivă, corect inscripţionate şi păstrate
- copia în suport electronic a arhivei hard-copy a proiectului

V. Asigurarea vizibilităţii proiectului

Această activitate are o deosebită importanţă în diseminarea oportunităţilor de finanţare puse la dispoziţia administraţiei publice pentru realizarea de sisteme informatice în vederea îmbunătăţirii calităţilor serviciilor către cetăţeni şi mediul de afaceri. Activitatea de informare şi publicitate va respecta reglementările Uniunii Europene, fiind pregătită de către Ministerul Comunicaţiilor şi Societăţii Informaţionale, împreună cu consultantul selectat, şi derulându-se pe tot parcursul proiectului.

Input:

- Planul de informare şi publicitate, informaţii privind proiectul

Output:

- Anunţuri de presă şi comunicate pe website-ul Ministerului Comunicaţiilor şi Societăţii Informaţionale
- Evenimente de începere şi finalizare a proiectului
- Pliante informative şi postere

Cerințe minime solicitate pentru managementul de proiect

Consultantul pentru servicii de management de proiect care urmează a fi contractat va îndeplini următoarele condiţii minime:

Să aibă specialişti în următoarele domenii:

- Managementul proiectului
- Fonduri nerambursabile
- Financiar
- Informare și Publicitate

- Formare / Instruire în managementul de proiect
- IT&C

I. Manager de proiect

Sarcini şi responsabilităţi

Managerul de proiect raportează direct Coordonatorului de proiect şi va asigura coordonarea echipei de consultanţi și asistenţa către Coordonatorului de proiect desemnat de Ministerul Comunicaţiilor şi Societăţii Informaţionale.

Responsabilități:

- Punct unic de contact în relația cu Beneficiarul
- monitorizarea implementării proiectului;
- elaborarea planului revizuit de activităţi şi urmărirea respectării termenelor proiectului;
- elaborarea Rapoartelor de progres ce vor fi înaintate spre aprobarea Ministerului Comunicaţiilor şi Societăţii Informaţionale;
- realizarea în colaborare cu responsabilul financiar a cererilor de rambursare;
- monitorizarea managementului financiar, incluzând verificarea cheltuielilor;
- identifică riscurile și modalitățile de atenuare/evitare a acestora;
- supraveghează îndeplinirea de către furnizor a obligaţiilor asumate în conformitate cu contractul semnat.
- elaborarea sistemului de arhivare a documentelor şi asigurarea pistei de audit aferente beneficiarului;
- coordonarea activităţilor de informare şi publicitate aferente fiecărei etape a proiectului;
- asigurarea accesului uşor la documentaţia proiectului în vederea realizării auditurilor financiare şi tehnice parţiale şi finale.

II. Expert Fonduri Structurale

Responsabilități:

- întocmirea rapoartelor trimestriale de progres;
- întocmirea rapoartelor de progres care însoțesc cererea de rambursare;
- întocmirea Cererilor de rambursare;
- arhivarea dosarului final cu documentele generate în cadrul proiectului (5 ani post-implementare).

III. Responsabil Financiar

Responsabilități:

- elaborarea, împreună cu Coordonatorul de proiect din partea Ministerului Comunicaţiilor şi Societăţii Informaţionale a planului de cheltuieli;
- verificarea disponibilităţii resurselor financiare necesare iniţierii proiectului;
- asistenţă la elaborarea cererii de prefinanţare;
- verificarea cheltuielilor;
- verificarea aspectelor financiare ale contractelor de achiziţii publice;
- elaborarea dosarului de rambursare;
- contribuţie la elaborarea rapoartelor de progres;
- asigurarea accesului la documentaţia financiar-contabilă pentru auditorul extern;
- transfer de cunoştinţe specifice de management financiar către echipa de implementare.

IV. Manager de proiect tehnic

Responsabilități:

- gestionarea implementării sistemului (componente hardware; software; securitate);
- coordonarea întregii echipe tehnice, cu alocarea sarcinilor pe fiecare membru al echipei;
- asigură o adresă de e-mail funcțională în scopul facilitării comunicării dintre echipa de proiect și beneficiar;
- asigură resurse pentru executarea serviciilor de implementare cuprinse în caietul de sarcini;
- menține și aplică managementul riscului și procedurile de asigurare a calității;
- întocmește toate rapoartele necesare conform cerințelor proiectului și /sau alte rapoarte cerute de către Managerul de Proiect.

V. Arhitect de soluție

Responsabilități:

- asigură proiectarea sistemului, începând din faza de analiză;
- asigură asistență și suport pentru pregătirea și validarea planurilor de calitate în vederea construirii și asigurării mentenanței sistemelor informatice
- raportează stadiului privind implementarea soluţiei către Managerul de proiect şi către Coordonatorul de proiect din partea Ministerului Comunicaţiilor şi Societăţii Informaţionale.

VI. Arhitect infrastructură hardware și comunicații

Responsabilități:

- evaluarea necesităților infrastructurii hardware și de comunicații, precum și implementarea părții de comunicații din proiect;
- raportarea stadiului privind implementarea soluţiei către Managerul de proiect şi către Coordonatorul de proiect din partea Ministerului Comunicaţiilor şi Societăţii Informaţionale.

VII. Expert analist de business

Responsabilități:

- realizează studii de consultanță cu privire la aspectele organizatorice în dezvoltarea TIC a sistemelor informatice;
- analizează și definește procesele de business (work-flow) și elaborează specificațiile de proces;
- coordonează analiza cerințelor de schimb de date cu toate structurile implicate și elaborează raportul diagnostic.

VIII. Specialist în informare și publicitate

Responsabilități:

- asigură informarea și publicitatea proiectului conform normelor de vizibilitate ale U.E;
- realizează comunicatele / anunțurile de presă;
- organizează evenimentele de informare din cadrul proiectului;
- realizează materiale promoționale.

IX. Specialist documentare tehnică și asigurarea calității

Responsabilități:

- pregătește întreaga documentație suport aferentă implementării și transferului de know-how către Beneficiar;
- urmărește implementarea metodologiilor de dezvoltare / instalare / testare / validare software;
- urmărește asigurarea calității în procesul de dezvoltare / instalare / testare / validare software;

X. Specialist în formare/instruire profesională

Responsabilități:

- Asigură formarea/instruirea în managementul de proiect;

Procedura de monitorizare utilizată de echipa de management

Procesul de monitorizare presupune obţinerea informaţiilor care să permită cunoaşterea şi înţelegerea stadiului proiectului la un moment dat, precum şi tendinţele de derulare a activităţilor incluse în proiect. Monitorizarea se poate face prin discuţii cu personalul implicat în derularea proiectului, prin înregistrarea rezultatelor şi a problemelor apărute, prin observarea activităţilor derulate. Monitorizarea permanentă a proiectului (se monitorizează activităţile, stadiul realizării planurilor, costurile, rezultatele proiectului) permite raportarea realizării acestuia, astfel obţinându-se informaţiile a căror procesare sprijină procesul de raportare.

Procedura de monitorizare a echipei de managementul proiectului contractate va include următoarele aspecte, fără a se limita doar la acestea:

- livrarea documentelor şi rapoartelor necesare la timp, respectând cerinţele impuse de Ghidul Solicitantului, Contractul de Finanţare şi anexele sale, procedurile europene, legislaţia românească relevantă, planul de activităţi şi termenele stabilite și înaintate spre aprobare Beneficiarului;
- activităţile de informare/publicitate (pentru serviciile de audit şi informare şi publicitate, dacă este cazul) sunt implementate conform planului de informare / publicitate și în conformitate cu Manualul de Identitate Vizuală;
- activităţile de achiziţii sunt finalizate conform planificării proiectului, fiind implementate conform legislaţiei româneşti în vigoare;
- rapoartele de progres pe baza rapoartelor de activitate ale proiectului, furnizate de către Consultant sunt aprobate de O.I.P.S.I.;
- cererile de rambursare înaintate către O.I.P.S.I. şi elaborate cu asistenţa Managerului de proiect;
- calitatea şi transparenţa sistemului de arhivare şi înregistrare a informaţiilor, vor fi monitorizate prin uşurinţa accesului specialiştilor care vor efectua auditurile tehnice şi financiare parţiale şi finale la documente, echipamente şi soluţii şi tehnologii.

Calendarul aferent activităţilor de monitorizare este reprezentat în tabelul de mai jos:

Activităţi de monitorizare	Perioada de monitorizare (fiecare celulă reprezintă 1 lună calendaristică)											
	1	2	3	4	5	6	7	8	9	10	11	12
Şedinţe de monitorizare												
Controlul costurilor												
Rapoarte lunare de activitate												
Rapoarte de progres												

Echipa consultantului, echipa internă a instituţiei şi Coordonatorul de proiect se vor întâlni bilunar, în şedinţe de câte două ore, pentru ca informaţiile discutate să poată fi transmise, asimilate şi puse în aplicare, într-un interval redus de timp. Şedinţele de monitorizare bilunare se vor finaliza cu un proces verbal, care va fi semnat de toţi participanţii şi care va fi arhivat, în original. Copii după procesul verbal vor fi transmise fiecărui participant şi măsurile implementate vor fi discutate în deschiderea şedinţei următoare.

Monitorizarea proiectului va urmări criteriile specificate mai sus şi va fi consecventă pentru toţi membrii echipei care urmează a implementa proiectul, atât reprezentanţi ai Consultantului, cât şi angajaţi ai instituţiei.

Această activitate se va baza în mod exclusiv pe date cuantificabile, pe indicatori şi surse de verificare agreaţi în prealabil, în şedinţa de începere a proiectului, când s-a fundamentat Planul de activităţi şi planul de jaloane (milestones) ale proiectului, pe procesele verbale ale şedinţelor de monitorizare precedente şi pe baza termenelor şi condiţiilor prevăzute în alte documente elaborate în cadrul proiectului (planul de achiziţii, planul de informare şi publicitate, etc.).

Persoanele desemnate în echipa tehnică asigură configurarea sistemul informatic în funcţie de soluţiile adoptate, le integrează în fluxul activităţilor Administrației Centrale, definesc planul testului de acceptanţă al sistemului implementat, realizează testele pe date reale ale sistemului, sesizează eventuale disfuncţiuni, propun modalităţi de rezolvare, modalităţi de abordare a problemelor apărute. Se asigură că implementarea tehnică a sistemului să fie executată conform scopului propus.

Instruirea personalului care va utiliza/administra aplicaţia va fi realizată în cadrul a două activităţi de instruire specifică organizate în funcţie de tipul de utilizatori (utilizatori şi administratori). Astfel sunt propuse următoarele:

instruirea dedicată utilizatori cheie (Ingineri suport sistem) ai soluţiei care urmează a fi achiziţionată;
instruirea dedicată persoane care vor asigura administrarea soluţiei (Administratori sistem).

Se urmăreşte ca activitatea de instruire să cuprindă minimul de topici din modulele din tabelul următor:

Denumire curs	Durată	Participanţi	Tematică minimă necesară
Administrare baze de date 1	5 zile	Administratori sistem; Ingineri suport sistem	Instalarea şi configurarea bazelor de date Crearea şi administrarea conturilor de utilizator Backup and Recovery
Administrare baze de date 2	5 zile	Administratori sistem;	Crearea şi gestionarea seturilor de backup şi a copiilor imaginilor Recuperarea bazelor de date la un moment anterior în timp Refacerea bazei de date Depistarea blocurilor corupte şi aplicarea măsurilor corespunzătoare pentru corectarea lor Utilizarea diverselor componente pentru monitorizarea şi îmbunătăţirea performanţei bazelor de date Controlul folosirii resurselor bazelor de date Simplificarea sarcinilor de management Monitorizarea fişierelor log în scopul unei diagnoze corecte Setări dependente de limbă şi teritoriu (globalizare) atât pentru sesiuni individuale, cât şi la nivelul bazei de date Monitorizarea şi gestionarea memoriei Gestionarea resurselor
Construirea de rapoarte	5 zile	Ingineri suport sistem; Administratori de sistem	Proiectarea şi rularea rapoartelor Lucrul cu dezvoltatorul de rapoarte Crearea unui raport de printat Îmbunătăţirea unui raport de bază de printat Administrarea modelelor de rapoarte Crearea unui raport web Îmbunătăţirea rapoartelor utilizând modelul de date: interogări şi grupuri Îmbunătăţirea rapoartelor utilizând modelul de date: surse de date Îmbunătăţirea rapoartelor utilizând modelul de date: crearea coloanelor Îmbunătăţirea rapoartelor utilizând

Denumire curs	Durată	Participanţi	Tematică minimă necesară
			layout-ul paginii Controlul layout-ului paginii: proprietăţi comune Controlul layout-ului paginii: proprietăţi specifice Raportare pe web Creşterea funcţionalităţii utilizând XML Crearea şi utilizarea parametrilor rapoartelor Încorporarea unui grafic într-un raport Îmbunătăţirea rapoartelor matriciale Creşterea funcţionalităţii Maximizarea performanţei Principii de eficienţă în construirea rapoartelor
Construirea, testarea şi exploatarea aplicaţiilor Internet	5 zile	Ingineri de suport sistem	Crearea modulelor formelor Lucrul cu blocuri de date şi frame-uri Utilizarea paletei de proprietăţi Utilizarea elementelor de intrare Utilizarea elementelor de tip „non-input” Crearea ferestrelor Elaborarea trigger-ilor Corectarea trigger-ilor Adăugarea de funcţionalităţi item-ilor Interogarea trigger-ilor Validare Navigare Procesarea tranzacţiilor Scrierea de cod flexibil Partajarea obiectelor şi a codului Utilizarea instrumentelor pentru interacţiunea cu clientul Prezentarea aplicaţiilor cu forme multiple
Programare	5 zile	Administratori de sistem; Ingineri suport sistem;	Declararea de identificatori Scrierea de instrucţiuni executabile Interacţiunea cu serverul Scrierea de structuri de control Lucrul cu tipuri de date compuse Folosirea de cursoare explicite Tratamentul excepţiilor Crearea de proceduri stocate Crearea de funcţii stocate Exemplificarea de noi concepte privind pachetele de date Folosirea pachetelor în dezvoltarea de aplicaţii

Denumire curs	Durată	Participanţi	Tematică minimă necesară
			Managementul dependenţelor Manipularea obiectelor mari Crearea triggerilor Aplicații bazate pe triggeri Înţelegerea şi influenţarea compilatorului

7.2 Resurse materiale

Beneficiarul va pune la dispoziţia echipei de proiectare a sistemului informatic următoarele:

O sală în care se vor derula întâlnirile de lucru dintre echipele de proiect din partea integratorului şi a beneficiarului;
Un spaţiu tehnic pentru amplasarea echipamentelor din cadrul proiectului;
Beneficiarul nu va asigura resurse de tip tehnică de calcul pentru echipa de proiect a integratorului (staţii de lucru, interconectare locală şi/sau acces la internet sau reţele de voce);

8 MENTENANTA ŞI SUSTENABILITATE

8.1 Mentenanţă

Mentenanţa soluţiei informatice:

În timpul perioadei de garanție de 36 luni (pentru produsele hardware si software), Furnizorul va furniza pe baza acestui Service Level Agreement (SLA) următoarele servicii de suport:

- Servicii de Help Desk;
- Fault Management;
- Suport în caz de urgentă;
- Rapoarte de deranjamente și corelarea erorilor;
- Subscripții software.

Problemele ridicate de Beneficiar vor fi înregistrate de către specialiști ai Furnizorului, în cadrul unei aplicații de tip HELPDESK.

Accesul la suportul telefonic, web sau e-mail va fi valabil șapte zile pe săptămână, 24 ore pe zi, 365 zile ale anului.

Clasificarea nivelelor de deranjament:

Definițiile priorităților de deranjament sunt cele de mai jos:

Prioritate	Descrierea nivelului de prioritate
CRITIC	Deranjamente care afectează serviciile, cauzând nefuncționarea sistemelor sau blocarea funcțiilor importante de rețea sau subsisteme. Aceste deranjamente afectează în mod direct serviciile furnizate de elementele sau subsistemele de rețea, restricționează în mod semnificativ activitățile de operare în rețea sau clientul este afectat în totalitate.
MINOR	Problemele minore nu au un impact semnificativ în funcționarea sistemelor și nu afectează în mod direct serviciile clienților. Aceste probleme sunt tolerate în folosința sistemelor.

Timpi de răspuns și rezoluții

Timpii de răspuns și rezoluțiile problemelor sunt stabilite pentru fiecare categorie în parte. La sfârșitul fiecărui caz deschis Furnizorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și va fi inclusă în recomandarea finală.

Furnizorul va respecta următorii timpi de răspuns:

Timp de răspuns	Timp soluție provizorie	Timp de remediere
8 ore	A doua zi lucrătoare	best-effort

Timpii de mai sus sunt calculați din momentul în care Furnizorul a fost înștiințat de apariția problemelor.

Furnizorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport software furnizate în cadrul acestui contract. În cazul în care apare un deranjament hardware, timpii de răspuns vor fi calculați, deasemenea, pe baza tabelului de mai sus.

Definițiile, descrise mai jos se vor aplica la Service Level Agreement:

Timp de Remediere	Durata de timp până la oferirea soluției finale
Timp de Răspuns	Timpul scurs de la contactul inițial dintre Beneficiar și HELPDESK și răspunsul primit de la echipa de suport tehnic a Furnizorului către Beneficiar. Această acțiune se va desfășura prin intermediul telefonului.
SLA	Service Level Agreement identifică funcționalitățile și definește procesele care implică livrarea de către Furnizor a diferite servicii de suport către Beneficiar.
Subscripție Software	Acces înregistrat la modificări, corectări, și/sau update-uri de Software; incluzând Hotfixuri, Service Packuri, Feature Packs, și/sau upgrade-uri majore, oferite către Beneficiar prin intermediul suportului electronic (e-mail) sau prin suport fix media.
Suport	Telefonul de suport tehnic, asistentă web și e-mail oferite de Furnizor pentru a ajuta Beneficiarul în rezolvarea problemelor apărute. Suportul este oferit la un Major Release al produsului și la un Release Secvențial Anterior al produsului. Furnizorul va oferi de asemenea asistentă tehnică pentru versiunile mai vechi ale produsului, dar rezolvarea problemei ar putea fi limitată la instalarea unui Major Release. Suportul nu include nici un fel de servicii educaționale sau profesionale. Serviciile de training sau de suport on site pot fi achiziționate în plus fată de cele de Suport.
HELPDESK	Un centru de asistentă tehnică ce oferă serviciul de preluare a cererilor prin telefon, web și e-mail operat de către personalul care face parte din suportul Furnizorului oferind asistentă cu diagnosticare și rezoluție a defecțiunilor și/sau avariilor apărute în cazul produselor CheckPoint care sunt în conformitate cu documentația publicată când produsele sunt instalate și utilizate conform specificațiilor software-ului CheckPoint.
Remediere Temporară	O modificare în cadrul procedurilor sau datelor care să evite erorile fără folosirea defectuoasă a produselor.

Mentenanța licenţelor achiziţionate

Descrierea Serviciilor

Furnizorul va furniza Servicii de Mentenanță după lansarea în producție a sistemului, care vor cuprinde:

- Suport pentru customizările și dezvoltările / extensiile din cadrul implementării
- Suport pentru produsele/modulele utilizate în dezvoltarea sistemului informatic
- Suport pentru platforma hardware/ sistem de operare utilizată

Pentru a permite o identificare proactivă a unor posibile soluții, se va asigura acces la o bază de cunoștințe tehnice și/sau documentație tehnică specifică.

Suport implementare:

Echipa de implementare va asigura suport la darea în producție pe o perioadă de 1 lună. După această perioadă va fi desemnat un singur punct de intrare pentru toate incidentele legate de soluția implementată și anume către Administratorul de Servicii al Furnizorului. Administratorul de Servicii al Furnizorului va:

- administra și monitoriza incidentele,
- lua legătura cu persoana desemnată ca punct de contact din partea Beneficiarului, pentru analiza stărilor incidentelor deschise,
- va răspunde tuturor întrebărilor legate de incidente.

Suportul va fi furnizat intre [09:00 și 18:00] ora României, de Luni până Vineri cu excepția sărbătorilor legale. Se va asigura diagnosticarea unui incident pentru determinarea problemei de bază. Se va monitoriza în permanentă incidentul până la închiderea acestuia

Urmărirea incidentelor

Persoana desemnată ca punct de contact din partea Beneficiarului va lansa un incident, Administratorul de Servicii al Furnizorului primind o notificare pe e-mail sau fax. Fiecare incident va avea atașat un nivel de prioritate (ca în exemplele de mai jos) care să reflecte impactul problemei asupra funcționării sistemului. Inițial atașarea nivelului de prioritate se va face cu ajutorul Administratorului de Servicii al Furnizorului pentru a facilita rezolvarea incidentului în timp util. Nivelul de prioritate poate fi modificat cu acordul părților în funcție de evoluția incidentului. Furnizorul poate să își rezerve dreptul de a modifica un incident dar cu anunțarea în avans a echipei Beneficiarului. Serviciile de Suport vor fi furnizate sub incidenta Clauzelor de Confidențialitate.

Asistenta poate fi de două tipuri:

- on site (la sediul clientului acolo unde e posibil)
- remote (clientul este responsabil să asigure acces VPN consultanților care vor remedia problema)

Nivele de Prioritate:

Nivel Prioritate	Descriere
Urgent	Impact Major asupra funcționării sistemului Problema împiedică desfășurarea activității instituției, procesul de activitate este serios afectat și nu mai poate continua pierderea funcționalităților devenind critice. Un incident de Nivel 1 are una sau mai multe din următoarele caracteristici: Date corupte Funcții importante indisponibile Sistemul este „agățat" cauzând întârzieri neacceptabile în accesul la resursele sistemului și/sau în timpul de răspuns Căderea completă a sistemului sau căderi repetate după restart
Critic	Impact Semnificativ asupra funcționării sistemului Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. Nici o soluție alternativă nu este disponibilă, iar activitatea utilizatorilor poate totuși continuă, însă într-un mod restrictiv.
Major	Impact Mediu asupra funcționării sistemului. Problema afectează minor funcționalitățile sistemului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.
Minor	Impact Minim asupra funcționării sistemului. Problema nu afectează funcționalitățile sistemului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor.

În cazul incidentelor cu nivel de prioritate "urgent" asistenta va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta Beneficiarul va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

Servicii de Mentenanța

Furnizorul va furniza următoarele Servicii de Mentenanță pentru Extensii (customizări și dezvoltări):

Suport pentru Extensii

Furnizorul va asigura suport pentru extensii dacă problema este de tip funcțional sau de performanță ce derivă din funcționalitățile din documentațiile referitoare la eventualele extensii.
Serviciile post-implementare vor fi oferite către Beneficiar în cadrul unui contract separat pentru toate customizările și modificările efectuate pe perioada desfășurării proiectului, în concordantă cu activitățile descrise mai sus.

8.2 Sustenabilitate

Sustenabilitatea instituţională va fi realizată prin:

instruirea a 10 utilizatori ai soluţiei care urmează a fi achiziţionată

instruirea a 4 persoane care vor asigura administrarea soluţiei.

După implementare, Beneficiarul va asigura atât operarea noului sistem cât și suport tehnic, după cum urmează:

Operare:

Autentificare / Autorizare;
Informare;
Acces la proceduri electronice;
Tracking & History;

Suport:

Probleme tehnice ale soluției;
Aspecte legate de utilizarea portalului, crearea fluxurilor de documente etc.;

Beneficiarul va defini grupuri care vor fi implicate în implementarea proiectului și care vor asigura ulterior menținerea rezultatelor după cum urmează:

Un grup cu atribuții de susținere a implementării soluției informatice având ca responsabilitate următoarele atribuţiuni de bază:

- implementarea aplicaţiilor pentru domeniile de activitate ale instituției;
- informatizarea activităţilor;
- elaborarea și validarea specificațiilor tehnice;

Un grup responsabil atribuții de analiză funcțională responsabil cu:

- analiza proceselor care vor fi derulate în urma implementării soluției informatice;
- elaborarea și validarea specificațiilor funcționale;