BANCA NAȚIONALĂ A ROMÂNIEI

Direcția Achiziții

CAIET DE SARCINI PRIVIND ACHIZIȚIA

"Platforma e-Commerce"

Forma documentului:

Inițială	**X**
Modificată	
Numărul revizuirii	

Denumirea contractului

Platforma e-Commerce

Cuprins

1. Introducere

Specificațiile tehnice, aferente caietului de sarcini, fac parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

Specificaţiile tehnice definesc caracteristicile solicitate privind produsul ce face obiectul achiziţiei.

În cadrul acestei achiziții, Banca Națională a României îndeplinește rolul de Autoritate contractantă, respectiv Autoritatea contractantă în cadrul Contractului de furnizare aplicație de tip eCommerce (magazin online).

2. Contextul realizării acestei achiziții de produse

O aplicație informatica de tip eCommerce (magazin online) va permite comercializarea on-line de către BNR a produselor sale numismatice.
Banca Naţională a României, banca centrală a României, cu sediul central în municipiul Bucureşti, consideră necesară achiziționarea unei astfel de aplicații informatice de tip eCommerce (magazin online) pentru a facilita procesul de valorificare a produselor numismatice emise.
Aplicația tip eCommerce (magazin online) va fi utilizată în centrala BNR şi în cele şase sucursale regionale Bucureşti, Iaşi, Cluj, Timiş, Dolj şi Constanţa.

3. Descrierea produselor si serviciilor solicitate

Soluţia informatica de tip eCommerce, va avea următoarele componente:

- Platformă software de tip eCommerce, inclusiv licenţele aferente
- Servicii de configurare platformă eCommerce pentru a răspunde cerințelor funcționale ale BNR, inclusiv dezvoltări software la cheie, dacă acestea vor fi necesare
- Servicii de instruire pentru utilizatori back-office
- Asistență la lansarea în producție a soluției eCommerce
- Servicii de suport tehnic și mentenanţă soluție pe o perioadă de 5 luni

Soluția va fi utilizată în centrala BNR şi în cele şase sucursale regionale București, Iaşi, Cluj, Timiş, Dolj şi Constanţa, de un numar de până la 20 de utilizatori.

Aplicaţia trebuie proiectată astfel încât să poată fi adăugaţi, la nevoie, şi alţi utilizatori, cu modificarea în consecinţă a conţinutului acesteia, dacă se va considera pe viitor necesar acest lucru.

Cerințe tehnice privind soluția eCommerce

Soluția eCommerce trebuie să fie bazată pe o platformă matură, disponibilă pe piață la momentul ofertării. Propunerea tehnică va include toate licențele necesare funcționării soluției, incluzând licențele de platformă eCommerce și mentenanța acestora pe perioada indicată.

Platforma pe care se bazează soluția eCommerce va fi instalată pe infrastructura pusă la dispoziție de către BNR, conform cerințelor hardware și software. BNR va pune la dispoziția ofertantului declarat câștigător infrastructura virtualizată incluzând sistemele de operare necesare instalării platformei eCommerce. Nu se acceptă platforme găzduite la furnizori de servicii sau platforme oferite ca și serviciu.

Platforma propusă trebuie să îndeplinească următoarele cerințe:

- Să beneficieze de update-uri periodice din partea producătorului, inclusiv pe partea de securitate
- Să ofere scalabilitate și posibilitatea de deploy în orice fel de arhitectură, fie ea clasică (monolit) sau bazată pe microservicii, într-un server dedicat sau într-unul care se bazează pe containere docker
- Să ofere modalități flexibile pentru importul și exportul de date și conectarea la diferite sisteme terțe (OMS-Order Management System, ERP-Enterprise Resource Planning, etc), fiind compatibila cu diverși conectori pentru realizarea acestor conexiuni
- Să fie dezvoltată pe o arhitectură modulară care permite adăugarea/scoaterea cu ușurință a diverselor componente în funcție de nevoile de implementare și de business
- Să recomande un set de bune practici ce trebuie respectate de către dezvoltator pentru a asigura posibilitatea unui upgrade in timp fără a afecta implementările adiționale cerute de către BNR
- Producătorul platformei să ofere un sistem de certificări pentru dezvoltatori astfel încât furnizorii de soluții bazate pe această platformă să ofere cele mai înalte standarde de calitate

- Platforma trebuie sa asigure un volum de trafic ridicat, dispunând de mecanisme pentru îmbunătățirea performanței
- Trebuie sa fie o platformă adoptata global, si trebuie sa aibă o comunitate activă și mare de utilizatori

Cerințe funcționale privind soluția eCommerce

a. Cerinte funcționale generale

Solutia eCommerce va asigura posibilitatea de achiziţionare online a produselor numismatice ale BNR si va oferi următoarele funcționalități:

Accesarea soluției - Soluţia va fi accesabilă printr-un link de tip subdomeniu (de exemplu eshop.bnr.ro) sau link dedicat (de exemplu www.bnr.ro/eshop) aflat pe site-ul BNR în pagina de prezentare a emisiunilor numismatice, în pagina comunicatului de presă şi în pagina de prezentare a fiecărui produs nou lansat după intrarea în producție a acesteia. Soluția va fi de sine stătătoare și va funcționa în afara site-ului BNR.

- Afișarea produselor - Soluția va prezenta clienților indiferent dacă sunt sau nu conectați în cont lista de produse disponibile pentru achiziție online, fiecare produs având o descriere textuală dar și câteva fișiere de tip imagine de prezentare vizuală a acelui produs, respectiv o informare cu titlu orientativ asupra stocului disponibil, de tip status bar.
- Înregistrarea clienților - Soluția trebuie să ofere clienților posibilitatea de a-şi crea un cont de utilizator. Prin crearea unui cont, un utilizator isi va putea completa datele de contact, de identificare fiscală în vederea emiterii facturilor de către BNR (în funcție de tipul de persoană fizică/juridică), respectiv va putea consulta istoricul comenzilor si statusul fiecărei comenzi, dar și alegerea ghișeului favorit de unde să ridice produsele. Crearea unui cont de utilizator va permite utilizatorilor să afișeze, indiferent de locația de conectare, toate informațiile din cont, inclusiv coșul de produse. Clientul va fi informat printr-un mesaj din pagina de creare a contului asupra modului în care vor fi folosite datele pe care le va furniza, o informare privind prelucrarea datelor cu caracter personal. După transmiterea acestor date soluţia va genera link de confirmare a contului, pe care-l va trimite pe e-mail-ul clientului, din pagina de creare a contului, în scopul validării acestuia.

- Plasarea comenzilor și achiziția online a produselor numismatice - Soluţia trebuie să permită ca produsele să poată fi cumpărate prin plasarea de comenzi în platformă, atât cu plata online cât şi cu plata la ghişeele sucursalelor regionale ale BNR. Achizițiile online se vor putea realiza de către utilizatorii înregistrați cu cont, sau direct fără a fi necesară crearea unui cont de utilizator. Înainte de plasarea unei comenzi, indiferent daca utilizatorul este înregistrat sau nu, se vor completa toate datele necesare emiterii facturii conform legislației cât și datele de contact ale clientului (nume și prenume, adresă email și număr telefon). Opțiunea legată de modalitatea de plată (online sau la ghișeu) va fi oferită doar utilizatorului conectat în cont la momentul plasării comenzii, în timp ce utilizatorii neînregistrați vor putea plăti exclusiv online. În pagina prin care se solicită clientului să opteze sau nu pentru crearea unui cont de utilizator, acesta va fi informat asupra celor de mai sus. Aplicația trebuie să identifice, după un criteriu ales, persoanele care optează pentru plata la ghişeu dar care nu se prezintă să cumpere produsul rezervat, în termenul stabilit în calendarul pus la dispoziție în pagina de cumpărare și comunicat ulterior prin e-mail, pentru a nu mai avea posibilitatea de rezervare a produsele numismatice, ci doar de cumpărare cu plată on-line. Aplicaţia va trebui să permită selectarea automată a clienţilor care se află în acestă situaţie şi să le trimită un mesaj automat pe e-mail în ziua imediat următoare după expirarea termenului de rezervare, cu informare în acest sens. Criteriul de selecție va fi în funcție de numărul de rezervări efectuate, dar fără realizarea achiziției efective a produselor numismatice, pe o anumită perioadă de timp stabilită și menționată în secțiunea *Termeni și condiții*. Criteriile de identificare vor fi nume și prenume, adresă de e-mail și număr de telefon. Din criteriile menționate se vor folosi doar câte două, alternativ.
- Gestionarea stocurilor online - Soluția va gestiona integral stocul de produse aflat în gestiunea online și îl va afișa utilizatorilor informațiile generale legate de stoc, te tip status bar. Adăugarea în coșul decumpărături a unui produs nu reprezintă o modalitate de rezervare a produselor. Soluția trebuie să informeze utilizatorii cu privire la disponibilitatea stocului de produse în procesul de plasare a comenzii, înainte de pasul de plată.
- Urmărirea livrării produselor - Produsele numismatice achiziţionate vor fi ridicate de la ghişeele sucursalelor regionale și nu fac obiectul transmiterii prin intermediul societăților de curierat. În schimb, soluția trebuie să genereze emailuri către clienți privind statusul de procesare al comenzii, inclusiv notificarea privind disponibilitatea de ridicare a produsului comandat de la ghişeele sucursalelor regionale.

- Integrarea cu un procesator de plăți online - În cazul plăţii online, produsele vor putea fi ridicate numai după confirmarea tranzacției de către procesatorul de plăți. În acest sens soluția trebuie să asigure confirmarea automată a tranzacțiilor din partea procesatorului de plăți, inclusiv prin trimiterea unui mesaj de confirmare pe adresa de e-mail a clientului cuprinzând informațiile de procesare a plății. În acest mesaj, clientul va fi informat asupra datei estimative începând de la care îşi va putea ridica produsele de la ghişeul sucursalei alese
- Notificări - Aplicaţia va trimite un mesaj pe e-mail-ul respectivei sucursale pentru a i se aduce la cunoştinţă că produsul poate fi înmânat clientului la momentul prezentării acestuia la ghişeu.

În situaţia în care optează pentru plata la ghişeu, clientul are obligaţia de a o efectua în termenul comunicat la efectuarea înregistrării.

Procesul de achiziţie online atât pentru clienţii care au cont, cât şi pentru cei fără, se va desfăşura astfel:

Clientul va selecta produsele dorite dintr-o secţiune a aplicaţiei creată în acest scop. În acestă secţiune vor fi afişate denumirea produselor, imaginile lor, caracteristicile lor tehnice, descrierea şi tirajul, cât și o indicație asupra stocului online disponibil, de tip status bar. Soluția va trebui să permită introducerea acestor date fără a limita numărul de caractere. În această secţiune vor fi încărcate toate produsele numismatice ale BNR disponibile la vânzare.

Produsele numismatice ale căror stocuri se epuizează vor rămâne afișate în magazinul virtual și după epuizarea stocului, dar cu mențiunea *stoc zero*. Ștergerea acestora se va realiza doar de administratorul aplicației.

b. Cerințe funcționale care privesc utilizatorii publici ai soluției

Interfața prezentată utilizatorilor publici va cuprinde următoarele secțiuni/ pagini:

- Secţiunea magazin în care sunt prezentate produsele numismatice disponibile şi în care clientul are posibilitatea să-şi selecteze produsul dorit. Fiecare produs va avea o limitare a numărului de bucăţi, care poate fi comercializat către un singur client (limită asupra cantității care se poate comanda în cadrul unei comenzi)
- Pagina Coş de cumpărături
- Pagină de logare şi recuperare a parolei.

- Pagina de creare/administrare a contului de utilizator, în care clientul îşi poate crea cont de utilizator, dacă nu are, sau poate modifica datele contului.
- Secţiunea de cumpărare, care cuprinde datele de identificare ale clientului. În cazul în care clientul are deja cont, datele lui de identificare sunt preluate automat în pagină din profilul său, iar dacă nu are cont de utilizator, clientul trebuie să-şi completeze datele de identificare (aceleaşi ca şi cele care se cer clienţilor care optează pentru a-şi face cont).

  Această secţiune cuprinde următoarele:

1. Denumirea sucursalelor BNR cu opţiune de selectare, astfel încât clientul să poate alege de unde doreşte să-şi ridice produsele.
2. Modalităţi de plată (i) on-line şi (ii) la ghişeul sucursalei selectate. În situaţia în care clientul nu are cont de utilizator va plăti doar on-line, rubrica plăţii la ghişeu va fi dezactivată.
3. Calendar de programare a datei achiziționării produsului selectat.
4. Câmp cu numele şi prenumele persoanei care se va prezenta la ghişeul sucursalei selectate pentru a ridica produsele în numele cumpărătorului în situaţia în care acesta nu se poate prezenta personal.
5. Termeni şi condiţii privind cumpărarea, cu bifă obligatorie de acceptare.
6. Informări privind protecţia datelor cu caracter personal, cu bifă obligatorie de acceptare, pentru a se putea trece mai departe.

Secţiunea de plată on-line conţine paginile specifice plăţilor directe cu cardul.

- După efectuarea plăţii on-line, aplicaţia va transmite automat pe e-mailul clientului un mesaj de confirmare a faptului că produsele dorite de acesta au fost reţinute pe numele lui. Totodată, aplicaţia va trimite un mesaj pe e-mailul sucursalei selectate de client pentru a i se aduce la cunoştinţă că produsul poate fi înmânat clientului la momentul prezentării acestuia la ghişeu. Clienţii care optează pentru plata online se vor prezenta la sediul sucursalei selectate, pentru a ridica produsele, iar factura se va genera în platformă, pe baza datelor deja introduse de aceştia în secţiunea de cumpărare.
- Pagină plată la ghişeu. Dacă se optează pentru plata la ghişeu în secţiunea de cumpărare, aplicaţia va transmite automat pe e-mailul clientului un mesaj de confirmare a faptului că produsele dorite de acesta au fost reţinute pe numele lui şi că se poate prezenta la ghişeul sucursalei selectate pentru a le achiziționa, în data aleasă.

Totodată, aplicaţia va trimite un email sucursalei respective, pentru a transmite datele personale ale clientului şi produsele pe care trebuie să le pregătească pentru acesta. Clienţii vor ridica produsele după achitarea contravalorii acestora, numerar sau cu cardul bancar. Factura se va emite şi în acest caz prin aplicaţie, prin importarea datelor de identificare comunicate de aceştia în secţiunea de cumpărare. În situația comenzilor plasate cu plată la ghișeu și neridicate în termenul stabilit, soluția va anula comanda și produsul respectiv va întoarce în stocul comercializării online.

În scopul celor de mai sus, aplicaţia va trebui să poată trimite date către aplicaţia contabilă a BNR.

c. Cerințe funcționale care privesc utilizatorii interni ai BNR

Interfaţa destinată administratorilor:

Soluția va genera rapoarte privind stocurile de produse şi modul de rezervare/ valorificare a acestora, pe fiecare produs sau pe grupe definibile de produse şi pe sucursale, etc.

Sucursalele vor avea alocate conturi de utilizatori privilegiati care le vor permite acestora sa efectueze urmatoarele operatii:

- urmarirea stocului propriu disponibil în gestiunea online,
- urmarirea comenzilor efectuate de clienti si care vor fi livrate prin unitatea respectiva
- emiterea facturilor la prezentarea clientului care a efectuat plata on-line
- emiterea facturilor pentru clientii care doresc sa faca plata la ghiseu

Soluția trebuie să poată genera rapoarte statistice la interogare de către utilizator privind stocurile de produse şi modul de valorificare a acestora, pe fiecare produs sau pe grupe definibile de produse şi zone, etc.

Utilizatorii cu rol de administrare-gestionare stocuri vor putea introduce noi produse în magazin, seta stocul total destinat comenzilor online, la nivel centralizat cât şi pe sucursale.

Utilizatorii cu rol de administrare clienţi vor avea acces şi drepturi depline la informaţiile înregistrate de clienţi (inclusiv ştergere din baza de date), verificarea istoricului comenzilor efectuate, a plăţilor, setarea parametrilor (bonitate) etc.

Parametrii sistemului vor fi accesibili utilizatorilor cu rol de admin.

Soluția trebuie să permită integrarea ulterioară a altor module (de exemplu un modul de management de urmărire a livrarilor produselor la client).

Cerințe legate de instruire și serviciile post implementare (mentenanță și suport tehnic)

- Componenta instruire şi consultanţă - furnizorul soluției informatice va asigura instruirea personalului BNR implicat în utilizarea acesteia, în centrala BNR si prin mijloace online cu utilizatorii din teritoriu. Totodată, furnizorul va include in oferta sa si o propunere de asigurare a unor servicii de consultanţă privind toate aspectele legate de funcţionarea în producție a soluției (hypercare). De asemenea, furnizorul va pune la dispoziție un manual de utilizare a aplicației cu descrierea etapelor ce trebuie parcurse (diagrame și capturi de ecran).
- Componenta servicii preventive post implementare - furnizorul solutiei eCommerce va asigura mentenanta preventivă a platformei prin instalarea patch-urilor de securitate, a bug-fix-urilor și a versiunilor minore de platforma pentru o perioadă de 5 luni de la intrarea în producție a platformei.
- Componenta servicii reactive post implementare - furnizorul va pune la dispoziție un call center disponibil 24x7 pentru preluarea solicitărilor din partea BNR cu privire la disfuncționalitățile solutiei (componenta reactivă) si va interveni pentru remedierea acestor disfunctionalitati pentru o durata de 5 luni de la data intrării în producție, astfel încât să se asigure buna funcționalitate a aplicației.

Cerinte de securitate

1.1.1 Controale generale

a) Soluția trebuie să se bazeze pe cele mai bune standarde ale industriei IT.
b) Soluția nu va utiliza standarde / arhitecturi proprietare care ar putea limita capacitățile de interconectare / integrare cu alte aplicații / produse.
c) Pentru toate componentele aplicației trebuie să existe suport valabil de la producător pe o perioada de minim 5 luni de la punerea în producție;
d) Soluția va asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă a sistemelor de prelucrare a datelor cu caracter personal;
e) Soluția trebuie să fie suficient de flexibilă pentru a permite opțiuni de configurare care să faciliteze integrarea în infrastructura IT a BNR și să aibă capacitatea de a restabili disponibitatea datelor cu caracter personal și accesul la acestea în timp util, în cazul în care are loc un incident de natură fizică sau tehnică;

f) Arhitectura trebuie să suporte modelul pe trei niveluri (3Tier): server-ul web, serverul de aplicație și cel de baze de date trebuie să fie separate în trei zone distincte de securitate;
g) Dezvoltatorul trebuie să furnizeze în cadrul soluției următoarea documentație: arhitectura completa a soluției, manuale de administrare, manuale de utilizare, instrucțiuni, tutoriale, documentația codului sursă, documentația modelului de date, fluxurile proceselor de date. Aceste documente trebuie să fie disponibile cel puțin în limba română;
h) Aplicațiile dezvoltate pentru BNR vor fi livrate împreună cu codul sursă;
i) Dezvoltatorul trebuie să ofere o listă a tuturor componentelor hardware și software, spre ex: platforma OS, platforma HW, DB, AS, middleware etc. pe care sistemul poate rula;
j) Documentația soluției trebuie să conțină o descriere a interfețelor necesare sau opționale, inclusiv structura și standardele sale, și anume: W3C, XML, J2EE etc. Furnizorul trebuie să menționeze dacă interfețele soluției (cum ar fi Enterprise Service Bus sau SOA), oferă detalii despre implementare, dacă sunt folosite în cadrul aplicației și metoda de interconectare. Interfețele de acces și de interconectare trebuie să publice servicii criptate pentru interconectarea cu alte sisteme / aplicații;
k) Dezvoltatorul trebuie să descrie capabilitățile de export și transfer de fișiere (preferabil pe baza API) și / sau integrate. În interiorul soluției trebuie să existe un mecanism de criptare a datelor înainte de export sau altă metodă de asigurare a confidențialității datelor (hashing, masquerading, filtrarea câmpurilor de date sensibile);
l) Dezvoltatorul trebuie să descrie modul în care se măsoară performanța aplicației (pe hardware-ul propus) cu diferite încărcări de lucru, de ex. numărul de utilizatori activi, dimensiunile bazei de date etc;
m) Dezvoltatorul trebuie să propună și să descrie caracteristicile de înaltă disponibilitate ale soluției (concept de *clustering* sau *fail-over*). Acestea includ subiecte precum: timpul necesar de întreținere programat pentru lucrările de întreținere (de exemplu backup, restaurare de date, arhivare etc.), opțiuni de configurare a soluției pentru disponibilitate ridicată (descrierea tipurilor de soluții de *cluster* / *fail-over* acceptate și testate).

1.1.2 Controale specifice la nivelul aplicației

Validarea datelor de intrare

a) Orice data introdusa de către utilizator prin intermediul unei interfețe trebuie validată din punct de vedere consistență, să corespundă cu tipul de dată așteptată a fi introdusa în acel câmp; validarea se face înainte a se executa codul program asupra datei respective. Orice data ce nu corespunde condițiilor de validare trebuie exclusa de la prelucrare in scopul protejarii impotriva atacurilor de tip „Code/command Injection”;
b) Vor fi implementate mecanisme de protecție împotriva utilizării abuzive sau supra-încărcării aplicației;
c) Vor fi utilizate exclusiv interogari parametrizate;
d) Tot codul ce urmează a fi executat se va afla exclusiv pe server și nu va fi disponibil sub nicio formă utilizatorului aplicației;
e) Vor fi implementate mecanisme eficiente împotriva încercarilor de manipulare a parametrilor aplicației;
f) Funcția „Autocomplete” va avea valoarea „off” pentru a împiedica stocarea locală de informații sensibile;
g) Următoarele informații nu vor fi prezente în URL-uri/URI-uri: nume de utilizator, parola, token-uri de acces, sau orice altă informație specifică procesului de autentificare/autorizare, precum și date cu caracter personal sau declarate a fi confidențiale;
h) Vor fi implementate mecansime de protejare a căilor de acces către fișiere specifice aplicației care să împiedice un potențial atacator să aibă acces la acestea („Path transversal”);
i) Orice intrare de tip XML va fi validată corespunzator în vederea evitării executării unor comenzi dictate de un atacator;
j) Orice referință internă către un obiect/fișier/director sau bază de date trebuie să includă un control al accesului la acestea;
k) Orice încercare de rulare/încărcare a fișierelor cu extensii neautorizate (de exemplu .dll, .config, .java, .cs, etc.) trebuie blocată.

a. Validarea datelor de intrare în aplicațiile web

În procesul de validare a datelor culese prin intermediul unor formulare web, aplicația trebuie sa aibă mecanisme eficiente de testare a datelor sau codurilor nesigure înainte de a le

trimite spre a fi executate și apoi afișate într-un browser web. Testarea trebuie să includă validarea împotriva atacurilor web comune (ex: XSS).

b. Tratarea erorilor

a) Mediul de producție trebuie configurat astfel încît sa nu dezvăluie erori din procesul de rulare (de ex. .Net, J2EE) pe ecran / în browser.
b) Paginile ce conțin mesaje de eroare trebuie personalizate și vor oferi minimul de informații pentru un utilizator.
c) În niciun mesaj de eroare al aplicației aflate în producție nu vor aparea următoarele informații: detalii cu privire la arhitectura aplicației (OS, versiune etc), eroare cu detalii de depanare, utilizatorul sau baza de date pe care rulează.

c. Generarea și păstrarea log-urilor de aplicație

a) Evenimentele legate de autentificare (succes sau eșec), utilizarea funcțiilor privilegiate, activitățile de administrare, precum și cele rezultate din pornirea/oprirea sistemului trebuie generate și stocate corespunzător, iar accesul la acestea se va face doar de către persoanele autorizate;
b) Logarea evenimentelor ce țin de securitatea sistemului vor fi stocate într-un fișier de tip jurnal separat, atunci când este posibil. Acesta va oferi flexibilitate suplimentară pentru orice investigație ulterioară (de exemplu crearea/modificarea de roluri/permisiuni speciale etc.);
c) Vor fi utilizate convenții de numire a fișierelor (de exemplu rotație, locație etc.) astfel încât aceste log-uri să poată fi integrate într-un sistem de tip SIEM;
d) Toate activitățile și acțiunile semnificative ale utilizatorilor (standard și tehnici) efectuate asupra datelor sau a elementelor de configurare din cadrul aplicației trebuie să fie înregistrate în scopuri de audit. Soluția trebuie să aibă capabilități de a exporta acel fișier log utilizând metode standard, cum ar fi syslog;
e) Soluția trebuie să aibă următoarele capabilități de logare și de audit:
    - toate operațiunile de acces și manipulare a informatiilor (crearea, modificarea, ștergerea, modificarea sau accesul la informațiile privind operatiile la nivel de baza de date);
    - toate activitățile cu rezultate în crearea, modificarea, ștergerea, modificarea sau accesarea fisierelor unde sunt stocate informațiile de autentificare și / sau de autorizare;

- toate acțiunile efectuate de utilizatorii privilegiați (administratori tehnici și / sau obișnuiți);
- înregistrarile din jurnale trebuie să conțină cel puțin următoarele informații: identificarea utilizatorului, marcajele de timp, tipul de operațiune și tipul de date accesate / modificate; în cazul modificărilor, jurnalele trebuie să conțină valoarea inițială și valoarea nouă;
- în cazul în care jurnalele conțin date sensibile, furnizorul trebuie să implementeze o metodă de anonimizare a acestora, în cazul în care ar fi exportate către terți;
- soluția trebuie să aibă capabilități pentru a controla / restrânge accesul și manipularea informațiilor din aceste fișiere log;

f) Soluția trebuie să aibă capacitățile de a se sincroniza cu o sursă NTP externă pentru a realiza coerența timpului.

1.1.3 Controale la nivelul comunicației între componente sau client/server

a) Protocolul HTTPS trebuie forțat pentru toate conexiunile din browser; Protocolul HTTP trebuie dezactivat;
b) Se vor utiliza protocoale TLS 1.2 sau versiuni ulterioare pentru a proteja conexiunile existente la nivelul aplicației (de exemplu: serverul de aplicații și conexiunile serverului DB);
c) In cazul procesării unor informații critice pentru BNR, se vor implementa mecanisme de autentificare și criptare a sesiunii;
d) Dezvoltatorul nu trebuie sa utilizeze propriul protocol de criptare.

1.1.4 Managementul credențialelor

a) Codul aplicației nu va stoca niciodată parole de utilizator; orice credențial al unui user tehnic trebuie protejat corespunzător;
b) Vor fi implementate mecanisme eficiente de protecție împotriva încercărilor repetate de autentificare nereușită;
c) Încercările de autentificare vor folosi protocoale securizate în schimbul credențialelor (de ex., TLS 1.2 sau o versiune ulterioară).
d) Nicio parolă nu trebuie să fie stocată în clar datorită riscului de compromitere. În schimb, acestea trebuie să fie transformate într-un hash.

1.1.5 Valabilitate sesiuni

a) Sesiunile autentificate vor avea un timp de expirare implementat;

b) ID-urile de sesiune vor fi aleatoare și suficient de lungi pentru a fi protejate împotriva atacurilor;

c) Token-urile folosite la autentificare/deconectare vor fi modificate de fiecare dată;

d) Transmiterea token-urilor se va face utilizand protocoale securizate (ex: TLS 1.2 sau o versiune ulterioară); funcția de logout va fi implementată astfel încât toate obiectele temporare și operațiile pe server să poată fi șterse/oprite. Această funcție va fi activată la cererea utilizatorului, după o perioadă de inactivitate stabilită (de exemplu, mai mult de 15 minute) sau după închiderea ferestrei din browser.

1.1.6 Controale la nivelul mecanismului de autentificare

a) Este necesară implementarea de mecanisme de autentificare integrate cu o bază de date consolidată a BNR, cum ar fi Secure LDAP, Kerberos sau RADIUS;

b) Permisiunile se acordă pe grupuri de utilizatori (nu utilizatorilor individuali), care vor fi revizuite periodic sau ori de câte ori este nevoie, pentru asigurarea faptului că orice salariat care are acces la date cu caracter personal nu prelucrează decât acele date.

c) Un mecanism de tip Single Sign On se recomandă a fi implementat;

d) Soluția trebuie să accepte cel puțin două dintre următoarele mecanisme de autentificare: nume de utilizator / parolă, certificate X.509, tokenuri hardware, OTP. Dacă autentificarea utilizată va fi o combinație de nume de utilizator / parolă, aplicația trebuie să accepte Politica de parole convenită în BNR. Soluția trebuie să aibă, de asemenea, politici diferite, cu granularitate specifică, pentru a stabili mecanismele de autentificare necesare pentru identitățile individuale, grupurile de identitate sau toate identitățile. Furnizorul trebuie să descrie modul în care utilizatorii sunt autentificați în aplicație;

e) Componentele ce gestionează date critice ale aplicației trebuie să suporte tehnologia 2FA;

f) Canalul de comunicare dintre modulul de autentificare al aplicației și baza de date centralizată cu utilizatorii aplicației trebuie să fie asigurat utilizând tehnici standard de criptare. Furnizorul trebuie să descrie conceptul de gestionare a utilizatorilor (unde sunt stocate în mod normal credentialele utilizatorului și modul în care software-ul poate fi integrat sau accesat din afara sistemelor printr-un sistem de tip IAM);

g) Soluția trebuie sa aibă capabilități pentru a implementa modelul de separare a sarcinilor (SoD) în funcție de cerințele de business și de cele tehnice. Utilizatorii de business trebuie să fie diferiți de cei tehnici. Utilizatorii tehnici nu trebuie să aibă

drepturi de acces sau de configurare / schimbare a parametrilor tehnici ai aplicației / platformei.

h) Soluția trebuie să aibă următoarele capabilități: mecanisme de control pentru accesarea datelor / obiectelor de către diferiți utilizatori cu roluri specifice sau în cadrul anumitor grupuri; administrarea de roluri / grupuri (în cadrul aplicației și / sau extern). Soluția trebuie să suporte / să utilizeze mecanismul de autorizare specific pentru diferite profiluri de utilizatori (ceea ce permite utilizatorilor să acceseze / să modifice pe baza profilului propriu). Este preferabil să existe în interiorul aplicației posibilitatea de a importa / exporta profilurile utilizatorilor (în ceea ce privește drepturile de utilizator / permisiunea de a manipula anumite date / articole) pentru a fi ușor de integrat cu alte sisteme / aplicații din cadrul BNR. Dezvoltatorul trebuie să descrie conceptul de autorizare (model RBAC - role-based access control) implementat la nivel de aplicație (de exemplu numărul și tipurile de roluri / grupuri, inclusiv rolurile administrative).

1.1.7 Configurarea securizată a aplicației

a) Codul sursă, bibliotecile și parametrii de configurare trebuie protejate corespunzator, conform principiului necesității de cunoaștere; scanarea vulnerabilității întregii soluții se va efectua înainte de punerea în producție. Aspectele critice vor fi remediate cu prioritate;

b) Funcțiile aplicației vor fi executate cu cel mai mic privilegiu posibil;

c) Componentele aplicației vor fi permanent actualizate;

d) Mecanisme de protecție a componentelor critice ale aplicației împotriva modificării neautorizate trebuie implementate;

e) Accesul la bazele de date trebuie implementat într-un mod securizat prin utilizarea tehnicilor de criptare a protocoalelor / API-urilor. Accesul logic la baza de date trebuie, de asemenea, să fie asigurat. Este de preferat ca niciun utilizator tehnic (hardcoded) să nu fie utilizat.

1.1.8 Controlul versiunii

Un sistem de control al versiunilor aplicației trebuie implementat; versiunea curentă a aplicației va fi disponibilă utilizatorilor.

1.1.9 Documentarea soluției

a) Furnizorul trebuie să furnizeze arhitectura completă a aplicației care să conțină o descriere detaliată a fluxurilor de comunicare între diferitele componente ale sistemului (ex: între servere și / sau clienți). Comunicarea / fluxurile de date între

diferitele componente ale soluției sau între soluția în sine și alte resurse IT (ca rezultat al integrării în infrastructura IT a BNR) trebuie să fie criptate folosind standarde și tehnici bine cunoscute (de exemplu IPSEC, SSL, TLS). De asemenea, furnizorul trebuie să descrie următoarele: ce cantitate de trafic este de așteptat (de exemplu, peste WAN), care sunt dimensiunile tipice ale fișierelor cu privire la cantitatea de date ce va fi procesata, care sunt limitările dacă una sau mai multe dintre componentele hardware sunt plasate în rețele separate, de exemplu conexiunea se face prin routere și / sau firewall-uri;

b) Furnizorul trebuie să descrie care browsere (versiuni) sunt suportate pe care sisteme de operare client și dacă sunt necesare de plug-in-uri suplimentare (Quicktime, Silverlight, Active-X, Flash, Java Applets). Aplicația trebuie să ruleze optim în Internet Explorer 11 sau ulterior, Microsoft Edge sau Chrome. Orice Third Party Component trebuie documentată corespunzator inclusiv la nivel de licențiere;
c) Pentru asigurarea posibilității de îndeplinire a clauzei 13.1.3 Separarea în reţele din ISO27002, furnizorul trebuie să programeze aplicația astfel încât fluxul de date dintre client și sistemele de servere să poată fi canalizat printr-un sistem proxy;
d) Dezvoltatorul trebuie să descrie strategiile de backup și arhivare în acord cu parametrii BCP ai proceselor de business susținute de către sistemul dezvoltat. Toate copiile bazei de date din cadrul soluției trebuie să aibă același nivel de securitate. Procesul de export / duplicare trebuie făcut în mod securizat și controlat numai de un cont / persoană autorizată.
e) Furnizorul trebuie să descrie procedurile de întreținere regulate și neprogramate, inclusiv procedurile de actualizare.
f) Soluția trebuie să ofere opțiunile de administrare (din punct de vedere operațional) dintr-o interfață centralizată. Furnizorul trebuie să descrie conceptul de administrare de la distanță.
g) Administratorii trebuie să utilizeze numai un protocol securizat pentru conexiunea la distanță la interfața de administrare a aplicației. Toate protocoalele / porturile nesecurizate disponibile pentru administrare la nivel de aplicație / bază de date trebuie să fie închise sau dezactivate înainte de a intra în mediul de producție. Interfața de administrare a aplicației trebuie să aibă capacitatea de autentificare a conturilor de utilizator personale / personalizate cu diferite niveluri de autorizare în ceea ce privește citirea / modificarea parametrilor de configurare.

1.1.10 Abateri acceptabile

Anumite elemente recomandate nu pot fi implementate în mod adecvat în contextul intern. Pentru respectivele elementele se pot accepta abateri de la recomandări în cazul în care se oferă justificări acceptate bazate pe specificul de funcționare al sistemului respectiv și numai după întocmirea unei analize de risc, nivelul de risc rezidual urmând a fi acceptat formal.

3.1. Descrierea situației actuale la nivelul Autorității contractante

În prezent, în Banca Națională a României nu există o astfel de aplicație, prin care cumpărătorii de produse numismatice să poată efectua plata on-line.

3.1.1. Livrare

Implementare și lansare în producție la sediul BNR.

Transferul drepturilor de proprietate intelectuală asupra solutiei software oferite se va realiza conform prevederilor legale privind cesiunea drepturilor de autor, în materia achizițiilor publice.

Beneficiarul va retine dreptul de proprietate intelectuala exclusiva doar pentru elementele (componente ale solutiei, cod sursa, documentatie sau tehnici) realizate suplimentar fata de functionalitatile standard existente in produsul „commercially available off-the-shelf (COTS)" ofertat, cu scopul de a acoperi cerintele contractului, si nu asupra intregului sistem multi-componenta ce va fi contractat.

Ofertantul va pune la dispozitie codul sursa si standardele si instrumentele de dezvoltare utilizate doar pentru elementele dezvoltate suplimentar fata de functionalitatile standard existente in produsul COTS ofertat.

După încetarea prezentului contract, Ofertantul nu va păstra copii ale documentelor şi/sau materialelor realizate şi nu le va utiliza în scopuri care nu au legătură cu prezentul contract, fără acordul scris prealabil al Beneficiarului. Datele introduse in baza de date sunt si rămân proprietatea BNR. Contractantul va asigura o modalitate tehnică prin care datele pot fi extrase în orice moment din sistemul existent într-o formă prelucrabilă (export într-un format standard, acces la baza de date etc.).

Beneficiarul poate să permită contractanților săi (incluzând, fără limitare, funcțiile de externalizare) să folosească programele (software-ul deținut sau distribuit de contractant și orice actualizări achiziționate prin suport tehnic) si documentele furnizate de contractant in cadrul prezentului contract, în scopul desfășurării propriilor activități interne.

3.1.2. Constrângeri privind locația unde se va efectua livrarea/instalarea

- Integrare/compatibilitate cu aplicațiile existente în BNR, cu care aplicația informatică de tip eCommerce va efectua schimb de date.

3.2. Atribuțiile și responsabilitățile Părților

Furnizorul va preda aplicația de tip eCommerce (magazin online), funcțională, conform condițiilor documentației de atribuire și la nivelul calitativ stabilit în cadrul caietului de sarcini, respectiv în cadrul propunerii tehnice prezentate.

3.3. Elemente solicitate

Aplicație informatică de tip eCommerce (magazin online)

- Platformă software de tip eCommerce, inclusiv licenţele aferente
- Servicii de configurare platformă eCommerce pentru a răspunde cerințelor funcționale ale BNR, inclusiv dezvoltări software la cheie, dacă acestea vor fi necesare
- Servicii de instruire pentru utilizatori back-office
- Asistență la lansarea în producție a soluției eCommerce
- Servicii de suport tehnic și mentenanţă soluție pe o perioadă de 5 luni

4. Recepția aplicației

Recepția aplicației se va efectua pe baza de proces verbal semnat de Contractant și Banca Națională a României.

Se va constitui o comisie de recepţie, care prin persoanele desemnate de BNR în acest scop, va verifica modul de implementare și funcționalitatea aplicației (toate operaţiunile aferente, în conformitate cu cerinţele detaliate din cadrul caietului de sarcini). În urma verificării, comisia de recepţie, va stabili dacă aceasta corespunde cerințelor specificate în caietul de sarcini.

5. Modalități si condiții de plata

Plata se va face în moneda națională, în contul indicat de furnizor, în termen de maximum 30 de zile de la înregistrarea facturii la Registratura BNR, doar după semnarea procesului verbal de recepţie, fără obiecţiuni.

6. Cadrul legal care guvernează relația dintre Autoritatea contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile legale aplicabile în domeniul mediului, social și al muncii.

7. Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

Riscuri și măsuri de gestionare a riscurilor asociate contractului, fără a avea un caracter exhaustiv:

Riscuri	Măsuri de gestionare
Livrarea cu caracteristici tehnice diferite de cerintele specificate in caietul de sarcini	Notificare catre furnizor in vederea remedierii aspectelor constatate; Aplicarea de penalitati in conformitate cu clauzele contractuale; Asigurarea unei verificari riguroase a conformitatii produsului ofertat, în raport cu cerintele documentației de atribuire și oferta prezentată, parte din contract.
Dificultati in gestionarea relatiei furnizorului cu subcontractantii (daca este cazul)	Preluarea de catre furnizor a partii/partilor din contract aferente activitatii subcontractate sau înlocuirea subcontractantului cu un nou subcontractant în condițiile prevazute contract.
Nerespectarea prevederilor legale referitoare la conflictul de interese	Aplicarea de sanctiuni, conform prevederilor legale referitoare la conflictul de interese, în materia achizițiilor publice.
Întârzieri peste termenul limită stabilit prin contract	Aplicarea de penalități conform clauzelor stipulate în contractul de achiziție.
Intarzieri in efectuarea platii de catre BNR	Aplicarea de penalități conform clauzelor stipulate în contractul de achiziție.