Specificații tehnice (F4.1)

[Acest tabel va fi completat de către ofertant în coloana 4, iar de către autoritatea contractantă - în coloanele 1,2,3,5]

Numărul procedurii de achiziție: **MTender ID ocds-b3wdp1-MD-1566039879852 din 17.08.2019**

Denumirea achiziției: ***Soluție pentru fortificarea securității informației la accesarea resurselor BNM (autentificarea multifactorială***

Cod CPV	Denumirea seviciilor	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5
Lotul 1: Soluție pentru fortificarea securității informației la accesarea resurselor BNM				
30191140-7	**1. Soluție de autentificare multifactoriala**	**Tip: Soluție de autentificare multifactoriala pe baza de certificate PKI** **Cantitate:** Licență de tip server pentru 300 utilizatori si licență de tip Client pentru 300 utilizatori. Este responsabilitatea Ofertantului de a determina modelul de licențiere. **Cerințe de licențiere:** - Toate licențele livrate vor include prețul pentru un an de suport si mentenanță, furnizat de producătorul licențelor, care va începe de la data acceptantei soluției. In cazul activării licențelor pana la data acceptantei soluției, toate costurile suportate de producătorul de licențe in timpul efectuării lucrărilor de instalare, configurare vor fi suportate de către ofertant. **Condiții generale:** Soluția de autentificare multifactorială propusa trebuie să se	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

Digitally signed by Cornei Andrian
Date: 2019.09.12 17:26:18 EEST
Reason: MoldSign Signature
Location: Moldova

		integreze cu soluția de autentificare Microsoft Active Directory exploatată in Sistemul Informațional al BNM. Soluția livrată trebuie să asigure posibilitatea utilizării semnăturii electronice avansate calificate, in condițiile stabilite de cadrul legal al Republicii Moldova. Ținând cont de acest fapt, soluția trebuie să corespunda tuturor cerințelor normative si tehnice in vigoare si să urmeze procedura de acreditare (efectuată de către SERVICIUL DE INFORMATII ȘI SECURITATE, in conformitate cu ORDINUL Nr. 69 din 15.07.2016 cu privire la aprobarea Normelor tehnice in domeniul semnăturii electronice avansate calificate, CAPITOLULII Crearea și administrarea cheilor publice și private - vezi http://lex.justice.md/md/365884/). ***Cerințe pentru Sistemul de Management: Caracteristici generale***: - să fie compatibilă cu orice aplicație standard bazata pe certificate criptografice (PKI); - să permită utilizatorilor sa-si gestioneze de sine stătător cardurile inteligente si certificatul PKI propriu; - să suporte accesul securizat, criptarea datelor si semnătura digitală, toate intru-un singur autentificator; - să suporte echipamente certificate conform standardelor FIPS si CC (Common Criteria); - configurare detaliata a politicilor de utilizare si securitate a utilizatorilor; - să suporte integrare cu alte aplicații bazate pe certificate PKI prin API-uri standardizate; - să suporte Tastieră Virtuală pentru introducerea parolei in lipsa tastierei fizice; - să conțină cel puțin localizările: Romana, Engleza; ***In ceea ce privește auditul si monitorizarea securității. se***		

		aplică următoarele cerințe: 1. Soluția de autentificare multifactoriala propusă va deține componente de audit ce vor colecta si gestiona centralizat înregistrările de audit la nivelul întregii soluții; 2. Fiecare înregistrare de audit va conține cel puțin: a) Momentul in timp al producerii evenimentului; b) Subiectul evenimentului (ID utilizator); c) Categoriile de date/parametri afectați; d) Evenimentul produs; e) Adresa IP a sursei ce a inițiat evenimentul, sau alta informație care ar permite identificarea sursei; 3. Componenta de audit va putea fi integrată in baza standardelor deschise cu soluții de tipul SIEM (Security Incident and Event Management) in vederea preluării înregistrărilor de audit produse in cadrul aplicației, de către soluțiile respective (de ex. Syslog, dblink etc.). 4. Soluția propusa trebuie sa aibă mecanisme sigure pentru a proteja integritatea informațiilor de audit înregistrate. ***Cerințe tehnice:*** - sa suporte minim următoarele sisteme de operare: • Microsoft Windows Windows Server 2016 (64-bit) Windows 10 (32-bit, 64-bit); • Distributive Linux Ubuntu 14,18; - să se integreze cu sistemul de virtualizare Citrix Virtual Apps and Desktops cu utilizarea terminalelor HP ThinClient t620 sau t630 cu sistem de operare ThinPro 7.1 si mai sus - să suporte minim următorii algoritmi de criptare: RSA 2048-bit, SHA-256, Elliptic Curve Cryptography (ECC), 3DES - să suporte minim următoarele API-uri: PKCS&11, MS		

		CryptoAPI and CNG (CSP, KSP), Mac Keychain (TokenD), PC/SC - sa suporte minim următoarele browsere: Internet Explorer, Google Chrome, Firefox;		
3016 2000 -2	**2. Card inteligent (Smartcard)**	**Tip: Cardurile inteligente oferite trebuie să suporte autorizarea cu PIN si politică pentru PIN.** Cardurile inteligente trebuie să fie compatibile cu soluția propusă la poziția 1. **Condiții generale:** Echipamentul oferit in cadrul achiziției trebuie să fie nou, calitativ, produs de serie brand (BRAND NAME), cu proveniență de la producătorii renumiți, bine cunoscuți internațional in domeniul TI. In cazul existentei certificatelor de atestare a calității, o copie sau referință Internet trebuie să fie inclusă in ofertă. **Cerințe tehnice:** Certificare: FIPS 140-2 Level 3 Memorie: - minim 10 containere pentru kei RSA sau Elliptic Curve; - să suporte păstrarea simultana a minimul 2 perechi de chei public/privat - una pentru autentificare bifactorială si una pentru aplicarea semnăturii electronice (ambele cu lungimea cheii de 2048-bit); Standarde: BaseCSP Minidriver v7(IDGo 800 Minidriver) PKCS#11 & CSP, DESFire/EV1 Protocoale de comunicare: T=0, T=1 Algoritmi criptografici: - RSA: up to RSA 2048 bits - RSA OAEP & RSA PSS - Elliptic curves: P-256, P-384, P-521 bits, ECDSA, ECDH - Hash: SHA-1, SHA-256, SHA-384, SHA-512 - Symmetric: 3DES (ECB, CBC), AES (128,192, 256 bits)	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

		Sistem de operare: Windows, Linux, MAC, Citrix Timpul de viată: - Retenția datelor minim 10 ani - Minim 250.000 de cicluri scriere/ștergere Culoare: alb cu posibilitate de imprimare pe ambele părți. Garanție: 24 luni Cerințe specifice in perioada de garanții: Pe perioada de garanție Ofertantul se obliga să schimbe Bunurile defectate din contul său, in conformitate cu legislația in vigoare, in termen de 20 zile lucrătoare din momentul înștiințării de către Cumpărător.		
3023 3300 -4	**3. Cititor de carduri inteligente**	**Condiții generale:** Echipamentul oferit in cadrul achiziției trebuie să fie nou, calitativ, produs de serie brand (BRAND NAME), cu proveniență de la producătorii renumiți, bine cunoscuți internațional in domeniul TI. In cazul existentei certificatelor de atestare a calității, o copie sau referință Internet trebuie să fie inclusă in ofertă. **Cerințe tehnice:** Standarde si certificări: ISO 7816, PC/SC, EMV Level 1, CCID, FCC part 15 class B, Mondex Level 1, Microsoft WHQL Protocoale de comunicare cu Cardul inteligent: Suportă carduri bazate pe microprocesor care utilizează T=0 sau T=1 Sistem de operare: Windows, Linux, MAC, Citrix, HP ThihPro 7.1 si mai sus Metoda de conectare la stație: USB Nota: Cititorul de carduri inteligente oferit trebuie să fie compatibil cu cardul inteligent oferite la poziția 2 Garanție: minim 12 luni Cerințe specifice in perioada de garanții: Pe perioada de garanție Ofertantul se obligă să schimbe	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

		Bunurile defectate din contul său, in conformitate cu legislația in vigoare, in termen de 20 zile lucrătoare din momentul înștiințării de către Cumpărător.		
3023 3320 -0	**4. Controler de acces**	**Condiții generale:** Echipamentul oferit in cadrul achiziției trebuie să fie nou, calitativ, produs de serie brand (BRAND NAME), cu proveniență de la producătorii renumiți, bine cunoscuți internațional in domeniul TI. In cazul existentei certificatelor de atestare a calității, o copie sau referință Internet trebuie să fie inclusă in ofertă. **Condiții tehnice:** Controlerul de acces oferit va include: 1. Cititor RFID cu următoarele caracteristici: EM/HID/Prox/MIFARE/iCLASS/DESFire/FeliCa/NFC - Frecventa joasa LF - 125KHz, frecventa înaltă HF - 13.5MHz 2. Cititor Biometric pe baza de amprenta digitală cu următoarele caracteristici: - Tip senzor: Optical Sensor - OP5 - Șablon: ISO 19794-2 / ANSI 378 Interfață: TCP/IP, RS232, RS485, Wiegand. TTL I/O, relay; Wiegand: 1ch input or output (selectable); Să suporte PoE: IEEE802.3af; Să se conformeze standardului: IP67, IK08; Să fie certificat: FCC, KC, CE, WEEE, REACH, RoHS, MINEX; Să fie capabil sa lucreze la temperaturile de la -20°C pana la 50°C si umiditate 0% ~ 80%; Să fie capabil sa stocheze local minim 1000 utilizatori si 100000 evenimente intrare/ieșire; Să fie compatibil cu cardurile inteligente oferite la poziția 2 Garanție: minim 24 luni	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

		Cerințe specifice in perioada de garanții: Pe perioada de garanție Ofertantul se obligă să schimbe Bunurile defectate din contul său, în conformitate cu legislația in vigoare, în termen de 20 zile lucrătoare din momentul înștiințării de către Cumpărător		
3023 2130 -4	**5. Imprimantă**	**Tip: Imprimantă carduri inteligente** **Condiții generale:** Echipamentul oferit in cadrul achiziției trebuie să fie nou, calitativ, produs de serie brand (BRAND NAME), cu proveniență de la producătorii renumiți, bine cunoscuți internațional in domeniul TI. In cazul existentei certificatelor de atestare a calității, o copie sau referință Internet trebuie să fie inclusă in ofertă. **Condiții tehnice:** Sa suporte imprimare pe o singura față si dual, color si monocrom cu laminare; Tipul de imprimare: sublimare directa a colorantului; Aria de imprimare a cardului: total; Rezoluție: minim 300 dpi color; Sa suporte tipurile de carduri: - PVC, Composite PVC si PET - Contact: ISO 7816 A/B/C Card, ISO 7816 1/2/3/4 Microprocessor Card - Contactless: ISO 14443 (Type A/B), MIFARE, DESFIRE, iCLASS Viteza de imprimare YMCKO maxim 30 sec/card Power Efficiency: ENERGY STAR certified Notă: Oferta trebuie sa includă si următoarele consumabilele: - Ribbon YMCKO (capacitatea de imprimare - minim 250 imprimări) (2 buc) -Security Film CPF (capacitatea de imprimare, minim 250 imprimări) (2 buc)	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

		Garanție: 24 luni Cerințe specifice in perioada de garanții: Ofertantul este obligat sa asigure deservirea tehnică a Bunurilor in următoarele condiții: a. constatarea (diagnosticarea) unei defecțiuni in maxim 2 zile lucrătoare; b. înlăturarea problemei nu va depăși 7 zile lucrătoare. înlăturarea problemei presupune repararea sau substituirea componentelor defectate, instalarea, configurarea și testarea funcționării adecvate a lor; c. In cazul unor defecțiuni mai grave, Bunurile se vor transporta la centrul de deservire autorizat de către Vânzător. In cazul in care reparația echipamentelor va dura mai mult de 7 zile lucrătoare, Vânzătorul va asigura un echipament echivalent pentru perioada reparației Bunului defectat. Toate serviciile legate de înlăturarea defecțiunilor (pieselor defecte) sau problemelor (inclusiv corespondenta cu producătorul, transportarea, vămuirea pieselor de schimb si celor defectate, etc.) vor fi efectuate de către Vânzător din contul Vânzătorului. Garanția include costul pieselor și al manoperei.		
72000000-5	**6. Servicii de implementare**	**Tip: Servicii de implementare a soluției de autentificare multifactoriala** Cerințe fata de serviciile de implementare asigurate de Ofertant: Serviciile de implementare trebuie sa fie efectuate on-site (la sediul BNM) si vor include: - Servicii de proiectare. După semnarea contractului, Ofertantul câștigător este responsabil, de comun acord cu Cumpărătorul, de a iniția lucrările de proiectare detaliată a implementării soluției, care va acoperi cel puțin următoarele aspecte:	Specificația tehnică propusă este conform Matricii de Conformitate Anexa Nr.1 care se anexează	

		• Proiectarea sistemului centralizat de autentificare multifactorială pentru accesul logic la resursele Sistemului Informatic al BNM și accesul fizic in sediul BNM; • Descrierea modului de funcționare a soluției (inclusiv stabilirea politicilor de grup de securitate, modul de gestionare a certificatelor și pin-urilor, modul de gestionare a amprentelor, modului de monitorizare, auditul, etc.); • Descrierea modului de integrare a soluției de autentificare multifactorială in mediul virtual - Citrix XenDesktop și XenApp, inclusiv a modului de configurare a terminalelor HP ThinClient t620 sau t630 cu sistemul de operare ThinPro 7.1; • Analiza aplicațiilor exploatate in cadrul Sistemului Informatic al BNM și stabilirea modului de autentificare multifactorial; • Descrierea modului de integrare a soluției pentru accesul fizic in sediul BNM (biometric/card) cu soluția existentă de control al accesului; - Servicii de instalare, configurare și testare a soluției - toate serviciile de instalare, configurare (inclusiv configurarea politicilor initiate), testarea, punerea in funcțiune a soluției, transferul de cunoștințe și asigurarea suportului la definirea/configurarea și exploatarea soluție pentru primul an de exploatare trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse in ofertă; - Serviciile de mentenanță și suport vor include: suportul, remedierea incidentelor, actualizări. Livrabile: - Documentația tehnică a soluției sau alte documente identificate in procesul de implementare a soluției. - Soluția implementată, testată si acceptată de Beneficiar		

Semnat:_____
Numele, Prenumele: **Andrian Cornei**
În calitate de: **Director**
Ofertantul:Reliable Solutions Distributor
Adresa: str. Alexandru cel bun 85, MD-2012, mun Chisinau, Republica Moldova.