CAIET DE SARCINI

Caietul de sarcini face parte integrantă din documentaţia de atribuire şi constituie ansamblul cerinţelor pe baza cărora se elaborează de către fiecare ofertant oferta tehnico-financiară.

Cerinţele impuse vor fi considerate ca fiind minimale. În acest sens orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, dar numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerinţelor minimale din caietul de sarcini. Ofertarea de produse cu caracteristici inferioare celor prevăzute în Caietul de sarcini atrage descalificarea ofertantului.

Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea „sau echivalent".

Specificaţii tehnice minimale:

Specificatii tehnice pentru achizitie certificate digitale

Numar servicii de certificare digitala - 14

Pachetul de servicii certificate digitale va cuprinde:

- Certificat digital calificat
- Dispozitiv securizat pentru crearea semnaturii
- Aplicatie software pentru semnarea electronica

Certificatele trebuie sa respecte urmatoarele cerinte:

Profilurile certificatelor sa respecte formatul descris în standardul ITU-T X.509 v.3, iar profilul OCSP sa respecte cerinţele RFC 6960.

Functiile hash si procedurile de criptare folositesa fie in conformite cu cu Art. 39 al Normelor Tehnice si Metodologice pentru aplicarea Legii nr. 455/2001 privind semnatura electronica si

ale Regulamentului (UE) nr. 910/2014 privind identificarea electronica si serviciile de incredere pentru tranzactiile electronice pe piata interna (functia hash-code SHA256 si algoritmul de criptare SHA256RSA)

Caracteristici campuri certificat

Field name	**Value or value's constraint**
Signature Algorithm	sha256WithRSAEncryption
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key); RSA key size.
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.

Dispozitivul securizat pentru crearea semnaturii trebuie sa respecte urmatoarele cerinte:

Descrierea tehnica a dispozitivului

Produsele asociate semnăturii electronice utilizate sa aiba un înalt grad de fiabilitate, sa fie protejate împotriva modificărilor şi sa asigure securitatea tehnică şi criptografică a desfăşurării activităţilor de certificare a semnăturii electronice.

Dispozitivul sa fie oferit impreuna cu driver standard PC/SC, sa suporte Windows smart card login si sa permita autentificare si criptare utilizand tehnologie cu chei asimetrice (chei publice). Dispozitivul sa poata fi inglobat in aplicatii PKI si sa raspunda oricaror cerinte de securitate pentru lucrul cu certificate digitale si semnatura electronica.

- Dispozitivul sa fie certificate FIPS 140-2 Nivelul 3.
- Dispozitivul sa fie certificat de Microsoft HCK / HLK şi să instaleze automat driverele de la Microsoft Windows Update.
- Dispozitivul sa suportea plicaţii standard de carduri inteligente, precum Log on Windows smart card, VPN, Bit Locker .etc.
- Dispozitivul sa utilizeze tehnologia smart card pe32 bitcare permite autentificarea de smart card şi autentificare puternică.
- procesele de criptare şi de criptare au loc la nivelul dispozitivului, reducand astfel spre minim riscul de a efectua procesul pe computerul local.

- Sa ofere procesul de semnarea digitală pe bază de jetoanen on-repudiere şi stocarea tranzacţiilor şi a documentelor prin intermediul tehnologiei PKI; asigurarea autenticităţii tranzacţiilor electronice în industriile de finanţe şi de vânzare cu amănuntul.
- Sa utilizeaza mai multi algoritmi de criptare aprobate înindustrie, inclusiv:
  SimetricAlgoritmul: DES, 3DES, AES168, AES192, AES256
  Algoritmulasimetrica: RSA1024 / 2048
  Digest Algorithm: MD5, SHA1, SHA256, SHA384, SHA512
- Sistem de fişiere securizat pentru stocarea de semnaturi digitale şi a fişierelor utilizând sistemul de permisiune pe trei niveluri.
- abilitatea automata de auto-blocare a dispozitivului, după o limită stabilită de numărul maxim de încercări de autentificare a fost atins.
- semnatura digitala in chip, cheia privata nu se exporta niciodata;
- generator de numere aleatoare (RNG) in chip;
- numar unic de identificarepe 64-bit;
- credentiale de encriptare :
  Microsoft CryptoAPI and CNG X509 v3 certificate storage
  SSL V3, IPSEC/KEC, PC/SC, CCID
  PKCS# 11 V2.20
  Microsoft SmartCard Mini Driver
- suport pentru diverse platforme multiple de compatibilitate, sisteme de operare, inclusiv XP, Server 2003, Vista şi 7,8,10, Mac OS X şi Linux
- customizare OEM, caracteristici distinctive, cum ar fi logo-urişiaspectul general al dispozitivului, carcasă, sa fiepersonalizabile la cerereaclienţilor.

Caracteristici tehnice:

Power supply	USB Port
Working Voltage	5V (USB Chargeable)
Working current	50mA
Working temperature	0 – 70□
Storing temperature	-20 – 85□
Casing Material	Metal
Communication	USB CCID
Interface Standard	USB 2.0 High speed support; compliant with 3.0
Processor	32-bit Smartcard chip
Memory	128KB EEPROM
Number of Read/Write Cycles	At least 500,000 write/erase cycles
Data Retention	At least 10 Years
Power Consumption	Less than 100mW

Cryptography Standards Compliant	Microsoft Smart Card Mini Driver Microsoft CryptoAPI and CNG PKCS# 11 V2.20 X509 v3 certificate storage SSL V3, IPSEC/KEC, PC/SC, CCID

- ISO 7816 Standard
- Suport pentru DES, 3DES, AES128/192/256, SHA1/SHA256/SHA384/SHA512, RSA(1024/2048)
- Suport pentru aplicatii multiple, containere multiple si certificate multiple;
- Suport pentrustocare si import certificate X.509 v3.

Solutii OS complete pentru sistemele de operare

Dispozitivul sa fie certificat conform standardelor internaţionale cross-platform, pentru sisteme de operare multiple. Sistemele de operare suportate:

- Windows XP, 2003, Vista, 7, 8, 10 (ambele 32 şi 64 de biţi)
- Windows Server 2003/2012/2015 şi mai mult
- Linux 2.6 şi versiuni mai recente
- Mac OS X 10 şi versiuni mai recente

Dispozitivul sa ofere interfata pentru Microsoft Mini Driver Microsoft Crypto API şi PKCS # 11.Dispozitivul sa suporte mai multe certificate şi perechi de chei.

Alte condiţii:
Termenul de plata este de 30 zile de la emiterea facturii si semnarea, fără obiecţiuni, de către Comisia de recepţie, serviciilor, pe baza facturii fiscale, emise de prestator.
Plata se va face în lei cu O.P. prin Trezorerie.

Intocmit,

Ec.Andrei Tărăbîc

Avizat IT&C