

SPECIFICAȚII TEHNICE

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5,]

Numărul procedurii de achiziție: [ocds-b3wdp1-MD-1665646233385 din 13.10.2022](#)

Obiectul achiziției: Dispozitiv securizat de creare a semnăturii electronice de tip HSM

Denumirea bunurilor/serviciilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referință
1	2	3	4	5	6	7
Bunuri/servicii						
Lotul nr. 1: Dispozitiv securizat de creare a semnăturii electronice de tip HSM	Utimaco CryptoServer CP5 Se1500 LAN V5	Germania	Utimaco IS GmbH	În conformitate cu Caietul de sarcini, (Anexa nr. 21) Cryptography algorithms o Support for FIPS-approved and NIST recommended algorithms, modes, curves, and key sizes for RSA (up to 8192, sizes 2048, 3072 and 4096 are mandatory), DSA, Diffie-Hellman, AES, SHA-2 family, and Elliptic Curve Cryptography (ECC); o NIST compliant Hardware Random Number Generator o Asymmetric algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) o Symmetric algorithms: AES, AES-GCM, DES, Triple DES, ARIA, SEED,	Cryptography algorithms o Support for FIPS-approved and NIST recommended algorithms, modes, curves, and key sizes for RSA (up to 8192, sizes 2048, 3072 and 4096 are mandatory), DSA, Diffie-Hellman, AES, SHA-2 family, and Elliptic Curve Cryptography (ECC); o NIST compliant Hardware Random Number Generator o Asymmetric algorithms: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) o Symmetric algorithms: AES, AES-GCM, DES, Triple DES, ARIA, SEED,	Certified FIPS 140-2 minimum Level 3; EN 60950 – 1; EN 55011

			<p>RC2, RC4, RC5, CAST</p> <ul style="list-style-type: none"> o Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160 <p>API Support</p> <ul style="list-style-type: none"> o PKCS#11 o Microsoft CAPI and CNG o Java (JCA or JCE) <p>Performance</p> <ul style="list-style-type: none"> o RSA-2048 signing ops > 8,000 o RSA-4096 signing ops > 3000 o ECC P256 signing ops > 8,000 o AES-GCM small packet encryption ops > 5,000 <p>Storage</p> <ul style="list-style-type: none"> o Partitioning/virtual device/tenant support for logical delimitation of key pairs (> 50 partitions) o Memory > 8MB <p>Supported Operating Systems</p> <ul style="list-style-type: none"> o Windows Server: 2012R2, 2016, 2019 o Linux: RHEL / CentOS 6, 7, 8. <p>Security</p> <ul style="list-style-type: none"> o Certified FIPS 140-2 minimum Level 3 o Multi-Tenancy support o Remote Management <p>Network Interface</p> <ul style="list-style-type: none"> o Minimum 2x Gigabit Ethernet ports o IPv4 and IPv6 <p>Physical Characteristics</p> <ul style="list-style-type: none"> o Standard 1U/2U rack mount chassis 	<p>RC2, RC4, RC5, CAST</p> <ul style="list-style-type: none"> o Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160 <p>API Support</p> <ul style="list-style-type: none"> o PKCS#11 o Microsoft CAPI and CNG o Java (JCA or JCE) <p>Performance</p> <ul style="list-style-type: none"> o RSA-2048 signing ops > 8,000 o RSA-4096 signing ops > 3000 o ECC P256 signing ops > 8,000 o AES-GCM small packet encryption ops > 5,000 <p>Storage</p> <ul style="list-style-type: none"> o Partitioning/virtual device/tenant support for logical delimitation of key pairs (> 50 partitions) o Memory > 8MB <p>Supported Operating Systems</p> <ul style="list-style-type: none"> o Windows Server: 2012R2, 2016, 2019 o Linux: RHEL / CentOS 6, 7, 8. <p>Security</p> <ul style="list-style-type: none"> o Certified FIPS 140-2 Level 3 o Multi-Tenancy support o Remote Management <p>Network Interface</p> <ul style="list-style-type: none"> o 2x Gigabit Ethernet ports o IPv4 and IPv6 <p>Physical Characteristics</p> <ul style="list-style-type: none"> o Standard 1U/2U rack mount chassis o Input Voltage: 100-240V, 50-60Hz 	
--	--	--	---	---	--

				<ul style="list-style-type: none"> o Input Voltage: 100-240V, 50-60Hz o Temperature: operating 0°C – 35°C, storage -20°C – 60°C o Relative Humidity: 5% to 95% (38°C) noncondensing <p>Safety and Environmental Compliance</p> <ul style="list-style-type: none"> o FCC, CE, UL, RoHS <p>Reliability</p> <ul style="list-style-type: none"> o Dual hot-swap power supplies o Field-serviceable components o Mean Time Between Failure for security module (MTBF) over 300,000 hrs <p>Management and Monitoring</p> <ul style="list-style-type: none"> o Remote configuration, administration, and monitoring o High-Availability disaster recovery o Backup and restore using FIPS 140-2 Level 2 Backup HSM o Secure audit logging o SNMP monitoring and diagnostics o Syslog diagnostics support <p>Warranty policy and support</p> <ul style="list-style-type: none"> o Minimum 2 years of warranty and tech support 	<ul style="list-style-type: none"> o Temperature: operating 0°C – 35°C, storage -20°C – 60°C o Relative Humidity: 5% to 95% (38°C) noncondensing <p>Safety and Environmental Compliance</p> <ul style="list-style-type: none"> o FCC, CE, UL, RoHS <p>Reliability</p> <ul style="list-style-type: none"> o Dual hot-swap power supplies o Field-serviceable components o Mean Time Between Failure for security module (MTBF) over 300,000 hrs <p>Management and Monitoring</p> <ul style="list-style-type: none"> o Remote configuration, administration, and monitoring o High-Availability disaster recovery o Backup and restore using FIPS 140-2 Level 2 Backup HSM o Secure audit logging o SNMP monitoring and diagnostics o Syslog diagnostics support <p>Warranty policy and support</p> <ul style="list-style-type: none"> 2 years of warranty and tech support 	
TOTAL						

Semnat: _____ Numele, Prenumele: Baci Victor În calitate de: Administrator

Ofertantul: SC Rapid Link SRL Adresa: str.Gh.Asachi 71/7 Chişinău R.Moldova