

## Chương V. YÊU CẦU VỀ KỸ THUẬT

### Mục 1. Yêu cầu về kỹ thuật

#### 1.1. Giới thiệu chung về dự án, gói thầu

Đây là một trong những gói thầu được phê duyệt tại Quyết định số 12/QĐ-CTSBMTT ngày 26/02/2026 của Cục trưởng Cục Chứng thực số và Bảo mật thông tin về việc phê duyệt Kế hoạch lựa chọn nhà thầu thực hiện chỉ tiêu kế hoạch và dự toán ngân sách năm 2026, cụ thể:

- Tên gói thầu: Gói thầu số 20: Mua sắm Sim PKI
- Giá gói thầu: 2.750.000.000 VND.
- Nguồn vốn: Ngân sách Quốc phòng - Chi Cơ yếu Chính phủ.
- Hình thức lựa chọn nhà thầu: Chào hàng cạnh tranh qua mạng.
- Phương thức lựa chọn nhà thầu: 01 giai đoạn; 01 túi hồ sơ.
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý I/2026.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện gói thầu: 100 ngày.

#### 1.2. Yêu cầu về kỹ thuật

Tóm tắt thông số kỹ thuật của hàng hóa và các dịch vụ liên quan phải tuân thủ các thông số kỹ thuật và các tiêu chuẩn sau đây:

Hạng mục số	Tên hàng hóa/dịch vụ liên quan	Thông số kỹ thuật và các tiêu chuẩn	
1	Sim PKI	<b>- UICC</b>	
		Hỗ trợ các chế độ điện áp	A, B, và C (5V, 3V, 1.8V)
		Bộ nhớ EEPROM	250,000 byte
		Giao thức truyền nhận	T=0
		Khả năng tăng tốc độ giao tiếp	Có, có thể lên đến 16 clocks/ETU
		Số kênh luận lý	4
		Môi trường bảo mật	Có, tuân thủ theo ISO 7816 ID 0 và 1 với ETSI TS 102.221
		<b>- Phần cứng</b>	
		CPU	32 bit MCU
		Bộ nhớ	16kB ROM cho boot loader 280kB Flash cho lập trình và lưu trữ dữ liệu 10kB cho RAM phân hệ thống 2kB cho RAM phân thuật toán
		Giao tiếp truyền dẫn nối tiếp	H/W UART cho truyền dẫn bán song công bất đồng bộ (tương thích với ISO 7816-3)
		Đặc tính bảo mật	Bộ tăng tốc tính toán phép nhân modular TORNADO-E Bộ tính toán phần cứng DES/Triple DES Bộ tính toán phần cứng AES lên đến 256 bit
		Bộ phát số ngẫu nhiên	Bộ phát số ngẫu nhiên 16-bit RNG Bộ phát số ngẫu nhiên thật 16-bit True RNG One 16-bit Digital True RNG

Bộ tính toán chẵn lẻ/CRC	Bộ tính toán chẵn lẻ cho 8/16/32 bit Bộ tính toán CRC-32
Chứng chỉ bảo mật	CC EAL5+

**- Ứng dụng GSM/USIM**

Thuật toán xác thực USIM	Milenage với kernel AES
Hỗ trợ bảo mật	3G, GSM
Bộ đếm xác thực GSM	Có
Chống nhân bản	Có
Assisted Roaming	Yes

**- JavaCard™**

Phiên bản Java Card (JC)	3.0.2 Classic Edition hoặc cao hơn
Kích thước bộ đệm JC APDU	263 bytes
Kích thước bộ đệm ghi JC	16 bytes
Kích thước phần header cho giao dịch JC	7 bytes
Kích thước stack nội bộ cho JC	24 bytes
Kích thước phần header cho JC Stack Frame	12 bytes
Kích thước JC Stack	Cấu hình, 248 bytes là mặc định
Kích thước bộ đệm JC Transaction	Cấu hình, 250 bytes là mặc định
Số lượng RAM khả dụng cho các JC Applet	11,483 bytes (chia sẻ với RFM)
Số lượng EEPROM khả dụng cho các JC Applet	250,000 bytes

Bộ mã hoá JC	ALG_DES_CBC_NOPAD, ALG_DES_CBC_ISO9797_M1, ALG_DES_CBC_ISO9797_M2, ALG_DES_ECB_NOPAD, ALG_DES_ECB_ISO9797_M1, ALG_DES_ECB_ISO9797_M2 Tất cả bộ mã hoá DES hỗ trợ khoá 8-, 16- và 24-byte. ALG_AES_BLOCK_128_CBC_NOPAD, ALG_AES_BLOCK_128_ECB_NOPAD, ALG_AES_BLOCK_256_CBC_NOPAD, ALG_AES_BLOCK_256_ECB_NOPAD Tất cả bộ mã hoá AES hỗ trợ khoá 16-, 24-, và 32-byte ALG_RSA_NOPAD, ALG_RSA_PKCS1 ALG_RSA_PKCS1_OAEP Tất cả bộ mã hoá RSA hỗ trợ khoá từ 512 đến 4096 bits
--------------	---

Bộ băm JC	ALG_SHA, ALG_SHA_224, ALG_SHA_256, ALG_SHA_384, ALG_SHA_512, ALG_MD5
-----------	---

Bộ ký số JC	ALG_DES_MAC4_NOPAD, ALG_DES_MAC8_NOPAD, ALG_DES_MAC4_ISO9797_M1, ALG_DES_MAC8_ISO9797_M1, ALG_DES_MAC4_ISO9797_M2, ALG_DES_MAC8_ISO9797_M2, ALG_DES_MAC4_PKCS5, ALG_DES_MAC8_PKCS5, ALG_DES_MAC4_ISO9797_1_M2_ALG3, ALG_DES_MAC8_ISO9797_1_M2_ALG3
-------------	---

		<p>Tất cả các chữ ký DES hỗ trợ khoá 8-, 16-, và 24-byte  ALG_AES_MAC_128_NOPAD  Tất cả các chữ ký AES hỗ trợ khoá 16-, 24-, and 32-byte  ALG_RSA_MD5_PKCS1  ALG_RSA_SHA_PKCS1  ALG_RSA_SHA_ISO9796  ALG_RSA_SHA_224_PKCS1  ALG_RSA_SHA_224_PKCS1_PSS  ALG_RSA_SHA_256_PKCS1  ALG_RSA_SHA_256_PKCS1_PSS  ALG_RSA_SHA_384_PKCS1 (yêu cầu độ dài khoá &gt; 624 bits)  ALG_RSA_SHA_384_PKCS1_PSS  ALG_RSA_SHA_512_PKCS1 (yêu cầu độ dài khoá &gt; 752 bits)  ALG_RSA_SHA_PKCS1_PSS (tới 512),  ALG_RSA_MD5_PKCS1_PSS  Tất cả các chữ ký RSA hỗ trợ khoá từ 512 tới 4096 bits  ALG_ECDSA_SHA  ALG_ECDSA_SHA_224  ALG_ECDSA_SHA_256  ALG_ECDSA_SHA_384  ALG_ECDSA_SHA_512  Hỗ trợ các chữ ký ECDSA hỗ trợ khoá 192 - 256 và 521-bit</p>	
	Bộ tính checksum JC	ALG_ISO3309_CRC16 ALG_ISO3309_CRC32	
	Bộ tính số ngẫu nhiên JC	ALG_PSEUDO_RANDOM ALG_SECURE_RANDOM	
	Hỗ trợ thuật toán javacard.security.KeyAgreement	ALG_EC_SVDP_DH, ALG_EC_SVDP_DH_PLAIN	
	Khoá JC	TYPE_DES TYPE_DES_TRANSIENT_RESET TYPE_DES_TRANSIENT_DESELECT TYPE_AES TYPE_AES_TRANSIENT_RESET TYPE_AES_TRANSIENT_DESELECT TYPE_RSA_CRT_PRIVATE, TYPE_RSA_PRIVATE, TYPE_RSA_PUBLIC (exponent lên đến 32 bits) (Hỗ trợ khoá RSA: 512 - 4096 bits) TYPE_EC_FP_PUBLIC, TYPE_EC_FP_PRIVATE (Hỗ trợ khoá ECDSA: 192, 256, 384, và 521 bits)	
	Cặp khoá JC	ALG_RSA, ALG_RSA_CRT, ALG_EC_FP	
	Phát sinh cặp khoá JC On Card	RSA: Chiều dài khoá từ 512 đến 4096 bits EC: Chiều dài khoá 192, 256, 384 và 521 bits	
	Hỗ trợ phần cứng JC	DES, AES, ECC/RSA	
	<b>- Open Platform/Global Platform</b>		
	Phiên bản Open Platform (OP)	2.2.1	
	Phiên bản gói org.globalplatform	1.5	
	Giao thức bảo mật kênh OP	SCP80 SCP81i07 SCP02i15 và i55	
	Phiên bản khoá OP	15	
	Thuật toán mã hoá kênh OTA	AES, DES	

		<b>- (U)SIM API cho JavaCard</b>			
		Phiên bản SIM API	43.019 v5.6.0		
		Phiên bản UICC API	102 241 v6.7.0		
		Phiên bản USIM API	31.130 v6.2.0		
		Bảo mật OTA	Bộ đếm, dùng DES cho mã hoá và tính checksum Tính checksum CRC32		
		- Bảo hành: 12 tháng			

**1.3. Các yêu cầu khác:** Không có.

**Mục 2. Bản vẽ:** Không có bản vẽ

**Mục 3. Kiểm tra và thử nghiệm**

Kiểm tra đúng, đủ số lượng, chất lượng của hàng hoá theo đúng yêu cầu tại Mục 1.2 - Yêu cầu về kỹ thuật.