

Guía de Seguridad de las TIC

CCN-STIC 2100-Anexo B

Cryptographic Mechanisms Evaluation Vendor Questionnaire - Lite



Noviembre de 2024



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

Fecha de Edición: noviembre de 2024
NIPO: 083-25-057-3.



CENTRO CRIPTOLOGICO
NACIONAL
cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2025.05.27 10:02:39 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

TABLE OF CONTENTS

2	
1	INTRODUCTION..... 5
1.1	OBJECTIVE5
1.2	STRUCTURE OF THE DOCUMENT5
2	TOE DEFINITION..... 7
3	CRYPTOGRAPHIC MECHANISMS IMPLEMENTATION 9
3.1	SYMMETRIC ELEMENTARY PRIMITIVES9
3.1.1	BLOCK CIPHER.....9
3.1.2	STREAM CIPHER.....9
3.1.3	HASH FUNCTIONS.....10
3.1.4	SECRET SHARING11
3.1.5	EXTENDABLE-OUTPUT FUNCTIONS (XOF)11
3.2	SYMMETRIC CONSTRUCTIONS.....13
3.2.1	SYMMETRIC ENCRYPTION (CONFIDENTIALITY ONLY)13
3.2.2	DISK ENCRYPTION.....14
3.2.3	INTEGRITY MODES: MESSAGE AUTHENTICATION CODE14
3.2.4	SYMMETRIC ENTITY AUTHENTICATION SCHEMES.....17
3.2.5	AUTHENTICATED ENCRYPTION (AE).....17
3.2.6	KEY PROTECTION18
3.2.7	KEY DERIVATION FUNCTIONS (KDF)19
3.2.8	PASSWORD PROTECTION/HASHING MECHANISMS24
3.3	ASYMMETRIC ELEMENTARY PRIMITIVES27
3.3.1	RSA/INTEGER FACTORIZATION.....27
3.3.2	MULTIPLICATIVE DISCRETE LOGARITHM PROBLEM (FFDLOG)28
3.3.3	ADDITIVE DISCRETE LOGARITHM PROBLEM (ECDLOG)29
3.4	ASYMMETRIC CONSTRUCTIONS.....33
3.4.1	ASYMMETRIC ENCRYPTION SCHEMES33
3.4.2	DIGITAL SIGNATURE34
3.4.3	KEY ESTABLISHMENT40
3.5	RANDOM NUMBER GENERATORS43
3.5.1	DETERMINISTIC RANDOM NUMBER GENERATOR CONSTRUCTION43
3.5.2	DRNG INITIALIZATION44
3.5.3	DRNG RESEEDING CONFIGURATION44
4	CRYPTOGRAPHIC PROTOCOLS IMPLEMENTATION 45
4.1	TRANSPORT LAYER SECURITY PROTOCOL (TLS)46
4.1.1	TLS V1.346
4.1.2	TLS V1.248
4.2	SECURE SHELL (SSH)52
4.3	INTERNET PROTOCOL SECURITY (IPSEC) WITH IKEV2.....54
5	REFERENCES..... 56
6	ACRONYMS..... 57

Note:

This document is an official reference document as part of the [CCN-MEMeC] methodology, so the **vendor shall** complete the vendor-specific version of this document.

1 INTRODUCTION

1.1 OBJECTIVE

1. This document is a vendor questionnaire that aims to gather the required information related to a cryptographic module implementation in order to comply with the Certification Level 1 (**CL1**) of the CCN Cryptographic Mechanisms Evaluation Methodology [CCN-MEMeC].
2. On the one hand, this document will help vendors provide information about their cryptographic implementation with guided questions regarding the cryptographic mechanisms implemented by the TOE. On the other hand, this document also will help the tester to gather all the needed information about the TOE cryptographic implementation by reducing the evaluation effort and time of reviewing.
3. Taking into account that this document contains the main topics related to the cryptographic mechanism implementation according to the [CCN-MEMeC] methodology, it will be useful for vendors to avoid inconsistencies or forget to include relevant information.

1.2 STRUCTURE OF THE DOCUMENT

4. The document is composed of a set of tables including the necessary questions to help the vendor specify the information that will be required by the lab in order to carry out the **CL1** of the CCN Cryptographic Mechanisms Evaluation.
5. The document is organized with a structure similar to the main sections of the [CCN-MEMeC] methodology and includes a table of questions for each type of cryptographic mechanism (usually associated with a cryptographic test). Therefore, this will help the tester to associate the vendor information with the specific evaluation tasks.
6. The specific structure is as detailed below:
 - The name of the question tables will be the same as their associated section identifier, followed by the vendor questionnaire identifier, represented in the following format: **SectionID-VQ**.
 - Each table contains one or several questions related to vendor requirements and evaluation tests that will be identified with the same number as the question number indicated under the column name **Q-ID**.
7. The format of the table is as detailed below:

Q-ID	SectionID-VQ
1	Description of Question 1
	Row for vendor Answer 1
2	Description of Question 2
	Row for vendor Answer 2
...	...
	...
N	Description of Question N
	Row for vendor Answer N

2 TOE DEFINITION

8. This section contains information related to the Target of Evaluation (TOE). The **vendor shall** provide the hardware, firmware, and/or software versions of the TOE and a brief description of its functionality from the cryptographic operation point of view.

Q-ID	TOE Description		
1	TOE Name The vendor shall provide the name/model of the TOE under evaluation.		
2	MEMEC Certification Level The vendor shall indicate the certification level (CL1, CL2, or CL3).		
	Certification Level 1 (CL1)		
3	TOE Versioning Information The vendor shall provide the version of the TOE under evaluation. Note: Indicate (N/A) if hardware, firmware, or software versions do not apply.		
	<table border="1"> <tr> <td>TOE Version</td><td></td></tr> </table>	TOE Version	
	TOE Version		
	<table border="1"> <tr> <td>Hardware Version</td><td></td></tr> </table>	Hardware Version	
	Hardware Version		
<table border="1"> <tr> <td>Firmware Version</td><td></td></tr> </table>	Firmware Version		
Firmware Version			
<table border="1"> <tr> <td>Software Version</td><td></td></tr> </table>	Software Version		
Software Version			
4	TOE Description The vendor shall provide a general description specifying the cryptographic capabilities of the TOE. This general description shall include at least the following information: - Description of the TOE, indicating its main cryptographic functionalities. - Descriptive figure of the TOE, indicating the cryptographic boundary that will be subject to evaluation. - List of all the cryptographic mechanisms included in each cryptographic implementation of the TOE. The purpose of each cryptographic mechanism implemented in the TOE shall be detailed in the tables associated with each of them.		
	<i>[TOE Description]</i> <i>[TOE Figure]</i> <i>[List of all the cryptographic mechanisms for each implementation]</i>		

Q-ID	TOE Description	
	Cryptographic Mechanism	Implementation

3 CRYPTOGRAPHIC MECHANISMS IMPLEMENTATION

9. This section contains the questions associated with the cryptographic mechanisms implemented in the TOE. It aims to provide the tester with all the needed information to demonstrate that the implementation of the cryptographic primitives and cryptographic constructions complies with the requirements from Section 3 “CCN Agreed Cryptographic Mechanisms” of the [CCN-MEMeC] methodology.

3.1 SYMMETRIC ELEMENTARY PRIMITIVES

3.1.1 BLOCK CIPHER

Q-ID	BlockCipher-VQ
1	Does the TOE implement <i>Block Cipher</i> cryptographic primitives? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Block Cipher</i> cryptographic primitives implemented in the TOE?
	☐ AES-128 ☐ AES-192 ☐ AES-256 ☐ Other(s) - Please indicate which one(s)
6	Please provide a brief description of the purpose of each implemented <i>Block Cipher</i> cryptographic primitive with its associated key length. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., AES-128 is implemented in the TOE as a primitive of the AES-128-GCM cryptographic mechanism of the cipher suites utilized by TLS v1.3)

3.1.2 STREAM CIPHER

Q-ID	StreamCipher-VQ
1	Does the TOE implement <i>Stream Cipher</i> cryptographic primitives? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
	What are the <i>Stream Cipher</i> cryptographic primitives implemented in the TOE?

Q-ID	StreamCipher-VQ
2	☐ ChaCha20
	☐ Other(s) - Please indicate which one(s)
5	Please provide a brief description of the purpose of each implemented <i>Stream Cipher</i> cryptographic primitive. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., Chacha20 is implemented in the TOE as a primitive of the ChaCha20-Poly1305 cryptographic mechanism of the cipher suites utilized by TLS v1.3)

3.1.3 HASH FUNCTIONS

Q-ID	Hash-VQ
1	Does the TOE implement <i>Hash</i> cryptographic primitives? Note: If the response is "No", the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Hash</i> cryptographic primitives implemented in the TOE?
	☐ SHA2-256 ☐ SHA2-384 ☐ SHA2-512 ☐ SHA2-512/256 ☐ SHA3-256 ☐ SHA3-384 ☐ SHA3-512 ☐ BLAKE2b
	☐ Other(s) - Please indicate which one(s)
4	Please provide a brief description of the purpose of each implemented <i>Hash</i> cryptographic primitive. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., All the CSPs stored in the TOE are encrypted with AES-256-KeyWrapping, moreover, their SHA-256 digests are also stored in order to protect their integrity)

Q-ID	Hash-VQ

3.1.4 SECRET SHARING

Q-ID	SecretSharing-VQ
1	Does the TOE implement the <i>Secret Sharing (Shamir)</i> cryptographic primitive? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
3	Please provide a brief description of the purpose of each implemented <i>Secret Sharing</i> cryptographic primitive. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., Secret sharing is utilized by the TOE to securely distribute a secret among a group of users)

3.1.5 EXTENDABLE-OUTPUT FUNCTIONS (XOF)

Q-ID	XOF-VQ
1	Does the TOE implement <i>XOF</i> cryptographic primitives? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>XOF</i> cryptographic primitives implemented in the TOE?
	☐ SHAKE128 ☐ SHAKE256 ☐ cSHAKE128 ☐ cSHAKE256
	☐ Other(s) - Please indicate which one(s)
4	Please provide a brief description of the purpose of each implemented <i>XOF</i> cryptographic primitive. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., cSHAKE is used by the TOE as an underlying primitive to KMAC)

Q-ID	XOF-VQ

3.2 SYMMETRIC CONSTRUCTIONS

3.2.1 SYMMETRIC ENCRYPTION (CONFIDENTIALITY ONLY)

Q-ID	SymEncryption-VQ
1	Does the TOE implement <i>Symmetric Encryption (Confidentiality Only)</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Symmetric Encryption (Confidentiality Only)</i> cryptographic constructions implemented in the TOE?
	☐ No-Padding
	☐ AES-CBC-128 ☐ PKCS#7
	☐ ISO 7816
	☐ No-Padding
	☐ AES-CBC-192 ☐ PKCS#7
	☐ ISO 7816
	☐ No-Padding
	☐ AES-CBC -256 ☐ PKCS#7
	☐ ISO 7816
	☐ AES-CBC-CS-128 ☐ AES-CBC-CS-192 ☐ AES-CBC-CS-256
	☐ AES-CFB-128 ☐ AES-CFB-192 ☐ AES-CFB-256
☐ AES-CTR-128 ☐ AES-CTR -192 ☐ AES-CTR -256	
☐ AES-OFB-128 ☐ AES-OFB-192 ☐ AES-OFB-256	
☐ Other(s) - Please indicate which one(s)	
3	Please indicate whether the implemented symmetric constructions are employed in conjunction with a cryptographic mechanism to provide data integrity and authentication. Note: Justify the answer either in the affirmative or negative case.

Q-ID	SymEncryption-VQ
7	Please provide a brief description of the purpose of each implemented <i>Symmetric Encryption</i> cryptographic construction with its associated key length. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The AES-CBC-256 No-Padding construction is used to encrypt the data received from the input interface)

3.2.2 DISK ENCRYPTION

Q-ID	DiskEncryption-VQ
1	Does the TOE implement <i>Disk Encryption</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered. ☐ Yes ☐ No
2	What are the <i>Disk Encryption</i> cryptographic constructions implemented in the TOE? ☐ AES-XTS-256 ☐ AES-XTS-512 ☐ Other(s) - Please indicate which one(s)
7	Please provide a brief description of the purpose of each implemented <i>Disk Encryption</i> cryptographic construction with its associated key length. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The AES-XTS-256 mode is used to perform disk encryption)

3.2.3 INTEGRITY MODES: MESSAGE AUTHENTICATION CODE

Q-ID	MAC-VQ
1	Does the TOE implement <i>Message Authentication Code</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.

Q-ID	MAC-VQ
	☐ Yes ☐ No
2	What are the <i>Message Authentication Code</i> cryptographic constructions implemented in the TOE?
	☐ AES-CMAC-128 ☐ AES-CMAC-192 ☐ AES-CMAC-256
	☐ AES-CBC-MAC-128 ☐ AES-CBC-MAC-192 ☐ AES-CBC-MAC-256
	☐ HMAC-SHA-1 ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-384
	☐ HMAC-SHA2-512 ☐ HMAC-SHA2-512/256 ☐ HMAC-SHA3-256
	☐ HMAC-SHA3-384 ☐ HMAC-SHA3-512
	☐ AES-GMAC-128 ☐ AES-GMAC-192 ☐ AES-GMAC-256
	☐ KMAC-128 ☐ KMAC-256
	☐ Poly1305
	☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>HMAC</i> cryptographic construction, please provide the size of the HMAC keys used.
	Note: Please, provide evidence for each HMAC implementation (e.g., a pointer to the source code, a piece of source code, etc.).
4	In the case of implementing the <i>CMAC</i>, <i>CBC-MAC</i>, or <i>HMAC</i> cryptographic construction, does the TOE implement MAC truncation? What is the output bit length of the truncation?
	Note: In affirmative case, please, describe how it is implemented and provide evidence of the implementation for each message authentication code cryptographic construction (e.g., a pointer to the source code, a piece of source code, etc.). Note: In the case of performing MAC truncation to 64 bits, please also provide evidence that the maximal number of MAC verifications performed for a given key over its lifetime can be bounded by 2^{20} .

Q-ID	MAC-VQ
5	In the case of implementing the <i>GMAC</i> cryptographic construction, does the TOE comply with the following requirements related to IV management? a. The IV length is equal to 96 bits. b. The IV is constructed according to the deterministic IV construction method [SP800-38D] section 8.2.1. Note: In affirmative case, please, describe how each requirement is implemented and provide evidence of the implementation for each GMAC cryptographic construction (e.g., a pointer to the source code, a piece of source code, etc.).
6	In the case of implementing the <i>GMAC</i> cryptographic construction, what is the output bit length of the MAC? Note: Please, provide evidence for each GMAC implementation (e.g., a pointer to the source code, a piece of source code, etc.).
7	In the case of implementing the <i>KMAC</i> cryptographic construction, please provide the following information: a. The size of the KMAC keys used. b. Is KMAC used in XOF mode? c. What is the output bit length of the MAC? d. Does the bit length of the MAC output correspond to the direct output of the algorithm or truncation is applied? Note: Please, provide evidence for each KMAC implementation (e.g., a pointer to the source code, a piece of source code, etc.).
10	Please provide a brief description of the purpose of each implemented <i>Message Authentication Code</i> cryptographic construction with its associated key length, underlying mechanism, etc. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The HMAC-SHA-256 algorithm is used to check the integrity and authenticity of a firmware update before installing it)

3.2.4 SYMMETRIC ENTITY AUTHENTICATION SCHEMES

Q-ID	EntityAuth-VQ
1	Does the TOE implement <i>Symmetric Entity Authentication</i> (challenge-response) cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the length ranges used in the <i>Symmetric Entity Authentication</i> cryptographic constructions implemented in the TOE?
	☐ $\text{len} \geq 125$ ☐ $96 \leq \text{len} < 125$
	☐ Other(s) - Please indicate which one(s)
5	Please provide a brief description of the purpose of each implemented <i>Symmetric Entity Authentication</i> cryptographic construction. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., A challenge-response authentication method, based on a zero-knowledge proof, is used as the initial step of communication)

3.2.5 AUTHENTICATED ENCRYPTION (AE)

Q-ID	AuthEncryption-VQ
1	Does the TOE implement <i>Authenticated Encryption</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Authenticated Encryption</i> cryptographic constructions implemented in the TOE?
	☐ Encrypt-then-MAC - Please indicate the encryption and MAC mechanism
	☐ AES-CCM-128 ☐ AES-CCM-192 ☐ AES-CCM-256
	☐ AES-GCM-128 ☐ AES-GCM-192 ☐ AES-GCM-256
	☐ AES-EAX-128 ☐ AES-EAX-192 ☐ AES-EAX-256

Q-ID	AuthEncryption-VQ
	☐ ChaCha20-Poly1305 ☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>GCM</i> cryptographic construction, does the TOE comply with the following requirements related to IV management? a. The IV length is equal to 96 bits. b. The IV is constructed according to the deterministic IV construction method [SP800-38D] section 8.2.1. Note: In affirmative case, please, describe how each is implemented and provide evidence of the implementation for each GCM cryptographic construction (e.g., a pointer to the source code, a piece of source code, etc.).
4	In the case of implementing any authenticated encryption cryptographic construction, what is the output bit length of the MAC (or tag)? Note: Please, provide evidence for each authenticated encryption construction and implementation (e.g., a pointer to the source code, a piece of source code, etc.).
10	Please provide a brief description of the purpose of each implemented <i>Authenticated Encryption</i> cryptographic construction with its associated key length. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The data sent through the communication channel is encrypted with AES-GCM-256, providing confidentiality, integrity, and authentication to the data)

3.2.6 KEY PROTECTION

Q-ID	KeyProtection-VQ
1	Does the TOE implement <i>Key Protection</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered. ☐ Yes ☐ No
2	What are the <i>Key Protection</i> cryptographic constructions implemented in the TOE? ☐ AES-SIV-256 ☐ AES-SIV-384 ☐ AES-SIV-512

Q-ID	KeyProtection-VQ
	☐ AES-KW-128 ☐ AES-KW-192 ☐ AES-KW-256 ☐ AES-KWP-128 ☐ AES-KWP-192 ☐ AES-KWP-256
	☐ Authenticated Encryption Construction(s) - Please indicate which one(s)
	☐ Other(s) - Please indicate which one(s)
8	Please provide a brief description of the purpose of each implemented <i>Key Protection</i> cryptographic construction with its associated key length. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The SSPs are entered into the TOE encrypted with AES-KWP-256)

3.2.7 KEY DERIVATION FUNCTIONS (KDF)

Q-ID	KeyDerivation-VQ
1	Does the TOE implement <i>Key Derivation</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Key Derivation</i> cryptographic constructions implemented in the TOE?
	☐ NIST SP800-56A/B/C One-Step KDF
	☐ NIST SP800-56A/B/C Two-Step KDF
	☐ NIST SP800-108 KDF in Counter Mode
	☐ NIST SP800-108 KDF in Feedback Mode
	☐ NIST SP800-108 KDF in Double-Pipeline Mode
	☐ NIST SP800-108 KDF using KMAC
	☐ ANSI-X9.63 KDF
	☐ PBKDF2
☐ HKDF (RFC 5869)	

Q-ID	KeyDerivation-VQ
	☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>NIST SP800-56A/B/C One-Step KDF</i> cryptographic construction, please indicate its parameterization.
	☐ SHA2-256 ☐ SHA2-384 ☐ SHA2-512 ☐ SHA2-512/256 ☐ SHA3-256 ☐ SHA3-384 ☐ SHA3-512
	☐ HMAC SHA1 ☐ HMAC SHA2-256 ☐ HMAC SHA2-384 ☐ HMAC SHA2-512 ☐ HMAC SHA2-512/256 ☐ HMAC SHA3-256 ☐ HMAC SHA3-384 ☐ HMAC SHA3-512
	☐ KMAC-128 ☐ KMAC-256
	☐ Other(s) - Please indicate which one(s)
	In the case of implementing the <i>NIST SP800-56A/B/C Two-Step KDF</i> cryptographic construction, please indicate its parameterization.
	Extraction Step
	☐ HMAC SHA1 ☐ HMAC SHA2-256 ☐ HMAC SHA2-384 ☐ HMAC SHA2-512 ☐ HMAC SHA2-512/256 ☐ HMAC SHA3-256 ☐ HMAC SHA3-384 ☐ HMAC SHA3-512
4	☐ AES-128-CMAC ☐ AES-192-CMAC ☐ AES-256-CMAC
	☐ Other(s) - Please indicate which one(s)
	Expansion Step
	☐ NIST SP800-108 KDF Please indicate which one(s) and the complete parameterization. It is necessary to complete the associated questions (Q-5 to Q-8) for the implemented NIST SP800-108 KDFs.
	☐ Other(s) - Please indicate which one(s)

Q-ID	KeyDerivation-VQ
5	In the case of implementing the <i>NIST SP800-108 KDF in Counter Mode</i> cryptographic construction, please indicate its parameterization.
	Underlying Mechanisms
	☐ HMAC SHA1 ☐ HMAC SHA2-256
	☐ HMAC SHA2-384 ☐ HMAC SHA2-512
	☐ HMAC SHA2-512/256 ☐ HMAC SHA3-256
	☐ HMAC SHA3-384 ☐ HMAC SHA3-512
	☐ AES-128-CMAC ☐ AES-192-CMAC
	☐ AES-256-CMAC
	☐ KMAC-128 ☐ KMAC-256
	☐ Other(s) - Please indicate which one(s)
	Supported Parameterization
	Counter <i>i</i> : XXX bits ☐ Big-endian ☐ Little-endian
	Requested length <i>L</i> : XXX bits ☐ Big-endian ☐ Little-endian
	Label: ☐ Yes ☐ No
	Context: ☐ Yes ☐ No
All-zero octet (<i>z</i>): ☐ Yes ☐ No	
The pattern for the input to the underlying PRF: (For example, <i>i</i> Label 0x00 Context <i>L</i>)	
6	In the case of implementing the <i>NIST SP800-108 KDF in Feedback Mode</i> cryptographic construction, please indicate its parameterization.
	Underlying Mechanisms
	☐ HMAC SHA1 ☐ HMAC SHA2-256
	☐ HMAC SHA2-384 ☐ HMAC SHA2-512
	☐ HMAC SHA2-512/256 ☐ HMAC SHA3-256
☐ HMAC SHA3-384 ☐ HMAC SHA3-512	

Q-ID	KeyDerivation-VQ
	☐ AES-128-CMAC ☐ AES-192-CMAC
	☐ AES-256-CMAC
	☐ KMAC-128 ☐ KMAC-256
	☐ Other(s) - Please indicate which one(s)
	Supported Parameterization
	Counter i : XXX bits ☐ Big-endian ☐ Little-endian
	Requested length L : XXX bits ☐ Big-endian ☐ Little-endian
	IV: ☐ Yes ☐ No
	Label: ☐ Yes ☐ No
	Context: ☐ Yes ☐ No
	All-zero octet (z): ☐ Yes ☐ No
	The pattern for the input to the underlying PRF: (For example, IV i Label 0x00 Context L)
	In the case of implementing the <i>NIST SP800-108 KDF in Double-Pipeline Mode</i> cryptographic construction, please indicate its parameterization.
	Underlying Mechanisms
☐ HMAC SHA1 ☐ HMAC SHA2-256	
☐ HMAC SHA2-384 ☐ HMAC SHA2-512	
☐ HMAC SHA2-512/256 ☐ HMAC SHA3-256	
☐ HMAC SHA3-384 ☐ HMAC SHA3-512	
☐ AES-128-CMAC ☐ AES-192-CMAC	
☐ AES-256-CMAC	
☐ KMAC-128 ☐ KMAC-256	
☐ Other(s) - Please indicate which one(s)	
Supported Parameterization	

7

Q-ID	KeyDerivation-VQ
	Counter <i>i</i> : XXX bits ☐ Big-endian ☐ Little-endian
	Requested length <i>L</i> : XXX bits ☐ Big-endian ☐ Little-endian
	Label: ☐ Yes ☐ No
	Context: ☐ Yes ☐ No
	All-zero octet (<i>z</i>): ☐ Yes ☐ No
	The pattern for the input to the underlying PRF: (For example, <i>i</i> Label 0x00 Context <i>L</i>)
8	In the case of implementing the <i>NIST SP800-108 KDF in KMAC mode cryptographic construction</i> , please indicate its parameterization.
	☐ KMAC-128 ☐ KMAC-256
	☐ Other(s) - Please indicate which one(s)
9	In the case of implementing the <i>ANSI-X9.63 KDF cryptographic construction</i> , please indicate its parameterization.
	☐ SHA2-256 ☐ SHA2-384
	☐ SHA2-512 ☐ SHA2-512/256
	☐ SHA3-256 ☐ SHA3-384
	☐ SHA3-512
	☐ Other(s) - Please indicate which one(s)
10	In the case of implementing the <i>PBKDF2 cryptographic construction</i> , please indicate its parameterization.
	☐ HMAC-SHA-1 ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-384
	☐ HMAC-SHA2-512 ☐ HMAC-SHA2-512/256 ☐ HMAC-SHA3-256
	☐ HMAC-SHA3-384 ☐ HMAC-SHA3-512
	☐ Other(s) - Please indicate which one(s)
12	In the case of implementing the <i>HKDF (RFC 5869) cryptographic construction</i> , please indicate its parameterization.
	☐ HMAC-SHA-1 ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-384

Q-ID	KeyDerivation-VQ
	☐ HMAC-SHA2-512 ☐ HMAC-SHA2-512/256 ☐ HMAC-SHA3-256 ☐ HMAC-SHA3-384 ☐ HMAC-SHA3-512 ☐ Other(s) - Please indicate which one(s)
15	Please provide a brief description of the purpose of each implemented <i>Key Derivation</i> cryptographic construction with its associated underlying mechanism, length of the derived key, etc. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The PBKDF2-HMAC-SHA-256 derives a new key of 256 bits using the user password)

3.2.8 PASSWORD PROTECTION/HASHING MECHANISMS

Q-ID	PasswordMechanisms-VQ
1	Does the TOE implement <i>Password Protection/Hashing</i> cryptographic constructions? Note: If the response is "No", the following questions in this table shall not be answered. ☐ Yes ☐ No
2	What are the <i>Password Protection/Hashing</i> cryptographic constructions implemented in the TOE? ☐ Argon2id ☐ PBKDF2 ☐ SCRYPT ☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>PBKDF2</i> cryptographic construction, please indicate its parameterization. ☐ HMAC-SHA-1 ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-384 ☐ HMAC-SHA2-512 ☐ HMAC-SHA2-512/256 ☐ HMAC-SHA3-256 ☐ HMAC-SHA3-384 ☐ HMAC-SHA3-512

Q-ID	PasswordMechanisms-VQ
	☐ Other(s) - Please indicate which one(s)
4	In the case of implementing the <i>SCRYPT</i> cryptographic construction, please indicate its parameterization.
	☐ PBKDF2 HMAC SHA2-256
	☐ Other(s) - Please indicate which one(s)
5	In the case of implementing the <i>Argon2id</i> cryptographic construction, please indicate the following parameterization. Note: Please, provide evidence for each Argon2id implementation (e.g., a pointer to the source code, a piece of source code, etc.).
	The memory size (m) is: XXX
	The number of passes (t) is: XXX passes
	The password length (P) is XXX bytes
	The degree of parallelism (p) is XXX lanes
	The salt (S) length is: XXX bits
	Is the salt unique for each password? ☐ Yes ☐ No
	The tag (T) length is: XXX bits
	The secret value (K) length is: XXX bytes
	The associated data (X) length is: XXX bytes
6	In the case of implementing the <i>PBKDF2</i> cryptographic construction, please indicate the following parameterization. Note: Please, provide evidence for each PBKDF2 implementation (e.g., a pointer to the source code, a piece of source code, etc.).
	The number of iterations is: XXX iterations
	The salt length is: XXX bits
9	Please provide a brief description of the purpose of each implemented <i>Password Protection/Hashing</i> cryptographic with its associated underlying mechanism, length of the derived key, etc. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The TOE protects the user password using PBKDF2-HMAC-SHA-256 cryptographic construction)

Q-ID	PasswordMechanisms-VQ

3.3 ASYMMETRIC ELEMENTARY PRIMITIVES

3.3.1 RSA/INTEGER FACTORIZATION

Q-ID	RSA-VQ
1	Does the TOE implement cryptographic primitives based on the <i>integer factorization problem (RSA)</i>? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>RSA</i> cryptographic primitives implemented in the TOE?
	☐ RSA-2048 bits ☐ RSA-3072 bits ☐ RSA-4096 bits ☐ Other(s) - Please indicate which one(s)
3	Please provide a brief description of the purpose of each implemented cryptographic primitive based on the <i>integer factorization problem (RSA)</i>. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., The TOE uses a digital signature based on RSA-2048 to perform firmware authentication)

Q-ID	RSA-IMPLEMENTATION-VQ
1	What are the <i>RSA</i> cryptographic operations implemented in the TOE? Please complete a row for each of the different RSA parameterizations and/or implementations. Add as many as necessary.
1-1	RSA Implementation – 1
	☐ Modular Exponentiation operations with an RSA Public Key
	☐ Modular Exponentiation operations with an RSA Public Key, where the value of e is equal to 65537
	☐ Modular Exponentiation operations with an RSA Private Key
	☐ Modular Exponentiation operations with extended parameters using recombination of the Chinese Remainder Theorem (CRT)
	☐ Other(s) - Please indicate which one(s)

1-2	RSA Implementation – 2
	☐ Modular Exponentiation operations with an RSA Public Key
	☐ Modular Exponentiation operations with an RSA Public Key, where the value of e is equal to 65537
	☐ Modular Exponentiation operations with an RSA Private Key
	☐ Modular Exponentiation operations with extended parameters using recombination of the Chinese Remainder Theorem (CRT)
1-3	...
...	...

3.3.2 MULTIPLICATIVE DISCRETE LOGARITHM PROBLEM (FFDLOG)

Q-ID	FFDLOG-VQ
1	Does the TOE implement <i>FFDLOG</i> cryptographic primitives? Note: If the response is “No”, the following questions in this table shall not be answered. ☐ Yes ☐ No
2	What are the <i>FFDLOG</i> cryptographic primitives implemented in the TOE? ☐ MODP-2048 bits ☐ MODP-3072 bits ☐ MODP-4096 bits ☐ MODP-6144 bits ☐ MODP-8192 bits ☐ FFDHE-2048 bits ☐ FFDHE-3072 bits ☐ FFDHE-4096 bits ☐ FFDHE-6144 bits ☐ FFDHE-8192 bits ☐ Other(s) - Please indicate which one(s)
3	Please provide a brief description of the purpose of each implemented asymmetric cryptographic primitive based on <i>FFDLOG</i>. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., The FFDHE-2048 group is used in the DH key establishment scheme of the cipher suites utilized by TLS v1.2)

3.3.3 ADDITIVE DISCRETE LOGARITHM PROBLEM (ECDLOG)

Q-ID	ECDLOG-VQ
1	Does the TOE implement <i>ECDLOG</i> cryptographic primitives? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>ECDLOG</i> cryptographic primitives implemented in the TOE?
	☐ BrainpoolP256r1 ☐ BrainpoolP384r1 ☐ BrainpoolP512r1
	☐ NIST P-256 ☐ NIST P-384 ☐ NIST P-521
	☐ FRP256v1 ☐ Curve25519 ☐ Curve448
	☐ Edwards25519 ☐ Edwards448
	☐ Other(s) - Please indicate which one(s)
3	Please provide a brief description of the purpose of each implemented asymmetric cryptographic primitive based on <i>ECDLOG</i>. If there is more than one implementation for the same primitive, please provide the purpose of each of them (on different rows). (e.g., The NIST P-256 curve is used in the ECDHE key establishment scheme of the cipher suites utilized by TLS v1.2)

Q-ID	ECDLOG-IMPLEMENTATION-VQ
1	What are the <i>Elliptic Curve</i> cryptographic operations implemented in the TOE? Please complete a row for each of the different ECDLOG parameterizations and/or implementations. Add as many as necessary. In the case of NIST P Curves, BrainpoolP Curves, and FRP256v1 Curve:
1-1	ECDLOG Implementation – 1
	☐ Key Generation Please indicate the associated operation
	☐ EC Scalar Multiplication with Fixed Basepoint $R = d \times G$ where G denotes the generator ☐ EC Scalar Multiplication $R = d \times P$

Q-ID	ECDLOG-IMPLEMENTATION-VQ	
		where P is generic and G is introduced into it as the generator ☐ Other(s) - Please indicate which one(s)
	☐ Signature Generation Please indicate the associated operation	☐ EC Scalar Multiplication $R = d \times P$ where P is a point lying on the curve ☐ Other(s) - Please indicate which one(s)
	☐ Signature Verification Please indicate the associated operation	☐ MultiScalar Multiplication $R = u \times S + v \times T$ where S and T are points lying on the curve S is generic and G is introduced into it as the generator ☐ MultiScalar Multiplication with Fixed Basepoint $R = u \times G + v \times T$ where T is a point lying on the curve and G denotes the generator ☐ Other(s) - Please indicate which one(s)
	☐ Preshared Secret Computation Please indicate the associated operation	☐ EC Scalar Multiplication $R = d \times P$ where P is a point lying on the curve ☐ Other(s) - Please indicate which one(s)
	...	
	...	
	What are the <i>Elliptic Curve</i> cryptographic operations implemented in the TOE? Please complete a row for each of the different ECDLOG parameterizations and/or implementations. Add as many as necessary. In the case of Curve25519 and Curve448:	
	ECDLOG Implementation – 1	
	☐ Key Generation	☐ EC Scalar Multiplication with Fixed Basepoint $R = d \times G$

Q-ID	ECDLOG-IMPLEMENTATION-VQ	
	Please indicate the associated operation	where G denotes the generator
		☐ EC Scalar Multiplication $R = d \times P$ where P is generic and G is introduced into it as the generator
	☐ Preshared Secret Computation Please indicate the associated operation	☐ EC Scalar Multiplication $R = d \times P$ where P is a point lying on the curve
		☐ Other(s) - Please indicate which one(s)
2-2	...	
2-3	...	
3	What are the <i>Elliptic Curve</i> cryptographic operations implemented in the TOE? Please complete a row for each of the different ECDLOG parameterizations and/or implementations. Add as many as necessary. In the case of Edwards25519 and Edwards448 curves:	
3-1	ECDLOG Implementation – 1	
	☐ Key Generation Please indicate the associated operation	☐ EC Scalar Multiplication with Fixed Basepoint $R = d \times G$ where G denotes the generator
		☐ EC Scalar Multiplication $R = d \times P$ where P is generic and G is introduced into it as the generator
		☐ Other(s) - Please indicate which one(s)
	☐ Signature Generation Please indicate the associated operation	☐ EC Scalar Multiplication $R = d \times P$ where P is a point lying on the curve
		☐ Other(s) - Please indicate which one(s)
☐ Signature Verification	☐ MultiScalar Multiplication	

Q-ID	ECDLOG-IMPLEMENTATION-VQ	
	Please indicate the associated operation	$R = u \times S + v \times T$ where S and T are points lying on the curve S is generic and G is introduced into it as the generator
		☐ MultiScalar Multiplication with Fixed Basepoint $R = u \times G + v \times T$ where T is a point lying on the curve and G denotes the generator
		☐ Other(s) - Please indicate which one(s)
3-2	...	
3-3	...	

3.4 ASYMMETRIC CONSTRUCTIONS

3.4.1 ASYMMETRIC ENCRYPTION SCHEMES

Q-ID	AsymEncryption-VQ																																
1	Does the TOE implement <i>Asymmetric Encryption</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.																																
	☐ Yes ☐ No																																
2	What are the <i>Asymmetric Encryption</i> cryptographic constructions implemented in the TOE?																																
	☐ RSA-OAEP (PKCS#1v2.1) ☐ RSA-PKCS#1v1.5																																
	☐ Other(s) - Please indicate which one(s)																																
3	In the case of implementing the <i>RSA-OAEP (PKCS#1v2.1)</i> cryptographic construction, please indicate its parameterization.																																
	<table border="1"> <thead> <tr> <th></th><th>Mod 2048-bit</th><th>Mod 3072-bit</th><th>Mod 4096-bit</th></tr> </thead> <tbody> <tr> <td>SHA2-256</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA2-384</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA2-512</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA2-512/256</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA3-256</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA3-384</td><td>☐</td><td>☐</td><td>☐</td></tr> <tr> <td>SHA3-512</td><td>☐</td><td>☐</td><td>☐</td></tr> </tbody> </table>		Mod 2048-bit	Mod 3072-bit	Mod 4096-bit	SHA2-256	☐	☐	☐	SHA2-384	☐	☐	☐	SHA2-512	☐	☐	☐	SHA2-512/256	☐	☐	☐	SHA3-256	☐	☐	☐	SHA3-384	☐	☐	☐	SHA3-512	☐	☐	☐
		Mod 2048-bit	Mod 3072-bit	Mod 4096-bit																													
	SHA2-256	☐	☐	☐																													
	SHA2-384	☐	☐	☐																													
	SHA2-512	☐	☐	☐																													
	SHA2-512/256	☐	☐	☐																													
	SHA3-256	☐	☐	☐																													
	SHA3-384	☐	☐	☐																													
SHA3-512	☐	☐	☐																														
☐ Other(s) - Please indicate which one(s)																																	
In the case of implementing the <i>RSA-PKCS#1v1.5</i> cryptographic construction, please indicate its parameterization.																																	
☐ Other(s) - Please indicate which one(s)																																	
☐ Other(s) - Please indicate which one(s)																																	
☐ Other(s) - Please indicate which one(s)																																	
☐ Other(s) - Please indicate which one(s)																																	
☐ Other(s) - Please indicate which one(s)																																	

Q-ID	AsymEncryption-VQ
	☐ RSA-2048 bits ☐ RSA-3072 bits ☐ RSA-4096 bits ☐ Other(s) - Please indicate which one(s)
8	Please provide a brief description of the purpose of each implemented <i>Asymmetric Encryption</i> cryptographic construction with its associated modulus, hash primitive, etc. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., User data are entered into the TOE encrypted with RSA-OAEP with modulus 2048 bits and SHA-256)

3.4.2 DIGITAL SIGNATURE

Q-ID	DigitalSignature-VQ								
1	Does the TOE implement <i>Digital Signature</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered. ☐ Yes ☐ No								
2	What are the <i>Digital Signature</i> cryptographic constructions implemented in the TOE? ☐ RSA-PSS (PKCS#1v2.1) ☐ RSA-PKCS#1v1.5 ☐ DSA ☐ KCDSA ☐ Schnorr (SDSA) ☐ EC-DSA ☐ EC-KCDSA ☐ EC-GDSA ☐ EC-Schnorr (EC-SDSA) ☐ EC-Schnorr (EC-FSDSA) ☐ EdDSA ☐ XMSS ☐ ML-DSA ☐ Falcon ☐ SLH-DSA ☐ Other(s) - Please indicate which one(s)								
3	In the case of implementing the <i>RSA-PSS (PKCS#1v2.1)</i> cryptographic construction, please indicate its parameterization. <table border="1"> <thead> <tr> <th></th> <th>Mod 2048-bit</th> <th>Mod 3072-bit</th> <th>Mod 4096-bit</th> </tr> </thead> <tbody> <tr> <td>SHA2-256</td> <td>☐</td> <td>☐</td> <td>☐</td> </tr> </tbody> </table>		Mod 2048-bit	Mod 3072-bit	Mod 4096-bit	SHA2-256	☐	☐	☐
	Mod 2048-bit	Mod 3072-bit	Mod 4096-bit						
SHA2-256	☐	☐	☐						

Q-ID	DigitalSignature-VQ					
	SHA2-384	☐	☐	☐		
	SHA2-512	☐	☐	☐		
	SHA2-512/256	☐	☐	☐		
	SHA3-256	☐	☐	☐		
	SHA3-384	☐	☐	☐		
	SHA3-512	☐	☐	☐		
	☐ Other(s) - Please indicate which one(s)					
4	In the case of implementing the <i>RSA-PKCS#1v1.5</i> cryptographic construction, please indicate its parameterization.					
		Mod 2048-bit	Mod 3072-bit	Mod 4096-bit		
	SHA2-256	☐	☐	☐		
	SHA2-384	☐	☐	☐		
	SHA2-512	☐	☐	☐		
	SHA2-512/256	☐	☐	☐		
	☐ Other(s) - Please indicate which one(s)					
5	In the case of implementing the <i>DSA</i> cryptographic construction, please indicate its parameterization.					
		MODP 2048-bit	MODP 3072-bit	MODP 4096-bit	MODP 6144-bit	MODP 8192-bit
	SHA2-256	☐	☐	☐	☐	☐
	SHA2-384	☐	☐	☐	☐	☐
	SHA2-512	☐	☐	☐	☐	☐
	SHA2-512/256	☐	☐	☐	☐	☐
	SHA3-256	☐	☐	☐	☐	☐
	SHA3-384	☐	☐	☐	☐	☐
	SHA3-512	☐	☐	☐	☐	☐
	☐ Other(s) - Please indicate which one(s)					

Q-ID	DigitalSignature-VQ							
6	In the case of implementing the <i>KCDSA</i> cryptographic construction, please indicate its parameterization.							
		MODP 2048-bit	MODP 3072-bit	MODP 4096-bit	MODP 6144-bit	MODP 8192-bit		
	SHA2-256	☐	☐	☐	☐	☐		
	SHA2-384	☐	☐	☐	☐	☐		
	SHA2-512	☐	☐	☐	☐	☐		
	SHA2-512/256	☐	☐	☐	☐	☐		
	SHA3-256	☐	☐	☐	☐	☐		
	SHA3-384	☐	☐	☐	☐	☐		
	SHA3-512	☐	☐	☐	☐	☐		
☐ Other(s) - Please indicate which one(s)								
7	In the case of implementing the <i>SDSA</i> cryptographic construction, please indicate its parameterization.							
		MODP 2048-bit	MODP 3072-bit	MODP 4096-bit	MODP 6144-bit	MODP 8192-bit		
	SHA2-256	☐	☐	☐	☐	☐		
	SHA2-384	☐	☐	☐	☐	☐		
	SHA2-512	☐	☐	☐	☐	☐		
	SHA2-512/256	☐	☐	☐	☐	☐		
	SHA3-256	☐	☐	☐	☐	☐		
	SHA3-384	☐	☐	☐	☐	☐		
	SHA3-512	☐	☐	☐	☐	☐		
☐ Other(s) - Please indicate which one(s)								
8	In the case of implementing the <i>EC-DSA</i> cryptographic construction, please indicate its parameterization.							
		P-256	P-384	P-521	Brainpool P256r1	Brainpool P384r1	Brainpool P512r1	FRP256v1
SHA2-256		☐	☐	☐	☐	☐	☐	☐

Q-ID	DigitalSignature-VQ							
	SHA2-384 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	SHA2-512 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	SHA2-512 /256 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	SHA3-256 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	SHA3-384 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	SHA3-512 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐							
	☐ Other(s) - Please indicate which one(s)							
9	In the case of implementing the <i>EC-KCDSA</i> cryptographic construction, please indicate its parameterization.							
		P-256	P-384	P-521	Brainpool P256r1	Brainpool P384r1	Brainpool P512r1	FRP256v1
	SHA2-256	☐	☐	☐	☐	☐	☐	☐
	SHA2-384	☐	☐	☐	☐	☐	☐	☐
	SHA2-512	☐	☐	☐	☐	☐	☐	☐
	SHA2-512 /256	☐	☐	☐	☐	☐	☐	☐
	SHA3-256	☐	☐	☐	☐	☐	☐	☐
	SHA3-384	☐	☐	☐	☐	☐	☐	☐
	SHA3-512	☐	☐	☐	☐	☐	☐	☐
☐ Other(s) - Please indicate which one(s)								
10	In the case of implementing the <i>EC-GDSA</i> cryptographic construction, please indicate its parameterization.							
		P-256	P-384	P-521	Brainpool P256r1	Brainpool P384r1	Brainpool P512r1	FRP256v1
	SHA2-256	☐	☐	☐	☐	☐	☐	☐
	SHA2-384	☐	☐	☐	☐	☐	☐	☐
	SHA2-512	☐	☐	☐	☐	☐	☐	☐
	SHA2-512 /256	☐	☐	☐	☐	☐	☐	

Q-ID	DigitalSignature-VQ							
	SHA3-256	☐	☐	☐	☐	☐	☐	☐
	SHA3-384	☐	☐	☐	☐	☐	☐	☐
	SHA3-512	☐	☐	☐	☐	☐	☐	☐
	☐ Other(s) - Please indicate which one(s)							
11	In the case of implementing the <i>EC-SDSA</i> cryptographic construction, please indicate its parameterization.							
		P-256	P-384	P-521	Brainpool P256r1	Brainpool P384r1	Brainpool P512r1	FRP256v1
	SHA2-256	☐	☐	☐	☐	☐	☐	☐
	SHA2-384	☐	☐	☐	☐	☐	☐	☐
	SHA2-512	☐	☐	☐	☐	☐	☐	☐
	SHA2-512 /256	☐	☐	☐	☐	☐	☐	☐
	SHA3-256	☐	☐	☐	☐	☐	☐	☐
	SHA3-384	☐	☐	☐	☐	☐	☐	☐
	SHA3-512	☐	☐	☐	☐	☐	☐	☐
	☐ Other(s) - Please indicate which one(s)							
12	In the case of implementing the <i>EC-FSDSA</i> cryptographic construction, please indicate its parameterization.							
		P-256	P-384	P-521	Brainpool P256r1	Brainpool P384r1	Brainpool P512r1	FRP256v1
	SHA2-256	☐	☐	☐	☐	☐	☐	☐
	SHA2-384	☐	☐	☐	☐	☐	☐	☐
	SHA2-512	☐	☐	☐	☐	☐	☐	☐
	SHA2-512 /256	☐	☐	☐	☐	☐	☐	☐
	SHA3-256	☐	☐	☐	☐	☐	☐	☐
	SHA3-384	☐	☐	☐	☐	☐	☐	☐
	SHA3-512	☐	☐	☐	☐	☐	☐	☐
	☐ Other(s) - Please indicate which one(s)							

Q-ID	DigitalSignature-VQ
13	In the case of implementing the <i>EdDSA</i> cryptographic construction, please indicate its parameterization.
	Ed25519 with SHA2-512 Ed448 with SHAKE256
	PureEdDSA ☐ Pre-Hash ☐
	☐ Other(s) - Please indicate which one(s)
15	In the case of implementing the <i>XMSS</i> cryptographic construction, please indicate its parameterization.
	☐ SHA2-256 ☐ SHA2-512 ☐ SHAKE128 ☐ SHAKE256
	☐ Other(s) - Please indicate which one(s)
16	In the case of implementing the <i>ML-DSA</i> cryptographic construction, please indicate its parameterization.
	☐ Supported Configuration(s) - Please indicate which one(s)
17	In the case of implementing the <i>Falcon</i> cryptographic construction, please indicate its parameterization.
	☐ Supported Configuration(s) - Please indicate which one(s)
18	In the case of implementing the <i>SLH-DSA</i> cryptographic construction, please indicate its parameterization.
	☐ Supported Configuration(s) - Please indicate which one(s)
23	Please provide a brief description of the purpose of each implemented <i>Digital Signature</i> cryptographic construction with its associated RSA modulus and scheme, finite field group, elliptic curve, hash primitive, etc. If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., Data sent through the communication channel is signed using ECDSA with P-256 curve with SHA-256 hash primitive)

Q-ID	DigitalSignature-VQ

3.4.3 KEY ESTABLISHMENT

Q-ID	KeyEstablishment-VQ
1	Does the TOE implement <i>Key Establishment</i> cryptographic constructions? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>Key Establishment</i> cryptographic constructions implemented in the TOE?
	☐ Diffie-Hellman (DH) ☐ DLIES-KEM
	☐ Elliptic Curve Diffie-Hellman (ECDH) ☐ ECIES-KEM
	☐ ML-KEM ☐ FrodoKEM
	☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>Diffie-Hellman (DH)</i> cryptographic construction, please indicate its parameterization.
	☐ Non-Ephemeral ☐ Ephemeral
	In case both apply, indicate which parameterization applies to each.
	☐ MODP-2048 bits ☐ MODP-3072 bits ☐ MODP-4096 bits
	☐ MODP-6144 bits ☐ MODP-8192 bits
	☐ FFDHE-2048 bits ☐ FFDHE-3072 bits ☐ FFDHE-4096 bits
	☐ FFDHE-6144 bits ☐ FFDHE-8192 bits
☐ Key Derivation Function - Please indicate which one(s) Please, complete the information according to those provided in Section 3.2.7 “Key Derivation Functions”	
☐ Other(s) Configuration(s) - Please indicate which one(s)	
4	In the case of implementing the <i>DLIES-KEM</i> cryptographic construction, please indicate its parameterization.

Q-ID	KeyEstablishment-VQ
	☐ Non-Ephemeral ☐ Ephemeral In case both apply, indicate which parameterization applies to each.
	☐ MODP-3072 bits ☐ MODP-4096 bits ☐ FFDHE-3072 bits ☐ FFDHE-4096 bits
	Key Derivation Function: ☐ HKDF with HMAC-SHA2-256
	☐ Other(s) Configuration(s) - Please indicate which one(s)
5	In the case of implementing the <i>Elliptic Curve Diffie-Hellman (EC-DH)</i> cryptographic construction, please indicate its parameterization.
	☐ Non-Ephemeral ☐ Ephemeral In case both apply, indicate which parameterization applies to each.
	☐ BrainpoolP256r1 ☐ BrainpoolP384r1 ☐ BrainpoolP512r1 ☐ NIST P-256 ☐ NIST P-384 ☐ NIST P-521 ☐ FRP256v1 ☐ Curve25519 (x25519) ☐ Curve448 (x448)
	☐ Key Derivation Function - Please indicate which one(s) Please, complete the information according to those provided in Section 3.2.7 "Key Derivation Functions"
	☐ Other(s) Configuration(s) - Please indicate which one(s)
6	In the case of implementing the <i>ECIES-KEM</i> cryptographic construction, please indicate its parameterization.
	☐ Non-Ephemeral ☐ Ephemeral In case both apply, indicate which parameterization applies to each.
	☐ BrainpoolP256r1 ☐ BrainpoolP384r1 ☐ BrainpoolP512r1 ☐ NIST P-256 ☐ NIST P-384 ☐ NIST P-521
	Key Derivation Function: ☐ HKDF with HMAC-SHA2-256

Q-ID	KeyEstablishment-VQ
	☐ Other(s) Configuration(s) - Please indicate which one(s)
7	In the case of implementing the <i>FrodoKEM</i> cryptographic construction, please indicate its parameterization.
	☐ Non-Ephemeral ☐ Ephemeral
	In case both apply, indicate which parameterization applies to each.
	☐ AES ☐ SHAKE128
	☐ FrodoKEM-640 ☐ FrodoKEM-976 ☐ FrodoKEM-1344
	☐ Other(s) Configuration(s) - Please indicate which one(s)
8	In the case of implementing the <i>ML-KEM</i> cryptographic construction, please indicate its parameterization.
	☐ Supported Configuration(s) - Please indicate which one(s)
13	Please provide a brief description of the purpose of each implemented <i>Key Establishment</i> cryptographic construction with its associated parameterization (finite field group, elliptic curve, etc.). If there is more than one implementation for the same construction, please provide the purpose of each of them (on different rows). (e.g., The TOE implements TLS 1.2 whose cipher suites rely on ECDHE with P-256 curve to perform key establishment)

3.5 RANDOM NUMBER GENERATORS

3.5.1 DETERMINISTIC RANDOM NUMBER GENERATOR CONSTRUCTION

10. **Note:** In case of multiple DRNG parameterizations and/or implementations, please complete the following tables for each of them, in order to clearly define them. Add as many tables as necessary.

Q-ID	DRNG-VQ
1	Does the TOE implement <i>DRNG</i> cryptographic constructions? Note: If the response is "No", the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>DRNG</i> cryptographic schemes implemented in the TOE?
	☐ HMAC-DRBG ☐ NR (Non-PredictionResistance and Non-Reseed) ☐ NPR (Non-PredictionResistance but with Reseed) ☐ PR (PredictionResistance and Reseed)
	☐ Hash-DRBG ☐ NR (Non-PredictionResistance and Non-Reseed) ☐ NPR (Non-PredictionResistance but with Reseed) ☐ PR (PredictionResistance and Reseed)
	☐ CTR-DRBG (AES) ☐ NR with DF (Non-PredictionResistance and Non-Reseed with Derivation Function) ☐ NR without DF (Non-PredictionResistance and Non-Reseed without Derivation Function) ☐ NPR with DF (Non-PredictionResistance with Reseed and Derivation Function) ☐ NPR without DF (Non-PredictionResistance with Reseed but without Derivation Function) ☐ PR with DF (PredictionResistance and Reseed with Derivation Function) ☐ PR without DF (PredictionResistance and Reseed but without Derivation Function)
	☐ Other(s) - Please indicate which one(s)

Q-ID	DRNG-VQ
7	Please provide a brief description of the purpose of the implemented <i>DRNG</i> cryptographic construction, indicating the SSPs that can be generated using it and the functionality class to which it belongs. (e.g., the HMAC-DRBG is used to generate the AES-256 bits key that is used by the TOE to encrypt the information entered through the data input interface)

3.5.2 DRNG INITIALIZATION

Q-ID	Initialization-VQ
1	A <i>DRNG</i> secure initialization depends on the number of bits of the Input (seed), Nonce, and Personalization String parameters. Note: Please indicate the length in bits of each of them during the DRNG initialization.
	The input (seed) length is: XXX bits
	The nonce length is: XXX bits
	The personalization string length is: XXX bits

3.5.3 DRNG RESEEDING CONFIGURATION

Q-ID	Reseeding-VQ
1	The <i>DRNG</i> reseeding depends on the number of bits used as Input Reseed and as Additional Input in every call to generate a new CSP. Note: Please indicate the length in bits of each of them during the reseeding.
	The input reseed length is: XXX bits
	The additional input length is: XXX bits

4 CRYPTOGRAPHIC PROTOCOLS IMPLEMENTATION

11. This section shall contain information related to the protocols implemented by the TOE which rely on cryptographic mechanisms. The proprietary and/or standard (e.g., TLS, SSH, etc.) protocols and their configuration shall be described justifying the ensured properties.
12. **Note:** This is the information that shall be included in each column:
- **Protocol:** The name of the implemented protocol.
 - **Configuration:** The cipher suites (for TLS) or cryptographic mechanisms configuration employed to implement the protocol.
 - **Properties:** The ensured properties with the protocol configuration. Some examples could be:
 - *Integrity protection of the exchanged messages*
 - *Anti-replay protections*
 - *Perfect forward secrecy*
 - *Post compromise secrecy*
 - *Quantum resistance*
 - **Justification:** Justification for each ensured property by the protocol configuration.
13. Please complete the following table with the protocols implemented by the TOE:

Protocol	Configuration	Properties	Justification

Table 1. Cryptographic Protocols Implementation and Configuration

4.1 TRANSPORT LAYER SECURITY PROTOCOL (TLS)

14. This subsection contains the questions associated with the TLS cryptographic protocol configurations implemented in the TOE. It aims to provide the tester with all the needed information to demonstrate that the implementation of the TLS cryptographic protocol complies with the requirements from Section 3 “CCN Agreed Cryptographic Mechanisms” of the [CCN-MEMeC] methodology.

4.1.1 TLS V1.3

Q-ID	TLS-VQ
1	Does the TOE implement <i>TLS v1.3</i>? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>TLS v1.3 Cipher Suites</i> implemented in the TOE?
	☐ TLS_AES_256_GCM_SHA384
	☐ TLS_AES_128_GCM_SHA256
	☐ TLS_AES_128_CCM_SHA256
	☐ TLS_CHACHA20_POLY1305_SHA256
	☐ Other(s) - Please indicate which one(s)
3	Please provide a brief description of the purpose of each <i>TLSv1.3</i> implementation with its associated cipher suites (on different rows). (e.g., The TOE implements TLSv1.3 with the cipher suite TLS_AES_256_GCM_SHA384 to establish secure channels with the server)

15. **Note:** Please complete the following table for each TLS v1.3 cipher suite implemented, where [ID] means the cipher suite name. Add as many tables as necessary.

Q-ID	TLSv1.3 CIPHER SUITE – [ID]
1	Please indicate the implemented <i>TLS v1.3 PSK</i> modes (if supported).
	☐ psk_ke ☐ psk_dhe_ke

Q-ID	TLSv1.3 CIPHER SUITE – [ID]
	☐ Other(s) - Please indicate which one(s)
2	In the case of implementing TLS v1.3 PSK modes, please provide evidence that the TOE does not allow the sending of zero Round-Trip Time data or 0-RTT data. (e.g., a pointer to the source code, a piece of source code, etc.)
3	Please indicate the implemented DH groups for TLS v1.3 Key Establishment. ☐ ffdhe2048 ☐ ffdhe3072 ☐ ffdhe4096 ☐ Other(s) - Please indicate which one(s)
4	Please indicate the implemented ECDH groups for TLS v1.3 Key Establishment. ☐ BrainpoolP256r1tls13 ☐ P-256 (secp256r1) ☐ BrainpoolP384r1tls13 ☐ P-384 (secp384r1) ☐ BrainpoolP512r1tls13 ☐ P-521 (secp521r1) ☐ Other(s) - Please indicate which one(s)
5	Please indicate the implemented xECDH groups for TLS v1.3 Key Establishment. ☐ x25519 ☐ x448
6	Please indicate the implemented TLS v1.3 Digital Signature Schemes to perform client-server digital signature. ☐ rsa_pss_rsae_sha256 ☐ rsa_pss_rsae_sha384 ☐ rsa_pss_rsae_sha512 ☐ rsa_pss_pss_sha256 ☐ rsa_pss_pss_sha384 ☐ rsa_pss_pss_sha512 ☐ ecdsa_brainpoolP256r1tls13_sha256 ☐ ecdsa_secp256r1_sha256 ☐ ecdsa_brainpoolP384r1tls13_sha384 ☐ ecdsa_secp384r1_sha384 ☐ ecdsa_brainpoolP512r1tls13_sha512 ☐ ecdsa_secp521r1_sha512 ☐ Ed25519 ☐ Ed448 ☐ Other(s) - Please indicate which one(s)

Q-ID	TLSv1.3 CIPHER SUITE – [ID]
7	Please indicate the implemented <i>TLS v1.3 Digital Signature Schemes</i> on certificates.
	☐ rsa_pkcs1_sha256 ☐ rsa_pkcs1_sha384
	☐ rsa_pkcs1_sha512 ☐ rsa_pss_rsae_sha256
	☐ rsa_pss_rsae_sha384 ☐ rsa_pss_rsae_sha512
	☐ rsa_pss_pss_sha256 ☐ rsa_pss_pss_sha384
	☐ rsa_pss_pss_sha512
	☐ ecdsa_brainpoolP256r1tls13_sha256 ☐ ecdsa_secp256r1_sha256
	☐ ecdsa_brainpoolP384r1tls13_sha384 ☐ ecdsa_secp384r1_sha384
	☐ ecdsa_brainpoolP512r1tls13_sha512 ☐ ecdsa_secp521r1_sha512
	☐ Ed25519 ☐ Ed448
☐ Other(s) - Please indicate which one(s)	

4.1.2 TLS V1.2

Q-ID	TLS-VQ
1	Does the TOE implement <i>TLS v1.2</i>? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	What are the <i>TLS v1.2 Cipher Suites</i> implemented in the TOE?
	☐ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	☐ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	☐ TLS_ECDHE_ECDSA_WITH_AES_256_CCM
	☐ TLS_ECDHE_ECDSA_WITH_AES_128_CCM
	☐ TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
	☐ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Q-ID	TLS-VQ
	☐ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ☐ TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ☐ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ☐ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ☐ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ☐ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ☐ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ☐ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ☐ TLS_DHE_RSA_WITH_AES_256_CCM ☐ TLS_DHE_RSA_WITH_AES_128_CCM ☐ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 ☐ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 ☐ TLS_RSA_WITH_AES_256_GCM_SHA384 ☐ TLS_RSA_WITH_AES_128_GCM_SHA256 ☐ TLS_RSA_WITH_AES_256_CCM ☐ TLS_RSA_WITH_AES_128_CCM ☐ TLS_RSA_WITH_AES_256_CBC_SHA256 ☐ TLS_RSA_WITH_AES_128_CBC_SHA256 ☐ TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ☐ TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 ☐ TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 ☐ TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 ☐ TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 ☐ TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256

Q-ID	TLS-VQ
	☐ TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 ☐ TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256 ☐ TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256 ☐ TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 ☐ TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 ☐ TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 ☐ TLS_DHE_PSK_WITH_AES_256_GCM_SHA384 ☐ TLS_DHE_PSK_WITH_AES_128_CCM ☐ TLS_DHE_PSK_WITH_AES_256_CCM ☐ Other(s) - Please indicate which one(s)
3	In the case of implementing a TLS cipher suite whose encryption mechanisms are based on CBC, please provide evidence that they are used in conjunction with the “<i>encrypt_then_mac</i>” extension. (e.g., a pointer to the source code, a piece of source code, etc.)
4	Please provide a brief description of the purpose of each <i>TLSv1.2</i> implementation with its associated cipher suites (on different rows). (e.g., The TOE implements <i>TLSv1.2</i> with the cipher suite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 to establish secure channels with the server)

16. **Note:** Please complete the following table for each TLS v1.2 cipher suite implemented, where [ID] means the cipher suite name. Add as many tables as necessary.

Q-ID	TLSv1.2 CIPHER SUITE – [ID]
1	Please indicate the implemented DH groups for <i>TLS v1.2 Key Establishment</i>. ☐ ffdhe2048 ☐ ffdhe3072 ☐ ffdhe4096

Q-ID	TLSv1.2 CIPHER SUITE – [ID]			
	☐ Other(s) - Please indicate which one(s)			
2	Please indicate the implemented ECDH groups for TLS v1.2 Key Establishment.			
	☐ BrainpoolP256r1tls13	☐ P-256 (secp256r1)		
	☐ BrainpoolP384r1tls13	☐ P-384 (secp384r1)		
	☐ BrainpoolP512r1tls13	☐ P-521 (secp521r1)		
	☐ Other(s) - Please indicate which one(s)			
3	Please indicate the implemented xECDH groups for TLS v1.2 Key Establishment.			
	☐ x25519	☐ x448		
4	Please indicate the implemented TLS v1.2 Digital Signature Schemes and Hash Functions.			
		RSA	DSA	ECDSA
	SHA2-256	☐	☐	☐
	SHA2-384	☐	☐	☐
	SHA2-512	☐	☐	☐
	☐ Ed25519 ☐ Ed448			
☐ Other(s) - Please indicate which one(s)				

4.2 SECURE SHELL (SSH)

17. This subsection contains the questions associated with the SSH cryptographic protocol configurations implemented in the TOE. It aims to provide the tester with all the needed information to demonstrate that the implementation of the SSH cryptographic protocol complies with the requirements from Section 3 “CCN Agreed Cryptographic Mechanisms” of the [CCN-MEMeC] methodology.
18. **Note:** In case of multiple SSH implementations, please complete the following table for each of them, in order to clearly define them. Add as many tables as necessary.

Q-ID	SSH-VQ
1	Does the TOE implement SSH-2 protocol? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	Please indicate the implemented DH groups for SSH-2 Key Establishment.
	☐ DH-exchange-SHA256 ☐ DH-group15-SHA512
	☐ DH-group16-SHA512 ☐ DH- group17-SHA512
	☐ DH- group18-SHA512
	☐ Other(s) - Please indicate which one(s)
3	In the case of implementing the <i>Diffie-Hellman-group-exchange-SHA256</i> for SSH-2 Key Establishment, please provide the following information:
	The prime p and its length in bits: XXX
	The generator g : XXX
	The prime p and its length in bits: XXX
4	Please indicate the implemented ECDH groups for SSH-2 Key Establishment.
	☐ secp256r1_sha512 ☐ secp384r1_sha512
	☐ secp521r1_sha512
	☐ Other(s) - Please indicate which one(s)
5	Please indicate the implemented SSH-2 Encryption Mechanisms.
	☐ AEAD_AES_128_GCM ☒ AEAD_AES_256_GCM

Q-ID	SSH-VQ
	☐ AES128-CTR ☐ AES192-CTR ☐ AES256-CTR ☐ Other(s) - Please indicate which one(s)
6	Please indicate the implemented SSH-2 Integrity and Authenticity Mechanisms. ☐ HMAC-SHA1 ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-512 ☐ AEAD_AES_128_GCM ☐ AEAD_AES_256_GCM ☐ Other(s) - Please indicate which one(s)
7	Please indicate the implemented SSH-2 Server-Client Authentication Mechanisms. ☐ ECDSA-SHA2-secp256r1 ☐ ECDSA-SHA2-secp384r1 ☐ ECDSA-SHA2-secp521r1 ☐ x509v3-ECDSA-SHA2-secp256r1 ☐ x509v3-ECDSA-SHA2-secp384r1 ☐ x509v3-ECDSA-SHA2-secp521r1 ☐ Other(s) - Please indicate which one(s)
9	Please provide a brief description of the purpose of the SSH-2 implementation with its associated configurations. (e.g., The TOE implements SSH-2 to allow remote access to users)

4.3 INTERNET PROTOCOL SECURITY (IPSEC) WITH IKEV2

19. This subsection contains the questions associated with the IPsec cryptographic protocol configurations implemented in the TOE. It aims to provide the tester with all the needed information to demonstrate that the implementation of the IPsec cryptographic protocol complies with the requirements from Section 3 “CCN Agreed Cryptographic Mechanisms” of the [CCN-MEMeC] methodology.
20. **Note:** In case of multiple IPsec implementations, please complete the following table for each of them, in order to clearly define them. Add as many tables as necessary.

Q-ID	IPsec-VQ
1	Does the TOE implement <i>IPsec</i> protocol with <i>IKEv2</i>? Note: If the response is “No”, the following questions in this table shall not be answered.
	☐ Yes ☐ No
2	Please indicate the implemented <i>Protocol Versions</i>.
	☐ IPsec ☐ IKEv2 ☐ ESP
4	Please indicate the implemented DH groups implemented for the <i>IKEv2 Key Establishment</i>.
	☐ 3072-bit MODP ☐ 4096-bit MODP ☐ 6144-bit MODP ☐ 8192-bit MODP ☐ Other(s) - Please indicate which one(s)
5	Please indicate the implemented ECDH groups implemented for the <i>IKEv2 Key Establishment</i>.
	☐ 256-bit random ECP ☐ 384-bit random ECP ☐ 521-bit random ECP ☐ brainpoolP256r1 ☐ brainpoolP384r1 ☐ brainpoolP512r1 ☐ Other(s) - Please indicate which one(s)
6	Please indicate the implemented xECDH groups implemented for the <i>IKEv2 Key Establishment</i>.
	☐ x25519 ☐ x448

Q-ID	IPsec-VQ
	☐ Other(s) - Please indicate which one(s)
7	Please indicate the implemented IKEv2 and ESP Encryption Mechanisms.
8	Please indicate the implemented IKEv2 and ESP Origin Integrity and Authenticity Mechanisms. ☐ HMAC-SHA2-256_128 ☐ HMAC-SHA2-384_192 ☐ HMAC-SHA2-512_256 ☐ AES-CMAC-96 ☐ AES-GMAC ☐ Other(s) - Please indicate which one(s)
9	Please indicate the implemented IKEv2 Pseudo-Random Functions. ☐ HMAC-SHA2-256 ☐ HMAC-SHA2-384 ☐ HMAC-SHA2-512 ☐ AES128-CMAC ☐ Other(s) - Please indicate which one(s)
10	Please indicate the implemented IKEv2 Authentication Mechanisms. ☐ RSA (RSASSA-PSS) with SHA-256 ☐ RSA (RSASSA-PSS) with SHA-384 ☐ RSA (RSASSA-PSS) with SHA-512 ☐ ECDSA-SHA-256 and P-256 ☐ ECDSA-SHA-384 and P-384 ☐ ECDSA-SHA-512 and P-521 ☐ ECDSA-256-BrainpoolP256r1 ☐ ECDSA-384-BrainpoolP384r1 ☐ ECDSA-512-BrainpoolP512r1 ☐ ECGDSA-256-BrainpoolP256r1 ☐ ECGDSA-384-BrainpoolP384r1 ☐ ECGDSA-512-BrainpoolP512r1 ☐ Other(s) - Please indicate which one(s)
11	Please provide a brief description of the purpose of each IPsec implementation with its associated configurations. (e.g., The TOE implements IPsec to establish secure channels over a VPN)

5 REFERENCES

- [CCN-MEMeC]** CCN Cryptographic Mechanisms Evaluation Methodology v1.3.3. November 2024
- [SP800-38D]** NIST. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology, Special Publication SP800-38D, November 2007.

6 ACRONYMS

AE	Authenticated Encryption
CCN	Centro Criptológico Nacional
CL1	Certification Level 1
CL2	Certification Level 2
CL3	Certification Level 3
DRBG	Deterministic Random Bit Generator
ECDLOG	Discrete Logarithm in Elliptic Curves
FFDLOG	Discrete Logarithm in Finite Fields
IPsec	Internet Protocol security
KDF	Key Derivation Function
MAC	Message Authentication Code
RNG	Random Number Generator
SSH	Secure Shell
TLS	Transport Layer Security Protocol
TOE	Target Of Evaluation
VQ	Vendor Questionnaire
XOF	Extendable-Output Function

