
jtsec
BEYOND IT SECURITY
Evolution of cryptographic evaluation in Europe

José Ruiz Gualda

jtsec Beyond IT Security

jruiz@jtsec.es

- Computer Engineer (University of Granada)
- Expert in Common Criteria, LINCE and FIPS 140-2 & FIPS 140-3
- Member of the SCCG (Stakeholder Cybersecurity Certification Group) at the European Commission.
- Secretary of SC3 at CTN320
- Editor of LINCE as UNE standard
- Editor in JTC13 WG3 of the FITCEM Methodology
- European Commission reviewer for the ERNCIP group "IACS Cybersecurity Certification".

INDEX

INDEX

History of the Cryptographic Evaluation

USA

NIST (National Institute of Standards and Technology) → Verification of Conformity according to FIPS 140-1, FIPS 140-2 and FIPS 140-3 → CMVP - Designed for certifying cryptographic modules

CAVP - Designed to certify cryptographic algorithms → Publication of multiple "Special Publications" specifying cryptographic algorithms and how to test them

ACVP

History of the Cryptographic Evaluation

International

Previously

Withdrawn
ISO/IEC 19790:2006

Withdrawn
ISO/IEC 19790:2006/Cor 1:2008

Now

Published
ISO/IEC 19790:2012

A standard is reviewed every 5 years
Stage: **90.92** (To be revised)

Will be replaced by

Under development
ISO/IEC WD 19790.3

Corrigenda / Amendments

Withdrawn
ISO/IEC 19790:2012/Cor 1:2015

History of the Cryptographic Evaluation

Spain

Certification Body for cryptographic modules - OC-CCN (Spanish National Cryptologic Centre)

ISO

- ISO/IEC 19790, Security Requirements for Cryptographic Modules
- ISO/IEC 24759, Test Requirements for Cryptographic Modules

Organismo de Certificación | Centro Criptológico Nacional

Buscar... B

OC-CCN

SOBRE OC PRODUCTOS CERTIFICADOS CATÁLOGO PRODUCTOS STIC TIPOS DE CERTIFICACIÓN SOLICITUDES Y FORMULARIOS

CRITERIOS Y METODOLOGÍAS

Criterios y metodologías de evaluación, en las versiones en uso por el Organismo de Certificación:

Common Criteria

- CC/CEM v3.1 release 5 (última versión en vigor)
  - Common Criteria Parte 1: Introduction and general model (1.27 MB)
  - Common Criteria Parte 2: Security functional requirements (2.83 MB)
  - Common Criteria Parte 3: Security assurance requirements (2.87 MB)
  - CEM: Common Evaluation Methodology (2.98 MB)
- CC/CEM v3.1 release 4
  - Common Criteria, parte 1 EDICIÓN 4 (597 KB)
  - Common Criteria, parte 2 EDICIÓN 4 (991 KB)
  - Common Criteria, parte 3 EDICIÓN 4 (1010 KB)
  - Common Evaluation Methodology EDICIÓN 4 (1.27 MB)

LINCE - Certificación Nacional Esencial de Seguridad

- Certificación Nacional Esencial de Seguridad (LINCE) versión 2.0
  - CCN-STIC-2001 Definición LINCE (1.07 MB)
  - CCN-STIC-2002 Metodología de Evaluación para la Certificación Nacional (1.10 MB)
  - CCN-STIC-2003 Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE) (978 KB)
  - CCN-STIC-2004 Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE) (1022 KB)
- Certificación Nacional Esencial de Seguridad (LINCE) versión 0.1
  - CCN-STIC-2001 Definición LINCE (929 KB)
  - CCN-STIC-2002 Metodología de Evaluación para la Certificación Nacional (1.24 MB)
  - CCN-STIC-2003 Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE) (903 KB)
  - CCN-STIC-2004 Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE) (1.06 MB)

La metodología LINCE está orientada a la evaluación y certificación de productos de seguridad TIC para su inclusión en el catálogo CPSTIC cómo producto cualificado para sistemas afectados por el ENS con categoría media o básica y también se puede emplear para la realización de Evaluaciones STIC complementarias conforme a lo especificado en las guías CCN-STIC-106 y CCN-STIC-140.

ITSEC/ITSEM

- ITSEC v1.2, junio 1991 (341 KB)
- ITSEM v1.0, septiembre 1993 (1.74 MB)

ISO

- ISO/IEC 19790, Security Requirements for Cryptographic Modules
- ISO/IEC 24759, Test Requirements for Cryptographic Modules

INDEX

Cryptographic Evaluation Today

Europe

- SOG-IS Crypto Evaluation Scheme Harmonised Cryptographic Evaluation Procedures v0.16 (December 2020)
- First SOG-IS evaluation methodology
  - Implementation of cryptographic mechanisms
  - Pitfalls Prevention Requirements

SOG-IS HEP

- SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.2 (January 2020)
  - Cryptographic mechanisms agreed and recommended by SOG-IS
    - Acceptable level of security
    - Implementation guidelines

SOG-IS ACM

Cryptographic Evaluation Today

Spain

CCN-STIC 130 Guide
Cryptologic Evaluation (DL) Requirements Guide (October 2017)

- Requirements for Approval of Encryption Products to Handle Classified National Information
- Full Product Evaluation Methodology
- Security Requirements Specification

CCN-STIC 130 Guide

MEC – LINCE
Cryptographic evaluation module within the LINCE methodology
Very light cryptographic conformance testing following the NIAP Protection Profiles approach
Botan-CCN Cryptographic Library

- CCN Reference implementation for cryptographic evaluations

Botan-CCN Cryptographic Library
Reference implementation for cryptographic evaluations of the CCN

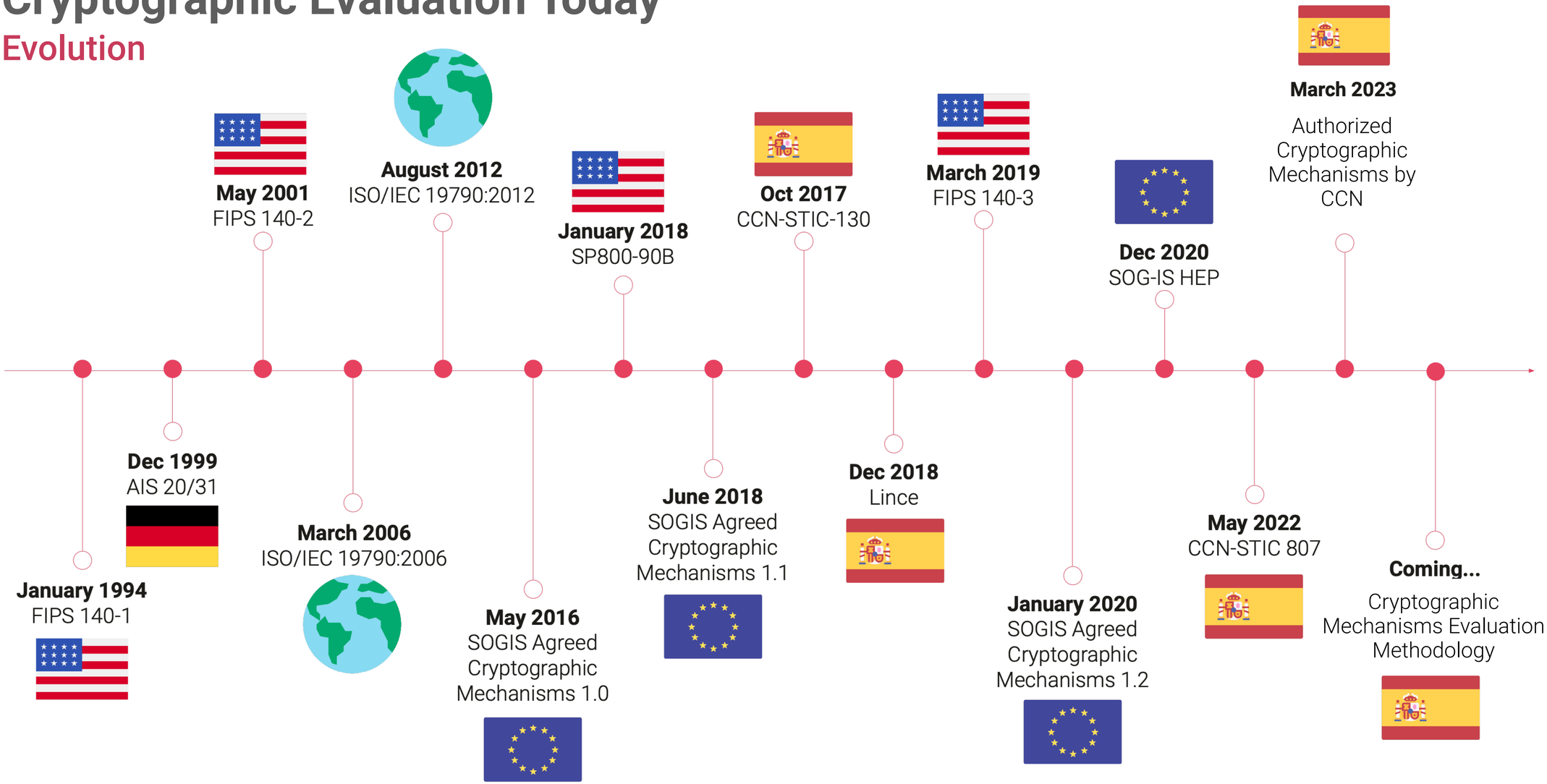
Cryptographic Evaluation Today

Spain

CCN-STIC 221 Guide
Cryptographic Mechanisms authorized by CCN
Includes new CCN-authorized algorithms with respect to the European ACM
Transversal use guide not limited to ENS

Cryptographic Evaluation Today

Evolution



Cryptographic Evaluation Today

Is it only a Spanish issue? | Reasons why the cryptographic methodology is necessary

FIPS and/or ISO FIPS:

- It only works when the module has been created to meet FIPS requirements.
- It works well for crypto modules but not for products integrating crypto
- Neither security-relevant implementation pitfalls nor limit values are checked.

STIC 130

- Does not include algorithm-level conformity and includes product implementation requirements.
- Not 100% focused on cryptographic mechanisms.
- Provides the security point of view.

We do not have a methodology that evaluates cryptographic mechanisms (algorithms and protocols.)

STIC 130

INDEX

Usage

CCN Cryptographic Mechanisms Evaluation Methodology

- Products whose main functionality requires cryptography (e.g., VPNs, ciphers, secure communications, etc.)
- During CC, LINCE and Complementary STIC certification processes.

Definition

Cryptographic Mechanisms Evaluation Methodology

DRAFT

Document Structure

- Cryptographic Requirements
- Approved Cryptographic Mechanisms
- Conformity Testing
- Common Implementation Pitfalls

Cryptographic Mechanisms Evaluation Methodology

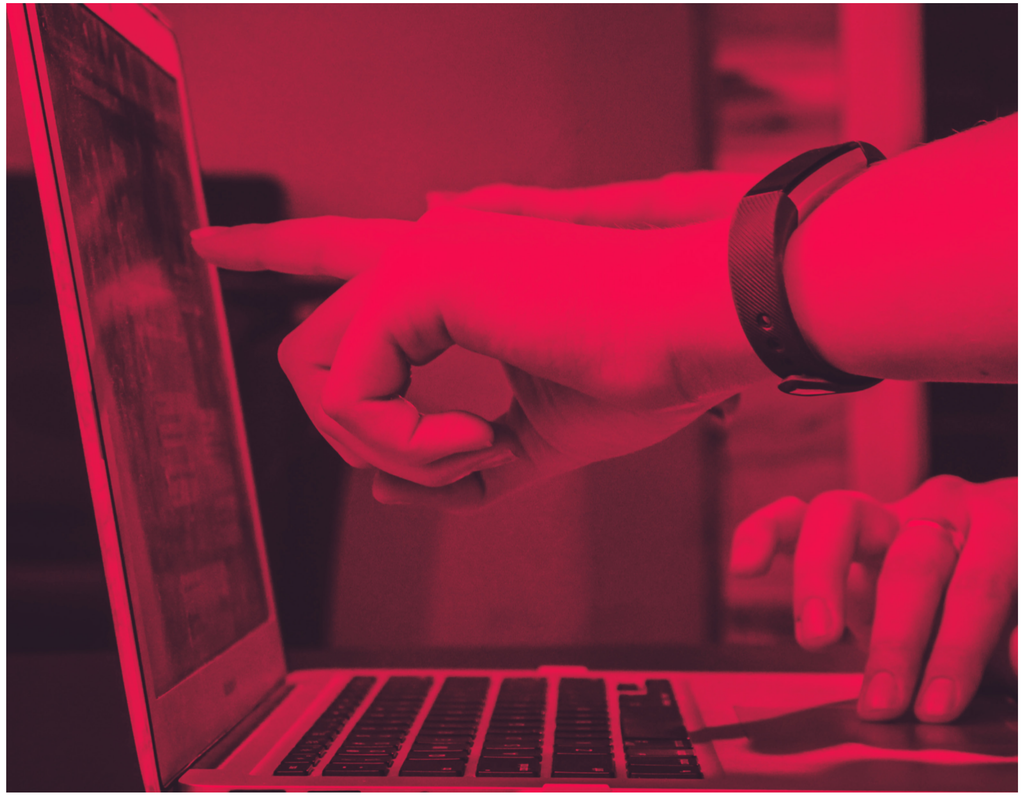
Structure

1. **Cryptographic Requirements**

Objective: To specify the requirements extracted by CCN from the CCN-STIC 130 guide that apply to cryptographic mechanisms and primitives implemented in relation to:

- Self-tests (not required by SOGIS)
- Critical Security Parameters (CSP) Management (not required by SOGIS)

Evaluation: The evaluator shall verify that the TOE complies with the cryptographic requirements listed in this section.



Cryptographic Mechanisms Evaluation Methodology

1. Cryptographic Requirements - Critical Security Parameters (CSP) Management

The methodology not only evaluates the SOGIS related Key Management requirements, but also assesses the entire life cycle of every SSP managed by the TOE.

This comprehensive approach ensures a thorough evaluation of the security posture of the TOE beyond just key management.

Example: SSP Life Cycle Management for AES_EDK

SSP	Strength (in bits)	Generation Method	Entry/Output	Storage	Applications or cryptographic operation	Zeroization	Evidence of zeroization and justification
AES_EDK	128, 256	DRBG (Hash_DRBG)	N/A	AES-256-KeyWrap	Encryption/decryption with: AES-CBC AES-CTR	Overwritten using zeros.	Include piece of source code and justification.

Table extracted from the Vendor Questionnaire document.

Cryptographic Mechanisms Evaluation Methodology

Structure

2. Approved Cryptographic Mechanisms

Objective: To specify the cryptographic mechanisms recognized and agreed by the SOG-IS Cryptographic Evaluation Scheme participants.

The Vendor Questionnaire (VQ) document is used to gather information related to the cryptographic mechanisms implemented by the vendor in order to comply with the Methodology. This document includes guided questions for the vendor about cryptographic mechanisms, CSP and sensitive data management to ensure all necessary information is included and evaluation efforts are reduced.

Evaluation: The evaluator shall verify that the cryptographic mechanisms included in the VQ are implemented by the TOE and comply with the guidelines presented by the SOG-IS in the SOG-IS ACM

Q-ID	[CCNCRYPTOGRAPHICREQUIREMENTS-BLOCKCIPHER]
1	***¿Does the TOE implement Block Cipher cryptographic primitive?*** ☐ Yes ☐ No **Note:** If the response is "No", then, the following questions in this table shall not be answered.
2	***What is the Block Cipher cryptographic primitive implemented in the TOE?*** ☐ AES-128 ☐ AES-192 ☐ AES-256 ☐Others (Indicate here)
3	***Does the TOE implement a KAT for each implemented key length?*** ***In affirmative case, please, describe how it is implemented and provide evidence of the implementation for each key length (e.g. pointer to the source code, piece of source code, etc).***
4	***Does the TOE implement a KAT for each direction (ciphering and deciphering)?*** ***In affirmative case, please, describe how it is implemented and provide evidence of the implementation for ciphering and deciphering operations (e.g. pointer to the source code, piece of source code, etc).***

Table extracted from the Vendor Questionnaire document.

Cryptographic Mechanisms Evaluation Methodology

Structure

3. Conformance Testing

Objective: To specify the requirements necessary to perform conformity testing of the cryptographic primitives and mechanisms implemented by the TOE. These tests shall determine whether the cryptographic primitives and mechanisms used by the TOE are correctly implemented. This is similar to what NIST does but also verifying parameterizations and limit values that often lead to errors.

Evaluation: The evaluation process is divided into four steps:

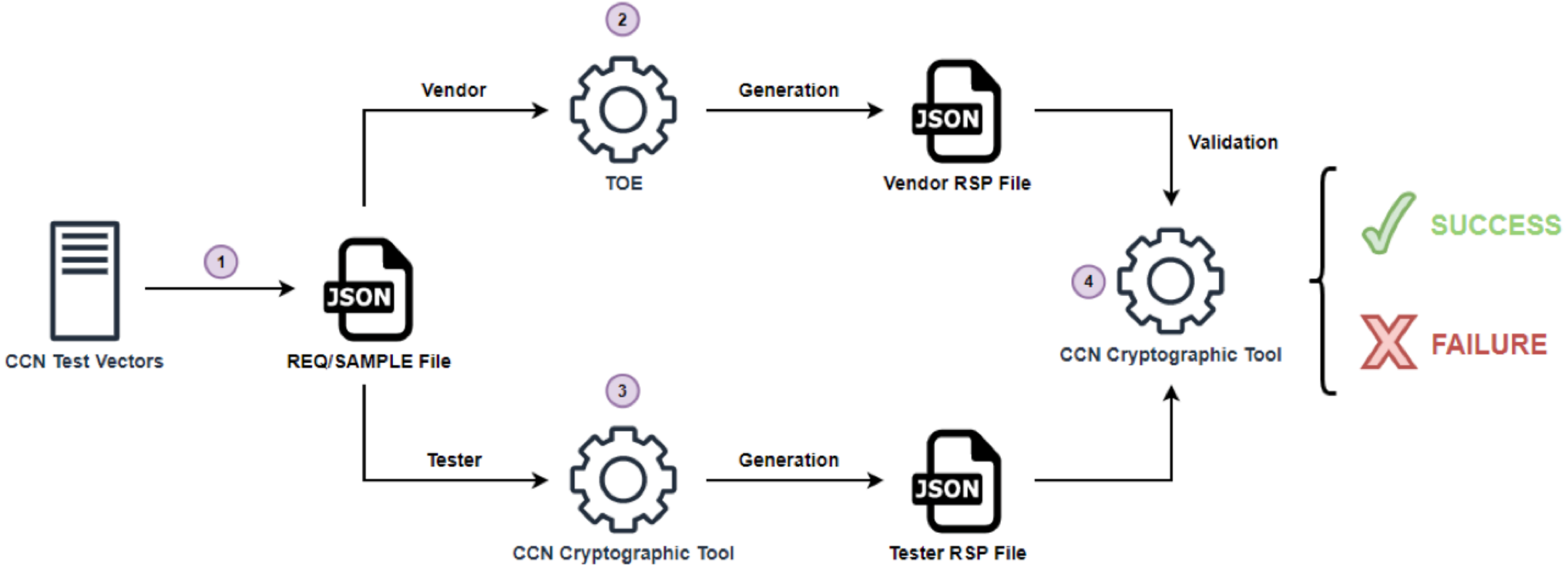
1. Generation of Test Vectors: Request and Sample files.
2. Generation of Results by the Vendor: Response File
3. Generation of Results by the Evaluator: Response File
4. Validation of Results by the Evaluator

centro criptológico nacional

CCN-STIC 221 Guide

Cryptographic Mechanisms Evaluation Methodology

Conformance Testing Evaluation Process Diagram



Cryptographic Mechanisms Evaluation Methodology

Test Vectors Generation

- The evaluator shall generate a 'REQUEST' file (in JSON format) for each cryptographic mechanism implemented by the TOE containing the test vectors associated to the supported parameterization.

- Additionally, the evaluator shall generate the 'SAMPLE' file (in JSON format) for each cryptographic mechanism implemented by the TOE containing an example solution to indicate the format of the expected result.

The evaluator shall send to the vendor a file package containing the 'REQUEST' and 'SAMPLE' files associated to all cryptographic mechanisms implemented by the TOE.

Cryptographic Mechanisms Evaluation Methodology

Generation of Results by the Vendor

- The vendor shall generate a 'RESPONSE' file associated with each cryptographic mechanism implemented, containing the output provided by the TOE for each of the test vectors provided in the 'REQUEST' file.
- The vendor shall retain the JSON format presented in the 'REQUEST' and 'SAMPLE' files for the generation of the 'RESPONSE' file.

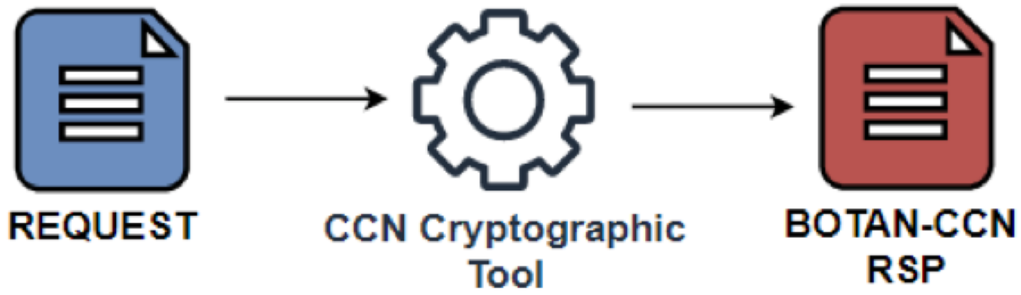
The vendor shall send to the evaluator a file package containing the 'RESPONSE' files associated with all cryptographic mechanisms implemented by the TOE.

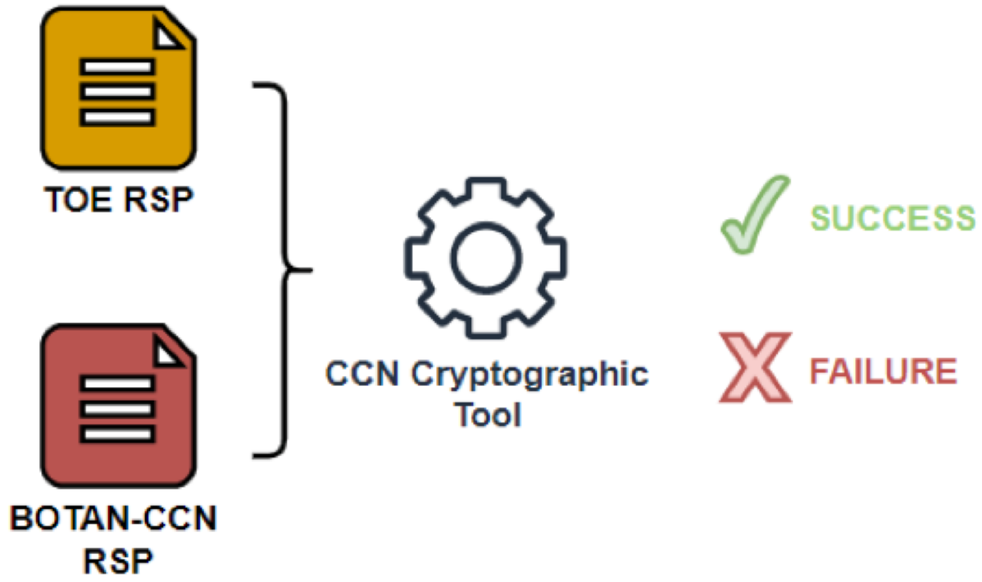
Cryptographic Mechanisms Evaluation Methodology

Generation of Results by the Evaluator

The evaluator shall generate the 'RESPONSE' file associated to each cryptographic mechanism implemented by the TOE, using the Botan-CCN library as reference cryptographic implementation.

The evaluator shall retain the JSON format presented in the 'REQUEST' and 'SAMPLE' files for the generation of the 'RESPONSE' file.





Cryptographic Mechanisms Evaluation Methodology

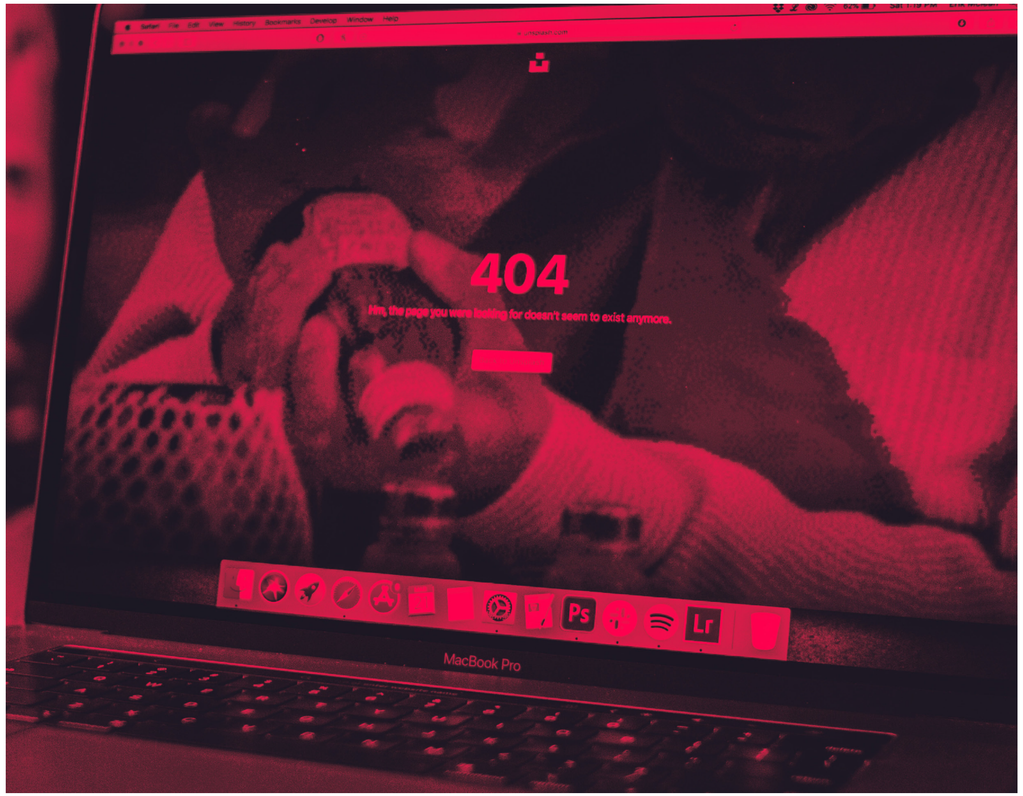
Validation of Results by the Evaluator

The evaluator shall validate the 'RESPONSE' files provided by the vendor for each cryptographic mechanism implemented by the TOE, comparing the results provided with those obtained in the previous step using the Botan-CCN cryptographic library.

The evaluator shall determine whether the TOE correctly implements the cryptographic mechanisms and primitives used and declared.

Cryptographic Mechanisms Evaluation Methodology

Structure



4. Common Implementation Pitfalls

Objective: To specify the requirements necessary to avoid implementation pitfalls in the cryptographic primitives and mechanisms implemented by the TOE.

Evaluation: The evaluator shall verify that the cryptographic mechanisms implemented by the TOE comply with the implementation pitfall avoidance guidelines presented by the SOG-IS in the SOG-IS Harmonized Cryptographic Evaluation Procedures guide.

Cryptographic Mechanisms Evaluation Methodology

Common Implementation Pitfalls - Example: GCM Implementation Pitfall

[IMPLEMENTATIONPITFALL-GCM-1]: The tester shall perform the following evaluation tasks:

- Verifying that no message of length strictly greater tan 2^{32} - 2 blocks can be encrypted.

Analysis: The counters are generated with the concatenation of a unique IV of 96 bits and an incremented counter denoted on 32 bits. This task avoids the overflow of the counter.

Cryptographic Mechanisms Evaluation Methodology

Advantages of the Cryptographic Evaluation | Methodology over SOG-IS

Cryptographic Mechanisms Evaluation Methodology

- **Complete evaluation methodology.** It establishes concrete evaluation tasks to be followed by the evaluator for each cryptographic mechanism to assess:
    - The CCN-STIC 130 implementation requirements
    - Usage of approved mechanisms
    - Conformity Testing
    - Common implementation pitfalls avoidance.
- **Self-tests.** The TOE is required to perform power-up and conditional self-tests. Several evaluation tasks are designed to evaluate their implementation and correct operation.

SOG-IS HEP and ACM

- List cryptographic requirements and agreed mechanisms and evaluation tasks **only** for conformity testing and for implementation pitfalls avoidance.
- Self-tests requirements are not specified.

SOGIS

Senior Officials Group
Information Systems Security

Cryptographic Mechanisms Evaluation Methodology

Advantages of the Cryptographic Evaluation | Methodology over SOG-IS

Cryptographic Mechanisms Evaluation Methodology

- **Life cycle management of each SSP managed by the TOE.** For each SSP, its strength, generation, entry/output, storage and zeroization methods are evaluated.
- **Complete list of conformity test vectors for all the agreed cryptographic mechanisms.** Example: AES Key Wrapping.

SOG-IS HEP and ACM

- Establishes general Key Management requirements, specifying only the recommended mechanism for each stage.
- The conformity test vectors of several algorithms are not defined or are not complete.

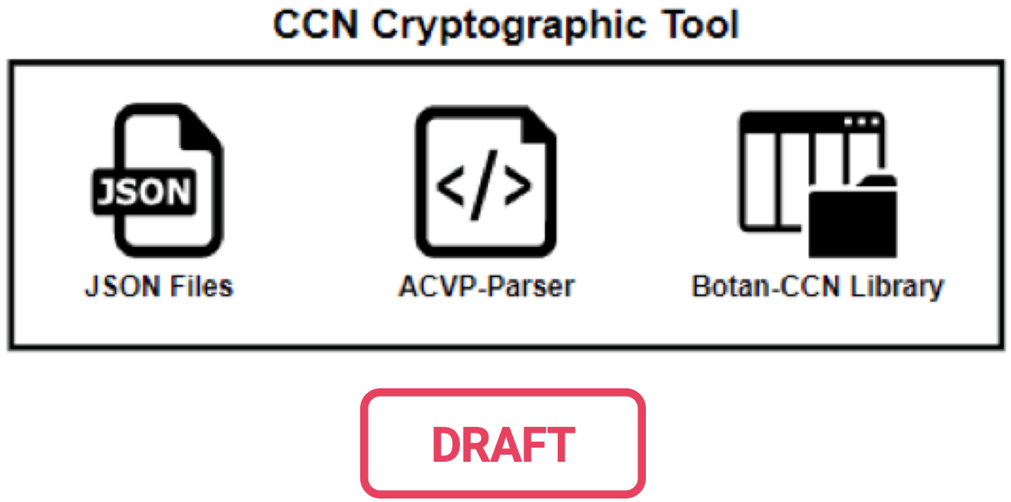
INDEX

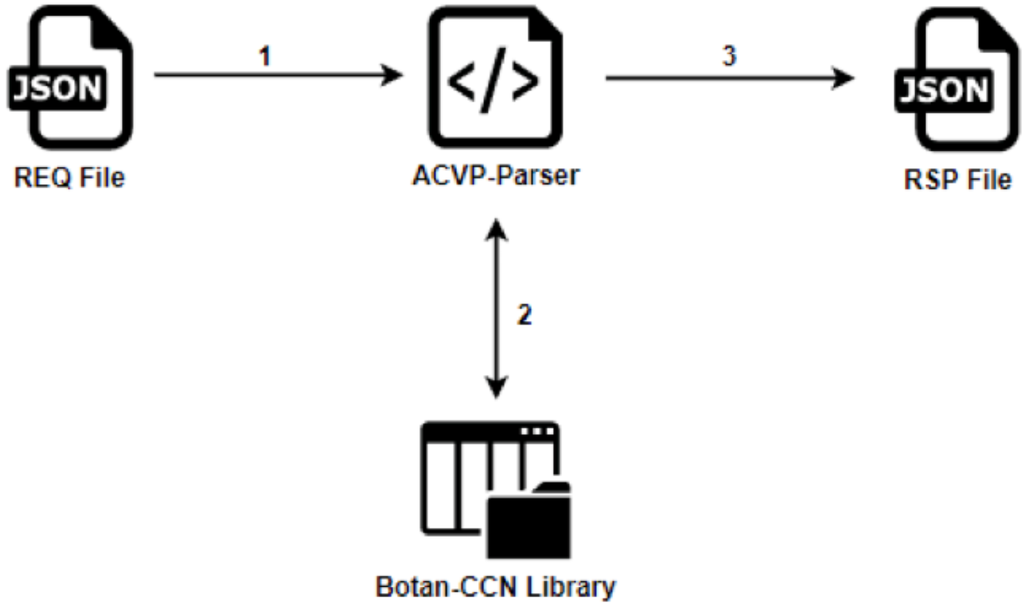
CCN Cryptographic Evaluation Tool

Definition

Performing Conformity Testing
Structure of the Tool

- JSON test files: test vectors in hexadecimal format according to SOG-IS methodology.
- ACVP-Parser: JSON file processing and extraction of parameters needed to invoke the cryptographic reference implementation.
- Botan-CCN Cryptographic Library: cryptographic reference implementation used to generate test vectors results and validate the correct cryptographic implementation of the TOE.





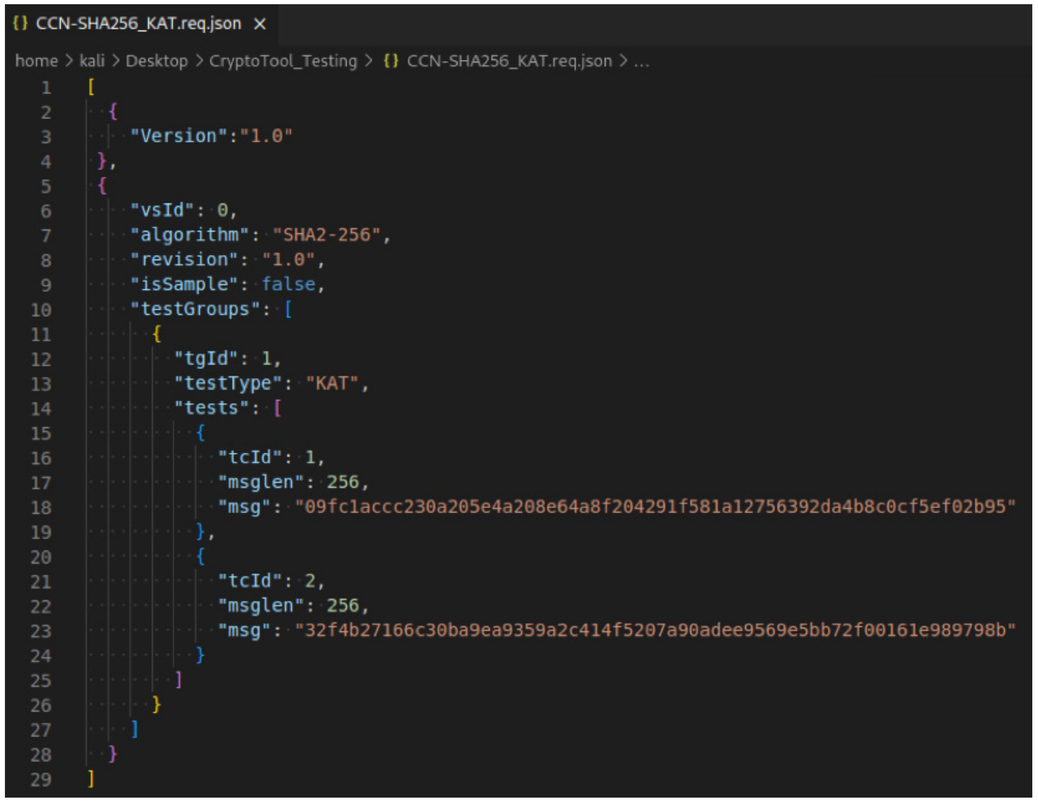
CCN Cryptographic Evaluation Tool

Flowchart

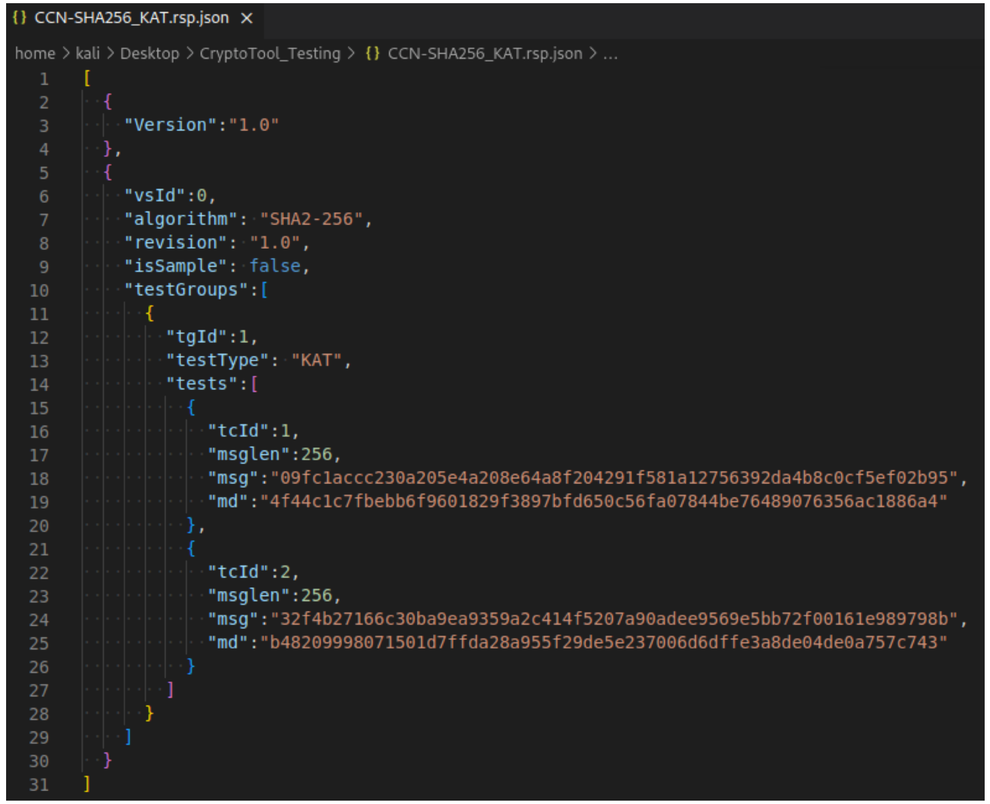
1. Processing of the test vectors to extract the parameters using the ACVP-Parser.
2. Invocation of the Botan-CCN cryptographic library to perform the generation of test vector results using the associated 'REQUEST' file.
3. Generation of the 'RESPONSE' file associated to a cryptographic mechanism using the associated 'REQUEST' file and the results obtained using the Botan-CCN cryptographic library.

Cryptographic Mechanisms Evaluation Methodology

Cryptographic Evaluation Tool - Usage Example: SHA-256



‘REQUEST’ file



‘RESPONSE' file generated by the Tool

Cryptographic Mechanisms Evaluation Methodology

Cryptographic Evaluation Tool - Usage Example: SHA-256

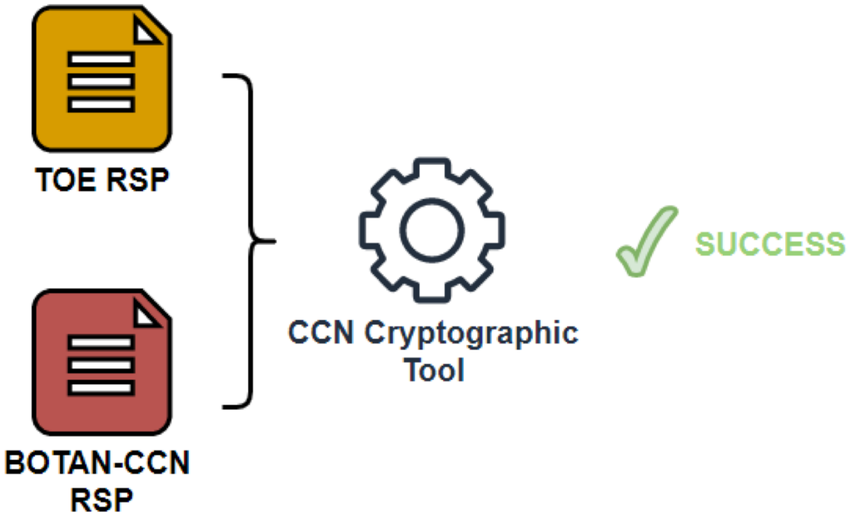
Vendor_CCN-SHA256_KAT.rsp.json


```
{} Vendor_CCN-SHA256_KAT.rsp.json > {} 1 > [ ] testGroups > {} 0 > [ ] tests > {} 1 > md
[
  {
    "Version":"1.0"
  },
  {
    "vsId":0,
    "algorithm": "SHA2-256",
    "revision": "1.0",
    "isSample": false,
    "testGroups":[
      {
        "tgId":1,
        "testType": "KAT",
        "tests":[
          {
            "tcId":1,
            "msglen":256,
            "msg":"09fc1accc230a205e4a208e64a8f204291f581a12756392da4b8c0cf5ef02b95",
            "md":"4f44c1c7fbebb6f9601829f3897bfd650c56fa07844be76489076356ac1886a4"
          },
                                                    PASS
          {
            "tcId":2,
            "msglen":256,
            "msg":"32f4b27166c30ba9ea9359a2c414f5207a90adee9569e5bb72f00161e989798b",
            "md":"b48209998071501d7ffda28a955f29de5e237006d6dffe3a8de04de0a757c743"
          }
                                                    PASS
        ]
      }
    ]
  }
]
```


‘RESPONSE' file generated by TOE

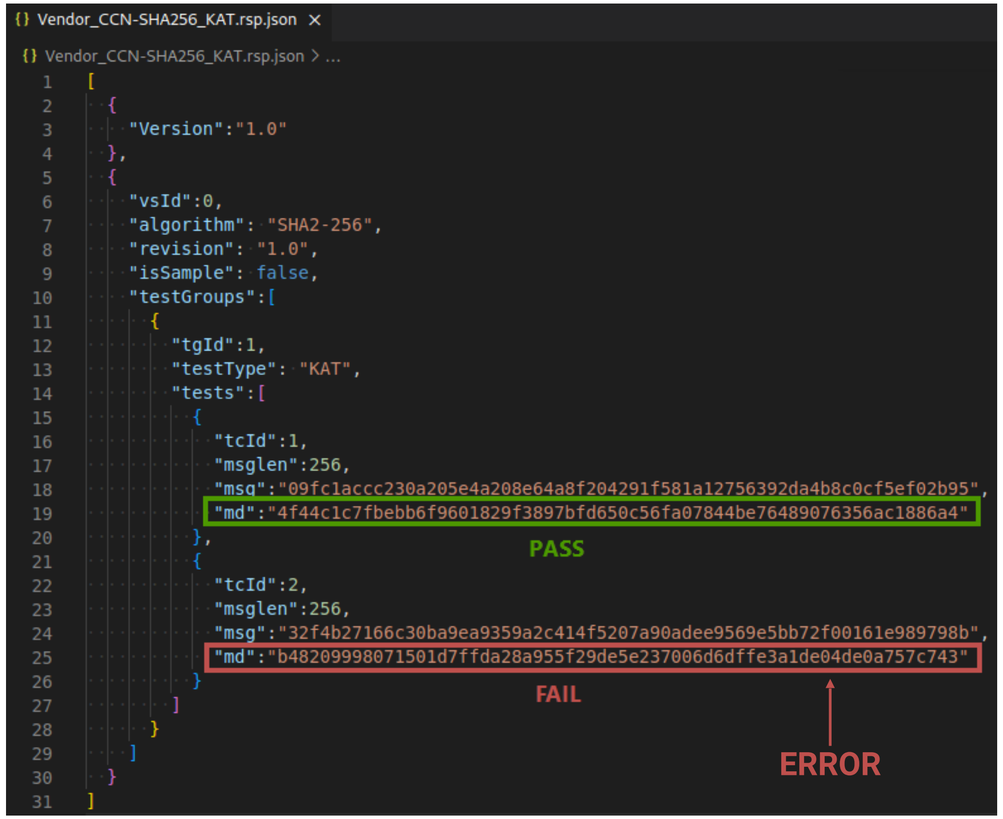
```
┌──(kali㉿kali)-[~/Desktop/acvpparser-master]
└─$ ./acvp-parser -e CCN-SHA256_KAT.rsp.json Vendor_CCN-SHA256_KAT.rsp.json -v
[PASSED] compare CCN-SHA256_KAT.rsp.json with Vendor_CCN-SHA256_KAT.rsp.json
```

Validation of results



Cryptographic Mechanisms Evaluation Methodology

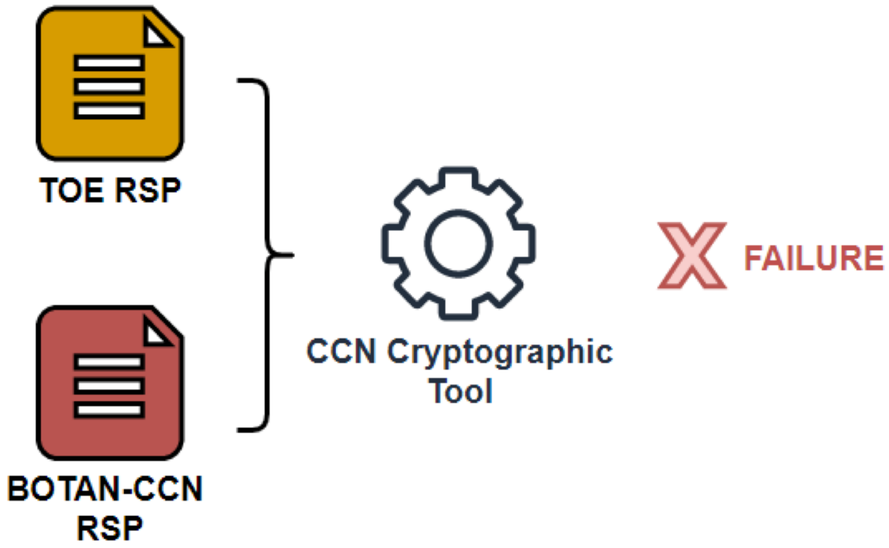
Cryptographic Evaluation Tool - Usage Example: SHA-256



'RESPONSE' file generated by TOE

```
┌──([redacted])-[~/Desktop/acvpparser-master]
└─$ ./acvp-parser -e CCN-SHA256_KAT.rsp.json Vendor_CCN-SHA256_KAT.rsp.json -v
[FAILED] compare CCN-SHA256_KAT.rsp.json with Vendor_CCN-SHA256_KAT.rsp.json
```

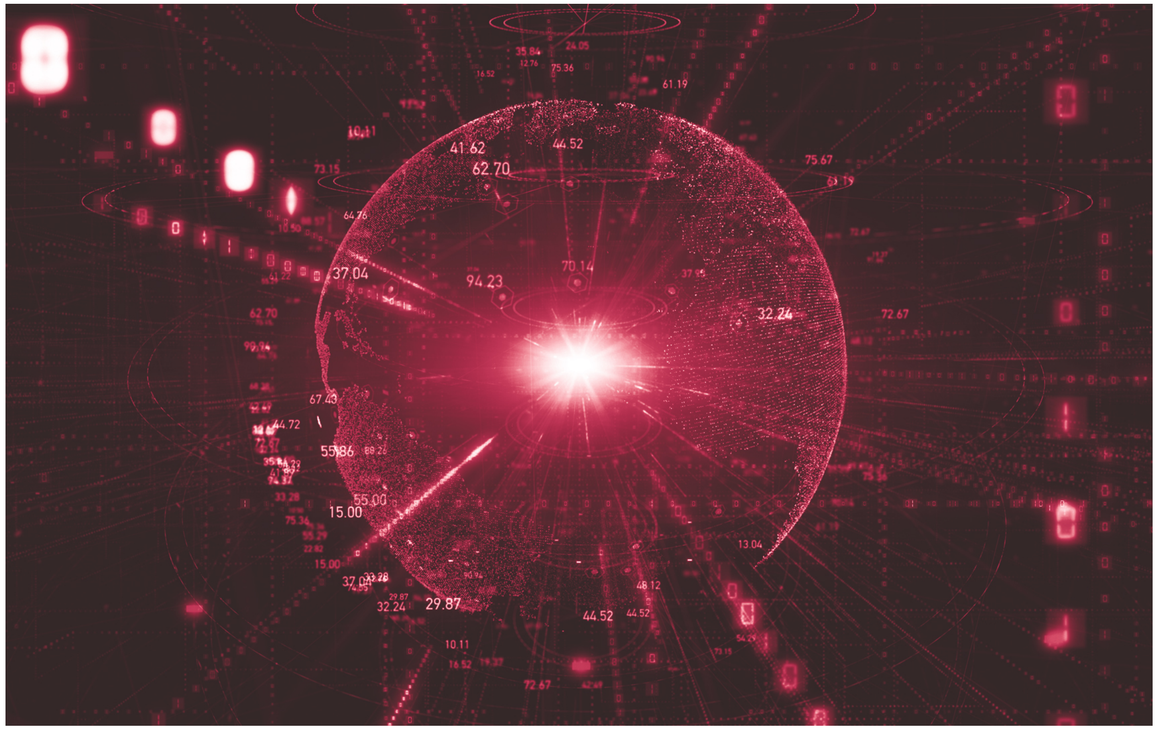
Validation of results



INDEX

Cryptographic Mechanisms Evaluation Methodology

Future directions



1.New Algorithms:

The Cryptographic Mechanisms Evaluation Methodology will be adapted in the future to include new "classical" and post-quantum algorithms recommended by the Spanish CCN in the new STIC 221 guide.

- **New recommended classical algorithms**: SCRYPT, ChaCha20_Poly1305 and EdDSA.

- **Post-Quantum Algorithms:** several post-quantum algorithms are recommended to face the quantum threat:
  - CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+ , Classic McEliece, BIKE, HQC and SIKE.
  - FrodoKEM is also recommended. It will not be standardised as part of NIST’s PQC project, mainly due to efficiency considerations, but there are currently no doubts about its security.

Cryptographic Mechanisms Evaluation Methodology

Future directions

2. Security Levels:

Different increasing qualitative levels of security will be defined for the methodology.

Each TOE will be evaluated according to the level of sensitivity of the information it handles and the global evaluation methodology to which the Cryptographic Methodology is being applied to.

Some evaluation tasks will be common for all levels and others will only apply depending on the security level.

INDEX

Conclusions

- Innovative, necessary and useful methodology to evaluate crypto mechanisms
- Contribution to complement European efforts
- It is necessary to harmonize the criteria at the national level in order to make life easier for laboratories and vendors


jtsec
BEYOND IT SECURITY
Thank you