Evolucionando la Evaluación Criptográfica

UN CIBERESCUDO ÚNICO PARA ESPAÑA

JOSÉ RUIZ GUALDA

jtsec Beyond IT Security

jruiz@jtsec.es

- Ingeniero en Informática (Universidad de Granada)
- Experto en Common Criteria, LINCE y FIPS 140-2 & FIPS 140-3
- Miembro del SCCG (Stakeholder Cybersecurity Certification Group) en la Comisión Europea
- Secretario del SC3 en CTN320
- Editor de LINCE como norma UNE
- Editor en JTC13 WG3 de la Metodología FITCEM
- Revisor de la Comisión Europea para el grupo ERNCIP "Certificación de Ciberseguridad IACS"

JUAN MARTÍNEZ ROMERO

jtsec Beyond IT Security

jmartinez@jtsec.es

- Ingeniero en Tecnologías de Telecomunicación (Universidad de Granada)
- Máster en Ciberseguridad (Universidad de Granada)
- Crypto Manager & Senior Cibersecurity Consultant
- Experto en FIPS 140-2, FIPS 140-3 y PCI-PTS, entre otras metodologías
- CriptoCert Certified Crypto Analyst

ÍNDICE

INTRODUCCIÓN

¿Qué es la criptografía?

"Arte de escribir con clave secreta o de un modo enigmático."
La criptografía es el **ámbito de la criptología** encargado del estudio de los algoritmos, protocolos y sistemas empleados para **dotar de seguridad** a las comunicaciones, a la información y entidades que se comunican.

Propiedades criptográficas

- Confidencialidad
- Integridad
- Autenticación
- No repudio

La criptografía es una **solución de ciberseguridad ideal para garantizar la seguridad de la información**.

HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

USA

NIST (National Institute of Standards and Technology)

- Verificación de la Conformidad según FIPS 140-1, FIPS 140-2 y FIPS 140-3
  - CMVP - Diseñado para certificar módulos criptográficos
  - CAVP – Diseñado para certificar algoritmos criptográficos
- Publicación de múltiples "Special Publications" especificando algoritmos criptográficos y como probarlos.

ACVP

HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

Internacional

HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA

España

Organismo de certificación de módulos criptográficos – OC-CCN (Centro Criptológico Nacional)

ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

Europa

SOG-IS Crypto Evaluation Scheme Harmonised Cryptographic Evaluation Procedures v0.16 (Diciembre 2020)

- Primera metodología de evaluación de SOG-IS
  - Implementación de mecanismos criptográficos
  - Requisitos para Prevención de Pitfalls

SOG-IS HEP

SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.2 (Enero 2020)

- Mecanismos criptográficos acordados y recomendados por SOG-IS
  - Nivel de seguridad aceptable
  - Indicaciones de implementación

SOG-IS ACM

ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

España

Guía CCN-STIC 130

Guía Requisitos Evaluación Criptológica (DL) (Octubre 2017)

- Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada
  - Enfoque similar a FIPS
  - Requisitos de seguridad

Guía CCN-STIC 130

MEC – LINCE

Módulo de evaluación Criptográfica dentro la metodología LINCE

- Pruebas muy ligeras de conformidad criptográfica siguiendo la aproximación de los Perfiles de Protección del NIAP

Botan-CCN Cryptographic Library

Implementación de referencia para evaluaciones criptográficas del CCN

ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

España

Guía CCN-STIC 807

Criptología de empleo en el Esquema Nacional de Seguridad
(Mayo 2022)

- Mecanismos criptográficos autorizados para su uso en el ENS
  - Fortaleza requerida según el nivel de seguridad
  - Protocolos Criptográficos
  - Requisitos para Prevención de Pitfalls

Guía CCN-STIC 807

Guía CCN-STIC 221

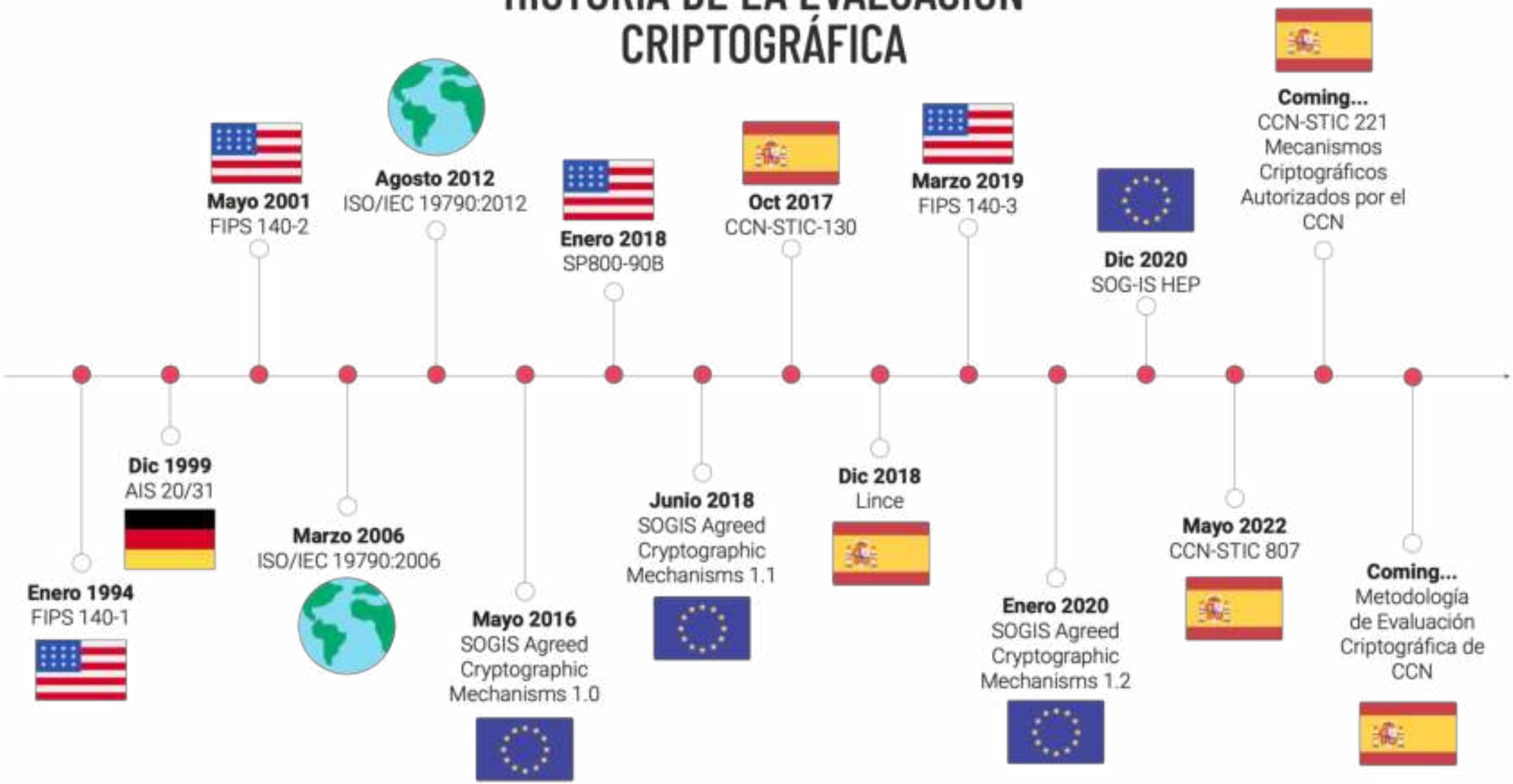
Mecanismos Criptográficos Autorizados por el CCN (Pendiente de Publicación)

- Mecanismos criptográficos autorizados por CCN
  - Inclusión de nuevos algoritmos autorizados por CCN respecto al ACM europeo.
  - Guía de uso transversal no limitada al ENS

NUEVO

Guía CCN-STIC 221

HISTORIA DE LA EVALUACIÓN CRIPTOGRÁFICA



ACTUALIDAD DE LA EVALUACIÓN CRIPTOGRÁFICA

¿Problemática a nivel nacional?

Razones por las que es necesaria esta metodología criptográfica

FIPS y/o ISO FIPS

- Solo funciona cuando el módulo se ha creado para cumplir los requisitos de FIPS.
- No funciona bien en productos que integran criptografía pero no usan un módulo criptográfico de un tercero.
- No se verifican errores de implementación que afecten a la seguridad ni valores límites. Es decir, las pruebas son muy de conformidad.

STIC 130

- No incluye conformidad a nivel de algoritmos e incluye requisitos de implementación de producto,
- No está 100% focalizada en la implementación criptográfica.
- Aporta el punto de vista de seguridad

No tenemos una metodología que evalúe algoritmos y protocolos criptográficos.

STIC 130

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Uso

Metodología de Evaluación Criptográfica de CCN

- Productos cuya funcionalidad principal requiera de criptografía (ej.- VPN, cifradores, comunicaciones seguras, etc...)
- Durante procesos de certificación CC, LINCE y STIC Complementaria

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Definición

Metodología de Evaluación Criptográfica de CCN
- Estructura del Documento

DRAFT

1. Requisitos Criptográficos
2. Mecanismos Criptográficos Aprobados
3. Pruebas de Conformidad
4. Errores Comunes de Implementación

centro criptológico nacional

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 1. Requisitos Criptográficos

Objetivo: Especificar los requisitos extraídos por CCN de la guía CCN-STIC 130 que aplican a la seguridad de los productos criptográficos en relación a los mecanismos y primitivas criptográficas implementadas en relación a:

- Implementación de algoritmos aprobados
- KATs (Know Answer Tests)
- Self-tests
- Gestión de parámetro críticos de la seguridad (PCS)

Evaluación: El evaluador deberá verificar que los el TOE cumple con los requisitos criptográficos recogidos en esta sección.

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 2. Mecanismos Criptográficos Aprobados

Objetivo: Especificar los mecanismos criptográficos reconocidos y acordados por los participantes del Esquema de Evaluación Criptográfica de SOG-IS.

Evaluación: El evaluador deberá verificar que los mecanismos criptográficos implementados por el TOE cumplen con las directrices presentadas por el SOG-IS en la guía SOG-IS Agreed Cryptographic Mechanisms.

CCN
centro criptológico nacional

Guía CCN-STIC 221

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Objetivo: Especificar los requisitos necesarios para la realización de las pruebas de conformidad de los mecanismos y primitivas criptográficas implementadas por el TOE. Estas pruebas determinarán si los mecanismos y primitivas criptográficas empleados por el TOE se han implementado de forma adecuada, de manera similar a lo realizado por el NIST, pero verificando además, parametrizaciones y valores límite que suelen inducir a error.

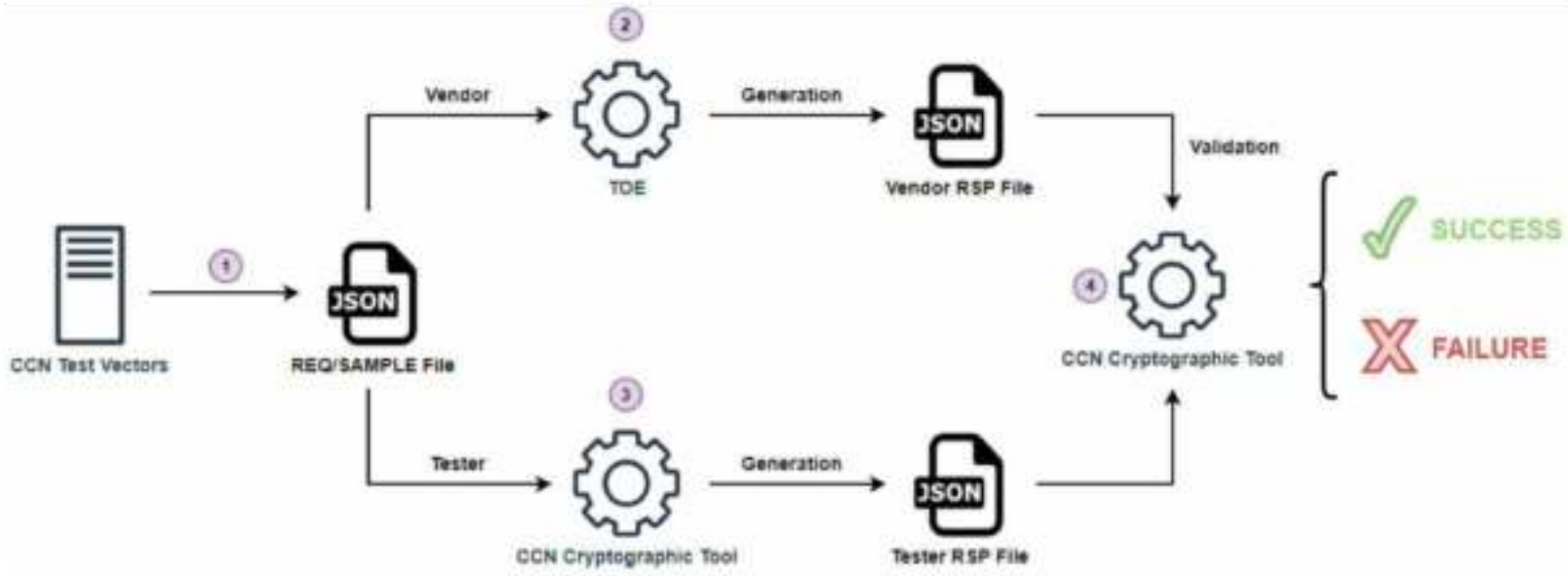
Evaluación: El proceso de evaluación se divide en cuatro fases:

1. Generación de Vectores de Prueba: Ficheros Request y Sample
2. Generación de Resultados por parte del Fabricante: Fichero Response
3. Generación de Resultados por parte del Evaluador: Fichero Response
4. Validación de Resultados por parte del Evaluador

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Diagrama del Proceso de Evaluación de las Pruebas de Conformidad



METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Generación de Vectores de Prueba

- El evaluador deberá generar un fichero 'REQUEST' (en formato JSON) para cada mecanismo criptográfico implementado por el TOE que contendrá los vectores de test asociados a la parametrización soportada.
- Adicionalmente, el evaluador generará el fichero 'SAMPLE' (en formato JSON) para cada mecanismo criptográfico implementado por el TOE que contendrá una solución de ejemplo para indicar el formato del resultado esperado.

El evaluador deberá enviar al fabricante un paquete de archivos que contenga los ficheros 'REQUEST' y 'SAMPLE' asociados a todos los mecanismos criptográficos implementados por el TOE.

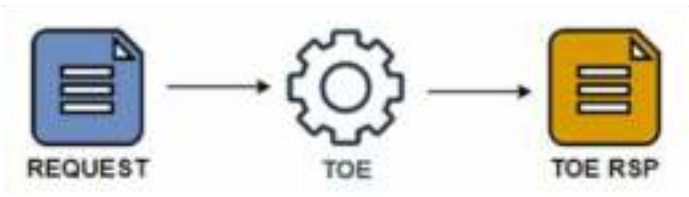
METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Generación de Resultados por parte del Fabricante

- El fabricante deberá generar un fichero 'RESPONSE' asociado a cada mecanismo criptográfico implementado, que contendrá la salida proporcionada por el TOE para cada uno de los vectores de test proporcionados en el fichero 'REQUEST'.
- El fabricante deberá conservar el formato JSON presentado en los ficheros 'REQUEST' y 'SAMPLE' para la generación del fichero 'RESPONSE'.

El fabricante deberá enviar al evaluador un paquete de archivos que contenga los ficheros 'RESPONSE' asociados a todos los mecanismos criptográficos implementados por el TOE.



METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Generación de Resultados por parte del Evaluador

- El evaluador deberá generar el fichero 'RESPONSE' asociado a cada mecanismo criptográfico implementado por el TOE, empleando la librería Botan-CCN como implementación criptográfica de referencia.
- El evaluador deberá conservar el formato JSON presentado en los ficheros 'REQUEST' y 'SAMPLE' para la generación del fichero 'RESPONSE'.

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 3. Pruebas de Conformidad de Algoritmos

Validación de Resultados por parte del Evaluador

- El evaluador deberá validar los ficheros 'RESPONSE' proporcionados por el fabricante para cada mecanismo criptográfico implementado por el TOE, comparando los resultados proporcionados con los obtenidos en la fase anterior empleando la librería criptográfica Botan-CCN.
- El evaluador determinará si el TOE implementa correctamente los mecanismos y primitivas criptográficas empleadas y declaradas.

METODOLOGÍA DE EVALUACIÓN CRIPTOGRÁFICA

Estructura / 4. Errores Comunes de Implementación

Objetivo: Especificar los requisitos necesarios para evitar errores de implementación en los mecanismos y primitivas criptográficas implementados por el TOE.

Evaluación: El evaluador deberá verificar que los mecanismos criptográficos implementados por el TOE cumplen con las directrices para evitar errores de implementación presentadas por el SOG-IS en la guía SOG-IS Harmonised Cryptographic Evaluation Procedures.

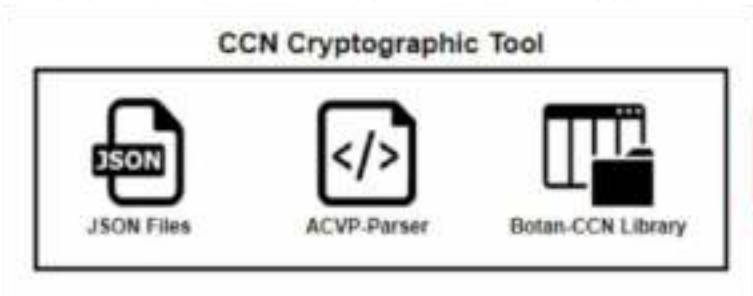
EJEMPLO:
El evaluador deberá verificar que un IV nunca puede ser reutilizado en el cifrado con la misma clave para diferentes entradas

HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

Definición

Herramienta de Evaluación Criptográfica de CCN

- Realización de Pruebas de Conformidad
- Estructura de la Herramienta
  - Ficheros de test JSON: vectores de test en formato hexadecimal de acuerdo a la metodología de SOG-IS.
  - ACVP-Parser: procesamiento de ficheros JSON y extracción de parámetros necesarios para invocar a la implementación criptográfica de referencia.
  - Botan-CCN Cryptographic Library: implementación criptográfica de referencia empleada para la generación de resultados de los vectores de test y la validación de la correcta implementación criptográfica del TOE.

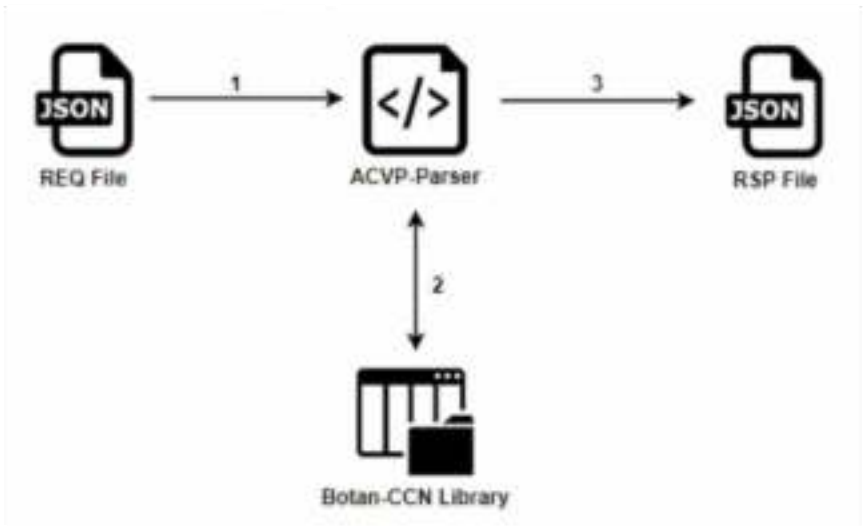


DRAFT

HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

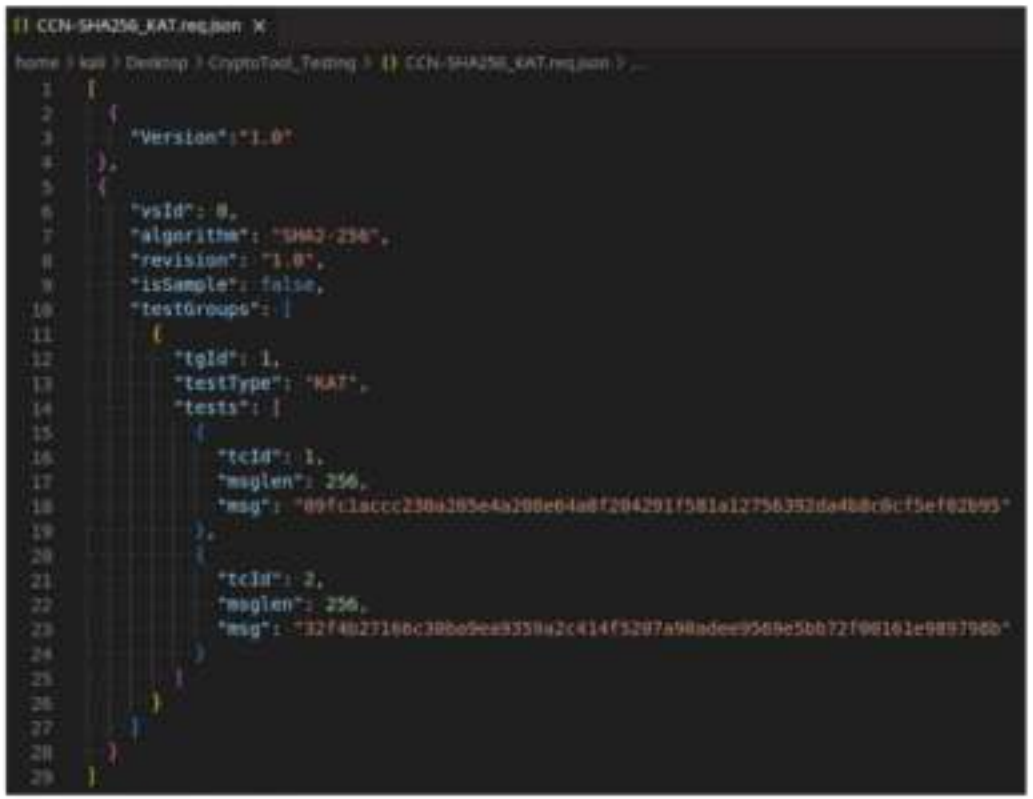
Diagrama de Flujo

1. Procesado de los vectores de tests para extraer los parámetros empleando el ACVP-Parser.
2. Invocación de la librería criptográfica Botan-CCN para realizar la generación de resultados de los vectores de tests haciendo uso del fichero 'REQUEST' asociado.
3. Generación de fichero 'RESPONSE' asociado a un mecanismos criptográfico empleando el fichero 'REQUEST' asociado y los resultados obtenidos empleando la librería criptográfica Botan-CCN.

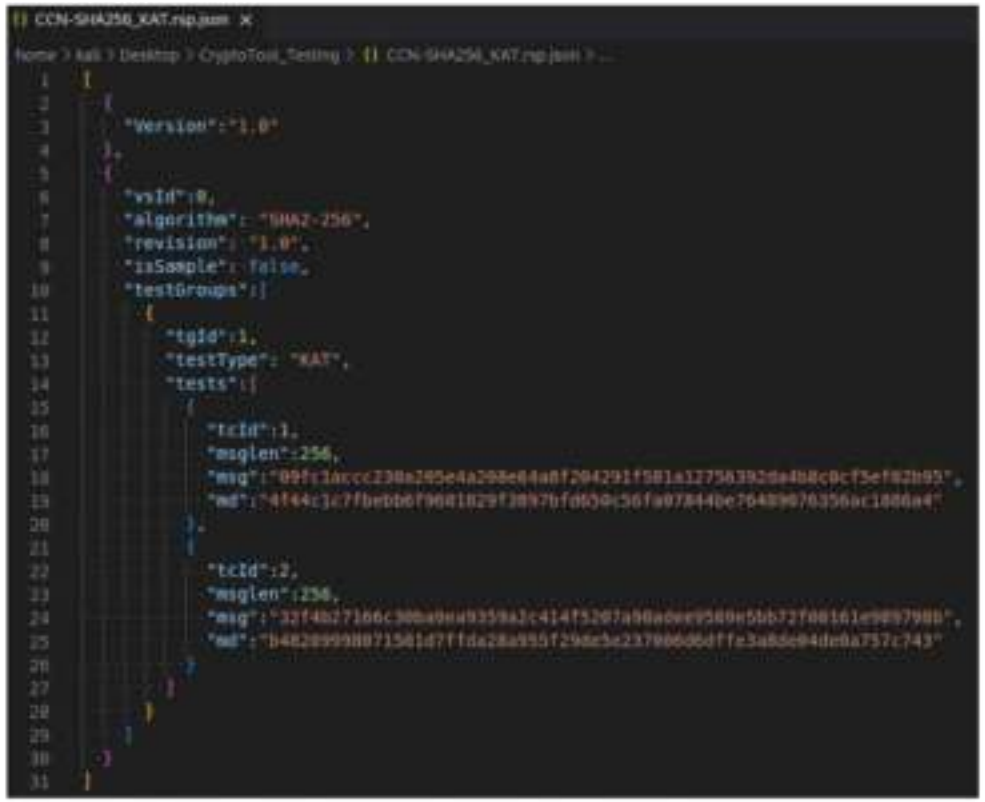


HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

Ejemplo de Uso: SHA-256



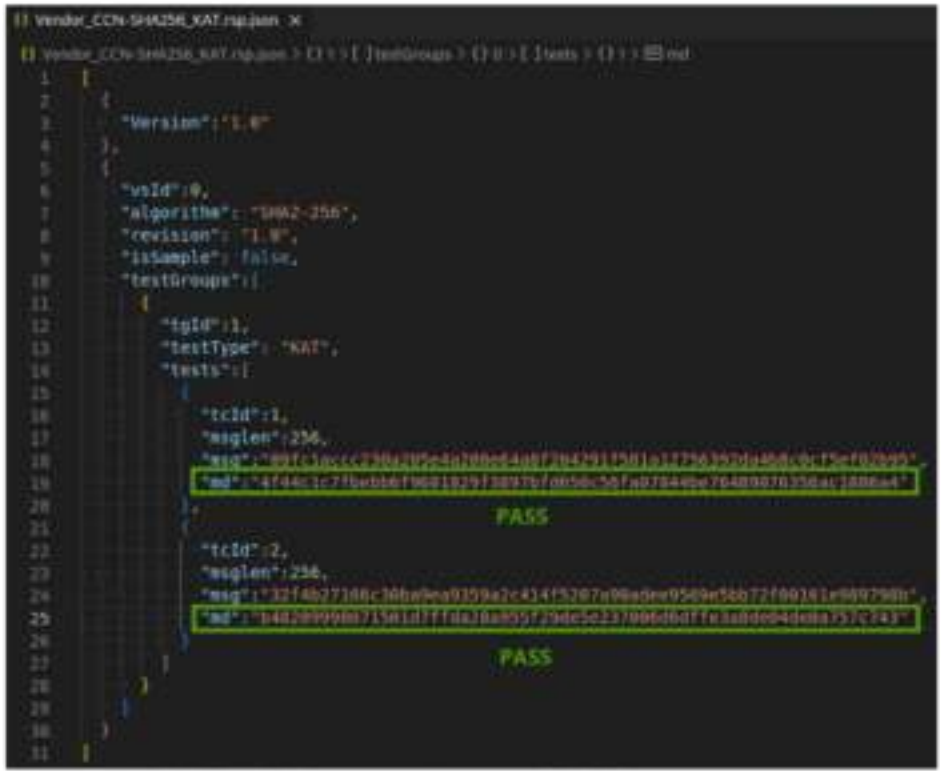
Fichero 'REQUEST'



Fichero 'RESPONSE' generado por la Herramienta

HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

Ejemplo de Uso: SHA-256



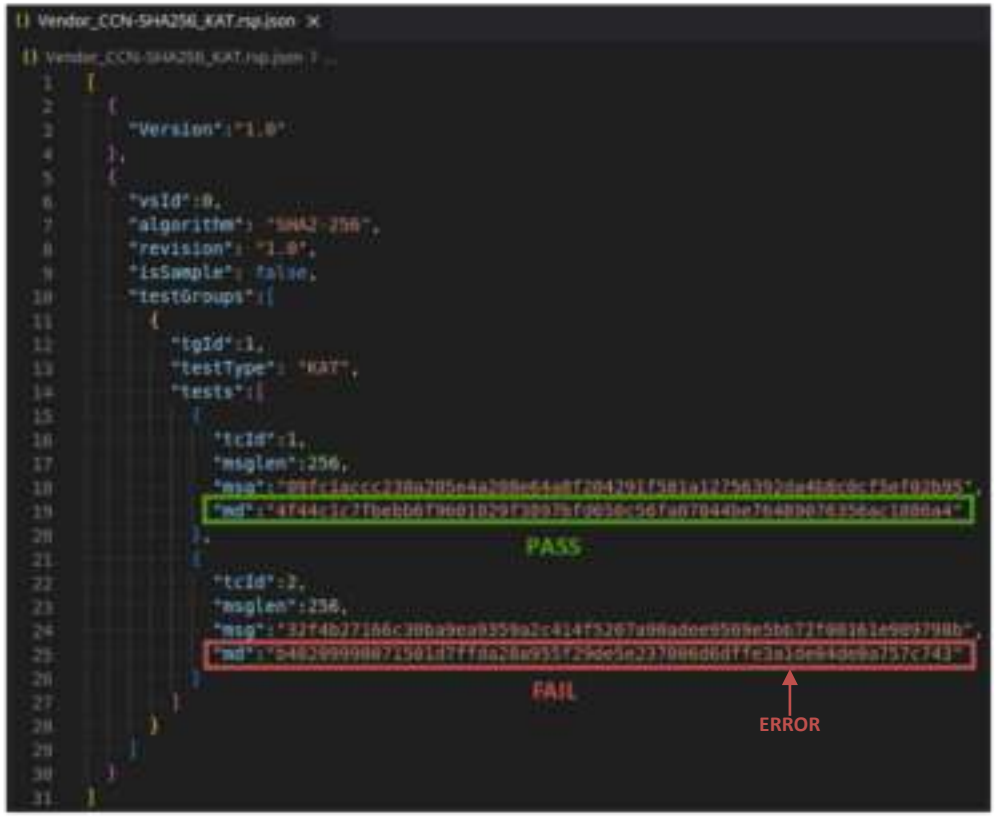
Fichero 'RESPONSE' generado por el TOE

```
┌──([redacted])-[~/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
```

Validación de resultados

HERRAMIENTA DE EVALUACIÓN CRIPTOGRÁFICA

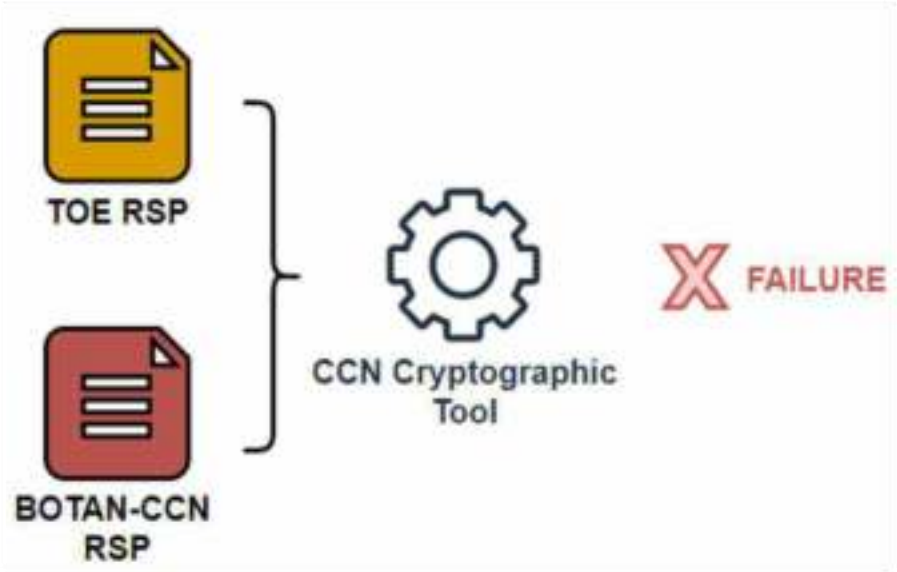
Ejemplo de Uso: SHA-256



Fichero 'RESPONSE' generado por el TOE

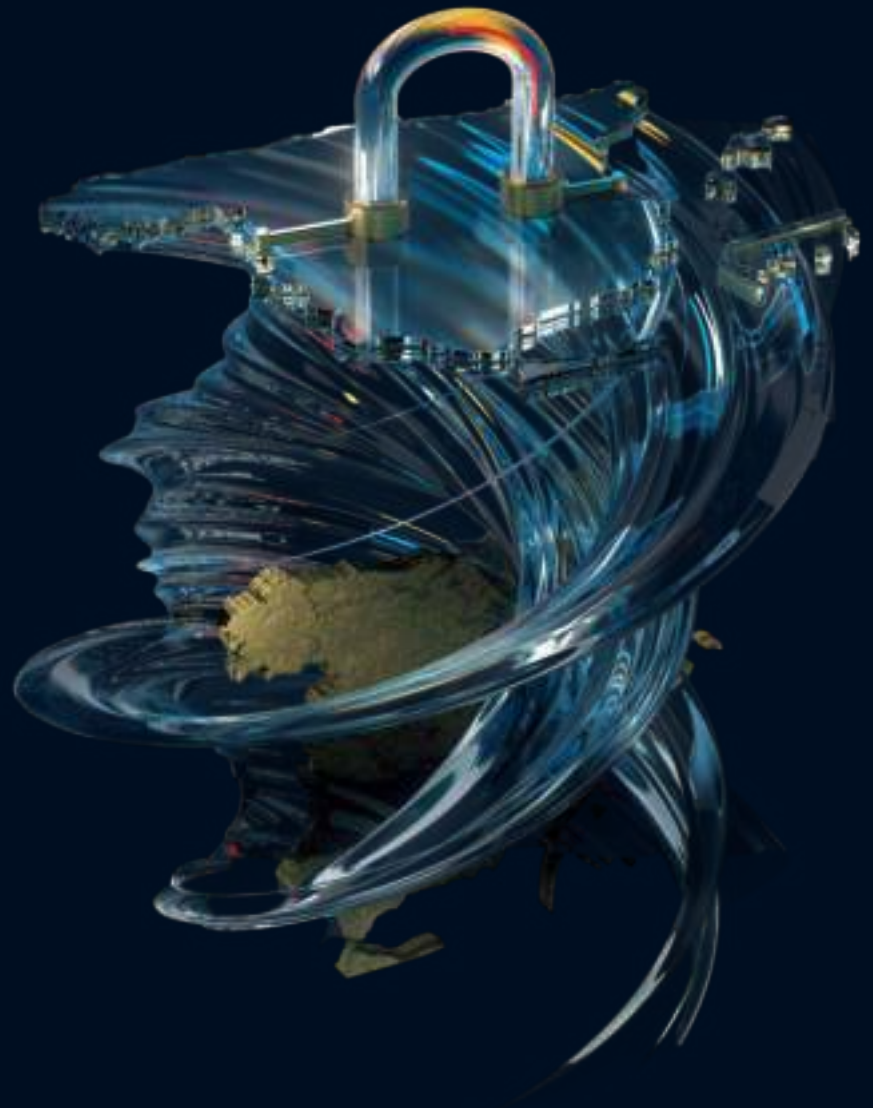
```
┌──(~/Desktop/acvpparser-master)
└─$ ./acvp-parser -e CCN-SHA256_KAT.rsp.json Vendor_CCN-SHA256_KAT.rsp.json -v
[FAILED] compare CCN-SHA256_KAT.rsp.json with Vendor_CCN-SHA256_KAT.rsp.json
```

Validación de resultados



CONCLUSIONES

- España es pionera en:
  - La creación de una metodología de evaluación criptográfica
  - La creación de una herramienta de validación de la conformidad de los algoritmos
- Contribución para complementar los esfuerzos europeos
- Resulta necesario y lógico unificar criterios en el sector para facilitar la vida a laboratorios y fabricantes.



MUCHAS GRACIAS

UN CIBERESCUDO ÚNICO PARA ESPAÑA