GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

# Guía de Seguridad de las TIC
# CCN-STIC 140

# Taxonomía de referencia para productos de seguridad TIC - Anexo F.4: Tarjetas inteligentes

Noviembre 2017

Edita:



CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:30:06 +01'00'


NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento y sus anexos.

# ÍNDICE

# 1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia Tarjetas Inteligentes para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Tarjetas Inteligentes** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

# 2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

## 2.1 FUNCIONALIDAD

6. La funcionalidad principal de los productos asociados a esta familia es la de ejecutar lógica programada para distintos fines en sus circuitos integrados, así como proporcionar interfaces para establecer comunicación con los sistemas con que deben interactuar.

7. Además, pueden implementar diferentes mecanismos de protección de los datos intercambiados y permitir almacenamiento seguro para información sensible como claves privadas, números de cuenta, contraseñas, información médica, etc.

8. Una tarjeta inteligente contiene un circuito integrado compuesto por un procesador, componentes de seguridad, interfaces de entrada/salida (de contacto, sin contacto) y memorias (volátiles y no volátiles). Este circuito integrado, que incorpora ciertos mecanismos de seguridad, permite a la tarjeta ejecutar programas y almacenar datos.

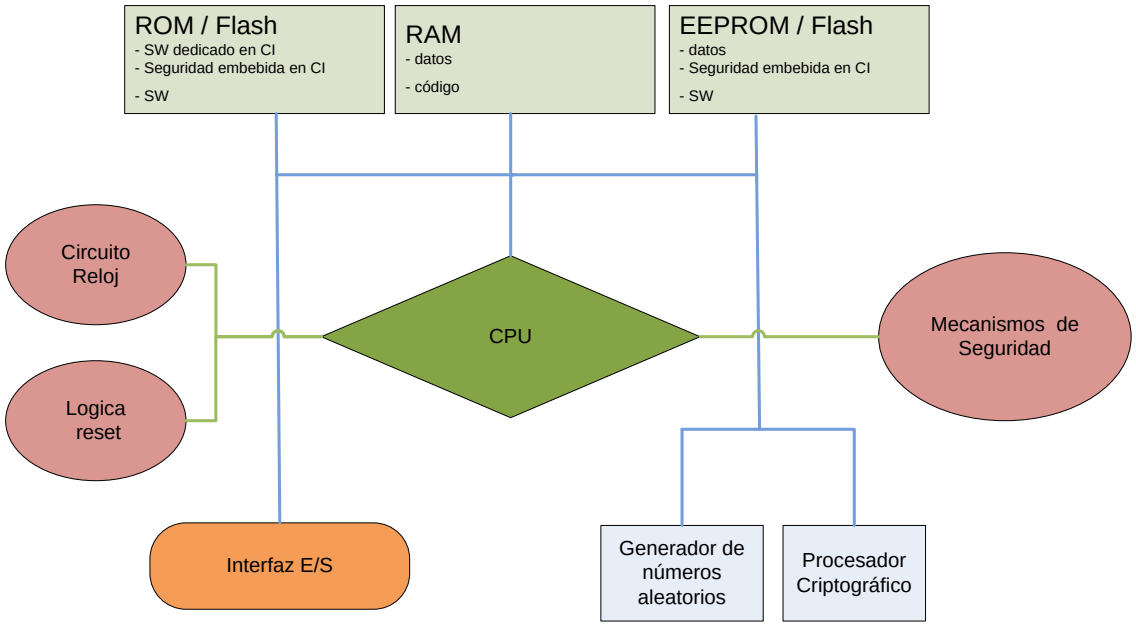


Figura 1 – Ejemplo Circuito inteligente de seguridad

## 2.2 DELIMITACIÓN DEL DISPOSITIVO EN ALCANCE

9. Este tipo de productos se presentan en formato de un circuito integrado provisto de firmware y software con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.

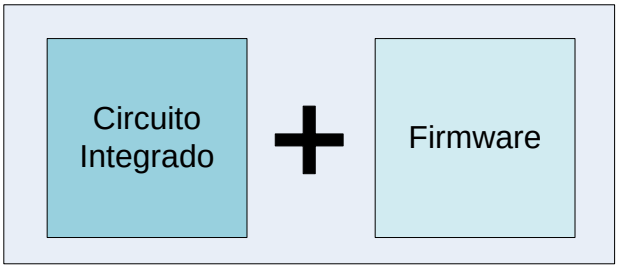


**Figura 2.** Formato de ejemplo de una tarjeta inteligente

## 2.3 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

10. El estándar Common Criteria (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
11. En el ámbito de CC se elaboran, mediante grupos de trabajo especializados, unos perfiles de seguridad conocidos como Protection Profiles (PP) que definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación e independientes de la implantación, para un dominio o categoría de productos.
12. Para esta familia de productos se han tenido en cuenta perfiles de protección elaborados por miembros de SOG-IS[1] y mantenidos por JIWG[2].
13. Debido a la gran diversidad de usos a los que se destinan las tarjetas inteligentes, existe una multitud de perfiles de protección existentes en CC. En el apartado 3 se indican los perfiles de protección aplicables a cada caso.

[1] https://www.sogis.org
[2] *Joint InterpretationsWorking Group.*

# 3. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

14. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

## 3.1 REQUISITOS CRIPTOGRÁFICOS

15. **REQ. 1** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

## 3.2 CIRCUITO INTEGRADO CONFIABLE

16. **REQ. 2** El producto deberá tener un circuito integrado confiable certificado con el siguiente perfil de protección certificado de acuerdo a la norma CC:

| PERFILES DE PROTECCIÓN | | | |
|---|---|---|---|
| **Perfil de protección** | **Versión** | **Fecha** | **Organismo responsable** |
| *Security IC Plattform Protection Profile with Augmentation Packages*[3] | 1.0 | 19/02/2014 | BSI[4] |

Tabla 1. Perfiles de protección

## 3.3 JAVA CARD

17. **REQ. 3** Se denomina *Java card* a la tarjeta inteligente que permite ejecutar software programado en java sobre un circuito integrado confiable.
18. En caso de este tipo de tarjetas, el producto deberá estar certificado con uno de los siguientes perfiles de protección:

[3] https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf
[4] *Bundesamt for Sicherheit in der Informationstechnik*

| PERFILES DE PROTECCIÓN | | | |
|---|---|---|---|
| **Perfil de protección** | **Versión** | **Fecha** | **Organismo responsable** |
| *Java Card™ System Closed Configuration*[5] | 2.6 | 16/12/2010 | ANSSI[6] |
| *Java Card™ System Open Configuration*[7] | 3.0 | 29/05/2012 | ANSSI |

Tabla 2. Perfiles de protección

## 3.4 DISPOSITIVO SEGURO DE CREACIÓN DE FIRMA

19. **REQ. 4** En el caso de que el producto sea un dispositivo seguro de creación de firma, deberá cumplir con los RFS del Anexo E.5 Dispositivos de creación de firma.

[5] https://www.sogis.org/documents/cc/pp/sc/others/anssi-cc_pp-profil-2010_07en.pdf
[6] *Agence Nationale de la Sécurité des systèmes d'information*
[7] https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-profil_PP-2010-03en.pdf

## 4. ABREVIATURAS

| | |
|---|---|
| **ANSSI** | *Agence Nationale de la Sécurité des systèmes d'information (Francia)* |
| **BSI** | *Bundesamt for Sicherheit in der Informationstechnik (Alemania)* |
| **CC** | *Common Criteria* |
| **CCN** | *Centro Criptológico Nacional* |
| **CI** | *Circuito Integrado* |
| **CPSTIC** | *Catálogo de Productos de Seguridad de las Tecnologías de Información y la Comunicación* |
| **E/S** | *Entrada / Salida* |
| **EEPROM** | *Electricially Erasable Programmable Read-Only Memory* |
| **ENS** | *Esquema Nacional de Seguridad* |
| **PP** | *Protection Profiles* |
| **RAM** | *Random Access Memory* |
| **RFS** | *Requisitos Fundamentales de Seguridad* |
| **ROM** | *Read Only memory* |
| **SOG-IS** | *Senior Officials Group Information Systems Security* |
| **SW** | *Software* |
| **USB** | *Universal Serial Bus* |
| **JIWG** | *Joint InterpretationsWorking Group* |