Calypso
Networks Association

GUÍA

para redactar licitaciones de tarjetas, ticketing móvil NFC y terminales bajo el estándar Calypso

Junio 2023

¿Cómo abrir su sistema de ticketing en las licitaciones?

TABLA DE CONTENIDOS

1 CONTEXTO

Los sistemas de ticketing son un tema altamente estratégico para las autoridades y operadores de transporte, ya que transforman la política de movilidad de su territorio y también aseguran que puedan generar ingresos. Estos sistemas están diseñados para ser sostenibles y flexibles, particularmente en lo que respecta a cambios tarifarios, extensiones de la red y la implementación de esquemas interoperables.

Para asegurar la durabilidad de un sistema de ticketing, es necesario poder integrar equipos, tarjetas y software de diferentes fabricantes durante su ciclo de vida. De hecho, el proveedor original del sistema no necesariamente tiene la capacidad o el deseo de proporcionar evoluciones a un precio razonable. Tener varios proveedores potenciales evita una situación de monopolio en las redes, lo que podría resultar en costos excesivos o la imposibilidad de realizar una actualización.

Para asegurar la compatibilidad e interoperabilidad técnica entre diferentes proveedores, es importante pasar de una lógica de producto (fija y generalmente propietaria en esencia) a una lógica de estándares, siempre que sean abiertos y multifuente. El cliente debe entonces tener requisitos para el cumplimiento de estas normas y estándares, cuya prueba debe ser proporcionada por el proveedor a través de la certificación de sus productos.

El estándar Calypso cumple con los requisitos establecidos por los organismos internacionales para la designación de estándares abiertos: "Se dice que un estándar es abierto cuando **se pone a disposición de todos, se desarrolla, se mantiene y se administra en un proceso colaborativo y consensuado. Un estándar abierto facilita la interoperabilidad y los datos intercambiados entre diferentes productos o servicios y está destinado a ser ampliamente adoptado**[1] ".

Calypso fue creado para ser desarrollado, mantenido y administrado por las autoridades y operadores de transporte que juntos forman Calypso Networks Association (CNA). CNA es una asociación sin fines de lucro que opera con el objetivo de garantizar escalabilidad, interoperabilidad e independencia de proveedores para todos los usuarios. Calypso es el único estándar de ticketing que es multifuente en todos los niveles, incluidos los componentes electrónicos de las tarjetas.

Es un importante proveedor de resiliencia en tiempos de escasez de componentes. Proporciona al mundo industrial especificaciones de referencia y un proceso de certificación para atestiguar la conformidad del producto. Es el estándar adoptado por muchas redes en todo el mundo. Por lo tanto, muchos proveedores de diferentes orígenes ofrecen productos Calypso en un esquema multi-fuente que ha tenido éxito durante más de 20 años. Esta competencia genuina garantiza que al comprador se le ofrecerán productos Calypso al precio justo.
El reto de las licitaciones de ticketing, más allá de la función de compra de hardware, es garantizar la compatibilidad entre los medios de pago (tarjetas sin contacto, teléfonos inteligentes NFC, ...) y las terminales de ticketing (validadores, dispositivos de venta y control, quioscos, ...) ya desplegadas y recién adquiridas. Sin este requisito previo de compatibilidad, es imposible implementar esquemas interoperables.

1 Según la definición de estándar abierto dada por la Unión Internacional de Telecomunicaciones

El documento “Ticketing para MaaS: mejores prácticas para sistemas duraderos” presenta todas las mejores prácticas a seguir al especificar un sistema de ticketing. En particular, nos recuerda que el modelo de datos no debe estar integrado en la licitación del sistema de ticketing o de las terminales, sino que debe ser gestionado de forma independiente, bajo el control del cliente, quien debe asegurar tener la propiedad del modelo de datos.

2 PROPÓSITO DEL DOCUMENTO

El propósito de este documento es esbozar lo que se requiere en **una licitación de tarjetas sin contacto, de sistemas de ticketing móvil NFC y de terminales para garantizar compatibilidad y escalabilidad.**

Una licitación pública debe permitir una competencia abierta y justa para todos los fabricantes. Este documento ha sido redactado de conformidad con los principios de los códigos de contratación pública franceses y, por lo tanto, puede utilizarse como guía para producir convocatorias de licitación.

CNA ofrece soporte para la redacción de su licitación, en particular asistencia en la definición de la configuración y personalización de sus tarjetas Calypso.

También se propone una verificación de la configuración y personalización de las tarjetas Calypso entregadas por los fabricantes.

Para obtener más información, contáctenos:
contact@calypsonet.org

3 PRINCIPIOS GENERALES

Los principios generales a continuación, se detallan en los capítulos dedicados a las tarjetas, teléfonos inteligentes NFC y terminales respectivamente:

- Referirse sistemáticamente a todas las normas y estándares aplicables al campo,
- Exigir productos certificados, prueba de cumplimiento de normas, o en ausencia de certificación existente, declaración de cumplimiento de normas aplicables en la materia,
- Referir los estándares compartidos existentes y las mejores prácticas cuando estén disponibles a nivel nacional (por ejemplo, en Francia NF P99-405-1[2], NF P99-512[3], etc.),
- De preferencia, solicite integrar la aplicación Calypso Hoplink en las tarjetas Calypso Prime y en los módulos de seguridad. Esto no agrega costo y permite la interoperabilidad futura,
- No se refiera a un nombre de producto comercial específico para una industria dada,
- No haga referencia a tecnologías, especificaciones o soluciones que se hayan vuelto obsoletas, en particular a través de la aparición de repositorios compartidos.

2 *Ticketing informático en el sector del transporte - Normas de interoperabilidad y codificación de ticketing informático (INTERCODE) - Parte 1: codificación de elementos y estructuras de datos*

3 *Gestión de tarifas de transporte - Sistema interoperable de gestión de tarifas (Interoperable Fare Back Office) - INTERBOB – Flujo de datos*

4 REQUERIMIENTOS ESPECÍFICOS **PARA TARJETAS SIN CONTACTO**

Un sistema Calypso correctamente implementado puede aceptar todas las tarjetas sin contacto certificadas por Calypso.

Calypso Networks Association ha creado tres productos:

Calypso® PRIME Calypso® LIGHT Calypso® basic

Todos ellos cuentan con los mismos mecanismos de seguridad y pueden ser gestionados por el mismo software del terminal, lo que garantiza la compatibilidad y una fácil integración.
software, ensuring compatibility and easy integration.

- Calypso® PRIME combina funcionalidades de transporte y multiaplicación/ multiservicio en una única tarjeta. También permite la gestión de múltiples contratos de ticketing y la interoperabilidad entre redes, incluidas las de escala internacional. Calypso Prime en su versión PKI también permite la autenticación de tarjetas sin necesidad de módulos de seguridad adicionales (SAM).

- Calypso® LIGHT es una versión refinada, más adecuada para usuarios ocasionales, con el mismo nivel de seguridad que Calypso Prime. Puede emitirse en plástico o papel ISO y pueden coexistir dos contratos de transporte del mismo operador en una tarjeta. Es también un producto específicamente adaptado a las arquitecturas ABT (Account Based Ticketing).

- Calypso® basic disponible desde 2022, es un ticket de papel recargable, sin contacto y de contrato único, adecuado para viajes sencillos.

En el contexto de una licitación, un mandatario debe exigir que las tarjetas estén certificadas tanto a nivel de radiofrecuencia (hardware/hardware) como a nivel funcional de Calypso (software/software), como se describe en los dos subcapítulos siguientes. La compra de tarjetas no certificadas presenta un grave riesgo de incompatibilidad tarjeta-terminal.

4.1. REQUERIMIENTOS Y CERTIFICACIONES DE RADIO FRECUENCIA (RF)

El primer requisito es que **la tarjeta sin contacto** debe cumplir con la última versión del **ISO/IEC TS 24192** (anteriormente **CEN/TS 16794**), que es la aplicación de transporte del **ISO/IEC 14443**.

El cumplimiento de este estándar garantiza que la tarjeta sea interoperable con terminales que cumplan con este estándar. Y también, con teléfonos inteligentes NFC que cumplan con los requisitos del NFC Forum (https://nfc-forum.org/) , especialmente cuando se utilizan para recargar un ticket en la tarjeta sin contacto.

El cumplimiento de este estándar debe demostrarse mediante la obtención de un certificado de un organismo de certificación aprobado por Smart Ticketing Alliance, que ha desarrollado e implementado el programa de certificación RF (https://www.smart-ticketing.org/certification/) durante varios años.

El proceso de certificación de RF lo lleva a cabo Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), un organismo de certificación independiente, que es el único actualmente autorizado para emitir la certificación de RF bajo el programa del Smart Ticketing Alliance.

La lista actual de tarjetas certificadas ISO/IEC TS 24192 (CEN/TS 16794) por PayCert es pública y se puede encontrar en el sitio web de PayCert: https://www.cna-paycert-certification.eu/rf-interface/picc/.

> IMPORTANTE: La certificación RF de una tarjeta se refiere al producto terminado, incluido el componente con su software, el embebido con antena y el cuerpo de la tarjeta, ensamblados.

Recomendamos enfáticamente no pedir tarjetas usando el protocolo B' (también llamado Innovatron). Este protocolo está obsoleto porque no hay ningún producto certificado que cumpla con este protocolo. Como recordatorio, el protocolo B' no permite la integración de Hoplink. No permite el tratamiento de teléfonos inteligentes NFC (Secure Element and Host Card Emulation) ni la implementación de interoperabilidad. Si la red opera solo en B', se recomienda solicitar tarjetas en modo dual (e ISO 14443 A|B) para facilitar la migración cuando llegue el momento.

Consulte la Sección 6.1.2 Gestión de la Obsolescencia para obtener más detalles sobre las consecuencias de mantener el protocolo B'.

4.2. REQUERIMIENTOS Y CERTIFICACIONES FUNCIONALES CALYPSO

CNA ha esbozado tanto las especificaciones de referencia a las que debe ajustarse cualquier tarjeta Calypso (Prime, Light, Basic) como también un esquema de certificación para garantizar esta conformidad. Esta certificación está gestionada por la entidad certificadora PayCert, única entidad autorizada para emitir certificados. Hay una certificación dedicada para cada una de las tres tarjetas (Prime, Light, Basic).

Cabe señalar que Calypso Prime se puede configurar en tres versiones. La licitación debe especificar qué configuración se solicita:

- Modo regular, (anteriormente rev 3.1); este modo incluye las funciones básicas de Calypso Prime con criptografía TDES y DESX.
- Modo extendido (anteriormente rev 3.2), con criptografía AES y cifrado de datos opcional además de las características del modo normal.
- Modo PKI (anteriormente rev 3.3), que agrega criptografía PKI asimétrica al modo extendido, permitiendo la autenticación de tarjetas sin un módulo de seguridad (SAM) en el terminal.

En una **convocatoria de licitación:**

- Para las tarjetas Calypso Prime, se requiere el cumplimiento de la certificación Calypso Prime, al mismo nivel (o superior) que la versión (regular, extendida o PKI) que se solicita. Se recomienda exigir al menos el cumplimiento de la certificación en modo extendido. Si necesita autenticación de tarjeta sin un módulo de seguridad, debe solicitar el cumplimiento del modo PKI.
- Para las tarjetas Calypso Light, se requiere el cumplimiento de la certificación Calypso Light.
- Para las tarjetas Calypso Basic, se requiere el cumplimiento de la certificación Calypso Basic.

Puede encontrar una lista de tarjetas certificadas Calypso en: https://www.cna-paycert-certification.eu/card/

4.3. CONFIGURACIÓN DE TARJETAS

Para todas las tarjetas **Calypso (Prime, Light y Basic)**, la configuración solicitada debe cumplir con las siguientes reglas:

- Utilice un identificador de aplicación (también llamado “AID” o “contenedor”) **estandarizado** por ISO y referenciado por CNA, específico del operador del sistema de ticketing. No utilice identificadores genéricos como “1TIC.ICA” para los que no se garantiza la unicidad y que son incompatibles con las soluciones de ticketing para teléfonos inteligentes NFC. CNA administra una lista de valores de Calypso AID registrados. Para solicitar un Calypso AID registrado, comuníquese con el soporte técnico de Calypso: support@calypsonet.org

- Utilice el identificador proporcionado por CNA tal cual, sin agregar ningún 00 adicional.

Para las tarjetas **Calypso Prime**, la configuración también debe respetar las siguientes reglas y recomendaciones:

- Configure siempre las aplicaciones en modo Normal, Extendido o PKI, según sea necesario (y no en Calypso Revisión 2.4 o una versión anterior).

- Integrar la aplicación Hoplink (recomendado porque en la mayoría de los casos no agrega ningún costo y permitirá la futura implementación de un esquema de interoperabilidad).

- Utilice las estructuras de archivos más recientes y evite las estructuras de archivos antiguas tanto como sea posible.

Una lista de estructuras de archivos a las que hace referencia CNA está disponible en el documento "Calypso File Structure Registry" document (ref. 060709-CalypsoFiles).

- Use conjuntos de llaves dedicados con criptografía reciente para cada aplicación: **TDES, AES o PKI**, y deje de usar criptografías obsoletas, como DES.

- Si existe la necesidad de compatibilidad con una red más antigua (Calypso revisión 2.4), se debe solicitar una tarjeta Prime certificada que emule la revisión 2.4.

Para las tarjetas **Calypso Light**, la configuración también debe respetar las siguientes reglas:

- Elija una de las dos estructuras de archivos permitidas (Referencia o Clásica), dependiendo de las estructuras existentes y sus necesidades futuras.
- Utilice, preferentemente, un conjunto de llaves específico para este producto. Las tarjetas Light solo utilizan criptografía TDES.

Para las tarjetas **Calypso Basic**, la configuración también respetar las siguientes reglas:

- Utilice un conjunto de llaves exclusivo para este producto. Las tarjetas Basic usan solo criptografía TDES.

Advertencia: No confunda la **estructura de archivos** de una tarjeta Calypso con la **estructura del contrato**, también llamada "instanciación". Estas dos estructuras no cubren la misma noción. La estructura de archivos define la organización de los archivos en la tarjeta. La estructura del contrato, "instanciación", se utiliza para codificar los tickets de transporte.

CNA ofrece soporte para la redacción de su licitación, en particular, asistencia en la definición de la configuración y personalización de sus tarjetas Calypso. También se propone una verificación de la configuración y personalización de las tarjetas Calypso entregadas por los fabricantes.

Para obtener más información, contáctenos: contact@calypsonet.org

4.4. TEXTO PARA LA CONVOCATORIA DE LICITACIÓN

Ver hoja de instrucciones n°1

5 REQUERIMIENTOS ESPECÍFICOS PARA EL TICKET MÓVIL NFC

5.1. SOLUCIONES: SE Y HCE

El **ticketing móvil NFC** es la tecnología que permite el uso de un teléfono inteligente NFC para comprar y/o validar boletos (es decir, modo lector) o para emular una tarjeta sin contacto.

En este documento nos centramos en la capacidad del teléfono inteligente NFC para emular una tarjeta sin contacto. El ticketing móvil NFC está disponible en varios modos dependiendo de si la seguridad se basa o no en un elemento de seguridad de hardware en el teléfono inteligente NFC:

- El ticketing móvil NFC en **SE** (Secure Element) utiliza un componente de microprocesador idéntico al que se encuentra en una tarjeta y, por lo tanto, tiene el mismo nivel de seguridad: Common Criteria EAL4+ al menos para el SE. Los SE están presentes en modelos recientes de teléfonos inteligentes NFC de varios fabricantes, incluidos Samsung y Apple.

  CNA proporciona un applet (aplicación de software) genérico de Calypso para que se cargue en el SE y, por lo tanto, emule completamente una tarjeta Calypso Prime.

  Esta solución tiene la ventaja de no requerir ninguna evolución de los terminales de venta de billetes existentes, solo unos pocos parámetros, siempre que el sistema cumpla al menos con Calypso Prime revisión 3, modo regular.

- El ticketing móvil NFC por **HCE** (Host Card Emulation) no se basa en el uso de un SE almacenado en el teléfono inteligente NFC, sino en la seguridad del software. Es compatible con todos los teléfonos inteligentes Android NFC. Para compensar la menor seguridad innata, debido a la falta de un elemento seguro para proteger los datos confidenciales, un mecanismo (llamado tokenización) actualiza regularmente las llaves secretas de la aplicación Calypso HCE almacenadas en el teléfono inteligente NFC, lo que limita el riesgo de fraude.

  Al igual que con la solución SE, el sistema debe cumplir al menos con la revisión 3 de Calypso Prime. Requiere una ligera evolución del software de los terminales de ticketing de validación para implementar medidas de seguridad específicas de la solución HCE.

5.2. REQUERIMIENTOS DE LA SOLUCIÓN CON ELEMENTO SEGURO (SE)

La solución SE puede obtenerse directamente de un proveedor dedicado o indirectamente a través de su integrador de ticketing. En ambos casos, el cliente deberá solicitar que el proveedor garantice:

- La solución de ticketing móvil NFC puede funcionar con cualquier teléfono inteligente NFC certificado por RF, ya sea basado en la certificación NFC Forum o en la certificación ISO/IEC TS 24192 en su última edición (o su versión CEN/TS 16794)

- El applet se carga solo en elementos seguros (SE), que han sido certificados funcionalmente como compatibles con el emparejamiento "Applet/SE" de Calypso. PayCert, una organización acreditada independiente, gestiona esta certificación y la lista de productos certificados está disponible en https://www.cna-paycert-certification.eu/card/calypso-prime-applet/. Si el par "Applet/SE" aún no está certificado, corresponde al proveedor solicitar esta certificación.

El cumplimiento de los requisitos del terminal, descritos más adelante en este documento, garantiza el cumplimiento de los requisitos específicos para las soluciones móviles NFC.

Las soluciones móviles NFC, ya sea que estén basadas en HCE o en el applet dentro del SE, son comercializadas por proveedores dedicados a cargo de instalar e inicializar la aplicación Calypso en el teléfono inteligente NFC.

5.3. REQUERIMIENTOS DE LA SOLUCIÓN CALYPSO HCE

La solución HCE se puede obtener directamente de un proveedor dedicado o indirectamente a través de su integrador de ticketing. En ambos casos, el cliente debe asegurarse de que se tienen en cuenta los siguientes requisitos:

- El proveedor garantiza que su solución de ticketing móvil NFC puede funcionar con cualquier teléfono inteligente Android NFC que haya sido certificado RF, ya sea sobre la base de la certificación NFC Forum o sobre la base de la certificación ISO/IEC TS 24192 en su última edición (o su versión CEN /TS 16794).

- Se requerirá **la certificación funcional del cumplimiento de las especificaciones de Calypso HCE** tan pronto como esté disponible (finales de 2023).

- **La certificación de seguridad Calypso HCE** se basa en un estándar de última generación para la resistencia al hacking de datos de teléfonos inteligentes. CNA emite este certificado con la asistencia del Internet of Trust (https://www.internetoftrust.com/) como organismo de certificación independiente. Una lista de proveedores que han pasado esta certificación está disponible en calypsonet.org.

- Cumplimiento de las Calypso HCE specifications and guidelines establecidos por la CNA en cuanto a los requisitos aplicables a la infraestructura del sistema de ticketing.

La solución Calypso HCE se basa únicamente en software y no puede depender de la clasificación de seguridad de un componente electrónico en el teléfono inteligente NFC. Para garantizar un nivel de seguridad que cumpla con el estándar Calypso, CNA ha implementado un conjunto de medidas de seguridad específicas para la solución HCE, que se pueden encontrar en las **especificaciones y lineamientos.**

Todos los proveedores de Calypso HCE están comprometidos por contrato, como licenciatarios, a cumplir con estas especificaciones y lineamientos.

5.4. TEXTO PARA LA CONVOCATORIA DE LICITACIÓN

Ver hoja de instrucciones n°2

6 REQUERIMIENTOS ESPECÍFICOS **PARA TERMINALES Y SOFTWARE DE TICKETING**

A efectos de este documento, una terminal es un dispositivo de venta, validación, control o personalización. El software de ticketing es aquel que habilita una transacción de ticketing, que en el ecosistema CNA incluye el software del lector, la biblioteca Calypso y la aplicación de ticketing, independientemente de que estén en el terminal o exportados a un servidor central.

RECORDATORIO: para garantizar la interoperabilidad entre varios elementos de la infraestructura de ticketing, especialmente tarjetas y lectores, es fundamental que cada uno esté certificado tanto a nivel de radiofrecuencia como a nivel funcional.

6.1. REQUERIMIENTOS Y CERTIFICACIÓN DE RADIO FRECUENCIA (RF)

El primer requisito es que la **radiofrecuencia (RF) de la terminal sin contacto** cumpla con la última versión del **ISO/IEC TS 24192** (anteriormente denominada **CEN/TS 16794**), que es la aplicación de transporte del **ISO/IEC 14443**.

El cumplimiento de este estándar garantiza la interoperabilidad de la terminal con tarjetas que cumplan con este estándar. Y también, con teléfonos inteligentes NFC que cumplan con los requisitos de NFC Forum, especialmente cuando se utilizan para emular una tarjeta de transporte sin contacto.

El cumplimiento de esta norma debe demostrarse mediante la obtención de un certificado de un organismo de certificación aprobado por Smart Ticketing Alliance, que ha desarrollado e implementado el programa de certificación de radiofrecuencia (https://www.smart-ticketing.org/certification/) durante varios años.

El proceso de certificación de RF lo lleva a cabo Paycert (https://www.cna-paycert-certification.eu/rf-interface-2), un organismo de certificación independiente y el único organismo actualmente autorizado para emitir la certificación de RF de acuerdo con el programa del Smart Ticketing Alliance.

La lista actual de terminales con certificación ISO/IEC TS 24192 (CEN/TS 16794) es pública y se puede encontrar en el sitio web de PayCert en https://www.cna-paycert-certification.eu/rf-interface/pcd/.

IMPORTANTE: La certificación RF de una terminal incluye:

- El producto terminado, incluido el hardware electrónico en su estado final de embalaje, con el software.
- O sobre un subconjunto del producto terminado, en la medida en que este submontaje se haya integrado en el producto acabado según las recomendaciones del fabricante, que garantizan la no pérdida de la certificación.

6.1.1. COMPATIBILIDAD CON TARJETAS Y APLICACIONES DE PAGO SIN CONTACTO EMV

Si se prevé la implementación de un servicio de **Pagos Abiertos** a corto, medio o largo plazo, es recomendable solicitar, además de la certificación RF, que los terminales estén certificados EMVCo nivel 1 (L1). **Este proceso de certificación se realiza con EMVCo** (https://www.emvco.com/).

La lista actualizada de terminales con certificación EMVCo L1 es pública y se puede encontrar en el sitio web de EMVCo en: https://www.emvco.com/approved-registered/approved-products/

6.1.2. COMPATIBILIDAD CON PRODUCTOS APPLE NFC

Si se prevé a corto, medio o largo plazo la implementación de **ticketing móvil NFC en el iPhone o Apple Watch**, es necesario solicitar, además de la certificación RF, que los terminales gestionen el protocolo específico de Apple («ECP») para admitir el modo Apple Express (https://support.apple.com/en-us/HT212171). **Este proceso de certificación se realiza con Apple Inc.**

A la fecha, no existe una lista pública de terminales que admitan el modo Apple Express.

6.1.3. GESTIÓN DE LA OBSOLESCENCIA

Las primeras tarjetas Calypso emitidas en la década de 2000 usaban el protocolo Innovatron (también llamado B' o B prime). Hoy en día, el estándar Calypso se basa exclusivamente en el ISO/IEC 14443 (tipo A o B). Pero las tarjetas antiguas que utilizan el protocolo B' todavía están en campo porque las terminales a veces no se actualizan para utilizar los protocolos ISO/IEC 14443 tipo A o B.

Solo unos pocos modelos de terminales aún integran el protocolo B' además del protocolo estándar, lo que genera un costo significativamente mayor de este equipo en comparación con las terminales estándar. Por lo tanto, es necesario cuestionar la pertinencia de mantener el protocolo B' en lugar de reemplazar las tarjetas B' aún en circulación.

Por otro lado, la gran variedad de terminales que cumplen con el estándar ISO/IEC TS 24192 (antes llamado CEN/TS 16794) garantiza un precio óptimo para este equipo. Finalmente, el protocolo B' no permite la integración de Hoplink, ni el manejo de teléfonos inteligentes NFC (SE y HCE), ni la gestión de MaaS.

La gestión de las tarjetas B' existentes solo debe continuar si es imperativo, y solo en este caso se debe especificar un terminal que admita tanto el protocolo estándar como el B'.

6.2. REQUERIMIENTOS DE SOFTWARE

6.2.1. ESTRUCTURADO EN TRES CAPAS DE SOFTWARE

CNA ha definido una estructura de software de tres capas para garantizar la escalabilidad, la modularidad y la capacidad de la terminal para manejar todas las tarjetas Calypso certificadas. Estas tres capas se describen en el sitio web https://calypsonet.org/calypso-for-terminals/.

Cada capa de software tiene su propio documento de requisitos, escrito por CNA.

6.2.2. CAPA DEL LECTOR (SOFTWARE DEL LECTOR)

La capa de software encargada de los intercambios entre la tarjeta y el lector, denominada "Reader Layer", puede gestionar todo tipo de tarjetas y SAMs, sea cual sea su tecnología: Calypso, CIPURSE, MIFARE, etc. Esta capa de software no contiene ningún elemento específico de Calypso. La capa de software de la aplicación accede a ella a través de APIs de referencia (API de lector y API de tarjeta) definidas por CNA.

A la fecha, el cliente debe solicitar al oferente la presentación de la carta de registro del lector emitida por CNA, la cual certifica, con carácter declarativo, el cumplimiento de los requisitos descritos en el documento "Requisitos de la Capa del Lector", establecidos por CNA. A fines de 2023, una certificación de "Capa del lector" reemplazará a la declarativa.

6.2.3. CAPA CALYPSO (LIBRERÍA FUNCIONAL CALYPSO)

La capa de software "Calypso Layer" permite la gestión específica de tarjetas y SAMs Calypso en estricto cumplimiento con las especificaciones funcionales de este estándar. Esta capa corresponde a la biblioteca Calypso, la capa de software de la aplicación accede a ella a través de una API de referencia (Application Programmable Interface) definida por CNA.

A la fecha, el cliente deberá solicitar al oferente la presentación de la carta de registro de la biblioteca Calypso emitida por CNA, que acredite, con carácter declarativo[4], el cumplimiento de los requisitos descritos en el documento "Requisitos de la Capa Calypso". A finales de 2023, una certificación de "Capa Calypso" reemplazará a la declarativa.

La declaración es un simple documento de compromiso del fabricante para respetar los requisitos (Capa de lector o Capa Calypso). La certificación verifica tanto el respeto de los requisitos como la conformidad con las APIs de referencia definidas por CNA; existe así una garantía de interoperabilidad.

4 Es importante recordar que esta es una declaración hecha por los fabricantes en su honor y no el resultado de pruebas realizadas por un laboratorio independiente. Cuando exista la certificación correspondiente (fines de 2023), se deberá exigir.

6.2.4. CAPA DE TICKETING

La Capa de Ticketing es la aplicación de ticketing (reglas comerciales y tarifarias, control de acceso, etc.) que está presente en la terminal, o remota en un servidor central (sistemas ABT).

CNA ha publicado un documento llamado **"Ticketing Layer Requirements"**.

Es tanto un documento de requisitos como una recomendación para el uso de las APIs de referencia definidas por CNA. También contiene las mejores prácticas a seguir en la implementación y gestión de un sistema de ticketing Calypso.

El documento "Requisitos de la Capa de Ticketing" no requiere certificación porque las aplicaciones de ticketing son específicas para cada red. Corresponde a cada red pedir su respeto y uso.

6.2.5. SOFTWARE ABIERTO: ECLIPSE KEYPLE

CNA recomienda que el software de código abierto Eclipse Keyple se incluya en las licitaciones. Eclipse Keyple está libre de derechos (Eclipse Public License 2.0 (or EPL-2.0)).

La confianza en el software de código abierto crea una solución duradera, ya que garantiza que el potencial de evolución sea independiente de un proveedor específico, evita un monopolio y aumenta la competencia, especialmente en lo que respecta al costo. El uso de Keyple garantiza que la terminal podrá procesar todas las tarjetas Calypso certificadas, incluidas las más recientes.

Keyple implementa las APIs de referencia definidas por CNA para terminales Calypso y cumple con los requisitos de la Capa de Lector y la Capa Calypso.

Keyple se compone de dos aplicaciones de software cada una asociada a una capa específica:

- **Keyple Core** corresponde con la "Capa del Lector", aquí, la integración del hardware (lector) se realiza a través de un plugin.
- **Keyple Calypso** corresponde con la "Capa Calypso".

Si se utiliza Keyple Calypso, el oferente puede proporcionar la carta de registro de la biblioteca Keyple Calypso directamente.

En caso de utilizar Keyple Core, el oferente deberá presentar la carta de registro del lector, que acredite, con carácter declarativo, el cumplimiento de los requisitos descritos en el documento "Requisitos de la Capa del Lector". Esta carta de registro garantiza el cumplimiento del paquete "Hardware de terminal/Plugin de Keyple/Keyple Core".

Cuando esté disponible, la certificación reemplazará la carta de registro.

El uso de Eclipse Keyple, como software de código abierto, garantiza una total independencia entre el hardware y el software del terminal:

- Por lo tanto, es posible reemplazar un hardware por otro, manteniendo el mismo software (Keyple Core, Keyple Calypso y software de aplicación) y utilizando (o desarrollando) el Keyple Plugin ad hoc para el nuevo hardware.
- Es posible intervenir en el software de una determinada terminal, sin implicación alguna en el hardware, lo que evita problemas de propiedad para la solución global de hardware/software.

6.3. CERTIFICACIÓN Y DECLARACIÓN DE CONFORMIDAD

La siguiente tabla indica las certificaciones y/o declaraciones a ser requeridas, según el tipo de hardware, hasta que la certificación esté disponible.

Tipo de Hardware/Software	Certificación requerida	Carta de registro a ser requerida		Carta compromiso a ser requerida
	ISO/IEC TS 24192	Capa del lector	Capa Calypso	Capa de Ticketing
Hardware sin librería Calypso	√	√		
Hardware con librería Calypso	√	√	√	
Equipos que integran la aplicación de ticketing en red	√	√	√	√
Solo librería Calypso			√	
Solo aplicación de Ticketing				√

La lista de terminales y software que han sido declarados compatibles está disponible en https://calypsonet.org/calypso-certification/.

Cada capa debe ser compatible para que un dispositivo se **considere compatible.**

6.4. REQUERIMIENTOS DE TERMINALES PARA MÓDULOS DE SEGURIDAD

Dependiendo del terminal, puede ser necesario proporcionar ranuras para la integración de módulos de seguridad (SAM).

El número de ranuras depende del contexto, el tipo de terminal y el tipo de tarjeta Calypso que se utilizará.

Para todas las terminales, se recomienda proporcionar al menos dos ranuras, y preferiblemente cuatro, para posibles actualizaciones del sistema.

El formato actual del módulo de seguridad (SAM) es el formato SIM (ID-1/1FF) del cual el formato mini SIM (2FF) es desmontable. Para necesidades específicas, es posible obtener los formatos micro SIM (3FF) o nano SIM (4FF).
The number of slots depends on the context, the type of terminal and the type of Calypso card that will be used.

For all terminals, it is recommended to provide at least two slots, and preferably four, for possible system upgrades.

The current format of the security module (SAM) is the SIM format (ID-1/1FF) of which the mini SIM format (2FF) is detachable. For specific needs, it is possible to obtain the micro SIM (3FF), or nano SIM (4FF) formats.

6.5. TEXTO PARA LA CONVOCATORIA DE LICITACIÓN

Ver hoja de instrucciones n°3

HOJA DE INSTRUCCIONES N°1

ESPECIFICANDO TARJETAS CALYPSO EN UNA CONVOCATORIA DE LICITACIÓN

Mencionamos aquí solo los elementos de texto (en negro), que se insertarán en una licitación, en relación con la conformidad de las tarjetas Calypso, con comentarios explicativos (en cursiva). Todas las demás características, restricciones físicas, ergonómicas, específicas, requisitos adicionales deben agregarse para que el oferente responda.

En cuanto a las tarjetas Calypso, el cumplimiento de todas las normas de referencia ISO/IEC 14443, ISO/IEC 7816, ISO/IEC TS 24192 (o CEN/TS 16794) se garantiza simplemente refiriéndose a la obligación de certificación RF de la tarjeta, que es un primer requisito previo a la interoperabilidad, solicitando al oferente que presente el certificado de la tarjeta propuesta:

"La tarjeta deberá estar certificada según la última edición del ISO/IEC TS 24192 (o por defecto CEN/TS 16794). El oferente proporcionará el certificado de la tarjeta propuesta. Como recordatorio, el certificado proporcionado se relaciona con el producto terminado, así como será entregado, incluyendo el componente con su software, el inlay con antena y el cuerpo de la tarjeta, ensamblados. No puede ser un certificado emitido para un producto diferente, en caso de que alguno de estos elementos haya sido modificado con posterioridad a la certificación. Ni puede ser un certificado emitido por el proveedor del componente basado en una incrustación diferente".

El cumplimiento de las especificaciones funcionales Calypso, que es el segundo prerrequisito para la interoperabilidad, se garantiza haciendo referencia al requisito de certificación funcional Calypso, que requiere que el oferente presente el certificado para la tarjeta propuesta:

"La tarjeta deberá haber sido objeto de la certificación funcional Calypso. El oferente deberá presentar el certificado de la tarjeta que propone."

- ***Si la tarjeta es una tarjeta Calypso Prime, se debe especificar el modo solicitado: Regular, Extendido (recomendado como mínimo) o PKI si se elige una tarjeta Calypso Prime que implemente criptografía asimétrica.***
- ***Si se trata de una tarjeta Calypso Light o Calypso Basic, no es necesario especificar más.***

- Junio 2023 -

En cuanto a los aspectos de configuración y personalización, los elementos (descritos en el apartado 4.3) se incluirán en el texto de la licitación.
Para cada aplicación contenida en la tarjeta Calypso Prime (aplicación de la red local, Hoplink, AMC, ...):

"Las tarjetas proporcionadas deben respetar la aplicación **(mencionar el nombre de la aplicación)**:

- Usar el identificador de la aplicación de la red (también llamado AID o contenedor) estandarizado por ISO y referenciado por CNA: **(mencione el identificador elegido proporcionado por CNA tal cual, sin agregar ningún 00 adicional)**,

- Estar configurado en modo Regular / Extendido / PKI **(dependiendo de la necesidad, poner la aplicación elegida (Regular, Extendido o PKI), o mencionar** "emulación de Calypso revisión 2.4" **solo si hay necesidad de compatibilidad con una red antigua**).

- Use un conjunto de llaves TDES / AES dedicado, el conjunto de llaves se proporcionará a posteriori **(elija una de las dos criptografías de acuerdo con los conjuntos de llaves existentes en la red y las necesidades futuras y deje de usar los conjuntos de llaves DES o DESX)**.

- Utilice la estructura de archivos: **(elija una estructura de archivos reciente según la necesidad y evite estructuras de archivos antiguas en la medida de lo posible. Una lista de estructuras de archivos a las que hace referencia CNA está disponible en el documento "Registro de Estructuras de Archivos Calypso" (ref. 060709-CalypsoFiles).**"

CNA ofrece soporte para la redacción de sus licitaciones, en particular asistencia en la definición de la configuración y personalización de sus tarjetas Calypso.

También se propone una verificación de la configuración y personalización de las tarjetas Calypso entregadas por los fabricantes.

Para obtener más información, contáctenos: contact@calypsonet.org

- Junio 2023 -

“Las tarjetas suministradas deberán respetar las siguientes condiciones para la aplicación Hoplink **(si el cliente lo elige, ya que no tiene costo extra)**:

- Utilizar el identificador Hoplink.
- Estar configurado en modo Regular/Extendido **(dependiendo de la necesidad, poner la mención elegida entre estos dos modos).**
- Utilice el conjunto de llaves Hoplink TDES.
- Utilice la estructura de archivos Hoplink: estructura 0Ch.
- Inicialice el archivo Environment de acuerdo con la especificación Hoplink.
- Imprima el logotipo de Hoplink (consulte la carta gráfica de Hoplink).

Para una tarjeta Calypso Light:

“Las tarjetas suministradas deben:

- Utilizar el identificador de aplicación de red (también llamado AID o contenedor) estandarizado por ISO y referenciado por CNA, específico del operador del sistema de ticketing: **(mencionar el identificador elegido proporcionado por CNA tal cual, sin añadir ningún 00 adicional)**,
- Estar configurado de acuerdo con la estructura de archivos de Referencia / Clásica **(elija una de las dos según las estructuras existentes en la red y las necesidades futuras)**,
- Use un conjunto de llaves TDES dedicado para este producto; el conjunto de llaves se proporcionará después”.

Para una tarjeta Calypso Basic:

“Las tarjetas suministradas deben:

- Utilizar el identificador de aplicación (también llamado AID o contenedor) estandarizado por ISO y referenciado por CNA, específico del operador del sistema de ticketing: **(mencionar el identificador elegido proporcionado por CNA tal cual, sin añadir ningún 00 adicional)**,
- Utilice un conjunto de llaves TDES dedicadas para este producto; el conjunto de llaves se entregará posteriormente.”

- Junio 2023 -

HOJA DE INSTRUCCIONES N°2

ESPECIFICANDO UNA SOLUCIÓN CALYPSO DE TICKET MÓVIL NFC EN UNA CONVOCATORIA DE LICITACIÓN

Para la solución Calypso de ticketing móvil NFC en SE:

"La solución propuesta Calypso de ticketing móvil NFC en SE debe tener la capacidad de ejecutarse en cualquier teléfono inteligente NFC certificado por RF, ya sea según la certificación NFC Forum o según la última edición de la certificación ISO/IEC TS 24192 (o su versión CEN/TS 16794).

El applet debe cargarse solo en elementos seguros (SE) que hayan sido certificados funcionalmente por PayCert, una organización acreditada independiente, que cumple con Calypso. La lista de productos certificados está disponible en https://www.cna-paycert-certification.eu/card/calypso-prime-applet/. El proveedor se compromete a asegurarse periódicamente durante el período del servicio contratado que todos los teléfonos inteligentes NFC en los que se carga el applet hayan obtenido la certificación funcional Calypso del par Applet/SE. Si un par Applet/SE aún no está certificado, corresponderá al proveedor solicitar esta certificación.

En la fecha de la oferta, el proveedor facilitará la lista exhaustiva de teléfonos inteligentes NFC (proveedor y referencia de producto) elegibles para el servicio de Calypso ticketing móvil NFC que propone. El proveedor se compromete a mantener una vigilancia activa sobre los teléfonos inteligentes NFC elegibles para la solución Calypso SE y actualizará periódicamente esta lista durante la duración del servicio."

- Junio 2023 -

Para la solución Calypso HCE de ticketing móvil NFC:

"La solución propuesta Calypso HCE de ticketing móvil NFC debe tener la capacidad de ejecutarse en cualquier teléfono inteligente NFC en el sistema operativo (SO) Android que haya sido certificado RF, ya sea basado en la certificación NFC Forum o basado en la certificación ISO/IEC TS 24192 en su última edición (o su versión CEN/TS 16794).

El proveedor deberá aportar certificados que acrediten haber obtenido:

- Certificación funcional Calypso del SDK Calypso HCE (próximamente)
- Certificación de seguridad del SDK Calypso HCE.

La solución Calypso HCE de ticketing móvil NFC debe basarse en las especificaciones y lineamientos de Calypso HCE y cumplir con todos los requisitos. El proveedor debe proporcionar una declaración jurada de que su solución Calypso HCE de ticketing móvil NFC cumple con las especificaciones y lineamientos de Calypso HCE en su totalidad.

En la fecha de la oferta, el proveedor proporcionará la lista exhaustiva de teléfonos inteligentes NFC con sistema operativo (SO) Android elegibles para el servicio Calypso HCE de ticketing móvil NFC que propone. El proveedor se compromete a mantener una vigilancia activa sobre los teléfonos inteligentes NFC elegibles para la solución Calypso HCE y actualizará periódicamente esta lista durante la duración del servicio."

- Junio 2023 -

HOJA DE INSTRUCCIONES N°3

ESPECIFICANDO LAS TERMINALES CALYPSO EN UNA CONVOCATORIA DE LICITACIÓN

Los textos que se insertarán en una licitación para terminales de un sistema de ticketing solo se refieren a la correcta implementación del estándar Calypso. Es necesario un estricto respeto de los requisitos definidos por CNA y detallados en el capítulo 6 para garantizar la compatibilidad con todas las tarjetas certificadas y las soluciones de ticketing móvil NFC.

Como recordatorio y de acuerdo con el documento «Ticketing para MaaS: mejores prácticas para sistemas duraderos», el modelo de datos no debe integrarse en una licitación de terminales, sino que debe administrarse de forma independiente bajo el control del originador que asegura la propiedad.

Con referencia a la tabla del capítulo 6.3, el siguiente texto corresponde a los equipos que integran la aplicación de ticketing de la red.

"La terminal propuesta deberá haber recibido el certificado de conformidad con la norma ISO/IEC TS 24192 (antes denominada CEN/TS 16794), que el oferente adjuntará en su oferta. Se recuerda que este certificado de radiofrecuencia de la terminal deberá cubrir el producto terminado que incluye el hardware electrónico en su empaque final, con el software.

El software de la terminal se estructurará en tres capas de software para garantizar la escalabilidad, la modularidad y la capacidad de la terminal para manejar todas las tarjetas Calypso certificadas. Estas tres capas se describen en https://calypsonet.org/calypso-for-terminals/.

El oferente deberá demostrar que cumple con los requisitos de estas tres capas de software proporcionando:

- The registration letter of the terminal card reader, which attests, on a declarative basis, to compliance with the requirements described in the "Reader Layer Requirements".
- The registration letter for the Calypso library, which attests, on a declarative basis, to compliance with the requirements described in the "Calypso Layer Requirements" document.
- A letter of commitment, which attests, on a declarative basis, to compliance with the requirements, recommendations and good practices described in the "Ticketing Layer Requirements" document.

- Junio 2023 -

Los dos primeros párrafos serán sustituidos por los dos párrafos siguientes tan pronto como la certificación esté disponible y, por lo tanto, sustituirán este registro con carácter declarativo:

- El certificado del lector de tarjetas de la terminal, que acredita el cumplimiento de los requisitos descritos en el documento "Requisitos de la Capa del Lector".
- El certificado de la biblioteca Calypso, que acredita el cumplimiento de los requisitos descritos en el documento "Requisitos de la Capa Calypso".

La terminal propuesta utilizará las APIs de referencia definidas por CNA: API de Lector, API de Tarjeta y API Calypso.

La terminal propuesta utilizará preferentemente el software de código abierto Eclipse Keyple. Eclipse Keyple está libre de derechos (Eclipse Public License 2.0 (o EPL-2.0)).

Al utilizar el módulo Keyple Core, el oferente deberá presentar la Carta de Registro del Lector, que acredite, de manera declarativa, el cumplimiento de los requisitos descritos en el documento de "Requisitos de la Capa del Lector". **(Se sustituirá por el certificado en cuanto se disponga de la certificación correspondiente).**

Si se utiliza el módulo Keyple Calypso, el oferente deberá proporcionar directamente la carta de registro de la biblioteca Keyple Calypso existente **(que será reemplazada por el certificado tan pronto como esté disponible la certificación correspondiente)**.

La terminal propuesta deberá tener un mínimo de dos, y preferentemente cuatro, slots reservados para la integración de los Módulos de Acceso Seguro (SAM) en el siguiente formato: **(a elegir entre SIM (ID-1/1FF), mini SIM (2FF), micro SIM (3FF), nano SIM (4FF)).''**

- Junio 2023 -

DEFINICIONES
Y ACRÓNIMOS

- **ABT o Centrado en Servidor**

Sistema de ticketing basado en cuentas de usuario (ABT), también conocido como Centrado en IDs, Centrado en Servidor, Basado en la Nube, Basado en Servidor (nombre ISO) o Seguridad en Sistema (nombre ISO). Estos términos se refieren a sistemas en los que el procesamiento tiene lugar en el back-office y en los que las tarjetas se utilizan simplemente para identificar de forma segura a los titulares y vincularlos a las cuentas.

- **AES**

Estándar de cifrado avanzado (como se define en ISO/IEC 18033-3). Algoritmo criptográfico simétrico que utiliza datos y llaves de 128 bits.

- **AID**

Identificador de Aplicación (también llamado «contenedor»): valor único en una tarjeta, que permite identificar de forma inequívoca una aplicación de tarjeta, tal y como se define en el ISO/IEC 7816-4 e ISO/IEC 7816-5.

- **AMC**

Aplicación Ciudadana Multiservicio: estándar cuyo objetivo es permitir el uso de un único medio (tarjeta o aplicación móvil) para acceder a diferentes servicios (transporte, cultura, recolección de residuos, estacionamiento, turismo, etc.). En Francia, la referencia de las normas es la NF 99-508.

- **API para Terminal**

Una API (Application Programmable Interface) para una terminal define una interfaz común para la gestión de aplicaciones de software. A nivel de terminal de ticketing pueden existir varias APIs, desde la gestión del lector contactless hasta aplicaciones de ticketing de más alto nivel.

- **APPLET**

Aplicación que puede cargarse en un Elemento Seguro (generalmente asociado con el entorno Java).

- **Sistemas basados en tarjetas**

Los sistemas basados en tarjetas en el transporte público utilizan tarjetas inteligentes o teléfonos móviles habilitados con NFC para almacenar el valor del viaje, productos de viaje (por ejemplo, un pase mensual), derechos de descuento (por ejemplo, para estudiantes o tercera edad) y boletos. Los boletos pueden ser prepago o de pago por uso (check-in check-out o check-in solamente). Los boletos se almacenan para que puedan ser inspeccionados. En los sistemas basados en tarjetas, el software del cálculo tarifario y el de la aplicación se encuentra en los diferentes equipos en campo (validadores, máquinas de venta, lectores para inspección, ...), es decir, en el front-office del sistema de ticketing.

- **CEN**

CEN (Comité Europeo de Normalización) es una asociación de organismos nacionales de estandarización de 34 países Europeos. CEN es un organismo de estandarización reconocido por la Unión Europea como responsable del desarrollo y definición de normas a nivel europeo en colaboración con ISO.

- **Chip**

Un chip o componente electrónico, diseñado y fabricado por fabricantes especializados de silicio. El chip está integrado en las placas de las que forma parte y es el elemento inteligente que almacena y procesa los datos.

- **CNA**

Asociación de Redes Calypso (Calypso Networks Association).

- **Tarjeta sin contacto**

Un medio sin contacto, e.g., una tarjeta inteligente, una tarjeta java, un teléfono inteligente, una memoria USB con una interfaz sin contacto o cualquier otro medio sin contacto disponible para los clientes.

- **Modelo de datos**

El propósito del modelo de datos es describir cómo se codifica y almacena la información en la tarjeta y sus reglas de gestión. El modelo de datos constituye un lenguaje común que permite la interoperabilidad entre actores de movilidad que comparten el mismo medio de pago del cliente.

- **DES**

Algoritmo de cifrado que produce 8 bytes de datos a partir de 8 bytes de entrada, utilizando una llave de 7 bytes (como se define en ANSI X3.92-1981). También llamado “DES Simple”, ahora obsoleto.

- **DESX**

Algoritmo de cifrado que produce 8 bytes de datos a partir de 8 bytes de entrada, usando una llave de 15 bytes (como se define en "Cómo proteger DES contra la búsqueda exhaustiva de llaves" por Kilian & Rogaway), ahora en desuso.

- **Eclipse**

La Fundación Eclipse es una organización sin fines de lucro que supervisa el desarrollo del IDE de código abierto Eclipse y proyectos relacionados, y ayuda a cultivar una comunidad de código abierto y un ecosistema de productos y servicios complementarios en torno a Eclipse.

- **ECP**

Apple VAS "Enhanced Contactless Polling" (ECP) es una extensión propietaria de Apple de EMV nivel 1 e ISO/IEC 14443.

- **EMVCo**

EMVCo es un organismo técnico global que facilita la interoperabilidad y la aceptación de transacciones de pago seguras en todo el mundo mediante la gestión y evolución de las especificaciones EMV y los procesos de prueba asociados. EMVCo es propiedad colectiva de American Express, Discover, JCB, Mastercard, UnionPay y Visa.

- **HCE**

Emulación de tarjetas basadas en el host (Host Card Emulation). A fines de 2013, Google lanzó la versión 4.4 de Android, llamada "KitKat", que introduce varias funcionalidades para las aplicaciones de Android, entre las que se encuentra la API Host Card Emulation (o "HCE"), dedicada a facilitar y fomentar el uso de teléfonos NFC como "tarjetas contactless".

- **HOPLINK**

Hoplink es la aplicación interoperable de ticketing desarrollada por CNA. Algunos datos y nombres de archivos/campos pueden usar el acrónimo Triangle 2, el nombre anterior de Hoplink.

- **Interoperabilidad**

La interoperabilidad es la capacidad de un sistema o producto para trabajar con otros sistemas o productos sin requerir acciones adicionales por parte del viajero.

- **ISO/IEC**

ISO (Organización Internacional de Estandarización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos nacionales que son miembros de ISO e IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO e IEC, también participan en el trabajo.

- **NFC**

NFC (Near Field Communication) es una tecnología de comunicación inalámbrica cuya principal ventaja es, en este caso, su corto alcance (hasta 10 cm).

- **Software de código abierto**

El software de código abierto es un software cuyo código fuente es de libre acceso, usable y modificable, distribuido bajo una licencia aprobada por la Open Source Initiative y que garantiza el cumplimiento de sus reglas.

- **PKI**

Infraestructura de Llave Pública (Public Key Infraestructure): sistema que garantiza la seguridad de la información basado en criptografía asimétrica, que permite proteger los datos compartiendo solo llaves públicas.

- **SE**

Elemento Seguro (Secure Element): microprocesador seguro capaz de almacenar y operar software, especialmente aplicaciones ISO/IEC 7816-4.

- **SAM**

Módulo de Acceso Seguro (Secure Access Module): El módulo de seguridad autentica la tarjeta, el terminal y todos los datos intercambiados entre ellos. Normalmente es una tarjeta inteligente, pero dado que hoy en día los servicios suelen ser proporcionados por servidores remotos, también puede ser un componente de hardware integrado en un servidor (HSM).

- **TDES**

El algoritmo criptográfico simétrico está formado por tres operaciones DES sucesivas (como se define en ISO/IEC 18033-3), también llamado “Triple-DES” o “3DES”.

Calypso
Networks Association

www.calypsonet.org
contact@calypsonet.org
@calypso-networks-association
@calypso-networks-association

Suscríbase al boletín de CNA a través del formulario de contacto

Sede central:
Calypso Networks Association,
Rue Royale 76,
1000 Bruxelles, Belgium

Paris:
Calypso Networks Association,
2 rue de la Roquette, Escalier Avril,
75011 Paris, France