

GUIDA

alla predisposizione dei documenti di gara per acquisto dispositivi carte e NFC per soluzioni di ticketing e mobile ticketing basati su standard Calypso

Giugno 2023



Come predisporre la propria soluzione di ticketing grazie alla gara per l'acquisto di dispositivi

INDICE DEI CONTENUTI

1	PREMESSA	03
2	OBIETTIVI DEL DOCUMENTO	04
3	PRINCIPI GENERALI	05
4	PRINCIPALI REQUISITI PER CARTE CONTACTLESS	06
	4.1. REQUISITI SULLA RADIOFREQUENZA (RF) E RELATIVE CERTIFICAZIONI	07
	4.2. REQUISITI FUNZIONALI E DI CERTIFICAZIONE DI CALYPSO	08
	4.3. CONFIGURAZIONE DELLE CARTE	09
	4.4. TESTO DEL BANDO DI GARA.....	10
5	SPECIFICHE E REQUISITI PER MOBILE TICKETING VIA NFC	11
	5.1. SOLUZIONI CON SE E HCE.....	11
	5.2. REQUISITI PER LA SOLUZIONE SECURE ELEMENTS (SE)	12
	5.3. REQUISITI PER LA SOLUZIONE HCE	13
	5.4. TESTO DEL BANDO DI GARA.....	13
6	REQUISITI E SPECIFICHE PER TERMINALI E SOFTWARE DI TICKETING	14
	6.1. REQUISITI E CERTIFICAZIONE PER LA RADIO FREQUENZA (RF).....	14
	6.1.1. COMPATIBILITA' CON SOLUZIONI APPLICATIVE DI PAGAMENTO BASATE SULLA TECNOLOGIA CONTACTLESS EMV.....	15
	6.1.2. COMPATIBILITA' CON PRODOTTI NFC SU DISPOSITIVI APPLE.....	15
	6.1.3. GESTIONE DELLA OBSOLESCENZA DEI PRODOTTI.....	15
	6.2. REQUISITI SOFTWARE	16
	6.2.1. L'ARCHITETTURA SOFTWARE SU TRE LIVELLI	16
	6.2.2. LIVELLO READER (SOFTWARE DEL LETTORE).....	16
	6.2.3. LIVELLO CALYPSO LAYER (LIBRERIA FUNZIONALITA' CALYPSO)	16
	6.2.4. LIVELLO APPLICATIVO TICKETING.....	17
	6.2.5. OPEN SOFTWARE: ECLIPSE KEYPLE	17
	6.3. CERTIFICAZIONE E DICHIARAZIONE DI CONFORMITA'.....	18
	6.4. REQUISITI PER I TERMINALI CON MODULO DI SICUREZZA.....	19
	6.5. TESTO DEL BANDO DI GARA.....	19
	ALLEGATO	20
	COME REFERENZIARE LE SPECIFICHE CALYPSO ALL'INTERNO DI UN DOCUMENTO DI GARA.....	20
	REFERENZIARE LE SPECIFICHE CALYPSO PER MOBILE NFC ALL'INTERNO DELLA DOCUMENTAZIONE DI GARA.....	23
	REFERENZIARE LE SPECIFICHE DI CALYPSO PER I TERMINALI ALL'INTERNO DELLA DOCUMENTAZIONE DI GARA... ..	25
	DEFINIZIONI E ACRONIMI	27

1 PREMESSA

I sistemi di bigliettazione rappresentano un tema altamente strategico per le autorità e gli operatori dei trasporti poiché trasformano la politica della mobilità per il loro territorio e garantendo anche la possibilità di ulteriori ricavi. Questi sistemi sono progettati per essere sostenibili e flessibili, in particolare per quanto riguarda le modifiche tariffarie, le estensioni della rete e l'implementazione di schemi di interoperabilità.

Per garantire la continuità di un sistema di bigliettazione è necessario essere in grado di integrare apparecchiature, carte e software di diversi produttori durante il suo ciclo di vita. In effetti, il fornitore originale del sistema potrebbe avere uno scarso interesse nel fornire manutenzioni evolutive a un prezzo ragionevole. Avere più fornitori potenziali evita una situazione di monopolio, che potrebbe comportare, per effettuare un aggiornamento, costi eccessivi o addirittura l'impossibilità stessa.

Va inoltre protetta la compatibilità e l'interoperabilità tecnica tra diversi fornitori, e per questo è importante passare da una logica di prodotto (fisso e generalmente proprietario nella sostanza) a una logica di standard, purché aperti e multisource. Il cliente deve poi possedere dei requisiti per il rispetto di tali norme e standard, la cui prova deve essere fornita dal fornitore attraverso la certificazione dei propri prodotti.

Lo standard Calypso soddisfa i requisiti stabiliti dagli organismi internazionali per la designazione di standard aperti: "Uno standard si dice aperto quando è **reso disponibile a tutti, sviluppato, mantenuto**

e gestito in un processo collaborativo e consensuale. Uno standard aperto facilita l'interoperabilità e lo scambio di dati tra diversi prodotti o servizi ed è destinato ad essere adottato su vasta scala"¹.

Calypso è stato ideato per essere sviluppato, mantenuto e gestito dalle autorità e dagli operatori dei trasporti che insieme formano la Calypso Networks Association (CNA).

CNA è un'associazione senza fini di lucro che opera con l'obiettivo di garantire scalabilità, interoperabilità e indipendenza dai fornitori per tutti gli utenti. Calypso è l'unico standard di biglietteria multi-fornitore a tutti i livelli, compresi i componenti elettronici delle carte.

CNA rappresenta un fenomeno di vera e propria resilienza, in tempi di carenza di componenti. Fornisce al mondo industriale specifiche di riferimento e un processo di certificazione per attestare la conformità del prodotto. È lo standard adottato da molte reti in tutto il mondo. Molti fornitori di diverse origini offrono quindi i prodotti Calypso in uno schema multi-source che ha successo da oltre 20 anni. Questa vera concorrenza garantisce che all'acquirente verranno offerti i prodotti Calypso al giusto prezzo.

La sfida delle gare sul ticketing, al di là della funzione di acquisto dell'hardware, è quella di garantire la compatibilità tra i media (carte contactless, smartphone NFC, ...) e i terminali di biglietteria (validatori, dispositivi di vendita e controllo, chioschi, ...) già installati e appena acquistati. Senza questo prerequisito di compatibilità, viene meno la possibilità implementare schemi interoperabili.



Il documento "Ticketing for MaaS: migliori pratiche per sistemi durevoli" presenta tutte le migliori pratiche da seguire quando si specifica un sistema di ticketing. In particolare, ricorda che il modello dati non deve essere integrato in un sistema di biglietteria o terminale di gara, ma deve essere gestito in autonomia, sotto il controllo del cliente, che deve garantire la proprietà del modello dati.

2 OBIETTIVI DEL DOCUMENTO

Lo scopo di questo documento è quello di delineare i principali requisiti per la **predisposizione di un bando di gara per carte contactless, sistemi e terminali di mobile ticketing NFC garantendone compatibilità e scalabilità.**

Una gara pubblica deve consentire una concorrenza aperta e leale per tutti i produttori. Questo documento è stato scritto in conformità con i principi dei codici francesi sugli appalti pubblici e può quindi essere utilizzato come guida per la redazione dei bandi di gara.

Questo documento è scritto da CNA, libero da copyright e può essere utilizzato liberamente in tutto o in parte.



CNA offre supporto e consulenza per la predisposizione del vostro bando di gara, in particolare assistenza nella definizione della configurazione e personalizzazione delle vostre carte Calypso.

Viene inoltre proposta una verifica della configurazione e della personalizzazione delle carte Calypso fornite dai produttori. Per ulteriori informazioni, contattateci all'indirizzo mail:

contact@calypsonet.org

3 PRINCIPI GENERALI

I principi generali di seguito riportati sono dettagliati nei capitoli dedicati rispettivamente alle carte, agli smartphone NFC e ai terminali. Sistematicamente si fa riferimento a tutte le norme e gli standard applicabili al settore.

- richiedere prodotti certificati, con relativa prova di conformità alle norme o, in assenza di certificazione, una dichiarazione di conformità alle norme applicabili al settore;
- fare sempre riferimento a standard condivisi e a best practice (quando disponibili e pubbliche) a livello nazionale;
- preferibilmente, richiedere l'integrazione di Calypso Hoplink all'interno delle carte Calypso Prime e relativo modulo di sicurezza. Questo significa avere garanzia di una soluzione già predisposta per servizi successivi di interoperabilità;
- non fare mai riferimento a nomi commerciali di prodotto o di specifici costruttori / fornitori;
- non citare specifiche, soluzioni o tecnologie che sono dichiaratamente obsolete.

4 PRINCIPALI REQUISITI PER CARTE CONTACTLESS

Un sistema Calypso correttamente implementato può accettare tutte le carte contactless certificate Calypso. Calypso Networks Association ha creato tre prodotti:

Calypso® **PRIME** Calypso® **LIGHT** Calypso® **basic**

Tutti hanno gli stessi meccanismi di sicurezza e possono essere gestiti dallo stesso software terminale, garantendo compatibilità e facile integrazione.

- | Calypso® **PRIME** Unisce in un'unica carta le funzionalità di trasporto e multiapplicazione/multiservizio. Consente inoltre la gestione di contratti di ticketing multiplo e l'interoperabilità tra reti, anche su scala internazionale. Calypso Prime consente inoltre l'autenticazione della carta senza richiedere moduli di sicurezza aggiuntivi (SAM) nella sua versione PKI.
- | Calypso® **LIGHT** È una versione più adatta agli utenti occasionali, con lo stesso livello di sicurezza di Calypso Prime. Può essere emessa su carta o plastica ISO e sulla stessa carta possono coesistere due contratti di trasporto dello stesso operatore. È inoltre un prodotto specificatamente adattato alle soluzioni di ticketing ABT (Account Based Ticketing).
- | Calypso® **basic** Disponibile dal 2022, è un biglietto cartaceo a contratto unico, contactless, ricaricabile, adatto a viaggi singoli.

Nell'ambito di una gara il committente deve richiedere che le carte siano certificate sia a livello di radiofrequenza (hardware/hardware) che a livello funzionale di Calypso (software/software), come descritto nei successivi capitoli. L'acquisto di carte non certificate comporta un serio rischio di incompatibilità del terminale con la carta.

4.1. REQUISITI SULLA RADIOFREQUENZA (RF) E RELATIVE CERTIFICAZIONI

Il primo requisito è che **la carta contactless** deve essere conforme all'ultima versione di **ISO/IEC TS 24192 (ex CEN/TS 16794)**, che è l'applicazione di trasporto della norma **ISO/IEC 14443**.

Il rispetto di questo standard garantisce che la carta sia interoperabile con i terminali conformi a questo standard. E anche con gli smartphone NFC che rispettano i requisiti del Forum NFC (<https://nfc-forum.org/>), soprattutto se utilizzati per ricaricare un biglietto sulla carta contactless.

La conformità a questo standard deve essere dimostrata tramite uno specifico emesso da un organismo di certificazione approvato dalla Smart Ticketing Alliance, che ha sviluppato e implementato il programma di certificazione RF (<https://www.smart-ticketing.org/certification/>) per molti anni.

Il processo di certificazione RF è effettuato da Paycert (<https://www.cna-paycert-certification.eu/rf-interface-2>), organismo di certificazione indipendente, che è l'unico attualmente autorizzato a rilasciare la certificazione RF come previsto dal programma Smart Ticketing Alliance.

L'elenco attuale delle carte certificate ISO/IEC TS 24192 (CEN/TS 16794) da PayCert è pubblico e può essere trovato sul sito web di PayCert: <https://www.cna-paycert-certification.eu/rf-interface/picc/>.



IMPORTANTE: La certificazione RF di una scheda riguarda il prodotto finito, compreso il componente con il relativo software, l'inserito con antenna e il corpo della scheda, assemblato.

Sconsigliamo vivamente di ordinare carte utilizzando il protocollo B' (chiamato anche Innovatron). Questo protocollo è obsoleto perché non esiste alcun prodotto certificato conforme a questo protocollo. Ricordiamo che il protocollo B' non consente l'integrazione di Hoplink. Non consente né il trattamento degli smartphone NFC (Secure Element e Host Card Emulation) né l'implementazione dell'interoperabilità. Se la rete opera solo in B', si consiglia di ordinare carte dual-mode (e ISO 14443 A|B) per facilitare la migrazione quando sarà il momento.

4.2. REQUISITI FUNZIONALI E DI CERTIFICAZIONE DI CALYPSO

CNA ha delineato sia le specifiche di riferimento a cui deve conformarsi qualsiasi carta Calypso (Prime, Light, Basic) sia uno schema di certificazione per garantire tale conformità. Tale certificazione è gestita dall'organismo di certificazione PayCert, unico soggetto autorizzato a rilasciare certificati. Esiste una certificazione dedicata per ognuna delle tre carte (Prime, Light, Basic).

Da notare che Calypso Prime può essere configurato in tre versioni. Nel documenti di gara dovrà essere specificato quale configurazione è richiesta:

- Modalità normale, (già rev 3.1); questa modalità include le funzioni base di Calypso Prime con crittografia TDES e DESX.
- Modalità estesa (già rev 3.2), con crittografia AES e crittografia dati opzionale oltre alle funzionalità della modalità normale.
- Modalità PKI (già rev 3.3), che aggiunge la crittografia PKI asimmetrica alla modalità estesa, consentendo l'autenticazione della carta senza un modulo di sicurezza (SAM) nel terminale.

Cosa prevedere all'interno **di un bando di gara**

- Per le carte Calypso Prime è richiesto il rispetto della certificazione Calypso Prime, pari al livello (o superiore) della versione (normale, estesa o PKI) richiesta. Si consiglia di richiedere almeno la conformità alla certificazione in modalità estesa. Se aveste bisogno dell'autenticazione della carta senza modulo di sicurezza, dovrete richiedere la conformità alla modalità PKI
- Per le carte Calypso Light, è richiesto il rispetto della certificazione Calypso Light.
- Per le carte Calypso Basic, è richiesto il rispetto della certificazione Calypso Basic.

La lista completa delle carte Calypso certificate è riportata al seguente indirizzo web: <https://www.cna-paycert-certification.eu/card/>

4.3. CONFIGURAZIONE DELLE CARTE

Per tutte le carte Calypso (**Prime, Light e Basic**), la configurazione richiesta deve rispettare le seguenti regole:

- Utilizzare un identificatore dell'applicazione (chiamato anche "AID" o "contenitore") standardizzato dall'ISO e referenziato dalla CNA, specifico per l'operatore del sistema di bigliettazione. Non utilizzare identificatori generici come "1TIC.ICA" per i quali non è garantita l'unicità e che sono incompatibili con le soluzioni di biglietteria NFC su smartphone. CNA gestisce un elenco di valori Calypso AID registrati. Per richiedere un AID Calypso registrato, contattare il supporto tecnico Calypso: support@calypsonet.org.
- Utilizza l'identificatore fornito dalla CNA così com'è, senza aggiungere ulteriori 00

Per le carte **Calypso Prime**, la configurazione deve rispettare anche le seguenti regole e raccomandazioni:

- Configurare sempre le applicazioni in modalità Normale, Estesa o PKI, secondo necessità (e non in Calypso Revisione 2.4 o versione precedente).
- Integrare l'applicazione Hoplink (consigliato perché nella maggior parte dei casi non prevede costi aggiuntivi e consentirà la futura implementazione di uno schema di interoperabilità).
- Utilizzare le strutture di file più recenti ed evitare il più possibile le vecchie strutture di file. Un elenco delle strutture di file a cui fa riferimento la CNA è disponibile nel documento "[Calypso File Structure Registry](#)" document (rif. 060709-CalypsoFiles).
- Utilizzare set di chiavi dedicati per ciascuna applicazione con crittografia recente: **TDES, AES o PKI** e non utilizzare più crittografie obsolete, come DES.
- Se è necessaria la compatibilità con una rete più vecchia (Calypso revisione 2.4), è necessario richiedere una carta Prime certificata che emuli la revisione 2.4.

Per le carte **Calypso Light** la configurazione deve rispettare anche le seguenti regole:

- Scegli una delle due strutture di file consentite (Riferimento o Classico), a seconda delle strutture esistenti e delle tue esigenze future.
- Utilizzare preferibilmente un set di chiavi dedicato per questo prodotto. Le carte Light utilizzano solo la crittografia TDES.

Per le carte **Calypso Basic** la configurazione deve inoltre:

- Utilizzare un set di chiavi dedicato per questo prodotto. Le carte Basic utilizzano solo la crittografia TDES.

Attenzione: non confondere la **struttura del file** di una carta Calypso con la **struttura del contratto**, detta anche "istanziamento". Queste due strutture non fanno riferimento alla stessa definizione. La struttura dei file definisce l'organizzazione dei file nella scheda. La struttura del contratto, "istanziamento", viene utilizzata per codificare i biglietti di trasporto.



CNA offre supporto per la redazione del vostro bando di gara, in particolare assistenza nella definizione della configurazione e personalizzazione delle vostre carte Calypso. Viene inoltre proposta una verifica della configurazione e personalizzazione delle carte Calypso consegnate dai produttori.

Per ulteriori informazioni, contattateci: contact@calypsonet.org

4.4. TESTO DEL BANDO DI GARA

Vedi foglio illustrativo n°1.

5 SPECIFICHE E REQUISITI PER MOBILE TICKETING VIA NFC

5.1. SOLUZIONI CON SE E HCE

Il **mobile ticketing NFC** è la tecnologia che consente l'utilizzo di uno smartphone NFC per acquistare e/o convalidare biglietti (tramite un lettore) o per emulare una carta contactless.

In questo documento ci si concentra sulla capacità dello smartphone NFC di emulare una carta contactless. Il mobile ticketing NFC è disponibile in diverse modalità a seconda che la sicurezza si basi o meno su un elemento di sicurezza hardware nello smartphone NFC:

- Il mobile ticketing NFC **SE** (Secure Element) utilizza un componente microprocessore identico a quello presente in una carta, e quindi ha lo stesso livello di sicurezza: Common Criteria EAL4+ almeno per la SE. Gli SE sono presenti nei modelli più recenti di smartphone NFC di diversi produttori, tra cui Samsung e Apple.

CNA fornisce un'applet Calypso standardizzata (applicazione software) da caricare nell'SE e quindi emulare completamente una carta Calypso Prime.

Questa soluzione ha il vantaggio di non richiedere alcuna evoluzione dei terminali di bigliettazione esistenti, ma solo pochi parametri di configurazione, a condizione che il sistema sia conforme almeno a Calypso Prime revisione 3, modalità "regular".

- Il mobile ticketing NFC **HCE** (Host Card Emulation) non si basa sull'uso di un SE memorizzato nello smartphone NFC, ma sulla sicurezza integrata nel software. È compatibile con tutti gli smartphone Android NFC. Per compensare la minore sicurezza innata, dovuta al mancato utilizzo di un Secure Element per la protezione dei dati sensibili, un meccanismo (chiamato tokenizzazione) aggiorna regolarmente le chiavi segrete dell'applicazione Calypso HCE memorizzate nello smartphone NFC, limitando il rischio di frode.

Come per la soluzione SE, il sistema deve essere conforme almeno alla revisione 3 di Calypso Prime. Richiede una integrazione all'interno del software dei terminali di validazione dei ticket per implementare le misure di sicurezza specifiche della soluzione HCE

5.2. REQUISITI PER LA SOLUZIONE SECURE ELEMENTS (SE)

La soluzione SE può essere acquistata direttamente da un fornitore dedicato o indirettamente tramite il tuo integratore del servizio di ticketing. In entrambi i casi il cliente dovrà richiedere al fornitore di garantire:

- La soluzione di mobile ticketing NFC può funzionare con qualsiasi smartphone NFC certificato RF, sia basato sulla certificazione NFC Forum che sulla certificazione ISO/IEC TS 24192 ultima edizione (o la sua versione CEN/TS 16794)
- L'applet viene caricata esclusivamente nel Secure Elements (SE), che sono stati certificati funzionalmente come conformi al software Calypso "Applet/SE". PayCert, un'organizzazione accreditata indipendente, gestisce questa certificazione e l'elenco dei prodotti certificati è disponibile su <https://www.cna-paycert-certification.eu/card/calypso-prime-applet/>. Se un abbinamento "Applet/SE" non è già certificato, spetta al fornitore richiedere tale certificazione.



Il rispetto dei requisiti del terminale, descritti più avanti in questo documento, garantisce il rispetto dei requisiti specifici per le soluzioni mobili NFC.

Le soluzioni mobili NFC, siano esse basate su applet in SE o HCE, sono commercializzate da fornitori dedicati che hanno la responsabilità di installare e inizializzare l'applicazione Calypso nello smartphone NFC.

5.3. REQUISITI PER LA SOLUZIONE HCE

La soluzione HCE può provenire direttamente da un fornitore dedicato o indirettamente tramite il tuo integratore del servizio di ticketing. In entrambi i casi il cliente deve garantire che vengano presi in considerazione i seguenti requisiti:

- Il fornitore garantisce che la sua soluzione di mobile ticketing NFC può funzionare con qualsiasi smartphone Android NFC certificato RF, sia sulla base della certificazione NFC Forum, sia sulla base della certificazione ISO/IEC TS 24192 ultima edizione (o la sua certificazione CEN /TS 16794 versione).
- La certificazione funzionale **di conformità alle specifiche Calypso HCE** sarà richiesta **non appena** sarà disponibile (fine 2023).
- **La certificazione di sicurezza Calypso HCE** si basa su uno standard all'avanguardia per la resistenza all'hacking dei dati degli smartphone. CNA rilascia questo certificato con l'assistenza di Internet of Trust (<https://www.internetoftrust.com/>) in quanto organismo di certificazione indipendente. Un elenco dei fornitori che hanno superato questa certificazione è disponibile su calypsonet.org. Si consiglia vivamente di richiedere tale certificazione, anche se attualmente non è richiesta dalla CNA.
- Rispetto delle specifiche [Calypso HCE e delle linee guida stabilite](#) da CNA in merito ai requisiti applicabili all'infrastruttura del sistema di bigliettazione.



La soluzione Calypso HCE è puramente basata su software e non può fare affidamento sulla classificazione di sicurezza di un componente elettronico nello smartphone NFC. Per garantire un livello di sicurezza conforme allo standard Calypso, CNA ha implementato una serie di misure di sicurezza specifiche per la soluzione HCE, reperibili **nelle specifiche e nelle linee guida**.

Tutti i fornitori di Calypso HCE sono contrattualmente impegnati, in quanto licenziatari, a rispettare queste specifiche e linee guida.

5.4. TESTO DEL BANDO DI GARA

Vedi foglio illustrativo n°2.

6 REQUISITI E SPECIFICHE PER TERMINALI E SOFTWARE DI TICKETING

Ai fini del presente documento, un terminale è un dispositivo di vendita, validazione e controllo. Il software di ticketing è ciò che consente una transazione di ticketing, che nell'ecosistema CNA include il software di lettura, la libreria Calypso e l'applicazione di ticketing, indipendentemente dal fatto che siano nel terminale o presenti su un server centrale.

PROMEMORIA: per garantire l'interoperabilità tra più elementi dell'infrastruttura di bigliettazione, in particolare tessere e lettori, è fondamentale che ciascun componente che partecipa alla interazione sia certificato sia a livello di radiofrequenza che a livello funzionale.

6.1. REQUISITI E CERTIFICAZIONE PER LA RADIO FREQUENZA (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**. Il primo requisito è che la **radiofrequenza (RF) del terminale contactless** sia conforme all'ultima versione di **ISO/IEC TS 24192** (precedentemente denominata **CEN/TS 16794**), che è l'applicazione di trasporto della norma **ISO/IEC 14443**.

La conformità a questo standard garantisce l'interoperabilità del terminale con le carte anch'esse conformi a questo standard. Stesso requisito per gli smartphone NFC conformi ai requisiti del Forum NFC, soprattutto se utilizzati per emulare una carta di trasporto contactless.

La conformità a questo standard deve essere dimostrata ottenendo la certificazione da un organismo di certificazione approvato dalla Smart Ticketing Alliance, che ha sviluppato e implementato il programma di certificazione della radiofrequenza (<https://www.smart-ticketing.org/certification/>) per diversi anni.

Il processo di certificazione RF è effettuato da Paycert (<https://www.cna-paycert-certification.eu/rf-interface-2>), organismo di certificazione indipendente e unico organismo attualmente autorizzato a rilasciare la certificazione RF secondo la normativa prevista dal Programma Smart Ticketing Alliance.

L'elenco attuale dei terminali certificati ISO/IEC TS 24192 (CEN/TS 16794) è pubblico e può essere trovato sul sito web PayCert all'indirizzo <https://www.cna-paycert-certification.eu/rf-interface/pcd/>.



IMPORTANTE: La certificazione RF di un terminale prevede:

- Il prodotto finito, compreso l'hardware con relativa elettronica nella sua confezione finale, con il software
- Un sottoinsieme del prodotto finito, nella misura in cui questo sottoinsieme è stato integrato nel prodotto finito secondo le raccomandazioni del produttore, che garantiscono la non perdita della certificazione.

6.1.1. COMPATIBILITA' CON SOLUZIONI APPLICATIVE DI PAGAMENTO BASATE SULLA TECNOLOGIA CONTACTLESS EMV

Se si prevede l'implementazione di un servizio di **Open Payment** nel breve, medio o lungo termine, è opportuno richiedere, oltre alla certificazione RF, che i terminali siano certificati EMVCo livello 1 (L1). **Questo processo di certificazione viene eseguito con EMVCo** (<https://www.emvco.com/>).

L'elenco aggiornato dei terminali certificati EMVCo L1 è pubblico e può essere trovato sul sito EMVCo all'indirizzo: <https://www.emvco.com/approved-registered/approved-products/>

6.1.2. COMPATIBILITA' CON PRODOTTI NFC SU DISPOSITIVI APPLE

Se si prevede l'implementazione del **mobile ticketing NFC su iPhone o Apple Watch** nel breve, medio o lungo termine è necessario richiedere, oltre alla certificazione RF, che i terminali gestiscano il protocollo specifico Apple («ECP»), al fine di supportare la modalità Apple Express (<https://support.apple.com/en-us/HT212171>). **Questo processo di certificazione viene eseguito con Apple Inc.**

Ad oggi non esiste un elenco pubblico di terminali che supportano la modalità Apple Express.

6.1.3. GESTIONE DELLA OBSOLESCENZA DEI PRODOTTI

Le prime carte Calypso emesse negli anni 2000 utilizzavano il protocollo Innovatron (chiamato anche B' o B prime). Oggi lo standard Calypso si basa esclusivamente sulla norma ISO/IES 14443 (tipo A o B). Ma le vecchie carte che utilizzano il protocollo B' sono ancora sul campo perché i terminali a volte non vengono aggiornati per utilizzare i protocolli ISO/IES 14443 di tipo A o B.

Solo pochi modelli di terminali integrano ancora il protocollo B' oltre al protocollo standard, il che comporta un costo notevolmente più elevato di queste apparecchiature rispetto ai terminali standard.

È necessario quindi interrogarsi sull'importanza di mantenere il protocollo B' piuttosto che di sostituire le carte B' ancora in circolazione. D'altra parte, l'ampia varietà di terminali conformi allo standard ISO/IEC TS 24192 (precedentemente chiamato CEN/TS 16794) garantisce un prezzo ottimale per questa apparecchiatura. Infine, il protocollo B' non consente l'integrazione di Hoplink, né la gestione degli smartphone NFC (SE e HCE), né la gestione del MaaS.

La gestione delle carte B' esistenti dovrebbe continuare solo se indispensabile e solo in questo caso dovrebbe essere specificato un terminale che supporti sia il protocollo standard che quello B'.

6.2. REQUISITI SOFTWARE

6.2.1. L'ARCHITETTURA SOFTWARE SU TRE LIVELLI

CNA ha definito una struttura software a tre livelli per garantire scalabilità, modularità e capacità del terminale di gestire tutte le carte Calypso certificate. Questi tre livelli sono descritti sul sito web <https://calypsonet.org/calypso-for-terminals/>.

Ogni livello software ha il proprio documento di requisiti, scritto da CNA.

6.2.2. LIVELLO READER (SOFTWARE DEL LETTORE)

Lo strato software preposto agli scambi tra la carta e il lettore, denominato "Reader Layer", può gestire tutti i tipi di carte e SAM, qualunque sia la loro tecnologia: Calypso, CIPURSE, MIFARE, ecc. Questo strato software non contiene alcun Calypso elementi specifici. Il livello software applicativo vi accede tramite API di riferimento (Reader API & Card API) definite da CNA.

Ad oggi, il committente dovrà chiedere all'offerente di presentare la lettera di registrazione del lettore rilasciata da CNA, che attesta, in via dichiarativa, il rispetto dei requisiti descritti nel documento "Reader Layer Requisiti", predisposto da CNA. Alla fine del 2023 una certificazione "Reader Layer" sostituirà quella dichiarativa.

6.2.3. LIVELLO CALYPSO LAYER (LIBRERIA FUNZIONALITA' CALYPSO)

Il livello software "Calypso Layer" consente la gestione di carte e SAM specifici di Calypso nel rigoroso rispetto delle specifiche funzionali di questo standard. Questo livello corrisponde alla libreria Calypso, il livello software applicativo vi accede tramite una API (Application Programmable Interface) di riferimento definita dalla CNA.

Ad oggi, il committente dovrà chiedere al concorrente di presentare la lettera di registrazione della libreria Calypso rilasciata da CNA, che attesta, in via dichiarativa⁴, il rispetto dei requisiti descritti nel documento "Calypso Layer Requisiti". Alla fine del 2023 una certificazione "Calypso Layer" sostituirà quella dichiarativa.⁴



La dichiarazione è un semplice documento di impegno da parte del produttore a rispettare i requisiti (strato Reader o Calypso). La certificazione verifica sia il rispetto dei requisiti che la conformità agli API di riferimento definiti dalla CNA; fornendo quindi una garanzia di interoperabilità.

⁴ È importante ricordare che si tratta di una dichiarazione impegnativa e liberatoria rilasciata dai produttori e non del risultato di test effettuati da un laboratorio indipendente. Quando sarà in vigore la certificazione corrispondente (fine 2023) sarà richiesta e ritenuta obbligatoria.

6.2.4. LIVELLO APPLICATIVO TICKETING

Il Ticketing Layer è l'applicazione (regole tariffarie e commerciali, gestione degli accessi, ecc.) presente nel terminale o remota, in un server centrale (sistemi ABT).

CNA ha pubblicato un documento denominato "[Requisiti Layer Ticketing](#)".

Si tratta sia di un documento di requisiti che di una raccomandazione per l'utilizzo delle API di riferimento definite dalla CNA. Contiene inoltre le "best practice" nell'implementazione e nella gestione di un sistema di ticketing Calypso

Il documento "Requisiti Layer Ticketings" non richiede certificazione perché le applicazioni di ticketing sono specifiche per ciascuna rete. Spetta a ciascuna rete chiederne il rispetto e l'utilizzo.

6.2.5. OPEN SOFTWARE: ECLIPSE KEYPLE

CNA raccomanda di inserire nei bandi di gara il software open source Eclipse Keyple. [Eclipse Keyple](#) è esente da diritti di proprietà intellettuale ([Eclipse Public License 2.0 \(or EPL-2.0\)](#)).

La dipendenza dal software open source crea una soluzione duratura, poiché garantisce che il potenziale di evoluzione sia indipendente da un fornitore specifico, impedisce un monopolio e aumenta la concorrenza, soprattutto per quanto riguarda i costi. L'utilizzo di Keyple garantisce che il terminale sarà in grado di elaborare tutte le carte Calypso certificate, comprese quelle più recenti.

Keyple implementa le API di riferimento definite da CNA per i terminali Calypso e rispetta i requisiti Reader Layer e Calypso Layer.

Keyple è composto da due applicazioni software ciascuna associata ad uno specifico livello:

- **Keyple Core** corrisponde al "livello Lettore", dove l'integrazione dell'hardware (lettore) avviene tramite un plugin.
- **Keyple Calypso** corrisponde allo "strato Calypso".

Se viene utilizzato Keyple Calypso, l'offerente può fornire direttamente la lettera di registrazione della libreria Keyple Calypso.

In caso di utilizzo di Keyple Core, l'offerente dovrà inviare la lettera di registrazione del lettore, che attesta, in via dichiarativa, il rispetto dei requisiti descritti nel documento "Requisiti Reader Layer". Questa lettera di registrazione garantisce la conformità del pacchetto "hardware terminale/Keyple Plugin/Keyple Core".

Quando disponibile, la certificazione sostituirà la lettera di registrazione.



L'utilizzo di Eclipse Keyple, in quanto software open source, garantisce una totale indipendenza tra l'hardware e il software del terminale:

- È quindi possibile sostituire un hardware con un altro, mantenendo lo stesso software (Keyple Core, Keyple Calypso e software applicativo) e utilizzando (o sviluppando) il Keyple Plugin ad hoc per il nuovo hardware.
- È possibile intervenire sul software di un determinato terminale, senza alcun intervento sull'hardware, evitando così eventuali problemi proprietari per la soluzione hardware/software globale.

6.3. CERTIFICAZIONE E DICHIARAZIONE DI CONFORMITA'

Nella tabella seguente sono indicate le certificazioni e/o dichiarazioni da richiedere, a seconda della tipologia di hardware, fino al rilascio della certificazione.

Tipo di Hardware/Software	Certificazione richiesta	Lettera di registrazione da richiedere		Impegno lettera di impegno da richiesta
	ISO/IEC TS 24192	Reader layer	Calypso layer	Ticketing layer
Hardware senza libreria Calypso	✓	✓		
Hardware con libreria Calypso	✓	✓	✓	
Apparecchiature che integrano l'applicazione di biglietteria in rete	✓	✓	✓	✓
Solo biblioteca Calypso			✓	
Solo applicazione di biglietteria				✓

L'elenco dei terminali e dei software dichiarati conformi è disponibile all'indirizzo <https://calypsonet.org/calypso-certification/>.

Affinché un dispositivo possa essere considerato conforme lo devono essere tutti i livelli sopra descritti

6.4. REQUISITI PER I TERMINALI CON MODULO DI SICUREZZA

A seconda del terminale, può essere necessario prevedere degli slot per l'integrazione dei moduli Security (SAM).

Il numero di slot dipende dal contesto, dal tipo di terminale e dal tipo di carta Calypso che verrà utilizzata.

Per tutti i terminali si consiglia di prevedere almeno due slot, preferibilmente quattro, per eventuali aggiornamenti del sistema.

Il formato attuale del modulo di sicurezza (SAM) è il formato SIM (ID-1/1FF), di cui il formato mini SIM (2FF) è staccabile.

Per specifiche esigenze è possibile ottenere il formato micro SIM (3FF), o nano SIM (4FF). Depending on the terminal, it may be necessary to provide slots for the integration of security modules (SAMs).

6.5. TESTO DEL BANDO DI GARA

Vedi foglio illustrativo n°3.

COME REFERENZIARE LE SPECIFICHE CALYPSO ALL'INTERNO DI UN DOCUMENTO DI GARA

Riportiamo qui solo gli elementi testuali (in nero), da inserire in un bando di gara, riguardanti la conformità delle carte Calypso, con commenti esplicativi (in corsivo). Tutte le altre caratteristiche, fisiche, ergonomiche, vincoli specifici, requisiti aggiuntivi devono essere aggiunti affinché l'offerente possa rispondere.

Per quanto riguarda le carte Calypso, la conformità a tutti gli standard di riferimento ISO/IEC 14443, ISO/IEC 7816, ISO/IEC TS 24192 (o CEN/TS 16794) è assicurata semplicemente facendo riferimento all'obbligo di certificazione RF della carta, che è un primo prerequisito di interoperabilità, chiedendo all'offerente di presentare il certificato della carta proposta:

“La carta deve essere certificata ISO/IEC TS 24192 ultima edizione (o per impostazione predefinita CEN/TS 16794). L'offerente fornirà il certificato della carta proposta. Si ricorda che il certificato fornito si riferisce al prodotto finito così come sarà essere consegnato, compreso il componente con il relativo software, l'inlay con antenna e il corpo della scheda, assemblati. Non può trattarsi di un certificato emesso per un prodotto diverso, nel caso in cui uno di questi elementi sia stato modificato dopo la certificazione. Né può essere un certificato rilasciato dal fornitore del componente sulla base di un inserto diverso.”

Il rispetto delle specifiche funzionali di Calypso, che costituisce il secondo prerequisito per l'interoperabilità, è assicurato facendo riferimento al requisito di certificazione funzionale di Calypso, richiedendo all'offerente di presentare il certificato per la carta proposta:

“La carta deve essere sottoposta alla certificazione funzionale Calypso. L'offerente dovrà presentare il certificato per la carta che propone.”

- *Se la carta è una carta Calypso Prime, è necessario specificare la modalità richiesta: Regular, Extended (consigliata come minimo) o PKI se si sceglie una carta Calypso Prime che implementa la crittografia asimmetrica.*
- *Se si tratta di una carta Calypso Light o Calypso Basic, non sono necessarie ulteriori specifiche.*

Per quanto riguarda gli aspetti di configurazione e personalizzazione, gli elementi (descritti al paragrafo 4.3) sono da inserire nel testo di gara.

Per ciascuna applicazione contenuta nella carta Calypso Prime (applicazione di rete locale, Hoplink, AMC, ...):

“Le carte fornite devono essere conformi all'applicazione **(indicare il nome della applicazione)**:

- Utilizzare l'identificatore dell'applicazione di rete (chiamato anche AID o contenitore) standardizzato dall'ISO e referenziato dalla CNA: **(menzionare l'identificatore scelto fornito dalla CNA così com'è, senza aggiungere ulteriori 00)**,
- Essere configurato in modalità Regular / Estesa / PKI **(a seconda della necessità, inserire l'applicazione scelta (Regular, Estesa o PKI), oppure menzionare “emulazione Calypso revisione 2.4” solo se è necessaria la compatibilità con una vecchia rete)**.
- Utilizzare un set di chiavi TDES / AES dedicato, il set di chiavi verrà fornito a posteriori **(scegliere una delle due crittografie in base ai set di chiavi esistenti nella rete e alle esigenze future e non utilizzare più set di chiavi DES o DESX)**.
- Utilizzare la struttura dei file: **(scegliere una struttura di file recente a seconda delle necessità ed evitare il più possibile le vecchie strutture di file. Un elenco delle strutture di file a cui fa riferimento CNA è disponibile nel documento "Calypso File Structure Registry" (rif. 060709-CalypsoFiles)."**

CNA offre supporto per la redazione delle vostre gare, in particolare assistenza nella definizione della configurazione e personalizzazione delle vostre carte Calypso.

Viene inoltre proposta una verifica della configurazione e personalizzazione delle carte

Calypso consegnate dai produttori. Per ulteriori informazioni, contattateci: contact@calypsonet.org

“Le carte fornite devono rispettare le seguenti condizioni per l'applicazione Hoplink **(se il cliente lo sceglie, in quanto non vi è alcun costo aggiuntivo)**:

- Utilizza l'identificatore Hoplink.
- Essere configurato in modalità Normale/Estesa **(a seconda della necessità, inserire la configurazione scelta tra queste due modalità)**.
- Utilizzare il set di chiavi Hoplink TDES.
- Utilizza la struttura del file Hoplink: struttura 0Ch.
- Inizializza il file di configurazione ambiente secondo le specifiche Hoplink.
- Stampa il logo Hoplink (vedi carta grafica Hoplink)."

Per una carta Calypso Light:

“Le carte fornite devono:

- Utilizzare l'identificatore dell'applicazione di rete (chiamato anche AID o contenitore) standardizzato dall'ISO e referenziato dalla CNA, specifico per l'operatore del sistema di biglietteria: **(menzionare l'identificativo scelto fornito dalla CNA così com'è, senza aggiungere ulteriori 00)**,
- Essere configurato secondo la struttura file Reference/Classic **(scegliere una delle due a seconda delle strutture esistenti nella rete e delle esigenze future)**,
- Utilizzare un set di chiavi TDES dedicato per questo prodotto; il set di chiavi verrà fornito successivamente.”

Per una carta Calypso Basic:

“Le carte fornite devono:

- Utilizzare l'identificatore dell'applicazione (chiamato anche AID o contenitore) standardizzato dall'ISO e referenziato dalla CNA, specifico per l'operatore del sistema di bigliettazione **(menzionare l'identificativo scelto fornito dalla CNA così com'è, senza aggiungere ulteriori 00)**,
- Utilizzare un set di chiavi TDES dedicate per questo prodotto; successivamente verrà fornito un set completo di chiavi.”

REFERENZIARE LE SPECIFICHE CALYPSO PER MOBILE NFC ALL'INTERNO DELLA DOCUMENTAZIONE DI GARA

Per la soluzione di biglietteria mobile Calypso NFC su SE:

“La soluzione di mobile ticketing Calypso NFC proposta su SE deve essere in grado di funzionare su qualsiasi smartphone NFC certificato RF, basato sulla certificazione NFC Forum o sulla certificazione ISO/IEC TS 24192 dell'ultima edizione (o la sua versione CEN/TS 16794).

L'applet deve essere caricato solo in uno dei Secure Elements (SE) che sono stati certificati funzionalmente da PayCert, organizzazione indipendente accreditata, come conformi a Calypso. L'elenco dei prodotti certificati è disponibile su <https://www.cna-paycert-certification.eu/card/calypso-prime-applet/>. Il fornitore si impegna a garantire regolarmente durante il periodo di servizio contrattualizzato che tutti gli smartphone NFC su cui è caricata l'applet abbiano ottenuto la certificazione funzionale Calypso dell'insieme Applet/SE. Se una insieme Applet/SE non è già certificato, sarà cura del fornitore richiedere tale certificazione.

Alla data dell'offerta, il fornitore fornirà l'elenco esaustivo degli smartphone NFC (fornitore e riferimento prodotto) idonei al servizio di mobile ticketing Calypso NFC da lui proposto. Il fornitore si impegna a tenere sotto controllo gli smartphone NFC idonei alla soluzione Calypso SE e ad aggiornare regolarmente questo elenco per tutta la durata del servizio.”

Per la soluzione di ticketing mobile Calypso NFC HCE:

“La soluzione di biglietteria mobile Calypso NFC HCE proposta deve essere in grado di funzionare su qualsiasi smartphone NFC con sistema operativo Android certificato RF, sia in base alla certificazione NFC Forum che in base alla certificazione ISO/IEC TS 24192 dell'ultima edizione (o la sua versione CEN/TS 16794).

Il fornitore deve fornire certificati comprovanti di aver ottenuto:

- Certificazione funzionale Calypso dell'SDK Calypso HCE (in arrivo)
- Certificazione di sicurezza Calypso HCE SDK.

La soluzione di ticketing mobile Calypso NFC HCE deve essere basata sulle specifiche e linee guida Calypso HCE e rispettare tutti i requisiti. Il fornitore deve fornire una dichiarazione giurata attestante che la sua soluzione di ticketing mobile Calypso NFC HCE è conforme alle specifiche e alle linee guida Calypso HCE nella loro interezza.

Alla data dell'offerta, il fornitore fornirà l'elenco esaustivo degli smartphone NFC con sistema operativo Android (OS) idonei al servizio di mobile ticketing Calypso NFC HCE da lui proposto. Il fornitore si impegna a tenere sotto controllo attivo gli smartphone NFC idonei alla soluzione Calypso HCE e aggiornerà regolarmente questo elenco per tutta la durata del servizio.”

REFERENZIARE LE SPECIFICHE DI CALYPSO PER I TERMINALI ALL'INTERNO DELLA DOCUMENTAZIONE DI GARA

I testi da inserire in un bando di gara per terminali di un sistema di ticketing riguardano esclusivamente la corretta implementazione dello standard Calypso. Per garantire la compatibilità con tutte le carte certificate e le soluzioni di mobile ticketing NFC è necessario un rigoroso rispetto dei requisiti definiti dalla CNA e dettagliati nel capitolo 6.

Si ricorda che, in conformità con il documento «Ticketing for MaaS: best practices for Sustainable Systems», il modello dati non deve essere previsto all'interno di una gara terminali ma gestito in modo indipendente sotto il controllo del progettista che ne garantisce la proprietà.

Con riferimento alla tabella del capitolo 6.3, il testo seguente corrisponde agli apparati di linea che integrano l'applicazione di ticketing.

“Il terminale proposto dovrà aver ricevuto il certificato di conformità alla norma ISO/IEC TS 24192 (precedentemente denominata CEN/TS 16794), che l'offerente allegnerà alla propria offerta. Si ricorda che il certificato di radiofrequenza del terminale deve coprire il prodotto finito che comprende l'hardware elettronico nel suo imballo finale, compreso il software.

Il software del terminale sarà strutturato in tre livelli software al fine di garantire scalabilità, modularità e capacità del terminale di gestire tutte le carte Calypso certificate. Questi tre livelli sono descritti su <https://calypsonet.org/calypso-for-terminals/>.

L'offerente dovrà dimostrare la propria conformità ai requisiti di questi tre livelli software fornendo:

- La lettera di registrazione del lettore di carte terminali, che attesta, a titolo dichiarativo, il rispetto dei requisiti descritti nei "[Requisiti del livello lettore](#)".
- La lettera di registrazione alla libreria Calypso, che attesta, in via dichiarativa, il rispetto dei requisiti descritti nel documento "[Calypso Layer Requisiti](#)".
- Una lettera di impegno, che attesta, su base dichiarativa, il rispetto dei requisiti, delle raccomandazioni e delle buone pratiche descritte nel documento "Requisiti del livello di ticketing "[Requisiti del livello di ticketing](#)".

I primi due paragrafi saranno sostituiti dai due commi seguenti non appena la certificazione sarà disponibile e sostituiranno quindi tale registrazione su base dichiarativa:

- Il certificato del lettore di carte terminali, che attesta il rispetto dei requisiti descritti nel documento "Requisiti del livello lettore".
- Il certificato della libreria Calypso, che attesta il rispetto dei requisiti descritti nel documento "Calypso Layer Requisiti".

Il terminale proposto utilizzerà le API di riferimento definite da CNA: Reader API, Card API e Calypso API.

Il terminale proposto utilizzerà preferibilmente il software open source Eclipse Keyple. Eclipse Keyple è privo di diritti (Eclipse Public License 2.0 (o EPL-2.0)).

In caso di utilizzo del modulo Keyple Core, l'offerente sarà tenuto a presentare la Reader Registration Letter, che attesta, in via dichiarativa, il rispetto dei requisiti descritti nel "Documento Reader Layer Requisiti". **(Da sostituire con il certificato non appena sarà disponibile la certificazione corrispondente).**

Se viene utilizzato il modulo Keyple Calypso, l'offerente dovrà fornire direttamente la lettera di registrazione della biblioteca Keyple Calypso esistente **(che sarà sostituita dal certificato non appena sarà disponibile la certificazione corrispondente).**

Il terminale proposto dovrà avere un minimo di due, e preferibilmente quattro, slot riservati per Security Module Integration (SAM) nel seguente formato: **(scegliere tra SIM (ID-1/1FF), mini SIM (2FF), micro SIM (3FF), nano SIM (4FF)).**

DEFINIZIONI E ACRONIMI

- **ABT o Ticketing basato su server**

Account-based Ticketing system (ABT), noto anche come incentrato sull'ID, incentrato sul server, basato sul cloud, basato sul server (nome ISO) o Security in System (nome ISO). Questi termini si riferiscono a sistemi in cui l'elaborazione avviene nel back-office e in cui le carte vengono utilizzate semplicemente per identificare in modo sicuro i titolari e collegarli ai conti.

- **AES**

Advanced Encryption Standard (come definito in ISO/IEC 18033-3). Cifratura simmetrica che utilizza un algoritmo a 128bit di chiave e dati.

- **AID**

Application Identifier (chiamato anche «container»): valore univoco in una carta, che consente di identificare in modo inequivocabile un'applicazione della carta, come definito nelle norme ISO/IEC 7816-4 e ISO/IEC 7816-5.

- **AMC**

Multi-service Citizen Application: uno standard il cui obiettivo è consentire l'utilizzo di un unico mezzo (carta o applicazione mobile) per accedere a diversi servizi (trasporti, cultura, smaltimento rifiuti, parcheggi, turismo, ecc.). In Francia, il riferimento delle norme è NF 99-508.

- **API per Terminal**

Una API (Application Programmable Interface) per un terminale definisce un'interfaccia comune per la gestione dell'applicazione software. A livello di terminale di ticketing possono esistere diverse API, dalla gestione del lettore contactless alle applicazioni di ticketing di livello superiore.

- **APPLET**

Applicazione che può essere caricata all'interno del Secure Element (di solito legata ad un ambiente Java).

- **Card base Ticketing (Sistema di ticketing basato su valori memorizzati su carte)**

Nei trasporti pubblici utilizzare le smart card o i telefoni cellulari abilitati NFC per memorizzare il valore del viaggio, i prodotti di viaggio (ad esempio un abbonamento mensile), i diritti di sconto (ad esempio per studenti o anziani) e i biglietti. I biglietti possono essere prepagati o Pay-As-You-Go (check-in check-out o solo check-in). I biglietti vengono memorizzati in modo che possano essere ispezionati. Nei sistemi card-based il calcolo tariffario ed i software applicativi sono localizzati nelle diverse apparecchiature di campo (validatori, macchine di vendita, lettori di ispezione, ...), ovvero nel front office del sistema di bigliettazione.

- **CEN**

CEN (European Committee for Standardisation) è un'associazione degli organismi nazionali di normalizzazione di 34 paesi europei. Il CEN è un organismo di normazione riconosciuto dall'Unione Europea come responsabile dello sviluppo e della definizione di norme a livello europeo in collaborazione con l'ISO.

- **Chip**

Un chip o componente elettronico, progettato e prodotto da produttori specializzati di silicio. Il chip è integrato nelle schede di cui fa parte ed è l'elemento intelligente che memorizza ed elabora i dati.

- **CNA**

Calypso Networks Association

- **Contactless card**

Un dispositivo senza contatto, ad es. una smart card, una Java Card, uno smartphone, una chiavetta USB con interfaccia contactless o qualsiasi altro mezzo contactless a disposizione dei clienti.

- **Modello dati**

Lo scopo del modello dati è descrivere come le informazioni vengono codificate e archiviate nella carta e le sue regole di gestione. Il modello di dati costituisce un linguaggio comune che consente l'interoperabilità tra gli attori della mobilità che condividono lo stesso mezzo

- **DES**

Algoritmo di cifratura che consente di ottenere 8 bytes di dato utilizzando una chiave di 7 bytes (come definito nello standard ANSI X3.92-1981). Definito anche "Simple DES", ora superato.

- **DESX**

Algoritmo di cifratura che consente di ottenere 8 bytes di dato utilizzando una chiave di 7 bytes (come definito nello standard ANSI X3.92-1981). Definito anche "Simple DES", ora superato.

- **Eclipse**

La Fondazione Eclipse è un'organizzazione no-profit che supervisiona lo sviluppo dell'IDE open source Eclipse e dei progetti correlati e aiuta a coltivare una comunità open source e un ecosistema di prodotti e servizi complementari attorno a Eclipse.

- **ECP**

Apple VAS Enhanced Contactless Polling (ECP), è una estensione “proprietaria” di Apple delle specifiche EMV level 1 e ISO/IEC 14443.

- **EMVCo**

EMVCo è un organismo tecnico globale che facilita l'interoperabilità e l'accettazione di transazioni di pagamento sicure in tutto il mondo gestendo e mantenendo le specifiche EMV e i processi di test associati. I principali soci di EMVCo sono American Express, Discover, JCB, Mastercard, UnionPay e Visa.

- **HCE**

Host Card Emulation. Alla fine del 2013, Google ha rilasciato la versione Android 4.4, chiamata “KitKat”, introducendo diverse funzionalità per le applicazioni Android, tra cui l'Host Card Emulation API (o “HCE”), dedicata a facilitare e favorire l'utilizzo dei telefoni NFC come “carte contactless”.

- **HOPLINK**

Hoplink è l'applicazione di ticketing interoperabile sviluppata da CNA. Alcuni dati e nomi di file/campi possono utilizzare l'acronimo Triangle 2, il nome precedente di Hoplink.

- **Interoperabilità**

L'interoperabilità è la capacità di un sistema o prodotto di funzionare con altri sistemi o prodotti senza richiedere azioni aggiuntive da parte del viaggiatore.

- **ISO/IEC**

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) costituiscono il sistema dedicato alla standardizzazione a livello mondiale. Gli organismi nazionali membri di ISO e IEC partecipano allo sviluppo di standard internazionali attraverso comitati tecnici istituiti dalle rispettive organizzazioni per occuparsi di particolari campi di attività tecnica. I comitati tecnici ISO e IEC collaborano in campi di reciproco interesse. Ai lavori prendono parte anche altre organizzazioni internazionali, governative e non governative, in collegamento con ISO e IEC.

- **NFC**

NFC (Near Field Communication) è una tecnologia di comunicazione senza fili il cui principale vantaggio è, in questo caso, il suo corto raggio (fino a 10 cm).

- **Open Source Software**

Open Source software è un software il cui codice sorgente è liberamente accessibile, utilizzabile e modificabile, distribuito sotto una licenza approvata dall'Open Source Initiative e che garantisce il rispetto delle sue regole.

- **PKI**

Public Key Infrastructure: sistema di sicurezza delle informazioni basato sulla crittografia asimmetrica, che consente di proteggere i dati condividendo solo le chiavi pubbliche.

- **SE**

Secure Element: microprocessore sicuro in grado di memorizzare ed eseguire software, in particolari applicazioni conformi agli standard ISO/IEC 7816-4.

- **SAM**

Il modulo di sicurezza autentica la carta, il terminale e tutti i dati scambiati tra loro. Normalmente si tratta di una smart card, ma poiché oggi i servizi vengono spesso forniti da server remoti, può anche essere un componente hardware integrato in un server (HSM).


- **TDES**


L'algoritmo crittografico simmetrico è composto da tre operazioni DES successive (come definito nella norma ISO/IEC 18033-3), chiamate anche "Triple-DES" o "3DES".

Calypso

Networks Association

 www.calypsonet.org

 contact@calypsonet.org

 [@calypso-networks-association](https://www.linkedin.com/company/calypso-networks-association)

 [@calypso-networks-association](https://www.youtube.com/channel/UC...)

Iscriviti alla newsletter CNA tramite il [modulo di contatto](#)

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

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