Tecnologie
Telematiche
Trasporti
Traffico
Torino

(allegato n. 1)

Sistema di qualificazione 5t srl
Periodo 2015-2018

Specifica tecnica della smartcard

INDICE DEL DOCUMENTO

1. Introduzione 3
1.1 Scopo del documento 4
1.2 Normativa e documenti di riferimento 4
1.3 Glossario 5
2. Requisiti tecnici 6
2.1.1 Requisiti fisici e meccanici 6
2.1.2 Requisiti elettrici 6
2.1.3 Protocolli di comunicazione 6
2.1.4 Struttura del file system 7
2.1.5 Lista dei File presenti sotto Master File 7
2.1.6 Lista dei File presenti sotto DF utilizzata dal sistema BIP 7
2.1.7 Lista dei File utilizzati per la gestione del Credito Trasporti 8
2.1.8 Lista dei File utilizzati per contratti di Servizi Aggiuntivi (partizione sempre presente) .. 8
2.1.9 Tabella nomi DF 8
2.2 Circuito di appartenenza 8
2.2.1 Introduzione 8
2.2.2 Startup Information 9
2.2.3 Codifica circuito appartenenza 9
2.3 Chiavi di sicurezza presenti sulla carta 9
2.4 Caricamento delle chiavi di sicurezza 9
2.5 Mascheratura BIP 10
2.5.1 Introduzione 10
2.5.2 Condizioni di accesso ai file 11
2.5.3 Codice seriale carta 12
3. Credito Trasporti (Stored Value) 13
4. Caratteristiche costruttive 14
4.1 Durata della carta 14
5. Certificazione delle smartcard 15
5.1 Processo di certificazione 15
5.1.1 Test di compatibilità elettromagnetica 15
5.1.2 Test meccanici 17
5.1.3 Risultati 17
5.1.4 Test del S.O. Calypso e della mascheratura BIP 17

1. Introduzione

La Regione Piemonte ha avviato il progetto “Biglietto Integrato Piemonte” (BIP) per rilanciare il sistema di Trasporto Pubblico del Piemonte migliorandone l’accessibilità, assicurandone la conoscenza, la gestione e la promozione del TPL, realizzando azioni di infomobilità e certificando quantità e qualità del servizio reso (www.bip.piemonte.it).

Il BIP coinvolge attualmente più di 50 operatori di trasporto pubblico su gomma (3.400 veicoli) e TRENITALIA (400 stazioni ferroviarie) ed è attivo nelle provincie di :

- Biella
- Cuneo
- Novara
- Torino
- Verbano Cusio Ossola

I residenti nella regione sono in grado di accedere in modo semplice, immediato e sicuro a diversi servizi già attivi grazie all’utilizzo di una unica smartcard.

La smartcard a microprocessore RFID full contactless aderente allo standard ISO 14443-B e con una struttura dati afferente alla tecnologia Calypso, è pensata infatti come una carta multi-servizio, che oltre a permettere l’accesso alla rete del trasporto pubblico regionale consente di utilizzare , ad esempio, i servizi di bike sharing, di car sharing, ed in un prossimo futuro l’accesso ai parcheggi in struttura ed il pagamento della sosta a raso sui parcometri.

Il progetto BIP adotta un titolo di viaggio a deconto contenente un monte unità di viaggio prepagate denominato "Credito Trasporti".

Inoltre la struttura dati BIP è integrata all’interno di altre smartcard quali ad esempio, la carta regionale della cultura e dei giovani Pyou, la card multifunzione degli studenti degli Atenei Piemontesi, la carta fidelity e finanziaria di TRENITALIA denominata Carta*FRECCIA*.

5T è il Gestore Tecnologico del sistema ed è l’unico soggetto autorizzato all’acquisto delle smartcard BIP su scala regionale, in tale ambito ne sono state approvvigionate nel periodo 2009-2015, più di **un milione**.

Il prodotto oggetto di qualificazione dovrà quindi rispondere alle linee guida deliberate descritte nella presente specifica tecnica.

Tutti gli elementi funzionali, tecnici, procedurali, di sicurezza, d’interfaccia e di affidabilità e disponibilità descritti nel presente documento, sono da intendersi come il livello minimo di prestazione che deve essere garantito dalla smartcard proposta dalle Società/ATI partecipanti al Sistema di qualificazione.

1.1 Scopo del documento

Questo documento ha l'obiettivo di descrivere le specifiche tecniche della carta a microprocessore adottata del progetto BIP che dovrà essere qualificata.

In particolare verranno descritti:

- I requisiti fisici, meccanici ed elettrici
- Il protocollo di comunicazione a basso livello tra carta e lettore di carte.
- L'organizzazione logica dei file contenuti nella carta ovvero il *file system*.
- Le componenti di sicurezza, che consentono di:
  - effettuare le operazioni di validazione dei titoli di viaggio,
  - effettuare le operazioni di vendita e rinnovo e ricarica dei titoli di viaggio,
  - attivare/emettere/aggiornare i titoli di viaggio,
  - incrementare e decrementare il Credito Trasporti,
  - utilizzare la seconda area di memoria in autonomia da parte di enti terzi autorizzati

In questo documento non verrà specificata la descrizione dei comandi APDU (Application Protocol Data Unit) delle specifiche Calypso, per i quali si rimanda alla documentazione specifica del consorzio Calypso (www.calypsonet-asso.org).

1.2 Normativa e documenti di riferimento

La tipologia di smartcard oggetto di fornitura deve essere conforme a quanto definito nelle norme e nei documenti di seguito elencati:

1. Calypso Specification Rev.3 - Portable Object Application Version 3.1;
2. Norme ISO 14443 parti da 1 a 4;
3. Norme ISO 7816 parte 1
4. Norme EN 1545 per la definizione del modello dati (per quanto applicabile).

1.3 Glossario

- AFI: Application Family Information.
- APDU: Application Protocol Data Unit , set di comandi di una smartcard a microprocessore per la lettura e la scrittura del file system, di verifica di accesso nonchè di autenticazione reciproca (carta e terminale) e dei dati scambiati.
- ATQ: Answer To Request, comando inviato dal PICC in risposta al REQ del PCD (protocollo ISO 14443 parte 3)
- ATQB: Answer To Request of Type B (dove Type B si riferisce al Type of PICC ovvero alla smartcard).
- ADF: Application DF
- CNA: *Calypso Network Association*
- DF: Dedicated File, equivale ad una directory di file ovvero può contenere più EF file.
- EF: Elementary File, file contentenenti dati. Esistono principalmente tre tipi di file EF: lineari, ciclici e contatori.
- EP: Electronic Purse, borsellino elettronico.
- MF: Master File: la directory radice del file system. Può contenere DF e EF file.
- PCD: Proximity Coupling Device, ovvero il lettore di smart card.
- PICC: Proximity Integrated Circuit Cards, ovvero la smart card.
- PVC: cloruro di polivinile, materiale plastico, utilizzato come supporto fisico del microprocessore e dell'antenna presenti nelle smart card.
- REQ: Request comando inviato dal PCD al PICC (protocollo ISO 14443 parte 3)
- REQB: Request Command, Type B
- RFID: Radio Frequency Identification, ovvero identificazione a radiofrequenza. Con questo termine si indicano quelle tecnologie che consentono il riconoscimento a distanza di oggetti, animali e persone sfruttando le onde radio.
- SAM : Secure Access Module
- SBE: Sistema di bigliettazione elettronico.
- TdV : Titolo di Viaggio
- WUP: Wake up comando inviato dal PCD al PICC (protocollo ISO 14443 parte 3).
- WUPB: Wake-Up Command, Type B

2. Requisiti tecnici

2.1.1 *Requisiti fisici e meccanici*

Le dimensioni fisiche delle carte dovranno essere conformi alle specifiche ISO 7816 Parte 1 in particolare il formato indicato con la sigla ID1 di dimensioni LxHxP 85,60mmx53,98mmx0,76mm.

Il materiale costruttivo della carta dovrà essere di tipo plastico (PVC, PET o equivalenti), nel caso sia utilizzato un differente supporto fisico dovrà essere fornita opportuna garanzia sulla qualità e sulla sua durata temporale. La rigidità meccanica dovrà essere conforme a quanto indicato nella stessa normativa.

Le carte dovranno essere conformi alle normative di resistenza allo stress meccanico (torsione, flessione) indicate dalle ISO 10373.

2.1.2 *Requisiti elettrici*

Si utilizzeranno smart card "**full contactless**".

Per quanto riguarda le caratteristiche in radiofrequenza si fa riferimento alle normative ISO 14443 parte 1 e 2.

2.1.3 *Protocolli di comunicazione*

Per quanto concerne il protocollo contactless, secondo quanto indicato dalla specifica ISO 14443 parte 3, le carte dovranno rispondere inviando il loro ATQB a tutti i comandi di REQB o WUPB inviati da un accoppiatore aventi il seguente valore del parametro AFI:

- AFI=00hex – nessuna preferenza, tutte le carte in campo devono rispondere.

La risposta ATQB che la carta dovrà inviare alla ricezione del comando di REQB o WUPB dovrà contenere i seguenti parametri relativi al protocollo (Protocol Info):

- **Protocol Type e TR2**, indica la tipologia di protocollo, i valori ammessi sono 1, 3, 5 e 7 che indica che il protocollo è pienamente conforme alle normative ISO 14443 compresa la parte 4;
- **Max_Frame_Size,** indica la lunghezza massima ammissibile di ogni pacchetto dati in trasmissione, saranno ammessi valori 07hex (frame di lunghezza 128byte) oppure 08hex (frame di lunghezza 256 byte);
- **Bit_Rate_Capability,** indica le velocità di protocollo ammesse dalla carta. L'accoppiatore ha facoltà di scegliere, in base ai valori dichiarati, velocità di *bit rate* superiori a quella di default, circa 106Kbps. Le velocità di trasferimento (*bit rate)* ammesse sono indicate nella tabella riportata di seguito (tabella 7.9.4.6 delle ISO14443-3). I valori massimi ammissibili del parametro Bit_Rate_Capability saranno:
    - Bit_Rate_Capability=B3hex, fino a 424Kbps in entrambe le direzioni.

7.9.4.6 Bit_Rate_capability

Table 19 — Bit rates supported by the PICC

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	PICC supports only 106 kbit/s in both directions
1	x	x	x	0	x	x	x	Same bit rate from PCD to PICC and from PICC to PCD compulsory
x	x	x	1	0	x	x	x	PICC to PCD, 1etu = 64 / fc, bit rate supported is 212 kbit/s
x	x	1	x	0	x	x	x	PICC to PCD, 1etu = 32 / fc, bit rate supported is 424 kbit/s
x	1	x	x	0	x	x	x	PICC to PCD, 1etu = 16 / fc, bit rate supported is 847 kbit/s
x	x	x	x	0	x	x	1	PCD to PICC, 1etu = 64 / fc, bit rate supported is 212 kbit/s
x	x	x	x	0	x	1	x	PCD to PICC, 1etu = 32 / fc, bit rate supported is 424 kbit/s
x	x	x	x	0	1	x	x	PCD to PICC, 1etu = 16 / fc, bit rate supported is 847 kbit/s
Other values (with b4 = 1) are RFU.								

2.1.4 *Struttura del file system*

Il file system minimo richiesto è formato dai file indicati di seguito.

Nella lista sono indicati soltanto i file utilizzati dall'applicazione BIP e non i file di sistema che contengono oggetti di sicurezza (chiavi e pin) ed altri file necessari alla funzionalità dell'applicazione Calypso.

I DF e il MF dovranno essere di tipo revision 3 (anche se non completamente aderente alla specifica, vedi Calypso rev.3 - R28).

La dimensione della memoria (EEPROM) deve essere adeguata all'applicazione nel seguito richiesta.

2.1.5 *Lista dei File presenti sotto Master File*

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
MF	MF	3F00h	-	na	na	Vedi tabella nomi DF
EF ICC	Linear	0002h	02h	1	29	n.a.
EF ID	Linear	0003h	03h	1	29	n.a.
EF ITP-ID	Linear	3F04h	04h	1	29	n.a.
EF ITP-TDV	Linear	3F05h	05h	1	29	n.a.

N.B.: il MF nella mascheratura delle smart card, per alcune tecnologie (p.e. Java card), potrebbe non essere presente. Le applicazioni che gestiranno le smart card BIP dovranno tenere conto di questo aspetto.

2.1.6 *Lista dei File presenti sotto DF utilizzata dal sistema BIP*

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
DF: Transport 1	DF	2000h	-	-	-	Vedi tabella nomi DF
EF Environment	Linear	2001h	07h	2	29	n.a.
EF Events Log	Cyclic	2010h	08h	3	29	n.a.
EF Contract List	Linear	2050h	1Eh	1	29	n.a.
EF Contracts	Linear	2020h	09h	8	29	n.a.
EF Special Events	Linear	2040h	1Dh	8	29	n.a.
All Counters	Counter	2069h	19h	1	29	n.a.

Supplementary Counters	Counter	206Ah	13h	1	29	n.a.
Free file	Linear	20F0h	01h	4	29	n.a.

2.1.7 *Lista dei File utilizzati per la gestione del Credito Trasporti*

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
DF: EP Stored value application	DF	1000h	-	-	-	Vedi tabella nomi DF
EF Load Log	Cyclic	1014h	14h	1	29	n.a.
EF Purchase Log	Cyclic	1015h	15h	3	29	n.a.

2.1.8 *Lista dei File utilizzati per contratti di Servizi Aggiuntivi (partizione sempre presente)*

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
DF: Services application 1	DF	3100h	-	-	-	Vedi tabella nomi DF
EF Parameters	Linear	3102h	17h	1	29	
EF Contracts	Linear	3120h	18h	8	29	
EF Counters	Linear	3169h	1Ah	1	29	
EF Miscellaneous	Linear	3150h	1Bh	8	29	

2.1.9 *Tabella nomi DF*

Le *DF name* previste ad oggi per le applicazioni BIP sono elencate nella seguente tabella:

DF Name	DF ID	Mixed Ascii – Hex	Application ID Hex
Master File (MF)	3F00	"3MTR.ICA" D380 1200 9001	334D54522E494341D38012009001
Calypso DF Transport application 1 (DF1)	2000	"1TIC.ICA" D380 1200 9101	315449432E494341D38012009101
Calypso DF Services application 1 (DF2)	3100	"1TIC.ICA" D380 1200 9301	315449432E494341D38012009301
Stored value application (EP)	1000	"0ETP.ICA" D380 1200 9201	304554502E494341D38012009201

2.2 Circuito di appartenenza

2.2.1 *Introduzione*

Esistono in questo momento in Piemonte diverse realtà che adottano una smartcard per l'accesso e la gestione di servizi oltre al trasporto pubblico:

- Giovani: biblioteche, musei, strutture sportive, cinema e teatri saranno accessibili tramite la carta **PYOU**;
- Università: gli studenti universitari per l'accesso ai servizi degli atenei utilizzano la carta **EDISU**.
- Trenitalia : i clienti dei trasporti regionali del Piemonte di Trenitalia per l'accesso ai servizi ferroviari utilizzano la smartcard **TRENITALIA**

Questi circuiti integrano anche le funzionalità del BIP previste per i servizi di mobilità e non è escluso che altri circuiti potranno afferire al BIP in futuro.

Ai fini di riconoscere a quale circuito originale appartiene la smartcard nella fase iniziale di comunicazione tra *coupler* e il *Portable Object*, si è scelto di sfruttare il byte *Application Subtype* nelle *Startup Information* inviato nella risposta al comando di *Select Application*.

2.2.2 *Startup Information*

Le applicazioni Calypso, nella risposta al comando di *Select Application*, devono restituire anche le *Startup information* come previsto dalle specifiche Calypso rev. 3.1 (par. 5.6 e 9.2.1). Tali dati sono preceduti dal TAG 53h.

All'interno delle *Startup Information* (7 byte) si trova il byte *Application Subtype* che verrà valorizzato in fase di produzione in modo da indicare il circuito di appartenenza della carta, i restanti byte sono da valorizzare come previsto dalla specifica Calypso Rev. 3.1

Il borsellino elettronico (SV) dovrà mantenere il byte *Application Subtype* al valore previsto dalle specifiche Calypso rev. 3.1 (requisito R157.1). Si ricorda che le prime forniture hanno posto tale valore per l'SV a 0xC0.

2.2.3 *Codifica circuito appartenenza*

Valore	Descrizione
C0h	BIP
C1h	PYOU
C2h	EDISU
C3h	NFC
C4h	TRENITALIA
C5h	CB
…	RFU

2.3 Chiavi di sicurezza presenti sulla carta

Sulla smartcard sono presenti differenti set di chiavi, ad ogni singola ADF è associato/gestito almeno un set di 3 chiavi in completa autonomia.

Sotto Master File (la cui presenza è legata alla tecnologia scelta) dovrà essere presente un set di chiavi indipendente con tre chiavi distinte ed un PIN, con lunghezza di almeno 4 byte, che potrà essere utilizzato in tutta la struttura del file system.

Le chiavi sono di tipo DES_X.

2.4 Caricamento delle chiavi di sicurezza

Sulle 5 smartcard destinate ai test di compatibilità della revision 3.1 di Calypso e della mascheratura BIP (vedi par. successivo) eseguiti da 5T, sarà cura dei Concorrenti caricare in modo opportuno i set di chiavi contenuti nel **SAM-TEST-F5v2** (con funzionalità di AnyUnDebit attivata) che, se non già in loro possesso in qualità di licenziatari Calypso, può essere richiesto presso la Società Spirtech (1 rue Danton - 75006 Paris – France, Tel: +33 140463620 - Fax: +33 140463629 http://www.spirtech.com/), provider tecnologico della CNA.

In particolare sulle smartcard andranno caricate le seguenti chiavi associate alle strutture:

Name	Keys
MF	MK_MF1_X ($617E) MK_MF2_X ($677E) MK_MF3_X ($707E)

DF1	MK_RT1_X2 ($217D) MK_RT2_X2 ($277D) MK_RT3_X2 ($307D)
DF2	MK_RT1_X3 ($217C) MK_RT2_X3 ($277C) MK_RT3_X3 ($307C)
EP	MK_SV1_X ($017E) MK_SV2_X ($077E) MK_SV3_X ($107E)

2.5 Mascheratura BIP

2.5.1 *Introduzione*

Tipi di chiavi segrete:

Key N°1 Issuer key	Chiave di personalizzazione e prepersonalizzazione. Usata tipicamente per inserire dati generici. Può essere usata all'interno di una sessione sicura.
Key N°2 Load key	Chiave di ricarica. Usata tipicamente per rinnovi o ricariche di TdV. Può essere usata all'interno di una sessione sicura.
Key N°3 Debit key	Chiave di validazione. Usata tipicamente per validare/decrementare TdV. Può essere usata all'interno di una sessione sicura.

I comandi di accesso ai file sono divisi in quattro gruppi:

Gruppo	DF	EF lineare	EF ciclico	EF contatore
0	Rehabilitate	Read Record	Read Record	Read Record
1	Invalidate	Update Record	Update Record	Update Record
2	(rfu)	Write Record	Write Record	Decrease Decrease Multiple
3	(rfu)	(rfu)	Append Record	Increase Increase Multiple

Esistono quattro metodi di accesso per ogni gruppo:

Access Mode	Descrizione
Always	Accesso libero: diritti di accesso sempre garantiti
Never	Accesso vietato: diritti d'accesso sempre negati
Pin	Accesso consentito solo se la carta ha preventivamente verificato con successo il codice PIN
Session	Accesso consentito solo all'interno di una sessione sicura usando la chiave corrispondente. Questo metodo di acesso può essere applicato solo ai comandi di modifica (non al *read*).

2.5.2 *Condizioni di accesso ai file*

Condizioni di accesso dei File presenti sotto Master File

MF / DF / EF	File type	Group 0 read/rehabilitate	Group 1 update/invalidate	Group 2 write/decrease	Group 3 append/increase
MF :	MF	Session 1	Session 3	n.a.	n.a.
EF ICC	Linear	always	never/Session 1	never	n.a.
EF ID	Linear	PIN	Session 2	never	n.a.
EF ITP-ID	Linear	always	Session 1	never	n.a.
EF ITP-TDV	Linear	always	Session 2	Session 3	n.a.

N.B.: la condizione d'accesso del file EF ICC per le carte native è never .

Condizioni di accesso dei File presenti sotto DF utilizzata dal sistema BIP

MF / DF / EF	File type	Group 0 read/rehabilitate	Group 1 update/invalidate	Group 2 write/decrease	Group 3 append/increase
DF: Transport 1	DF	Session 1	Session 3	n.a.	n.a.
EF Environment	Linear	always	Session 1	never	n.a.
EF Events Log	Cyclic	always	Session 3	Session 3	Session 3
EF Contract List	Linear	always	Session 3	never	n.a.
EF Contracts	Linear	always	Session 2	Session 3	n.a.
EF Special Events	Linear	always	Session 3	never	n.a.
All Counters	Counter	always	Session 2	Session 3	Session 2
Supplementary Counters	Counter	always	Session 2	Session 3	Session 2
Free file	Linear	always	always	always	always

Condizioni di accesso dei File utilizzati per la gestione del Credito Trasporti

MF / DF / EF	File type	Group 0 read/rehabilitate	Group 1 update/invalidate	Group 2 write/decrease	Group 3 append/increase
DF: EP	DF	Session 1	Session 3	n.a.	n.a.
EF Load Log	Cyclic	always	never	never	never
EF Purchase Log	Cyclic	always	never	never	never

Condizioni di accesso ai File utilizzati per contratti di Servizi Aggiuntivi (partizione sempre presente)

MF / DF / EF	File type	Group 0 read/rehabilitate	Group 1 update/invalidate	Group 2 write/decrease	Group 3 append/increase
DF: Transport 2	DF	Session 1	Session 3	n.a.	n.a.
EF Parameters	Linear	always	Session 1	never	n.a.
EF Contracts	Linear	always	Session 2	Session 3	n.a.
EF Counters	Counters	always	Session 2	Session 3	Session 2
EF Miscellaneous	Linear	always	Session 3	never	n.a.

NB: prima di accedere ad un file di una applicazione è obbligatorio inviare un comando di SelectApplication.

2.5.3 *Codice seriale carta*

Il codice seriale della carta è formato da 8 byte. Esso identifica univocamente la carta a livello universale. L'emissione dei codici carta viene regolamentata dalla *Calypso Network Association* che ne definisce le modalità di emissione e di utilizzo.

Nel caso del progetto BIP sono stati riservati dei codici seriali univoci presso la CNA. La gestione di tali codici è in capo al Centro Servizi Regionale del BIP.

L'identificativo della carta è contenuto nel file ICC così come da specifiche Calypso 3.0.

Nel caso delle campionature di smartcard (n° 5) da consegnare a 5T per le verifiche della rev.3.1 di Calypso e della mascheratura BIP, i Concorrenti possono utilizzare generici S/N purchè consecutivi.

3. Credito Trasporti (Stored Value)

Il progetto BIP prevede un titolo di viaggio a deconto contenente un monte unità di viaggio prepagato denominato "Credito Trasporti".

La smartcard oggetto di qualificazione deve disporre di un'applicazione che permetta la gestione (lettura, scrittura, aggiornamento) di un valore memorizzato come previsto dalla specifica Calypso revision 3.1.

Le funzionalità richieste all'SV (Stored Value) sono le seguenti:

- Leggere lo stato dell'SV ovvero il valore memorizzato.
- Incrementare una quantità al valore corrente dell'SV.
- Decrementare una quantità al valore corrente dell'SV.
- Annullare, in parte o completamente, l'ultimo decremento effettuato.

La lettura dello stato dell'SV è libera.

Per incrementarne il valore, in fase di ricarica è richiesto che l'operazione sia effettuata in una sessione sicura Calypso tramite l'utilizzo della SAM CL.

Per decrementare, annullare parzialmente o totalmente l'ultimo decremento è richiesto che l'operazione venga effettuata in una sessione sicura Calypso tramite l'utilizzo di SAM CV.

Il SAM CV che effettua l'annullamento può differire da quello che ha effettuato il decremento.

4. Caratteristiche costruttive

4.1 Durata della carta

I processi produttivi delle smartcard devono garantire una durata di almeno **4 anni** e pertanto devono essere particolarmente curate le seguenti attività:

- l'embedding, soprattutto in relazione al collegamento dell'antenna al microprocessore,
- la stampa e tutte le attività produttive che possono causare stress meccanici ed elettrici.

A tale proposito si rammenta la conformità alle norme citate nel documento per quanto riguarda le caratteristiche fisiche ed in particolare la ***ISO/IEC 14443-1 paragrafo 4*** e le relative norme collegate (ISO/IEC 10373).

I 5 campioni da consegnare a 5T per le verifiche della rev.3.1 di Calypso e della mascheratura BIP devono presentare il seguente layout sul quale **è riportata l'indicazione BIP in alfabeto Braille.**

5. Certificazione delle smartcard

Il processo di certificazione a cura del concorrente, verrà richiesto a tutte le Società/ATI o raggruppamenti che intendono iscriversi al sistema di qualificazione.

L'ente individuato dal Concorrente deve rispondere al seguente requisito:

- possedere la certificazione ISO 9001 rilasciata da ente accreditato SINCERT o altri enti facenti parte dell'EA (European co-operation for Accreditation) per le "attività di certificazione e testing di laboratorio elettromagnetico" con un sistema di gestione delle norme ISO 17025 e una procedura di certificazione ISO 14443.

5.1 Processo di certificazione

5.1.1 *Test di compatibilità elettromagnetica*

La realizzazione delle prove di conformità per le smartcard dovrà essere realizzata sulla base dei seguenti riferimenti normativi:

1. ISO/IEC 14443-1 First edition 2000-04-15 "Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1: Physical characteristics"
2. ISO/IEC 14443-2 First edition 2001-07-01 "Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 2: Radio frequency power and signal interface"
3. ISO/IEC 14443-3 — Identification cards — Contactless integrated circuit(s) cards – Proximity cards — Part 3: "Initialization and anticollision"
4. ISO/IEC 10373-6 2001 "Identification cards — Test methods — Part 6: Proximity cards"

La valutazione di conformità riguarderà le prove sull'Interfaccia a Radio Frequenza secondo lo standard ISO/IEC 10373-6:2001.

Per dimostrare l'aderenza alla ISO/IEC 14443-3, visto che tale layer di standardizzazione non possiede una specifica procedura di certificazione, i Concorrenti dovranno produrre all'interno della documentazione tecnica richiesta dal disciplinare del sistema di qualificazione una "Dichiarazione di conformità a tale norma riferita al prodotto/i oggetto della procedura di qualifica" tale dichiarazione può essere sottoscritta dal Concorrente o dal laboratorio certificatore o da entrambi.

Le prove di certificazione dovranno essere svolte su almeno 20 esemplari di smartcard, prodotte da **almeno 10 giorni,** identificate dalla relativa documentazione quale ad esempio :

- *Descrizione dettagliata del/i prodotto/i proposto/i con particolare riferimento alle caratteristiche hardware utilizzate - produttore del microprocessore, numero di pezzi difettosi normalmente attesi, e ogni altra notizia utile per la valutazione;*

- *Documentazione tecnica completa (specifiche tecniche, specifiche funzionali, manuale d'uso e di programmazione) ed eventuali tools di personalizzazione.*

- *Indicazione di quali delle seguenti fasi del ciclo produttivo le imprese richiedenti sono in grado di effettuare la gestione diretta (esclusa soltanto la fabbricazione del chip):*
  - *assemblaggio del micromodulo*
  - *assemblaggio dell'inlet o stampa serigrafica dell'antenna*
  - *applicazione del chip*
  - *test di qualità*
  - *pre-personalizzazione elettrica*
  - *personalizzazione finale (elettrica, termografica, ecc.)*

Le prove di laboratorio che dovranno essere effettuate sono elencate di seguito:

Requisito/Test	Rif. Normativo	Descrizione
Alternating magnetic field test	ISO14443-1 Cap. 4.3	Lettura del campo magnetico a 0 A/m e 12 A/m rms
Minimum operating field measurement	ISO14443-2 Cap. 6.2	Misurazione del campo H sul PICC da Hmin=1.5 A/m a Hmax=7.5 A/m
Capacity of reception test	ISO10373-6 AM 02 Cap. 7.2	Verifica dell"abilità di un PICC di rispondere ad un comando di richiesta inviato dal PCD con una certa forma d'onda
Load modulation amplitude measurement	ISO14443-2 Cap. 8.2, 9.2	Il load modulation deve essere ≥ 30/H1,2 mvpp TX rate = 106 Kbps Fsubcarrier = 847 KHz
Misura della Frequenza di risonanza	ISO10373-6 Cap.6.1, 6.3	Misura dell'impedenza e della frequenza (massimizzazione della parte Re)
Misura del Coefficiente di merito (Q)	ISO10373-6 Cap. 6.1, 6.3	Misura dell'impedenza e della frequenza (massimizzazione della parte Re)
Class 1 maximum loading effect	ISO10373-6 Cap 7.4	Questa misura permette di valutare se il loading effect che caratterizza il PICC (Hp) sotto esame non supera il valore di riferimento Hr.
Effect of type A command on type B card	ISO14443-3 AM1 Cap. 5.2	Analizzare il comportamento di un PICC di tipo B in presenza di comandi di tipo A

5.1.2 *Test meccanici*

I test richiesti per verificare le caratteristiche meccaniche delle smartcard in base a quanto previsto dalla ISO/IEC 10373 - parte 1 sono :

- Stress reiterati di flessione
- Stress reiterati di torsione
- Stabilità meccanica in temperatura ed umidità
- Adesione bloccaggio meccanico

5.1.3 *Risultati*

Le prove indicate nei paragrafi 5.1.1 e 5.1.2 dovranno essere condotte, a cura dell'Ente individuato dal Concorrente, presso propri laboratori o presso laboratori preventivamente qualificati secondo i propri standard di qualità richiesti per laboratori di misura e prove a scopo di certificazione.

I laboratori di cui sopra dovranno essere indipendenti dal punto di vista funzionale ed amministrativo dai costruttori di prodotti appartenenti alla categoria oggetto della certificazione.

Le prove dovranno essere condotte nel pieno rispetto dei principi di mutua riservatezza. A tale scopo non potrà essere permessa la presenza di rappresentanti dello stesso Fornitore durante lo svolgimento delle prove.

L'esito positivo della valutazione sarà ufficializzato a 5T per mezzo di un "Rapporto di prova" a standard ISO/IEC 17025, del prodotto esaminato.

5.1.4 *Test del S.O. Calypso e della mascheratura BIP*

A seguito del ricevimento della documentazione prevista al paragrafo precedente e dei 5 campioni, 5T provvederà :

- allo svolgimento dei test di verifica della conformità alla rev.3.1 di Calypso, solamente nel caso il prodotto presentato non sia già in possesso della certificazione "Calypso Portable Object Certification" in corso di validità rilasciata dalla CNA;
- allo svolgimento dei test di verifica della mascheratura dati (CDM) adottata dal BIP.

Il **Calypso Portable Object Certification**, dovrà essere allegato alla documentazione presentata in sede di domanda di partecipazione al Sistema di Qualificazione.

.

I test saranno effettuati su 5 esemplari di smartcard, tramite l'utilizzo di opportuni tool di test.

Verranno verificate le Strutture dati della smartcard e per i prodotti non certificati dalla CNA i principali comandi della rev.3.1 di Calypso, in particolare :

- la conformità della struttura dati con quella richiesta nella presente specifica:
  - verifica della struttura dati, selezione dei file e verifica delle condizioni di accesso,
  - verifica degli indici di chiave di sessione (key ID e key version),
  - verifica del buon funzionamento della sessione, congruità dei dati ai casi limite dove la sessione viene interrotta prematuramente per cause accidentali e/o premeditate,

- la conformità dei comandi del sistema operativo alla specifica Calypso 3.1:
  - test dei singoli comandi di base del sistema operativo per la lettura e la scrittura dei file ([1]cap. 9.2 e 9.4), la gestione delle sessioni sicure ([1] cap. 9.5);

- la conformità dei comandi del sistema operativo relativi alla gestione del borsellino elettronico ([1] cap.10):
    - verifica del funzionamento dei comandi del sistema operativo relativi alla gestione del borsellino elettronico:
        - SV Get,
        - SV Debit,
        - SV Undebit, SV AnyUndebit con SAM-CV differente,
        - SV Reload.

I test saranno eseguiti da 5T entro 10 giorni lavorativi dalla consegna dei campioni e della documentazione di cui sopra.

Al termine del processo l'esito positivo della valutazione sarà ufficializzato da 5T per mezzo di un "Attestato di conformità BIP" del prodotto esaminato.

Lo svolgimento dei test relativi alla verifica della conformità alla rev.3.1 di Calypso ed alla mascheratura adottata dal BIP è a totale carico di 5T S.r.L.