



**5T S.R.L.**

Corso Novara 96 — 10152 Torino (IT)

T +39 011 227 4101

info@5t.torino.it / direzione5t@legalmail.it

www.5t.torino.it

C.F. - P.IVA 06360270018

C.C.I.A.A. TORINO 2825/1992

CAP. SOCIALE € 100.000,00 i.v.



# **Specifica tecnica della smartcard Edisu BIP (Allegato A2)**

<b>INDICE DEL DOCUMENTO</b>
-----------------------------

1.	Introduzione .....	3
1.1	Scopo del documento .....	4
1.2	Normativa e documenti di riferimento .....	4
1.3	Definizioni ed Acronimi.....	5
2.	Requisiti tecnici .....	6
2.1	Requisiti generali.....	6
2.1.1	Requisiti fisici e meccanici .....	6
2.1.2	Requisiti elettrici .....	6
2.1.3	Protocolli di comunicazione .....	6
2.2	Struttura del File System.....	7
2.2.1	Lista dei File presenti sotto Master File.....	7
2.2.2	Lista dei File presenti sotto DF utilizzata dal sistema BIP .....	7
2.2.3	Lista dei File utilizzati per la gestione del Credito Trasporti.....	8
2.2.4	Lista dei File utilizzati per contratti di Servizi Aggiuntivi (partizione sempre presente)..	8
2.2.5	Tabella nomi DF .....	8
2.3	Circuito di appartenenza .....	8
2.3.1	Introduzione.....	8
2.3.2	Startup Information .....	9
2.3.3	Codifica circuito appartenenza nella Startup Information .....	9
2.4	Chiavi di sicurezza presenti sulla smartcard.....	9
2.5	Utilizzo del Credito Trasporti (SV) .....	10
2.6	Condizioni di accesso ai files .....	10
2.6.1	Codice seriale della smartcard.....	12
3.	Ulteriori caratteristiche.....	13
3.1	Banda magnetica .....	13
3.2	Caratteristiche costruttive e durata del supporto .....	13
4.	Layout .....	14
4.1	Layout 1 - Università di Torino.....	14
4.2	Layout 2 - Politecnico di Torino .....	15
5.	Confezionamento .....	16
5.1	Contenitori di smartcard .....	16
5.2	Confezionamento in scatole .....	16
6.	File di produzione.....	18
	Indice delle figure.....	19
	Indice delle tabelle .....	20

## 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, realizzando azioni di infomobilità e certificando quantità e qualità del servizio reso ([www.bip.piemonte.it](http://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
- Vercelli

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 carta.

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 tramite parcometri.

Il progetto BIP prevede anche 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 altri Portable Object 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 di smartcard BIP/Pyou su scala regionale. Nell’ambito del sistema BIP sono state approvvigionate, nel periodo 2009-2018, più di **un milione** di smartcard.

La smartcard oggetto di fornitura dovrà quindi rispondere a tutti gli elementi funzionali, tecnici, di sicurezza e d’interfaccia descritti nella presente specifica.

## 1.1 Scopo del documento

Questo documento ha l'obiettivo di descrivere le specifiche tecniche delle smart card contactless a microprocessore adottata del progetto BIP che dovranno essere fornite.

In particolare verranno descritti:

- i requisiti fisici, meccanici ed elettrici;
- il protocollo di comunicazione a basso livello tra smartcard e lettore;
- l'organizzazione logica dei file contenuti nella smartcard 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 in autonomia la seconda area di memoria 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 cui si rimanda alla specifica documentazione del consorzio Calypso ([www.calypsonet-asso.org](http://www.calypsonet-asso.org)).

## 1.2 Normativa e documenti di riferimento

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

1. Specifiche del sistema operativo "Calypso" – release 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);
5. Norme ISO 10373.

### 1.3 Definizioni ed Acronimi

Acronimo	Definizione
<b>AFI</b>	Application Family Information
<b>APDU</b>	Application Protocol Data Unit, set di comandi di un PO Calypso per la lettura e la scrittura del file system, di verifica di accesso nonché di autenticazione reciproca (carta e terminale) e dei dati scambiati.
<b>ATQ</b>	Answer To Request, comando inviato dal PICC in risposta al REQ del PCD (protocollo ISO 14443 parte 3)
<b>ATQB</b>	Answer To Request of Type B (dove Type B si riferisce al Type of PICC ovvero al PO).
<b>ADF</b>	Application DF
<b>CNA</b>	Calypso Network Association
<b>DF</b>	Dedicated File, equivale ad una directory di file ovvero può contenere più EF file.
<b>REQ</b>	Elementary File, file contenenti dati. Esistono principalmente tre tipi di file EF: lineari, ciclici e contatori.
<b>REQB</b>	Electronic Purse, borsellino elettronico.
<b>RFID</b>	International Organization for Standardization
<b>ISO</b>	Master File: la directory radice del file system. Può contenere DF e EF file.
<b>MF</b>	Proximity Coupling Device, ovvero il lettore di PO.
<b>PCD</b>	Proximity Integrated Circuit Cards, ovvero la smartcard.
<b>PICC</b>	Portable Object Calypso (in questo caso una smartcard a microchip)
<b>PO</b>	cloruro di polivinile, materiale plastico, utilizzato come supporto fisico del microprocessore e dell'antenna presenti nella smartcard.
<b>PVC</b>	Request comando inviato dal PCD al PICC (protocollo ISO 14443 parte 3)
<b>REQ</b>	Request Command, Type B
<b>REQB</b>	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.
<b>RFID</b>	Secure Access Module
<b>SAM</b>	Sistema di bigliettazione elettronico
<b>SBE</b>	Serial Number, indicato nel documento anche come Codice Seriale o numero di serie.
<b>S/N</b>	Stored Value, applicazione borsellino elettronico
<b>SV</b>	Titolo di Viaggio
<b>TdV</b>	Wake up comando inviato dal PCD al PICC (protocollo ISO 14443 parte 3).
<b>WUP</b>	Wake-Up Command, Type B
<b>WUPB</b>	

## 2. Requisiti tecnici

### 2.1 Requisiti generali

#### 2.1.1 *Requisiti fisici e meccanici*

Le dimensioni fisiche della smartcard devono essere conformi alle specifiche ISO 7816 Parte 1, con particolare riferimento al formato indicato con la sigla ID1 di dimensioni LxHxP 85,60 x 53,98 x 0,76 mm.

Il materiale costruttivo della smartcard dovrà essere di tipo plastico (PVC, PET o equivalenti), nel caso venga 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 smartcard dovranno essere conformi alle normative di resistenza allo stress meccanico (torsione, flessione) indicate dalle ISO 10373.

#### 2.1.2 *Requisiti elettrici*

La smartcard oggetto di fornitura è di tipo "**full contactless**",

#### 2.1.3 *Protocolli di comunicazione*

Il protocollo contactless utilizzato nel BIP è unicamente l'**ISO 14443B**.

Il suddetto protocollo **ISO 14443B** deve essere l'unico attivo sulla smartcard oggetto di fornitura.

Inoltre secondo quanto indicato dalla specifica ISO 14443 parte 3, le smartcard 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 smartcard 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 smartcard. 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.

**Bit\_Rate\_capability**

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.								

Tabella 1 – Bit Rate supportato dalla smartcard

**2.2 Struttura del File System**

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

I DF e il MF dovranno essere di tipo Calypso rev3.1 (anche se non completamente aderente alla specifica, vedi requisito R28).

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

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

**2.2.1 Lista dei File presenti sotto Master File**

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
<b>MF</b>	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.

Tabella 2 - Lista dei File presenti sotto Master File

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

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
<b>DF: Transport 1</b>	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.

## BIP - Biglietto Integrato Piemonte

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.

**Tabella 3 - Lista dei File presenti sotto DF utilizzata dal sistema BIP**

### 2.2.3 Lista dei File utilizzati per la gestione del Credito Trasporti

MF / DF / EF	File type	LID	SFI	Num Rec.	Rec size	DF Name
<b>DF: EP Stored value application</b>	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.

**Tabella 4 - Lista dei File utilizzati per la gestione del Credito Trasporti**

### 2.2.4 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
<b>DF: Services application 1</b>	DF	3100h	-	-	-	Vedi tabella nomi DF
EF Parameters	Linear	3102h	17h	1	29	n.a.
EF Contracts	Linear	3120h	18h	8	29	n.a.
EF Counters	Counter	3169h	1Ah	1	29	n.a.
EF Miscellaneous	Linear	3150h	1Bh	8	29	n.a.

**Tabella 5 - Lista dei File utilizzati per contratti di Servizi Aggiuntivi**

### 2.2.5 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 aka SV)	1000	"0ETP.ICA" D380 1200 9201	304554502E494341D38012009201

**Tabella 6 - Tabella nomi DF**

## 2.3 Circuito di appartenenza

### 2.3.1 Introduzione

Esistono in questo momento in Piemonte diverse realtà che adottano smartcard analoghe alla Carta BIP 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 carta Unica **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.

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

### 2.3.2 **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 smartcard, 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.

### 2.3.3 **Codifica circuito appartenenza nella Startup Information**

Il byte *Application Subtype* delle *Startup Information* relativo alle smartcard EDISU oggetto di Fornitura, dovrà essere valorizzato in fase di produzione con il valore **C2h** (Circuito EDISU).

In generale, i valori ammissibili sono riportati nella tabella seguente.

Valore	Descrizione
C0h	BIP
C1h	Pyou
<b>C2h</b>	<b>EDISU</b>
C3h	NFC
C4h	TRENITALIA
C5h	CB
...	RFU

**Tabella 7 - Circuito di appartenenza nelle Startup Information**

## 2.4 **Chiavi di sicurezza presenti sulla smartcard**

Sulla smartcard dovranno essere presenti differenti set di chiavi, ad ogni singola ADF dovrà essere 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 e un PIN, con lunghezza di almeno 4 byte, che potrà essere utilizzato in tutta la struttura del file system. Il PIN dovrà essere inizializzato al valore 0x30303030 cioè '0000'

Per le funzionalità del Credito Trasporti dovranno essere previste almeno due chiavi indipendenti.

Le chiavi saranno di tipo DES\_X.

La fornitura dei moduli SAM verrà effettuata da 5T. Ulteriori dettagli sull'utilizzo dei moduli SAM verranno forniti ai costruttori delle smartcard in sede di aggiudicazione delle gare.

## 2.5 Utilizzo del Credito Trasporti (SV)

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

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

Le funzionalità richieste all'EP (Electronic Purse) sono le seguenti:

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

La lettura dello stato EP 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 della **SAM CV**.

## 2.6 Condizioni di accesso ai files

Tipi di chiavi segrete:

Chiave	Descrizione
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.

Tabella 8 - Tipi di chiavi segrete

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

Tabella 9 - Gruppi dei comandi di accesso ai file

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 smartcard 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 accesso può essere applicato solo ai comandi di modifica (non al read).

Tabella 10 - Metodi di accesso ai file

Le condizioni di accesso ai file sono definite nelle seguenti tabelle:

**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
<b>MF :</b>	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.

Tabella 11 - Master File - Condizioni di accesso ai file

**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
<b>DF : Transport 1</b>	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

Tabella 12 – Dedicated File - Condizioni di accesso ai file

**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
<b>DF :EP</b>	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

Tabella 13 - Credito Trasporti - Condizioni di accesso ai file

**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
<b>DF :Transport 2</b>	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.

Tabella 14 - Servizi aggiuntivi - Condizioni di accesso ai file

**2.6.1 Codice seriale della smartcard**

I numeri di serie Calypso sono espressi su 8 byte; essi identificano univocamente un PO Calypso a livello universale. L'attribuzione dei codici seriali ai lotti di produzione viene regolamentata dalla *Calypso Network Association*, che ne definisce le modalità di utilizzo.

**Nel caso il progetto BIP sono stati riservati dei codici seriali univoci presso la CNA. La gestione di tali codici è in capo a 5T, pertanto i fornitori di smartcard dovranno utilizzare per la produzione delle smartcard esclusivamente i codici seriali comunicati da 5T.**

Il numero di serie della smartcard è contenuto nel file ICC, così come indicato dalle specifiche Calypso.

### 3. Ulteriori caratteristiche

#### 3.1 Banda magnetica

Le smartcard devono essere dotate di una banda magnetica ad alta coercitività posta sul retro della carta, nella parte superiore.

#### 3.2 Caratteristiche costruttive e durata del supporto

I processi produttivi delle smartcard devono garantire una durata di almeno **5 anni** e pertanto devono essere particolarmente curate le seguenti attività:

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

A tale proposito si rammenta la conformità alle norme citate nel paragrafo 1.2 per quanto riguarda le caratteristiche fisiche ed in particolare **ISO/IEC 14443-1 paragrafo 4** e le relative norme collegate (ISO/IEC 10373).

## 4. Layout

Le smartcard dovranno essere fornite con i layout riportato nel seguito, completi di grafica e testi.

Sul retro delle smartcard dovrà essere riportato il Codice Seriale Calypso, in notazione decimale. Per ciò che riguarda il range dei valori vale quanto indicato al par.2.6.1.

Ogni layout riporta l'elenco completo dei codici colore.

Il retro della carta è concepito per lasciare uno spazio adeguato alla banda magnetica.

### 4.1 Layout 1 - Università di Torino



#### Colori di base (comuni a tutte le carte):

- PANTONE Black
  - PANTONE 185
  - PANTONE COOL GRAY 5
  - PANTONE 285
  - PANTONE GREEN
- } Colori Regione Piemonte

#### Logo UniTO.it:

- PANTONE 185
- PANTONE 424






unito.it

Figura 1 – Layout 1 - Università di Torino

## 4.2 Layout 2 - Politecnico di Torino



### Colori di base (comuni a tutte le carte):

-  PANTONE Black
  -  PANTONE 185
  -  PANTONE COOL GRAY 5
  -  PANTONE 285
  -  PANTONE GREEN
- } Colori Regione Piemonte

### Logo Politecnico:

-  PANTONE 7463C



Figura 2 – Layout 2 - Politecnico di Torino

## 5. Confezionamento

### 5.1 Contenitori di smartcard

Le smartcard dovranno essere fornite in ordine di Codice Seriale in contenitori chiusi da massimo 500 unità. All'interno di un singolo contenitore non potranno essere contenute smartcard aventi layout differenti.

All'esterno di ogni contenitore dovrà essere indicato:

- un codice composto da un numero sequenziale per ogni contenitore e dal numero totale di contenitori che compongono il lotto (ad es. "1 di 80" o "1/80" per il contenitore numero 1 di 40 totali);
- la tipologia di smartcard contenute (ad es. "Università di Torino");
- la quantità di smartcard nel contenitore (ad es. 400);
- il numero di serie della prima e dell'ultima smartcard.

Viene di seguito riportato un esempio di etichetta, al solo scopo esemplificativo.



Figura 3 - Esempio di etichetta per confezione smartcard

### 5.2 Confezionamento in scatole

In caso di ulteriore confezionamento in scatole, all'esterno di ogni scatola dovrà essere indicato:

- un codice composto da un numero sequenziale per ogni scatola e dal numero totale di scatole che compongono il lotto (ad es. "1 di 20" o "1/20" per la scatola numero 1 di un lotto di 20 scatole);
- la tipologia di smartcard contenute (ad es. "Università di Torino");
- la quantità totale di smartcard nella scatola (ad es. 1600);
- l'elenco dei contenitori presenti nella scatola (elenco di codici composti dal numero sequenziale della confezione e dal numero totale di confezioni del lotto (ad es. "1/80, 2/80, 3/80, 4/80" nel caso la scatola contenga le stecche numero 1, 2, 3 e 4 di 80 totali);
- il numero di serie della prima e dell'ultima smartcard contenute nella scatola.

Ogni scatola dovrà contenere al massimo 2.400 smartcard.

**In ogni scatola è possibile posizionare solo contenitori di smartcard aventi il medesimo layout.**

Il confezionamento dovrà prevedere accorgimenti opportuni per evitare il rischio di danneggiamenti nelle fasi di trasporto e stoccaggio.



Viene di seguito riportato un esempio di etichetta, al solo scopo esemplificativo.

**BOX 1 di 20 – Edisu**

Tot. smartcard: 1600

Contenitori: 1-2-3-4 di 80

SN da 950000001 a 950001600

**Figura 4 - Esempio di etichetta per scatola esterna**

## 6. File di produzione

Contestualmente alla consegna dei singoli lotti di smartcard, il fornitore dovrà consegnare su supporto elettronico (file batch di produzione) l'elenco dei numeri di serie (serial number Calypso) attribuiti alle smart card consegnate.

Il file batch deve contenere i seguenti dati:

- identificativo grafica, ovvero:
  - 1, per layout 1 - Università di Torino,
  - 2, per layout 2 - Politecnico di Torino,
  - 3, per layout 3 - Università del Piemonte Orientale,
  - 4, per Layout 4 - Edisu Piemonte;
- data di codifica;
- il valore codificato nel byte *Application Subtype* delle *Startup Information* (vedi par.2.3.3);
- codice seriale della smartcard codificata.

I formati file ammessi sono:

- .txt
- .CSV

Il fornitore dovrà altresì predisporre, su eventuale richiesta da parte di 5T, un file batch relativo all'intera fornitura richiesta, contenente le seguenti informazioni:

- identificativo grafica, ovvero:
  - 1, per layout 1 - Università di Torino,
  - 2, per layout 2 - Politecnico di Torino,
  - 3, per layout 3 - Università del Piemonte Orientale,
  - 4, per Layout 4 - Edisu Piemonte;
- data di codifica;
- codice seriale della smartcard codificata;
- il valore codificato nel byte *Application Subtype* delle *Startup Information* (vedi par.2.3.3);
- stato della spedizione, ovvero:
  - 1, per "in attesa di informazioni", ovvero il fornitore ha bisogno di informazioni per procedere con la lavorazione;
  - 2, per "in lavorazione", ovvero in fase di produzione;
  - 3, per "pronto per l'invio", ovvero smartcard prodotte e confezionate, in attesa del ritiro da parte del corriere;
  - 4, per "in transito", ovvero smartcard ritirate dal corriere ma non ancora consegnate;
  - 5, per "consegnato", ovvero recapitate nella sede di 5T (o altra sede concordata).

I formati file ammessi sono:

- .txt
- .CSV

## Indice delle figure

---

Figura 1 – Layout 1 - Università di Torino .....	14
Figura 2 – Layout 2 - Politecnico di Torino .....	15
Figura 5 - Esempio di etichetta per confezione smartcard .....	16
Figura 6 - Esempio di etichetta per scatola esterna .....	17

## Indice delle tabelle

---

Tabella 1 – Bit Rate supportato dalla smartcard .....	7
Tabella 2 - Lista dei File presenti sotto Master File .....	7
Tabella 3 - Lista dei File presenti sotto DF utilizzata dal sistema BIP .....	8
Tabella 4 - Lista dei File utilizzati per la gestione del Credito Trasporti .....	8
Tabella 5 - Lista dei File utilizzati per contratti di Servizi Aggiuntivi .....	8
Tabella 6 - Tabella nomi DF .....	8
Tabella 7 - Circuito di appartenenza nelle Startup Information .....	9
Tabella 8 - Tipi di chiavi segrete .....	10
Tabella 9 - Gruppi dei comandi di accesso ai file .....	10
Tabella 10 - Metodi di accesso ai file .....	11
Tabella 11 - Master File - Condizioni di accesso ai file .....	11
Tabella 12 – Dedicated File - Condizioni di accesso ai file .....	11
Tabella 13 - Credito Trasporti - Condizioni di accesso ai file .....	11
Tabella 14 - Servizi aggiuntivi - Condizioni di accesso ai file .....	12