Requisiti tecnici delle smartcard BIP (Card Data Model)

Nota Tecnica

Sistema BIP

Versione 3.1.7 del 05/10/2018

ID Documento: IID5T-173-6489

Indice

1. Introduzione 5
1.1 Scopo del documento 5
1.2 Normativa e documenti di riferimento 6
1.3 Lista delle revisioni 6
1.4 Acronimi 6
1.5 Riferimenti 7
2. Requisiti tecnici smartcard a microprocessore 8
2.1 Introduzione 8
2.2 Requisiti fisici e meccanici 8
2.3 Requisiti elettrici 8
2.4 Protocolli di comunicazione 8
2.5 Struttura del file system 9
2.5.1 Lista dei File presenti sotto Master File 10
2.5.2 Lista dei File presenti sotto DF utilizzata dal sistema BIP 10
2.5.3 Lista dei File utilizzati per la gestione del Credito Trasporti 10
2.5.4 Lista dei File utilizzati per contratti di Servizi Aggiuntivi (partizione sempre presente) 10
2.5.5 Tabella nomi DF 11
2.6 Circuito di appartenenza 11
2.6.1 Introduzione 11
2.6.2 Startup Information 12
2.7 Chiavi di sicurezza presenti sulla carta 12
2.8 Accesso al file system Calypso 12
2.8.1 Condizioni di accesso ai file 13
3. Dati contenuti sulla carta (card data model) 15
3.1 Introduzione 15
3.2 Byte Order 15
3.2.1 Esempi 15
3.3 Codice seriale carta 15
3.4 Codifica della data 16
3.5 Codifica dati cliente 16
3.6 Codifica EF ITP-ID 16
3.7 Codifica EF ITP-IDV 16

3.8 Codifica EF Environment 16
3.8.1 Codifica campo ID Formato 17
3.8.2 Codice profilo cliente 17
3.8.3 Durata profilo 17
3.8.4 Codice stato carta 18
3.8.5 Codifica codice fiscale 18
3.8.6 Codifica circuito carta 19
3.9 EF Contract list 19
3.10 EF Contracts 20
3.10.1 Descrizione TAG estensione contratto 21
3.11 Estensioni 22
3.11.1 Estensione FORMULA 22
3.11.2 Estensione numero passeggeri 23
3.11.3 Estensione titoli aziendali Trenitalia 23
3.11.4 Estensione O/D 24
3.11.5 Estensione Polimetrica 24
3.11.6 Estensione TDSE Plurisettimanale 180 ore 25
3.11.7 Record aggiuntivi 26
3.11.8 Riepilogo codici estensioni 26
3.12 EF special events 27
3.12.1 Tipo apparato Codificatore 27
3.13 EF Event Log 28
4. Utilizzo del credito trasporti 30
4.1 Introduzione 30
4.2 Logica applicativa di utilizzo del Credito Trasporti 30
4.3 Comandi APDU 32
4.3.1 Transazione interrotta prematuramente 32
4.4 Get EP / SV Get 33
4.5 Debit EP / SV Debit 35
4.6 Undebit EP / SV Undebit 37
4.7 Reload EP APDU 39
5. Le carte a basso costo 43
6. Caratteristiche costruttive 44

6.1 Durata della smart card 44

1. Introduzione

Il progetto BIP, Biglietto Integrato Piemonte, prevede l'utilizzo di una tipologia di smart card e la possibilità di utilizzare delle card a basso costo (chip on paper) nei diversi bacini provinciali.

Le carte a microprocessore consentono la gestione di Titoli di Viaggio Elettronici (TDVE o semplicemente TdV) e Credito Trasporti (CT).

Nell'ottica di consentire lo sviluppo del sistema BIP, con particolare riguardo agli aspetti di compatibilità ed interoperabilità, ci si pone l'obiettivo di definire le linee guida tecniche e tecnologiche per l'utilizzo delle smartcard (o più in generale dei *Portable Object* – PO) previste dal progetto BIP. Tale documento ha l'obiettivo di uniformare le modalità di utilizzo della carta tra i vari bacini BIP, rendere semplici, chiare ed inequivocabili le modalità secondo cui un sistema SBE debba interagire con la carta per la gestione operativa dei TDVE, dare delle linee guida sulla gestione dei dati da utilizzarsi sulla smart card.

Il gruppo di lavoro del progetto BIP intende sviluppare affrontare tali problematiche nel seguente documento. Esso tratterà problematiche inerenti alle smartcard a microprocessore ed ai PO in generale.

1.1 Scopo del documento

Questo documento fornisce le specifiche tecniche della Carta Regionale dei Trasporti del progetto BIP per quanto concerne le funzionalità contactless in particolare:

Carte a microprocessore:

- La componente di File System;
- Le componenti di sicurezza che consentono di:
  - effettuare le operazioni di obliterazione (validazione) di 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 terzi autorizzati
- Indicare i comandi APDU conformi alle specifiche Calypso 2 e 3,
- Indicare un modello dati che gli operatori dovranno adottare per codificare in maniera univoca i titoli di viaggio.

1.2 Normativa e documenti di riferimento

È richiesta la conformità a quanto definito nelle norme e nei documenti di seguito elencati:

1. Specifiche del sistema operativo “Calypso” – revision 3.1 - reperibile sul sito del Calypso Network Association;
2. Norme ISO 14443 parti da 1 a 4;
3. Norme ISO 7816 parti da 1 a 4 e successive in conformità con quanto definito al punto “2”;
4. Norme EN 1545 per la definizione del modello dati (per quanto applicabile).
5. 5T-Nota Tecnica BIP-Tabella Operatori e CCA [1]

1.3 Lista delle revisioni

Data	Versione	Riassunto dei cambiamenti
14-ott-2014	3.1.4	[Versione pubblicata su redmine.5t.torino.it in data 12/04/2014]
26-giu-2015	3.1.5	Corretto valore in tabella Master File (par. 2.8.1)
01-giu-2016	3.1.6	• Aggiunti riferimenti ad altre note tecniche • Inseriti riferimenti incrociati a paragrafi e note esterne • Liberato valore “7” in Special Event (par. 3.12) Aggiunti valori per “Tipo operazione” e descrizione campo “Seriale del contratto” in Event Log (par. 3.13)
05-ott-2018	3.1.7	• Aggiunto esempio di codifica della data • Rivista formattazione e colore tabelle

1.4 Acronimi

Acronimo	Definizione
BCD	Binary Code Digit
BIP	Biglietto Integrato Piemonte
CB	Carta Bancaria
CCA	Centro di Controllo Aiendale
CSR	Centro Servizi Regionale
CT	Credito Trasporti
DF	Directory File
EDISU	Ente per il Diritto allo Studio Universitario

Acronimo	Definizione
EF	Elementary File
EP	Electronic Purse (Borsellino Elettronico, contiene CT)
MF	Master File
NFC	Near Field Communication
NH	Nibble High
NL	Nibble Low
PIN	Personal Identification Number
RFID	Radio Frequency IDentification
PO	Portable Object, ovvero qualsiasi supporto in grado di interagire come una smartcard BIP (Java card, smartphone NFC, ecc.)
RFU	Riservato per Futuri Usi
SAM	Secure Access Module
SC	Smart Card
SV	Store Value (Borsellino Elettronico, indica un valore per il CT)
TdV	Titolo di Viaggio
TDVE	Titolo Di Viaggio Elettronico
TDSE	Titolo Di Sosta Elettronico
TPL	Trasporto Pubblico Locale

1.5 **Riferimenti**

Riferimento	Descrizione
[1]	5T-Nota_Tecnica_BIP_Tabella_Operatori
[2]	5T-Nota_Tecnica_BIP_Firma_e_Verifica_SC
[3]	Elenco_Localita_BIP
[4]	5T-Nota_Tecnica_BIP_Tabella_Profili
[5]	5T-Nota_Tecnica_BIP_Gestione_date

2. Requisiti tecnici smartcard a microprocessore

2.1 Introduzione

Nel seguente paragrafo vengono trattate le tipologie di smart card dotate di microprocessore o dispositivi equivalenti quali telefonini NFC, token o tag RFID compatibili. Le smartcard gestite saranno di tipo 2 (Calypso rev. 2.4) e di tipo 3 (Calypso rev. 3.1).

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

2.3 Requisiti elettrici

Si utilizzeranno preferibilmente smart card "**cless only**" oppure in via opzionale le **Dual Interface**.

Le caratteristiche elettriche riguardanti la parte a contatti delle DI dovranno rispettare la normativa ISO 7816 parte 2.

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

Le carte dovranno essere conformi per quanto concerne il protocollo RFID alla normativa ISO 10373 – parte 6.

2.4 Protocolli di comunicazione

Il protocollo a contatti delle carte Dual Interface dovrà essere conforme alle normative ISO 7816 parte 3, protocollo T=0.

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, il 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.								

2.5 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.

2.5.1 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 smartcard, per alcune tecnologie (p.e. Java card), potrebbe non essere presente. Le applicazioni che gestiranno le smartcard BIP dovranno tenere conto di questo aspetto.

2.5.2 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.

2.5.3 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.

2.5.4 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
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	Counter	3169h	1Ah	1	29	
EF Miscellaneous	Linear	3150h	1Bh	8	29	

Per esigenze future si prevede la possibilità di utilizzare prodotti con aree di memoria di dimensione superiore ai 2K byte. In tal caso la struttura del file system potrà contenere ulteriori ADF così come previsto dalla specifica Calypso.

Le ADF aggiuntive potranno essere strutturalmente identiche alle precedenti o presentare diverse strutture a oggi non determinabili. In ogni caso dovranno avere *DF name* differenti e LID Differenti.

2.5.5 Tabella nomi DF

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

2.6 Circuito di appartenenza

2.6.1 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*.

2.6.2 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 (vedi par. Codifica circuito 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.

2.7 Chiavi di sicurezza presenti sulla carta

Sulla carta 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 ed un PIN, con lunghezza di almeno 4 byte, che potrà essere utilizzato in tutta la struttura del file system.

Le chiavi saranno di tipo DES_X.

Ulteriori dettagli sull'utilizzo dei moduli SAM, la cui fornitura verrà effettuata a cura della Regione Piemonte, saranno forniti ai costruttori delle smartcard in sede di aggiudicazione delle gare.

2.8 Accesso al file system Calypso

Categorie di chiavi segrete

Key N°1 Issuer key	Chiave di personalizzazione e prepersonalizzazione[1]. 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 TDVE. Può essere usata all'interno di una sessione sicura.
Key N°3 Debit key	Chiave di validazione. Usata tipicamente per validare/decrementare TDVE. Può essere usata all'interno di una sessione sicura.

I comandi di accesso ai file sono divisi in quattro gruppi

[1] Per i prodotti Revision 2 che necessitano della key N°0 per la pre-personalizzazione questa chiave deve assumere gli stessi valori della key N°1.

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*).

2.8.1 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.

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	n.a.

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: SV	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	Counter	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.

3. Dati contenuti sulla carta (card data model)

3.1 Introduzione

Nel seguente paragrafo vengono indicate le modalità di codifica e di interpretazione dei dati sulle smartcard.

I vari dispositivi che devono leggere e/o aggiornare i dati sulle carte dovranno seguire le modalità di seguito descritte.

3.2 Byte Order

Il byte order scelto è il big-endian, quindi per campi di grandezza maggiore di un byte avremo all'indirizzo più basso il byte più significativo. Quando un campo si estende in un nibble del byte seguente dovranno essere utilizzati i suoi 4 bit più significativi. Con lo stesso ragionamento quando un campo che occupa anche una frazione di byte comincia a metà di un byte stesso dovrà occupare il nibble meno significativo.

3.2.1 Esempi

Campo da 2 byte. Il valore 0x0123 dovrà essere memorizzato come segue:

Byte 0	Byte 1	Byte 2	Byte 3	…
0x01	0x23	…	…	
0000 0001b	0010 0011b	…	…	

Campo da 1,5 byte. Valore 0x123 che si estende al nibble successivo:

Byte 0		Byte 1		Byte 2		Byte 3		…
Nibble H	Nibble L	Nibble H	Nibble L	Nibble H	Nibble L	Nibble H	Nibble L	
…	…	1	2	3	…	…	…	

Campo da 1,5 byte. Valore 0xABC che comincia dal nibble precedente:

Byte 0		Byte 1		Byte 2		Byte 3		…
Nibble H	Nibble L	Nibble H	Nibble L	Nibble H	Nibble L	Nibble H	Nibble L	
…	A	B	C	…	…	…	…	

3.3 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 il progetto BIP sono stati riservati dei codici seriali univoci presso il CNA. La gestione di tali codici è in capo al CSR (Centro Servizi Regionale), pertanto i vari fornitori, previa opportuna richiesta, riceveranno gli stessi dal CSR prima della fase di produzione delle smartcard.

L'identificativo della carta è contenuto nel file ICC così come da specifiche Calypso rev3.

Il codice seriale della carta è inoltre restituito, preceduto dal tag C7h e dalla sua lunghezza (08h), in seguito al comando di Select Application.

3.4 Codifica della data

Le date verranno codificate utilizzando campi lunghi tre byte ad aventi valori binari.

Il valore binario indicherà i minuti trascorsi a partire dalla data del 1 gennaio dell'anno 2005, ore 00.00.

L'ora legale non influisce sul calcolo della data.

Per tutti i TDVE in *EF Contract* (estensioni escluse) le date di inizio e fine validità sono da scrivere in complemento a 1 in modo da aumentare il livello di sicurezza del sistema BIP. Tale meccanismo non deve essere implementato per altri EF contenenti campi data.

Il massimo valore possibile corrisponde al valore esadecimale FFFFFFh, in decimale 16.777.215. Essendoci 60x24=1440 minuti al giorno, utilizzando tre byte possono essere rappresentati circa 11.650 giorni che corrispondono a circa 31 anni.

Maggiori approfondimenti ed esempi di codifica sono presenti nella nota tecnica 5T-Nota_Tecnica_BIP_Gestione_date [5] alla voce "Codifica delle date – Metodo 2".

3.5 Codifica dati cliente

I dati relativi al possessore della carta saranno codificati nel file EF Environment tramite l'iscrizione del Codice Fiscale.

3.6 Codifica EF ITP-ID

RFU

3.7 Codifica EF ITP-IDV

RFU

3.8 Codifica EF Environment

Nel file EF Environment saranno contenuti dati relativi all'azienda che ha curato la fase di emissione della carta e al suo possessore.

La scrittura di questo file è consentita solamente tramite la modalità "update" durante la sessione di personalizzazione (CP) chiave 1.

La lettura è libera.

Nome campo	Lunghezza	Offset	Descrizione	Valori ammissibili
ID Formato	1 byte	00h	Identifica il formato utilizzato per codificare dati	Vedi par. 3.8.1

Codice Azienda	1 byte	01h	Identifica l'azienda emettitrice della carta	Vedi Tabella Operatori [1]
Codice Cliente	4 byte	02h	Identifica univocamente il Cliente della singola Azienda TPL	A discrezione dell'azienda emettitrice
Profilo Cliente	1,5 byte	06h	Identifica l'appartenenza dell'utilizzatore ad una particolare profilo tariffario	Vedi par. 3.8.2
Durata profilo	1 byte	07,5h	Indica la durata del profilo cliente	00h = nessuna scadenza 01h - FFh = numero di mesi di validità dalla data di emissione
Stato Carta	1 nibble	08,5h	Stato della carta	Vedi par. 3.8.4
Data emissione	3 byte	09h	Data della prima emissione della carta	Vedi par. 3.4
Codice Fiscale	16 byte	0Ch	Codice fiscale del cliente	Vedi par. 3.8.5
Circuito Carta	1 byte	1Ch	Circuito di emissione della carta	Vedi par. 3.8.6

3.8.1 Codifica campo ID Formato

La seguente tabella definisce i valori ammissibili per il campo ID Formato. Tale campo rappresenta la versione della mascheratura dati (GTT o BIP) e viene richiamato in diversi EF.

Valore sull' EF	Revisione/Circuito	Note
00h	GTT	
01h	GTT	
02h	BIP 2.2	Prima implementazione on field
03h	BIP 2.3	Aggiunta firma estensioni
04h	BIP 2.4	EF IPT, circuito su AID DF1, tolto circuito da EF Env.
05h	BIP 2.5 / BIP 3.0 / BIP 3.1	EF IPT-ID, EF IPT-TDV, profilo utenti, durata profilo, … (vedi tabella 1.3)

3.8.2 Codice profilo cliente

I clienti verranno profilati utilizzando la seguente codifica: 1 nibble per indicare il CCA di appartenenza (CSR per i profili regionali) e 1 byte il codice del profilo.

Per maggiori dettagli consultare l'apposita nota tecnica (*5T_Nota_Tecnica_BIP_Tabella_Profili* [2]).

3.8.3 Durata profilo

Indica l'eventuale scadenza del profilo cliente. Il valore 0 indica nessuna scadenza, un valore >0 indica il numero di mesi di validità del profilo dalla data di emissione. La data di emissione non deve essere modificata.

3.8.4 Codice stato carta

Durante l'utilizzo le smartcard si possono trovare in differenti stati logici.

Distinguiamo gli stati logici della carta descrivendo il ciclo delle fasi di utilizzo che sono state previste.

Le carte arrivano dalla fabbrica nello stato di **pre-personalizzate**. Questo stato corrisponde a carte che hanno già subito il processo di pre personalizzazione che consiste nell'inserimento del numero seriale e nel caricamento delle chiavi di sicurezza tramite l'utilizzo delle SAM-CPP.

La carta viene successivamente emessa dalla singola azienda effettuando la personalizzazione dei dati effettuando con l'inserimento del profilo relativo al cliente, in questo stato diremo che la carta è **Personalizzata**, pronta quindi per essere utilizzata.

- **Pre-Personalizzata**
- **Personalizzata**

In seguito la tabella dei valori associati ai codici di stato carta:

Valore	Stato carta associato
0h/1h	Carta pre-personalizzata (vergine)
2h	Carta Personalizzata
RFU	

Durante l'utilizzo da parte dell'utente la carta può essere posta nello stato di Black Listed, quindi bloccata, se essa risulta presente nella relativa lista. Per portare lo stato logico della carta in Black Listed il validatore oppure lo strumento di lettura/scrittura dovrà utilizzare il comando di “Invalidate” presente nel sistema operativo. Il comando dovrà operare sulla ADF Trasporti sospendendone temporaneamente le funzionalità della carta fino allo sblocco della carta effettuabile presso le biglietterie aziendali autorizzate dotate di appositi terminali di lettura/scrittura.

3.8.5 Codifica codice fiscale

Il codice fiscale del possessore della smart card verrà codificato nel formato indicato dal decreto ministeriale del 23 dicembre 1976 in formato ASCII ISO 646.

Di seguito viene illustrato un esempio di codifica.

Mario Pautasso, nato il 9 novembre 1974 a Torino: PTS MRA 74S09L219Q

Esempio di codifica codice fiscale in formato ASCII ISO646															
P	T	S	M	R	A	7	4	S	0	9	L	2	1	9	Q
50h	54h	51h	4Dh	52h	41h	37h	34h	53h	30h	39h	4Ch	32h	31h	39h	51h

3.8.6 Codifica circuito carta

Questo campo identifica il circuito di provenienza della smart card. Di seguito sono riportati i possibili valori di tale campo:

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

3.9 EF Contract list

Il file EF Contract List conterrà l'indicazione dei contratti presenti sulla carta e dei relativi contatori ad essi associati. Esso sarà utile per velocizzare le attività di lettura dei contratti durante le fasi di verifica e controllo.

La scrittura di questo file è consentita tramite la modalità “update” durante la sessione di validazione, rinnovo o ricarica (a partire dalla SAM-CV) con la chiave 3.

Nel caso di aggiunta di nuovi contratti oppure di cancellazione di contratti preesistenti, il terminale di vendita dovrà obbligatoriamente aggiornare il relativo campo valore nel presente file.

Nel caso di TDVE scaduti, il relativo campo nel presente file potrà essere aggiornato dai terminali di validazione.

La lettura è libera.

Nome campo	Lunghezza	Offset	Descrizione	Valori ammissibili
ID Formato	1 byte	00h	Identifica il formato utilizzato per codificare dati	Vedi par. 3.8.1
Codifica contratto sul record numero 1	3 byte	01h	Vedi tabella successiva	Vedi tabella successiva
.....	.....	.....	.....	.....
Codifica contratto sul record numero 8	3 byte	16h	Vedi tabella successiva	Vedi tabella successiva
RFU	4 byte	19h		

Codifica contratto sul record numero n	3 Byte	1 Byte	Codice azienda che ha emesso il contratto	Vedi Tabella Operatori [1]
		1 Nibble H	Tipo di contratto	Fh = estensione del contratto. La codifica delle tipologie di contratto è lasciata alla singola azienda. Valori da 0h

		1 Nibble L	Validità del contratto	0h non valido/scaduto 1h valido
		2 Nibble	Contatori associati al contratto	Nibble H – contatore X, X:=1,…,9 Nibble L – contatore Y, Y:=1,…,9 Y≠X 0h = nessun contatore associato

3.10 **EF Contracts**

Nel file EF Contratti saranno contenuti dati relativi ai contratti venduti.

La scrittura di questo file è consentita:

- tramite la modalità “update” durante sessione personalizzazione vendita con chiave 2
- tramite la modalità “write” durante la sessione di validazione con chiave 3.

La lettura è libera.

Per i TDVE che lo prevedono le date di inizio e fine validità dovranno essere impostate dal validatore al primo utilizzo del titolo (prima validazione).

Per tutti i TDVE il calcolo della firma (MAC contratto) dovrà essere effettuato considerando le date di inizio e fine validità a 0.

Per tutti i TDVE le date di inizio e fine validità sono da scrivere in complemento a 1 in modo da aumentare il livello di sicurezza del sistema BIP. Così facendo un’eventuale azione fraudolenta per mezzo di SAM-CV potrebbe solamente retrodatare la validità del TDVE.

Ogni azienda appartenente al sistema BIP potrà scrivere o aggiornare il proprio contratto in questo file.

La struttura dei contratti è formata da una parte a campi fissi, sempre presenti in qualsiasi tipologia di contratto, localizzati a offset definiti. Altre informazioni supplementari che caratterizzano il singolo contratto verranno inserite in aggiunta ai campi fissi in modalità TAG-VALUE. Le informazioni aggiuntive non avranno un ordine fisso ma potranno essere individuate tramite i loro tag.

Un TDVE non potrà occupare più di 3 record.

La struttura del contratto si compone dei seguenti gruppi di valori:

- informazioni relative all'azienda emettitrice
- informazioni relative alla tipologia di contratto
- validità temporale
- zone di competenza
- descrizione O/D
- firma Operatore TPL

Nome campo	Lunghezza	Offset	Descrizione	Valori ammissibili
Codice Azienda	1 byte	00h	Identifica l'azienda	Vedi Tabella Operatori [1]

Emettitrice del contratto			emettitrice del contratto	
ID Formato	1 byte	01h	Identifica il formato utilizzato per codificare dati	Vedi par. 3.8.1
RFU	1 byte	02h	RFU	RFU
Codice tariffa aggiuntiva	1 byte	03h	Codice tariffa ATI	Codice tariffa ATI
Codice Tariffa	2 byte	04h	Codice listino vendita titoli della singola azienda	Codice in formato numerico
Seriale di emissione del contratto	3 byte	06h	Numero in formato binario	Seriale univoco a livello aziendale del contratto
Periodo di validità-start	3 byte	09h	Data di inizio validità del contratto oppure inizio validità dalla prima timbratura validazione	Vedi par. 3.4
Periodo di validità-end	3 byte	0Ch	Data di fine validità del contratto oppure fine validità dalla prima validazione	Vedi par. 3.4
Giorni di validità del contratto	1 byte	0Fh	Giorni settimanali di validità, validità festivi	BITMAP: b1= 1 valido il lunedì b2= 1 valido il martedì b3= 1 valido il mercoledì b4= 1 valido il giovedì b5= 1 valido il venerdì b6= 1 valido il sabato b7= 1 valido la domenica b8= 1 valido tutti i giorni festivi
SAM serial number	4 byte	10h	Serial number del SAM che ha emesso il TDVE	
SAM counter	3 byte	14h	Valore del counter del SAM che ha emesso il TDVE	
TAG estensione contratto	2 byte	17h	TAG per l'estensione ad altri record della codifica del TDVE	Vedi par. 3.11
MAC contratto	4 byte	19h		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

All'offset *17h* se il valore è diverso da A000h è presente un TAG di estensione contratto.

3.10.1 Descrizione TAG estensione contratto

Il campo supplementare di "estensione contratto" indica la presenza di ulteriori record associati al presente che contengono indicazioni descrittive del contratto.

I record del file contratti sono in numero di 8, enumerati da 1 a 8.

Un contratto può essere codificato su più record, in questo caso il seguente campo descrittivo supplementare indica la concatenazione esistente tra i record associati al contratto.

Campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte	TAG	A0h per il record originale, per le estensioni vedi tabelle successive
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.

3.11 **Estensioni**

3.11.1 Estensione FORMULA

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte	segue descrizione formula	F1h - formula
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Peso delle zone di validità	1 byte	Si compone di un valore binario	0xFF = intera area oppure peso delle zone di validità (U+A=3, A+B=2, ecc.)
Codice località origine	3 byte	(Località porta)	Vedi nota tecnica Elenco_Localita_BIP [3]
Codice località destinazione	3 byte		Vedi nota tecnica Elenco_Localita_BIP [3]
Tipo espansione	1 nibble (H)	Tipo espansione se presente	0 - Non presente (niente fasce) 1 - GTT 2 - Trenitalia 3 - ExtraTo
Numero di fasce di espansione	1 nibble (L)	Numero di fasce attraversabili	Da 1 a 7 se presenti
Zone di validità	n byte	Sequenza dei valori ASCII che indicano le zone di validità	U (Urbana Torino) I (Urbana Pinerolo) A,B,C,D,E,F,G,H,L,M,N,O,P,Q,R,S,T
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero).

3.11.2 Estensione numero passeggeri

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte		A1h - numero di passeggeri trasportabili segue 1 byte
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Numero passeggeri trasportabili	1 byte		Valore binario da 1 a 255
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero).

3.11.3 Estensione titoli aziendali Trenitalia

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte		A7h - informazioni titoli Trenitalia seguono 3 byte
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Classe Titolo	1 nibble (H)	Prima, seconda classe altre tipologie da definire	Valore binario da 1 a 15
Tipologia	1 nibble (L)	Standard supplemento supplemento Eurostar supplemento alta velocità	
Fasce chilometriche	2 byte		Numero chilometri
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero).

3.11.4 Estensione O/D

Nel campo O/D sono codificate le fermate/zone ammesse per l'effettuazione della corsa.

Vengono definite innanzitutto le fermate di origine e di destinazione. A seguire vengono indicate tutte le fermate/zone intermedie ordinate in maniera sequenziale.

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte		C0h contratti con Origine-Destinazione descrizione codice fermata origine, destinazione e zone intermedie
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Codice Fermata/Zona Origine	3 byte		Codice fermata/zona Origine
Codice Fermata/Zona destinazione	3 byte		Codice fermata/zona Destinazione
Numero zone	1 byte		XXh – con XX da 1h a FFh, per i contratti con Origine-Destinazione indica il numero totale di fermate/zone intermedie
Segue una successione ordinata di x codici zone			
Codice fermata/zona intermedia	3 byte		Codice zona/area intermedia
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero). Se fossero necessari più record negli ultimi 4 byte di ognuno di essi va apposto il MAC.

3.11.5 Estensione Polimetrica

L'estensione è stata aggiunta in accordo con BIP-ToP, al fine di agevolare i loro *system integrator* nel descrivere percorsi diversi aventi stessa località di origine e di destinazione, senza elencare alcuna località intermedia. L'estensione consente infatti di identificare tali percorsi mediante un codice univoco a livello di azienda, definito "polimetrica".

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte		D0h contratti con Origine-Destinazione descrizione codice fermata origine, destinazione e codice polimetrica

Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Codice Fermata/Zona Origine	3 byte		Codice fermata/zona Origine
Codice Fermata/Zona destinazione	3 byte		Codice fermata/zona Destinazione
Distanza	1 byte	Distanza della relazione	Numero di zone attraversate, oppure numero di km, a seconda del prodotto tariffario
Codice Azienda	1 byte	00h	Identifica l'azienda cui si riferisce il codice polimetrica, secondo la Tabella Operatori [1]
Codice polimetrica	2 byte		Codice della polimetrica
RFU	13 byte	RFU	RFU
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero).

3.11.6 Estensione TDSE Plurisettimanale 180 ore

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte	segue descrizione	E0h
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Data 1	3 byte	Data di validazione della settimana 1	Vedi par. 3.4
Ore residue 1	1 byte		0 – 45 in complemento a 1
Data 2	3 byte	Data di validazione della settimana 2	Vedi par. 3.4
Ore residue 2	1 byte		0 – 45 in complemento a 1
Data 3	3 byte	Data di validazione della settimana 3	Vedi par. 3.4
Ore residue 3	1 byte		0 – 45 in complemento a 1
Data 4	3 byte	Data di validazione della settimana 4	Vedi par. 3.4

Nome campo	Lunghezza	Descrizione	Valori ammissibili
Ore residue 4	1 byte		0 – 45 in complemento a 1
RFU	7 byte		
MAC estensione	4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

I byte non utilizzati devono essere impostati a 0 (zero).

3.11.7 Record aggiuntivi

Eventuali record aggiuntivi non necessiteranno più dell'intestazione dell'estensione e avranno quindi la seguente struttura (i primi due byte saranno sempre l'estensione contratto così come descritto nel par. 3.10.1):

Nome campo	Lunghezza	Descrizione	Valori ammissibili
TAG	1 byte		Cyh – con y da 1h a Fh che indica il numero di zone intermedie nel record
Numero del record associato	1 byte	Vi sono due nibble, NH e NL con codifica in BCD. NH indica l'identificativo del record che precede NL indica l'identificativo del record che segue	00h indica che non è puntato alcun record. 02h significa che segue al record numero 2. 10h significa che non segue alcun record ma il presente è la continuazione del record numero 1.
Segue una successione ordinata di y codici zone			
Codice zona/area intermedia	3 byte		Codice zona/area intermedia
MAC estensione	Ultimi 4 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

3.11.8 Riepilogo codici estensioni

Codice estensione (TAG)	Nome estensione
F1h	Formula
A1h	Numero passeggeri
A7h	Trenitalia
C0h	O/D
Cxh (C1h – CFh)	Località intermedie
D0h	Polimetrica
E0h	TDSE Plurisettimanale 180 ore

3.12 **EF special events**

Il file *EF Special Events* è utilizzato per tenere traccia delle scritture in differita dei TDVE o delle ricariche EP precedentemente acquistati online. A ogni CCA viene quindi riservato un record per tale scopo (se necessario) e non potrà utilizzare gli altri record riservati ad altri bacini (vedi tabella seguente), questo allo scopo di **regolamentare l'accesso** a tale EF in modo da non creare **problemi di interoperabilità** delle SC a livello Regionale.

Il file è lineare ed è composto da 8 record. Le prime forniture di smartcard prevedevano solo i primi 4 record e per questo ai bacini ad oggi in esercizio o in via di implementazione sono stati assegnati i primi 4 record.

Record	CCA assegnato	Record	CCA assegnato
1	Bacino di Cuneo	5	Bacino di Novara
2	Bacino di Torino	6	Bacino di VCO
3	Trenitalia	7	RFU
4	Bacino di Alessandria	8	RFU

Nome campo	Lunghezza	Offset	Descrizione	Valori ammissibili
ID Formato	1 byte	00h	Identifica il formato utilizzato per codificare dati	Vedi par. 3.8.1
Codice Azienda Emettitrice del contratto	1 byte	01h		Vedi Tabella Operatori [1]
RFU	2 byte	02h		
Codice Tariffa	2 byte	04h	Codice listino vendita titoli della singola azienda	Codice in formato numerico
Data di vendita	3 byte	06h	Codifica temporale	Vedi par. 3.4
Seriale di emissione del contratto	3 byte	09h	Numero in formato binario	Seriale univoco a livello aziendale del contratto
Tipo dell'apparato utilizzato	1 byte	0Ch	Vedi tabella in seguito	
Codice seriale apparato di vendita/rinnovo	2 byte	0Dh	Identificatore seriale	
ID SAM di vendita	4 byte	0Fh		
RFU	8 byte	13h		
MAC special events	2 byte	1Bh		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

3.12.1 Tipo apparato Codificatore

Codice	Descrizione	Codice	Descrizione
0	Riservato	7	Vendita a bordo

1	Codificato in biglietteria o Super-rivendita	8	Centro massivo
2	POS rete vendita	9	Parcometro
3	PDA terminale di verifica	10	…
4	TVM		
5	Terminali self service		
6	Vendita tramite E-commerce		

3.13 **EF Event Log**

Il seguente file è di tipo circolare. Esso contiene 3 record di 29 byte che vengono utilizzati in maniera sequenziale per mantenere traccia delle ultime attività di check e/o verifica effettuate.

Nome campo	Lunghezza	Descrizione	Valori ammissibili
ID Formato	1 byte	Identifica il formato utilizzato per codificare dati	Vedi par. 3.8.1
Codice azienda emettitrice del contratto	1 byte	Indica l'azienda che ha emesso il contratto, o l'azienda che firma il log, nel caso del credito trasporti	Vedi Tabella Operatori [1]
Seriale del contratto	3 byte		Seriale del contratto, come in EF Contracts, o valore arbitrario nel caso di CT
Tipo operazione	1 nibble H	Definisce l'ultima operazione effettuata	0h check-in SV 1h check-out SV 2h check-in TDVE 3h check-out TDVE 4h verifica 5h check-in TDSE 6h check-out TDSE 7h Uso aziendale GTT 8h Uso aziendale GTT
Numero passeggeri saliti alla convalida	1 nibble L		
Data di convalida	3 byte	Indica la data in cui è stata eseguita l'operazione	Vedi par. 3.4
Fermata / area operazione	3 byte		
Codifica linea	3 byte		
Codifica corsa	3 byte		
Checkin – importo scalato Checkout - Importo riaccreditato	2 byte		Valore >= 0 che esprime gli €cent.

Data di convalida del primo check in regime di integrazione	3 byte		Vedi par. 3.4
Credito totale scalato a partire dalla prima validazione in regime di integrazione	2 byte		
Num. Record contratto	1 Nibble H		Da 1 a 8 indica record di EF Contracts Fh per utilizzo EP
Km percorsi al momento checkout	1,5 byte	Per agevolare il calcolo delle tariffe in integrazione.	
MAC event log	2 byte		Vedi nota tecnica BIP Firma_e_Verifica_SC [2]

È importante notare come nel caso di utilizzo di CT, i campi “Codice azienda emettitrice del contratto” e “Seriale del contratto” non fanno riferimento ad alcun contratto presente in “EF Contracts”, dunque in questo caso si assume che l’azienda emettitrice del contratto sia quella presso la quale il CT viene utilizzato (che in effetti grazie all’utilizzo del CT garantisce al cliente BIP un diritto di accesso, alla stregua di un contratto). L’azienda emettitrice del contratto, quindi, nel caso del CT sarà sempre anche quella che scrive il record di EF Event Log ad esso relativo.

Allo stesso modo, il record “Seriale del contratto”, non può essere valorizzato come nel caso di un contratto scritto nell’EF Contracts, quindi è ammissibile sia il valore 000000h, sia un qualsiasi altro valore arbitrario a discrezione dell’azienda (ad es. nel caso di GTT viene utilizzato per tenere traccia dell’accesso in metropolitana).

4. Utilizzo del credito trasporti

4.1 Introduzione

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 Calypso revision 3.1.

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

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

La lettura dello stato dello SV è libera.

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

Per stornare parzialmente o totalmente l'ultimo addebito è richiesto che l'operazione possa essere effettuata in una sessione sicura Calypso tramite l'utilizzo di moduli SAM-CV.

Il modulo SAM che effettua lo storno può differire da quello che ha effettuato il decremento.

4.2 Logica applicativa di utilizzo del Credito Trasporti

Per Credito Trasporti si intende un titolo a consumo prepagato.

La tipologia di Titolo di Viaggio acquistata tramite il Credito Trasporti è sempre la Corsa Semplice in ambito urbano ed un Origine/Destinazione in ambito extraurbano.

Il sistema di bordo (validatore) deve essere in grado di calcolare la tariffa corretta per ogni viaggio e di decrementarla dal contratto Credito Trasporti aggiornando l'importo residuo.

L'importo verrà calcolato secondo il Tariffario Regionale vigente.

- ✓ La funzione di "Check-in/check-out" si applica soltanto al servizio extraurbano ed alle linee extraurbane abilitate al servizio urbano. Il cliente deve convalidare sia in salita che in discesa. In salita, il validatore calcola l'importo corrispondente tra l'origine (fermata di salita) ed il capolinea (destinazione). Tale importo è decrementato dal valore del CT con l'esecuzione del comando di SV Debit e, contemporaneamente, vengono memorizzati in un campo temporaneo sulla smart card (file di Log) le informazioni relative alla fermata di salita ed all'ammontare addebitato. Se l'importo residuo del CT non è sufficiente, il saldo sulla smart card assumerà valori al di sotto del minimo credito consentito. In discesa (check-out), il validatore ricalcola l'importo corrispondente relativo alla corsa realmente effettuata e, nel caso che l'importo

dovuto fosse minore del valore già decrementato, procederà automaticamente al riaccredito della differenza operando un comando di SV Undebit.

- ✓ Nel caso in cui il cliente non effettui il check-out il CT rimarrà al valore decrementato, l'importo pagato sarà quindi equivalente all'intera corsa (origine-capolinea).

- ✓ L'applicazione SV a bordo della smartcard utilizza 3 byte per memorizzare e gestire l'ammontare del CT. Tale valore è un numero con segno ed ha il seguente range: da -8.388.608 a +8.388.607. Nel progetto BIP, l'applicazione di SV non prevede l'utilizzo di valori negativi limitando così il range: da 0 a +8.388.607. Per potere gestire valori di credito negativi (così come richiesto dagli opertatori in sede Regionale) si è deciso di realizzare una logica applicativa che interpreta il contenuto dello SV seguendo alcune direttive:

	Limite inferiore	Zero logico	Limite superiore
Range effettivo dell'EP (valore numerico nell'EP)	0	+4.194.304	+8.388.607
Valore interpretato dal SW (€cent)	-4.194.304	0	+4.194.303
Valore in €	-41.943,04	0	+41.943,03

Quindi uno SV che contiene il valore +4.194.304 (0x400000) esprime in realtà una cifra, per il circuito BIP, pari a € 0 (zero). Si tratta quindi di effettuare una semplice "conversione" sottraendo al valore letto dalla smartcard la costante 4.194.304. Il valore letto dall'EP e "convertito" come appena descritto è espresso in €cent e va quindi ancora diviso per 100 (cento) per ottenere la cifra in €.

Esempio 1

Credito del cliente: +10,50 €

Valore dell'EP	+4.195.354
Valore interpretato dal SW (€cent)	+1050
Valore in €	+10,50

Esempio 2

Credito del cliente: -7,20 €

Valore dell'EP	+4.193.584
Valore interpretato dal SW (€cent)	-720
Valore in €	-7,20

Il CT può essere ricaricato presso i punti vendita dell'azienda che ha emesso la smart card oppure presso la rete di vendita degli altri operatori di trasporto aderenti al BIP.

Il CT può essere utilizzato per effettuare l'acquisto/pagamento dei singoli Titoli di Viaggio del BIP e di altri servizi di mobilità quali parcheggi di struttura, sosta, car sharing, bike sharing.

4.3 **Comandi APDU**

I comandi APDU che vengono utilizzati sulle smart card per eseguire le operazioni di incremento e decremento del Credito Trasporti sono i seguenti:

Calypso Rev. 2	Calypso Rev. 3
Get EP	SV Get
Debit EP	SV Debit
Undebit EP	SV Undebit
Reload EP	SV Reload

I singoli comandi vengono descritti in dettaglio di seguito.

La transazione di Reload (incremento del valore del Credito Trasporti), di Purchase (decremento del valore) oppure di Purchase-Cancellation (riaccredito dell'ultimo pagamento) consiste nella sequenza ordinata di due comandi; il primo è il *Get EP/SV Get* seguito dal comando di *Reload EP/SV Reload* per la ricarica, di *Debit EP/SV Debit* per il pagamento oppure dal comando *Undebit EP/SV Undebit* per la cancellazione totale o parziale dell'ultimo pagamento. La sequenza può essere eseguita più volte, compatibilmente con limitazioni imposte dai singoli comandi, se eseguita all'esterno di una sessione. Può essere eseguita una sola volta all'interno di una sessione.

La transazione viene considerata eseguita correttamente quando si conclude con successo oppure, qualora venga eseguita all'interno della sessione, questa viene terminata correttamente.

Per dispositivi Rev. 2 la classe da utilizzare (byte CLA) è 0xFA, per la Rev. 3 invece è 0x00.

4.3.1 Transazione interrotta prematuramente

Una transazione di Borsellino Elettronico viene correttamente eseguita quando il terminale di scrittura/lettura riceve dalla carta la risposta di corretta esecuzione dell'ultimo comando della transazione e, successivamente, è in grado di far verificare al SAM la correttezza della firma di transazione inviata dalla carta.

È possibile che una transazione s'interrompa prematuramente. Ciò avviene quando la comunicazione tra la carta ed il terminale si interrompe dopo che quest'ultimo ha inviato l'ultimo comando della sequenza.

Il terminale, non ricevendo risposta dalla carta, non è in grado di stabilire se la carta ha effettivamente eseguito correttamente il comando oppure lo abbia ignorato.

Al fine di verificare lo stato della carta e ripristinare il suo corretto valore è necessario che la carta venga immediatamente ripresentata al terminale.

Questo, tramite il comando di *Get EP/SV Get*, è in grado di verificare lo stato della carta e verificare i seguanti casi:

- il comando è stato correttamente processato, allora i valori di risposta alla *Get EP/SV Get* indicano che il valore sequenziale di operazione sulla carta è stato incrementato. In questo caso il lettore può procedere alla verifica della firma carta da parte del SAM,
- il comando non è stato processato, infatti, il valore sequenziale di operazione sulla carta non è stato incrementato. La transazione deve essere interamente ripetuta.

4.4 Get EP / SV Get

Il comando Get EP/SV Get può essere eseguito dopo aver selezionato la ADF EP. Esso fornisce numerose informazioni relative allo stato dell'EP, indica il valore corrente (amount), lo stato dell'ultima transazione effettuata ed altri dati necessari alle successive attività di incremento-decremento.

Il comando non effettua alcuna modifica ai file. Esso può essere eseguito solamente allo scopo di ottenere informazioni riguardanti lo stato dell'EP.

L'esecuzione del comando è libera (free).

SV Get / Get EP	
CLA	FAh per prodotti Rev. 2 00h per prodotti Rev. 3
INS	7Ch
P1	00h
P2	07h->preparazione alla ricarica, segue il comando Reload 09h->preparazione al pagamento, segue il comando Debit oppure di Undebit
Lc	assente
dati	assenti
Le	21h se P2=07h 1Eh se P2=09h

Dati di output del comando		
Offset	**Dimensione**	**Valore**
00h	1h	KVC della chiave associata al successivo comando
01h	2h	Current card EP transaction number (numero di operazione

		sequenziale sulla carta)
03h	3h	Previous CryproLo-Ultimi 3 byte (meno significativi) relativi alla firma della transazione precedente
06h	2h	Card Challenge 2 byte
08h	3h	Current balance – valore numerico corrente dell'EP
Caso di una operazione di Reload P2=07h		
0Bh	3h	3 byte che indicano la data dell'ultima ricarica effettuata su 3 byte
0Eh	1h	Load KVC, valore KVC della chiave utilizzata per l'ultima ricarica (Key#2 ADF EP)
0Fh	1h	1 byte a 00h RFU
10h	3h	Load balance – valore dell'EP dopo l'ultima ricarica
13h	3h	Load Amount – valore dell'ultimo incremento di ricarica
16h	2h	RFU da lasciare a 00h
18h	4h	SAM ID - Serial Number del SAM che ha consentito l'ultima ricarica
1Ch	3h	SAM Transaction Number- numero sequenziale di operazione di ricarica della SAM che ha consentito l'ultima ricarica
1Fh	2h	Load Card Transaction Number- numero sequenziale di operazione di ricarica della carta
Caso di una operazione di Debit/Undebit P2=09h		
0Bh	2h	Purchase amount
0Dh	4h	Purchase Date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h
11h	1h	Purchase KVC, indica di chiave necessaria per il successivo comando di Debit-Undebit (Key #3 ADF EP)
12h	4h	Purchase SAM ID, identificativo seriale del SAM che ha consentito l'ultima operazione di Debit
16h	3h	Purchase SAM transaction number – numero sequenziale di operazione eseguita sul SAM che ha consentito l'ultima operazione di Debit
19h	3h	Purchase Balance, valore del B.E. (amount) dopo l'operazione di Debit
1Ch	2h	Purchase Card transaction number, numero sequenziale di operazione sulla carta

Risposte al comando-Status Words

SW1-SW2	descrizione
67 00h	Le non corretto
69 85h	Seconda operazione di EP non consentita all'interno di una sessione
6A 81h	Parametro P2 non corretto
6A 86h	Le non correttamente impostato rispetto a P2
90 00h	Comando eseguito correttamente

4.5 Debit EP / SV Debit

Il comando *Debit EP / SV Debit* deve essere eseguito successivamente al comando di Get EP/SV Get.

Se eseguito correttamente, esso modifica lo stato dell'EP decrementando il valore corrente (amount) dell'importo indicato ed aggiornando automaticamente il file di Purchase Log, sovrascrivendo l'ultimo record con i dati della transazione appena conclusa.

Il comando verrà rifiutato se si tenta di decrementare un valore maggiore del valore corrente dell'EP.

La corretta esecuzione del comando è vincolata alla verifica della firma valutata dal SAM.

Debit EP / SV Debit	
CLA	FAh per prodotti Rev. 2 00h per prodotti Rev. 3
INS	BAh
P1	SAM Challenge – MSbyte of SAM challenge - byte numero 1 del SAM challenge
P2	SAM Challenge - byte numero 2 del SAM challenge
Lc	14h – numero di byte in input
data	Vedi tabella seguente
Le	03h
Data Out	3 LSByte della firma calcolata dalla carta della transazione

dati di input del comando		
Offset	**Dimensione**	**Valore**
00h	1h	SAM Challenge – LSbyte of SAM challenge - byte numero 3 del SAM challenge
01h	2h	Purchase amount – valore con segno (<=0)
03h	4h	Purchase Date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h
07h	1h	Purchase KVC, indica di chiave utilizzata per l'esecuzione del comando
08h	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione
0Ch	3h	SAM Transaction Number- numero sequenziale di operazione di Debit del SAM utilizzato per l'operazione
0Fh	5h	5 byte (Msbyte) relativi alla firma dell'operazione calcolati dal SAM

Risposte al comando SW

SW1-SW2	**descrizione**
62 00h	Comando eseguito correttamente, la risposta del comando viene rimandata successivamente al termine della sessione corrente
64 00h	Buffer di sessione pieno, operazione non consentita
67 00h	Lc non corretto
69 00h	Operazione non eseguita poiché il numero di operazioni ha raggiunto il massimo valore consentito.
69 85h	Operazione non eseguita per i seguenti possibili motivi: ● DF EP è stata invalidata, ● non è stato precedentemente eseguito un comando Get EP, ● il valore dell'EP (amount) non è sufficiente per eseguire la Debit.
69 88h	La firma del SAM è incorretta
90 00h	Comando eseguito correttamente.

Se il comando di Debit EP viene eseguito correttamente esso automaticamente effettua un aggiornamento di un record del file di Purchase Log.

Il record viene sovrascritto con i seguenti dati:

Record corrente aggiornato del file Purchase Log		
Offset	**Dimensione**	**Valore**
00h	2h	Purchase amount – valore decrementato all'EP
02h	4h	Purchase Date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h (valore indicato nei dati di input del comando)
06h	1h	Purchase KVC, indica di chiave utilizzata per l'esecuzione del comando
07h	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)
0Bh	3h	SAM Transaction Number- numero sequenziale di operazione di Debit del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)
0Eh	3h	Valore corrente dell'EP (amount) dopo l'operazione di decremento
11h	2h	Card Transaction Number- numero sequenziale corrente relativa alla operazione di Debit della carta incrementato dopo l'ultimo comando eseguito
13h	3h	CryptoLo – firma del comando elaborata dalla carta
16h	7h	Dati non utilizzati da lasciati a 00h....00h

4.6 Undebit EP / SV Undebit

Il comando Undebit EP deve essere eseguito successivamente al comando di Get EP/SV Get la precedente operazione sul borsellino elettronico deve essere un comando di Debit EP/SV Debit.

Lo scopo del comando di Undebit è di ri-accreditare l'intero valore, oppure una sua parte, sottratto durante l'ultima operazione di Debit.

Se eseguito correttamente, esso modifica lo stato dell'EP incrementando il valore corrente (amount) di un importo al massimo uguale all'ultimo valore decrementato. Analogamente al comando di Debit esso aggiorna automaticamente il file di Purchase Log sovrascrivendo l'ultimo record con i dati della transazione appena conclusa.

La chiave utilizzata per eseguire il comando è la stessa utilizzata per il comando di Debit.

Undebit EP/ SV Undebit	
CLA	FAh per prodotti Rev. 2

	00h per prodotti Rev. 3
INS	BCh
P1	SAM Challenge – MSbyte of SAM challenge - byte numero 1 del SAM challenge
P2	SAM Challenge - byte numero 2 del SAM challenge
Lc	14h – numero di byte in input
data	Vedi tabella seguente
Le	03h
Data Out	3 LSByte della firma calcolata dalla carta della transazione

dati di input del comando		
Offset	**Dimensione**	**Valore**
00h	1h	SAM Challenge – LSbyte of SAM challenge - byte numero 3 del SAM challenge
01h	2h	Purchase undebit amount – valore da incrementare all'EP compreso tra 000001h e l'ultimo valore decrementato
03h	4h	Purchase undebit date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h
07h	1h	Purchase KVC, indica di chiave utilizzata per l'esecuzione del comando
08h	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione
0Ch	3h	SAM Transaction Number- numero sequenziale di operazione di Undebit del SAM utilizzato per l'operazione
0Fh	5h	5 byte (MSbyte) relativi alla firma dell'operazione calcolati dal SAM

Risposte al comando SW

SW1-SW2	**descrizione**
62 00h	Comando eseguito correttamente, la risposta del comando viene rimandata successivamente al termine della sessione sicura
64 00h	Buffer di sessione pieno, operazione non consentita
67 00h	Lc non corretto
69 00h	Operazione non eseguita poiché il numero di operazioni ha raggiunto il massimo valore consentito.

69 85h	Operazione non eseguita per i seguenti possibili motivi: ● DF EP è stata invalidata, ● non è stato precedentemente eseguito un comando Get EP, ● l'ultima operazione eseguita non è stata una Debit.
69 88h	La firma del SAM è incorretta
6A 80h	Valore dell'incremento incorretto
90 00h	Comando eseguito correttamente.

Se il comando di Unebit EP viene eseguito correttamente esso automaticamente effettua un aggiornamento di un record del file di Purchase Log.

Il record viene sovrascritto con i seguenti dati:

Record corrente aggiornato del file Purchase Log		
Offset	**Dimensione**	**Valore**
00h	2h	Purchase undebit amount – valore inecrementato all'EP
02h	4h	Purchase undebit date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h (valore indicato nei dati di input del comando)
06h	1h	Purchase KVC, indica la chiave utilizzata per l'esecuzione del comando
07h	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)
0Bh	3h	SAM Transaction Number- numero sequenziale di operazione di Undebit del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)
0Eh	3h	Valore corrente dell'EP (amount) dopo l'operazione di incremento
11h	2h	Card Transaction Number- numero sequenziale dell'operazione di Debit della carta incrementato dopo l'operazione
13h	3h	CryptoLo – firma del comando elaborata dalla carta
16h	7h	Dati non utilizzati da lasciati a 00h....00h

4.7 **Reload EP APDU**

Il comando Reload EP deve essere eseguito successivamente al comando di GET EP.

Se eseguito correttamente, esso modifica lo stato corrente dell'EP incrementando il valore corrente (amount) dell'importo indicato. Esso aggiorna automaticamente il file di Load Log sovrascrivendo l'ultimo record con i dati della transazione appena conclusa.

Il comando viene rifiutato se l'ammontare dell'incremento genera un totale maggiore del massimo consentito.

APDU Debit EP	
CLA	FAh per prodotti Rev. 2 00h per prodotti Rev. 3
INS	B8h
P1	SAM Challenge – MSbyte of SAM challenge - byte numero 1 del SAM challenge
P2	SAM Challenge - byte numero 2 del SAM challenge
Lc	17h – numero di byte in input
data	Vedi tabella seguente
Le	03h
Data Out	3 LSByte della firma calcolata dalla carta della transazione

dati di input del comando		
Offset	**Dimensione**	**Valore**
00h	1h	SAM Challenge – LSbyte of SAM challenge - byte numero 3 del SAM challenge
01h	3h	Reload Date – data codificata sugli ultimi 3 byte meno significativi, il primo byte si lascia a 00h
04h	1h	Load KVC, indica di chiave utilizzata per l'esecuzione del comando
05h	1h	RFU- non utilizzato lasciare a 00h
06h	3h	Reload amount- valora da incrementare (>=0)
09h	2h	RFU -Non utilizzati porre a 00 00h
0Bh	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione
0Fh	3h	SAM Transaction Number- numero sequenziale di operazione di Reload del SAM utilizzato per l'operazione
12h	5h	5 byte (Msbyte) relativi alla firma dell'operazione calcolati dal SAM

Risposte al comando SW

SW1-SW2	descrizione
62 00h	Comando eseguito correttamente, la risposta del comando viene rimandata successivamente al termine della sessione corrente
64 00h	Buffer di sessione pieno, operazione non consentita
67 00h	Lc non corretto
69 00h	Operazione non eseguita poiché il numero di operazioni ha raggiunto il massimo valore consentito.
69 85h	Operazione non eseguita per i seguenti possibili motivi: ● DF EP è stata invalidata, ● non è stato precedentemente eseguito un comando Get EP, ● il valore da incrementare è troppo elevato, il totale sarebbe maggiore del consentito FFFFFEh.
69 88h	La firma del SAM è incorretta
90 00h	Comando eseguito correttamente.

Se il comando di Reload EP viene eseguito correttamente esso automaticamente effettua un aggiornamento di un record del file di Load Log.

Il record viene sovrascritto con i seguenti dati:

Record corrente aggiornato del file Load Log		
Offset	**Dimensione**	**Valore**
00h	3h	Load Date – data codificata su3 byte (valore indicato nei dati di input del comando)
03h	1h	Load KVC, indica di chiave utilizzata per l'esecuzione del comando (Key #2 ADF EP)
04h	1h	RFU- non utilizzato lasciare a 00h
05h	3h	Valore corrente dell'EP (amount) dopo l'operazione di ricarica
08h	3h	Load amount – valore incrementato all'E.P.
0Bh	2h	RFU- non utilizzato, lasciare a 00 00h
0Dh	4h	SAM ID - Serial Number del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)
11h	3h	SAM Transaction Number- numero sequenziale di operazione di Reload del SAM utilizzato per l'operazione (valore indicato nei dati di input del comando)

14h	2h	Card Transaction Number- numero sequenziale relativo all'operazione di Reload della carta incrementato dopo l'operazione
16h	3h	CryptoLo – firma del comando elaborata dalla carta
19h	4h	RFU - dati non utilizzati da lasciati a 00h

5. Le carte a basso costo

Nel sistema BIP all'interno delle varie comunità tariffarie possono essere utilizzate delle carte a memoria di basso costo per la vendita di Titoli di Viaggio impersonali da utilizzarsi occasionalmente, quali ad esempio la corsa semplice, il carnet di biglietti e le carte valore.

Possono essere utilizzate carte a memoria, impropriamente chiamate "Chip on Paper" per il fatto che sono costruite utilizzando un supporto cartaceo di spessore 0,4mm e non una laminazione plastica come prevista dalle normative ISO7810 di spessore 0,78mm.

Si consiglia di utilizzare Chip on Paper con una capacità di memoria di almeno 512 bit.

È pertanto lasciata facoltà ai diversi Centri di Controllo Aziendale, l'implementazione e la gestione di tali supporti.

6. Caratteristiche costruttive

6.1 Durata della smart card

I processi produttivi delle carte 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 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).