GARA EUROPEA
PER LA FORNITURA DI SMART CARD PER GLI ATENEI PIEMONTESI
(N. 06_17)

CAPITOLATO SPECIALE D'APPALTO

(REQUISITI TECNICI)

Gennaio 2018

SOMMARIO

1 Oggetto dell'appalto 3
2 Consegna e Durata 3
3 Specifiche tecniche delle smart card 4
4 Verifica del lotto di pre-fornitura 15
5 Verifica e Accettazione della fornitura 17
6 Fornitura difettosa / non funzionante 17
7 Penali 17

1 OGGETTO DELL'APPALTO

Oggetto dell'appalto è la fornitura di 77.000 smart card con tecnologia Java Card-Dual Interface secondo le specifiche descritte nel presente documento.

Le specifiche tecniche delle smart card riportate nel seguito sono definite in modo che le card possano supportare i seguenti servizi:

- identificazione a vista all'interno degli Atenei;
- accesso e pagamento del servizio di ristorazione gestito dall'E.DI.S.U. (E.DI.S.U. Card System);
- gestione titoli di trasporto standard BIP (Biglietto Integrato Piemonte) per abbonamento al trasporto pubblico e servizi che utilizzano tale tecnologia;
- servizi del circuito Pyou Card del sistema culturale piemontese;
- Bike Sharing;
- Car Sharing;
- autenticazione ai portali degli atenei e ai servizi di e-government della P.A. con certificati digitali CNS (Carta Nazionale Servizi);
- realizzazione di documenti firmati digitalmente con certificati di sottoscrizione a valore legale.

Il layout grafico e la configurazione dei servizi a bordo del supporto è demandata da E.DI.S.U. agli erogatori dei servizi (secondo le specifiche emanate dagli Atenei), mentre la stampa degli elementi variabili sulle Card sarà effettuata dai singoli Atenei.

2 CONSEGNA E DURATA

La consegna delle 77.000 Smart Card oggetto del presente appalto dovrà avvenire, a cura e spese del Fornitore Aggiudicatario, in **due tranche** distinte da 38.500 carte ciascuna, con le seguenti modalità:

- la prima tranche da 38.500 carte con consegna **entro il 30 giugno 2018** (o comunque non oltre l'eventuale altra data che verrà comunicata dalla Stazione Appaltante), per consentire il regolare avvio delle attività di immatricolazione per l'anno accademico 2018-2019;
- la seconda tranche da 38.500 carte con consegna **entro il 30 giugno 2019** (o comunque non oltre l'eventuale altra data che verrà comunicata dalla Stazione Appaltante) – e non prima del 1° maggio 2019 –, per consentire il regolare avvio delle attività di immatricolazione per l'anno accademico 2019-2020.

Tutte le Smart Card dovranno essere consegnate presso le sedi dei singoli Atenei e dell'E.DI.S.U., situate sul territorio regionale, con modalità che saranno comunicate successivamente dalla Stazione Appaltante.

Il Fornitore effettuerà tutte le consegne dei beni oggetto della presente procedura a proprio rischio, assumendo in prima persona tutte le spese che dovessero rendersi necessarie. I rischi di perdite e/o di danni ai beni durante il trasporto sono posti a carico dell'Appaltatore.

Il contratto derivante dalla procedura avrà **decorrenza dalla data di stipula, o dall'eventuale esecuzione anticipata dello stesso, e avrà durata sino al termine di 24 mesi** decorrenti dalla data di rilascio, con esito positivo, del verbale di accettazione relativo alla prima tranche di fornitura, per consentire l'eventuale sostituzione di Smart Card difettose e non funzionanti.

3 SPECIFICHE TECNICHE DELLE SMART CARD

3.1 Certificazioni del prodotto richieste

Ciascuna smart card oggetto della fornitura dovrà essere conforme a quanto definito nelle norme e nei documenti di seguito elencati:

1. ISO/IEC 7810:2003 sezione 5.1.1 caratteristiche dimensionali
2. ISO 7810 ID-1
3. ISO/IEC 7816-1 sezione 4.2.3 superficie e il profilo dei contatti.
4. ISO/IEC 7816-1:1998 sezioni 4.2.9 e 4.2.10 test di flessione e torsione.
5. ISO 7816-6
6. ISO 7816-8
7. ISO 7816-9
8. ISO/IEC 10373:1993 e ISO/IEC 10373-1:2006
9. ISO 14443 parti da 1 a 4
10. Norme EN 1545 per la definizione del modello dati (per quanto applicabile)
11. Specifiche del sistema operativo "Calypso" – release 3.1 – reperibili sul sito del Calypso Network Association (www.calypsonet-asso.org)
12. Common Criteria EAL6+ certification for Hardware

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 sopra indicata.

3.2 Certificazione CNS

Le caratteristiche elettriche di ciascuna carta oggetto della fornitura, riguardanti la parte a contatti dovranno rispettare la normativa ISO 7816 parte 2 e 3.

In particolare dovranno essere garantiti i seguenti requisiti

- supporto a comandi e file system conformi alle specifiche CNS;
- certificazione di sicurezza Common Criteria EAL4+ secondo il protection profile CWA 14169 (Type 2 e Type 3) (Criteri non inferiori a quelli previsti dal livello di valutazione E3 e robustezza HIGH dell'ITSEC, o dal livello EAL 4 della norma ISO/IEC 15408 o superiori);
- supporto RSA supporto RSA con lunghezza delle chiavi non inferiore a 2048: richiesta di gestione a bordo chiavi crittografiche secondo l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 2048 bit. Dovranno in oltre essere in grado di utilizzare chiavi crittografiche di secure messaging DES e 3DES;

3.3 Certificazione Calypso

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.

La card dovrà essere certificata dalla CNA (Calypso Network Association)

In particolare dovranno essere garantiti le specifiche del sistema operativo “Calypso” – release 3.1 – reperibili sul sito del Calypso Network Association (www.calypsonet-asso.org).

3.4 Protocolli di comunicazione

Il protocollo a contatti delle carte dovrà essere conforme alle normative ISO 7816 parte 3.

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):

- **ProtocolType e TR2**, indica la tipologia di protocollo, i valori ammessi sono 1, 3, 5 e 7 che indica che il protocollo è pienamente conforme alle normative ISO 14443 compresa la parte 4;

- **Max_Frame_Size**, indica la lunghezza massima ammissibile di ogni pacchetto dati in trasmissione, saranno ammessi valori 07hex (frame di lunghezza 128byte) oppure 08hex (frame di lunghezza 256 byte);
- **Bit_Rate_Capability**, indica le velocità di protocollo ammesse dalla carta. L'accoppiatore ha facoltà di scegliere, in base ai valori dichiarati, velocità di bit rate superiori a quella di default, circa 106Kbps. Le velocità di trasferimento (bit rate) ammesse sono indicate nella tabella riportata di seguito (tabella 7.9.4.6 delle ISO14443-3). I valori massimi ammissibili del parametro Bit_Rate_Capability saranno:
  - Bit_Rate_Capability=B3hex, fino a 424Kbps in entrambe le direzioni.

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.								

3.5 Banda magnetica

Banda magnetica ad **alta coercitività (HICO)** sul retro.

3.6 Personalizzazione grafica

Le smart card dovranno essere fornite con una personalizzazione grafica sia sul fronte sia sul retro, con elementi grafici e testuali che verranno forniti dal CSI direttamente all'Aggiudicatario.

Entro 5 giorni solari dalla stipula del contratto, l'Appaltatore dovrà pertanto comunicare al CSI il formato/i del file grafico che intende utilizzare per il trasferimento del layout sulle smart card ai fini della stampa.

Le personalizzazioni grafiche previste interessano sia il fronte sia il retro con 4 diversi layout per il fronte e 1 layout per il retro come di seguito indicato, ciascuna personalizzazione sarà prodotta su una prefissata quantità di card destinata ad ogni ente, come da tabella:

Ripartizione card	Università degli Studi di Torino	Politecnico di Torino	Università degli Studi Piemonte Orientale	Altri
Q.tà card 1° tranche	19.000	12.500	4.500	2.500
Q.tà card 2° tranche	19.000	12.500	4.500	2.500
Q.tà card totale	**38.000**	**25.000**	**9.000**	**5.000**

La personalizzazione grafica sul fronte dovrà consentire la successiva stampa mediante termografia dei dati specifici dell'utente (dati anagrafici, foto ed altro)

Sulla smart card dovrà essere riportato il Serial Number BIP sul retro in basso a destra. I Serial Number necessari alla produzione delle smart card saranno comunicati all'appaltatore successivamente.

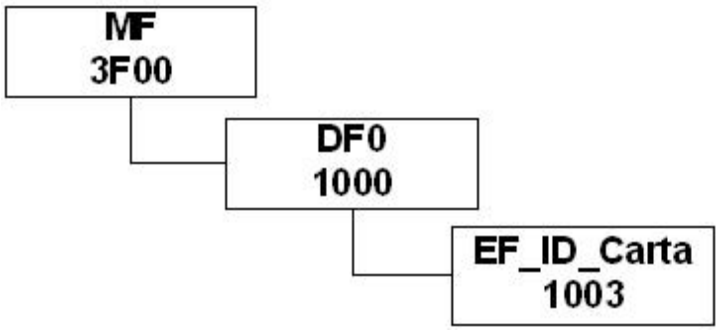
3.7 E.DI.S.U. Card System: accesso e pagamento al servizio di ristorazione

Viene richiesto che, nel funzionamento via interfaccia a contatti, l'applet dedicata all'emulazione CNS abbia carattere di priorità rispetto all'applet BIP-trasporti.

3.7.1 File System

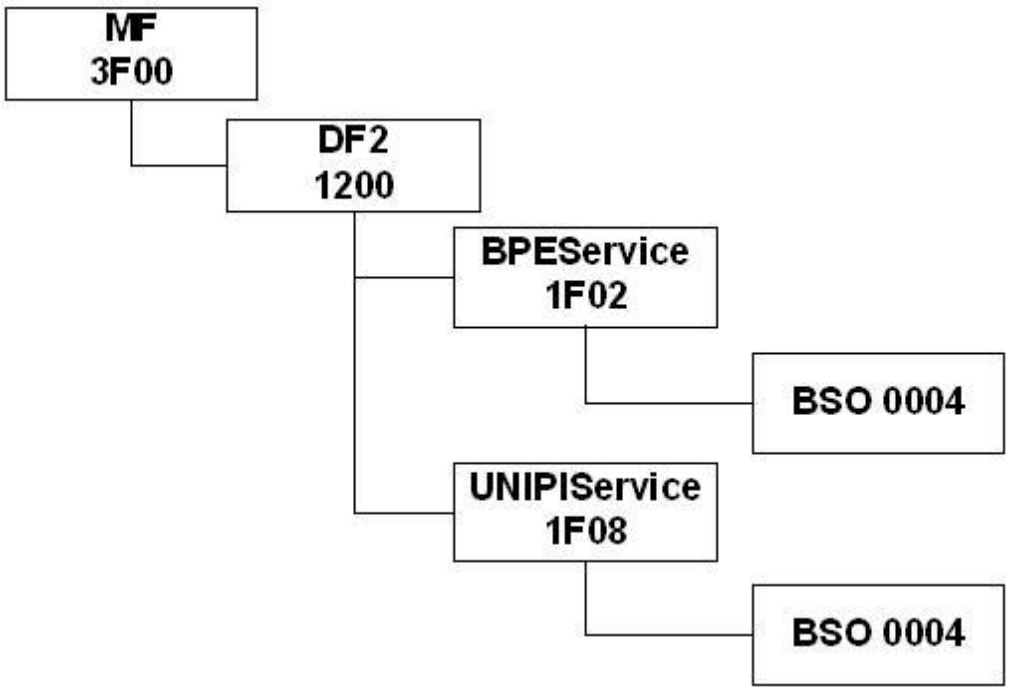
Nel prosieguo del documento, relativamente alle strutture dati, sono riportati degli identificativi ID o LID (MF/DF/EF) non univoci all'interno della smart card.

Porzione necessaria del file system CNS
Lo schema seguente descrive la porzione di file system CNS che dovrà essere creata al momento della produzione delle smart card in quanto necessaria al corretto funzionamento degli applicativi POS.



Il file EF_ID_Carta contiene il numero seriale univoco della smart card composto da 16 caratteri numerici in notazione ASCII.

File system servizi BPE E UNIPI
Il seguente disegno descrive il file system che dovrà essere creato al momento della produzione delle smart card per il servizio BPE e per il servizio UNIPI.



NB: Il DF 1F02 è il FID autorizzato da CNIPA per QSAVE Technology.

BSO
Per la produzione delle carte è necessario un solo BSO di tipo TEST (PIN) con codice 0004 in entrambi i DF.

La valorizzazione del BSO può essere fissa o derivata tramite algoritmo. La derivazione serve a migliorare la sicurezza della fase di trasporto ed è quindi preferibile alla valorizzazione fissa.

La scelta di valorizzare in modo fisso il BSO o derivarlo da algoritmo dipende dalle caratteristiche offerte dal sistema di produzione carte.

Il valore del BSO sarà comunque sempre modificato in fase di attivazione del servizio BPE.

Valorizzazione fissa del BSO
Nel caso il sistema di produzione sia in grado di valorizzare solo in modo fisso il BSO, il PIN (0004) dovrà avere il seguente valore:

KCARD_PIN1 = 0xN1 0xN2 0xN3 0xN4 0xN5 0xN6 0xN7 0xN8

Derivazione del BSO
Nel caso il sistema di produzione sia in grado di derivare la valorizzazione del BSO, il PIN (0004) dovrà essere calcolato nel modo seguente:

Il PIN viene generato tramite cifratura DES con chiave :

KCMAST1 = 0xM1 0xM2 0xM3 0xM4 0xM5 0xM6 0xM7 0xM8

dei seguenti 8 byte del CARD_ID e del byte CHECK DIGIT (file EF_ID_CARTA)..

ID = ID_CARD[15] + ID_CARD[6-12]

PIN1 = DES(ID, KCMAST1)

Il PIN1 ottenuto dalla cifratura deve essere convertito in modulo 10 per il vincolo numerico dei PIN CNS.

Access Condition
Di seguito vengono specificate le AC per il DF BPEService (1F02) e per il DF UNIPIService (1F08) e per i relativi BSO PIN 1 (0004), il securemessaging dovrà essere presente ed impostato a “no securemessaging” (0xff) per tutti i file.

DF BPEService (1F02) E UNIPIService (1F08)

ID	PATH	Tipo file	Dim	Condizioni di accesso
1F02	1200/1F02	DF	2048	**UPDATE** PIN1 (0x04) **APPEND** PIN1 (0x04) **ADMIN** PIN1 (0x04) **CREATE** PIN1 (0x04) **DEACTIVATE** NEV **ACTIVATE** NEV
1F08	1200/1F08	DF	2048	**UPDATE** PIN1 (0x04) **APPEND** PIN1 (0x04) **ADMIN** PIN1 (0x04) **CREATE** PIN1 (0x04) **DEACTIVATE** NEV **ACTIVATE** NEV

BSO PIN1(0004)

ID	PATH	Tipo file	Dim	Condizioni di accesso
0004	1200/1F02/0004	BSO		**USE** ALW

				CHANGE PIN1 (0x04) **UNBLOCK** NEV Il numero massimo di tentativi deve essere impostato a 0x0a
0004	1200/1F08/0004	BSO		**USE** ALW **CHANGE** PIN1 (0x04) **UNBLOCK** NEV Il numero massimo di tentativi deve essere impostato a 0x0a

3.8 Gestione titoli di trasporto standard BIP

Ciascuna smart card oggetto della fornitura dovrà supportare la funzionalità dello standard Calypso, rispettando in particolare le specifiche tecniche di seguito riportate.

Tale smart card a microprocessore gestisce i Titoli di Viaggio Elettronici (TDVE) ed il Credito Trasporti (SV).

Viene richiesto che, nel funzionamento via interfaccia RFID, l'applet dedicata ai trasporti abbia carattere di priorità rispetto all'applet CNS

3.8.1 Struttura del file system

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

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) né gli altri file necessari alla funzionalità dell'applicazione Calypso.

La porzione di memoria EEPROM riservata ai trasporti deve essere adeguata all'applicazione nel seguito richiesta.

3.8.2 Lista dei File presenti sotto Master File

MF / DF / EF	File type	LID	SFI	NumRec.	Recsize	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.

3.8.3 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.

3.8.4 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.

3.8.5 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	

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

3.8.6 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
Storedvalueapplication (EP)	1000	“0ETP.ICA” D380 1200 9201	304554502E494341D38012009201

3.8.7 Identificazione circuito di appartenenza

In Piemonte attualmente, oltre alle smart card universitarie oggetto del presente appalto, vi sono altre card, sempre basate su tecnologie Calypso, che offrono servizi di gestione titoli di trasporto (fra le quali la carta BIP e la carta PYOU).

Al fine di consentire il riconoscimento della tipologia di circuito originale a cui appartiene la smart card si è scelto di sfruttare il byte Application Subtype nelle Startup Information inviato nella risposta al comando di Select Application.

Startup Information

L’applicazione Calypso, nella risposta al comando di *Select Application*, deve restituire anche le *Startup information* come previsto dalle specifiche Calypso Rev. 3 (par. 5.6 e 9.2.1). Tali dati sono preceduti dal TAG 53h.

All’interno delle *Startup Information* (7 byte) si trova il byte *Application Subtype* che verrà valorizzato in fase di produzione in modo da indicare il circuito di appartenenza della carta, i restanti byte sono da valorizzare come previsto dalla specifica Calypso Rev. 3.

Codifica circuito appartenenza

Valore	Descrizione
C0h	BIP
C1h	PYOU
C2h	E.DI.S.U.
C3h	NFC
C4h	TRENITALIA
C5h	CB
…	RFU

Per le smart card oggetto del presente appalto il byte *ApplicationSubtype* legata al DF trasporti, dovrà essere valorizzato in fase di produzione con **il valore C2h**. Il

byte *ApplicationSubtype* del DF Store Value, verrà valorizzato a **20h** come da specifica Calipso v3.1.

I valori in esadecimale, da impostare in sede di produzione relativamente alla STARTUP_INFO ed al PIN sono :

- STARTUP_INFO= 0A2C23C21010FF
- PIN= 30303030

3.8.8 Chiavi di sicurezza presenti sulla carta

Su ciascuna carta oggetto della fornitura 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.

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

Le chiavi saranno di tipo DES_X.

Le attività di seguito elencate, relative alla pre-personalizzazione elettrica delle smart card (applicazione trasporti) saranno a carico del Fornitore in sede di produzione:

- caricamento delle chiavi di sicurezza (SAM CPP – fornite da CSI Piemonte)
- attivazione delle chiavi

3.8.9 Condizioni di accesso ai files

Tipi di chiavi segrete:

Key N°1 Issuerkey	Chiave di personalizzazione e pre-personalizzazione. Usata tipicamente per inserire dati generici. Può essere usata all'interno di una sessione sicura.
Key N°2 Loadkey	Chiave di ricarica. Usata tipicamente per rinnovi o ricariche di TdV. Può essere usata all'interno di una sessione sicura.
Key N°3 Debitkey	Chiave di validazione. Usata tipicamente per validare/decrementare TdV. Può essere usata all'interno di una sessione sicura.

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

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

Esistono quattro metodi di accesso per ogni gruppo:

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

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
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 :EP	DF	Session 1	Session 3	n.a.	n.a.
EF Load Log	Cyclic	always	never	never	never
EF Purchase Log	Cyclic	always	never	never	never

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

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

4 VERIFICA DEL LOTTO DI PRE-FORNITURA

Entro il termine massimo di 15 giorni solari decorrenti dalla data di comunicazione di avvenuta proposta di aggiudicazione, l'Aggiudicatario dovrà, con oneri a suo carico, predisporre e consegnare al CSI-Piemonte un lotto di pre-fornitura pari a n. 100 carte, senza personalizzazione grafica e con banda magnetica, al fine di consentire la verifica di conformità delle principali componenti (terminale e applicativi sw) che ospiteranno i servizi.

Le attività di testing saranno funzionali a verificare il funzionamento rispetto ai servizi che saranno fruiti con le carte:

- trasporti
- buoni pasto elettronici
- certificati

Entro 7 gg. **solari** dalla data di consegna del lotto di pre-fornitura, la Stazione Appaltante, di concerto con l'E.DI.S.U. e gli Atenei, provvederà alle attività di verifica di conformità dello stesso.

L'Aggiudicatario dovrà fornire tutta la documentazione per effettuare i test di funzionamento con particolare riferimento a:

- Funzionamento smart card (ai fini dell'accertamento, in corso di contratto, della presenza di smart card difettose o non funzionanti)
- Funzionamento lettore
- Funzionamento modulo trasporti
- Funzionamento/caricamento buoni pasto
- Test di caricamento certificati CNS

In caso di difformità tra i beni forniti e i beni richiesti, o in caso di eventuali anomalie o malfunzionamenti relativi anche ad uno solo degli ambiti di utilizzo del prodotto, il CSI-Piemonte provvederà a inviare all'Aggiudicatario comunicazione scritta mediante posta elettronica certificata, contenente l'informativa tecnica della problematica emersa.

L'Aggiudicatario dovrà garantire, **entro 5 gg lavorativi** dalla ricezione della comunicazione, la consegna di un secondo lotto di pre-fornitura, senza alcun addebito aggiuntivo per il CSI-Piemonte, per consentire una nuova sessione di verifica.

In caso di un secondo esito negativo delle attività di verifica della pre-fornitura il CSI si riserva la facoltà di **dichiarare la decadenza della proposta di aggiudicazione** e di procedere nei confronti del successivo migliore offerente in graduatoria.

Il positivo esito della verifica della pre-fornitura sarà certificato tramite la redazione di apposito verbale – che sarà trasmesso dal CSI all'Aggiudicatario tramite posta elettronica certificata –, dal quale dovrà risultare:

- la data di esecuzione dei test di conformità;
- l'esecutore dei test;
- la tipologia delle verifiche effettuate;
- l'esito della verifica delle funzionalità.

A seguito della trasmissione del suddetto verbale, l'Aggiudicatario dovrà procedere alla consegna della fornitura di 38.500 Smart Card, secondo le modalità e entro i termini di cui al paragrafo 2 del presente documento.

5 VERIFICA E ACCETTAZIONE DELLA FORNITURA

Entro 30 gg. solari dalla consegna della prima tranche di 38.500 Smart Card, secondo le tempistiche indicate all'articolo 2 del presente documento, previa verifica di rispondenza dei beni forniti ai beni richiesti, il CSI-Piemonte provvederà a rilasciare apposito verbale di accettazione della fornitura stessa che dovrà essere allegato alla fattura.

6 FORNITURA DIFETTOSA / NON FUNZIONANTE

Nel corso dell'esecuzione del contratto, in caso di segnalazione, da parte degli utenti, di carte difettose o non funzionanti per cause non riconducibili al normale utilizzo delle stesse, l'Appaltatore dovrà garantire la sostituzione delle smart card difettose o non funzionanti **entro 2 gg. lavorativi.**

Tale sostituzione dovrà essere garantita sino al termine di 24 mesi decorrenti dalla data di rilascio, con esito positivo, del verbale di accettazione relativo alla prima tranche di fornitura.

In caso di mancata sostituzione entro il temine indicato, il CSI si riserva di applicare le penali secondo quanto indicato al paragrafo 6.

7 PENALI

In caso di mancato rispetto da parte dell'appaltatore delle prescrizioni di cui al presente capitolato il CSI-Piemonte si riserva di applicare le penali secondo quanto di seguito indicato.

Tempi di consegna

Per ogni giorno di ritardo rispetto alle tempistiche di consegna indicate relativamente a ciascuna tranche, il CSI si riserva la facoltà di applicare una penale giornaliera pari a:

$$P_X = P_U \times (Q_T - Q_C)$$

Dove:

- P_X è l'importo totale della penale per il giorno X
- P_U è pari a 0,10 €
- Q_T è la quantità totale di carte previste da ciascuna tranche di fornitura oggetto del presente capitolato (38.500)
- Q_C è la quantità totale di carte (facenti parte della tranche di fornitura oggetto del presente capitolato) in possesso di CSI al giorno X

Forniture non conformi

In caso di mancato rispetto del termine di sostituzione delle smart card difettose o non funzionanti indicati nei precedenti paragrafi, il CSI si riserva di applicare una penale pari a € 5,00 per ogni giorno di ritardo e per ciascuna smart card.

Qualora si registrino casi di carte difettose/non funzionanti per cause non riconducibili al normale utilizzo in misura superiore allo 0,5% della fornitura, ferma restando la necessaria sostituzione delle smart card, il CSI si riserva la facoltà di applicare una penale aggiuntiva pari a € 10,00 per ogni smart card la cui difettosità ha concorso al superamento della soglia dello 0,5% sopra indicata.