Appendice 3 al
CAPITOLATO TECNICO
Verifiche Tecniche

Contratto Quadro per la Fornitura di Carte Nazionali dei Servizi
con funzione di Tessera Sanitaria, e servizi annessi
per il Sistema di Monitoraggio della Spesa Sanitaria

INDICE

1. PREMESSA

I concorrenti risultati primi nella graduatoria rispettivamente del lotto 1 e del lotto 2 dovranno fornire un Campione della fornitura con allegata dichiarazione di conformità dello stesso a tutte le specifiche tecniche e funzionalità indicate nel Capitolato tecnico, conforme al fac-simile contenuto nell'Allegato (A) della presente Appendice ed attestato di conformità alla ISO 1443 resa da un laboratorio certificato. La Consip procederà ad una verifica del Campione avvalendosi di apposito Laboratorio accreditato OCSI in grado di effettuare tutti i test di funzionalità.

Il presente documento descrive quindi gli elementi essenziali dell'attività di Verifica che sarà condotta dal Laboratorio.

Si tenga presente che quanto nel seguito riportato rappresenta in modo indicativo l'insieme dei test ai quali saranno sottoposte le smart-card oggetto di fornitura.

La verifica del Campione della fornitura è composta di due fasi: una di tipo fisico meccanico, l'altra di tipo logico.

La prima fase di verifica del Campione della fornitura prevede l'esecuzione di test fisici ed elettromagnetici, in particolare, in merito alla normativa ISO/IEC 14443 e alla ISO/IEC 7816. In ogni caso saranno effettuate verifiche sia per la componente "contactless" che "contact".

Le prove saranno effettuate su 20 carte "neo-prodotte" (da almeno 10 giorni), sia per il lotto 1 che per il lotto 2, ed i relativi test saranno strutturati secondo standard ISO 14443-1/2; saranno inoltre eseguite le prove meccaniche di resistenza e qualità (dynamic stress e torsione).

Dal punto di vista logico, la seconda fase della verifica prevede lo sviluppo di prove e test sulla struttura dati secondo le specifiche di riferimento delle CNS.

Si riportano nel seguito le specifiche generali delle due fasi sopra menzionate.

2. SET UP DI CERTIFICAZIONE 14443

Lo standard ISO 14443 definisce i requisiti dei dispositivi (smart card e reader) contactless operanti alla frequenza di 13,56MHz utilizzati nei sistemi di bigliettazione elettronica e controllo accessi. Lo schema di base di questo tipo di dispositivi prevede l'utilizzo di un microchip a radiofrequenza (inclusivo di un microprocessore e di diversi tipi di memorie) collegato ad un'antenna a loop magnetica. Il principio di funzionamento risiede nella trasmissione dell'energia a radiofrequenza necessaria per l'attivazione delle carte che vengono alimentate dal flusso magnetico generato dall'antenna del reader; Tale flusso genera una corrente indotta sull'antenna della carta tale da attivare il microchip interno alla stessa.

Lo standard ISO14443 distingue due tipologie di carte (Tipo A e Tipo B) secondo gli schemi di modulazione utilizzati per la trasmissione dei dati. Nel caso specifico delle CNS, è richiesto il solo standard di tipo B.

Per quel che riguarda le componenti applicative della card vi sono differenti standard proprietari che determinano le modalità di interazione sicura della card con il sistema reader con cui transisce (tra i più noti Mifare, Calypso, MIT, etc). Si riporta nella tabella (1) seguente lo stack protocollare complessivo (dal fisico all'applicativo) interno ad una card contactless.

	Layer	International Standard
7	Security Managment and Architecture	Soluzioni proprietarie
6	Terminal Applicative Software	
5	Data Model	
4	Card and Security Mechanism	
3	Card Data structure	CEN EN 1545
2	Card OS and Files structure & Commands	ISO 7816-4
1	Communication Interface	ISO 14443 A/B 1-4

Tabella 1: Stack protocollare Contactless

La certificazione della conformità allo standard 14443 garantisce il funzionamento specifico della carte in termini di potenze di attivazione, distanze e tempi di lettura.

Tali elementi risultano cruciali per rendere misurabile alcune modalità di funzionamento della carta e di conseguenza le modalità di utilizzo della carta da parte dell'utente stesso. In tal modo è possibile avere parametri certi e certificati per meglio definire le caratteristiche del servizio per l'utente ed in tal senso meglio regolarlo in termini di effettiva volontà di operare e/o di effettuare una specifica transizione.

In uno scenario tecnologico così delicato la garanzia di affidabilità e di interoperabilità degli apparati passa inevitabilmente dal controllo del rispetto dei requisiti a radiofrequenza definiti dallo standard. La ISO definisce nella normativa ISO10373-6 i parametri e i limiti per la verifica delle caratteristiche a radiofrequenza dei reader e delle carte per garantire la conformità alla ISO14443.

La conformità allo stardard 14443 prevede dunque un livello di testing e verifiche specifiche secondo una procedura dettagliata delle ISO10373-6.

Per quanto riguarda le carte, la test list (cfr. Tabella 2) definita dalla certificazione prevede delle prove volte soprattutto alla verifica della capacità di trasmissione e ricezione del segnale e della capacità di mantenere intatte le caratteristiche fisiche anche in condizioni limite di stress. In più viene effettuata anche la misura dei parametri costruttivi a radiofrequenza fondamentali, che sono frequenza di risonanza e fattore Q.

I riferimento normativi per la certificazione 14443 sono:

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

Le test list è la seguente:

Requirement/Test	Normative Ref.	Description
Alternating magnetic field test	ISO14443-1 Cap. 4.3	Testing stress with magnetic field at 0 A/m and 12 A/m
Minimum operating field measurement	ISO14443-2 Cap. 6.2	Measurement of H on PICC between Hmin=1.5 A/m and Hmax=7.5 A/m
Capacity of reception test	ISO10373-6 AM 02 Cap. 7.2	Verifying of the capacity of answering of the PICC in presence of different waveforms of

		interrogation
Load modulation amplitude measurement	ISO14443-2 Cap. 8.2, 9.2	Load modulation must be ≥ 30/H1,2 mvpp TX rate = 106 Kbps Fsubcarrier = 847 KHz
Resonance Frequency measurement	ISO10373-6 Cap.6.1, 6.3	
Q Factor measurement	ISO10373-6 Cap. 6.1, 6.3	Misura dell'impedenza e della frequenza (massimizzazione della parte Re)
Class 1 maximum loading effect	ISO10373-6 Cap 7.4	This measurement enable to appreciate the loading effect of PICC (Hp) under test.
Effect of type B command on type A card & effect of type A command on type B card	ISO14443-3 AM1 Cap. 5.2	
Measure of minimum interruption time to reset a card (type A only)	ISO14443-3 AM1 Cap. 5.4	Cut-off time ≤ 5 ms
Mechanical Test	ISO IEC 10373-1:	- Dinamic Bending Test - Dinamic Torsion Test

Tabella 2: Test list 14443

3. TEST SULLA STRUTTURA DATI

I test standard previsti per la struttura dati possono essere riassunti nelle seguenti specifiche prove:

- Verifica di conformità della struttura del file system;
- Verifica della personalizzazione dei dati utente;
- Verifica della personalizzazione Netlink;
- Verifica di conformità delle specifiche del sistema operativo (APDU);
- Verifica di scrittura e lettura dati tramite interfaccia contactless;
- Verifica del profilo del certificato di autenticazione;
- Verifica delle funzioni di blocco e sblocco del PIN;
- Verifica delle funzionalità delle librerie MS CSP e PKCS#11, in particolare per quanto riguarda l'autenticazione in rete tramite protocollo TLS/SSL v3;
- Verifica della generazione di chiavi di sottoscrizione e inserimento del certificato di firma digitale utilizzando la libreria con interfaccia PKCS11;
- Verifica delle funzionalità di firma digitale;
- Verifica dell'inserimento e rimozione di un nuovo servizio nell'area dedicata ai servizi aggiuntivi (DF2).

L'ambiente di test che verrà utilizzato sarà installato su più postazioni di lavoro con sistemi operativi Windows XP, Windows 7 (quest'ultimo a 64 bit), Linux Ubuntu 11.10 e MAC OS X nelle versioni a 32 e 64 bit.

ALLEGATO A – FAC SIMILE DI DICHIARAZIONE DI CONFORMITA'

Il sottoscritto _____, nato a _____ il _____C.F._____, domiciliato per la carica presso la sede societaria ove appresso, nella sua qualità di _____ e legale rappresentante avente i poteri necessari per impegnare la _____ nella presente procedura, con sede in _____, Via _____, capitale sociale Euro _____ (_____), iscritta al Registro delle Imprese di ___ al n. ___, codice fiscale n. _____ e partita IVA n. _____ (codice Ditta INAIL n. _____, Posizioni Assicurative Territoriali – P.A.T. n. _____ e Matricola aziendale INPS n. _____ CCNL applicato _____ Settore _____ tipo Ditta _____, (in R.T.I. costituito/costituendo o Consorzio con le Imprese _____ _____ _____) di seguito denominata "Impresa",

- ai sensi e per gli effetti dell'art. 76 D.P.R. 445/2000 consapevole della responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o formazione od uso di atti falsi, nonché in caso di esibizione di atti contenenti dati non più corrispondenti a verità e consapevole altresì che qualora emerga la non veridicità del contenuto della presente dichiarazione la scrivente Impresa decadrà dai benefici per i quali la stessa è rilasciata;

DICHIARA SOTTO LA PROPRIA RESPONSABILITÀ

che il Campione fornito ai fini della verifica è conforme ai requisiti minimi e alle prescrizioni indicate nel Capitolato Tecnico della presente gara, ed allega a tal fine le dichiarazioni specifiche relative alle caratteristiche tecniche del Campione medesimo.

_____, li _____

Firma

_____

Requisiti obbligatori tecnici e funzionali	Caratteristiche tecniche e funzionali del Campione
Supporto in materiale plastico, con laminazione trasparente su 2 lati, completo di antenna	Specificare tipologia di supporto fornito
Banda magnetica HiCo altezza mm. 12,75 a norma ISO/IEC	Dichiarare la conformità al requisito obbligatorio richiesto
Stampa in quadricromia per personalizzazione grafica	Specificare la tipologia di stampa proposta
Microchip dual-interface (con interfaccia contactless)	Specificare modello e produttore
Conformità allo standard ISO/IEC 7816 part 1-2 secondo quanto previsto dalla normativa vigente, in particolare dal Decreto 9 dicembre 2004 del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e finanze (avviso in G.U. 18 dicembre 2004, n. 296), "Le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi" (o successive modifiche)	Dichiarare la conformità alle parti dell'ISO/IEC 7816 come richiesto dalla normativa vigente
Conformità allo standard ISO/IEC 7810: 1995 per carta di tipo ID-1	Dichiarare la conformità al requisito obbligatorio richiesto
Conformità alla norma ISO/IEC 7816 secondo quanto previsto dal documento DigitPA "CNS - Carta Nazionale dei Servizi Functional Specification" per l'interfaccia a contatti	Dichiarare la conformità alle parti dell'ISO/IEC 7816 come richiesto dalla normativa vigente

Requisiti obbligatori tecnici e funzionali	Caratteristiche tecniche e funzionali del Campione
Rispetto delle specifiche del sistema operativo (APDU) pubblicate sul sito di DigitPA	Dichiarare la conformità del sistema operativo (APDU) rispetto alle specifiche pubblicate sul sito di DigitPA
Conformità ISO/IEC 14443 type B dell'interfaccia contactless del microchip, part 1-4	Dichiarare la conformità al requisito obbligatorio richiesto
supporto protocollo T=1	Dichiarare la conformità al requisito obbligatorio richiesto
Velocità di trasmissione ISO/IEC 14443 selezionabile fino al massimo 424 kbit/s	Dichiarare velocità di trasmissione minima e massima supportate
Certificazioni di sicurezza del microchip e del sistema operativo	Dichiarare le certificazioni di sicurezza conseguite, in particolare quelle richieste dalla normativa vigente per l'utilizzo come dispositivo sicuro per la firma digitale
coprocessore crittografico	Dichiarare la conformità al requisito obbligatorio richiesto
crittografia asimmetrica RSA con chiavi a 1024 e 2048 bit	Dichiarare la conformità al requisito obbligatorio richiesto
possibilità di generare chiavi RSA all'interno del chip	Dichiarare la conformità al requisito obbligatorio richiesto

Requisiti obbligatori tecnici e funzionali	Caratteristiche tecniche e funzionali del Campione
crittografia simmetrica DES	Dichiarare la conformità al requisito obbligatorio richiesto
crittografia simmetrica 3DES con chiavi ad almeno 128 bit	Dichiarare la conformità al requisito obbligatorio richiesto
funzione di hashing SHA-1 e SHA-256	Dichiarare la conformità al requisito obbligatorio richiesto, specificando se tali funzioni sono implementate come comando APDU o se sono assicurate in alternativa dalle librerie software PKCS#11 e MS CSP fornite contestualmente alla TS/CNS
Numero di cicli di lettura/scrittura garantiti (minimo 100.000)	Dichiarare il numero massimo di cicli garantito
Periodo garantito di ritenzione dei dati (minimo 10 anni)	Dichiarare periodo di ritenzione massimo garantito
Dimensione EEPROM (minimo 64 Kbytes)	Specificare EEPROM fornita, indicando la quantità disponibile per servizio di firma digitale e servizi aggiuntivi
Conformità del File System alla normativa vigente per la CNS, in particolare alla documentazione DigitPA dal titolo “Carta Nazionale dei Servizi – CNS - File System”	Dichiarare la conformità al requisito obbligatorio richiesto
Conformità alle specifiche Netlink, in particolare alla documentazione.	Dichiarare la conformità al requisito obbligatorio richiesto, specificando eventuali ulteriori caratteristiche tecniche e/o funzionali Netlink pubblicata dal DigitPA sulle CNS