

Allegato A - Descrizione indicativa del prodotto da fornire, i requisiti minimi dei badge bianchi con tecnologia "CRS-LIKE" o equivalente

I Badge da fornire saranno sostanzialmente costituiti da smart card aventi supporto plastico bianco, personalizzati con il solo numero seriale secondo gli specifici layout predefiniti a cura di Regione Lombardia.

Il Badge dovrà essere dotato di un microcontrollore integrato (Chip), del tipo uguale o equivalente a quello già impiegato e certificato per le CRS "Dual Interface" di Regione Lombardia.

Gli integrati attualmente certificati per le CRS di Regione Lombardia risultano a oggi essere i seguenti:

- INFINEON SLE66CLX800PE e sistema operativo interno OS Siemens CardOS V4.2c;
- ATMEL AT90SC -12872RCFT e Sistema Operativo interno OS Athena.

Caratteristiche minime da garantire:

- Almeno 32k byte di memoria EEPROM;
- Coprocessore crittografico;
- Crittografia asimmetrica RSA con chiavi 1024 bit per servizi aggiuntivi e 2048 bit per firma e CNS;
- Possibilità di generare chiavi RSA all'interno del chip;
- Crittografia simmetrica DES;
- Crittografia simmetrica 3DES con chiavi ad almeno 128 bit;
- Capacità di ritenzione dei dati di almeno 10 anni;
- Numero di cicli R/W in EEPROM maggiore di centomila;
- Interfaccia duale (a contatti e contact-less);
- Conformità alla norma ISO/IEC 7816 secondo quanto previsto dal documento AgID "CNS - Carta Nazionale dei Servizi Functional Specification" (versione 1.1.6) per l'interfaccia a contatti;
- Conformità alla norma ISO/IEC 14443 part 1-4 in modalità Type B per l'interfaccia contact-less nella banda di frequenza HF 13,56 MHz;
- Velocità di trasmissione ISO/IEC 14443 selezionabile fino ad almeno 424 kbit/s;
- Supporto protocollo T=1.

È previsto peraltro che il Badge di RL risponda alle seguenti caratteristiche fondamentali della CRS Dual Interface:

- Allineamento alle indicazioni e prescrizioni AgID "CNS - Carta Nazionale dei Servizi Functional Specification" (versione 1.1.6), che definiscono tra l'altro:
- Il protocollo di comunicazione della CRS con i terminali esterni;
- La struttura dati interna del File System della CRS;
- Il set di comandi APDU (Application Protocol Data Unit) della CRS;

Deve essere previsto che il Badge di RL, qualora equivalente, possa funzionare sugli stessi sistemi che oggi adottano i due precedenti integrati.

L'inizializzazione del protocollo di comunicazione tra un Badge di RL e un terminale lettore dovrà pertanto consentire la rilevazione di badge basati su entrambe le configurazioni, riconoscendo dinamicamente ed automaticamente i parametri di sincronizzazione per l'avvio della comunicazione contenuti nelle strutture dati ATR (Answer to Reset -ISO 7816) e ATQB (Answer to Request 8 -ISO 14443-8).

I Badge, replicheranno l'architettura interna e la struttura dati del File System delle CRS Dual Interface di Regione Lombardia limitando però gli elementi presenti e popolati solo ai dati strettamente indispensabili per la gestione delle funzioni previste nel Controllo Accessi.

Di seguito gli elementi essenziali del File System, maggiori dettagli necessari alla realizzazione dei Badge di RL saranno messi a disposizione delle ditte interessate alla gara.

In particolare nell'attuale File System sono presenti le seguenti strutture dati:

- a) MF (FID = 3F00h)
- b) EF_ATR (FID = 2F01h) - Composizione dell'ATR per la sincronizzazione con terminali di rilevazione Cless.
- c) EF_CIF (FID = FE14h) - Serial Number del Badge RL (16 numeri decimali in formato binario ovvero 8 bytes ovvero 16 nibbles).
- d) DF0 (FID = 1000h)
 - o EF_Idcarta (FID = 1003h) - Serial Number del Badge RL (16 caratteri numerici ASCII -16 bytes).
- e) DF1 (FID = 1100h)
 - o EF_Datipersonali (FID = 1102h) - Valorizzato con:
 - (1) Nome fittizio: CARL BADGE (10 caratteri alfanumerici ASCII-Convenzionale);
 - (2) Cognome fittizio: xxx.xxx.xxx.xxx (12 caratteri numerici ASCII - ultimi 12 caratteri del Serial Number del Badge);
 - (3) Pseudo Codice Fiscale: CARL.xxx.xxx.xxx.xxx (16 caratteri alfanumerici -ASCII).
- f) DFO1 (FID = 5401h) - Primo componente delle applicazioni trasporti, contenente:
 - o BS01_1 (ID = 11h) - BSO 3DES riferimento per la funzione "Internal Authentication" di autenticazione sicura del Badge RL. Il BSO è valorizzato con la chiave derivata (specifiche Netlink e CRS trasporti) da una master key e dal seriale nel formato memorizzato in EF_CIF.

Il File System del nuovo Badge RL dovrà risultare codificato in modo anonimo con dati fittizi convenzionali e privo di dati anagrafici effettivi. Non risulteranno cioè significativi i dati personali memorizzati nella CRS che ne caratterizzavano l'appartenenza al suo titolare.

Il legame tra Badge RL e persona titolare sarà infatti definito nelle anagrafiche del Sistema SCAI, assegnando ad uno specifico titolare il Serial Number di un Badge RL anonimo.

Dal punto di vista dei dati contenuti nel File System non sussisteranno quindi differenze sostanziali tra i badge assegnati al personale e i badge utilizzati come sostitutivo o visitatore. La specifica assegnazione d'uso del Badge RL sarà caratterizzata solo attraverso la sua personalizzazione con la stampa del supporto plastico del badge.