Specifiche Tecniche Terminali Controllo Accessi

Indice

1 Caratteristiche del badge usato in SpA Autovie Venete

1.1 Formato del badge

Mifare Classic – ISO/IEC14443A

- Frequenza : 13.56 MHz
- Protocollo : ISO14443A
- ID Univoco : 32 bits
- Dimensione EEPROM : 1024 Bytes
- Materiale : PVC
- Temperatura : -20°C ~ +50°C
- Dimensioni : 85.6 × 54 × 0.86 (mm)

1.2 Codifica dei dati

I dati contenuti all'interno del badge, relativi alla identificazione univoca della persona associata sono composti da:

- Serial ID Mifare (8 caratteri es. “bc cf fa e2”)
- ID utente (5 cifre)
- Checksum

2 Caratteristiche teste di lettura

Ciascun apparato di controllo accessi dovrà essere equipaggiato per gestire non più di due teste di lettura, ciascuna delle quali dovrà pilotare il relè di controllo ad essa associato.

Le teste di lettura potranno essere posizionate fino a 4 metri di distanza dall'apparato di controllo accessi e dovranno essere alimentate dall'apparato di controllo accessi stesso.

3 Caratteristiche apparato

Di seguito si riportano le caratteristiche minime che l'apparato dovrà supportare.

3.1 Configurazione

La prima configurazione dell'apparato dovrà essere effettuata attraverso una apposita interfaccia web accessibile via rete Ethernet.

L'interfaccia web permetterà di configurare le seguenti informazioni:

- ID terminale
- IP dispositivo
- Netmask dispositivo
- Gateway dispositivo
- IP server di servizio
- IP server DNS
- IP server NTP

L'interfaccia web dovrà inoltre permettere il caricamento manuale di una Whitelist di accesso, lo scaricamento degli accessi effettuati negli ultimi 30 gg e la visualizzazione dei parametri di funzionamento del sistema.

3.2 White list

Il dispositivo dovrà avere installato ed implementato il protocollo ssh per ricevere dal server di servizio le whitelist. Il nome del file deve essere “whitelist.txt” .E’ un file di testo che contiene tante righe nel seguente formato:

Data inizio del’attivazione nel formato “MM-GG-AAA hh:mm:ss”

Serial ID Mifare : 11 caratteri(il seriale è composto da 8 caratteri che vengono esposti separati da blank a due a due)

ID utente : 5 cifre

es.: 09-30-2016 20:54:00|7a de 55 57|08389

I campi sono separati dal carattere “|”(pipe):

La whitelist verrà aggiornata ad intervalli regolari dal server di servizio dei controlli accessi: contestualmente verrà rinomata l’ultima presente nel dispositivo ed archiviata in una sottocartella “whitelists”. I files relativi alle whitelists debbono essere mantenute per trenta giorni.

L'apparato dovrà validare autonomamente gli accessi, utilizzando l'ultima whitelist valida acquisita, indipendentemente dalla disponibilità di connessione in rete verso il sistema centralizzato di controllo accessi.

3.3 Log files

L'apparato dovrà memorizzare, al proprio interno, lo storico degli accessi, registrando le seguenti informazioni minime:

- Data Ora formato iso tipo YYYY-MM-DD hh:mm:ss
- ID utente 5 cifre
- Serial ID Mifare
- Note per es. esito dell’operazione di invio al server di servizio

Tali logs debbono essere facilmente consultabili e debbono essere tenuti per trenta giorni.

3.4 Invio dati al server di servizio

Per l'inserimento dei dati viene messo a disposizione un webservice SOAP/XML/WSDL 2.0 mediante una funzione:
Es.

```
int insertData (
      char C_TERM,            (ID terminale)
      int C_NUM_BDG,          (ID utente)
      char D_DATA_ORA,        (Data Ora timbratura)
      char C_SERIALE          (Serial ID)
      char C_OPERAZIONE       (Risultato Operazione)
      char T_NOTE             (Eventuali note per es. “NON PRESENTE in WHITELIST”)

)
```

Dove:

C_TERM: stringa di 8 caratteri
C_NUM_BDG: numero intero id badge
D_DATA_ORA: timbratura in formato iso tipo YYYY-MM-DD hh:mm:ss
C_SERIALE: 8 caratteri, seriale badge
C_OPERAZIONE: 1 carattere (**A** – Accettato; **R** - Rifiutato)
T_NOTE : testo massimo di 200 caratteri

return code numerico che equivale a 0 se tutto OK diversamente è un errore.

In caso di disconnessione dalla rete, il dispositivo dovrà essere in grado di immagazzinare tutti gli accessi e trasmetterli al server di servizio non appena si ristabilisce la connessione.

3.5 Messaggi vita

Il dispositivo , ogni ora, dovrà inviare al server di servizio un messaggio di vita tramite un webservice SOAP/XML/WSDL 2.0 mediante una funzione:
Es.

```
int insertVita (
      char C_TERM,          (ID terminale)
      char D_DATA_ORA,            (Data Ora locale)
      char NRO_ACC          (Numero  accessi processati nel giorno)
      )
```

Dove :

C_TERM: stringa di 8 caratteri
D_DATA_ORA: timbratura in formato iso tipo YYYY-MM-DD hh:mm:ss
NRO_ACC: 5 caratteri numerici

return code numerico che equivale a 0 se tutto OK diversamente è un errore.

3.6 NTP

L'apparato dovrà sincronizzare il proprio orologio interno con il sistema di riferimento fornito da S.p.A. Autovie Venete.

La sincronizzazione avverrà utilizzando il protocollo NTP.

3.7 Rete dati

L'apparato dovrà essere dotato di una porta ethernet 10/100Mbps e dovrà supportare il protocollo IPv4.

4 Caratteristiche Hardware

4.1 Protezione

L’apparato dovrà essere contenuto in un involucro protetto contro la polvere, contro l'accesso con un filo e contro i getti d'acqua (grado di protezione IP55)

4.2 Display

Non necessario.

4.3 Alimentazione elettrica

Tramite POE 802.3af . . Il dispositivo dovrà essere dotato di batteria tampone per la durata almeno di un’ora.

4.4 Memoria disco

Il dispositivo dovrà tenere in memoria almeno gli accessi, le logs e le whitelist degli ultimi trenta giorni .

5 Funzionalità

Il dispositivo dovrà essere provvisto di buzzer per indicare con un suono lungo che l’accesso è rifiutato.