SERVIZIO LAVORI PUBBLICI E OSSERVATORIO CONTRATTI E INVESTIMENTI PUBBLICI.
EDILIZIA E SICUREZZA DEI CANTIERI EDILI

REPAC **RE**gistratore **P**resenze **A**utorizzate nei **C**antieri

"Specifiche tecniche per i produttori dei dispositivi di controllo accessi"

Versione 1 del 17 settembre 2010

Regione Emilia-Romagna – **Leonardo Draghetti** (responsabile del Servizio Lavori pubblici ed Osservatorio dei contratti e degli investimenti pubblici. Edilizia e sicurezza dei cantieri edili)
Maurizio Baldisserri (P.O. Controllo e vigilanza sugli operatori edilizi)

NuovaQuasco – Area Appalti Pubblici: **Massimo Cataldi**

Progettazione informatica – **Paolo Foresti (SIXI)**

Sommario

Premessa

Queste specifiche sono relative alla versione multi cantiere del sistema informativo REPAC per la registrazione delle presenze autorizzate nei cantieri, adeguato alle specifiche del bando “Security Plus” della Regione Emilia-Romagna.

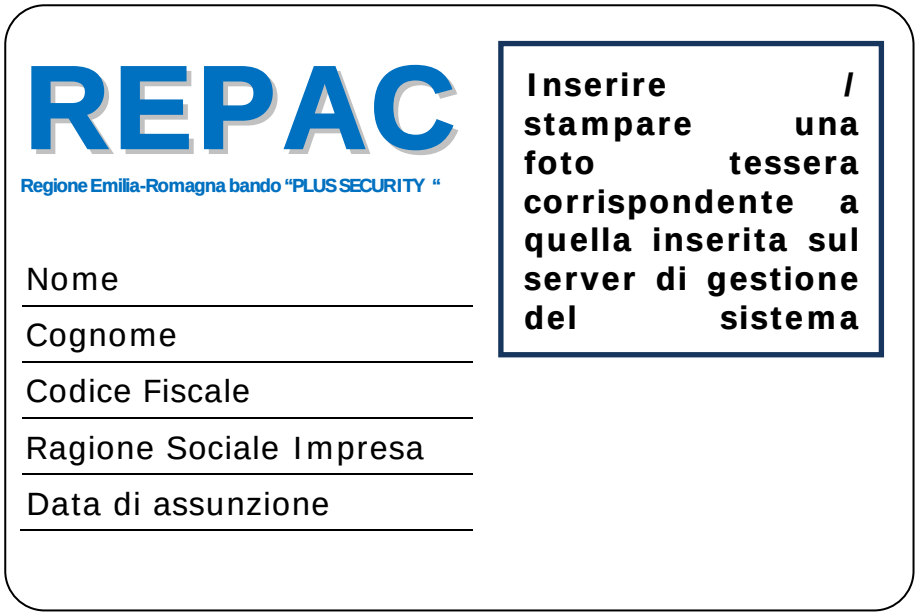
Nel caso le specifiche tecniche dettagliate in questo documento dovessero essere modificate, per necessità specifiche della Regione Emilia-Romagna, si provvederà ad avvisare con adeguato anticipo tutti i fornitori di dispositivi di rilevazione accessi già collaudati e conformi alle modalità operative del sistema informativo REPAC.

A seguire sono dettagliate le specifiche tecniche a cui attenersi per ottenere la compatibilità dei dispositivi di controllo accessi e dei badge di identificazione dei soggetti al sistema informativo REPAC.

Specifiche del Badge RFID

Il tesserino identificativo dell'operatore (badge RFID) dovrà avere le seguenti caratteristiche fisiche:

- formato tipo carta di credito;
- costituita di materiale plastico;
- avere tutti gli elementi costitutivi, antenna e TAG, annegati nel materiale plastico senza evidenze esterne;
- riportare stampate e non rimovibili le seguenti informazioni del soggetto identificato:
    - una foto in formato tessera;
    - nome e cognome;
    - codice fiscale;
    - ragione sociale impresa;
    - data di assunzione.



Il TAG RFID incorporato nel badge, per rendere possibile l'uso del tesserino con sistemi di rilevazione accessi di produttori diversi, dovrà avere le seguenti caratteristiche:

- TAG di tipo passivo[1];
- La frequenza di trasmissione non è al momento prefissata anche se, conformemente all'obiettivo di dotare gli attori e gli operatori di un tesserino rilevabile da qualsiasi dispositivo di rilevazione, si consiglia che i tesserini funzionino in alta frequenza (HF) 13,56 MHz.
- Protocollo di comunicazione ISO 14443 (vedi punto precedente). In relazione a questo il lettore del tesserino dovrà essere di standard ISO 14443 o 15693

[1] Nel caso nei cantieri fossero previste misure di controllo legate alla memorizzazione sul badge di codici biometrici del portatore, il badge dovrebbe disporre di una capacità di memoria pari ad almeno 1.024 bit.

Specifiche scambio dati con REPAC

Il sistema REPAC acquisisce i dati di accesso degli operatori per mezzo dei dispositivi di controllo accessi che sono situati presso i cantieri (una o più postazioni per cantiere). Questi dispositivi, ad intervalli regolari (ogni 5-10 min), si devono connettere al server che gestisce il servizio e scaricare questi dati nel sistema di gestione.

Il sistema REPAC mette a disposizione un web service apposito cui tutti i dispositivi dovranno collegarsi e scaricare i dati.

Il web service è stato progettato e realizzato per utilizzate il protocollo SOAP nella sua versione 1.1. Su questo web service sono implementati i seguenti metodi (web methods):

- Metodo “HelloWorld”;
- Metodo “HelloWorld2”;
- Metodo “PutTransitEvent”;
- Metodo “GetEnabledBadges”.

La descrizione formale di tutti i web methods (schema wsdl) la si può ottenere al seguente url: http://www.repac.it/services/repac_data_mc.asmx?WSDL.

Lo scambio dati con i dispositivi di controllo accessi di cantiere è la parte fondamentale ed abilitante del sistema REPAC. Esiste tuttavia anche la possibilità di scambiare col sistema REPAC i dati delle anagrafiche, sia delle persone fisiche che di quelle giuridiche. Tale scambio dati avviene mediante upload o download di file in formato XML su apposite pagine web del sito REPAC: l’uso di tale funzionalità è riservata al Gestore REPAC di Cantiere.

Questi file in formato XML, venendo scaricati o inseriti dal Gestore REPAC di Cantiere, viaggeranno su canale protetto (HTTPS) per cui verranno scambiati in chiaro, senza necessità di criptazione.

Logica di funzionamento e convenzioni

A seguire i punti più significativi sul funzionamento e sulle convenzioni del sistema REPAC:

- ogni transito ai varchi di cantiere (ingresso od uscita) è un evento REPAC;
- ogni evento REPAC deve essere caricato sul server web REPAC mediante chiamata al metodo "PutTransitEvent" del web service;
- gli eventi di transito vanno caricati sul server immediatamente o in differita. In caso di differita, ogni evento deve essere caricato sul server entro 15 minuti dal momento di rilevazione, salvo problemi temporanei di collegamento ad Internet;
- i dispositivi di controllo accessi devono poter memorizzare in locale gli eventi di transito in caso di temporanea indisponibilità del server web REPAC o della linea di comunicazione Internet. Alla prima riattivazione del servizio o della linea, dovranno scaricare sul server tutti gli eventi accumulati;
- i dispositivi di controllo accessi devono permettere l'accesso solo ai tesserini RFID autorizzati dal sistema REPAC;

- il sistema REPAC fornisce l'elenco di tutti e soli i tesserini autorizzati tramite il metodo "GetEnabledBadges" del web service;
- i dispositivi di controllo accessi devono collegarsi al sistema REPAC per scaricare l'elenco dei badges autorizzati almeno ogni 15 minuti;
- il sistema REPAC implementa la sicurezza dei dati scambiati con i dispositivi di controllo accessi di cantiere mediante la criptazione del contenuto dei messaggi. Tale criptazione viene implementata mediante algoritmo di criptazione a chiave simmetrica del tipo AES con lunghezza chiave a 256 bit;
- eccetto il metodo “HelloWorld” tutti gli altri metodi del web service di REPAC prevedono l'uso di un IV (Initial Vector) per migliorare la "robustezza" della procedura di criptazione dati. Per semplificare le operazioni, non verrà passato il vettore vero e proprio ma una stringa di testo. Questa stringa dovrà essere di almeno 16 caratteri e generata in maniera casuale ad ogni chiamata dei suddetti metodi del web service. Una volta generata questa stringa, i dispositivi dovranno produrre un hash a 128 bit della stessa ed utilizzare quest'ultimo per inizializzare la proprietà IV dell'encriptor. L’algoritmo utilizzato per generare l’hash per l’IV è del tipo MD5. La trasformazione da stringa ad array di byte avviene mediante codifica UNICODE;
- la chiave di criptazione di ogni dispositivo di controllo accessi sarà generata in maniera casuale dal sistema REPAC mediante apposita pagina web a disposizione del Gestore REPAC di cantiere (GRC);
- durante la fase di creazione dell’entità “dispositivo di controllo accessi” sul sistema REPAC, oltre ad essere generata una chiave di criptazione viene generato anche un ID del dispositivo (intero a 32 bit). L’accoppiata ID e chiave di criptazione deve essere impostata sul dispositivo di controllo accessi in fase di setup del dispositivo stesso;
- Per semplificare la comunicazione della chiave, come anche nel caso del parametro IV, non verrà comunicata la chiave di criptazione vera e propria ma una "stringa chiave". Per ottenere la chiave di criptazione con cui inizializzare l'encriptor occorrerà sottoporre la stringa chiave a procedimento di hashing a 256 bit. L’algoritmo utilizzato per generare l’hash per la chiave è del tipo SHA e la trasformazione della chiave da stringa ad array di byte avviene mediante codifica UNICODE.

Metodo “HelloWorld”

Questo web method ha scopo puramente di test. Serve per testare la sola disponibilità del servizio web: accetta come parametro di input una stringa qualsiasi e la restituisce come valore di ritorno (se più lunga di 50 caratteri tale stringa viene troncata).

Metodo “HelloWorld2”

Come il metodo descritto sopra, anche questo web method ha scopo di test. In questo caso però il dispositivo di controllo accessi è anche in grado di testare se le chiavi di criptazione dei due sistemi (REPAC e dispositivo di controllo accessi) sono allineate. Questo metodo presenta tre parametri di ingresso:

1. CryptedString: parametro stringa;
2. IV: stringa del Initial Vector;
3. DeviceID: intero a 32 bit: ID del dispositivo (valore che viene assegnato dal REPAC in fase di setup del dispositivo).

Il valore di ritorno è di tipo string.

Il parametro “IV” rappresenta il valore stringa casuale che deve essere generato ad ogni chiamata del metodo.

Il parametro DeviceID è il valore intero a 32 bit assegnato al dispositivo in fase di setup.

Il parametro “CryptedString” rappresenta il valore criptato dell’ID del dispositivo.

Procedura per la costruzione del parametro criptato

L’algoritmo esatto è il seguente:

1. Si trasforma l’intero a 32 bit che rappresenta l’ID del dispositivo in stringa: ad esempio se l’ID assegnato è 32 costruiamo la stringa “32”;
2. si genera un valore casuale della stringa di IV;
3. trasformiamo la stringa di IV in array di byte con trasformazione di tipo UNICODE;
4. costruiamo l’IV vero e proprio sottoponendo ad hash (a 128 bit MD5) l’array di byte di cui sopra;
5. trasformiamo la stringa chiave in array di byte con trasformazione di tipo UNICODE;
6. costruiamo la chiave di criptazione vera e proprio sottoponendo ad hash l’array di byte della chiave appena ottenuto (hash a 256 bit SHA);
7. Ora inizializziamo l’encryptor utilizzando l’IV e la chiave di criptazione;
8. Accodiamo alla stringa IV la stringa che rappresenta l’ID del dispositivo (vedi punto 1); la stringa risultante la trasformiamo in array di byte mediante trasformazione UNICODE quindi la crittografiamo utilizzando l’encryptor;
9. l’array cryptato risultante lo trasformiamo in stringa con una trasformazione cosiddetta a base 64.

Procedura per la costruzione del valore di ritorno

Il web method esegue il processo opposto:

1. Sulla base del valore del parametro “DeviceID” il REPAC controlla che tale valore esista nella base dati;
2. se esiste ne recupera la chiave di criptazione assegnata;
3. con la chiave di criptazione ed il valore del parametro “IV” arrivato, inizializza l’encryptor (vedi punti da 3 a 7 del parargrafo precedente).
4. Quindi trasforma il parametro “CryptedString in array di byte e lo sottopone all’encryptor per la decriptazione;
5. Ottenuta la stringa decrittata, rimuove la stringa di IV e converte in intero a 32bit il valore rimanente;
6. se il valore decrittato coincide del valore del parametro “DeviceID” allora la procedura è andata a buon fine e viene restituita la stringa “OK”;
7. in caso contrario viene restituita una stringa di errore.

Metodo “PutTransitEvent”

Il web method “PutTransitEvent” è quello che permette ai dispositivi di controllo accessi di far affluire i dati all’applicativo web di gestione REPAC. Questo metodo presenta tre parametri di ingresso:

1. CryptedString: parametro stringa;
2. IV: stringa del Initial Vector;
3. DeviceID: intero a 32 bit. È l’ID del dispositivo (valore che viene assegnato dal REPAC in fase di setup del dispositivo).

Il valore di ritorno è di tipo string.

Il parametro “IV” rappresenta il valore stringa casuale che deve essere generato ad ogni chiamata del metodo.

Il parametro DeviceID è il valore intero a 32 bit assegnato al dispositivo in fase di setup.

Il parametro “CryptedString” rappresenta il valore criptato dell’evento REPAC (ingresso od uscita dal cantiere).

Procedura per la costruzione del parametro criptato

L’algoritmo esatto è il seguente:

1. Si costruisce un albero xml secondo lo schema fornito a parte (“event.xml”) e lo si “popola” con i dati dell’evento. Una volta costruito tale albero xml lo si trasforma in stringa;
2. si genera un valore casuale della stringa di IV;
3. trasformiamo la stringa di IV in array di byte con trasformazione di tipo UNICODE;
4. costruiamo l’IV vero e proprio sottoponendo ad hash (a 128 bit MD5) l’array di byte di cui sopra;
5. trasformiamo la stringa chiave in array di byte con trasformazione di tipo UNICODE;
6. costruiamo la chiave di criptazione vera e proprio sottoponendo ad hash l’array di byte della chiave appena ottenuto (hash a 256 bit SHA);
7. Ora inizializziamo l’encryptor utilizzando l’IV e la chiave di criptazione;

8. Trasformiamo la stringa contenente l'albero xml di cui sopra (punto 1) in array di byte mediante trasformazione di tipo UNICODE;
9. procede alla criptazione di questo array sottoponendolo all'encryptor di cui sopra;
10. ottenuto il valore criptato lo trasformiamo in stringa con una trasformazione cosiddetta a base 64.

Procedura per la costruzione del valore di ritorno

Il web method esegue il processo opposto:

1. Sulla base del valore del parametro "DeviceID" controlla che tale valore esista nella base dati;
2. se esiste ne recupera la chiave di criptazione assegnata;
3. con la chiave di criptazione ed il valore del parametro "IV" arrivato, inizializza l'encryptor quindi procede alla decriptazione del parametro "CryptedString". Il procedimento è esattamente analogo ma inverso a quanto dettagliato al capitolo precedente;
4. una volta ottenuta la stringa decriptata, la si trasforma in albero xml e si vanno ad estrarre tutti i dati dell'evento.
5. se l'evento viene accettato dal sistema viene restituita la stringa "OK";
6. in caso contrario viene restituita una stringa di errore.

Albero XML dei dati di evento

La definizione esatta del formato dell'albero XML può essere dedotta dall'XML di esempio che sarà rilasciato su richiesta in formato su file.

Metodo "GetEnabledBadges"

Il web method "GetEnabledBadges" è quello che permette ai dispositivi di controllo accessi di scaricare l'elenco dei badge autorizzati per l'accesso al cantiere. Tale metodo deve essere chiamato almeno ogni 15 minuti da parte dei dispositivi di controllo accessi.

Questo metodo presenta tre parametri di ingresso:

1. CryptedString: parametro stringa;
2. IV: stringa del Initial Vector;
3. DeviceID: intero a 32 bit: ID del dispositivo (valore che viene assegnato dal REPAC in fase di setup del dispositivo).

Il valore di ritorno è di tipo string.

Il parametro "IV" rappresenta il valore stringa casuale che deve essere generato ad ogni chiamata del metodo.

Il parametro DeviceID è il valore intero a 32 bit assegnato al dispositivo in fase di setup.

Il parametro "CryptedString" rappresenta il valore criptato dell'ID del dispositivo.

Procedura per la costruzione del parametro criptato

La procedura di costruzione è identica a quella relativa al metodo "HelloWorld2".

Procedura per la costruzione del valore di ritorno

Il web method invece esegue il seguente processo:

1. Sulla base del valore del parametro "DeviceID" controlla che tale valore esista nella base dati;
2. se esiste ne recupera la chiave di criptazione assegnata;
3. con la chiave di criptazione ed il valore del parametro "IV" arrivato, inizializza l'encryptor. Quindi procede alla decriptazione del parametro "CryptedString";
4. ottenuta la stringa decrittata, rimuove la stringa di IV e converte in intero a 32bit il valore rimanente;
5. se il valore decrittato coincide del valore del parametro "DeviceID" allora la procedura è andata a buon fine (il dispositivo è autenticato); in caso contrario viene restituita una stringa di errore;
6. in caso di corretta autenticazione, il web service costruisce un albero xml secondo lo schema fornito a parte ("enabled_badges.xml") e lo "popola" con l'elenco dei badge autorizzati per quel cantiere. Una volta costruito tale albero xml lo trasforma in stringa;
7. inizializziamo l'encryptor utilizzando il IV e la chiave di criptazione assegnata;
8. sottoponiamo a criptazione la stringa contenente l'albero xml: ottenuto il valore criptato lo trasformiamo in stringa con una trasformazione cosiddetta a base 64;
9. tale stringa criptata viene restituita al dispositivo di controllo accessi;
10. in maniera assolutamente analoga il dispositivo di cantiere decripterà la stringa ed otterrà l'albero xml da cui estrarrà i valori dei badge autorizzati.

Albero XML dei badge autorizzati

La definizione esatta del formato dell'albero XML può essere dedotta dall'XML di esempio che sarà rilasciato su richiesta in formato su file.

Albero XML delle anagrafiche delle persone fisiche e giuridiche

La definizione esatta del formato dell'albero XML può essere dedotta dai due XML di esempio che saranno rilasciati su richiesta in formato su file.