ALLEGATO 5

Dichiarazione d'impegno, contenente l'elenco degli apparecchi AWP dei quali non si intende voler cessare il nulla osta

Il concessionario per la composizione dell'allegato 5 deve presentare ad AAMS su supporto informatico non riscrivibile, l'elenco degli apparecchi di gioco dei quali non si intende cessare il nulla osta, ognuno dei quali comprensivo di nulla osta di esercizio e data di rilascio dello stesso, di cui è titolare, seguendo le specifiche tecniche indicate nel presente documento.

Il CD deve essere costituito da un file .csv riportando le informazioni di seguito descritte ed un file firma.txt.

1) <u>Caratteristiche del supporto informatico</u>

Il supporto informatico da utilizzare è costituito da CD-ROM non riscrivibile di dimensioni standard.

Ogni CD-ROM deve contenere:

- un file denominato "codice fiscale concessionario".csv
- un file denominato "firma.txt"

Sul CD-ROM deve essere altresì apposta un'etichetta in cui deve essere riportato la denominazione del concessionario, la scritta "Allegato 5" nonché la data di produzione del CD.

2) <u>Caratteristiche del file contenuto nel CD-ROM</u>

Il file deve possedere le seguenti caratteristiche:

- organizzazione del file di tipo sequenziale;
- tipo di codifica = ASCII STANDARD;
- gli ultimi due caratteri di ciascun record riservati ai caratteri ASCII, CR e LF (valori esadecimali "0D" e "0A").
- l'estensione del file deve essere ".csv"
- il nome del file deve essere composto nel seguente modo: [codice fiscale del concessionario] .[estensione del file]
- non sono accettati file multi-volume nel CD.

I campi, separati dal carattere riservato " ; " (punto e virgola), sono alfabetici (A), alfanumerici (AN) e numerici (N) e contengono esclusivamente le cifre da 0 a 9 e le lettere dell'alfabeto dalla A alla Z, con inclusione di:

apostrofo, accento, spazio, punto, "&", "/", "\", "-", "@" ed esclusione di qualsiasi altro carattere speciale. Si precisa comunque che nel campo indirizzo non sono accettati i caratteri speciali "&", "/", "\", "-", "@".

Ciascun record presente nel file rappresenta in ordine le seguenti informazioni, come riportato come primo record del file stesso:

CAMPI CONTENUTI NEL RECORD	
PROGRESSIVO	**DESCRIZIONE**
1	NOME DELL'ALLEGATO
2	CODICE NULLA OSTA
3	DATA RILASCIO NULLA OSTA
4	CODEID DEFINITIVO APPARECCHIO DI GIOCO AWP

Note di compilazione:

Tutti i campi previsti devono essere compilati e sono presenti nel Nulla Osta di Esercizio in carico al concessionario.

Il campo 1 deve essere valorizzato con il valore "ALLEGATO5" (senza doppi apici).

3) Criteri di accettazione del CD-ROM

Le applicazioni informatiche di AAMS verificano la firma presente nel CD – ROM come descritto nella sezione 4) e nel caso in cui l'esito sia favorevole si procede all'elaborazione del file .CSV contenuto nel CD–ROM.

Qualora il file rispetti anche la struttura richiesta nella sezione 2), le informazioni sono acquisite generando una reportistica di quanto dichiarato dal concessionario segnalando eventuali anomalie rispetto quanto presente in banca dati di AAMS.

4) Firma: Costruzione e Verifica

Per la firma del file dovranno essere utilizzati algoritmi di "hashing" ed il "digest" cosi ottenuto dovrà essere crittografato con la chiave privata del concessionario e codificato base64.

Dovranno essere utilizzate funzioni che consentono il calcolo del digest da parte del concessionario e la verifica dello stesso da parte del sistema di controllo AWP.

I prodotti di riferimento per l'implementazione sono le librerie Open Source MHASH ed OPENSSL, ed il formato delle chiavi private e delle chiavi pubbliche è il PEM (Privacy Enhanced Mail).

A livello applicativo, il sistema di controllo interfaccia MHASH ed OPENSSL tramite le funzioni PHP (versione: 5.2.9) mhash, openssl_private_encrypt ed openssl_public_decrypt, i cui sorgenti in linguaggio C sono liberamente disponibili ed ai quali si rimanda per i dettagli implementativi.

Si precisa che le citate funzioni di encrypt/decrypt utilizzano il valore di default per il quarto parametro; di conseguenza, le chiamate alle funzioni OPENSSL di basso livello RSA_private_encrypt e RSA_public_decrypt prevedono un "padding" di tipo RSA_PKCS1_PADDING (PKCS #1 v1.5).

E' data facoltà al concessionario di utilizzare prodotti alternativi a quelli di riferimento, a patto che essi siano in grado di produrre risultati equivalenti ed intercambiabili.

L'algoritmo di hashing utilizzato è MD5; se il concessionario utilizza per l'implementazione gli stessi prodotti utilizzati dal sistema di controllo, il digest si ottiene mediante la chiamata PHP mhash(MHASH_MD5, $msg).

Per il calcolo della firma i passi da seguire sono i seguenti:

1. applicare l'algoritmo di hashing al file .csv;

2. crittografare il digest ottenuto con la propria chiave privata;
3. codificare base64 il digest crittografato.

La verifica della firma, il cui esito positivo sarà propedeutico ai controlli sul file .csv descritto nel presente documento, presenta i seguenti passi:

4. individuare la chiave pubblica associata al concessionario;
5. decifrare la firma presente nel file .txt presente nel CD-Rom, utilizzando la chiave pubblica individuata con le modalità descritte al punto precedente;
6. applicare l'algoritmo di hashing al file .csv presente nel file contenuto nel CD-Rom.

Se le due stringhe ottenute con le modalità descritte ai punti 5 e 6 coincidono, il destinatario è certo dell'identità del mittente e della integrità dei dati ricevuti e la verifica della firma è da considerarsi conclusa con esito positivo, altrimenti negativo.