SPECIFICHE TECNICHE PER LA REALIZZAZIONE DEI SISTEMI DI BIGLIETTERIE AUTOMATIZZATE IDONEI ALLA VENDITA E AD ALTRE FORME DI COLLOCAMENTO, ATTRAVERSO RETI DI COMUNICAZIONE ELETTRONICA, DI TITOLI DI ACCESSO AD ATTIVITÀ DI SPETTACOLO AI SENSI DELL'ARTICOLO 3 DEL DECRETO DEL MINISTRO DELL'ECONOMIA E DELLE FINANZE 12 MARZO 2018.

INDICE

1. GLOSSARIO

Bot (abbreviazione di roBot): un programma che accede alla rete attraverso lo stesso tipo di canali utilizzati dagli utenti umani simulandone l'operatività

Decreto: Decreto Ministeriale 12 marzo 2018 del Ministero dell'Economia e delle finanze di concerto con il Ministro della Giustizia e il Ministro dei beni e delle attività culturali e del turismo (GU 27 aprile 2018)

OTP (One-Time Password): è una password che è valida solo per una singola sessione di accesso.

Secondary ticketing: fenomeno della vendita di titoli di accesso ad attività di spettacolo effettuata da soggetti diversi dai titolari dei sistemi di emissione dei biglietti

Carta di attivazione: carta a microcircuito di attivazione, rilasciata dall'Agenzia delle entrate, contenente il software per la generazione delle chiavi segrete, necessarie per il calcolo di codici di autenticazione utilizzati per la trasmissione dati, e l'algoritmo per la determinazione del sigillo fiscale.

Sigillo fiscale: identificativo unico associato in maniera univoca ad ogni titolo di accesso rilasciato tramite un sistema che utilizza una determinata carta di attivazione.

Check out dell'ordine: operazione di conferma dell'ordine nell'ambito di ciascun processo di acquisto.

2. FINALITÀ DEL DOCUMENTO

Il decreto disciplina la modalità di adozione delle "specificazioni" e delle regole tecniche attuative dell'art. 1, comma 545, della legge 11 dicembre 2016, n. 232, volte a migliorare la tutela dei consumatori e la sicurezza informatica nella vendita, tramite biglietterie automatizzate, dei titoli di accesso "per ciascuna manifestazione da intrattenimento" o "spettacolistica", contrastando la vendita o qualsiasi altra forma di collocamento di titoli di accesso ad attività di spettacolo ove effettuata da soggetto diverso dai titolari dei sistemi per la loro emissione.

L'articolo 3, comma 2, del decreto prevede l'emanazione di un provvedimento del direttore dell'Agenzia delle entrate, previa intesa con l'Autorità per le garanzie nelle comunicazioni, che definisca le specifiche tecniche per la realizzazione di sistemi informatici di biglietterie automatizzate che, essendo idonei a distinguere l'accesso effettuato da una persona fisica rispetto a quello effettuato da un programma automatico, impediscano l'acquisto da parte di tale programma, nonché siano in grado di identificare l'acquirente. Il provvedimento deve stabilire, altresì, le modalità e i termini di applicazione delle suddette specifiche tecniche.

È compito della Commissione per l'approvazione dei modelli di apparecchi misuratori fiscali, di cui all'articolo 5 del decreto del Ministro delle finanze 23 marzo 1983, effettuare l'attività di "riconoscimento di idoneità" dei sistemi informatici che viene chiesto all'Agenzia delle entrate dai soggetti legittimati. Per espletare questa attività la Commissione viene integrata da un rappresentante del Ministero dei beni e delle attività culturali e del turismo e da un rappresentante dell'Autorità per le garanzie nelle comunicazioni.

3. SOLUZIONI TECNICHE DA ADOTTARE NEI SISTEMI DI BIGLIETTERIE AUTOMATIZZATE PER LA VENDITA DI TITOLI DI ACCESSO ATTRAVERSO RETI DI COMUNICAZIONE ELETTRONICA

3.1 MISURE MINIME PER IMPEDIRE L'ACQUISTO DA PARTE DI UN PROGRAMMA AUTOMATICO (PUNTO 4.1 DEL PROVVEDIMENTO)

Al momento della composizione dell'ordine dei titoli di accesso desiderati (ovvero del loro inserimento all'interno di un "carrello") il sistema presenta all'utente acquirente un test CAPTCHA o re-CAPTCHA, superato il quale l'operazione viene effettuata con successo.

Per determinare se l'utente del sistema sia un umano e non un programma, il sistema sottopone l'utente ad un test logico denominato CAPTCHA. Esiste un gran numero di diverse realizzazioni pratiche di CAPTCHA, ma tutte devono soddisfare i seguenti requisiti:

- completa automazione: non deve essere necessario alcun intervento umano da parte di chi somministra il test, come da definizione;

- algoritmo pubblico: il programma che somministra il test può essere anche brevettato e commercializzato, ma la pubblicazione dell'algoritmo serve a dimostrare che per superare il CAPTCHA è necessario risolvere un problema di Intelligenza Artificiale (IA), assai ostico per un computer ma non per un essere umano;

- non è obbligatorio ricorrere a tecniche visive: qualunque problema di intelligenza artificiale che abbia lo stesso grado di complessità, ad esempio il riconoscimento vocale, è adatto a fare da base per un test di questo tipo. Alcune implementazioni consentono all'utente di scegliere in alternativa un test basato su tecniche auditive. Inoltre, è possibile ricorrere ad altri tipi di verifiche che richiedano un'attività di comprensione testuale, quali la risposta a una domanda o a un quiz logico, il seguire delle specifiche istruzioni per creare una password, ecc.

Per soddisfare le presenti specifiche, il problema di Intelligenza Artificiale da risolvere deve richiedere l'uso simultaneo di tre abilità distinte, tipiche dell'essere umano:

- riconoscimento invariante: il nostro cervello è in grado di riconoscere correttamente oggetti e forme, anche se deformati in una moltitudine

di modi diversi; programmare un bot per simulare questo comportamento è invece molto complesso.

- segmentazione: si riferisce alla capacità di distinguere tra di loro oggetti e forme, anche in assenza di una evidente separazione spaziale.

- olismo: la corretta interpretazione del CAPTCHA dipende anche dalla interazione tra i diversi oggetti e forme che lo compongono; ad esempio, in una parola di senso compiuto quello che dalla grafica deformata potrebbe sembrare una "m" in realtà dovrebbe essere interpretato come "in" oppure "un".

Tra i CAPTCHA che soddisfano i criteri elencati, quelli di uso più comune sono basati sul riconoscimento di sequenze di lettere e/o numeri, di cui viene offerta una rappresentazione grafica e, su richiesta, una versione audio pensata per permetterne l'utilizzo agli ipovedenti. In tal caso, la soluzione da adottare deve prevedere:

- sequenze di almeno 5 caratteri

- una dimensione minima dell'immagine di 400x200 pixel (LxH)

- l'utilizzo congiunto o disgiunto di almeno 2 font distinti

- la deformazione indipendente di ciascun carattere

- una sfocatura casuale dei caratteri, più o meno accentuata

- uno o più elementi di disturbo (es: linee che attraversano i caratteri, rumori di fondo nell'audio)

- il supporto audio in lingua italiana ed in lingua inglese

- almeno 2 voci (maschile e femminile) per scandire i singoli caratteri

- il supporto del formato audio MP3 ed opzionalmente del WAV e dell'SWF

- il supporto del formato grafico JPG ed opzionalmente del PNG e del GIF

Per garantire prestazioni ottimali, le immagini ed i file audio associati devono essere pregenerati in numero sufficiente a rispondere al traffico di picco previsto; dopo l'utilizzo, una sequenza di caratteri può essere riusata ma il file corrispondente deve essere ricostruito in asincrono, variandone (pseudo)casualmente la rappresentazione grafica oppure audio.

Indipendentemente dalle caratteristiche sopraelencate il tipo di CAPTCHA prescelto deve comunque corrispondere ai più recenti standard disponibili sul mercato.

3.2 LIMITAZIONI PER L'ACQUISTO DI UN TITOLO DI ACCESSO (PUNTO 4.2 DEL PROVVEDIMENTO)

Nel corso del processo di acquisto il sistema applica le seguenti regole:

a) l'utente acquirente può concludere l'operazione di acquisto di uno o più titoli di accesso solo se identificato sul sistema.

b) Il sistema prevede il limite massimo, per ciascun evento, di 10 titoli di accesso acquistabili da un singolo utente identificato.

c) il titolo di accesso non può essere rilasciato direttamente dal sistema alla conclusione dell'acquisto, ma inviato successivamente all'utente identificato con una delle modalità da lui scelte fra quelle rese disponibili dal sistema.

d) il sistema registra le informazioni relative a ciascuna transazione di acquisto, secondo le modalità di cui al successivo punto 3.5.

3.3 REGISTRAZIONE E IDENTIFICAZIONE DELL'UTENTE ACQUIRENTE (PUNTO 4.3 DEL PROVVEDIMENTO)

Per poter identificare univocamente i diversi utenti acquirenti, il sistema prevede una fase di registrazione, che consente di attribuire ad ogni utente registrato credenziali di accesso ed un codice univoco da utilizzare per il tracciamento delle operazioni di cui al punto 3.5.

La registrazione può essere effettuata anche in più fasi ma deve essere conclusa con successo prima di procedere all'acquisto del primo titolo di accesso.

In fase di registrazione il sistema prevede che l'utente fornisca i seguenti dati:

- Nome
- Cognome
- Data di nascita

- Luogo di nascita
- Indirizzo e-mail
- Numero di cellulare

Il numero di cellulare deve essere univoco nel sistema e non può essere associato ad utenti diversi.

Per la validazione della fase di registrazione, alla fine del processo di raccolta dei dati, il sistema invia all'utente un SMS contenente un codice autorizzativo non riutilizzabile, di almeno 4 cifre (c.d. OTP), che egli dovrà inserire in un apposito pannello applicativo per confermare la registrazione. L'attività di registrazione si ritiene completata con esito positivo solo al termine dell'operazione di validazione.

In momenti successivi, utilizzando le sue credenziali, l'utente potrà accedere al proprio profilo per modificare il numero di telefono cellulare. In questo caso, fino a quando questa informazione non viene nuovamente validata, l'utente non potrà più procedere all'acquisto di titoli di accesso.

3.4 IDENTIFICAZIONE DELL'UTENTE ACQUIRENTE TRAMITE SPID (PUNTO 4.4 DEL PROVVEDIMENTO)

Per identificare univocamente i diversi utenti acquirenti, il sistema può utilizzare l'identità digitale SPID di livello 1 o superiore.

In tal caso:

- non è necessario che il sistema proceda alla fase di registrazione utente, di cui al punto 3.3;
- nel caso in cui non si proceda alla fase di registrazione, i dati utilizzati nel processo di acquisto sono quelli dell'identità SPID;
- il codice univoco dell'utente è costituito dal codice identificativo (*spidCode)* come indicato nella Tabella degli attributi relativi all'identità SPID definita da Agid, o, in alternativa, il codice univoco dell'utente deve essere collegato in modo esclusivo allo *spidCode*.

3.5 TRACCIAMENTO DELLE OPERAZIONI DI ACQUISTO (PUNTO 4.5 DEL PROVVEDIMENTO)

Al fine di consentire le opportune verifiche, il sistema registra tutte le iterazioni degli utenti e tutti gli eventi di acquisto, come di seguito specificato, ed è predisposto per fornirle su richiesta degli organi di controllo mediante un apposito *file di log*.

Al fine di proteggere la privacy degli acquirenti, i dati del *file di log* contengono solo un codice univoco associato agli utenti identificati, ma non i loro dati anagrafici, in modo che non sia possibile risalire all'identità dell'acquirente se non su specifica richiesta degli organi di controllo.

I dati del *file di log* sono indicati nel decreto del Direttore dell'Agenzia delle entrate del 23 luglio 2001 e sono resi disponibili in formato XML.

3.6 SICUREZZA DELL'ACCESSO DEL SISTEMA DI VENDITA

Per consentire che l'utente acceda al sistema di vendita attraverso un canale sicuro che cripti i dati in entrata ed in uscita impedendo a terze parti di leggere, inserire o modificare i messaggi nel passaggio tra client e server, il sito adotta il canale di comunicazione HTTPS implementando almeno la versione TLS 1.2 del protocollo di connessione.