---

1. Introduzione e Obiettivi

I sistemi di biglietteria automatizzata devono soddisfare i seguenti obiettivi principali, come definiti nei documenti e nei provvedimenti citati:

- **Emissione dei titoli di accesso** in formato fisico (es. biglietti cartacei) o digitale (es. QR code, PDF leggibile su dispositivo mobile o stampabile), con sigilli fiscali univoci e dati obbligatori.

- **Controllo degli accessi** in tempo reale o differito, con validazione e invalidazione dei titoli per prevenire utilizzi multipli, supportando settori specifici dell'evento.

- **Tracciabilità fiscale** delle transazioni, con registrazione di tutte le operazioni e trasmissione dei dati alla SIAE (Società Italiana degli Autori ed Editori) in formati standardizzati (XML, ASCII a campi fissi).

- **Protezione contro usi impropri**, come il bagarinaggio, attraverso autenticazione utente (OTP o SPID), limiti di acquisto e misure anti-bot (es. CAPTCHA).

- **Supporto al *secondary ticketing***, con registrazione degli acquirenti originali e nuovi titolari, rispettando il Decreto del Ministro dell'Economia e delle Finanze (MEF) del 12 marzo 2018 (GU 27 aprile 2018).

- **Conformità agli standard tecnici**:

    - XML 1.0 (W3C, 10 febbraio 1998) per i file di log e di riepilogo.

    - TLS 1.2 o superiore per la sicurezza delle comunicazioni.

    - RFC-2822 per i timestamp.

    - S/MIME per la trasmissione sicura dei dati alla SIAE.

- **Protezione della privacy** (GDPR, Regolamento UE 2016/679), con minimizzazione dei dati personali nei log e cifratura dei dati sensibili.

I documenti allegati (*Allegato A*, *Allegato B*, *Allegati 1-4*) forniscono specifiche tecniche dettagliate, modifiche ai formati dei dati e misure di sicurezza, aggiornando i requisiti dei Provvedimenti del 23 luglio 2001 e 22 ottobre 2002. Gli *Allegati 1-4* contengono contenuti limitati ("30", "31", "32", "33 - 33"), probabilmente numeri di pagina o codici di riferimento, senza dettagli tecnici significativi.

---

2. Requisiti Normativi e Funzionali

2.1 Emissione dei Titoli di Accesso

- **Formato dei Titoli** (*Allegato A, punto 3; Provvedimento 4 marzo 2008, art. 7*):
    - I titoli possono essere emessi in formato fisico (biglietti stampati su carta) o digitale (es. QR code, PDF leggibile su smartphone o stampabile).
    - **Dati obbligatori** per ogni titolo:
        - **Codice univoco del titolo**: identificativo alfanumerico unico (es. “TICKET123456”).
        - **Sigillo fiscale**: identificativo univoco generato dalla carta di attivazione.
        - **Codice richiedente emissione sigillo**: codice di 8 caratteri che identifica il canale di emissione (dettagli in 2.1.1).
        - **Dati dell’evento**:
            - Nome dell’evento (es. “Concerto di Artista X”).
            - Data e ora dell’evento (formato ISO 8601, es. `2025-06-30T20:00:00Z`).
            - Luogo dell’evento (es. “Teatro Y, Roma”, conforme a ISO 3166 per i codici paese).
            - Settore e posto, se applicabile (es. “Tribuna A, Posto 12”).
            - Prezzo del titolo, comprensivo di IVA (es. “€50,00, IVA inclusa”).
            - Eventuali codici promozionali o sconti applicati.
    - **Titoli digitali**:
        - Devono essere associati a un supporto identificabile (es. smartphone tramite app dedicata o stampa fisica di un PDF con QR code).
        - Devono essere leggibili da dispositivi di controllo (es. scanner QR code).
    - **Verificabilità**:
        - I dati del titolo (codice, sigillo fiscale, ecc.) devono essere verificabili dagli organi di controllo (SIAE, Agenzia delle Entrate) durante

l’accesso all’evento.

- **Carta di Attivazione** (*Allegato A, Glossario; Provvedimento 4 marzo 2008, art. 7*):
    - Una carta a microcircuito rilasciata dall’Agenzia delle Entrate per ogni sistema di biglietteria.
    - **Contenuto**:
        - Software per generare chiavi segrete per l’autenticazione dei dati trasmessi.
        - Algoritmo per generare sigilli fiscali univoci per ogni titolo.
    - **Funzioni**:
        - Generazione di sigilli fiscali per ogni titolo emesso.
        - Firma digitale dei file XML trasmessi alla SIAE.
    - **Implementazione tecnica**:
        - Integrare la carta tramite un modulo hardware di sicurezza (HSM) o un’interfaccia software fornita dall’Agenzia delle Entrate.
        - Configurare il sistema per accedere alla carta durante l’emissione dei titoli e la firma dei file.
        - Garantire la protezione fisica e logica della carta (es. accesso limitato, cifratura delle comunicazioni).
    - **Processo di ottenimento**:
        - Richiedere la carta all’Agenzia delle Entrate, fornendo dettagli sul sistema di biglietteria (es. descrizione tecnica, flussi operativi).
        - Testare l’integrazione durante la fase di certificazione, in collaborazione con la Commissione dell’Agenzia delle Entrate.
- **Codice Richiedente Emissione Sigillo** (*Allegato B, punto 1a*):
    - Sostituisce il campo “Codice punto vendita” nel formato ASCII a campi fissi (posizioni 85-92, lunghezza 8 caratteri).
    - **Struttura**:
        - **Primi 2 caratteri**: tipologia del richiedente:

        - `01` (PV): Punto vendita fisico (es. ricevitoria, ticket point).
        - `02` (SW): Sito web con web service a protocollo sicuro (es. HTTPS).
        - `03` (CL): Client locale connesso in rete LAN.
        - `04` (CW): Client web remoto connesso via WAN o internet.
        - `05` (AP): Applicazione mobile per tablet o smartphone.
    - **Ultimi 6 caratteri** (posizioni 3-8): codice univoco del sistema richiedente, assegnato dall'Agenzia delle Entrate o dal gestore del sistema.
  - **Requisiti**:
    - Deve essere riportato su ogni titolo emesso (fisico o digitale) per garantire la tracciabilità del canale di emissione.
    - Deve essere incluso nei file XML trasmessi alla SIAE.
    - Il campo "note" (*Allegato B, punto 1a*) specifica:
      - "Il Codice richiedente emissione sigillo deve essere riportato sul titolo."
      - "Il campo è valorizzato con una stringa alfanumerica di 8 caratteri in cui i primi 2 caratteri sono riservati alla codifica della tipologia del richiedente."
  - **Esempio**:
    - Un biglietto emesso da un sito web potrebbe avere il codice `02ABCDEF`, dove `02` indica il canale web e `ABCDEF` è il codice univoco del sistema.
  - **Implementazione tecnica**:
    - Generare il codice durante l'emissione del titolo, in base al canale utilizzato (es. sito web, app mobile).
    - Verificare che il codice sia correttamente riportato sul titolo e nei file XML.
- **Limiti di Acquisto** (*Allegato A, punto 3.2*):

    - **Limite massimo**: 10 titoli di accesso per evento per singolo utente identificato, per prevenire il bagarinaggio.

    - **Implementazione tecnica**:

        - Verificare l'identità dell'utente tramite il codice univoco generato durante la registrazione o tramite SPID.

        - Controllare il numero di titoli acquistati per evento nel database, bloccando tentativi di acquisto oltre il limite.

        - Registrare ogni tentativo di acquisto (riuscito o fallito) nel log delle operazioni, con codice utente, timestamp e indirizzo IP.

        - Mostrare un messaggio di errore chiaro all'utente in caso di superamento del limite (es. "Limite massimo di 10 biglietti raggiunto per questo evento").

- **Registrazione e Identificazione Utente** (*Allegato A, punto 3.3*):

    - **Dati obbligatori**:

        - Nome (es. "Mario").

        - Cognome (es. "Rossi").

        - Data di nascita (formato ISO 8601, es. `1990-05-15`).

        - Luogo di nascita (es. "Roma", conforme a ISO 3166 per i codici paese).

        - Indirizzo e-mail (es. "mario.rossi@example.com").

        - Numero di cellulare (univoco, es. "+393331234567", conforme a E.164).

    - **Validazione della registrazione**:

        - Inviare un OTP (One-Time Password) di almeno 8 cifre, non riutilizzabile, via SMS al numero di cellulare fornito.

        - Fornire un pannello applicativo (es. campo di input su una pagina web o app mobile) per l'inserimento dell'OTP.

        - Implementare un timeout per l'OTP (es. 5 minuti) e un limite di tentativi (es. 3).

        - La registrazione è valida solo dopo la verifica positiva dell'OTP.
    - **Gestione del profilo utente**:
        - Fornire un'area riservata con autenticazione sicura (es. username e password con lunghezza minima di 8 caratteri, inclusi lettere, numeri e simboli).
        - Consentire la modifica dei dati, incluso il numero di cellulare, con nuova validazione OTP per il cellulare.
        - Bloccare gli acquisti fino alla validazione del nuovo numero di cellulare.
    - **Processo di registrazione**:
        - Può essere suddiviso in più fasi (es. raccolta dati anagrafici, poi validazione OTP).
        - Deve essere completato con successo prima dell'acquisto del primo titolo.
    - **Unicità del numero di cellulare**:
        - Verificare nel database che ogni numero di cellulare sia associato a un solo utente per evento.
        - Implementare controlli per impedire la registrazione multipla con lo stesso numero (es. query SQL per verificare l'unicità).
    - **Implementazione tecnica**:
        - Creare un form di registrazione con validazione client-side e server-side (es. regex per e-mail, formato data).
        - Integrare un servizio di invio SMS (es. Twilio, Nexmo) per l'OTP.
        - Memorizzare i dati utente in un database cifrato (es. AES-256).
- **SPID come Alternativa** (*Allegato A, punto 3.4*):
    - Il sistema può utilizzare l'identità digitale SPID per autenticare gli utenti, eliminando la necessità di registrazione manuale.
    - **Dati acquisiti tramite SPID**:

        - Nome, cognome, data di nascita, come definiti nella Tabella degli attributi SPID di AgID.
        - Codice identificativo (`spidCode`), utilizzato come codice univoco dell'utente o collegato a un codice interno esclusivo.
    - **Implementazione tecnica**:
        - Integrare le API dei provider SPID accreditati (es. PosteID, ArubaID).
        - Mappare i dati SPID ai campi obbligatori (nome, cognome, data di nascita).
        - Associare lo `spidCode` a un codice univoco interno nel database, garantendo l'unicità.
        - Implementare il flusso di autenticazione SAML o OpenID Connect per SPID.
    - **Conformità**:
        - Rispettare il Regolamento di Sistema SPID e le specifiche tecniche di AgID.
        - Testare l'integrazione con scenari reali (es. autenticazione con diversi provider SPID).
        - Garantire la sicurezza delle comunicazioni con il provider SPID (es. TLS 1.3).
- **Tracciabilità dei Pagamenti** (*Allegato A, punto 3.2*):
    - **Metodi di pagamento**:
        - Carte di credito/debito (es. Visa, Mastercard).
        - Bonifici bancari.
        - Wallet digitali conformi (es. PayPal, Satispay).
    - **Dati da registrare**:
        - Data e ora della transazione (formato RFC-2822, es. `2025-06-30T18:43:00Z`).
        - Importo totale, comprensivo di IVA.

        - Metodo di pagamento (es. “Visa”, “Bonifico”).
        - Codice univoco del titolo associato.
        - Sigillo fiscale.
        - Codice richiedente emissione sigillo.
    - **Implementazione tecnica**:
        - Integrare un gateway di pagamento che supporti la tracciabilità (es. Stripe, PayPal).
        - Memorizzare i dettagli del pagamento nel database, associandoli al codice titolo.
        - Garantire la sicurezza delle transazioni con PCI DSS compliance.
- **Consegna dei Titoli** (*Allegato A, punto 3.2*):
    - I titoli non possono essere rilasciati immediatamente al termine dell’acquisto.
    - **Modalità di consegna**:
        - Download da un’area riservata del sito o app.
        - Invio via e-mail in formato PDF con QR code.
        - Visualizzazione su app mobile tramite QR code.
    - **Requisiti**:
        - Solo l’utente identificato (tramite credenziali o SPID) può accedere al titolo.
        - Il QR code deve codificare codice titolo, sigillo fiscale e dati dell’evento.
    - **Implementazione tecnica**:
        - Creare un’area riservata con autenticazione sicura (es. JWT, OAuth2).
        - Generare QR code con una libreria standard (es. ZXing).
        - Inviare e-mail con PDF protetti da password o link sicuri.

2.2 Controllo degli Accessi

- **Lista Unica dei Titoli** (*Provvedimento 4 marzo 2008, punto 3*):
    - **Contenuto**:
        - **Codice titolo**: identificativo univoco.
        - **Sigillo fiscale**: generato dalla carta di attivazione.
        - **Stato**: valido, annullato, modificato.
        - **Dati dell'evento**: nome, data, luogo, settore/posto (se applicabile).
        - **Codice richiedente emissione sigillo**.
        - **Codice utente**: per tracciare l'acquirente.
    - **Aggiornamento**:
        - In tempo reale, se connessa a internet.
        - Trasferita ai dispositivi di controllo prima dell'evento, se offline.
    - **Accesso per gli organi di controllo**:
        - Fornire un'interfaccia web o API per visualizzare la lista unica.
        - Generare report stampabili o digitali (es. PDF, XML) su richiesta.
    - **Implementazione tecnica**:
        - Memorizzare la lista unica in un database relazionale.
        - Fornire un endpoint API (es. REST con autenticazione OAuth2) per l'accesso in tempo reale.
        - Supportare filtri per evento, settore, stato o codice utente.
- **Invalidazione dei Titoli** (*Provvedimento 4 marzo 2008, punto 1.1.1*):
    - **Processo**:
        - Al primo accesso, il titolo è invalidato per prevenire utilizzi multipli.
        - Il dispositivo di controllo verifica il codice titolo e il sigillo fiscale contro la lista unica.
        - Aggiorna lo stato a "annullato" con:

        - Timestamp (formato RFC-2822).
        - Codice del dispositivo o operatore.
    - **Settori specifici**:
        - Supportare la validazione per settori (es. “Tribuna A”) o l’intero evento.
        - Verificare i dati del settore/posto durante il controllo.
    - **Gestione errori**:
        - Segnalare tentativi di accesso multipli con lo stesso titolo.
        - Rifiutare titoli non validi o non trovati nella lista unica.
    - **Implementazione tecnica**:
        - Implementare un sistema di validazione basato su QR code o codici a barre.
        - Aggiornare il database in tempo reale o in modalità batch (offline).
- **Accesso Offline** (*Provvedimento 4 marzo 2008*):
    - **Requisiti**:
        - I dispositivi di controllo devono funzionare senza connessione internet.
        - Memorizzare i dati di validazione localmente (codice titolo, timestamp, stato).
        - Sincronizzare i dati con il server centrale quando la connessione è disponibile.
    - **Implementazione tecnica**:
        - Sincronizzare la lista unica sul dispositivo prima dell’evento (es. tramite file JSON o database locale).
        - Utilizzare una memoria locale cifrata (es. AES-256).
        - Implementare un meccanismo di sincronizzazione (es. API REST per l’upload dei dati).
- **Funzioni di Controllo** (*Provvedimento 4 marzo 2008, punto 6*):

    - **Accesso per organi di controllo**:
        - Fornire un portale dedicato con autenticazione tramite certificati digitali.
        - Visualizzare la lista unica e i log delle operazioni.
        - Supportare filtri per evento, settore, stato o codice utente.
    - **Report**:
        - Generare report in formato XML o PDF, con dettagli sui titoli validati.
        - Fornire statistiche (es. numero di accessi per settore).
    - **Implementazione tecnica**:
        - Creare un'interfaccia web per gli organi di controllo.
        - Implementare endpoint API per l'accesso ai dati.
        - Garantire la sicurezza con autenticazione a due fattori.
- **Conservazione e Trasmissione Dati** (*Provvedimento 4 marzo 2008, punti 9-10*):
    - **Conservazione**:
        - Salvare la lista unica quotidianamente in un file XML con estensione `.XST`.
        - Firmare digitalmente il file con la carta di attivazione (es. SHA-256 per l'integrità, RSA per la firma).
    - **Trasmissione alla SIAE**:
        - Entro 5 giorni lavorativi dall'evento.
        - Via e-mail S/MIME con soggetto: `AAAA>AMM>GG>SSSSSSSS>MP>TT>V`:
            - **AAAA**: anno dell'evento (es. `2025`).
            - **AMM**: mese e giorno (es. `0630` per 30 giugno).
            - **SSSSSSSS**: codice univoco del sistema (8 caratteri).

        - **MP**: modalità di pagamento (es. `CC` per carta, `BO` per bonifico).
        - **TT**: tipo di titolo (es. `BI` per biglietto, `AB` per abbonamento).
        - **V**: versione del file (es. `V01>00`).
    - Esempio: `2025>06>30>12345678>CC>BI>V01>00`.
- **Implementazione tecnica**:
    - Configurare un client e-mail S/MIME con certificati digitali.
    - Validare il formato del soggetto e del file XML prima dell'invio.
    - Implementare un sistema di monitoraggio per confermare la ricezione.

2.3 Sicurezza e Protezione

- **Protezione da Bot** (*Allegato A, punto 3.1*):
    - **Requisiti**:
        - Implementare CAPTCHA conformi agli standard più recenti (es. reCAPTCHA v3).
        - Integrare CAPTCHA in tutte le fasi critiche:
            - Accesso al sistema di vendita.
            - Selezione dei titoli.
            - Checkout dell'ordine.
        - Il CAPTCHA deve essere difficile da eludere per i bot, ma semplice per gli utenti umani.
    - **Implementazione tecnica**:
        - Utilizzare un servizio CAPTCHA (es. Google reCAPTCHA) con analisi comportamentale (es. movimenti del mouse, tempi di interazione).
        - Monitorare i tentativi di accesso ripetuti, bloccando gli IP dopo 5 tentativi falliti in 1 minuto.
        - Registrare i tentativi sospetti nel log, con indirizzo IP e timestamp.

        - Implementare un sistema di rate limiting per prevenire attacchi automatizzati.

- **Cifratura delle Comunicazioni** (*Allegato A, punto 3.6*):
    - **Requisiti**:
        - Utilizzare HTTPS con TLS 1.2 o superiore (preferibilmente TLS 1.3).
        - Cifrare i dati in entrata e in uscita (es. dati utente, sigilli fiscali, dettagli di pagamento).
        - Impedire a terze parti di leggere, modificare o inserire messaggi durante la trasmissione.
    - **Implementazione tecnica**:
        - Configurare certificati SSL/TLS validi (es. Let's Encrypt, DigiCert).
        - Utilizzare algoritmi di cifratura robusti (es. AES-256, ECDSA).
        - Implementare HSTS (HTTP Strict Transport Security) per forzare connessioni sicure.
        - Verificare la configurazione TLS con strumenti come SSL Labs.
- **Log delle Operazioni** (*Allegato A, punto 3.5; Allegato B, punto 1*):
    - **Dati da registrare**:
        - **Codice univoco dell'utente**: generato durante la registrazione o tramite SPID.
        - **Codice titolo**.
        - **Sigillo fiscale**.
        - **Identificativo evento** (es. "EVENT123").
        - **Timestamp** (formato RFC-2822, es. `2025-06-30T18:43:00Z`).
        - **Tipo di operazione** (es. "Acquisto", "Validazione", "Annullamento").
        - **Indirizzo IP della transazione** (*Allegato B, "IndirizzoIPMedzioneIPTitlo"*).

- **Protezione della privacy** (GDPR):
  - Utilizzare solo il codice univoco dell'utente nei log, senza dati anagrafici.
  - Cifrare i dati sensibili durante l'archiviazione (es. AES-256).
  - Fornire accesso ai dati anagrafici solo su richiesta degli organi di controllo, con autenticazione sicura.
- **Formato**:
  - File XML conforme al Decreto del 23 luglio 2001.
  - Esempio di struttura:
    - : elemento radice.
    - : codice univoco dell'utente.
    - : codice del titolo.
    - : data e ora.
    - : tipo di operazione.
    - : indirizzo IP (IPv4 o IPv6).
- **Accesso ai log**:
  - Fornire un'interfaccia per gli organi di controllo (es. portale web).
  - Conservare i log per almeno 5 anni, come previsto dalle normative fiscali.

- **Sigillo Fiscale** (*Allegato A, Glossario; Provvedimento 4 marzo 2008*):
  - **Requisiti**:
    - Generato dalla carta di attivazione per ogni titolo.
    - Associato al codice richiedente emissione sigillo.
    - Riportato sul titolo e nei file XML.
    - Verificabile dagli organi di controllo.

- **Implementazione tecnica**:
    - Generare il sigillo tramite l'algoritmo della carta di attivazione.
    - Verificare l'integrità del sigillo durante il controllo accessi (es. confronto con la lista unica).

2.4 Secondary Ticketing

- **Normative Specifiche** (*Allegato A; Provvedimento 21 dicembre 2021*):
    - Il Decreto MEF del 12 marzo 2018 disciplina il *secondary ticketing* (rivendita di titoli da parte di soggetti diversi dai titolari dei sistemi di emissione).
    - Il Provvedimento del 21 dicembre 2021 proroga di 10 mesi i termini per l'adeguamento dei sistemi (scadenza indicativa: ottobre 2022, da verificare per ulteriori proroghe al 30 giugno 2025).
- **Identificazione Acquirenti** (*Allegato A, punti 3.3, 3.4*):
    - Applicare le stesse regole di registrazione e validazione (OTP o SPID) per gli acquirenti nel mercato secondario.
    - **Dati da registrare**:
        - **Acquirente originale**: nome, cognome, data di nascita, luogo di nascita, e-mail, cellulare, codice fiscale (se richiesto).
        - **Nuovo titolare**: stessi dati, con aggiornamento del codice univoco associato al titolo.
    - **Tracciamento del trasferimento**:
        - Aggiornare la lista unica con il nuovo codice utente.
        - Registrare il trasferimento nel log delle operazioni.
- **Prezzo di Rivendita**:
    - Impedire la rivendita a prezzi superiori al valore nominale, salvo commissioni autorizzate.
    - Verificare il prezzo di rivendita rispetto al prezzo originale durante la transazione.
- **Trasmissione Dati** (*Provvedimento 4 marzo 2008*):

- Includere le transazioni di *secondary ticketing* nella lista unica.
- Trasmettere i dati alla SIAE entro 5 giorni lavorativi in formato XML `.XST`.

---

3. Struttura dei Dati

3.1 Formati dei File

- **Formato ASCII a Campi Fissi** (*Allegato B, punto 1a; Provvedimento 4 marzo 2008, Allegato A*):
  - **Struttura**:
    - Campi alfanumerici: allineati a sinistra, spazi per valori non significativi.
    - Campi numerici: allineati a destra, zeri per valori non significativi.
  - **Campo chiave**: “Codice richiedente emissione sigillo”:
    - Posizioni: 85-92.
    - Lunghezza: 8 caratteri.
    - Esempio: `02ABCDEF` (02 = sito web, ABCDEF = codice univoco).
  - **Altri campi**:
    - Codice titolo.
    - Sigillo fiscale.
    - Dati dell’evento (nome, data, luogo).
  - **Implementazione tecnica**:
    - Generare file ASCII per compatibilità con sistemi legacy.
    - Validare la lunghezza e il formato dei campi prima della trasmissione.
- **Formato XML** (*Allegato B, punto 1b; Provvedimento 4 marzo 2008, Allegato C*):
  - **Conformità**: XML 1.0 (W3C, 10 febbraio 1998).

- **Struttura per i titoli**:
  - : elemento radice.
  - : identificativo univoco (testo).
  - : identificativo dell'evento (testo).
  - : stato del titolo (es. "Valido", "Annullato").
  - : sigillo fiscale (testo).
  - : codice univoco dell'utente (testo).
  - : indirizzo IP della transazione (testo, *Allegato B*).
- **Struttura per i log** (*Allegato A, punto 3.5*):
  - : elemento radice.
  - : codice univoco dell'utente.
  - : codice del titolo.
  - : data e ora (RFC-2822).
  - : tipo di operazione.
  - : indirizzo IP (IPv4 o IPv6).
- **File di riepilogo accessi**:
  - Estensione: `.XST`.
  - Conformità al DTD specificato nell'Allegato C del Provvedimento 4 marzo 2008.
- **Nomenclatura dei file** (*Allegato B, punto 10*):
  - Lettere maiuscole o minuscole.
  - Seguire il formato del soggetto e-mail (es. `2025>06>30>12345678>CC>BI>V01>00`).
- **Implementazione tecnica**:

        - Utilizzare una libreria XML (es. lxml per Python, JAXB per Java) per generare e validare i file.
        - Validare i file contro il DTD prima della trasmissione.

- **Campi Obbligatori nel Formato XML** (*Allegato B, punto 4*):
    - : tipo di emissione (es. “Primaria”, “Secondaria”).
    - : valuta (es. “EUR”).
    - : stato dell’emissione (es. “Completata”).
    - : identificativo della carta di attivazione.
    - : gestione della carta di attivazione (es. versione del software).
    - : data di emissione (ISO 8601).
    - : numero progressivo del titolo.
    - : tipo di titolo (es. “Biglietto”, “Abbonamento”).
    - : probabile errore di OCR per “codice transazione” o simile.
    - : informazioni sulla cassa emittente (probabile errore di OCR).
    - : numero di cellulare (testo).
    - : codice dell’abbonamento, se applicabile (testo).
    - : codice del concedente (es. organizzatore).
    - : codice fiscale dell’acquirente (testo, probabilmente obbligatorio una sola volta).
    - **Nota**: Le ripetizioni di e in *Allegato B* sono probabili errori di OCR. Verificare con il documento ufficiale.
- **Indirizzo IP** (*Allegato B, “IndirizzoIPMedzioneIPTitlo”*):
    - Registrare l’IP (IPv4 o IPv6) per ogni transazione di acquisto.
    - Descrizione: “Gruppo di informazioni relative all’indirizzo IP dal quale è stata effettuata la transazione.”

- Includerlo nei log XML e nei file `.XST`.

3.2 Dati Obbligatori

- **Dati Utente** (*Allegato A, punto 3.3*):
  - Nome, cognome, data di nascita, luogo di nascita, indirizzo e-mail, numero di cellulare univoco.
  - Per SPID: dati acquisiti dallo `spidCode` (nome, cognome, data di nascita).
  - Codice fiscale (opzionale, obbligatorio su richiesta degli organi di controllo).
- **Dati Titolo** (*Allegato B; Provvedimento 4 marzo 2008*):
  - Codice univoco, sigillo fiscale, codice richiedente emissione sigillo, data e luogo dell'evento, settore/posto (se applicabile), prezzo, stato, valuta, tipo di titolo.
- **Log delle Operazioni** (*Allegato A, punto 3.5*):
  - Codice univoco dell'utente, codice titolo, sigillo fiscale, identificativo evento, timestamp, tipo di operazione, indirizzo IP.

---

4. Flusso di Lavoro per lo Sviluppatore

4.1 Progettazione del Sistema

- **Backend**:
  - Sviluppare un server robusto (es. Node.js, Java Spring, Python Flask/Django) per:
    - Emissione dei titoli con sigilli fiscali.
    - Validazione e invalidazione dei titoli.
    - Trasmissione dei dati alla SIAE.
  - **Database**:
    - Utilizzare un database relazionale (es. PostgreSQL, MySQL) con tabelle:

            - **Utenti**: codice univoco, nome, cognome, data di nascita, luogo di nascita, e-mail, cellulare, codice fiscale.
            - **Titoli**: codice titolo, sigillo fiscale, codice richiedente, dati evento, stato, prezzo.
            - **Log**: codice utente, codice titolo, timestamp, tipo operazione, indirizzo IP.
        - Implementare indici per ricerche rapide (es. su codice titolo, sigillo fiscale).
    - **Integrazione carta di attivazione**:
        - Configurare un HSM o un'interfaccia software per la carta.
        - Generare sigilli fiscali e firme digitali.
        - Testare l'integrazione con scenari reali.
- **Frontend**:
    - Creare un'interfaccia utente (es. React, Angular) con:
        - Modulo di registrazione con validazione dei dati.
        - Pannello per l'inserimento dell'OTP.
        - Visualizzazione dei titoli digitali (QR code).
        - Controlli per limiti di acquisto (max 10 titoli).
        - CAPTCHA in tutte le fasi critiche.
    - Garantire accessibilità (es. WCAG 2.1) e usabilità.
- **Integrazione Pagamenti**:
    - Integrare un gateway di pagamento (es. Stripe, PayPal) con PCI DSS compliance.
    - Memorizzare i dettagli del pagamento nel database.
    - Associare ogni transazione al codice titolo e al sigillo fiscale.
- **Generazione Titoli**:

    - Generare titoli con sigillo fiscale e codice richiedente.
    - Supportare formati fisici e digitali.
    - Implementare la consegna differita tramite download, e-mail o app mobile.

4.2 Autenticazione e Validazione

- **Registrazione Utente** (*Allegato A, punto 3.3*):
    - Implementare un form di registrazione con validazione client-side e server-side.
    - Integrare un servizio SMS (es. Twilio) per OTP di 8 cifre.
    - Creare un pannello per l'inserimento dell'OTP con timeout e limite di tentativi.
    - Verificare l'unicità del numero di cellulare.
- **SPID (Opzionale)** (*Allegato A, punto 3.4*):
    - Integrare le API dei provider SPID accreditati.
    - Mappare i dati SPID ai campi obbligatori.
    - Associare lo `spidCode` a un codice univoco interno.
    - Testare l'autenticazione con diversi provider SPID.
- **Protezione da Bot** (*Allegato A, punto 3.1*):
    - Configurare reCAPTCHA v3 per tutte le fasi di acquisto.
    - Implementare rate limiting e blocco IP per tentativi sospetti.
    - Registrare i tentativi nel log delle operazioni.

4.3 Controllo Accessi

- **Dispositivi di Controllo** (*Provvedimento 4 marzo 2008*):
    - Sviluppare un'app mobile (iOS, Android) per la scansione di QR code/codici a barre.
    - Supportare la lettura di titoli fisici e digitali.

    - Mostrare lo stato del titolo (valido, annullato, non trovato).

- **Invalidazione** (*Provvedimento 4 marzo 2008, punto 1.1.1*):
    - Invalidare il titolo al primo accesso, aggiornando la lista unica.
    - Gestire settori/posti specifici.
    - Segnalare errori (es. titolo già usato).
- **Accesso Offline**:
    - Sincronizzare la lista unica prima dell'evento.
    - Memorizzare le validazioni localmente in formato cifrato.
    - Sincronizzare i dati con il server centrale.
- **Accesso per Organi di Controllo** (*Provvedimento 4 marzo 2008, punto 6*):
    - Creare un portale con autenticazione a due fattori.
    - Fornire filtri per evento, settore, stato o codice utente.
    - Generare report in XML o PDF.

4.4 Trasmissione Dati alla SIAE

- **Generazione File** (*Provvedimento 4 marzo 2008, punti 9-10*):
    - Creare file XML `.XST` giornalieri con la lista unica.
    - Firmare i file con la carta di attivazione.
    - Validare i file contro il DTD.
- **Invio** (*Provvedimento 4 marzo 2008*):
    - Configurare un client e-mail S/MIME.
    - Usare il formato del soggetto corretto.
    - Monitorare la trasmissione e gestire errori.

4.5 Test e Certificazione

- **Test Funzionali**:
    - Simulare acquisto, validazione, annullamento, trasmissione dati.
    - Testare la protezione anti-bot e l'accesso offline.
    - Validare i file XML contro il DTD.
- **Certificazione** (*Provvedimento 4 marzo 2008, punto 8*):
    - Presentare il sistema alla Commissione dell'Agenzia delle Entrate.
    - Fornire documentazione tecnica dettagliata.
    - Testare l'integrazione della carta di attivazione.

---

5. Considerazioni Aggiuntive

- **Proroga COVID-19** (*Provvedimento 21 dicembre 2021*):
    - Scadenza indicativa: ottobre 2022, da verificare al 30 giugno 2025 per ulteriori proroghe.
- **Errori di OCR**:
    - Correggere errori come "spetttacolo" (spettacolo), "luggu" (luglio), "biagletterie" (biglietterie), "codiscortione" (codice transazione).
    - Verificare i documenti ufficiali sul sito dell'Agenzia delle Entrate.
- **Allegati 1-4**:
    - Contengono numeri di pagina o codici di riferimento ("30", "31", "32", "33 - 33").
- **Privacy** (*Allegato A, punto 3.5*):
    - Conformità al GDPR con minimizzazione dei dati e cifratura.
    - Fornire un'informativa privacy chiara.
- **Scalabilità**:
    - Utilizzare infrastrutture cloud (es. AWS) con bilanciamento del carico.

- **Supporto Tecnico**:
    - Creare un canale di supporto per utenti e organi di controllo.

---

6. Riferimenti Normativi

- **Leggi e Decreti**:
    - DPR 26 ottobre 1972, n. 633 (IVA).
    - DPR 26 ottobre 1972, n. 640 (Imposta sugli spettacoli).
    - Decreto Legislativo 26 febbraio 1999, n. 60.
    - Decreto MEF 12 marzo 2018 (GU 27 aprile 2018).
    - Legge 11 dicembre 2016, comma 545.
- **Provvedimenti Agenzia delle Entrate**:
    - 23 luglio 2001.
    - 22 ottobre 2002.
    - 3 agosto 2004.
    - 4 marzo 2008.
    - 9 maggio 2014.
    - 21 dicembre 2021.
- **Standard Tecnici**:
    - ISO 3166 (codici paese).
    - W3C XML 1.0 (10 febbraio 1998).
    - RFC-2822 (timestamp).
    - TLS 1.2 o superiore.
    - S/MIME.

---

7. Raccomandazioni Finali

- **Collaborazione con SIAE**: Contattare la SIAE per ottenere la carta di attivazione e chiarimenti tecnici.
- **Documentazione**: Fornire schema del database, flussi operativi, specifiche di sicurezza.
- **Monitoraggio Normativo**: Verificare aggiornamenti sul sito dell'Agenzia delle Entrate.
- **Test di Conformità**: Simulare scenari reali e verificare la conformità dei file XML.
- **Integrazione SPID**: Collaborare con provider accreditati AgID.
- **Gestione Errori**: Implementare notifiche chiare e log dettagliati.
