SPECIFICHE TECNICHE

LOTTERIA DEGLI SCONTRINI ISTANTANEA

Versione 1.0

INDICE

1. FINALITÀ DEL DOCUMENTO

L'articolo 1, commi da 540 a 544, della legge 11 dicembre 2016, n. 232 è stato modificato introducendo, tra l'altro, la lotteria degli scontrini ad estrazione istantanea, che prevede una verifica immediata della vincita.

Con il provvedimento interdirettoriale del Direttore dell'Agenzia delle dogane e dei monopoli d'intesa con il Direttore dell'Agenzia delle entrate n. 80217 del 5 marzo 2020 e successive modificazioni, sono stabilite le regole per la partecipazione alle lotterie degli scontrini.

Con il presente documento vengono definite le specifiche tecniche necessarie per l'attuazione della lotteria istantanea.

In particolare, sono definiti:

- i meccanismi e le procedure finalizzate a garantire la sicurezza dei dati da trasmettere, mediante l'utilizzo di un codice bidimensionale da riportare su ciascun documento commerciale che rispetti i requisiti previsti dal provvedimento interdirettoriale del 5 marzo 2020 e successive modificazioni sopra citato;
- i servizi di interoperabilità tra il sistema lotteria e i registratori telematici ovvero i server-RT (nel seguito del presente documento, "dispositivi"), attraverso cui gestire il processo e la sicurezza necessaria alla partecipazione dei cittadini alla lotteria istantanea.

Infine, vengono descritte le interfacce utente dedicate ai soggetti passivi IVA titolari dei registratori telematici (nel seguito del presente documento, RT) ovvero dei server-RT per salvaguardare le informazioni di sicurezza utilizzate per la lotteria istantanea.

2. REQUISITI TECNICI LOTTERIA SCONTRINI ISTANTANEA

2.1 MEMORIZZAZIONE E STAMPA CODICE BIDIMENSIONALE

La presenza di un Codice Bidimensionale (nel seguito del presente documento, CB) sul documento commerciale è un elemento indispensabile per la partecipazione alla lotteria istantanea e deve contenere tutte le informazioni necessarie per permettere la successiva fase di verifica. Il suddetto codice bidimensionale è memorizzato nella memoria permanente del dispositivo insieme al documento commerciale a cui si riferisce.
I registratori telematici rispettano il nuovo layout di stampa definito nell'allegato "Allegato – Layout documento commerciale v5", comprensivo di codice bidimensionale.

Il CB deve essere eventualmente inserito in aggiunta al codice lotteria, se quest'ultimo viene fornito dal consumatore, e non deve essere presente nel caso venga comunicato il codice fiscale.

Per la generazione del CB, i dispositivi devono rispettare i seguenti vincoli tecnici:

- per la generazione del CB deve essere utilizzato lo standard ISO/IEC 16022:2006 (Data Matrix);
- il sistema di correzione dell'errore adottato deve essere ECC200;
- la codifica alfanumerica.

La produzione del CB deve rispettare i medesimi vincoli in ambito RT e Server-RT ad eccezione e limitatamente agli apparati, RT o punti cassa, che non siano in grado di produrre un Data Matrix. Esclusivamente per tali dispositivi è ammessa la produzione di un CB in formato QR Code secondo lo standard ISO/IEC 18004:2015 con un sistema di correzione d'errore Level H (High).

2.2 SICUREZZA CODICE BIDIMENSIONALE

La produzione del Codice Bidimensionale deve prevedere misure di sicurezza allo scopo di mitigare il rischio rispetto alla produzione di codici fittizi e tali che garantiscano l'autenticità e integrità delle informazioni in esso contenute. Per raggiungere tale risultato sono stabiliti meccanismi di cifratura delle informazioni attraverso l'utilizzo di chiavi di cifratura rilasciate dall'Agenzia delle entrate mediante la chiamata al servizio dedicato denominato "rilascio codici" descritto dei successivi paragrafi.

I dispositivi al fine di rendere inalterabili le informazioni contenute nel CB devono aggiungere un elemento di signature prodotto mediate l'applicazione dell'algoritmo HMAC specificato allo standard RFC 2104, utilizzando la funzione di "message digest" SHA256 ed il codice rilasciato dal suddetto servizio: l'output prodotto dall'algoritmo è di 32 bytes (64 caratteri).

Per garantire tale sicurezza ciascun RT e ciascuna cassa collegata al Server-RT devono gestire una coppia di codici, codice segreto e codice offuscato, con validità

giornaliera rilasciati dall'Agenzia delle entrate, le cui modalità di utilizzo sono descritte nel dettaglio nei paragrafi successivi.

2.3 SICUREZZA DI COLLOQUIO

Per il recupero delle coppie di codici con validità giornaliera il sistema lotteria istantanea deve prevedere il servizio "rilascio codici", richiamabile dal dispositivo.
La cornice di sicurezza utilizzata è la medesima già in uso dal sistema dei corrispettivi per il colloquio fra RT e sistema Agenzia delle entrate con l'aggiunta di ulteriore cifratura dei dati scambiati.

Tale ulteriore meccanismo di cifratura prevede:

- la predisposizione da parte del sistema Agenzia delle entrate di una nuova chiave AES a 256 bits temporanea valida per il solo set di informazioni scambiate (Content Encryption Key – CEK);
- l'utilizzo della chiave CEK per cifrare i valori del set informativo. Il meccanismo di cifratura da utilizzare è di tipo AES in modalità CBC (Cipher Block Chaining) senza l'utilizzo di padding, secondo le specifiche NIST Special Publication 800-38A "Recommendation for Block Cipher Modes of Operation: Methods and Techniques". L'algoritmo deve utilizzare un vettore d'inizializzazione di 16 bytes (IV), predisposto da Agenzia delle entrate e distinto per ogni singola operazione di cifratura effettuata;
- la cifratura della chiave CEK, con l'ultima chiave pubblica rilasciata al singolo RT (Key Encryption Key - KEK). Il meccanismo di cifratura deve essere RSAES-PKCS1-v1_5, come specificato in "PKCS #1 version 2.2" (RFC 8017);
- la trasmissione della chiave CEK cifrata, degli IV e del set informativo cifrato al dispositivo.

La chiave CEK di cifratura del set di informazioni di sicurezza è temporanea e varia ad ogni richiamo al servizio, analogamente per i vettori d'inizializzazione IV, anche nel caso di medesimo set di informazioni restituito.

Ciascun RT deve richiedere i codici di propria competenza, mentre ogni Server-RT si deve occupare di gestire i codici di tutti i punti cassa ad esso collegati.

La comunicazione tra Server-RT e punto cassa deve garantire un adeguato livello di sicurezza nel trasferimento dei codici segreti ai punti cassa, adottando modalità di cifratura dei valori ed attraverso il canale sicuro esistente. In particolare, il punto cassa richiede al server la sua chiave Pubblica (quella del certificato dispositivo), utilizzando la quale invia al Server-RT un proprio codice criptato. A sua volta il Server-RT, con la sua chiave privata, recupera tale codice criptato e lo utilizza per cifrare il pacchetto dei dati da trasmettere al punto cassa.

La comunicazione tra punto cassa e server RT deve seguire i seguenti requisiti minimi:

- predisposizione da parte del punto cassa di una nuova chiave AES a 256 bits temporanea valida per il solo set di informazioni scambiate (Content Encryption Key – CEK);

- cifratura della chiave CEK da parte del punto cassa con la chiave pubblica del certificato dispositivo serverRT mediante il meccanismo RSAES-PKCS1-v1_5 descritto nei periodi precedenti;

- I codici giornalieri inviati dal Server-RT al punto cassa devono essere cifrati mediante la chiave CEK utilizzando il meccanismo AES-CBC senza utilizzo di padding descritto nei periodi precedenti.

Nei casi in cui il Server-RT non riesca a decifrare la chiave CEK inviatagli dal punto cassa, questo non deve mai fornire in risposta un esito che dettagli il motivo per cui l'operazione di decifratura non sia stata possibile (ad es. errore sul padding) ma sia un valore generico di "errore decifratura dati".

Inoltre si ricorda quanto riportato nelle Specifiche tecniche V11 in materia di punti cassa: "*I singoli punti cassa da cui provengono i dati dei corrispettivi devono essere connessi direttamente, o tramite il server di consolidamento presente nel punto vendita, al RT, prevedendo in particolare un protocollo di scambio dati interno che garantisca un adeguato livello di inalterabilità e confidenzialità dei dati scambiati*".

2.4 SICUREZZA NELLA MEMORIZZAZIONE DELLE INFORMAZIONI

Un altro aspetto di protezione riguarda la modalità di memorizzazione nel dispositivo delle informazioni di sicurezza che il sistema lotteria istantanea rilascia al singolo dispositivo, come la chiave CEK e la coppia di codici (segreto e offuscato).

I vincoli ed il livello di protezione devono essere analoghi a quelli attualmente in uso per i certificati utilizzati nel Sistema dei Corrispettivi telematici, con la finalità di garantirne integrità ed inalterabilità. In particolare, i vincoli da rispettare sono i seguenti:

- i codici segreti devono essere memorizzati in una delle memorie disponibili sul RT diversa da quella di lavoro, anche in funzione dello spazio realmente disponibile per le diverse tipologie di dispositivo *(Cfr. Specifiche tecniche V11: "modulo fiscale" è composto da: una memoria non alterabile" (a sola lettura) contenente un programma ("firmware fiscale") per la gestione esclusiva dei dati fiscali, separato dal punto di vista logico e funzionale dai software gestionali, …una "memoria permanente" non riscrivibile atta a contenere i dati fiscali… La "memoria permanente" si articola in due componenti: la memoria di "riepilogo" e la memoria di "dettaglio", entrambe allocate all'interno dell'involucro contenente il modulo fiscale e protetto dal sigillo fiscale in modo da garantirne l'inaccessibilità.)*. Tali codici devono essere cifrati mediante la chiave CEK e memorizzati. Deve essere decifrato il solo codice segreto in corso di validità giornaliera. I codici segreti devono poter essere fruibili per la sola predisposizione dei CB e per il solo periodo di validità. I dispositivi non devono poter più leggere e utilizzare i codici già fruiti ovvero, nel caso di memorizzazione di nuovi codici, non possono più leggere e utilizzare i codici precedentemente memorizzati.

- la chiave CEK temporanea può essere memorizzata anche nella memoria di lavoro *(Cfr. Specifiche tecniche V11: memoria atta a contenere dati temporanei prima*

del loro consolidamento nella memoria permanente. …In assenza di alimentazione elettrica esterna, un'idonea batteria tampone garantisce il mantenimento dei dati contenuti nella memoria di lavoro). La chiave CEK può essere salvata sovrascrivendo o senza sovrascrivere la chiave CEK valida per il precedente set di informazioni di sicurezza. Nel secondo caso può essere previsto un processo di cancellazione periodica delle chiavi CEK relative a set di informazioni di sicurezza inerenti periodi di validità trascorsi, al fine di ridurre i tempi di esaurimento della memoria di lavoro.

In ambito memorizzazione vengono esplicitate alcune peculiarità di ciascuna tipologia di dispositivo. Per gli RT è sufficiente rispettare i vincoli già descritti in precedenza con l'accortezza di utilizzare una memoria sicura. Nell'architettura dei Server-RT, a garanzia della memorizzazione sicura, i codici devono essere mantenuti sul server e non nel punto cassa, garantendo un grado di sicurezza analogo a quello previsto per i dati fiscali in ambito Corrispettivi giornalieri. Per consentire la predisposizione del CB sul punto cassa, utilizzando le informazioni di sicurezza necessarie, i produttori dei Server-RT devono realizzare una nuova API implementata sul Server-RT che permetta al punto cassa di richiedere giornalmente i codici segreti in corso di validità giornaliera. Si precisa che l'API richiamata dal generico punto cassa deve restituire i codici in corso di validità giornaliera e validi per la giornata successiva salvandoli come descritto nel par. 3.2 (punti elenco codici in chiaro e criptati). Nel caso in cui il punto cassa sia impossibilitato a contattare il Server-RT per il recupero del codice giornaliero i documenti commerciali prodotti non riportano il codice bidimensionale.

Come ulteriore aspetto di sicurezza rispetto alla memorizzazione delle informazioni, i dispositivi devono garantire l'accesso ai codici segreti ricevuti ai soli processi informatici, per la loro gestione e per la predisposizione del CB sul documento commerciale.

3. GESTIONE CODICI

Per produrre un Codice Bidimensionale sicuro i dispositivi hanno bisogno di recuperare dal Sistema lotteria istantanea tutti i dati che consentono la cifratura delle informazioni. In particolare:

- la chiave CEK ed i relativi vettori d'inizializzazione IV;
- i codici segreti con validità giornaliera.

Per produrre un CB idoneo, il dispositivo deve disporre giornalmente di una coppia di chiavi valide e la chiave CEK corrispondente; in caso contrario i documenti commerciali prodotti dal dispositivo non devono riportare alcun CB.

Il Sistema lotteria istantanea mette a disposizione un apposito servizio "rilascio codici", mentre il dispositivo deve essere evoluto per il recupero, la memorizzazione e la gestione delle informazioni di sicurezza. Infine, è necessario introdurre la gestione dell'annullamento dei codici di sicurezza per far fronte a tutti gli eventi che richiedono di inibirne l'utilizzo.

Il servizio "rilascio codici" deve essere disponibile a partire dalla data stabilita dal provvedimento interdirettoriale in materia di lotteria istantanea. Fino a quel momento il servizio potrebbe risultare non disponibile ovvero rispondere con "HTTP 410", a segnalare che la chiamata è avvenuta prima della data di effettiva partenza della lotteria istantanea. Il software dei dispositivi deve essere in grado di inserire una data programmata, antecedente a quella prevista per la partenza della lotteria istantanea, prima della quale il servizio rilascio codici non deve essere richiamato. Nel caso in cui la risposta è "HTTP 410", i documenti commerciali prodotti non devono contenere il codice bidimensionale e riportare qualsiasi riferimento alla lotteria istantanea.

3.1 RILASCIO CODICI

Per fornire le coppie di codici con validità giornaliera il Sistema Lotteria Istantanea espone il servizio "rilascio codici", richiamabile direttamente dal dispositivo.

La chiamata deve avvenire in modalità "API-REST" su canale cifrato esclusivamente con protocollo TLS 1.2, in analogia a quanto già avviene in ambito corrispettivi giornalieri e lotteria degli scontrini.

Tale servizio deve poter essere richiamato solo da dispositivi con stato "IN_SERVIZIO", impostato con la prima trasmissione del tracciato dei corrispettivi giornalieri. Pertanto, una volta attivato il dispositivo, il primo tracciato da trasmettere è quello relativo all'invio dei dati dei corrispettivi giornalieri (per modificare lo stato); successivamente possono essere effettuate le necessarie chiamate al servizio di rilascio dei codici di sicurezza. Se un dispositivo viene sottoposto ad un cambio di stato non potrà effettuare il recupero dei codici per la lotteria istantanea se non viene precedentemente riportato nello stato "IN_SERVIZIO", con le regole stabilite in ambito corrispettivi giornalieri.

Quando il dispositivo invoca il servizio, mediante la predisposizione di un apposito file XML firmato con il certificato dispositivo e la chiamata all'endpoint dedicato, il Sistema Lotteria Istantanea effettua prima le verifiche sul file di input, formato e firma, e solo successivamente controlla il dispositivo chiamante, esistenza e stato. Esclusivamente nel caso in cui i controlli hanno esito positivo il Sistema Lotteria Istantanea predispone il file di risposta, firmato dal sistema Agenzia delle entrate in analogia a quanto già avviene nel Sistema Corrispettivi.

In particolare, il dispositivo deve effettuare un invio al Sistema Lotteria Istantanea del file xml conforme al tracciato "Allegato - Tipi Dati Rilascio Codici_ver1.0", utilizzando il certificato "dispositivo" per firmarlo. L'invio, invocando il servizio "rilascio codici", restituisce un numero fisso di coppie di codici, con la corrispondente validità, e la chiave CEK utilizzando un file xml conforme al tracciato "Allegato - Tipi Dati Esito Rilascio Codici_ver1.0". Il servizio e le strutture dati sono dettagliate negli appositi allegati, i cui riferimenti sono indicati nel paragrafo Allegati Tecnici.

Di seguito si riporta l'elenco delle informazioni necessarie alla produzione del CB rilasciate dal sistema lotteria istantanea:

- identificativo univoco del codice segreto (5 caratteri); da concatenare alle informazioni presenti nel CB;
- codice offuscato fornito dal sistema Agenzia delle entrate (32 byte o 64 caratteri); da concatenare alle informazioni del CB prima della cifratura;
- codice segreto (32 byte o 64 caratteri); utilizzato come chiave dell'algoritmo HMAC;
- data di validità delle precedenti informazioni.

Il servizio ad ogni chiamata restituisce 12 elementi diversi con validità giornaliera per coprire 12 giorni a partire da quello in cui viene invocato, in conformità con la norma che regola sia l'invio dei corrispettivi telematici giornalieri sia dei dati Lotteria degli scontrini. Questo permette al dispositivo di gestire eventuali situazioni di mancata connessione e consente di ridurre le interazioni con il Sistema Lotteria Istantanea per il recupero del set di informazioni di sicurezza.

Quindi, la modalità ordinaria di richiamo al servizio prevede un paio di invocazioni all'interno del periodo dei 12 giorni coperti dalla singola chiamata. Sono da considerare residuali i casi in cui il dispositivo effettui più chiamate all'interno della stessa giornata. Al fine di evitare la concentrazione di operazioni negli orari di apertura e/o chiusura delle casse, la richiesta deve avvenire utilizzando un orario casuale all'interno dell'intervallo di funzionamento del dispositivo. Tuttavia, la chiamata al servizio "rilascio codici" viene protetta, configurando un limite massimo di richieste al minuto dallo stesso dispositivo. Il software dei dispositivi deve implementare un controllo che impedisca richieste ravvicinate di codici, nel caso si superasse il limite previsto nel minuto, il sistema restituisce il codice http 429. Nel caso il dispositivo richiami il servizio "rilascio codici" prima dei 12 giorni, vengono restituiti la quota parte dei codici validi già inviati in relazione alla corrispondente data di validità. In particolare, il primo codice segreto è quello utilizzabile per la data corrente al momento della richiesta e seguono quelli validi per gli 11 giorni successivi. In questo caso la chiave CEK è diversa dalla precedente, così come i

relativi vettori d'inizializzazione IV, pertanto la precedente chiave CEK non risulterà più valida per l'utilizzo.

Anche nel caso di Server-RT, il servizio restituisce 12 elementi validi per ciascuna chiamata, con la differenza che devono essere effettuare tante chiamate quanti sono i suoi punti cassa mappati. A tal fine, al momento della chiamata, il Server-RT deve valorizzare un parametro relativamente alla matricola del singolo punto cassa per il quale si stanno richiedendo i codici. Il Sistema Lotteria Istantanea manterrà la mappatura dei codici con il punto cassa a cui sono stati rilasciati, che verrà controllata nella fase di interrogazione del CB.

Per motivi di sicurezza le informazioni presenti nel file di risposta, predisposto dal Sistema Lotteria Istantanea, da mantenere riservate, devono essere cifrate prima di poter essere inviate al dispositivo.
Tale ulteriore meccanismo di cifratura, i cui requisiti tecnici sono stati già definiti nel capitolo 2, prevede:

- predisposizione di una chiave AES temporanea (CEK), generata dal Sistema Lotteria Istantanea e valida per un solo set di informazioni scambiate;

- cifratura della chiave AES con la chiave pubblica del dispositivo e suo inserimento nel file di risposta;

- utilizzo della chiave AES in chiaro unitamente ai vettori d'inizializzazione IV, generata per cifrare i singoli elementi di sicurezza del set informativo da rilasciare nella sessione corrente. Di ciascun elemento <BloccoCodici> devono essere cifrati esclusivamente i codici che devono rimanere riservati, quindi <CodOffuscato> e <CodSegreto>. Tutte le restanti informazioni sono in chiaro.

Si precisa che l'operazione di cifratura viene sempre seguita da una conversione in base64 della stringa ottenuta, quindi il dispositivo per recuperare i valori in chiaro deve effettuare le medesime operazioni in senso inverso. Le caratteristiche dei singoli campi sono descritte nel tracciato che il servizio "rilascio codici" restituisce all'apparato (Allegato-Tipi Dati Esito Rilascio Codici_ver1.0).

Si evidenzia che la chiave CEK di cifratura del set di informazioni di sicurezza è temporanea e varia ad ogni richiamo al servizio "rilascio codici", anche nel caso debba essere restituito il medesimo set di informazioni. Analogamente per i vettori d'inizializzazione utilizzati.

Come fattore di verifica della validità delle informazioni scambiate fra il sistema Lotteria Istantanea e il singolo dispositivo, viene utilizzato un ulteriore elemento, costruito applicando l'algoritmo di hash SHA-256. In particolare, il sistema concatena il generico set di codici, composto da identificativo univoco del codice segreto, data validità, codice offuscato in chiaro e codice segreto in chiaro ed applica la funzione di hashing. Il valore in chiaro ottenuto viene aggiunto come ulteriore informazione nella risposta al servizio "rilascio codici' dopo la trasformazione in base64. Quando il dispositivo, RT o Server-RT, decifra le informazioni ha la possibilità di ricalcolare il valore del HASH inviato e verificare l'integrità delle informazioni di sicurezza. Qualora venisse riscontrata una non corrispondenza è possibile richiamare nuovamente il servizio per ottenere un nuovo set di informazioni di sicurezza.

Il sistema prevede la possibilità di richiedere codici di sicurezza fittizi per poter effettuare tutte le operazioni sui dispositivi non soggette alla certificazione dei corrispettivi. A tal fine è necessario richiamare il servizio di rilascio codici impostando nel tracciato xml di input “Allegato - Tipi Dati Rilascio Codici_ver1.0” l’apposito attributo simulazione='true' nel primo tag, che permette di classificare la tipologia di invio come “di prova”. In tutti i casi in cui tale attributo risulta assente l’invio sarà considerato reale.

3.2 RECUPERO CODICI

Il dispositivo (RT o Server-RT), a seguito della chiamata al servizio “rilascio codici”, ottiene in risposta un file xml conforme al tracciato “Allegato-Tipi Dati Esito Rilascio Codici_ver1.0”.

Di seguito vengono descritti i passi che deve fare il dispositivo al fine di recuperare le informazioni e memorizzarle nel rispetto dei vincoli precedentemente indicati, tenendo conto della cifratura e della chiave CEK inviata.

Il dispositivo in sequenza, utilizzando gli algoritmi e i parametri già descritti nel capitolo 2, deve:

1. recuperare sia la chiave CEK, cifrata e convertita in base64 insieme ai vettori d’inizializzazione IV sia il corrispondente set informativo di sicurezza;

2. effettuare la decodifica dalla rappresentazione in base64 e poi decifrare la chiave CEK, utilizzando la chiave privata del certificato “dispositivo”;

3. memorizzare opportunamente la chiave CEK ed i vettori d’inizializzazione;

4. salvare il set di informazioni di sicurezza cifrato, nel rispetto dei vincoli di sicurezza precedentemente descritti nel documento.

Con tale procedura l’RT ed il Server-RT hanno memorizzato la chiave CEK ed il set di informazioni di sicurezza cifrate. Per gestire l’operazione di decodifica il dispositivo può seguire una delle due soluzioni di seguito proposte:

1. <u>codici in chiaro</u>

Per ciascuna giornata deve essere recuperato esclusivamente il set informativo corrispondente, decifrato e memorizzato in chiaro per gli utilizzi previsti nella specifica, mentre tutti gli altri codici rimangono memorizzati criptati per evitare alterazioni. L’RT ha ora tutti gli elementi che gli permettono di produrre il codice bidimensionale mentre il singolo punto cassa, mediante la nuova API dedicata, deve recuperare dal Server-RT i codici segreti in corso di validità giornaliera, cifrati dal Server-RT, e salvarli nella memoria di lavoro in chiaro.

2. <u>codici criptati</u>

Non vengono effettuate operazioni di decodifica preventiva del set informativo giornaliero, dalla rappresentazione in base64 prima e di decifratura successiva. Il set

informativo corrispondente alla giornata di riferimento deve essere recuperato e decifrato esclusivamente al momento dell'utilizzo senza mai memorizzarlo in chiaro. L'RT deve, a questo punto, eseguire le operazioni di decodifica e decifratura al momento di produrre il codice bidimensionale, mentre il singolo punto cassa, mediante la nuova API dedicata, deve recuperare dal Server-RT i codici segreti in corso di validità giornaliera e validi per la giornata successiva salvandoli cifrati dal Server-RT come descritto al paragrafo 2.3 in una qualsiasi memoria disponibile.

L'operazione per decifrare il set di informazioni di sicurezza deve riguardare esclusivamente i codici in corso di validità giornaliera, mentre tutti gli altri codici rimangono memorizzati nel punto cassa, RT o Server-RT criptati per evitare alterazioni.

Si ricorda che per decifrare i codici di sicurezza, segreto ed offuscato, è necessario utilizzare anche il vettore d'inizializzazione di 16 bytes (IV) presenti per ciascun elemento del <Blocco codici>, come descritto nel paragrafo 2.3.

Inoltre, per decifrare correttamente si deve utilizzare la chiave CEK temporanea valida esclusivamente per lo specifico set di informazioni di sicurezza che si deve trattare, dopo aver eseguito la decodifica dalla rappresentazione in base64. Infatti, una chiave CEK è valida in associazione ad una sola richiesta di codici di sicurezza e non può essere utilizzata per decodificare le informazioni di sicurezza restituite con una diversa invocazione del servizio "rilascio codici".
Come ulteriore elemento di verifica si deve utilizzare il valore del HASH inviato e verificare l'integrità delle informazioni di sicurezza, ricordando di concatenare identificativo univoco del codice segreto, codice offuscato in chiaro, codice segreto in chiaro e data validità.

3.3 ANNULLAMENTO CODICI

Per la gestione dei codici di sicurezza devono essere predisposte anche funzioni di annullamento.

In caso si verifichino episodi che possano ridurre la riservatezza dei codici di sicurezza devono essere disponibili apposite funzionalità per segnalare la criticità mettendo fine alla validità dei codici già rilasciati al dispositivo.

Per ottenere tale risultato è stato previsto un automatismo legato al cambio di stato del dispositivo. Il cambio di stato viene corredato dell'informazione relativa alla sorgente richiedente, portale o dispositivo, in modo da poter gestire eventuali comunicazioni al consumatore all'atto della partecipazione.

A seguito del cambio di stato il Sistema Corrispettivi deve interagire con il Sistema Lotteria per consentire di annullare i codici di sicurezza. Anche sul dispositivo (RT, Server-RT e Punto Cassa) il cambio di stato deve implicare l'annullamento dei codici sicurezza memorizzati.

Una volta annullati i codici di sicurezza il loro utilizzo produrrà codici bidimensionali non validi ai fini della partecipazione alla Lotteria.

4. GESTIONE CODICE BIDIMENSIONALE

La lotteria istantanea prevede che l'acquirente partecipi utilizzando il Codice Bidimensionale presente sul documento commerciale di acquisto. Tutti i documenti commerciali di importo pari o superiore ad 1 euro e pagati interamente in modalità elettronica devono riportare un codice bidimensionale comprensivo di tutte le informazioni necessarie alla partecipazione. Inoltre, la partecipazione alla lotteria istantanea è consentita entro un intervallo temporale prestabilito rispetto all'emissione dello scontrino.

Affinché la verifica dell'intervallo di partecipazione, come stabilito dal provvedimento interdirettoriale, non risenta del disallineamento delle date sui dispositivi sia gli RT sia i singoli punti cassa collegati ai Server-RT, devono mantenere l'orario sempre aggiornato. Il sistema dei corrispettivi mette a disposizione un servizio di allineamento timing per la sincronizzazione delle date impostate localmente sui dispositivi RT, punti cassa e Server-RT. Questi ultimi devono propagare l'aggiornamento ai loro punti cassa.
I Codici Bidimensionali prodotti dal singolo dispositivo devono garantire la sicurezza delle informazioni, che vengono verificare dal sistema lotteria.
Gli aspetti sottoposti a verifica riguardano:

- la compatibilità dello stato del dispositivo nel sistema dei corrispettivi rispetto alla data del documento commerciale;
- la validità dei codici segreti in relazione alla giornata in cui viene emesso il documento commerciale;
- la validità dei codici segreti in relazione al dispositivo che ha emesso il documento commerciale;
- la validità dei codici segreti rispetto ad eventuali annullamenti, effettuabili dall'esercente mediante apposita funzionalità ovvero bloccati da un cambio di stato eseguito sul dispositivo.

4.1 INFORMAZIONI E STRUTTURA

Il CB deve contenere le informazioni che consentono all'acquirente la partecipazione alla lotteria istantanea. In particolare, i dati necessari sono i seguenti:

- Identificativo della versione dati, per gestire eventuali evoluzioni della struttura informativa rispetto all'attuale CB (2 caratteri);
- Partita iva dell'esercente (11 caratteri);
- Matricola del dispositivo, come censito nel sistema Corrispettivi (11 caratteri);
- Matricola cassa, presente solo nel caso di Server-RT (8 caratteri) e valorizzata con un carattere spazio nei casi di RT;
- Numero del documento commerciale: tale numero progressivo deve essere composto dalla concatenazione di due blocchi di 4 numeri ciascuno diviso dal trattino (es: 0001-0001) che indicano, rispettivamente, il n. di chiusura giornaliera prevista e il numero progressivo del documento (9 caratteri);

- Data e ora di emissione del documento commerciale: deve essere utilizzato il formato ISO 8601:2004 con la precisione seguente: YYYYMMDDTHHMM (13 caratteri);

- Ammontare complessivo del documento commerciale: espresso in formato decimale. I decimali saranno di due cifre e si utilizzerà il punto come separatore (max 11 caratteri). Si precisa che l'ammontare complessivo deve coincidere con l'importo pagato elettronicamente;

- Codice lotteria (8 caratteri): tale informazione sarà presente solamente nei casi in cui il soggetto ha scelto di partecipare anche alla lotteria degli scontrini differita, comunicandolo all'esercente. In tutti gli altri casi il campo deve essere valorizzato con un carattere spazio e l'informazione sarà aggiunta dall'APP per consentire la partecipazione alla lotteria;

- Identificativo univoco del codice segreto decifrato (5 caratteri): tale informazione viene restituita dal servizio "rilascio codici" ed ha validità giornaliera;

- Numero ore di differenza rispetto all'orario UTC dell'orologio sul dispositivo, RT o Server-RT (1 carattere). Valori ammessi 1 o 2.

Il contenuto informativo del CB deve essere ottenuto concatenando tali informazioni con il carattere separatore $. Le informazioni devono essere contenute complessivamente in un'unica stringa testuale ottenuta corredando ogni informazione con il carattere separatore e concatenando fra loro tutti i dati.

Di seguito due esempi dell'operazione di concatenazione che i dispositivi devono eseguire:

1. con tutti i campi valorizzati

01$01234567890$MATRICOLA11$cassa001$5005-0001$20210902T1250$948.00$ADE02020$12345$1

2. in caso di mancanza di matricola cassa e codice lotteria

01$01234567890$MATRICOLA11$ $5005-0001$20210902T1250$948.00$ $12345$1

4.2 GENERAZIONE E CIFRATURA

Gli elementi informativi precedentemente elencati oltre ad essere opportunamente strutturati devono essere anche arricchiti degli elementi di sicurezza prima di poter generare il CB.

In particolare, i dispositivi devono prevedere un secondo elemento nel tracciato del CB per contenere il valore della "Signature" ottenuta applicando l'algoritmo di HMAC, con i parametri descritti al cap. 2.2, alla stringa informativa descritta nel paragrafo precedente. A tale scopo devono essere utilizzati i due codici decifrati (segreto e offuscato) esclusivamente per l'operazione di cifratura e non devono essere inseriti come dati in chiaro nel tracciato del CB. Infine, i due elementi generati dal dispositivo, quello informativo e quello di sicurezza, devono essere concatenati mediante l'introduzione del carattere separatore *.

Di seguito viene schematizzato il processo che il dispositivo preposto alla produzione del CB deve eseguire. Il processo può essere suddiviso in due parti, per la generazione del contenuto informativo del CB necessario per la partecipazione alla Lotteria Istantanea e per la sicurezza.

Al fine di generare il contenuto informativo si deve:

1. recuperare le informazioni accessorie (Identificativo della versione, Numero ore da UTC);

2. recuperare le informazioni inerenti il dispositivo (Partita IVA, Matricola, Matricola Cassa);

3. recuperare le informazioni relative al documento commerciale (Numero, Data, Ammontare, Codice lotteria);

4. recuperare le informazioni di sicurezza decifrate (identificativo univoco del codice segreto);

5. concatenare le informazioni indicate nei quattro punti precedenti, prevedendo di aggiungere il carattere $ come separatore dei dati. Questa stringa ottenuta è il contenuto informativo del CB necessario per la partecipazione alla Lotteria Istantanea.

Per aggiungere gli elementi di sicurezza bisogna:

6. concatenare alla stringa del contenuto informativo del CB, ottenuta nel punto 5 del flusso precedente, il codice offuscato giornaliero decifrato, corrispondente all'identificativo univoco del codice segreto utilizzato al precedente punto 4;

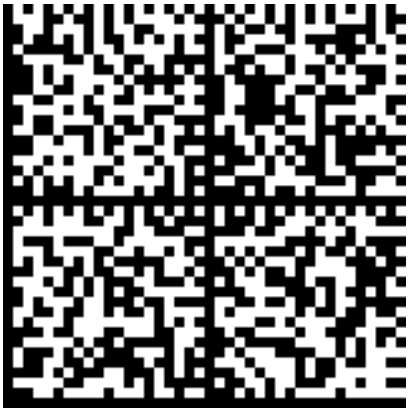
7. cifrare la stringa al precedente punto 6 Per ottenere tale elemento di cifratura del CB viene applicato l'algoritmo HMAC utilizzando come chiave dell'algoritmo il codice segreto giornaliero decifrato corrispondente all'identificativo univoco del codice segreto indicato al precedente punto 4;

8. concatenare la stringa del contenuto informativo del CB con il corrispondente elemento di cifratura appena ottenuto mediante il carattere separatore *.

Quest'ultima sequenza di caratteri, contenuto informativo insieme agli elementi di sicurezza, deve essere letta dal generatore di codice bidimensionale da inserire nel documento commerciale.

Le immagini seguenti mostrano un esempio dell'intera struttura da cui si deve generare il codice bidimensionale:

01$01234567890$MATRICOLA11$cassa001$5005-5001$20210902T1250$948.00$ADE02020$12345$1***1ee5804f28de8c6d979d0701e47f57e339c92a3b0c3ffed4ddde7982398ed8dd***

DATA MATRIX	QR CODE
	

La generazione del CB dovrà rispettare opportuni vincoli dimensionali per essere inserito sul documento commerciale che il generico dispositivo produce.

5. GESTIONE RESI ED ANNULLI

Per poter effettuare i controlli sulla validità dei documenti commerciali che partecipano alla lotteria istantanea è necessario avere a disposizione anche i dati di tutti i documenti commerciali relativi alle operazioni di reso ed annullo inerenti documenti commerciali madre contenenti il codice bidimensionale.

Verrà utilizzato l'attuale flusso dati del Sistema Lotteria degli scontrini differita in quanto già gestisce la trasmissione dei dati dei soli documenti commerciali di reso ed annullo.

Il tracciato XML ed il servizio esposto sono i medesimi già utilizzati in ambito lotteria degli scontrini differita con l'accortezza di inserire il codice lotteria dello scontrino originario dove presente perché comunicato dal consumatore ed utilizzare il codice fittizio "AAAAAAAA" negli altri casi.

In questo modo il Sistema Lotteria istantanea, colloquiando con il Sistema Lotteria degli scontrini differita, dispone della totalità dei documenti di reso ed annullo relativi a documenti commerciali originari di importo pari o superiore ad 1 euro e pagati interamente in modalità elettronica.

Di seguito viene riportato un esempio:

```
<DocumentoCommerciale>
<IdCliente>AAAAAAAA</IdCliente>
<DataOra>2022-02-16T11:00:00</DataOra>
<NumeroProgressivo>0001-0013</NumeroProgressivo>
<Ammontare>111.11</Ammontare>
<ResoAnnullo>
    <Tipologia>A</Tipologia>
    <DataOra>2022-02-10T11:01:00</DataOra>
    <Progressivo>5002-5005</Progressivo>
    <Dispositivo>
        <MatrTrasm>RT000000001</MatrTrasm>
        <MatrCassa>cassa01</MatrCassa>
    </Dispositivo>
</ResoAnnullo>
</DocumentoCommerciale>
```

Le restanti regole già esistenti per il sistema lotteria degli scontrini differita rimangono valide e invariate.

6. ALLEGATI TECNICI

Si riportano di seguito i documenti tecnici allegati alla presente specifica:

- l'interfaccia del servizio *rilascio codici* è riportata nell'allegato "*Allegato – Api Rest Lotteria Istantanea*" ed è richiamabile dai dispositivi esposti verso Agenzia delle entrate con l'indirizzo https://apid-ivaservizi.agenziaentrate.gov.it/v1/dispositivi/;

- il dettaglio della lista dei codici di risposta a copertura delle diverse casistiche del sistema viene rappresentato nel documento "*Allegato - Code List_lotteria istantanea_ver1.0*";

- lo schema dati di input al servizio è descritto nel documento *"Allegato - Tipi Dati Rilascio Codici_ver1.0"*;

- lo schema dati di output al servizio è descritto nel documento "*Allegato - Tipi Dati Esito Rilascio Codici_ver1.0*".