Divisione Risorse
Direzione Centrale Tecnologie e Innovazione
Ufficio Sistemi Trasversali

Chiarimenti e precisazioni in merito alla lotteria degli scontrini istantanea.

LAYOUT DEL DOCUMENTO COMMERCIALE

- Il layout del documento commerciale prevede il posizionamento del Codice Bidimensionale prima della matricola;
- l'ultima informazione da stampare è l'appendice dei pagamenti e le informazioni accessorie.

STAMPA CODICE BIDIMENSIONALE

In tutte le situazioni in cui il dispositivo è in grado di stampare un Documento Commerciale valido ed è in possesso di codici lotteria validi per quella determinata data, il dispositivo deve consentire anche la stampa del Codice Bidimensionale.

REPORT INFORMATIVI E RISTAMPE

- Un documento commerciale (e relativo Codice Bidimensionale) può essere ristampato sia come ristampa dell'ultimo scontrino che nel rendiconto della memoria di dettaglio, con mantenimento dello stesso Codice Bidimensionale del documento originale;
- è possibile avere una funzionalità attraverso la quale produrre un report informativo che consente di verificare lo stato del dispositivo in termini di codici disponibili e utilizzabili ai fini della produzione dei Codici Bidimensionali; dal report non devono essere in nessun modo visibili i codici di sicurezza;
- è possibile stampare un report degli esiti relativo al servizio "Rilascio codici".

SALVATAGGIO CODICE BIDIMENSIONALE

Il Codice Bidimensionale, insieme al documento commerciale, va salvato nella memoria permanente di dettaglio.

MEMORIZZAZIONE CODICE SEGRETO, OFFUSCATO E CEK

- Come previsto nelle specifiche tecniche par. 2.4 ("Sicurezza nella memorizzazione delle informazioni"), i codici di sicurezza devono essere salvati nelle memorie disponibili sul RT diversa dalla memoria di lavoro. Le memorie disponibili sono di differenti tipologie: "memoria non alterabile" e "memoria non riscrivibile", entrambe devono consentire la memorizzazione dei codici di sicurezza in modalità "append" ed eventuali cancellazioni devono essere di tipo logico;

- è possibile salvare l'intero file xml nella memoria DGFE. In tal caso la chiave CEK va mantenuta in chiaro se memorizzata nella memoria di lavoro e non nelle memorie permanenti.

CODICI INVIATI AI PUNTI CASSA

Il software dei Punti Cassa, a fronte dei codici segreti in corso di validità giornaliera e validi per la giornata successiva restituiti dall'API richiamata dalla cassa, scarica i codici criptati, li salva e decifra solo quelli per l'uso giornaliero salvandoli in chiaro, mentre gli altri restano criptati fino al giorno di utilizzo.

MESSAGGIO GIUSTIFICATIVO SU DOCUMENTI COMMERCIALI SENZA CODICE BIDIMENSIONALE

Nei casi in cui il documento commerciale viene prodotto senza Codice Bidimensionale (perché il Punto Cassa è impossibilitato a chiamare il Server RT per il recupero del codice giornaliero oppure perché il dispositivo non dispone della coppia di chiavi valide, della chiave CEK corrispondente e dei relativi vettori di inizializzazione), NON deve essere presente alcun messaggio sul documento prodotto che giustifichi l'assenza del Codice Bidimensionale.

DATA INIZIO LOTTERIA

Come indicato nelle specifiche tecniche della Lotteria degli Scontrini ad Estrazione Istantanea (par. 3 Gestione Codici) "*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.*"
La data da impostare sui dispositivi è il 16 ottobre 2023.

RICHIESTA DI SCARICO CODICI

- Per richiedere i codici mediante il richiamo del servizio rilascio codici, il dispositivo deve risultare nello stato IN SERVIZIO (unico stato dell'RT che permette di effettuare tale operazione). Nel caso in cui l'esito della richiesta sia negativo o non vada a buon fine, il dispositivo funziona normalmente ma non sarà in grado di produrre e stampare il Codice Bidimensionale sullo scontrino;
- sarà consentita l'acquisizione dei codici sicurezza per la generazione dei Codici Bidimensionali preliminarmente alla data di avvio della lotteria istantanea.

Limite richieste codici per unità di tempo:

- è previsto un limite di 10 chiamate ogni 60 secondi come limite massimo di richieste di accesso al servizio di rilascio codici che possono essere effettuate dallo stesso dispositivo RT o Server RT.

MODALITÀ SIMULAZIONE SERVIZIO RILASCIO CODICI E MODALITÀ DEMO DISPOSITIVI

- In modalità simulazione del servizio rilascio codici, occorre utilizzare gli appositi codici segreti "fittizi" rilasciati a fronte di richiesta codici in modalità simulazione e non devono essere annullati i codici di produzione;
- in caso di utilizzo di modalità simulazione successive alla prima, quindi nell'arco di 12 giorni, il dispositivo può utilizzare i codici segreti in simulazione precedentemente scaricati;
- se il dispositivo è in modalità 'demo', il Codice Bidimensionale non deve essere stampato e non devono essere annullati i codici già recuperati.

VERIFICA ED INTEGRITÀ DEI CODICI DI SICUREZZA

Il controllo dell'integrità delle informazioni di sicurezza attraverso il campo "Hash" dei codici di sicurezza deve essere calcolato ed eseguito giornalmente ed in caso di mancata corrispondenza è necessario richiedere un nuovo set di codici.

ALLINEAMENTO TIMING

Viene reso disponibile sul sistema di accoglienza un servizio di allineamento timing per la sincronizzazione date su RT e SERVER RT (il servizio è già presente da marzo 2023 in ambiente di validazione). Il servizio è definito e descritto all'interno delle specifiche tecniche v.11, ma si precisa che per richiamarlo non è necessario aver adeguato il dispositivo alle suddette specifiche.

RESI E ANNULLI

Nei casi in cui il documento originale non contenga il codice lotteria, sul corrispondente documento di reso o annullo va riportato, come codice lotteria, il valore AAAAAAAA. Non verrà applicato nei casi in cui il reso o annullo sia di tipo POS, VR e ND.

ANNULLAMENTO CODICI SEGRETI IN RELAZIONE ALLO STATO DEL DISPOSITIVO RT

Premesso che l'annullamento dei codici segreti da parte del Sistema Lotteria avviene esclusivamente in dipendenza dello stato del dispositivo RT comunicato al sistema dei Corrispettivi dell'Agenzia delle entrate, gli unici stati di un dispositivo RT che comportano l'annullamento dei codici segreti dei quali fosse entrato precedentemente in possesso, quando il suo stato lo consentiva, sono:

- DISATTIVATO
- DISMESSO
- RICHIESTA DI RIPRISTINO

L’annullamento dei codici per gli stati indicati sopra deve essere effettuato anche sul dispositivo.
Negli stati seguenti non è previsto annullamento dei codici:

- ERRORE o CENSITO, in quanto l’RT non ha mai ricevuto alcun codice
- ATTIVATO, in quanto l’RT non ha mai ricevuto alcun codice oppure quelli ricevuti precedentemente sono già stati annullati
- FUORI SERVIZIO, in quanto l’RT genera i Codici Bidimensionali solo per i documenti fiscalmente validi
- IN SERVIZIO

ANNULLAMENTO CODICI SEGRETI IN RELAZIONE ALLO STATO DEL DISPOSITIVO SERVER RT

Premesso che l’annullamento dei codici segreti da parte del Sistema Lotteria avviene esclusivamente in dipendenza dello stato del dispositivo SERVER RT comunicato al sistema dei Corrispettivi dell’Agenzia delle entrate, gli unici stati di un dispositivo SERVER RT che comportano l’annullamento dei codici segreti, dei quali fosse entrato precedentemente in possesso quando il suo stato lo consentiva, installati sia su SERVER RT che sui PUNTI CASSA sono:

- DISATTIVATO
- DISMESSO
- RICHIESTA DI RIPRISTINO

In questi casi il SERVER RT rende inutilizzabili i codici per tutti i suoi PUNTI CASSA. Ove possibile il SERVER RT informa i PUNTI CASSA di procedere con l’annullamento dei codici trasmessi in precedenza.
Negli stati seguenti non è previsto annullamento dei codici:

- ERRORE o CENSITO, in quanto il SERVER RT non ha mai ricevuto alcun codice
- ATTIVATO, in quanto il SERVER RT non ha mai ricevuto alcun codice oppure quelli ricevuti precedentemente sono già stati annullati
- FUORI SERVIZIO, in quanto il PUNTO CASSA, se in possesso dei codici, genera i Codici Bidimensionali solo per i documenti fiscalmente validi
- IN SERVIZIO

RECUPERO CODICI SEGRETI – SPECIFICHE TECNICHE PAR. 3.2

Ad integrazione di quanto riportato al par. 3.2 delle specifiche tecniche si precisa che si deve utilizzare il valore del HASH inviato per verificare l’integrità delle informazioni di sicurezza, ricordando di concatenare identificativo univoco del codice segreto convertito dal formato intero al formato binario, data validità convertita dal formato stringa (YYYY-MM-DD) al formato binario, codice offuscato in chiaro (già in formato binario) e codice segreto in chiaro (già in formato binario).
L’ordine dei byte che deve essere “big-endian”.

Si riporta di seguito un esempio a titolo esemplificativo della procedura di concatenazione da eseguire:

- IdUnicoSegreto:
    - Valore intero: 51
    - Array di byte: [(byte) 0x33]
- Data validità:
    - Valore in stringa: 2023-02-21
    - Array di byte [(byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x33, (byte) 0x2d, (byte) 0x30, (byte) 0x32, (byte) 0x2d, (byte) 0x32, (byte) 0x31]
- Codice offuscato in chiaro già in formato binario
- Codice segreto in chiaro già in formato binario

Risultato della concatenazione degli array di byte su cui calcolare l'HASH di verifica:

[(byte) 0x33, (byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x33, (byte) 0x2d, (byte) 0x30, (byte) 0x32, (byte) 0x2d, (byte) 0x32, (byte) 0x31, …]

GENERAZIONE E CIFRATURA – SPECIFICHE TECNICHE PAR. 4.3

Ad integrazione di quanto riportato al par. 4.3 delle specifiche tecniche si riportano di seguito alcune precisazioni in riferimento ai punti 6, 7 e 8.

6. concatenare alla stringa del contenuto informativo del Codice Bidimensionale, ottenuta nel punto 5. del flusso precedente e convertita in formato binario, il codice offuscato giornaliero decifrato (già formato binario), corrispondente all'identificativo univoco del codice segreto utilizzato al precedente punto 4.;

7. cifrare il dato binario al precedente punto 6. Per ottenere tale elemento di cifratura del Codice Bidimensionale viene applicato l'algoritmo HMAC utilizzando come chiave dell'algoritmo il codice segreto giornaliero decifrato (già dato binario) corrispondente all'identificativo univoco del codice segreto indicato al precedente punto 4.;

8. convertire il risultato dell'operazione eseguita al punto 7 in una stringa in formato esadecimale; si precisa che il numero complessivo di caratteri della suddetta stringa deve essere sempre pari. Nel caso in cui il primo byte sia minore di 0x10 è necessario anteporre il carattere "0" all'esadecimale rappresentato. Per esempio, il (byte) 0x0a dovrà diventare in esadecimale "0a" e non "a".

A titolo esemplificativo, si riporta di seguito un esempio della procedura di conversione da eseguire

Contenuto informativo

String: 01$01234567890$LTERT000091$ $5005-0101$20230215T1611$948.00$ADE02020$27$1

Conversione del contenuto informativo in binario

byte[]: [(byte) 0x30, (byte) 0x31, (byte) 0x24, (byte) 0x30, (byte) 0x31, (byte) 0x32, (byte) 0x33, (byte) 0x34, (byte) 0x35, (byte) 0x36, (byte) 0x37, (byte) 0x38, (byte) 0x39, (byte) 0x30, (byte) 0x24, (byte) 0x4c, (byte) 0x54, (byte) 0x45, (byte) 0x52, (byte) 0x54, (byte) 0x30, (byte) 0x30, (byte) 0x30, (byte) 0x30, (byte) 0x39, (byte) 0x31, (byte) 0x24, (byte) 0x20, (byte) 0x24, (byte) 0x35, (byte) 0x30, (byte) 0x30, (byte) 0x35, (byte) 0x2d, (byte) 0x30, (byte) 0x31, (byte) 0x30, (byte) 0x31, (byte) 0x24, (byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x33, (byte) 0x30, (byte) 0x32, (byte) 0x31, (byte) 0x35, (byte) 0x54, (byte) 0x31, (byte) 0x36, (byte) 0x31, (byte) 0x31, (byte) 0x24, (byte) 0x39, (byte) 0x34, (byte) 0x38, (byte) 0x2e, (byte) 0x30, (byte) 0x30, (byte) 0x24, (byte) 0x41, (byte) 0x44, (byte) 0x45, (byte) 0x30, (byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x30, (byte) 0x24, (byte) 0x32, (byte) 0x37, (byte) 0x24, (byte) 0x31]

Codice offuscato binario

byte[]: [(byte) 0x8a, (byte) 0xba, (byte) 0x2b, (byte) 0xc5, (byte) 0x7a, (byte) 0x35, (byte) 0x78, (byte) 0xb7, (byte) 0x97, (byte) 0x42, (byte) 0x53, (byte) 0xe0, (byte) 0x36, (byte) 0xa5, (byte) 0x3f, (byte) 0x21, (byte) 0x79, (byte) 0xca, (byte) 0x7f, (byte) 0xd0, (byte) 0xfc, (byte) 0xbb, (byte) 0xa6, (byte) 0xd1, (byte) 0x50, (byte) 0x51, (byte) 0x79, (byte) 0xb4, (byte) 0x2d, (byte) 0x4e, (byte) 0x04, (byte) 0x86]

Concatenamento Contenuto informativo + Codice offuscato

byte[]:[(byte) 0x30, (byte) 0x31, (byte) 0x24, (byte) 0x30, (byte) 0x31, (byte) 0x32, (byte) 0x33, (byte) 0x34, (byte) 0x35, (byte) 0x36, (byte) 0x37, (byte) 0x38, (byte) 0x39, (byte) 0x30, (byte) 0x24, (byte) 0x4c, (byte) 0x54, (byte) 0x45, (byte) 0x52, (byte) 0x54, (byte) 0x30, (byte) 0x30, (byte) 0x30, (byte) 0x30, (byte) 0x39, (byte) 0x31, (byte) 0x24, (byte) 0x20, (byte) 0x24, (byte) 0x35, (byte) 0x30, (byte) 0x30, (byte) 0x35, (byte) 0x2d, (byte) 0x30, (byte) 0x31, (byte) 0x30, (byte) 0x31, (byte) 0x24, (byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x33, (byte) 0x30, (byte) 0x32, (byte) 0x31, (byte) 0x35, (byte) 0x54, (byte) 0x31, (byte) 0x36, (byte) 0x31, (byte) 0x31, (byte) 0x24, (byte) 0x39, (byte) 0x34, (byte) 0x38, (byte) 0x2e, (byte) 0x30, (byte) 0x30, (byte) 0x24, (byte) 0x41, (byte) 0x44, (byte) 0x45, (byte) 0x30, (byte) 0x32, (byte) 0x30, (byte) 0x32, (byte) 0x30, (byte) 0x24, (byte) 0x32, (byte) 0x37, (byte) 0x24, (byte) 0x31, (byte) 0x8a, (byte) 0xba, (byte) 0x2b, (byte) 0xc5, (byte) 0x7a, (byte) 0x35, (byte) 0x78, (byte) 0xb7, (byte) 0x97, (byte) 0x42, (byte) 0x53, (byte) 0xe0, (byte) 0x36, (byte) 0xa5, (byte) 0x3f, (byte) 0x21, (byte) 0x79, (byte) 0xca,

(byte) 0x7f, (byte) 0xd0, (byte) 0xfc, (byte) 0xbb, (byte) 0xa6, (byte) 0xd1, (byte) 0x50, (byte) 0x51, (byte) 0x79, (byte) 0xb4, (byte) 0x2d, (byte) 0x4e, (byte) 0x04, (byte) 0x86]

Codice Secreto binario

byte[]: [(byte) 0xff, (byte) 0x38, (byte) 0xc6, (byte) 0x09, (byte) 0x2d, (byte) 0x88, (byte) 0x85, (byte) 0xa0, (byte) 0xad, (byte) 0x81, (byte) 0xbf, (byte) 0xea, (byte) 0x9c, (byte) 0x5a, (byte) 0x19, (byte) 0x33, (byte) 0xbb, (byte) 0x70, (byte) 0xb4, (byte) 0x86, (byte) 0x36, (byte) 0x8f, (byte) 0x63, (byte) 0x6c, (byte) 0x53, (byte) 0x16, (byte) 0xc4, (byte) 0xd3, (byte) 0x6f, (byte) 0xce, (byte) 0x92, (byte) 0x40]

Risultato dell'algoritmo HMAC

byte[]: [(byte) 0x6b, (byte) 0xbc, (byte) 0xed, (byte) 0x37, (byte) 0xb5, (byte) 0xbf, (byte) 0x81, (byte) 0x96, (byte) 0x71, (byte) 0xd2, (byte) 0xc7, (byte) 0xe3, (byte) 0x48, (byte) 0xea, (byte) 0x6b, (byte) 0x0b, (byte) 0x75, (byte) 0x8e, (byte) 0x79, (byte) 0xb1, (byte) 0x3f, (byte) 0xae, (byte) 0x09, (byte) 0x53, (byte) 0x5f, (byte) 0x98, (byte) 0x96, (byte) 0xbe, (byte) 0xa8, (byte) 0xe5, (byte) 0x47, (byte) 0x44]

Convertito in una stringa esadecimale:

6bbced37b5bf819671d2c7e348ea6b0b758e79b13fae09535f9896bea8e54744

Contenuto del Codice Bidimensionale

String: 01$01234567890$LTERT000091$ $5005-0101$20230215T1611$948.00$ADE02020$27$1*6bbced37b5bf819671d2c7e348ea6b0b758e79b13fae09535f9896bea8e54744

ALLEGATO ALLE SPECIFICHE TECNICHE FILE "LOTTERIAISTANTANEAESITOTYPES_V1.1.XSD"

In riferimento al tag IdUnicoSegretoType che sostituisce l'espressione regolare come di seguito riportata:

```
<xs:restriction base="xs:integer">
        <xs:pattern value="\d{1,5}"/>
</xs:restriction>
```

il campo IdUnicoSegretoType deve essere riportato della lunghezza di 5 byte indipendentemente dalla dimensione (da 1 a 5) che si riceve nel file XML.

il campo IdUnicoSegretoType deve necessariamente riportare l'indicazione della lunghezza minima (1 byte) e massima (5 byte) poiché l'output è variabile in funzione della risposta del Sistema Lotteria per il rilascio dei codici di sicurezza e non prevede l'utilizzo del padding.

Si precisa che la nuova versione del file xsd è stata pubblicata sul sito istituzionale dell'Agenzia Entrate in data 15 giugno 2023.

DOCUMENTO COMMERCIALE DEMATERIALIZZATO

Il documento commerciale dematerializzato è il documento elettronico riportante tutti i dati fiscali del documento commerciale cartaceo come definito dall'Agenzia delle entrate.
Allo scopo di far partecipare l'acquirente alla lotteria istantanea tramite documenti commerciali dematerializzati, il dispositivo deve aggiungere a tale documento un «allegato» di tipo testuale (in formato Json) riportante il contenuto del Codice Bidimensionale per la partecipazione alla lotteria istantanea non alterando la visualizzazione del documento.
Il nome del file allegato deve essere "lotteria_istantanea.txt". Il json deve essere così strutturato:

- chiave: "ldsi_contenutocb"
- valore: contenuto del Codice Bidimensionle in forma testuale.

L'app "Gioco legale" dell'Agenzia delle Dogane e dei Monopoli sarà in grado di processare i documenti commerciali dematerializzati predisposti come indicato e firmati esclusivamente PADES, per consentire la partecipazione alla Lotteria Istantanea.
La firma deve essere applicata successivamente all'inserimento dell'allegato.
La codifica dei caratteri del file è UTF-8.
Di seguito un esempio di allegato testuale per la lotteria istantanea:
{"ldsi_contenutocb":"01$01234567890$MATRICOLA11$cassa001$5005-5001$20210902T1250$948.00$ADE02020$12345$1*1ee5804f28de8c6d979d0701e47f57e339c92a3b0c3ffed4ddde7982398ed8dd"}

Si precisa che la funzione di cui sopra è facoltativa e si applica ai soli modelli per i quali il produttore decide di semplificare la partecipazione dell'acquirente alla lotteria istantanea anche quando il documento commerciale è prodotto in formato dematerializzato.

MODALITA' SIMULAZIONE SERVIZIO DI RILASCIO CODICI SEGRETI PRIMA DELL'AVVIO DELLA LOTTERIA ISTANTANEA

A partire dalla data del 16 ottobre 2023 il servizio rilascio codici segreti potrà essere invocato per le richieste di codici segreti "fittizi" in modalità simulazione. Qualora venissero inviate delle richieste in modalità reale il servizio risponderà come previsto dalle specifiche tecniche con "HTTP 410".
Si precisa che, il servizio di rilascio codici in modalità simulazione può essere utilizzato per eventuali verifiche tecniche dei dispositivi in ambiente di produzione, mentre per le attività di test e integrazione del software deve essere utilizzato l'ambiente di validazione e collaudo.

Roma, 4 agosto 2023