SCHEDULE 2

(Regulation 21(b))

TECHNICAL GUIDELINE FOR ACCREDITED E-SDCs TABLE OF CONTENTS

1. Introduction

This Guideline is the technical guideline for implementing E-SDCs. This Guideline sets standards that will enable simple integration of accredited E-SDCs with the IRS System.

V-SDC is a web service published and maintained by the Commissioner and it represents an integral part of the IRS System. E-SDC is a device provided by an accredited supplier.

E-SDCs must comply with the protocols.

2. EFDs

2.1. Accredited POS

An accredited POS is responsible for submitting transaction data on receipts to E-SDC for fiscalisation and for printing fiscal invoices received from the SDC.

When the E-SDC is restarted, the user is required to enter the PIN code to authorise E-SDC to access the secure element.

2.2. E-SDC

High-Level Requirements are:

1. An E-SDC will sign a receipt only if the previous receipt is signed by the same digital certificate unless -
   - the last operation was local or remote audit; or
   - the E-SDC memory is empty-no receipts have been signed by this device since the beginning of an audit operation.
2. The E-SDC will submit proof of audit that will be generated by the IRS System to the secure element to reset maximum invoice amount counter to zero as soon as the E-SDC receives that piece of information as web response in case of remote audit or from a SD card in case of a local audit.
3. The E-SDC will process all commands received from the IRS System in a consecutive order. These commands might include time synchronisation, locking of the device and so forth.
4. The E-SDC does not have to keep audit data that is submitted and successfully stored on the IRS System.
5. The E-SDC encrypts audit data and stores it locally in an encrypted form.
6. The E-SDC is required to keep audit data locally until proof of audit has been received from the IRS System that the audit data has been securely stored on the IRS System.
7. The E-SDC should not store the secure element's PIN Code except in the working memory. Once the E-SDC is restarted, the cashier will be required to enter the PIN Code again.

2.3. Fiscalisation of Normal Receipt Processes are:

1. the accredited POS generates a receipt;
2. the accredited POS sends the receipt and journal template to E-SDC;
3. the E-SDC verifies the format of the receipt;
4. the E-SDC verifies if tax calculation is correct based on applied tax rates;
5. the E-SDC sends the receipt to the secure element for fiscalisation providing current date and time and PIN code/password for digital certificate;
6. the secure element verifies if all amounts are positive numbers;
7. the secure element calculates internal data and encrypts it with the IRS System public key;
8. the secure element signs the receipt;
9. the E-SDC produces a journal file;
10. the E-SDC stores the receipt with signature and journal in one package, generates one-time key and encrypts a package using symmetric algorithm. The E-SDC encrypts one-time symmetric key using the IRS System public key and adds it to the package so that the IRS System can decrypt symmetric key and access package content once it arrives on the IRS System.

2.4. Dump Audit Data Kept on E-SDC when Secure Element is Damaged

If the secure element is damaged and data cannot be restored from the card, but the E-SDC is operational, IRS will be able to dump data from E-SDC device and upload audit data using the same application used to upload audit data submitted by a taxpayer.

2.5. E-SDC Process Commands Sent from IRS Systems Commands are means of communication between the IRS System and occasionally connected E-SDC. Commands are stacked in the queue list on the server for specific E-SDC and submitted to the E-SDC as part of the response once it reports to the IRS System using remote or local audit.

Time server URL	E-SDC will update URL of the time server used to keep local clock in sync
Tax rates	E-SDC will update tax rates and check new invoices against updated tax rates from effective date
Print message	E-SDC will print this message(s) in consecutive order next time accredited POS contacts E-SDC device
Proof of audit	Proof of audit is transmitted to the secure element to unlock signing or to update maximum allowed sum of fiscal invoice amounts counter
Lock device	Send command to secure element
Unlock device	Send command to secure element
Current state of secure element	Returns current internal data of the fiscal card to the IRS System, plus E-SDC date and time. Executes and returns data to IRS System immediately

Update maximum allowed sum of fiscal invoice amounts	Updates maximum sum of fiscal invoice amounts allowed for the particular secure element - used to limit total number of fiscal invoices issued between two audits

2.5.1. Synchronisation of E-SDC Clock Online

The E-SDC will check the time server specified in configuration and keep internal clock in sync.

2.5.2. Lock/Unlock Card

1. Lock/Unlock command is issued by the IRS System in case the COMMISSIONER suspects that illegal activities are carried out by the taxpayer or in case the secure element has to be disabled due to the outstanding debt to supplier.
2. Content of command is verified by the secure element and the state is changed accordingly.
3. If the secure element is locked, no new receipts of any type may be signed by the secure element.

2.5.3. Update Maximum Allowed Sum of Fiscal Invoice Amounts

1. Maximum allowed sum of fiscal invoice amounts limit is set by the IRS System on the secure element during personalisation for a particular taxpayer or during exploitation if for any reason that limit has to be increased or decreased by IRS.
2. Content of command is verified by the secure element and the limit is changed to the new value. Once new value is applied,

all new fiscal invoices are verified against the new limit. Changing this value on the fly has the same technical implications.

2.5.4. Apply New Tax Rates

The E-SDC has to prevent fiscalisation of receipts with invalid tax rates.

The E-SDC will keep current and all new tax rates (with effective dates) in memory.

2.6. E-SDC

This paragraph describes specifics of an E-SDC.

An E-SDC can work in the following modes:

2.6.1 Offline

In the offline mode, the secure element signs a receipt and the E-SDC device stores it locally in a secure manner.

2.6.2 Semi-offline

In the semi-offline mode, the secure element signs a receipt and the E-SDC device will immediately try to contact the IRS System and perform remote audit. If the IRS System is not accessible, the E-SDC will switch to offline mode.

2.7. Authentication

Authentication against the IRS System is performed using taxpayer digital certificate.

3. Digital Certificates

3.1. IRS System Issues Secure Element to Taxpayer

1. A taxpayer's digital certificate is stored on the secure element.
2. The secure element is stored on the smart card.
3. The PIN or Password is generated and printed on PIN mailer.
4. The secure element and PIN code are securely delivered to taxpayer.

4. **Test Digital Certificates**

4.1. Acquisition of Test Digital Certificate

IRS will issue the required number of test digital certificates to each accredited supplier and each accredited taxpayer.

5. **Fiscal Invoices**

5.1. Unique Identification of Fiscal Invoice

A fiscal invoice is uniquely identified with the combination of the receipt ordinal number and the secure element identification number.

5.2. Elements

This paragraph defines the minimum set of attributes required to produce a fiscal invoice.

A fiscal invoice may contain additional data as required by a specific industry.

1. A fiscal invoice consists of two parts produced by an accredited POS and associated secure element.
2. An accredited POS submits the information specified in regulation *12(2)(a), (b), (c), (d), (e), (J), (g), (Commissioner), (i)* and *(j)* to the V-SDC or E-SDC.
3. The V-SDC or E-SDC returns the response data to the POS which contains the additional information specified in regulation *12(2)(k), (l), (m), (n)* and *(o).*

5.3. Signature

Fiscalisation of a receipt is a process of applying digital signature by the secure element on the electronic content of the receipt.

5.4. Internal Data

Internal data contains fiscal data in encrypted form. Content of internal data is readable by IRS only.

5.5. QR Code

QR code contains URL of verification service used to verify the authenticity of the fiscal invoice for customer convenience.

6. Audits

Audit data represents machine readable formatted fiscal invoice signed by a taxpayer's private key followed by journal data—textual representation of a fiscal invoice generated by an E-SDC.

Content of audit data is kept in encrypted form that makes sure no changes have been made and that no one was able to access its content after creation except the Commissioner (and the IRS System) after successful audit.

Each package of audit data has associated metadata - ordinal number of package. It is used to track order and make sure audit data is submitted in the consecutive order.

6.1. Encryption of Audit Data

Encryption of audit data prevents access to sales data by unauthorised persons and enables addition of fiscal lottery to the IRS System in the future. The only one who can decrypt audit data is the IRS System software running on IRS premises and by the Commissioner only.

6.2. Proof of Audit

Proof of audit is generated by the IRS System once audit data has been received and securely stored on the IRS System.

Minimum information contained in proof of audit must ensure that proof of audit can be used only by the secure element which signed receipts that are contained in the audit data received by the IRS System.

6.3. Audit Process

An audit is a process of sequential transfer of audit data from an E-SDC to the IRS System and handling the response generated by the IRS System for the specific device.

There are three specific scenarios: remote audit, local audit initiated by a taxpayer and local audit initiated by IRS. Basic rules and processes described in this paragraph apply to all scenarios.

An audit is always a synchronous process. Depending on the amount of data and means of communication, it can take from less than a second to a couple of hours or even days to complete.

6.4. SD Card or USB Flash Memory Stick

SD cards or USB memory stick are used as transport mechanism instead of internet connection in cases of local audits initiated by a taxpayer or by IRS. In any case, the carrier has to be empty for an E-SDC to initiate dumping of audit data.

Once the E-SDC receives audit data (signed receipt and journal) from the secure element, it is encrypted and stored in the permanent memory (hard drive, flash or internal SD card).

An E-SDC device is fully functional during audit. The taxpayer must be able to sign new receipts as long as the secure element permits. There is a mechanism in place that is responsible for continuous operation of the secure element and E-SDC while audit data is on its way to the IRS System.

Depending on the connection availability audit may be triggered by the arrival of a signed receipt from the secure element or insertion of an

external memory device into the E-SDC. No matter which event triggered the audit, the following conversation will take place between the E-SDC, the IRS System and the secure element:

1. the E-SDC signals the beginning of the audit to the secure element;
2. the secure element returns token to the E-SDC;
3. the E-SDC starts sending (by HTTPS) or dumping on external memory (SD card, USB flash) audit data starting with the oldest unaudited package in piecemeal fashion. A token is sent to the IRS System using the same communication channel;
4. the IRS System receives audit data, decrypts packages and does a basic verification;
5. if verification is successful, the IRS System will generate proof of audit and return it using the same transport channel;
6. the E-SDC receives proof of audit and passes it to secure the element;
7. the secure element verifies if proof of audit is signed by the IRS System private key, which ensures that audit data has been successfully received by the IRS System;
8. if proof of audit is valid, the secure element will conclude audit process;
9. the E-SDC stores proof of audit in its long-term memory. Consequently -

   (i) **audit data created before beginning of audit** is considered safe for deleting because it has been received by the IRS System;

   (ii) **audit data created after beginning of audit** is considered unaudited and E-SDC is responsible to preserve this

audit data unit which is submitted to the IRS System in the next audit;

(iii) **audit data created after end of audit** is considered unaudited and E-SDC is responsible to preserve this audit data unit which is submitted to the IRS System in the next audit.

6.5 Remote Audit

Remote audit is the process of transferring data to the IRS System using internet connection. It is the most common way to perform audit for any occasionally connected device.

An E-SDC checks if the IRS System is online. If it is online, the E-SDC authenticates the IRS System by using server-side certificate installed on the API endpoint, enabling HTTPS protocol. The IRS System authenticates the E-SDC using digital certificate issued on the secure element. The E-SDC starts sending audit data in small chunks, performing a series of audits until no more unaudited data is stored on its long-term memory.

Not all E-SDC devices are required to perform remote audit. In cases where the network connection is not available due to the interruption of the service or missing GPRS modem or network card, the E-SDC will still be able to perform Local Audit.

6.6. Local Audit Initiated by Taxpayer

Local audit initiated by a taxpayer is a common scenario for devices that lack ability to connect to internet due to the technical limitations of the devices or limited infrastructure.

An audit is initiated by attaching an empty SD card or USB Flash to E-SDC device. An E-SDC

will verify if media is empty. If not, the E-SDC will signal error to the user.

6.7. Submitting Data in IRS Office

The Commissioner can upload data using specific application that will store deleted audit data from media and save proof of audit generated by the IRS System to media once audit data has been received.

6.8. Submitting Data Using Web Application

Anyone should be able to upload limited amount of audit data (for example, up to 30Mb) using web site. The IRS System will verify received audit data and generate proof of audit as a response. A user will be required to manually delete audit data from media and save received proof of audit for later use.

6.9. Completing Audit in Progress

A taxpayer inserts media with proof of audit file on it. An E-SDC loads proof of audit and verifies if the format is valid. If the format is valid, proof of audit is sent to the secure element for processing.

If the format is invalid or the E-SDC and the secure element cannot process proof of audit for any reason, the E-SDC signals error message to the operator.

6.10. Local Audit Initiated by IRS

Local Audit initiated by the Commissioner is required when the taxpayer is not reporting transactions for any reason. If an E-SDC and the secure element are operational, the Commissioner will dump data using the same scenario as the taxpayer.