EXTRAORDINARY

GOVERNMENT OF FIJI GAZETTE SUPPLEMENT

No. 19 THURSDAY, 1st JUNE 2017

[LEGAL NOTICE NO. 37]

TAX ADMINISTRATION ACT 2009

Tax Administration (Electronic Fiscal Device) Regulations 2017

TABLE OF PROVISIONS

PART 1—PRELIMINARY

PART 2—ELECTRONIC SYSTEM

Division 1—Establishment and description of electronic system

Division 2—Operational components of electronic system

PART 3—ROLES, RESPONSIBILITIES AND CONDUCT

PART 4—MISCELLANEOUS

Division 1—Guidelines and protocols

IN exercise of the powers conferred upon me under section 118A(2) of the Tax Administration Act 2009, I hereby make these Regulations—

PART 1—PRELIMINARY

Short title and commencement

1.—(1) These Regulations may be cited as the Tax Administration (Electronic Fiscal Device) Regulations 2017.

(2) These Regulations come into force on 1 June 2017.

Interpretation

2.—(1) In these Regulations, unless the context otherwise requires—

"accredited", in relation to a POS or E-SDC, means accredited by the CEO under regulation 8 or 9;

"application" means an application that is in a form approved by the CEO;

"audits and investigations" means audits and investigations under section 37 of the Act;

"Authority" means the Fiji Revenue and Customs Authority established under section 3 of the Fiji Revenue and Customs Authority Act 1998;

"Authority's system" means the electronic information system that the Authority must operate under regulation 6(1);

"be part of a fiscal invoice" means recorded on the fiscal invoice and payable as part of the total amount payable specified on the fiscal invoice;

"business" means a business supplying goods and services that is operated by a taxpayer;

"cashier" means a person who, as part of his or her employment, operates a POS for a business;

"company" means a company registered under the Companies Act 2015;

"customer" means a person to whom, or to which, a business supplies goods and services;

"customer compliance award program" means a customer compliance award programme conducted under regulation 26;

"digital certificate" means a unique electronic document issued by the CEO for each EFD that—

(a) authenticates the EFD when it links with the Authority's system; and

(b) contains public and private key for creating, producing and verifying the digital signature of the EFD;

"digital signature" means an encrypted digital code that—

(a) is created by an SDC using private key;

(b) is recorded on each fiscal invoice by the SDC;

(c) identifies the taxpayer; and

(d) verifies the integrity of the SDC when it transmits fiscal data to the Authority's system;

"electronic fiscal device" or "EFD" means a system, composed of one SDC and at least one POS connected together, that—

(a) receives, records, analyses and stores fiscal data;

(b) formats fiscal data into fiscal invoices;

(c) has a secure element which transmits the fiscal data to the Authority's system; and

(d) produces fiscal invoices and issues them to a customer;

"external SDC" or "E-SDC" means a SDC that is hardware set up as a separate component of the EFD used by a taxpayer;

"fiscal data" means the transaction data that the Authority requires for calculating and imposing a tax;

"fiscal invoice" means a receipt that—

(a) is issued from an EFD to acknowledge that a transaction has occurred between a business and a customer; and

(b) has printed on it the fiscal data and other information relating to the transaction specified in regulation 12(2);

"FRCA employee" means a person appointed by the Authority under section 26 of the Fiji Revenue and Customs Authority Act 1998 for the purpose of carrying out its functions and duties;

“Guideline set out in a Schedule” means a guideline specified in regulation 20;

“issue”, in relation to a fiscal invoice, means to make available for a customer to receive and retain;

“POS” means a point of sale invoicing device or software which is an electronic device or software application that is—

(a) used by a business for management control in the areas of sales analysis and stock control; and

(b) a component of the business’s EFD—

(i) into which a cashier enters the transaction data for each transaction made by the business; and

(ii) from which a fiscal invoice for the transaction is issued;

“protocol” means a protocol made available to the public by the CEO under regulation 21(2);

“receipt” means a receipt or invoice;

“SDC” means a sales data controller which is the component of an EFD that—

(a) receives transaction data from a POS component of the EFD;

(b) analyses the transaction data into fiscal data;

(c) formats the fiscal data as a fiscal invoice, creates the digital signature for the EFD and records the digital signature on the fiscal invoice;

(d) transmits the fiscal invoice to the POS;

(e) preserves the transaction data and fiscal data in an irrevocable and secure manner; and

(f) transmits the fiscal data to the Authority’s system;

“secure element” means the software and hardware used by an EFD and the Authority to prevent tampering and unauthorised use of fiscal data transmitted to the Authority’s system and to maintain the integrity of the fiscal data;

“supplier” means a person who supplies an EFD or a component of an EFD to a taxpayer;

“supply” means—

(a) supply within the meaning of the Sale of Goods Act 1979; or

(b) providing services under an agreement for installing, implementing, servicing or maintaining an EFD or a component of an EFD;

“tax” means—

(a) the tax as defined in section 2 of the Value Added Tax Act 1991;

(b) the Service Turnover Tax as defined in section 2 of the Service Turnover Tax Act 2012;

(c) the Environmental Levy as defined in section 2 of the Environmental Levy Act 2015; or

(d) any other tax that is specified by the CEO by notice in the Gazette to be part of a fiscal invoice;

"taxpayer" means—

(a) a taxpayer as defined in section 2 of the Value Added Tax Act 1991;

(b) an accountable person as defined in section 2 of the Service Turnover Tax Act 2012;

(c) an accountable person as defined in section 2 of the Environmental Levy Act 2015; or

(d) any other person who is required by a tax law to issue a receipt;

"transaction" means a transaction between the business of a taxpayer and a customer by which—

(a) the business supplies goods or services to the customer and the customer pays the price for the supply of the goods and services to the business; or

(b) the business pays the customer a refund of the whole or a part of the price the customer has paid for goods or services previously supplied by the business to the customer;

"transaction data" means the data relating to a transaction entered into a POS by a cashier; and

"V-SDC" means a virtual SDC that is software attached to the Authority's system.

(2) In these Regulations, words and phrases have the same meaning as under the Act unless the context otherwise requires.

(3) A reference in these Regulations to the supply of goods and services is a reference to a supply of goods and services that is charged with a tax.

(4) A reference to—

(a) a Schedule is a reference to a Schedule to these Regulations; and

(b) a Schedule by number is a reference to a Schedule so numbered.

Objective

3. The objective of these Regulations is to implement an electronic system that enables the Authority to securely obtain, monitor and assess accurate fiscal data for calculating and imposing a tax that is required to be part of a fiscal invoice.

PART 2—ELECTRONIC SYSTEM

Division 1—Establishment and description of electronic system

Establishment of electronic system

4.—(1) There is an electronic system that transmits, receives, records, analyses, formats, stores and monitors fiscal data.

(2) The electronic system is composed of—

(a) the Authority's system; and

(b) the EFDs used by taxpayers in operating their businesses.

(3) The function of the electronic system is to obtain and monitor accurate data to create a database for assessing, calculating and imposing liability for a tax.

Description of operations of electronic system

5. The following are the operational components of the electronic system—

(a) an electronic information system operated by the Authority that receives, verifies, records, analyses, stores and transmits fiscal data;

(b) EFDs operated by taxpayers for their businesses that connect and communicate electronically to the Authority's system using a secure encryption protocol and mutual authentication;

(c) POSes that transmit transaction data for every transaction to SDCs, receive fiscal invoices for every transaction from SDCs and issue the fiscal invoices;

(d) SDCs that receive transaction data from POSes, instantly format that data into fiscal data and fiscal invoices, transmit the fiscal data to the Authority's system and transmit the fiscal invoices to POSes;

(e) the Authority's system authenticates the SDCs transmitting fiscal data to it and receives, stores, analyses and verifies the fiscal data;

(f) security features for the hardware and software of the Authority's system and the EFDs securely maintain the privacy and integrity of the fiscal data using secure encryption protocols, digital certificates and mutual authentication mechanisms for receiving, verifying, recording, analysing, storing and transmitting fiscal data;

(g) a software feature in the Authority's system enables taxpayers and customers to access fiscal data stored on the Authority's system to verify the following in relation to either a single transaction or more than one transaction—

(i) that the Authority's system has received fiscal data transmitted to it;

(ii) the accuracy of fiscal data stored on the Authority's system.

Division 2—Operational components of electronic system

Authority to operate an electronic information system

6.—(1) The Authority must operate an electronic information system that has hardware and software that—

(a) connects electronically with each taxpayer's EFD;

(b) authenticates each SDC that transmits fiscal data to the system;

(c) receives, records, analyses and stores fiscal data transmitted by an SDC;

(d) securely maintains the privacy and integrity of the secure elements, digital certificates, digital signatures and the fiscal data it receives, analyses, stores and transmits;

(e) manages the secure elements, digital certificates and digital signatures;

(f) manages an auditing process for monitoring and supervising EFDs and fiscal data;

(g) provides accurate data to the Authority for assessing the taxes payable by taxpayers; and

(h) enables taxpayers and customers to access fiscal data stored on the Authority's system to verify the following in relation to either a single transaction or more than one transaction—

(i) that the Authority's system has received fiscal data transmitted to it;

(ii) the accuracy of fiscal data stored on the Authority's system.

(2) The operations of the Authority's system must comply with the Guidelines set out in the Schedules.

Electronic fiscal devices

7.—(1) A taxpayer must operate an EFD for each business of the taxpayer.

(2) An EFD must comply with the following—

(a) the components of the EFD are one or more POSes and one SDC (which may be an E-SDC or V-SDC);

(b) each POS and E-SDC are accredited;

(c) each POS transmits to the SDC a receipt, on which is recorded the transaction data specified in regulation 12(2), for each transaction of the business;

(d) the SDC receives the transaction data, analyses the data and calculates taxes to produce fiscal data for the transaction, and puts the digital signature on the receipt;

(e) there is a digital certificate that authenticates the EFD and enables the SDC to transmit the fiscal data to the Authority's system;

(f) the SDC transmits the fiscal data to the Authority's system and the Authority's system verifies the fiscal data and transmits it back to the SDC;

(g) the SDC formats a fiscal invoice for the transaction, records the digital signature on the fiscal invoice and transmits the fiscal invoice to the POS;

(h) a fiscal invoice is produced for each transaction.

(3) The operations of the EFD must comply with the Guidelines set out in the Schedules.

Accreditation of POSes and E-SDCs—applications by suppliers

8.—(1) A supplier, who wants to supply to a taxpayer a POS or E-SDC of a particular brand, model and specification that is not an accredited POS or E-SDC, must apply to the CEO for accreditation of the POS or E-SDC of that brand, model and specification.

(2) On receiving the application, the CEO must take steps to determine whether to accredit the brand, model and specification of the POS or E-SDC. In doing so, the CEO must comply with the processes set out in the Guideline set out in Schedule 3.

(3) During the accreditation process, the supplier must provide the CEO with access to information and equipment, and any other assistance, the CEO reasonably requires for carrying out the process.

(4) After completing the accreditation process, the CEO—

(a) accredits, or refuses to accredit, the brand, model and specification of a POS or E-SDC in accordance with the Guideline set out in Schedule 3; and

(b) must, without delay—

(i) give notice in writing to the supplier of the CEO's decision to accredit or refuse to accredit; and

(ii) give to the supplier a copy of the accreditation report produced under paragraph 4 of the Guideline.

(5) The CEO must, without delay after accrediting a POS or E-SDC under this regulation, publish the details of the brand, model and specification of the POS or E-SDC, and the date it is accredited, on the Authority's website.

(6) The accreditation of a POS or E-SDC under this regulation does not have effect unless the details of the brand, model and specification of the POS or E-SDC, and the date of its accreditation, are specified on the Authority's website.

Accreditation of POSes and E-SDCs—applications by taxpayers

9.—(1) A taxpayer, who wants to develop, install and implement an EFD for a business of the taxpayer, must, before implementing the EFD, apply to the CEO for accreditation of each POS and E-SDC of the EFD.

(2) On receiving the application, the CEO must take steps to determine whether to accredit each POS and E-SDC of the taxpayer's EFD. In doing so, the CEO must comply with the processes set out in the Guideline set out in Schedule 3.

(3) During the accreditation process, the taxpayer must provide the CEO with access to information and equipment, and any other assistance, the CEO reasonably requires for carrying out the process.

(4) After completing the accreditation process, the CEO—

(a) accredits, or refuses to accredit, each POS and E-SDC of the EFD in accordance with the Guideline set out in Schedule 3; and

(b) must, without delay—

(i) given notice in writing to the taxpayer of the CEO's decision to accredit or refuse to accredit; and

(ii) give to the taxpayer a copy of the accreditation report produced under paragraph 4 of the Guideline.

(5) The accreditation of an EFD under this regulation is not effective until the taxpayer receives the CEO's notice given under subregulation (4)*(b)*(i).

Revocation of accreditation

10.—(1) The CEO may revoke the accreditation of a POS or E-SDC if the POS or E-SDC does not comply with a Guideline set out in a Schedule.

(2) If the CEO revokes the accreditation of a POS or E-SDC that was accredited under regulation 8, the CEO must, without delay—

(a) remove the details of the POS or E-SDC from the Authority's website; and

(b) give notice in writing of the revocation to the suppliers supplying the POS or E-SDC.

(3) If the CEO revokes the accreditation of a POS or E-SDC that was accredited under regulation 9, the CEO must, without delay, give notice in writing of the revocation to the taxpayer operating the EFD of which the POS or E-SDC is a component.

(4) A notice of a decision under this regulation must specify the reasons for the decision.

Digital certificates

11.—(1) There must be a digital certificate for the EFD of a taxpayer's business that does the following—

(a) reproduces the taxpayer's digital signature for recording on each fiscal invoice issued by the taxpayer to a customer;

(b) reproduces the protected password or PIN code of the taxpayer and securely delivers the password or PIN Code to the Authority's system to enable the EFD to link to the Authority's system and securely transmit the fiscal data to the Authority's system;

(c) records the date on which the data is transmitted to the Authority's system.

(2) The CEO must issue the digital certificate for an EFD.

(3) The CEO must not issue more than one digital certificate for an EFD.

Fiscal invoices

12.—(1) There must be a fiscal invoice for each transaction of a business.

(2) The fiscal invoice must specify the following particulars—

(a) the type of receipt;

(b) the type of transaction;

(c) the method of payment;

(d) the name or unique identification of the cashier;

(e) the name or unit code of each good or service supplied;

(f) the unit price and quantity of each good or service supplied;

(g) the total price of the goods or services supplied;

(h) the taxes that are a part of the invoice and the tax rates applied;

(i) the total amount payable by the customer;

(j) if the customer is a taxpayer, the customer's TIN;

(k) the name and TIN of the business, and the identification of the business premises where the transaction occurred;

(l) the date and time the receipt is issued;

(m) the sequential serial number of the receipt;

(n) the serial number of the digital certificate of the business's EFD;

(o) the digital signature of the EFD.

(3) The type of receipt referred to in subregulation (2)*(a)* must be one of the following types—

(a) a normal receipt, which is the receipt that is issued when a transaction occurs and which affects tax liability;

(b) a copy of a receipt, which is generated as a copy of a normal receipt when a transaction occurs and does not affect tax liability;

(c) a training receipt that is used for training purposes only and does not affect tax liability;

(d) a pro-forma receipt, which has the characteristics of a normal receipt, but is not proof of a transaction and does not affect tax liability.

(4) The type of transaction referred to in subregulation (2)*(b)* must be one of the following types—

(a) a supply of goods and services;

(b) a refund of a payment or part of a payment made for a previous supply of goods or services.

(5) The method of payment referred to in subregulation (2)*(c)* includes, and is not limited to, payment by cash, credit or debit card, cheque, voucher, promissory note, direct debit transfer and wire transfer.

(6) A training or pro-forma receipt referred to in subregulation (3)*(c)* or *(d)* must be clearly distinguishable from a normal receipt by recording on the receipt—

(a) "TRAINING" or "PRO-FORMA", as the case requires, below the receipt header and above the item description section; and

(b) "THIS IS NOT A FISCAL INVOICE" below the total amount payable.

(7) The text referred to in subregulation (6) must be—

(a) recorded on the receipt in such a manner so that it may not be altered or erased; and

(b) in a font size that is at least twice the size of the text on the receipt that specifies the total amount payable.

PART 3—ROLES, RESPONSIBILITIES AND CONDUCT

Role and responsibilities of CEO

13.—(1) The CEO is responsible for the administration of these Regulations.

(2) In administering these Regulations, the CEO is responsible for—

(a) operating the Authority's system in a manner that complies with these Regulations;

(b) receiving appropriate advice on technical matters relating to electronic information systems, electronic fiscal devices, fiscal invoicing and fiscal data for administering these Regulations;

(c) authorising FRCA employees to perform tasks that enable the CEO to comply with these Regulations;

(d) establishing and maintaining, in an electronic form and in any other form that the CEO considers appropriate, an accurate up-to-date record of—

(i) the name and address of each taxpayer;

(ii) the address of each premises where the taxpayer operates a business;

(iii) details of the EFD operated for the taxpayer's business;

(iv) details of any erroneous data entered into a POS and the manner in which it was corrected or cancelled; and

(v) details of a defect in or misuse of an EFD;

(e) accrediting POSes and E-SDCs;

(f) receiving complaints and reports about EFDs;

(g) setting up and maintaining a system that enables taxpayers and customers to access fiscal data stored on the Authority's system to verify the following in relation to either a single transaction or more than one transaction—

(i) that the Authority's system has received fiscal data transmitted to it;

(ii) the accuracy of fiscal data stored on the Authority's system;

(h) publishing information, including by publishing information on a website or in another electronic form, about the process by which taxpayers and customers access and verify the matters referred to in paragraph *(g)*;

(i) conducting audits, inspections and other supervisory activities for ensuring the Authority's system and each taxpayer's EFD do not contravene these Regulations;

(j) taking steps and making decisions for prosecuting persons who allegedly commit offences against these Regulations or compounding those offences and ordering the offender to pay money under section 59 of the Act; and

(k) conducting a customer compliance award programme.

Role and responsibilities of suppliers

14.—(1) A supplier may supply an accredited POS or E-SDC to a taxpayer.

(2) If a supplier becomes aware of a defect in, or misuse of, an accredited POS or E-SDC, the supplier must report the defect and its cause (if known), or the misuse, to the CEO as soon as practicable after becoming aware of it.

(3) In subregulation (3), "defect" includes failure to operate, incorrect labelling, damage or missing a part.

(4) A supplier, who has an agreement with a taxpayer to install and implement an EFD or component of an EFD in the taxpayer's business, may, for and on behalf of the taxpayer obtain the digital certificate of the EFD.

Conduct of suppliers

15. A supplier must not offer for sale, or supply, a POS or E-SDC (whether as an EFD or as a component of an EFD) to a taxpayer unless the POS or E-SDC is accredited.

Role and responsibilities of taxpayers—EFDs

16.—(1) A taxpayer is responsible for operating an EFD for each business of the taxpayer in accordance with the Guidelines set out in the Schedules.

(2) The POS and E-SDC components of the EFD for a taxpayer's business must be accredited.

(3) A taxpayer is responsible for giving the CEO the following information—

(a) the taxpayer's name and address;

(b) the name and address of each business operated by the taxpayer;

(c) the brand, model and specifications of each component of the EFD the taxpayer operates for the business of the taxpayer;

(d) justification for each case when a normal refund is issued by the business.

(4) A taxpayer is responsible for making a report to the CEO if the taxpayer is not able to verify any of the following matters by the system referred to in regulation 13(2)*(g)*—

(a) that the Authority's system has received fiscal data transmitted to it by the taxpayer's EFD;

(b) the accuracy of fiscal data transmitted by the taxpayer's EFD to the Authority's system.

Role and responsibilities of businesses of taxpayers—issue of fiscal invoices

17.—(1) A taxpayer is responsible for ensuring that, at each business of the taxpayer—

(a) a fiscal invoice is issued to a customer for each transaction between the business and the customer; and

(b) there is displayed, in each premises where the transactions of the business are conducted, on or beside each POS operated on the premises, the following notice—

"NOTICE TO ALL CUSTOMERS: The Tax Administration (Electronic Fiscal Device) Regulations 2017 requires the operator of this business to issue a fiscal invoice to each customer. DO NOT PAY FOR THE GOODS AND SERVICES SUPPLIED TO YOU UNLESS YOU ARE ISSUED A FISCAL INVOICE. You may verify the authenticity of each invoice issued to you on the Fiji Revenue and Customs Authority's website - www.frca.org.fj".

(2) The notice referred to in subregulation (1)*(b)* must be displayed in the manner and position that ensures that its wording is clearly visible to the customers of the business.

Conduct of taxpayers

18.—(1) A taxpayer must not operate a business unless the taxpayer—

(a) operates an EFD for the business; and

(b) each POS and E-SDC of the EFD is accredited.

(2) A taxpayer must install, implement and operate the EFD in accordance with the Guidelines set out in the Schedules.

(3) A taxpayer must issue a fiscal invoice to a customer for each transaction between the taxpayer's business and the customer.

(4) Subregulation (3) applies even if a customer fails or refuses to take the fiscal invoice.

(5) A taxpayer must not issue a fiscal invoice that does not comply with regulation 12 to a customer.

(6) If a transaction of a business of the taxpayer is a business to business transaction or a business to government transaction, the taxpayer must—

(a) request the customer to provide the customer's TIN to the taxpayer; and

(b) on being given the TIN, enter it into the taxpayer's POS as part of the transaction data for the transaction.

(7) A taxpayer must not fail to give the information specified in regulation 16(3) to the CEO.

(8) A taxpayer must not fail to display a notice in accordance with regulation 17(1)*(b)*.

(9) A taxpayer must comply with the Authority's procedures and requests for auditing an EFD and fiscal data.

Role and responsibilities of customers

19.—(1) A customer is responsible for checking each fiscal invoice issued to the customer and verifying the information recorded on the fiscal invoice.

(2) A customer who has been issued a fiscal invoice may, by the system referred to in regulation 13(2)*(g)*, verify that the fiscal data recorded on the fiscal invoice has been received by the Authority's system.

(3) A customer must report the following matters to the CEO as soon as practicable after they happen—

(a) that the customer has not been issued a fiscal invoice for a transaction;

(b) that fiscal data printed on a fiscal invoice issued to the customer is not an accurate record of the transaction it was issued for;

(c) that the customer is not able to verify, by the system referred to in regulation 13(2)*(g)*, whether the Authority's system has received fiscal data recorded on a fiscal invoice issued to the customer.

(4) A customer, who is eligible to do so, may participate in a customer compliance awards programme.

(5) If a customer enters into a transaction that is a business to business transaction or a business to government transaction and the taxpayer operating the business requests the customer to provide the customer's TIN, the customer must provide the TIN to the taxpayer so it may be entered into the taxpayer's POS as part of the transaction data for the transaction.

PART 4—MISCELLANEOUS

Division 1—Guidelines and protocols

References to Guidelines

20. The Guidelines referred to in these Regulations are set out in the Schedules as follows—

(a) Technical Guideline for Accredited POSes is set out in Schedule 1;

(b) Technical Guideline for Accredited E-SDCs is set out in Schedule 2;

(c) Technical Guideline for Accreditation Methodology is set out in Schedule 3.

Protocols for communication and data exchange between EFDs and Authority's system

21.—(1) The CEO must establish and maintain protocols to ensure that—

(a) the secure elements of EFDs and the Authority's system are integrated; and

(b) communication and data exchange between EFDs and the Authority's system is established in a manner that message confidentiality, integrity, origin and authenticity are secured.

(2) The CEO must publish each protocol on the Authority's website in a format that enables a person to download a copy of the protocol.

(3) A protocol does not have effect unless it is made available to the public under subregulation (2).

Division 2—Offences and penalties

Supplier must comply with regulation 15

22.—(1) A supplier who contravenes regulation 15 commits an offence and is liable upon conviction to—

(a) a fine not exceeding—

(i) if the gross annual turnover of the supplier's business is less than $500,000, $10,000;

(ii) if the gross annual turnover of the supplier's business is $500,000 or more but less than $1,500,000, $25,000; or

(iii) if the gross annual turnover of the supplier's business is $1,500,000 or more, $50,000;

(b) a term of imprisonment not exceeding 24 months; or

(c) both a fine and imprisonment.

(2) Where a supplier under subregulation (1) is a company, each director of the company is also liable upon conviction to a term of imprisonment not exceeding 24 months.

Taxpayer must comply with regulation 18

23.—(1) A taxpayer who contravenes regulation 18 commits an offence and is liable upon conviction to—

(a) a fine not exceeding—

(i) if the gross annual turnover of the taxpayer's business is less than $500,000, $10,000;

(ii) if the gross annual turnover of the taxpayer's business is $500,000 or more but less than $1,500,000, $25,000; or

(iii) if the gross annual turnover of the taxpayer's business is $1,500,000 or more, $50,000;

(b) a term of imprisonment not exceeding 24 months; or

(c) both a fine and imprisonment.

(2) Where a taxpayer under subregulation (1) is a company, each director of the company is also liable upon conviction to a term of imprisonment not exceeding 24 months.

Offences for dishonest and fraudulent conduct

24.—(1) A person commits an offence if the person operates an EFD installed and implemented in a taxpayer's business, or a component of the EFD, in a manner that results in the person—

(a) entering false data into a POS;

(b) tampering with, altering or falsifying data transmitted to or received, recorded, analysed, formatted or stored by the EFD or a component of the EFD;

(c) causing the EFD or a component of the EFD to malfunction or to cease operating; or

(d) causing the EFD or a component of the EFD to—

(i) transmit incorrect or false fiscal data; or

(ii) operate in a manner that results in a taxpayer avoiding or evading paying a tax.

(2) A person who commits an offence against subregulation (1) is liable upon conviction to—

(a) a fine not exceeding $50,000;

(b) a term of imprisonment not exceeding 24 months; or

(c) both a fine and imprisonment.

Division 3—Other miscellaneous matters

Publication of conditions and procedures for accessing Authority's system to verify receipt and accuracy of fiscal data

25. The CEO—

(a) must set up, in a manner that is in accordance with the Guidelines set out in the Schedules, the system referred to in regulation 13(2)*(g)*; and

(b) may publish the conditions and procedures for accessing the system.

Customer compliance award programme

26.—(1) The CEO may conduct a customer compliance award programme involving a fiscal invoice lottery.

(2) The procedure and criteria for participation in the customer compliance award programme are those specified in writing by the CEO and publicly displayed on the premises of the businesses that are part of the programme.

Audits and investigations

27. The CEO must conduct audits and investigations at different levels to ensure that taxpayers are complying with these Regulations, including by—

(a) checking if the taxpayer is issuing valid fiscal invoices;

(b) checking if the POSes and E-SDC for the taxpayer's business are accredited;

(c) checking if the EFD complies with the Guidelines set out in the Schedules;

(d) checking the operation of the protocols; and

(e) requiring taxpayers to provide relevant information and documents as necessary.

Enforcement of compliance

28.—(1) In this regulation—

"EFD" means an EFD of which each POS and E-SDC is accredited;

"group of businesses" means a group of businesses specified by the Minister by notice in the Gazette; and

"time specified by the Minister in respect of a group of businesses" means the period of time specified by the Minister, by notice in the Gazette, within which a taxpayer, who has a business that is a member of the group, must be operating an EFD for the business.

(2) There must be, before the expiry of the time specified by the Minister in respect of a group of businesses, an EFD installed, implemented and operating for each business in the group.

(3) A taxpayer, who operates a business that is a member of a group of businesses, commits an offence if the taxpayer fails to install, implement and operate an EFD for the business before the expiry of the time specified by the Minister in respect of the group of businesses.

(4) A taxpayer who commits an offence against subregulation (3) is liable upon conviction to—

(a) a fine not exceeding—

(i) if the gross annual turnover of the taxpayer's business is less than $500,000, $10,000;

(ii) if the gross annual turnover of the taxpayer's business is $500,000 or more but less than $1,500,000, $25,000; or

(iii) if the gross annual turnover of the taxpayer's business is $1,500,000 or more, $50,000;

(b) a term of imprisonment not exceeding 24 months; or

(c) both a fine and imprisonment.

(5) Where a taxpayer under subregulation (4) is a company, each director of the company is also liable upon conviction to a term of imprisonment not exceeding 24 months.

Made this 1st day of June 2017.

A. SAYED-KHAIYUM
Attorney-General and Minister for Economy

SCHEDULE 1
(Regulation 20(a))

TECHNICAL GUIDELINE FOR ACCREDITED POSes

TABLE OF CONTENTS

1. Introduction

Each accredited POS should be able to connect to an E-SDC or V-SDC and issue a fiscal invoice. Accredited POSes are developed for different platforms, designed to use a variety of communication standards to connect to other software or hardware components. As wide acceptance and low cost of integration are crucial for successful fiscalisation, the Authority is dedicated to providing detailed integration instructions for all manufacturers and software developers (suppliers).

This Guideline is the technical guideline for activation of accredited POSes and integration with an E-SDC or V-SDC service. This Guideline sets standards that will enable seamless integration of accredited POSes with the V-SDC that is part of the Authority's system.

2. Interpretation

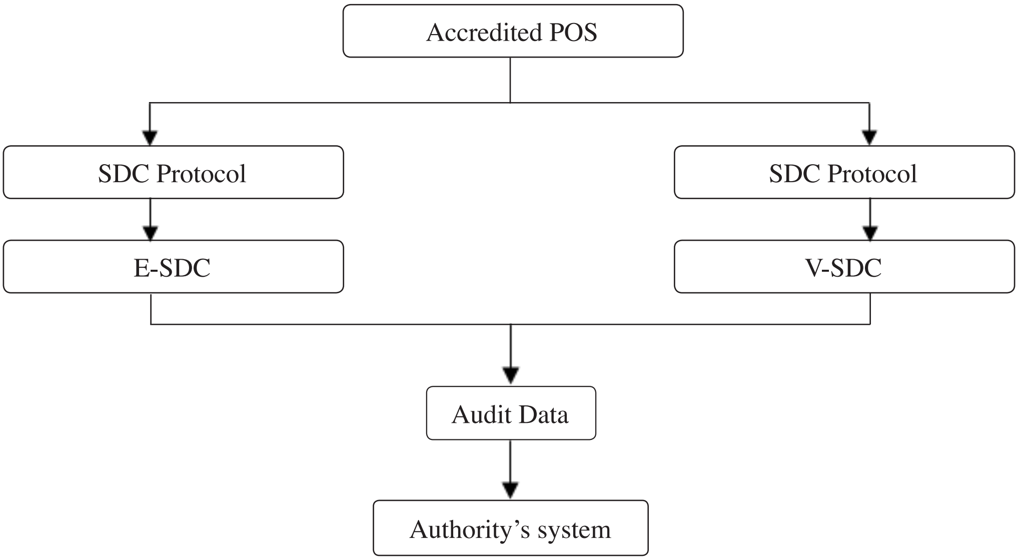
In this Guideline—

"ERP" means the enterprise resource planning software system that enables the integration of a POS with other systems operated by a taxpayer such as an accounting system;

"QR code" means a Quick Response code, which is a matrix barcode that is easily read with a device equipped with a bar code reader; and

"verification URL" means the unified resource location used to verify a particular fiscal invoice.

3. High Level Architecture of the Authority's system



This Guideline describes high level requirements for an accredited POS for all possible scenarios.

3.1. Connected Scenarios

The simplest scenario is software application (taxpayer) creates receipts, designates taxes and calls V-SDC web service to fiscalise invoices. V-SDC authenticates caller (verifies taxpayer digital certificate), performs initial validation, calculates taxes, signs receipt and returns response to a taxpayer.

A response consists of digital signature of receipt or invoice data, internal data field containing an encrypted message to the Authority, digital certificate metadata, textual representation of fiscal invoice and verification URL.

The taxpayer has to generate QR code from verification URL and print textual representation of fiscal invoice and QR code. In case fiscal invoice is delivered in electronic form, verification URL should be rendered as 'clickable' hyperlink in email or web page.

Advantages

1. Does not require specialised hardware.
2. Accredited POS can be implemented as mobile application.
3. Existing ERPs can integrate quickly.
4. Cost of fiscalisation is reduced.

Disadvantages

1. Internet connection is required to issue fiscal invoice.

3.2. Semi-Connected Scenarios

Semi-Connected systems are designed around E-SDCs to fiscalise receipts while internet connection is not available for short or long periods of time. Some E-SDCs could be designed to work offline all the time.

In order to fiscalise a receipt in semi-connected or disconnected mode, an E-SDC receives a receipt from an accredited POS, prepares it for signing and submits the same to the secure element (implemented as smart card containing digital certificate and special applet). The secure element returns signature and internal data to the E-SDC, the E-SDC adds metadata and creates textual representation of a fiscal invoice and returns it to the accredited POS.

As in the connected scenario, a response consists of digital signature of receipt or invoice data, internal data field containing an encrypted message to the tax authority, digital certificate metadata, textual representation of the fiscal invoice and verification URL.

A taxpayer has to generate QR code from verification URL and print textual representation of the fiscal invoice and QR code. In case the fiscal invoice is delivered in electronic form, verification URL should be rendered as 'clickable' hyperlink in email or web page.

The E-SDC will automatically take care of audit data delivery to the Authority when the device comes online or manually, using SD cards or USB Flashes.

Advantages

1. Works without internet connection.

Disadvantages

1. Requires specialised hardware.
2. Prone to physical destruction.
3. Requires network of maintenance shops.

4. Development Environment

The Authority will setup and run development environment accessible to all developers of accredited POS and E-SDC components. Development environment has to expose same application programming interfaces and protocols as production environment.

5. Obtaining Test Certificates

Everyone who registers as a software developer of an accredited POS on the Authority website should receive a set of test certificates, technical documentation and user manual. Test certificates should make possible to test failing scenarios like trying to fiscalise a receipt with an expired certificate.

6. Data Structures

A fiscal invoice consists of two parts. The first part (Invoice Request) is created by an accredited POS and contains the information specified in regulation 12(2)*(a)*, *(b)*, *(c)*, *(d)*, *(e)*, *(f)*, *(g)*, *(h)*, *(i)* and *(j)* and other industry specific information. An invoice request is then submitted by the accredited POS using protocol for communication to V-SDC or E-SDC, depending on implementation specifics of an accredited POS system and targeted audience.

The second part (Invoice response) is generated by V-SDC or E-SDC after data validation. A response contains the information specified in regulation 12(2)*(k)*, *(l)*, *(m)*, *(n)* and *(o)*. V-SDC or E-SDC returns response data to the accredited POS. Response data is an integral part of a fiscal invoice, and a receipt cannot be a fiscal invoice without it.

7. Test Cases

7.1 Issue of Fiscal Invoice for a Normal Receipt

A receipt and fiscal invoice must contain visible markings indicating receipt type "NORMAL".

7.1.1. Steps

Cashier on an accredited POS selects the NORMAL type of receipt, and registers sale by: typing items, selecting items from previously made list or scanning with a bar code reader. At the end, cashier is choosing way of payment and finishing receipt.

An accredited POS is sending message to V-SDC or E-SDC. After positive invoice data verification, receipt is digitally signed, counters and totals are updated and internal data is finished.

V-SDS or E-SDC is sending back a fiscal invoice response to an accredited POS.

A fiscal invoice is issued to the customer.

7.1.2. Expected Results

A fiscal invoice is the final result of this process and can be printed or sent by SMS or email message if a customer requests it. A normal receipt is digitally signed. Internal data is stored in the data base of the Authority's system. Internal data is shown at the end of the fiscal invoice in the form of a QR code. The invoice counter is in the form 5/7NS (5-number of normal receipts/ 7-total number of receipts issued by E-SDC or V-SDC, NS – designation of normal receipt.)

7.2. Issue of Fiscal Invoice for a Refund Receipt

A receipt and fiscal invoice must contain visible markings indicating "REFUND".

The totals on refund receipts and fiscal invoices are negative, starting with "-".

7.2.1. Steps

Cashier on an accredited POS is selecting refund type of receipt, registering sale by: typing items, selecting items from previously made list or scanning with a bar code reader. At the end, cashier is choosing way of payment and finishing receipt.

An accredited POS is sending message to V-SDC or E-SDC. After positive invoice data verification, receipt is digitally signed, counters and totals are updated and internal data is finished.

V-SDS or E-SDC is sending back a fiscal invoice response to an accredited POS.

A fiscal invoice is issued to the customer.

7.2.2. Expected Results

A fiscal invoice is the final result of this procedure and can be printed or sent by SMS or email message if the customer is asking for it. A receipt for refund is digitally signed. Internal data is stored in the data base of the Authority's system. Internal data is present on the end of the fiscal invoice in the form of a QR code. A fiscal invoice counter is in the form 5/7NR (5-number of normal receipts for refunds/7-total number of receipts issued by E-SDC or V-SDC, NR – designation of normal receipt for refund).

7.3. Issue of Fiscal Invoice for a Copy Receipt

Receipts and fiscal invoices must contain visible markings indicating the receipt type "COPY".

7.3.1. Steps

(a) Cashier on an accredited POS is selecting copy type of receipt. Depending on the implementation method, an accredited POS may offer to select already issued receipt from the journal memory or recall receipt number. At the end, cashier is choosing the selected receipt and producing a copy of it.

(b) An accredited POS is sending message to V-SDC or E-SDC. After positive invoice data verification, a receipt is digitally signed, counters are updated.

(c) V-SDC or E-SDC is sending back a fiscal invoice response to an accredited POS.

(d) A copy of a fiscal invoice is issued to the customer.

7.3.2. Expected Results

A copy of already issued fiscal invoice is the final result of this procedure. A fiscal invoice counter is in the form 1/9 CS (1-number of copies of normal receipts/9-total number of receipts issued by E-SDC or V-SDC, CS – designation of copy of normal receipt).

7.4. Issue of Fiscal Invoice for a Training or Pro-forma Receipt

Receipts and fiscal invoices must contain visible markings indicating the receipt type “TRAINING” or “PRO-FORMA”.

Training or pro-forma receipts and fiscal invoices are produced in the same way as normal receipts and fiscal invoices, with an exception that totals are not accounted for.

7.4.1. Steps

(a) Cashier on an accredited POS is selecting Training or Pro-forma type of the receipt, is registering sale by: typing items, selecting items from previously made list or scanning with a bar code reader. At the end, cashier is choosing way of payment and finishing receipt.

(b) An accredited POS is sending message to V-SDC or E-SDC. After positive invoice data verification, a receipt is digitally signed and counters are updated.

(c) VSDS or E-SDC is sending back a fiscal invoice response to an accredited POS.

(d) A fiscal invoice is issued.

7.4.2. Expected Results

Training or pro-forma fiscal invoice is the final result of this procedure. A fiscal invoice counter is in the form 3/8TS (3-number of receipts for training or pro-forma receipts/8-total number of receipts issued by E-SDC or V-SDC, TS – designation of receipts for training or pro-forma receipts).

7.5. Issue of Fiscal Invoice for Normal or Refund Receipt for a Business to Business Transaction

A receipt and fiscal invoice must contain visible markings of receipt type "NORMAL", or "REFUND".

Receipts and fiscal invoices contain business customer data, name and TIN.

7.5.1. Steps

(a) Cashier on an accredited POS is selecting receipt type, is asking customer for and inputting provided TIN, is registering sale by: typing items, selecting items from previously made list or scanning with a bar code reader. At the end, cashier is choosing way of payment and finishing receipt.

(b) An accredited POS is sending message to V-SDC or E-SDC. After positive invoice data verification, a receipt is digitally signed, counters and totals are updated and internal data is finished.

(c) VSDS or E-SDC is sending back a fiscal invoice response to an accredited POS.

(d) *A* fiscal invoice is issued to the customer.

7.5.2. Expected Results

A fiscal invoice is the final result of this procedure and can be printed or sent by SMS or email message if the customer is asking for it. A normal or refund receipt is digitally signed. Internal data is stored in the data base of the Authority's system. Internal data is shown at the end of the fiscal invoice in the form of a QR code. A receipt counter is in the form 5/7NS or NR number of normal receipts or normal receipts for refunds/7-total number of receipts issued by E-SDC or V-SDC, NS or NR – designation of normal receipt or normal receipt for refund).

SCHEDULE 2
(Regulation 20(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 Authority's system.

V-SDC is a web service published and maintained by the CEO and it represents an integral part of the Authority's 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 Authority's 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 Authority's 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 Authority's 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 Authority's system that the audit data has been securely stored on the Authority's 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 Authority's 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 Authority's system public key and adds it to the package so that the Authority's system can decrypt symmetric key and access package content once it arrives on the Authority's 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, the Authority 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 Authority's Systems

Commands are means of communication between the Authority's 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 Authority's system using remote or local audit.

Command Type	Action
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 Authority's system, plus E-SDC date and time. Executes and returns data to Authority's 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 Authority's system in case the CEO 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 Authority's 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 the Authority.

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 Authority's system and perform remote audit. If the Authority's system is not accessible, the E-SDC will switch to offline mode.

2.7. Authentication

Authentication against the Authority's system is performed using taxpayer digital certificate.

3. Digital Certificates

3.1. Authority's 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

The Authority 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)*, *(f)*, *(g)*, *(h)*, *(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 the Authority 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 CEO (and the Authority's 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 Authority's system in the future. The only one who can decrypt audit data is the Authority's system software running on the Authority premises and by the CEO only.

6.2. Proof of Audit

Proof of audit is generated by the Authority's system once audit data has been received and securely stored on the Authority's 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 Authority's system.

6.3. Audit Process

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

There are three specific scenarios: remote audit, local audit initiated by a taxpayer and local audit initiated by the Authority. 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 the Authority. 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 Authority's 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 Authority's 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 Authority's system using the same communication channel;
4. the Authority's system receives audit data, decrypts packages and does a basic verification;
5. if verification is successful, the Authority's 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 Authority's system private key, which ensures that audit data has been successfully received by the Authority's 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 Authority's 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 Authority's 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 Authority's system in the next audit.

6.5 Remote Audit

Remote audit is the process of transferring data to the Authority's system using internet connection. It is the most common way to perform audit for any occasionally connected device.

An E-SDC checks if the Authority's system is online. If it is online, the E-SDC authenticates the Authority's system by using server-side certificate installed on the API endpoint, enabling HTTPS protocol. The Authority's 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 Authority Office

The CEO can upload data using specific application that will store deleted audit data from media and save proof of audit generated by the Authority's 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 Authority's 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 Authority

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

SCHEDULE 3
(Regulation 20(c))

TECHNICAL GUIDELINE FOR ACCREDITATION METHODOLOGY

TABLE OF CONTENTS

1. Introduction

This Guideline is the technical guideline for accreditation of a POS or E-SDC.

The CEO accredits the brand, model and specification of each POS or E-SDC supplied by a supplier. The CEO accredits each POS and E-SDC of an EFD developed, installed and implemented by a taxpayer. This is done to ensure that EFDs for taxpayers' businesses are operating in accordance with these Regulations.

2. Interpretation

In this Guideline—

"application" means an application for accreditation under regulation 8 or 9;

"applicant" means a supplier or taxpayer who makes an application.

3. Evaluation process

The evaluation process commences when the CEO receives an application for accreditation of a POS or E-SDC.

The evaluation process consists of an administrative review and a technical review of the working processes of the applicant's POS and E-SDC together as an EFD or a POS or E-SDC as a separate component.

The CEO evaluates the POS or E-SDC by testing the applicant's internal procedures. The purpose is to check that the applicant is complying with all administrative and technical requirements and to test and verify all deliverables.

The CEO evaluates documentation by cross-examining functionality stated in the user manual and other documentation to ensure described implemented functions.

The technical review identifies whether there are any of the following type of issues:

1. Non-compliance: represents a deviation of the expected output, and must be solved by the applicant;

2. Bug: represents a failure, flow or fault in software that produces incorrect or unexpected results, and must be solved by the applicant;
3. Doubt: represents uncertainty due to misinterpretation and is resolved by investigation and clarification by the applicant;
4. Observation: represents minor faults, mainly in documentation or sample appearance; these issues shall contain sub-class mandatory or voluntary which will reflect the applicant's level of obligation to solve;
5. Improvement: represents proposal to improve functionality, which the applicant may solve or not.

The CEO writes test reports about technical review findings and specifies issues.

All issues that are non-compliance, bugs, doubts and observations with mandatory sub-class must be solved before accreditation is granted.

The applicant responds to each issue identified by preparing and finalising deliverables for resolving the issue and updating the testing report with answer and version number. Example is:

> File name: "*Testing report EFD01_15 ver.1.doc*" containing history of revisions and description of the issue number 15 of application ID EFD01 shall be returned to the same address from which it has been received after being saved by the applicant as file name: "*Testing report EFD01_15 ver.2.doc*" containing updated history of revisions and answer on the evaluation issue. This upgrading of version number shall be continuous until the issue number 15 is resolved.

Communication between the CEO and applicant is open, honest and co-operative in dealing with each issue.

Possible difficulties arising during the evaluation process are:

1. the applicant's delays preparing the required deliverables for resolving issues identified during the evaluation process;
2. necessity for numerous testing reports containing problems and questions which are found during evaluation;
3. misinterpretation of the requirements.

The CEO may allow the applicant additional time to respond to issues and finalise deliverables.

4. Outcomes

When the issues are resolved and finalised to the satisfaction of the CEO and applicant, the CEO writes the accreditation report describing the evaluation process and the outcome of the process and making recommendation for or against accreditation.

If the outcome of the evaluation process indicates that the applicant's administrative and technical processes comply with these Regulations, the CEO accredits the POS or E-SDC.

The CEO refuses to accredit the applicant if applicant is unable to prepare and finalise deliverables for resolving issues identified during the evaluation process with the effect that the applicant's administrative and technical processes do not comply with these Regulations.

Price: $2.60

S. NAVUNILAWA, Government Printer, Suva, Fiji – 2017
Official Printer Since 1883

72/FGGS/17—700