MODERNISING IRELAND'S ADMINISTRATION OF VALUE-ADDED TAX (VAT)

Real-time digital reporting and electronic invoicing

Prepared for

Revenue Commissioners

Ireland

vatmodernisation@revenue.ie

Prepared by

Data Tech International

Belgrade, Serbia

[redacted]

www.dti.rs

Based on request for contributions, comments and feedback - Public Consultation on Real-time Digital Reporting and Electronic Invoicing

PROJECT # IR3101-1

Abbreviations

AIS	Accredited Invoicing System (AIS) means a point of sale invoicing device or software (EPOS)
API	Application Programming Interface – Application access point accessible to other software systems
B2C	Business to Consumer
B2B	Business to Business
B2G	Business to Government
CIS	AIS in Rwanda
ECR	Electronic Cash Register
EFD	Electronic Fiscal Device (EFD) is composed of an AIS and SDC connected into one system. The EFD produces fiscal receipts and reports audit data to a Tax Core.
EBM	EFD in Rwanda
Fiscalization	A process of issuing invoice or 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 EFD technical specification.
LDAP	Lightweight Directory Access Protocol – Standard protocol used for communication with directory of user, roles and organizational structure
MOF	Ministry of Finance
MRC	Machine Registration Code – AIS's unique serial number
POS	Point of Sale
SDC	Sales Data Controller is a mechanism in a form or a special software or device connected to a AIS and designed to receive specific receipt data from a AIS. The SDC performs data processing and generates response data, which is sent back to a AIS for further actions. Response data provides authenticity of receipt data. SDC also store receipts to its own internal memory and includes features that enable audit. SDC can be implemented as: • virtual SDC – cloud based software for receipt signing in real-time, which operates in accordance with the regulation (V-SDC) • external SDC – controller device (HW,SW) with remote audit capability which operates in accordance with the regulation (E-SDC)
SDC ID	Sales Data Controller identification number - SDC's and V-SDC's unique serial number
TaxCore®	**TaxCore®** is set of web services, sites and database management software installed on the side of the Tax Service for communication with the AIS and SDC's.
TIN	Tax Identification Number
UI	User Interface – Application's Access point accessible to human users
VAT	Value Added Tax

Table of Contents

Abbreviations 2
1 Introduction 4
1.1 Our Proposal 4
2 Previous Installations, Results, Lessons Learned 4
2.1 Types of Fraud 4
2.1.1 Risk 1: Under-reporting 5
2.1.1.1 Risk 1.1: Not issuing invoices 5
2.1.1.2 Risk 1.2: Double set of books 5
2.1.2 Risk 1.3: Use of automated sales suppression techniques (zappers and phantom-wares) 5
2.1.3 Risk 2: Applying the wrong tax rate 6
2.1.4 Risk 3: Collected but unremitted tax 6
2.1.5 Risk 4: Missing trader 6
2.1.6 Risk 5: False claims for credit/refund 6
2.2 Reference projects 7
2.2.1 Federal Public Service - FPC Finance of Belgium 7
2.2.2 Ethiopian Revenue and Customs Authority – ERCA of Ethiopia 7
2.2.3 Rwanda Revenue Authority – RRA of Rwanda 8
2.2.4 Fiji Revenue and Customs Service – FRCS of Fiji 8
2.2.5 Department of Revenue – DOR of Washington State 9
2.2.6 Ministry for Customs and Revenue – MCR of Samoa 10
2.3 Ministry of Finance and Serbian Tax Authority - STA 11
3 Conclusion 12
3.1 Expected Benefits 12
3.1.1 For Irish Tax and Customs 12
3.1.2 For Taxpayers 12
3.1.3 For Invoicing System Vendors 13
3.1.4 For Customers 13
3.2 High Level System requirements 13
3.3 Critical Success Factors 14

1 Introduction

Data Tech International (DTI) is revolutionizing tax collection and changing the landscape of fiscal economy. Over the last decade, DTI has successfully carried out complex fiscal projects for governments across the world, by using all the benefits of modern technology, we managed to create a software platform that guarantees the security of confidential records and prohibits data manipulation.

TaxCore®[1], DTI's flagship system, ensures fraud-free TAX collection monitoring.

Most importantly, TaxCore® is independent of any administration information and database systems in use. This means that it complements any integrated tax administration system already in use.

1.1 Our Proposal

DTI is proposing a solution to REVENUE that is not only single economic sector stopgap measure. Fraudsters will only stop when *they know* there is a high probability they will be caught. The most successful fraud prevention efforts around the world follow this approach. Digitally secure invoices will send this message. DTI's proposal provides Revenue Authority with advanced notice of every commercial transaction in a manner that would allow risk analysis, and remote audit. Cross-border sales would be digitally matched with purchases, and *fraudsters would know this.* Fiji has implemented this solution.

The commercial time needed for full transactional compliance is less than a second if processed online, but it is also possible with offline stand-alone devices secured by Irish Tax and Customs. **Encryption assures privacy, data integrity and nonrepudiation of each and every invoice or receipt.**

2 Previous Installations, Results, Lessons Learned

The following is a selection of previous and current DTI projects for detecting VAT related fraud.

2.1 Types of Fraud

In Rwanda and Fiji Islands, the two jurisdictions in which DTI and our consultants have delivered a turnkey solution, taxpayers who are registered for trading in domestic or cross-border environment are under obligation to electronically register tax collected on behalf of the revenue authority for every taxable good and service exchanged for cash, cashless payment or any other form of compensation. Furthermore, the total sum of all sales, including the totals for non-

[1] [1] TaxCore® is a product name of Data Tech International. It provides the back-end functionality for numerous government monitoring systems. For example, in **Fiji** the VAT Monitoring System (VMS) is powered by TaxCore®, as is the Tax Invoice Monitoring System (TIMS) in **Samoa**, the System for Fiscalization Management (SUF) in **Serbia** known as efiscalization, the Electronic Monitoring Agreement in **Washington State** and the un Système de facturation électronique normalisée (FNE) in **Ivory Coast**.

taxable items or services, is levied by way of an income tax (minus all permitted deductibles) at the end of the fiscal period prescribed by the Government. The following sub-sections discuss the high tax collection risks that were identified in both Rwanda and Fiji and explain how EFDs have mitigated those risks:

2.1.1 Risk 1: Under-reporting

A taxpayer discloses only part of their sales data to the Revenue Authority, usually by falsifying books or deleting sales records. The two most common types are:

2.1.1.1 Risk 1.1: Not issuing invoices

It is very common for consumers to not ask for their invoice, as they don't usually have any motivation to justify of their purchases, unless they require an invoice for possible deductions on personal income tax and similar activities. As a result, taxpayers simply neglect to issue invoices and avoid creating sales records. This applies to participants from all sectors, from retailers who take payments and give change without ringing them, to service providers such as lawyers who render services and simply pocket the payment without recording it.

Mitigated by EFD: The Revenue Authority implemented an ordinance according to which only verifiable invoices issued through EFDs can be processed for VAT refund claims in cases of B2B transactions. For sensitization purposes, all B2C transactions issued through EFDs are eligible to participate in the Consumer Compliance Awareness program (CCA), which randomly awards consumers who submit their EFD receipts.

2.1.1.2 Risk 1.2: Double set of books

The "Two sets of books" practice consists of hiding or disguising certain financial transactions from auditors by having a set of fraudulent accounting records for official use and another set for personal records. This malpractice is usually found in family-owned businesses where the accounting is not outsourced.

Mitigated by EFD: Every activated EFD is personalized for each individual taxpayer. Such an EFD is capable of producing unique invoices that unambiguously identify the issuer. It is not possible to use unregistered EFDs, as invoices produced by the latter would immediately be recognized by the system as a fake.

2.1.2 Risk 1.3: Use of automated sales suppression techniques (zappers and phantom-wares)

A more sophisticated way to under-report sales in an attempt to deceive any professional auditor is to use software, which is orchestrated by series of parameters provided by **manipulators to alter the original sales records and reduce the total tax liability by the desired rate.**

Mitigated by EFD: Every registered transaction remains in the system in encrypted form, which eliminates any risk of tampering. The counters of the records originate from the secure source of the EFD and thus cannot be changed.

2.1.3 Risk 2: Applying the wrong tax rate

Some goods and services are VAT-exempted. However, business people may not be up to date as regards VAT rates or may intentionally apply a lower rate in an attempt to reduce tax liability. For example, IT equipment in Rwanda is subject to a 0% rate, whereas IT accessories are not. By putting them in the same category, fraudsters may achieve a competitive advantage.

Mitigated by EFD: In the legislation taxpayer's obligation are clearly stated, for example in accordance with item 5 of article 11, "Obligations of an EFD user", of the Ministerial Order No. 002/23/10TC of 31/07/2013, one of these obligations is "*to ensure that all items or services sold through certified electronic billing machines have a clearly defined name and appropriate tax rate*"[2]. The EFD sends all receipts to a back-office server where each item can be analyzed, which makes it possible to easily detect the instances in which a taxpayer has applied the wrong tax rate.

2.1.4 Risk 3: Collected but unremitted tax

In practice, taxpayers often initiate a cessation of business before being properly audited and thus neglect to pay their taxes, *which* remain unreported.

Mitigated by EFD: Every activated certificate installed in EFD is accounted for by the Revenue Authority. The EFD is programmed to report automatically and inspectors can easily retrieve audit records locally, in cases when the EFD is experiencing technical difficulties and is unable to access the operator's network. It is not possible for the Revenue Authority officer to approve the cessation of business unless all information from EFD has been transmitted to the back-office system, which will show the amount of the tax that is due.

2.1.5 Risk 4: Missing trader

Some companies are set up solely to generate invoices that allow for the recovery of VAT in cross-border (less often domestic) trading. They exploit the lack of capacity for conducting proper cross-examination for every invoice against the evidence that earlier tax has been paid.

Mitigated by EFD: Every invoice issued by the exporter from Revenue Authority is created by its personal EFD and can be publicly verified by anybody (even by the foreign jurisdiction), thus justifying the legality of the trader's registration in the country of origin.

2.1.6 Risk 5: False claims for credit/refund

According to the general rules, all business-to-business (B2B) transactions must be made in such a way that clearly states the seller's and the buyer's identities using their unique tax identification number and address, followed by a description of the sold good/service and the unit (both excluding and including VAT). These requirements are necessary for inspection cross-checking analysis. The refund period is usually 30-45 days, but due to a very high number of requests, inspection is only focused on certain categories, which represents a risk, but this

[2] https://www.rra.gov.rw/typo3conf/ext/complete/Resources/Public//download/pdf/ogazette.pdf

mostly concerns the requests that demand payback. Many credit requests can pass uncontrolled at the time of submission and it is very easy to fake them.

Mitigated by EFD: Revenue Authority inspectors working on the verification of VAT refund claims, can easily check, using the TaxCore, whether the invoice submitted for justification is the original and is dedicated to the recipient who has filed the claim. Fraudsters are reluctant to file false claims, knowing that these claims will immediately be verified against the original EFD invoices.

2.2 Reference projects

2.2.1 Federal Public Service - FPC Finance of Belgium

Deployed into operation as of January 1, 2016 with the country's MoF cash register working group, this system is an improved variant of the Swedish model[3], which was officially presented as very successful by the Swedish Tax Authority. As of May 2016, there are no official results to report for Belgium, however it is expected to achieve similar results as Sweden. DTI has developed a proof of concept and presented prototype based on which technical specification was developed[4].

2.2.2 Ethiopian Revenue and Customs Authority – ERCA of Ethiopia

System was installed in 2008 with 800 sales recording machines equipped with remote audit capabilities. As of 2016 it has more than 100,000 registered devices. Tasks provided by DTI include:

- Designing Technical Specification;
- Assisting the project office in the planning, managing and controlling of implementation of Sales Register Systems based on the facts provided by the tax collecting organs;
- Advising the project office on how to enforce technical parameters and set standards in the regulations and the guidelines;
- Designing and implementing work systems, procedures and manuals supporting the project implementation unit;
- Training the project members on how to investigate applications, issuing accreditation compliance and follow test cases before certification;
- Describing business cases for mobile operator;
- Inspection and documentation of reports; and
- Preparing implementation reports with detailed analysis of progress and problems.

[3] Swedish Tax Agency (Skatteverket), Requirements of Cash Registers - Impact Evaluation of the Cash Register Act 2010 (Krav på kassaregister - Effektutvärdering (June 26, 2013) (in Swedish, translation available on request).
[4] Fiscal Data Module (FDM), circular (AAFisc No 33/2016 (No.ET124.747) on November 8, 2016: http://www.salesdatacontroller.com/belgium/

2.2.3 Rwanda Revenue Authority – RRA of Rwanda

DTI supported creation of the Design Technical Specification, including secure crypto algorithms, and assisted the project office in the planning, managing and controlling of implementation of a Certified Invoicing System based on the facts provided by the tax collecting organizations. Tasks provided include:

- Advising the project office on how to enforce technical parameters and set standards in the regulations and the guidelines;
- Designing and implementing work systems, procedures and manuals supporting the project implementation unit;
- Training the project members on how to investigate applications, issuing accreditations compliance and follow test cases before certification;
- Providing Business process reengineering required for the development of the software development and to manage the Certified Systems Invoicing software;
- Conducting testing software;
- Describing business cases for mobile operators;
- Inspection and documentation of reports;
- Preparing implementation reports with detailed analysis of progress and problems;
- Delivered software;
- Security key management module;
- Certification module;
- Audit module;
- Receipt verification module.

System is successful according to the Rwanda Government reports, IGC research [5]and IMF report.

Since RRA introduced EBMs in 2013, they helped collect about Rwf110.5 billion in Value Added Tax (VAT), which increased to Rwf169.5 billion in 2014, while it went up to Rwf196 billion in 2015, and Rwf220 billion in 2016, according to information from RRA. These statistics show that EBM system resulted in VAT increase of over 90 percent since its inception[6].

2.2.4 Fiji Revenue and Customs Service – FRCS of Fiji

In the years 2017-2018, DTI implemented VAT Monitoring System (VMS) in Fiji. The project started with a feasibility study on the basis of which a request for the delivery of a comprehensive system was obtained. The project included drafting of a fiscal law with system technical specification.

[5] https://www.theigc.org/project/evaluation-of-electronic-billing-machines-effectiveness-of-tax-administration/

[6] http://rwandainspirer.com/2017/10/13/technology-becomes-an-enabler-for-rwandas-revenue-collection-progress/

Tasks provided include:

- Inception Report
- Fiscal Law Draft
- Draft protocol specifications
- Draft accreditation procedures
- V-SDC
- TaxCore
- FreePOS
- WebPOS
- Audit module
- QR code receipt verification
- Manuals
- Training on site
- Security key management module;
- Accreditation module;

System has been successful according to the FRCS and independent research by Professor Richard T. Ainsworth. As Ainsworth stated: "There are exceptional efficiencies in this comprehensive digital invoice regime. Fiji is the first VAT jurisdiction in the South Pacific, and one of the few globally to secure real-time, encrypted reporting of all taxable transactions, business-to-business (B2B), and business-to-consumer (B2C). Many of the traditional VAT frauds are simply unworkable in this system. Enforcement flows directly from the technology."[7]

2.2.5 Department of Revenue – DOR of Washington State

A Taxpayer who is mandated to use electronic monitoring (EFD) of the business's sales by a method acceptable to the Washington Department of Revenue (TaxCore) for five years at the business's expense, as per the criminal charge and the offense of WAC 458-20-254, according to which all records must be open for inspection and examination at any time by the department, upon reasonable notice, and must be kept and preserved for a period of five years.

Electronic Monitoring Solution: TaxCore, a software-based security system purchased from Data Tech International, integrated with Dinerware POS system, is configured to securely store all sales information as well as allowing Washington State Department of Revenue to have access to the web-based back-office system at any time via the internet.

[7] https://www.dti.rs/whitepapers/FIJI_digital_invoices.pdf

The penalties taxpayer is charged with are:

- Class C Felony
- 5 years confinement in a state correctional institution and/or $10,000
- Seizure and forfeiture of ESS devices as well as any devices that used the electronic sales suppression (ESS), or property that is traceable to ESS, including specifically the business's Electronic Cash Registers, and Point of Sales systems

Conditional loss of business permits, unless:

- All taxes, penalties and interest is paid
- All additional penalties and fines are paid
- An electronic monitoring agreement acceptable to the Department is entered into between the taxpayer and the Department for 5 years.

2.2.6 Ministry for Customs and Revenue – MCR of Samoa

In 2019-2020, DTI implemented Tax Invoice Monitoring System (TIMS) in Samoa. The project started with inception phase, including consultancy services on modeling the legislation to merge local and technical requirements in regard to all stakeholders' responsibilities and mandates. Tasks provided include:

- Services
  - Project Inception
  - Draft Legislation
  - Integration with the Client's core system
  - API Documentation
  - User Documentation
  - Personalization workstations and smartcard printers
- Modules
  - TaxCore Backoffice
  - Virtual Sales Data Controller Service
  - Communication protocols and standards
  - Invoice Verification Service
  - Secure element - smart card applet
  - Development Portal
  - SDC Accreditation Software
  - POS Accreditation Software
  - Taxpayer Admin Portal
  - Audit Software
  - Key Management and Activation
  - SDC Management
  - Basic Reporting

- Web-based POS (free for taxpayers)
- Mobile POS app (Android/iOS, free for taxpayers)
- Mobile Invoice Verification app (Android/iOS)
- In-depth Invoice Validations
- Taxpayer Compliance Center
- CCA – Fiscal lottery

- Installation and configuration
- Maintenance and Support

2.3 Ministry of Finance and Serbian Tax Authority - STA

Serbia is a country with a long tradition of fiscalization, since 2003. It is known as the first country to introduce regular transfer of daily reports from fiscal cash registers via GPRS terminal to the tax administration server. In 2021, the Ministry of Finance decided to replace the outdated and dysfunctional model of fiscalization based on fiscal cash registers and fiscal printers with the latest from the market and much more efficient. Data Tech International (DTI) was selected as the supplier of the new fiscalization model with expanded coverage which implies that all data from fiscal cash registers were signed by unique cerificate and transferred to the STA server regardless of whether they were created in offline or online mode.

In May 2022, DTI started the enrollment of about 100,000 taxpayers and successfully completed it by the end of the year.

The main component of fiscalization delivered by DTI is the Fiscalization management system (SUF), which serves to receive and archive transactions forwarded by the Electronic Fiscal Devices (EFU). SUF is completely under the control of the STA.

The SUF (DTI's TaxCore®) allows EFU taxpayers and suppliers to easily comply with the law and manages all the STA processes to make each fiscal receipt issued unique and easily verifiable.

Robust and scalable PKI Certificate Authority software is integrated with SUF to provide PKI framework, including issuing and revoking certificates, storing keys, acting as RA (Registration Authority) managing CRLs (Certificate Revocation Lists), OCSP (Online Certificate Status Protocol) responder, etc.

SUF ensures the compliant provisioning of all POS/ECR device/software, the secure transport of all invoices from each device/software, and management of both online and offline behavior. SUF also can fill gaps in data, detect anomalies in transactions based on pre-defined rules, and find hidden patterns in data that may escape detection by human analysts.

Today, SUF processes on average 11 million fiscal invoices on a daily basis. The services include:

- Integration with STA core system
- API Documentation

- User Documentation
- Personalization workstations and smart card printers
- Accreditation procedures and tools
- TaxCore® integrates with existing certificate authorities to produce digital certificates used by Secure Elements to fiscalize invoices.
- Advanced reporting provides Tax Authority users with in-depth insight into taxpayer activities and trends.
- Tools for the preaparation, evidence and reporting of the field visit to a taxpayer's business location
- Export all data to STA advanced analytics application further processing.

3 Conclusion

3.1 Expected Benefits

The use of Electronic Fiscal Devices will increase efficiency while at the same time raising revenues and the quality of the tax returns. The benefit for focusing on tax collection processes lies not only on the side of the REVENUE. The taxpayer will also benefit in terms of more straightforward administrative procedures, increased certainty and reduced administrative costs.

REVENUE will benefit from receiving tax returns of higher quality and reduced need for treatment of individual cases.

3.1.1 For Irish Tax and Customs

- Significant increase of tax collection due to the registration of taxpayers' turnover
- Decreasing activity of gray economy share due to organized evidence of registered taxpayers, their activities and their sales locations
- Suppression of tax evasion due to the comprehensive insight of all taxpayer's activity
- Security of the whole system is based on proven technologies (PKI) and does not rely on 3rd party Vendors

3.1.2 For Taxpayers

- Protecting honest taxpayers from unfair competition
- Eliminating unfair competition
- Minimizing the cost of compliance per taxpayer and per sales point
- Free Compliance (for some businesses)
- Simplified Tax Returns

- Registration of both sales and purchases in business-to-business transactions enables easy cross-checking for processing tax returns and tax refunds
- Irish Tax and Customs and Taxpayer work with the same data which reduces the chance of misunderstanding
- No need to keep receipts or invoices in paper format
- Quicker Tax Refunds through automatic validation of all sales and purchases
- Management and/or Owners will have better insight into business operation
- Small businesses will get simple reporting tools on Taxpayer Admin Portal

3.1.3 For Invoicing System Vendors

- Transparency and level playing field for all suppliers of fiscal equipment
- Affordable and simple Accreditation Process
- Modernizing sale outlets with management tools designed to better serve taxpayers business

3.1.4 For Customers

- A rise of consumer awareness by receiving certified invoices along with purchased goods or services, with a clear and true specification of tax amount dedicated to the government.
- Getting incentives for activities under the Customer Compliance Award program
- Paperless transactions (i.e. scan QR Code on point of sale to transfer receipt to a customer or send an invoice by email)

3.2 High Level System requirements

Proposed solution is compliant with these high-level requirements outlined:

1. TaxCore® system has the ability to receive and transmit fiscal receipts from taxpayers with all the information required by the REVENUE in an industry-standard format;
2. All fiscal receipts are authenticated through an authentication method;
3. TaxCore® verifies that all fiscal receipt data are correct through the automated verification of the validity of the Taxpayer Identification Numbers (TIN) or corporate number or national ID number as well as tax calculation;
4. It has the ability to interact with taxpayers in order to correct the fiscal receipt through credit and debit notes;
5. It has the ability for buyers to verify that fiscal receipt has been received and have gone through automated verification by REVENUE;

6. It has facility to develop and generate reports, KPIs and statistics;
7. Through the integration facility it can detect anomalies and has the ability to interface with the existing Tax legacy systems;
8. It has the ability to differentiate between multiple transactions;
9. It has the ability to handle real time submission of individual transactions as well as batched submission of multiple transactions;

It does not require any specialized equipment from the taxpayer;

DTI offers a reliable, complete and cost-effective anti-sales-suppression application to REVENUE. Similar world-wide implementations enable us to plan and adapt to the demands of real time event invoice analysis in order to detect instances of fraud. The software components we provide are highly modular and can adapt to any EPOS required. This experience has led us to identify the following success criteria.

3.3 Critical Success Factors

- Executive leadership and commitment;
- Well-written compliance requirements;
- Good technical reference documents;
- Good planning in terms of the interoperability of secure components;
- Transparent accreditation process;
- Unique secure element;
- Customer Compliance Award program;
- Administrative benefits for compliant taxpayers;
- Consultation of stakeholders;
- Serious penalties for non-compliance;
- Revocation of administrative privileges for the taxpayers who refuse to comply;
- Good communication campaign.

Finally, we emphasize what gives flexibility and strength to our solution.

The Tax Administration creates a **Secure Element** for each individual AIS and assigns it to the taxpayer with information about the taxpayer from the unique taxpayer's register. Secure Element signs each invoice and stores counters and cumulative amounts from the invoice (mini blockchain principle).

Internal data is created for each invoice, by the Sales Data Controller and contains data from the Secure Element.

Real time invoice verification is a basic check by which the customer or inspector can check the authenticity of the invoice immediately after receipt, regardless of whether the invoice was issued in online or offline mode. Verification is supervised by TaxCore®.

Various invoice validation, which is upgraded through the regular development of TaxCore®, is a higher degree of verification of invoice data and a good source for advanced analysis of taxpayer behaviour.

The **audit** is possible in several ways, the standard is remote, but it does not differ from the local audit. Each audit is followed by a **Proof of Audit** action by which TaxCore® confirms the successful receipt of invoices.

The system supports several types of invoices, the main ones being Sale and Refund. Customer identification (B2B and B2G) allows control and analysis of commercial invoices.

The **Tax Administration Portal** is a part of TaxCore® where taxpayers can access their data and invoices.

We look forward to any questions or further discussion around the anti-ESS software, architecture or methodology.

Annex 1 – Case study - VAT Monitoring System (VMS) in Fiji Islands

taxnotes® international

Volume 92, Number 7 ■ November 12, 2018

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Fiji: A Digital Invoice System Fights Fraud And Enforces Real-Time VAT Compliance

by Richard T. Ainsworth and Goran Todorov

Reprinted from *Tax Notes International*, November 12, 2018, p. 697

For more *Tax Notes International* content, please visit www.taxnotes.com.

tax notes international®

Fiji: A Digital Invoice System Fights Fraud And Enforces Real-Time VAT Compliance

by Richard T. Ainsworth and Goran Todorov

Richard T. Ainsworth is an adjunct professor at the Boston University graduate tax program and the New York University graduate tax program. Goran Todorov is the CEO of Data Tech International Ltd. and a technical advisor and subject matter expert on the prevention of electronic sales suppression. Email: prof482@bu.edu, todorov011@hotmail.com

In this article, the authors examine Fiji's VAT management system, a digital system designed to track all taxable transactions and increase tax compliance by eliminating many of the most common VAT frauds.

Fiji, the largest of the Pacific Island countries, is implementing a comprehensive digital invoice regime. The ambitious goal: to provide automatic, real-time, and encrypted reporting of all taxable transactions, including both business-to-business (B2B) and business-to-consumer (B2C) transactions.

In late 2017 Fiji launched a successful pilot project.[1] The first phase — transitioning the supermarket and pharmacy sectors to the new system — was initially set to be completed December 31, 2017,[2] but the time for completion was extended until February 28, 2018. As of June 2018, phase 1 remains "open" because the tax authority has not commenced enforcement actions to clean up the registry. The second phase includes hardware companies, accounting firms, medical centers, travel agencies, and law firms. It was set for completion June 30, 2018.[3] Announced "completion targets" have been missed largely because Fiji has tried to make adoption a non-intrusive process. Initially, emails are sent directly to taxpayers to "invite" them onboard. This normally triggers business associations to organize meetings with the Fiji Revenue & Customs Service (FRCS) to better understand how the system works. The FRCS accepts requests to meet with every taxpayer and association that needs to have more information. Time is extended for preparation and for existing point-of-sale (POS) vendors to meet compliance needs. This approach has been successful, but it has pushed deadlines back. No penalties for non-compliance have been issued to date, but all taxpayers belonging to the concerned groups are monitored. Those who fail to express interest and show progress are issued a written warning. The second "warning" (not used yet) will be in the form of a hefty fine.

Fiji's technology reform is intended to increase VAT compliance. It has attracted global attention because it is accompanied by a 40 percent reduction in the VAT rate, an expansion of the VAT base, and a prediction that VAT revenue will increase. Fiji reduced its single rate from 15 percent to 9 percent January 1, 2016. At the same time, it expanded the VAT base by removing exemptions on rice, cooking oil, fish, flour, tea, powdered milk, and kerosene. Notably, these are supermarket inventory items and therefore part of the first group phase.

The 2016 budget estimated that the net impact of these changes would be a short-term reduction

[1] "VMS/EFD Pilot Successful: FRCS," FBC News (Dec. 19, 2017).

[2] 18(62) Government of Fiji Gazette (July 3, 2017), publishing regulation 28 of the Tax Administration (Electronic Fiscal Device) Regulations 2017 (hereinafter, the EFD regulation). *See also* Fiji Revenue & Customs Service (FRCS), "Notice of Extension and Phase 2 Group" (Dec. 27, 2017).

[3] 18(122) Government of Fiji Gazette (Dec. 22, 2017), publishing regulation 28 of the Tax Administration (Electronic Fiscal Device) Regulations 2017. *See also* "No Extension of Time Limits for VMS Implementation: FRCS," FBC News (Dec. 19, 2017).

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

in VAT revenues of FJD 87.4 million (about $40.66 million). However, in his 2016 budget speech (delivered November 6, 2015), Minister of Finance Aiyaz Sayed-Khaiyum assured Parliament that the VAT reforms would produce a long-term revenue gain of FJD 38.5 million. These are extremely difficult predictions to make and it appears that both estimates missed the mark. Short-term reductions were deeper, but long-term gains will most likely be greater.

According to the FRCS's "2016/17 Annual Report (August 1st to July 31st)," the actual short-term reduction in VAT revenues totaled about FJD 225.4 million. To meet 2016-2017 revenue projections, Fiji would need to collect 32 percent more VAT. VAT revenues were expected to be FJD 928.2 million. Actual collections were closer to FJD 702.8 million. This was a 22.6 percent improvement over 2015, but still far short of the revenue target — which was set well in advance of the rate reduction and the base expansion. Based on the available numbers, there appears to be an unexplained revenue loss of some FJD 138 million. The question becomes: What accounts for this shortfall?

The projection of short-term revenue losses was based on the fact that the rate reduction was universal and immediate, while the adoption of digital security measures was gradual. This tension could have been mitigated if Fiji had tied the rate reduction to the business groups adopting the technology — when grocery stores adopted the digital security measures, the rate for groceries could have dropped to 9 percent, while other rates remained at 15 percent.

Notably, the plans do not appear to account for all potential revenues. There is revenue yet to be realized — between FJD 214.5 million and FJD 217.35 million. First, roughly FJD 185 million (at a minimum) in revenue can be garnered from the full rollout of the technology reform. Second, revenue can also be increased by closing structural flaws in Fiji's VAT. This includes the inherent flaws that affect a residence-based VAT when dealing with cross-border trade in services and low-value goods. For Fiji, these flaws amount to an estimated loss of between FJD 29.5 million and FJD 32.35 million annually. Combining the unexplained shortfall with the projected long-term gain, Fiji will need over FJD 176.5 million to meet the promised long-term revenue gains. This is some FJD 37.9 million to FJD 40.8 million less than what we believe can be realized.

This article will focus on the mechanisms for the first of these (projected) increased revenue flows — that is, the potential benefits of successfully applying modern technology to Fiji's VAT. We will take a close look at how Fiji's system functions because this understanding is critical to fully appreciating why it can successfully prevent many common VAT frauds.

While this article will not focus on the potential revenue that might be gained by addressing structural problems in the VAT, we note that Fiji would be well advised to look to New Zealand and Australia on that front. Those countries have been actively working to reshape their own residence-based VATs to address the rapidly changing nature of world trade.

Overview and Rollout of the EFD Regs

Jurisdictions that have enhanced their existing transaction taxes — whether a VAT or retail sales tax — with a real-time security system that automatically encrypts and reports all transactions to the tax authority have seen significant increases in revenue as a result.

Ethiopia, for example, began its reform effort in Addis Ababa in February 2008. The reform mandated the use of certified electronic tax registers, also known as sales register machines. By today's standards, the technology is outdated and costly. However, by January 2013, electronic tax registers were in wide use in Ethiopia. A comparison of pre-transition (2005-2006) revenues with post-transition (2011-2012) revenues shows a total revenue increase of 42.3 percent — 20.4 percent from corporate tax and 21.9 percent from VAT. A 2014 study noted a sharp rise in VAT revenues in 2008 that coincided with the introduction of the electronic tax registers:

> The trend of indirect domestic tax revenue indicates clearly how VAT and turnover tax revenue collection has improved after the introduction of [electronic tax registers] in 2008/09.[4]

[4] Hamdu Kedir Mohammed and Zinash Degife Gela, "Challenges of Electronics Tax Register Machine (ETRS) to Businesses and Its Impact in Improving Tax Revenue," 5(3) *Int'l J. of Sci. Knowledge — Computing and Info. Techn.* 20 (July 2014).

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Similar stories of dramatic revenue improvement following the introduction of secure, real-time compliance systems can be found in the Czech Republic (100 percent), Rwanda (20 percent), and Croatia (42 percent).

When the electronic system is fully operational, the resulting revenue boost for the VAT alone is rarely less than 20 percent. At that rate — and, again, many nations see an even greater increase — a complete and successful rollout in Fiji could result in an increase in VAT revenues of approximately FJD 185 million.

In February 2015 Fiji published a technology tender based on a thorough study of global compliance systems in Asia and Europe. Fiji settled on the Belgian approach[5] — a blend of Germany's smart card and Sweden's control unit technology. After careful study and a visit to Belgium to observe its system in operation, Fiji's tax authority decided to move forward with its own regulations, planning to implement the policies in measured phases at roughly three-month intervals.[6] Initially called a VAT monitoring system (VMS), it became known as the electronic fiscal device (EFD) system when officials realized that it could also be used to monitor compliance with other taxes.

The pace of Fiji's program has understandably led to more muted revenue improvements; increases will be gradual, not immediate. Although there is no published overall timetable for rollout, it appears that the FRCS will treat each group of businesses in a similar manner, affording each group the same amount of time and devoting the same level of government resources to ensure a smooth transition.

There is a built-in flexibility and a clear learning path for the FRCS. This is evident in an announcement made by the FRCS during the rollout of EFDs to the first group:

> For the first phase, the supermarket and pharmacy sectors will be required to implement an EFD. We estimate that it will take between 1 to 3 months for sectors to comply. However, phase 1 is given 6 months because this is the first round of implementation process and it will take some time for nominated stakeholders to adjust.[7]

Broadly, the EFD regulations envision a business-government digital partnership that will produce "an electronic system that transmits, receives, records, analyses, formats, stores and monitors fiscal data." The partnership includes TaxCore (the tax authority's system) and the mandatory EFDs (the part of the system used by taxpayers as they conduct business). As we will demonstrate, the system is built specifically to fight common forms of VAT fraud.

The Electronic Fiscal Device

From the taxpayer's perspective, the central tool used in Fiji's program is the EFD. As noted above, while the FRCS initially referred to the project as a VMS, it soon became clear that the system could do much more: The underlying transactions include other taxes that can be digitally recorded along with VAT such as the service turnover tax, the environmental levy, and (occasionally) the stamp duty.[8]

Although the name appears to describe a specific physical product, an EFD is actually a system, not a single device. An EFD has two parts, either or both of which may be entirely software-based:

- a POS system or, more generally, an accredited invoice system; and
- a sales data controller (SDC) with a secure element.

The POS System

A POS system is one specific application on an accredited invoice system, which is an umbrella term for devices and systems that can produce receipts (normally issued in B2C transactions) and invoices (normally issued in B2B transactions). While all POS systems perform the same basic

[5] For a discussion (in French) of the Belgian precursor system as currently in use, see Belgian Federal Public Service Finance, "Le Système de Caisse Enregistreuse."

[6] *See, e.g.*, FRCS, "Step by Step Instructions on the Road to Fiscalization (VMS/EFD)."

[7] FRCS, "VMS FAQs."

[8] A similar confluence of taxes, recordkeeping, and enforcement can be seen in the VATs adopted within the Gulf Community Council. *See, e.g.*, Richard T. Ainsworth and Musaad Alwohaibi, "The First Real-Time Blockchain VAT: GCC Solves MTIC Fraud," *Tax Notes Int'l*, May 22, 2017, p. 695.

For more *Tax Notes International* content, please visit www.taxnotes.com.

functions of a traditional cash register, including issuing receipts, modern POS systems are much more complicated than basic electronic cash registers. They typically include a computer, monitor, cash drawer, receipt printer, customer display, and bar code scanner along with a debit/credit card reader.

More specifically, Fiji's EFD regulation defines a POS as follows:

> "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.

The POS in the EFD must be accredited. Schedule 1 of the EFD regulation provides accreditation guidelines. An accredited POS must be able to connect with an accredited SDC and be able to issue a fiscal invoice. Essentially, the regulation takes a wide (market) view of accreditation, recognizing that the POS market is both diverse and dynamic[9] and that the government needs to work with the market as a regulator of the outcomes, not as an advocate of a one-size-fits-all POS system. The regulation states:

> 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 fiscalization, the Authority is dedicated to providing detailed integration instructions for all manufacturers and software developers (suppliers).

Schedule 1 of the EFD regulation identifies two ways to produce a fiscal receipt using an accredited POS. One uses an external SDC (E-SDC). This non-internet, semi-connected scenario can involve either a hardware or software solution. The other — an internet-connected scenario — is a software solution that uses a virtual SDC (V-SDC). Based on how the taxpayer's business is set up and how it connects with the outside world, the taxpayer must choose between using a POS plus E-SDC or using a POS plus V-SDC. Regardless of this choice, the EFD must satisfy the specified compliance outcomes.

To help the market achieve these goals and ensure compliant systems are available for taxpayer use, the regulation tasks the FRCS with creating a development environment that is accessible to all software developers that want to produce an accredited POS or accredited E-SDC components. By registering on the FRCS webpage, a developer can receive test certificates, technical documentation, and a user manual.

Fiji's EFD system is built on top of the public key infrastructure system and uses a certificate authority, which is a significant improvement over systems that rely on hardware vendor manufacturers to provide security. The public key infrastructure allows for mutual authentication of the taxpayer and tax authority, prevents the repudiation of digital signatures, and ensures data transport security and invoice integrity. The FRCS acts as a registration authority, verifying identity information before issuing digital certificates to taxpayers.

Ultimately, the EFD's goal is to create a fully compliant fiscal invoice. A fiscal invoice includes two data-intensive parts:

- an invoice request sent by an accredited POS to an E-SDC or V-SDC; and
- an invoice response that is generated by the E-SDC or V-SDC.

To be fully compliant, both the request and the response must include specific pieces of data listed in section 12 of the EFD regulation.

[9] For example, the POS systems used in legalized marijuana dispensaries in the United States are unique. Mark Goldfogel constructed the first marijuana-specific POS. *See* Goldfogel, "The Ugly Truth About POS in the Cannabis Industry," Cannabis Business Executive — Cannabis and Marijuana Industry News (Apr. 7, 2015). Also, see the five-part series by Ainsworth and Brendan Magauran, "Taxing and Zapping Marijuana: Blockchain Compliance and Trump," in *State Tax Notes*, Apr. 16, 2018, p. 241 (Part 1); *State Tax Notes*, Apr. 30, 2018, p. 419 (Part 2); *State Tax Notes*, June 18, 2018, p. 1213 (Part 3); *State Tax Notes*, July 2, 2018, p. 39 (Part 4); and *State Tax Notes*, July 9, 2018, p. 157 (Part 5).

For more *Tax Notes International* content, please visit www.taxnotes.com.

The invoice request (from the POS) must include:

- the type of receipt;
- the type of transaction;
- the method of payment;
- the name of or other unique identifier of the cashier;
- the name or unit code of each good or service supplied;
- the unit price and quantity of each good or service supplied;
- the total price of the goods or services supplied;
- the taxes that are part of the invoice and the tax rates applied;
- the total amount payable by the customer; and
- if the customer is a taxpayer, the customer's taxpayer identification number.

The invoice response (issued by the SDC) must include:

- the name and TIN of the business, and the identification of the business premises where the transaction occurred;
- the date and time when the receipt is issued;
- the sequential serial number of the receipt;
- the serial number for the digital certificate of the business's EFD; and
- the digital signature and internal data of the EFD.

Internal data, which only the authority can read, refers to the fiscal data — a system of counters described below — in encrypted form.

The EFD regulation also lists five types of receipts that an accredited POS must be able to issue when connected to an accredited SDC: normal receipts; refund receipts; copy receipts; training or pro forma receipts; and normal or refund receipts for B2B transactions. It sets out the steps for each type and the expected results of testing.

The Sales Data Controller

The SDC is the second part of the EFD. As indicated above, there are both hardware (E-SDC) and software (V-SDC) versions. Accreditation is not an issue for the V-SDC since it is under the authority's control. Accreditation is, however, critical for E-SDCs. In this context, accreditation requires that the E-SDC can integrate fully with the authority's system. Only accredited suppliers may provide taxpayers with an E-SDC, and the specific E-SDC must be properly accredited before it can be sold at retail in Fiji. The EFD regulation states that neither unaccredited SDCs nor unaccredited POSs may be sold in Fiji. Businesses cannot operate without an accredited POS and SDC.

Why allow E-SDCs? Access to the V-SDC is internet-dependent. The V-SDC option is typically simpler for the taxpayer, but if the internet is unreliable — or wholly unavailable — then an E-SDC offers another way to connect the taxpayer's POS with the tax authority's system. The difficulty with E-SDCs is that they move a secure function out from under the protection of the authority's firewall. Thus, the tax authority must be sure their operations remain fully secure and that data cannot be compromised or manipulated. The EFD regulations use the term "secure element" to describe this protection. Safeguarding the secure element is a major concern for E-SDCs and part of what makes the E-SDC option more complicated than the V-SDC option.

The Secure Element

The tax authority provides the secure element to an accredited E-SDC on a smart card designed to prevent tampering and the unauthorized use of the fiscal data that the taxpayer will transmit to the authority using the card. The smart card that implements the secure element contains a digital certificate and a special applet (that is, a small application).

The Invoice Process

Like the technology behind Fiji's entire digital system, the invoice process is specifically crafted to prevent common forms of VAT fraud.

Procedurally, the first step in generating a digital invoice using an E-SDC is for the accredited POS to generate a receipt using the transaction data entered by the operator.

Next, the transaction data are sent to the E-SDC, which verifies its format and the tax information, date, time, and a PIN or password for the digital certificate. The digital certificate:

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

- reproduces the taxpayer's digital signature to be recorded on the fiscal invoice that the taxpayer issues to the customer;
- reproduces the taxpayer's protected password or PIN and securely delivers it to the authority so that the EFD can link to the authority's system and securely transmit the fiscal data; and
- records the date on which the data are transmitted to the authority's system.

Third, the data are sent to the secure element for fiscalization — the process by which the transactional data become fiscal data. As the EFD regulation explains in section 5(d), the transformation of transaction data into fiscal data and a fiscal invoice is instant:

> 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. [Emphasis added.]

The fourth step is for the secure element to verify that all numbers are positive. It then recalculates the internal data, encrypts the data with the authority's public key, and signs the receipt.

The fifth and final step is for the SDC to transmit a fiscal invoice back to the POS, permanently preserving the transactional and fiscal data while simultaneously transmitting the fiscal data to the authority. The transmission may be delayed until there is a communication opportunity, whether through a revived internet connection, another communication medium, or even manually through the delivery of a memory stick to the FRCS.

The customer at the POS terminal where the initial data entry occurs will not see much of a difference in terms of timing compared with a normal transaction at a stand-alone register. The visible difference is that a scannable QR Code will appear on the printed receipt. This code will allow the customer to match the data on the receipt with the record of the transaction on the authority's system. The availability of instantaneous verification does not depend on the type of SDC employed. The customer can always — and immediately — scan the QR Code on the receipt and confirm the transaction with TaxCore, the tax authority's system. The customer might scan a receipt and thereby send data to TaxCore before an E-SDC transmits them (because of an unreliable internet connection or other issue), but verification is assured with a valid QR Code.

The following figures illustrate the difference between using an E-SDC and a V-SDC.

Illustrating the Process: Using a V-SDC

Figures 1 and 2 show an EFD that includes an accredited POS and V-SDC. They show the entire process: the transaction data being entered into an accredited POS; the data passing to the secure element (within the authority's system); fiscalization; and the data returning to the customer in the form of a fiscal invoice, complete with a QR Code that allows for instant verification of the transaction.

Figure 1 starts with an accredited POS. The POS manufacturer has already followed the technical instructions for POS and cash register developers and received accreditation. The taxpayer must register to receive a digital certificate and POS access code. Notably, the FRCS offers a free POS option for small and medium-size enterprises that is:

> designed to resolve the need for a minimally functional mobile POS solution required in retail stores, and where the necessity to satisfy compliance and a customer convenience is of the utmost importance. This provision allows a retailer to have an accredited EFD *free of charge* or [a] substitute EFD in case[s] [where the] primary EFD fails. EFD regulation recognizes no exemption from issuance of digital fiscal receipt, thus taxpayers are advised to have [the] *free POS option* as a backup.[10] [Emphasis added.]

The taxpayer enrolls by activating an administrative card that allows him to use the taxpayer access point, through which he can

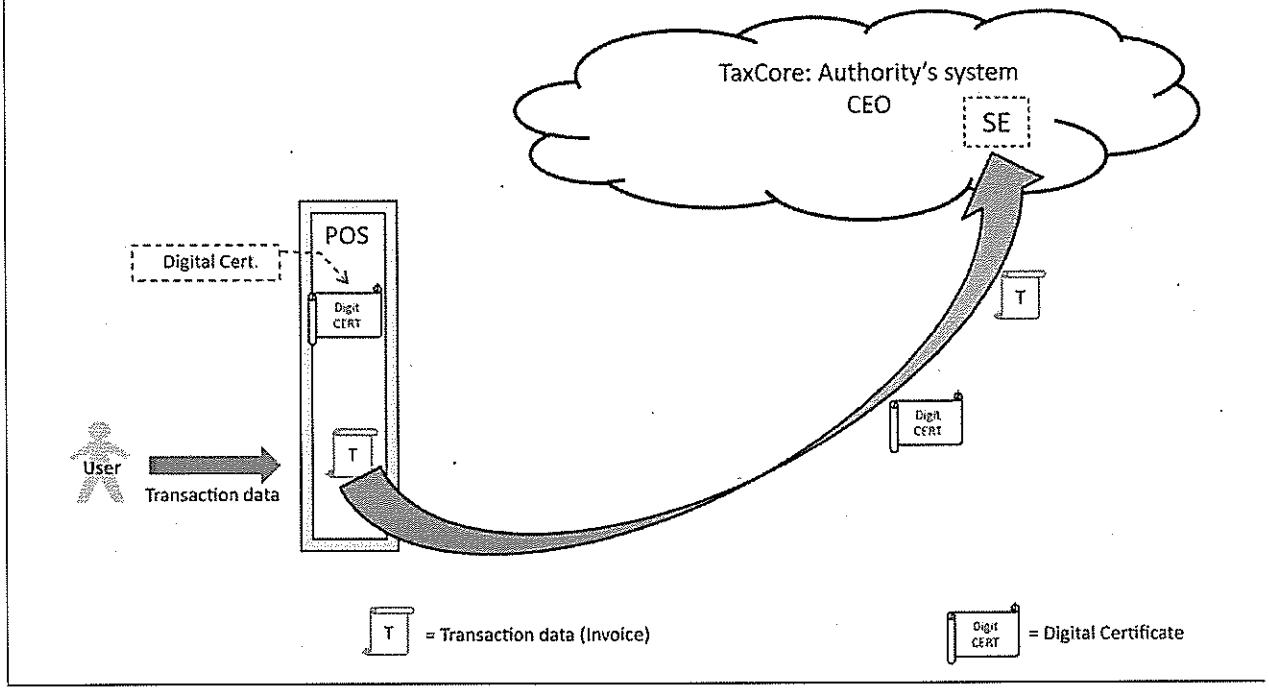
[10] FRCS, "FRCS Free POS Installation and User Manual iOS 11 (11.3.0)" (May 15, 2018). Both the user manual and a related YouTube video explain how to use the product. *See* Fiji Revenue and Customs Marketing, "FRCS Free POS for iOS Installation Guide" (June 5, 2018).

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Figure 1. Request for Fiscal Invoice (Accredited POS With V-SDC)



delegate certificates to himself.[11] An enrollment officer at the FRCS oversees the granting of digital certificates and smart e-cards. The taxpayer who files the electronic request receives identification numbers and POS access codes that only he knows.

The initial data entry process — which occurs when an authorized user accesses the POS terminal to make a sale — produces a transaction data invoice. This pro forma invoice includes the substantive data that will be included in the request for a fiscal invoice.

The Request — Figure 1

The request is an automatic process. Immediately after the POS has assembled the transaction data — which can come from a range of sources including a standard POS, a mobile POS app, a cashier using a computer, or an online shopping forum — the accredited POS makes a direct internet-based request for fiscalization using an associated V-SDC residing within the authority.

EFD regulation section 12(2)(a)-(j) spells out the required data elements in the request. The POS sends the data elements, the POS's digital certificate, and the POS access code to the secure element. The secure element verifies and identifies the caller — that is, the taxpayer using the POS. The V-SDC has an accompanying digital certificate that verifies its identity.

The Response — Figure 2

The secure element confirms the validity of the request and associates the transactional data with the elements required by EFD regulation section 12(2)(k)-(o). It also provides a digital signature and the verification URL through which the POS can generate a QR Code. The result is the fiscal invoice. The customer can scan the QR Code to confirm that the authority has recorded the invoice data.

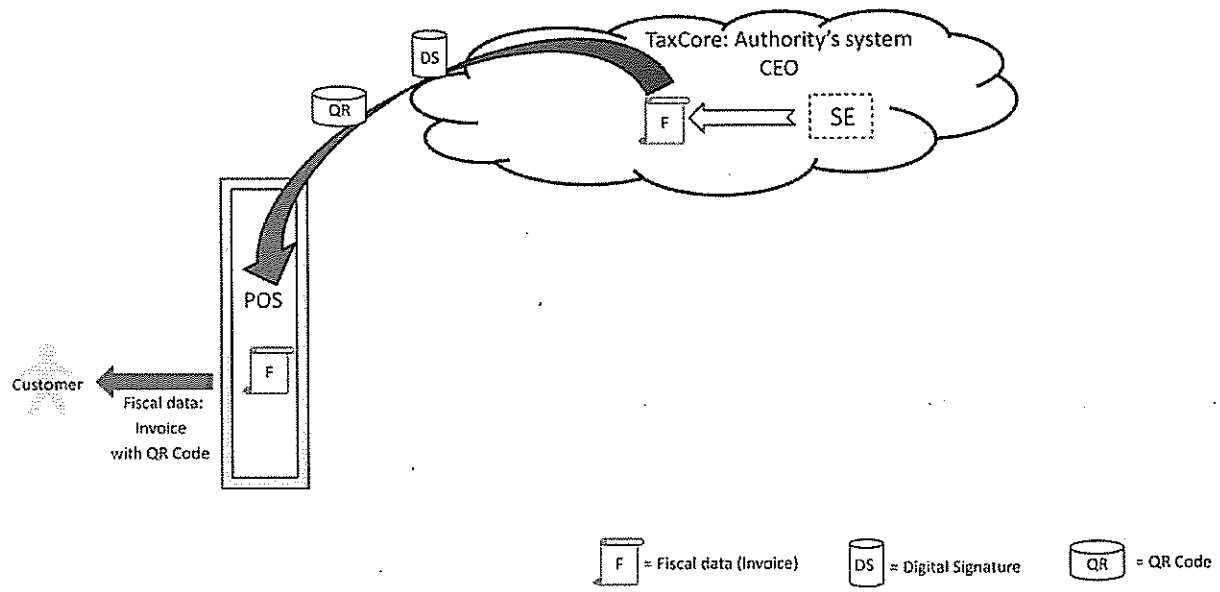
Illustrating the Process: Using an E-SDC

Performing the same invoice fiscalization process using an E-SDC is more complicated, so the FRCS encourages taxpayers to use the V-SDC

[11] "Step by Step Instructions," *supra* note 6, explains the six administrative steps that a taxpayer must take to enroll and secure both smart cards and digital certificates. The FRCS also provides the "Taxpayer Portal User Manual (Version 1.4)," which explains the actual invoicing process.

For more *Tax Notes International* content, please visit www.taxnotes.com.

Figure 2. Response to Request for Fiscal Invoice (Accredited POS With V-SDC)



whenever possible.[12] An accredited POS can use either an E-SDC or a V-SDC. Typically, the supplier sets the POS to use one of the systems. However, a supplier could also set it to toggle back and forth between the two, favoring the V-SDC unless the internet is unavailable.

Figures 3, 4, and 5 chart the fiscalization pathway with an E-SDC. Figure 3 illustrates the first two steps: (a) integrating an accredited POS with an accredited E-SDC; and (b) securing and installing the secure element in the E-SDC. Schedules 1 and 2 of the EFD regulation provide technical guidelines for accrediting POSs and E-SDCs, with additional specifications included in the technical instructions. Usually, if a taxpayer purchases a POS and E-SDC in Fiji, the manufacturer will have satisfied the accreditation steps. The taxpayer will only need to assemble the parts and select a password so that the POS and the E-SDC will recognize each other during data transfers and communications.

As Schedule 2, section 3.1 explains, the next step is for the taxpayer to receive the secure element (stored on a smart card) from the authority and install it in the E-SDC. The EFD regulations define a secure element as:

> the software and hardware used by an EFD and the Authority to prevent tampering and unauthorized use of fiscal data transmitted to the Authority's system and to maintain the integrity of the fiscal data.

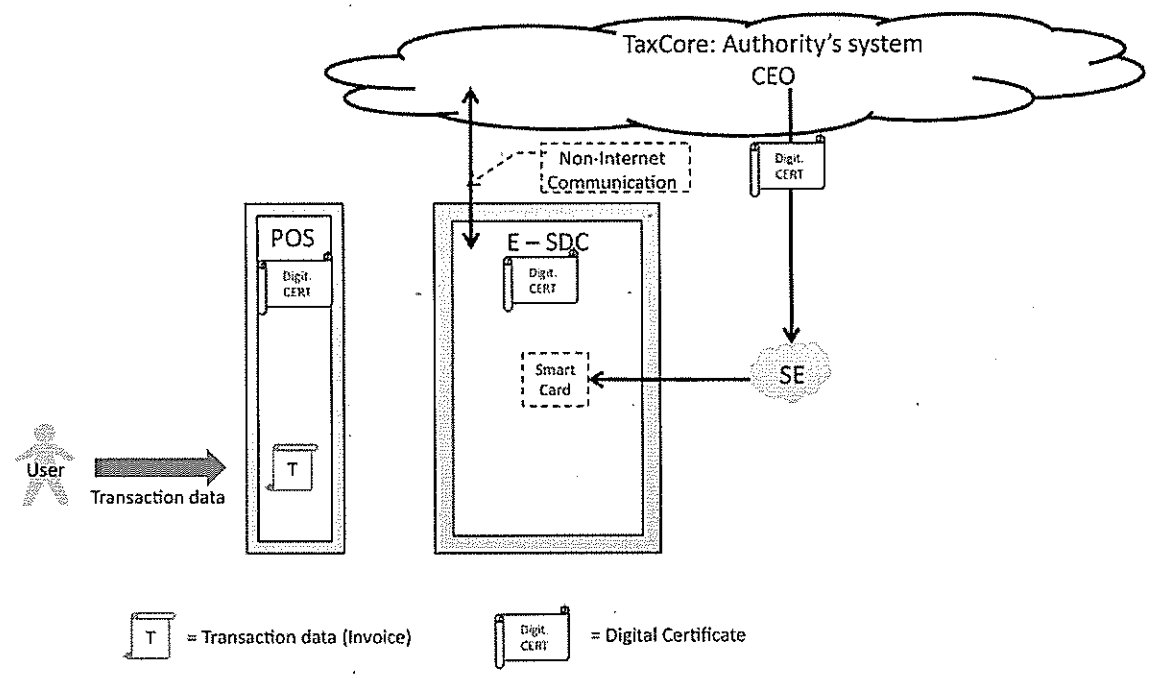
The secure element allows the authority to own and control the security on each E-SDC — much like they do with the V-SDCs that reside within the authority's firewalls — and to exercise this control independently from the POS or E-SDC vendor. After receiving a request for fiscalization from a taxpayer who recently purchased an accredited POS and E-SDC, the authority validates the information and sends the taxpayer an invitation to enroll.[13] The taxpayer selects a PIN, which is recorded in the system. The authority then produces a secure element and places it on a smart card. The authority sends a notification to the taxpayer that the application has been approved and the smart card (secure element) is available for pick up at an FRCS

[12] FRCS, "Technical Instructions for POS and Cash Register Developers (Version 2.3)" (Apr. 2018).

[13] *See* FRCS, "Step by Step Instructions," *supra* note 6.

For more *Tax Notes International* content, please visit www.taxnotes.com.

Figure 3. Setting Up an E-SDC for an EFD



location. After obtaining the card, the taxpayer slots it into a reader connected to the computer and uses a web browser to access the TaxCore administration portal. The login page will ask for the user's PIN and read the user's credentials from the smart card.

Figure 4 shows the same request for fiscalization of transaction data as Figure 1 does, except the request is presented to the secure element within the E-SDC instead of the V-SDC within the authority's system. The E-SDC is needed because the internet is not always available. The secure element is designed to replicate the functions of the authority's system after the E-SDC prepares the transactional data for signing.

Except for the proof of audit function — a topic considered separately below because of its importance to Fiji's system and the system's ability to prevent fraud — Figure 5 is the final diagram that presents the E-SDC. Although both chart the response to the request for a fiscal invoice, Figure 5 is far more complex than Figure 2.

When the secure element in an E-SDC fiscalizes the transaction data from the POS (a process detailed in Schedule 2, section 2 of the EFD regulation), it verifies the amounts and calculations, signs, and encrypts the file for two purposes (described in Schedule 1):

- to prepare the file for transmission back to the POS, which will issue a fiscal receipt with a QR Code for the customer; and
- to prepare it for transmission to the authority's system when the internet connection is restored or using an alternate transmission mechanism, which can involve manual delivery of the data to an FRCS office.

The secure element will retain fiscal data on location until it transfers the fiscal data and receives a notification from the authority's system that the transfer is complete.

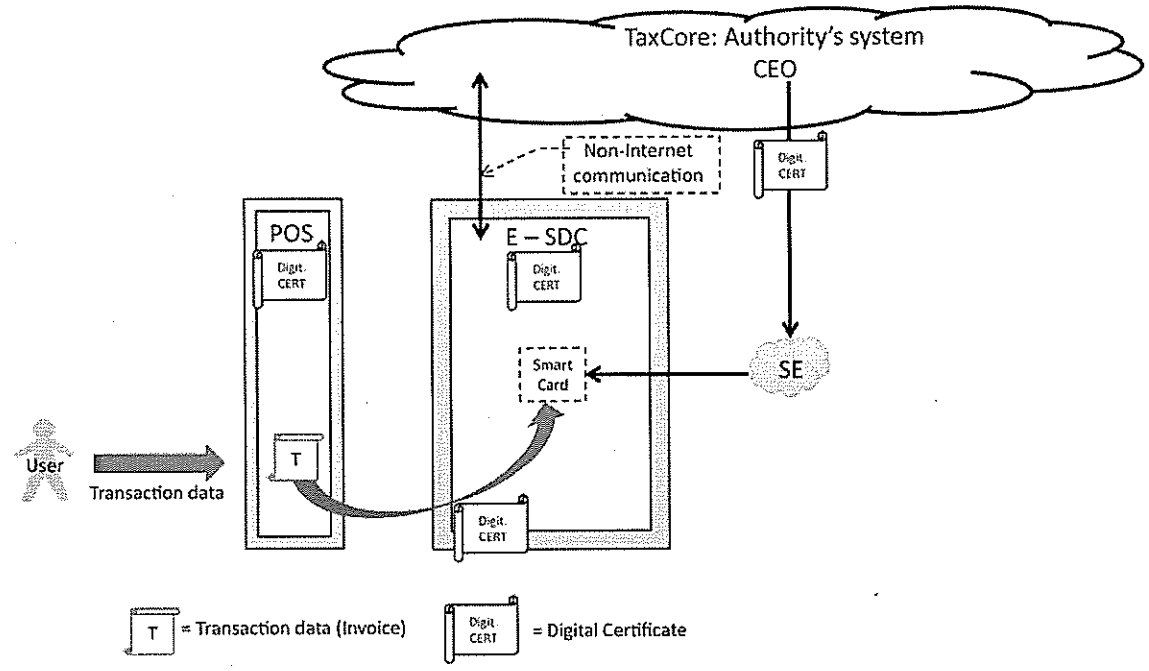
The Proof of Audit Function

Proof of audit[14] is not only the most unique aspect of Fiji's VAT Monitoring System, it is the most creative and important aspect. Data Tech

[14] FRCS, "Technical Instructions for E-SDC Developers (Version 2.3)" (Apr. 2018).

For more *Tax Notes International* content, please visit www.taxnotes.com.

Figure 4. Request for Fiscal Invoice (Accredited POS With E-SDC)



International designed and developed the proof of audit system for the FRCS. Proof of audit is a risk analysis template that is simpler to use than artificial intelligence, achieves more granular results, and provides real-time solutions to attempted tax fraud. Proof of audit uses automatic counters built into each fiscal invoice by processes in TaxCore and the secure element. The counters identify fraud attempts before they are established and automatically stop standard frauds before they begin. This is a unique attribute of the Fiji VAT — an element that is sure to be emulated.

To fully understand proof of audit in the context of Fiji's technology-intensive VMS, at least one term needs defining — or, more accurately, redefining — and the proof of audit processes need to be set out. The term, which is not given an accountant's definition, is "audit." According to a technical manual published by the FRCS:

> An audit is a process of *sequentially* transferring *audit packages* from an E-SDC (or an SDC) to the Tax Authority's system [TaxCore] and handling the *response* generated . . . for the specific device.[15] [Emphasis added.]

This definition is cast in terms of technology: The SDC makes a request (accomplished through the sequential transfer of audit packages) and TaxCore generates a response. The vehicle for the proof of audit is the audit package generated by the SDC. An audit, therefore, is the process by which the data in the technology devices at the business location are fully replicated in — and thus proven to be in sync with — TaxCore. It is the technological equivalent of sending a human auditor from the tax administration to the taxpayer's place of business to confirm every line item on an invoice, repeating this process for every invoice produced by the taxpayer, and then recording the results in a sequential record that replicates the original transactions.

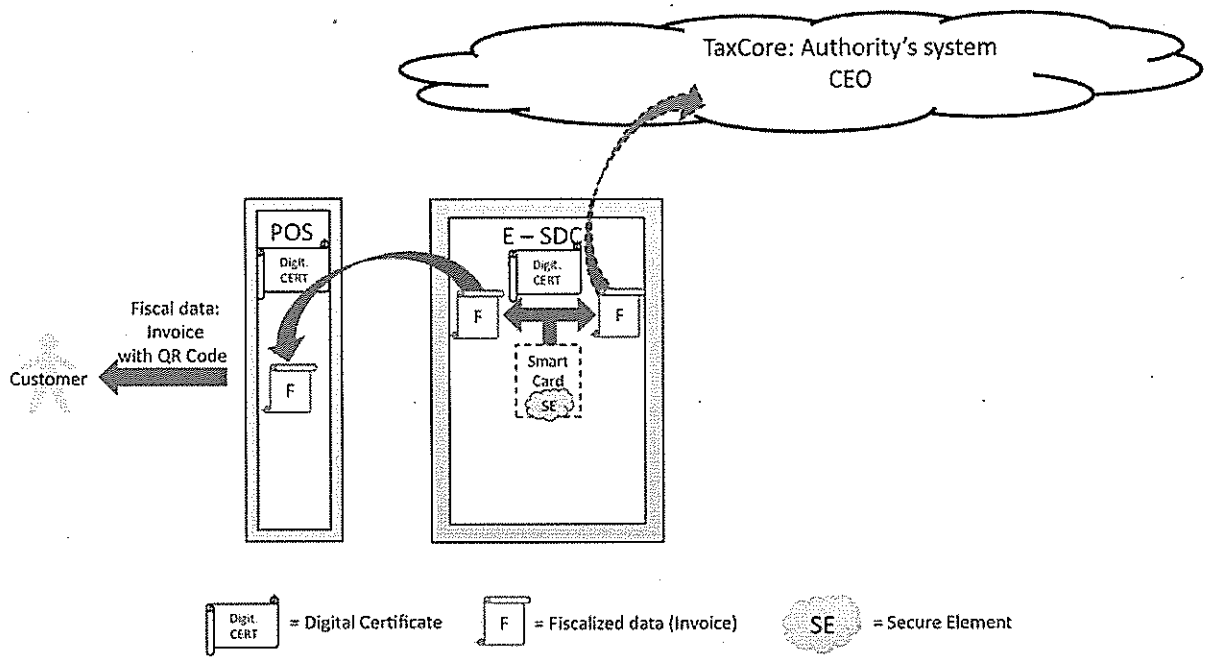
A second definition is also useful and similarly context-specific. According to the manual, a proof of audit "is a confirmation generated by a Tax Service System once all

[15] *Id.* at 37.

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Figure 5. Response to Request for Fiscal Invoice (Accredited POS With E-SDC)



expected audit packages have been received from an E-SDC." The audit package consists of the receipts or invoices that are assembled for a single proof of audit as they pass through the taxpayer's POS.

When is an EFD ready to engage in a proof of audit? The answer, found in the same technical manual, is surprisingly simple:

> Once an invoice is created (Invoice Fiscalization Request and Invoice Fiscalization Result) the E-SDC is ready to create an audit package and store it in the non-volatile memory.

Thus, proof of audit can go forward with just one invoice.

The FRCS goes into much more detail, setting out the 11-step process for creating an audit package. Notably, these steps — posed in technological terms — are essentially the same as the steps for creating a fiscal invoice recorded in Figure 5. Essentially, the audit is a secure digital conversation involving three machines — the SDC, TaxCore, and the secure element. The full audit involves the sequential confirmation that all the data that the taxpayer entered into the POS are precisely the same data that reside in TaxCore — no changes, no omissions, and no manipulations.[16]

Ultimately, the proof of audit provides a real-time confirmation of transactional data accuracy, preserved and validated in the sequence it was created.

What triggers an audit? Because we are dealing with machines, not people, and because we are conducting a complete, line-by-line audit of all transactions, not a partial sampling of suspect transactions, the audit can be — and needs to be — preprogrammed and nearly simultaneous with the execution of the underlying transactions. If a proof of audit cannot be completed, no subsequent proof of audit can occur until the errors are corrected. The system triggers a proof of audit:

- every five minutes;
- whenever a fiscal invoice is completed;
- on the tax authority's demand; and
- on the taxpayer's demand.

[16] A detailed, technical explanation of the process for creating the audit package and the steps in the multi-system audit conversation are available in "Technical Instructions for E-SDC Developers." *Id.*

For more *Tax Notes International* content, please visit www.taxnotes.com.

The incentive for a taxpayer to request an audit from the tax authority is not immediately apparent. Another special feature of Fiji's VMS — counters — helps provide this incentive.

Counters

Counters count the tax attributes on each invoice sequentially as the attributes are placed on invoices. The QR codes on invoices contain the results of the counting function. Counting is non-discretionary — that is, counters cannot be turned off. Counters can be adjusted and the cap on each counter can be changed, but only the tax authority can do that.

Each counter has a customized cap. When the secure element in an E-SDC or V-SDC recognizes that a particular counter is getting close to its cap, the secure element notifies the operator that it will shut down unless it receives a proof of audit notification from TaxCore. This may happen if a business has been offline and normal remote audits (with accompanying proof of audit notifications) have not occurred. To prevent shutdown, the taxpayer may need to use a secure phone line or manually take the records to the tax authority using a memory card or memory stick. Only a proof of audit can reset the counters to zero and prevent the secure element from going to sleep and leaving the taxpayer unable to issue fiscal invoices.

Because Fiji's VMS employs both V-SDC and E-SDC devices, proof of audit and the counter structure can appear complex. There is an EFD counter assigned to the secure element for each E-SDC and V-SDC. This counter records the signed receipts that the POS issues, counts them sequentially, and subdivides the count by type of receipt. Types of receipts include normal sales, normal refund, copy sales, copy refund, training sales, training refund, and pro forma sales. There are also secure element counters that record cumulative line item totals. They record information like cumulative turnover, total tax, refund totals, per tax refund totals, and more.

Figure 6 contrasts an EFD structure using an E-SDC with an EFD structure using a V-SDC. For simplicity, the example assumes there are only four business taxpayers — (a), (b), (c), and (d) — using four systems — POS(a), POS(b), POS(c), and POS(d). Business (a) uses an E-SDC. Businesses (c) and (d) use a V-SDC that is housed within the authority's system. Business (b) switches from an E-SDC to a V-SDC after the first six invoices, illustrated by the invoices labeled 1E through 6E and 1V through 4V.

The authority's system has direct, immediate control over the invoice data for businesses (c) and (d), but indirect control over the invoice data when businesses (a) and (b) use E-SDCs. Figure 6 shows a simple one-to-one transmission from POS(c) and POS(d) to the V-SDC that is housed within the authority's system. When transaction data are forwarded to the V-SDC, TaxCore checks, encrypts, and retains the data sequentially. Counters apply immediately. Fiji currently has three V-SDCs operating 24/7 to ensure that the FRCS can respond to any request for a fiscal receipt in under one second. Proof of audit can be immediate, almost real-time, with a V-SDC.

It is a different story with POS(a) and POS(b). They are using E-SDCs, which the authority's system cannot control in real time. To allow the taxpayers to issue a valid fiscal receipt with a QR Code to customers in less than a second, the data must be checked, encrypted, and securely stored on location using the secure element and then transmitted to the authority's system later. This delay is an inherent security risk, but technology mitigates that risk. Under Fiji's system, each transaction shows the gap between the last successful transaction and the current one.

The timing difference in receiving audit data from the E-SDCs and V-SDCs will likely result in the fiscal invoices 1V, 2V, 3V, and 4V issued by POS(b) arriving at TaxCore before some of the earlier issued fiscal invoices by POS(b) numbered 1E, 2E, 3E, 4E, 5E, or 6E. Nonetheless, TaxCore will align and save the invoices in sequential order by issue date. The secure element assigns each invoice a unique number containing its ordinal position. Thus, even if something is amiss and the date and time are recorded wrong, the VMS can still reproduce the correct invoice order.

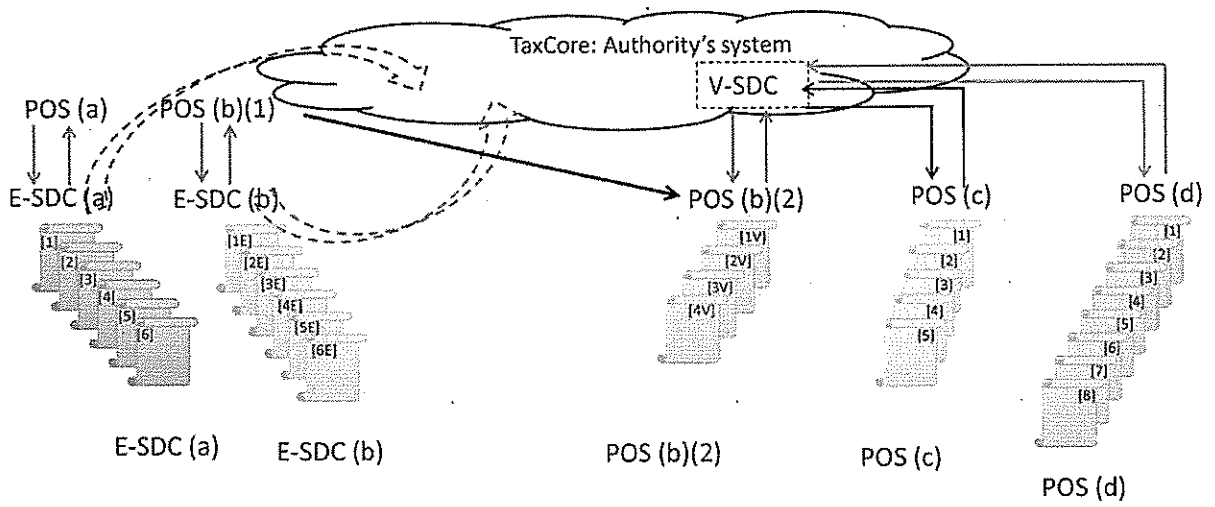
One of the main reasons for the extensive use of counters in Fiji's VMS is to close the risk gap caused by the inherent delay in TaxCore's receipt of invoices from various E-SDCs and V-SDCs. The FRCS can adjust the caps on the counters on a case-by-case basis determined on individual risk analysis estimates.

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Figure 6. Comparison of EFD Counters With E-SDC and V-SDC



Each digital certificate that requests a digital signature on the fiscal invoice has a unique identifier that, combined with unique identifier for the secure element that signs the invoice. Set off in sequential pairs — that is, the identification number for the requesting certificate paired with the identifier for the signing element — and accompanied by the count, they provide a unique identifier for the invoices themselves. When using the E-SDC, the "requested by" and the "signed by" identifiers match because the same secure element is performing both tasks. However, when the V-SDC is used, the "signed by" identifier is different.

Invoices and the Audit Function

To better illustrate the audit function, the structure in Figure 6 needs to be a little more granular. Figure 7 provides a breakdown of some of the tax data collected on each invoice for business (a). There is a digital signature that verifies the accuracy of the data that appear on each document. Each invoice can be called up and checked as needed. These are fiscal invoices containing QR codes.

The first invoice is a normal sale invoice. The system designates it as the first transaction from E-SDC(a) and the first normal sale in the sequence (TR: 1/1 NS). A second normal sale (TR: 2/2 NS) and a third normal sale (TR: 3/3 NS) follow. Internal data indicate that the invoice amounts for these three sales were 100, 20, and 230. The total sales counter shows running totals of 100, 120, and 350. Assuming a 10 percent VAT, the VAT counter does the same: It shows that the VAT collected on each invoice is 10, 2, and 23; the running VAT totals show 10, 12, and 35.

The fourth invoice is for a normal refund of 20, including a return of VAT for 2. It is the first normal refund and the fourth invoice in this sequence (TR: 1/4 NR). The counters show an aggregate collected VAT of 35 (no change), VAT refunded of 2 (new data), total normal sales of 350 (no change), and total normal returns of 20 (new data). Importantly, all of the counters are positive and the counters do not combine the total VAT collected (35) and total VAT refunded (2) to get a net of 33. Each amount is kept separate.

The fifth invoice (TR: 1/5 TS) is a sales training invoice. Once again there is no impact to the aggregate VAT (35) or total sales (350). However, there are new records for total training sales (200) and total training VAT (20) recorded.

Finally, the sixth invoice records a fourth normal sale transaction (TR: 4/6 NS). The sale is for 1,000 with VAT of 100. This increases the aggregate sales counters to 1,350 and the aggregate VAT to 135.

The same process occurs for every invoice that is sent for fiscalization for the entire Fiji VMS.

For more *Tax Notes International* content, please visit www.taxnotes.com.

Ultimately, that should be every business and every transaction in Fiji. Currently, it is limited by the rollout process. Fiscalization takes less than a second for each invoice. It is comprehensive and thorough.

Fighting Common VAT Frauds

To help readers fully appreciate the importance of the innovations in Fiji, this section will consider some standard VAT fraud schemes and look at how Fiji's VMS responds. The importance of proof of audit and the central role of the counters in defeating fraud are both evident and notable.

Common VAT Fraud Schemes

The following schemes are common in VAT jurisdictions around the world — but they will not succeed under Fiji's VMS:

- Fraud 1 (zappers) — A retail business issues accurate paper receipts with a POS. Later, the fraudster inserts a transaction-deleting program on a memory stick into the POS, deleting either entire records or specific items from some transactions.[17]
- Fraud 2 (phantomware) — A retail business issues accurate paper receipts with a POS. Later, the fraudster accesses a hidden program in the POS and deletes either the entire record or line items on a record for specific transactions.[18]
- Fraud 3 — A business issues one valid receipt early in the business day for a commonly purchased item, such as a large cheese pizza (B2C context) or commercial building supplies (B2B context). The fraudster photocopies the receipt and uses these copies throughout the day instead of issuing a new receipt or invoice when this item is sold. Customers assume the receipt is valid, but the business does not report the transaction.[19]
- Fraud 4 — A fraudster either manufactures false invoices with an accredited POS and E-SDC stolen from a legitimate business or steals valid invoices. The fraudster sells the invoices to businesses seeking additional VAT deductions.[20]
- Fraud 5 — The fraudster switches an accredited POS in and out of training mode, even though all transactions are normal business exchanges. The taxpayer keeps the tax he collects on these "training" sales for himself.[21]

Traditionally, the response to VAT avoidance is an audit. In Fiji, it is no different. However, Fiji's audit response is fully automated and close to real time. The proof of audit function makes this possible.

How Fiji's VMS Prevents Fraud

Fraud Schemes 1 and 2

Zappers and phantomware are both electronic sales suppression devices. The only difference is that a zapper is stored externally (that is, apart from the POS), while phantomware is stored internally (embedded in the POS). Both use specially designed programs to alter the internal records of the POS after sales transactions are completed.

[17] On Aug. 30, 2017, a plea was entered in *State of Washington v. Wong*, No. 16-1-00179-0 (Wash. Super. Ct. 2017), a case involving the possession and use of a zapper. In a companion case, a salesman pleaded guilty to selling zapper software and agreed to pay $3,445,589 in restitution. *United States v. John Yin*, Case 2:16-cr-00314-RAJ (W.D. Wash. 2017).

[18] *See The Grande Café Dudok*, District Court of Rotterdam, LJN: AX6802 (June 2, 2006) (in Dutch, translation on file with author); judgment affirmed by the District Court of The Hague, LJN: BC5500 (Feb. 29, 2008) (in Dutch, translation with author).

[19] The pizza example is from Dave Bergeron, deputy director general of the Ministry of Revenue Quebec. *See* email from Bergeron (June 6, 2008) (on file with author). *See also* Ainsworth and Bergeron, "Zappers (Automated Sales Suppression)," New York Prosecutors Training Institute (July 31, 2008) (unpublished presentation on file with authors).

[20] China's Golden Tax Project implemented a rudimentary digital security system. For a case involving a stolen POS and security system, see *Nanjing Shuangchao Trade Co. Ltd. v. Xuanwu District State Tax Bureau, Nanjing Municipality* (Judgment of the First Instance, Xuanwu District People's Court, Nanjing Municipality, Jiangsu Province (2005) Xuan Xing Chu Zi No. 70). For a case involving the misuse of (possible stolen) invoices from a certified POS with Golden Tax Project security systems in place, see *Inspection Bureau of Zhanjiang Municipal State Tax Bureau v. Shengjie Trading Co. Ltd., Zhanjiang Development Zone* (2012) in the Intermediate People's Court of Zhanjiang Municipality, Guangdong Province (2012) Zhan Zhong Fa Xing Zhong Zi No. 112 (Sept. 13, 2012). *See also* Alan Schenk, Victor Thuronyi, and Wei Cui, "Denial of Input Credit for 'Sham' Invoices," in *Value Added Tax — A Comparative Approach* (2015).

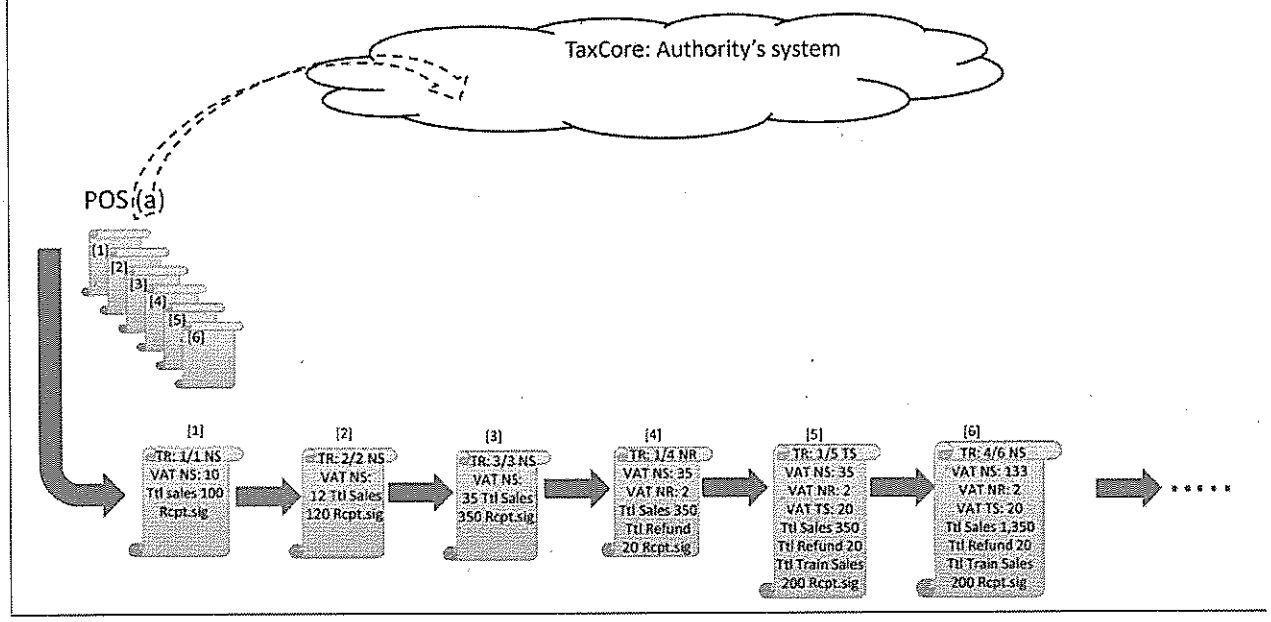
[21] *See* OECD, "Electronic Sales Suppression: A Threat to Tax Revenues" (2013) (discussing the misuse of functions within the electronic cash register or operating system software, specifically training mode, for the entire till or for a specific clerk so that items are not recorded in the normal reports).

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

Figure 7. Fiscal Counters Supporting the Proof of Audit Structure (Assuming 10 Percent VAT)



Traditionally, POS machines made and stored retail records locally, meaning in the POS machine itself. Zappers and phantomware operate by altering this record within the taxpayer's POS. They can manipulate selected items on a receipt or delete the entire receipt. The deletions — and, of course, the related removal of cash — normally occur after business hours. There is a strong preference for targeting cash transactions.

Fiji's VMS severely limits the taxpayer's ability to manipulate records with zappers or phantomware, preventing the programs from eliminating specific line items from a receipt or substituting less expensive items for pricier items actually purchased. With Fiji's VMS, data pass too quickly for line-item manipulation frauds. In less than a second, data go from the keystroke entry by the POS operator into the secure element, and return in encrypted and signed form with a QR Code.

While the VMS eliminates line-item manipulation, there is a slight possibility that a zapper or phantomware could delete an entire audit package (the whole invoice) before an audit is completed. This must be done within a short five-minute window since the next proof of audit is likely to occur soon — waiting until closing time to use an electronic sales suppression device will no longer work. If this occurred and the customer scanned the QR Code on the receipt, then the difference between the amount paid by the customer and the amount recorded by the VMS would be visible. A message would notify the customer to compare the amounts and report any difference to the FRCS.

Regardless, even if the deletion is successful, the ultimate fraud will not be. With a deleted audit package in the commercial trail, the next proof of audit cannot occur because sequential data will be missing from the chain of transactions.

Recall in Figure 7, TR: 1/1 NS is followed by TR: 2/2 NS, TR: 3/3 NS, TR: 1/4 NR, TR: 1/5 TS, and TR: 4/6 NS. Suppose the large sale represented by the third invoice (TR: 3/3 NS) is deleted by a sales suppression program. When it attempts an audit, the secure element will notify TaxCore that an invoice is missing. Simply put, TR: 2/2 cannot be followed by TR: 1/4. The system cannot issue a proof of audit, nor can it issue any subsequent proof of audit. Instead, the secure element will shut down. The secure element also shuts down whenever a counter reaches a cap. No resets are possible. The taxpayer will be offline without the

For more *Tax Notes International* content, please visit www.taxnotes.com.

possibility of generating a fiscal invoice. As Schedule 2, section 2.5 of the EFD regulation explains:

> Proof of audit is transmitted to the secure element to unlock signing or to update maximum allowed sum of fiscal invoice amounts counter. . . . 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.

The tax authority will be immediately aware of the secure element shutdown. The enforcement response involves either scanning the last receipt to obtain the internal data from the QR Code or auditing the secure element. Effectively, if a fraudster tries to use a zapper or phantomware in Fiji's system, the technology will quickly defeat the fraud.

Fraud Schemes 3 and 4

While fraud schemes 1 and 2 involve missing fiscal invoices, fraud schemes 3 and 4 involve false fiscal invoices. In fraud scheme 3 — which can involve either B2B or B2C transactions — the fraudster photocopies a single invoice and reissues it throughout the day to customers purchasing the same product. In fraud scheme 4 — a B2B scenario — fraudsters secure apparently valid invoices for resale on the black market, either by manufacturing the invoices on stolen equipment or stealing them outright.

Fiji's VMS uses two tools to stop these frauds: a lottery (customer compliance award) and the VMS's verification function.

B2C compliance is particularly difficult to automate. This is largely because the non-taxpayer consumer is half of the transaction and there are few incentives for him to report potential fraud to the tax authority. In a 2017 report titled "Technology Tools to Tackle Tax Evasion and Tax Fraud," the OECD discusses the benefits of programs that encourage "compliance awareness among customers" and cites successful lottery programs in Colombia and Portugal.

Fiji is developing a customer compliance award or lottery system. While it is not in place yet, the lottery's outlines are in the regulations. Section 26 of the EFD regulation provides that:

> (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.

Once in place, the system will provide a webpage through which individuals or businesses can scan the QR codes on their receipts to enter a lottery. The FRCS wants customers to provide a verifiable record of the sale and all the associated data on the QR Code. Getting consumers to demand a valid receipt is the best way to ensure that businesses provide receipts. A lottery provides an incentive for consumers to tell the tax authority about transactions. Allowing businesses to participate in the lottery when they participate in B2B transactions — likely for a different type of prize — helps make scanning the QR Code a cultural habit.

While a chance to win is the incentive in lottery systems, other incentives that can be used. For example, in Brazil, contracts are only enforceable if the party has a digital original document. Similarly, a jurisdiction could hold that a transaction is only enforceable if the party seeking to enforce it has a fiscal invoice with valid QR Code.

Selecting the right lottery prize has an impact on participation. Some jurisdictions, like Malta, prefer lotteries that distribute relatively modest awards monthly.[22] Other jurisdictions prefer large expensive prizes: Portugal awarded 40 new Audi automobiles in a year.[23] A particularly fitting award would be free prepaid mobile minutes, awarded more frequently in industry segments that demonstrated low compliance rates. In other instances, the award could be a tax-free purchase the next time the customer patronizes the same

[22] *See* Michael Graham, "VAT Lottery Results: Four Wins in Nine Months!" *Times of Malta*, Apr. 27, 2016 (reporting that one individual won the monthly VAT lottery in July 2015 (€233), November 2015 (€233), December 2015 (€550), and March 2016 (€1,569)).

[23] *See* Patricia Kowsmann, "Get Receipts, Win a Car: How Greece's VAT Lottery Plan Worked in Portugal," *The Wall Street Journal*, Mar. 10, 2015.

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

establishment — essentially, a limited tax holiday. The customer could simply scan the old, "winning" receipt into the POS system, and the VAT would be removed on the next purchase. This incentive encourages both the customer and business owner to embrace the technology.

Encouraging customers to ask for receipts and then scan them has two effects. First, it discourages collusion frauds. Second, it allows the authority to develop an enforcement database of individuals who claim to own the same receipt — thus fighting the large cheese pizza example in fraud scenario 3. When Fiji's lottery is operational, the VMS will be able to flag duplicate claims of invoice ownership. Enforcement should be swift. The FRCS can immediately terminate the ability of the business to issue fiscal invoices.

As to fraud scheme 4, it is reasonable to assume that the individual whose POS and E-SDC are stolen will notify the authority. If the thief knows the PIN of the POS and begins to process invoices, then the owner's call to the FRCS customer service desk will effectively be a request that the certificate in the stolen POS be revoked. That POS will no longer be able to issue fiscal invoices.

If the POS is using a V-SDC within TaxCore, revocation will be instantaneous. The same result would happen with an E-SDC because TaxCore can revoke an E-SDC certificate remotely. Any invoice issued after the revocation order will be automatically marked "INVALID."

Fraud Scheme 5

The fifth common VAT fraud scheme has a long history. Ever since electronic cash registers arrived in the mid-1960s, businesses have been manipulating the programming to allow the registers to function perfectly, while keeping the records in "training mode." The taxpayer could exclude these records from the electronic memory or delete them altogether. Training mode data manipulation efforts remain popular today.[24]

During late 2005 and early 2006, the EU Fiscalis Committee Project Group 12 presented one of the first multinational studies of electronic sale suppression.[25] It described the enforcement efforts in use at that time and offered projections for the future. As the Fiscalis report notes, some fraudsters reprogram electronic registers to delete training mode data from internal records. In other instances, the data are recorded separately but blended in with the general sales files without any indication that the included training amounts are not part of the sales totals (in other words, the training tickets data are hiding in plain sight).

In 2005 the United Kingdom told Fiscalis about a single restaurant in London that used the training mode to remove over £500,000 of VAT from the records and stole other tax revenue exceeding £1 million. Belgium presented similar examples. This kind of fraud is nearly impossible in Fiji. If it started, it would be identified and quickly stopped because the system preserves training mode data in detail and makes its operation transparent.

Invoice 5 in Figure 7 is a sales training invoice. The EFD counters operate exactly the same for training sales as they do for normal sales. The counters aggregate and align the training mode invoices, place them in sequence, and account for each invoice. If we extended the Figure 7 fact pattern, we might have TR: 1/5 TS followed by TR: 2/10 TS, TR: 3/11 TS, and TR: 4/15 TS. This shows that the fifth, 10th, 11th, and 15th invoices are all part of a training program. The secure element's counters would preserve the total training mode sales amounts and the total training mode VAT amounts. The data are kept clear, separate, and not aggregated and not aggregated with the actual sales data.

When it issues a training mode invoice, the VMS produces a QR Code that indicates that the receipt was issued for training purposes. The training receipt cannot be used to claim an input credit or to apply for a customer compliance award (the lottery). The counters in the Fiji VMS along with the proof of audit would eliminate this variation on fraud schemes 1 and 2. It is common for businesses using a zapper or phantomware application to record the sales that they wish to

[24] "Electronic Sales Suppression," *supra* note 21 (discussing the misuse of functions, specifically the training mode, for either the entire till or an individual clerk so that items are not recorded in the normal reports).

[25] European Commission, Fiscalis Committee Project Group 12, "Cash Register Project Group, Cash Register Good Practice Guide, v. 1.00" (Dec. 28, 2005-Jan. 2, 2006) (restricted for administrative use only, draft copy on file with authors).

For more *Tax Notes International* content, please visit www.taxnotes.com.

eliminate in "training mode," and then use the suppression technology to eliminate all training mode traces. Because the VMS would produce a "training mode" QR Code, the transaction would not "disappear" from the record of sales as it does currently, and the customer would be able to easily identify the manipulation, thereby qualifying for an award.

Further, for training invoices, the VMS retains the identification of the person being trained, as well as the time and duration of the training session. The FRCS can cap the number of hours per day that the training mode is used, cap the number of hours of training each employee undergoes, and compare the sales volumes during training with the sales volumes in the normal business at the same time. These caps can force the owner to perform a self-audit — namely, transmitting E-SDC data to TaxCore and receiving back a proof of audit.

Conclusion

In Fiji's VAT system, basic data cannot be manipulated. The VMS captures transaction data and fiscalizes them before any other functions in the POS touch them. The VMS and the secure element counters actually capture much more than just basic information: All critical data elements are preserved. The system records total sales, total VAT, and the totals for other taxes like the 10 percent services turnover tax, the 6 percent environmental and health levy, and the plastic bag levy.[26] One of the distinct advantages of Fiji's system is that it can uniformly implement a tax rate increase (or decrease) throughout the country at a moment's notice. New taxes can be accommodated easily.

The strength — and the uniqueness — of Fiji's VMS is its real-time data collection, its data protection, and its data retention capabilities. When fully implemented, the technological reforms promise to capture lost revenues in Fiji of at least FJD 185 million. The amount could be much higher, but it is unlikely to be lower.

Although not the focus of this article, the fact that Fiji's VMS is built on public key infrastructure means that it benefits from associated services including non-repudiation, time stamping, encryption, and safe encryption key exchange. One recent example is notable. The western side of Fiji was hit hard by a cyclone March 31.[27] Four people were killed. The IT manager for a group of supermarkets called FRCS to report that two of their three stores were completely flooded and all of the POS equipment had been destroyed. They needed new secure element smart cards for their stores; specifically, they needed 20 cards for 20 POSs. The FRCS immediately revoked the old cards and issued new cards; it takes about 60 seconds to produce one card. Before revocation, all of the data on the old cards were successfully stored on FRCS servers. If any of the old secure elements remained viable and someone tried to use them, the FRCS would know immediately and the attempted verification would show the invoice to be invalid.

There are exceptional efficiencies in this comprehensive digital invoice regime. Fiji will be the first VAT jurisdiction in the South Pacific — and one of only a few globally — to secure real-time, encrypted reporting of all taxable transactions, including both B2B and B2C. Many of the traditional VAT frauds are simply unworkable in this system. Enforcement flows directly from the technology.

A considerable portion of the auditing function in Fiji will be automated. The proof of audit concept and the counters are unique, as well as the use of E-SDCs and V-SDCs around TaxCore.

Fiji's tax system is now a prime example of the principle that the code — meaning the computer code — is the law.[28] As Lawrence Lessig explains:

> Our choice is not between "regulation" and "no regulation." The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus, the choice is not whether people will decide how cyberspace regulates. People — coders — will. The only choice is whether we

[26] *See* FRCS, Taxpayer's User Guides.

[27] "Tropical Cyclone Josie Claims Four Lives in Fiji," Radio New Zealand (Apr. 2, 2018).

[28] Lawrence Lessig, "Code Is Law: On Liberty and Cyberspace," *Harvard Magazine*, Jan. 1, 2000.

For more *Tax Notes International* content, please visit www.taxnotes.com.

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

collectively will have a role in their choice — and thus in determining how these values regulate — or whether collectively we will allow the coders to select our values for us.

The code — or the data structures and data collection mechanisms of Fiji's VAT — compels compliance. For example, an invoice without a QR Code is noticeably invalid. An invoice with a QR Code is not necessarily valid, but it can be immediately validated at any time, in any place by scanning the QR Code. The coding makes this a truth of the tax system. ■

© 2018 Tax Analysts. All rights reserved. Tax Analysts does not claim copyright in any public domain or third party content.

For more *Tax Notes International* content, please visit www.taxnotes.com.