فاتورة

هيئة الزكاة والضريبة والجمارك
Zakat, Tax and Customs Authority

E-invoicing Detailed Technical Guidelines

Version 1

فـاتورة
Fatoora

JUNE 29 - 2022

Contents

1.	**General Information**	**6**
1.1.	Introduction	6
1.1.1.	Objectives	7
1.1.2.	Scope	7
1.1.3.	Intended Audience	8
1.1.4.	Recommended Reading	8
2.	**Taxpayer E-invoicing Journey**	**9**
2.1.	The Taxpayer E-invoicing Journey	9
2.1.1.	Compliance of EGS	9
2.1.2.	Onboarding	10
2.1.3.	Sharing invoices and notes (Clearance and Reporting)	10
2.1.4.	Additional Step - Compliance and Enablement Toolbox	11
2.1.5.	Additional Step - Integration Sandbox	11
3.	**Onboarding**	**12**
3.1.	Introduction and Objectives of the Onboarding Functionality	12
3.2.	Onboarding Overview	13
3.2.1.	Onboarding of a new EGS Unit(s)	13
3.2.2.	Renewal of existing CSID(s) for EGS Unit(s)	16
3.2.3.	Revocation of CSID(s) for one or more EGS Unit(s) by the Taxpayer	18
3.3.	Description of the Onboarding Process	19

3.3.1.	Taxpayer accessing and logging into the Fatoora Portal using Single Sign On (SSO) of Taxpayer Portal	19
3.3.1.1.	Description	19
3.3.1.2.	Process Flow	20
Onboarding and Renewal		**21**
3.3.2.	Generating an OTP to obtain a CSID for the first time or renewing an existing CSID (Manual OTP entry)	21
3.3.2.1.	Description	21
3.3.2.2.	Process Flow	22
3.3.3.	Sending a Certificate Signing Request (CSR) in order to receive a Compliance CSID	26
3.3.3.1.	Description	26
3.3.3.2.	Process Flow	30
3.3.4.	Completion of the Compliance Checks by the EGS Unit	30
3.3.4.1.	Description	30
3.3.4.2.	Process Flow	31
3.3.5.	Generating a new CSID for the EGS Unit or Renewing the existing CSID	32
3.3.5.1.	Description	32
3.3.5.2.	Process Flow	32
3.3.6.	View List of EGS Unit(s)	32
3.3.6.1.	Description	32
3.3.6.2.	Process Flow	33
Revocation of an existing CSID		**35**

3.3.7.	Manual revocation of an existing CSID by the Taxpayer	35
3.3.7.1.	Description	35
3.3.7.2.	Process Flow	35
3.3.8.	Automatic revocation of CSID(s) due to VAT Deregistration or Suspension	38
3.3.8.1.	Description	38
3.3.8.2.	Process Flow	39
3.4.	VAT Group Onboarding Scenarios	40
3.4.1.	Specific tax group Onboarding Scenarios	40
3.4.2.	VAT Group Onboarding Roles	42
3.5.	Common Onboarding/CSID related scenarios faced by Taxpayers	43
3.5.1.	Centralized Server - On Premise or Cloud	43
3.5.2.	Branch Based Smart POS Devices Issuing and Sending Invoices	43
3.5.3.	Branch Based Standard POS Devices with Branch Servers and Centralized Sending Server	43
3.5.4.	POS Devices Unable to Sign Invoices	44
4.	**Reporting and Clearance of E-invoices**	**45**
4.1.	Introduction and Objectives of Reporting and Clearance	45
4.2.	Reporting and Clearance Overview	46
4.3.	Description of the Reporting and Clearance Processes	47
4.3.1.	Reporting	49
4.3.2.	Clearance	50

5.	**Signing Process**	**52**
5.1.	SHA-256 Hash - Hashing algorithm	52
5.2.	Signing steps	52
6.	**QR code**	**58**
6.1.	TLV - TAG - LENGTH - VALUE construction and file format	59
6.2.	Creation of TLV QR code	60
6.3.	Common mistakes in building the QR code	64
6.4.	Manual decoding a TLV QR Code	64
6.5.	Creation of QR code in JAVA - Javascript - nodeJS	66
7.	**Business FAQs**	**70**
8.	**Appendix**	**78**

1. General Information

1.1 Introduction

The e-invoicing implementation in the Kingdom of Saudi Arabia is enforced into two phases:

- Phase One (Generation Phase): Generation of Electronic Invoices phase, where persons subject to the E-Invoicing Regulations must generate Electronic Invoices and associated Electronic Notes in accordance with the clauses set forth under the Resolution on the Controls, Requirements, Technical Specifications and Procedural Rules and any subsequent resolutions. This phase has been implemented effectively on 4th of December 2021.
- Phase Two (Integration Phase): Integration Phase, where persons subject to the E-Invoicing Regulations must integrate their systems with the Authority's system in accordance with the clauses set forth under the Resolution on the Controls, Requirements, Technical Specifications and Procedural Rules and any subsequent resolutions. Such phase shall be implemented starting from 1st of January 2023. The integration phase will be implemented in phases and will be mandated to Persons subjected to the E-Invoicing Regulations based on a certain set of criteria determined by the Authority. The target groups will be informed of the integration procedures with the authority's systems at least six months before the date set for integration with the target group or groups. The tax invoices should follow the clearance model whereas the simplified tax invoices should follow the reporting model.

And to support the taxpayers and solution providers to comply with the e-invoicing requirements, the authority has published the "Developer Portal" which consist of:

1. Compliance and Enablement Toolbox (SDK): an offline downloadable tool, which can be used to validate an XML, based e-invoice, credit or debit note files in accordance with the ZATCA published requirements, standards and guidelines. It also allows validation of the QR codes as per the prescribed structure. Developers can integrate their EGS units with the SDK locally (offline) or also test using a Command Line Interface (CLI).
2. Integration Sandbox: a test ZATCA backend system, which EGS units can integrate with to make API calls to simulate and test the Onboarding process followed by the submission of test e-invoices, credit and debit notes for Reporting and Clearance in accordance with the ZATCA published requirements, standards and guidelines.

The Authority has developed "Fatoora" platform, which is the platform where the taxpayer is obliged to integrate with; this platform will have the following functionalities:

- receives these documents via API from the Taxpayer's E-invoicing Generation Systems (EGS)
- processes and validates submitted documents as part of the Clearance and Reporting in line with the standards mentioned above
- sends back the outcome of the validations to the Taxpayer's EGS (and additionally key events and failure points will be communicated using notifications)
- stores valid and accepted documents (with warnings) for ZATCA
- allows ZATCA Mobile App users to provide the QR code of scanned documents as well as the out-come of the offline QR code validation done by the app.

1.1.1. Objectives

After reading this guideline the Taxpayer should be able to:

1. Understand how to complete the Onboarding process
2. Understand the Reporting and Clearance process at a high level

1.1.2. Scope

This guideline acts as a guide for users to understand the Taxpayer's user journey in preparing and successfully onboarding their E-invoice Generation Solution Units, fulfilling and monitoring their compliance with the E-invoicing regulations with respect to cleared and reported invoices. More specifically, this guideline covers the following processes and functionalities:

- An overview of the Taxpayer E-invoicing Journey
- Onboarding related processes, such as:
    - Taxpayer accessing and logging into the Fatoora Portal
    - Generating an One Time Password (OTP) to obtain a new Cryptographic Stamp Identifier (CSID) or renew an existing CSID (manually and automatically)
    - Sending a Certificate Signing Request (CSR) in order to receive a Compliance CSID
    - Completion of the Compliance checks by the EGS unit
    - Generating a new CSID for the EGS unit or renewing the existing CSID
    - Viewing a list of the onboarded EGS units
    - Revocation of existing CSIDs
    - Specific Tax Group onboarding scenarios
    - Common onboarding scenarios faced by Taxpayers

- Reporting and Clearance of electronic invoices, credit and debit notes related processes, such as:
  - Recommended tools that can be utilised prior to the generation and submission of e-documents to ZATCA
  - Reporting related processes and functionalities enabling the submission of e-documents to ZATCA and their validation
  - Clearance related processes and functionalities enabling the submission of e-documents to ZATCA and their validation and clearance

1.1.3. Intended Audience

This document is intended to be used by Taxpayers and/or other persons (e.g. service providers, providers of EGS or other) that may be conducting e-invoicing related activities on behalf of Taxpayers.

1.1.4. Recommended Reading

Users accessing this guideline should also go through the following documents:

1. E-invoicing Regulation (Link)
2. E-invoicing Implementation Resolution (Link)
3. Data Dictionary (Link)
4. XML Implementation Standards (Link)
5. Security Features and Implementation Standards (Link).
6. API Documentation (Link)

2. Taxpayer E-invoicing Journey

2.1. The Taxpayer E-invoicing Journey

The Taxpayer E-invoicing User Journey represents the key steps that Taxpayers can take in order to be able to fulfil their obligations for the Integration Phase of E-invoicing. It should be noted that some of these steps represent optional steps or capabilities that the authority has made available to Taxpayers and EGS system developers in order to better equip and provide a full suite of tools allowing compliance with the E-invoicing requirements. The core steps and processes indicated within this Guideline represent mandatory steps that need to be undertaken by Taxpayers in order to meet their E-invoicing obligations.

Listed below, are the three key steps of the Taxpayer Journey for obtaining an EGS system and successfully onboarding it with ZATCA, for the purposes of submitting e-documents to ZATCA:

- The taxpayer should make sure the e-invoicing solution is compliant with the e-invoicing requirements
- The Taxpayers' ability to onboard their EGS devices for integration with ZATCA; and
- The Taxpayers' ability to successfully submit electronic invoices, credit notes and debit notes for Clearance or Reporting to ZATCA.

More details about each of these steps is provided in the sections below.

2.1.1. Compliance of EGS

The taxpayer has to make sure that his EGS is compliant with the e-invoicing requirements. For more details on the requirements, please check the E-invoicing Implementation Resolution (here)

2.1.2. Onboarding

The second step of the Taxpayer E-invoicing Journey involves the onboarding of Taxpayers' EGS units and devices with Fatoora Platform. This step is a mandatory step that all Taxpayers who are subject to E-invoicing must undertake and comply with. In line with the integration waves for targeted Taxpayer groups that ZATCA will be enforcing from 1 January, 2023 onwards.

By accessing ZATCA's Fatoora Portal, Taxpayers can access the onboarding related options and initiate the process to onboard their EGS units and devices and integrate them with ZATCA. Onboarding is a highly automated process between the EGS(s) and Fatoora Platform with very limited interaction required by Taxpayers. A Taxpayer or user simply needs to indicate how many devices they would wish to onboard, generate the respective One Time Passwords (OTP(s)) which can then be inserted into their EGS and the rest of the process should be automated through APIs between the Taxpayer's solution and ZATCA's systems.

For the full details and options of the onboarding process, as well as the detailed guidance of the steps involved, please refer to Section 3 of this Guideline.

2.1.3. Sharing invoices and notes (Clearance and Reporting)

Following the successful completion and onboarding of the Taxpayer's EGS, Taxpayers can start submitting documents to ZATCA for clearance or reporting. ZATCA's Fatoora Platform will perform all required validations against the documents submitted.
For more details regarding the processes of clearance and reporting and all relevant information, please refer to Section 4 of this Guideline.

2.1.4. Additional Step - Compliance and Enablement Toolbox

In addition to the above, another optional step in the Taxpayer E-invoicing Journey which can be followed by Taxpayers, is the ability of Taxpayers to verify and confirm the compliance of their electronic documents. In order to do that, Taxpayers and their system developers can use the Compliance and Enablement Toolbox that can be accessed from ZATCA's Developer Portal or through ZATCA's website. Through both the Developer Portal and ZATCA's website, Taxpayers can download the SDK and integrate it on their solutions or use the command line interface. Furthermore, Taxpayers who are less technical users can also access and use an online Portal-based validator, which allows Taxpayers to upload specific XML files and check their compliance directly through the validator.
For more details and information about the Compliance and Enablement Toolbox and how to access and use it through ZATCA's Developers Portal, please refer to the Developer Portal Guideline (Link)

2.1.5. Additional Step - Integration Sandbox

Furthermore, another optional step in the Taxpayer E-invoicing Journey that can be followed, is Taxpayers being able to test and confirm their ability to successfully integrate with ZATCA's systems through APIs. In order to check the integration, Taxpayers can use the Integration Sandbox, which can also be accessed through ZATCA's Developer Portal.

Taxpayers can access ZATCA's Developer Portal and navigate to the dedicated page for the Integration Sandbox. From here they can access the API integration documentation and the different swagger files. Using these swagger files, developers can simulate the different integration calls that Taxpayers' Solutions will have to do with ZATCA's Fatoora Platform and test these integrations, including simulating the integrations required to onboard their solutions and obtain their test CSID(s), but also simulating and testing the submission of standard (B2B) and simplified documents (B2C) to ZATCA.

For more details and information about the Compliance and Enablement Toolbox and how to access and use it through ZATCA's Developers Portal, please refer to the Developer Portal User Manual (Link).

3. Onboarding

IMPORTANT: The Onboarding section acts as a guide for Taxpayers to help users operate the Onboarding ZATCA Portal in order to obtain the necessary Cryptographic Stamp Identifiers (CSID) and perform any other relevant activities such as the revocation of CSID(s). Please note that Taxpayers should refer to the Guidelineof the E-Invoicing Generation Solution (EGS) Unit for any steps taking place on the Taxpayer's EGS Unit.

3.1. Introduction and Objectives of the Onboarding Functionality

The Onboarding functionality is developed by ZATCA in order to provide Taxpayers who are using E-invoicing Generation Solution Unit(s) (EGS Unit(s)) with a way to obtain the necessary Cryptographic Stamp Identifiers (CSID(s)) to allow for the first-time onboarding of their EGS Unit(s). In addition, the CSID(s) needs to be renewed and Taxpayers can request for the renewal of their CSID(s) before the expiry of the existing CSID. In certain situations, Taxpayers may need to revoke their existing CSID(s). Hence, the Onboarding functionalities also include a way for Taxpayers or ZATCA to initiate the revocation process for their existing CSID(s).

A CSID is technically a cryptographic certificate, which is a credential that is used for authentication and signing purposes. The certificate is also known as a public key certificate or an identity certificate. It is an electronic document used as proof of ownership of a public key. A CSID is used to uniquely identify an Invoice Generation Solution Unit associated with a Taxpayer for the purpose of stamping (technically cryptographically signing) Simplified Invoices (B2C) and for accessing the Reporting and Clearance APIs.

The Onboarding feature in Fatoora portal is the starting point for the onboarding process. It allows Taxpayers to initiate the onboarding and renewal process by generating a One-Time-Password (OTP) to be used for their EGS Unit(s), in addition to accessing a list of all of their Onboarded EGS Units, which is also the starting point for revoking any CSID(s).

The primary objective of the Onboarding functionality enables:

- Taxpayers to undergo the first-time onboarding of their EGS Unit(s) by receiving the necessary CSID(s)
- Taxpayers to renew CSID for onboarded EGS Unit(s) before the expiry date of the existing CSID(s)
- Taxpayers to request the revocation of an existing CSID for onboarded EGS Unit(s) through the Fatoora Portal.

3.2. Onboarding Overview

The Onboarding functionality aims to address the following:

- Onboarding of a new EGS Unit(s) (i.e. receiving a CSID for the first-time)
- Renewal of existing CSID(s) for EGS Unit(s)
- Revocation of CSID(s) for one or more EGS Unit(s) (by the Taxpayer or automatically by ZATCA)

3.2.1. Onboarding of a new EGS Unit(s)

The first-time onboarding process requires the generation of a One-Time-Password (OTP) from the Fatoora Portal, which is entered into the Taxpayer's EGS Unit(s) either manually or automatically, followed by the generation of a CSR. The Taxpayer's EGS Unit(s) would then need to undergo the necessary compliance checks. Upon successful completion, ZATCA CA generates the CSID(s) for every EGS Unit(s) which are then sent to the Taxpayer's EGS Unit(s).

There are two methods to generate an OTP. The first method involves the Taxpayer receiving an OTP through the Fatoora Portal, which would be manually entered into the Taxpayer's EGS Unit(s). The second option involves the Taxpayer accessing the Fatoora Portal through their own EGS Units and receiving the OTP, and hence the OTP would be automatically read by their EGS Unit(s). In the first method, it is possible that the Taxpayer would be able to onboard or renew the CSID for single or multiple EGS Unit(s) at the same time, whilst the second option only allows the onboarding or renewing of the CSID for a single EGS Unit.

Diagram 1: Taxpayer receiving a CSID for the first time for one or more EGS Unit(s) - Manual OTP entry option

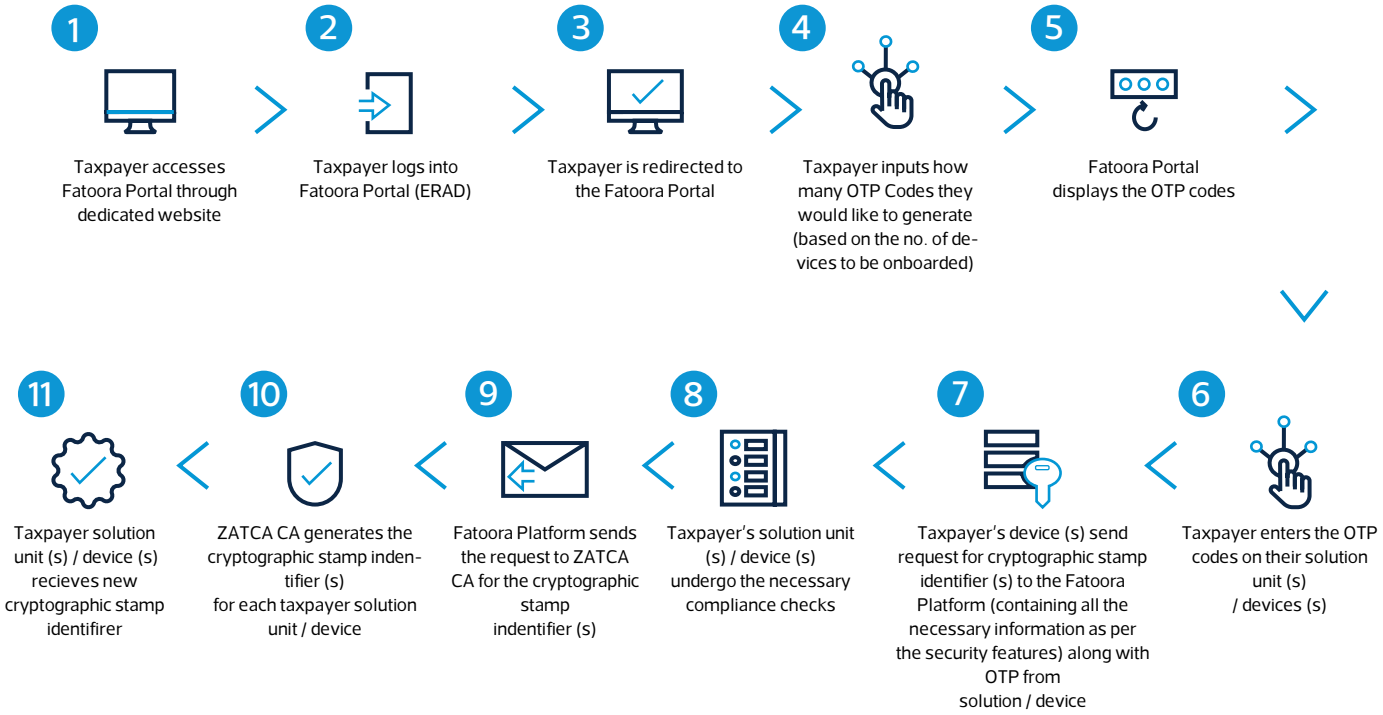
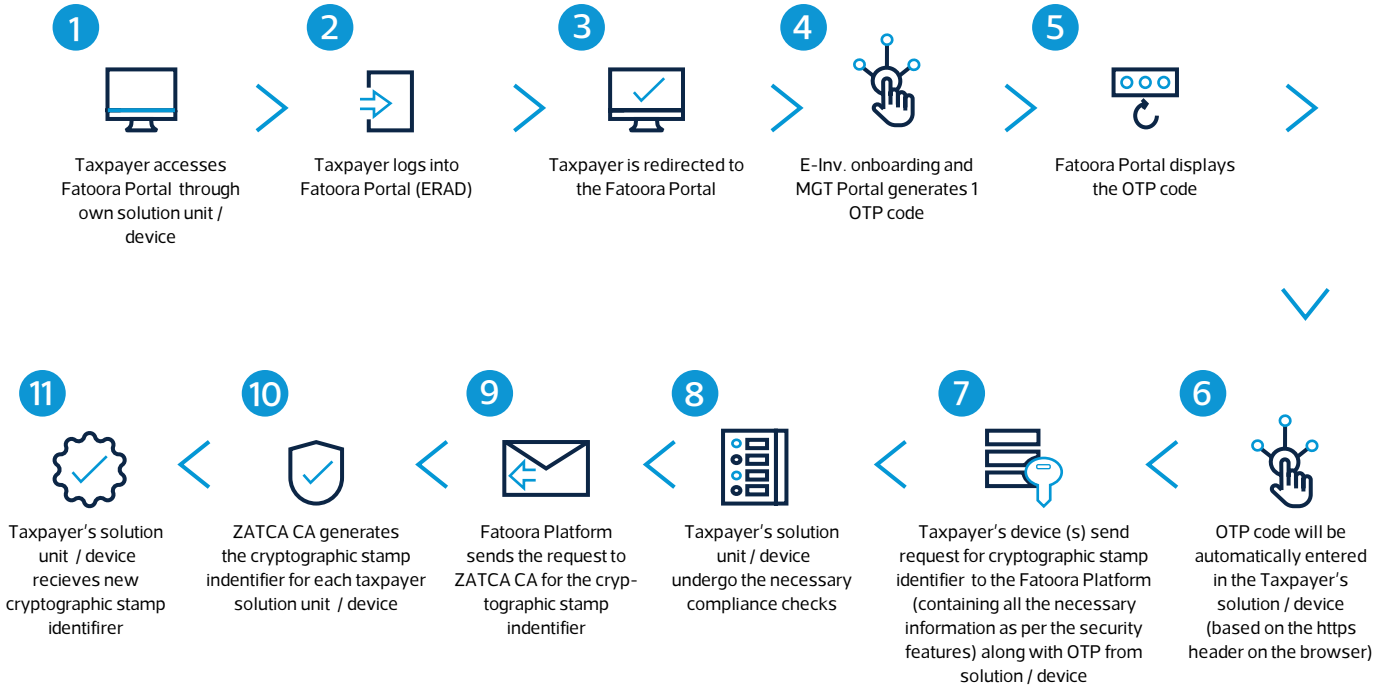


Diagram 2: Taxpayer receiving a CSID for the first time for a single EGS Unit - Automatic OTP entry



3.2.2. Renewal of existing CSID(s) for EGS Unit(s)

The process for the renewal of a CSID is similar to that of first-time onboarding; however, it involves the revocation of the existing CSID and the issuance of a new one.

Diagram 3: Taxpayer renewing the existing CSID for one or more EGS Unit(s) through manual OTP entry (includes revocation of existing CSID and issuance of a new CSID)

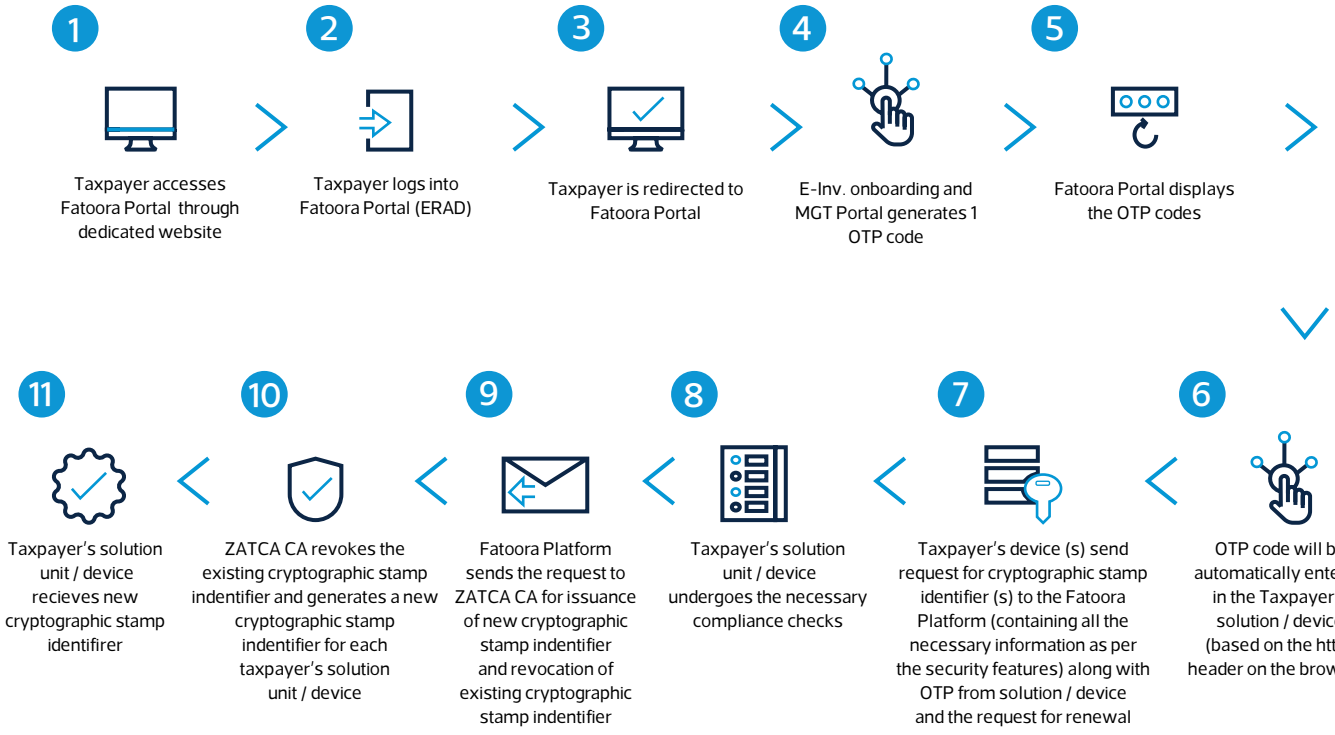
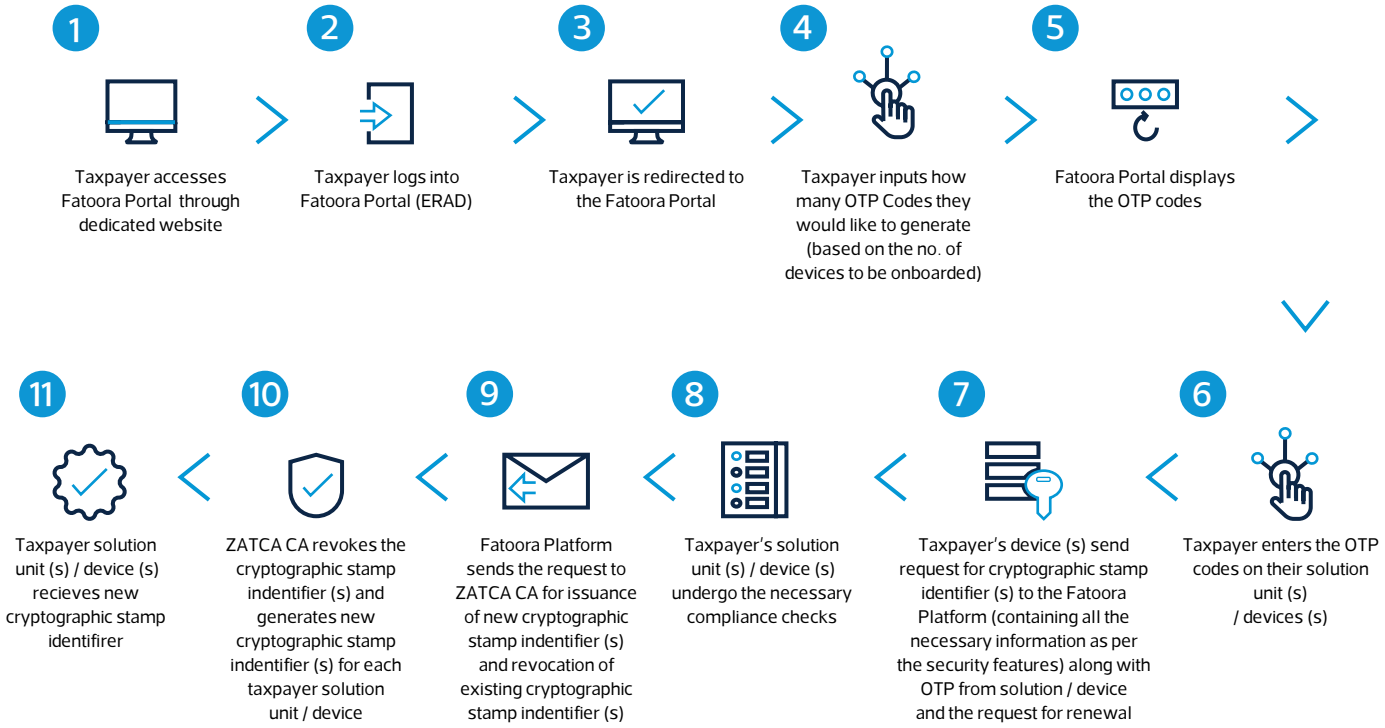


Diagram 4: Taxpayer renewing the existing CSID for one or more EGS Units through automatic OTP entry (includes revocation of existing CSID and issuance of a new CSID)



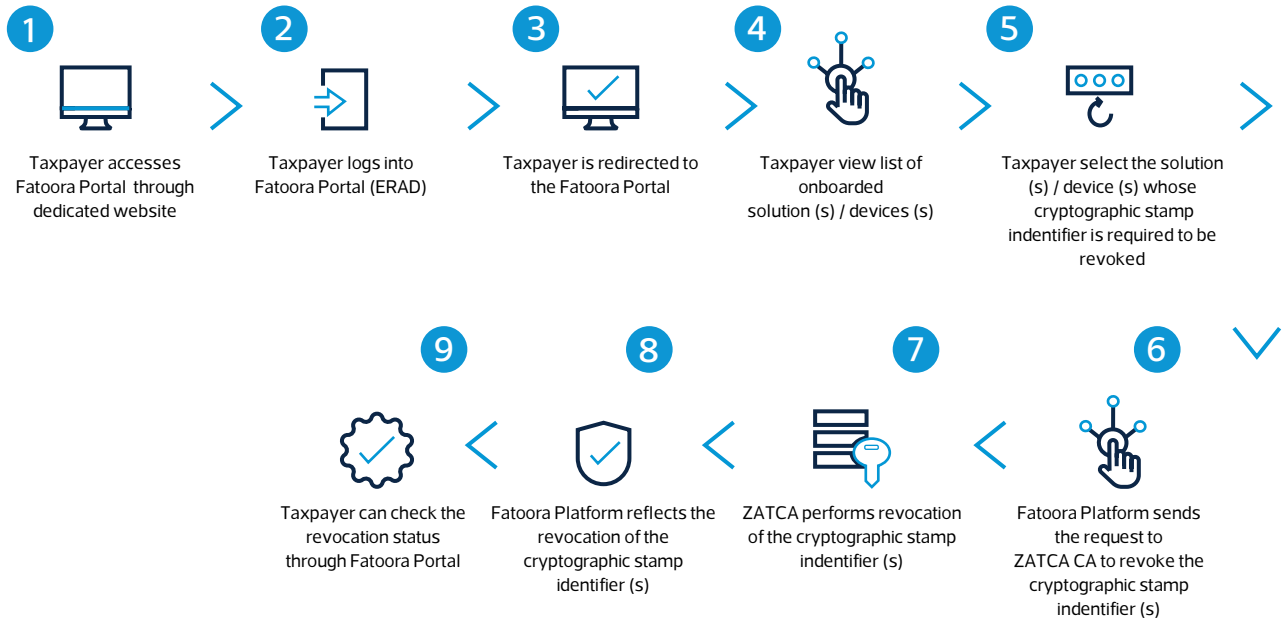
3.2.3. Revocation of CSID(s) for one or more EGS Unit(s) by the Taxpayer

Taxpayers may wish to revoke their existing CSID(s) for a number of reasons, including:

- If the Taxpayer believes that the private key or the EGS Unit itself is compromised
- If the EGS Unit is discontinued or transferred to another Taxpayer or sold
- If the Taxpayer discovers that the information in the CSID is not accurate
- If the EGS Unit is lost, stolen or damaged
- If the Taxpayer discovers that unauthorized onboarding of a EGS Unit has occurred
- If there is a major upgrade in the EGS unit.

In order to revoke existing CSID(s), Taxpayers need to access the Onboarding and Management Portal and view a list of all of their onboarded EGS Units(s) and select the ones with active CSID(s) that they would like to revoke.

Diagram 5: Taxpayer revoking the CSID for one or more EGS Unit(s)



3.3. Description of the Onboarding Process

3.3.1. Taxpayer accessing and logging into the Fatoora Portal using Single Sign On (SSO) using the existing credentials of Fatoora Portal (ERAD)

3.3.1.1. Description

The Fatoora Portal is the front-end aspect of the Onboarding functionality and it is regarded as the starting point for Taxpayers to generate CSID(s) for their EGS Unit(s) for the first time, renew their existing CSID(s) and revoke them. Through the Fatoora Portal, Taxpayers can generate One-Time-Passwords (OTPs) for the first-time onboarding and the renewal process. Taxpayers can also view a list of all of their onboarded EGS Units along with the status of each unit and revoke existing CSID(s).

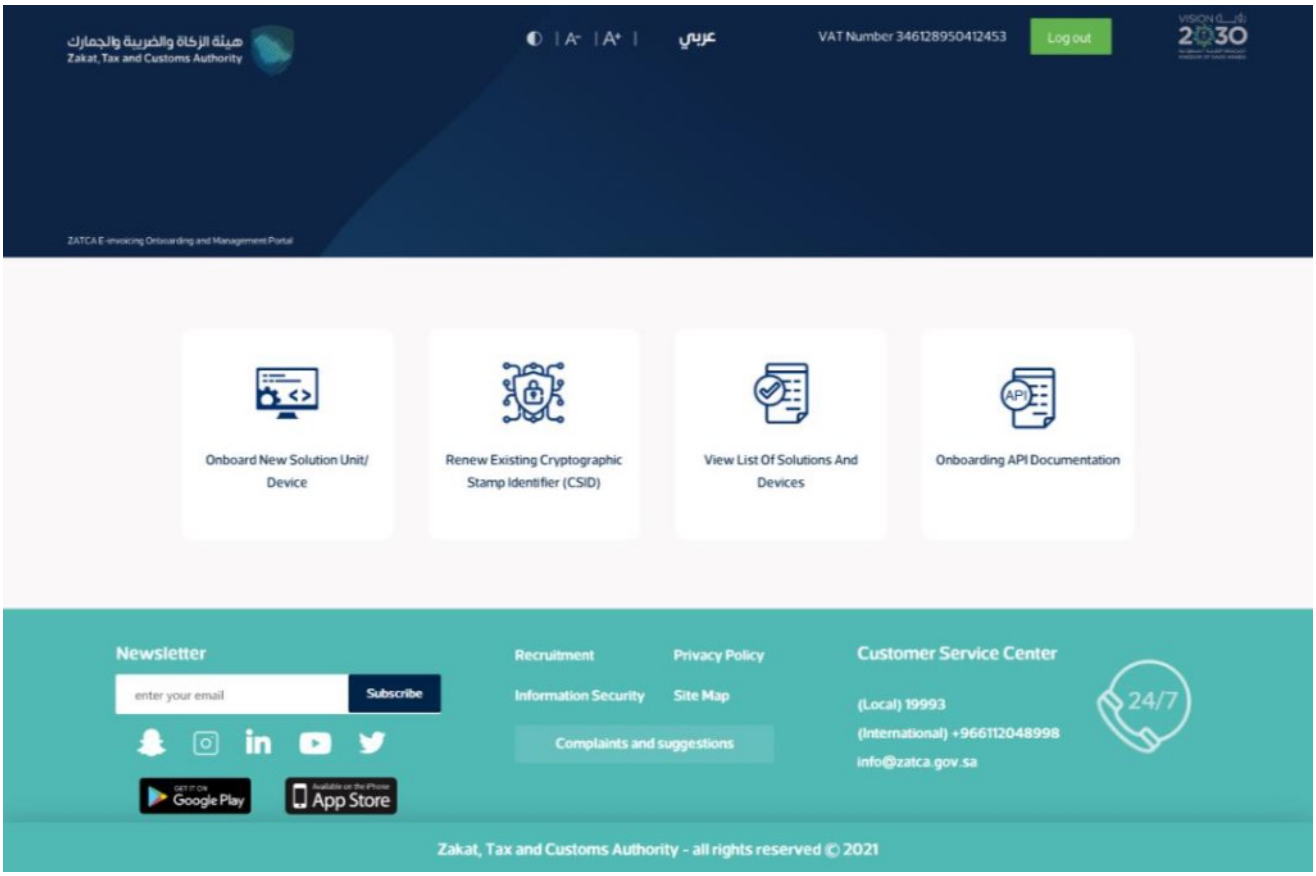
- The Onboarding and Management Portal can be accessed and all of its functionalities can be used by all Taxpayers who are registered on the main Fatoora Portal (ERAD) for VAT purposes and who have a VAT Registration (TRN) status of "Active" or "Reactive".
- Taxpayers who have a TRN status of "Deregistered" or "Suspended" would not be able to access the Onboarding and Management Portal.
- Taxpayers whose VAT registration status used to be "Active" or "Reactive" but changes to "Deregistered" or "Suspended" would be able to access the Onboarding and Management portal for a period of 90 days but can only view a list of their previously onboarded EGS Units and cannot use any other onboarding functionalities such as generating an OTP. Once the buffer period of 90 days is over, these Taxpayers will no longer be able to access the Onboarding and Management Portal.

3.3.1.2. Process Flow

The process of accessing the Onboarding and Management Portal is as follows:

1. The Taxpayer accesses the Onboarding and Management Portal by clicking on the relevant tile on the Fatoora Portal (ERAD).
2. The Taxpayer is redirected to the Fatoora Portal (ERAD) SSO in order to provide their Fatoora Portal (ERAD) credentials and log-in.
3. Upon the successful log-in (authentication) and meeting of the authorization criteria, the Taxpayer is redirected again to the Onboarding and Management Portal landing page.
4. On the main landing page, the Taxpayer can see the following tiles:

    - Onboard New Solution Unit/Device
    - Renew Existing Cryptographic Stamp Identifier (CSID)
    - View List of Solutions and Devices
    - Onboarding API Documentation



Fatoora Platform Landing Portal

In case the Taxpayer does not meet the defined authentication and authorization criteria for accessing the Onboarding and Management Portal, the Taxpayer will not be able to log in and an error message is displayed indicating that the Taxpayer cannot access the Onboarding and Management Portal.
Note: The Taxpayer can choose to toggle the language between English and Arabic by using the icon on the header of the page.

Onboarding and Renewal

3.3.2. Generating an OTP to obtain a CSID for the first time or renewing an existing CSID (Manual OTP entry)

3.3.2.1. Description

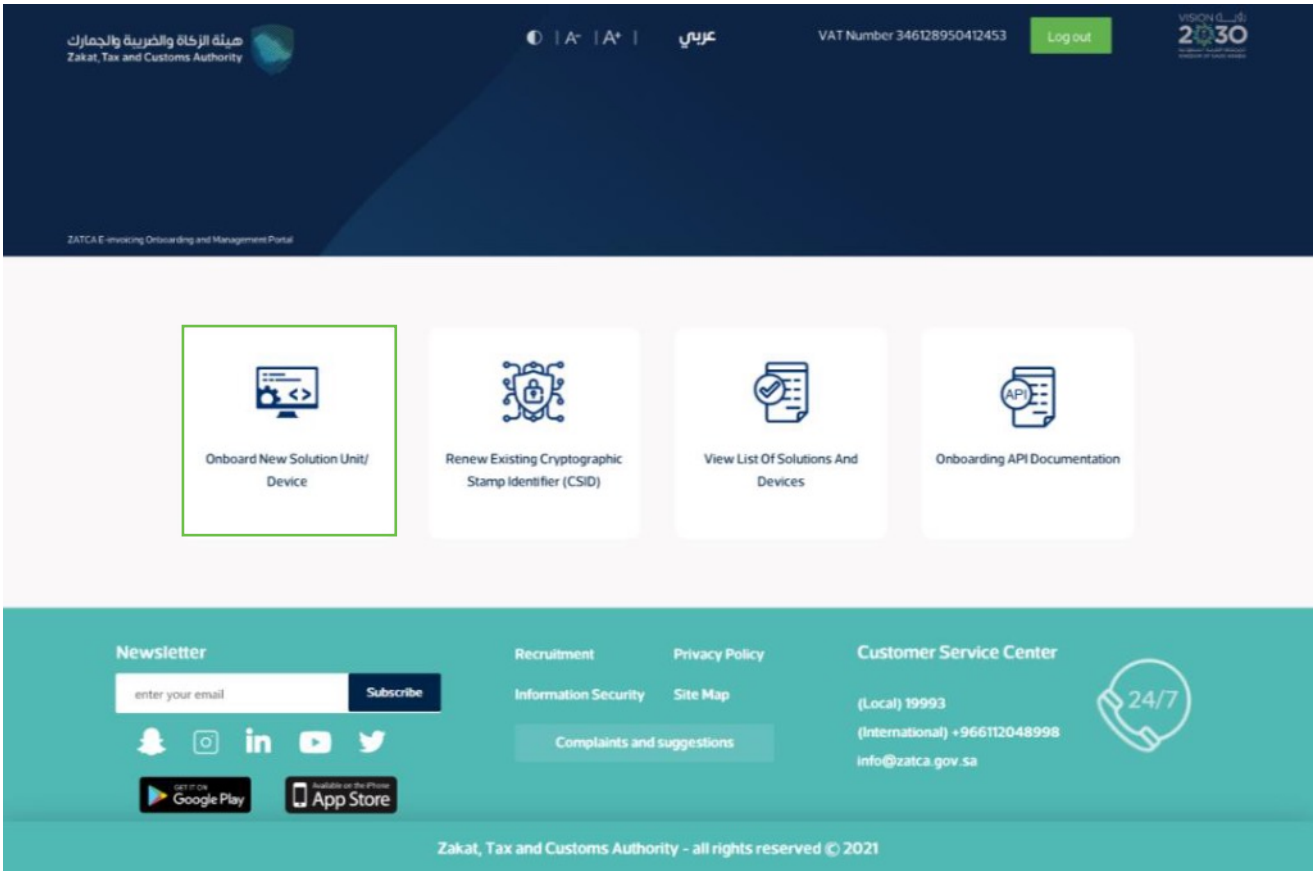
The onboarding and renewal process begins with the Taxpayer accessing the Onboarding and Management Portal to generate an OTP. For a Taxpayer generating an OTP through the Onboarding and Management Portal, there are two options. The first option assumes the manual OTP entry, whereby Taxpayers can generate up to 100 OTPs in one request, which can then be used to onboard multiple EGS Unit(s) at the same time or renew the existing CSID(s). In the first option, the Taxpayer would need to manually enter the OTP(s) into the EGS Unit(s).
The second option assumes an automatic OTP entry, whereby the Taxpayer can access the Onboarding and Management Portal through their own EGS Unit, and the EGS Unit would then automatically read the OTP code through the header and automatically enter it into the EGS Unit, with no interference from the Taxpayer. The second scenario only allows for onboarding or renewing of the CSID for a single EGS Unit.

3.3.2.2. Process Flow

Option 1 - The process for generating the OTP code(s) on the Fatoora Portal and entering them manually is as follows:

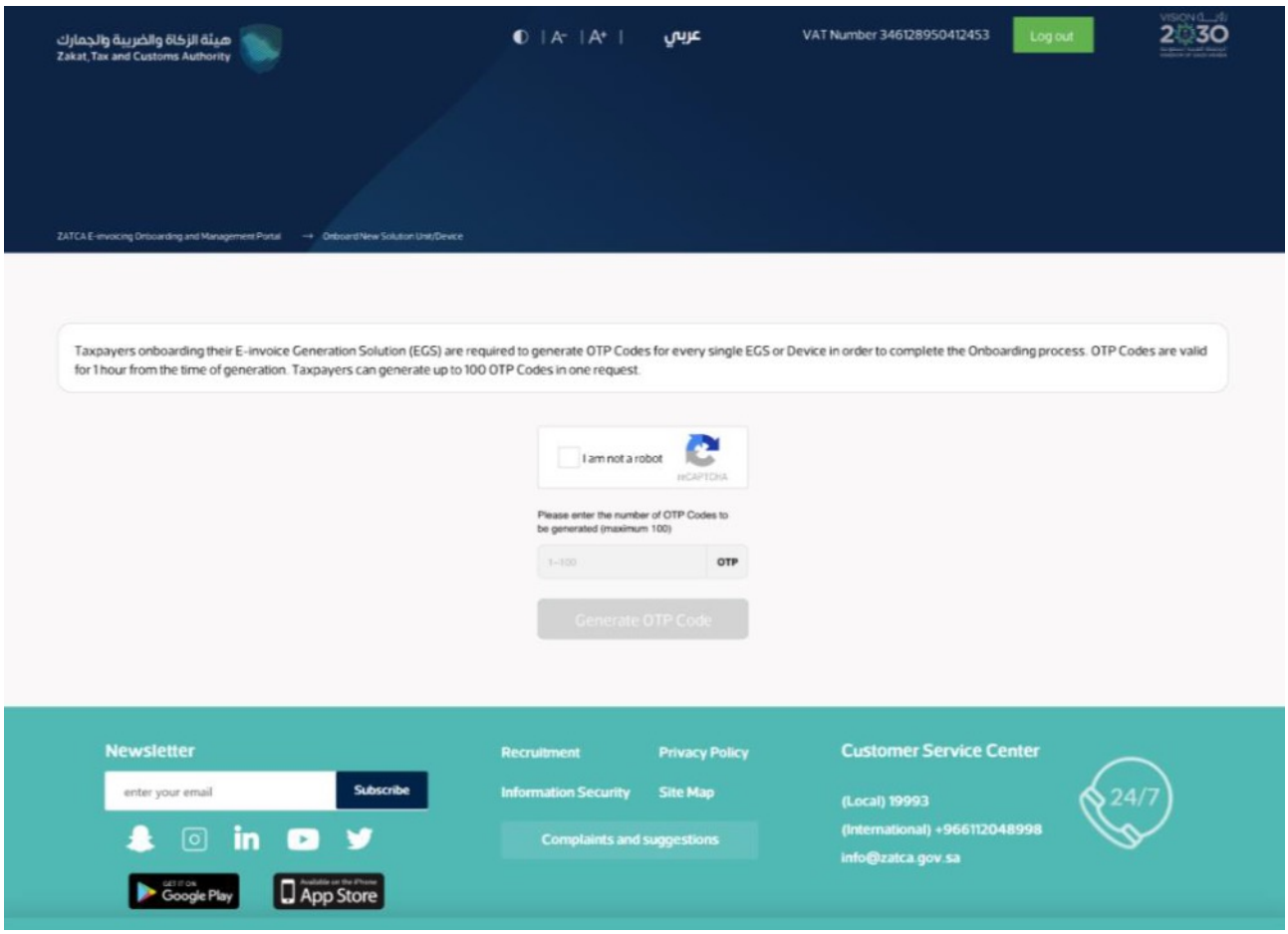
1. The Taxpayer accesses the Fatoora Portal through a browser (e.g. on a computer) that is not a part of their EGS Unit(s).

2. The Taxpayer clicks on a tile named "Onboard new solution unit/device" and is prompted to click on "Generate OTP code".



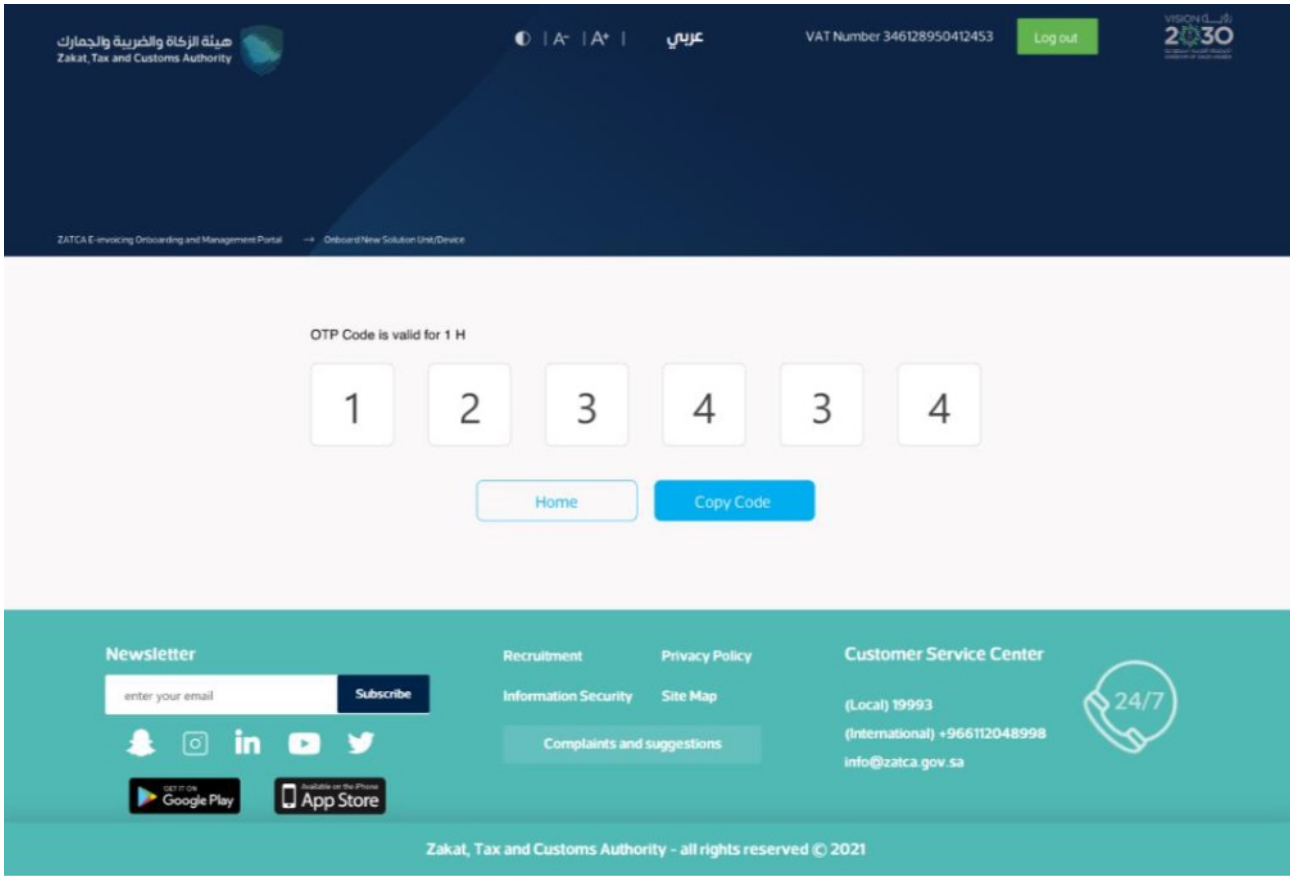
Fatoora Portal - accessing the "onboard new solution unit/device"

3. The Taxpayer choses to generate OTP code(s) for single or multiple EGS Unit(s) by entering the number of OTP codes they would like to be generated (User should enter 1 or more (up to 100 per request) based on the number of EGS Unit(s) that they would like to onboard).

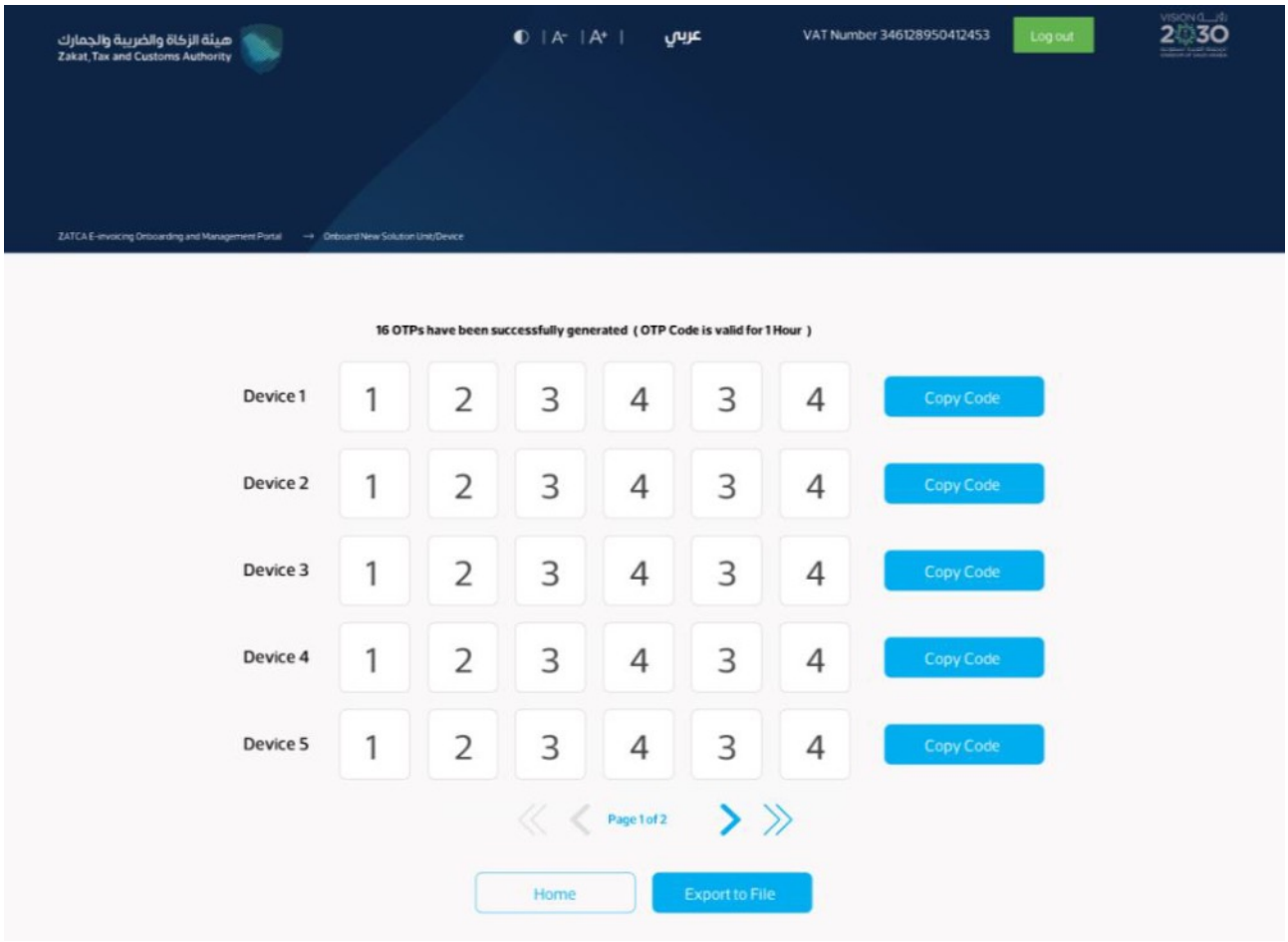


Fatoora Portal - specifying the number of OTPs needed by the taxpayer

4. The Fatoora Portal generates the OTP code(s) (valid for 1 hour), which will be displayed on the Portal and can be copied or downloaded in a file.



Fatoora Platform - single OTP generated to be entered manually on the EGS



Fatoora Platform - multiple OTPs generated to be entered manually on the EGS

5. The Taxpayer enters the OTP code(s) on their own EGS Unit(s) within 1 hour of the OTP code's generation.

Option 2 - The process for generating an OTP code on the Fatoora Portal through automatic entry is as follows:

1. The Taxpayer accesses the Fatoora Portal through their own EGS Units
2. The E-invoicing Generation Solution Onboarding and Management Portal automatically generates the OTP code (valid for 1 hour). As the Taxpayer is using their own EGS Unit to access the Onboarding and Management Portal, the OTP code will be automatically entered in the Taxpayers EGS Units (based on the https header on the browser) without interference from the Taxpayer.

3.3.3. Sending a Certificate Signing Request (CSR) in order to receive a Compliance CSID

3.3.3.1. Description

As a part of the first-time onboarding and renewal process, the Taxpayer's EGS Unit(s) must submit a Certificate signing request (CSR) to the E-invoicing Platform once an OTP is entered into the EGS unit. The CSR is an encoded text that the EGS Unit(s) submits to the E-invoicing Platform and the ZATCA CA in order to receive a Compliance CSID. This is a self-signed certificate issued by the E-invoicing Platform allowing clients to continue the Onboarding process.

The CSR inputs are as follows:

Inputs	Business Term	Description	Specification	Type of input (Manual/Auto-mated)
Common Name	Name or Asset Tracking Number for the Solution Unit	Provided by the Taxpayer for each Solution unit: Unique Name or Asset Tracking Number of the Solution Unit	Free text	Manual (Some solutions can have the feature to fill this automatically)

Inputs	Business Term	Description	Specification	Type of input (Manual/Automated)
EGS Serial Number	Manufacturer or Solution Provider Name, Model or Version and Serial Number	Automatically filled and not by the Taxpayer: Unique identification code for the EGS.	Free text	Manual (Some solutions can have the feature to fill this automatically)
Organization Identifier	VAT or Group VAT Registration Number	VAT Registration Number of the Taxpayer (Taxpayer / Taxpayer device to provide this to allow to check if the OTP is correctly associated with this TIN)	15 digits, starting and ending with 3	Automated (depending on solution)
Organization Unit Name	Organization Unit	The branch name for Taxpayers. In case of VAT Groups this field should contain the 10-digit TIN number of the individual group member whose EGS Unit is being onboarded	If 11th digit of Organization Identifier is not = 1 then Free text If 11th digit of Organization Identifier = 1 then needs to be a 10 digit number	Automated (depending on solution)
Organization Name	Taxpayer Name	Organization/Taxpayer Name	Free text	Automated (depending on solution)
Country Name	Country Name	Name of the country	2 letter code (ISO 3166 Alpha-2)	Automated (depending on solution)

Inputs	Business Term	Description	Specification	Type of input (Manual/Automated)
Invoice Type (Functionality Map)	Functionality Map	The document type that the Taxpayer's solution unit will be issuing/generating. It can be one or a combination of Standard Tax Invoice (T), Simplified Tax Invoice (S), (X), (Y). The input should be using the digits 0 & 1 and mapping those to "TSXY" where: 0 = False/Not supported 1= True/Supported (X) and (Y) are for future use and should be set to 0 by default for the time being. For example: 1000 would mean Solution will be generating Standard Invoices only. 0100 would mean Solution will be generating Simplified invoices (B2C) only and 1100 means Solution will be generating both Standard (B2B) and Simplified invoices (B2C).	Free text	Manual (Some solutions can have the feature to fill this automatically)

Inputs	Business Term	Description	Specification	Type of input (Manual/Automated)
Location	Location of Branch or EGS Unit	The address of the Branch or location where the device or solution unit is primarily situated (could be website address for e-commerce). Preferably in the Short Address format of the Saudi National Address https://splonline.com.sa/en/national-address-1/	Free Text	Automated (depending on solution)
Industry	Industry or Location	Industry or sector for which the device or solution will generate invoices	Free Text	Manual

Note: All CSR fields are mandatory and the input must follow the specification; otherwise, a CSR could be rejected.

Please refer to the EGS vendor's manual or support for information on how to resolve issues.

3.3.3.2. Process flow

The process for sending a CSR is as follows:

Once the OTP(s) has been entered into the Taxpayer's EGS Unit(s), either by the Taxpayer or through the automated process, the CSR process is initiated as per the below steps:

- Create CSR and include the required data
- Generate public/private key pair
- Send CSR to generate self signed certificate.

Possible errors that can occur when submitting a CSR include:

- Invalid OTP/OTC (not exactly six digits, not numeric)
- OTP/OTC not matching for this VAT Registration Number (OTP/OTC provided does not match an active valid OTP/OTC that was generated for this Taxpayer on the portal)
- OTP/OTC expired
- Invalid VAT Registration Number (Syntax, not corresponding to a valid VAT Registration Number on Fatoora Portal (ERAD)
- Invalid request type
- Missing fields (with details of the fields missing)
- One or more of the compliance steps has failed.

Please refer to the EGS vendor's manual or support for information on how to resolve issues.

3.3.4. Completion of the Compliance checks by the EGS Unit

3.3.4.1. Description

Once a CSR is sent successfully and the Compliance CSID is obtained, the Taxpayer's EGS Unit(s) must undergo compliance checks in order to ensure that the EGS Unit is able to generate compliant invoices. Upon successful completion and passing of the compliance checks, the EGS Unit receives a Production CSID. The Production CSID is a certificate issued by the ZATCA CA to enable clients to authenticate and use the core e-invoicing APIs.

3.3.4.2. Process Flow

It must be noted that the EGS performs the steps for the completion of the compliance checks automatically. The Taxpayer should refer to the EGS Guideline for the onboarding procedure appropriate to their device. The process for the completion of the compliance checks is as follows:

1. Formulate a compliant CSR and receive the CSID for onboarding / renewal (checking the capability of the EGS Units to perform renewal). Note that reaching compliance checks implicitly means that the EGS Unit has successfully acquired a compliance CSID
2. Based on the invoice type that has been added to the CSR, validation checks are required.

    a. If the Invoice Type is "1000", then the user should send 3 requests for
        i. Standard Tax Invoice (B2B)
        ii. Standard Debit Note (B2B)
        iii. Standard Credit Note (B2B)
    b. If the Invoice Type is "0100", then the user should send 3 requests for
        i. Simplified Tax Invoice (B2C)
        ii. Simplified Debit Note (B2C)
        iii. Simplified Credit Note (B2C)

The compliance verification of an EGS is concluded when the EGS Unit has undergone the compliance checks:

- The submitted documents are checked against all the validations as well as the relevant referential/ additional checks and all tests are successfully passed.
- Once found to be compliant, the compliance flag is checked.

In the case where one or more tests have failed or are not completed, the Taxpayer's EGS Unit will have to re-initiate the onboarding/renewal process starting from issuing a new OTP and a CSR and undergo the compliance tests again. For further details, please refer to the EGS User Manual.

3.3.5. Generating a new CSID for the EGS Unit or Renewing the existing CSID

3.3.5.1. Description

The CSID generation process occurs at the back-end of the E-invoicing Generation Solution and is initiated upon the successful completion of the compliance checks and can be regarded as the final step in the journey of receiving a new CSID. The process flow is common for both receiving a CSID for the first-time and also for renewing the existing CSID. However, for renewal, the existing CSID of the EGS Unit is revoked and a new one is issued.

3.3.5.2. Process Flow

The process for the generation and renewal of a CSID is as follows:

1. The EGS Unit(s) submit(s) a request to receive its production CSID(s).
2. ZATCA CA issues the CSID(s) for the Taxpayer's EGS Unit(s). In cases of renewal, the ZATCA CA first revokes the existing CSID and then issues the new one.
3. The Fatoora Platform relays the new CSID(s) to the Taxpayer's EGS Unit that originally submitted the CSR to the Fatoora Platform.

3.3.6. View List of EGS Unit(s)

3.3.6.1. Description

The Fatoora Portal has a tile that can be accessed from the dashboard, which contains a summary list of the logged-in Taxpayer's onboarded EGS Unit(s).

The list includes the following information for each EGS Unit that are provided as part of the CSR:

- Common Name: Name or Asset Tracking Number for the Solution Unit
- EGS Serial Number: Manufacturer or Solution Provider Name, Model or Version and Serial Number
- Organization Identifier: VAT or Group VAT Registration Number
- Organization Unit Name: Organization Unit
- Organization Name: Taxpayer Name
- Country Name
- Invoice Type: Functionality Map
- Location: Location of Branch or Device or Solution Unit
- Industry: Industry or location

In addition, the list also presents the following:

- CSID Status (Active or expired or revoked)
- Onboarding Date
- Certificate Expiry Date
- Revocation Date (if applicable)
- Revoke CSID (checkboxes to be selected)

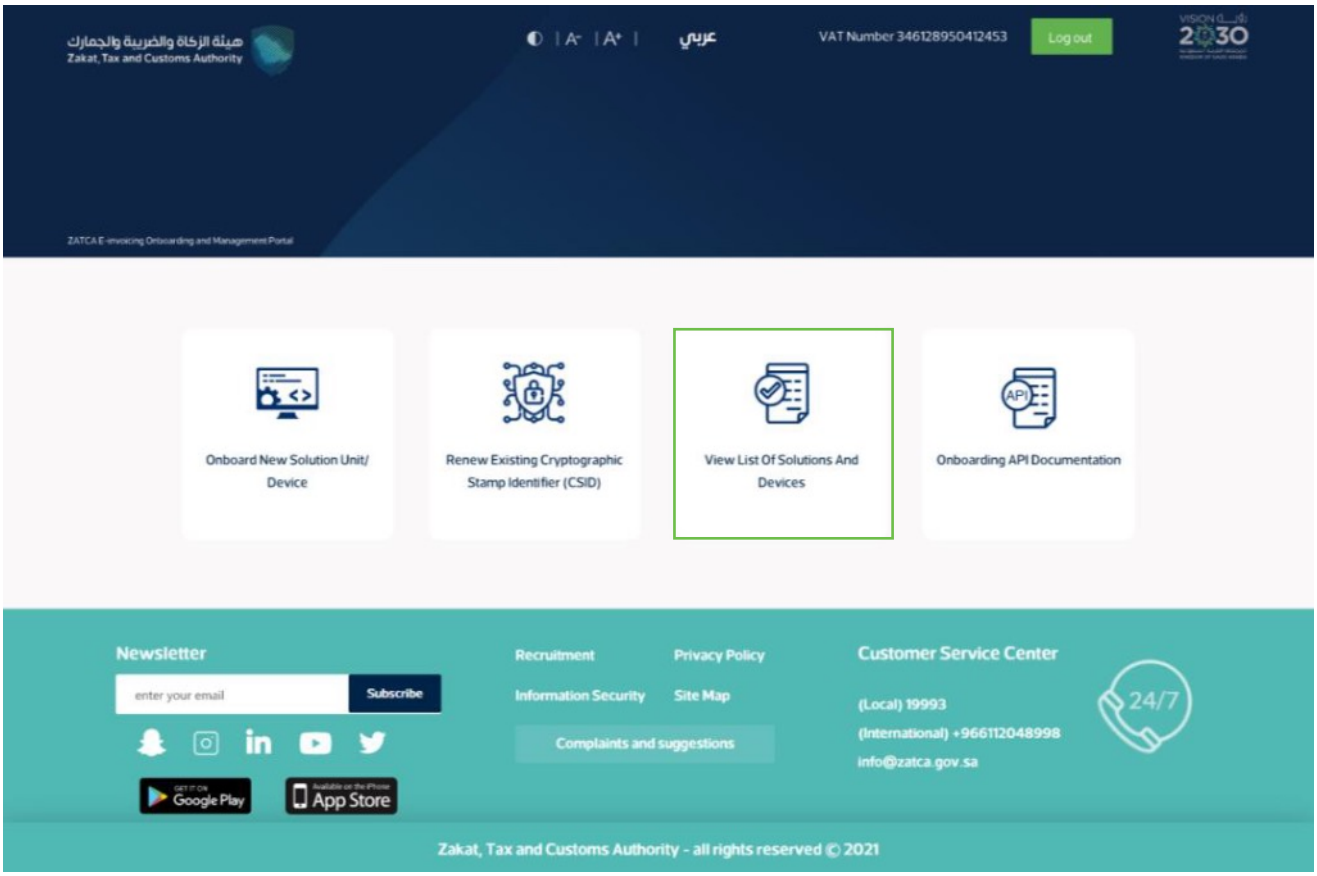
As an action button:

- Revoke CSID(s) (button appears upon selection of devices to be revoked)

3.3.6.2. Process Flow

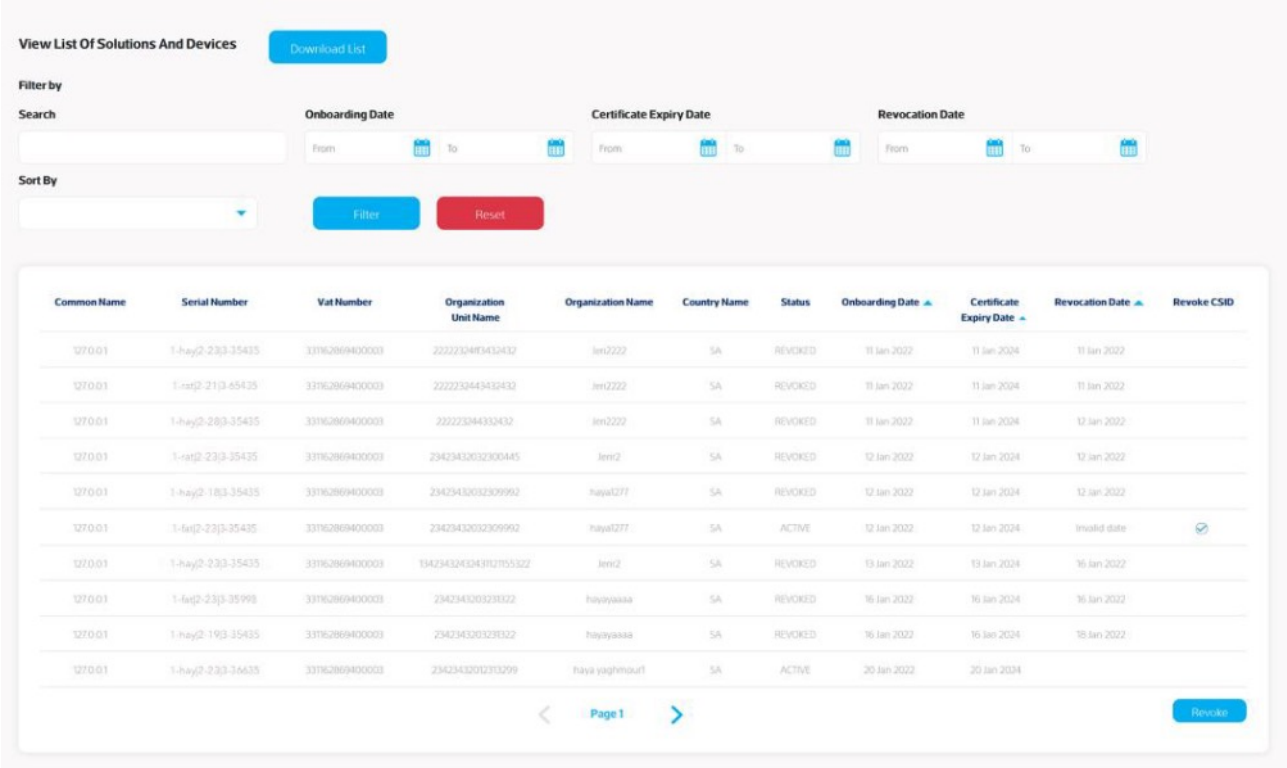
The process for viewing the list of all onboarded EGS Unit(s) on the Fatoora Portal as follows:

1. The Taxpayer accesses the Fatoora Portal
2. The Taxpayer clicks on "View List of Solutions and Devices"



Fatoora Platform - accessing the list of solution and devices

3. The Taxpayer will be able to view a list that includes a summary of all EGS Unit(s) that have been onboarded by the Taxpayer, as per the information provided above. The Taxpayer can filter, sort and search based on specific inputs available in the list of Solutions and Devices. (Sorting can take place using the blue arrows next to column headings as shows in the picture below).



Fatoora Platform - Dashboard for the onboarded solutions

***Please note that a Serial Number in the following example format "1-hayl2-23l3-35435" stand for: "1-Manufacturer or Solution Provider Namel2-Model or Versionl3-SerialNumber".**

Revocation of an existing CSID

3.3.7. Manual revocation of an existing CSID by the Taxpayer

3.3.7.1. Description

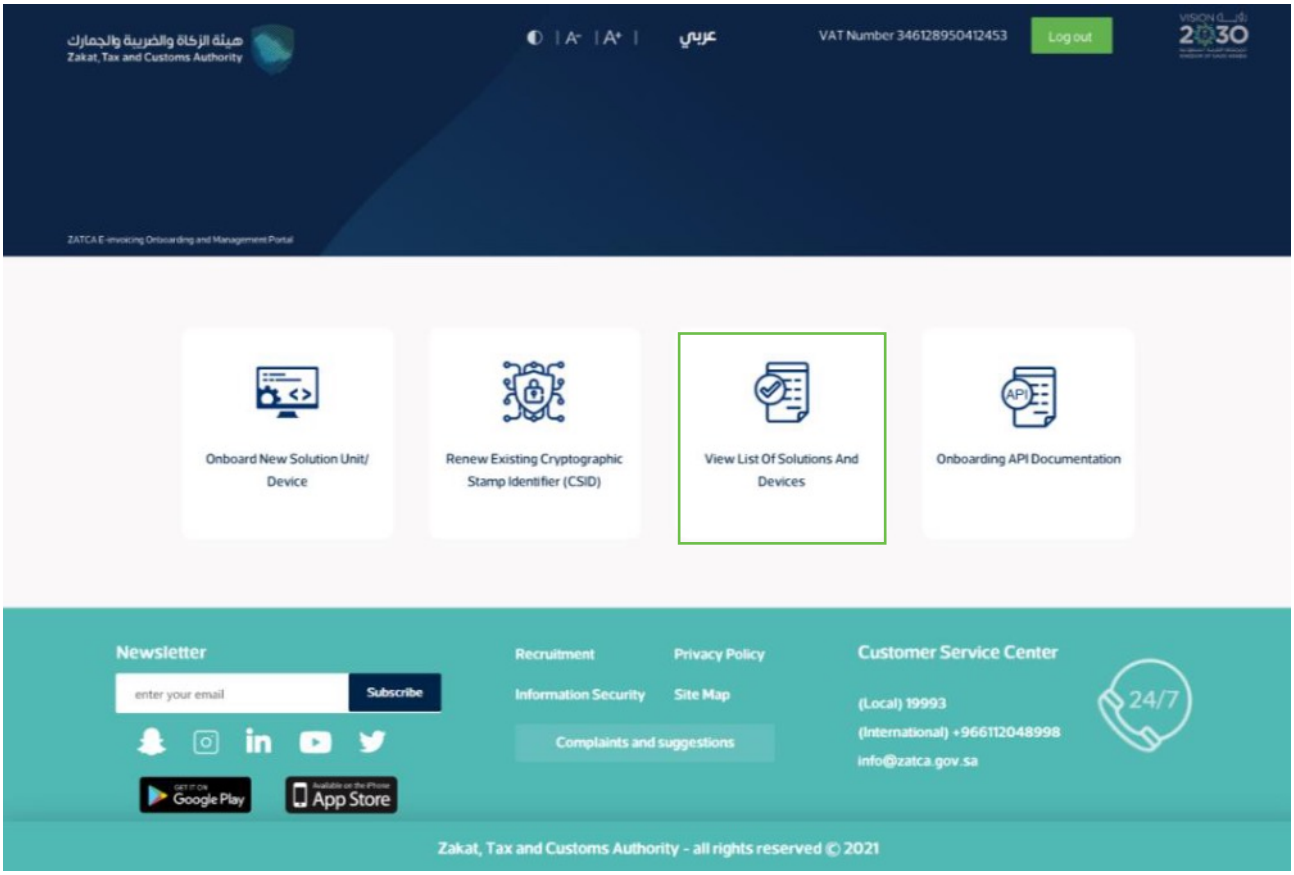
Taxpayers may wish to revoke their existing CSID(s) for a number of reasons, including:

- If the Taxpayer believes that the private key or the EGS Unit itself is compromised
- If the EGS Unit is discontinued or transferred to another Taxpayer or sold
- If the Taxpayer discovers that the information in the CSID is not accurate
- If the EGS Unit is lost, stolen or damaged
- If the Taxpayer discovers that unauthorized onboarding of a EGS Unit has occurred.

3.3.7.2. Process Flow

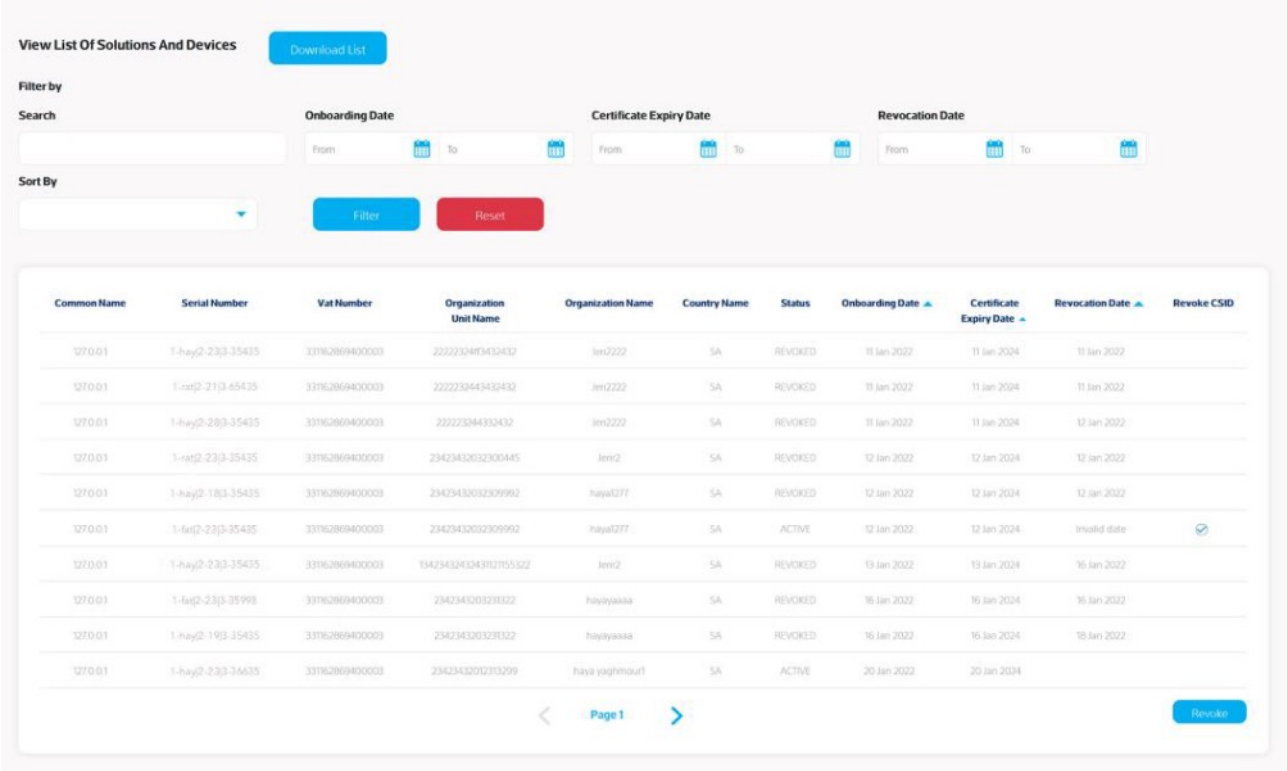
The process for Taxpayers revoking one or more CSID(s) is as follows:

1. The Taxpayer accesses the Fatoora Portal
2. The Taxpayer clicks on "View List of Solutions and Devices"



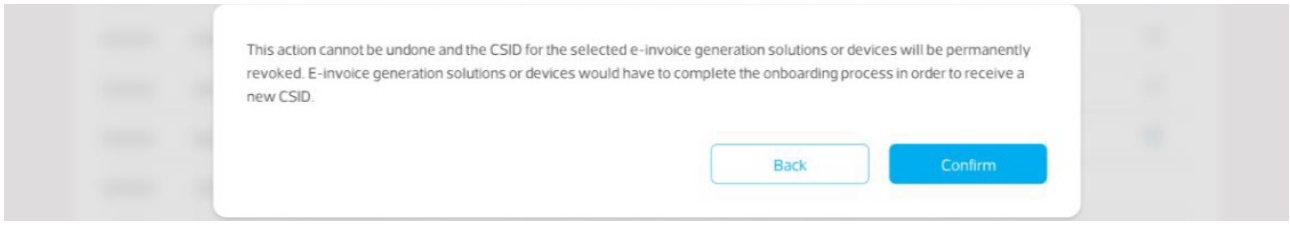
Fatoora Platform - accessing the list of solution and devices

3. The Taxpayer can see which devices are active and can select the EGS unit(s) to be revoked
4. The Taxpayer clicks on the "Revoke" button at the bottom of the screen



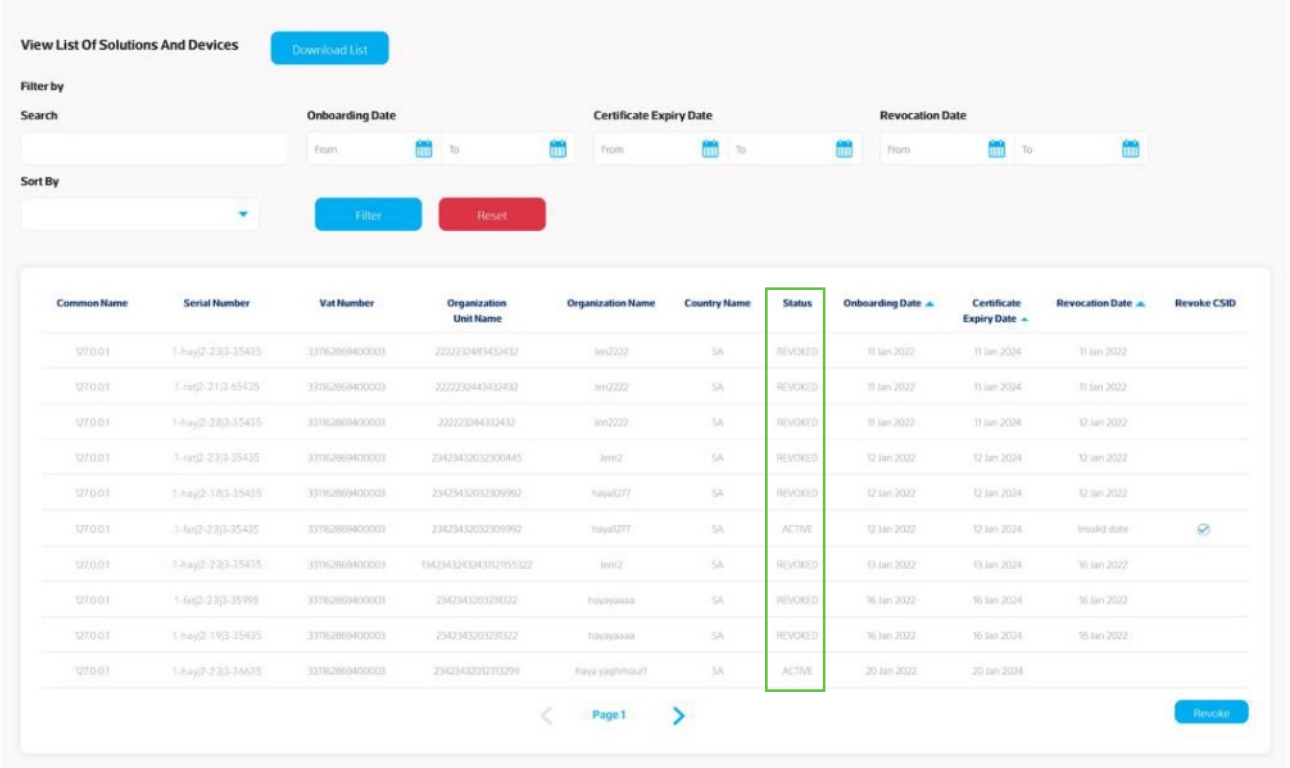
Revocation of an existing CSID

5. The Taxpayer is prompted to click on a confirmation message before proceeding with the revocation



6. The CSID(s) is/are revoked and the EGS Unit(s) is/are longer active

7. The Status of the CSID of the devices can be seen as 'Revoked' on the View List.



3.3.8. Automatic revocation of CSID(s) due to VAT Deregistration or Suspension

3.3.8.1. Description

The automatic revocation process involves ZATCA CA performing a revocation of CSID(s) associated with Taxpayers whose VAT registration number status (TRN) on the Fatoora Portal (ERAD) changes from "Active" or "Reactive" to "Deregistered" or "Suspended". In this process, ZATCA CA revokes the CSID(s) for Taxpayers with a VAT registration status of "Deregistered" or "Suspended".

For individual VAT Taxpayers, automatic revocation of the CSID(s) would apply in the following case:

1. The Taxpayer's VAT registration status on the Fatoora Portal (ERAD) is "Deregistered" or "Suspended".

For VAT groups, automatic revocation of CSID(s) would apply in the following cases:

1. Creating a tax group: ZATCA automatically revokes any existing CSIDs associated with the individual Taxpayers (whether they are the group representative or members) who have joined the tax group (if applicable).
2. Adding one or more members to an existing group: ZATCA automatically revokes any existing CSIDs associated with the individual Taxpayers (group members) who have joined the group (if applicable).
3. Entire group is disbanded: ZATCA automatically revokes any existing CSIDs associated with the group (whether they are for shared devices or devices associated with individual group members).
4. Group representative changes (replaced by existing member or new member): ZATCA automatically revokes any existing CSIDs associated with the group

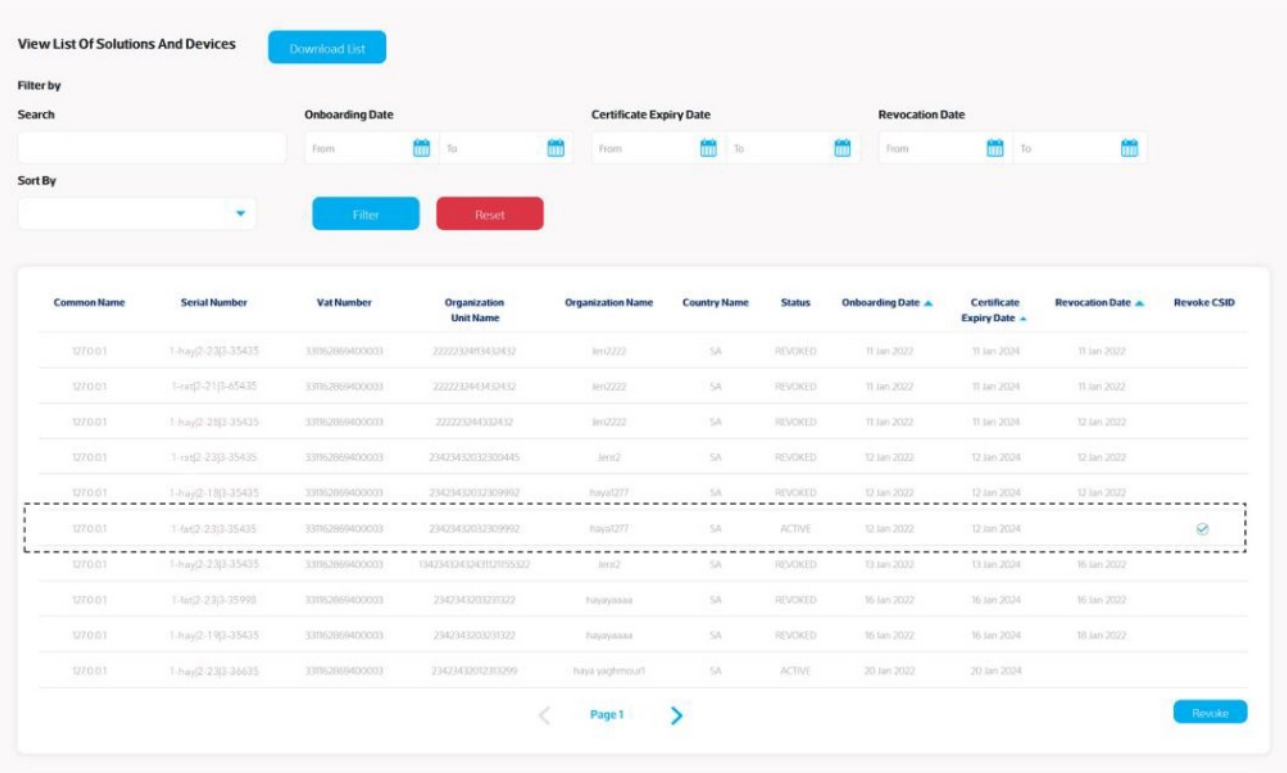
(whether they are for shared devices or devices associated with individual group members).

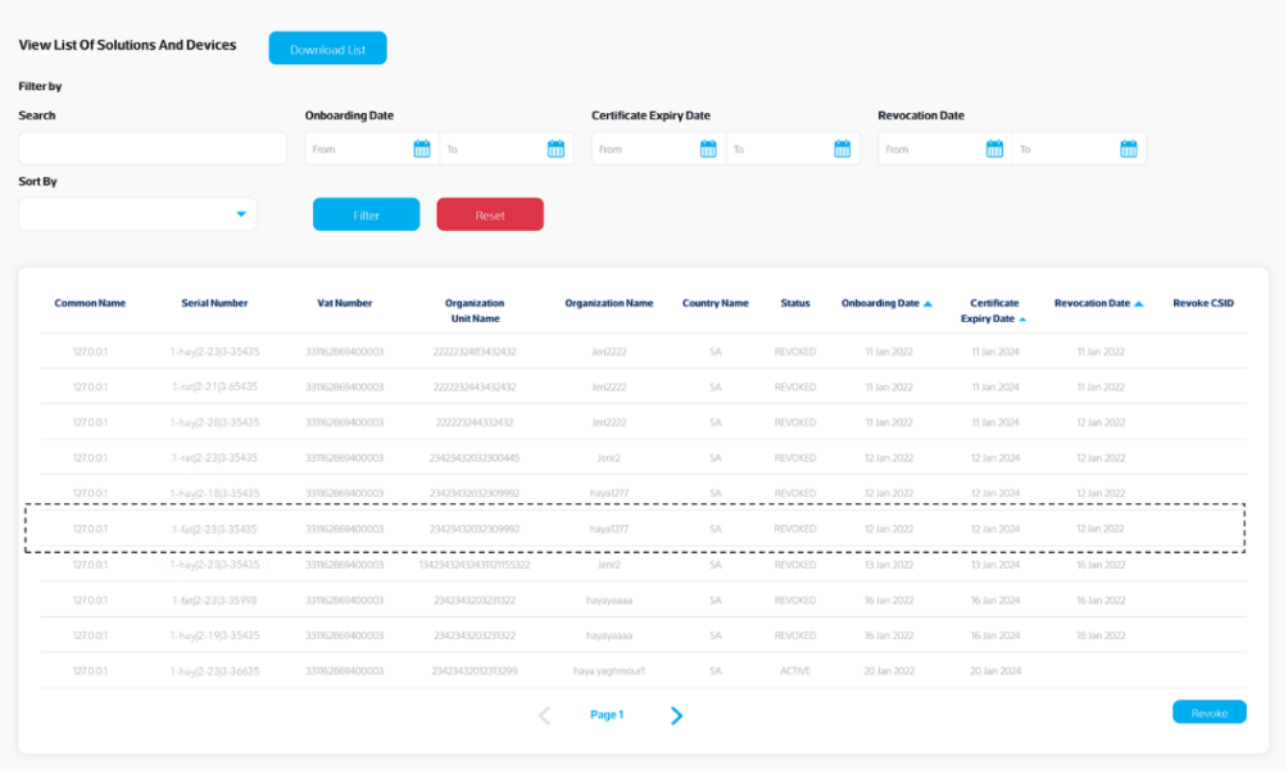
Note: Taxpayers whose VAT registration status used to be "Active" or "Reactive" but changes to "Deregistered" or "Suspended" would still be able to access the Fatoora Portal for a period of 90 days but can only view a list of their previously onboarded EGS Units and cannot use any other onboarding functionalities such as generating an OTP. Once the buffer period of 90 days is over, these Taxpayers will no longer be able to access the Onboarding and Management Portal.

3.3.8.2. Process Flow

The process for the automatic revocation of a CSID is as follows:

1. Taxpayer's VAT registration status on the Fatoora Portal (ERAD) changes from "Active" or "Reactive" to "Deregistered" or "Suspended"
2. ZATCA CA revoke the CSID(s) for Taxpayers with a VAT registration status of "Deregistered" or "Suspended"
3. The CSID status available on the list of devices changes from "Active" to "Revoked"





3.4. VAT Group Onboarding Scenarios

3.4.1. Specific tax group Onboarding Scenarios

VAT Groups follow the same onboarding, renewal and revocation processes as individual Taxpayers. The table below summarizes the scenarios applicable to VAT groups that would have an impact on Onboarding:

#	Group Scenarios	Impact on e-invoicing (Onboarding)
1	Creating a Tax Group	• Tax group representative conducts the Onboarding and mentions in the CSR the members associated with the device (in the Organization Unit Name field which would contain the TIN of the member(s) who will be using the device) • ZATCA automatically revokes any existing CSIDs associated with the individual Taxpayers (whether they are the group representative or members) who have joined the tax group (if applicable)

#	Group Scenarios	Impact on e-invoicing (Onboarding)
2	Adding one or more members to an existing group (Add another TIN to an existing device)	• If the device is owned at a group level (i.e. shared device) and a new member joins the group, this has no impact on the CSID. The liability is on the group and the tax group representative to ensure that the shared device is issuing correct invoices on behalf of the group • If the device is owned by an individual specific member of the group, the group representative would need to onboard the device associated with this specific member • ZATCA automatically revokes any existing CSIDs associated with the individual Taxpayers (whether they are the group representative or members) who have joined the group (if applicable)
3	Removing one or more existing members from the group (Cannot include the representative)	• If the device is owned at a group level (i.e. shared device) and a member leaves the group, this has no impact on the CSID. The liability is on the group representative to ensure that the shared device is issuing correct invoices on behalf of the tax group • If the device is owned by an individual specific member of the group, the group representative would need to revoke the device associated with this specific member • The individual Taxpayer would have to onboard any devices which they will be using to generate e-invoices (individually and not as part of a group) (if applicable)
4	Entire group is disbanded	• ZATCA automatically revokes any existing CSIDs associated with the group (whether they are for shared devices or devices associated with individual group members) • The individual Taxpayer would have to onboard any devices which they will be using to generate e-invoices (individually and not as part of a group) (if applicable)
5	Group representative changes (replaced by existing member or new member)	• ZATCA automatically revokes any existing CSIDs associated with the group (whether they are for shared devices or devices associated with individual group members) • New tax group representative conducts the onboarding process according to the latest group setup

3.4.2. VAT Group Onboarding Roles

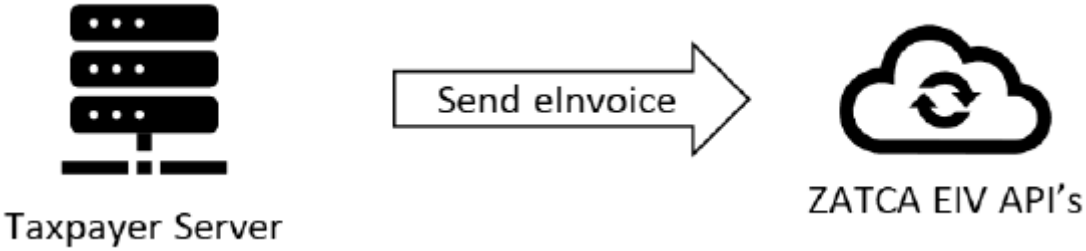
Step	Group Representative	Group Member
Login to Fatoora Platform	Yes	No
Click on onboard new device	Yes	No
Generate OTP	Yes	No
Enter OTP and generate CSR from device (including assigning single TIN)	Yes (must mention TIN to be associated with the device)	Yes (must mention TIN to be associated with the device)
Complete compliance	-	-
Install CSID	-	-
View List of Devices	Yes	Yes (only for the first 90 days (configurable) from the date when they join the group)
Revoke CSID	Yes	No

3.5. Common Onboarding/CSID related scenarios faced by Taxpayers

This section provides an overview of the most common invoicing structures implemented by Taxpayers and identifies for each scenario, how the CSID structure should be set up in order to allow accurate issuing, signing and sending of e-invoices to ZATCA's e-invoicing APIs.

3.5.1. Centralized Server - On Premise or Cloud

In the case of a centralized server, whether it is on premise or cloud, a CSID is required on the server for both signing and authentication to ZATCA e-invoicing APIs. There should be one CSID per Taxpayer and also one CSID per unique sequence of generated documents.



3.5.2. Branch Based Smart POS Devices Issuing and Sending Invoices

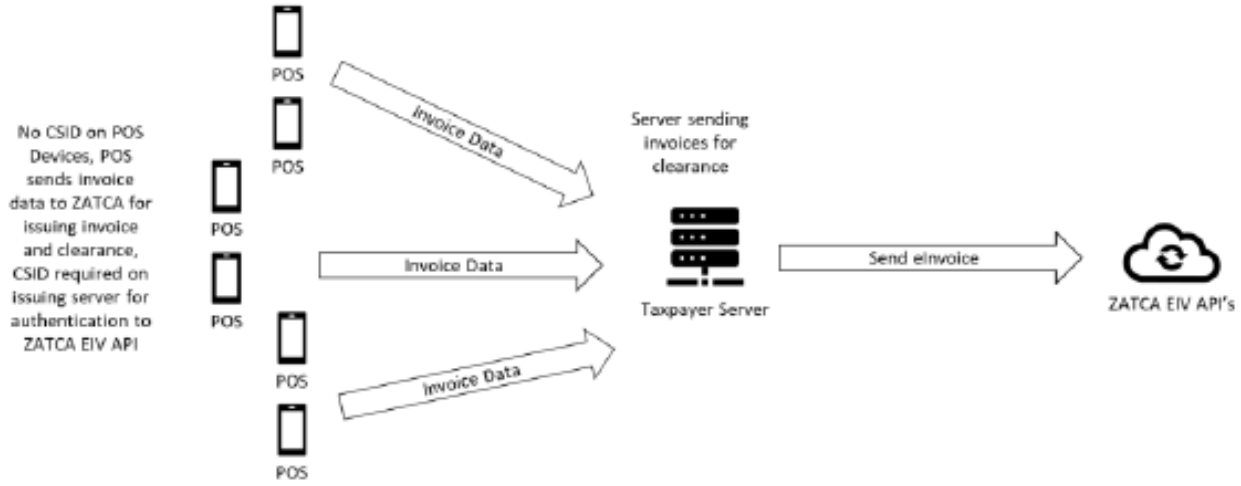
In cases where Branch POS devices are issuing and sending invoices, a CSID is required on each POS device that will be signing and sending invoices to ZATCA e-invoicing APIs.

3.5.3. Branch Based Standard POS Devices with Branch Servers and Centralized Sending Server

For branch based POS devices with branch servers issuing invoices and a centralized server sending invoices to the ZATCA e-invoicing APIs - if the POS devices are dumb terminals and the server stamps the invoices before presenting them to the customers, then no CSIDs are required on the POS devices. However, a CSID is required on the branch-based servers for signing the invoices and a CSID is required on the server sending the invoices for authentication to ZATCA's e-invoicing APIs.

3.5.4. POS Devices Unable to Sign Invoices

In the case of dumb terminal POS devices issuing invoices and sending them to a Taxpayer server, which will send the invoices to the ZATCA e-invoicing APIs for clearance - then the server must stamp the invoices and apply the QR code before presenting the invoice to the customers from the POS. In this case, the POS device does not need to have its own CSID and the CSID can be on the server which is stamping and applying the QR code on simplified invoices (B2C). It is important to note that Standard documents (B2B) are still expected to be submitted prior to completing the transaction as the Buyer is expected to receive a valid document which has been cleared by ZATCA.



4. Reporting and Clearance of e-invoices

4.1. Introduction and Objectives of Reporting and Clearance

The primary objective of the Reporting and Clearance functionalities is to allow all Taxpayers subject to e-invoicing in the Kingdom to submit their e-invoices, credit or debit notes to ZATCA. The documents need to be submitted by the Seller in most cases with the exception of Self-Billed documents which need to be submitted by the Buyer.
Once Taxpayers' EGS have been successfully onboarded and have obtained their unique Cryptographic Stamp Identifiers (CSIDs), they will be able to submit e-invoices, credit and debit notes to ZATCA's Fatoora platform using APIs. As mentioned earlier in the Onboarding section, the EGS can continue to submit e-invoices, credit or debit notes as long as the:

- Associated CSID has not expired
- Associated CSID has not been revoked either by the Taxpayer itself or as a result of VAT De-registration or Suspension (due to joining a VAT Group)
- Associated CSID was obtained for the correct Functionality Map
    - 1000 for Standard documents only (B2B)
    - 0100 for Simplified documents only (B2C)
    - 1100 for both Standard (B2B) and Simplified documents (B2C)

Similar to the Integration Sandbox, the Reporting and Clearance process is completely an API driven process, i.e. after an EGS has been successfully onboarded, it will communicate directly with the Fatoora platform without the need to login to the Fatoora portal.

4.2. Reporting and Clearance Overview

As mentioned above both Reporting and Clearance are two different e-invoicing transactions between Taxpayer's EGS units and ZATCA's Fatoora platform using APIs. The sharing of the e-invoices, credit or debit notes between the Seller and Buyer happens outside of this interaction that is not controlled by ZATCA.

The Fatoora Platform is the ZATCA system that:

- receives these documents via API from the Taxpayer's E-invoicing Generation Systems (EGS)
- processes and validates submitted documents as part of the Clearance and Reporting in line with the standards mentioned above
- sends back the outcome of the validations to the Taxpayer's EGS (and additionally key events and failure points will be communicated using notifications)
- stores valid and accepted documents (with warnings) for ZATCA.

The primary requirement for Taxpayers for Reporting and Clearance is to have compliant E-invoice Generation Solutions (EGS) which have been onboarded and associated with unique Production Cryptographic Stamp Identifiers (PCSIDs) before they can start submitting generated e-invoices, credit or debit notes to Fatoora Platform.

As with the Onboarding, Taxpayers need to be registered for VAT in order to submit e-invoices, credit or debit notes to ZATCA. The Fatoora Platform will automatically revoke PCSIDs associated with VAT Taxpayers who have been de-registered or suspended (after joining a VAT Group). In case of the latter, the VAT Group will need to re-onboard the EGS of all members and obtain PCSIDs which are associated with the VAT Registration Number (TRN) of the VAT Group. The Representative Member of the VAT Group is responsible for initiating the Onboarding, Renewal and managing of the Revocation processes.

4.3. Description of the Reporting and Clearance Processes

Taxpayer's EGS unit(s) must submit their documents to ZATCA in the XML format and not in the PDF A/3 format.

A Standard Invoice, Standard Credit Note and Standard Debit Note are collectively referred to as "Standard Documents" (B2B).

Similarly, A Simplified Invoice, Simplified Credit Note and Simplified Debit Note are collectively referred to as "Simplified Documents" (B2C).

The processing first involves validating the documents based on the following:

- Business rules in the XML Implementation Standards, Data Dictionary and E-invoicing Resolution
- Additional referential checks which are additional validations performed
- Exception handling which offers some tolerances to the outcomes of the validations by treating some errors as warnings without rejecting the submitted document entirely.

There are three potential outcomes of the validations:

- Invalid document - The document has at least one fatal error that results in it not being considered as a valid document
- Accepted document with warnings - The document has no fatal errors but has at least one warning that results in it not being considered as a compliant document (note that this is essentially the outcome of the exception handling mentioned above) however one that can still be considered as an accepted document
- Valid / complaint document - The document has no fatal errors and no warnings that results in it being considered as a valid document.

Taxpayers are encouraged to make suitable arrangements with an EGS service provider for resolving the errors or warnings notified by ZATCA's Fatoora Platform in a timely manner.

Additionally for invalid documents, the Fatoora Platform generates a hash of the entire document including UBL extensions and stores this as a reference and as a comparison point.

In the case of Standard documents (B2B), the Fatoora Platform applies a cryptographic stamp on behalf of ZATCA as well as a QR code during Clearance process.

Along with the storage, the Fatoora Platform sends the response back to the Taxpayers' EGS based on the following:

Outcome	Standard Documents (B2B)	Simplified Documents (B2C)
Valid Document	Send the Document back to the Taxpayer's EGS along with the applied ZATCA cryptographic stamp and QR code string	Send a confirmation back to the Taxpayer's EGS via API response that the document is valid
Accepted Document with warnings	Send the Document back to the Taxpayer's EGS along with the applied ZATCA cryptographic stamp, QR code string and the warning messages	Send a confirmation back to the Taxpayer's EGS that the document has been accepted along with the warning messages
Invalid Document	Send a response back to the Taxpayer's EGS stating that the document was rejected along with the error message/s	Send a response back to the Taxpayer's EGS stating that the document was rejected along with the error message/s

Taxpayers must generate documents in a single sequence per EGS that it has onboarded and this sequence applies to both Standard (B2B) and Simplified (B2C) documents it has generated. The Previous Document Hash (PDH) of a document should always be equal to the Hash of the last document that generated prior to the Submission. Note that documents need not be submitted in the same sequence as they were generated as long as the PDH in the document always refers to document of the last document that was generated. The PDH must be maintained even in the case of documents which were rejected by ZATCA's Fatoora platform as the platform does record the document hash of rejected submissions.

4.3.1. Reporting

As mentioned above Reporting applies for Simplified documents (B2C) which are generally applicable for B2C (Business to Consumer) transactions. Accordingly, ZATCA's E-invoicing regulations allow Taxpayers (Sellers) to submit their Simplified Documents (B2C) within 24 hours of the transaction being completed.

In that respect, the Reporting process involves:

1. The Seller generates an e-invoice, credit or debit note for a transaction using its EGS
2. The Seller submits the document to ZATCA's Fatoora Platform using the Reporting API within 24 hours
3. The Fatoora Platform validates the submitted document against ZATCA specified standards and specifications
4. Depending on the validations, the submission is either:
    1. Accepted as a valid document which is sent as a confirmation in the API response
    2. Accepted with one or more warning(s) which is (are) listed in the API response
    3. Rejected with one or more error(s) which is (are) listed in the API response
5. Steps 1-4 are repeated with the next submission.

Notes:

- **In the case of 4(1) and 4(2) above, the Fatoora Platform stores the submitted document (excluding any additional fields over and above the ZATCA specifications) along with any warning details.**
- **The Seller must include its Cryptographic Stamp and QR code as part of the submission. ZATCA's Fatoora Platform does not stamp Simplified documents (B2C).**
- **For warnings or errors, the Taxpayer must reach out to its Solution Developer / Provider and can leverage ZATCA's published XML Implementation Standards, Data Dictionary, Security Features, Compliance and Enablement Toolbox (SDK or Web based Validator) and/or Integration Sandbox to ensure the compliance of future submissions.**

4.3.2. Clearance

As mentioned above Clearance applies for Standard documents (B2B) which are applicable for B2B (Business to Business) transactions and generally involves two VAT Registered Taxpayers. ZATCA's e-invoicing regulations require that the Seller submit their Standard documents (B2B) for Clearance prior to providing the documents to the Buyer. In other words the Standard document (B2B) is only considered valid if it has already been cleared by ZATCA (i.e. it includes ZATCA's Clearance stamp).

Standard documents (B2B) are generally submitted by the Seller; however, Standard documents (B2B) under Self-Billing are submitted by the Buyer. It is mandatory for the Seller and Buyer to be in a Self-Billing agreement which has been approved by ZATCA.

Accordingly the Clearance process involves:

1. The Seller (or Buyer in the case of Self-Billing) generates an e-invoice, credit or debit note for a transaction using its EGS
2. The Seller (or Buyer in the case of Self-Billing) submits the document to ZATCA's Fatoora platform using the Clearance API
3. The Fatoora platform validates the submitted document against ZATCA specified standards and specifications
4. Depending on the validations, the submission is either:
    1. Accepted as a valid document and the Fatoora platform Stamps the document and includes/updates the QR code as part of the API response
    2. Accepted with one or more warning(s) and the Fotoora platform Stamps the documents and includes/updated the QR code as part of the API response along with list and details of the warnings
    3. Rejected with one or more error(s) which is (are) listed in the API response
5. Steps 1-4 are repeated with the next submission.

Notes:

- In the case of 4(1) and 4(2) above, the Fatoora Platform stores the submitted document (excluding any additional fields over and above the ZATCA specifications) along with any warning details.
- The Seller may optionally include its Cryptographic Stamp and QR code as part of the submission. In such cases, the response from ZATCA's Fatoora Platform will add an additional Stamp to the document and update the QR code.
- If ZATCA has disabled the Clearance functionality, even Standard documents (B2B) can be submitted using the Reporting API. In such cases, ZATCA's Platform does not stamp Standard documents (B2B).
- For warnings or errors, the Taxpayer must reach out to its Solution Developer / Provider and can leverage ZATCA's published XML Implementation Standards, Data Dictionary, Security Features, Compliance and Enablement Toolbox (SDK or Web based Validator) and/or Integration Sandbox to ensure the compliance of future submissions.

5. Signing Process

In this section, step-by-step instructions will be demonstrated towards acquiring a Signed Invoice.

5.1 SHA-256 Hash - Hashing algorithm

The main reason for using SHA-256 is to strengthen the security and protect the data by ensuring it doesn't have any known vulnerabilities that make it insecure, and it has not been "broken" unlike some other popular hashing algorithms.
The output of a hashing algorithm SHA256 will always be the same, consisting of 256 bits (32 bytes), which is displayed as 64 alphanumeric characters.

5.2 Signing steps

Step 1: Generate Invoice Hash

To generate the invoice hash below steps can be followed:

1. Open the invoice XML file.
2. Remove the tags mentioned in the table below using the XPath.
3. Remove the XML version, all the comments and empty lines.
4. Hash the new invoice body using SHA-256 (output). (e.g.:4275447b15b89d6bf809a137f5af-fae89a7f3973bf7af1d0f290e51bbc1eabfe)
5. Encode the hashed invoice using base64 (output). (e.g.:NDI3NTQ0N2IxNWI4OWQ2YmY4MDlhMT-M3ZjVhZmZhZTg5YTdmMzk3M2JmN2FmMWQwZjI5MGU1MWJiYzFlYWJmZQ==)

   Note: All these values will be used in later steps.

Tags to be removed from invoice	XPath, Use this path to find the target tag
UBLExtension	*[local-name()='Invoice']//*[local-name()='UBLExtensions']
QR	*[local-name()='AdditionalDocumentReference'][cbc:ID [normalize-space(text()) = 'QR']]
Signature	*[local-name()='Invoice']//*[local-name()='Signature']

Step 2: Generate Digital Signature

1. Sign the generated invoice hash with ECDSA using the private key (output). (e.g.:MEQCIGvLa-1f3uMCe0AidKUWJ5ghMiDMRcC0qO78ntcTKVOYgAiAKBkX+uuFhbIcye3JznNa45qH1twILFu/qPzEQ9HMNLw==)
   Note: This value will be used in later steps.

Values to be used
Generated Invoice Hash from Step 1 (not encode)
Private key

Step 3: Generate Certificate Hash

1. Hash the certificate using SHA-256 (output). e.g.:69a95fc237b42714dc4457a33b94cc452fd9f-110504c683c401144d9544894fb
2. Encode the hashed certificate using base64 (output).

e.g.:NjlhOTVmYzIzN2I0MjcxNGRjNDQ1N2EzM2I5NGNjNDUyZmQ5ZjExMDUwNGM2ODNjNDAx-MTQ0ZDk1NDQ4OTRmYg==

Note: All these values will be used in later steps.

Values to be used
Certificate

Step 4: Populate the Signed Properties Output

1. Open the original invoice (not updated in Step 1).
2. Remove the tags UBLExtentions, QR and Signature (refer to their XPath mentioned in Step 1).
3. Replace the removed tags mentioned below with the same tags but without values (to be filled in later steps).
4. Refer to the below table to fill mentioned fields with their corresponding values using the related XPath.

Notes:

- The original invoice XML file is used in this step (not the one updated in the 1st step).
- Populated Signed Properties will be used in the next step.

Fields	Values	XPath
DigestValue	Encoded certificate hashed from Step 3	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningCertificate/xades:Cert/xades:CertDigest/ds:DigestValue
SigningTime	Sign timestamp as current datetime	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningTime
X509IssuerName	Certificate issuer name	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties/xades:SignedSignatureProperties/xades:SigningCertificate/xades:Cert/xades:IssuerSerial/ds:X509IssuerName
X509SerialNumber	From the certificate (decoded)	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:Object/xades:QualifyingProperties/xades:SignedProperties//xades:SignedSignatureProperties/xades:SigningCertificate/xades:Cert/xades:IssuerSerial/ds:X509SerialNumber

Step 5: Generate Signed Properties Hash

1. Get the properties tag only using the XPath (don't remove from XML file).
2. Hash the property tag using SHA-256 (output). (e.g.:c1c0ccb5481fb9a539432b-fe72a81a3da660a231339df6be513913be25f7ac14)
3. Encode the hashed property tag using base64 (output). (YzFjMGNjYjU0ODFmYjlhNTM5NDMyYm-ZlNzJhODFhM2RhNjYwYTIzMTMzOWRmNmJlNTEzOTEzYmUyNWY3YWMxNA==)

Note: All these values will be used in later steps.

Values to be used	XPath
Populated Signed Properties from Step 4	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:-Object/xades:QualifyingProperties/xades:SignedProperties

Step 6: Populate The UBL Extensions Output

1. Use the invoice XML file acquired from Step 4.
2. Refer to the below table to fill mentioned fields with their corresponding values using the related XPath.

Note: We are using the updated invoice acquired from the Step 4

Fields	Values	XPath
SignatureValue	Digital Signature from Step 2	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:SignatureValue
X509Certificate	Certificate	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate
DigestValue	Encoded signed Properties hash from Step 5	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:SignedInfo/ds:Reference[@URI='#xadesSignedProperties']/ds:DigestValue
DigestValue	Encoded invoice hash from Step 1	/Invoice/ext:UBLExtensions/ext:UBLExtension/ext:ExtensionContent/sig:UBLDocumentSignatures/sac:SignatureInformation/ds:Signature/ds:SignedInfo/ds:Reference[@Id='invoiceSignedData']/ds:DigestValue

To finalize the signing, refer to the Section 6 - QR code.

Additional reference: Openssl commands & urls for support

Openssl:

- Hash function: openssl dgst -sha256 <xml_file_name>
- Generate private key: openssl ecparam -name secp256k1 -genkey -noout -out PrivateKey.pem
- Generate public key: openssl ec -in PrivateKey.pem -pubout -conv_form compressed -out PublicKey.pem
- Generate csr: openssl req -new -sha256 -key privateKey.pem -extensions v3_req -config config.cnf -out taxpayer.csr

URLs:

- XML Canonical online tool: http://www.soapclient.com/xmlcanon.html
- XPATHER ONLINE TOOL: http://xpather.com/
- Hashing online tool: https://emn178.github.io/online-tools/sha256.html
- ENCODER BASE64 online: https://www.base64encode.org/
- ECDSA SIGN online: https://8gwifi.org/ecsignverify.jsp
- CSR and certificate decoder online: https://certlogik.com/decoder/
- TEXT to HEXA online: https://www.online-toolz.com/tools/text-hex-convertor.php
- private key decoder online: http://certificate.fyicenter.com/2145_FYIcenter_Public_Private_Key_Decoder_and_Viewer.html#Result
- TLV QR decoder online: https://emvlab.org/tlvutils/

6. QR code

Structure of the QR code For Electronic Tax Invoices

It is mandatory to generate and print QR code encoded in Base64 format with up to 700 characters that must contain the fields specified in the below table as per Annex (2) of the Controls, Requirements, Technical Specifications and Procedural Rules for Implementing the Provisions of the E-Invoicing Regulation.

The QR code fields shall be encoded in Tag-Length-Value (TLV) format with the tag values specified in the "Tag" column of the adjacent table.

The TLV encoding shall be as follows:

- Tag: The tag value as mentioned above stored in one byte.
- Length: The length of the byte array resulted from the UTF8 encoding of the field value. The length shall be stored in one byte.
- Value: The byte array resulting from the UTF8 encoding of the field value.

Field Definition for the QR Code

Description	Tag	Enforcement date
Seller's name	1	December 4th, 2021
VAT registration number of the seller	2	
Time stamp of the invoice (date and time)	3	
Invoice total (with VAT)	4	
VAT total	5	
Hash of XML invoice	6	Starting Jan 1st, 2023 in waves
ECDSA signature	7	
ECDSA public key	8	
For Simplified Tax Invoices and their associated notes, the ECDSA signature of the cryptographic stamp's public key by ZATCA's technical CA	9	

6.1 TLV - TAG - LENGTH - VALUE construction and file format

- QR code is the base64 encoded TLV (Tag, Length, Value)
- Type/Tag-Length-Value (TLV) is an encoding scheme used in many communication protocols to encode data. A TLV-encoded message has a defined structure which consists of 3 sections/parts, see Figure (1). Those are:
  - Code of the message type (T) - 1 Byte
  - Message value length (L) - 1 Byte
  - Message value itself. (V) - Variable
- The Tag/Type and Length are of fixed sizes of 1 bytes while the value has a variable size.
- As the general idea behind encoding is to transform abstract data into a stream of bits, using TLV, there are different sets of encoding rules that can be used according to the Abstract Syntax Notation Version 1 (ASN.1). We are using a simple version of Basic Encoding Rules (BER).

6.2 Creation of TLV QR code

Description	Tag	Length	Value	Hex
Seller's name	1	23	Ahmed Mohamed AL Ahmady	41 68 6d 65 64 20 4d 6f 68 61 6d 65 64 20 41 4c 20 41 68 6d 61 64 79
VAT registration number of the seller	2	15	301121971500003	33 30 31 31 32 31 39 37 31 35 30 30 30 30 33
Time stamp of the invoice (date and time)	3	20	2022-03-13T14:40:40Z	32 30 32 32 2d 30 33 2d 31 33 54 31 34 3a 34 30 3a 34 30 5a
Invoice total (with VAT)	4	6	1108.90	31 31 30 38 2e 39 30
VAT total	5	45	114.90	31 31 34 2e 39 30
Hash of XML invoice	6	44	QnVEexW4nWv4CaE39a/ 66Jp/ OXO/evHQ8pDI-G7weq/4=	51 6e 56 45 65 78 57 34 6e 57 76 34 43 61 45 33 39 61 2f 36 36 4a 70 2f 4f 58 4f 2f 65 76 48 51 38 70 44 6c 47 37 77 65 71 2f 34 3d 20
ECDSA signature	7	192	4d 45 55 43 49 51 44 35 7a 78 79 58 4f 42 37 4e 76 57 66 36 32 72 56 45 5a 41 59 55 37 31 6a 70 79 39 48 45 45 6e 5a 30 71 39 4f 39 36 77 72 4c 36 51 49 67 51 4a 7a 43 47 48 62 77 36 59 42 48 4c 59 56 64 4f 31 77 6e 55 68 42 67 4b 6d 38 6a 4d 54 79 76 63 6b 39 4d 2b 72 50 39 78 59 59 3d	4d 45 55 43 49 51 44 35 7a 78 79 58 4f 42 37 4e 76 57 66 36 32 72 56 45 5a 41 59 55 37 31 6a 70 79 39 48 45 45 6e 5a 30 71 39 4f 39 36 77 72 4c 36 51 49 67 51 4a 7a 43 47 48 62 77 36 59 42 48 4c 59 56 64 4f 31 77 6e 55 68 42 67 4b 6d 38 6a 4d 54 79 76 63 6b 39 4d 2b 72 50 39 78 59 59 3d
ECDSA public key	8	48	30 56 30 10 06 07 2a ef bf bd 48 ef bf bd 3d 02 01 06 05 2b ef bf bd 04	30 56 30 10 06 07 2a ef bf bd 48 ef bf bd 3d 02 01 06 05 2b ef bf bd 04
For Simplified Tax Invoices and their associated notes, the ECDSA signature of the cryptographic stamp's public key by ZATCA's technical CA	9	144	30 46 02 21 00 ee 61 d3 eb 28 3c e6 3b 50 19 6a 77 33 bb 4f 4f b2 64 db ec ec bd 51 c6 b3 76 d4 e5 9e d8 13 af 02 21 00 fa d1 e6 d0 6a 66 23 62 f7 5e 6e 71 63 35 fc 78 5f 87 68 a7 b2 ec 10 11 42 35 2b 0b 63 42 05 69	30 46 02 21 00 ee 61 d3 eb 28 3c e6 3b 50 19 6a 77 33 bb 4f 4f b2 64 db ec ec bd 51 c6 b3 76 d4 e5 9e d8 13 af 02 21 00 fa d1 e6 d0 6a 66 23 62 f7 5e 6e 71 63 35 fc 78 5f 87 68 a7 b2 ec 10 11 42 35 2b 0b 63 42 05 69

XML Elements for QR code:

Description	Tag	XML element
Tag1	Seller's name	/Invoice/cac:AccountingSupplierParty/ cac:Party/cac:PartyLegalEntity /cbc:RegistrationName
Tag2	VAT registration number of the seller	/Invoice/cac:AccountingSupplierParty /cac:Party/cac:PartyTaxScheme/ cbc:CompanyID
Tag3	Time stamp of the invoice (date and time)	Date Xpath /Invoice/cbc:IssueDate Time xpath /Invoice/cbc:IssueTime Issue date combination between issue date and issue time, expression sample from the invoice yyyy-MM-dd'T'HH:mm:ss'Z'
Tag4	Invoice total (with VAT)	/Invoice/cac:LegalMonetaryTotal /cbc:TaxInclusiveAmount
Tag5	VAT total	/Invoice/cac:TaxTotal/cbc:TaxAmount
Tag6	Hash of XML invoice	Invoice/ext:UBLExtensions /ext:UBLExtension/ext:ExtensionContent /sig:UBLDocumentSignatures /sac:SignatureInformation /ds:Signature/ds:SignedInfo /ds:Reference/ds:DigestValue
Tag7	ECDSA signature	/Invoice/ext:UBLExtensions/ext: UBLExtension/ext:ExtensionContent /sig:UBLDocumentSignatures /sac:SignatureInformation/ds:Signature /ds:SignatureValue
Tag8	ECDSA public key	/Invoice/ext:UBLExtensions/ext:UBLExtension /ext:ExtensionContent /sig:UBLDocumentSignatures /sac:SignatureInformation /ds:Signature/ds:KeyInfo /ds:X509Data/ds:X509Certificate
Tag9	For Simplified Tax Invoices and their associated notes, the ECDSA signature of the cryptographic stamp's public key by ZATCA's technical CA	/Invoice/UBLExtensions/ UBLExtension/ExtensionContent /UBLDocumentSignatures /SignatureInformation/Signature /KeyInfo/X509Data/X509Certificate

The hex representation:

T	L	V

01 17 41 68 6d 65 64 20 4d 6f 68 61 6d 65 64 20 41 4c 20 41 68 6d 61 64 79 02 0f 33 30 31 31 32 31 39 37 31 35 30 30 30 30 33 03 14 32 30 32 32 2d 30 33 2d 31 33 54 31 34 3a 34 30 3a 34 30 5a 04 07 31 31 30 38 2e 39 30 05 05 31 34 34 2e 39 06 2c 51 6e 56 45 65 78 57 34 6e 57 76 34 43 61 45 33 39 61 2f 36 36 4a 70 2f 4f 58 4f 2f 65 76 48 51 38 70 44 6c 47 37 77 65 71 2f 34 3d 07 60 4d 45 55 43 49 51 44 35 7a 78 79 58 4f 42 37 4e 76 57 66 36 32 72 56 45 5a 41 59 55 37 31 6a 70 79 39 48 45 45 6e 5a 30 71 39 4f 39 36 77 72 4c 36 51 49 67 51 4a 7a 43 47 48 62 77 36 59 42 48 4c 59 56 64 4f 31 77 6e 55 68 42 67 4b 6d 38 6a 4d 54 79 76 63 6b 39 4d 2b 72 50 39 78 59 59 3d 08 58 30 56 30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 0a 03 42 00 04 61 83 0c a0 e6 85 60 08 4c 3b fb 2d 7a 8b 5f 67 26 af af aa 75 d5 24 a5 c2 c2 bd 6b 39 ac 2d 8e db d5 bf 85 2e 1a 8c 02 b8 41 d9 da 87 29 ba 31 a8 a3 5f be 42 83 78 f8 69 aa 3b a2 e6 17 27 d1 09 48 30 46 02 21 00 ee 61 d3 eb 28 3c e6 3b 50 19 6a 77 33 bb 4f 4f b2 64 db ec ec bd 51 c6 b3 76 d4 e5 9e d8 13 af 02 21 00 fa d1 e6 d0 6a 66 23 62 f7 5e 6e 71 63 35 fc 78 5f 87 68 a7 b2 ec 10 11 42 35 2b 0b 63 42 05 69

Field Definition for the QR Code

ARdBaG1lZCBNb2hhbWVkIEFMIEFobWFkeQIPMzAxMTIxOTcxNTAwMDAzAxQyMDIyLT-AzLTEzVDE0OjQwOjQwWgQHMTEwOC45MAUFMTQ0LjkGLFFuVkVIeFc0bId2NENhRT-M5YS82NkpwL09YTy9IdkhROHBEbEc3d2VxLzQ9B2BNRVVDSVFENXp4eVhPQj-dOdIdmNjJyVkVaQVIVNzFqcHk5SEVFblowcTIPOTZ3ckw2UUlnUUp6Q0dIYnc2WUJIT-FIWZE8xd25VaEJnS204ak1UeXZjazlNK3JQOXhZWT0IWDBWMBAGByqGSM49AgEGB-SuBBAAKA0IABGGDDKDmhWAITDv7LXqLX2cmr6+qddUkpcLCvWs5rC2O29W/hS4ajAK4Qdnahym6MaijX75Cg3j4aao7ouYXJ9EJSDBGAiEA7mHT6yg85jtQGWp3M7tPT7Jk2+zsv-VHGs3bU5Z7YE68ClQD60ebQamYjYvdebnFjNfx4X4dop7LsEBFCNSsLY0IFaQ==

In order to get the value for Tag9 i.e. the Digital Signature of the Certificate please follow the steps below:

1. Get a hold of your device's PCSID (You get this once you have successfully onboarded the device)
2. Decode the PCSID. One available online tool is: https://certlogik.com/decoder/

You should get results that look like the diagram below:

```
                    5f:67:26:af:af:aa:75:d5:24:a5:c2:c2:bd:6b:39:
                    ac:2d:8e:db:d5:bf:85:2e:1a:8c:02:b8:41:d9:da:
                    87:29:ba:31:a8:a3:5f:be:42:83:78:f8:69:aa:3b:
                    a2:e6:17:27:d1
                ASN1 OID: secp256k1
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DirName:/SN=1-TST|2-TST|3-47f16c26-806b-4e15-b269-7a803884be9c/UID=312345678900003/title=1100/registeredA
            X509v3 Subject Key Identifier:
                3B:96:62:53:B3:5A:91:4D:DE:7A:35:5A:DC:8D:92:D4:1D:AC:0F:09
            X509v3 Authority Key Identifier:
                keyid:76:60:8C:FB:06:A0:AC:67:57:35:9D:CF:9A:AC:A7:2B:99:35:B5:2F

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://tstcrl.zatca.gov.sa/CertEnroll/TSZEINVOICE-SubCA-1.crl

            Authority Information Access:
                OCSP - URI:http://tstcrl.zatca.gov.sa/CertEnroll/TSZEinvoiceSCA1.extgazt.gov.local_TSZEINVOICE-SubCA-1(1)
                OCSP - URI:http://tstcrl.zatca.gov.sa/ocsp

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, Code Signing
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
    Signature Algorithm: ecdsa-with-SHA256
         30:46:02:21:00:ee:61:d3:eb:28:3c:e6:3b:50:19:6a:77:33:
         bb:4f:4f:b2:64:db:ec:ec:bd:51:c6:b3:76:d4:e5:9e:d8:13:
         af:02:21:00:fa:d1:e6:d0:6a:66:23:62:f7:5e:6e:71:63:35:
         fc:78:5f:87:68:a7:b2:ec:10:11:42:35:2b:0b:63:42:05:69
```

3. Copy the value of "Signature Algorithm: ecdsa-with-SHA256"
4. Populate the value from step three as the value for Tag9 in the QR

6.3 Common mistakes in building the QR code

- Tag and Length are binary values, converted to Hex EXAMPLE: 21 should be represented as 15 in Hex, if the string is converted it becomes 32 31 (1 and 5)
- Value must also be converted to Hex before encoding to Base64
- There should be no padding or separators between the TLV sets in the resulting file
- Not using UTF8 Encoding for Arabic Text

6.4 Manual decoding a TLV QR Code

The QR code can be Extracted and Converted to Hex using publicly available tools

Step 1: Example Base64 Encode QR Code, extracted using QR Code reader (i.e. Mobile Phone):

ARVCb2JzIEJhc2VtZW50IFJIY29yZHMCDzEwMDAyNTkwNjcwMDAwMwMUMjAyMi0wN-C0yNVQxNTozMDowMFoECjIxMDAxMDAuOTkFCTMxNTAxNS4xNQ==

Step 2: Decode this to a hex representation, this can be done at the following site: cryptii

01 15 42 6f 62 73 20 42 61 73 65 6d 65 6e 74 20 52 65 63 6f 72 64 73 02 0f 31 30 30 30 32 35 39 30 36 37 30 30 30 30 33 03 14 32 30 32 32 2d 30 34 2d 32 35 54 31 35 3a 33 30 3a 30 30 5a 04 0a 32 31 30 30 31 30 30 2e 39 39 05 09 33 31 35 30 31 35 2e 31 35

Step 3: Hex Representation can be read by a TLV reader, i.e. : emvlab

Step 4: UTF8 Encoded values can be read using an online tool, i.e. : onlineutf8tools

Using a TLV Decoder to split the record shows the Hex Values, these can then be decoded using a hex to string decoder

Tag	Hex Value	Hex to string
Seller's name	426F627320426173656D656E7420 5265636F726473	Bobs Basement Records
VAT registration number of the seller	31303030323539303 6373030303033	100025906700003
Time stamp of the invoice (date and time)	323032322D30342D32355431353 A33303A30305A	2022-04-25T15:30:00Z
Invoice total (with VAT)	3231303031303302E3939	2100100.99
VAT total	33313530313152E3135	315015.15

6.5 Creation of QR code in JAVA - Javascript - nodeJS

This function takes in 2 args:

- tagNum: Tag Number
- tagValue: Value of Message

Convert the tagNum into byte array

Get the length of the value and convert it into byte array

Convert the value into byte array

Once we have 3 byte arrays, we concat them into 1 byte array representing our TLV Message

```
function getTLVForValue(tagNum, tagValue) {

    var tagBuf = Buffer.from([tagNum], 'utf8');


    tagValueLenBuf = Buffer.from([tagValue.length], 'utf8')


    var tagValueBuf = Buffer.from(tagValue, 'utf8');


    var bufsArray = [tagBuf, tagValueLenBuf, tagValueBuf]


    return Buffer.concat(bufsArray);
}
```

You do the previous steps for each of the Tags you want to add to the QR code. For example, here we have sellerName, VatReg, etc.

Concat those buffs into a single array representing the QR code (see 1, 2)

Afterwards, encode into Base64 (see 3)

```
// 1. Seller Name
var sellerNameBuf = getTLVForValue("1", "salah hospital");

// 2. VAT Registration
var vatRegistrationNameBuf = getTLVForValue("2", "31234567890123");

// ....
```

```
var tagsBufsArray = [sellerNameBuf,
    vatRegistrationNameBuf,
(1) timeStampBuf, taxTotalNameBuf, vatTotalBuf,
    hashedXmlBuf, keyBuf, signatureBuf];

var qrCodeBuf = Buffer.concat(tagsBufsArray)(2)

var qrCodeB64 =  qrCodeBuf.toString('base64');
                                              (3)
```

Dart - Use the BytesBuilder class to add each segment of each TLV message i.e. 3 per message.
We repeat for each message we want to add to the QR Code

```
BytesBuilder bytesBuilder = BytesBuilder();

// 1. Seller Name
bytesBuilder.addByte(1);
List<int> sellerNameBytes = utf8.encode(sellerName);
bytesBuilder.addByte(sellerNameBytes.length);
bytesBuilder.add(sellerNameBytes);

// 2. VAT Registration
bytesBuilder.addByte(2);
List<int> vat_registrationBytes = utf8.encode(vat_registration);
bytesBuilder.addByte(vat_registrationBytes.length);
bytesBuilder.add(vat_registrationBytes);

// .....
```

```
Uint8List qrCodeAsBytes = bytesBuilder.toBytes();
final Base64Encoder b64Encoder = Base64Encoder();
return b64Encoder.convert(qrCodeAsBytes);
```

Once all messages are added to the builder, convert it into bytes (see 1) which gives you Uint8List (Darts way of byte []), then encode the list into Base64 using an instance of the Base64Encoder class (see 2).

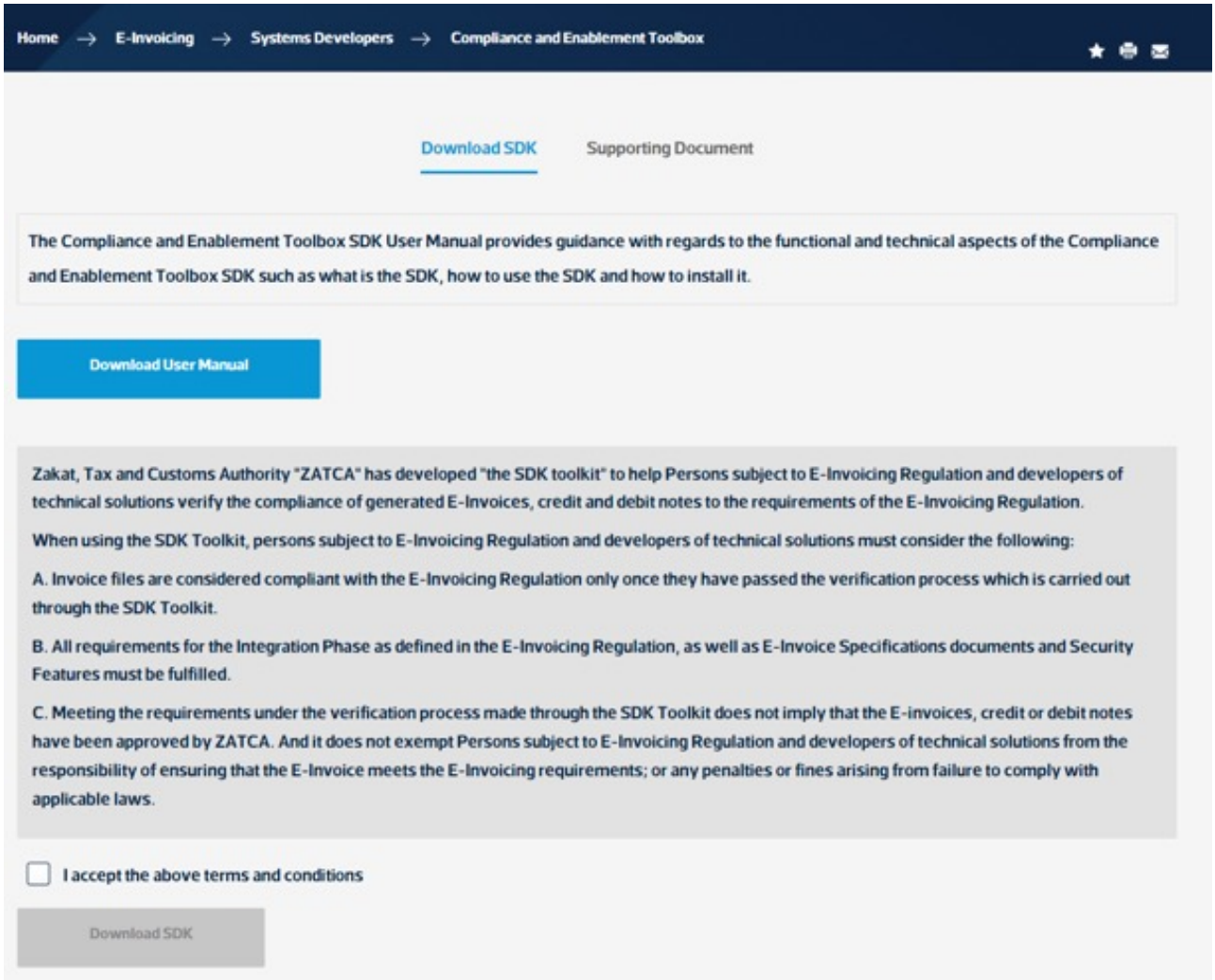
Representation of the QR code Data Examples:

Hyperlink to a Website https://zatca.gov.sa/en/pages/default.aspx	Data in Text Format Seller's name Bobs Records VAT registration number 310122393500003 Time stamp 2022-04-25T15:30:00Z VAT total 1000.00 VAT total 150.00	 TLV Base64 string AQxCb2JzI-FJIY29yZHMCDzMx-MDEyMjM5MzU-wMDAwMwMUM-jAyMi0wNC0yN-VQxNTozMDowM-FoEBzEwMDAuM-DAFBjE1MC4wMA==
Empty or unknown numbers 2000555663314	Hyperlink to the invoice online https://mcusercontent.com a90cefeb037ed376188308d34/files/2ca406b2-8627-66d9-45a4-94d186a4f3a5/User_Manual_Software_Development_Kit_SDK_.01.pdf	

SDK validation

The QR code can be validated using SDK available on ZATCA's website (https://zatca.gov.sa/en/E-Invoicing/SystemsDevelopers/ComplianceEnablementToolbox/Pages/DownloadSDK.aspx).

Command line	Results
fatoorah - v	To display (Version)
fatoorah - h	Help window
fatoorah validateqr -qr	Validate QR code structure
fatoorah generate -f (Invoicename.xml) -q	Generate compliant QR code



7. Business FAQs

Questions (EN)	Answers (EN)
Is there a limit on the number of decimals for unit price of an invoice?	No, as specified in the table provided under paragraph 7.3 of XML Implementation Standard, there are no restrictions on the decimal places for Unit Price.
Can taxpayer sign and submit invoices from different devices?	Yes, as long as the submitting device submits the document with the CSID of the device that stamped the document. It is recommended that each EGS independently is able submit documents to ZATCA.
How long after VAT registration can Taxpayer submit or receive invoices?	Newly registered VAT Taxpayers are required to wait for 2 business days before they can onboard their EGS and start submitting documents to ZATCA. Similarly documents issued to newly registered VAT Taxpayers will be rejected unless and until 2 business days have passed.
Can Taxpayer use their existing device to submit invoices after joining a VAT Group?	Once a Taxpayer joins a VAT Group, their own VAT Registration is suspended and all CSIDs associated with their VAT Registration Number will be automatically revoked. To continue using the same EGS as part of the VAT Group, the Group Lead (Representative) needs to onboard the EGS under the Group VAT Registration Number and provide the OTP(s) to the Group member. The Member can then obtain a new CSID which is associated with the Group and can then start submitting documents to ZATCA as part of the VAT Group.
How will Taxpayer know when Clearance is disabled?	When Clearance is disabled, any Standard documents submitted to the Clearance API will return a 303 response indicating that Clearance is off and the document needs to be submitted using the Reporting API. When Clearance is disabled, the Reporting API will accept Standard documents. Note that Standard documents submitted using the Reporting API will still undergo validations associated with Standard documents however there will be no stamp or QR code returned by the Core E-invoicing Solution and the document will instead be Reported.

Questions (EN)	Answers (EN)
Can Taxpayer resubmit a rejected documented?	Rejected documents can be resubmitted as a new document however this new document should indicate the Previous Document Hash as the hash of the document that was generated immediately before the resubmitted document and not of the document that was generated before the original rejected document. For example, consider the scenario: Document 1 is submitted and accepted Document 2 is submitted and accepted Document 3 is submitted and accepted Document 4 (Resubmission of Document 2 after addressing errors) In this case the Previous Document Hash of the Resubmitted document should be the hash of Document 3 and not Document 1. Note that the ZATCA's platform will be storing and tracking the hash of rejected documents as well. Accordingly, in the example above Document 3 should have its Previous Invoice Hash as the hash of Document 2 even though it was rejected.
What is the difference between error and warning?	An error is a validation failure associated with a rejected document, while a warning is a validation failure associated with an accepted document. If a submitted document has even one error, it will be rejected entirely.
When re-submitting an invoice, should it be updated with the re-submitted time or left as it was in the original submission ?	The time can be updated based on the re-submitted document generation time; it does not need to capture the time of original submission. Re-submission is similar to submitting a new invoice, it does not need to have any link to the original document that was rejected.
For Standard Tax Invoices, what should be done if the clearance fails before issuing the invoice to the buyer?	In case of Standard Tax Invoices, if clearing fails (Response is 400 Error), then the taxpayer must submit another invoice for clearance after rectifying the errors. Please note that every document shall have its own hash and counter value. Rejected document's hash and counter value should not be changed or updated.

Questions (EN)	Answers (EN)
In case a Standard Tax Invoices (B2B) is submitted and not cleared / rejected from ZATCA, should the invoice be resubmitted with different invoice counter value?	Invoice counter value should not be re-used. Once a document is generated with an Invoice Counter Value (ICV), then that ICV cannot be mentioned on another document. A new document should have its own ICV.
For Simplified Tax Invoices, what should be done if the reporting fails after issuing the invoice to the buyer?	In case of Simplified Tax Invoices, if the reporting fails, then the taxpayer must correct the error from to prevent it from happening on subsequent documents. The error in rejected document can be rectified and a new document can be submitted for Reporting. As the invoice would have already been issued to customer, there is no need to issue another invoice (in most cases customer may not be available to share the invoice again and therefore such a requirement would be impractical). Transaction should be included in monthly or quarterly VAT return submission. Intention is not to stop B2C transactions for technical failures or errors in XML documents.
Can taxpayers report invoices not cleared from ZATCA in their VAT return reports?	Taxpayers must determine VAT liability based on their transactions. Technical failure or error on XML does not invalidate the transaction. VAT becomes due irrespective of whether a valid invoice was issued or not. There are different penalties relating to "Non payment of VAT" and "Not issuing valid Tax Invoices". These two are separate events. Therefore, sometimes there will be scenario where taxpayers may have to include even the rejected invoices in VAT returns as the VAT becomes due for the tax period.
What will happen if we sign some invoices with non-valid certificates?	Invoices signed with invalid certificates will be rejected. Taxpayer must complete the "Onboarding process" to receive valid Cryptographic Stamp Identifier (CSID) Certificate.
Do we have to wait for the previous invoice to be cleared before sending the next invoice?	There is no dependency on ZATCA's clearance for generating new invoice. ZATCA's stamp or QR Code string is not part of the Hash. Taxpayers can continue generating invoices without waiting for Clearance from ZATCA as Clearance does not change the hash of the document.

Questions (EN)	Answers (EN)
What is the Billing Reference ID found in Debit and Credit Notes?	Billing Reference ID is the link to Original Invoices for which Debit and Credit Note is generated. It is a mandatory field. As per Article 54 of KSA VAT Regulations, every Debit and Credit Note should refer to Original Invoice that it relates to. This is not a new requirement, it existed since 1 Jan 2018.
Is it possible to send to ZATCA multiple "Supply dates" and "Supply end dates" for one credit note?	UBL standard does not allow multiple "Supply dates". Taxpayers may select a supply date range which covers all original invoices to which the particular credit note relates.
Is there an option to report simplified invoices by bulk?	No - there is currently no option to do bulk reporting.
What is the Fatoora Portal?	The Fatoora Portal is provided by ZATCA to Taxpayers in order to allow them to onboard their E-invoicing Generation Solution Unit(s) . It is considered as the starting point for Taxpayers who want to onboard a EGS Unit and receive a Cryptographic Stamp Identifier (CSID) for the first-time, renew an existing CSID or revoke an existing CSID. Taxpayers can also use the Portal in order to view a summary list of all their onboarded EGS Unit(s) along with specific EGS Unit information that is provided as a part of the Certificate Signing Request (CSR).
How does the log-in to Fatoora Portal work?	The Fatoora Portal uses Single Sign On (SSO) based on the Taxpayers credentials for the Taxation Portal (ERAD).
Who is authorized to use the Fatoora Portal?	The Fatoora Portal can be accessed and all off its functionalities can be used by all Taxpayers who are registered on the Taxation Portal (ERAD) for VAT and who have a VAT Registration (TRN) status of "Active" or "Reactive". Taxpayers whose VAT registration status used to be "Active" or "Reactive" but changes to "Deregistered" or "Suspended" would be able to access the Fatoora Portal for a period of 90 days but can only view a list of their previously onboarded EGS Units and cannot use any other onboarding functionalities such as generating an OTP. Once the buffer period of 90 days is over, these Taxpayers will no longer be able to access the Onboarding and Management Portal.

Questions (EN)	Answers (EN)
What is the difference between the Onboarding and Renewal process?	Both Onboarding and Renewal follow the same process and steps from a Taxpayer point of view. From a technical point of view, the request type submitted by the E-invoicing Generation Solution Unit (EGS Unit) is different and the renewal process includes revoking the existing Cryptographic Stamp Identifier (CSID) of the EGS Unit and issuing a new one.
What is the validity period of the OTPs?	OTPs are valid for 1 hour from the date of their generation.
Are there any differences between the onboarding process for VAT groups and individual Taxpayers?	Both individual Taxpayers and VAT groups follow a uniform process for onboarding in terms of the steps required to complete an onboarding, renewal or revocation. However, there are certain aspects that are specific to VAT groups, namely: In case of VAT groups, the Organization Unit Name that is a field in the Certificate Signing Request (CSR), should contain the 10-digit TIN number of the individual group member whose EGS Unit is being onboarded, in case the EGS Unit is to be used by a particular group member. The access rights for using the Fatoora Portal differ, whereby only the group lead would be able to meet the authorization criteria to access and use the functionalities provided by the Portal.
How will I know that my E-invoicing Generation Solution Unit (EGS Unit) has been successfully onboarded, renewed or revoked?	Email notifications will be sent to the Taxpayer once the status of an EGS Unit changes. In addition, Taxpayers can view the status of their EGS Unit(s) through the summary list of onboarded EGS Unit(s) that is a part of the Fatoora Portal. Once an EGS Unit has been onboarded, renewed or revoked, the respective fields of the list are updated to reflect the status accordingly.

Questions (EN)	Answers (EN)
What is a Certificate Signing Request (CSR)?	A certificate signing request (CSR) is one of the first steps towards getting the EGS's own Cryptographic Stamp Identifier (Certificate). It includes the following: Common Name: Name or Asset Tracking Number for the Solution Unit EGS Serial Number: Manufacturer or Solution Provider Name, Model or Version and Serial Number Organization Identifier: VAT or Group VAT Registration Number Organization Unit Name: Organization Unit Organization Name: Taxpayer Name Country Name Invoice Type: Functionality Map Location: Location of Branch or Device or Solution Unit Industry: Industry or location Please refer to Section 3.3.3 of the Taxpayer User Manual for more details on the CSR fields and the inputs required.
What are possible CSR failure situations?	Possible CSR failure situations including inserting the wrong algorithm, providing invalid values, missing information, inputting the wrong format or including expired/invalid OTP (note that the OTP is provided in the API header).
What is a Cryptographic Stamp Identifier (CSID)?	A CSID is technically a cryptographic certificate, which is a credential that allows for authenticated signing and encryption of communication. The certificate is also known as a public key certificate or an identity certificate. It is an electronic document used as proof of ownership of a public key. A CSID is used to uniquely identify an Invoice Generation Solution Unit in possession of a Taxpayer for the purpose of stamping (technically cryptographically signing) Simplified Invoices (B2C) and for accessing the Reporting and Clearance APIs.

Questions (EN)	Answers (EN)
What is a Compliance CSID?	A Compliance CSID is a CSID that is used by the EGS to call the compliance APIs and perform compliance checks, specifically the Compliance CSID is added as a request header when calling those APIs. Moreover, the Compliance CSID is generated by the e-invoicing platform itself rather than ZATCA CA since it is used only to ensure the compliance of the EGS with ZATCA specifications.
What is a Production CSID?	A Production CSID is a CSID that is used by the EGS to call the core e-invoicing production APIs such as reporting, clearance, etc. This CSID is generated by ZATCA CA and returned to the EGS which it can use to invoke the aforementioned APIs. Additionally, the Production CSID is added as a request header and also is used to authenticate and authorize the EGS.
What is the OTP generation process	The process of OTP generation is provided on the Fatoora portal for security and authentication reasons. Note that EGS providers can enhance their solutions to obtain the OTP automatically from the header after successful login. Currently, OTPs are valid for 1 hour providing sufficient time for Taxpayers with a large number of EGS units to be onboarded. OTP generation is managed by the Fatoora portal and must be taken from the portal itself, no need for any API. The OTP step is mandatory for the Onboarding / Renewal processes.

Questions (EN)	Answers (EN)
Is there a way to get an OTP through an API?	There is no API for OTP. You can only get OTPs thought the portal.
What is the maximum number of OTP we can request at once?	Each request can have till up to 100 OTPs.
What should we do with our UUID and ICV if an invoice gets rejected?	After an invoice gets rejected UUID and ICV should not be re-used. System should assign a new ICV when the document is submitted after fixing errors.
What are possible compliance checks failure situations?	Possible compliance checks failure situations include invalid documents/inputs or missing/invalid/expired Compliance CSID.
In case we sent an Invoice with errors and got the response from Reporting API «status: NOT_REPORTED», what should we do next?	In the case that an invoice is not accepted, the error should be checked, the invoice should be cancelled via a credit note and a new invoice generated. Once "Not Reported" the invoice is deemed invalid.
How does Single Sign On (SSO) work?	The SSO enables the Taxpayer to sign in only once to access different portals and websites. It allows the Taxpayer to access our platform of different components as if they were a single portal.

8. Appendix

Glossary

ZATCA	ZAKAT, Tax and Customs Authority
QR Code	Quick Response Code
PKI	Public Key Infrastructure
EGS Unit	E-invoice Generation Solution Unit
API	Answers (EN) Application Programming Interface
CA	Certificate Authority
OTP	One time Password
CSR	Certificate Signing Request
CSID	Cryptographic Stamp Identifier
SSO	Single Sign On
TRN	Tax Registration Number
CN	Credit Note
DN	Debit Note

External Document

This guide has been prepared for educational and awareness purposes only, its content may be modified at any time. It is not considered in any way binding to ZATCA and is not considered in any way a legal consultation. It cannot be relied upon as a legal reference in and of itself, It is always necessary to refer to the applicable regulations in this regard. Every person subject to zakat, tax and customs laws must check his duties and obligations, he is solely responsible for compliance with these regulations. ZATCA shall not be responsible in any way for any damage or loss The taxpayer is exposed to that results from non-compliance with the applicable regulations.