



FISCAL DEVICE GATEWAY API SPECIFICATION

Doc. No. v3.0

2023-05-02

CONTENTS

Contents	2
1. Document summary	4
1.1. Purpose	4
1.2. Definitions	4
2. Fiscal Device Gateway usage scenarios.....	5
2.1. Device registration	5
2.2. Fiscal device communication modes.....	5
2.3. Fiscal day (in online mode)	6
3. Object statuses.....	8
3.1. Fiscal day statuses.....	8
4. Fiscal Device Gateway API interfaces	9
4.1. registerDevice	9
4.2. issueCertificate	10
4.3. getConfig	10
4.4. getStatus	11
4.5. openDay	12
4.6. submitReceipt	13
4.8. closeDay	18
4.9. getServerCertificate	19
4.10. Request and response examples.....	19
5. Data Types	20
5.1. Address	20
5.2. Contacts	20
5.3. SignatureData	20
5.4. Enums	20
5.4.1. DeviceOperatingMode.....	20
5.4.2. FiscalDayStatus	21
5.4.3. FiscalDayReconciliationMode	21
5.4.4. FiscalCounterType.....	21
5.4.5. MoneyType.....	21
5.4.6. ReceiptType	21
5.4.7. ReceiptLineType	22
5.4.8. ReceiptPrintForm	22
5.4.9. FiscalDayProcessingError	22
6. Fiscal counters	23
7. Integration Setup Requirements	24
7.1. Communication and security protocols.....	24
7.2. Environment addresses.....	24
7.3. Authentication and authorization	24
7.4. Timeout Settings.....	24
8. Errors.....	25
8.1. Http statuses.....	25
8.2. Error codes.....	25
8.3. Validation errors	26
9. Requirements for fiscal devices.....	28
10..... Standard fiscal receipt, invoice and report views	30

10.1. Receipt48 view.....	30
10.2. InvoiceA4 view	31
10.3. Receipt and invoice view fields descriptions.....	32
10.4. Z Report / X Report.....	35
10.5. Z report and X report fields description	36
11.....Receipt QR code rules	39
12..... Certificate signing request (CSR) and Certificate examples	40
12.1. Example keys used	40
12.1.1. ECC ECDSA on SECG secp256r1	40
12.1.2. RSA 2048.....	40
12.2. CSRs and Certificates	42
12.2.1. ECC ECDSA on SECG secp256r1	42
12.2.1.1. CSR.....	42
12.2.1.2. Certificate	43
12.2.2. RSA 2048.....	44
12.2.2.1. CSR.....	44
12.2.2.2. Certificate	45
13..... Signatures generation and verification rules	48
13.1. Signature an hash generation algorithm	48
13.2. Receipt signature generation and verification	48
13.2.1. Receipt device signature	48
13.2.2. Receipt FDMS signature	49
13.3. Fiscal day signature generation and verification	50
13.3.1. Fiscal day device signature	50
13.3.2. Fiscal day FDMS signature.....	51

1. DOCUMENT SUMMARY

1.1. Purpose

This document describes the Fiscal Device Gateway API to be exposed towards fiscal devices. It defines exposed methods, input and output parameters, data formats, error codes, communication rules, etc.

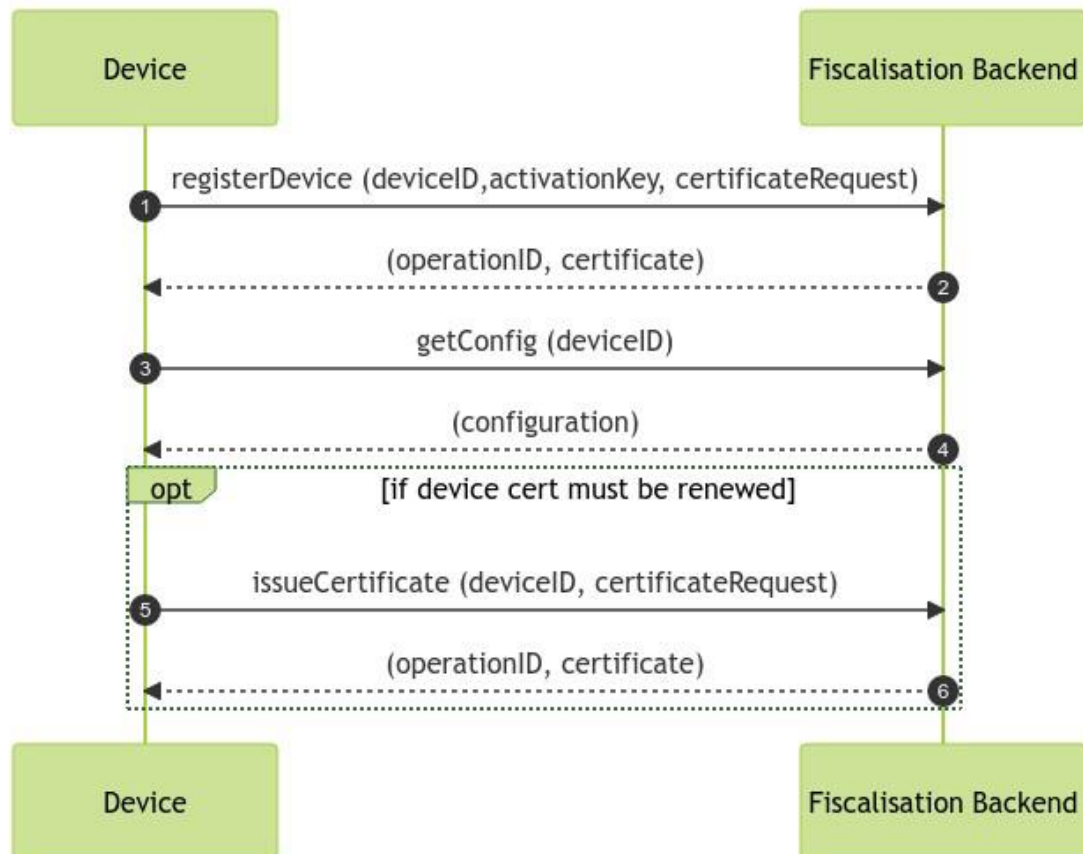
1.2. Definitions

Term	Description
Device or Fiscal device	Hardware based or software-based solution which is accounting sales (issues fiscal invoices, debit or credit notes) and submits them to FDMS.
Device signature	Receipt signature signed by fiscal device before submission of a receipt to Fiscal Device Gateway API.
Fiscal Device Gateway API	FDMS system module responsible for fiscal invoices, debit, or credit notes acceptance from fiscal devices.
Fiscalisation Data Management System (FDMS)	Fiscalisation Data Management System means Fiscalisation Backend system used by the Commissioner or the Zimbabwe Revenue Authority to receive, control and monitor User business transactions recorded by Electronic Fiscal Devices interfaced to it and to generate various required reports for the purposes of tax revenue administration.
FDMS signature	Receipt signature signed by FDMS after submission of a fiscal invoices, debit, or credit notes to Fiscal Device Gateway API.
QR code	A machine-readable code consisting of an array of black and white squares storing fiscal invoices, debit, or credit notes identification information, required to validate a receipt.
QR code data	QR code data is one of few receipt identification fields stored in QR code, which represents fiscal invoices, debit, or credit notes device signature.
Receipt	Receipt encompasses fiscal invoice, debit, or credit note.
ZIMRA	Zimbabwe Tax Revenue Authority.

2. FISCAL DEVICE GATEWAY USAGE SCENARIOS

2.1. Device registration

Device registration must be done once before starting to use a new device. After device registration, it needs to get its config from FDMS.



2.2. Fiscal device communication modes

Fiscal device communicates with Fiscal Device Gateway API in one of two possible communication modes:

- Online
- Offline (out of MVP scope, will be implemented in another project phase)

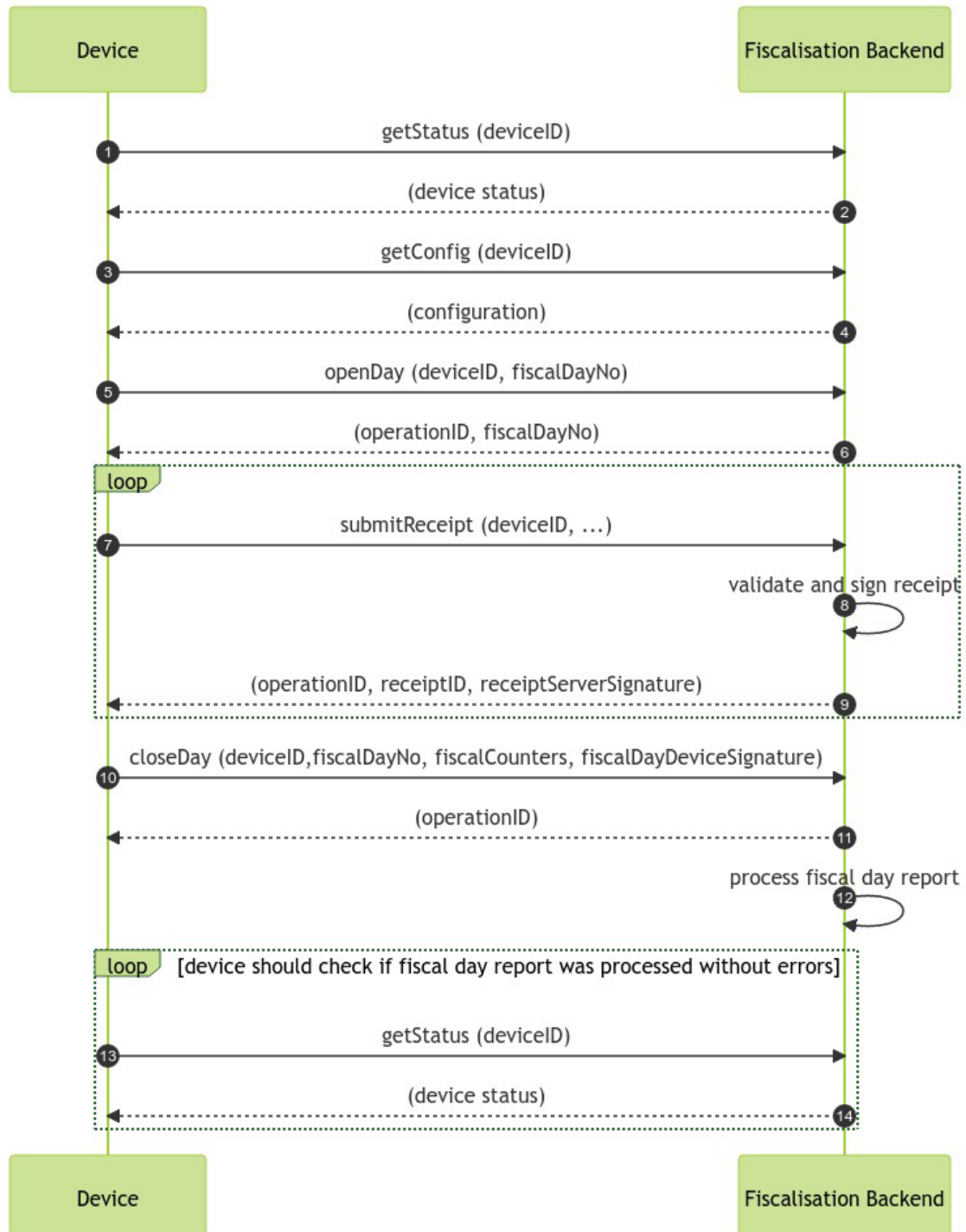
Online communication mode represents fiscal device communication in a way when fiscal device must have online access to FDMS (must have internet connection available) when it wants to close fiscal day. Fiscal day opening and submission of a receipt to FDMS should be done immediately after opening a day or printing receipt or invoice for buyer respectively, however in case of missing internet connection, day opening message and submission of a receipt may be delayed but must be done before closing a fiscal day. In case fiscal day was opened and receipt was issued without internet connection, it is mandatory, that fiscal day opening message would be sent before sending receipts. Otherwise, receipts will not be accepted.

Offline communication mode represents fiscal device communication in a way, when fiscal device may not have internet, and its receipts and fiscal report data will be provided to

FDMS by using files (by uploading file using Self-service, or by sending file to Fiscal Device Gateway API, whenever connection will be available).

2.3. Fiscal day (in online mode)

After successful device registration, it can be used for submitting sales to FDMS. Sales submission is possible only when fiscal day is opened. When work is finished with device, it must close fiscal day.



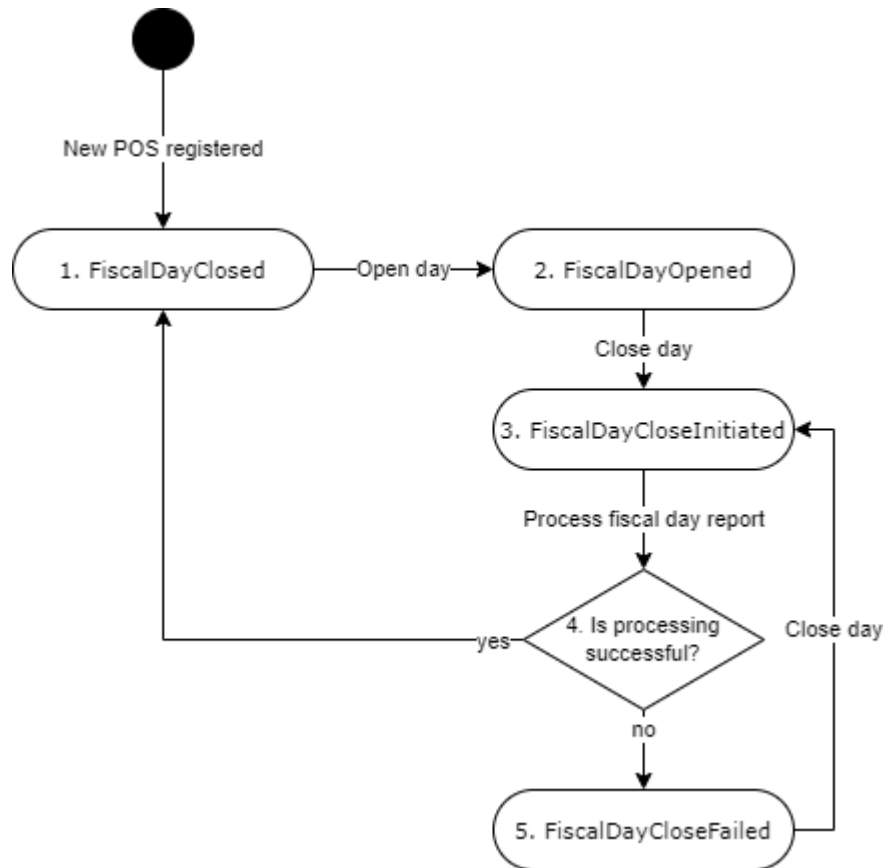
In case of error in fiscal day report processing report must be corrected on device and resubmitted to FDMS. Report resubmission can be done unlimited number of times. In case it



does not give successful result, and supplier cannot fix it to submit successful report, fiscal day may be closed manually by supplier in Public Portal, or by ZIMRA officer.

3. OBJECT STATUSES

3.1. Fiscal day statuses



Status	Description
1. FiscalDayClosed	Status used when fiscal device has successfully closed fiscal day. New fiscal day opening is possible only from this status.
2. FiscalDayOpened	Fiscal day is opened. Invoices can be created only when fiscal day is in this status.
3. FiscalDayCloseInitiated	Closure of fiscal day is initiated, however FDMS not yet validated fiscal counters. While Fiscal day is in status “FiscalDayCloseInitiated”, no new request to initiate fiscal day closure will be accepted from device or user. New invoices will not be accepted as well.
4. Is processing successful?	If processing of report is successful, fiscal day status is changed to FiscalDayClosed, if processing of report is not successful status is changed to FiscalDayCloseFailed.
5. FiscalDayCloseFailed	FDMS validated fiscal day report received from device, however there are validation errors. Device must correct issues and repeatedly submit fiscal day closure message.

4. FISCAL DEVICE GATEWAY API INTERFACES

Fiscal Device Gateway API exposes its methods using REST JSON interface. All methods except closeDay are synchronous. closeDay method returns response about accepted request synchronously, however processing of information is done asynchronously.

Each request must contain these HTTP headers:

Header name	Mandatory	Description
DeviceModelName	Yes	Device model name as registered in ZIMRA
DeviceModelVersionNo	Yes	Device model version number as registered in ZIMRA

4.1. registerDevice

registerDevice endpoint is used to get device certificate and register device in FDMS (link device with FDMS).

This API endpoint does not require certificate for authentication.

Input parameters:

Name	Type	Mandatory	Description
deviceId	Int	Yes	Device ID
activationKey	String (8)	Yes	Activation key. Case insensitive 8 symbols key.
certificateRequest	String	Yes	<p>Certificate signing request (CSR) for which certificate will be generated (in PEM format).</p> <p>Assigned by ZIMRA device name (format: ZIMRA-<Fiscal_device_serial_no>-<zero_padded_10_digit_deviceId>) should be provided in CSR's Subject CN.</p> <p>Other CSR's Subject fields are optional, however if provided must match these values (otherwise device registration will be rejected):</p> <ul style="list-style-type: none"> C = ZW O = Zimbabwe Revenue Authority S = Zimbabwe <p>Supported algorithms and key types (in order of suggested preference):</p> <ol style="list-style-type: none"> ECC ECDSA on SECG secp256r1 curve (also named as ANSI prime256v1, NIST P-256); Signature Algorithm: ecdsa-with-SHA256. RSA 2048; Signature Algorithm - SHA256WithRSA. <p><i>Note:</i> RSA 2k and ECC 256 implement same security level, which is considered safe until 2030 year (considering trends due to upgrade in computer software and hardware combination).</p> <p>Most cryptographic tools and libraries support this format giving easy-to-use API and hiding all technical representation and encoding details.</p> <p>CSR is "CertificationRequest" structure, as defined by PKCS #10 (CSR syntax specified by RFC2986).</p> <p>Serialized in PEM format (i.e., base64 encoded with "-----BEGIN CERTIFICATE REQUEST-----" header and "-----END CERTIFICATE REQUEST-----" footer).</p> <p>For more info, please refer to "12 Certificate signing request (CSR) and Certificate examples".</p>

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.

certificate	String	Yes	<p>X.509 v3 type device certificate (in PEM format). It must be used by device in further communication with Fiscal Device Gateway API. Certificate is multi-purpose:</p> <ul style="list-style-type: none"> Client Certificate for SSL with Client Authentication. For data signing when device signature is required. <p>Certificate is "Certificate" structure specified by RFC5280. Serialized in PEM format (i.e. base64 encoded with "-----BEGIN CERTIFICATE-----" header and "-----END CERTIFICATE-----" footer). For more info, please refer to "12 Certificate signing request (CSR) and Certificate examples".</p>
-------------	--------	-----	--

4.2. issueCertificate

issueCertificate endpoint is used to renew certificate before the expiration of the current certificate.

It is recommended to renew certificate a month before its expiration.

Certificate reissuance can be done at any time. It does not depend on fiscal day status, however it is recommended to be done before opening a new fiscal day.

Input parameters:

Name	Type	Mandatory	Description
deviceId	Int	Yes	Device ID
certificateRequest	String	Yes	Certificate signing request (CSR) for which certificate will be generated (in PEM format). certificateRequest requirements are specified in registerDevice endpoint description.

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.
certificate	String	Yes	X.509 v3 type device certificate (in PEM format). Certificate requirements are specified in registerDevice endpoint description.

4.3. getConfig

getConfig endpoint is used to retrieve taxpayers and device information and configuration.

Input parameters:

Name	Type	Mandatory	Description
deviceId	Int	Yes	Device ID

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.
taxPayerName	String (250)	Yes	Taxpayer name
taxPayerTIN	String (10)	Yes	Taxpayer TIN code
vatNumber	String (12)	No	Taxpayer's VAT number. Field is not returned if taxpayer is not a VAT payer.

			If taxpayer which is not a VAT taxpayer, gets VAT number and its fiscal device has opened fiscal day, fiscal day must be closed and newly opened in order taxpayer could submit receipts with VAT.
deviceSerialNo	String (20)	Yes	Device serial number assigned by manufacturer.
deviceBranchName	String (250)	Yes	Device branch name (or trade name) assigned by taxpayer.
deviceBranchAddress	Address	Yes	Device branch address.
deviceBranchContacts	Contacts	No	Device branch contacts information.
deviceOperatingMode	DeviceOperatingMode	Yes	Specifies what are allowed receipt processing modes for this device. Possible values: - Online - Offline Device operational mode can be changed only by ZIMRA officer.
taxPayerDayMaxHrs	Int	Yes	Maximum fiscal day duration in hours.
taxpayerDayEndNotificationHrs	Int	Yes	How much time in hours before end of fiscal day device should show notification to salesperson.
applicableTaxes	Tax array	Yes	List of applicable tax rates which can be used by this taxpayer and are valid during getConfig request time or will be valid in the future.
certificateValidTill	Date	Yes	Date till when device certificate is valid. Device must reissue new certificate before this date. After this date device will not be able to submit any request to Fiscal Device Gateway.
qrUrl	String (50)	Yes	URL for QR preparation.

Tax

Name	Type	Mandatory	Description
taxID	Int	Yes	Tax ID uniquely identifying a tax. This tax ID must be used in submitting invoices.
taxPercent	Decimal (5,2)	No	Tax percent. In case of exempt, field will not be returned.
taxName	String (50)	Yes	Tax name.
taxValidFrom	Date	Yes	Date from which tax is valid.
taxValidTill	Date	No	Date till which tax is valid.

4.4. getStatus

getStatus endpoint is used to get fiscal day status.

Input parameters:

Name	Type	Mandatory	Description
deviceId	Int	Yes	Device ID

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.
fiscalDayStatus	FiscalDayStatus	Yes	Device Fiscal day status.
fiscalDayReconciliationMode	FiscalDayReconciliationMode	No	In case fiscal day status is "FiscalDayClosed" defines how it was closed: automatically or manually.
fiscalDayServerSignature	SignatureDataEx	No	Fiscal day report signature prepared by FDMS.

			<p>This field is returned only when <code>fiscalDayStatus</code> is "FiscalDayClosed".</p> <p>This signature is not used in further communication or any data preparation for FDMS. It is confirmation from FDMS that fiscal day is closed and should be stored on device.</p> <p>Signature verification rules are described in section 13.3.</p>
<code>fiscalDayClosed</code>	<code>DateTime</code>	No	<p>Date and time when fiscal day report was processed, and fiscal day status was changed to "FiscalDayClosed". Time is provided in local time without time zone information.</p> <p>This field is returned only when <code>fiscalDayStatus</code> is "FiscalDayClosed".</p> <p>If device has never started a new fiscal day, this field is not returned.</p>
<code>fiscalDayClosingErrorCode</code>	<code>FiscalDayProcessingError</code>	No	<p>Code of error which appears during fiscal day closure. Possible codes are defined in section 5.4.9 FiscalDayProcessingError. This field is returned only when <code>fiscalDayStatus</code> is "FiscalDayCloseFailed". Error codes</p>
<code>fiscalDayCounters</code>	<code>FiscalDayCounter</code> array	No	<p>List of fiscal day counters. This field is returned only when <code>fiscalDayStatus</code> is "FiscalDayClosed" and <code>fiscalDayReconciliationMode</code> is "Manual". List contains only non-zero value fiscal counters.</p> <p><code>FiscalDayCounter</code> type description provided in <code>closeDay</code> endpoint.</p>
<code>fiscalDayDocumentQuantities</code>	<code>FiscalDayDocumentQuantity</code> array	No	<p>List of fiscal day document quantities. This field is returned only when <code>fiscalDayStatus</code> is "FiscalDayClosed" and <code>fiscalDayReconciliationMode</code> is "Manual". <code>FiscalDayDocumentQuantity</code> type description provided in <code>FiscalDayDocumentQuantity</code> table.</p>
<code>lastReceiptGlobalNo</code>	<code>Int</code>	No	<p>Last submitted <code>receiptGlobalNo</code> field value of fiscal invoice, credit note or debit note. In case no document is yet submitted from this fiscal device, this field is not returned.</p>
<code>lastFiscalDayNo</code>	<code>Int</code>	No	<p>In case fiscal day is opened, current fiscal day <code>fiscalDayNo</code> is returned. In case fiscal day is closed, last closed fiscal day <code>fiscalDayNo</code> is returned.</p> <p>In case fiscal device is new and not yet opened its first fiscal day, this field is not returned.</p>

FiscalDayDocumentQuantity

Name	Type	Mandatory	Description
<code>receiptType</code>	<code>ReceiptType</code>	Yes	Type of receipt.
<code>receiptCurrency</code>	<code>String (3)</code>	Yes	Receipt currency (ISO 4217 currency code).
<code>receiptQuantity</code>	<code>Int</code>	Yes	Total quantity of receipts of particular receipt type and currency for fiscal day.
<code>receiptTotalAmount</code>	<code>Decimal (19,2)</code>	Yes	Total receipt amount (including tax) of receipts of particular receipt type and currency for fiscal day.

4.5. openDay

`openDay` endpoint is used to open a new fiscal day. Opening of new fiscal day is possible only when previous fiscal day is successfully closed (fiscal day status is "FiscalDayClosed"). Opening of a new fiscal day in a fiscal device may be done without internet connection. It is important that such delayed request about day opening is sent before sending receipts.

Input parameters:

Name	Type	Mandatory	Description
------	------	-----------	-------------

deviceID	Int	Yes	Device ID
fiscalDayOpened	DateTime	Yes	Date and time when fiscal day was opened on a device. Time is provided in local time without time zone information.
fiscalDayNo	Int	No	<p>Fiscal day number assigned by device.</p> <p>If this field is not sent, FDMS will generate fiscal day number and return it to device.</p> <p>Validation rules:</p> <ul style="list-style-type: none"> - fiscalDayNo must be equal to 1 for the first fiscal day of fiscal device - fiscalDayNo must be greater by one from the last closed fiscal day fiscalDayNo.

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.
fiscalDayNo	Int	Yes	<p>Fiscal day number of opened day.</p> <p>In case device has sent fiscalDayNo in request, it is returned in this field. In case device has not sent it, new fiscal day number will be generated by FDMS.</p>

4.6. submitReceipt

submitReceipt endpoint is used to submit a receipt to FDMS in online mode and get a FDMS signature for it (signature is not a QR code, it is an acknowledgement of FDMS about received receipt). Receipt can be submitted only when fiscal day status is “FiscalDayOpened” or “FiscalDayCloseFailed”.

In case device tried to close a fiscal day and attempt was unsuccessful, device still have a possibility to submit a new receipt.

In case the same receipt (with the same deviceID, receiptGlobalNo and receiptHash) is submitted more than once, Fiscal Device Gateway API will return successful result to fiscal device with the same original receipt receiptID, receiptServerSignature, however different operationID.

Each submitted receipt is validated. Receipt will not be accepted, error will be returned to fiscal device (as specified in 8.2 Error codes), in these cases:

- fiscal device status is other than “Active”;
- fiscal day status is other than “FiscalDayOpened” or “FiscalDayCloseFailed”;
- receipt message structure is not valid.

In case the above-mentioned validations have passed, but receipt has other validation issues specified below (described in “Validation rules”), receipt will be accepted and signed, but will be marked as invalid with validation color code assigned (as specified in 8.3. Validation errors).

Each submitted receipt, must increase fiscal day counters as specified in 6. *Fiscal counters*.

Input parameters:

Name	Type	Mandatory	Description
deviceID	Int	Yes	Device ID
receipt	Receipt	Yes	Receipt data

Receipt:

Name	Type	Mandatory	Description
receiptType	ReceiptType	Yes	Type of receipt.
receiptCurrency	String (3)	Yes	Receipt currency (ISO 4217 currency code). Validation rules RCPT010: currency code must be present in FDMS and must be valid at the time of receiptDate.
receiptCounter	Int	Yes	Daily ascending serial number of receipt assigned by taxpayer's device. Validation rules: RCPT011: receiptCounter must be equal to 1 for the first receipt in fiscal day and receiptCounter must be greater by one from the previous receipt's receiptCounter value for the second and other receipt in fiscal day.
receiptGlobalNo	Int	Yes	Cumulative ascending serial number of total receipts issued since device activation date. Taxpayer is allowed to reset this receiptGlobalNo counter to start from 1, however this is allowed to be done only for the first receipt in a fiscal day. Validation rules: RCPT012: receiptGlobalNo must be greater by one from the previous receipt's receiptGlobalNo or may be equal to 1 for the first receipt in fiscal day.
invoiceNo	String (50)	Yes	Invoice number generated by accounting system. Validation rules: RCPT013: invoiceNo must be unique in taxpayer context.
buyerData	Buyer	No	Buyer information.
receiptNotes	String	No	Receipt notes. Usually used for FiscalInvoice.
receiptDate	DateTime	Yes	Date and time of device when receipt is printed for customer. Time is provided in local time without time zone information. Validation rules: RCPT014: - receiptDate must be greater than fiscal day opening date and time RCPT030: - receiptDate must be greater than previously submitted receiptDate RCPT031: - receiptDate must not be greater than current time (time difference set in AllowedTimeDifferenceForReceiptSubmission setting is allowed). RCPT041: - receiptDate must be less or equal than fiscal day opened + taxpayerDayMaxHrs.
creditDebitNote	CreditDebitNote	No*	Credited or debited receipt information. This field is mandatory in case receipt type is CreditNote or DebitNote. Validation rules: RCPT015: - creditDebitNote object is mandatory for receiptType CreditNote and DebitNote RCPT032: - credited or debited receipt must exist in FDMS RCPT033: - credited or debited receipt must be issued not earlier than 12 months before credit or debit note receiptDate RCPT034:

			<p>- fiscal device of credited or debited receipt must belong to the same taxpayer of submitted credit or debit note.</p> <p>RCPT035:</p> <p>- total credit note amount must not exceed original receipt amount with all previously submitted credit and debit notes amounts (where amount is calculated in this way original receipt amount - all submitted credit notes amounts + all submitted debit notes amounts. Result must be ≥ 0).</p> <p>RCPT036:</p> <p>- credit or debit note must have all or part of tax percentages used as in the original invoice. It cannot have new taxes, that are not in original invoice (example, if original invoice has exempt and 15% VAT tax lines, credit or debit note may have only exempt, 15% VAT or both tax lines, but cannot have 0% tax line). Non VAT taxpayer can still send VAT tax line if it was present on original invoice.</p> <p>RCPT029:</p> <p>- in case CreditDebitNote object is provided for FiscalInvoice document, received data will be saved with validation RCPT029 error.</p>
receiptLinesTaxInclusive	Boolean	Yes	<p>Specifies if receipt lines are tax inclusive or not. Possible values:</p> <ul style="list-style-type: none"> - True, all receipt lines are tax inclusive - False, all receipt lines are tax exclusive
receiptLines	ReceiptLine array	Yes	<p>Receipt lines.</p> <p>Validation rules:</p> <p>RCPT016: at least one line must be provided.</p>
receiptTaxes	ReceiptTax array	Yes	<p>Receipt taxes.</p> <p>Validation rules:</p> <p>RCPT017: at least one line must be provided.</p>
receiptPayments	Payment array	Yes	<p>Means of payments how receipt was paid.</p> <p>Validation rules:</p> <p>RCPT018: at least one line must be provided.</p>
receiptTotal	Decimal (19,2)	Yes	<p>Total receipt amount which is paid/received by buyer.</p> <p>Validation rules:</p> <p>RCPT019:</p> <p>- receiptTotal must be equal to sum of receiptLineTotal of all receiptLines in case receiptLinesTaxInclusive is true.</p> <p>RCPT037:</p> <p>- receiptTotal must be equal to sum of receiptLineTotal of all receiptLines plus sum of taxAmount of all receiptTaxes in case receiptLinesTaxInclusive is false.</p> <p>RCPT038:</p> <p>- receiptTotal must be equal to sum of salesAmountWithTax of all receiptTaxes.</p> <p>RCPT039:</p> <p>- receiptTotal must be equal to sum of paymentAmount of all receiptPayments.</p> <p>RCPT040:</p> <p>- receiptTotal must be greater than 0 for FiscalInvoice and DebitNote, receiptTotal must be less than 0 for CreditNote.</p>
receiptPrintForm	ReceiptPrintForm	No	<p>The format in which printed invoice was delivered to buyer (as a receipt, on A4 paper, etc.).</p> <p>Default value if field is not sent: Receipt48.</p>
receiptDeviceSignature	SignatureData	Yes	<p>SignatureData structure with SHA256 hash of receipt fields (hash used for signature) and receipt device signature prepared by using device private key as described in section 13.2.</p> <p>Validation rules:</p> <p>RCPT020: receiptDeviceSignature must be valid</p>

Buyer:

Name	Type	Mandatory	Description
buyerRegisterName	String (250)	Yes	Buyer company name or physical person name and surname.
buyerTradeName	String (250)	No	Buyer trade name (store name, or branch name).
buyerTIN	String (10)	No	Buyer TIN (provided for companies having TIN number). Foreign companies and local not registered companies will provide only buyerRegisterName.
VATNumber	String (12)	No	Buyer VAT number
buyerContacts	Contacts	No	Buyer contacts.
buyerAddress	Address	No	Buyer address.

CreditDebitNote:

Name	Type	Mandatory	Description
receiptID	Bigint	No	Receipt ID of credited or debited receipt which is credited or debited by current receipt. receiptID must be sent or deviceID with receiptGlobalNo and fiscalDayNo must be sent.
deviceID	Int	No	Device ID of credited or debited receipt which is updated by current receipt. In case receiptID is sent, this field is ignored.
receiptGlobalNo	Int	No	Receipt global No of credited or debited receipt which is updated by current receipt. In case receiptID is sent, this field is ignored.
fiscalDayNo	Int	No	fiscalDayNo of credited or debited receipt which is updated by current receipt.

ReceiptLine:

Name	Type	Mandatory	Description
receiptLineType	ReceiptLineType	Yes	Type of receipt line (for example sales or discount).
receiptLineNo	Int	Yes	Line sequence number in receipt.
receiptLineHSCode	String (8)	No	Product or service code from National Harmonized System codes list.
receiptLineName	String (200)	Yes	Product or service name
receiptLinePrice	Decimal (19,3)	No	Price of product or service in receipt currency (for single item). It may not be provided if the price for quantity of several prices is set (i.e., when selling 3 items for 1 USD). Validation rules: RCPT022: value must be greater than 0 for FiscalInvoice and DebitNote, value must be less than 0 for CreditNote.
receiptLineQuantity	Decimal (19,3)	Yes	Product quantity Validation rules: RCPT023: value must be greater than 0
receiptLineTotal	Decimal (19,2)	Yes	Total price of receipt line (receiptLinePrice * receiptLineQuantity). Validation rules: RCPT024: in case receiptLinePrice is provided, receiptLineTotal must be equal to receiptLinePrice * receiptLineQuantity
taxCode	String (3)	No	Tax code representation in receipt. This field is not mandatory; however, it must be provided for all receipt lines or none of them. It is not allowed to provide taxCode for just a part of lines.
taxID	Int	Yes	Applied tax ID uniquely identifying used tax. Validation rules: RCPT025:

			- VAT tax ID value must be one of the allowed tax ID values - receiptDate must be in a period of tax valid from and valid till period RCPT021: - VAT tax percent value determined by tax ID is greater than 0% and taxpayer is not VAT taxpayer.
taxPercent	Decimal (5,2)	No	Applied tax percent. In case of no VAT sale, 0 value should be used, in case of exempt this field should not be provided. Validation rules: RCPT025: - Tax percent and tax ID combination must be the same as in FDMS.

ReceiptTax:

Name	Type	Mandatory	Description
taxCode	String (3)	No	Tax code representation in receipt.
taxID	Int	Yes	Applied tax ID uniquely identifying used tax. Validation rules: RCPT025: - VAT tax ID value must be one of the allowed tax ID values - receiptDate must be in a period of tax valid from and valid till period RCPT021: - VAT tax percent value determined by tax ID is greater than 0% and taxpayer is not VAT taxpayer.
taxPercent	Decimal (5,2)	No	Applied tax percent. In case of no VAT sale, 0 value should be used, in case of exempt this field should not be provided. Validation rules: RCPT025: -Tax percent and tax ID combination must be the same as in FDMS.
taxAmount	Decimal (19,2)	Yes	Total tax amount for this tax percent. $\text{taxAmount} = \text{SUM}(\text{receiptLineTotal of the same taxCode}) * \text{taxPercent} / (1 + \text{taxPercent})$. In case of Non VAT and exempt, 0 should be sent in this field. Validation rules: RCPT026: - taxAmount must be equal to $\text{SUM}(\text{receiptLineTotal}) * \text{taxPercent} / (1 + \text{taxPercent})$ of all receiptLines with the same taxPercent and taxCode values in case receiptLinesTaxInclusive is true - taxAmount must be equal to $\text{SUM}(\text{receiptLineTotal}) * \text{taxPercent}$ of all receiptLines with the same taxPercent and taxCode values in case receiptLinesTaxInclusive is false
salesAmountWithTax	Decimal (19,2)	Yes	Total sales amount (including tax) for this tax percent. Validation rules: RCPT027: - salesAmountWithTax must be equal to sum of receiptLineTotal of all receiptLines with the same taxPercent and taxCode values in case receiptLinesTaxInclusive is true - salesAmountWithTax must be equal to $\text{SUM}(\text{receiptLineTotal}) * (1 + \text{taxPercent})$ of all receiptLines with the same taxPercent and taxCode values in case receiptLinesTaxInclusive is false

Payment:

Name	Type	Mandatory	Description
moneyTypeCode	MoneyType	Yes	Code of payment mean by which payment was done.
paymentAmount	Decimal (19,2)	Yes	Amount paid by this payment type in receipt currency. In case customer gave bigger amount (bill) in cash than total amount to be pay, it is needed to send amount without change to buyer. Validation rules: RCPT028: value must be greater than 0 for FiscalInvoice and DebitNote, value must be less than 0 for CreditNote.

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.
receiptID	Bigint	Yes	Receipt ID assigned by FDMS.
serverDate	DateTime	Yes	Date and time when FDMS signed a receipt.
receiptServerSignature	SignatureDataEx	Yes	Receipt FDMS signature generated by FDMS. This signature is not used in further communication or any data preparation for FDMS. It is confirmation from FDMS that receipt is accepted and should be stored on device. Signature verification rules are described in section 13.2.

4.8. closeDay

closeDay endpoint is used to initiate fiscal day closure procedure. This method is allowed when fiscal days status is “FiscalDayOpened” or “FiscalDayCloseFailed”.

In case fiscal day contains at least one “Grey” or “Red” receipt (as specified in 8.3. Validation errors), FDMS will respond to *closeDay* request with error (fiscal day will remain opened). Otherwise, if fiscal day does not have “Grey” and “Red” receipts, validation of submitted *closeDay* request will be executed. In case of fiscal day validation fails (as specified below in “Validation rules”), fiscal day remains opened, and its status is changed to “FiscalDayCloseFailed”.

Input parameters:

Name	Type	Mandatory	Description
deviceId	Int	Yes	Device ID
fiscalDayNo	Int	Yes	Fiscal day number. Validation rules: - fiscalDayNo must be the same as provided/received fiscalDayNo value in openDay request.
fiscalCounters	FiscalDayCounters array	Yes	List of fiscal counters. Zero value counters must not be submitted to FDMS.
fiscalDayDeviceSignature	SignatureData	Yes	SignatureData structure with SHA256 hash of fiscal day report fields (hash used for signature) and fiscal day report device signature prepared by using device private key as described in section 13.3. Validation rules: - fiscalDayDeviceSignature must be valid
receiptCounter	Int	Yes	receiptCounter value of last receipt of current fiscal day.

FiscalDayCounter:

Name	Type	Mandatory	Description
fiscalCounterType	FiscalCounterType	Yes	Fiscal counter type.
fiscalCounterCurrency	String (3)	Yes	Fiscal counter currency (ISO 4217 currency code).
fiscalCounterTaxID	Int	No*	Tax ID of fiscal counter. Must be provided for all fiscal counter types “byTax”.
fiscalCounterTaxPercent	Decimal (5,2)	No*	Tax percentage of fiscal counter. Must be provided for all fiscal counter types “byTax”. In case of exempt, this field must not be provided.
fiscalCounterMoneyType	MoneyType	No*	Code of payment mean of fiscal counter. Must be provided for fiscal counter type “BalanceByMoneyType”.
fiscalCounterValue	Decimal (19,2)	Yes	Fiscal counter value in counter currency. Validation rules:

Name	Type	Mandatory	Description
			- value must be greater than or equal to 0 for SaleByTax, SalesTaxByTax, DebitNoteByTax and DebitNoteTaxByTax fiscal counter types - value must be less than or equal to 0 for CreditNoteByTax and CreditNoteTaxByTax fiscal counter types

Output parameters:

Name	Type	Mandatory	Description
operationID	string (60)	Yes	Operation ID assigned by FDMS.

4.9. getServerCertificate

getServerCertificate endpoint is used to retrieve FDMS certificate for FDMS signature validation.

This API endpoint does not require certificate for authentication.

Input parameters:

Name	Type	Mandatory	Description
thumbprint	Binary (20)	No	Thumbprint of FDMS signing certificate which should be returned. If field is not provided, currently active FDMS signing certificate is returned. Together with the certificate, all certificate chain is returned.

Output parameters:

Name	Type	Mandatory	Description
certificate	String array	Yes	FDMS certificate chain (according to x.509 standard) to validate FDMS signatures.
certificateValidTill	Date	Yes	Date till when FDMS signing certificate is valid (despite that in the certificate parameter all the certificate chain is returned, this field shows validity time of the child certificate in the chain). Value is provided in UTC time.

4.10. Request and response examples

Request and response examples are provided in a separate document.

5. DATA TYPES

5.1. Address

Address object is used to define address object for returning information from FDMS and for accepting buyers information.

Name	Type	Mandatory	Description
province	String (100)	Yes	Province name
city	String (100)	Yes	City, town, growth point, farming area, mining area
street	String (100)	yes	Street, stand number, village
houseNumber	String (100)	Yes	House number

5.2. Contacts

Contacts object is used to define Taxpayers and device contact information.

Name	Type	Mandatory	Description
phoneNo	String (20)	No*	Phone number
email	String (100)	No*	E-mail address

* at least one of fields is mandatory.

5.3. SignatureData

SignatureData:

Name	Type	Mandatory	Description
hash	Binary (32)	Yes	SHA-256 hash.
signature	Binary (256)	Yes	Cryptographic signature, for which <i>hash</i> was used. More details see in "13 Signatures generation and verification rules". Field length is variable depends on cryptographic algorithm.

SignatureDataEx:

Name	Type	Mandatory	Description
SignatureData fields			
certificateThumbprint	Binary (20)	Yes	SHA-1 Thumbprint of Certificate used for <i>signature</i> .

5.4. Enums

Enum, short for "enumerated," is a data type that consists of predefined values. A variable defined as an enum can store one of the values listed in the enum declaration.

5.4.1. DeviceOperatingMode

Specifies what are allowed receipt processing modes for this taxpayer, possible values:

Enum value	Enum order
Online	0
Offline	1

5.4.2. FiscalDayStatus

Device Fiscal day status, possible values:

Enum value	Enum order
FiscalDayClosed	0
FiscalDayOpened	1
FiscalDayCloseInitiated	2
FiscalDayCloseFailed	3

5.4.3. FiscalDayReconciliationMode

Defines how fiscal day was closed, possible values:

Enum value	Enum order
Auto	0
Manual	1

5.4.4. FiscalCounterType

Fiscal counter type, possible values:

Enum value	Enum order
SaleByTax	0
SaleTaxByTax	1
CreditNoteByTax	2
CreditNoteTaxByTax	3
DebitNoteByTax	4
DebitNoteTaxByTax	5
BalanceByMoneyType	6

5.4.5. MoneyType

Code of payment mean of fiscal counter, possible values:

Enum value	Enum order
Cash	0
Card	1
MobileWallet	2
Coupon	3
Invoice	4
BankTransfer	5
Other	6

5.4.6. ReceiptType

Type of receipt. Possible values:

Enum value	Enum order
FiscalInvoice	0
CreditNote	1
DebitNote	2

5.4.7. ReceiptLineType

Type of receipt line. Possible values:

Enum value	Enum order
Sale	0
Discount	1

5.4.8. ReceiptPrintForm

Type of receipt or invoice visual representation template in which form it was printed and delivered to buyer. Possible values:

Enum value	Enum order	Description
Receipt48	0	Printed as receipt on receipt paper, 48 characters per line.
InvoiceA4	1	Printed on A4 paper as invoice.

5.4.9. FiscalDayProcessingError

Messages which are shown in case of error during fiscal day closure. Possible values:

Enum value	Enum order	Description
BadCertificateSignature	0	Close day is not allowed. Bad certificate signature is used.
MissingReceipts	1	Close day is not allowed. There are missing receipts in fiscal day ("Grey" validation error).
ReceiptsWithValidationErrors	2	Close day is not allowed. There are receipts with validation errors in fiscal day ("Red" validation error).
CountersMismatch	3	Close day is not allowed. There are mismatches between counters.

6. FISCAL COUNTERS

With each submitted receipt (FiscalInvoice, CreditNote and DebitNote), fiscal counters are updated.

After fiscal device finishes a fiscal day, it must close it by sending fiscal day report with fiscal counters provided in the table below to Fiscal Device Gateway API. Fiscal counter is optional to be sent in case it's value is zero.

Counters list and calculation rules for different types of receipt and different types of receipt lines are provided below. Please take a note to use correct sign when calculating a counter (add or subtract value from counter). In case negative receipt total amount is sent, fiscal counters become a negative sign too.

Fiscal day counters are reset after fiscal day close. Starting from a new fiscal day, counters start to be counted from zero.

Table below lists fiscal counters and specifies either they are calculated for different tax percents, currencies and/or payment methods:

Counter	By tax	By currency	By payment method	Description
SaleByTax	X	X		Total sales amount (after discount) by tax and by currency during fiscal day including tax. Does not include debit notes and credit notes.
SaleTaxByTax	X	X		Total tax amount by tax and by currency from sales (after discount) during fiscal day. Does not include debit notes and credit notes.
CreditNoteByTax	X	X		Total credit notes amount by tax and by currency during fiscal day including tax.
CreditNoteTaxByTax	X	X		Total tax amount by tax and by currency from credit notes during fiscal day.
DebitNoteByTax	X	X		Total debit notes amount by tax and by currency during fiscal day including tax.
DebitNoteTaxByTax	X	X		Total tax amount by tax and by currency from debit notes during fiscal day.
BalanceByMoneyType		X	X	Total collected or paid amount of money by money type and by currency during fiscal day.

Table below shows, which counters each submitted receipt type is changing and which fields from submitted receipt are used:

Receipt type	Fiscal invoice	Credit note	Debit note
Counter			
SaleByTax	+salesAmountWithTax		
SaleTaxByTax	+taxAmount		
CreditNoteByTax		-salesAmountWithTax	
CreditNoteTaxByTax		-taxAmount	
DebitNoteByTax			+salesAmountWithTax
DebitNoteTaxByTax			+taxAmount
BalanceByMoneyType	+paymentAmount	-paymentAmount	+paymentAmount

7. INTEGRATION SETUP REQUIREMENTS

7.1. Communication and security protocols

Fiscal Device Gateway API can be accessed using HTTPS protocol only. All Fiscal Device Gateway API methods except registerDevice and getServerCertificate use client authentication certificate which is issued by FDMS.

7.2. Environment addresses

Fiscal Device Gateway API is accessible in testing and production (real) environments. URL to access API:

Environment	URL
Testing environment	<Will be provided later after deployment is done> Testing environment's API can also be accessed using Swagger on <URL will be provided later after deployment is done>
Production environment	<Will be provided later after deployment is done>

7.3. Authentication and authorization

Fiscal Device Gateway uses mutual TLS authentication (https://en.wikipedia.org/wiki/Mutual_authentication) to authenticate fiscal device using fiscal device certificate. Fiscal device certificate is validated against issuing certificate to allow or deny access to API endpoints.

Note: endpoint 4.1 registerDevice is public and do not require authentication.

After authentication provided fiscal device certificate is checked against issued certificate (see 4.1 registerDevice and 4.2 issueCertificate methods for fiscal device certificate issuing) to check if the fiscal device certificate was issued to calling device (by method parameter deviceId) and the fiscal device certificate was not revoked.

The Fiscal Device Gateway will return HTTP 401 unauthorized code if:

- The provided fiscal device certificate was issued not by Fiscal Device Gateway.
- The provided fiscal device certificate was revoked.
- The provided fiscal device certificate expired.
- The provided fiscal device certificate was not issued to calling fiscal device.

7.4. Timeout Settings

Fiscal Device Gateway API response timeout for any synchronous operation - 30 seconds.

8. ERRORS

In case of API error, the system will return 4xx or 5xx http error code with response body containing a detailed problem details structure as described in <https://www.rfc-editor.org/rfc/rfc7807> .

ProblemDetails:

Name	Type	Mandatory	Description
type	String	Yes	
title	String	Yes	human readable problem definition
status	Integer	Yes	Http status code
errorCode	String	No	specific error code, for exact meaning see below

8.1. Http statuses

API can return such http statuses for errors:

Http status	Description
400	bad request - the message is malformed and could not be processed by Fiscal Backend Gateway
401	Authentication error (see Authentication and authorization)
404	Resource not found (call to not existing endpoint)
405	method not allowed - trying to access API using unsupported HTTP methos, e.g., POST to get config
422	Unprocessable Content - the instructions given by fiscal device to Fiscal Backend Gateway are incorrect, the response object ProblemDetails should contain ErrorCode to indicate the exact failing condition (e.g., DEV01 - device is blocked and therefore no instructions could be processed from such device)
500	Infrastructure error - the Fiscal Backend Gateway server is not available, or some infrastructure error occurred. The fiscal device should retry to send message later.
502	Bad gateway - the Fiscal Backend Gateway server could not be contacted. The fiscal device should retry to send message later.

8.2. Error codes

Error Code	Description	API methods
DEV01	Device not found or not active	All
DEV02	Activation key is incorrect	registerDevice
DEV03	Certificate request is invalid	registerDevice issueCertificate
FISC01	Open day is not allowed	openDay
RCPT01	Submit receipt is not allowed. Fiscal day is closed or fiscal day close initiated	submitReceipt
RCPT02	Submit receipt failed. The receipt structure invalid or field requirements not satisfied (e.g., provided field value length is greater then allowed)	submitReceipt
FISC03	Close day is not allowed. Close day is in progress.	closeDay
FISC04	Close day is not allowed. Fiscal day not opened.	closeDay

8.3. Validation errors

When *submitReceipt* request is received by FDMS and it is not rejected, FDMS validates receipt data. After a validation, receipt is stored and signed by FDMS. Receipt validation status may be valid or invalid. In case of invalid receipt, validation errors are categorized by one of these colors:

Color	Description
Grey	This means that received receipt violates receipt chain and makes a gap in receipt chain (previous receipt is missing). Such receipt is marked in "Grey". With each of the next received receipt, such "Grey" receipt will be revalidated (in case newly received receipt is the previous for the "Grey" receipt). After repeated validation it will remain "Grey" (if newly received receipt is not the previous for it) or become valid. Fiscal day will not be allowed to be closed automatically if it has at least one "Grey" receipt.
Yellow	"Yellow" validation errors are minor ones. Fiscal day will be allowed to be closed automatically if it contains only "Yellow" validation errors.
Red	"Red" validation errors are major ones. Fiscal day fill is not allowed to be closed automatically if it has at least one "Red" receipt.

Possible validation errors and their color codes:

Validation error	Color	Validation error text
RCPT010	Red	Wrong currency code is used
RCPT011	Grey / Red	Receipt counter is not sequential.
RCPT012	Grey / Red	Receipt global number is not sequential.
RCPT013	Red	Invoice number is not unique
RCPT014	Yellow	Receipt date is earlier than fiscal day opening date
RCPT015	Red	Credited/debited invoice data is not provided
RCPT016	Red	No receipt lines provided
RCPT017	Red	Taxes information is not provided
RCPT018	Red	Payment information is not provided
RCPT019	Red	Invoice total amount is not equal to sum of all invoice lines
RCPT020	Red	Invoice signature is not valid
RCPT021	Red	VAT tax is used in invoice while taxpayer is not VAT taxpayer
RCPT022	Red	Invoice line price must be greater than 0 (less than 0 for Credit note)
RCPT023	Red	Invoice line quantity, must be positive
RCPT024	Red	Invoice line total is not equal to unit price * quantity
RCPT025	Red	Invalid tax is used
RCPT026	Red	Incorrectly calculated tax amount
RCPT027	Red	Incorrectly calculated total sales amount (including tax)
RCPT028	Red	Payment amount must be positive (negative for credit note)
RCPT029	Red	Credited/debited invoice information provided for regular invoice
RCPT030	Grey / Red	Invoice date is earlier than previously submitted receipt date
RCPT031	Yellow	Invoice is submitted with the future date

RCPT032	Red	Credit / debit note refers to non-existing invoice
RCPT033	Red	Credited/debited invoice is issued more than 12 months ago
RCPT034	Red	Credited/debited invoice refers to another taxpayer issued invoice
RCPT035	Red	Total credit note amount exceeds original invoice amount
RCPT036	Red	Credit/debit note uses other taxes than are used in the original invoice
RCPT037	Red	Invoice total amount is not equal to sum of all invoice lines and taxes applied
RCPT038	Red	Invoice total amount is not equal to sum of sales amount including tax in tax table
RCPT039	Red	Invoice total amount is not equal to sum of all payment amounts
RCPT040	Red	Invoice total amount must be greater than 0 (less than 0 for Credit note)
RCPT041	Yellow	Invoice is issued after fiscal day end

9. REQUIREMENTS FOR FISCAL DEVICES

This chapter specifies requirements for fiscal devices to be met:

1. Fiscal device must open a new fiscal day before issuing receipts and invoices (in case fiscal day status opening failed, fiscal device must not allow to issue new receipt or invoice).
2. Fiscal device must retrieve configuration from FDMS (*getConfig* endpoint) before opening a new fiscal day.
3. Fiscal device must save data from *getConfig* response about taxpayer and/or its branch (taxpayer name, address, contacts, etc.) and use it for receipt and invoice printing.
4. Fiscal device must track the time passed from opening a fiscal day, that it would not exceed maximum allowed fiscal day length (specified in parameter *taxPayerDayMaxHrs*) and forbid issuing new receipts and invoices after that.
5. Fiscal device must inform user about the approaching fiscal day end. Notification must be shown to the user a few hours before maximum fiscal day length is reached. The exact number of hours left to maximum fiscal day length is specified in parameter *taxpayerDayEndNotificationHrs*.
6. Fiscal device must assign *receiptGlobalNo* value to a receipt in a sequential order starting from 1 and continue numbering despite fiscal day close.
7. In case *receiptGlobalNo* value becomes very big and taxpayer would like to reset it, this can be done by submitting the first receipt in a new fiscal day.
8. Fiscal device must assign *receiptCounter* value to a receipt in a sequential order starting from 1 and continue numbering only in the same fiscal day. After fiscal day closure, *receiptCounter* must be reset to 0.
9. Fiscal device must not allow to add goods or services with VAT tax to receipt or invoice if taxpayer is not a VAT taxpayer (*VATNumber* value is received in *getConfig* response). In case taxpayer gets VAT number in the middle of fiscal day, fiscal device must not allow to issue new receipts or invoices and must require closing fiscal day first.
10. Fiscal day opening message must be sent immediately after opening a fiscal day, however if there is no connection, it can be delayed.
11. Receipt must be sent to Fiscal Device Gateway API only after successfully opening a fiscal day.
12. Fiscal device must send receipt to Fiscal Device Gateway API only after finishing it (when receipt is printed).
13. Fiscal device must send receipt to Fiscal Device Gateway API one by one in ascending *receiptGlobalNo* order, not skipping any of receipt. In case submission of receipt failed, issue must be fixed, and receipt submission must be repeated.



14. Fiscal device must send receipt to Fiscal Device Gateway API immediately after finishing it in case there is an internet connection and there are no waiting receipts to be sent, otherwise receipt must be put to the queue on device and send later when connection will be restored.
15. Fiscal device must update counters after issuing a receipt and reset counters after starting a new fiscal day as specified in 6. Fiscal counters.
16. Fiscal device must renew certificate which is near to expire before its expiration date.

10. STANDARD FISCAL RECEIPT, INVOICE AND REPORT VIEWS

10.1. Receipt48 view

Receipt48 view is used for tax inclusive invoice printed on receipt paper, which can print 48 characters of text per line.

Receipt field name	
[1] Taxpayer logo	
[2] Taxpayer company legal name	
[3] Taxpayer TIN	
[4] VAT number	
[5] Taxpayer's branch name	
[6] Taxpayer's branch address	
[7] Taxpayer's branch e-mail	
[8] Taxpayer's branch phone	
[9] Static text: Fiscal tax invoice or Fiscal invoice	
[10] Buyer's information	
[11] Buyer's registered name	
[12] Buyer's trade name	
[13] Buyer's TIN	
[14] Buyer's address	
[15] Buyer's e-mail	
[16] Buyer's phone	
[17], [18], [19] Receipt numbers, Fiscal day number	
[20] Invoice number	
[21] Device serial number	
[22] Fiscal device ID	
[23] Receipt date and time	
Printed only for Debit and Credit note	
[24] Static text "Credit note" or "Debit note"	
[25] Credited/debited invoice device serial No	
[26], [27] Credited/debited receipt No and date	
[28] Credited/debited invoice No	
List of receipt items	
[30], [33], [34], Item name, total amount, tax code	
[31], [32] item quantity, unit price	
[35], [36] receipt currency, total amount to pay	
[35], [37], [38] receipt currency, payment method, paid amount	
[39] number of items	
Tax table	
[40], [41], [42], [43], [44] tax code, tax percent, amount without tax, tax amount, total amount inclusive tax	
[45] QR code	
[46] Receipt verification code	

	
Company legal name TIN: 123111000 VAT No: 12341234	
Downtown location Z B Centre Cnr Nkwame Nkrumah Ave / First Street, Harare zimra@email.com (0242) 758 891-5	
FISCAL TAX INVOICE	
Buyer: Company ABC, Ltd. Food Market ABC TIN: 19870123 12 Southgate Hwange john.smith@email.com (081) 20875	
Receipt No: 15 / 451 Fiscal day No: 45 Invoice No: CISN-000040321 Device Serial No: 12345678901234567890 Device ID: 6543210 Date: 03 / 07 / 23 18 : 48	
CREDIT NOTE	
Device Serial No: 9876543210123456789 Receipt No: 450 Date: 03 / 07 / 23 18 : 48 Invoice No: CISN-000040320	
Description	Amount
Item1 name	13200.00 VT
Item2 with very long name which does not fit in a single line	
3 each @ 5000.00	15000.00 VT
Item3 name	
0.555 @ 1081.08	600.00 NV
Item4 name	1200.00 EX
Total ZWL	30000.00
ZWL Cash	-5000.00
ZWL Card	-25000.00
Number of Items:	5.555
VAT %	Net. Amt VAT Amount
EX	1200.00 0.00 1200.00
NV	600.00 0.00 600.00
VT	24521.74 3678.26 28200.00
	
Verification code: 4C8B-E276-6333-0417	
You can verify this receipt manually at https://receipt.zimra.org/	

10.2. InvoiceA4 view

InvoiceA4 view is used for tax inclusive, or tax exclusive invoice printed on A4 paper.



[1] Taxpayer logo

Verification code
4C8B-E276-6333-0417 [46]
You can verify this receipt manually at
<https://receipt.zimra.org/>



[45] QR code

FISCAL TAX INVOICE [9]

SELLER

Company legal name [2]

TIN: 1234567890 [3]

VAT No: 12345678 [4]

Downtown location [5]

ZB Centre Cnr Nkwame Nkrumah Ave/ First Street, Harare [i]john.smith@email.com [15]

zimra@email.com [7]

(0242)758 891-5 [8]

BUYER

Company ABC, Ltd. [11]

Food Market ABC [12]

TIN: 19870123 [13]

12 Southgate Hwange [14]

(081) 20875 [16]

Receipt No: 15[17]/451[18]

Invoice No: CISN-0000040012 [20]

Device Serial No: 12345678901234567890 [21]

Fiscal day No: 45 [19]

Date: 03/07/23 18:48 [23]

Fiscal device ID: 674473 [22]

CREDIT NOTE [24]

Receipt No: 450 [26]

Invoice No: CISN-0000040011 [28]

Device Serial No: 12345678901234567890 [25]

Date: 03/07/23 6:48PM [27]

Code [29]	Description [30]	Qty [31]	Price [32]	VAT [34]	Amount (excl. tax) [33]
12345678	Item1 name	1	13200.00	15%	13200.00
11223344	Item2 name with very long name which does not fit in a single line	3	5000.00	15%	15000.00
12312312	Item3 name	1	600.00	0%	600.00
12341234	Item4 name	1	1200.00		1200.00

Total [47] 30000.00

Total15% [41] VAT 4320,00 [44]

Invoice total, ZWL [36] 34320,00 [35]

10.3. Receipt and invoice view fields descriptions

Fields in “Field name in which device sends data to FDMS” refers to Fiscal Device Gateway API endpoint *submitReceipt* fields. Fields in “Field name in which device receives data from FDMS” refers to Fiscal Device Gateway API endpoint *getConfig* fields.

Ob. No	Object name	Object description	Field name in which device sends data to FDMS	Field name in which device receives data from FDMS	Mandatory
Taxpayer block					
[1]	Taxpayer's logo	Taxpayer's logo. If printer is not capable to print logo, field is not displayed.	-	-	N
[2]	Taxpayer's name	Taxpayer's company legal name.	-	taxpayerName	Y
[3]	Taxpayer's TIN	Taxpayer's identification number, displayed with label “TIN: ”.	-	taxpayerTIN	Y
[4]	Taxpayer's VAT No	Taxpayer's VAT number. Must be displayed if taxpayer is VAT taxpayer	-	VATNumber	Y
Taxpayer address and contacts block					
[5]	Taxpayer's branch name	Taxpayer's branch name (to which fiscal device is assigned) Field displayed only if it differs from Taxpayer's name.	-	deviceBranchName	Y*
[6]	Taxpayer's branch address	Taxpayer's branch address, where fiscal device is located. Displayed in this order: houseNumber, street, city, province	-	deviceBranchAddress	Y
[7]	Taxpayer's branch e-mail	E-mail address.	-	deviceBranchContacts. email	N
[8]	Taxpayer's branch phone number	Phone number.	-	deviceBranchContacts. phoneNo	N
Fiscal tax invoice block					
[9]	Label	Static text “FISCAL TAX INVOICE” if taxpayer is VAT payer or “FISCAL INVOICE” if taxpayer is non-VAT payer	-	-	Y
Buyer block					
Buyer block is displayed only if buyer information is provided.					
[10]	Block label	Static text “Purchaser:”.	-	-	Y
[11]	Buyer's Name.	Buyer's register name (or individual person name, foreign company name or not registered trader name).	buyerRegisterName	-	Y
[12]	Buyer's trade name	Buyer's trade name	buyerTradeName	-	N
[13]	Buyer TIN	Buyer's TIN.	buyerTIN	-	N
[14]	Buyer's address	Buyer's address. Displayed in this order: houseNumber, street, city, province	buyerAddress	-	N
[15]	Buyer's e-mail	Buyer's e-mail address.	buyerContacts. email	-	N

[16]	Buyer's phone number	Purchaser's phone number. Field displayed if not empty.	buyerContacts. phoneNo	-	N
Receipt information block					
[17]	Receipt No	Receipt number in fiscal day - current day receipt counter.	receiptCounter	-	Y
[18]	Receipt global No	Receipt global No.	receiptGlobalNo	-	Y
[19]	Fiscal day No	Receipt Fiscal day number.	-	fiscalDayNo	Y
[20]	Invoice No	Receipt's invoice number	invoiceNo		Y
[21]	Device Serial No	Fiscal device serial number.	-	deviceSerialNo	Y
[22]	Device ID	Fiscal device ID (assigned by FDMS during device registration).	deviceID	-	Y
[23]	Receipt date and time	Receipt date and time.	receiptDate	-	Y
Credit note or Debit Note information block (displayed only in case of receipt type Credit Note or Debit Note)					
[24]	Label	Static text "Credit note" or "Debit note". Displayed only for Credit notes and Debit notes respectively.	-	-	Y
[25]	Device Serial No	Device Serial No of credited or debited receipt	creditNote.deviceID	-	Y
[26]	Receipt global No	Receipt global No of credited or debited receipt.	creditNote. receiptGlobalNo	-	Y
[27]	Receipt date	Date of credited or debited receipt	receiptDate of credited or debited receipt	-	Y
[28]	Invoice No	Invoice No of credited or debited receipts	invoiceNo of credited or debited receipt	-	Y
Receipt lines block					
[29]	Item HS code	Receipt line item National Harmonized System code.	receiptLineHSCode	-	N
[30]	Item name	Item name. If item name does not fit into 1 row it is split into more rows depending on item name length.	receiptLineName	-	Y
[31]	Quantity	Receipt line item Quantity. May not be displayed in case quantity is 1.	receiptLineQuantity,	-	N
[32]	Unit price	Receipt line item unit price. May not be displayed in case quantity is 1.	receiptLinePrice	-	N
[33]	Total amount	Receipt line total. In case of InvoiceA4 view, amount can be displayed inclusive or exclusive tax. In case total amount of exclusive tax is used, this must be indicated in column header.	receiptLineTotal	-	Y
[34]	Tax code	Tax code of receipt line. In case of InvoiceA4 view, tax percent value may be used alternatively.	taxCode or taxPercent	-	N
Receipt settlement block					
[35]	Currency	Receipt currency code.	receiptCurrency	-	Y

[36]	Total receipt amount	Total receipt amount to be paid.	receiptTotal	-	Y
[37]	Payment method	Payment method.	moneyTypeCode	-	Y
[38]	Total paid	Total paid by payment method.	paymentAmount	-	Y

Number of Items block

[39]	Number of Items	Number of items in receipt. SUM(Quantity) of all Sales lines. If item is weighed weight is added. For example: if one item is quantitative and quantity is 4, and another item is weighed, and weight is 0,555 kg, number of items should be $4+0,555=4,555$.	-	-	Y
------	-----------------	--	---	---	---

Taxes block

Receipt rows are grouped by tax percent and tax code. This block is not shown on receipt, if taxpayer is not VAT taxpayer.

[40]	Tax code	Tax code	-	-	N
[41]	Vat %	Tax percentage. In case of exempt, no value is displayed.	-	-	Y
[42]	Net.Amt	Amount without tax, salesAmountWithTax - taxAmount	-	-	Y
[43]	VAT	Tax amount	taxAmount	-	Y
[44]	Amount	Sales amount with tax	salesAmountWithTax	-	Y
[47]	Total	Used in InvoiceA4 when exclusive tax line totals are used. It sums total amount exclusive tax.			N

Receipt verification block

[45]	QR code	Generated QR code. More details in <i>Receipt QR code rules</i> . Optional if printer cannot print QR picture.	-	-	N*
[46]	Receipt verification code	QR code value (receiptQRData) of generate QR displayed in four characters groups separated by "- ". More details in <i>Receipt QR code rules</i> .	-	-	Y



10.4. Z Report / X Report

Company legal name TIN: 123111000 VAT No: 12341234			Receipt field name
Downtown location ZB Centre Cnr Nkwame Nkrumah Ave / First Street, Harare zimra@email.com (0242) 758 891-5			[1] Taxpayer company legal name
			[2] Taxpayer TIN
			[3] VAT number
			[4] Taxpayer's branch name
			[5] Taxpayer's branch address
			[6] Taxpayer's branch e-mail
			[7] Taxpayer's branch phone
			[8] Static text: Z REPORT or X REPORT
Z REPORT			[9] Fiscal day number
Fiscal day No: 45			[10] Fiscal day opening date
Fiscal day opened: 03/04/2023 18:01			[11] Fiscal day closing date
Fiscal day closed: 04/04/2023 18:01			[12] Device serial No
Device Serial No: 9876543210123456789			[13] Device Id
Device Id: 1450			[14] Static text: Daily totals
			List of counters in particular currency. Currency/counters information is shown only if there are sales with corresponding currency.
			[15] Currency (currencies are in alphabetical order)
Daily totals			[16] Static text: Total net sales
ZWL			[17], [18] Static text "Net", tax name, net amount (sales without tax) (ordered by tax percentage descending)
Total net sales			[19], [20] Static text: Total net amount, total amount
Net, VAT 15%	10 000.00		
Net, VAT 9%	5 000.00		
Net, Non-VAT 0%	15 000.00		
Net, Exempt	2 500.00		
Total net amount	55 000.00		
Total taxes			[21] Static text: Total taxes
Tax, VAT 15%	1 500.00		[22], [23] Static text "Tax", tax name, tax amount (tax amount) (ordered by tax percentage descending)
Tax, VAT 9%	4 500.00		
Total tax amount	1 950.00		[24], [25] Static text: Total tax amount, total amount
Total gross sales			[26] Static text: Total gross sales
Total, VAT 15%	11 500.00		[27], [28] Static text "Total", tax name, total amount (sales with tax) (ordered by tax percentage descending)
Total, VAT 9%	5 450.00		
Total, Non-VAT 0%	15 000.00		
Total, Exempt	2 500.00		
Total gross amount	56 950.50		[29], [30] Static text: Total gross amount, total amount
Documents			[31], [32], [33] Static texts: Documents, Quantity, Total amount
Invoices	50	56 950.50	[34], [35], [36] Static text "Invoices", quantity of documents, total amount (sales with tax for invoices)
Credit notes	1	- 500.00	[37], [38], [39] Static text "Credit notes", quantity of documents, total amount (sales with tax for credit notes, value can be negative)
Debit notes	1	500.00	[40], [41], [42] Static text "Debit notes", quantity of documents, total amount (sales with tax for debit notes)
Total documents	52	56 950.50	[43], [44], [45] Static text "Total documents", total quantity, total sum of amounts
USD			
Total net sales			
Net, VAT 15%	1 000.00		
Net, VAT 9%	100.00		
Net, Non-VAT 0%	500.00		
Net, Exempt	2 000.00		
Total net amount	3 600.00		
Total taxes			
Net, VAT 15%	150.00		
Net, VAT 9%	9.00		
Net, Non-VAT 0%	0.00		
Net, Exempt	0.00		
Total tax amount	159.00		
Total gross sales			
Net, VAT 15%	1 150.00		
Net, VAT 9%	109.00		
Net, Non-VAT 0%	500.00		
Net, Exempt	2 000.00		
Total gross amount	3 759.00		
Documents			
Invoices	10	3 759.00	
Credit notes	2	- 100.00	
Debit notes	3	100.00	
Total documents	15	3 759.00	

10.5. Z report and X report fields description

Z report /X report are daily reports. Fields are described according getConfig, openDay, getStatus APIs, Enums and Fiscal counters.

Ob. No	Object name	Object description	Field name
Taxpayer block			
[1]	Taxpayer name	Taxpayer's company legal name.	taxpayerName
[2]	Taxpayer TIN	Taxpayer's identification number, displayed with label "TIN: ".	taxpayerTIN
[3]	Taxpayer VAT No	Taxpayer's VAT number, displayed with label "VAT No:". Must be displayed if taxpayer is VAT taxpayer	VATNumber
Taxpayer address and contacts block			
[4]	Taxpayer's branch name	Taxpayer's branch name (to which fiscal device is assigned) Field displayed only if it differs from Taxpayer's name.	deviceBranchName
[5]	Taxpayer's branch address	Taxpayer's branch address, where fiscal device is located. Displayed in this order: houseNumber, street, city, province	deviceBranchAddress
[6]	Taxpayer's branch e-mail	E-mail address.	deviceBranchContacts. email
[7]	Taxpayer's branch phone number	Phone number.	deviceBranchContacts. phoneNo
Report block			
[8]	Label	Static text "Z REPORT" or "X REPORT". If FiscalDayStatus is FiscalDayClosed text "Z REPORT" is shown. If FiscalDayStatus is not FiscalDayClosed text "X REPORT" is shown.	-
[9]	Fiscal day No	Fiscal day number.	fiscalDayNo
[10]	Fiscal day opening date	Fiscal day opening date.	fiscalDayOpened
[11]	Fiscal day closing date	Fiscal day closing date. Is shown if FiscalDayStatus is FiscalDayClosed.	fiscalDayClosed
[12]	Device Serial No	Fiscal device serial number.	deviceSerialNo
[13]	Device ID	Fiscal device ID (assigned by FDMS during device registration).	deviceId
Daily totals block			
[14]	Label	Static text: Daily totals.	-
[15]	Currency	List of counters in particular currency. Block for particular currency is shown only if there are sales with corresponding currency. Blocks by currency is listed in alphabetical order by currency code.	fiscalCounterCurrency
[16]	Total net sales text	Static text "Total net sales".	-
[17]	Net name	List of Net amounts for each tax. Static text "Net" + tax name. Taxes are ordered by tax percentage in descending order. If tax percent is equal to 0, or exempt - line for that tax is not shown.	taxName
[18]	Net amount	Total net amount (sales without tax) by tax. NB. Credit note counter is added total because that it's value is negative.	SaleByTax - SaleTaxByTax + CreditNoteByTax - CreditNoteTaxByTax +

			DebitNoteByTax - DebitNoteTaxByTax by particular tax.
[19]	Total net amount text	Static text "Total net amount"	-
[20]	Total net amount	Total net amount for all values, all taxes. NB. Credit note counter is added total because that it's value is negative.	Sum of (SaleByTax - SaleTaxByTax + CreditNoteByTax - CreditNoteTaxByTax + DebitNoteByTax - DebitNoteTaxByTax)
[21]	Total taxes text	Static text "Total taxes".	-
[22]	Tax name	List of Tax amounts for each tax. Static text "Tax" + tax name. Taxes are ordered by tax percentage in descending order. If tax percent is equal to 0, or exempt - line for that tax is not shown.	taxName
[23]	Tax amount	Tax amount. NB. Credit note counter is added total because that it's value is negative.	SaleTaxByTax + CreditNoteTaxByTax + DebitNoteTaxByTax by particular tax.
[24]	Total tax amount text	Static text "Total tax amount"	-
[25]	Total tax amount	Total tax amount for all values, all taxes. NB. Credit note counter is added total because that it's value is negative.	Sum of (SaleTaxByTax + CreditNoteTaxByTax + DebitNoteTaxByTax)
[26]	Total gross sales text	Static text "Total gross sales".	-
[27]	Tax name	List of Total gross amounts for each tax. Static text "Total" + tax name. Taxes are ordered by tax percentage in descending order. If tax percent is equal to 0, or exempt - line for that tax is not shown.	taxName
[28]	Gross sales amount	Gross sales amount (sales with tax). NB. Credit note counter is added total because that it's value is negative.	SaleByTax + CreditNoteByTax + DebitNoteByTax by particular tax.
[29]	Total gross amount text	Static text "Total gross amount"	-
[30]	Total gross amount	Total gross amount for all values, all taxes. NB. Credit note counter is added total because that it's value is negative.	Sum of (SaleByTax + CreditNoteByTax + DebitNoteByTax)
[31]	Documents text	Static text "Documents".	-
[32]	Quantity text	Static text "Quantity".	-
[33]	Total amount text	Static text "Total amount".	-
[34]	Invoices text	Static text "Invoices".	-
[35]	Quantity of invoices	Quantity of invoices during fiscal day.	Number of issued documents where ReceiptType=FiscallInvoice
[36]	Total amount for invoices	Total amount (sales with tax for invoices).	Sum of SaleByTax
[37]	Credit notes text	Static text "Credit notes".	-
[38]	Quantity of credit notes	Quantity of credit notes during fiscal day.	Number of issued documents where ReceiptType=CreditNote
[39]	Total amount for credit notes	Total amount (sales with tax for credit notes). Is shown with minus sign.	Sum of CreditNoteByTax

[40]	Debit notes text	Static text "Debit notes".	-
[41]	Quantity of debit notes	Quantity of debit notes during fiscal day.	Number of issued documents where ReceiptType=DebitNote
[42]	Total amount for debit notes	Total amount (sales with tax for debit notes).	Sum of DebitNoteByTax
[43]	Total documents text	Static text "Total documents".	-
[44]	Total quantity	Quantity of documents during fiscal day. NB. Credit note counter is added total because that it's value is negative.	Number of issued documents
[45]	Total amount	Total amount for all documents, all taxes. NB. Credit note counter is added total because that it's value is negative.	Sum of SaleByTax + Sum of CreditNoteByTax + Sum of DebitNoteByTax

11. RECEIPT QR CODE RULES

Each issued receipt and invoice must contain QR code value printed as text and preferably also QR code picture (in case printer is capable to print it). QR code represents deep link URL with receipt identification information. QR code consists of this information:

Name	Length*	Description
qrUrl		URL for QR validation
deviceId	10	Device ID represented in 10 digits number with leading zeros.
receiptDate	8	Invoice date (receiptDate field value) represented in 8 digits (format: ddMMyyyy).
receiptGlobalNo	10	Receipt global number (receiptGlobalNo field value) issued by device represented in 10 digits with leading zeros
receiptQrData	16	Receipt QR data field (first 16 hexadecimal characters of MD5 hash from ReceiptDeviceSignature value).

* - length specifies a fixed length of value, which should be included in QR. In case value is shorter than indicated length, leading zeros must be added in front.

Example

Name	Example No 1	Example No 2
qrUrl	https://invoice.zimra.co.zw/	https://invoice.zimra.co.zw/
deviceId	0000000321	0000000322
receiptDate	03042023	04042023
receiptGlobalNo	1112223331	0000001332
receiptQrData	4C8BE27663330417	C10B0476B3B14678
Result (receiptQrCode)	https://invoice.zimra.co.zw/00000003210304202311122233314C8BE27663330417	https://invoice.zimra.co.zw/00000003220404202300000001332C10B0476B3B14678
QR		

12. CERTIFICATE SIGNING REQUEST (CSR) AND CERTIFICATE EXAMPLES

12.1. Example keys used

NOTE.

Those example keys are supplied only for illustration of CSR and Certificate generation, they are in unencrypted form and should **NEVER BE USED IN REAL LIFE**.

Device should generate their own keys and securely store them in encrypted form, never letting private key to go outside of device.

12.1.1. ECC ECDSA on SECG secp256r1

ECC ECDSA on SECG secp256r1 (ANSI prime256v1, NIST P-256) private key used in examples:

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIBXgREh8BvsXj0FjjcZ29EQiVjWGJuqHQp55+L1Zd6waoAoGCCqGSM49
AwEHoUQDQgAE+79w7206UY0Jc9mf08EjME19uysJawJ0kVellIj46at17FAG4NpY
VDe6t5pTSW1M6qCj5qKealESKalmnV32qQ==
-----END EC PRIVATE KEY-----
```

This key in textual representation form:

Private-Key: (256 bit)

priv:

15:e0:44:48:7c:06:fb:17:8f:41:63:8d:c6:76:f4:
44:22:56:35:86:26:ea:87:42:9e:79:f8:b9:59:77:
ac:1a

pub:

04:fb:bf:70:ef:63:ba:51:83:89:73:d9:9f:3b:c1:
23:30:49:7d:bb:2b:09:69:62:74:91:57:a5:94:88:
f8:e9:ab:65:ec:50:06:e0:da:58:54:37:ba:b7:9a:
53:49:69:4c:ea:a0:a3:e6:a2:9e:6a:51:12:29:a9:
4c:9d:5d:f6:a9

ASN1 OID: prime256v1

NIST CURVE: P-256

12.1.2. RSA 2048

RSA 2048 private key used in examples:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA52kCd2bXK+W72vC0+KlQ+tLUBNBsYNk9Gg+NPTx+fD+92lFg9
sPW8B1MFxT0+Kpw5MRzArB6M3LZ3pj00525vLcgT301bridwTgpSfzqtoHFhgTox
My94lMiYSK94w2Rxs1aMyDm4dCXGfU5AlAiuuegVFz056jV/Ik7jFjQLG5GQnRhW
tGkI2TKZLOlBsJhxUKLKPwUCPtKfZmDig/fXE1XigqSOGMoxQ9BTxJ/i8wWU3AR1
Tjou41EFisa0Kpan4xqeRnvNr0s0eIccBFRXBCB78tLTZgE9yqgwoQ5oQpNm8450
kFXQ0F770cy0sx+C020npdQisRK8WDx95kKjIQIDAQABAOIBAFar6/KQoBKe7ucn
tIBV2jC3ehV7grwbYVvk7bej7jZdIVx9klwAMayqzG7wqjxUiggE1BazxnEymQtY0
lGB16ko5X8gJD0eBGf0AvLl0Xu1yydQ+2WkUaxM+tlqy7gYwvqz04de0Vr0Z2mfg
QSuwvNCAbjXQBrSd4mQVK9SLFYXzHuYPXDVgTnBktjVQpedV+gqdLV08yMm1Fpv3
bB/tvotBmxHKsVR6AZmGME1tt00HR4L6Ha4d1ao5FK4+LtvowFSpSssQ7wyczJmO
ualE4qt/S87Fvm1hYU7VLbm7pAcZMa15FhIVcWZar2RRwwhvm7XwZbnippNgETMC
9bDsogECgYEA87D38++I3eCvm+bJ8Qpsu8yKVS2Bqv+dAyFLG9wFmA60JhNrpQ+f
JxSmv6sxiz492j4I+uHXuo9y1Sg8NQmdtouNRD2Gb0Xb5K6W0zftnoj05P8zJkkR
Z9RyoSXppLblazzT6LqUSk1/PwsX30X1liNEh4babqsU6fartlWrqtECgYEA8xk9
yz46DOKtu5GE17i2pe2mMXNG3Ed/Bas1mwa1isnKPFjNNGLuMaITYvXDK+/09hq0
ESWIRg/sjQ1NaHrbZ3izYgqBPYPVX8inA/w+4Yb6CVHY+9KJGVqzqrv1WwkMkd6K
IqL4SQAxWJQ1Ua1znbuB5TZ6tcZ4QcbVVcgB2FECgYEAwK+xn2RLqIUoRvmZu8ou
Z+A3kVpGkVusXwk4RnMWyUDZSpV91H+2fVutaejqSIX7hsXJqjk11MNmvsRgC52
Uhz00qMbZwirkoqqH6Eddj18yoUvgJpN9Pd7HAjKUB98b+rM9DxzFL0CWyIO4E+3
1ZtVWIQ8uzzzcHvnEm1zL8ECgYEA51P0Fp14yuijDwqLBG3AsGoAgu3j/6XGFgrn
mWC79SnH8XF5y97ILEKR97s/Fov6HXD/j4NuIGPKDsLByvJMmbjT0sAtmAvNLea
```



```
ds4yjeAjW10vJzmNKHalsGiioKRsqnEF1FewwwnptzGFa0PaPWKBajk5/qxzGG9Z
hhMgnGECgYEAh3K9PsQSTT2tjxu0yyYjldQDn7exl81i8XLeVKDOL7uQM6m3VICo
F8KdKY2hrwe71pQMI6+P+GkDgx4J7qW01EMZdMDcUDgzQemUQiUuFDFZ7FnUOkUS
2RbcYyo9m5kGzHzfQPAAlk9J1tJ3/xm8Hi44b2ZpiCpHYNW+RtB2qjA=
-----END RSA PRIVATE KEY-----
```

This key in textual representation form:

RSA Private-Key: (2048 bit, 2 primes)

modulus:

```
00:e7:69:02:77:66:d7:2b:e5:bb:da:f0:b4:f8:a9:
50:fa:d2:d4:04:d0:6c:60:d9:3d:1a:0f:8d:3d:3c:
5f:0f:ef:76:94:58:3d:b0:f5:bc:07:53:05:c5:33:
be:2a:9c:39:31:1c:c0:ac:1e:8c:dc:b6:77:a6:3d:
0e:e7:6e:6f:2d:c8:13:df:4d:5b:ae:27:70:4e:0a:
52:7f:3a:ad:a0:71:61:81:3a:31:33:2f:78:94:c8:
98:48:af:78:c3:64:71:b2:56:8c:c8:39:b8:74:25:
c6:7d:4e:40:94:08:ae:b9:e8:15:17:3d:39:ea:35:
7f:22:4e:e3:16:34:0b:1b:91:90:9d:18:56:b4:69:
08:d9:32:99:2c:e9:41:b2:38:71:50:a2:ca:3f:05:
02:3e:d9:1f:66:60:e2:83:f7:d7:13:55:e2:82:a4:
8e:18:ca:31:43:d0:53:c4:9f:e2:f3:05:94:dc:04:
75:4e:3a:2e:e3:51:05:8a:c6:8e:2a:96:a7:e3:1a:
9e:46:7b:cd:ac:eb:34:78:87:1c:04:54:57:04:20:
7b:f2:d2:d3:66:01:3d:ca:a8:30:a1:0e:68:42:93:
66:f3:8e:4e:90:55:d0:d0:5e:fb:d1:cc:b4:b3:1f:
82:3b:63:a7:a5:d4:22:b1:12:bc:58:3c:7d:e6:42:
64:21
```

publicExponent: 65537 (0x10001)

privateExponent:

```
56:ab:eb:f2:90:a0:12:9e:ee:e7:27:b4:80:55:da:
30:b7:7a:15:7b:82:bc:1b:61:59:3b:6d:e8:fb:8d:
97:48:57:1f:64:95:66:8c:03:2a:b3:1b:bc:2a:8f:
15:22:82:01:35:05:ac:f1:9c:4c:a6:42:d6:0e:94:
60:75:ea:4a:39:5f:c8:09:0f:47:81:19:fd:00:bc:
b9:4e:5e:ed:72:c9:d4:3e:d9:62:94:6b:13:3e:b6:
5a:b2:ee:06:30:be:ac:ce:e1:d7:b4:56:b3:99:da:
67:e0:41:2b:b0:bc:d0:80:6e:35:d0:06:bb:03:e2:
64:15:2b:d4:8b:15:85:f3:1e:e6:0f:5c:35:60:4e:
70:64:b6:35:50:a5:e7:55:fa:0a:9d:2d:5a:3c:c8:
c9:b5:16:9b:f7:6c:1f:ed:be:8b:41:9b:11:ca:b1:
54:7a:01:99:86:30:4d:6d:b4:ed:07:47:82:fa:1d:
ae:1d:d5:aa:39:14:ae:3e:2e:db:e8:c0:54:a9:4a:
cb:10:ef:0c:9c:cc:99:8e:b9:a9:44:e2:ab:7f:4b:
ce:c5:be:6d:61:61:4e:d5:2d:b9:bb:a4:07:19:31:
ad:79:16:12:15:71:66:5a:af:64:51:c3:08:6f:9b:
b5:f0:65:b9:e2:a6:93:60:11:33:02:f5:b0:ec:a2:
01
```

prime1:

```
00:f3:b0:f7:f3:ef:88:dd:e0:95:9b:e6:c9:f1:0a:
6c:bb:cc:8a:55:2d:81:aa:ff:9d:03:21:4b:1b:dc:
05:98:0e:8e:26:13:6b:a5:0f:9f:27:14:a6:bf:ab:
31:8b:3e:3d:da:3e:08:fa:e1:d7:ba:8f:72:95:28:
3c:35:09:9d:b6:8b:8d:44:3d:86:6f:45:db:e4:ae:
96:d3:37:ed:9e:88:f4:e4:ff:33:26:49:11:67:d4:
72:a1:25:e9:a4:b6:e5:6b:3c:d3:e8:ba:94:4a:4d:
7f:3d:6b:17:dc:e5:e5:96:23:44:87:86:da:6e:ab:
14:e9:f6:ab:b6:55:ab:aa:d1
```

prime2:

```
00:f3:19:3d:cb:3e:3a:0c:e2:ad:bb:91:84:97:b8:
b6:a5:ed:a6:31:73:46:dc:47:7f:05:ab:35:9b:06:
b5:8a:c9:ca:3c:58:cd:34:62:ee:31:a2:13:62:f5:
```

```
c3:2b:ef:ce:f6:1a:8e:11:25:88:46:0f:ec:8d:0d:
4d:68:7a:db:67:78:b3:62:0a:81:3f:23:d5:5f:c8:
a7:03:fc:3e:e1:86:fa:09:51:d8:fb:d2:89:19:5a:
b3:aa:bb:e5:5b:09:0c:91:de:8a:22:a2:f8:49:00:
31:58:94:35:51:ad:73:9d:bb:81:e5:36:7a:b5:c6:
78:41:c6:d5:55:c8:01:d8:51
```

exponent1:

```
00:c0:af:b1:9f:64:4b:a8:85:28:46:f9:99:bb:ca:
2e:67:e0:37:91:5a:46:29:5b:ac:5f:09:38:46:73:
16:c9:40:d9:0d:2a:55:f7:51:fe:d9:fb:ee:4d:a7:
a3:a9:22:31:ee:1b:17:26:a8:e4:d7:53:0d:9a:fb:
11:80:2e:76:52:1c:ce:3a:a3:1b:65:68:ab:92:8a:
aa:1f:a1:1d:76:39:7c:ca:85:2f:80:9a:4d:f4:f7:
7b:1c:08:ca:51:bf:7c:6f:ea:cc:f4:3c:73:7c:bd:
02:5b:22:0e:e0:4f:b7:d5:9b:55:58:84:3c:bb:3c:
f3:70:7b:e7:12:69:73:2f:c1
```

exponent2:

```
00:e6:53:ce:16:99:78:ca:e8:a3:0f:0a:8b:04:6d:
c0:b0:6a:00:82:ed:e3:ff:a5:c6:16:0a:e7:99:60:
bb:f5:29:c7:f1:71:79:cb:de:c8:2c:42:91:f7:bb:
3f:16:8b:fa:1d:77:7f:8f:83:6e:20:63:ca:0e:c2:
c1:ca:f2:4c:9b:36:e3:4f:4b:00:b6:60:2f:34:b7:
9a:76:ce:32:8d:e0:23:5b:5d:2f:27:39:8d:28:76:
a5:b0:68:a2:a0:a4:6c:42:71:05:94:57:b0:c3:09:
e9:b7:31:85:6b:43:da:3d:62:81:6a:39:39:fe:ac:
73:18:6f:59:86:13:20:9c:61
```

coefficient:

```
00:87:72:bd:3e:c4:12:4d:3d:ad:8f:1b:8e:cb:26:
23:94:3a:83:9f:b7:b1:97:cd:62:f1:72:de:54:a0:
ce:2f:bb:90:33:a9:b7:54:80:a8:17:c2:9d:29:8d:
a1:af:07:bb:d6:94:0c:23:af:8f:f8:69:03:83:1e:
09:ee:a5:8e:d4:43:19:74:c0:dc:50:38:33:41:e9:
94:42:25:2e:14:31:59:ec:59:d4:3a:45:12:d9:16:
dc:63:2a:3d:9b:99:06:cc:7c:df:40:f0:00:96:4f:
49:d6:d2:77:ff:19:bc:1e:2e:38:6f:66:69:88:2a:
47:60:d5:be:46:d0:76:aa:30
```

12.2. CSRs and Certificates

In examples we assume that device has:

- Keys described in “12.1 Example keys used”.
- deviceId is 42.
- Assigned by ZIMRA device name for use in CSR Subject CN is “ZIMRA-SN0001-0000000042”.

12.2.1. ECC ECDSA on SECG secp256r1

12.2.1.1. CSR

ECC ECDSA on SECG secp256r1 CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIHYMIGAAgEAMBA4xHDAABgNVBAMME1pSQi11VkZELTAwMDAwMDAwNDIwWTATBgcq
hkjOPQIBBggqhkhkjOPQMBBwNCAAT7v3DvY7pRg41z2Z87wSMwSX27KwlpYnSRV6WU
iPjpq2XsUAbg2lhUN7q3m1NJaUzqoKPmop5qURIpqUydXfapoAAwCgYIKoZIzj0E
AwIDRwAwRAIgLM EJQDh18bUE9waT2UXzP0+8FcGukpcIegMxd1A4JaQCIaZkzmEH
e0aaZ2jIcZArZo+rWzI4IwnSxtJqXLrpGUML
-----END CERTIFICATE REQUEST-----
```



In textual representation form:

Certificate Request:

Data:

```
Version: 1 (0x0)
Subject: CN = ZIMRA-SN0001-0000000042
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
  pub:
    04:fb:bf:70:ef:63:ba:51:83:89:73:d9:9f:3b:c1:
    23:30:49:7d:bb:2b:09:69:62:74:91:57:a5:94:88:
    f8:e9:ab:65:ec:50:06:e0:da:58:54:37:ba:b7:9a:
    53:49:69:4c:ea:a0:a3:e6:a2:9e:6a:51:12:29:a9:
    4c:9d:5d:f6:a9
  ASN1 OID: prime256v1
  NIST CURVE: P-256
Attributes:
  a0:00
Signature Algorithm: ecdsa-with-SHA256
  30:44:02:20:2c:c1:09:40:38:75:f1:b5:04:f7:06:93:d9:45:
  f3:3f:4f:bc:15:c1:ae:92:97:08:7a:03:31:77:50:38:25:a4:
  02:20:06:64:ce:61:07:7b:46:9a:67:68:c8:71:90:2b:66:8f:
  ab:5b:32:38:23:09:d2:5e:d2:6a:5c:ba:e9:19:43:0b
```

12.2.1.2. Certificate

ECC ECDSA on SECG secp256r1 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIC6TCCAdGgAwIBAgIFAKsSzWowDQYJKoZIhvcNAQELBQAwZDELMAkGA1UEBhMC
TFQxETAPBgNVBAoMCEdvb2QgTHRkMScwJQYDVQQLDB5Hb29kIEx0ZCBZDZXJ0aWZp
Y2F0ZSBDbDxRob3JpdHkxGTAXBgNVBAMMEEdvb2QgTHRkIFJvb3QgQ0EwHhcNMjE0
MDAzMTU1NzA1WWhcNMjE0MDAzMTU1NzA1WjBfMQswCQYDVQGEwJWUjERMA8GA1UE
CAwIWmFuemliYXN0ZXQxHjAdBgNVBAoMF1phbnppYmFyIFJldmVudWUgQm9hcmQxHDAa
BgNVBAMME1pScQ11VkJELTAwMDAwMDAwNDIwWTATBgqhkJOPQIBBgqhkJOPQMB
BwNCAAT7v3DvY7pRg4l2Z87wSMwSX27KwlpYnSRV6WUiPjpq2XsUAbg21hUN7q3
m1NJaUzqoKmpop5qURIpqUydxFapo3IwcDAJBGNVHRMEAjAAMB8GA1UdIwQYMBAA
FK1RXHm1plvaintqlWaxDs1X3LX+MB0GA1UdDgQWBBrqr96XrCUbuwCQawx00//n
TOCoNTA0BgNVHQ8BAf8EBAMCBeAwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZI
hvcNAQELBQADggEBANr1Wk1cVZB96yobFgK3rQv9oXW+Jle7Jh36J2o4wSSB+RH
lfMojDrqKVQCLrFDcF+8JIA3RTRKdduIXgBAr13xQ8JkHd1/o23yN6a2DaYgh0wr
Drnd1R6y1yG0vQuurJ3IgXmC0ldM5+VhalgmoCKFV9JJsUD+GhOyJ6Nwlc0SqvJCs
3RZLYwZ4MNViPbRy0Kbp0ufY1zTbh02Gw9aVfFzUwL8GS00iMb4MnSav1xur7wQh
BoF3PpNvu003P7f1eVJ62qVD2LWwntfn0mL1aRmDe2wpMQAKHxto+sDb2mfJ6G6
PftwMHe7BUfiwTzGYqav21h1w/amPxxNVQ7Li4M=
-----END CERTIFICATE-----
```

In textual representation form:

Certificate:

Data:

```
Version: 3 (0x2)
Serial Number:
  ab:12:cd:6a
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = LT, O = Good Ltd, OU = Good Ltd Certificate Authority, CN
= Good Ltd Root CA
Validity
  Not Before: Oct 3 15:57:05 2019 GMT
  Not After : Oct 12 15:57:05 2020 GMT
Subject: C = ZW, O = Zimbabwe Revenue Authority, CN = ZIMRA-SN0001-
0000000042
Subject Public Key Info:
```

```

Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
    04:fb:bf:70:ef:63:ba:51:83:89:73:d9:9f:3b:c1:
    23:30:49:7d:bb:2b:09:69:62:74:91:57:a5:94:88:
    f8:e9:ab:65:ec:50:06:e0:da:58:54:37:ba:b7:9a:
    53:49:69:4c:ea:a0:a3:e6:a2:9e:6a:51:12:29:a9:
    4c:9d:5d:f6:a9
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Authority Key Identifier:

keyid:AD:51:5C:79:B5:A6:5B:DA:8A:7B:6A:95:66:97:0E:CD:57:DC:B5:FE

    X509v3 Subject Key Identifier:
        6A:AF:DE:97:AC:25:1B:BB:00:90:6B:0C:4E:D3:FF:E7:4C:E0:A8:35
    X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Client Authentication
Signature Algorithm: sha256WithRSAEncryption
da:f5:5a:4d:5c:55:90:7d:eb:2a:1b:16:02:b7:ad:04:2f:f6:
85:d6:f8:99:5e:ec:98:77:e8:9d:a8:e3:04:92:07:e4:47:95:
f3:28:8c:3a:ea:29:54:02:2e:b1:43:70:5f:bc:24:80:37:45:
34:4a:75:db:88:5e:00:40:af:5d:f1:43:c2:64:1d:dd:7f:a3:
6d:f2:37:a6:b6:0d:a6:20:87:4c:2b:0e:b9:dd:95:1e:b2:d7:
21:b4:bd:0b:ae:ac:9d:c8:81:79:82:d2:57:4c:e7:e5:61:6a:
58:26:a0:22:85:57:d2:6c:50:3f:86:84:ec:89:e8:d5:a5:73:
44:aa:bc:90:ac:dd:16:4b:63:06:78:30:d5:62:3d:b4:72:d0:
a6:e9:d2:e7:d8:d7:34:db:87:4d:86:c3:d6:95:7c:5c:d4:c0:
bf:06:4b:4d:22:31:be:0c:9d:26:af:d7:1b:ab:ef:04:21:06:
81:77:3e:93:6f:bb:4d:37:3f:b7:f5:79:52:7a:da:a5:43:d8:
b5:96:9e:d7:e7:d2:62:f5:69:19:83:7b:6c:29:31:02:80:2a:
1c:6d:a3:eb:03:6f:69:9f:27:a1:ba:3c:5b:70:30:77:bb:05:
47:e2:c1:3c:c6:62:a6:af:db:58:75:c3:f6:a6:3e:4c:4d:55:
0e:cb:8b:83
  
```

12.2.2. RSA 2048

12.2.2.1. CSR

RSA 2048 CSR:

```

-----BEGIN CERTIFICATE REQUEST-----
MIICYzCCAUSCAQAwHjEcmBoGA1UEAwTWlJCLWVRkQtMDAwMDAwMDA0MjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOdpAndm1yvlu9rwtPipUPrS1ATQ
bGDZPRoPjT08Xw/vdpRYPbD1vAdTBcUzviqcOTecwKwejNy2d6Y9Duduby3IE99N
W64ncE4KUn86raBxYYE6MTMveJTImEiveMNkcbJWjMg5uHQ1xn10QJQIrrnoFRc9
Oeo1fyJ04xY0CxuRkJ0YVrRpCNkymSzpQbI4cVCiyj8FAj7ZH2Zg4oP31xNV4oKk
jhjKMUPQU8Sf4vMFLNwEdU46LuNRBYrGjiqWp+MankZ7zazrNHhHARUVwQge/LS
02YBPcqoMKEoEaEKTZvOOTpBV0NB+9HMTLMfgjtjp6XUIrESvFg8feZCZCECAwEA
AaAAMA0GCSqGSIb3DQEBCwUAA4IBAQBBeU11K7MWhroA8Fz302KXI7fJqc7sj9Ip/
jhN1ISfi8fJ3M3i58KqMSuXuBPF6Wv8NSncr3CmLa6no0ZnfWTfrWG+4vLYi5MfA
//6orI54K8kOe1NFk4Hr+QdUtdFJ8/6AE9a5dwp04IHSWR23kz7lAjgxrx29y2UF
9Ad4j8CM0NQifL5KHNS1Emh1DP/JCkmlMBkumSS8f1RfijWvnJ0mMc+Tbe+giMpp
qYE8b0Eqku+I3CKfVb4s7TJd6KNI6BEe2EYgcZKUxdIsrZy8SgqKE7iRstPo/Xgq
o02dqr4n1W0pFUHntP9M1lhqeoXHZcrC5ShdDpSY0/1DP5Jh9Vg9
-----END CERTIFICATE REQUEST-----
  
```

In textual representation form:

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = ZIMRA-SN0001-0000000042

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

```
00:e7:69:02:77:66:d7:2b:e5:bb:da:f0:b4:f8:a9:
50:fa:d2:d4:04:d0:6c:60:d9:3d:1a:0f:8d:3d:3c:
5f:0f:ef:76:94:58:3d:b0:f5:bc:07:53:05:c5:33:
be:2a:9c:39:31:1c:c0:ac:1e:8c:dc:b6:77:a6:3d:
0e:e7:6e:6f:2d:c8:13:df:4d:5b:ae:27:70:4e:0a:
52:7f:3a:ad:a0:71:61:81:3a:31:33:2f:78:94:c8:
98:48:af:78:c3:64:71:b2:56:8c:c8:39:b8:74:25:
c6:7d:4e:40:94:08:ae:b9:e8:15:17:3d:39:ea:35:
7f:22:4e:e3:16:34:0b:1b:91:90:9d:18:56:b4:69:
08:d9:32:99:2c:e9:41:b2:38:71:50:a2:ca:3f:05:
02:3e:d9:1f:66:60:e2:83:f7:d7:13:55:e2:82:a4:
8e:18:ca:31:43:d0:53:c4:9f:e2:f3:05:94:dc:04:
75:4e:3a:2e:e3:51:05:8a:c6:8e:2a:96:a7:e3:1a:
9e:46:7b:cd:ac:eb:34:78:87:1c:04:54:57:04:20:
7b:f2:d2:d3:66:01:3d:ca:a8:30:a1:0e:68:42:93:
66:f3:8e:4e:90:55:d0:d0:5e:fb:d1:cc:b4:b3:1f:
82:3b:63:a7:a5:d4:22:b1:12:bc:58:3c:7d:e6:42:
64:21
```

Exponent: 65537 (0x10001)

Attributes:

a0:00

Signature Algorithm: sha256WithRSAEncryption

```
5e:53:5d:4a:ec:c5:a1:ae:80:3c:17:3d:ce:d8:a5:c8:ed:f2:
6a:73:bb:23:f4:8a:7f:8e:13:65:21:27:e2:f1:f2:77:33:78:
b9:f0:aa:8c:4a:e5:ee:04:f1:7a:5a:ff:0d:4a:77:2b:dc:29:
8b:6b:a9:e8:39:99:df:59:37:eb:58:6f:b8:bc:b6:22:e4:c7:
c0:ff:fe:a8:ac:8e:78:2b:c9:0e:7b:53:45:93:81:eb:f9:07:
54:b5:d1:49:f3:fe:80:13:d6:b9:77:0a:68:e0:81:d2:59:1d:
b7:93:3e:e5:02:38:31:af:1d:bd:cb:65:05:f4:07:78:8f:c0:
8c:d0:d4:22:7c:be:4a:1c:de:65:12:68:65:0c:ff:c9:0a:49:
a5:30:19:2e:99:24:bc:7f:54:5f:8a:35:af:9c:9d:26:31:cf:
93:6d:ef:a0:88:ca:69:a9:81:3c:6f:41:2a:92:ef:88:dd:c2:
9f:55:be:2c:ed:32:5d:e8:a3:62:e8:11:1e:d8:46:20:73:32:
94:c5:d2:2c:ad:9c:bc:4a:0a:8a:13:b8:91:b2:d3:e8:fd:78:
2a:a3:4d:9d:aa:be:27:d5:6d:29:15:41:e7:b4:ff:4c:d6:58:
6a:7a:85:c7:65:ca:c2:e5:28:5d:0e:94:98:3b:fd:43:3f:92:
61:f5:58:3d
```

12.2.2.2. Certificate

RSA 2048 Certificate:

-----BEGIN CERTIFICATE-----

```
MIIDtDCCApYgAwIBAgIFAKsSzWswDQYJKoZIhvcNAQELBQAwZDELMAkGA1UEBhMC
TFQxETAPBgNVBAoMCEdvb2QgTHRkMScwJQYDVQQLEDB5Hb29kIEx0ZCBZDZXJ0aWZp
Y2F0ZSBDbXR0b3JpdHkxGTAXBgNVBAMTEEdvb2QgTHRkIFJvb3QgQ0EwHhcNMjE0
MDA5MTU1NzE2WWhcNMjE0MDA5MTU1NzE2WjBfMQswCQYDVQQGEwJ1bWljERMA8GA1UE
CwAwIWMFuemliYXNpdHkxGTAXBgNVBAoMFlphbnppYmFyIFJldmVudWUgQm9hcmQxHDAa
BgNVBAMTE1pSQi1lVkJELTAwMDAwMDAwNDIwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAAoIBAQNDAQJ3Ztcr5bva8LT4qVD60tQE0Gxg2T0aD409PF8P73aUWD2w
9bwHUwXFM74qnDkxHMCsHozctnemPQ7nbm8tyBPfTVuuJ3BOC1J/Oq2gcWGB0jEz
L3iUyJhIr3jDZHGyVozIObh0JcZ9TkCUCK656BUXPTnqNX8iTuMWNAsbkZCdGFa0
aQjZMpkS6UGyOHFQoso/BQI+2R9mYOKD99cTVeKCPi4YyjFD0FPEn+LzBZTcBHVO
```



```
Oi7jUQWKxo4qlqfjGp5Ge82s6zR4hxEVFcEIHvy0tNmAT3KqDChDmhCk2bzjk6Q
VdDQXvvRzLSzH4I7Y6el1CKxErXYPH3mQmQhAgMBAAGjcjBwMAKGA1UdEwQCMAAw
HwYDVR0jBBgwFoAUrVFceBwMw9qKe2qVZpcOzVfctf4wHQYDVR00BBYEFDLA7tgo
7/JLz5ayFa4HP3a7Kyf2MA4GA1UdDwEB/wQEAwIF4DATBgNVHSUEDDAKBggrBgEF
BQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAI7n2fUonnpbOJCUaX7/bDwDmdQ2SEJfH
ro/rWfp/fhD8sBK0ZzZ0AZHH20szBQ0wBqX3+hyMMwAyBlsHdan971vdNuSZtTnm
HjtuOFYuF9o69BMCPMNHgj3XhikuNlh7NPzr1nU2ec6/tgx5guosoo0gZNsCpdbt
ee4pJydnA4vmx4c6wbEWBJA1YhZLloGi9VR2NVI00nxYuvlinqIHvNypJL+3aDT5
yvjRY+suDKf+u3J8nRlrx22b/YvPu3U4BhK6FJk/JSxy3qOMz1EUR4uPt9ci06E
50hpF9PSdcWt8NtC4f+i4EtwGcsj5XHp10WN+Ko0ksK9ZcwaJpQ7DQ==
-----END CERTIFICATE-----
```

In textual representation form:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

ab:12:cd:6b

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = LT, O = Good Ltd, OU = Good Ltd Certificate Authority, CN

= Good Ltd Root CA

Validity

Not Before: Oct 3 15:57:16 2019 GMT

Not After : Oct 12 15:57:16 2020 GMT

Subject: C = ZW, O = Zimbabwe Revenue Authority, CN = ZIMRA-SN0001-

0000000042

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

```
00:e7:69:02:77:66:d7:2b:e5:bb:da:f0:b4:f8:a9:
50:fa:d2:d4:04:d0:6c:60:d9:3d:1a:0f:8d:3d:3c:
5f:0f:ef:76:94:58:3d:b0:f5:bc:07:53:05:c5:33:
be:2a:9c:39:31:1c:c0:ac:1e:8c:dc:b6:77:a6:3d:
0e:e7:6e:6f:2d:c8:13:df:4d:5b:ae:27:70:4e:0a:
52:7f:3a:ad:a0:71:61:81:3a:31:33:2f:78:94:c8:
98:48:af:78:c3:64:71:b2:56:8c:c8:39:b8:74:25:
c6:7d:4e:40:94:08:ae:b9:e8:15:17:3d:39:ea:35:
7f:22:4e:e3:16:34:0b:1b:91:90:9d:18:56:b4:69:
08:d9:32:99:2c:e9:41:b2:38:71:50:a2:ca:3f:05:
02:3e:d9:1f:66:60:e2:83:f7:d7:13:55:e2:82:a4:
8e:18:ca:31:43:d0:53:c4:9f:e2:f3:05:94:dc:04:
75:4e:3a:2e:e3:51:05:8a:c6:8e:2a:96:a7:e3:1a:
9e:46:7b:cd:ac:eb:34:78:87:1c:04:54:57:04:20:
7b:f2:d2:d3:66:01:3d:ca:a8:30:a1:0e:68:42:93:
66:f3:8e:4e:90:55:d0:d0:5e:fb:d1:cc:b4:b3:1f:
82:3b:63:a7:a5:d4:22:b1:12:bc:58:3c:7d:e6:42:
64:21
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Authority Key Identifier:

keyid:AD:51:5C:79:B5:A6:5B:DA:8A:7B:6A:95:66:97:0E:CD:57:DC:B5:FE

X509v3 Subject Key Identifier:

32:C0:EE:D8:28:EF:F2:4B:CF:96:B2:15:AE:07:3F:76:BB:2B:27:F6

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment

X509v3 Extended Key Usage:

TLS Web Client Authentication

Signature Algorithm: sha256WithRSAEncryption

```
23:b9:f6:7d:4a:27:9e:96:ce:24:25:1a:5f:bf:db:0f:00:e6:
75:0d:92:10:97:c7:ae:8f:eb:59:fa:7f:7e:10:fc:b0:12:b4:
67:36:74:03:31:c7:d8:eb:33:05:03:b0:06:a5:f7:fa:1c:8c:
33:00:32:06:5b:07:75:a9:fd:ee:5b:dd:36:e4:99:b5:39:e6:
1e:3b:6e:38:56:2e:17:da:3a:f4:13:02:3c:c3:47:82:3d:d7:
86:29:2e:36:58:7b:34:fc:eb:d6:75:36:79:ce:bf:b6:0c:79:
82:ea:2c:a2:8d:20:64:db:02:a5:d6:ed:79:ee:29:27:27:67:
03:8b:e6:c7:87:3a:c1:b1:16:04:90:35:62:16:4b:96:81:a2:
f5:54:76:35:52:34:3a:7c:58:ba:f9:62:9e:a2:07:bc:dc:a9:
24:bf:b7:68:34:f9:ca:f8:d1:63:eb:2e:0e:41:7e:bb:72:7c:
9d:19:6b:c5:cd:b6:6f:f6:2f:3e:ed:d4:e0:18:4a:e8:52:64:
fc:94:b1:cb:7a:8e:33:3d:44:51:1e:2e:3e:df:5c:8b:4e:84:
e4:e8:69:17:d3:d2:75:c5:ad:f0:db:42:e1:ff:a2:e0:4b:70:
19:cb:23:e5:71:e9:94:e5:8d:f8:aa:0e:92:c2:bd:65:cc:1a:
26:94:3b:0d
```

13. SIGNATURES GENERATION AND VERIFICATION RULES

13.1. Signature and hash generation algorithm

Below algorithm is used to generate receipt and fiscal day hash and signature:

- 1) Receipt or fiscal day fields must be converted to string (by rules as described in table below) and concatenated (no concatenation character is used);
- 2) Concatenated line must be hashed using SHA256;
- 3) Hash must be signed with private key.

Formula to get a hash: $\text{Hash} = \text{SHA-256}(x_1 || x_2 || \dots || x_n)$;

Formula to get a signature:

Signature = $\text{RSA}(\text{Hash}, d, n)$ - in case RSA keys are used

or

Signature = $\text{ECC}(\text{Hash}, \text{CURVE}, g, n)$ - in case ECC keys are used

Where

$||$ - means field concatenation;

x_1, x_2, \dots, x_n - receipt or fiscal day fields;

d - secret RSA exponent;

n - RSA modulus

CURVE - the elliptic curve field and equation used

G - elliptic curve base point, a point on the curve that generates a subgroup of large prime order n

n - integer order of G , means that $n \times G = O$, where O is the identity element.

13.2. Receipt signature generation and verification

Receipt hash and signature are generated according to the rules provided in section 13.1.

13.2.1. Receipt device signature

Fields included in receipt hash which is used for device signature are (these fields must be included in hash in the same order as provided below):

Order	Field name	Description
1	deviceId	Device ID
2	receiptType	Receipt type value in upper case.
3	receiptCurrency	Currency code (ISO 4217 currency code).
4	receiptGlobalNo	Receipt global number.
5	receiptDate	Date in ISO 8601 format <date>T<time>, YYYY-MM-DDTHH:mm:ss (hours are represented in 24 hours format, local time). Example: 2019-09-23T14:43:23
6	receiptTotal	Receipt total is included in signature in cents. Examples: - If receiptTotal is 500 ZWL, value 50000 must be used in signature. - If receiptTotal is 12,34 USD, value 1234 must be used in signature.
7	receiptTaxes	Concatenated receiptTaxes, where each line is concatenated in this way: taxCode taxPercent taxAmount salesAmountWithTax. In case of taxPercent is not sent, empty value should be used in signature. Amounts are represented in cents. In case taxPercent is not an integer there should be dot between the integer and fractional part. In case of

		exempt which does not send tax percent value, empty value should be used in signature. Taxes are ordered by taxID in ascending order.
8	previousReceiptHash	Previous receipt hash is included into current receipt device signature. This will create a chain of receipts. This field is not used in signature when current receipt is first in fiscal day.

Example

Name	Exmple No 1	Example No 2																																			
deviceID	321	322																																			
receiptType	FISCALINVOICE	FISCALINVOICE																																			
receiptCurrency	ZWL	USD																																			
receiptGlobalNo	432	85																																			
receiptDate	2019-09-19T15:43:12	2019-09-19T09:23:07																																			
receiptTotal	9450,00	51,50																																			
receiptTaxes	<div>Tax lines:<table><tr><th>taxCode</th><th>taxPercent</th><th>taxAmount</th><th>salesAmountWithTax</th></tr><tr><td>A</td><td></td><td>0,00</td><td>2500,00</td></tr><tr><td>B</td><td>0</td><td>0,00</td><td>3500,00</td></tr><tr><td>C</td><td>15</td><td>150,00</td><td>1150,00</td></tr><tr><td>C</td><td>15</td><td>300,00</td><td>2300,00</td></tr></table></div> <div>Result: A000250000B0000350000C1515000115000C153000230000</div>	taxCode	taxPercent	taxAmount	salesAmountWithTax	A		0,00	2500,00	B	0	0,00	3500,00	C	15	150,00	1150,00	C	15	300,00	2300,00	<div>Tax lines:<table><tr><th>taxPercent</th><th>taxAmount</th><th>salesAmountWithTax</th></tr><tr><td></td><td>0,00</td><td>7,00</td></tr><tr><td>0</td><td>0,00</td><td>10,00</td></tr><tr><td>14.5</td><td>1,50</td><td>11,50</td></tr><tr><td>14.5</td><td>3,00</td><td>23,00</td></tr></table></div> <div>Result: 0007000000100014.5150115014.53002300</div>	taxPercent	taxAmount	salesAmountWithTax		0,00	7,00	0	0,00	10,00	14.5	1,50	11,50	14.5	3,00	23,00
taxCode	taxPercent	taxAmount	salesAmountWithTax																																		
A		0,00	2500,00																																		
B	0	0,00	3500,00																																		
C	15	150,00	1150,00																																		
C	15	300,00	2300,00																																		
taxPercent	taxAmount	salesAmountWithTax																																			
	0,00	7,00																																			
0	0,00	10,00																																			
14.5	1,50	11,50																																			
14.5	3,00	23,00																																			
previousReceiptHash	YyXTSizBBRmJmK4VQL+sCnR+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWRmkeZsuAyFSnFkU2A+pKm91sOHVdjeRBebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkle+Bc=	I7CuFF8iHb4KNAN4dGaYTOaY3nmbhl7GfBA8x09HdWOZbexTuAZToN2RzVwu+K8TLWz7iJhi0FZUlyHut4+4h+SeT8etj5BY1trBM5At2ExPjZUkzaQSDxBvdFmgbwnDtkAHGksiX6zgqax1qz7j14FOjELG10tlqEqFGARt4=																																			
Result used for hash generation	321FISCALINVOICEZWL4322019-09-19T15:43:12945000A000250000B0000350000C1515000115000C153000230000YyXTSizBBRmJmK4VQL+sCnR+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWRmkeZsuAyFSnFkU2A+pKm91sOHVdjeRBebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkle+Bc=	322FISCALINVOICEUSD852019-09-19T09:23:0751500007000000100014.5150115014.53002300I7CuFF8iHb4KNAN4dGaYTOaY3nmbhl7GfBA8x09HdWOZbexTuAZToN2RzVwu+K8TLWz7iJhi0FZUlyHut4+4h+SeT8etj5BY1trBM5At2ExPjZUkzaQSDxBvdFmgbwnDtkAHGksiX6zgqax1qz7j14FOjELG10tlqEqFGARt4=																																			
Generated receipt hash in base64 representation	99I7KGnvNlvDsJ5CGXg7wpwYuAnUSyHhL2+l/066TY=	fSforS3nWjOAYjm1A936SJ79SoJJp30FLBR5T4Raa6w=																																			

13.2.2. Receipt FDMS signature

Receipt FDMS signature may be verified by decrypting receiptServerSignature with FDMS public key and comparing if it matches with prepared receipt hash. receiptServerSignature is generated only for receipt submitted in “Online” receipt mode. Hash generation algorithm is provided in section 13.1.

Fields included in receipt hash which is used for FDMS signature are (these fields must be included in hash in the same order as provided below):

Order	Field name	Description
1	receiptDeviceSignature	
2	receiptID	
3	serverDate	Date in ISO 8601 format <date>T<time>, YYYY-MM-DDThh:mm:ss (hours are represented in 24 hours format, local time). Example: 2019-09-23T14:43:23

Example

Name	Exmple
receiptDeviceSignature	YyXTSizBBRmJmK4VQL+sCnR+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWRmkeZsuAyFSnFkU2A+pKm91sOHVdjeRBebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkle+Bc=

receiptID	48377
serverDate	2019-09-19T15:43:12
Result used for hash generation	YyXTSizBBBrMjMk4VQL+sCnr+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWrmKeZsuAyFSnFkU2A+pKm91sOHVdJeR BebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkLe+Bc=483772019-09-19T15:43:12
Generated hash in base64 representation	JQolo/AgOsvm+PUQpvlQ/U7YMei3m/jbygNrBVfz6Sg=

13.3. Fiscal day signature generation and verification

Fiscal day report hash and signature are generated according to the rules provided in section 13.1.

13.3.1. Fiscal day device signature

Fields included in fiscal day hash used for device signature are provided below (these fields must be included in hash in the same order as provided below):

Order	Field name	Description
1	deviceId	Device ID
2	fiscalDayNo	Fiscal day number
3	fiscalDayDate	Fiscal day date (date when fiscal day was opened). Date in ISO 8601 format YYYY-MM-DD. Example: 2019-09-23
4	fiscalDayCounters	Concatenated fiscal day counter lines, where each line is concatenated in this way: fiscalCounterType fiscalCounterCurrency fiscalCounterTaxPercent or fiscalCounterMoneyType fiscalCounterValue. All text values are concatenated in upper case. Amounts are represented in cents. Only non-zero value fiscal counters are included in concatenation. Fiscal counters are concatenated in this order: <ul style="list-style-type: none"> fiscalCounterType (in ascending order) fiscalCounterCurrency (in alphabetical ascending order) fiscalCounterTaxID (in ascending order) / fiscalCounterMoneyType (in ascending order) In case taxPercent is not an integer there should be dot between the integer and fractional part. In case of exempt which does not send tax percent value, empty value should be used in signature.

Example

Name	Exmple			
deviceId	321			
fiscalDayNo	84			
fiscalDayDate	2019-09-23			
fiscalDayCounters	fiscalCounterType	fiscalCounterC urrency	fiscalCounterTaxPercent / fiscalCounterMoneyType	fiscalCounterValue
	SaleByTax	ZWL		23000,00
	SaleByTax	ZWL	0	12000,00
	SaleByTax	USD	14.5	25,00
	SaleByTax	ZWL	15	12,00
	SaleTaxByTax	USD	15	2,50
	SaleTaxByTax	ZWL	15	2300,00
	BalanceByMoneyType	ZWL	CARD	15000,00
	BalanceByMoneyType	USD	CASH	37,00
BalanceByMoneyType	ZWL	CASH	20000,00	
Result:				

	SALEBYTAXZWL2300000SALEBYTAXZWL01200000SALEBYTAXUSD14.52500SALEBYTAXZWL151200SALETAXB YTAXUSD15250SALETAXBYTAXZWL15230000BALANCEBYMONEYTYPEUSDLCASH3700BALANCEBYMONEYTYP EZWLCASH2000000BALANCEBYMONEYTYPEZWL CARD1500000
Result used for hash generation	321842019-09-23 SALEBYTAXZWL2300000SALEBYTAXZWL01200000SALEBYTAXUSD152500SALEBYTAXZWL151200SALETAXB YTAXUSD15250SALETAXBYTAXZWL15230000BALANCEBYMONEYTYPEZWL CARD1500000BALANCEBYMONEYTYP EUSDLCASH3700BALANCEBYMONEYTYPEZWL CARD2000000
Generated hash in base64 representation	Qa1YoTyZrGCP9oVZfO1Uz1XK7Xe2lVy8lesXZJKHO5o=

13.3.2. Fiscal day FDMS signature

Fiscal day FDMS signature may be verified by decrypting `fiscalDayServerSignature` with FDMS public key and comparing if it matches with prepared fiscal day hash.

Hash generation algorithm is provided in section 13.1.

Fields included in fiscal day hash used for FDMS signature are provided below (these fields must be included in hash in the same order as provided below):

Order	Field name	Description
1	<code>deviceId</code>	Device ID
2	<code>fiscalDayNo</code>	Fiscal day number
3	<code>fiscalDayDate</code>	Fiscal day date (date when fiscal day was opened). Date in ISO 8601 format YYYY-MM-DD. Example: 2019-09-23
4	<code>fiscalDayUpdated</code>	Date and time when fiscal day was closed. Date in ISO 8601 format <date>T<time>, YYYY-MM-DDThh:mm:ss (hours are represented in 24 hours format, local time). Example: 2019-09-23T14:43:23
5	<code>reconciliationMode</code>	Defines how fiscal day was close: automatically or manually. Possible values (in upper case): - AUTO - MANUAL
6	<code>fiscalDayCounters</code>]
7	<code>fiscalDayDeviceSignature</code>	Fiscal day signature generated by device. In case fiscal day is closed manually, this field is not included into hash for FDMS signature.

Example

Name	Exmple			
deviceId	321			
fiscalDayNo	84			
fiscalDayDate	2019-09-23			
fiscalDayUpdated	2019-09-23T22:21:14			
reconciliationMode	AUTO			
fiscalDayCounters	fiscalCounterType	fiscalCounterC urrency	fiscalCounterTaxPercent / fiscalCounterMoneyType	fiscalCounterValue
	SaleByTax	ZWL		23000,00
	SaleByTax	ZWL	0	12000,00
	SaleByTax	USD	15	25,00
	SaleByTax	ZWL	15	12,00
	SaleTaxByTax	USD	15	2,50
	SaleTaxByTax	ZWL	15	2300,00
	BalanceByMoneyType	ZWL	CARD	15000,00
	BalanceByMoneyType	USD	CASH	37,00
BalanceByMoneyType	ZWL	CASH	20000,00	
Result:				
SALEBYTAXZWL2300000SALEBYTAXZWL01200000SALEBYTAXUSD152500SALEBYTAXZWL151200SALETAXB XUSD15250SALETAXBYTAXZWL15230000BALANCEBYMONEYTYPEZWL CARD1500000BALANCEBYMONEYTYPEUS DLCASH3700BALANCEBYMONEYTYPEZWL CASH2000000				



fiscalDayDeviceSignature	YyXTSizBBRmJmK4VQL+sCnr+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWrMkeZsuAyFSnFkU2A+pKm91sOHVdjeRBebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkle+Bc=
Result used for hash generation	321842019-09-232019-09-23T22:21:14AUTOSALEBYTAXZWL2300000SALEBYTAXZWL01200000SALEBYTAXUSD152500SALEBYTAXZWL151200SALETAXBYTAXUSD15250SALETAXBYTAXZWL152300000BALANCEBYMONEYTYPEZWLCARD1500000BALANCEBYMONEYTYPEUSDLCASH3700BALANCEBYMONEYTYPEZWLCASH2000000YyXTSizBBRmJmK4VQL+sCnr+2AC6aQbDAn9JMV2rk3yJ6MDZwie0wqQW3oisNWrMkeZsuAyFSnFkU2A+pKm91sOHVdjeRBebjQgAQQIMTCVlcYrx+BizQ7Ib9iCdsVI+Jel2nThqQiQzfRef6EgtgsalAN+PV55xSrHvPkle+Bc=
Generated hash in base64 representation	//To59fLHvuoRe2slUpN2grJu5adaodOW6kW10Yvf/c=