Audit

An audit is a process of sequential transferring of audit packages from an SDC to the [*TaxCore.TaxCoreConfiguration.ElectronicMonitoringShortName*]] system and handling the response generated by the system for the specific taxpayer's [secure element.

There are two common scenarios:

- Remote Audit
- Local Audit

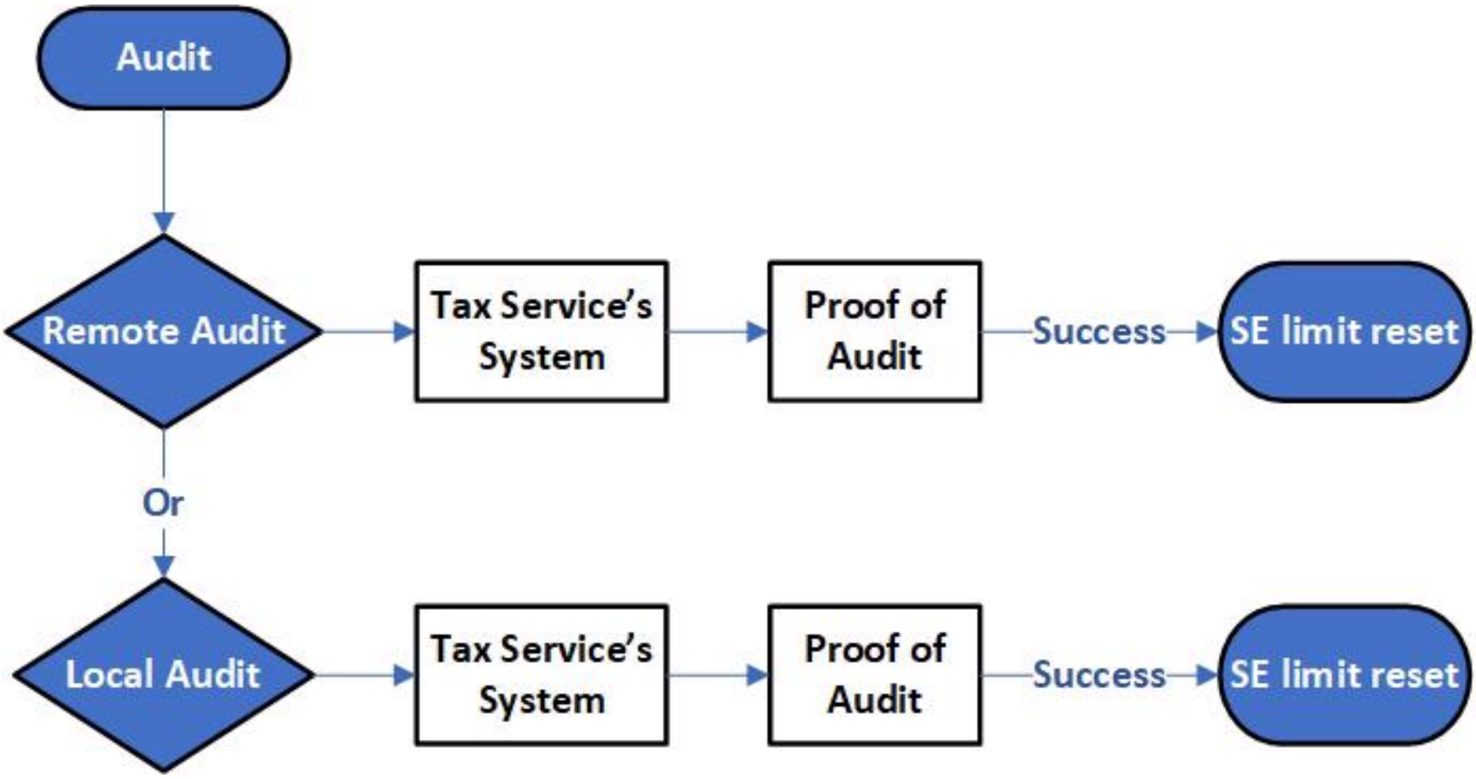
and two specific ones:

- Scanning the QR code on an invoice (performed by customers of tax auditors)
- Secure Element Audit (performed by tax auditors)

	Remote Audit	Local Audit	QR Scan	SE Audit
Audit type	Automatic	On Demand	On demand	On Demand
Data set submitted to VMS	Full	Full	Subset	Internal data only
Journal and Items	Full	Full	No	No
Security	Full	Full	Full	Full

An audit is always an asynchronous process. Depending on the amount of data and means of communication, it can take from less than a second to a couple of hours.

Once audit is completed, VMS will generate and deliver a Proof of Audit for a specific Secure Element. If the Proof of Audit is valid, the Secure element will reset the limit imposed during the personalization process.



Read more

- Local Audit
- Remote Audit
- Audit Request Payload - ARP
- Proof of Audit - POA

Local Audit

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

An audit is initiated by inserting an SD card or a USB Flash drive to an E-SDC device.

During the Local Audit, the E-SDC doesn't submit audit packages to the tax authority system directly; instead, those files are saved to an SD Card or a USB Flash Drive.

Local Audit from the perspective of a taxpayer:

1. Transfer the audit packages and ARP file from an E-SDC to external storage (e.g. SD card or a USB Flash drive)
2. Upload the audit packages and the ARP file using the section Upload audit packages on the Taxpayer Administration Portal
3. Check if there are pending commands for your E-SDC using the section Download Commands on the Taxpayer Administration Portal
4. If there are pending commands, download them to the external storage

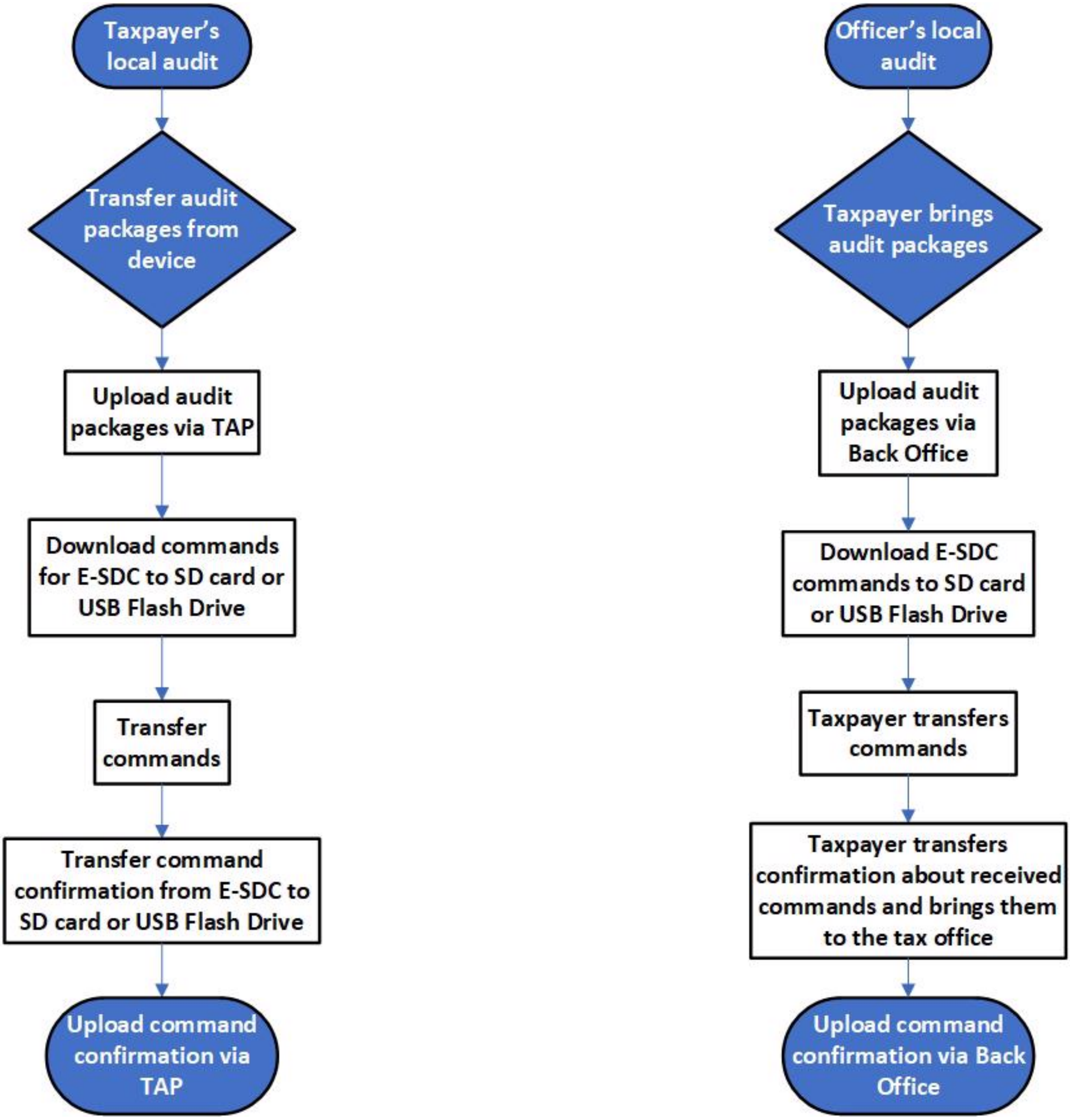
NOTE:
If you do not have any internet access, you can take the SD Card or USB Flash Drive to a tax office where a VMS officer will perform steps 2, 3 and 4.

5. Transfer the commands from the external storage to the same E-SDC
6. Transfer the confirmation about receiving the commands from the E-SDC to the external storage
7. Upload the confirmation using the Upload Commands Status on the Taxpayer Administration Portal.

NOTE:
If you do not have any internet access, you can take the SD Card or USB Flash Drive to a tax office where a VMS officer will perform step 7.

Local Audit from the perspective of a VMS officer:

1. A taxpayer brings an external storage unit (e.g. SD card or a USB Flash drive) containing audit packages transferred from their E-SDC or gives it to a Tax Inspector who is visiting the taxpayer's business premise
2. Upload the audit packages using the section Upload audit packages on the Back Office platform
3. Check if there are pending commands for the taxpayer's E-SDC using the section Download SDC Commands on the Back Office platform
4. If there are pending commands, download them to external storage
5. The taxpayer transfers the commands from the external storage to the same E-SDC
6. The taxpayer transfers the confirmation about receiving the commands from the E-SDC to external storage and brings it to the tax office or gives it to the Tax Inspector at their business premise
7. Upload the confirmation using the Upload SDC Commands Result section on the Back Office.


Taxpayer's local audit
Transfer audit packages from device
Upload audit packages via TAP
Download commands for E-SDC to SD card or USB Flash Drive
Transfer commands
Transfer command confirmation from E-SDC to SD card or USB Flash Drive
Upload command confirmation via TAP
Officer's local audit
Taxpayer brings audit packages
Upload audit packages via Back Office
Download E-SDC commands to SD card or USB Flash Drive
Taxpayer transfers commands
Taxpayer transfers confirmation about received commands and brings them to the tax office
Upload command confirmation via Back Office

Remote Audit

Remote audit is the process of transferring audit packages to the VMS system using the internet connection. It is the most common way to perform audits for any device with a stable internet connection.

Remote audit is executed automatically if there is an internet connection between the taxpayer's E-SDC and VMS system.

An E-SDC checks if the VMS system is reachable. If it is reachable, the E-SDC authenticates the VMS system by using a server-side certificate installed on the VMS system's endpoint, enabling HTTPS protocol. The tax authority’s system authenticates the E-SDC using a digital certificate issued on the Secure Element and issues a token for that session.

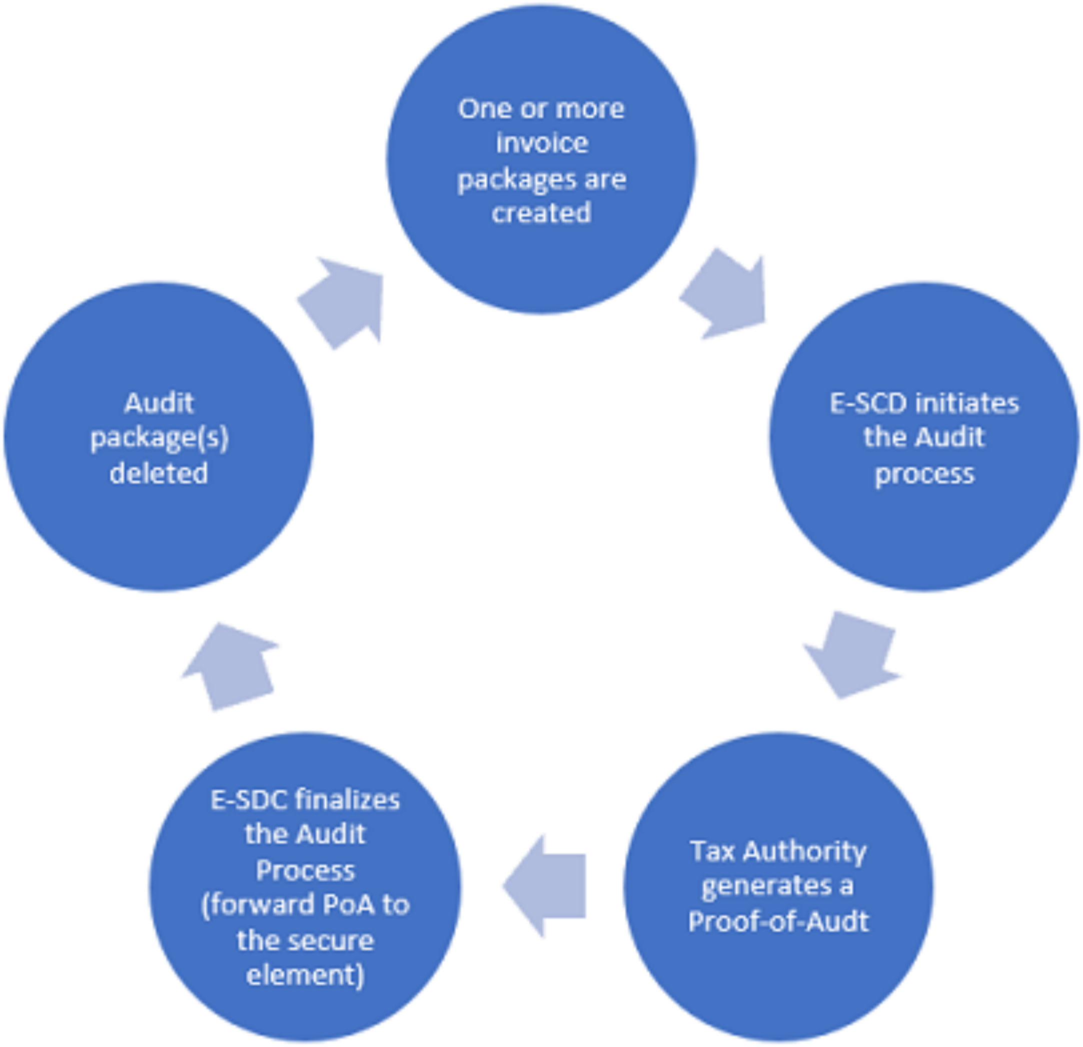
The E-SDC starts sending audit packages, performing a series of audits until no more unaudited data is stored on its non-volatile memory.

Performing a remote audit is not the only option for an E-SDC. If the network connection is not available due to the interruption of the service or a missing GPRS modem or network card, E-SDC will still be able to perform a local audit.

Proof of Audit - POA

Proof-of-Audit is a confirmation from the tax authority system that all the invoices issued with a particular secure element (one taxpayer can have more secure elements) have been stored in its database.

NOTE:
This article describes the default operation mode of the *Proof of Audit Service*. However, upon the Tax Authority’s decision, the service can use different strategies for issuing a proof-of-audit. For the currently applicable non-standard issuance strategies, see Currently Applicable Non-Standard Strategy for Issuing Proof of Audit.


One or more invoice packages are created
E-SCD initiates the Audit process
Tax Authority generates a Proof-of-Audt
E-SDC finalizes the Audit Process (forward PoA to the secure element)
Audit package(s) deleted

A Proof-of-Audit can be issued after each fiscal invoice (remote audit) or after a group of delayed invoices reaches the database (remote audit facing technical issues or local audit). It also confirms that the same data entered in the taxpayer's POS was transferred to the tax authority database.

However, not receiving a Proof-of-Audit does not immediately prevent the taxpayer from issuing new fiscal invoices. The taxpayer can continue issuing fiscal invoices without a Proof-of-Audit but there is always a preset limit until when a Proof-of-Audit can be delayed.

This setup forces taxpayers to report regularly.

Even if the internet failure prevents normal invoice transmission to the database, the taxpayer will be informed that the preset limit is approaching. The taxpayer can then perform a local audit in order to obtain a Proof-of-Audit from the tax authority.

Suppose due to the failure of the EFD component, or some other reason, the taxpayer is unable to send data on one or more issued invoices. In that case, the Tax Authority still has the option to issue a Proof-of-Audit if it can determine the tax liability for that secure element.

Currently Applicable Non-Standard Strategies for

Issuing Proof of Audit

In this article, you can read a description of the currently applicable strategies for issuing proof of audit (POA), if it deviates from the standard mode of operation of the Proof of Audit Service. Entries are divided by tax jurisdiction:

Serbia (PURS)

According to the decision of the Serbian tax authority (PURS), the eFiscalization system, on its production environment, currently implements a strategy of issuing POA after each valid request that the system receives from the taxpayer's E-SDC. In other words, the condition that, prior to the POA issuance, all invoices issued by that security element must be stored in the system's database does not apply.