Architecture

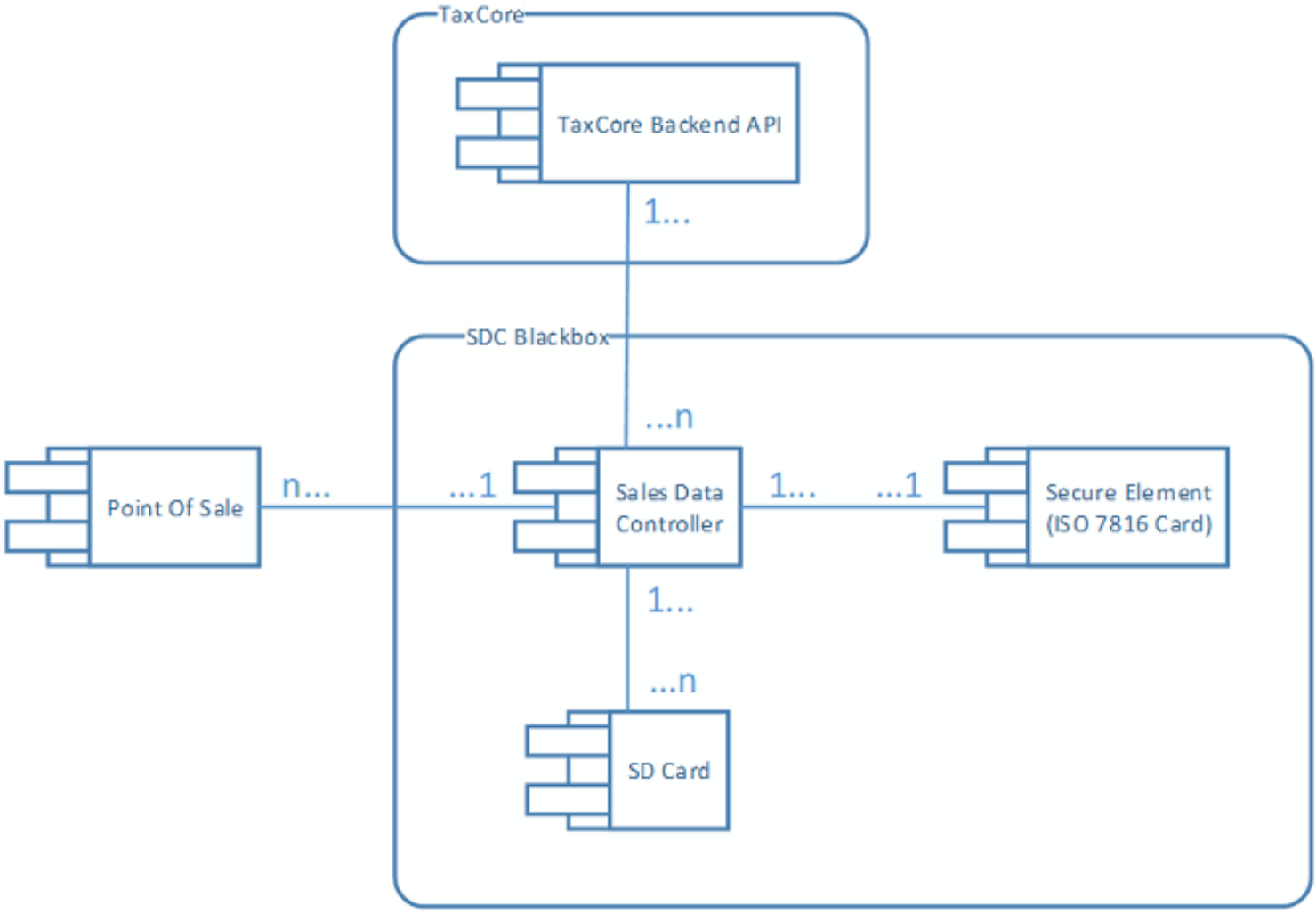
Content

1. [E SDC Implementation]
   E-SDC can be implemented as a hardware device or a software service depending on the E-SDC manufacturer's decision and clients' infrastructure. E-SDC can also be implemented as an integral part of a POS.

2. [Smart Cards]
   For standard operations, each E-SDC requires a Smart card issued by a tax authority, which consists of two applets:

3. [E SDC States]
   The diagram below shows the basic E-SDC states and transitions.

This figure shows the components of a fiscalization system and their mutual relationship.



ESDC Architecture – Image showing the components of a fiscalization system and their mutual relationship

E-SDC Implementation

E-SDC can be implemented as a hardware device or a software service depending on the E-SDC manufacturer's decision and clients' infrastructure. E-SDC can also be implemented as an integral part of a POS.

In any of those cases, the E-SDC component has to pass the same accreditation process and prove that E-SDC is implemented according to the instructions described in this document.

1. Ports
   Each E-SDC must provide ports or connectivity for the following purposes

2. Standards
   E-SDC device complies with all current local regulations regarding safety usage, electromagnetic compatibility, temperature range and power supply.

3. Power Supply
   It is allowed to use both AC and DC voltage for power supply. In the case of the AC voltage, a device shall work with the frequency range 50-60 Hz. The power supply circuit used by the E-SDC shall be protected with an automatic circuit breaker, suitable for electronic devices (type I).

Ports

Each E-SDC must provide ports or connectivity for the following purposes

Secure Element

E-SDC has a smart card reader in compliance with ISO/IEC 7810 and ISO/IEC 7816 standard. Smart Card reader may be internal to the E-SDC device or external usually connected via USB port with computer running E-SDC software.

The supported Smart Card sizes are 1FF (credit card size) and 2FF (mini SIM card size).

SIM card	Standard reference	Length (mm)	Width (mm)	Thickness (mm)	Volume (mm^3)

Full-size (1FF)	ISO/IEC 7810:2003, ID-1	85.60	53.98	0.76	3511.72
Mini-SIM (2FF)	ISO/IEC 7810:2003, ID-000	25.00	15.00	0.76	285.00

Audit

If the E-SDC device uses a USB flash drive for a Local Audit, USB connectors "USB Type B female" must be used.

Applied USB communication protocol shall be “USB 2.0” or higher.

For situations when an SD Flash memory card is used for a Local audit, a device must have an easily accessible Micro SD card connector.

For a Remote Audit, these Instructions do not limit a manufacturer in choosing a communication port as long as the invoice signing is not interrupted.

POS Connectivity

POS must be able to connect to the E-SDC using at least one of the following ports:

Ethernet

Ethernet port in compliance with IEEE 802.3 standard, present on an E-SDC device. The minimum speed of the Ethernet port is at least 10 Mb/s.

Wireless

Wireless connection in compliance with IEEE 802.11 (Wi-Fi/Bluetooth) to a POS device and a local network.

Standards

E-SDC device complies with all current local regulations regarding safety usage, electromagnetic compatibility, temperature range and power supply.

Particularly, in terms of electromagnetic compatibility, a product shall comply with the following standards

- EN 55022:2010
- EN 55032:2012
- EN 55024:2010 A1:2015.

A device's operational temperature range shall be 0° - 70° C (Commercial range).

Power Supply

It is allowed to use both AC and DC voltage for power supply. In the case of the AC voltage, a device shall work with the frequency range 50-60 Hz. The power supply circuit used by the E-SDC shall be protected with an automatic circuit breaker, suitable for electronic devices (type I).

In order to protect sensitive electronic components, the smart card and data stored on non-volatile memory, besides the mandatory basic protection, it is recommended that device is equipped with the additional fast overcurrent protection in the form of a fast fuse, e-fuse or similar device with the short time of operation.

When the DC voltage is used, protection against the reverse polarity shall be applied.

If the power supply voltages are higher than 75 Vdc or 50 Vac, a manufacturer shall obtain the appropriate certificate from a local authority, or represent a certificate valid in the country of use.

Smart Cards

For standard operations, each E-SDC requires a Smart card issued by a tax authority, which consists of two applets:

- Secure element Applet - used to apply a digital signature and maintain a set of fiscal counters in the offline mode
- PKI Applet - used to authenticate and establish a secure connection with the TaxCore.API web service

Both applets share the same PIN code. PIN is chosen during the process of requesting a secure element - see Requesting Additional Certificates.

PIN cannot be changed after it is selected.

Each smart card is uniquely identified by a UID - Unique Identifier. Each digital certificate issued for E-SDCs has UID embedded in the certificate's subject field.

1. Secure Element Applet
   Secure element (SE) is a fiscal component implemented as a special software or a device designed to receive invoice data, perform signing and data processing and generate a response which is sent back to the caller for further actions.

2. PKI Applet
   PKI Applet contains a digital certificate and a private key used to authenticate E-SDC to TaxCore.API web

services.

Secure Element Applet

Introduction

Secure element (SE) is a fiscal component implemented as a special software or a device designed to receive invoice data, perform signing and data processing and generate a response which is sent back to the caller for further actions.

This response provides the authenticity of invoice data.

Secure Element is issued and controlled by the tax authority. The main purpose of the SE is to sign invoices using a taxpayer's digital certificate, control audits and maintain a set of fiscal counters.

Each taxpayer is uniquely identified using digital certificates based on the Public Key Infrastructure (PKI).

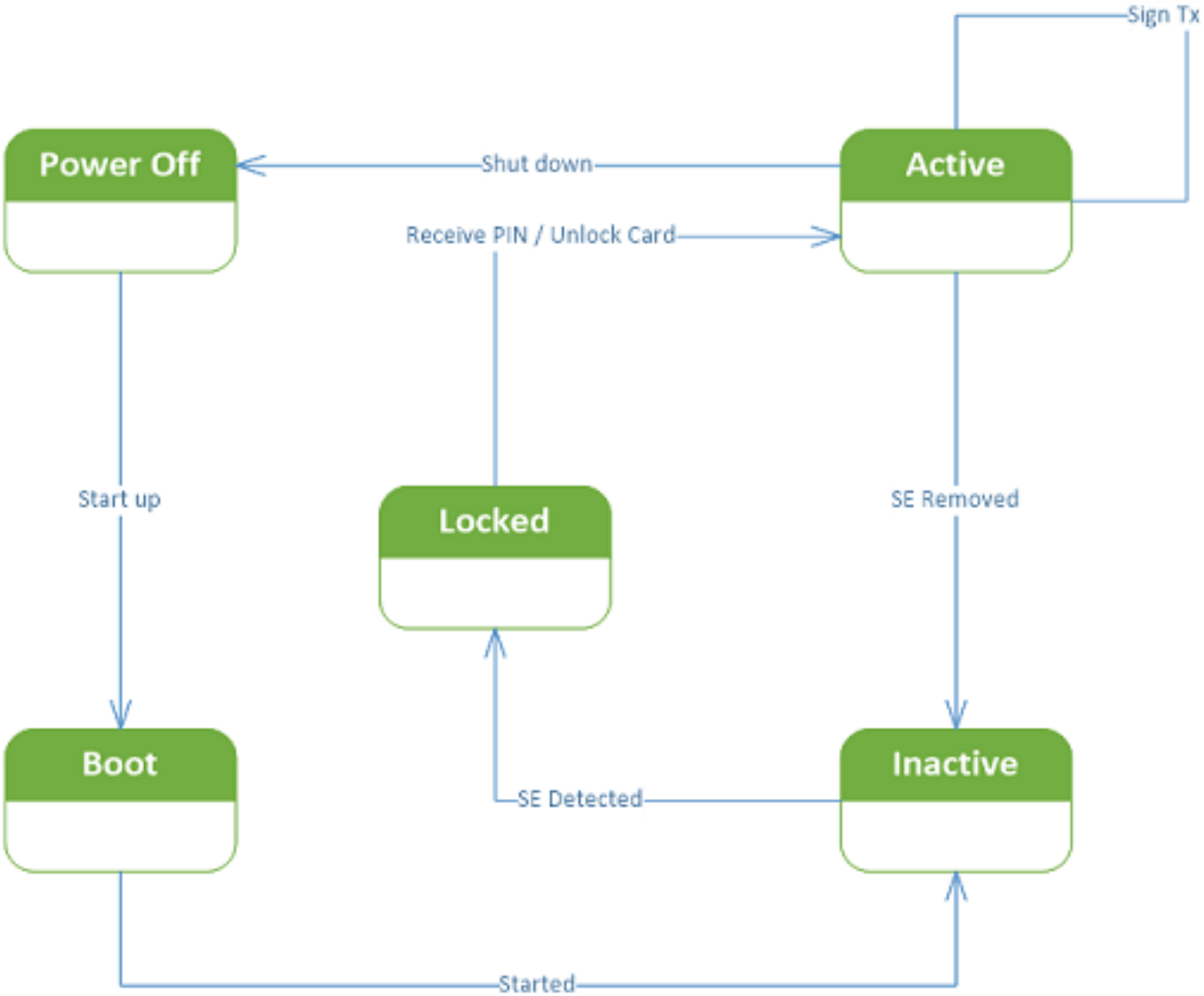
Secure element will stop issuing invoices if the maximum allowed amount for that particular fiscal device is exceeded – this facilitates the regular audit and forces taxpayers to report back to the tax authority system. Likewise, the SE will continue to produce fiscal invoices once it receives proof from TaxCore.API that audit has been received and stored on the tax authority's system.

PKI Applet

PKI Applet contains a digital certificate and a private key used to authenticate E-SDC to TaxCore.API web services.

E-SDC States

The diagram below shows the basic E-SDC states and transitions.



E-SDC States – Image showing the basic E-SDC states and transitions