



MD 29/04/2024
REGISTERED CASH REGISTER
SYSTEM – TECHNICAL
SPECIFICATIONS -

ADDENDUM 1 TO THE DETAILED
DESCRIPTION OF THE OPERATION
AND COMMUNICATION BETWEEN
THE CASH REGISTER SYSTEM AND
THE FISCAL DATA MODULE

VERSION 1.0 – 16/02/2026



CHANGELOG

Version	Date	Summary
1.0	16/02/2026	Translation NL-ENG



INTRODUCTION..... 1

Chapter 1 – Reason for the creation of this addendum 2

Chapter 2 - consequences 3

Chapter 3 – Technical provisions 4

 3.1. General provisions..... 4

 3.2. Technical conditions for FDM BII for POS-FDM connection..... 4

 3.3. Communication steps 5

Chapter 4 –target group restriction..... 6

 4.1 Definition of a fully cloud-based POS 6

 4.2 Scope of this definition 6



INTRODUCTION

The detailed descriptions POS and FDM provide in a more technical and detailed way the technical provisions of the ministerial decree of 29/04/2024 concerning the technical aspects and certification of the cash register system.

These documents may undergo minor changes due to potential regulatory decisions or to correct any errors.

However, if the changes are such that they require separate certification, an addendum will be published for this purpose.

Additional information can be obtained from the competent service, NCI department RCRS via secr.gksce@minfin.fed.be.

CHAPTER 1 – REASON FOR THE CREATION OF THIS ADDENDUM

Chapter 2 – POS – FDM Interaction describes the physical connection between POS and FDM in section 1.

The second paragraph contains the important note that this wireless connection via Wi-Fi **can also be established via the internet.**

Various POS integrators of cloud-based POS therefore use intermediate hardware, such as a Raspberry Pi. Once that POS has been certified, the FPS Finance no longer has control over the correct implementations on site (software updates, software modifications, etc.).

To avoid these risks, preference is given to an FDM bridge internet interface (hereinafter referred to as FDM BII), which is described in more detail below.

CHAPTER 2 - CONSEQUENCES

The application is, as mentioned below, only intended for fully closed-based POS. In order to guarantee the traceability of the installations, the authorised FDMs will receive a new certificate for this purpose.

This also means that changes to the certified solution, as well as firmware modifications to the FDM itself, must be communicated and approved in accordance with the Law of 30 July 2013 on the certification of registered cash register systems before they are implemented for end users. Undescribed functionalities may lead to the withdrawal of the certificate.

CHAPTER 3 – TECHNICAL PROVISIONS

The proposed FDM BII is **not** managed by the FPS Finance. However, through this addendum, the FPS Finance provides a generic and **mandatory** framework for the benefit of manufacturers. After all, FDM manufacturers know exactly where each FDM is located through its network address (e.g. for firmware updates, administration console, etc.).

The proposed functionality is **not** mandatory one, but may be offered to their customers, provided that it is submitted to the competent department of the FPS Finance as part (or update) of their certification.

To this end, the FDM manufacturer must provide the FPS Finance with a complete, detailed description, together with the product, for verification and testing. Given its nature, the certification procedure may involve an on-site visit to the FDM manufacturer's server environment.

3.1. GENERAL PROVISIONS

- Each manufacturer is free to develop its own solution, under its own responsibility.
- Responsibility for the security of the connection lies with the manufacturer, who must, however, comply with the requirements described below.
- If the connection is lost, the POS cannot reach the FDM and the POS stops working.
- Under **no** circumstances may the FDM manufacturer store data that passes through its servers via this connection.
- The solution offered is disabled by default. Only if the end customer requests it, through the use of a cloud-based system that meets the definition set out in Chapter 4, may this solution be enabled.
- If FDM BII is **offline**, **no** communication between POS and FDM may be possible.
- The solution must be completely **transparent** to FPS Finance. This includes:
 - **permanent** access and the ability to log in,
 - the ability to track which FDMs are actively using the solution.

3.2. TECHNICAL CONDITIONS FOR FDM BII FOR POS-FDM CONNECTION

- The POS sends its GraphQL mutation to the **network address of the FDM BII of the FDM manufacturer** instead of to the direct network address of the FDM, via a **secure TLS connection** (i.e. with encryption);
- The FDM BII verifies to which FDM the request should be sent; the **fdmId** must therefore be included **in the header of the GraphQL request** ;
- The FDM BII also **verifies** whether the end user (vatNo, estNo & posId) is authorised to use this FDM BII functionality;
- The FDM BII forwards the request via a **secure TLS** (encrypted) to the relevant FDM.
- The FDM's response follows the reverse route.
- If the FDM is unavailable, exactly the same procedure is followed as for a physical connection (retries, etc.).

3.3. COMMUNICATION STEPS

1. The FDM BII receives a request from a POS
 - a. Request is missing necessary headers: error message 'INTERNAL_FDM_BII_SERVER_ERROR'
2. The FDM BII verifies whether the combination of vatNo, estNo and posId is authorised to use the functionality each time a request is received
 - a. not authorised: error message 'FDM BII_NOT_ALLOWED'
 - b. authorised: the cloud application forwards to the called FDM
3. FDM is not active: error message 'FDM_NOT_OPERATIONAL'
4. FDM is active but cannot be reached: error message: "FDM_NOT_CONNECTED"
5. FDM is active but no response is received after 5 seconds: "TIMEOUT"
6. FDM is active and responds to the request: the FDM BII forwards the response to the requesting POS.

CHAPTER 4 –TARGET GROUP RESTRICTION

This functionality is reserved for installations where a fully cloud-based POS is linked to the FDM.

4.1 DEFINITION OF A FULLY CLOUD-BASED POS

A cash register system in which all core functions – such as transaction processing, stock management, reporting, customer management and integrations with external services – run entirely on servers in the cloud, rather than on a local server or solely on the cash register itself. Access is via the internet, which means that data is synchronized in real time and available on any connected device (PC, tablet, smartphone, payment terminal). Such POS cannot function without an internet connection (the entire backend runs in the cloud).

4.2 SCOPE OF THIS DEFINITION

A **fully** cloud-based POS meets the following 5 requirements:

- **No local server or software installation is required:** only an internet connection and a compatible device.
- **All functionalities are managed centrally in the cloud,** including updates, security and backups.
- **Real-time synchronization** exists between multiple branches, cash registers or sales channels (e.g. web shop + physical shop).
- **Flexible integrations** with external applications are possible (accounting, e-commerce, loyalty programs, payment providers).
- **Accessibility is guaranteed anywhere and anytime** via a secure login.