

FTFS® POS TERMINAL MANAGEMENT

POS Terminal & GT

USER MANUAL

FTFS® POS Terminal & GT

User Manual

Confidential

Document ed.1 of 24/03/2023

Authors

Francesco Fiume

Product Release 5.4.0.X (and following)

N&TS GROUP Networks & Transactional System Group S.p.A.
Strada 4 Palazzo A5 Milanofiori – 20057 Assago MI – Tel. +39 02822765.1

INDEX

1	Application Base Concepts	8
1.1	Microchip POS Terminals and GT	8
1.2	Authorization and Settlement.....	10
2	Consultation Guidelines.....	11
2.1	Manual Conventions.....	12
3	Access to the System	13
3.1	Access Authorization to the Functionalities.....	14
4	Exit from the System	18
5	Interface Operations	19
5.1	Standard Elements of the User's Interface Pages.....	19
5.2	Data Format	21
5.3	Insert New Data	21
5.4	Modify a Record Data	22
5.5	Remove a Record	22
5.6	FTFS MC Diagnostics	22
6	Navigation Chart	23
6.1	Home Page Flow Chart.....	23
6.2	Users Flow Chart.....	24
6.1	Amministration Flow-Chart.....	24
6.1.1	Acquirers.....	25
6.1.2	EMV Application	25
6.1.3	Connectivity POS / NCR CB2.....	26
6.1.4	Technical Profiles	26
6.1.5	Banks	27
6.1.6	Routing.....	27
6.1.7	CA Keys.....	28
6.1.1	CB2 Certificate Keys	28
6.2	Merchants/Terminals Flow Chart.....	29
6.3	Operativity Flow Chart	30

7	Users.....	31
8	Administration	32
8.1	Acquirers.....	33
8.1.1	Table: Acquirers and Interbank Data Detail	35
8.2	EMV Applications.....	47
8.2.1	Table: EMV Applications	48
8.3	Connections.....	49
8.3.1	Table: Connections	50
8.4	Technical Profiles	54
8.5	Banks.....	56
8.6	Routing.....	57
8.7	CA Keys.....	59
8.7.1	Table: Manual Load.....	60
8.7.2	Table: Load from File	61
8.8	CB2 Keys – certificates.....	62
8.8.1	Table: CB2 Key Detail.....	62
	Table: RSA-BANCOMAT Key Detail.....	62
	Table: RSA-POS Key Detail	62
	Table: POS Key Detail.....	62
8.8.2	Table: Certificate Detail	64
8.8.3	List of Requested Keys	66
8.8.4	Table: KMP Keys List.....	67
9	Merch / Store / Term.....	68
9.1	New Merchant.....	68
9.2	Merch/Store/Term Search.....	70
9.2.1	Merchants List.....	71
9.2.2	Merchant Point of Sale.....	72
9.2.3	Terminal List	76
9.3	Statistics DLL.....	93
9.4	Amounts List	94
10	Operations.....	95

10.1	Table: Transaction Detail	96
	Table: Last Transactions Detail	96
10.2	Exporting of Transactions	97
10.3	Manual Transaction Insertion	98
11	Operating Routes	99
11.1	Preliminary Configurations	100
11.2	Terminal Configuration	101
11.3	Terminal Accreditation	103
11.4	Preliminary Operations for CB2: Certificate Request	105
11.5	RSA Key Activation	108
11.6	Key and Certificate Already in Client Possession	109
11.7	KMP Key Creation	110
12	Appendixes:	111
	Appendix A: Dynamic Routing Mode Agreement	111
	Appendix B: Keys and Certificates Generation	117
13	Glossary	119

EDITION HISTORY

EDITION	DATE	CHANGES	CHAPTER
Edition 01	21/07/2022	First Edition: FTFS-5.4.0_mutEN	//
Edition 1	24/03/2023	First Edition: New N&TS GROUP document management model application	All document
		New Cover design	Cover

Purpose of the document

The manual describes the **FTFS**[®] User Interface developed using technologies that comply with the **PA-DSS** standard.

Pictures included within this manual are intended only as examples.

At Whom it is Aimed

The manual is intended for **FTFS**[®] administrators and users.

1 Application Base Concepts

FTFS® is the N&TS GROUP® product for the Microchip POS terminals concentration (Terminal Manager) and is aimed at organizations known as SERVICE CENTERS.

The task of a **Terminal Manager** is to provide the technical management of POS terminals installed at merchants, interfacing them in the authorization and accounting processes, with relevant entities. It provides the necessary information to the acquirer for the credit to the merchants, and to the Issuer the billing information of the cardholder.

1.1 Microchip POS Terminals and GT

The market introduction of cards and terminals with microchip technology, has led to the entities that manage these parts a material adjustment to the information systems.

When it comes to the POS terminals not only the technology has changes significantly but also the functionalities: they are no longer simple transaction devices for debit/credit card payments, but in conformity with the EMV specifications, must support one or more payment products, the *microcircuit applications*, parameters and data as a whole that alter the microcircuit card behavior so that it may perform the operations asked for the particular payment product.

The operation and the roles of the bank Acquirer (concessions operators, routing of requests for authorization, and accounting) remain largely unchanged with the advent of the microchip. Tasks assigned to service center change substantially for the correct function of microcircuit cards by their own terminals.

Phases of initialization and parameters update are particularly necessary for the management of the acquiring phase (quantity of security and applicative parameters).

Generally, the following types of information may be identified.

- *Quantity of security to protect the path between Terminals - Terminals Manager and to manage the card authentication phase.*
- *Acquiring parameters.*
- *Technical parameters used for the Terminal function.*

When it comes to the security mechanisms management, the FTFS functions are:

- *Generate the security quantities for the terminal path POS-GT.*
- *Distribute to the terminals the versions of public keys of the Certification Authorities necessary to the card authentication process.*

These are all carried out invisibly, compared to the interface.

Other FTFS functions are:

- *Information load that define the functional profile on terminals according to the modality known as DLL.*
 - *Management of transactions that are authorized through the service center in ON LINE TRANSACTIONAL mode, that is registered in the POS-GT track in ISO8583 EMV (see doc. ref. [1] and ref. [2]). The ISO protocol contains the authorizations and return operations of credit and debit card. Some service operations are included that do not have accounting value, like total requests and key realignment message. For authorization and return operations in ON LINE TRANSACTIONAL mode, the service center would normally refer to external acquirers, that are contacted with the interbank protocol (ISO8583).*
 - *Management of previously authorized operations in OFFLINE mode from the terminals.*
 - *Periodic creation of accounting logs to inform banks and companies of the transactions. The formats for the banks are owners, as they are established based on bilateral agreements between the Banks and their own Service Centers. For credit card companies, the “Log Unico” is produced, see doc. “ref. [3]”.*

The interface presented in this manual allows the management of this second group of functions.

1.2 Authorization and Settlement

The credit card financial transaction is normally completed in two distinct phases that are mainly for regulatory reasons:

AUTHORIZATION REQUEST

Check the availability of a certain amount to the credit card. The transaction authorization request is normally available from acquirers in online mode, wherein the processing unit is the single transaction and the response is immediate. This is due to the fact that the authorization systems are designed to serve primarily authorization sale at a real selling point.

MOVEMENT or FINANCIAL ACCOUNTING

After a time that depends on the type of product or service that the merchant delivers, the acquirer is required to credit the account of the operator of an amount corresponding to a request for authorization previously executed. The financial transaction handling is normally available from acquirers only in batch mode, or in a file that includes a lot of financial transactions and not in online mode as the authorization.

For the ATM card the distinction between authorization and financial movement is not normally applicable, which is still run by the acquiring entity.

The ATM card is therefore suitable only for contextual payments.

2 Consultation Guidelines

ATTENTION The information cited in this chapter, are omitted in the next descriptions of the manual.

This manual provides a description of the main technical and functional characteristics of **FTFS**, produced and distributed by N&TS, illustrating the basic concepts that compose it, the features/components/parts that make it up and the tables on which it is based on.

With regard to the operations, the description provides an illustration of the interface with specific reference to FUNCTIONALITY and PAGE.

The manual has been written describing in a conceptual manner the specifications, the objectives, the possibilities of management of the **functional** data of the application and some sub-areas also known as sub-features, **avoiding self-explanatory descriptions**.

The pages relating to the functionality of insertion, modification or deletion of data are only described in the following paragraphs of this chapter, because of the constant presence in the application.

The description of each feature may be supplemented by a **Table** that lists the descriptions/notes of the page fields of the interface of a function, exclusively in cases where:

Data input is not guided

and/or caption is not self-explanatory

and/or a special syntax is required.

If complex or significant, “*Operating Routes*” are described if relative to the insertion of new data of a procedure that, for example, must be “connected” to the data of other application procedures see dedicated chapter “**Operating Routes**”.

2.1 Manual Conventions

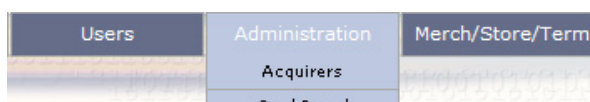
To access a function of the application, possibly referring to the masts proposed in the chapter "Navigation Tree", follow the trail that can be represented:

- from the menu section of the required voice (Example. main menu function HOME PAGE - subset functions)
- by "clicking" a video button or a link.

EXAMPLE

Path to access the editing function of the data relating to an acquirer (See the Acquirer Detail page):

Administration, Acquirers, link corresponding to the acquirer.



Select from the navigation bar, in succession:

1 the **Administration** button to display the sub-features;

2 the **Acquirers** button to display the page with a list of companies (table) already configured.

	Acquirer	Description	DLL Capability
	AMEX	AMERICAN EXPRESS	DLL

Select, from the table in the work area, the **link** corresponding to the **Acquirer required** to display the page that lets you change the related data.

3 Access to the System

The client stations that have-to-have access to the user interface may simply do so through an HTML browser.

Activating the connection through the browser, typing the URL **https://<host>:port/FTFS** where *host* is the IP address or symbolic name where the operator interface is installed and *port* is the port configured for the publication of the pages – see ref. [2] the **FTFS** login page is shown with the fields for the user authentication (login, password and image code identification or CAPTCHA).

Based on the specified identifier (Username field) privileges are granted correlated to the type of user you have been assigned. Belonging to a category determines what functions are enabled.

Based on the category belonging to a user, some operations are automatically denied through the elimination of the menu voices that permit reaching it.

In defining the access possibilities, five kinds of users have been provided:

- 1 *Belonging to the **Admin** profile.*
- 2 *Belonging to the **Technical Operator** profile.*
- 3 *Belonging to the **Financial Operator** profile.*
- 4 *Belonging to the **Routing Operator** profile.*
- 5 *Belonging to the **User** profile.*

Users belonging to the **USER** profile are exclusively allowed to the consultation of archives limited to information relating to the companies belonging to the Business Unit associated with them.

There are 3 types of **OPER** profiles:

- **Technical Operator:** *an operator that has the rights to create or change any parameter that is related to terminals, changing the types of cards accepted, setting and changing the technical parameters of the terminal.*
- **Financial Operator:** *an operator who is involved in financial management and has the right to arrange (e.g. voiding) any previously performed payment. The financial operator can debit a cardholder / debit a merchant or (the opposite) credit a cardholder / debit the merchant.*
- **Routing Operator:** *an operator that has the capability to set the connection parameters that are distributed to the terminals that use different connection modes and protocols or networks.*

Users belonging to the **ADMIN** profile, in addition to the prerogatives of users OPER, have rights to the consultation and modification of the contents of the product configuration tables.

The menu structure reported later in the document covers all the pages, as they are shown for the user which has the ADMIN role with Super User privileges. For users that have logged in with users associated with a more limited role, the restrictions cited above are valid.

When it comes to access control mode, the system follows the rules “Minimal Security Measures”, complying with the legal mandatory (DPR-318/99), through an authentication gateway.

3.1 Access Authorization to the Functionalities

The following table illustrated the access authorization to the FTFS interface based of the user category.

Based on the identifier specified in the system access page (user field) privileges that correspond to the user category on which you have been assigned are acquired.

Belonging to a category determines which applicative functions you have enabled (fully described in the previous paragraphs). User management is made external to the system and is not subject to this documentation.

Following is the menu with the type of user that may have access.

If not specified, access is read/write (**rw**).

Abbreviations are:

(**AA**) Admin

(**OO**) Technical Operator

(**FF**) Financial Operator

(**OC**) Routing Operator

(**UU**) User

Home (AA, OO, FF, OC, UU)

System (AA, OO, FF, OC, UU)

> Service

Users (AA, OO, FF, OC, UU)

> Change Password (AA, OO, FF, OC, UU)

> Business Unit (AA, OO, FF)

> Remove Business Unit (AA rw)

> New Business Unit (AA rw)

> Business Unit Detail (AA rw, OO r, FF r)

Administration

> Acquirers (AA rw, OO r)

> New Record

> Acquirer detail

> Associate EMV Application

> NCR Data

> CB2 Data

> Interbank Data Detail

> EMV Applications (AA rw, OO r)

> New Record (AA rw, OO r)

> EMV Application Detail (AA rw, OO r)

> Connectivity NCR

> Remove Connectivity NCR (AA rw, OO rw)

> New Connectivity NCR (AA rw, OO rw)

> Connectivity NCR Detail (AA rw, OO rw)

> Connectivity CB2

> Remove Connectivity CB2 (AA rw, OO rw)

> New Connectivity CB2 (AA rw, OO rw)

> Connectivity CB2 Detail (AA rw, OO rw)

> Remote Data Connection

> Remove Remote Data Connection (AA rw, OO rw)

> New Remote Data Connection (AA rw, OO rw)

> Remote Data Connection Detail (AA rw, OO rw)

> Technical Profile

> Remove Technical Profile (AA rw, OO rw)

> New Technical Profile (AA rw, OO rw)

> Technical Profile Detail (AA rw, OO rw)

- > Banks (AA rw, OO r)
 - > Remove Bank
 - > New Bank
 - > Bank Detail
- > Routing Debit Card (AA rw, OO r)
 - > Remove Routing Debit Card
 - > Increase Priority Routing Debit Card
 - > New Routing Debit Card
 - > Routing Debit Card Detail
- > Routing Credit Card (AA rw, OO r)
 - > Remove Routing Credit Card
 - > Increase Priority Routing Credit Card
 - > New Routing Credit Card
 - > Routing Credit Card Detail
- > CA KEYS (AA rw, OO r)
 - > Remove CA key
 - > Manual Load
 - > Load from File
 - > CA key Detail
- > CB2 keys - Certificate (AA rw, OO r)
 - > TM Key Detail
 - > RSA BANCOMAT key Detail
 - > RSA POS key Detail
 - > KMP Detail
 - > POS Detail
 - > TM Certificate Detail
- > Merchant Code (AA rw, OO r)
 - > New Merchant Code
 - > Remove Merchant Code

Merch/Store/Term (AA, OO, FF, OC, UU)

Note: The user can not insert Merchant if has not got a Business Unit .

- > New Merchant (AA, OO)
- > Search Merch/Store/Terminal (AA, OO, FF, OC, UU)
 - > Merchant List
 - > Merchant Detail
 - > New Store (AA, OO)
 - > Store List

- > Remove Store (AA)
- > Store List
 - > Store Detail
 - > Terminal List
 - > Remove Terminal (AA)
 - > New Terminal Standard - Virtual - Operative (AA, OO)
 - > Terminal Transaction List
 - > Detail Terminal
- > Terminal List
 - > Remove Terminal (AA, OO)
 - > New Terminal (AA, OO)
 - > Terminal Detail (AA rw, OO rw, FF r, UU r)

Note: In Terminal Details OC can only modify 'TECHNICAL PARAMETR' and Connection TM1/TM2 and TM3'

- > DLL characteristics
- > Terminal Total amount
- > Total amount List
- > New Accreditation (AA, OO)
- > New Cashier (AA, OO)
- > Acquirer Accreditation List
- > Remove Acquirer Accreditation (AA, OO)
- > Acquirer Accreditation Detail
 - > CB1/CB2 Data
 - > EMV Applications List
 - > Remove EMV Application (AA, OO)
 - > Associate EMV Application (AA, OO)
 - > Alternative Routing Management
 - > New Alternative Routing (AA, OO)
- > DLL Statistics (AA, OO, FF, OC, UU)
- > Total Amount List (AA, OO, FF, OC, UU)

Operations (AA, OO, FF, OC, UU)

- > Search TRX (AA, OO, FF, OC, UU)
- > TR Manual Insert (AA, FF)
- > Recent TRX (AA, OO, FF, OC, UU)
- > Export TRX (AA, OO, FF, OC, UU)

Amount (AA, FF)

Note: A user can execute searches only if he has shops.

4 Exit from the System

It is always opportune to exit from FTFS, if you leave your computer unattended. This is even truer once the work session of the user connected is over.

To exit from the application, use the **Logout** button (present in every page).

If there is no activity for a time greater than the value set for the system parameter **Validity Seconds** of the **Web Session**, the session will be automatically closed.

5 Interface Operations

5.1 Standard Elements of the User's Interface Pages

The following page is an example that describes the standard elements of the application interface. The user interface is divided and organized into features consisting of a set of pages that collect uniform information. Each feature can be composed of one or more pages.

All FTFS pages are logically split into areas/core functions.

The screenshot shows the FTFSn&ts application interface. The top navigation bar includes links for Home, Utenti, Amministrazione, Eser/Vend/Term, Operativita', and Logout. The main content area displays a table titled 'Lista Acquirers' with columns for Acquirer, Descrizione, Abilitazione DLL, Stato Connessione, Identificativo Acquirer, N. Applicaz. EMV, Creazione, Modifica, and Dati Interbancario. The table lists various acquirers such as MAESTRO, MC, PB, SECETI_ACI, SETEFICC, SETEFIPB, SI_ACI, SSBCCA, and VISA. A 'Nuovo record' button is located above the table. The footer indicates '9 record trovati.' and '© Networks & Transactional Systems SpA'.

1. Page Header

Present in all pages and contain:

- The name of the N&TS GROUP application, the user nickname.
- The navigation bar.

2. Navigation Bar

May contain the following buttons:

HOME (displays the Home Page), LOGOUT and the items that allow you to access the FTFS functionality of and sub-functionality of a macro-area (displayed only if the user is enabled).

NOTE *the LOGOUT function allows immediate exit from the user interface; for data confidentiality, it is always recommended to use it at the end of the working section.*

3. Title Page

Contains the **title of the page** with the functionality.

4. Workspace



May contain:


- lists of consultations compared to the data already entered (tables)
- fields or drop-down lists, option buttons, check fields, etc.. To **enter, modify and/or delete** data and/or **enable/disable** specific operations
- fields to set the criteria for a search
- the results of a search, etc.

It can contain buttons that provide access to **sub-functions** related to a specific page.

Each table present in the workspace can be **sorted** by selecting the column header for which you want to execute the order.

The tables in the workspace can contain one or more **links** that mainly allow:

- display the Key Features 
- delete a record 
- enable/disable the status of a function

Gestione Esito :	00	
<ul style="list-style-type: none"> • Approvazione trans. a fronte di AAC carta dopo approv. online • Storno trans. a fronte AAC carta dopo approvazione online 		

4. Workspace

Each Drop-down list allows you to select one of the options present. Clicking the drop-down list, options are displayed (if available, use the scroll bar to view all items), point to the one you want and select it. For example:



The Option buttons link two options relating to one activity (one of the two always active) and allow you to select one of the two exclusively.

It may contain one or more buttons (ex. Create, Update, Search, etc..) that are enabled to:

- store the new data entered;
- store the changes to a pre-existing record;
- perform searches against the criteria set by displaying the results, etc:

5.2 Data Format

The fields of the user interface can represent alphabetic, numeric, alphanumeric data type.

For each input field, the interface checks, if required, the obligatory nature of the data and/or the type of data (numeric, alphanumeric, etc.).

5.3 Insert New Data

The page, if required in a procedure, allows the user to enter all the data of a new item or records of a registry.

In the insert page, already filled out fields in relation with a principal element previously defined may be present.

The specifications of the fields are described in the table relative to the macro-area.

In lists, the Creating and Editing columns of the field will not be listed in the tables.

The fields marked with **red** text are required

ONCE ENTRY IS COMPLETE:

select the button, usually positioned in the lower part of the page, enabled to store the new record.

5.4 Modify a Record Data

Usually, the page that allows the user to edit data for a *record* already present in a registry, is the detail page,

It is possible:

- *correct the data in a field by typing the new values;*
- *select or enable/disable a different option using: drop-down lists, option buttons, check fields, etc.*

There may be fields not editable, since they represent a reference to a principal element.

ONCE DATA MODIFICATION HAS BEEN COMPLETED:

select the button, usually located at the bottom of the page, which is enabled to store the changes to a pre-existing record.

5.5 Remove a Record

Generally, a record present in a list can be deleted by selecting the corresponding **Remove Link**, or via a button in the navigation bar or in the workspace of the page.

Usually, the interface asks for confirmation and indicates whether it implies eliminations of dependent items from the one selected.

5.6 FTFS MC Diagnostics



For every operation performed on the data base, the application returns a page or a box with the outcome of the operation. In the event of a failure, generally, a given a description of the type of error that occurred is given.

6 Navigation Chart

The **FTFS** user interface is composed of a set of pages hierarchically organized, as described in the following paragraphs, where **all the branches of the application functions** are described to which the user, with an **Administrator** role, can access.

Please note that **users with an Operator or User role**, have a **personalized menu** in which only **options that they are enabled for appear**.

These types of fields, used in every branch function indicate:

-  = **Button** present in the navigation bar;
-  = **Link** present in the table of the page viewed.

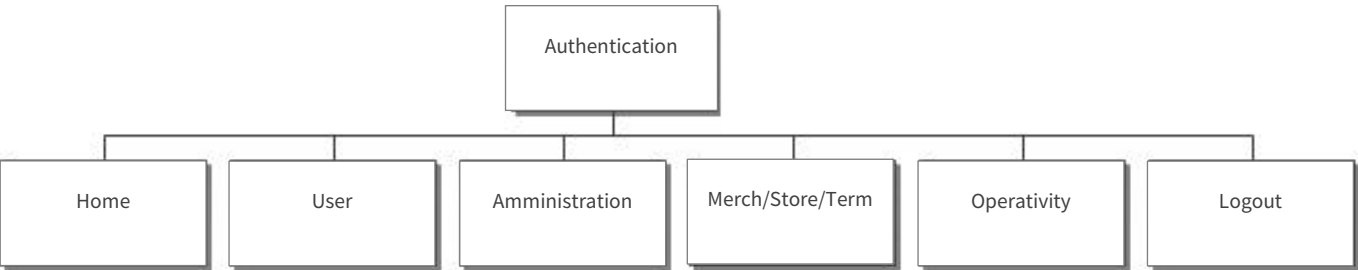
NOTE Most of the detail pages allow you to change all or part of this data.

6.1 Home Page Flow Chart

At the end of the identification of the user, it is possible to access the main menu that constitutes the FTFS operator interface. Using this page (to which you return whenever you select from the navigation bar, the Home button), you can access, if enabled, to the features of:

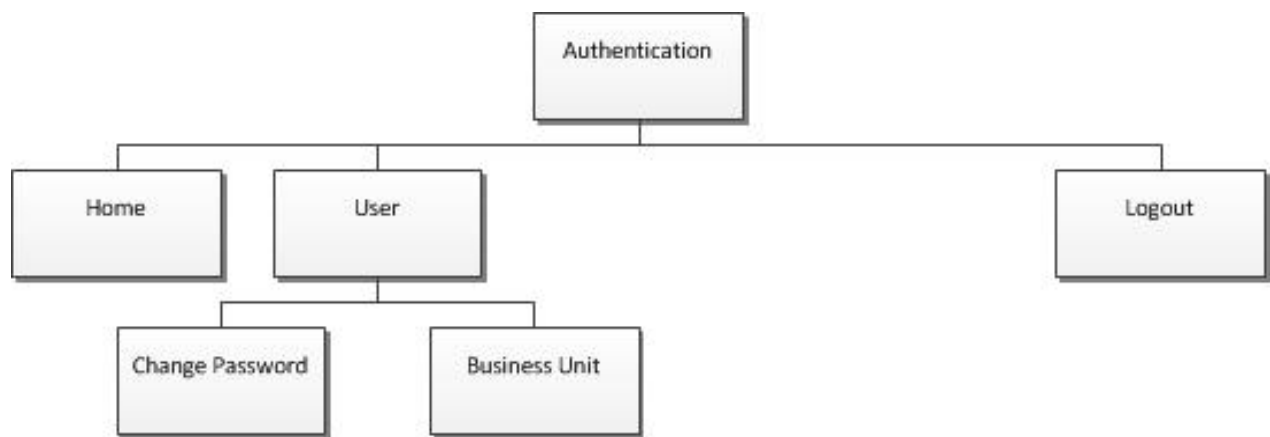
- *General Administration (enabled to: admin)*
- *Configuration Data Administration (enabled to: admin - superuser)*
- *Archive Query (enabled to: admin - superuser - user).*

In the present manual, functions enabled for the user with admin role (administrator) are described.

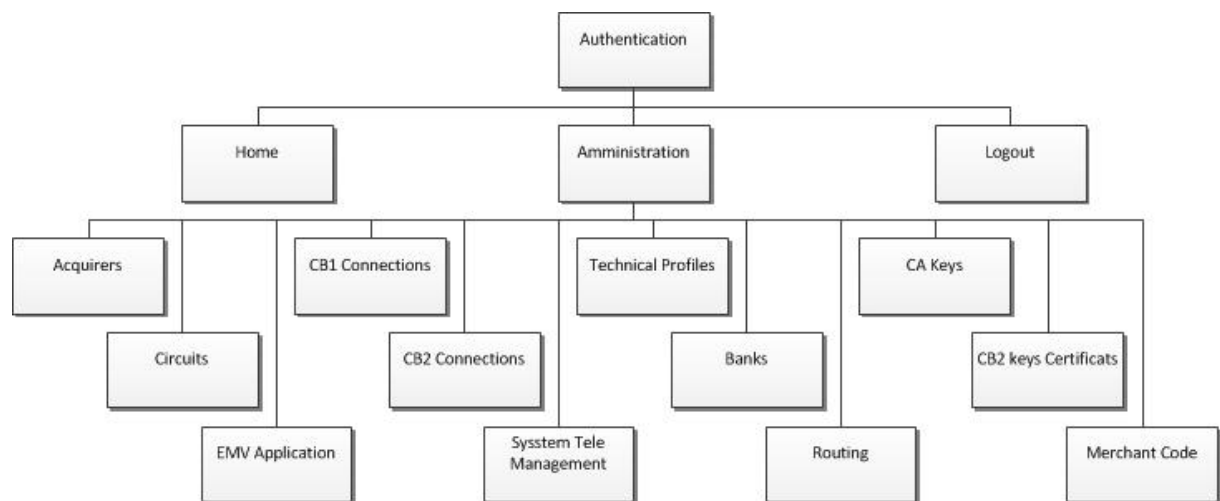


NOTE The **LOGOUT** function permits the immediate exit of the user interface.
For data confidentiality, it is recommended to **always use it at the end of the work session.**

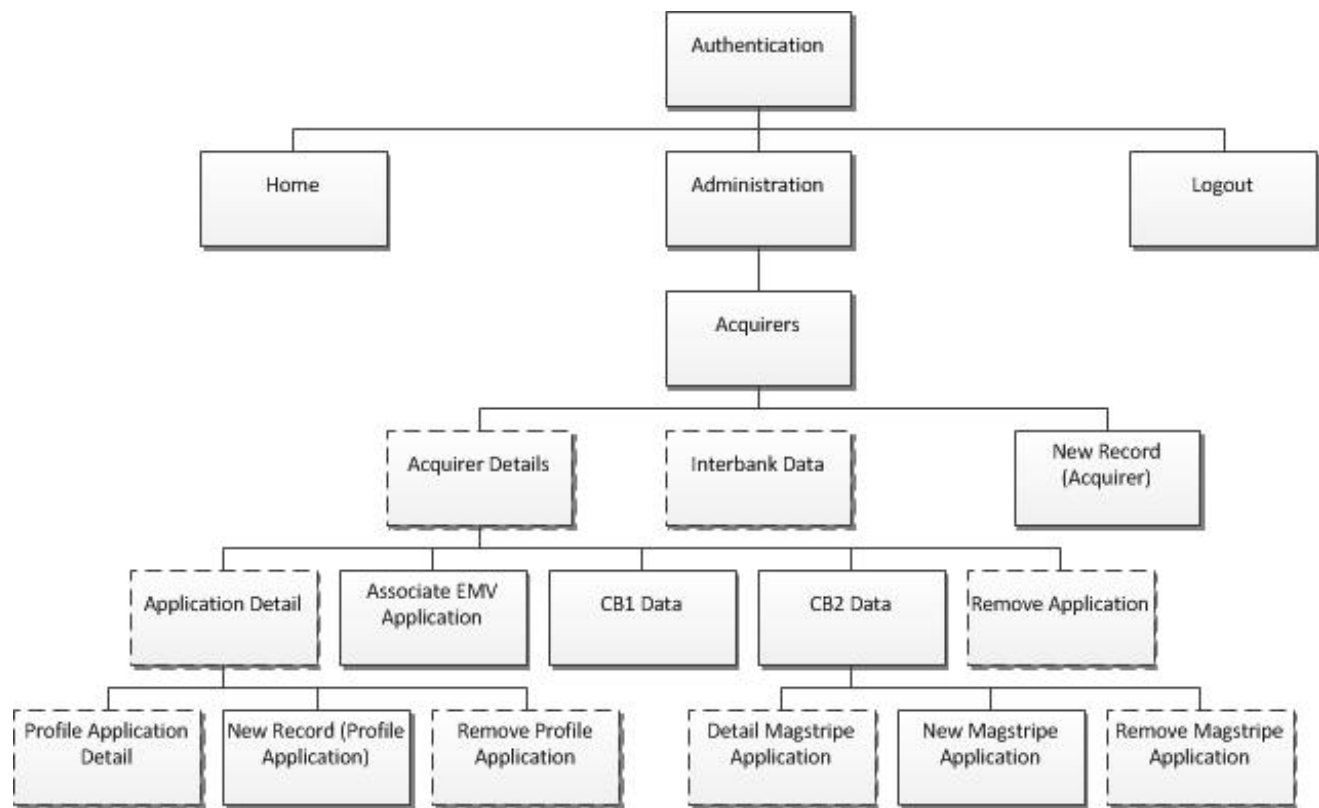
6.2 Users Flow Chart



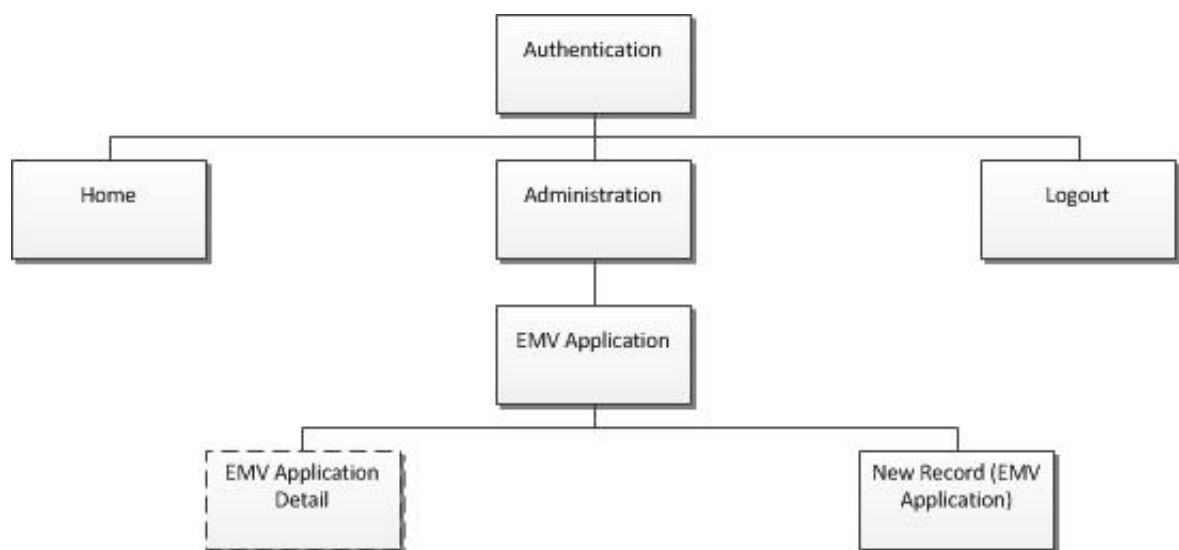
6.1 Amministration Flow-Chart



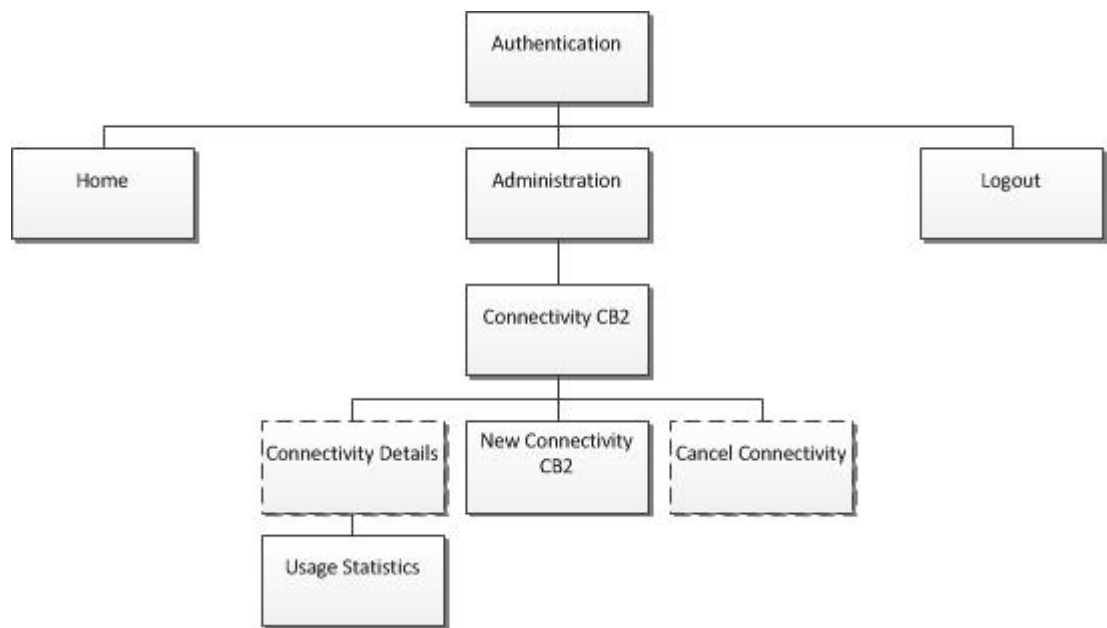
6.1.1 Acquirers



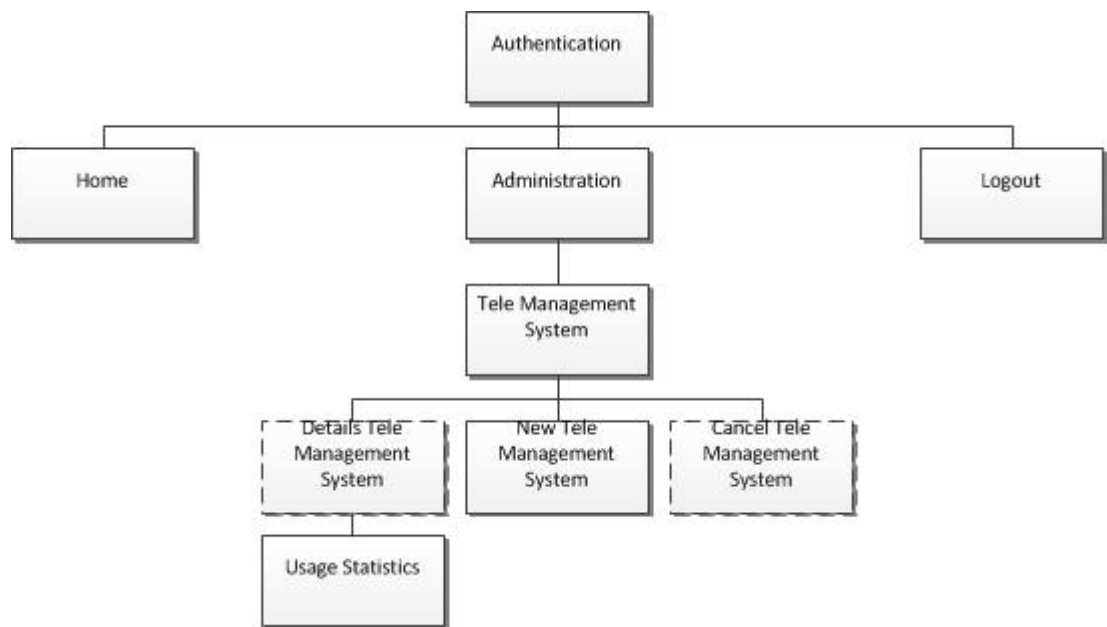
6.1.2 EMV Application



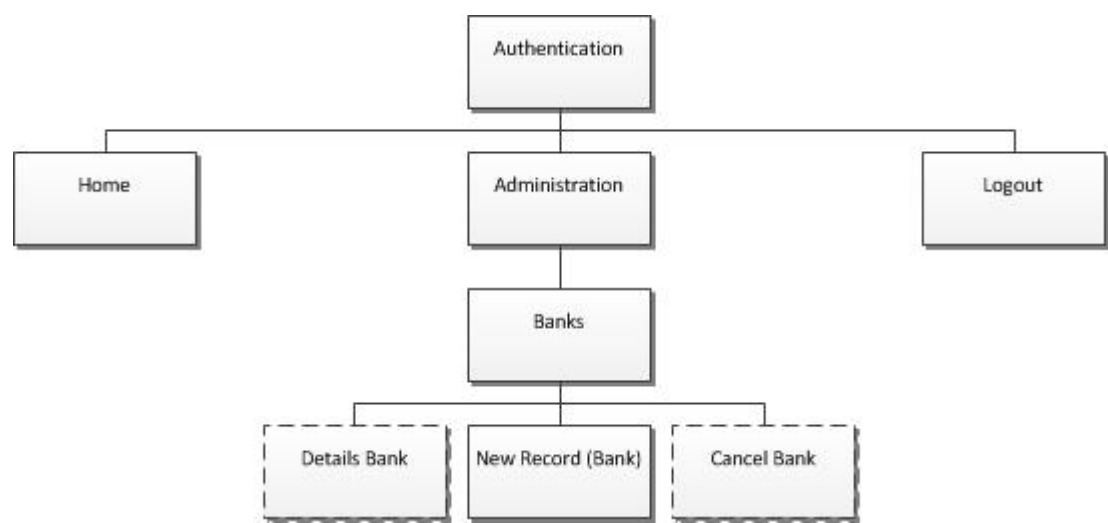
6.1.3 Connectivity POS / NCR CB2



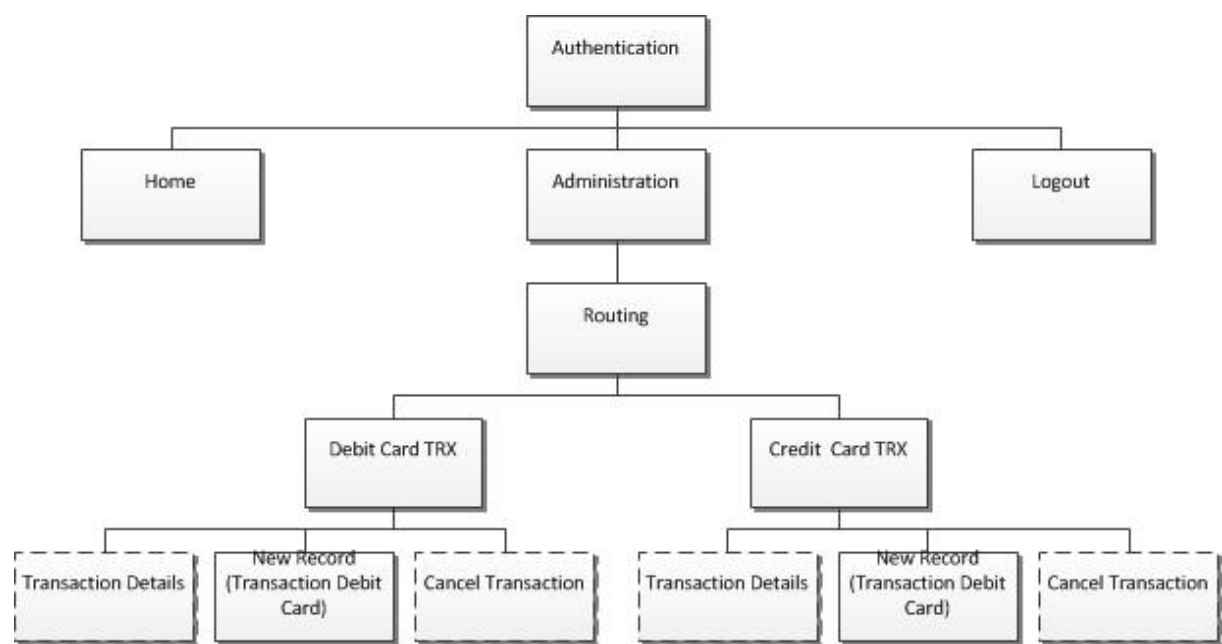
6.1.4 Technical Profiles



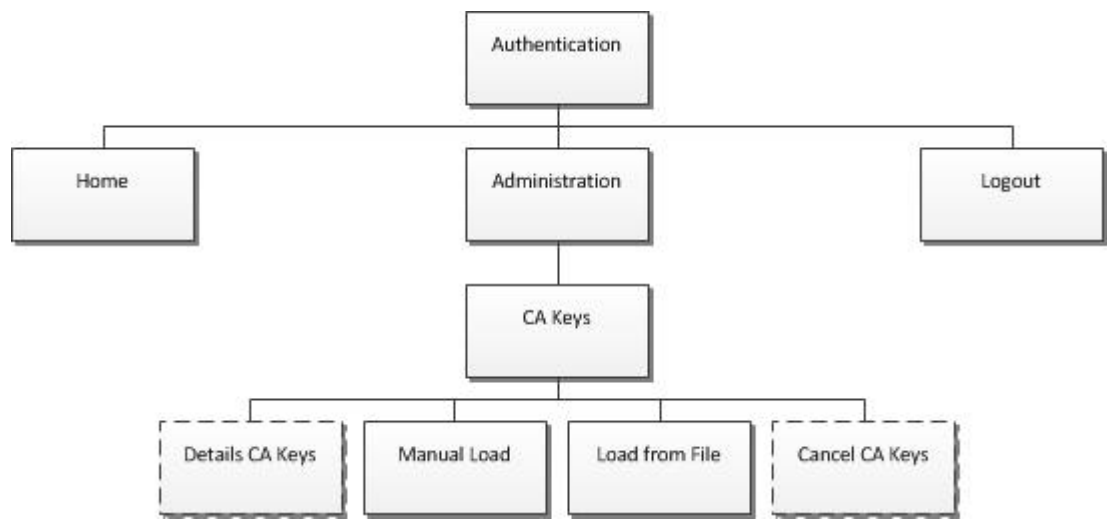
6.1.5 Banks



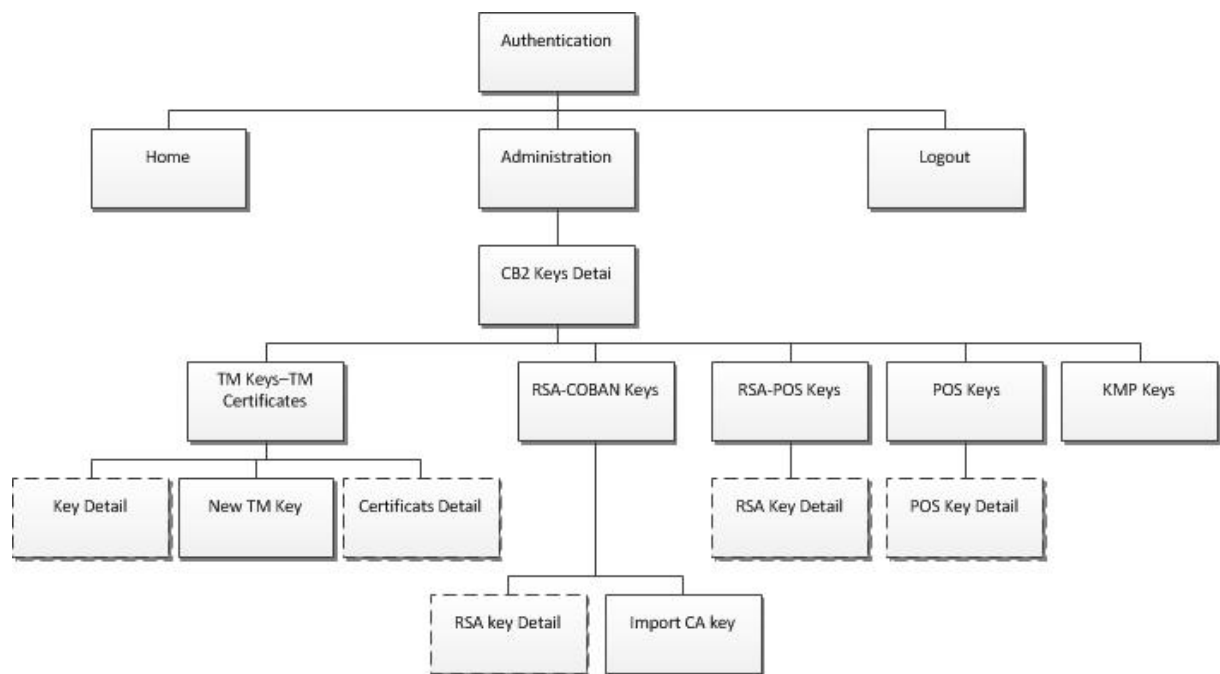
6.1.6 Routing



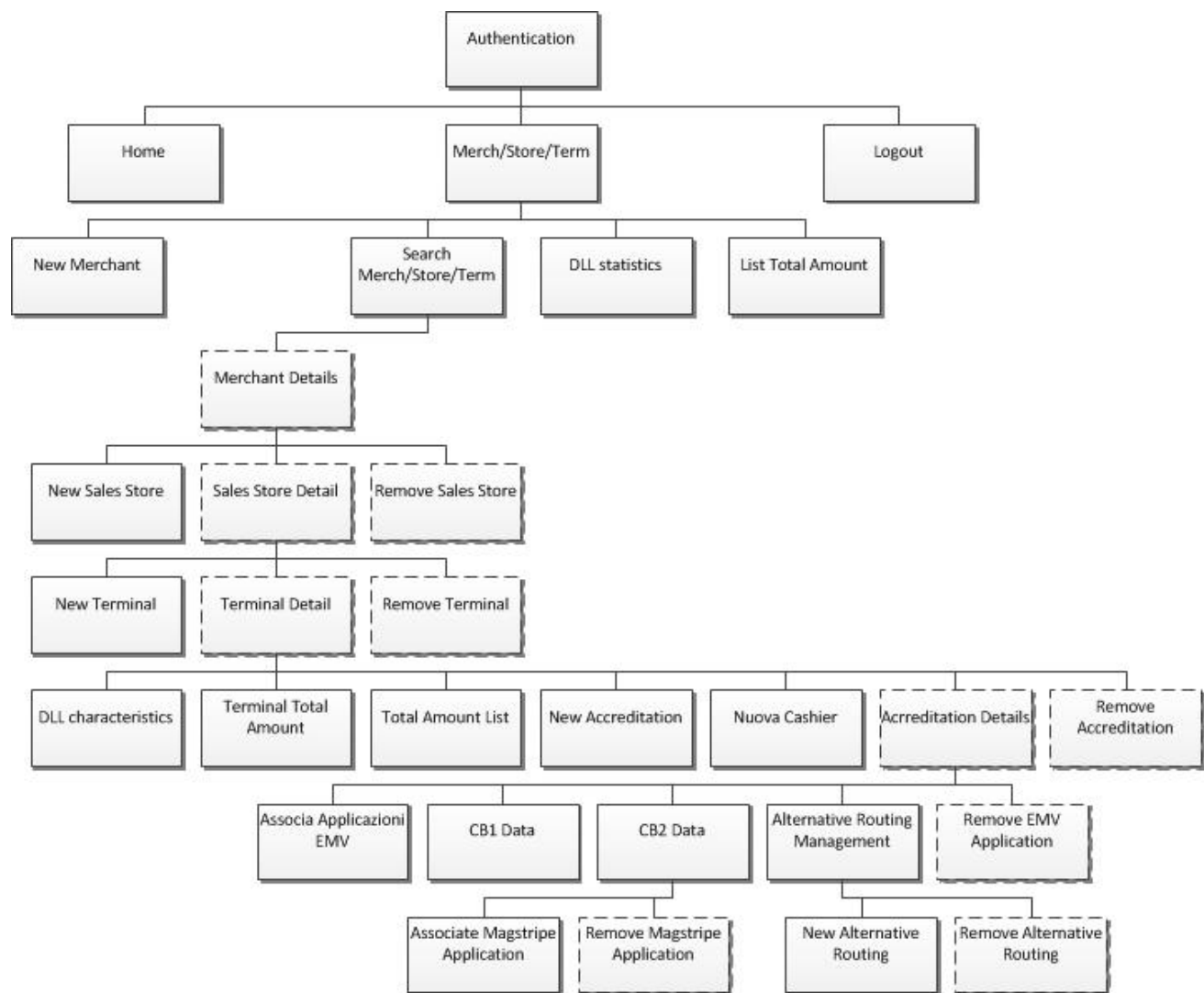
6.1.7 CA Keys



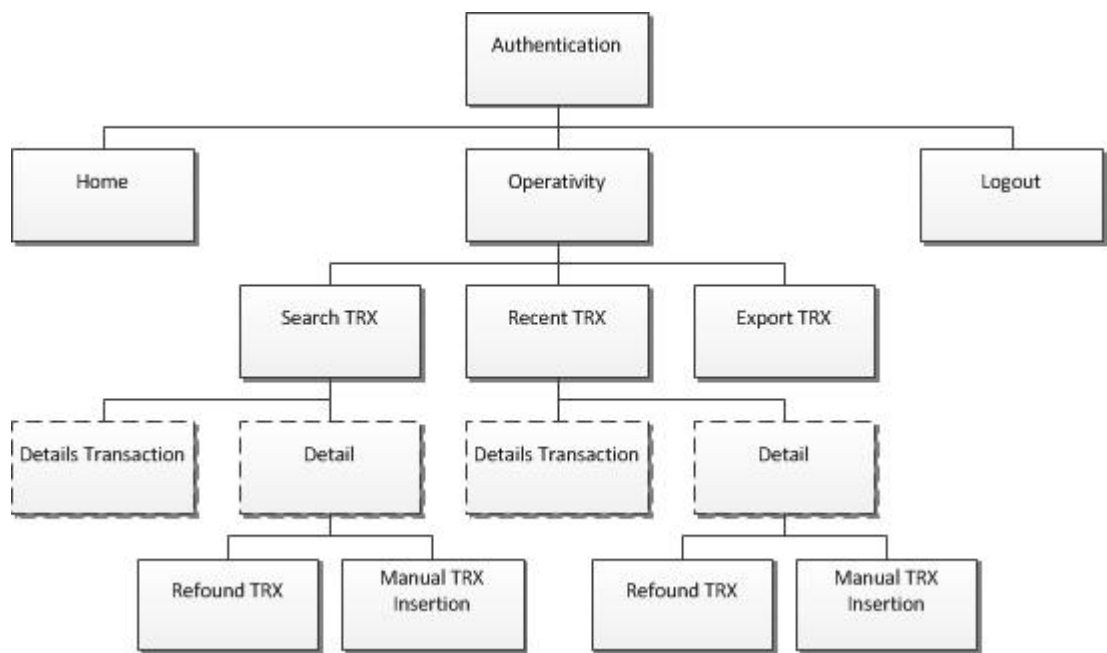
6.1.1 CB2 Certificate Keys



6.2 Merchants/Terminals Flow Chart



6.3 Operativity Flow Chart



7 Users

In this menu it is possible to change the password for the current user as well as create the Business Unit.

8 Administration

The function handles the procedures relating to the administration of the configuration tables that define the behavior of the FTFS system Terminal Manager.

The first page displays, in the navigation bar, the menu of sub-functions of the "Administration" area which is shortly described below:

Areas

- *Defines for the area a group of abi banking. Used for the management of accesses in “multi bank” mode to select access to information only (merchants, terminals, transactions, etc) of the abi enabled on the user.*

Acquirers

- *Definition of the Acquirers' general data (name, mode, description)*
- *Definition of the **acquiring general parameters** (denomination, enabled functions, receipt data).*
- *Definition of data for Acquirers that manage the payment cards EMV and EMV Application profiles.*
- *Definition of data to foreword to Service Centers/Companies.*

EMV Applications

- *EMV Applications management for which the system is enabled to operate. Visualization of the eventual CA Public Keys associated to each application.*

Connections

- *Definition of **general connection parameters** of POS to the GT and to the Remote Management Center, for Bancomat CB2 versions.*

Technical Profiles

- *Definition of **general working profiles for technical parameters** for POS terminals, in other words, of the data that characterize the terminals independently of the agreement, for Bancomat NCR and POS CB2 versions.*

Banks

Routing

- *Definition of Banks managed by the system and the Applicative Centers of reference.*
- *Routing definition relating to the BIN card data.*

CA Keys

- *management, load and removal of CA public keys associated to the payment circuits.*

CB2 Keys

- *Allows the management of the keys as from the 1.1.2 specifications [ref 2, 4].; for details reference to [ref. 12] and to “Appendix B: Keys and Certificates Generation” in this manual.*

8.1 Acquirers

The pages relative to the function ACQUIRERS allow you to define acquirers to manage payment cards accepted by POS terminals and operate on the **general parameters of acquiring**. These are normally established by agreements between the acquirers themselves and the GT center. Among the parameters you have, for example: the qualifications of the features supported by the acquirer, custom data to print on the receipt, etc...

In addition, to the Acquirer that handles microchip payment card, are present data to be sent to the terminal (in DLL phase) related to the process of risk control and the data of EMV applications.

Relative to the applications, we emphasize that each Acquirer can foresee one or more EMV application. To give flexibility to the application definition a structure in "profiles" has been adopted, providing the possibility of defining, for each application, one or more **Acquirer Application Profile** for which you can define the **general profiles of the EMV applications**, i.e. the configuration parameters that concur in the management of payment cards microcircuit. Between these: transaction result management, Terminal Action Code (TAC), random selection parameters, Application Version Number (AVN), etc.

The pages related to the ACQUIRERS area enable to display and manage:

- *the list of defined Acquirers (list)*
- *the detail of an ACQUIRER and the eventual modification of configuration data (insert/edit functions)*

In the ACQUIRERS function page, in the navigation bar the following button is present:

New Record

- *to insert configuration data for a new ACQUIRER (detail).*

The data related to an Acquirer are split in two “sections”: ACQUIRER DATA addressed as “Acquirer detail” and INTERBANK DATA.

In particular, the ACQUIRER DATA, in turn are divided into:

Data:

- *Acquirer data*
- *Acquirer identification*
- *microchip transaction management*
- *offline operation*
- *enabling Acquirer functionalities.*

NCR Data:

- *receipt data*
- *magstripe transaction management*
- *qualifications.*

POS CB2 Data:

- *receipt data*
- *optional functions data*
- *parameters to update acquiring profiles*
- *parameters ATM magstripe.*

INTERBANK DATA are related to:

- *interbank circuit connection data*
- *iso abicipa, data necessary to route the transactions to the interbank circuit*
- *PIN block data management*

In ACQUIRER DATA detail, if this manages EMV Applications for microchip cards, in the page below, the summary table of the defined EMV applications is displayed.

Other applications can be “associated” to the Acquirer using the insert page **Associate Application**.

Notes	The modification of the data present in the ACQUIRER detail produces a DLL reminder to all terminals that have an agreement with the Acquirer modified.
	The modification of the data present in the DATA INTERBANK detail does not produce a DLL reminder to all terminals that have an agreement with the Acquirer modified in the interbank section.
	For each Acquirer data is managed in version 1.0.1 (CB1) and 1.1.2 (CB2).

8.1.1 Table: Acquirers and Interbank Data Detail

Table relative to the detail of the fields of the following pages:

- *Acquirers List*
- *New Acquirer Definition*
- *View/Modify Acquirer Detail*
- *View/Modify Acquirer Interbank Data Detail*
- *Associate Acquirer Application*

ACQUIRER DETAIL

FIELD	DESCRIPTION	NOTES
Acquirer Data		
Acquirer	Unique Mnemonic code for identifying the acquirer in the system.	
Description	String that describes the Acquirer.	
Status	Acquirer enabled status. Values: Enabled, Disabled.	The Disabled state produces an outcome '907' on requests for authorization/reversal.
Debit Card Enabling	Indicates whether the acquirer is able to accept Debit Cards.	To be enhanced with "Enabled" for debit card acquirers.
DLL Enabling	Values: DLL only, DLL+Routing, Routing only.	To use option GDO.
Acquirer Identification		
ID Acquirer (*)	Identifies the Acquirer of the payment cards regardless of the technology; this Id is printed on the POS receipt.	See doc. ref. [1] FIELD 72 TAG 9F01
Acquirer Denomination (*)	Acquirer name, used by the terminal in the printing of receipts and messages displayed on the LCD.	See doc. ref. [1] FIELD 72 TAG DF38
Microcircuit Transaction Management		
DDAOL (*)	Represents the list of default data for the terminal necessary for the authentication of dynamic data.	Present for acquirers that handle EMV payment. See doc. ref. [1] FIELD 72 TAG 9F49
TCDOL (*)	Represents the list of default data in the terminal necessary for the calculation of the TC Hash Value if this is required in CDOL.	Optional. Present for Acquirers that handle EMV payment. See doc. ref. [1] FIELD 72 TAG 97
Offline Operations		

FIELD	DESCRIPTION	NOTES
Offline Auth Message (*)	Contains the message of authorization for transactions authorized in <i>off-line</i> that the terminal displays to <i>display</i> and prints on the receipt; the field must contain at least one character enhanced with '*': the number of '*' determines the size of the authorization code .	For acquirer that handle transactions for magnetic stripe and microcircuit. See doc. ref. [1] FIELD 72 TAG DF3E

Max Range Aut Offl Min Range Aut Offl (*)	Two subfields of 6 numeric characters each, which define a numeric range within which the terminal calculates a <i>random</i> number which is the authorization code for the transactions carried out with magnetic stripe cards and chip approved off-line.	Present for Acquirers that handle transactions for this magstripe in track 2 and microcircuit transactions. See doc. ref. [1] FIELD 72 TAG DF3D
--	--	---

Magstripe Transaction Management

Tel Voice-Contact (*)	Number for the phone call to the Voice Authorization Center.	Present for acquirers that handle transactions stripe track 2. See doc. ref. [1] FIELD 72 TAG DF3F
------------------------------	--	--

Profiles List

Number of Existing Profiles	Number of general profiles present for an EMV Application defined by the Acquirer.	Table field present for acquirers that handle EMV applications.
EMV Application (*)	Name of the EMV Application.	Table field present for acquirers that handle EMV applications.
AID (*)	Identifier of the EMV payment application and used by the terminal to identify and propose the card owner the selection of applications mutually supported by the terminal.	Table field present for acquirers that handle EMV applications. See doc. ref. [1] FIELD 72 TAG 9F06

(*) Data provided to the POS terminal in the DLL. The modification of this data produces a **DLL reminder** to all terminals that use them directly or indirectly.

ACQUIRER INTERBANK DATA DETAIL

FIELD	DESCRIPTION	NOTES
Data Connection		
Status Connection	Values: Active – Not Active	
ISO ABICIPA Data		
MAC Key	Value of the key used for the calculation of the mac mod sia.	The value is not presented on the screen for security problems
Confirm Mac Key	Confirmation previously entered.	
I033 Forwarding Inst ID	Identification code of the entity making the request of the transaction: ABI or company code.	For routing circuit interbank transaction.
I093 Destination Inst ID	Code identifying the final receiving institution of the transaction.	For routing circuit interbank transaction.
I094 Originator Inst ID	Code identifying the institution that originated the transaction.	For routing circuit interbank transaction.
I100 Receiving Inst ID	Code identifying the institution receiving the request or notification of a transaction: ABI, id circuit or company code.	For routing circuit interbank transaction.
ABI	Assigned Abi to the Company – optional.	For Batch / Accounting.
Company ID	Company code - optional.	For Batch / Accounting.
JTMS Queue	Queue name associated to the protocol in .xml file of physical communication management	In not valued, the transaction shows 909.
Timeout	Time-out waiting message.	If not valued uses the standard value (15 sec).
Pin Block Data Management		
PIN Block Key	Key used to encrypt the Pin Block on the interbank.	The value shown is not the key in "clear", but of the key encrypted under the LMK from the encryption form used by the system.

FIELD	DESCRIPTION	NOTES
PIN Block Key Check Value	Optional	
Encryption Type	Type of encryption used in the interbank Pin Block track.	S= Static D= Dynamic

(*) Data provided to the POS terminal in the DLL. The modification of this data produces a **DLL reminder** to all terminals that use them directly or indirectly.

ACQUIRER DETAIL - NCR DATA

FIELD	DESCRIPTION	NOTES
Sales Receipt Data		
Courtesy Message (*)	Message that the terminal prints on the receipt bottom of successful transactions.	See doc. ref. [1] field 72 TAG DF40
Magstripe Transaction Management		
Floor 1 (*)	Floor limit 1 for magnetic stripe.	Optional. See doc. ref. [1] field 72 TAG DF3B
Random Selection (*)	The rules of use are the same as currently in force for the data capture application (<i>off-line</i> approval of the transaction in less than a random selection for an on-line authorization request, subject to the controls on the type of transaction, on the floor limit, the mode of acquisition of PAN and Service code).	2-digit numeric For Acquirers that manage magnetic stripe transactions. See doc. ref. [1] field 72 TAG DF48
Enabled Ranges (*)	Ranges enabled for the Acquirer. See NOTES to this section.	Acquirer that handle transactions for mag stripe in track 2. See doc. ref. [1] field 72 TAG DF39
Functions		
Enabled Functions (*)	Allows the GT to enable specific features for the Acquirer.	See doc. ref. [1] field 72 TAG DF3A
Extended Functions	Allows you to enable/disable the functions of: Agos promotions disables the chip for payment card.	To value only on Agos acquirer with a management of extended promotions
(*) Data provided to the POS terminal in the DLL. The modification of this data produces a DLL reminder to all terminals that use them directly or indirectly.		

ACQUIRER DETAIL – CB2 DATA

FIELD	DESCRIPTION	NOTES
Sales Receipt Data		
First Line (*)	First line Acquirer ticket, required.	See doc. Ref. [1] field 72 TAG FF04 DF24
Second Line (*)	Second line Acquirer ticket, required.	See doc. Ref. [1] field 72 TAG FF04 DF25
Header (*)	Acquirer ticket header, optional.	See doc. Ref. [1] field 72 TAG FF04 DF26
Footer (*)	Acquirer ticket footer, optional.	See doc. Ref. [1] field 72 TAG FF04 DF27
Third Line (*)	Acquirer ticket third line, optional.	See doc. Ref. [1] field 72 TAG FF04 DF50
MSG OK (*)	Message printed on the receipt in front of a positive outcome, Required.	See doc. Ref. [1] field 72 TAG FF04 DF51
MSG KO (*)	Message printed on the receipt in case of an adverse outcome, Required.	See doc. Ref. [1] field 72 TAG FF04 DF52
Fourth Line (*)	Acquirer ticket fourth line, optional.	See doc. Ref. [1] field 72 TAG FF04 DF6B
Optional Functions Data		
TIP Percentage (*)	Determines the maximum percentage acceptable by the POS for the tip in respect to the amount of the transaction. Values from 00-99 If you valued 00 will be assumed.	See doc. Ref. [1] field 72 TAG DF45
Cash Back Parameters (*)	Contains parameters for the validation of the amount of cash back. Optional.	See doc. Ref. [1] field 72 TAG DF6D
Preauthorization Total Value (*)	Contains the amount that must be used for the preauthorization fuels. Required only if the acquirer has enabled this "preauthorization Fuel" feature.	See doc. Ref. [1] field 72 TAG DF6E

FIELD	DESCRIPTION	NOTES
Update Parameters Acquirer Profiler		
Frequency (gg) (*)	Acquirer profiles update parameters. Optional.	See doc. Ref. [1] field 72 TAG DF6E
Update Time (hh:mm) (*)	Acquirer profiles update parameters. Optional.	See doc. Ref. [1] field 72 TAG DF6E
Debit Card Magnetic Strip Parameters		
PBB ID Service (*)	Uniquely identifies the service.	See doc. ref. [1] field 72 TAG FF0D DF6A
PBB Name Service (*)	Debit card magnetic strip service name.	See doc. ref. [1] field 72 TAG FF0D DF49
PBB Features Enabled (*)	Bitmap of enabled functions for debit card magnetic strip.	See doc. ref. [1] field 72 TAG FF0D DF3A
<p>(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly</p> <p>(**) Only if the acquirer is enabled to magnetic strip debit card. Composed of 3 sub-fields id service, service name, functions enabled. See doc. Ref.[1] field 72 tag ff0d</p>		

In

Debit Card Magnetic Strip Application List

Magnetic Strip Applications Detail

the following fields are displayed:

FIELD	DESCRIPTION	NOTES
Service ID (*)	Uniquely identifies the service.	See doc. Ref. [1] field 72 TAG FF0A DF6A
Service Name (*)	Magnetic strip application service name.	See doc. Ref. [1] field 72 TAG FF0A DF6A
Description	Description for internal use.	

FIELD	DESCRIPTION	NOTES
Bin Table (*)	Key used to encrypt the Pin Block on the interbank.	See doc. Ref. [1] field 72 TAG FF0A DF39
Floor1 (*)	Floor limit for magnetic strip.	See doc. Ref. [1] field 72 TAG FF0A DF3B
RSL (*)	Random selection.	See doc. Ref. [1] field 72 TAG FF0A DF48
Enabled Functions (*)	Bitmap functions enabled.	See doc. Ref. [1] field 72 TAG FF0A DF57

Notes For more information about acquiring parameters see doc. "ref. [1] - Field 72 ACQUIRINGPARAMETERS " and "ref. [1] - Field 72 ACQUIRING PARAMETERS"

RANGES AUTHORIZED Field (NCR VERSION):

- A string of numeric characters and separators (valued at ' = ') ; each range can have a maximum size equal to 6 numeric characters.

In addition to the normal range specified in the field, which lay the cards on the plots two ISO to accept with the signature, the range of cards in ISO track 2 to accept the PIN verification (range, PIN -based) can be also specified. The range of PIN-based encoding is made by adding to the range the value "C" to the normal range encoding. The final separator of the range, the character " = ", remains unchanged in any case.

- You can define through the range, if the terminal needs to perform the control of the Service Code for the verification of the presence of the chip. The range must be coded with the value "B" placed before the field separator " = ". If the range contains this value, the terminal will not have to check for the presence of the chip via the Service Code for the application of payment of the indicated range, and then allows the use of the application for the magnetic strip transaction.

- In addition, it is now possible to specify the range indicating the interval between two values. The realization of this is done with the use of the value "A" between the extremes of the two intervals. The interval range as defined this way needs to be closed by the " = " separator in the case of signature acceptance, while it must be followed by "C", in turn closed by the separator " = " in the case of acceptance with the PIN.

BIN TABLE field (VERSION CB2):

The data is always present if given the tag FF0A, contains the range of BIN enabled for the Acquirer; it is used by the terminal to identify the list of acquirers with whom you can negotiate the payment card presented.

The data is present only for acquirers that handle magnetic strip track 2 payment cards.

Maximum length: 400 (encoding type "ns .. 800 ").

Value: This field contains the range (single BIN or BIN intervals) that identify the cards managed by the specific acquirer. It is BCD encoded (4 bits for each decimal digit or character separator). Each range consists of a minimum of 1 digit to a maximum of 12 digits. The field also contains the following special characters:

- 'B' (1011 semi byte) = indicates if the range below should be considered in addition to any range already granted to the terminal.
- 'C' (1100 semi byte) = indicates if the range below should be eliminated from any range already granted to the terminal.
- 'A' (1010 semi byte) = identifies the end of the first range and the beginning of the second range (interval).
- 'E' (1110 semi byte) = identifies the end of the range (or range of interval).

8.1.1.1 Table: Associates Application-Acquirer

Table relative to the details of the fields of the following page (self-explanatory excluded):

Definition of the EMV Application to Associate to the Acquirer

FIELD	DESCRIPTION	NOTES
Acquirer	Mnemonic code uniquely identifying the acquirer in the system.	
Application (*)	Name of the new application to associate with EMV acquirer.	Among the list of EMV Applications configured for the system.

(*) Data provided to the POS terminal in the DLL. The modification of these data produces a **DLL reminder** to all terminals that use them directly or indirectly.

Note On the **Associate Application** page used to define a new application for the Acquirer, the list of available applications is made up of the sole EMV applications available to the system and which have not yet been linked to the Acquirer. Afterwards you need to define **at least 1 Application Profile** for the Acquirer, to allow the EMV application to be usable in the Acquirer concession of the POS terminals.

8.1.1.2 Table: EMV Application Profiles List Table: Acquirer Application Profile

Table relative to the details of the fields of the following pages (self-explanatory excluded):

EMV Application Profile list

Acquirer Application Profile (detail)

FIELD	DESCRIPTION	NOTES
Profile	Mnemonic description assigned to the profile.	
AID (*)	EMV payment application identifier and is used by the terminal to identify and suggest to the card owner the selection of applications mutually supported by the card and the terminal.	See doc. ref. [1] field 72 TAG 9F06
Floor Limit (*)	Value used by the terminal for the management of the issue of <i>off-line</i> authorization.	See doc. Ref. [1] field 72 TAG 9F1B
Application Version Number		
AVN1 (*) AVN2 (*)	EMV application version.	2 possible values. See doc. Ref. [1] field 72 TAG 9F09
Transaction After ACC Card Outcome		
Outcome Management (*)	Outcome management of the transaction.	Establishes the method by which the machine handles the transaction outcome: in this specifications version the outcome of on-line transactions approved by the Issuer in exclusively encoded but that obtain an AAC from the card. The data is present only for the Acquirers that manage the EMV payment cards; if the data is not present, the terminal uses, as default mode, the rejection of the transaction, coherently with the AAC generated by the card. See doc. Ref. [1] field 72 TAG DF47

FIELD	DESCRIPTION	NOTES
Random Selection Parameters		
Perc. Target (*)	Parameters that regulate the activation on a random basis in the management of the <i>online</i> transaction.	Allowed values: Target Percentage: 00-99 See doc. Ref. [1] field 72 TAG DF41
Threshold Value(*)	Parameters that regulate the activation on a random basis in the management of the <i>online</i> transaction.	Allowed values: Threshold value: 0 –less than FloorLimit 1 See doc. Ref. [1] field 72 TAG DF41
Max.Perc.Target (*)	Parameters that regulate the activation on a random basis in the management of the <i>online</i> transaction.	Allowed values: Max target percentage: 00-99 greater than or equal to target percentage. See doc. Ref. [1] field 72 TAG DF41
Terminal Action Code		
Tac Denial Tac Online Tac Default (*)	How to manage transactions from the POS terminal.	Bitmap field made as such: 3 groups of 10 hexadecimal characters (each group represents 5 binary bytes) In order: Denial, Online, Default. See doc. Ref. [1] field 72 TAG DF42
Emv (CB2) Application Parameters		
Service ID (*)	Id service - meaningful only for cb2 pos.	See doc. Ref. [1] field 72 TAG FF09 DF6A
Service name(*)	Service name - meaningful only for cb2 pos.	See doc. Ref. [1] field 72 TAG FF09 DF49
Enabled functions (*)	Features' Bitmaps enabled for Acquirer and emv application - meaningful only for cb2 pos.	See doc. Ref. [1] field 72 TAG FF09 DF33
(*) Data provided to the pos terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.		

Notes For more information about the parameters of the EMV applications see doc. “**ref. [1] – Field 72 PARAMETERS OF ACQUIRING**”.

FOR CB2 TERMINALS the name of the defined tag “**See doc. ref. [1] CAMPO 72**” may be different, see **doc. ref. [1]**.

8.2 EMV Applications

The GT has the role to distribute on his own terminals the CA public keys of the applications used by the terminals to manage the payment with the microchip cards, keys necessary to the authentication process of the cards.

Every EMV applications can have more than one key, with a minimum of one that has to be usable by the system.

The pages related to the EMV APPLICATION allow to view and manage:

- *the list of EMV Applications defined in the system (list)*
- *the detail of an EMV Application (insert/modify), the number of CA public keys, and eventually modify the configuration data (enable/disable a CA public key).*

In the EMV APPLICAZIONE functions page, the following button is present in the navigation bar:

New Record

to insert configuration data for a new EMV Application.

Notes The insertion of information about an **EMV New Application** is only possible if FTFS is already in possession of at least one CA public key. The link between the two entities is as follows: the first 5 bytes (viewed in 10 hexadecimal characters) of the AID of the application are the same as the RID belonging to one or more CA public keys.

The insertion of CA public keys does not happen through the operator interface, but according to the alignment procedures provided for by national standards according to the methods and roles of the entities involved.

8.2.1 Table: EMV Applications

Table relative to the details of the fields of the following pages (self-explanatory excluded):

EMV Applications

EMV Application Detail

FIELD	DESCRIPTION	NOTES
AID (*)	EMV payment application identifier and is used by the terminal to identify and suggest to the card owner the selection of applications mutually supported by the card and the terminal.	Viewable hexadecimal format. See doc. Ref. [1] field 72 TAG 9F06
Description	Name and description of the application	
RID (*)	CA key Identifier.	Corresponds to the first 10 hexadecimal characters of the AID data. See doc. Ref. [1] field 59 TAG DF43
CA Public Keys		
Status	Values: ACTIVE enables the public key to be given in the DLL to the terminals; OFF the key should NOT be given to the terminals because disabled/expired.	Check box
Active Keys	Number of ACTIVE keys for the application.	Only active keys are transferred to the terminal in DLL phase.
Key Index (*)	The index of the CA's public key.	See doc. Ref. [1] field 59 TAG DF43
Start Date	Date and time of activation of the CA key.	
Expiry Date	Date and time of expiry of the CA key.	
Sent in the DLL	Boolean value yes/no referred to the CA key.	
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.		

8.3 Connections

The telephone numbers, the characteristics of the line and the connection modality of the terminals certified on a Service Center/GT can be shared between all the terminals or differentiated based on the type of service (GT center or Telemanagement service), are defined on each terminal, but are described on a specific table to which the terminal profiles refer to. In a minimal case then, the connection table contains only one record, more likely at least 2.

For each transaction the terminal executes three attempts, on a total of two connections that were communicated to him in the profile loading phase:

- *the data of the first connection is used for the first and second attempt, that are performed in an exact way*
- *for the third and last attempt the terminal uses the data of the third connection, which is usually certified on a different service center entrance.*

It is possible to also define the set of parameters eventually used by the terminals (is optional data) for the connection to the Telemanagement Center.

The pages related to the CONNECTIONS function allow to define the **general connection parameter profiles**, in particular it is possible to view and manage:

- *the list of the defined connections profiles (list)*
- *the detail of a connection and eventually to modify the configuration data*
- *remove a defined connection.*

On the navigation bar of the page, the following buttons are present and are briefly described:

New NCR Connection

Definition of a new profile connection with NCR specifications

New CB2 Connection

Definition of a new profile connection with CB2 specifications

For each type of connection exists a button:

Usage statistics

Display the POS terminal numbers, among all those surveyed, which use the connection.

Note The modification of the data present in the Connection detail produces a **DLL reminder** to all terminals that use the selected connection.

8.3.1 Table: Connections

Table relative to the details of the fields of the following pages (self-explanatory excluded):

Connections

New NCR Connection

New CB2 Connection

Connection Detail

8.3.1.1 NCR Specifics Version

FIELD	DESCRIPTION	NOTES
Connection		
Code	Unique private identifier of FTFS generated with a sequence and used as the key records pointing to the connection.	
Service Type	Specifies the use of the profile.	Allowed values: Connection to GM Connection to the Telemanagement center
Description	Name and description of the application.	
Line Type Type Net Speed (*)	Connection type and speed.	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2A TAGDF2E TAG DF32
Telephone (*)	Telephone number of the GT access.	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2B TAG DF2F TAG DF33
NUA (*)	Network User Address.	Optional DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2D

FIELD	DESCRIPTION	NOTES
		TAG DF31 TAG DF35
NUI (*)	Network User Identifier.	Optional DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF2C TAG DF30 TAG DF34
Version Specifications		Allowed values: CB1 CB2
Data for Special GSM, GPRS e TCP/IP Connectivity (**)		
Remote Data Management (only if the connection type is remote management)		
Tlg Start Date Tlg End Date Num. of Attempts Delay (*)	Remote data management mode.	REMOTE DATA MANAGEMENT section See doc. Ref. [1] field 72 TAG FF08 DF36
Message for Merchant (*)	Message addressed to the merchant used to inform about the TLG activity programmed on the terminal.	REMOTE DATA CONNECTION section See doc. Ref. [1] field 72 TAG FF08 DF37
<p>(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.</p> <p>(**) They are not documented in the Bancomat Spa specifications, if the POS provides for its implementation; they are to be determined on the basis of bilateral agreements with the POS supplier.</p>		

8.3.1.2 POS CB2 Specifics Version

FIELD	DESCRIPTION	NOTES
Connection		
Code	Unique identifier of private FTFS generated with a sequence and used as key from the records that point to the connection.	
Service Type	Specifies the use of the profile.	Values permitted: GT connection Telemanagement connection
Description	Name and description of the application.	
Connection Type NET Type Speed (*)	Connection type and speed.	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2A
Telephone (*)	GT access phone number.	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2B
NUI (*)	NUI	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2B
NUA (*)	NUA	DATA CONNECTION section See doc. Ref. [1] field 72 TAG DF2D
Data for Special GPRS e TCP/IP Connection		
Protocol Type (*)	Protocol Type (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF53
Transport Protocol (*)	Transport Protocol (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF53
PPP Timeout (*)	Issue of Context (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF53
User ID (*)	PPP authentication parameter (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF54

FIELD	DESCRIPTION	NOTES
Password (*)	PPP authentication parameter (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF54
Authentication Type (*)	PPP authentication parameter (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF54
APN Name (*)	Apn name (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF55
IP Address (*)	IP parameters (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF56
Port (*)	IP parameters (special connections).	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG DF56
Telemanagement Data (only if the connection type and management)		
TLG Start Date	Telemanagement mode.	DATA TELEMANAGEMENT Section See doc. Ref. [1] field 72 TAG FF08 DF36
TLG End Date		
Num. of Trials		
Delay (*)		
Message for Merchant (*)	Message addressed to the merchant used to inform about the TLG activity programmed on the terminal	DATA CONNECTION Section See doc. Ref. [1] field 72 TAG FF08 DF37
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly		

Note For more information about the technical parameters see doc. "ref [1] - Field 72 TECHNICAL PARAMETERS".

If the profile of connections is relative to Telemanagement, all the data of the corresponding section must be given.

The reference to "remote management connection" in the TERMINAL detail is deleted automatically once conferred in the DLL to the POS, to avoid duplication of costly remote management on the POS.

8.3.1.3 *Table: Usage Statistics*

Table relative to the details of the fields on the page:

Connectivity Statistics.

In the first part of the page the data connection that vary depending on whether the connection follows the specific POS/NCR version is shown, and whose fields have been described in the previous paragraph. In the second part the use of the connection compared to the terminals configured is reported.

FIELD	DESCRIPTION	NOTES
GT 1.2 Connection Attempt	Indicates the number of terminals that have used the connection.	Tested for use in: Connection to the GT for 1st and 2nd attempt.
GT 3 Connection Attempt	Indicates the number of terminals that have used the connection.	Tested for use in: Connection to the GT for 3rd attempt.
Remote Data Management	Indicates the number of terminals that have used the connection.	Tested for use in: Connection to the remote data management center.

Note Displaying the connection usage statistics may be useful in case one needs to delete a connection profile in favor of another one, to check if all terminals have been updated.

8.4 Technical Profiles

The applicative technical parameters of the terminals that have been certified on a Service Center/GT may be the same as all the terminals or differentiated, are defined on each terminal but are described in specific table to which the profiles of the terminal recall it. In the minimal case then, the table of the Technical Profiles contains only one record.

Pages relative to the TECHNICAL PROFILES function allow to define and to operate on profiles of **general technical applicative parameters** of the terminals, as in response waiting time and enabled functionalities.

In the navigation bar of the page the following button is present:

New Record

new technical profile definition.

The pages relative to the TECHNICAL PROFILE function display and manage:

- *the list of technical profiles defined (list)*
- *the detail of each technical profile and eventually to modify the configuration data*
- *remove a defined profile.*

Table relative to the detail of the fields of the following pages:

Technical Profiles

Technical Profile Detail

FIELD	DESCRIPTION	NOTES
ID	Profile ID.	
Description	Description of the profile string.	
Carrier Wait 1/2 Attempt Response Wait 1/2 Attempt: Carrier Wait 3 Attempt Response Wait 3 Attempt (*)	Time out applications in seconds used by the terminals that use the profile.	TERMINAL TIME-OUT Section See doc. Ref. [1] field 72 TAG DF29
Enabled Functions (*)	Allows you to enable the functions to the terminals that use it.	ENABLE section See doc. ref. [1] field 72 TAG DF23

(*)Data provided to the POS terminal in the DLL. The modification of these data produces a **DLL reminder** to all terminals that use them directly or indirectly

8.5 Banks

When it comes to the FTFS behavior relative to the Debit cards, we remind you of the following fundamental points:

- *FTFS is a multibank product: a Service Center can manage terminals related to more banks and every bank can behave in a different way.*
- *The service center can have the deposit cards of a bank: in this case, the terminals of that bank's property, for the same bank, obtain the authorization on the same service center.*
- *If the service center does not manage a deposit and even in the case it does manage it, it will normally have an applicative default center for the circularization relative to the "not on us" cards. This default may not be the same for all the banks managed.*
- *To determine the behavior relative to the Debit card functions, two parameters are set it: The ABI of the bank owner of the terminal and the ABI of the bank issuing the card that is paying, in other words, the first 5 characters of the card.*

Crossing the ABI of the card and terminal, the Acquirer relative to that card is determined. The function of finding the Acquirer for the sending of the transaction is called "**routing**".

To avoid the multiple definitions of the pairings, it is possible to create groups of ABI, called "consortium", to join and subject the same behavior to both the banks that own the terminals as well as those of the cards.

In the navigation bar of the page the following button is present:

New Record

new bank definition.

The pages relative to the BANKS function allow to display and manage:

- *the list of banks defined (list)*
- *the detail of a bank and eventually the modification of the configuration data*
- *the removal of a defined bank.*

Table relative to the details of the fields of the following pages:

Banks

Bank detail

FIELD	DESCRIPTION	NOTES
ABI	Unique code of the bank	
CIN	Unique code of the bank supplementary to the ABI	
Financial Institution	Bank name	
Applicative Center	Applicative Centre for PB	
Unique ABI	Value of the ABI used in the configuration of “ABIUNICO” (example, 08000)	

8.6 Routing

See previous chapter for the definition of ROUTING.

In the navigation bar of the page the following button is present:

New Record

new Routing record definition

The pages relative to the ROUTING function allow to display and manage:

- *the list of routing definitions for Credit Card Transaction and for Debit Card Transactions (list)*
- *the detail of a routing and eventually the modification of the configuration data*
- *the removal of a defined routing.*

Table relative to the details of the fields of the following pages:

Debit Card Routing Detail

Credit Card Routing Detail

Debit Card Routing

Credit Card Routing

FIELD	DESCRIPTION	NOTES
BIN	BIN cards.	
Priority	Has a range from 0 to 9 where 9 is the lowest priority.	
Increase priority	Increases the priority.	
Acquirer	Unique Mnemonic code to identify the Acquirer in the system.	
Transaction Type	Values: ALL With PIN Without PIN	
Reason	Free string.	

8.7 CA Keys

The CA keys are issuer keys used for chip cards authentication, both static and dynamic.

In the navigation bar of the page the following button is present:

Manual loading

loads the key enabling the insertion of the module and hash of the key as strings

File loading

*loads the key reading the file *.HEP and *.SEP that are sent by the Certificate Authority.*

The pages relative to the CA keys allow to display and manage:

- *the list of Certificate Authority keys (list)*
- *the detail of keys and eventually the modification of the module*
- *the removal of a key.*

FIELD	DESCRIPTION	NOTES
RID	CA Key Identifier.	Corresponds to the first 10 hexadecimal characters of the AID data. See doc. ref. [1] field 59 TAG DF43
Key Index	Hexadecimal value.	CA Key Identifier.
Status	Indicates whether it is on or off.	
Start Date	Date of activation of the key.	
Expiry Date	Expiration date of the key.	
Check Sum	Check sum value of the key.	
Module	Module of the key.	

8.7.1 Table: Manual Load

Table relative to the detail of the fields of the page:

Manual Load.

FIELD	DESCRIPTION	NOTES
RID	CA Key Identifier.	Corresponds to the first 10 hexadecimal characters of the given AID See doc. ref. [1] field 59 TAG DF43
Key Index	Hexadecimal value of the index key	
Hash Algorithm	Values 01 - sha-1 (default)	
Key Algorithm	Values 01 - rsa (default)	
Length Module (Hex)	Hexadecimal length of the length of the key module	
Exponent Length	Values 01 (default)	
Exponent	Values 03 (default)	
Hash	Hash of the key.	
Expiry Date	Expiration date of the key	
Module	Module of the key.	

8.7.2 Table: Load from File

Table relative to the detail of the fields of the page:

Load From File.

FIELD	DESCRIPTION	NOTES
Inserting File.SEP	File sent by the CA.	
Inserting File.HEP	File sent by the CA	

8.8 CB2 Keys – certificates

In the navigation bar of the page the following buttons are present:

GT keys - GT Certificates

Lists the keys and GT certificates.

RSA-BANCOMAT Keys

Lists the RSA public keys of the BANCOMAT SPA.

RSA-POS Keys

Lists the public key of the POS providers sent by the POS used for the mutual CB2 authentication.

KMP Keys

Lists the KMP keys.

POS Keys

Lists the public RSA of the POS used for the mutual CB2 authentication and for the transport of the DES track keys.

The pages relative to the various functions allow to view and manage:

- *the list of keys/certificates (list)*
- *the detail of keys and eventually the modification of the module*
- *the removal of a key.*

8.8.1 Table: CB2 Key Detail

Table: RSA-BANCOMAT Key Detail

Table: RSA-POS Key Detail

Table: POS Key Detail

The pages relative to the CB2 Keys function allows to view and manage:

- *The list of CB2 keys (list)*
- *the detail of CB2 keys and eventually the modification of the configuration data.*

FIELD	DESCRIPTION	NOTES
ID	Unique identifier of the key.	
Name	Name of the key.	
Status	Indicates whether it is on or off.	
INS/MOD Operator	Name of the operator that made the entry or modification	
Start Date of Validity	Date and time of key validity	
End Date of Validity	Date and time of key expiration	
Description	Of mnemonic use.	
Type	Allowed values: CA GT FOR POS	CA =Certificate Authority GT =Terminals Manager FOR =POS Supplier POS =Terminal
CA Key Index	Index key.	Valued only for keys of CA type
Public Key Module Length	Public key module length.	
Public Key Module	Complete module of the public key.	
Public Key Exponent Length	Public key exponent length	
Public Key Exponent	Public Key Exponent.	
Hash Key	Hash key.	
Secret Key	Encryption of the secret key value returned by the 'HSM.	Valued only for keys of type GT
Import CA Certificate	Certificate number assigned by the CA.	
Self Certified	Certificate number assigned by the GT.	
Hash Algorithm	01 = Sha1	

8.8.2 Table: Certificate Detail

The pages relative to the Certificate function allow to view and manage:

- *The list of certificates (list)*
- *The detail of the certificates*

FIELD	DESCRIPTION	NOTES
Name	Name of certificate	SC_ + certified key name
Status	Indicates whether it is active or inactive.	
Input Date	Date and time of creation of the certificate.	
Ins/Mod User	Name of the operator who made the entry or modification.	
Validity Start Date	Date and time of certificate validity	
Validity End Date	Date and time of certificate expiration	
ID	Certificate Number assigned by the GT (unique)	
Description	Free text of mnemonic use	
Format	Type of EMV certificate	0B = GT
Subject Code	Identification code of the GT	
Expiry Date (mm-yy)	Expiration date of the certificate established by CA	
Hash Algorithm	01 = Sha1	
Public Key Certificate	Public key certificate provided by the CA	
Public Key Algorithm	01 = RSA	
Public Key Exponent		

FIELD	DESCRIPTION	NOTES
Public Key Module	Part of the module of the public key contained in the certificate	The two fields together constitute the module of the public key
Public Key Remainder	Part of the module of the public key not inserted in the certificate	
Hash Public Key	Hash of the certificate	

8.8.3 List of Requested Keys

This list shows the requests processed or to be processed by form of the KeyManager process (list).

FIELD	DESCRIPTION	NOTES
Request Date		
Method	Function requested	
Name	Name of the key	
Certificate Length/Name	Contains the length of the RSA key if it is the key or the name of the certificate if it is the certificate	Present only in the GT Keys List and GT Certificates
Description		Present only in the GT Keys List and GT Certificates
GT Code	Operator GT Code	Present only in the GT Keys List and GT Certificates
Num. Certificate		Present only in the GT Keys List and GT Certificates
Status	Status of the request	
Result	Outcome of the operation	
1st Operation	Name of the first operator	The creation of the keys must be requested by 2 operators, the first operator creates the request, and the second one operator must confirm it
Actions	Button with the action to be taken	Example: confirmation or execute

8.8.4 Table: KMP Keys List

The pages related to the KMP Keys function (Master Key TDES 128 bit long, used to derive the K_{IP} key) allow to view the list of the KMP keys (list).

FIELD	DESCRIPTION	NOTES
Acquirer	Acquirer of reference	
Description	Description	
KMP	Cryptogram of the key	
KMP Check Value	Check value	
Modification Date	Date and time of modification of the key.	

9 Merch/Store/Term

In order to give flexibility to the definition of Terminals, a tiered structure has been adopted: at the root of the definition of all the terminals there is the Merchants table. **Each terminal derives** (indirectly) **from a Merchant record, is associated with a single Point of Sale** (from which it directly derives).

A Merchant with more Stores and with many Terminals is defined only once; at each Store (example: shop), relative to the Merchant, there may be more than one Terminals associated.

The MERCHANT/TERMINAL allows, as a whole, to view and manage:

- *The personal data and enabling of a Merchant (insertion/modification)*
- *the data and enabling of the related elements (Insertion/modification and in some cases cancellation) in the following order:*
 1. *Stores*
 2. *Terminals*
 3. *Conventions for Terminal*
 4. *EMV Application Enabling for the Terminal convention.*

9.1 New Merchant

The pages relative to NEW MERCHANT function allow to:

insert configuration data of a new Merchant and his first Store.

FIELD	DESCRIPTION	NOTES
Merchant		
Currency (*)	Code of the currency used by the country for the year (shown in the NATION).	ISO Encoding. See doc. ref. [1] field 72 TAG 5F2A
Country (*)	Nation code/Country of the shop.	ISO Encoding. See doc. ref. [1] field 72 TAG 9F1A
Company Name	Company name of the Merchant.	The name used as a search key in the function SEARCH MERCHANTS (at

FIELD	DESCRIPTION	NOTES
		least the first 3 characters to search by partial name).
Merchant Code	Unique and private Merchant Code of FTFS.	
Store		
Type	Traditional operator or barrier tills.	
Store Banner	Banner	
Store Code	SIA Code of the store	
Address	Address	
City	City name	
Province	Province	
Zip Code	ZIP code	
Telephone Telephone 2	Phone numbers of point of sales or of the contact person at the point of sale.	
Contact Name	Contact name of the person of reference at the Store.	
Sort Code or IBAN	Banking Sort code	
VAT Code	VAT code	Must be present for the hotels/ car rentals pre-authorization function
F3	Field for private use.	
Store Operation		
Status	Enabled or Disabled	In the case of disabled state purchase transactions are denied
HOST Code	HOST proprietary bank of POS	

FIELD	DESCRIPTION	NOTES
Merchandise Category (*)		Section: Off-line Operation (Point of Sale). See doc. ref. [1] field 72 TAG 9F15
Offline Operations		
Download Log Enabling (*)	Flag of enabled manual log download	Section Off-line: Operation (Point of Sale). See doc. ref. [1] field 72 TAG DF28
Max Number TR Offline in Memory (*)	Maximum number of offline transactions in memory.	Section: Off-line Operation (Point of Sale). See doc. ref. [1] field 72 TAG DF28
Automatic Session Logout Time (*)	Automatic session closing time.	Section: Off-line Operation (Point of Sale). See doc. ref. [1] field 72 TAG DF28
Data for Receipt		
Receipt Header	Header lines of the receipt that the terminal prints for each transaction.	Section: Data for receipt
Receipt Line 1		Required information
Receipt Line 2		See doc. ref. [1] field 72 TAG FF04
Receipt Footer		
(*)		
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.		

9.2 Merch/Store/Term Search

The pages relative to the MERCHANT SEARCH function allow, as a whole, to view and manage:

- *The list of defined Merchants (list)*
- *The list Stores defined for a Merchant (List).*
- *The list of Terminals defined for each Store (list)*
- *The configuration data (detail) of a Merchant (editing)*

- *The configuration data (detail) of a Store (insertion/editing)*
- *The configuration data of a Terminal (insertion/editing)*
- *Cloning a Terminal belonging to a Store, creating this last additional terminal without having to repeat the data definitions of the new POS.*

The merchant search can be done for:

Merchant Search

Performs the search and visualization of a Merchant and his Points of Sales (stores).

Stores Search

Performs the search and visualization of a Point of Sale (stores) and its Terminals.

Terminals Search

Performs the search and visualization of the detail of a POS and its Conventions.

9.2.1 Merchants List

The first possibility of the MERCHANT SEARCH function enables the search between the registered merchant, through the input of the company name (or part of it) or the SIA Merchant Code. The outcome will show the list of defined Merchants that satisfy the search criteria. From this page, by pushing the corresponding **Link** it is possible to access:

Merchant detail, view and eventually edit the data, including the Points of Sale connected to it.

Note The Deletion of a MERCHANT is possible only if all its Points of Sale and Terminals have been previously deleted.

On the navigation bar in the page of MERCHANT DETAIL function, the following button is present:

New Store

Definition of a new Store, for information in regards to the fields of these functions, please see POS DETAIL table that follows

9.2.1.1 Table: Merchant Detail

Table relative to the detail of the fields of the page:

Merchant Detail

FIELD	DESCRIPTION	NOTES
Currency (*)	Code of the currency used by the country for the year (shown in the NATION).	ISO Encoding. See doc. Ref. [1] field 72 TAG 5F2A
Country (*)	Nation code/Country of the shop.	ISO Encoding. See doc. Ref. [1] field 72 TAG 9F1A
Company Name	Company name of the Merchant.	The name used as a search key in the function SEARCH MERCHANTS (at least the first 3 characters to search by partial name).
Merchant Code	Unique and private Merchant Code of FTFS.	
Operativity	Valori: ENABLED DISABLED	
Payment Facilitator ID	Payment Facilitator Management	
Payment Facilitator Sender	Payment Facilitator Management	

(*)Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.

9.2.2 Merchant Point of Sale

Under the definition of a Merchant exists at least one Point of Sale. Each terminal derives directly by a Point of Sale. A Point of Sale with many terminals is defined only once.

The function allows to view the list of Point of Sales already configured (relative to the merchant selected previously) and to access the functions that manage them (view/entry/editing/deletion).

From this page, pushing one of the corresponding **Links**, it is possible to access to:

- *Point of Sale detail, viewing and eventually modifying data, including the Terminals.*
- *Deletion of a Point of Sale.*

Note Deletion of a POINT of SALE is possible only if all its Terminals have previously been deleted.

On the navigation bar in the page of POINT-OF-SALE DETAIL function, the following button is present:

New Standard Terminal

*Definition of a new Terminal, for information regarding the fields of such functions see the following **TERMINAL DETAILS** table. (??)*

New Operative Terminal

*Definition of a new Terminal, for information regarding the fields of such functions see the following **TERMINAL DETAILS** table. (??)*

New Virtual Terminal

*Definition of a new Virtual Terminal present only for points of sales of **Barrier Class** type, for information regarding the fields of such functions see the following **TERMINAL DETAILS** table. (??)*

9.2.2.1 *Table: Point of Sale*

Contains the Point-of-Sale registration data and some technical parameters shared between all POS assigned during the DLL phase.

Note Modification of data present in the point-of-sale detail produces a DLL reminder to all terminals belonging to the edited Point of Sale. This is necessary because some data of the Point of Sale anyhow represent some “technical parameters” for the terminals (Ex. Merchandise category, receipt data, log download, etc.).

Table relative to the detail of the fields in the following pages:

Point of Sale Detail New Point of Sale

FIELD	DESCRIPTION	NOTES
Point of Sale		
Type	Traditional or Barrier Registers	
Store Banner	Banner	
Codice Stabilimento SIA	SIA code of the store	
Address	Address	
City	City	
Province	Province	
ZIP Code	Zip Code	
Telephone Telephone 2	Phone numbers of point of sales or of the contact person at the point of sale.	
Reference Name	Contact name of the person of reference at the Store.	
Sort Code or IBAN	Banking Sort code	
VAT Code	VAT code	
F3	Field for private use.	

FIELD	DESCRIPTION	NOTES
Point of Sale Operativity		
Status	Enabled or Disabled	
HOST Code	HOST proprietary bank of POS	
Merchandise Category (*)		Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG 9F15
Offline Operativity		
Download LOG Enabling (*)	Flag of enabled manual log download	Section Off-line: Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Max Number TR Offline in Memory (*)	Maximum number of offline transactions in memory.	Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Automatic Session Logout Time (*)	Automatic session closing time.	Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Data for Receipt		
Receipt Header Receipt Line 1 Receipt Line 2 Receipt Footer (*)	Header lines of the receipt that the terminal prints for each transaction.	Section: Data for receipt Required information See doc. Ref. [1] field 72 TAG FF04
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly.		

9.2.3 Terminal List

The function allows to view the list of Terminals already configured (relative to the Point of Sale previously selected) and to access the functions that manage (view/insert/edit/delete) the personal data and of Terminal configuration.

From this page, pushing one of the corresponding **Links**, it is possible to access to:

- *Terminal detail, to display and eventually modify the data.*
- *List of transactions of the corresponding Terminal*
- *Removal of a Terminal.*

9.2.3.1 Table: Terminal Detail

The data relative to a POS Terminal can be subdivided in the following sections:

- *Summary data of the POINT OF SALE and MERCHANT belonging to the terminal.*
- *Operation summary data: REMINDER TO THE DLL for the terminal.*
- *Terminal configuration data mandatory and optional that, for omission, are inherited by the Point of Sale.*
- *ACQUIRER AGREEMENT (table at the bottom of the detail page).*
- *CB2 Data, if the Terminals are CB2.*

Besides the summary data, it is possible to operate on the configurations with entry/edit/deletion function.

From this page, pushing one of the corresponding **Links**, it is possible to access to:

- *Acquirer Agreement Detail.*
- *Deletion of Agreement.*

Note Between the TERMINAL data, there is a section of optional data.
The value of the optional fields of the Terminal, **if omitted**, is inherited from the ones specified in the Point of Sale.

On the navigation bar in the terminal detail page, the following buttons are present:

DLL Characteristics

Viewing of the information that identify the characteristics of the POS Terminal, given by the same terminal to the GT during the DLL procedure

Terminal Totals

Viewing of the current amounts.

Total List

Allows to search and view the list of the total transactions of the Terminal selected by changing the search date or the hour range.

New Agreement

Definition of a new acquirer agreement, for information regarding the fields of such functions, see table "Agreement Detail" below.

New Cashier

Creation of a new terminal for the Point of Sale, as identical copy of the terminal to which the detail is being viewed for, besides the TERMINAL CODE (to insert) that is always unique for FTFS.

Table relative to the detail of the fields of the pages:

- *Terminal Detail*
- *New Standard Terminal*
- *New Virtual Detail*
- *New Operative Terminal*

FIELD	DESCRIPTION	NOTES
Merchant Data		
Company Name	Company name.	The name used as a search key in the SEARCH MERCHANTS function (at least the first 3 characters to search by partial name).
Currency (*)	Code of the currency used by the country of the store (shown in the NATION field).	ISO encoding. See doc. Ref. [1] field 72 TAG 5F2A
Country (*)	Nation code/Country for the year.	ISO encoding. See doc. Ref. [1] field 72 TAG 9F1A
Merchant SIA Code	Unique Merchant Code, private of FTFS	
POS Data		
Register Type	Traditional or Barrier Registers	
POS Banner	Banner of the store	
Establishment SIA Code	SIA Establishment code	
Telephone Telephone 2	Phone numbers of point of sale or contact person at the point of sale.	
Contact Name	Contact name of person at the Point of Sale.	
Max Number TR Offline in Memory (*)	Maximum number of offline transactions in memory.	Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Automatic Session Logout Time (*)	Automatic session closing time.	Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Download LOG Enabling (*)	Flag of enabled manual log download	Section Off-line: Operation (Point of Sale). See doc. Ref. [1] field 72 TAG DF28
Merchandise Category (*)		Section: Off-line Operation (Point of Sale). See doc. Ref. [1] field 72 TAG 9F15

FIELD	DESCRIPTION	NOTES
ABI		
Receipt Header	Header lines of the receipt that the terminal prints for each transaction.	Section: Data for receipt
Receipt Line 1		Required information
Receipt Line 2		See doc. Ref. [1] field 72 TAG FF04
Receipt Footer		
(*)		
Terminal Data		
Terminal Code (*)	Code assigned by the acquirer for the agreement.	Agreement Table.
SIA Register Code	Register code value	
Technical Parameters	Reference to technical parameters table records associated to the terminal	
GT 1 and 2 Connection GT 3 Connection Tele Management (*)	Choice of one of the profiles for connections: 1st and 2nd attempt 3rd attempt Tele management.	
Acquirer (*)	Acquirer of the agreement	Agreement Table
Offline Off Line Operations	Flag of off line operations	See doc. Ref. [1] field 48 TAG DF22
Merchant Code Terminal Code (*)	Codes assigned by the acquirer for the agreement.	Agreement table.
Agreement (*)	Description of the acquirer's agreement.	Agreement table.

FIELD	DESCRIPTION	NOTES
Date Last Operation	Date of the last online transaction.	
Date Last DLL	Date of last DLL transaction.	
Oper Number	Identification of on-line operation received from the POS	
Technical Parameters (*)	Choice of one of the technical profiles configured on the FTFS system .	See par. "Technical Profiles"
Terminal Code (*)	Code assigned by the acquirer for the agreement.	Agreement Table.
Term ID	Terminal Code	Unique for FTFS
Optional Terminal Data		
ABI	ABI of the owning Terminal's bank	
Merchandise Category (*)	Identifies the merchandise category of the merchant on which the POS is installed. If the data is not present, the one of the Point of Sale is valid.	Section: "Optional Terminal Data" See doc. Ref. [1] field 72 TAG 9F15
Receipt Header	Header lines of the receipt that the terminal prints for each transaction.	Section: "Data for Receipt" Required information See doc. Ref. [1] field 72 TAG FF04
Receipt Line 1		
Receipt Line 2		
Receipt Footer		
(*)		
Payment Facilitator Submerchant Code	Payment Facilitator Management.	Build byMerchant+Store+Register
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly		

9.2.3.1.1 Table: DLL Characteristics

Table relative to the detail of the fields of the page:

Terminal Characteristics

The data are originated from the POS in the DLL and are not modifiable.

FIELD	DESCRIPTION	NOTES
Terminal Data		
Terminal ID	Terminal code.	Unique to FTFS.
Serial Number	Terminal Serial Number.	From POS, msg 1846, field 47, tag DF32
Term Model	Terminal model.	From POS, msg 1846, field 47, tag DF01
Pin Pad Model	Pin pad model.	From POS, msg 1846, field 47, tag DF02
Term Type	Terminal Type.	From POS, msg 1846, field 47, tag 9F35
Terminal Capabilities	Terminal Capabilities.	From POS, msg 1846, field 47, tag 9F33
Additional Term Capabilities	Additional Terminal Capabilities.	From POS, msg 1846, field 47, tag 9F40
Functions Managed	Bit map terminal features.	From POS, msg 1846, field 47, tag DF0B
Last DLL Date	Last DLL date.	
Terminal Software		
Code of Basic Software Release	Release basic terminal software.	From POS, msg 1846, field 47, tag FF0B, subtag DF03

FIELD	DESCRIPTION	NOTES
Base Check Sum	Check sum release of basic terminal software.	From POS, msg 1846, field 47 , tag FF0B, subtag DF04
Release Code of Applicative Software	Applicative terminal software release.	From POS, msg 1846, field 47 , tag FF01, subtag DF05
Check Sum Applicative Software	Checksum release software applicative terminal.	From POS, msg 1846, field 47 , tag FF01, subtag DF06
Pin Pad Software		
Code of Basic Software Release	Pin Pad base release code software.	From POS, msg 1846, field 47 , tag FF02, subtag DF07
Base Check Sum	Pin Pad base Check sum release software.	From POS, msg 1846, field 47 , tag FF02, subtag DF08
App Pin Pad Release	Pin Pad applicative release code software.	From POS, msg 1846, field 47 , tag FF03, subtag DF09
Check Sum App Software	Checksum release applicative Pin Pad software.	From POS, msg 1846, field 47 , tag FF03, sub tag DF0A

9.2.3.1.2 Table: New Register

Table relative to the detail of the fields on the page:

Terminal Clone

FIELD	DESCRIPTION	NOTES
Register Code Automatic Numerical Progression		
Last Register Code	Last register code of the point of sale	
New Terminal Data		
New Terminal Code	TERMINAL ID to create	
Number of Terminals	Number of new terminals that you want to clone from the current one.	
Do you want to clone all accreditations?	Indicates whether to copy the accreditations present on the starting terminal on the cloned ones	
Do you want to increase terminal code?	Indicates if the start up terminal code or the new one must be kept as TERM field in the agreement.	Note: In some cases, more point of sale terminals are present on the interbank with the same terminal code.

9.2.3.2 Table: Agreement Detail

The link between an Acquirer that must be managed by a Terminal and the Terminal itself is represented by defining a record of *Agreement Detail*.

The data relative to the Agreement may be split in the following sections:

- **ACQUIRER DATA** *summarized, viewed to supply a significant reference.*
- **PERSONALIZED ACQUIRER DATA** *for the Terminal, for which an omission, the ones predefined in the Acquirer Data section will be used.*
- **DATA OF AGREEMENT ASSIGNED BY THE ACQUIRER.**

If the Acquirer of the agreement manages EMV applications, at the bottom of the detail page, you will find a **list of EMV applications** and the relative state of enabling or not in respect to the Terminal. For example, if an Acquirer possesses 3 EMV applications, for the agreement of a terminal, you may choose to enable only one application.

At the time of activation, the user must choose a technical profile of the application, between the ones defined in the EMV applications, *see par. "Acquirers"*.

On the navigation bar in the terminal detail page, the following buttons are present:

Associate EMV Application

Allows to associate or not, to the agreement, the EMV applications defined on Acquirer level.

NCR Data

In case the Terminal follows the NCR standards

POS CB2 Data

In case the Terminal follows the CB2 standards

Routing Management

Manages a specific routing for a particular agreement.

Table relative to the detail of the fields of the pages:

Agreement Detail

New Agreement

Agreement List

FIELD	DESCRIPTION	NOTES
Terminal Code	POS Terminal code	
Acquirer Data		
Acquirer	FTFS ACQUIRER code (ACID)	
Acquirer ID	Acquirer ID.	
Magstripe Transaction Management		
Tel Voice-Contact	Number for the phone call to the vocal Authorization Center.	Present for Acquirers that handle transactions stripe in track 2. See doc. Ref. [1] field 72 TAG DF3F

FIELD	DESCRIPTION	NOTES
Microcircuit Transaction Management		
DDAOL (*)	Represents the list of default data for the terminal necessary for dynamic authentication data.	Present for acquirers that handle EMV payment cards. See doc. Ref. [1] field 72 TAG 9F49
TCDOL (*)	Represents the list of default data in the terminal necessary for the calculation of the TC Hash Value if this is required in CDOL.	Optional. Present for a Acquirers that handle EMV payment. See doc. Ref. [1] field 72 TAG 97
Offline Operation		
Automatic Offline Message (*)	Contains the message of authorization for transactions authorized in <i>off-line</i> that the terminal views to <i>display</i> and prints on the receipt.	For Acquirers that handle transactions for magnetic stripe and microcircuit. See doc. Ref. [1] field 72 TAG DF3E
Max Range Offline Auth Min Range Offline Auth (*)	Two subfields of 6 numeric characters each, which define a numeric range within which the terminal calculates a <i>random</i> number which is the authorization code for the transactions carried out with magnetic stripe cards and microcircuit approved off-line.	Present for Acquirer that handle transactions for mag stripe in track 2 and microcircuit transactions. See doc. Ref. [1] field 72 TAG DF3D
Personalized Agreement		
Agreement Description	Agreement name.	
Magstripe Transaction Management		
Tel Voice-Contact (**)	Number for the phone call to the Vocal Authorization Center.	Present for Acquirers that handle stripe transactions in track 2. See doc. Ref. [1] field 72 TAG DF3F
Microcircuit Transactions Management		
DDAOL (*)	Represents the list of default data for the terminal necessary for dynamic authentication data.	Present for acquirers that handle EMV payment cards. See doc. Ref. [1] field 72 TAG 9F49
TCDOL (*)	Represents the list of default data in the terminal necessary for the calculation of the TC Hash Value if this is required in CDOL.	Optional. Present for a Acquirers that handle EMV payment. See doc. Ref. [1] field 72 TAG 97
Offline Operation		

FIELD	DESCRIPTION	NOTES
Automatic Offline Message (*)(**)	Contains the message of authorization for transactions authorized in <i>off-line</i> that the terminal views to <i>display</i> and prints on the receipt.	Acquirer that handle transactions for magnetic stripe and chip. See doc. Ref. [1] field 72 TAG DF3E
Max Range Aut Offl Min Range Aut Offl (*)(**)	Two subfields of 6 numeric characters each, which define a numeric range within which the terminal calculates a <i>random</i> number which is the authorization code for the transactions carried out with magnetic stripe cards and microcircuit approved off-line.	Acquirer that handle transactions for this magstripe in2 track and chip transactions. See doc. Ref. [1] field 72 TAG DF3D
Agreement Assigned by the Acquirer		
Merchant Code(*)	Agreement Merchant code.	Assigned by the Acquirer/Company. See doc. Ref. [1] field 72 TAG 9F16
Terminal Code (*)	POS terminal agreement code.	Assigned by the acquirer/Company.
(*) Data provided to the POS terminal in the DLL. The modification of these data produces a DLL reminder to all terminals that use them directly or indirectly		
(**) If filled in it will replace the parameter inherited by the acquirer.		

9.2.3.2.1 Table: EMV Application List

Shows the applications associated with this agreement.

FIELD	DESCRIPTION	NOTES
ID	Service ID – significant only for cb2 pos.	See doc. Ref. [1] field 72 TAG FF09 DF6A
Service Name(*)	Service name – significant only for cb2 pos.	See doc. Ref. [1] field 72 TAG FF09 DF49
Description	Name/Description of the Application available for the AID Acquirer application.	
AID (*)	AID application	See doc. Ref. [1] field 72 TAG FF09 9F06

FIELD	DESCRIPTION	NOTES
		See doc. Ref. [1] field 72 TAG 9F06

(*) Data provided to the POS terminal in the DLL. The modification of these data produces a **DLL reminder** to all terminals that use them directly or indirectly

9.2.3.2.2 Table: Alternative Routing Management

Address the alternative routing for the current accreditation for the present terminal.

FIELD	DESCRIPTION	NOTES
Acquirer	FTFS Acquirer code for routing transaction.	
Merchant Code (*)	Agreement merchant code.	Assigned by the acquirer/Company.
Terminal Code (*)	Agreement POS terminal code.	Assigned by the acquirer/Company.

(*) Data used for sending transactions on the interbank it. The change does not trigger the DLL parameters at the POS

9.2.3.2.3 Table: EMV Application Association

Table relative to the detail of the fields of the page:

EMV Application Association

FIELD	DESCRIPTION	NOTES
Active	To activate the application	
Acquirer	FTFS acid	
Application	EMV application	
Service ID	Service ID - significant only for cb2	
Service Name	Service Name - significant only for cb2	
AID	AID associated with the application	
Profile	Application Profile	The detail of the profile is viewable from the Acquirer menu.

9.2.3.2.4 Table: NCR Data

Table relative to the detail of the fields of the page:

NCR detail

FIELD	DESCRIPTION	NOTES
Acquirer Data		
Acquirer	FTFS Acquirer code	
Description	Description	
Receipt Data		

FIELD	DESCRIPTION	NOTES
Courtesy Message	Courtesy message	field 72- tag DF40 Is the data present on the Acquirer
Magstripe Transactions Management		
Floor Limit 1	Floor limit 1 (for magnetic stripe)	field 72- tag DF3B Is the data present on the Acquirer
Random Selection	Random selection (for magnetic stripe)	field 72- tag DF48 Is the data present on the Acquirer
Enabled Ranges	Acquirer rank.	field 72- tag DF39 Is the data present on the Acquirer
Enabled Functions		
Enabled Functions	Bitmap features enabled	field 72- tag DF3A Is the data present on the Acquirer
Agreement Personalization		
DS Agreement	Agreement description	
Data for Receipt		
Courtesy Message	Courtesy message personalization for this agreement.	To be enhanced in different than the value in the general table Acquirer; if present it will be conferred in the DLL
Magstripe TRX Management		
Floor Limit 1	Personalization value for this convention.	To be enhanced in different than the value in the general table Acquirer; if present it will be conferred in the DLL
Random Selection	Personalization value for this convention.	To be enhanced in different than the value in the general table Acquirer; if present it will be conferred in the DLL
Enabled Range	Personalization value for this convention.	To be enhanced in different than the value in the general table Acquirer; if present it will be conferred in the DLL

FIELD	DESCRIPTION	NOTES
Enabled Funcions		
Enabled Funcions	Personalization values for this convention.	To be enhanced in different than the value in the general table Acquirer; if present it will be conferred in the DLL

9.2.3.2.5 Table: CB2 Data

Table relative to the detail of the fields of the page:

CB2 detail

FIELD	DESCRIPTION	NOTES
Receipt Data		
First Line (*)	Acquirer receipt first line, Required	See doc. Ref. [1] field 72 TAG FF04 DF24
Second Line (*)	Acquirer receipt second line, Required	See doc. Ref. [1] field 72 TAG FF04 DF25
Header (*)	Acquirer receipt header, optional.	See doc. Ref. [1] field 72 TAG FF04 DF26
Closing (*)	Acquirer receipt closing, Optional.	See doc. Ref. [1] field 72 TAG FF04 DF27
Third Line (*)	Third line Acquirer receipt, Optional.	See doc. Ref. [1] field 72 TAG FF04 DF50
Positive Outcome Message (*)	Printed message on the receipt in regards to a positive outcome, Required.	See doc. Ref. [1] field 72 TAG FF04 DF51
Negative Outcome Message (*)	Printed message on receipt in regards to a negative outcome, Required.	See doc. Ref. [1] field 72 TAG FF04 DF52
Fourth Line (*)	Fourth line Acquirer receipt, Optional.	See doc. Ref. [1] field 72 TAG FF04 DF6B

FIELD	DESCRIPTION	NOTES
Optional Functional Data		
Tip Percentage (*)	Determines the maximum acceptable from the POS to the tip with respect to the amount of the transaction. Values from 00-99 If not valued assume it to be 00.	See doc. Ref. [1] field 72 TAG DF45
Cash Back Parameters(*)	Contains parameters for the validation of the amount of cash back. Optional.	See doc. Ref. [1] field 72 TAG DF6D
Pre-Auth Amount (*)	Contains the amount that must be used for the preauthorization fuels. Required only if the acquirer has enabled this functionality 'of "pre-authorization Fuel".	See doc. Ref. [1] field 72 TAG DF6E
Acquiring Profile Updating Parameters		
Frequency (gg) (*)	Parameters Profile Update acquiring. Optional.	See doc. Ref. [1] field 72 TAG DF6E
Update Time (hh: mm) (*)	Parameters Profile Update acquiring. Optional.	See doc. Ref. [1] field 72 TAG DF6E
Magnetic Stripe Debit Card Parameters		
Service ID (*)	Identifies the service uniquely.	See doc. Ref. [1] FIELD 72 TAG FF0D DF6A
Service Name (*)	Debit card magnetic stripe service name	See doc. Ref. [1] FIELD 72 TAG FF0D DF49
Enabled Functions (*)	Bitmap of the enabled magnetic strip debit card functions. Read only	See doc. Ref. [1] FIELD 72 TAG FF0D DF3A
Agreement Functions (*)	Bitmap of the enabled magnetic strip debit card functions for this agreement. Overwrites the previous field.	See doc. Ref. [1] FIELD 72 TAG FF0D DF3A

(*) Data provided to the POS terminal in the DLL. The modification date Produces Of These **DLL** reminder to all terminals use them That Directly or Indirectly.

(**) Only if the acquirer is enabled for magnetic stripe debit card. Composed of 3 subfields service ID, service name, enabled functions. **See doc. Ref. [1] FIELD 72 TAG FF0D.**

In the
Magnetic Stripe Credit Card Applications List

FIELD	DESCRIPTION	NOTES
ID (*)	Uniquely identifies the service.	See doc. ref. [1] field 72 TAG FF0A DF6A
Service Name(*)	Magnetic stripe application service name	See doc. ref. [1] field 72 TAG FF0A DF6A
Description	Description for internal use.	
Description To The POS (*)	Values: New Current.	

9.2.3.2.6 Table: Routing

It is possible to add alternative routing for the particular agreement:

FIELD	DESCRIPTION	NOTES
Acquirer	Acquirer of the Agreement.	
Merchant Code	Codes assigned by the acquirer for the agreement.	
Terminal Code (*)		
ABI	Abi code to be used on the interbank track	

9.3 Statistics DLL

The scope of the DLL transactions is that of distributing (or updating) the operative/applicative parameters to the POS terminal. These parameters are subdivided in three macro-categories:

- **Parameters for the security management** that consists in the exchange of the session keys, of PIN protection and card authentication (Certification Authority of public keys).
- **Technical Parameters** of POS functioning (ex. Web type, telephone number, transmission speed, etc.)
- **Acquiring Parameters** (ex. Issuer ranges, agreement codes, floor limit, specific functions, etc.).

The above cited parameters may be uploaded on the terminal using two activation modes:

- **Initiative of the Periphery**
In manual mode, from an explicit request originated by the technical installer or in automatic after the physical installation and the upload of minimal parameters necessary for the GT connection (terminal ID, telephone num., speed, and connection type).
- **GT Reminder**
In correspondence to the reminded foreseen at the response to any online transaction.

The reminder to perform a DLL is indicated by the GT any time that configuration data connected to the terminal are edited. Based on the type of operation, the GT activates the provision of all parameters foreseen for the terminal or just a part of them.

The pages relative to the STATISTICS function supply a general operability test of the defined terminals in the FTFS system, these are:

total number of POS terminals configured

total number of terminals with operative status “Activated” and “Deactivated”

total number of active terminals that have done the parameters update, split by DLL type.

Note

DLL Types:

- Complete DLL
- DLL Technical Parameters
- Acquiring DLL Parameters
- DLL Technical Parameters + Acquiring
- DLL C.A. keys

9.4 Amounts List

The page relative to the Amounts List function, allows to perform a search of closings on a specific Terminal on a specific date and time:

FIELD	DESCRIPTION	NOTES
Terminal Code	POS CODE	
Cashier code		Displayed only in case the POS record data relative to the Cashier.
Day of Search	Closing Day	
Begin Time	Time search begins	
End Time	Time search ends	

Note

The search must always have valued:

*Terminal Code or Cashier Code or both
Day and time range in the day*

The following results will be viewed:

In case of searching only by Terminal Code + time range.

All closings of that specific terminal in that specific time range.

In case of searching only by Cashier Code + time range:

All closings of that specific cashier ion that specific time range.

In case of searching only by Terminal Code + Cashier Code + time range:

All closings of that specific terminal used by that specific cashier in that specific time range.

10 Operations

The functions allow to monitor the function of the FTFS Terminal Manager system, through the sub-functions **Transaction Search, Last Transactions, Preauthorized Transactions Search**.

The pages relative to the TRANSACTION SEARCH allow to view the transactions originating from the POS terminals, both those of service (DLL parameters conferment, balancing of totals, etc) as well as financial ones (purchases, returns, confirmations).

The implicit operations of the FTFS MC are recorded (implicit returns).

It is possible:

View the list of the POS operations and, through a record selection, access to the viewing of every single transaction detail.

The search criteria are:

- *Terminal Code*
- *Company Name*
- *Banner*
- *Operation Type (service and/or financial)*
- *Card Code*
- *Acquirer*
- *Amount*
- *RRN*
- *Begin search date (mandatory)*
- *End search date (mandatory)*

When it comes to the detail page, the data is divided in three sections:

- **GENERAL TRANSACTION DATA:** *requested by the POS, replied to the POS*
- **TRANSACTION DETAIL DATA and eventual MICROCIRCUIT DATA:** *operation type requested, outcome, card, amount, etc.*
- **INTERBANK CIRCUIT DATA:** *request and reply from the interbank circularity.*

Note In the TRANSACTION DETAIL page for service operations like DLL, balancing of totals only the GENERAL TRANSACTION DATA section is present, while the other two sections are relative only to the financial operations (purchases and returns).

10.1 Table: Transaction Detail

Table: Last Transactions Detail

FIELD	DESCRIPTION	NOTE
Pos Data Code		
General POS Transactions Data		
Terminal	POS Terminal code of agreement	
Point of sale	Name of point of sale	
ABI	Italian Bank Association represents the credit institution	
POS Data	POS date	
GT Data	GT date	
Operation Number	Number of the operation made	
Note	General notes	
Number of Tries	Number of tries made	
Function Code Requested	Code of the function requested	
Transaction Detail Data		
Transaction type	Indicates what type of transaction was made	
Pan	Number of the credit card. Synonym of CARD-NUMBER	
Amount	Amount	
Authorization code	Indicates the authorization code	
TR Outcome	Indicates the outcome of the transaction	

FIELD	DESCRIPTION	NOTE
Interbank Circuit Data		
Acquirer	Unique mnemonic code to identify the Acquirer in the system	
RRN	rrn	
IB Outcome		
Interbank Reply Additional Data		
Message	Reply message	
Payment Facilitator		
Payment Facilitator ID	Payment Facilitator Management	
Payment Facilitator Sender	Payment Facilitator Management	

10.2 Exporting of Transactions

Create a file with a list of transactions.

FIELD	DESCRIPTION	NOTE
Maximum Number of Transaction 20.000		
Terminal POS	POS terminal code of the agreement	
Banner	Store name	
FILE Type	FILE Formant	Excel or csv
Operazion Type	Type of operation searched	All, Financial, Service
Start Date	Start date	
End Date	End date	

10.3 Manual Transaction Insertion

This function allows you to edit a transaction in the archive manually entering the data to change.

The transaction type can be either an authorization or a refund, but it refers exclusively to a card type "CREDIT". No special controls are applied, except for the existence of the terminal code for which you are entering the transaction.

It should be considered as an emergency procedure available to the Customer, to recover, in the face of an unexpected anomaly, handling the accounting.

In the detail of the transaction is reported evidence of the type of entry made through manual mode from the user interface.

FIELD	DESCRIPTION	NOTE
General POS Transaction Data		
Terminal	POS terminal code of the agreement	
Point of sale	Banner of the point of sale	
ABI	Italian bank Association that represents the credit institution	
POS data	POS date	
GT data	GT date	

11 Operating Routes

The heart of the GT system is obviously the POS TERMINAL, but one needs to take into account many other information that are directly or indirectly linked to this.

As it has already been mentioned in the chapters that describe the FTFS functions, the data that can be generalized and used by one or more entities are described in tables called *General Profiles*, to which reference is made later on by defining each of the terminal specific profiles used. This type of configuration does not preclude, however, the "personalization" of the individual components, but rather makes more flexible the definition of each of the parts that come in an essential way in the constitution of the GT system.

The operating routes are intended to aid the user in configuring the system by indicating the steps to take to "connect" the data of the various FTFS functions.

It is necessary to proceed in the sequence of the operations indicated in the following paragraphs. For more details of the functions or of the fields on the page, see the relevant paragraphs and tables given in the manual.

Note The process, which is called FTFS_ABI2_KEY_MANAGEMENT and is launched with the script `startKM.sh` if Unix `startKM.cmd` if Windows, must be activated prior to the execution of commands on keys and certificates. Keep in mind that this process is configured to end alone after one hour of inactivity.

11.1 Preliminary Configurations

1 DEFINITION OF AT LEAST ONE CONNECTION.

Page: Connections List

Path: Home, Administration, Connections

NOTE: access to the detail of new CB1/CB2 connection by selecting on the navigation bar, the new button. Most likely at least two connections are defined: one for the 1st/2nd attempt and one for the 3rd attempt.

2 DEFINITION OF AT LEAST ONE TECHNICAL PROFILE.

Page: Technical Profiles List

Path: Home, Administration, Technical Profiles

NOTE: access to the new profile detail by selecting the new button on the navigation bar.

3 DEFINITION OF EMV APPLICATIONS (OPTIONAL).

Page: EMV Applications List

Path: Home, Administration, EMV Applications

Note: access to the New Application Detail, by selecting the button New Application on the Navigation Bar. New applications to which the system possesses at least one c.a. Public key may be entered.

4 DEFINITION OF AT LEAST ONE ACQUIRER.

Page: Acquirer List

Path: Home, Administration, Acquirer

Note: access to the New Acquirer Detail by selecting the New Button on the Navigation Bar. Proceed with the general data and interbank data definitions. -+-+

5 DEFINITION OF EMV APPLICATIONS FOR ACQUIRER (OPTIONAL).

Page: Associate Application – Acquirer

Path: Home, Administration, Acquirers, Acquirer Detail

Note: access to the Acquirer Detail, selecting the corresponding link from the Acquirer Detail List Page on the Navigation Bar, press the associate applications button. Proceed with the selection of one application from the ones suggested from the drop down list.

6 DEFINITION OF AT LEAST ONE EMV APPLICATION FOR ACQUIRE (ONLY AFTER POINT 5 HAS BEEN DONE).

Page: EMC Application List Profiles

Path: Home, Administration, Acquirers, Acquirer Detail, Profiles List

Note: access to the Acquirer Detail, selecting the corresponding link from this in the applications table at the bottom of the page, push the Profiles List (applications) link that corresponds to the application previously defined. Proceed with the definition of one or more profiles, by pushing the New Profile (new record) button on the Navigation Page.

11.2 Terminal Configuration

It is assumed that the “Preliminary Configurations” have already been defined, see previous paragraph. The definitions of the structure on more levels of merchant – point of sale – terminal are also needed. See chap. “Merch/Store/Term”.

1 DEFINITION OF AT LEAST ONE OPERATOR.

Page: Merchant Definition

Path: Home → Administration → Merch/Store/Term

NOTE: access to the New Merchant Detail by selecting on the Navigation Bar, the New Merchant button. The data of his (first) point of sale must also be defined. If the merchant has already been configured, we may proceed to point 2.

2 DEFINITION OF A POINT OF SALE ADDITIONAL TO THE MERCHANT

Page: Point of Sale Definition

Path: Home → Administration → Merch/Store/Term → Merchant Search → Merchant List → Point of Sales List

NOTE: from the Merchant List, push the corresponding like Point of Sales List, access to the New Point of Sale entry detail by selecting the button New Point of Sale on the Navigation Bar. If the Point of Sale has already been configured, we may proceed with point 3 or 4.

3 DEFINITION OF THE TERMINAL.

Page: Terminal Definition

Path: Home → Administration → Merch/Store/Term → Merchant Search → Merchant List → Point of Sale List → Terminal List

NOTE: from the Merchant or Point of Sales List, enter in the detail and select on the Navigation Bar, the New Traditional Terminal button.

4 DEFINITION OF A TERMINAL ADDITIONAL TO THE POINT OF SALE.

Page: Clone Terminal

Path: Home → Administration → Merch/Store/Term → Terminal Research → Terminal Details

NOTE: from the Terminal Detail page, press the New Register button. Enter the New Terminal Code. Following, by accessing this detail, it will be possible to eventually personalize the data.

11.3 Terminal Accreditation

It is assumed that the terminal is already defined. The first 3 points are part of the PRELIMINARY CONFIGURATIONS, see previous paragraphs.

- 1 MAKE SURE THAT THE ACQUIRER WITH WHICH A NEW AGREEMENT HAS BEEN STIPULATED, IS DEFINED.

Page: Acquirer List

Path: Home → Administration → Acquirers

NOTE: access to the acquirer detail by selecting the corresponding link to verify the configuration data.

- 2 IN CASE IN WHICH, FROM THE VERIFICATION OF THE PREVIOUS POINT, THE ACQUIRER IS NOT CONFIGURED, ACCESS TO THE PAGE THAT ALLOWS THE INPUT OF A NEW RECORD.

Page: New Acquirer

Location: Home → Administration → Acquirer → New Acquirer+

- 3 IN CASE IN WHICH, THE ACQUIRER SHOULD HANDLE SOME EMV APPLICATION FOR THE MICROCIRCUIT CARDS PAYMENT, ACCESS TO THE PAGE THAT ALLOWS TO ASSOCIATE TO THE ACQUIRER AN EMV APPLICATION FROM THE ONES DEFINED.

Page: Associate Application – Acquirer

Path: Home → Administration → Acquirer → Acquirer Detail → Associate Application Link

NOTE: following, from the acquirer detail define a profile page for the application, selecting the profiles link list.

4 ENTER A NEW AGREEMENT TO THE TERMINAL, USING THE DATA (AGREEMENT CODE/MERCHANT - TERMINAL CODE) RELEASED BY THE ACQUIRER.

Page: agreement definition

Path: Home → Administration → Merchants/Terminals → Terminal Research → Terminal Detail → from the Navigation Bar → Press the New Agreement Button.

NOTE: insert the agreement codes released by the acquirer.

Following, **from the agreement detail, activate the eventual EMV applications** (activate link) **associated to the acquirer, selecting the previously chosen profile** for the agreement.

11.4 Preliminary Operations for CB2: Certificate Request

NOTE The process, which is called FTFS_ABI2_KEY_MANAGEMENT and is launched with the script `startKM.sh` if Unix or `startKM.cmd` if Windows, must be activated prior to the execution of the following commands. Keep in mind that this process is configured to terms alone after one hour of inactivity.

The GT must ask to the Certification Authority (CO.BAN) to certify its public key, that certificate will be then used during the mutual authentication with the terminals (DLL phase 1). The steps to be taken are the following:

1 CREATE A COUPLE OF RSA KEY

Page: List of GT keys and GT Certificates

Path: Home → Administration → Keys-CB2-Certificates → GT keys-GT Certificates → New GT key

Insert all data requested from the following fields:

KEY NAME = Mnemonic Name of the Couple of Keys

LENGTH = Length of the Module in Bit

DESCRIPTION = Free Text that Describes the use of the Key

GT CODE = GT Identifier (Pseudo ABI)

CERTIFICATE NUM. = Certificate Number

PRESS "CREATE".

In Requested keys List, the status of key creation elaboration will be displayed which will need "to be confirmed".

The Key creation must be, for security reasons, managed by two authorized people. For this reason, after the previous step, it must be confirmed by the second user enabled for such operation.

2 CONFIRMATION OF KEY CREATION

Page: GT keys list and GT Certificates

Path: Home → Administration → Keys-CB2 Certificates → GT Keys - GT Certificates → List Requested Keys

PRESS “CONFIRM” ON THE CORRESPONDING LINE TO THE REQUESTED KEY.

In Requested Keys List, the operations resulting from the creation of the keys and their outcome will be displayed: Creation, Signature and Shipping to the CA.

In addition to the key generated in the GT Key List, in the GT certified list, a new line with the generated certificate will be displayed.

NOTE: It is necessary to refresh the window to see the new rows appear.

With this function in the directory:

.../files/certified

Two files are created:

xxxxx.sip containing the self-certified public key

xxxxx.hip containing the 'hash

The files must be sent to the Bancomat following the modality established by Bancomat itself.

Bancomat Spa will send in reply the files containing the certificate of the GT public key (xxxxx.Cnn where nn is the index of Bancomat's public key) and the corresponding Bancomat Spa public key for the verification (yyyyyy.hep, yyyyyy.sep).

The received file shall be copied into:

.../files/certificate

The files will then be able to be imported, remembering to activate with the command **startKM** the FTFS_ABI2_KEY_MANAGEMENT process.

3 IMPORT CA PUBLIC KEY

Page: CA Key Import

Path: Home → Administration → Keys - CB2 Certificates → RSA Keys-BANCOMAT → Import CA Key

INSERT DATA IN THE **NAME** FIELD = FILE NAME TO BE IMPORTED (WITHOUT EXTENSION. SEP)
PRESS "IMPORT"

4 IMPORT THE CERTIFICATE

Page: GT Keys List and GT Certificates

Path: Home → Administration → CB2 Keys Certificates → GT Keys- GT Certificates → GT Certificates List

PRESS "IMPORT" (corresponding link of the key).

11.5 RSA Key Activation

NOTE The process, which is called FTFS_ABI2_KEY_MANAGEMENT and is launched with the startKM.sh script if Unix or startKM.cmd if Windows must be enabled before executing the following commands. Keep in mind that this process is configured to end alone after one hour of inactivity.

If the previous steps were made with success, the key will be activated at the opportune time through activation.

1 KEY ACTIVATION

Page: Gt keys List and GT Certificates

Path: Home → Administration → Keys - CB2 Certificates → GT Keys - GT Certificates → GT Keys List

PRESS "ACTIVATE" (CORRESPONDING KEY LINK).

NOTE: *It is necessary to refresh the window to see the status change.*

So, this key becomes the “Active” key, while the one that was “Active” before changes status to “Expired”.

11.6 Key and Certificate Already in Client Possession

In some cases, the client may have more GT installations. In this case, the steps of paragraphs 11.4 and 11.5 are only to be made for the first GT. For the next installations, both RSA key as well as the GT certificate must be exported from the first GT and imported in the new installation.

In order to do so, also in this case, the process FTFS_ABI2_KEY_MANAGEMENT is used.

The steps are:

1. On the machine where the GT is positioned with information to be cloned, whether its for test or production,
 - in /app/nets/FTFS/KEYMANAGER launch

```
sudo -u ftfs ./startConsole.sh
$>list GT
```

Lists the keys and certificates present, indicating which one is active, since even the old certificates/expired remain in the database.

```
$>exportcert <numero certificato> P
```

Export the certificate and the production keys, indicate T for the test one or P for the production one. Generate the xxx.sql file in the directory

/app/nets/FTFS/KEYMANAGER

2. On the machine of the new GT
 - Copy the file import_XXXXX_NNNN.sql in /app/nets/FTFS/KEYMANAGER/files/ file
 - In /app/nets/FTFS/KEYMANAGER launch

```
sudo -u ftfs ./startConsole.sh
$>importcert <numero certificato> P
```

Import the certificate and the production keys, indicate T for the test one or P for the production one.

11.7 KMP Key Creation

NOTE The process, which is called FTFS_ABI2_KEY_MANAGEMENT and is launched with the startKM.sh script if Unix or startKM.cmd if Windows must be enabled before executing the following commands. Keep in mind that this process is configured to end alone after one hour of inactivity.

For each defined acquirer it is possible to define a KMP key or modify it, if necessary.

1 KMP KEY CREATION

Page: KMP keys list

Path: Home → Administration → Keys - CB2 Certificates → KMP keys

PRESS "INSERT" (LINK OF THE ACQUIRER).

In Requested keys List, the status of key creation elaboration will be displayed which will need “to be confirmed”.

NOTE: It is necessary to refresh the window to see the status change.

The Key creation must be, for security reasons, managed by two authorized people. For this reason, after the previous step, it must be confirmed by the second user enabled for such operation.

2 KEY CREATION CONFIRMATION

Page: KMP Keys List

Path: Home → Administration → Keys-CB2 Certificates → KMP keys

PRESS “CONFIRM” ON THE LINE THAT CORRESPONDS TO THE KEY REQUESTED.

In Requested keys List, the status of key creation elaboration will be displayed. Which may be “Error” or “Processed”. If it is “Processed” the key will be visible in the Keys List.

NOTE: It is necessary to refresh the window to see the new lines.

12 Appendixes:

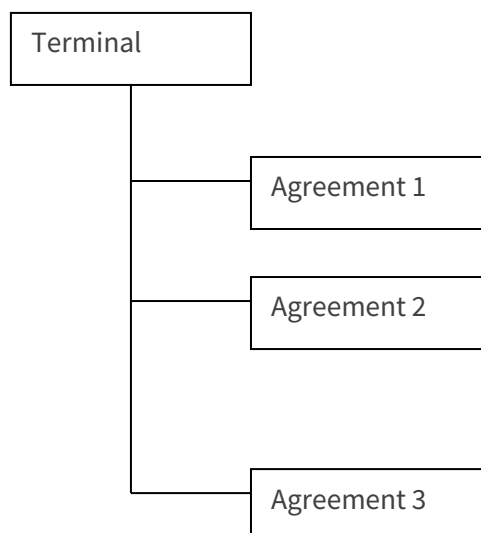
Appendix A: Dynamic Routing Mode Agreement

Following is described the FTFS option relative to the **AGREEMENT** of the clients following the specific modes of **DYNAMIC ROUTING (DR)**.

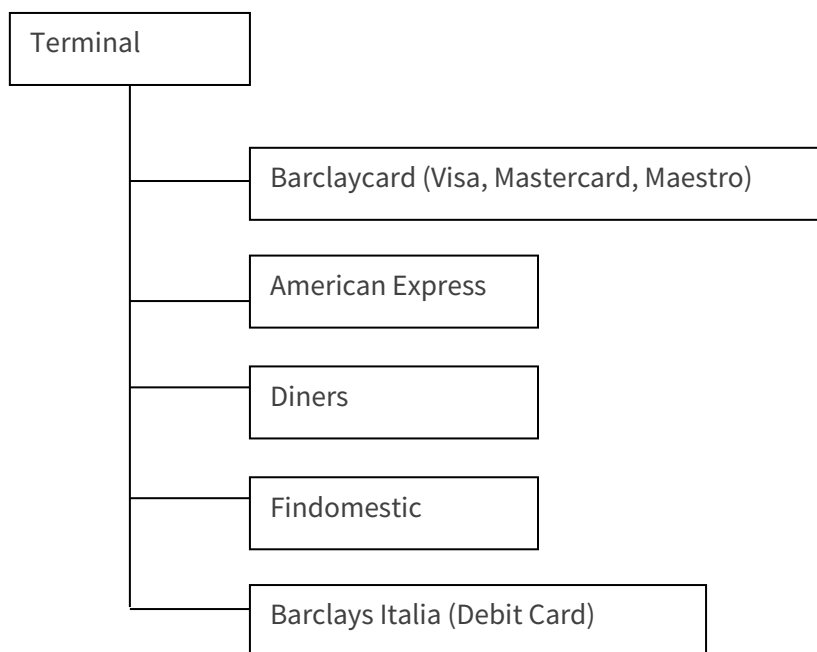
Through this option, FTFS may be configured to dynamically route the transactions to the acquirers.

The classic scheme of the agreement of a bank terminal foresees for a terminal a direct relationship with an acquirer for the types of cards contractually provided. Normally, the types of cards do not overlap between one acquirer and another.

Agreements have been added to cover the types of cards of interest to the Merchant.

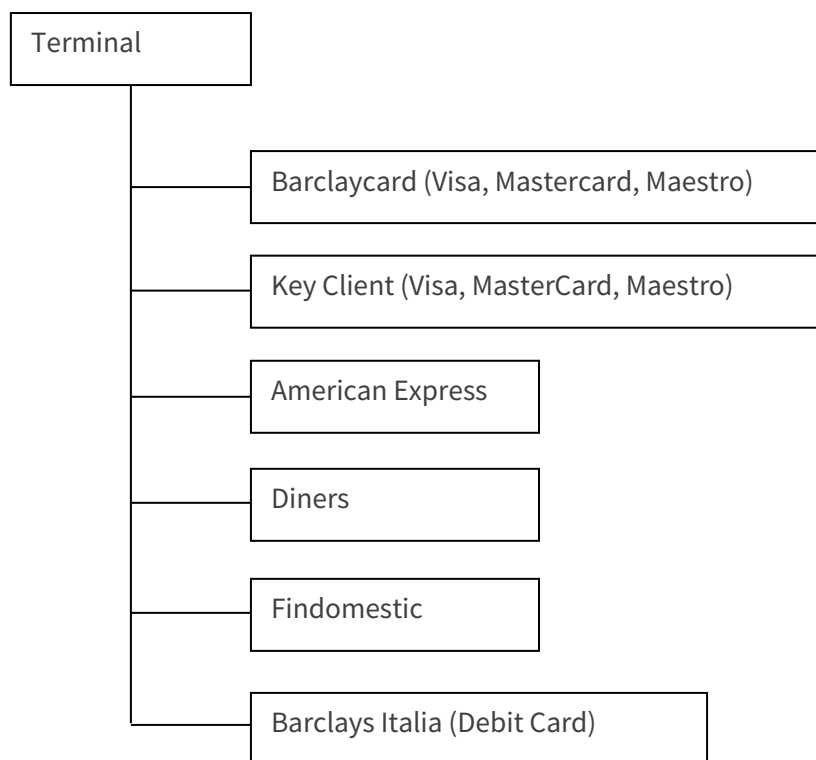


A traditional agreement example to cover the debit cards, Visa, MasterCard, Maestro, American Express, Diners and Findomestic cards, may be completed in the following way:



For a traditional terminal, the way to have a relationship with more acquirers in a same type of card context (for functional backup reasons), requires the definition of agreements directly on a terminal level. The drawbacks of a situation of this type may be recapped in two points:

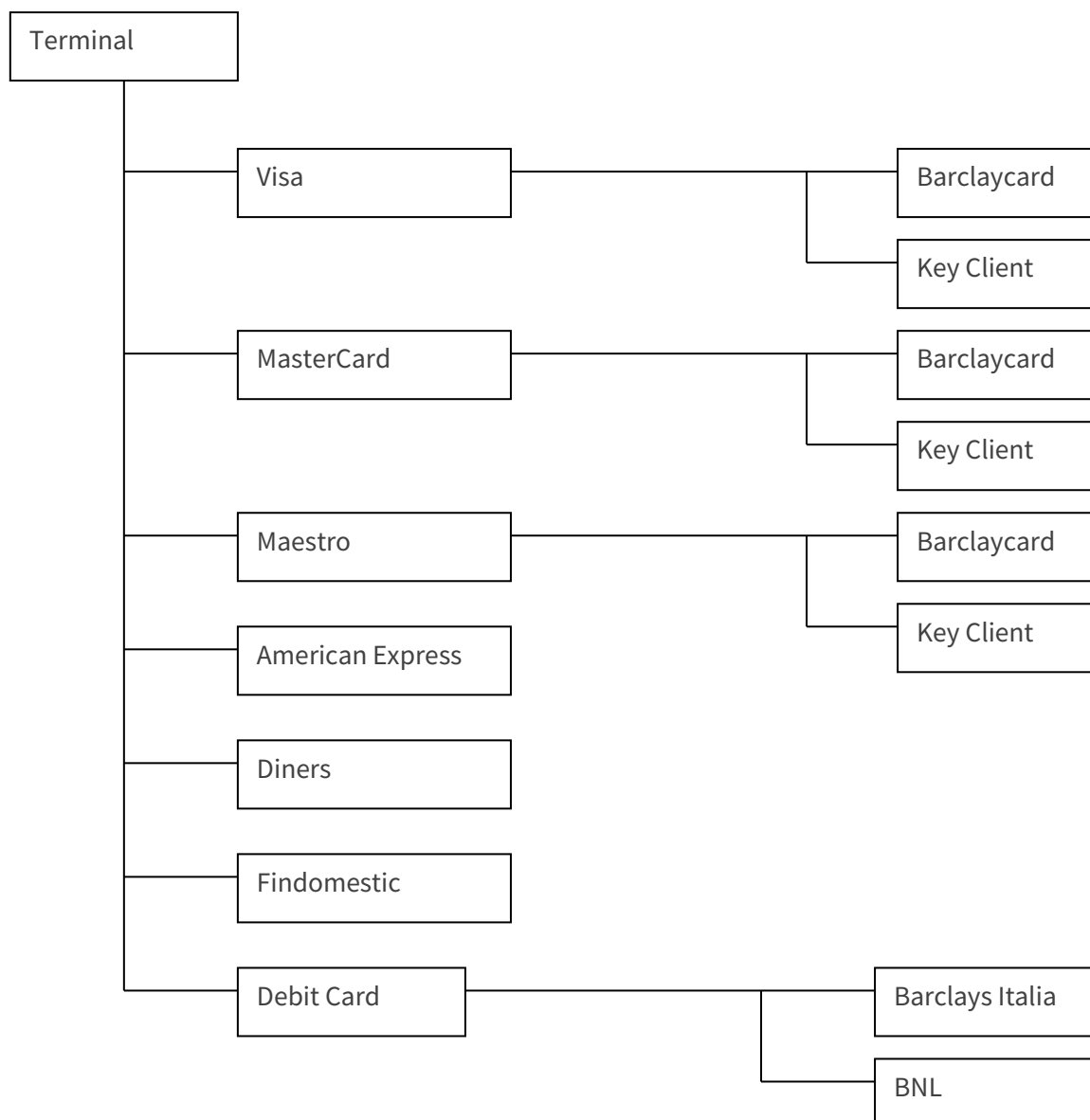
- *The selection between two equivalent acquirers must be made at the cashier point. Following, the choice of a backup acquirer, in case the “primary” one may not be operative, may require to be proposed again on the backup after an empty attempt on the primary one;*
- *The necessity to add a new acquirer would require a review the configuration giving a new set of parameters.*



The situation of a terminal that operates within big distribution or big companies with a payment cards acceptance web requires more flexibility and therefore FTFS in **DR** version is slightly different under these aspects:

Two types of acquirers are defined:

- *The DLL only acquirers correspond to the cards brands, but not to specific financial institutions. In other words they are not directly usable for the routing of transactions towards financial circuits and are comprised of a sort of virtual acquirer;*
- *The acquirers defined for DLL/routing are used to confer to the terminal the configurations to which there is direct correspondence with the agreed upon financial institution, or to send the transaction from an “only DLL” acquirer to a real financial institution.*



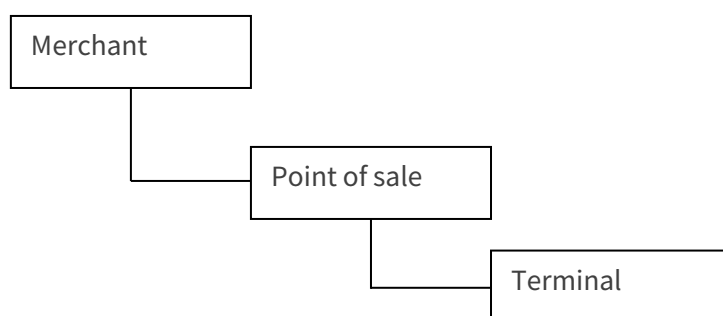
The terminal that receives a payment with a card marked Visa (PAN starts with 4) finds in the BIN conferred to a nominated acquirer that is the one of “DLL only” which we gave the VISA name. To a terminal level, it is not automatically know which will be the real authoritative institution. The decision is made by the terminal’s manager on the basis of the rules established under the Administration/Routing masks, in which the BIN generic 4 may be subdivided by the best criteria between many real “routing” acquirers.

The setting of the terminals manager must then take place by performing the following steps:

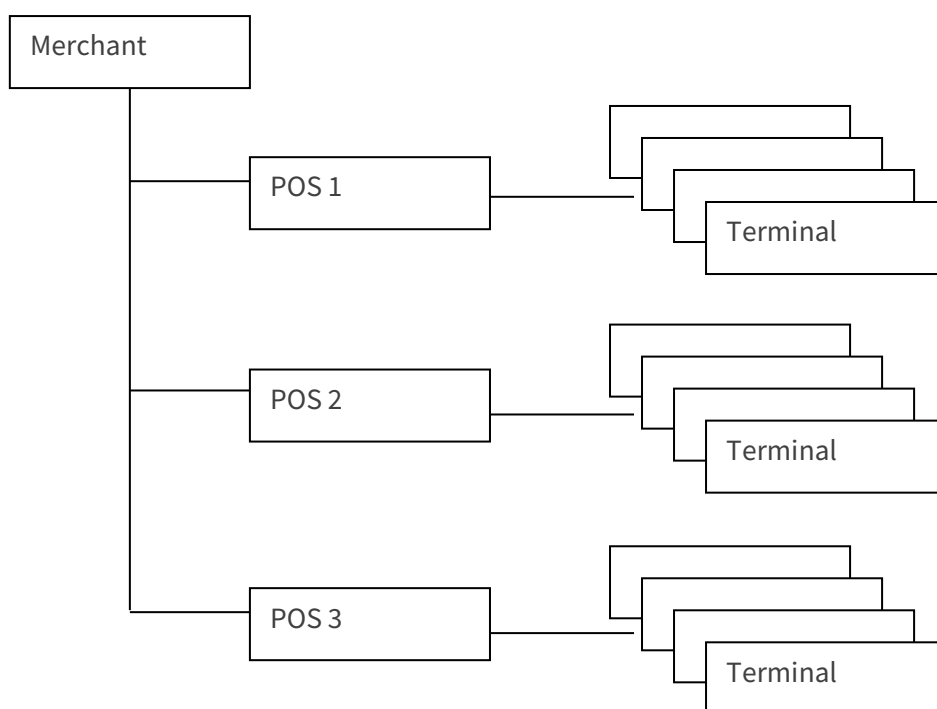
- *Definition of the acquirers: (Administration/Acquirer) is made during the initial system set up or in case of addition of new acquirers. This operation is extremely specific (all technical parameters must be defined) because of this, it is usually performed by N&TS GROUP.*

- *Definition of the routing rules: (Administration/Routing) is set up during the initial phase so that all the rules that have to do with the routing acquirers are covered. Once the rules have been set up (By N&TS GROUP) the client may easily modify them to conform to the changes that may arise.*

Once these general characteristics settings have been made, independently from the points of sale, the definition of data of the points of sale and the relative terminals needs to be defined. FTFS foresees a definition on 3 levels (Merchant, Point of Sale, and Terminal).



In a situation typical of configuration typology (DR) only one Merchant exists, from which all points of sales depend on, each with a terminal barrier.



In this situation, it is easy to define new points of sale or terminals that usually are the same as the preexisting one. It is then necessary to:

- *Define a point of sale (merchant - terminal/merchant search/new point of sale)*
- *Define a terminal belonging to a point of sale (merchants-terminals/merchant search/point of sale search/new terminal). The remaining terminals of the point of sale may be obtained successively once the first terminal is completed with a function that clones its configuration.*
- *Define the agreements for the terminal (from terminal detail: new agreement).*
- *These could be of two types:*
 - *Directly mapped on real acquirers for types of cards to which routing is not requested by the GT*
 - *On DLL only acquirers for types of cards to which it is not determined in advanced which is the authoritative acquirer. For these, it is subsequently necessary in addition to the agreement to specify one or more routing acquirers.*

Appendix B: Keys and Certificates Generation

Following here the database tables are shown which are subject to variations following the operations described in paragraph “Preliminary operations for CB2: certificate request” (see Chap. “Operating Routes”) making reference to the steps of the paragraph.

1- GENERATE A COUPLE OF RSA KEYS

AND

2- CONFIRMATION OF KEY CREATION

The creation inputs:

gt_rsakeys
ABI2 GT chiave per cert COGEBAN

At the signature the following table is modified:

gt_cert
SC_ABI2 2001

3- IMPORT CA PUBLIC KEY

gt_rsakeys
ABI2 GT key for COGEBAN cert
COGEBANxx CA

4- IMPORT THE CERTIFICATE

gt_cert
SC_ABI2 2001 IPKCERT

At the same time, the table that is subject to variation following the operations described in paragraph “KMP Key Creation” (see Chap. “Operating Rules”) making reference to the steps of the paragraph.

1. KMP KEY CREATION

AND

2. CONFIRMATION OF KEY CREATION

ac
VISA KMP KMP_CHECKVALUE

13 Glossary

Terminology to which reference is made in the manual.

NAME / ACRONYM	DESCRIPTION
ACQUIRER	A financial or banking institution, which through an agreement, offers shopkeepers or merchants services for credit card transactions belonging to certain circuits. There are acquirers that offer their services to only one circuit or to multiple circuits. The acquirer can be a bank, a service company, or the same circuit brand owner (this is the case with AMERICAN EXPRESS and DINERS who operate directly as acquirers). The merchant selects one or more acquirers based on the market, service, or for economic reasons. In any case the merchant has a contractual agreement with the acquirer, at times through a banking institution.
EMV APPLICATION	A group of parameters and data that determine the behavior of the micro circuit card so that it may perform the operations requested for the specific payment product.
BANK	<p>By virtue of the Italian system in which there is a local inter-bank circuit of debit cards (bank cards) owned by ABI, banks play a central role as in the vast majority of cases they are the owners of the POS used by merchants. Depending on the policies of each bank account, holders are offered diverse credit card products, and the merchants are offered agreements with various credit card circuits.</p> <ul style="list-style-type: none"> • In this sense, banks are in the middle of the phenomena of merchant management and act as financial intermediaries in various ways: • The payment of transactions to merchants both for debit card and credit cards is normally carried out by the banks which have provided the merchant with the POS; • The bank could be the issuer of the credit card, directly or through a company (for example Cartasi); • The bank could be the acquirer of the credit card, directly or through a company (for example Cartasi); • In the case of Debit Card, the card is definitely issued by a bank; • The bank could be the body carrying out the authorizations of the debit cards
CA - CERTIFICATION AUTHORITY	Certification Authority, public or private subject to administrate the generation, the signature, the distribution and the revocation of keys and certificates. The Certification Authorities, by emitting digital certificates, play the roles of third party guarantors of the identity of the owner of a given the public key. Each circuit (domestic, VISA, Europay, etc.) establishes its own CA; on issued micro circuit cards, data relative to the to each CA based on the applications managed.
CIRCUIT	We will use this term to define the brand to which a credit card is assigned. There are brands, for example, like VISA, MASTERCARD, AMERICAN EXPRESS, DINERS, JCB,

NAME / ACRONYM	DESCRIPTION
	MAESTRO EDC. The circuit takes care of routing the transactions received by the acquirers to the issuer through the network and the procedures which are defined circuit by circuit.
COMPANY	Is a term whose use often creates ambiguity. The company is often identified with the circuit, which however is not intended to be a synonym. Normally a credit card company (for example Cartasi) provides issuing and acquiring services. Within FTFS we mean, for simplicity, the term as being synonymous with the acquirer, identifying a point of view of the merchant.
CRYPTOGRAPHY	<p>Mathematical process by which a set of data is encrypted or encoded so as to be incomprehensible to those not authorized to its use.</p> <p>Modern encryption systems are distinguished on the basis of the public or private nature of the code ("key") they utilize. In private or symmetric key systems (such as DES - Digital Encryption Standard), the receiver of the message, to be able to decode it, must know the key with which the sender has encrypted the message. In asymmetric or public key systems, including one of the best known being RSA, there is no need to share a secret key. The encryption, in fact, is done by using a "public key" that is made available and used by anyone to encrypt and send data, while decoding, or making the message understandable, can be done through a secret key that only the recipient knows. In the digital signature the sender uses the secret key, while the recipient uses the public key.</p>
CVR	Card Verification Results, Table of flags issuer-proprietary set up by the EMV application and used during the Card Action Analysis to determine whether the transaction "exits" from the established criteria following the applicative parameters of the card.
DES	See Cryptography
DLL	Down Line Load, is the compound of transactions exchanged between GT and POS for the conferment or update of the operative/applicative parameters of the terminal functioning
EMV	Europay Mastercard Visa. Constitutes an international standard to which many service based smartcard (micro circuit cards) releasing companies refer to. The EMV specifics are about the software characteristics for cards, terminals and applications.
MERCHANT	Is the body or company engaged in a commercial business in which among the payment methods offers that of credit cards. They have a contractual agreement with the acquirer.
PAYMENT FUNCTION	An integrated set of executable commands that define the rules for the procedures to apply; defined in the EMV standard.
GT	Synonym of Terminal Manager.

NAME / ACRONYM	DESCRIPTION
ISSUER	Is an institution that issues credit cards. The cards are always associated with a circuit. The relationship with the issuer concerns the cardholder and not the merchant, who has the relationship with its acquirer.
SETTLEMENT FILE	A file containing data for sales transactions, cash advances, reversals, and for the accounting within the acquiring part of the procedure.
MAC	Message Authentication Code.
MUTUAL AUTHENTICATION	Preliminary phase between GT and POS to guarantee the authenticity of the keys used (the keys come from an authenticated entity and from an authenticated terminal). Only at the completion of this phase, the GT activated the DLL parameters.
POS	Point of Sale. Peripheral terminal, installed at a merchant to carry out debit or credit transactions.
PAYMENT PRODUCT	Standardized set of rules and processes that defines the payment transaction (e.g. Visa Credit, Debit Cards etc). A payment product is linked to an application that identifies the data and parameters that must be provided at the payment Function.
RID	Registered Application Provider Identifier
ROUTER	A router is a device (hardware or software) that manages the connection between two or more networks. It is an essential device for connecting networks also of different types, through which it manages the routing of messages.
RSA	See cryptography.
TAC	Terminal Action Code, supply an inspection on some aspects of the EMV transaction, simply put, whether to go online or decline and the behavior in case of “unable to go online”.
EMV TERMINAL	Device compliant with the EMV 4.1 specifications [Ref.9] which supports one or more payment products; for ex.: Point of Sale (POS).
CARDHOLDER	Is the holder of the card with which payment is made. Has a contractual agreement with the issuer.
TRANSACTION	Is an operation with which verification is requested for a certain card to establish the availability of funds for the spending of a determined amount or handling a financial movement, or to reverse an authorization or a financial movement.
TVR	Terminal Verification Results. Flags Table set up by the terminal during the Terminal Risk Analysis that reflects the status of a transaction. Example: black listed card, PIN requested but not entered, etc.

EXTERNAL DOCUMENTATION

The following table shows the documents and / or manuals that can provide further specifications for completing the topics covered.

ID	TITLE	EDITION /RELEASE	OWNER
[1]	SPECIFICATIONS FOR INTERFACE POS TERMINAL - MANAGER TERMINAL CODE SPE-DEF-040	2.2.1	BANCOMAT SpA
[2]	NG-FTFS_POS_TerMan-PA_DSS_Guide-ASI_Ed1.pdf	1	N&TS GROUP
[3]	Log Unico POS – SIA Rel	8.8	NEXI (ex SIA)

NOTE For further information and to consult the specific documentation we refer you to the website that you can visit at the following address: **<http://www.bancomat.it/it>**

LEGAL NOTICE

Intellectual property

All information contained herein, including text, images, graphics, are the exclusive property of N&TS GROUP Networks & Transactional Systems Group S.p.A. (hereinafter N&TS GROUP) and are protected by copyright and other intellectual property documentation. It is absolutely forbidden to reproduce, appropriate, without any limits, reproduce and/or copy the content or images of the present document without the prior written authorization of N&TS GROUP. This document may be subject to revision and/or modifications.

Confidentiality Obligations

The recipient of this document is required to keep all the information contained therein strictly confidential as well as to protect it from any disclosure and/or communication, in whole or in part and for any reason whatsoever, to third parties.

Brands®

N&TS GROUP owns the following ® brands: N&TS GROUP Networks & Transactional Systems Group S.p.A. - company logo N&TS GROUP - Globemark N&TS GROUP - ACFS® - IGFS® - FTFS® - MTFs® - NTFS®. Any other brands and names are registered trademarks of their respective owners who have given N&TS GROUP authorization to use them for the purposes referred to herein.

