



Digital Transaction Register

Acquirer Interface Agreement

Version: 5.0

Status: Draft

Change History

The following table shows the history of changes to this document.

Date	Author	Change history
28/02/2020	Stefano Menotti	First version Draft
28/04/2020	Luca Somaruga	Timestamp field format update
21/05/2020	Debora Arena	<p>Updates:</p> <ul style="list-style-type: none"> - Chapter "Digital payment transactions covered by the service": added constraint on enrolled HashPans. - Paragraph "Integration with Acquirer": added constraint on enrolled HashPans. <p>Added:</p> <ul style="list-style-type: none"> - Chapter "Batch service for HashPan control" <p>Update:</p> <ul style="list-style-type: none"> - "Appendix 1 - File transfer mode": the batch service will send the flows to the Platform sFTP
22/05/2020	Stefano Menotti	Version exportable to Acquirer stakeholders
27/06/2020	Debora Arena	<p>Updates:</p> <ul style="list-style-type: none"> - Standard PagoPA flow - Addition of the chapter "Onboarding Merchant through Acquirer"
30/07/2020	Rodolfo Viti	<p>Update:</p> <ul style="list-style-type: none"> - Standard PagoPA flow - Appendix 4 - Salt recovery service - Appendix 5 - Service for downloading HPANs registered in CentroStella - Appendix 6 - Acquirer Services Authentication <p>Added:</p>

		<ul style="list-style-type: none"> - Appendix 7 - Acquirer Services Authorisation - Appendix 8 - Environments
02/09/2020	Rodolfo Viti	Update: <ul style="list-style-type: none"> - Standard PagoPA flow (field length)
02/10/2020	Denisa Braho	Added: <ul style="list-style-type: none"> - "Proposed functional solution" paragraph containing the process happy flow and the relative drawing Update: <ul style="list-style-type: none"> - "circuit_type" field (circuit "00-PagoBancomat" will be managed exclusively by the Bancomat Acquirer)
14/12/2020	Denisa Braho	Update: <ul style="list-style-type: none"> - Happy flow - "circuit_type" field (circuit "03-AMEX" will be managed exclusively by Amex)
15/12/2020	Denisa Braho	Update: <ul style="list-style-type: none"> - Happy flow - "circuit_type" field (circuit Diners will be managed exclusively by Diners)
13/04/2021	Denisa Braho	Updated: <ul style="list-style-type: none"> - paragraph "Standard PagoPA flow" by adding a new field in the file (parameter: PAR) - updated description of the parameter "hash_pan"



Document Approval

The following table lists the stakeholders with whom the document was shared and approved.

Stakeholder (name)	Approval date	Validated processes



Index

Change History	2
Document Approval	4
Index	5
Introduction and purpose of the document	6
Regulatory reference	6
Privacy and data processing	7
Introduction and scope of the initiative	7
Objective:	8
Functional solution proposed: Digital Payments Bonus	8
Happy Flow	8
Digital payment transactions covered by the service	9
Information Perimeter	9
Process for sending transactions to RTD	10
Acquirer Integration with PagoPA CentroStella	10
Standard PagoPA flow	11
Batch service for controlling enrolled HPANs	17
Merchant Onboarding via Acquirer and saving data on the FA Platform	18
Acquirer Registration Service on API Gateway	19
Show T&C	19
Retrieving Billing Provider List	20
T&C acceptance, sending Merchant data and saving on the FA Platform	21
Appendix 1 - PGP Public Key	24
Appendix 2 - File Transfer Mode	25
Appendix 3 - sFTP SIA access manual	25
Appendix 4 - Salt recovery service	26
Appendix 5 - Service for downloading HPANs registered in CentroStella	27
Appendix 6 - Acquirer Services Authentication	28
Appendix 7- Acquirer Services Authorisation	29
Appendix 8 - Environments	33
Appendix 9 - PGP Production Public Key	33

Introduction and purpose of the document

The purpose of this document is to describe the application solution, in all its interfaces and the different flows of incoming or outgoing events to be managed and the related data exchange methods, as well as the High Level executive architecture, with particular reference to the interfaces presented by the Acquirer subjects to PagoPa SpA systems (CentroStella).

Regulatory reference

The service has as its regulatory reference Italian Legislative Decree 26/10/19 no. 124 converted by conversion Law of 19 December 2019, no. 157 published in the Official Journal no. 301 of 24-12-2019, and in particular in Article 21:

Art. 21: Tax certifications and electronic payments

*1. In Article 5 of Italian Legislative Decree no. 82 of 7 March 2005, the following are added after ((paragraph 2))-quinquies: **"2-sexies. The technological platform referred to in paragraph 2 may also be used to facilitate and automate, through electronic payments, the tax certification processes between private parties, including electronic invoicing and** the storage and transmission of daily fee data referred to in Articles 1 and 2 of Italian Legislative Decree no. 127 of 5 August 2015.*

2-septies. By decree of the President of the Council of Ministers or of the Minister Delegate for Technological Innovation and Digitisation, in agreement with the Minister of Economy and Finance, the technical operating rules of the technological platform and the processes referred to in paragraph 2-sexies are defined".

Privacy and data processing

Please refer to the document DPIA approved by the Privacy Guarantor.

Introduction and scope of the initiative

The objective of the project is the creation of a technological infrastructure which allows to enable new use cases and services for citizens and businesses, mainly focused on the digitalisation of payments through the use of cards and payment instruments through physical POSs.

The pillar of the new infrastructure is communications with the Acquirer entities operating in Italy.

The PagoPa platform CentroStella must manage information that must comply with all the requirements of the GDPR; in particular, it must not be allowed to trace the individual transaction and recover the personal data of the payers and/or the payment in any way.

The macro components covered by the initiative are listed below:

DIGITAL TRANSACTION LOG (RTD) Aggregates commercial transactions carried out through digital payment instruments, both by individuals and by companies through physical POSs throughout Italy. A single log that enables the creation of electronic billing, welfare and automation incentive solutions.	
AUTOMATIC BILLING Relies on the Digital Transaction Log for the automatic issuance of electronic invoices in the context of a payment made by a company.	DIGITAL PAYMENTS BONUS Relies on the Digital Transaction Log to award bonuses to citizens who make payments through digital payment instruments.

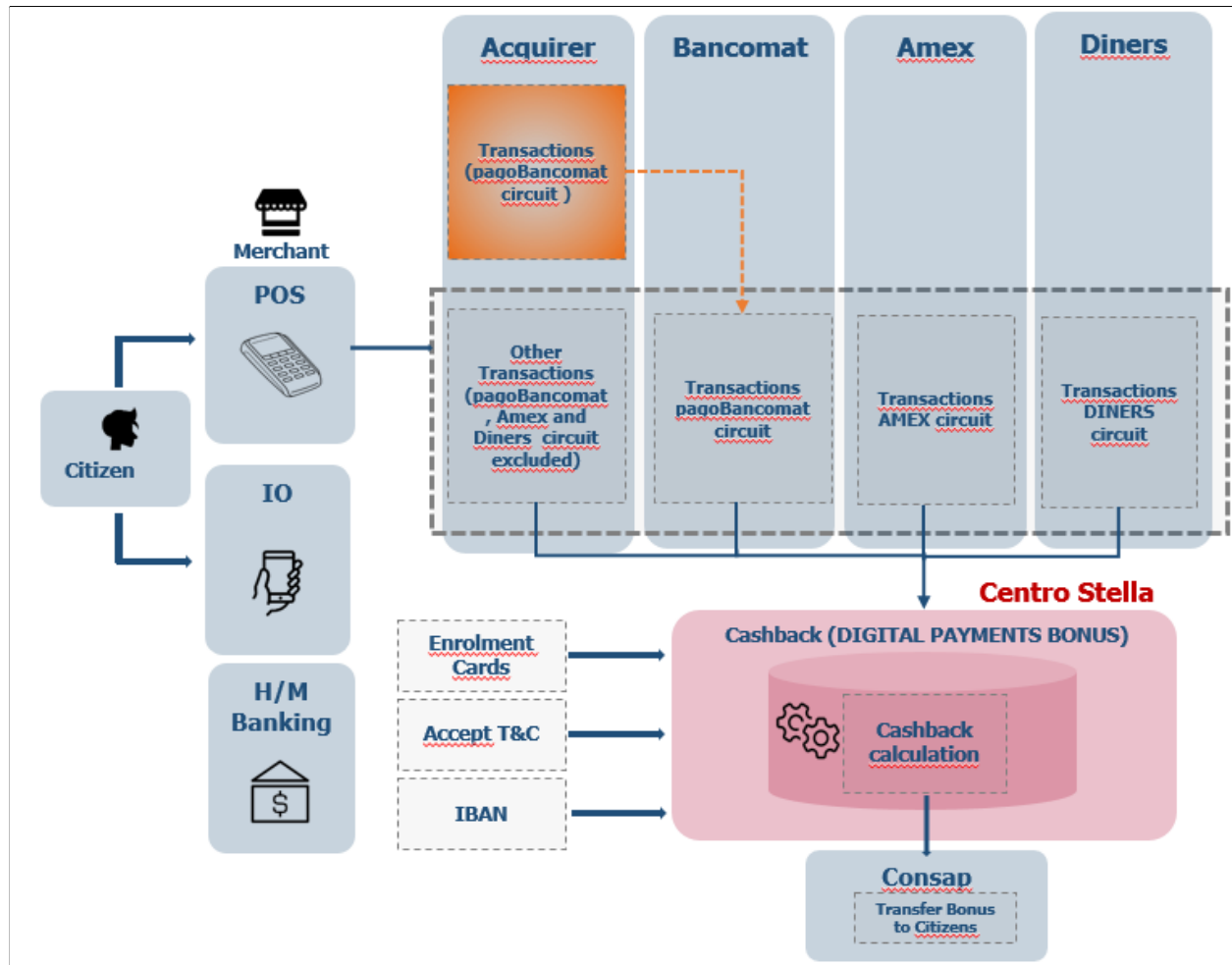
Objective:

The Digital Transaction Log is therefore the enabling platform for different and future use cases that see the role of electronic payments as central, maintaining a unique integration with Acquirer entities operating in Italy.

The main objectives of the project are therefore:

- to encourage payments by electronic means to reduce the use of cash, creating rewarding conditions and a cumulative result even if achieved with different payment instruments.
- to boost the adoption of e-billing by small operators by simplifying the exchange of information between all the actors involved in the process.

Functional solution proposed: Digital Payments Bonus



Happy Flow

The Happy Flow is explained below, summarising the proposed functional solution of the project:

- The Citizen securely stores their payment instrument on the platform CentroStella
- The Citizen makes a payment to a physical operator in Italy
- The Acquirer, after posting the transaction, sends the transaction data to the platform BPD
 - The Acquirers participating in the service will send to Centro Stella only the transactions related to circuits different from PagoBancomat, Amex and Diners.
 - The Acquirers will send only the transactions carried out on the PagoBancomat circuit to Bancomat
 - Bancomat, Amex and Diners will send directly to CentroStella all the transactions carried out on their own circuit (including those received from the other Acquirers in case of Bancomat)
- CentroStella assigns points to the transaction



- e. Cashback awards are assigned based on the accumulated points
- f. The Citizen enters the IBAN of their current account through the IO App or H/M Banking to be credited with the accrued cashback.

Digital payment transactions covered by the service

Information Perimeter

The **digital electronic payments** to be considered are all payments made through *physical POSs in Italy*, using the following payment instruments:

- debit cards on international and ATM circuits,
- credit cards,
- prepaid cards (rechargeable cards not linked to a current account, rechargeable cards linked to a current account, rechargeable cards with account functions),
- applications related to credit transfers or other settlement systems

For a correct provision of services, and with the aim of not discriminating against any type of citizen/payment transaction, **the Acquirer must also convey the transactions including any on-us modes to PagoPA** and including any reversal operations.

The object of the service will be only transactions in *EUR currency*.

The following transactions are therefore excluded from the perimeter:

- related to cashback (cash withdrawal)
- cash advance on POS (MCC = 6010)
- cash advance on ATM (MCC = 6011)
- related to e-commerce
- Dynamic Currency Conversion (DCC)
- carried out in the territory of San Marino

It should also be noted that, according to the process approved by the Privacy Guarantor, only transactions with HashPans relating to payment instruments for which the Citizen/Buyer has enrolled in one of the services activated on the CentroStella platform of PagoPa will be able to flow to the PagoPA systems (CentroStella).

Process for sending transactions to RTD

The process of sending transactions to the CentroStella Platform (RTD) consists of the following phases:

- a. The CentroStella Platform generates a flow containing the HPANs enrolled in the CentroStella service.

- b. The Acquirer consolidates the data relating to all transactions of interest accounted for in the last settlement cycle with the merchant. It therefore generates a text file in csv format (with file naming and detailed layout in the paragraph "Standard PagoPA Flow") and deposits it in a folder on which the batch is being polled. The deposit of the file is the trigger that starts the batch process.
- c. The Batch installed at the Acquirers invokes the service displayed by the Platform, through which a one-shot link is generated and activated temporarily to download the flow of HPANs enrolled in the CentroStella platform services.
- d. The Batch calls the service presented by CentroStella to obtain the constant hashing key to add to the PAN to hash the PANs contained in the transaction flow.
- e. The Batch reads both input flows (HPAN list and transactions) and, for each line of the transaction file:
 - i. hashes the PAN in the transactions flow;
 - ii. determines whether the transaction row should be discarded or reported in the filtered output flow.
- f. After the processing in the previous point, the Batch finishes writing the filtered flow in output, and deletes all the data received in input.
- g. The Batch performs PGP encryption of the output flow. "Appendix 2" shows the public key to be used for encrypting the file produced in the previous point.
- h. The Batch deposits the filtered transaction flow on CentroStella sFTP. For more information on instructions and how to access the SIA sFTP, refer to the indications in Appendix 3. It should also be noted that the Batch deposits the output file in the directory /Inbox/.
- i. Finally, CentroStella deletes all the files received in input.

Acquirer Integration with PagoPA CentroStella

Accredited *Acquirers* (i.e., those who have entered into an agreement with PagoPA S.p.A.), at the end of the successfully concluded payment transaction, will generate the daily flow of transactions.

The latter will be filtered in order to verify that the HPANs present in the various paths correspond to those enrolled in the CentroStella Platform, before being sent to the same.

This control will be guaranteed by a batch service installed on the Acquirers' systems, which PagoPa will give to the Acquirer, in the form of an *opensource* code, to be used to facilitate integration and minimise efforts. For more details see the paragraph "Batch service for HPAN control"



Given the above, it should be noted that the Acquirers will have the right to use one or more integration modes and, for each mode, one or more daily files to cover the entire set of transactions to be transmitted to CentroStella.

PagoPA SpA will ask the accredited *Acquirers*, maintaining the objective of minimising the technological effort for each Acquirer and, at the same time, ensuring *compliance* with PCI¹ regulations, the sending of one or more **batch flows** in the "**PagoPA standard**" format: PagoPA SpA will provide a simple implementation flow specification that includes the minimum subset of data, described in the following paragraphs of this document.

PagoPA SpA (CentroStella Platform) is responsible for managing the data in the PCI environment according to current legislation and maintaining only the minimum subset of anonymised data (**filtered for enrolled HashPans**), necessary for the operation of the Platform, eliminating any data of transactions that have not been made with payment instruments voluntarily enabled by the Citizen on the Platform. The card data will be saved with an **irreversible cryptographic hash function**.

In this respect, the integration of the Acquirers with CentroStella is divided into two phases:

- Standard PagoPa flow
- Batch service for enrolled HPAN Control

The details of the points listed above are shown in the following paragraphs.

Standard PagoPA flow

The following describes the details of the Standard PagoPA Flow.

The naming convention of the file is as follows:

- [service].[ABI].[filetype].[date].[time].[nnn].csv

in particular:

- service: fixed as 'CSTAR' (5 alphanumeric digits)
- ABI: Sender ABI (5 numeric digits)
- filetype: fixed as file type (6 alphanumeric digits)
- nnn: progressive file (3 numeric digits)

¹ Payment Card Industry: security certification with which all payment systems must comply.

field	format	notes
-------	--------	-------

service	Alphanumeric - 5 char	fixed value CSTAR
ABI	Alphanumeric - 5 char	sender ABI code
file_type	Alphanumeric - 6 char	type of flow sent. Fixed value TRNLOG
[date].[time]	YYYYMMDD.HHMISS	file creation timestamp
nnn	Alphanumeric - 3 char	Progressive value of the file (e.g. 001)

Please note that:

- The file is in .csv format, with separators “;”
- the file is encrypted with a pgp public key issued by PagoPa SpA
- The contents of the file do not include head and tail records but only detail records, according to this layout:

Fields in the Standard PagoPA Flow.

field	Type	Mandatory	Notes
acquirer_code	Alphanumeric max 20 char	- YES	ABI code of Acquirer bank.
operation_type	Alphanumeric regexp [0-9]{2}	- YES	Operation type: 00 - payment 01 - reversal of payment 02 - payment with ApplePay 03 - payment with GooglePay xx - future uses Types 02 and 03 will not always be valued by the Acquirers
circuit_type	Alphanumeric regexp [0-9]{2}	- YES	Payment circuit: 00 – Pagobancomat - Transactions on this circuit will be sent exclusively by the Acquirer Bancomat. 01- Visa

			<p>02- Mastercard</p> <p>03- Amex</p> <ul style="list-style-type: none"> - Transactions on this circuit will be sent exclusively by AMEX. <p>04- JCB</p> <p>05- UnionPay</p> <p>06- Diners</p> <ul style="list-style-type: none"> - Transactions on this circuit will be sent exclusively by Diners. <p>07- PostePay Code</p> <p>08- BancomatPay</p> <p>09- SatisPay</p> <p>10- private circuit (onus, owen)</p> <p>xx - future uses</p>
hash_pan	Alphanumeric – max 64 char	YES	<p>Hash of the PAN of the payment instrument used.</p> <p>In the case of a non-card based circuit, it represents the unique identifier of the proprietary payment instrument, which the user can register through the IO App or touch point of the Issuer bank.</p> <p>In case the payments are done with a tokenized payment instrument, this field must contain the hash Token that uniquely identifies the payment instrument (es. Apple Pay; Google Pay etc)</p>

date_time	DateFormat <i>ISO8601 FORMAT</i> yyyy-MM-ddTHH:mm:ss.SSSXXXX X	YES	Timestamp of the payment transaction carried out with the Merchant. Please note that the second details are not always available for all transactions. In this circumstance, the detail will be padded with all '0's
id_trx_acquirer	Alphanumeric - max 255 char	YES	Unique identifier of the transaction at the Acquirer level. - can be populated with the <i>ARN</i> , or if this data is not present, with a <i>unique id</i> that allows to uniquely identify the transaction on the Acquirer side.
id_trx_issuer	Alphanumeric - max 255 char	NO	Authorisation code issued by the Issuer (ex: AuthCode)
correlation_id	Alphanumeric - max 255 char	NO	Correlation identifier between payment transaction and possible reversal. In certain cases, the data cannot be retrieved by the Acquirer and the information in the field in question will not be sent

total_amount	Numeric	YES	Valued in euro cents (ex: 10€ = 1000) and expressed in absolute value: the sign is assumed from the type of operation "00-payment, 01-reversal"
currency	Alphanumeric - max 3 char	NO	Fixed value 978 = EUR. International ISO coding is used.
acquirer_id	Alphanumeric max 255 char	YES	<p>Unique Acquirer ID. In the case of card transactions, it represents the homonymous value conveyed on the international circuits.</p> <ul style="list-style-type: none"> - In the Pagobancomat circuit it corresponds to the field <i>codice_sia_abi</i> - Visa/Mastercard Circuit: <i>acquirer_id</i> <p>In other cases the field will be valued with fixed data depending on the reference Acquirer</p>
merchant_id	Alphanumeric max 255 char	YES	<p>Unique identifier of the physical store of the Acquirer (also known to the Merchant and used by the same to register on the Automatic Billing platform).</p> <ul style="list-style-type: none"> - In the Pagobancomat circuit it can correspond to the field: merchant
terminal_id	Alphanumeric max 255 char	YES	<p>Identification of the Merchant's terminal/POS (Point of Sale).</p> <ul style="list-style-type: none"> - In the Pagobancomat circuit it

			corresponds to the field: <i>cashier premises</i> - Visa/Mastercard circuit: <i>terminal_id</i>
bank_identification_number (BIN)	Alphanumeric or - regex [0-9]{6}[[0-9]{8}	YES	Code containing the first 8 digits of the payment instrument. - In the Pagobancomat circuit it corresponds to the field: <i>codice_abi</i>
MCC	Alphanumeric max 5 char	YES	Merchant Category Code.
PAR	Alphanumeric	NO	Payment Account reference The field must contain the information of the PAR, which can be defined as a collector capable to associate each TokenPAN with the PAN of the physical card, thanks to the unique and immutable association between PAN and PAR and Token and PAR

Batch service for controlling enrolled HPANs

The service will be developed by CentroStella and installed at the accredited Acquirers. However, it should be noted that the maintenance of the service, and any modifications thereof, are the responsibility of the Acquirer. PagoPa will provide the source code in opensource logic, published in public repositories to facilitate integration and minimise efforts.

Operating Mode

The artefact consists of an executable jar produced with *spring-boot*, therefore all



the project dependencies

are contained within the jar along with the classes that contain its business logic.

In this way the artefact is completely autonomous and usable on any device that has a JVM.

The installation and execution of the batch requires:

- Java 1.8+
- *Batch-transaction-filter.jar* artefact

With regard to the parameters and execution commands, please refer to the indications in the README file in the public repository accessible via the link:

<https://github.com/pagopa/rtd-ms-transaction-filter/blob/master/README.md>

Minimum requirements

Below are the minimum requirements for the execution of the batch described above:

Software:

- JVM 1.8+

Hardware:

- CPU:
 - Architecture: x86_64
 - CPU 32-bit,
op-mode(s): 64-bit
 - CPU(s): 4
 - CPU MHz: 2992.966
- RAM: 4 GB
- HD: Depending on the size of the transaction file. To the previous file must be added the size of the file containing the pan hashes which is around 300 MB (in pgp format).

Execution status management

The batch service manages the files used in cases where a blocking error occurs or when the execution is completed successfully.

The behaviour of the various steps of the service will be affected by the configuration of the property `deleteLocal`, which requires possible deletion at the end of the execution of all processed files, if active.

If otherwise configured, the appropriate behaviour is archiving the files processed in the flow, both for the file containing the list of PANs, and for that of transactions, for



any management alongside the same.

In case of successful execution, the pan file will be removed, along with all temporary files generated before the final output file is sent. The transaction file obtained will be stored in a dedicated directory.

It will also be possible to configure, for generic errors in processing individual file records, a margin of tolerance with respect to the number of rows for which an error was found, using the property skipLimit.

The file will be processed without exceeding the configured threshold value, a success will be reported conditioned on the presence of some errors, which can possibly be managed on the sides.

Merchant Onboarding via Acquirer and saving data on the FA Platform (in review)

In order to be able to Onboard the Merchant to Automatic Billing services, the Acquirer's systems will invoke the APIs displayed by the CentroStella platform to census the Merchant and will display a service to communicate the Merchant's data to the Platform.

Subsequently, the FA system will save this information in the internal database.

Having said the above, the following APIs are expected to be presented to Acquirers:

- Service subscription T&C display [showT&C]
- Acceptance of T&C service subscription [acceptT&C]
- Retrieving Billing provider list
- Sending Merchant data and saving on the FA Platform

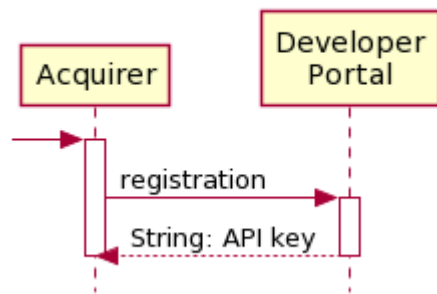
The following paragraphs describe the services and parameters necessary for correct integration with the Automatic Billing service.

Acquirer Registration Service on API Gateway

The "Acquirer Registration" service allows the Acquirer to register on the API Gateway portal and obtain the key used for authentication on CentroStella.

Acquirer Registration

Registrazione Acquirer



For more details, refer to [Appendix 7](#).

Show T&C

Path: fa/tc/html

Method: GET

Path Parameters

No parameters envisaged

Query Parameters

No parameters envisaged

Request Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by initialisation (UUID)

Request Body

No parameters envisaged

Response Code

HTTP Response Code 200

Response Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by caller or system (UUID)



Response Body

The service responds with HTML containing the Automatic Billing Terms and Conditions.

HTTP Error Codes

Below is the list of error messages and the associated response codes

HTTP Response Code	Error code	Description
404	FILE_NOT_FOUND	file not found
500	GENERIC_ERROR	generic error

Retrieving Billing Provider List

Through the service in question, it will be possible to retrieve the list of Providers integrated with the FA platform during the Onboarding phase of a Merchant through the Acquirer and select the Provider indicated by the Merchant, i.e., the Provider with which the Merchant signed the contract.

Path: /fa/provider/list

Method: GET

Path Parameters

No parameters envisaged

Query Parameters

No parameters envisaged

Request Body

No parameters envisaged

Response Code

HTTP Response Code 200

Response Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by caller or system (UUID)

Response Body

field	format	Mandatory	Description
providerList	Alphanumeric	YES	List of providers participating in the service: 1. providerID 2. providerDesc

HTTP Error Codes

Below is the list of error messages and the associated response codes

HTTP Response Code	Error code	Description
401	TOKEN_NOT_VALID	invalid token
500	GENERIC_ERROR	error retrieving user profile

T&C acceptance, sending Merchant data and saving on the FA Platform

Path: /fa/onboarding/merchant/{vatNumber}

Method: PUT

Path Parameters

Field	Format	Description
vatNumber	Alphanumeric	VAT number of the Merchant

Query Parameters

No parameters envisaged

Request Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by initialisation (UUID)



Authorisation	String	YES	Bearer <token> (JWT format)
----------------------	--------	-----	-----------------------------

Request Body

Field	Format	Mandatory	Description
timestampTC	Timestamp	YES	T&C timestamp acceptance. FORMAT ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX
token	Numeric	YES	authentication token between the portal and FA Platform
fiscalCode	Alphanumeric	NO	id of the natural person associated with the merchant that corresponds to the tax code
acquirerMerchantId	Alphanumeric	YES	Merchant ID separated from the Acquirer
providerID	Alphanumeric	YES	Unique ID of the Billing Provider where the Merchant has integrated with the platform

Response Code

HTTP Response Code 200

Response Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by caller or system (UUID)

Response Body

field	format	Mandatory	Description
vatNumber	Alphanumeric	YES	VAT number of the Merchant

HTTP Error Codes

Below is the list of error messages and the associated response codes

HTTP Response Code	Error code	Description
--------------------	------------	-------------

400	INVALID_DATE	incorrect date value or format
401	TOKEN_NOT_VALID	invalid token
500	GENERIC_ERROR	error retrieving user profile
400	INVALID_PIVA	Invalid VAT ID

Appendix 1 - PGP Public Key

For any problems related to the use of the public key and for the issuance of specifications and/or updates relating to the public key to be used to encrypt the file, you must contact the responsible office delegated by PagoPa (ref. SIA OPE Innovative Payments - sistemisti_bigdata@sia.eu)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

```
mQENBF6QNPABCAC3R3mV17UnvyiBIHssvXmYlHgS8dMDnqkwTNTw+7qt4cASzlwd
uaX4MvltwtYRt5oMMFKdAjVmDJrVZu0xpdoklet/LJX/3NhZTsJNnP/vckNc2QOt
NhfcJ5lrsBoNTCUL25VJicM5KQeqCGIPF6gcSKVGkvTwjgRctIL85ua7syDM9pU6
3PhTz8mpN3PTnzNTOPPK3GxMg7NI5BcHrNb7gA/SiNZpuBZ4BaEIIOCIiAhHE+5j
Elv8mWQiiRXohJUH3+R7nkU96rKbXk8/pN5Ey/SS2r/jb+xoJvh/knCSHNndY72q
DdnEj6/hqXwk4axx3RmhiNi3ywYltpMKHSFtABEBAAAG0HnJ0ZGJhdGNoVEkgPHJO
ZGJhdGNoVElAc2lHmVlPokBPwQTAQIAKQIbAwcLCQgHAwIBBhUIAgkKCwQWAgMB
Ah4BAheABQJexNWjBQkNkwezAAoJEOYoxTAGG4FpxZ4H/AkE2IzuIHE8pnVp3p2
JtmE78k/O8VC33jfoE9sDyUyFEi8CZqAp1BA+B8i0dv6/ccP1SfXs79QdyFyfU
JtjcrXgwbVmiilkHkt38/5oSiSzlC/OOEcyAuRvEthZFeXfDHS+/UIJ2BuTpmwNf
+pG4gAEjTRnzve3+TimUZVIMEnWmL2lJzk7romiHHGs6zMA97NcFxb/gbDk3AF/H
uplUoSgUWlwiYx3D3TyAfNWmZBSe8fJ/gWRLxpGYfG+Ckgul02u6N3ZL/htFvUMGP
d/ydHLaJR4SHSpMabJtyVrEMoRblapDINWykeMDxIvDW7sLFuFo8aLKzRwoEPahW
/T+JATKEEWECACMFAl6QNPACGwMHCwkIBWMCAYVCAIJCgsEFgIDAQIeAQIXgAAK
CRDmKMUwIBuBaS4vB/4lMttoQoMNXklqC78Qq9flpMZNohNdyOIP4rPex5mnMsMi
wQ6hiFZTjdPismMZOX/bxWwF6lJdI2tbkUBPnblsCMpasWIEy0RMCnIwjJonFqn
VflziiHXCShGfN25SdcIltFeZ8iG1yP7eMG7reInfoH3RF9wlySUu6h45Bj4jdc
mfERQikWa4oOmoCVOP350yF0FtLY8Dt+jLRv9lBnFoyYWuCElZ0knMI5yBbs+MI7
yGo5bl4xD+LcYsklmhQ7C42Bh/IVDWXAvGX7EC1s0QT2wDuEIG+tdqi+odMe/DWP5
i3ISvPCTWZ7y3wQMChsSIPTPcwthzCLGIkkoee5vuQENBF7E3H4BCADEwPaEMNsJ
28jQKJvxeqqautkXtjaSx8UJDWgZP+mUTQe/DAohqFXcnOUI5l+E+KfC4DMpOY3g
waPMrw6tUBB7Ee5V4Ym5yAlIqXK+fzi+ImHn9dqsng48LLx6Q1S9l8xsui+yxZo0
ifG36coQOYI2ATp9DPwTOdBRm8NCgJzc1VXMUqUxmmJ9Zl7sevUvFeLVURXnMIwe
UbFsGwJH3XX2vM3qJBMPKq0QqxZg7AsnVftxgStgaVZRbNg0A2lItZHpcZu12tz8
xMZyJlZ3GJHnWGM+sbZy/oi9psTffhJLVzqtLYU5X82+YLn9WGTGJ4VYPsOX7BQl
iMLQTVwA/AthABEBAAAGJASUEGAEC8FAI7E3H4CGwwFCQ1eZwAACgkQ5ijFMCAb
gWmWJQf+MjXBwb8GSwp/ILglGFTXqKTL057Z/VjmuPpOJ3Y/blB/wgXgt4KXlsbM
YliHrhJSHK64+DPA6OZD0ZQPwGOLk+VDFw6T2iEDtbOSIQHBHkwyysNr9jn9mmo8
yM+xEguUoYcCnn+NdkH+zvJgDHUORNZOOWOIOWR5yeLRePTLMgG673Cp+MoWePay
FWM+hcdZDKwvU9Hzb5Laq7rXNGhdehPcZTHX+SvhjidOuvoKX/PbLa/9Hm+9F0vE
kVT7HK68ya8KZOJ3lmWzdsD9wVeQWRcYijTT7CeeGBqil3JN4+2jBw0/PLalQBew
v5HOUCTpJORE/SpdV6BcCbyldgtNtQ==
=b6IE
-----END PGP PUBLIC KEY BLOCK-----
```


Appendix 2 - File Transfer Mode

The CentroStella Platform provides an sFTP server on a public network, where the batch service installed on the systems of each Acquirer can deposit the files subject to the service in a specific folder.

The details of the Secure File Gateway (SFG) public Internet IPs are as follows:

Env	IP	Port	Protocol	User	Auth Type	Upload Dir	Details
UAT	193.203.229.79	20022	SFTP	"ABI user"	Key Auth (RSA – min. 2048 bit)	/Inbox/	SFG – Internet
PROD	185.91.56.144	8022	SFTP	"ABI user"	Key Auth (RSA – min. 2048 bit)	/Inbox/	SFG – Internet

Each subject accesses with authentication modes to be defined, through unique keys. For configuration and any problems related to sFTP access, please refer to the following contact person delegated by PagoPa:

➤ **MFT Specialist** Mauro Cauli OPE
 SIA S.P.A.
 Managed File Transfer
 Via Gonin, 36 - 20147 Milan, Italy P. +39 02.6084.4301
 M. +39 335.13.30.882

Alternatively, if the Acquirer already has active transmission channels that guarantee the same security standards with PagoPA's technological partner, these channels may be used, subject to the development of the batch service in question.

Appendix 3 - sFTP SIA access manual

[FTP access to SIA Spa systems on the Internet – v.1.0.pdf](#)



Appendix 4 - Salt recovery service

CentroStella PagoPA (internal Payment Manager component) provides a REST service

for the recovery of the SALT to be chained to the original pan before hashing.

For details on Authentication and Authorisation, refer to [Appendix 6](#) and [Appendix 7](#).

Below is the API detail:

Path: /rtd/payment-instrument-manager/salt

Method: GET

Path Parameters

No parameters envisaged

Query Parameters

No parameters envisaged

Request Header

Field	Type	Mandatory	Description
Ocp-Apim-Subscription-Key	Alphanumeric	YES	Subscription key associated with the issuer

Request Body

No parameters envisaged

Response Code

HTTP Response Code 200

Response Header

No parameters envisaged

Response Body

The service responds with the salt to be used during hashing.

HTTP Error Codes

Below is the list of error messages and the associated response codes

HTTP Response Code	Error code	Description
500	GENERIC_ERROR	generic error

Appendix 5 - Service for downloading HPANs registered in CentroStella

After appropriate verification of the presence of the file, which is generated daily by a batch process, the HPAN download service provides the possibility of downloading the file containing the pan hash. On the first call, the service redirects (http 302) to the download url.

The downloaded file will be in csv format (the estimated size for a file containing 10 million HPANs is about 300 MB).

The file is produced daily and is available from 2:00 am. Specifically, the file of day T contains all the payment instruments participating in CentroStella services registered by 23:59:59 on T-1.

For details on Authentication and Authorisation, refer to [Appendix 6](#) and [Appendix 7](#).

Below is the API detail:

Path: /rtd/payment-instrument-manager/hashed-pans

Method: GET

Path Parameters

No parameters envisaged

Query Parameters

No parameters envisaged

Request Header

Field	Type	Mandatory	Description
Ocp-Apim-Subscription-Key	Alphanumeric	YES	Subscription key associated with the issuer



Request Body

No parameters envisaged

Response Code

HTTP Response Code 302 (FOUND).

Response Header

Field	Type	Mandatory	Description
x-request-id	String	NO	Request ID, unique identifier determined by caller or system (UUID)

Response Body

The service responds with a redirect to the link to download the csv file containing the hash of the PANs registered for the BPD and FA program.

HTTP Error Codes

Below is the list of error messages and the associated response codes

HTTP Response Code	Error code	Description
404	FILE_NOT_FOUND	file not found
500	GENERIC_ERROR	generic error

Appendix 6 - Acquirer Services Authentication

The interactions for Acquirer batch services use a mutual authentication mechanism on TLS 1.2 protocol, through the exchange of public certificates, issued by a CA (certifying authority), used for verification by both actors with respect to the keys in their possession. For this mechanism to be applicable, the following is therefore necessary:

- the Client must be configured to send requests over TLS 1.2 protocol, indicating a store containing the chain of certificates necessary to verify the reliability of the server on which the request is made; in addition, a store containing at least the private and public key with which the client authenticates with the



machine contacted.

- the API must be configured to accept requests over TLS 1.2 protocol, it must be configured to use a collection of keys on which to apply certificate verification, it must be configured to provide a public certificate, used by the Client for the authentication of the machine to which the request is directed.

To generate the Certificate Signed Request it is necessary to use the [client-certificate.cnf](#) configuration template (suitably reconfigured with the information of the specific Acquirer). The command to invoke for generating the csr and its private key (using OpenSSL) is as follows:

```
openssl req -new -config client-certificate.cnf -keyout client-certificate.key  
-out client-certificate.csr
```

To enable the authentication process, certificates related to CAs in ".cer" format must be provided to the API publisher (since they must contain only the public key, the password is not mandatory, otherwise it must also be provided).

Client certificates must be provided to the Publisher API in ".pfx" format (containing only the public key), together with the relative password. The command to invoke for generating pfx from the client certificate (using OpenSSL) is as follows:

```
openssl pkcs12 -export -in client-certificate-signed.pem -nokeys -out public-cert.pfx
```

N.B: for tests in the SIT environment, the client certificate can be self-signed, and must be provided to the API publisher in ".pfx" format, while for higher environments it must be signed by the PagoPA internal CA, and it is not necessary to share it with the API Publisher. Consequently, the file containing the CA's public key should only be provided by the Acquirers in the SIT environment. In higher environments the PagoPA CA certificate will already be preconfigured. If it is necessary to obtain a certificate with a signature valid for environments above SIT, send the .csr to be signed to security@pagopa.it.

The APIs will be presented and configured to enable the mutual authentication process based on a given certificate. In the case of services used by Acquirers, a dedicated policy is introduced to allow the authentication process through multiple certificates, to allow the use of certificates for the Acquirers.

Appendix 7- Acquirer Services Authorisation

Issuer system developers who need to use the published APIs must include a valid subscription key in HTTP requests when making calls to those APIs. Otherwise, the calls are immediately rejected by the API Management gateway and, as a result, are not forwarded to back-end services.



To obtain a subscription key for API access, a subscription is required. A subscription is essentially a container for a pair of subscription keys. Developers who need to use published APIs can obtain the subscriptions in two ways (depending on how they were configured):

- with the approval of API publishers;
- without the need for API publisher approval.

API publishers can also create subscriptions directly for API consumers.



After subscribing, the client can invoke the services (for which it has subscribed) by entering the field **Ocp-Apim-Subscription-Key** as the parameter of the request header. The value of the field must match the code obtained after registering with the developer portal Azure.

Below are the steps necessary to register to test the behaviour of the services;
Access the dev address dedicated to developers (see appendix 8)



1. After clicking on the yellow button, you will be directed to the registration page where the credentials for the account configuration must be entered



2. After completing the credential entry process, we will receive via email the necessary configurations to complete the verification via a link.

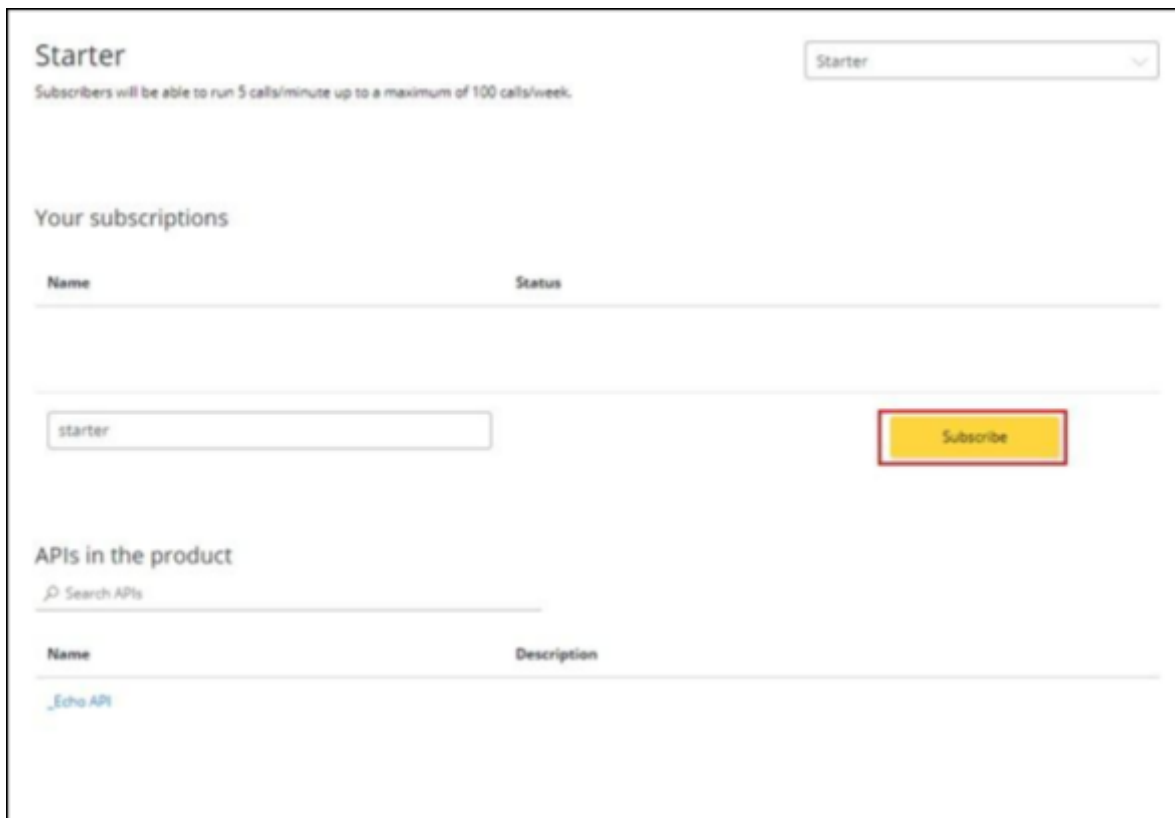
3. After clicking on the link contained in the email, you will be redirected to the login page where you will have to authenticate with the created user. To create the subscription and its keys you must select the "Products" option.



4. At this stage, you must select the subscription type RTD_API_PRODUCT to access the services displayed for the Acquirers



5. Enter a name and select the Subscribe option.



6. The outcome of the subscription will be visible under "Profile" in the menu.



Appendix 8 - Environments

Environment	IP address	API URL Gateway	Developer Portal URL
SIT	104.40.204.96	https://bpd-dev.azure-api.net	https://bpd-dev.developer.azure-api.net
UAT	20.54.178.216	https://test.cstar.pagopa.it	https://developer-test.cstar.pagopa.it
PROD	51.137.18.218	https://prod.cstar.pagopa.it	https://developer.cstar.pagopa.it

Appendix 9 - PGP Production Public Key

For any problems related to the use of the public key and for the issuance of specifications and/or updates relating to the public key to be used to encrypt the file, you must contact the responsible office delegated by PagoPa (ref. SIA OPE Innovative Payments - sistemisti_bigdata@sia.eu)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

```
mQENBF+IZlWBCADQ4KTeUitBNzQScZMdJEP7GLmqvU0GCN7rrWG6qdhK7OvzQt/q
b2lRntqvilciGii59GfgsgyMORlpr5mkvPOv7noIKY5xW7r0cOylBhKtX+xeFVbL
Ozu3YhqjSycinunTH8zbiSSTIE6p/+SzCyV23IXwP0yjHvUskCeIdnDM+ceJxQc
jQ46sBQ4vXJtA3TkaTwyBMrCft0TW84mecdDtTw2b4zt0FcQtnpG0B8ZanFO+cqH
d9Z6qLhTcHQzMC8ISKljKagPrWLJPfGuHzRh0YDIXS3p2alqirfuHVDctN1dTqcV
JhP39qf6WOKJULEV8jFvWRR2QPkLzAw5gcQ/ABEBAAG0HnJ0ZGJjaHBhYmDEgPHJ0
ZGJjaHBhYmDFac2lhLmVlPokBOQQTAKIAIwUCX4hmXAlbAwcLCQgHawIBBhUIAgkK
CwQWAgMBAh4BAheAAAJEFpOgVpChNKWddIIAJfx2Oh5zym2PLk8M40DGvcaVvyD
ZLsatwCCXknmD9xxOK7fg3084nSvYfdXS8+UXFZvO4FZolVzPMpZC/ODIDWOF4MC
4F7wMSGaia5Wf6Tp+KOGInDzaWzBlU9K5YspHG/ee5h0ioMBTcwq1Q0ck1Bbn35j
t8uBXlID47Ea/F0F3AIME5OKt+JC8t3RYN4DuTwEnhUL6TeVoVkiOWrvOIHqKD
4BCeB/awllihbl8e3CLC0QNQqrH4CmiJDxjDv/Ozf9ldRqIXg34rtpdrgZnzC8Uo
ubyzq8dwkbl0hErFkpcxBSPhehn2bVER5zbleu5gv6Jbyzbglj6ugUr9V9G5AQOE
```



```
X4hm3gEIALoyR2/IQfdSVvkiP+HfVHdv2Vp1z98C+BhflPuQ2kknBUXZaYMr5IB/  
NYycLs+QFbxHtkA50qOAGzY/gjLv/+YrI9J0Wu5xIkZ1HCNWlPnMQwKWt8nh1vYo  
EslweSZVRhDeCgwHzDDwdo/Xa/xlzdAqiMyxoS8yJVCwN11iyvNOgbwQUXFHe0BR  
AIlBKKwibQi8DNI+9NU2gzZyiLh6WsAQQLVoIF3cS9sjhWcl+OB0NsffJ+oqkIb2  
/wgpDwtUHclcTKGcB5HfueXCYNABs+O/TO4W5w42UpG52s5tm9Mvaz8xbZW2ipi4  
lyjeaPwm39aV/qTqkhwwlk3YpQH4BCUAEQEAAYkCPgQYAQIACQUcX4hm3gIbAgEp  
CRBaToFaQoTslsBdIAQZAQIABgUCX4hm3gAKCRAe9FqPx6cAANZAB/0eU9DXf6+s  
Q6FeanXhDjzC1BP2qLtrED1hmIj8IrbAtk4AGyeTDhI5f1XiOuEqy9ATR9LOu4ap  
97/3ritsX6J49gJEtCUYhBAEcJtRXHoU44PnyxYj1xn/kQqSd6iq/xtUDqSJrpxa  
q42x/ISUmBhNZTa1JFPNWE4aedph9eiWIN/gT8/9m0cA/ZXfZuOKbq8EeTTJiSsd  
Jq5blTitdbclREc781L2gCR2KHbunLXNSFYBAco/Pn6DR8PPmvKIPsKDVMLHO3u2  
h/nrMmUMZ8t9u4TxMsX/V6DWdPVnmv8YWOFQdQGGMOlpJfEArp4j9+yPq7w9yMBD  
uZcQyI6V91aQz8IH/RoYJOeVBMXbjRwtwcFIJIECH7LuGmVatq9x1ApqFnevxFb8  
bZHltBgiPIChVrK4yttePP3/mv6ZzWSMhvDO9vVZuTZS1X9uAkk9rSBUnAFg0uj5  
jF2sNw5x4UcP3qWlffY0DH5XEJhIOXfcAs/oIGIkJaK6PkioephcX5QlprKzUZBO  
W0/XNa4R2IPVUdqIUdoBQd+7WzMoqfH6/30L+zw3mXVmaxgh0YLCdDYZapkeZ/Fn  
nHTvJst7UUr0y/JwRCHL7Jc7R2lppkcRkhMoltbNF4JwktGog4wDDbdBDS3wrg  
wRHxmjkRkZFGinR9pwteFVmh+jVgZu4Lx5GBBQc=  
=fKwP  
-----END PGP PUBLIC KEY BLOCK-----
```