Registro Transazioni Digitali

Digital Transactions Register

Acquirer Interface Agreement

Version: 3.0

Status: Final

Change History

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

Date	Author	Change History
28/02/2020	Stefano Menotti	First Draft version
28/04/2020	Luca Somaruga	Update Timestamp format
21/05/2020	Debora Arena	Update: - Chapter "Scope" adding constraints on enrolled HashPan. - Paragraph "The process of integration of the Acquirer and CentroStella": adding constraints on enrolled HashPan. Update: - "Appendix 2 - File transfer": the batch service will send the files to the platform's SFTP
22/05/2020	Stefano Menotti	Update: new document version
27/06/2020	Debora Arena	Update: - Standard PagoPa file
30/07/2020	Rodolfo Viti	Update: - Standard PagoPa file - Appendix 4 - Salt recovery service - Appendix 5 - HPAN's download service - Appendix 6 - Acquirer Services Authentication Added: - Appendix 7 - Acquirer's Authorization - Appendix 8 - Environments
02/09/2020	Rodolfo Viti	Update:

		- Standard PagoPa file (fields length)
02/10/2020	Denisa Braho	Added: - paragraph "Happy flow" containing the process happy flow and related design Update: - "tipo_circuito" field (the "00-PagoBancomat" circuit will be managed exclusively by Bancomat)

Table of Contents

Change History 2

Table of Contents 4

Introduction and purpose of the document 5

Normative references 5

Privacy and data processing 5

Introduction and scope of the initiative 5

Objective 6

Happy Flow 7

Scope 8

The process of transmitting transactions to CentroStella 9

The process of integration of the Acquirer and CentroStella PagoPA 10

PagoPA Standard File 11

Check HPAN batch service 16

Appendix 1 - Public Key PGP 18

Appendix 2 - File transfer 19

Appendix 3 - Manual sFTP SIA 20

Appendix 4 - SALT recovery Service 20

Appendix 5 - HPAN's Download 22

Appendix 6 - Acquirer's Authentication 24

Appendix 7 - Acquirer's Authorization 26

Appendix 8 - Environment 30

Introduction and purpose of the document

The purpose of this document is to describe the application solution, in all its interfaces and the various flows of events in input, output and the data exchange methods, as well as the High Level executive architecture, with particular reference to the interfaces exposed from the Acquirers to PagoPa SpA (Centro Stella).

Normative references

The regulatory reference of the service is the D.L. 26/10/19 n. 124 converted with the conversion law of 19 December 2019, n. 157 published in the "Gazzetta Ufficiale" No. 301 of 24-12-2019, and in particular in Article 21:

Art. 21: Certificazioni fiscali e pagamenti elettronici

1. *All'articolo 5 del decreto legislativo del 7 marzo 2005, n. 82, dopo il ((comma 2))-quinquies sono aggiunti i seguenti::* ***«2-sexies. La piattaforma tecnologica di cui al comma 2 può' essere utilizzata anche per facilitare e automatizzare, attraverso i pagamenti elettronici, i processi di certificazione fiscale tra soggetti privati, tra cui la fatturazione elettronica e*** *la memorizzazione e trasmissione dei dati dei corrispettivi giornalieri di cui agli articoli 1 e 2 del decreto legislativo 5 agosto 2015, n. 127.2-septies. Con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, di concerto con il Ministro dell'economia e delle finanze, sono definite le regole tecniche di funzionamento della piattaforma tecnologica e dei processi di cui al comma 2-sexies.».*

Privacy and data processing

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

Introduction and scope of the initiative

The main goal of this project is to create a technological infrastructure that will enable new services for citizens and businesses, focusing on the digitization of the payment system by promoting the use of cards and other electronic payment instruments for the payments via POS in stores/shops.

The pillar of the new infrastructure is the interaction with the Acquirers operating in the Italian territory.

PagoPa/CentroStella has to manage the data received in compliance with the GDPR requirements; in particular, it is not allowed to track the single transaction and to retrieve personal data related to the citizen and/or the transaction.

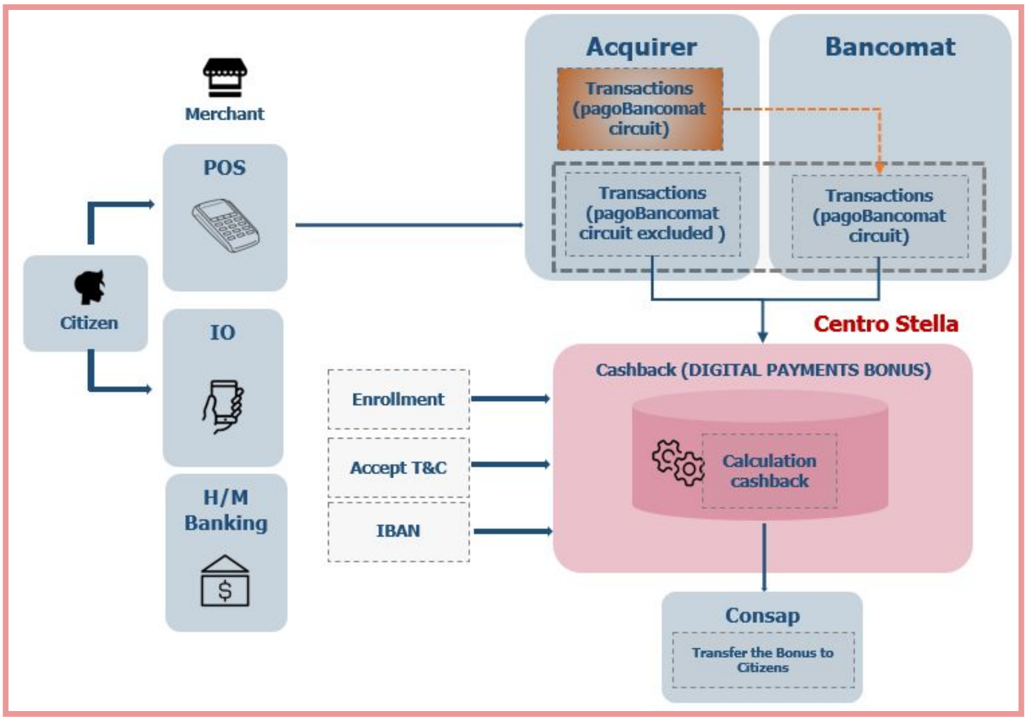
The macro components of the initiative are the following:

<table>
<tr><td colspan="2"><b>REGISTRO TRANSAZIONI DIGITALI (RTD)</b>
<b>DIGITAL TRANSACTION REGISTER</b>
It aggregates transactions made by individuals and businesses via POS in the national territory.
A unique Register that enables the creation of incentive solutions for electronic invoicing, welfare and automatization processes.</td></tr>
<tr><td><b>FATTURAZIONE AUTOMATICA (FA)</b>
<b>AUTOMATED INVOICING</b>
It relies on the “Registro Transazioni Digitali” and consists in the <i>automatic</i> issue of electronic invoices.</td><td><b>BONUS PAGAMENTI DIGITALI (BPD)</b>
<b>CASHBACK</b>
It relies on the “Registro Transazioni Digitali” in order to provide bonuses to citizens who make transactions using electronic payment instruments.</td></tr>
</table>

Objective

“Registro Transazioni Digitali” is a platform that aims to maintain a unique integration with Acquirers operating in the Italian territory. The main objectives of the project are:

- Encouraging payments by cards or any other electronic payment instruments in order to reduce the use of cash, by creating rewarding conditions for citizens, including the generation of *cumulative* cashbacks in case of transactions made with different payment instruments.
- Giving a boost to the use of electronic invoices by small businesses by simplifying the data exchange system between all the parties involved in the process.


Merchant
POS
Citizen
IO
H/M Banking
Acquirer
Transactions (pagoBancomat circuit)
Transactions (pagoBancomat circuit excluded)
Bancomat
Transactions (pagoBancomat circuit)
Centro Stella
Enrollment
Accept T&C
IBAN
Cashback (DIGITAL PAYMENTS BONUS)
Calculation cashback
Consap
Transfer the Bonus to Citizens

Happy Flow

The following Happy Flow summarizes the functional solution proposed for the “Bonus Pagamenti Digitali” project:

a. The Citizen saves in a secure way the data related to his payment instrument on CentroStella (via APP IO or the Home Mobile Banking website)

b. The Citizen makes a payment **via POS in a shop/store in the Italian territory**

c. The Acquirer sends to CentroStella the information related to the payment made

    i. The Acquirers will send to Bancomat (not directly to CentroStella) the transactions within the PagoBancomat network, while all the other transactions on other payment circuits (es. Visa, Mastercard etc) will be sent to CentroStella

    ii. Bancomat, will send to CentroStella all the transactions of the PagoBancomat network, including the ones received from the Acquirers

d. CentroStella will assign points (cashback) to each transaction received from Bancomat and Acquirers
e. The cashback of each Citizen will be accumulated until the end of the award period
f. The Citizen must insert the IBAN of his account (on APP IO or H/M Banking) in order to receive his reimbursement from Consap.

Scope

The payment transactions will generate a cashback if made through a POS of a store located in the Italian national territory and through the following payment instruments:

- Debit cards on international circuits and ATMs
- 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 connected to bank transfers or other settlement systems

Only transactions in EUR will be processed.

In order to guarantee the correct functioning of the service, Acquirers must send to PagoPA also transactions that include any *on-us* modalities (including reversal payments).

The following transactions are therefore excluded:

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

The process allows PagoPA to receive *only* the transactions made with payment instruments that have been *enrolled* in the Centro Stella's services (BPD/FA).

The process of transmitting transactions to CentroStella

The process of transmitting all the transactions of interest to CentroStella consists of the following stages:

a. The CentroStella Platform produces a file containing the hashed PANs of the cards which have been enrolled in the Centro Stella's services.
b. The Acquirer consolidates the required data related to the transactions in scope
c. The Acquirer produces a file in .csv format (detailed in the paragraph "PagoPA Standard File") and deposits it in a folder on which the batch is polling.
d. The file's arrival in the destination folder is the trigger that causes the start of the batch elaboration process.
e. The installed batch invokes the service exposed by CentroStella. The invoke will generate a *one-shot link* that will be temporarily active in order to allow the download of the file that contains all the HPANs enrolled in the CentroStella's services.
f. The Batch calls the service exposed by CentroStella in order to obtain the *constant hashing key*. The key is necessary to hash the PANs contained in the transactions file.
g. The Batch reads both input files (HPAN list and transactions file) and for each line of the transactions file:
    i. Hashes the PAN
    ii. Determines whether the transaction should be processed or not.
h. The Batch, after the conclusion of the step described in the previous point, completes the writing procedure of the output file, and deletes all the data received in input.
i. The Batch performs the PGP encryption of the output file.
    i. In Appendix 2 can be found the public key that should be used to encrypt the output file.
j. The Batch sends the final output file to CentroStella sFTP
    i. For further details, please refer to Appendix 3.
k. CentroStella deletes all the input files.

The process of integration of the Acquirer and CentroStella PagoPA

Acquirers who have signed an agreement with PagoPA S.p.A will generate a daily transactions file, but only the transactions made with HPANs registered on the Centro Stella's services will be sent to the platform.

This check will be guaranteed by the batch service provided by PagoPA *(an open source code in order to facilitate the integration and minimize effort)* that will be installed on the Acquirer's systems. For more details see the paragraph "Check HPAN batch service"

It will be possible for the Acquirers to use one or more integration methods and for each method, they can send one or more daily files to CentroStella in order to cover the entire set of transactions.

PagoPA SpA will require the Acquirers to send one or more batch files in the "Standard PagoPA" format. PagoPA SpA will provide the required file structure that contemplates the minimum subset of data, described in the following paragraph. The objective is to minimize the technological effort required for the Acquirers and at the same time, guaranteeing compliance with the PCI regulations.

PagoPA SpA (CentroStella) will be responsible for managing the information received from the Acquirers in accordance with the current legislation and saving only the minimum subset of anonymized data necessary for the correct functioning of the Platform. The platform will delete any other data related to transactions, which are made with not registered cards.

The payment instrument's information will be saved with an irreversible cryptographic hash function.

The integration of the Acquirers with the CentroStella consists into two main stages:

- PagoPa Standard File
- Batch Service for the enrolled HPANs

The following paragraphs provide the details of the phases listed above.

PagoPA Standard File

The details of the PagoPA Standard Flow are described below:

The file naming convention is as follows:

- **[service]. [ABI]. [file type]. [date]. [time]. [nnn] .csv**

in particular:

- service: 'CSTAR' (5 alphanumeric digits)
- ABI: ABI of the Acquirer sending the file (5 digit numeric)
- file type: the file typology (6 alphanumeric digits)
- nnn: progressive file (3 numeric digits)

Field	Format	Note
service	Alphanumeric - 5 char	fixed value “CSTAR”
ABI	Alphanumeric - 5 char	ABI code of the sender
file type	Alphanumeric - 6 char	file typology Valore fisso a TRNLOG
[date].[time]	YYYYMMDD.HHMISS	timestamp
nnn	Alphanumeric - 3 char	Progressive number of the file (es. 001)

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

The details of the “PagoPA Standard File”:

Field	Type	Obligatory	Note
codice_acquirer	Alphanumeric - max 20 char	YES	ABI Code of the Acquirer

tipo_operazione	Alphanumeric - regexp [0-9]{2}	YES	Transaction type: 00 - payment 01 - reversal payment 02 - ApplePay payment 03 - GooglePay payment xx - future uses Some Acquirers are able to provide only the 00 and 01 codes.
tipo_circuito	Alphanumeric - regexp [0-9]{2}	YES	Circuit: 00 – Pagobancomat - These transactions will be sent exclusively from Bancomat. 01 - Visa 02 - Mastercard 03 - Amex 04 - JCB 05 - UnionPay 06 - Diners 07 - Codice PostePay 08 - BancomatPay 09 - SatisPay 10 - private network (onus, owen) xx - future uses
hash_pan	Alphanumeric – max 64 char	YES	Hash of the PAN of the payment instrument used. In the case of a

			non-card based circuit, it represents the unique identifier of the private payment instrument, which the user can register through the APP IO or touch point of the Issuer.
date_time	DateFormat *FORMAT ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX*	YES	Timestamp of the payment transaction. The details regarding the *seconds* are not always available for all transactions. In this case, the detail will be padded with all '0'
id_trx_acquirer	Alphanumeric – max 255 char	YES	Acquirer’s unique identifier of the transaction. The field contains the ARN code. If the information is not available, the field can contain other codes that represent the Acquirer’s unique identifier of the single transaction
id_trx_issuer	Alphanumeric – max 255 char	NO	Authorization code issued by the Issuer (eg: AuthCode)
correlation_id	Alphanumeric – max 255 char	NO	Correlation identifier between the payment

			transaction and the reversal payment.. In some cases, the data cannot be provided from the Acquirer.
total_amount	Number	YES	Amount in absolute value: the sign is deducted 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	Acquirer Identifier In case of payment made with credit cards represents the acquirer id value transmitted to international circuits. In particular: - Visa / Mastercard circuit: *acquirer_id* - It corresponds to the *codice_sia_abi* field in case of PagoBancomat - In other cases, the field will be enhanced with

			a fixed data depending on the Acquirer
merchant_id	Alphanumeric – max 255 char	YES	Unique identifier of the physical store . - In the Pagobancomat circuit it can correspond to the field: *esercente*
terminal_id	Alphanumeric – max 255 char	YES	Terminal / POS (Point of Sale) Identifier - Pagobancomat: corresponds to the field: *stabilimento cassa* - Visa/Mastercard: *terminal_id*
bank_identification_number (BIN)	Alphanumeric – regexp [0-9]{6}|[0-9]{8}	YES	Code containing the first 6 or 8 digits of the payment instrument. - Pagobancomat: it corresponds to the field: *codice_abi*
MCC	Alphanumeric – max 5 char	YES	- Merchant Category Code.

Check HPAN batch service

CentroStella will develop and install the service, while the maintenance of the service or any changes will be in charge of the Acquirer.
PagoPa will provide the source code in *opensource* (published on public repositories in order to facilitate integration and minimize the effort).

The artifact consists in an executable jar produced with *spring-boot*, therefore all the dependencies of the project are available in the jar, including the categories that contain the business logic.
Therefore, the artifact is completely autonomous and can be used on any device that has a JVM.
For the installation and execution of the batch you need:

- Java 1.8+
- Batch-transaction-filter.jar artifact

Regarding the execution parameters and commands, refer to the indications in the README contained in the public repository that can be reached via the link:

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

Minimum requirements
The minimum requirements for the execution of the batch described above are the following:
Software:

- JVM 1.8+

Hardware:

- CPU:

- Architecture:	x86_64
- CPU op-mode(s):	32-bit, 64-bit
- CPU(s):	4
- CPU MHz:	2992.966

- RAM: 4 GB
- HD: depends on the size of the transaction file. The size of the file containing the hashed PANs, which has a size that is around 300 MB (in pgp format), must be added to the previous file

Execution status

The batch service also includes the management of cases of error (blocking errors) and the case of the successful execution of the procedure.

The process will be conditioned by the configuration of the ***deleteLocal*** parameter which, if active, will force the cancellation of all processed files at the end of the execution. If otherwise configured, the process will proceed with the archiving of the processed files, including the file containing the list of PANs and the transaction’s files.

In case of a correct processing of the records, the PAN’s file will be removed, including all the temporary files generated before the final transmission of the output file. The file containing the transactions will be stored in a dedicated directory.

It will also be possible to configure parameters related to errors occurring during the processing of single records, such as a tolerance margin with respect to the number of lines for which an error has been found. This check can be implemented using the ***skipLimit*** parameter.
If the file will be processed without exceeding the configured threshold value set (skipLimit), a success will be reported indicating also the presence of some errors, which can eventually be managed.

Appendix 1 - Public Key PGP

For any problems or updates related to the encryption public key, contact the following team: **ref. SIA OPE Innovative Payments - sistemisti_bigdata @ sia.eu**

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

mQENBF6QNPABCAC3R3mV17UnvyiBIHssvXmYIhgS8dMDnqkwTNTw+7qt4cASzlwd
uaX4MvItwtYRt5oMMFKdAjVmDJrVZu0xpdokIet/LJX/3NhZTsJNnP/vckNc2QOtNhfcJ5lrsBoNTCUL25VJicM5KQeqCGIPF6gcSKVGkv
TwjgRctIL85ua7syDM9pU6
3PhTz8mpN3PTnzNToPPK3GxMg7NI5BcHrNb7gA/SiNZpuBZ4BaElI0ClIAhHE+5j
E1v8mWQiiRXohJUH3+R7nkU96rKbxk8/pN5Ey/SS2r/jb+xoJvh/knCSHNndY72q
DdnEj6/hqXwk4axx3RmhiNi3ywY1tpMKHSFtABEBAAG0HnJ0ZGJhdGNoVEkgPHJ0
ZGJhdGNoVElAc2lhLmV1PokBPwQTAQIAKQIbAwcLCQgHAwIBBhUIAgkKCwQWAgMB
Ah4BAheABQJexNWjBQkNkwezAAoJEOYoxTAgG4FpxZ4H/AkE2IzuIHE8pnVpP3p2
JtmE78k/O8VC33jfoE9sDyIuYuFEi8CZqAp1BA+B8i0dv6/ccP1SfXs79QdyFyfU
JtjcrXgwbVmiilkHkt38/5oSISzlc/OOEcYAuRvEthZFeXfDHS+/UIJ2BuTpmwNf
+pG4gAEjTRnzve3+TimUZV1MEnWmL21Jzk7romiHHGs6zMA97NcFxb/gbDk3AF/H
uplUoSgUWIwiyxD3TyAfNWmZBSe8fJ/gWRlxpGYfG+Ckgul02u6N3ZL/ntFvUMGP
d/ydHLaJR4SHSpMabJtyVrEMoRbIaPDINWykeMDx1VDW7sLFuFo8aLKzRwoEPahW
/T+JATkEEwECACMFAl6QNPACGwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAK
CRDmKMUwIBuBaS4vB/41MttoQoMNxKlqC78Qq9flpMZNohNdyO1P4rPex5mnMsMi
wQQ6hIFZTjdPismMZOx/bxWwF61JdI2tbkUBPnblsCMpasWIEy0RMCnIwjJonFqn
VfIziiHXCSHGfN25Sdcl1tFEz8iG1yP7eMG7relNfoH3RF9wIySUu6h45Bj4jidc
mfERQikWa4oOmoCVOP350yF0FtLY8Dt+jLRv9lBnFoyYWuCElZ0knMl5yBbs+Ml7
yGo5bl4xD+LcYSklmhQ7C42Bh/lVDWXAvGX7EC1s0QT2wDuEIG+tqi+odMe/DWP5
i31SvPCTWZ7y3wQMChsS1PTPcwthzCLGIkkoee5vuQENBF7E3H4BCADEwPaEMNsJ
28jQKJvxeqqautkXtjaSx8UJDWgZP+mUTQe/DAohqFXcnOUI5l+E+KfC4DMpOY3g
waPMrw6tUBB7Ee5V4Ym5yALIqxK+fzi+ImHn9dqsng48LLx6Q1S9I8xsui+yxZo0
ifG36coQOYI2ATp9DPwTOdBRm8NCgJzc1VXMuqUxmmJ9Zl7sevUvFeLVURXnMIwe
UbFsGwJH3XX2vM3qJBMPKq0QqxZg7AsnVftxgStgaVZRbNg0A2IltZHpcZu12tz8
xMZYJ1z3GJHnWGm+sbZy/o19psTffhJLVzqtLYU5X82+YLni9WTGJ4VYPsOX7BQl
iMLQTVwA/AthABEBAAGJASUEGAECAA8FAl7E3H4CGwwFCQ1eZwAACgkQ5ijFMCAb
gWmWJQf+MjXBwb8GSwP/lLglGF1XqKTL057Z/VjmuPpOJ3Y/bIB/wgXgt4KXlsbM
YIiHrhJSHK64+DPA6OZD0ZQPwGOLk+VDfW6T2iEDtbOS1QHBHkwyysNr9jn9mmo8
yM+xEguUoYcCnn+NdkH+zvJgDHUORNZ0OwOIOWR5yeLRePTLMgG673Cp+MoWePAy
FWM+hcdZDKwvU9Hzb5Laq7rXNGhdehPcZTHX+SvhjidOuvoKX/PbLa/9Hm+9F0vE
kVT7HK68ya8KZOJ3lmWzdsD9wVeQWRcYijTT7CeeGBqil3JN4+2jbw0/PLalQBew
v5HOUCTpJORE/SpdV6BcCby1dgtNtQ==
=b61E
-----END PGP PUBLIC KEY BLOCK-----
```

Appendix 2 - File transfer

CentroStella provides a sFTP server on a public network, where the installed batch service can deposit the files in the specific folder. The details of the Internet public IPs of the SFG (Secure File Gateway are the following):

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 party involved can access through unique keys. For any configuration problem or any other problems related to the *accessing procedure* to sFTP, 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

Note that there can be used existing channels in case the Acquirer has already active transmission channels that guarantee the same safety standards as PagoPA's technological partner.

Appendix 3 - Manual sFTP SIA

Accesso FTP ai sistemi SIA Spa su Internet – v.1.0.pdf

Appendix 4 - SALT recovery Service

Centro Stella PagoPA (internal component of Payment Manager) provides a REST service for the recovery of the SALT that will be applied to the PAN before the hashing procedure. For details on Authentication and Authorization, refer to Appendix 6 and Appendix 7.

API's details

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

Path Parameters

No parameter

Query Parameters

No parameter

Request Header

Field	Type	Obligatory	Description
Ocp-Apim-Subscription-Key	Alphanumeric	YES	Subscription Key

Request Body

No parameter

Response Code

HTTP Response Code 200

Response Header

No parameter

Response Body

The service responds with the SALT to use in the hashing procedure.

HTTP Error Codes

Below is the list of error messages and associated response codes

HTTP Response Code	Error Code	Description
500	GENERIC_ERROR	generic error

Appendix 5 - HPAN's Download

The HPAN's download service starts after verifying that the HPAN's file, which is generated daily by a batch process, is available in the specified path. Upon the first call, the service redirects towards the *download url* (http 302).

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

The file will be produced daily and will be available starting at 02:00. The file of day T contains all the payment instruments enrolled to the CentroStella services registered in the day T-1 (until 23:59:59 of day T).

For details on Authentication and Authorization, refer to Appendix 6 e Appendix 7.

API's details:

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

Path Parameters

No parameter

Query Parameters

No parameter

Request Header

Field	Type	Obligatory	Description
Ocp-Apim-Subscription-Key	Alphanumeric	YES	Subscription Key

Request Body

No parameter

Response Code

HTTP Response Code 302 (FOUND).

Response Header

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

Response Body

The service responds with a redirect to the link that allows downloading the csv file containing the hashPANs.

HTTP Error Codes

Below is the list of error messages and associated response codes

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

Appendix 6 - Acquirer's Authentication

The interactions related to the batch services use a mutual authentication mechanism on the TLS 1.2 protocol, through the exchange of public certificates, issued by a CA (the certifying authority).

For this mechanism, it will therefore be necessary the following steps:

- The Client should be configured in order to send requests on the TLS 1.2 protocol, by indicating a store that should contain the *certificates*, which are necessary to verify the reliability of the server on which the request is made; moreover, the store must contain at least the private and the public key with which the client authenticates with the machine.

- The API must have a configuration that allows to:
    - accept requests on the TLS 1.2 protocol
    - use a collection of keys on which to apply certificate verification
    - provide a public certificate, used by the Client to authenticate the machine where the request is directed to.

For the generation of the "Certificate Signed Request" it is necessary to use the configuration template *client-certificate.cnf* (appropriately reconfigured with the information of the specific Acquirer). The command that needs to be invoked in order to generate the **csr** and its **private key** (using OpenSSL) is the following:

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

The authentication process can be performed if the certificates relating to the CAs are provided to the API publisher in the *".cer"* format (since they have to contain only the public key, the password is not mandatory, otherwise the password must also be provided).

Client certificates must be provided to the API Publisher in the *".pfx"* format (containing only the public key and password). The command that will generate the pfx from the client certificate (using OpenSSL) is the following:

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

Please note: In order to perform tests in the SIT environment, the client certificate can be *self-signed*, and must be sent to the API publisher in the ".pfx" format, while for higher environments must be signed by the PagoPA internal CA. In this case, it is not necessary to share the certificate with the API Publisher.
Acquirers have to provide the file containing the public key of the CA only in the SIT environment. In higher environments, the PagoPA CA certificate will be already preconfigured.

If there is any necessity to obtain a certificate with a valid signature for environments higher than SIT (UAT/PROD), the .csr must be sent to ***security@pagopa.it.***

The APIs will be configured in order to enable the mutual authentication process based on a given certificate. In case of services used by the Acquirers, a specific policy will be introduced. This policy will enable the authentication process via multiple certificates.

Appendix 7 - Acquirer’s Authorization

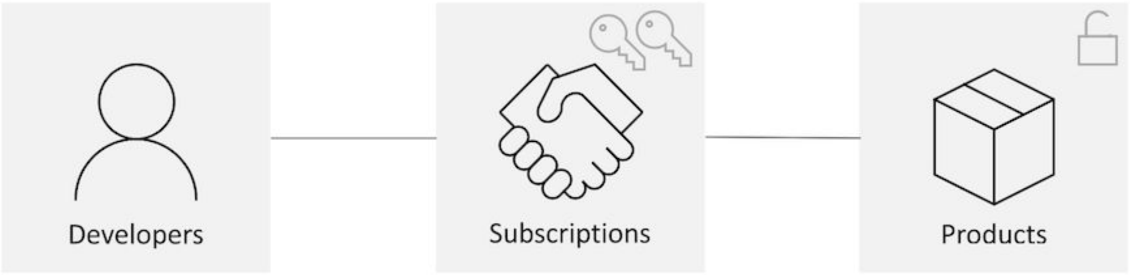
Developers who need to consume published APIs must include a valid subscription key in HTTP requests when making calls to those APIs. Otherwise, the API Management gateway will immediately reject the calls and, consequently, they will not be forwarded to the back-end services.

The subscription is necessary in order to obtain a subscription key to access the APIs.

The subscription is essentially a container of pairs of subscription keys. Developers who need to consume the published APIs can get a subscription in two different ways (depending on their configuration):

- with the approval of the APIs publisher;
- without an approval from the APIs publisher.

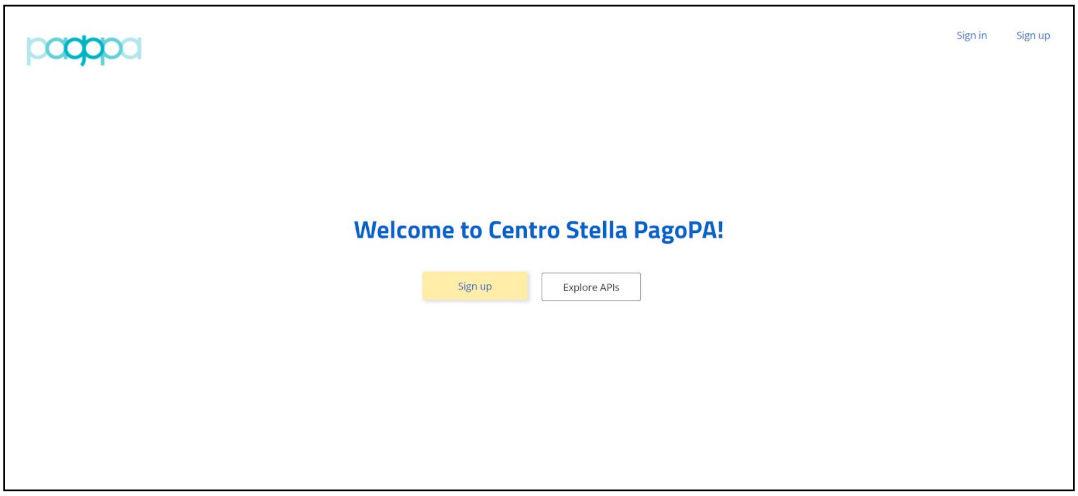
API publishers can also create subscriptions directly for the API consumers.



After subscribing, the Client can invoke the services (for which he has already subscribed) by entering the ***Ocp-Apim-Subscription-Key*** field as a parameter of the request header. The value of the field must match the code obtained after registering on the Azure Developer Portal.

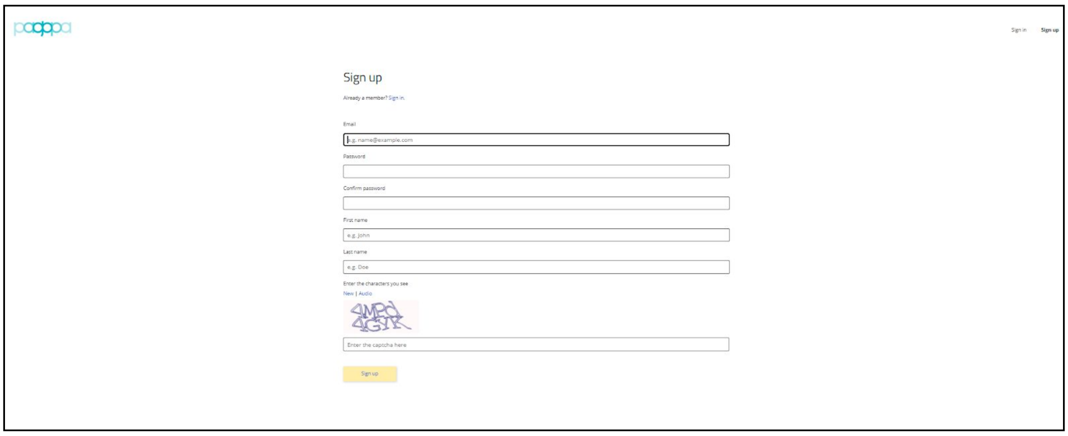
Below are described all the steps necessary to register:

1. Access the dev address dedicated to developers (see Appendix 8)



Welcome to Centro Stella PagoPA!

2. after clicking on the highlighted yellow button you will be directed to the registration page where all the necessary fields must be filled in.



Sign up

Already a member? Sign in.

Email

e.g. name@example.com

Password

Confirm password

First name

e.g. John

Last name

e.g. Doe

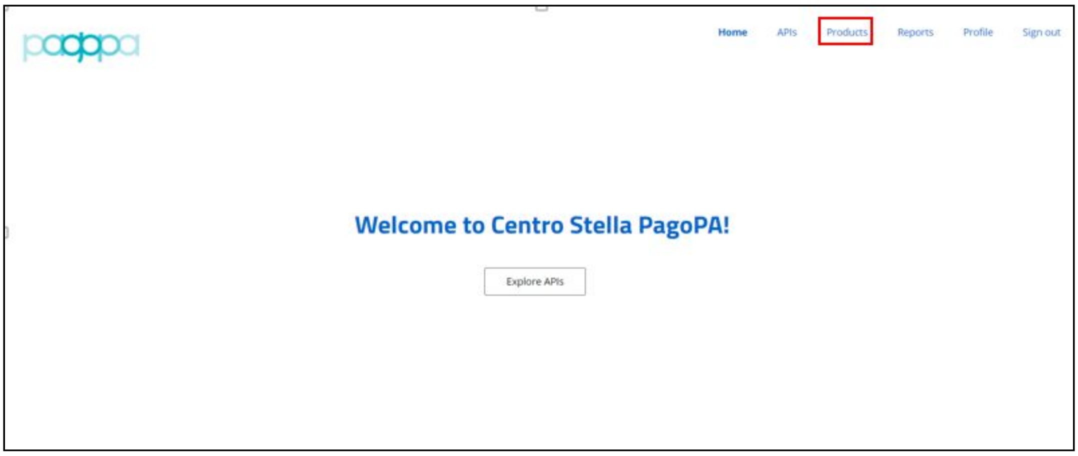
Enter the characters you see

New | Audio

Enter the captcha here

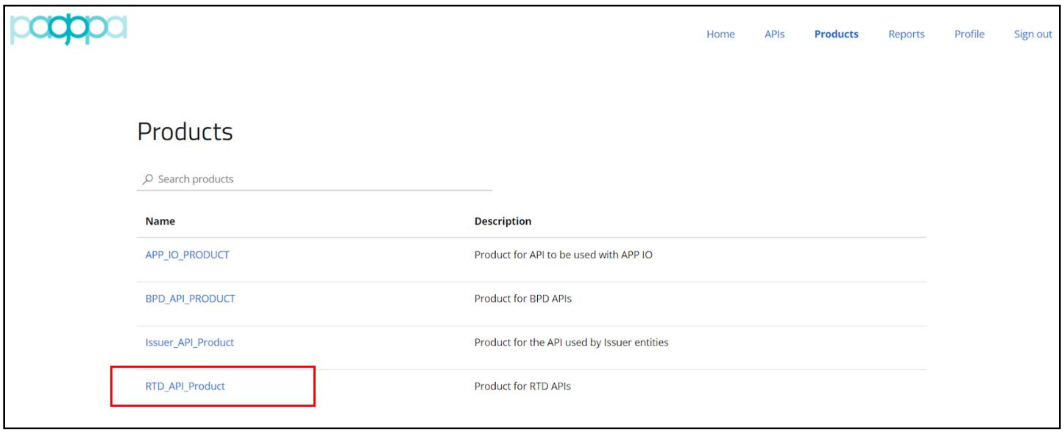
3. After inserting the credentials, the configuration data will be sent via email. The email will contain a link necessary to complete the verification procedure.

4. After clicking on the link contained in the email, you will be redirected to the login page where you will need to authenticate with the created User and Password. In order to create a subscription and the related keys, select the "Products" option.



Welcome to Centro Stella PagoPA!

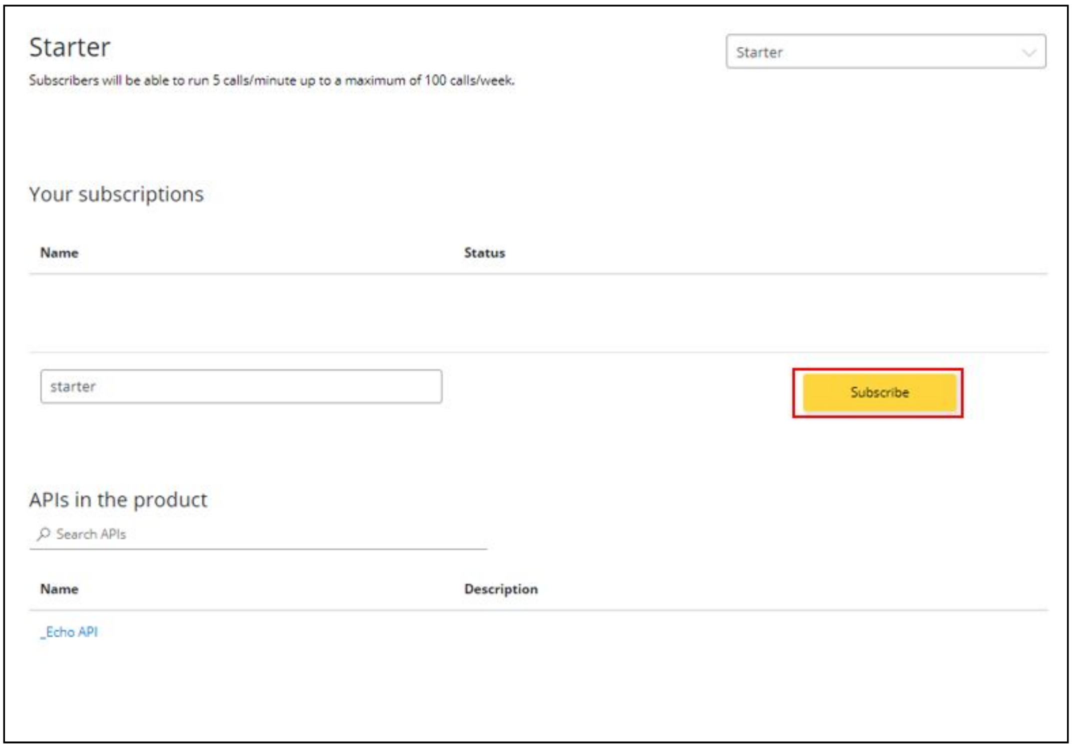
5. In the Products view, must be chosen the subscription “RTD_API_PRODUCT”



Products

Name	Description
APP_IO_PRODUCT	Product for API to be used with APP IO
BPD_API_PRODUCT	Product for BPD APIs
Issuer_API_Product	Product for the API used by Issuer entities
RTD_API_Product	Product for RTD APIs

6. Create a name for the selected product and select “Subscribe”.



Starter

Subscribers will be able to run 5 calls/minute up to a maximum of 100 calls/week.

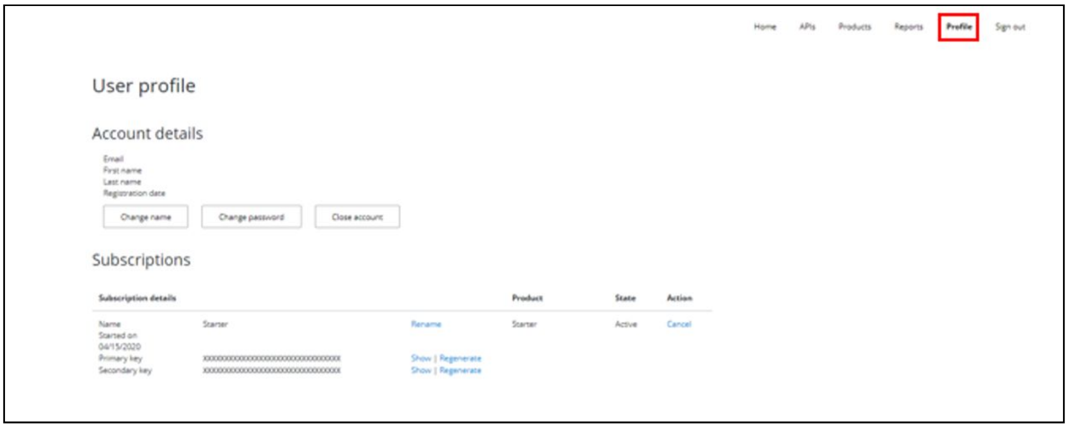
Your subscriptions

Name	Status

APIs in the product

Name	Description
_Echo API	

7. The Status of the subscription will be visible in the "Profile" menu item.



User profile

Account details

Email
First name
Last name
Registration date

Subscriptions

Subscription details			Product	State	Action
Name	Starter	Rename	Starter	Active	Cancel
Started on 04/15/2020					
Primary key	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Show | Regenerate			
Secondary key	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Show | Regenerate			

Appendix 8 - Environment

Ambiente	Indirizzo IP	URL API Gateway	URL Portale Sviluppatori
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://test.cstar.pagopa.it/
PROD	51.137.18.218	https://prod.cstar.pagopa.it/	https://developer.cstar.pagopa.it/