



Registro Transazioni Digitali

Issuer Interface Agreement

Versione: 2.0

Stato: Versione Finale

Cronologia Modifiche

Nella seguente tabella è riportata la cronologia delle modifiche al presente documento.

Data	Autore	Cronologia modifiche
25/03/2020	Luca Somaruga	Prima versione Draft
02/09/2020	Denisa Braho	Versione Finale
22/09/2020	Denisa Braho	- Aggiornamento "Enrollment Strumento di pagamento" (paragrafi 1.1.4, 1.2.5). Aggiornati i parametri delle chiamate di request e response
08/10/2020	Michael Desogus	- Aggiunte appendice 1 e 2, inerenti ai certificati ed alla procedura guidata di autenticazione

14/10/2020	Denisa Braho	- Aggiornati i parametri della chiamata di "Impostazione/Modific a IBAN"
------------	--------------	--

Approvazione Documento

Nella seguente tabella è riportata la lista degli stakeholder con cui il documento è stato condiviso e da cui è stato approvato.

Stakeholder (nome)	Data approvazione	Processi validati

Glossario

Nella tabella di seguito riportata si riassume la lista dei termini e degli acronimi riportati nel documento in oggetto.

Termine/Acronimo	Definizione
RTD	Registro Transazioni Digitali

BPD	Bonus Pagamenti Digitali
FA	Fatturazione Automatica
CF	Codice Fiscale dell'utente
PAN	Primary Account Number
HPAN	Hash del PAN (Primary Account Number) di uno strumento di pagamento digitale
MVP	Minimum Viable Product
TBD	To Be Defined
N/A	Not applicable
T&C	Terms & Conditions

Definizioni e semantica

Nella tabella seguente si riporta la semantica dei termini chiave utilizzati nel documento al fine di enunciare le logiche della Piattaforma.

Termine	Definizione
Utente	<p>Identifica colui che effettua l'operazione di acquisto con carta presso un determinato <i>Merchant</i> e rappresenta il soggetto al quale verrà riconosciuto il <i>Bonus</i>.</p> <p>Nel seguente documento verranno utilizzati alcuni sinonimi del termine <i>Utente</i>, come <i>User</i> o <i>Cardholder</i> (per sottolineare la titolarità della carta).</p>
Merchant	L'entità <i>Merchant</i> identifica tutti i esercenti presenti a sistema.
Acquirer	Istituto di pagamento o banca che offre i suoi servizi di incasso agli esercenti, installando presso di essi POS fisici o comunque intermediando le operazioni di pagamento.
Issuer	Soggetto aderente ad un Circuito, che emette Carte o altro strumento di pagamento, gestendo il rapporto con i Titolari.

Indice

Cronologia Modifiche	2
Approvazione Documento	3
Glossario	3
Definizioni e semantica	4
Indice	6
Introduzione e scopo del documento	8
Introduzione e scope dell'iniziativa	8
Obiettivo	9
Soluzione funzionale proposta Bonus Pagamenti Digitali	10
Happy Flow	10
Contesto Generale	11
Processi principali	12
Definizione delle interfacce	15
Registrazione Issuer	15
Integrazione Issuer	16
1.1 BPD	16
1.1.1 Restituzione file HTML T&C	16
1.1.2 Impostazione/modifica IBAN da H/M Banking	18

1.1.3 Enrollment Strumento Pagamento H/M Banking (in review - due date 21/10)	21
1.1.4 Accettazione T&C da H/M Banking	23
1.1.5 Status Citizen H/M Banking	26
1.1.6 Status Strumento Pagamento H/M Banking	28
1.1.7 Disabilitazione Strumento Pagamento H/M Banking	31
1.2 FA	33
1.2.1 Restituzione file HTML T&C	33
1.2.2 Accettazione T&C da H/M Banking	34
1.2.3 Status Customer H/M Banking	36
1.2.4 Enrollment Strumento Pagamento H/M Banking (in review - due date 21/10)	39
1.2.5 Status Strumento Pagamento H/M Banking	42
1.2.6 Disabilitazione Strumento Pagamento H/M Banking	44
Appendice 1 - Autenticazione Issuer	47
Appendice 2 - Autorizzazione Servizi Issuer	50
Appendice 3 - Ambienti	57

Introduzione e scopo del documento

Il presente documento ha lo scopo di descrivere la soluzione applicativa, in tutte le sue interfacce e i diversi flussi degli eventi da gestire in ingresso o uscita e le relative modalità di scambio dati, nonché l'architettura esecutiva High Level, con particolare riferimento alle interfacce esposte dai sistemi di PagoPa SpA verso i soggetti Issuer.

Introduzione e scope dell'iniziativa

Obiettivo del progetto è la realizzazione di una infrastruttura tecnologica, che permetta di abilitare nuovi use case e servizi per il cittadino e le imprese che vedono come perno principale la digitalizzazione dei pagamenti tramite utilizzo di carte e strumenti di pagamento attraverso POS fisici.

Pillar della nuova infrastruttura è la comunicazione con i soggetti Acquirer che operano sul territorio nazionale.

La piattaforma PagoPa CentroStella deve gestire informazioni che devono rispettare tutti i requisiti del GDPR; in particolare non deve essere consentito in nessun modo di risalire alla singola transazione e di recuperare i dati personali dei pagatori e/o del pagamento.

Le macro componenti oggetto dell'iniziativa sono le seguenti:

REGISTRO TRANSAZIONI DIGITALI (RTD)
--

Aggrega le transazioni commerciali eseguite tramite strumenti di pagamento digitali, sia da privati che da imprese attraverso POS fisici sul territorio nazionale. Un unico registro che abilita la creazione di soluzioni di incentivo fatturazione elettronica, di welfare, di automazione.

FATTURAZIONE AUTOMATICA

Si appoggia al Registro Transazioni Digitali per l'emissione automatica di fatture elettroniche nel contesto di un pagamento effettuato da un'impresa.

BONUS PAGAMENTI DIGITALI

Si appoggia al Registro Transazioni Digitali per l'assegnazione di bonus ai cittadini che effettuano pagamenti tramite strumenti di pagamento digitali.

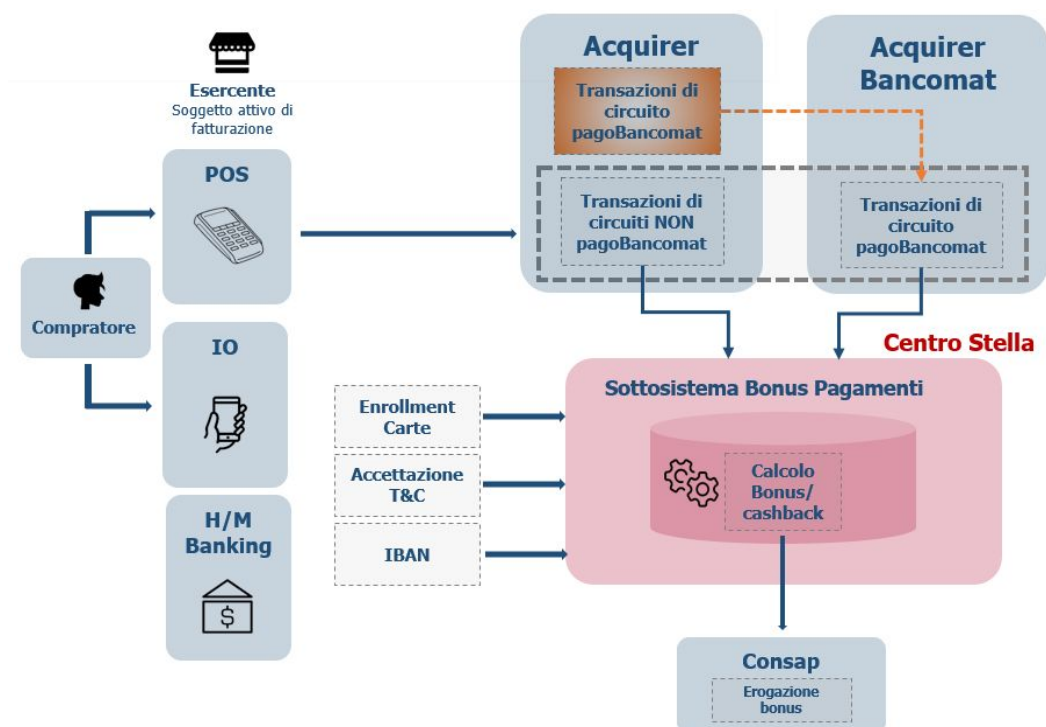
Obiettivo

Il Registro delle Transazioni Digitali è la piattaforma abilitante per diversi e futuri use case che vedono centrale il ruolo dei pagamenti elettronici, mantenendo unica l'integrazione con i soggetti Acquirer operanti sul territorio nazionale italiano.

Gli obiettivi principali del progetto sono dunque:

- incentivare i pagamenti con strumenti elettronici per ridurre l'uso del contante, creando delle condizioni premianti e un risultato cumulabile anche se raggiunto con strumenti di pagamento diversi.
- dare un impulso all'adozione della fattura elettronica da parte di piccoli esercenti attraverso la semplificazione dello scambio di informazioni fra tutti gli attori coinvolti nel processo.

Soluzione funzionale proposta Bonus Pagamenti Digitali



Happy Flow

Di seguito, si riporta l'Happy Flow che sintetizza la soluzione funzionale proposta della progettualità:



- Il Cittadino memorizza in modo sicuro il suo strumento di pagamento sulla piattaforma Centro Stella
- Il Cittadino effettua un pagamento presso un esercente fisico sul territorio italiano
- L'Acquirer dopo la contabilizzazione dell'operazione, invia i dati della transazione alla piattaforma BPD
 - Gli Acquirer aderenti al servizio invieranno verso Bancomat le transazioni effettuate su circuito PagoBancomat, mentre invieranno verso CentroStella esclusivamente le transazioni afferenti a circuiti diversi da PagoBancomat
 - Bancomat, invierà verso CentroStella tutte le transazioni effettuate su circuito PagoBancomat, comprensive di quelle ricevute dagli altri Acquirer
- Il Centro Stella assegna i punti alla transazione
- Su base punteggio accumulato vengono assegnati i premi (cashback)
- Il Cittadino inserisce attraverso l'App IO o l'H/M Banking l'IBAN del proprio conto corrente per esser accreditato del cashback maturato.

Contesto Generale

Qualora un soggetto Issuer di uno strumento di pagamento decida, di sua iniziativa, di far fronte all'integrazione con la piattaforma Centro Stella, dovrà principalmente:

- riconoscere in modo forte (equivalente a SPID) l'identità del cittadino con particolare riferimento al codice fiscale dello stesso
- permettere allo stesso di usufruire ad un subset anche minimo di funzionalità, quali:
 - accettazione/rifiuto esplicita dei T&C e iscrizione al servizio



- attivazione/disattivazione e degli strumenti di pagamenti emessi dalla Banca Issuer
- invio dell'IBAN su cui ricevere il cashback
- visualizzazione cashback totale maturato nel periodo e ranking

Processi principali

Di seguito vengono riportati i processi principali inerenti all'integrazione con i sistemi Bancari degli Issuer e comuni ad entrambi gli scenari (Bonus Pagamenti Digitali e Fatturazione Automatica).

1. Processi di autenticazione al Centro Stella tramite API key

Il processo di autenticazione della Banca Issuer sul Centro Stella sarà preliminare al fine di garantire la comunicazione tra i due sistemi. Le singole chiamate verso la piattaforma RTD (e relativi sottosistemi BPD/FA) verranno effettuate tramite una chiave di autenticazione, *API Key*, ottenuta attraverso la registrazione della Banca Issuer sul *portale API Gateway*.

Descrizione del processo
<ul style="list-style-type: none">a. l'Issuer effettua l'accesso sul portale API Gateway per richiedere la registrazioneb. A seguito della registrazione, il portale restituisce la chiave API necessaria per autenticarsi sul CentroStella

2. Comunicazione dei dati di consenso dell'utente (Accettazione dei T&C)

Per permettere all'utente di aderire al servizio di proprio interesse, verrà reso disponibile, tramite Home e/o Mobile Banking, il contratto contenente i Terms & Conditions del servizio Bonus Pagamenti Digitali/Fatturazione Automatica. A seguito dell'accettazione dei T&C da parte dell'utente, la Banca Issuer invierà al CentroStella la richiesta di salvataggio della data di accettazione dei T&C.

Descrizione del processo
<ul style="list-style-type: none">a. La Banca Issuer effettua una chiamata verso il Centro Stella per il salvataggio della data T&C;b. Il Centro Stella effettua il salvataggio della data di accettazione dei T&C sui propri sistemi.

3. Gestione degli strumenti di pagamento

Gli Issuer sfruttando le APIs messe a disposizione dal CentroStella potranno gestire, tramite i canali Home e/o Mobile Banking, tutti gli strumenti di pagamento emessi alla stessa Banca Issuer.

In particolare sarà possibile enrollare/disattivare una carta rispetto ai servizi Bonus Pagamenti Digitali e Fatturazione Automatica.

Descrizione del processo

1. Enrollment dello strumento di pagamento emesso dalla Banca Issuer:
 - a. Home/Mobile Banking chiama un servizio esposto dal Centro Stella al fine di attivare lo strumento di pagamento sul servizio BPD/FA. Tra i parametri inviati alla Piattaforma vi sarà il PAN della carta in chiaro.
 - b. CentroStella chiama un servizio di hashing esposto dal PM comunicando l'ID univoco della carta
 - c. Il PM effettua l'hashing del PAN dello strumento di pagamento ed invia l'HPAN al Centro Stella
 - i. I dati relativi alla carta enrollata vengono salvati, in modo da essere recuperabili dall'APP IO.
 - d. Il Centro Stella procede con il salvataggio delle seguenti informazioni, in seguito alle quali il servizio sullo strumento sarà attivo
2. Disattivazione dello strumento di pagamento emesso dalla Banca Issuer:
 - a. l'utente seleziona dal H/M Banking l'opzione di richiesta disattivazione del servizio BPD/FA dallo strumento di pagamento. Pertanto H/M Banking invia verso il Centro Stella la chiamata di disattivazione servizio.
 - i. Tra i parametri inviati alla Piattaforma vi sarà il PAN della carta in chiaro.

- b. Centro Stella chiama un servizio di hashing esposto dal PM comunicando l'ID univoco della carta
- c. Il PM effettua l'hashing del PAN dello strumento di pagamento ed invia l'HPAN al Centro Stella
- d. Il Centro Stella procede con la disattivazione del servizio e l'informazione sulla disattivazione viene salvata sul database interno.

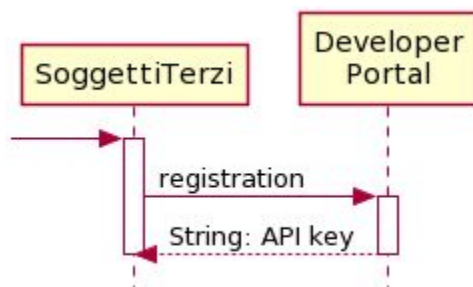
Nei paragrafi successivi verranno analizzate in dettaglio le singole interfacce.

Definizione delle interfacce

Registrazione Issuer

Il servizio di “Registrazione” permetterà agli Issuer di registrarsi sul portale API Gateway per poter ottenere la chiave utilizzata per l'autenticazione sul CentroStella.

Dopo aver effettuato l'accesso sul portale API Gateway e completato la procedura di registrazione, il portale restituirà agli Issuer la chiave API necessaria per autenticarsi sul CentroStella (vedi Appendice 2).



Integrazione Issuer

Nei successivi paragrafi sono declinate le API e i parametri necessari per una corretta integrazione con i servizi di Bonus Pagamenti Digitali e Fatturazione Automatica.

1.1 BPD

1.1.1 Restituzione file HTML T&C

API utilizzata per il recupero del file html contenente i Termini e Condizioni del servizio Bonus Pagamenti Digitali.

Path: /bpd/tc/html

Method: GET

Path Parameters

Nessun parametro previsto



Query Parameters

Nessun parametro previsto

Request Header

Nessun parametro previsto

Request Body

Nessun parametro previsto

Response Code

HTTP Response Code 200

Response Header

Nessun parametro previsto

Response Body

Il servizio risponde con il file html, contenente i Termini e Condizioni del Bonus Pagamenti Digitali.

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
404	FILE_NOT_FOUND	file non trovato
500	GENERIC_ERROR	errore generico



1.1.2 Impostazione/modifica IBAN da H/M Banking

La piattaforma BPD metterà a disposizione un servizio tramite il quale l'utente potrà salvare/aggiornare, da Home/Mobile Banking, l'IBAN sul quale desidera ricevere il versamento del premio. Nel caso di inserimento IBAN dal H/M Banking, l'utente può inserire solo IBAN a lui intestati associati esclusivamente a conti aperti presso la Banca Issuer che mette a disposizione il portale.

URL: bpd/hb/citizens/{id}

METHOD: PATCH

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dell'utente, che corrisponde al codice fiscale

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer



x-request-id	String	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)
---------------------	--------	----	--

Request Body

campo	formato	Obbligatorio	Descrizione
accountHolderCF	String	SI	CF dell'intestatario IBAN
accountHolderName	String	SI	Nome dell'intestatario IBAN
accountHolderSurname	String	SI	Cognome dell'intestatario IBAN
payoffInstr	String	SI	mezzo di pagamento, ad. es. IBAN utente
payoffInstrType	enum	SI	tipologia di strumento di pagamento per la riscossione del premio

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

19 di 57



Campo	Tipo	Obbligatorio	Descrizione
validationStatus	String	SI	Stato di validazione a seguito della chiamata al checkIban, i valori possibili saranno: <ul style="list-style-type: none"> • OK: l'IBAN è associato all'utente • KO: l'IBAN non è associato all'utente • UNKNOWN_PSP: non è stato possibile verificare

HTTP Error Codes

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente
403	TC_NOT_ACCEPTED	T&C non sono stati accettati
400	IBAN_NOT_VALID	Iban inserito è sintatticamente errato

1.1.3 Enrollment Strumento Pagamento H/M Banking *(in review - due date 21/10)*

API utilizzata per l'abilitazione di uno strumento di pagamento (carta) al programma bonus pagamenti digitali.



Path: /bpd/hb/payment-instruments/{id}

Method: PUT

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento

Query Parameter

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

Campo	Tipo	Obbligatorio	Descrizione
fiscalCode	Alfanumerico	SI	id dell'utente, che corrisponde al codice fiscale
expireYear	Number	SI	anno scadenza dello strumento di pagamento
expireMonth	Alfanumerico	SI	mese scadenza dello strumento

21 di 57





			di pagamento
issuerAbiCode	Alfanumerico	SI	codice ABI della banca emittente carta
brand	Alfanumerico	SI	tipo di circuito (es. Visa, Mastercard etc)
holder	Alfanumerico	NO	titolare carta
type	Alfanumerico	SI	tipologia carta (es. PP, DEB, CRD)

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

Campo	Tipo	Obbligatorio	Descrizione
activationDate	Timestamp	SI	timestamp dell'attivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX



HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio
500	GENERIC_ERROR	errore durante il recupero del profilo utente

1.1.4 Accettazione T&C da H/M Banking

API utilizzata per l'enrollment dell'utente, che di fatto consiste nell'accettazione dei Termini e Condizioni del servizio Bonus Pagamenti Digitali

Path: /bpd/hb/citizens/{id}

Method: PUT

Path Parameters

Campo	Formato	Descrizione
id	Alfanumerico	id dell'utente, che corrisponde al codice fiscale

Query Parameters



Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer

Request Body

No request body

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

campo	formato	Obbligatorio	Descrizione
fiscalCode	Alfanumerico	SI	id dell'utente, che corrisponde al codice fiscale

24 di 57



payoffInstr	Alfanumerico	NO	identificativo dello strumento di pagamento per la riscossione del premio
payoffInstrType	Alfanumerico	NO	tipologia di strumento di pagamento per la riscossione del premio
enabled	Booleano	SI	stato dell'abilitazione al servizio da parte del citizen
timestampTC	Timestamp	SI	timestamp dell'accettazione dei T&C. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXX XX

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente

1.1.5 Status Citizen H/M Banking

API utilizzata per recuperare le informazioni relative alla risorsa citizen.

Path: /bpd/hb/citizens/{id}

Method: GET



Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dell'utente, che corrisponde al codice fiscale

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

Nessun parametro previsto

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
-------	------	--------------	-------------



x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)
---------------------	--------	----	--

Response Body

Campo	Tipo	Obbligatorio	Descrizione
fiscalCode	Alfanumerico	SI	id dell'utente, che corrisponde al codice fiscale
payoffInstr	Alfanumerico	NO	identificativo dello strumento di pagamento per la riscossione del premio
payoffInstrType	Alfanumerico	NO	tipologia di strumento di pagamento per la riscossione del premio
enabled	Booleano	SI	stato dello dell'abilitazione al servizio da parte del citizen
timestampTC	Timestamp	SI	timestamp dell'accettazione dei T&C. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio



500	GENERIC_ERROR	errore durante il recupero del profilo utente
-----	---------------	---

1.1.6 Status Strumento Pagamento H/M Banking

API utilizzata per l'abilitazione di uno strumento di pagamento (carta) al programma di fatturazione automatica.

Path: /bpd/hb/payment-instruments/{id}

Method: GET

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer





x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)
---------------------	--------------	----	--

Request Body

No Request Body

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

Campo	Tipo	Obbligatorio	Descrizione
hpan	Alfanumerico	SI	<ul style="list-style-type: none">id dello strumento di pagamento, che corrisponde all'hash del PAN (Primary Account Number) del metodo di pagamento
fiscalCode	Alfanumerico	SI	Codice fiscale legato allo strumento di pagamento





status	Alfanumerico	SI	stato dello strumento di pagamento. Può assumere i seguenti valori: <ul style="list-style-type: none">• ACTIVE• INACTIVE
activationDate	Timestamp	SI	timestamp dell'attivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX
deactivationDate	Timestamp	SI	timestamp della disattivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio
500	GENERIC_ERROR	errore durante il recupero del profilo utente





1.1.7 Disabilitazione Strumento Pagamento H/M Banking

API utilizzata per disabilitare lo strumento di pagamento dal programma fatturazione automatica.

Path: /bpd/hb/payment-instruments/{id}

Method: DELETE

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	String	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

31 di 57





No request body

Response Code

HTTP Response Code 204

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

No response body

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
400	HPAN_NOT_FOUND	hpan non trovato
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente





1.2 FA

1.2.1 Restituzione file HTML T&C

API utilizzata per il recupero del file HTML di Termini e Condizioni del servizio Fatturazione Automatica

Path: /fa/tc/html

Method: GET

Path Parameters

Nessun parametro previsto

Query Parameters

Nessun parametro previsto

Request Header

Nessun parametro previsto

Request Body

Nessun parametro previsto

Response Code

HTTP Response Code 200

Response Header

Nessun parametro previsto

Response Body

33 di 57





Il servizio risponde con il HTML (MediaType = text/html) contenente i Termini e Condizioni del servizio di Fatturazione Automatica.

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
404	FILE_NOT_FOUND	file non trovato
500	GENERIC_ERROR	errore generico

1.2.2 Accettazione T&C da H/M Banking

API utilizzata per inviare l'accettazione da HB dei Terms & Conditions di un customer che vuole onboardarsi sul servizio di fatturazione automatica

Path: /fa/hb/customer/{id}

Method: PUT

Path Parameters

Campo	Formato	Descrizione
id	Alfanumerico	id dell'utente, che corrisponde al codice fiscale

Query Parameters

Nessun parametro previsto

34 di 57



Request Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer

Request Body

Campo	Formato	Obbligatorio	Descrizione
vatNumberList	Lista di String	NO	lista di id dell'utente, che corrisponde alla P.IVA
SDI	Alfanumerico	SI	codice destinatario o PEC

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

campo	formato	Obbligatorio	Descrizione
fiscalCode	String	SI	id dell'utente, che corrisponde al codice fiscale
vatNumberList	String	NO	lista di id dell'utente, che corrisponde alla P.IVA
timestampTC	Timestamp	SI	timestamp dell'accettazione di T&C. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXX X

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente

1.2.3 Status Customer H/M Banking

API utilizzata per recuperare le informazioni di stato di un customer onboardato al programma di fatturazione automatica.

Path: /fa/hb/customer/{id}

Method: GET



Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id del customer, che corrisponde a codice fiscale

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

Campo	Tipo	Obbligatorio	Descrizione

Response Code

HTTP Response Code 200





Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

Campo	Tipo	Obbligatorio	Descrizione
id	Alfanumerico	SI	id del customer, che corrisponde a codice fiscale
vatNumberList	List alfanumerici	NO	Lista delle P.IVA del customer
status	Alfanumerico	SI	stato dello strumento di pagamento. Può assumere i seguenti valori: <ul style="list-style-type: none">• ACTIVE• INACTIVE
activationDate	Timestamp	SI	timestamp dell'attivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXX X
deactivationDate	Timestamp	SI	timestamp della disattivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXX X

HTTP Error Codes

38 di 57





Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio
500	GENERIC_ERROR	errore durante il recupero del profilo utente

1.2.4 Enrollment Strumento Pagamento H/M Banking *(in review - due date 21/10)*

API utilizzata per l'abilitazione di uno strumento di pagamento (carta) al programma di fatturazione automatica.

Path: /fa/hb/payment-instruments/{id}

Method: PUT

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento





Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

Campo	Tipo	Obbligatorio	Descrizione
fiscalCode	Alfanumerico	SI	id dell'utente, che corrisponde al codice fiscale
expireYear	Number	SI	anno scadenza dello strumento di pagamento
expireMonth	Alfanumerico	SI	mese scadenza dello strumento di pagamento
issuerAbiCode	Alfanumerico	SI	codice ABI della banca emittente carta
brand	Alfanumerico	SI	tipo di circuito (es. Visa, Mastercard etc)
holder	Alfanumerico	NO	titolare carta
type	Alfanumerico	SI	tipologia carta (es. PP, DEB, CRD)





Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

Campo	Tipo	Obbligatorio	Descrizione
activationDate	Timestamp	SI	timestamp dell'attivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio



500	GENERIC_ERROR	errore durante il recupero del profilo utente
-----	---------------	---

1.2.5 Status Strumento Pagamento H/M Banking

API utilizzata per recuperare le informazioni di stato di uno strumento di pagamento (carta) enrollato al programma di fatturazione automatica.

Path: /fa/hb/payment-instruments/{id}

Method: GET

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Ocp-Apim-Subscription-Key	Alfanumerico	SI	Chiave di sottoscrizione associata all'issuer
x-request-id	Alfanumerico	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)



Request Body

Campo	Tipo	Obbligatorio	Descrizione

Response Code

HTTP Response Code 200

Response Header

Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

Campo	Tipo	Obbligatorio	Descrizione
hpan	Alfanumerico	SI	id dello strumento di pagamento, che corrisponde all'hash del PAN (Primary Account Number) del metodo di pagamento
fiscalCode	Alfanumerico	SI	Codice fiscale legato allo strumento di pagamento
status	Alfanumerico	SI	stato dello strumento di pagamento. Può assumere i seguenti valori: <ul style="list-style-type: none">• ACTIVE• INACTIVE



activationDate	Timestamp	SI	timestamp dell'attivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXX XX
deactivationDate	Timestamp	SI	timestamp della disattivazione dello strumento di pagamento. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXX XX

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
401	TOKEN_NOT_VALID	token non valido
403	TC_NOT_ACCEPTED	Terms & Condition non accettati. Per abilitare uno strumento di pagamenti l'utente deve prima registrarsi accettando i T&C del servizio
500	GENERIC_ERROR	errore durante il recupero del profilo utente

1.2.6 Disabilitazione Strumento Pagamento H/M Banking

API utilizzata per disabilitare lo strumento di pagamento dal programma fatturazione automatica.

Path: /fa/hb/payment-instruments/{id}



Method: DELETE

Path Parameters

campo	formato	Descrizione
id	Alfanumerico	id dello strumento di pagamento, che corrisponde al PAN (Primary Account Number) del metodo di pagamento

Query Parameters

Nessun parametro previsto

Request Header

Campo	Tipo	Obbligatorio	Descrizione
Authorization	String	SI	Bearer <token>
x-request-id	String	NO	ID della request , identificativo univoco determinato da inizializzazione (UUID)

Request Body

No request body

Response Code

HTTP Response Code 204

Response Header

45 di 57





Campo	Tipo	Obbligatorio	Descrizione
x-request-id	String	NO	ID della request , identificativo univoco determinato dal chiamante o dal sistema (UUID)

Response Body

No response body

HTTP Error Codes

Di seguito la lista dei messaggi di errore ed i codici di risposta associati

HTTP Response Code	Codice di Errore	Descrizione
400	HPAN_NOT_FOUND	hpan non trovato
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente



Appendice 1 - Autenticazione Issuer

Le interazioni dell'issuer utilizzano un meccanismo di mutua autenticazione su protocollo TLS 1.2, mediante lo scambio di certificati pubblici, rilasciati da una CA (l'autorità certificante), utilizzati per la verifica da parte di entrambi gli attori rispetto alle chiavi in proprio possesso. Perché questo meccanismo sia applicabile sarà quindi necessario che:

- il Client dovrà essere configurato per l'invio di richieste su protocollo TLS 1.2, indicando uno store contenente la catena di certificati necessaria per verificare l'attendibilità del server su cui viene effettuata la richiesta; inoltre, uno store contenente almeno la chiave privata e pubblica con cui il client si autentica con la macchina contattata.
- l'API dovrà essere configurata per accettare richieste su protocollo TLS 1.2, dovrà essere configurato per utilizzare una collezione di chiavi su cui applicare la verifica dei certificati, dovrà essere configurata per fornire un certificato pubblico, utilizzato dal Client per l'autenticazione della macchina a cui è diretta la richiesta.

Per la generazione della Certificate Signed Request è necessario utilizzare il template di configurazione client-certificate.cnf (opportunamente riconfigurato con le informazioni dello specifico Issuer). Il comando da invocare per la generazione della csr e della relativa chiave privata (utilizzando OpenSSL) è il seguente:

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



Per abilitare il processo di autenticazione, dovranno essere forniti all'API publisher i certificati relativi alle CA nel formato “.cer” (siccome dovranno contenere solamente la chiave pubblica, la password non è obbligatoria, in caso contrario dovrà essere fornita anch'essa).

I certificati client dovranno essere forniti all'API Publisher nel formato “.pfx” (contenente solamente la chiave pubblica), assieme alla relativa password. Il comando da invocare per la generazione del pfx a partire dal certificato client (utilizzando OpenSSL) è il seguente:

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

N.B: per i test nell'ambiente di SIT il certificato client può essere self-signed, e dev'essere fornito all'API publisher nel formato “.pfx”, mentre per gli ambienti superiori dovrà essere firmato dalla CA interna di PagoPA, e non è necessario condividerlo con l'API Publisher. Di conseguenza, il file contenente la chiave pubblica della CA dovrà essere fornito dagli Issuer solo nell'ambiente di SIT. Negli ambienti superiori il certificato della CA di PagoPA sarà già preconfigurato. Nel caso sia necessario ottenere un certificato con una firma valida per gli ambienti superiori al SIT, inviare il .csr da firmare a security@pagopa.it.

Le API saranno esposte e configurate in modo da abilitare il processo di mutua autenticazione sulla base di un determinato certificato. Nel caso dei servizi utilizzati dagli Issuer viene introdotta una policy dedicata per permettere il





processo di autenticazione tramite multipli certificati, per permettere l'utilizzo di certificati per gli Issuer.



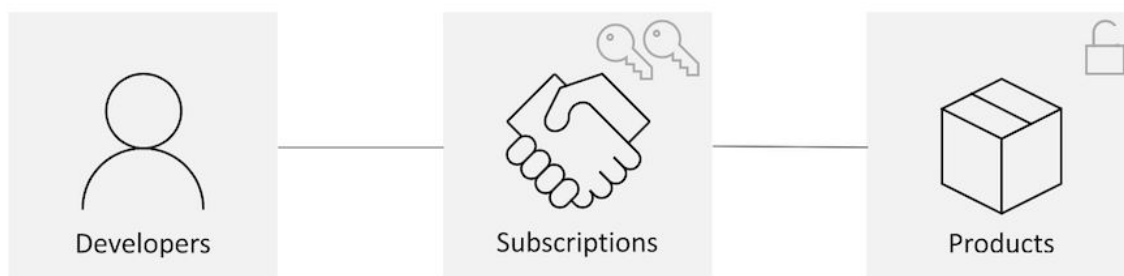
Appendice 2 - Autorizzazione Servizi Issuer

Gli sviluppatori dei sistemi Issuer che hanno bisogno di consumare le API pubblicate devono includere una chiave di sottoscrizione valida nelle richieste HTTP quando effettuano chiamate a tali API. In caso contrario, le chiamate vengono immediatamente rifiutate dal gateway dell'API Management e, di conseguenza, non vengono inoltrate ai servizi di back-end.

Per ottenere una chiave di sottoscrizione per l'accesso alle API, è necessaria una sottoscrizione. Una sottoscrizione è essenzialmente un contenitore per una coppia di chiavi di sottoscrizione. Gli sviluppatori che hanno bisogno di consumare le API pubblicate possono ottenere delle sottoscrizioni con due modalità (in base alla come sono state configurate):

- con l'approvazione degli API publisher;
- senza la necessità dell'approvazione degli API publisher.

Gli editori di API possono anche creare abbonamenti direttamente per API consumers.

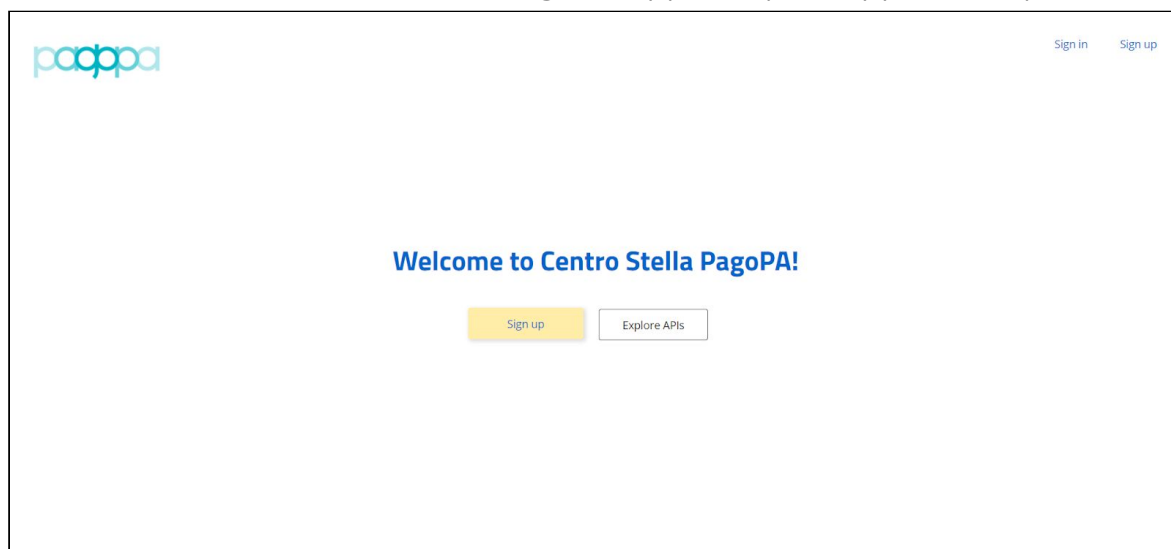




Dopo aver effettuato la sottoscrizione, il client può invocare i servizi (per i quali si è sottoscritto) inserendo il campo **Ocp-Apim-Subscription-Key** come parametro dell'header della request. Il valore del campo deve corrispondere al codice ottenuto in seguito registrazione al portale Azure.

Di seguito gli steps necessari per effettuare la registrazione per testare il comportamento dei servizi;

Accedere all'indirizzo dev dedicato agli sviluppatori (vedi Appendice 3)



1. dopo aver cliccato sul tasto giallo in evidenza si verrà indirizzati alla pagina di registrazione nel quale dovremo inserire le credenziali per la configurazione dell'account





The screenshot shows the 'Sign up' page of the pagoPA system. At the top left is the pagoPA logo, and at the top right are links for 'Sign in' and 'Sign up'. The main heading is 'Sign up', followed by a link 'Already a member? Sign in.' Below this are several input fields: 'Email' (with a placeholder 'e.g. name@example.com'), 'Password', 'Confirm password', 'First name' (with a placeholder 'e.g. John'), and 'Last name' (with a placeholder 'e.g. Doe'). There is also a 'Recaptcha' section with a visual puzzle and a text input field labeled 'Enter the captcha here'. A yellow 'Sign up' button is at the bottom of the form.

2. Dopo aver completato la procedura di inserimento credenziali, riceveremo via mail le configurazioni necessarie per terminare la verifica tramite un link.
3. Dopo aver cliccato sul link contenuto nella mail si verrà reindirizzati alla pagina di login nella quale bisognerà autenticarsi con l'utenza creata. Per creare la subscription e le relative chiavi bisognerà selezionare l'opzione "Products".





4. In questa fase, bisognerà selezionare la tipologia di sottoscrizione





The screenshot shows the 'Products' page of the PagoPA system. At the top, there is a navigation bar with links for Home, APIs, Products (which is highlighted), Reports, Profile, and Sign out. Below the navigation bar, the title 'Products' is displayed. A search bar labeled 'Search products' is present. A table lists the available 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

5. Inserire un nominativo e selezionare l'opzione Subscribe.





Starter

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

Starter

Your subscriptions

Name	Status
starter	<div>Subscribe</div>

APIs in the product

Search APIs

Name	Description
_Echo API	

6. L'esito della sottoscrizione sarà visibile alla voce "Profile" del menu'.





HomeAPIsProductsReportsProfileSign out

User profile

Account details

Email

First name

Last name

Registration date10/08/2020

Change name

Change password

Close account

Subscriptions

Subscription details		Product	State	Action	
Name		Rename	APP_IO_PRODUCT	Submitted	Cancel
Requested on	10/08/2020				
Primary key	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Show Regenerate			
Secondary key	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Show Regenerate			





Appendice 3 - Ambienti

Ambiente	IP API Gateway	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://developer-test.cstar.pagopa.it/
PROD	51.137.18.218	https://prod.cstar.pagopa.it/	https://developer.cstar.pagopa.it/

