CentroStella - Registro Transazioni Digitali

Acquirer Interface Agreement

Versione: 2.0

Stato: Draft

Cronologia Modifiche

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

Data	Autore	Cronologia modifiche
28/02/2020	Stefano Menotti	Prima versione Draft
28/04/2020	Luca Somaruga	Aggiornamento formato campo timestamp
21/05/2020	Debora Arena	Aggiornamenti: - Capitolo "Transazioni di pagamento digitali oggetto del servizio": aggiunto vincolo su HashPan enrollati. - Paragrafo" Integrazione con Acquirer": aggiunto vincolo su HashPan enrollati. Aggiunto: - Capitolo "Servizio batch per controllo HashPan" Aggiornamento: - "Appendice 1 - Modalità di file transfer": il servizio batch invierà i flussi verso l'sFTP della Piattaforma
22/05/2020	Stefano Menotti	versione esportabile agli stakeholder Acquirer
27/06/2020	Debora Arena	Aggiornamenti: - flusso Standard PagoPa - inserimento capitolo "Onboarding Merchant tramite Acquirer"
30/07/2020	Rodolfo Viti	Aggiornamento: - flusso Standard PagoPa

		- Appendice 4 - Servizio per recupero del salt - Appendice 5 - Servizio per il download degli HPAN registrati a CentroStella - Appendice 7 - Autenticazione Servizi Acquirer Aggiunto: - Appendice 8 - Autorizzazione Servizi Acquirer - Appendice 9 - Ambienti
02/09/2020	Rodolfo Viti	Aggiornamento: - flusso Standard PagoPa (lunghezza campi)

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

Indice

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 soggetti Acquirer verso sistemi di PagoPa SpA (Centro Stella).

Riferimento normativo

Il servizio trova il suo riferimento normativo nel D.L. 26/10/19 n. 124 convertito con legge di conversione del 19 dicembre 2019, n. 157 pubblicata in Gazzetta Ufficiale n.301 del 24-12-2019, e in particolare nell'articolo 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 e trattamento dei dati

Si faccia riferimento al documento DPIA approvato dal Garante della Privacy.

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:

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>FATTURAZIONE AUTOMATICA
Si appoggia al Registro Transazioni Digitali per l'emissione automatica di fatture elettroniche nel contesto di un pagamento effettuato da un'impresa.</td><td>BONUS PAGAMENTI DIGITALI
Si appoggia al Registro Transazioni Digitali per l'assegnazione di bonus ai cittadini che effettuano pagamenti tramite strumenti di pagamento digitali.</td></tr>
</table>

Obiettivo

Il Registro delle Transazioni Digitali è quindi 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.

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

Transazioni di pagamento digitali oggetto del servizio

Perimetro Informativo

I **pagamenti elettronici digitali** da considerare sono tutti i pagamenti effettuati tramite *POS fisici* sul *territorio nazionale italiano*, per il tramite dei seguenti strumenti di pagamento:

- carte di debito su circuiti internazionali e bancomat,
- carte di credito,
- carte prepagate (ricaricabili non agganciate a conto corrente, ricaricabili agganciate ad un conto corrente, ricaricabili con funzioni di conto).
- applicazioni collegate a bonifico o ad altri sistemi di settlement

Per una corretta erogazione dei servizi, e con obiettivo di non discriminare nessun tipo di cittadino/transazione di pagamento, **è necessario che l'Acquirer veicoli a PagoPA anche le transazioni comprensive di eventuali modalità on-us** ed incluse le operazioni di storno.
Oggetto del servizio saranno le sole transazioni in *valuta EUR*.

Sono pertanto escluse dal perimetro le seguenti transazioni:

- relative a cashback (prelievo contante)
- di anticipo contante su POS (MCC = 6010)
- di anticipo contante su ATM (MCC = 6011)
- relative ad e-commerce
- DCC (Dynamic Currency Conversion)
- effettuate nel territorio di San Marino

Si evidenzia inoltre che, il processo approvato dal Garante della Privacy, prevede che potranno affluire verso i sistemi di PagoPA (CentroStella) solo le transazioni con HashPan afferenti a strumenti di pagamento per i quali è stato effettuato l'Enrollment da parte del Cittadino/Compratore ad uno dei servizi attivati sulla piattaforma CentroStella di PagoPa.

Processo invio transazioni verso RTD

Il processo di invio delle transazioni verso la Piattaforma CentroStella (RTD) è composto dalle fasi di seguito declinate:

PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

a. La Piattaforma CentroStella genera un flusso contenente gli HPAN enrollati al servizio CentroStella.

b. L'Acquirer consolida i dati relativi a tutte le transazioni di interesse contabilizzate nell'ultimo ciclo di regolamento verso l'esercente. Provvede pertanto alla generazione di un file di testo in formato csv (con naming file e tracciato dettagliati nel paragrafo "Flusso Standard PagoPA") e lo deposita su una folder su cui è in polling il batch.
Il deposito del file è il trigger che fa partire il processo di elaborazione del batch.

c. Il Batch installato presso gli Acquirer invoca il servizio esposto dalla Piattaforma tramite il quale viene generato un link one shot e attivo temporalmente per effettuare il download del flusso HPAN enrollati ai servizi della piattaforma CentroStella.

d. Il Batch chiama il servizio esposto da CentroStella per ottenere la chiave di hashing costante da aggiungere al PAN per effettuare l'hashing dei PAN contenuti nel flusso delle transazioni.

e. Il Batch legge entrambi i flussi in input (lista HPAN e transazioni) e, per ogni riga del file di transazione:

    i. effettua Hash del PAN nel flusso delle transazioni;
    ii. determina se la riga di transazione deve essere scartata o riportata nel flusso filtrato in output.

g. Il Batch, conclusa l'elaborazione al punto precedente, termina la scrittura del flusso filtrato in output, ed elimina tutti i dati ricevuti in input.

h. Il Batch effettua la cifratura PGP del flusso di output.

    In "Appendice 2" è riportata la chiave pubblica da utilizzare per la cifratura del file prodotto al punto precedente.

i. Il Batch deposita il flusso delle transazioni filtrato su sFTP di CentroStella.

    Per ulteriori informazioni su istruzioni e modalità di accesso all'sFTP di SIA si faccia riferimento a quanto indicato in Appendice 3.

Si precisa inoltre che il Batch deposita il file in output all'interno della directory /Inbox/.

f. Infine il CentroStella cancella tutti i file ricevuti in input.

Integrazione Acquirer con CentroStella PagoPA

Gli *Acquirer* accreditati (ovvero che hanno stipulato una convenzione con PagoPA S.p.A.), al termine della transazione di pagamento conclusa positivamente, genereranno il flusso giornaliero delle transazioni.

Quest'ultimo verrà filtrato al fine di verificare che gli HPAN presenti nei vari tracciati, corrispondano a quelli enrollati sulla Piattaforma CentroStella, prima di essere inviati alla stessa.

Tale controllo sarà garantito da un servizio batch installato sui sistemi degli Acquirer, che PagoPa metterà a disposizione dell' Acquirer stesso, sotto forma di codice sorgente *opensource*, da utilizzare per facilitare l'integrazione e minimizzare l'effort.

Per maggiori dettagli si veda il paragrafo "Servizio batch per controllo HPAN"

Ciò premesso, si precisa che sarà facoltà degli Acquirer utilizzare una o più modalità di integrazione e, per ciascuna modalità, uno o più file giornalieri per coprire l'intero insieme delle transazioni da trasmettere al CentroStella.

PagoPA SpA chiederà agli *Acquirer* accreditati, mantenendo l'obiettivo di minimizzare l'effort tecnologico per ciascun Acquirer e, nel contempo, garantire la *compliance* alla normativa PCI[1], l'invio di uno o più **flussi batch** nel formato **"standard PagoPA":** PagoPA SpA fornirà una specifica di flusso di semplice realizzazione che contempla il sottoinsieme minimo di dati, descritto nei paragrafi successivi di questo documento.

Sarà onere di PagoPA SpA (Piattaforma CentroStella) gestire i dati in ambiente PCI secondo normativa vigente e mantenere solo il sottoinsieme minimo dei dati anonimizzati (**filtrato per HashPan enrollati**), necessario al funzionamento della Piattaforma, eliminando ogni dato delle transazioni che non siano state fatte con strumenti di pagamenti abilitati volontariamente dal Cittadino sulla Piattaforma.

[1] Payment Card Industry: certificazione di sicurezza cui tutti i sistemi di pagamento devono sottostare.

Il dato carta verrà salvato con una **funzione crittografica di hash irreversibile**.

Ciò premesso, l'integrazione degli Acquirer con il CentroStella si divide in due fasi:

- Flusso Standard PagoPa
- Servizio Batch per controllo HPAN enrollati

Nei paragrafi successivi si riportano i dettagli dei punti sopra elencati.

Flusso Standard PagoPA

Di seguito vengono descritti i dettagli relativi al Flusso Standard PagoPA.

La naming convention del file è la seguente:

- [servizio].[ABI].[tipofile].[data].[ora].[nnn].csv

in particolare:

- servizio: fisso a 'CSTAR' (5 digit alfanumerico)
- ABI: ABI del mittente (5 digit numerico)
- tipofile: fisso a tipologia di file (6 digit alfanumerico)
- nnn: progressivo file (3 digit numerico)

campo	**formato**	**note**
servizio	Alfanumerico - 5 char	valore fisso CSTAR
ABI	Alfanumerico - 5 char	codice ABI del mittente
tipo_file	Alfanumerico - 6 char	tipologia del flusso inviato. Valore fisso a TRNLOG
[data].[ora]	YYYYMMDD.HHMISS	timestamp di creazione del file
nnn	Alfanumerico - 3 char	Valore progressivo del file (es. 001)

Si precisa che:

- Il file è in formato .csv, con separatori ";"
- il file è cifrato con chiave pubblica pgp rilasciata da PagoPa SpA
- Il contenuto del file non prevede record di testa e coda ma solo record di dettaglio, secondo questo tracciato:

Campi presenti nel Flusso Standard PagoPA.

campo	Tipo	Obb.	Note
codice_acquirer	Alfanumerico - max 20 char	SI	Codice ABI della banca Acquirer.
tipo_operazione	Alfanumerico - regexp [0-9]{2}	SI	Tipo operazione: 00 - pagamento 01 - storno pagamento 02 - pagamento con ApplePay 03 - pagamento con GooglePay xx - usi futuri La tipologia 02 e 03 non sempre risulterà valorizzata dagli Acquirer
tipo_circuito	Alfanumerico - regexp [0-9]{2}	SI	Circuito di pagamento: 00 - Pagobancomat 01 - Visa 02 - Mastercard 03 - Amex 04 - JCB 05 - UnionPay 06 - Diners 07 - Codice PostePay 08 - BancomatPay 09 - SatisPay

			10 - circuito privativo (onus, owen) xx - usi futuri
hash_pan	Alfanumerico – max 64 char	SI	Hash del PAN dello strumento di pagamento utilizzato. Nel caso di circuito non card based rappresenta l'identificativo univoco dello strumento di pagamento privativo, che l'utente può registrare attraverso App IO o touch point della banca Issuer.
date_time	DateFormat *FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXX*	SI	Timestamp dell'operazione di pagamento effettuata presso l'Esercente. Si precisa che non è sempre disponibile il dettaglio in merito al secondo per tutte le transazioni. In tale circostanza, il dettaglio sarà paddato con tutti '0'
id_trx_acquirer	Alfanumerico – max 255 char	SI	Identificativo univoco della transazione a livello di Acquirer. Tale campo può coincidere con la seguente concatenazione di dati: - RRN e STAN, - Term ID, RRN, STAN Inoltre per alcune transazioni con tipo circuito '07' è previsto un codice proprietario di 75 digit

id_trx_issuer	Alfanumerico – max 255 char	SI	Codice autorizzativo rilasciato dall' Issuer (es: AuthCode) Tale codice non è disponibile per tutte le transazioni
correlation_id	Alfanumerico – max 255 char	NO	Identificativo di correlazione fra operazione di pagamento ed eventuale storno/reversal. In certi casi, il dato non può essere recuperato dall' Acquirer e l'informazione non sarà inviato nel campo in questione
total_amount	Numerico	SI	Valorizzato in centesimi di euro (es: 10€ = 1000) ed espresso in valore assoluto: il segno è dedotto dal tipo operazione *"00-pagamento, 01-storno "*
currency	Alfanumerico - max 3 char	NO	Valore fisso 978 = EUR. Si utilizza codifica internazionale ISO.
acquirer_id	Alfanumerico – max 255 char	SI	Identificativo univoco dell'Acquirer. Nel caso di transazione con carta rappresenta il valore omonimo veicolato nei tracciati dei circuiti internazionali. - Nel circuito Pagobancomat

			corrisponde al campo *codice_sia_abi* - Circuito Visa/Mastercard: *acquirer_id* In altri casi il campo sarà valorizzato con un dato fisso a seconda dell' Acquirer di riferimento
merchant_id	Alfanumerico – max 255 char	SI	Identificativo univoco del negozio fisico presso l'Acquirer (noto anche all'Esercente ed utilizzato dallo stesso per registrarsi alla piattaforma di Fatturazione Automatica). - Nel circuito Pagobancomat può corrispondere al campo: esercente
terminal_id	Alfanumerico – max 255 char	SI	Identificativo del terminale/POS (Point of Sale) presente presso l'Esercente. - Nel circuito Pagobancomat corrisponde al campo: *stabilimento cassa* - Circuito Visa/Mastercard: *terminal_id*

bank_identification_number (BIN)	Alfanumerico – regexp [0-9]{6}|[0-9]{8}	SI	Codice contenente le prime 8 cifre dello strumento di pagamento. - Nel circuito Pagobancomat corrisponde al campo: *codice_abi*
MCC	Alfanumerico – max 5 char	SI	Merchant Category Code.

Servizio batch per controllo HPAN enrollati

Il servizio sarà sviluppato dal CentroStella ed installato presso gli Acquirer accreditati. Si precisa tuttavia che la manutenzione del servizio, ed eventuali modifiche dello stesso sono a carico dell'Acquirer. PagoPa fornirà il codice sorgente in logica opensource pubblicato su repository pubblici per facilitare l'integrazione e minimizzarne l'effort.

Modalità Operativa

L'artefatto consiste in un jar eseguibile prodotto con *spring-boot*, pertanto tutte le dipendenze del progetto sono contenute all'interno del jar insieme alle classi che ne contengono la business logic.
In questo modo l'artefatto è completamente autonomo ed utilizzabile su un qualsiasi dispositivo che disponga di una JVM.

Per l'installazione ed esecuzione del batch sono necessari:

- Java 1.8+
- Artefatto *batch-transaction-filter.jar*

Relativamente ai parametri e comandi di esecuzione, si faccia riferimento alle indicazioni presenti nel README contenuto nel repository pubblico raggiungibile tramite il link: https://github.com/pagopa/rtd-ms-transaction-filter/blob/master/README.md

Requisiti Minimi

Di seguito riportati i requisiti minimi per l'esecuzione del batch sopra descritto:

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: in funzione delle dimensioni del file delle transazioni. Al precedente file va sommata la dimensione del file contenente gli hash dei pan che ha una dimensione che si attesta intorno ai 300 MB (in formato pgp).

Gestione stato di esecuzione

Il servizio batch prevede la gestione dei file impiegati nei casi in cui occorra un caso di errore bloccante o nel caso di esecuzione completata con successo.

Il comportamento tenuto nei vari passaggi del servizio sarà condizionato dalla configurazione della proprietà deleteLocal, che impone eventuale cancellazione al termine dell'esecuzione di tutti i file processati, qualora attiva.

Se diversamente configurata, il comportamento sarà quello di procedere all'archiviazione dei file processati nel flusso, sia per il file contenente la lista dei PAN, che per quello delle transazioni, per l'eventuale gestione a margine degli stessi.

Nel caso di un'esecuzione corretta, il file dei pan verrà rimosso, assieme a tutti i file temporanei generati prima dell'invio finale del file di output. Il file delle transazioni ottenute sarà archiviato in una directory dedicata.
Sarà inoltre possibile configurare, per errori generici nel processamento dei record dei singoli file, un margine di tolleranza rispetto al numero di righe per le quali si è riscontrato un errore, tramite la proprietà skipLimit.

Sel file sarà processato senza superare il valore di soglia configurato, verrà riportato un successo condizionato alla presenza di alcuni errori, che potranno eventualmente essere gestiti a margine.

Onboarding Merchant tramite Acquirer e salvataggio dei dati sulla Piattaforma FA

Al fine di poter effettuare l'Onboarding del Merchant ai servizi di Fatturazione Automatica, i sistemi dell'Acquirer invocheranno le API esposte dalla piattaforma CentroStella per censire l'Esercente ed esporranno un servizio per comunicare alla Piattaforma i dati del Merchant.
Successivamente il sistema FA salverà tale parco informativo nell'anagrafica interna.

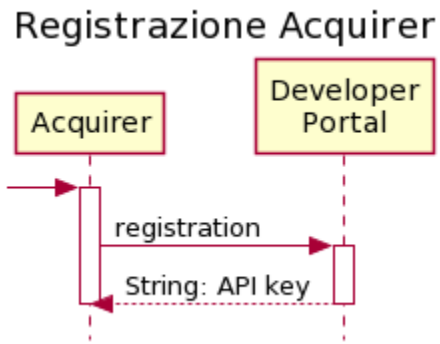
Ciò anticipato, si prevede di esporre verso gli Acquirer le seguenti API:

- Visualizzazione T&C di adesione al servizio [showT&C]
- Accettazione T&C di adesione al servizio [acceptT&C]
- Recupero lista Provider di fatturazione
- Invio dati del Merchant e salvataggio sulla Piattaforma FA

Nei successivi paragrafi sono declinati i servizi ed i parametri necessari per una corretta integrazione con il servizio di Fatturazione Automatica.

Servizio Registrazione Acquirer su API Gateway

Il servizio "Registrazione Acquirer" permette all'Acquirer di registrarsi sul portale API Gateway ed ottenere la chiave utilizzata per l'autenticazione sul Centro Stella.



Per ulteriori dettagli, fare riferimento ad Appendice 8.

Show T&C

Path: fa/tc/html

Method: GET

Path Parameters
Nessun parametro previsto

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)

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

Il servizio risponde con il HTML contenente i Termini e Condizioni della Fatturazione Automatica.

HTTP Error Codes

Di seguito la lista dei 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

Recupero Lista Provider di fatturazione

Attraverso il servizio in oggetto sarà possibile recuperare in fase di Onboarding di un Merchant tramite l'Acquirer, la lista dei Provider integrati alla piattaforma FA e selezionare il Provider indicato dal Merchant, ovvero il Provider con il quale il Merchant ha stipulato il contratto.

Path: /fa/provider/list

Method: GET

Path Parameters

Campo	Formato	Descrizione

Query Parameters

Nessun parametro previsto

Request Body

Campo	Formato	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	formato	Obbligatorio	Descrizione
providerList	Alfanumerico	SI	Lista Provider aderenti al servizio: 1. providerID 2. providerDesc

HTTP Error Codes

Di seguito la lista dei 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

Accettazione T&C, invio dati del Merchant e salvataggio sulla Piattaforma FA

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

Method: PUT

Path Parameters

Campo	Formato	Descrizione
vatNumber	Alfanumerico	P.IVA del Merchant

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)
Authorization	String	SI	Bearer <token> (formato JWT)

Request Body

Campo	Formato	Obbligatorio	Descrizione
timestampTC	Timestamp	SI	timestamp dell'accettazione di T&C. FORMATO ISO8601 yyyy-MM-ddTHH:mm:ss.SSSXXXXX
token	Numerico	SI	token di autenticazione tra il portale e Piattaforma FA
fiscalCode	Alfanumerico	NO	id della persona fisica associata al merchant che corrisponde al codice fiscale
acquirerMerchantId	Alfanumerico	SI	ID del merchant staccato dall' Acquirer
providerID	Alfanumerico	SI	ID univoco del Provider di fatturazione presso cui il Merchant si è integrato alla piattaforma

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
vatNumber	Alfanumerico	SI	P.IVA del Merchant

HTTP Error Codes

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

HTTP Response Code	Codice di Errore	Descrizione
400	INVALID_DATE	valore o formato data non corretto
401	TOKEN_NOT_VALID	token non valido
500	GENERIC_ERROR	errore durante il recupero del profilo utente
400	INVALID_PIVA	PIVA non valida

Appendice 1 - Chiave pubblica PGP

Per qualsiasi problema relativo all'utilizzo della chiave pubblica e per il rilascio delle specifiche e/o aggiornamento relativi alla chiave pubblica da utilizzare per cifrare il file, è necessario contattare la struttura delegata da PagoPa di competenza (rif. 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/vckNc2QOt
NhfcJ5lrsBoNTCUL25VJicM5KQeqCGIPF6gcSKVGkvTwjgRctIL85ua7syDM9pU6
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-----
```


PagoPA S.p.A.
società per azioni con socio unico
capitale sociale di euro 1,000,000 interamente versato
sede legale in Roma, Piazza Colonna 370, CAP 00187
n. di iscrizione a Registro Imprese di Roma, CF e P.IVA 15376371009

Appendice 2 - Modalità di file transfer

La Piattaforma CentroStella mette a disposizione un server sFTP su rete pubblica, presso cui il servizio batch installato sui sistemi di ogni Acquirer, possa depositare su una cartella specifica i file oggetto del servizio.

Di seguito sono indicati i dettagli degli IP pubblici Internet dell'SFG (Secure File Gateway):

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

Ogni soggetto accede con modalità di autenticazione da definire, attraverso chiavi univoche. Per la configurazione e qualsiasi problema relativo all'accesso al sFTP, si faccia riferimento al seguente referente delegato da 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

In alternativa, se l'Acquirer ha già canali di trasmissione attivi che garantiscano gli stessi standard di sicurezza con partner tecnologico di PagoPA, si potranno utilizzare tali canali, previo sviluppo del servizio batch in oggetto.

Appendice 3 - Manuale accesso sFTP SIA

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

Appendice 4 - Servizio per recupero del salt

Centro Stella PagoPA (componente interna Payment Manager) mette a disposizione un servizio REST per il recupero del SALT da concatenare al pan originale prima di effettuare l'hashing.

Per i dettagli in merito ad Autenticazione ed Autorizzazione, fare riferimento ad Appendice 7 e Appendice 8.

Di seguito il dettaglio dell'API:

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

Path Parameters

Nessun parametro previsto

Query Parameters

Nessun parametro previsto

Request Header

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

Request Body

Nessun parametro previsto

Response Code

HTTP Response Code 200

Response Header

Nessun parametro previsto

Response Body

Il servizio risponde con il salt da utilizzare in fase di hashing.

HTTP Error Codes

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

HTTP Response Code	Codice di Errore	Descrizione
500	GENERIC_ERROR	errore generico

Appendice 5 - Servizio per il download degli HPAN registrati a CentroStella

Il servizio di download degli HPAN fornisce previa opportuna verifica di presenza del file, che viene generato giornalmente da un processo batch, la possibilità di scaricare il file contenente l'hash del pan. A fronte della prima chiamata il servizio effettua una redirect (http 302) verso l'url di download.
Il file scaricato sarà in formato pgp (la dimensione stimata per un file contenente 10 milioni di HPAN è circa 300 MB).

Per i dettagli in merito ad Autenticazione ed Autorizzazione, fare riferimento ad Appendice 7 e Appendice 8.

Di seguito il dettaglio dell'API:

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

Path Parameters

Nessun parametro previsto

Query Parameters

Nessun parametro previsto

Request Header

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

Request Body

Nessun parametro previsto

Response Code

HTTP Response Code 302 (FOUND).

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

Il servizio risponde con una redirect, verso il link per il download del file PGP contenente l'hash dei PAN registrati al programma BPD e FA.

HTTP Error Codes

Di seguito la lista dei 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

Appendice 6 - Documentazione

File	descrizione	autore	numero pagine

Appendice 7 - Autenticazione Servizi Acquirer

Le interazioni per i servizi del batch Acquirer 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 Acquirer). 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, mentre per gli ambienti superiori dovrà essere firmato dalla CA interna di PagoPA. Di conseguenza, il file contenente la chiave pubblica della CA dovrà essere fornito dagli Acquirer solo nell'ambiente di SIT. Negli ambienti superiori il certificato della CA di PagoPA sarà già preconfigurato.

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 Acquirer viene introdotta una policy dedicata per permettere il processo di autenticazione tramite multipli certificati, per permettere l'utilizzo di certificati per gli Acquirer.

Appendice 8 - Autorizzazione Servizi Acquirer

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.

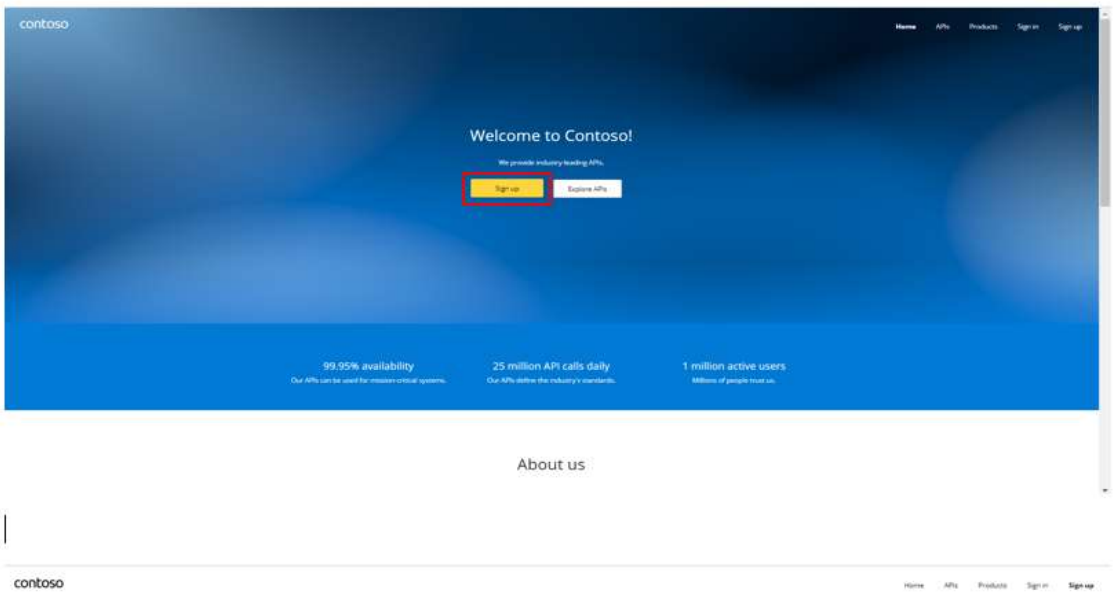
Per ottenere una chiave di sottoscrizione per l'accesso alle API, è necessaria una sottoscrizione. Una sottoscrizione è essenzialmente un contenitore per una coppia di chiavi di sottoscrizione. Gli sviluppatori che hanno bisogno di consumare le API pubblicate possono ottenere delle sottoscrizioni con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

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

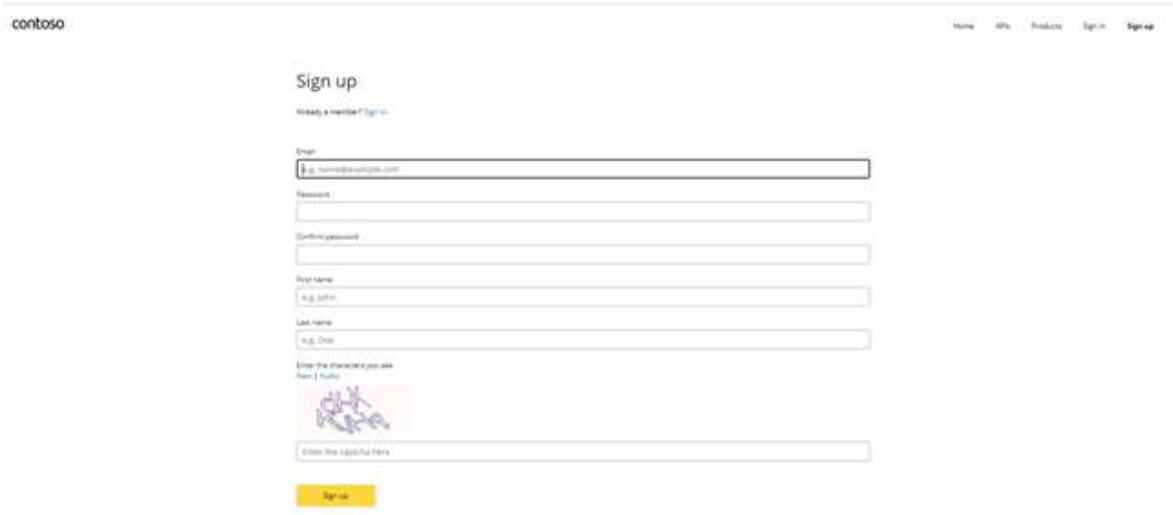
Gli editori di API possono anche creare abbonamenti direttamente per API consumers.

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 sviluppatori di 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 B)

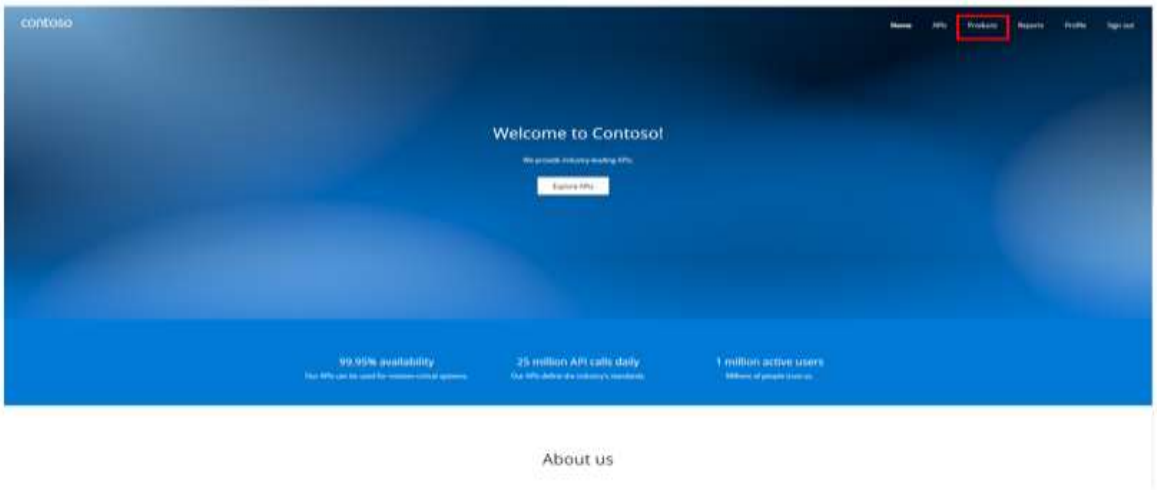


A questo punto dopo aver cliccato sul tasto giallo in evidenza si verrà indirizzati alla pagina di registrazione nel quale dovremo inserire le credenziali per la configurazione dell'account

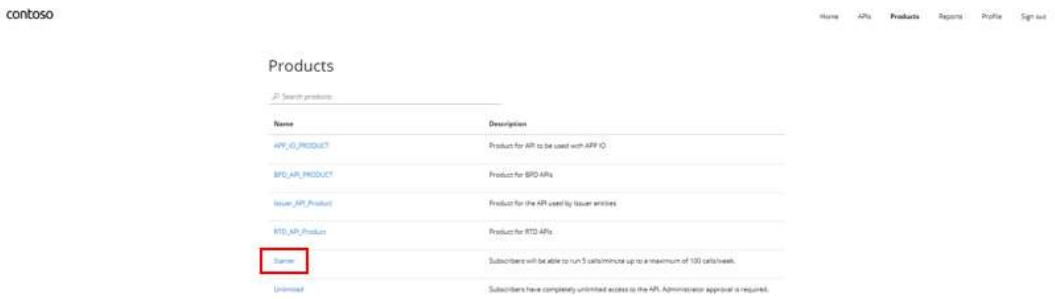


Una volta fatto riceveremo via mail le configurazioni necessarie per terminare la verifica tramite un link.

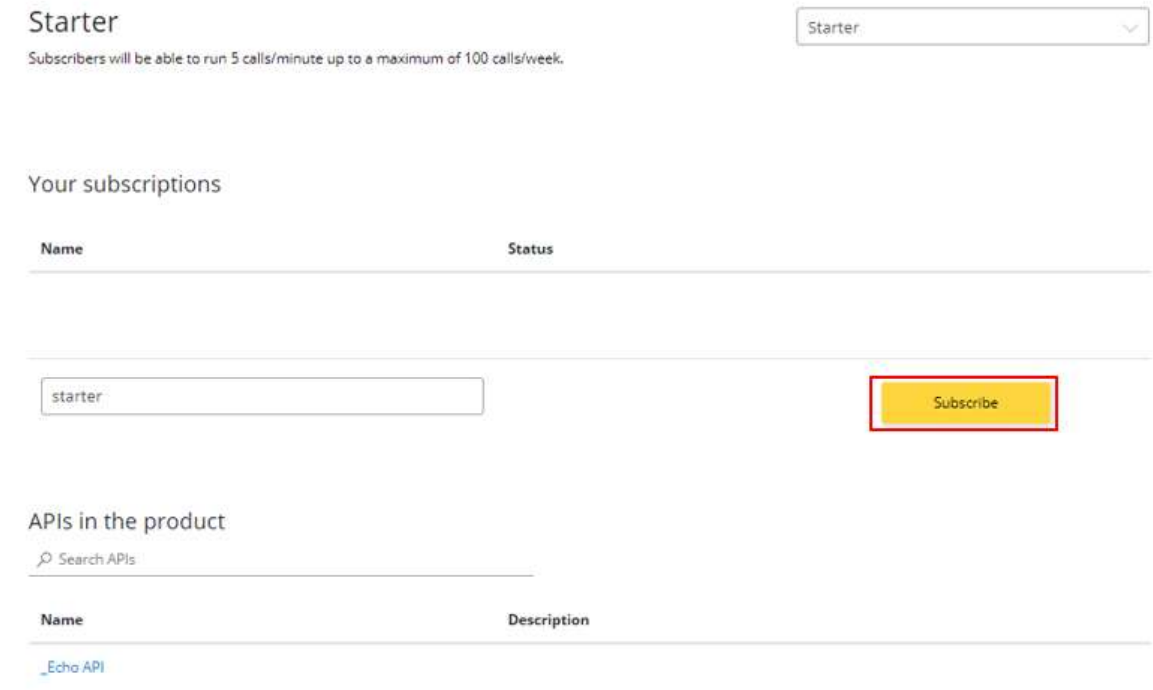
Dopo aver cliccato sul link contenuto nella mail si verrà reindirizzati alla pagina di login nella quale bisognerà autenticarsi con l'utenza creata, a questo punto per creare la subscription e le relative chiavi bisognerà selezionare l'opzione Products



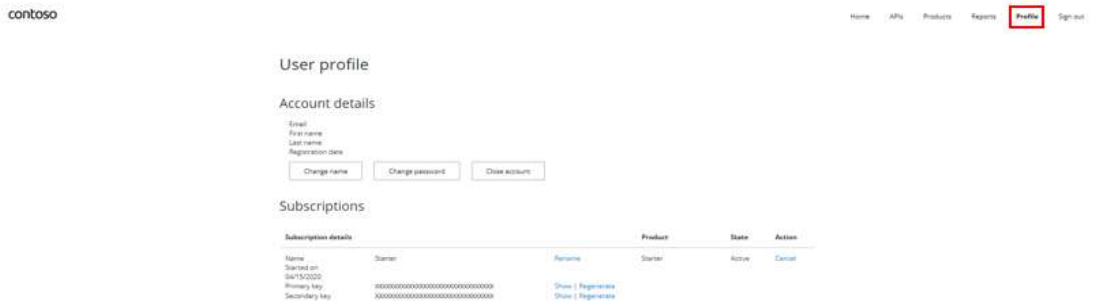
A questo punto bisognerà selezionare la tipologia di sottoscrizione



inserire un nominativo e selezionare l’opzione subscribe



l'esito della sottoscrizione sarà visibile alla voce Profile del menu'



Appendice 9 - Ambienti

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	-	-