CAPITOLATO

PROCEDURA NEGOZIATA SENZA PREVIA PUBBLICAZIONE DEL BANDO DI GARA, AI SENSI DELL'ART. 75 DEL D-L 17 MARZO 2020, N. 18 E DELL'ART. 63, CO. 2, LETT. C) DEL D.LGS. 18 APRILE 2016, N. 50, PER L'AFFIDAMENTO DELL'IMPLEMENTAZIONE PER L'AFFIDAMENTO DELL'IMPLEMENTAZIONE DELLA SOLUZIONE TECNOLOGICA CHECK-IBAN E DEI SERVIZI EVOLUTIVI -

CIG 8284797EC0

Introduzione

PagoPA S.p.A. (nel seguito anche "**PagoPA**" o la "**Società**") è alla ricerca di un fornitore che possa offrire sia (1) lo sviluppo di una soluzione tecnologica specifica di cui potranno beneficiare anche gli Enti Pubblici e Privati interessati ("Enti Fruitori"), volta *inter alia* alla validazione dell'IBAN, al fine di consentire agli Enti Fruitori di verificare, in particolare, la corretta corrispondenza tra l'identificativo di conto corrente (IBAN) ed i dati identificativi dell'intestatario del conto stesso - codice fiscale o partita IVA (nel seguito "**Soluzione Check-iban**"); sia (2) servizi di sviluppo tecnologico a consumo per la realizzazione di eventuali ulteriori soluzioni tecnologiche da integrare ai progetti che fanno capo alla Società ("**Servizi Evolutivi**").

1. Soluzione Check-iban

In primis, PagoPA intende, dunque, realizzare la "Soluzione Check-iban" volta, nella sua prima funzionalità ed impiego, a consentire la verifica dell'effettivo collegamento fra persone fisiche o giuridiche e codici IBAN da essi forniti. Tale soluzione verrà realizzata al fine di garantire agli Enti interessati (nel seguito anche "Enti Fruitori") la possibilità concreta di effettuare una validazione degli IBAN forniti dai propri utenti i quali ad esempio, nel corso dei prossimi mesi, vorranno aderire ai provvedimenti di stimolo ed aiuto che saranno implementati per far fronte alla grave crisi economica derivante dalla pandemia Covid-19 attualmente in corso.

Punti cardine della Soluzione Check-iban richiesta sono:

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

- ❖ capacità di effettuare la validazione in modalità sincrona ed in real-time abilitando così gli enti pubblici alla realizzazione di applicativi performanti, resilienti e garantendo alta scalabilità della soluzione complessiva.
- ❖ utilizzo di uno standard di mercato riconosciuto, ben noto e frutto delle migliori "best-practices" sul mercato: Open API.
- ❖ possibilità futura di espandere tale piattaforma applicativa ad altri moduli applicativi (VAS - Servizi a Valore Aggiunto) i quali, secondo il paradigma "open banking", possano rappresentare un nuovo modo di gestire lo scambio di dati tra banche e pubbliche amministrazioni garantendo, nel contempo, rapidi tempi di sviluppo dei casi d'uso e semplicità di implementazione per tutti gli enti coinvolti.

PagoPA, dunque, ricerca un fornitore tecnologico qualificato in grado di implementare una piattaforma API tramite la quale erogare tale Soluzione Check-iban, che sia in grado - *inter alia* - di esporre funzioni per lo scambio di dati che rendano semplice e "normalizzato" l'accesso a informazioni strutturate provenienti dal sistema bancario italiano.

1.1. Descrizione della Soluzione Check-iban

(a) Perimetro delle funzionalità richieste

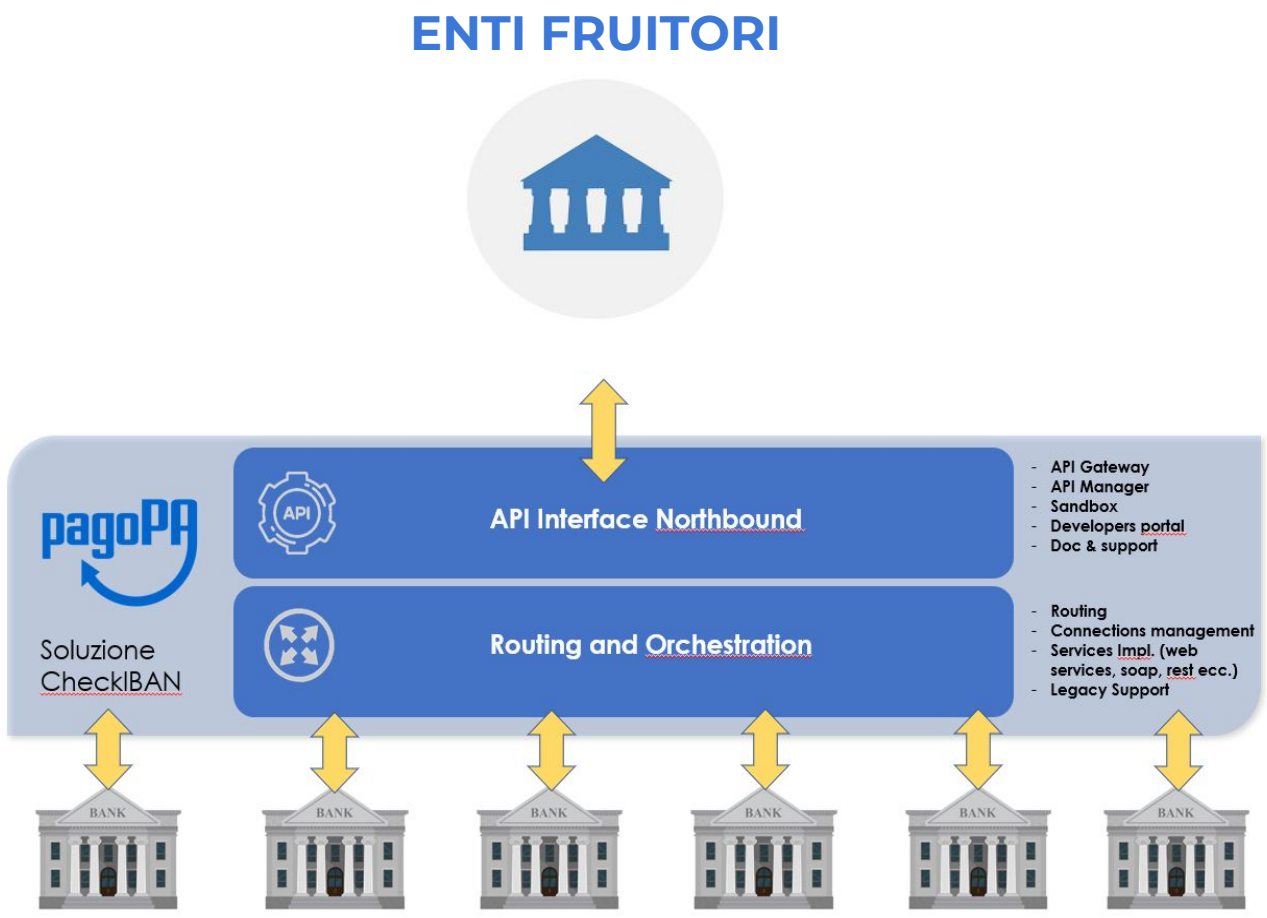
L'architettura di alto livello della Soluzione Check-iban si pone come punto di scambio delle informazioni tra PagoPA e gli Istituti di radicamento dei conti di pagamento ovvero i Payment Service Provider (PSP).

In particolare, la Soluzione Check-iban:

- dovrà consentire agli Enti Fruitori di poter avere a disposizione un'unica interfaccia API REST esposta sulla rete Internet per la verifica della corrispondenza tra IBAN e dati identificativi dell'intestatario;
- agirà da gateway per l'instradamento delle richieste di verifica presso i vari Istituti di radicamento dei conti, avendo preventivamente integrato in modo opportuno le interfacce messe a disposizione da questi ultimi;

- effettuerà le necessarie operazioni di “protocol routing” tali da garantire ai PSP la possibilità di fornire in tempo reale i dati scegliendo fra una gamma di modalità quella che sia la più confortevole secondo i propri bisogni.

L’architettura di business risulta così definita:



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

Il fornitore deve **realizzare e manutenere** la Soluzione Check-iban nelle sue diverse componenti ossia:

- **modulo** CORE denominato **API Interface Northbound** (Api Gateway)
- **modulo** CORE denominato **Request Router** il quale orchestra e instrada le chiamate verso gli istituti bancari
- **eventuali moduli VAS offerti** in sede di offerta tecnica per ampliare le funzionalità della soluzione.

(b) Modalità di erogazione e caratteristiche architetturali

La modalità di erogazione della Soluzione deve essere quella del modello SaaS - dove quindi il fornitore si impegna a realizzare la soluzione software e a garantirne l'esercizio su sistemi propri o di terzi. Il fornitore dunque potrà erogare la Soluzione Iban-check con *hosting* su *data center* interno al fornitore ovvero su cloud, senza nessun onere ulteriore da addebitare alla PagoPA S.p.A. oltre quelli già compresi nell'offerta. Qualora la modalità di erogazione scelta dal fornitore sia quella su modello cloud, il fornitore dovrà altresì garantire l'utilizzo di un CSP (Cloud Service Provider) qualificato nell'ambito del *Cloud Marketplace* di AgID (piattaforma che espone i servizi e le infrastrutture qualificate da AgID secondo quanto disposto dalle Circolari AgID n. 2 e n.3 del 9 aprile 2018) per l'erogazione di servizi SaaS per il Cloud della PA e in possesso dei rispettivi requisiti così come definiti nelle circolari AgID applicabili.
Nell'erogazione della Soluzione, considerata anche la sua natura e dei dati trattati nell'ambito del medesimo, si richiede che il fornitore:

- sia dotato di un adeguato* piano di Disaster Recovery, formalizzato attraverso un piano di Business Continuity che garantisca parametri di RTO (Recovery Time Objective) non superiori alle 12 (dodici) ore;
- rispetti adeguate* caratteristiche di sicurezza informatica e contrasto al cybercrime;
- sia dotato di un'adeguata* organizzazione interna, volta a garantire livelli di servizio di eccellenza nell'erogazione dei servizi ICT;
- garantisca il collegamento tecnologico attraverso apposite VPN (*Virtual Private Network*), dal proprio *data center*, tutti i PSP ed i centri servizi aderenti alla soluzione che lo richiedano;

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

- ❖ garantisca massima scalabilità e capacità di gestire grandi volumi di richieste*
- ❖ garantisca su base trimestrale i seguenti **Livelli di Servizio** (i) una disponibilità del servizio pari almeno a 99.8%; (ii) una latenza non superiore a 500ms tra le interfacce Northbound e l'istituto di pagamento per almeno il 99,5% delle *calls*; e (iii) tempo di risoluzione massimo di ciascuna segnalazione pari ad 12 (dodici) ore per *bug* bloccante/critico.*
- ❖ garantisca un contatto privacy dedicato all'interno dell'organizzazione del fornitore ("**Referente Privacy**") ed il rispetto dei seguenti ulteriori **Livelli di Servizio** minimi, in aggiunta a quanto previsto al punto successivo, con riferimento a tematiche privacy e di privacy compliance della soluzione: (i) il Referente Privacy deve avere una seniority di almeno 4 anni su tematiche privacy ed essere parte dell'ufficio del DPO (ii) in caso di richiesta di assistenza su tematiche privacy, il Referente Privacy deve fornire un primo riscontro con conferma di presa in carico entro 24 ore, 7 giorni su 7, e con immediata fornitura di tempistiche certe di riscontro/attuazione/output (iii) il Referente Privacy deve assicurare la produzione della documentazione richiesta senza ingiustificato ritardo e comunque in nessun caso **non** oltre 7 (sette) giorni lavorativi dal riscontro di cui al punto (ii) sopra, salvo diverso termine concordato con la Società.
- ❖ predisponga e presenti una Data Protection Impact Assessment (DPIA) della Soluzione Check-iban entro 10 (dieci) giorni dall'aggiudicazione.

*__N.B.__ *Questi aspetti e l'adeguatezza degli stessi rispetto alle aspettative della Stazione appaltante saranno valutati in sede di offerta tecnica nei termini e nelle modalità indicati nel par. 24 del Disciplinare di gara ed esplicitati altresì nel template della relazione tecnica al medesimo allegato.*

(c) Caratteristiche del Modulo "API Interface Northbound"

Il modulo "API Interface Northbound" si occuperà di esporre le API che verranno richiamate dalle procedure degli Enti Pubblici. Tale modulo dovrà:

1. **utilizzare uno strumento di API Gateway** in grado di esporre "API REST" con uno specifico end-point che esponga una funzione di validazione dell'effettivo collegamento IBAN<->Codice Fiscale oppure IBAN<->Partita IVA e restituisca in

output anche l'informazione accessoria riguardante la presenza di eventuali cointestatari o meno del conto in oggetto.

A titolo di esempio l'end point previsto potrebbe essere così definito:

Endpoint
POST {domain-for-pagopa}/api/pagopa/banking/v4.0/utils/validate-account-holder

Pertanto, dato il suddetto esempio di endpoint, le *requests* e le *responses* devono essere le seguenti:

Options
L'endpoint presenta parametri opzionali per consentire la necessaria flessibilità funzionale:

a. *?require-single=true*
Parametro opzionale che consente di richiedere che il check di corrispondenza abbia successo solo se l'intestatario indicato è anche l'unico intestatario (esclude i conti con intestazioni multiple).

Request

```
{
        "account": {
                "value": "IT23J0326822300123456789012",
                "valueType": "IBAN | BBAN",
                "bicCode": null
        },
        "accountHolder": {
                "holderId": "MRLFNC81L04A859O",
                "type": "PERSON_NATURAL | PERSON_LEGAL"
        }
}
```

Parametro		Tipo di dato	Note
Account	obbligatorio	JSON Object	
account.value	obbligatorio	String	
account.valueType	obbligatorio	Enum : {IBAN | BBAN }	BBAN consente di specificare il conto corrente come coppia numero conto e codice BIC (riservato per usi futuri)
account.bicCode	opzionale	String	Codice BIC della banca di radicamento del conto (riservato per usi futuri)
accountHolder	obbligatorio	JSON Object	
accountHolder.holderId	obbligatorio	String	
accountHolder.type	obbligatorio	Enum: {PERSON_NATURAL | PERSON_LEGAL}	

Response

```
{
        "validationStatus": "OK | KO",
```

```
        "account": {
                "value": "IT23J0326822300123456789012",
                "valueType": "IBAN",
                "bicCode": null,
                "status": "OPERATIONAL | BLOCKED | CLOSED | MIGRATED"
        },
        "accountHolder": {
                "holderId": "MRLFNC81L04A859O",
                "type": "PERSON_NATURAL | PERSON_LEGAL",
                "relation": "SINGLE | MULTI"
        }
}
```

Parametro		Tipo di dato	Note
validationStatus	obbligatorio	Enum: {OK | KO}	Risultato della validazione
Account	obbligatorio	JSON Object	
account.value	obbligatorio	String	
account.valueType	obbligatorio	Enum : {IBAN | BBAN }	
account.bicCode	opzionale	String	
account.status	opzionale	Enum: {OPERATIONAL | BLOCKED | CLOSED | MIGRATED}	Stato del conto corrente (se disponibile)
accountHolder	obbligatorio	JSON Object	
accountHolder.holderId	obbligatorio	String	
accountHolder.type	obbligatorio	Enum: {PERSON_NATURAL | PERSON_LEGAL}	
accountHolder.type	opzionale		Tipologia di intestazione (se disponibile) SINGLE: indica che l'intestatario è l'unico per il conto MULTI: indica che il conto ha una intestazione multipla con altri soggetti

Si chiarisce che l'endpoint indicato è a titolo di esempio, L'EndPoint definitivo andrà confermato dalla Società prima di rilasciare il prodotto.

2. **Esporre un ambiente di test** (sandbox) che consenta agli sviluppatori degli Enti Fruitori l'integrazione della soluzione.
3. **Gestire in sicurezza l'accesso alle API mediante** un meccanismo di identity management delle API REST basato su API Key. Il fornitore dovrà inoltre mettere a disposizione un'area riservata della soluzione che consenta di:
    a. Generare e scaricare la propria identità segreta (API KEY).
    b. Impostare gli indirizzi IP o i range di indirizzi in modalità "white list" da cui abilitare le invocazioni.
    c. Potere eventualmente disabilitare l'operatività come condizione di emergenza in caso di problemi di sicurezza sulle proprie infrastrutture collegate in modalità "Server2Server"

d. Accesso alla visualizzazione dei propri log delle chiamate API verso il gateway
e. Opportuna gestione e profilazione dei poteri delle utenze nei portali per gestire abilitazioni in lettura/scrittura

Il fornitore si impegna a definire e mettere a disposizione meccanismi di connessione con cui vengono abilitati gli enti, da valutarsi di volta in volta anche in base alle esigenze di questi ultimi.

4. **Avere un sistema di logging di tracing/logging** delle chiamate incluse le sotto chiamate interne ad ogni singola invocazione con un apposito strumento di ricerca tale da consentire una adeguata attività di "troubleshooting" e di ricostruzione forense dell'invocazione alle chiamate.

Si evidenzia altresì che il fornitore dovrà rendere disponibile adeguata documentazione per gli sviluppatori degli Enti Fruitori e dei PSP sotto forma di volta in volta di: Documentazione online, manuali, file swagger.

(d) Caratteristiche del Modulo "Router and Orchestration"

Il modulo "Router and Orchestration" è un'interfaccia "Southbound" che consente la comunicazione con gli Istituti di radicamento dei conti che il fornitore provvederà ad integrare in modo opportuno per consentire il corretto routing e l'esecuzione diretta delle richieste di verifica.
Tale routing verrà effettuato basandosi sull'IBAN fornito, che sarà il discriminante per l'invocazione del singolo Istituto connesso.

Dal punto di vista architetturale, le interconnessioni con gli Istituti di radicamento dei conti devono tenere in considerazione per quanto possibile le specificità di ciascun Istituto. Al fine di limitare la numerosità delle integrazioni da effettuare, il fornitore deve proporre una serie di alternative relative alle modalità di interconnessione ed ai dati scambiati, in modo da definire quanto più possibile una gamma di interfacce "standard" per il dialogo con ciascun Istituto, tenendo presente che i requisiti primari che devono essere soddisfatti dai servizi messi a disposizione da ciascun Istituto di radicamento dei conti sono o possono essere (dove indicato come opzionale) i seguenti:

a. Modalità di esecuzione sincrona (ossia capacità di fornire la risposta direttamente in relazione a ciascuna richiesta senza prevedere esecuzioni di tipo batch o con callback per la restituzione del risultato della verifica).
b. Accettazione obbligatoria in input dell'identificativo di conto corrente (IBAN) e del soggetto di cui si richiede verifica (codice fiscale o partita IVA).
c. Accettazione in input (opzionale) della richiesta di verifica dell'esclusività di intestazione del conto corrente.
d. Erogazione obbligatoria nell'output dell'esito della verifica.
e. Erogazione nell'output (opzionale) del tipo di intestazione del conto corrente (intestazione singola o multipla).
f. Erogazione nell'output (opzionale) dello stato del conto corrente (distinguendo se operativo, bloccato o chiuso).

Nell'ambito di questa gamma di funzioni che verranno esposte dai PSP, il fornitore dovrà garantire l'accesso agli Istituti di radicamento dei conti tramite le seguenti modalità di interconnessione:

a. Interfacce API REST (JSON over HTTP)
b. Web Services SOAP
c. Flussi batch (SFTP, Thema..)

Il fornitore si impegnerà, quindi, a definire delle interfacce standard di comunicazione valide per tutti i protocolli e a gestire l'integrazione di almeno 15 istituti di credito/centri servizi/aggregatori.

Inoltre il fornitore gestirà come metodi di autenticazione per l'accesso alle interfacce dei singoli Istituti le seguenti modalità:

- modalità di trasporto (tutte):
  a. Internet pubblica (a cui aggiungere obbligatoriamente una modalità di autenticazione a livello applicativo)
  b. Connessione TLS con mutua autenticazione (single o mutual con possibilità di utilizzare certificati EiDAS)
  c. VPN punto-punto opportunamente configurata con ciascun Istituto

- modalità di autenticazione a livello applicativo. Tali modalità devono ricadere tra (almeno una delle seguenti):
  a. Una delle modalità di HTTP Authentication (basic o bearer)
  b. Utilizzo di APIKey
  c. OAuth 2.0 for server2server connection.

Il fornitore dovrà altresì garantire, qualora il singolo istituto lo richiedesse, l'uso di certificati di firma EiDAS di sigillo per la firma digitale dell'invocazione su ciascuna API Call.

*__N.B.__ *Le alternative proposte saranno valutate in sede di offerta tecnica nei termini e nelle modalità indicati nel par. 24 del Disciplinare di gara ed esplicitati altresì nel template della relazione tecnica al medesimo allegato.*

(e) Processi a supporto e manutenzione ordinaria e correttiva

Il fornitore garantirà, durante la vigenza del contratto, a supporto della Soluzione Check-iban, l'erogazione dei seguenti servizi:

1. supporto allo sviluppo del software tramite opportuno tool di ITMS
2. Supporto per "problem-management" tramite opportuno tool di ITMS
3. manutenzione ordinaria e correttiva della Soluzione Check-iban
4. manutenzione della documentazione per gli sviluppatori
5. attività di migrazione della Soluzione Check-iban verso altro fornitore, ovvero da una soluzione di *hosting* ad un'altra

Con riferimento ai processi a supporto, il Fornitore si impegna a trovare un accordo con la Società su modalità e processi di *problem-management* e relativi livelli di servizio.

(f) Gestione

Il fornitore garantirà, durante la vigenza del contratto:

1. la gestione della Soluzione Check-iban, comprensiva delle vpn

2. la gestione delle “calls” fino ad un massimo di 150.000.000 (centocinquanta milioni) *calls*/anno e relative attività connesse

Il servizio di gestione verrà remunerato a consumo sulla base delle effettive *calls/anno* gestite dal fornitore durante l’erogazione della Soluzione Check-iban.

Con riferimento alla gestione, il Fornitore si impegna a trovare un accordo con la Società su modalità e processi di *problem-management* e relativi livelli di servizio.

2. *Servizi evolutivi*

Al fine di provvedere a sviluppi **evolutivi** della Soluzione Check-iban (diversi dai VAS inclusi nell’offerta tecnica) ovvero ad altre attività evolutive, legate a servizi tecnologici relativi al ‘mondo bancario’ e dei pagamenti e per lo sviluppo di funzionalità inerenti ai progetti che fanno capo alla Società, volti a favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, potranno essere richieste al fornitore, durante il periodo di esecuzione del contratto, giornate uomo, a consumo, di profili professionali che abbiamo expertise nell’architettura, sviluppo e gestione di soluzioni tecnologiche del tipo descritto, entro il limite massimo di 600 giornate uomo.

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