SPECIFICHE DI CONNESSIONE AL SISTEMA PAGOPA

DOCUMENTO MONOGRAFICO INTEGRATO ALLE SANP2.0

Versione 2.2 ***- Febbraio 2019***

Stato del documento

revisione	data	note
1.0	Ottobre 2017	Prima stesura in bozza
1.0.3	Febbraio 2018	Versione approvata
2.2	Febbraio 2019	Versione aggiornata

Sintesi dei cambiamenti

lista dei principali cambiamenti rispetto la revisione precedente:
Razionalizzazione delle modalità di connessione al Sistema pagoPA e precisazione sulle misure di sicurezza minime per i soggetti direttamente aderenti

Redazione del documento	Verifica del documento
Mauro Bracalari; Mario Gammaldi; Giulia Montanelli; Gianni Papetti	Mauro Bracalari; Giulia Montanelli

Indice dei contenuti

DEFINIZIONI E ACRONIMI

Definizione / Acronimo	Descrizione
AgID **Agenzia per l'Italia Digitale**	Istituita ai sensi del decreto legge n. 83 del 22 giugno 2012 convertito con legge del 7 agosto 2012, n. 134, è il gestore del "Sistema pagoPA-SPC"
EC **Enti creditori**	Le pubbliche amministrazioni definite nell'articolo 2, comma 2 del CAD ed i gestori di pubblici servizi "nei rapporti con l'utenza".
Sistema pagoPA **Sistema pagoPA - SPC**	Piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le Pubbliche Amministrazioni e i Prestatori di Servizi di Pagamento di cui all'art. 81, comma 2 bis del CAD
PSP **Prestatore di Servizi di Pagamento**	Banche, Istituti di pagamento o moneta elettronica, abilitati da Banca d'Italia ad effettuare servizi di pagamento
RT **Ricevuta Telematica**	Oggetto informatico inviato dal PSP all'Ente creditore attraverso il Sistema pagoPA-SPC in risposta ad una Richiesta di Pagamento Telematico effettuata da un Ente creditore .
SANP	Specifiche Attuative del Sistema pagoPA-SPC - Allegato B alle "Linee guida per l'effettuazione dei pagamenti elettronici a favore delle pubbliche amministrazioni e dei gestori di pubblici servizi"

1 Introduzione

Il presente documento fornisce le specifiche di dettaglio destinate ai soggetti aderenti (EC e/o PSP) del sistema pagoPA per l'applicazione del nuovo modello di interoperabilità predisposto per l'attestazione al sistema.

2 Specifiche di connessione

Qualsiasi soggetto direttamente aderente a pagoPA può attivare e gestire una connessione diretta al NodoSPC. Si fa presente che con il termine "connessione diretta" si intende sempre l'insieme complessivo dei collegamenti ridondati fra un sito primario e uno di backup (sito secondario da attivarsi in caso di *disaster recovery*) del soggetto direttamente aderente ai corrispondenti siti primario e backup di erogazione del servizio. Il dimensionamento della connessione diretta è stabilità dal soggetto direttamente aderente il quale è sottoposto al rispetto di requisiti di disponibilità, performance e sicurezza. Il NodoSPC rende inoltre disponibile un sito di test esterno a cui si potrà accedere nel rispetto dei medesimi requisiti di sicurezza.

Il NodoSPC è raggiungibile di default da rete Internet o da rete SPC Infranet.

Il NodoSPC si rende inoltre disponibile a valutare modalità di connessione alternative purché la soluzione proposta dal soggetto direttamente aderente rispetti i seguenti requisiti minimi:

- osservanza degli SLA di cui al documento "*Indicatori di Qualità per i Soggetti Aderenti*";
- invarianza dei livelli di sicurezza del sistema pagoPA;
- non comporti assunzione di ulteriore responsabilità da parte del sistema pagoPA;
- non comporti l'assunzione di ulteriori oneri a carico del sistema pagoPA.

In ogni caso, per qualsiasi modalità di connessione, il soggetto direttamente aderente dovrà comunque garantire l'utilizzo di connettività ridondata ad alte prestazioni sia per il sito primario che per il secondario dedicato al *disaster recovery*.

Di seguito si descrivono nel dettaglio le soluzioni di default che ogni soggetto ha facoltà di adottare senza ulteriori formalità e le possibilità alternative disponibili.

2.1 Connessioni di default

2.1.1 Connessione a pagoPA mediante rete Internet

Il soggetto direttamente aderente può connettersi al sistema pagoPA usufruendo della connettività mediante rete Internet, nel rispetto dei seguenti vincoli:

- utilizzo del protocollo di trasporto *https* con canale cifrato e autenticato mediante *Transport Layer Security* (TLS) versione 1.2 o superiore, abilitando la mutua autenticazione tra le parti (*client-authentication*). A tal fine è obbligatorio l'utilizzo di certificati digitali x.509 per la creazione del canale TLS. Il sistema pagoPA autenticherà sempre l'aderente controparte, sia in fase di ricezione delle richieste (*client-authentication*), sia in fase di spedizione delle stesse (*server-authentication*);
- utilizzo di IP pubblici statici nelle regole di NAT, da non modificare se non preventivamente concordato con il NodoSPC.

2.1.2 Connessione a pagoPA mediante rete SPC Infranet

Si fa presente che la connessione tramite rete SPC mediante Porta di Dominio è deprecata.

Pertanto, i soggetti già connessi al NodoSPC tramite rete SPC Infranet o di nuova attivazione, potranno connettersi al NodoSPC nel rispetto dei vincoli previsti al § 2.1.1 per la rete Internet.

2.2 Modalità alternative di connessione

Nel presente paragrafo sono descritte le modalità alternative di connessione disponibili che, per qualsiasi motivo, il soggetto direttamente aderente intenda adottare.

2.2.1 Attestazione del NodoSPC a rete privata

Il NodoSPC può attestarsi su una rete privata purché la stessa abbia caratteristiche di rilevanza nell'ambito del sistema pagoPA. Il NodoSPC garantisce altresì nel tempo la continuità di tale attestazione al servizio purché permangano le condizioni precedentemente individuate per le modalità di connessione alternative.

Il soggetto attestato su una rete privata a cui partecipa il NodoSPC e che intenda usufruire di tale modalità, dovrà darne comunicazione a pagoPA. La procedura di configurazione della connessione sarà comunicata al soggetto direttamente aderente dal gestore del NodoSPC che effettuerà le verifiche previste.

Il NodoSPC, oltre alla rete SPC, è già attestato sulla rete Sianet (rete privata gestita dalla società SIA) in virtù della constatazione che numerosi PSP operanti in Italia già impiegano tale rete per il proprio business.

2.2.2 Connessione con il gestore del NodoSPC

Il NodoSPC può autorizzare i soggetti direttamente aderenti a connettersi utilizzando modalità eterogenee rese disponibili dal gestore del NodoSPC stesso. In tale circostanza è necessaria l'instaurazione di un rapporto contrattuale con il gestore della connessione da esibire a pagoPA. Esempi di connessioni già autorizzate sono rappresentati da linee dedicate con gestione *in house* degli apparati di terminazione o connessioni mediante VPN.

In linea generale tale tipo di connessione rappresenta una soluzione custom e pertanto ogni soggetto direttamente aderente che intenda avvalersi di tale possibilità provvede in maniera autonoma sia in termini tecnici sia in termini di costi associati.

Nel caso in cui venissero a mancare le condizioni che consentono il perdurare dell'attestazione al NodoSPC, ogni soggetto direttamente aderente interconnesso tramite tali modalità non sarà in alcun modo mallevato da pagoPA e dovrà farsi carico di ogni onere connesso alle attività di migrazione che si dovessero rendere necessarie, al rispetto delle tempistiche previste e al mantenimento dei livelli di servizio richiesti.

2.2.3 Misure di sicurezza

L'accesso alle risorse del sistema pagoPA è consentito attraverso il riconoscimento del soggetto direttamente aderente a livello di connettività fisica mediante una "*white list*" centrale, contenente gli indirizzi IP dei sistemi perimetrali dei soggetti direttamente aderenti autorizzati all'accesso.

Pertanto, la raggiungibilità del sistema pagoPA sarà garantita esclusivamente alla condizione che si utilizzino gli indirizzi IP già comunicati nel corso della procedura di attivazione e di conseguenza censiti all'interno della *white list*.

Oltre a quanto dichiarato nelle modalità di connessione, il soggetto direttamente aderente dovrà adottare il seguente insieme minimo di misure di sicurezza:

- funzionalità di gestione degli accessi e tracciatura:
  - raccolta delle connessioni, invocazioni SOAP sia in ingresso che in uscita su supporti di memorizzazione che ne garantiscano l'integrità e tracciatura nel tempo. A titolo esemplificativo e non esaustivo si menzionano: sistemi SIEM, server SYSLOG, apparati o applicazioni di Data Analytics & Management;
  - filtraggio delle connessioni provenienti da sorgenti di traffico non autorizzate, al fine di evitare accessi indebiti;
  - storicizzazione dei log diagnostici delle applicazioni utilizzate per pagoPA a supporto dell'accertamento di malfunzionamenti.

    Le informazioni raccolte attraverso tali funzionalità devono essere rese disponibili secondo modalità, tempistiche e formati specificati nel documento "*Indicatori di Qualità per i Soggetti Aderenti*".
- *best practice* di controllo, disaccoppiamento e filtraggio tipici dei servizi esposti su rete pubblica:
  - architetture multi-layer (*presentation – application - persistence*), con segregazione in DMZ distinte, sotto-reti sicure per RDBMS e server applicativi;
  - protezione dei *web server* tramite infrastruttura di firewall, Proxy/Reverse Proxy, Web Application Firewall;
  - configurazioni di sicurezza di sistema avanzate da adottare sui sistemi che ospitano le applicazioni web (es. SELinux/CHRoot su sistemi Linux Red Hat):
- processi canonici di verifica dei livelli di sicurezza da applicare semestralmente:
  - attività di *Vulnerability Assessment* di tutte le componenti infrastrutturali ed applicative che concorrono all'erogazione dell'applicazione pagoPA;
  - attività di *Penetration Testing* del *web application* destinate all'Utilizzatore finale.

Si fa presente che è fatto obbligo al soggetto direttamente aderente di fornire riscontro in merito all'applicazione delle suddette misure minime di sicurezza attraverso la produzione di documentazione dedicata da presentare a pagoPA, secondo quanto specificato nella Sezione IV delle SANP.

3 Procedura di attivazione della connessione di *default*

La procedura è identica per la connessione a ogni ambiente del sistema pagoPA: sito di test esterno, sito primario di produzione, sito secondario di *disaster recovery*:

1) il soggetto direttamente aderente a pagoPA deve dotarsi di un certificato digitale X509 Extended Validation emesso da una Certification Authority che compaia fra i membri del CA/Browser Forum (https://cabforum.org/members/). È facoltà del NodoSPC autorizzare la connessione utilizzando un certificato emesso da differente CA e autorizzare la connessione all'ambiente di test esterno utilizzando altro tipo di certificato;
2) il campo "*Subject*" di ogni certificato deve contenere un CN coerente con il FQDN della URL del servizio che intende esporre;
3) pagoPA espone il servizio Portale delle Adesioni per la configurazione automatica del soggetto direttamente aderente. Il Referente Tecnico di un soggetto direttamente aderente che disponga di un accesso a tale servizio fornisce i certificati digitali tramite apposita funzione di *uploading*. I soggetti direttamente aderenti che non dispongono di accesso al Portale delle Adesioni inviano i certificati tramite PEC all'indirizzo protocollo.pec@agid.gov.it ;
4) devono essere fornite, per le opportune configurazioni nell'infrastruttura del sistema pagoPA, le seguenti informazioni:
   a) indirizzo IP del sistema fruitore dei *web services* esposti dal sistema pagoPA;
   b) indirizzo IP e porta di esposizione dei *web services* esposti dal soggetto direttamente aderente;
   c) *url* del servizio applicativo che si intende esporre nel formato: https://FQDN/nomeservizio. Lo FQDN deve coincidere con il CN specificato al precedente 2).

In fase di avvio della procedura di attivazione, saranno rese disponibili al soggetto direttamente aderente le seguenti informazioni:

- indirizzo IP del sistema pagoPA per l'utilizzo dei *web services* esposti dal soggetto direttamente aderente;
- indirizzo IP e porta di esposizione dei *web services* esposti dal sistema pagoPA;
- certificato digitale X509 del sistema pagoPA.

La procedura di attivazione si conclude con la verifica della reciproca raggiungibilità dei sistemi.

FINE DOCUMENTO