Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

SPECIFICHE DI CONNESSIONE AL SISTEMA PAGOPA

DOCUMENTO MONOGRAFICO INTEGRATO ALLE SANP2.0

Versione 1.0.3 ***- Febbraio 2017***

Stato del documento

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

Sintesi dei cambiamenti

lista dei principali cambiamenti rispetto la revisione precedente:
Revisione del testo

Redazione del documento	Verifica del documento
Alberto Carletti; Mauro Bracalari; Giulia Montanelli	Antonio Samaritani

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 "Nodo dei Pagamenti-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".
NodoSPC **Nodo dei Pagamenti - SPC**	Piattaforma tecnologica per l'interconnessione e l'interoperabilutà 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 Nodo dei Pagamenti-SPC in risposta ad una Richiesta di Pagamento Telematico effettuata da un Ente creditore .
SANP	Specifiche Attuative del Nodo dei Pagamenti-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 specifiche di dettaglio destinate ai soggetti aderenti (EC e/o PSP) del sistema pagoPA per l'applicazione del Nuovo modello di Interoperabilità emanato da AgID.

2 Specifiche di connessione

Dalla pubblicazione delle presenti specifiche la connessione diretta diventa la modalità di colloquio tecnico di default, attivabile da qualsiasi soggetto direttamente aderente. Nel seguito sono riportati i requisiti di sintesi e le relative specifiche di connessione:

- L'utilizzo della busta di e-gov gestita nel modello SPCoop è deprecato.
- Per la connessione è obbligatorio l'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 v3 Extended Validation per la creazione del canale TLS. Il Nodo dei Pagamenti autenticherà sempre l'Aderente controparte, sia in fase di ricezione delle richieste (Client-authentication), sia in fase di spedizione delle richieste (Server-authentication). AgID potrà derogare a tale obbligo nel caso esistano analoghe condizioni di trust per l'identificazione dell'organizzazione aderente.
- Per quanto riguarda la connettività fisica, è possibile l'accesso, anche in modalità infranet, mediante SPC per i Soggetti che possono o devono utilizzare tale sistema, in accordo con il CAD. I Soggetti che non utilizzano SPC acquisiscono dal mercato equivalenti servizi di connettività di rete pubblica internet, purché ridondati e comunque in grado di garantire gli stessi livelli di continuità operativa, con particolare attenzione ai collegamenti relativi ai siti primario/backup dei Soggetti con i corrispondenti siti di erogazione di pagoPA. In tal caso l'Aderente deve dotarsi di servizi di connettività che garantiscano la univocità e staticità degli indirizzi IP.
- Per quanto riguarda le misure di sicurezza, sono previsti due distinti livelli di controllo degli accessi degli Aderenti alla infrastruttura centrale del Nodo dei Pagamenti.
    - Il primo livello è rappresentato dal processo di autorizzazione basato sull'identificazione dell'Aderente a livello di connettività fisica mediante una "white list" centrale contenente gli indirizzi IP dei sistemi degli Aderenti autorizzati all'accesso all'infrastruttura centrale del Nodo dei Pagamenti, limitando pertanto la raggiungibilità dei sistemi che implementano il servizio stesso. Si sottolinea che gli indirizzi IP comunicati nel corso della Procedura di Attivazione saranno i soli autorizzati ad accedere ai servizi del Nodo dei Pagamenti.
    - Il secondo livello è rappresentato dal processo di autorizzazione basato sull'identificazione dell'Aderente mediante utilizzo dei certificati x.509 di cui sopra associati a ogni Aderente e necessari per instaurare il canale TLS di collegamento con l'infrastruttura centrale del Nodo dei Pagamenti.
- Oltre alle misure indicate sopra, il Soggetto Aderente deve implementare almeno le seguenti ulteriori funzionalità di gestione degli accessi e tracciatura:
    - Raccolta delle invocazioni ricevute;
    - Filtraggio delle richieste, al fine di evitare accessi indebiti;
    - Storicizzazione dei dati a supporto della diagnosi di malfunzionamenti.
- Devono inoltre essere adottati da parte del Soggetto Aderente i meccanismi di controllo, disaccoppiamento e filtraggio tipici dei servizi esposti su rete pubblica e segnatamente:

- Architetture multi-layer, con segregazione in DMZ distinte tra Database e server applicativi;
- Protezione dei Web server tramite infrastruttura di firewall, Proxy/Reverse Proxy
- Configurazioni di sicurezza di sistema avanzate da adottare sui sistemi che ospitano le applicazioni web (es. SELinux/CHRoot su sistemi Linux Red Hat).

3 Specifiche transitorie

Il colloquio applicativo rimane basato su Web-Services SOAP, già oggi in essere nel colloquio applicativo tra l'applicazione dell'Aderente e il Nodo dei Pagamenti. Le attuali modalità di connessione a pagoPA, in particolare il colloquio SPCoop mediante la componente Porta di Dominio presso l'aderente pagoPA sono deprecate. Pertanto tutti i soggetti aderenti hanno la facoltà di dare immediatamente attuazione a un piano di migrazione. La scadenza ultimativa per l'attuazione di tale piano sarà fissata dall'emanazione del Nuovo Modello di Interoperabilità da parte di AgID.

4 Procedura di attivazione

Nella procedura di attivazione che descritta nel seguito ci si riferisce esclusivamente a un Soggetto aderente direttamente connesso La procedura è identica per la connessione diretta a ogni ambiente del sistema pagoPA: produzione, DR, test esterno:

1) L'Aderente pagoPA che intende adottare la modalità di connessione diretta WS-SOAP deve dotarsi un certificato digitale X509 v3 Extended Validation emesso da una Certification Authority dello stesso soggetto aderente o che compaia fra i membri del CA/Browser Forum (https://cabforum.org/members/). È possibile in ogni caso per il soggetto Aderente può chiedere un parere a AgID circa l'utilizzo di una diversa tipologia di CA.
2) Il campo "Subject" di tale certificato deve contenere un CN coerente con il FQDN della URL del servizio che intende esporre.
3) Il Referente Tecnico di un Soggetto Aderente, che disponga di un accesso al Portale delle Adesioni, fornisce il certificato tramite apposita funzione di uploading. I Soggetti Aderenti che non dispongono di accesso al Portale delle Adesioni inviano il certificato ad AgID tramite PEC.
4) Devono essere forniti, per le opportune configurazioni nell'infrastruttura del Nodo dei Pagamenti, le seguenti informazioni:
   a) Indirizzo IP del sistema che utilizza i web services esposti dal Nodo dei Pagamenti;
   b) Indirizzo IP e porta di esposizione dei i web services esposti dal Soggetto aderente;
   c) URL del servizio che si intende esporre nel formato: https://FQDN/nomeservizio. Lo FQDN deve coincidere con il CN specificato al precedente 2).

In avvio di procedura di attivazione, AgID renderà disponibile al Soggetto Aderente tramite il Portale delle adesioni, le seguenti informazioni:

- Indirizzo IP del Nodo dei Pagamenti per l'utilizzo dei web services esposti dal Soggetto aderente;
- Indirizzo IP e porta di esposizione dei i web services esposti dal Nodo dei Pagamenti;
- Certificato digitale X509 v3 Extended Validation del Nodo dei Pagamenti.

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

FINE DOCUMENTO