OpenSPCoop Enterprise

Una soluzione di API Management aderente ai requisiti normativi Italiani ed Europei

OpenSPCoop è una soluzione di API Management progettata esplicitamente per le esigenze della Pubblica Amministrazione Italiana, sulla base di oltre 10 anni di esperienza maturata da Link.it nello sviluppo e nella gestione della Porta di Dominio SPCoop.

L'esperienza degli ultimi anni, non solo in Italia, ha evidenziato come la condivisione di dati e servizi tra istituzioni pubbliche comporti la gestione di complessi aspetti peculiari, non altrettanto rilevanti in ambito Enterprise:

- ✔ la conformità a complessi requisiti cogenti, imposti dalle normative nazionali italiane, come SPC e SPID, ed europee, come eDelivery;
- ✔ la criticità dei servizi offerti: mentre la maggior parte delle API disponibili in ambito Enterprise sono finalizzate esclusivamente alla commercializzazione di servizi, monetizzati in termini di quantità di Api invocate, molte API della Pubblica Amministrazione hanno un ruolo essenziale in workflow applicativi estremamente rilevanti per la vita dei cittadini e per il business delle aziende;
- ✔ la pariteticità dei rapporti tra i soggetti cooperanti: è frequente che in ambito Pubblica Amministrazione l'attivazione di un nuovo servizio digitale richieda un insieme di scambi applicativi, implementati sia come erogazioni che come fruizioni di API svolte da entrambe le parti cooperanti; non esiste quindi una parte (tipicamente l'erogatore dedl servizio) che possa imporre le regole all'altra, ma piuttosto entrambe le parti devono concordare su standard e regole condivise;
- ✔ l'erogazione dello stesso servizio da parte di molteplici soggetti: l'identica Api di un servizio pubblico può dover essere implementata da una molteplicità di soggetti. Si pensi a servizi come la Fatturazione Elettronica, dove la specifica delle API viene stabilita una volta per tutte da un soggetto terzo, ma gli erogatori delle API saranno tutti i soggetti che devono ricevere o emettere fatture elettroniche. Anche in questo caso, i requisiti di interoperabilità sono necessariamente diversi da quanto sufficiente nei casi tipici in ambito Enterprise (si pensi alle API di Google o di Spotify), laddove esiste un unico soggetto che emette le regole di utilizzo ed eroga le API.

Queste ed altre esigenze specifiche del processo di trasformazione digitale in corso nella Pubblica Amministrazione italiana trovano in OpenSPCoop una risposta puntuale, che permette di ridurre i rischi e i costi dei progetti, velocizzando drasticamente i tempi di delivery di nuovi servizi.

I principali vantaggi dell'adozione di OpenSPCoop

- ✔ **Prodotto Rodato**: OpenSPCoop è un prodotto utilizzato con successo da oltre 10 anni come API gateway per la quasi totalità dei servizi della Pubblica Amministrazione italiana, sia a livello locale che centrale.

- ✔ **Modello di Governance**: OpenSPCoop è basato su un modello di governance, mutuato dall'esperienza della cooperazione applicativa italiana, esplicitamente progettato, e successivamente ben rodato, sulle caratteristiche del dominio applicativo della Pubblica Amministrazione. I concetti di Accordo di Cooperazione, Accordo di Servizio, di Adesione, di Servizio Applicativo, di Porta Delegata e Applicativa, di Tracciamento e di Correlazione Applicativa, sono concetti ormai ampiamente condivisi che permettono di governare in maniera elegante ed efficace le diverse modalità di utilizzo dei servizi.

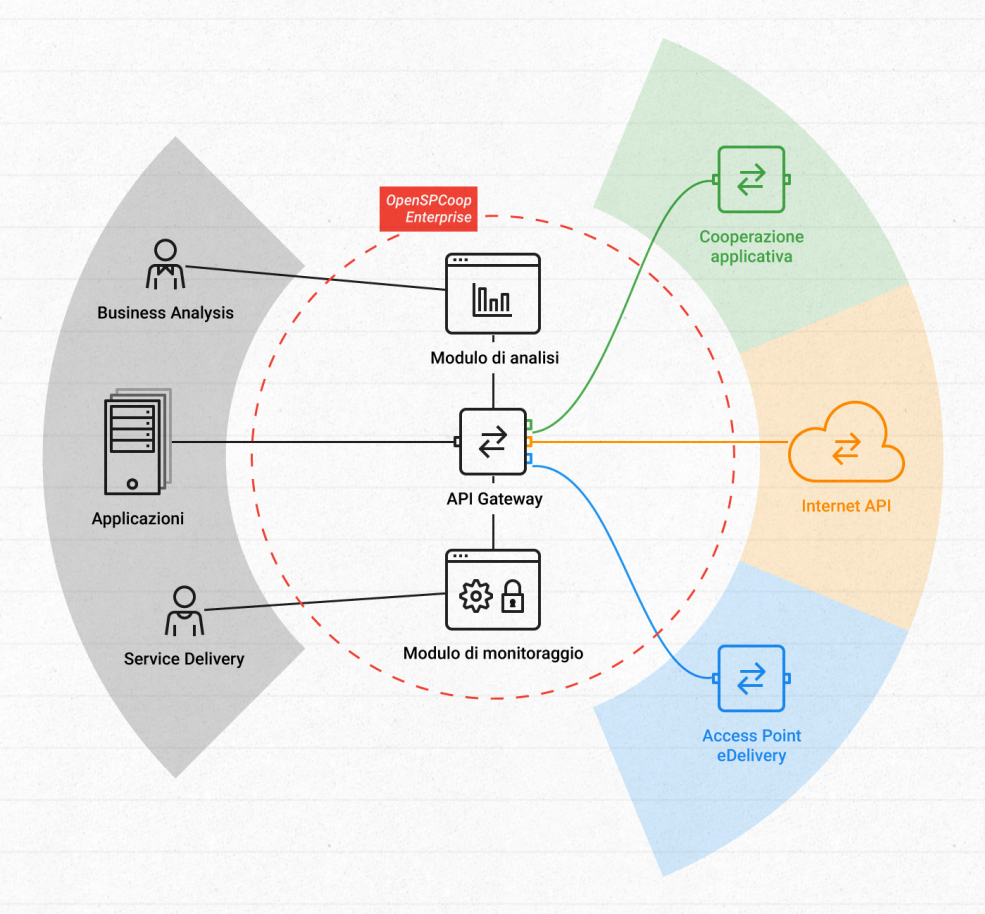
- ✔ **Semplicità d'uso**: la configurazione di OpenSPCoop avviene utilizzando direttamente le concettualizzazioni del modello di cooperazione applicativa, ottenendo configurazioni chiare e a prova di errore. Al contrario, l'uso di piattaforme generiche di API Management richiede la definizione di complesse catene di handler (o policy) per poter realizzare configurazioni corrispondenti alle reali esigenze della cooperazione applicativa in ambito Pubblica Amministrazione.

- ✔ **In linea con l'evoluzione normativa**: OpenSPCoop viene continuamente aggiornato in linea con le evoluzioni normative, garantendo l'immediato adeguamento della propria infrastruttura in conformità con le norme di legge.

- ✔ **Protezione dell'Investimento**: preserva gli investimenti già fatti sulla cooperazione applicativa, mantenendo le stesse modalità operative utilizzate sinora per SPCoop e supportando una transizione alle nuove specifiche di cooperazione applicativa, senza alcun impatto sulle infrastrutture già realizzate.

Overview del Prodotto

OpenSPCoop Enterprise è una soluzione di API Management composta da tre diversi moduli: l'API Gateway, il Modulo di Monitoraggio Applicativo ed il Modulo di Analisi dei Dati. Una soluzione completa per l'erogazione e l'adesione ai servizi della Pubblica Amministrazione, e per il monitoraggio e l'analisi del loro utilizzo. La figura che segue mostra un tipico scenario d'uso di OpenSPCoop, in cui l'API gateway permette alle applicazioni del proprio Dominio di dialogare con API esterne, indipendentemente dai diversi profili normativi richiesti, gestiti in maniera trasparente dal gateway. Dopo l'attivazione, l'uso di queste API potrà essere comunque monitorato ed analizzato in maniera uniforme, indipendentemente dalle modalità di dialogo richieste dai diversi profili utilizzati.



Nel resto del documento vengono presentate le funzionalità principali dei tre moduli software.

OpenSPCoop API Gateway

L'Api Gateway opera come intermediario per le invocazioni di API tra le applicazioni interne al dominio dell'ente e le applicazioni esterne. Di seguito le principali caratteristiche del prodotto.

- ✔ Conformità agli standard di mercato: il Gateway è in grado di processare messaggi conformi a qualunque protocollo standard di mercato, come SOAP 1.1 e 1.2, API restful serializzate in Json o XML o semplici dati binari su Http.
- ✔ Conformità alle specifiche italiane per l'interoperabilità: supporto nativo del protocollo SPCoop e delle nuove linee guida per l'interoperabilità di AGID.
- ✔ Conformità alle specifiche dell'interoperabilità europea: supporto del protocollo AS4, tramite integrazione con il Building Block eDelivery.
- ✔ Funzionalità di API Registry: censimento delle interfacce delle API, degli applicativi erogatori e fruitori di ogni API, delle politiche di gestione delle invocazioni (autenticazione, autorizzazione, validazione, routing). La registrazione delle API può avvenire manualmente o tramite caricamento dei descrittori delle interfacce (Swagger, RAML, WADL per i servizi REST, WSDL per i servizi SOAP, Accordi di Servizio per i servizi SPCoop).
- ✔ Autenticazione: gestione dell'autenticazione delle richieste in ingresso e in uscita dal proprio dominio, tramite supporto nativo dei protocolli HTTP-Basic e TLS o tramite integrazione di sistemi esterni di Identity Management.
- ✔ Autorizzazione: gestione dell'autorizzazione delle richieste in arrivo, tramite registrazione interna dei fruitori delle API gestite e dei loro ruoli, o tramite integrazione con sistemi esterni di Identity Management. Supporto dei protocolli di Autorizzazione Oauth2 e XACML, con la possibilità di gestire la valutazione delle policy XACML localmente o utilizzando un Policy Decision Point esterno.
- ✔ Validazione: validazione dei contenuti dei messaggi in transito, con verifica dei messaggi XML per i servizi SOAP e JSON o XML per i servizi REST. La validazione viene effettuata rispetto alle descrizioni delle API (Swagger, WSDL, JSON Schema, XSD) così come pubblicate sull'API Registry.
- ✔ Sicurezza dei contenuti: il gateway può intervenire per introdurre o verificare la sicurezza dei messaggi scambiati. Nel caso di API SOAP sono supportate le funzionalità WS-

Security di cifratura, firma, timestamp e token. La porta di dominio è inoltre in grado di creare o validare asserzioni SAML presenti all'interno del messaggio. Nel caso di API REST sono supportati i protocolli XMLEncryption e XMLSignature.

- ✔ Gestione del formato MTOM: il gateway è in grado di imbustare o sbustare in accordo al protocollo MTOM il messaggio in transito. In caso di validazione di un messaggio MTOM, il gateway potrà normalizzare il messaggio prima di effettuarne la validazione per poi ripristinare il formato originale una volta completato il processo di validazione.
- ✔ Tracciamento: emissione di una traccia per ogni richiesta e risposta transitata dal gateway, conforme alle normative della cooperazione applicativa e arricchita da un token JWT generato e firmato dal gateway per maggiore conformità agli standard. Oltre ai metadati riguardanti la richiesta di servizio (id transazione, mittente, destinatario, ..) è possibile indicare gli eventuali elementi parte dei messaggi in transito da includere nelle tracce; la modalità di estrazione supportate dal prodotto sono: XPath , Espressioni Regolari e JSONPath.
- ✔ Routing della richiesta: consegna della richiesta ai servizi di backend, con supporto nativo per i seguenti protocolli di connessione: http, https con mutua autenticazione, jms e scrittura su file. Ulteriori connettori possono essere realizzati come semplici plugin.
- ✔ Console di Gestione: cruscotto web per la registrazione delle definizioni di API, delle Erogazioni, delle Fruizioni e delle policy che le regolano. La gestione di vari profili di utenza, permette di selezionare le funzioni di gestione sulla base dei ruoli dei diversi gestori. Tutte le operazioni sono sottoposte ad auditing, in modo da poter sempre individuare gli autori delle modifiche di configurazione effettuate.
- ✔ Console di Monitoraggio: cruscotto web rivolto alla diagnostica ed al monitoraggio del traffico gestito dall'API gateway; ai gestori dell'infrastruttura permette un controllo totale sui messaggi in transito, aiutandoli a diagnosticare e prevenire qualunque tipo di anomalia; ai responsabili di progetto offre la possibilità di analizzare i flussi di utilizzo, gli esiti e l'efficienza complessiva delle API utilizzate nel proprio progetto.

Il Modulo di Monitoraggio Applicativo

Questo modulo fornisce funzionalità essenziali (sonde, gestione allarmi, rate limiting, controllo congestione) per il completo controllo del comportamento della Porta di Dominio e dei servizi applicativi erogati o fruiti dal Dominio Applicativo di un Ente.

Gestione degli Allarmi Applicativi

- Possibilità di attivare da Console nuovi allarmi relativi al comportamento di specifici servizi, decidendo il tipo ed il valore dei valori di soglia di ogni allarme.
- Possibilità di monitorare da Console lo stato degli allarmi.
- Supporto di allarmi attivi (attivati automaticamente a scadenze prefissate) o passivi (sollevati dall'esterno o dai moduli di analisi dei dati).
- Supporto di notifiche via mail o a sistemi di monitoraggio esterni
- Disponibilità di allarmi predefiniti attivabili per le seguenti tipologie di controlli:
  - tempi medi di risposta dei servizi superiori alla soglia attesa
  - numero di errori superiori alla soglia attesa
  - numero di messaggi in transito superiore alla soglia attesa
  - numero di messaggi in transito inferiore alla soglia attesa
  - eventi legati alla funzionalità di controllo congestione
- Possibilità di realizzare, tramite scripting Java, ulteriori tipologie di allarmi in grado di rilevare qualunque tipo di anomalia relativa alle informazioni presenti nel datamart di monitoraggio (ad esempio, sarà possibile sollevare un allarme nel caso in cui sia ricevuto un messaggio contenente un particolare contenuto).

Sonde per il Monitoraggio dei Servizi

Possibilità di attivare sonde applicative mirate alla verifica del regolare funzionamento di servizi erogati (porte applicative) o fruiti (porte delegate) tramite la Pdd. Le sonde possono essere istanziate dinamicamente tramite la console di gestione della Porta di Dominio, specificando le caratteristiche del messaggio di test (soggetto mittente, servizio, azione, contenuto del messaggio). Le sonde istanziate, tipicamente agganciate ai sistema di monitoraggio del Cliente, restituiscono l'esito nell'invocazione del servizio monitorato (Ok, Fail o Warning) ed un dettaglio in grado di indirizzare sul tipo di problema riscontrato in caso di errore. L'esito sarà individuato in base ai codici http di risposta o anche in base all'analisi del contenuto della risposta, effettuata tramite pattern xpath o xquery.

Rate Limiting

Funzionalità finalizzata alla regolamentazione del traffico in entrata sulla PdD OpenSPCoop Enterprise, limitando il numero di richieste o la dimensione di banda occupata per uno specifico erogatore (porta applicativa) o da uno specifico fruitore (porta delegata).

Le politiche di controllo, stabilite in modo puntuale dal gestore della PdD durante la fase di configurazione, permettono di:

- controllare il numero massimo di richieste accettabili dalla PdD in un dato intervallo di tempo per ogni fruizione/erogazione;
- controllare la quantità massima di dati accettabili dalla PdD in un dato intervallo di tempo per ogni fruizione/erogazione;
- nel caso in cui sia selezionata l'opzione 'warning only', le situazioni di violazione degli SLA impostati saranno segnalate ad uso del modulo di allarmistica, senza ridurre effettivamente il numero di richieste gestite per quel servizio.
- filtrare le transazione, nei pannelli di ricerca, anche sulla base della violazione o meno del rate limiting.
- filtrare le transazione, nei report statistici, anche sulla base della violazione o meno del rate limiting.

Controllo Congestione Servizi

Funzionalità finalizzata alla regolamentazione del traffico in entrata sulla PdD OpenSPCoop Enterprise, per impedirne il congestionamento causato da eventuali degradi prestazionali di specifici servizi o da picchi elevati di richieste simultanee.

Le politiche di controllo, stabilite in modo puntuale dal gestore della PdD durante la fase di configurazione, permettono di:

- registrare i tempi medi di risposta attesi per ogni servizio/operation;
- registrare il numero massimo di richieste simultanee gestibili per ogni servizio/azione in condizioni ottimali;
- registrare il numero massimo di richieste simultanee gestibili per ogni servizio/azione in condizioni di degrado prestazionale (tempi medi di risposta superiori ai tempi attesi);
- attivare il controllo di congestione su specifici servizi/operation. In tali situazioni il numero massimo di richieste gestibili simultaneamente per quel servizio sarà ridotto alla soglia massima impostata per le situazioni di degrado prestazionale;
- l'opzione di 'warning only', segnala le situazioni di degrado prestazionale ad uso del modulo di allarmistica, senza ridurre effettivamente il numero di richieste gestite per il servizio.

Log Analysis

Un componente software di tipo batch che produce report di analisi degli errori che si sono verificati, di grande supporto per l'indagine diagnostica anche di tipo proattivo.

- Utilizza algoritmi di similitudine per classificare gli errori rilevati sulla PdD, eliminando il complesso lavoro di analisi manuale sulla Console Diagnostica delle singole transazioni con esito errore. Il numero di occorrenze di errori dovuti alla stessa causa scatenante è infatti quasi sempre molto elevato e genera quindi notevole rumore di fondo.
- Ordina le casistiche di errore per numero di occorrenze, dando priorità agli errori più impattanti.
- Fornisce una collocazione temporale delle occorrenze relative a ciascun caso di errore (con relativa percentuale sul totale) offrendo una chiara visione della gravità del problema.
- Per ogni tipologia di errore, l'indagine diagnostica viene supportata dalla presenza di tutti i dati di contesto:
  - Soggetto Erogatore, Servizio, Esito e Ruolo, invarianti per tutte le transazioni dello stesso caso;
  - il numero di transazioni appartenenti al caso di errore (Occorrenze);
  - Dati della transazione capostipite: Timestamp, Id Transazione, Id Messaggio, Messaggi Diagnostici, Fault Cooperazione e Fault Integrazione
  - Timestamp dell'ultima transazione del caso di errore
  - Latenza Media Servizio e Latenza Media Porta relative a tutte le transazioni del caso di errore
- Periodi di osservazione configurabili: mensili, settimanali, giornalieri.
- Report distinti per servizi erogati e servizi fruiti, che inludono:
  - Distribuzione degli esiti: Numero Errori/Totale Richieste su base giornaliera o oraria.
  - Distribuzione degli esiti per servizio: Numero Errori/Totale Richieste per singolo servizio su base giornaliera o oraria.
  - Occupazione banda distinta per esito per ciascun servizio: per ciascun servizio il numero di bytes veicolati dai casi OK e da quelli in errore.
  - Distribuzione dei tempi medi di latenza per servizio: per ciascun servizio vengono mostrati il tempo medio di latenza totale, la sola latenza media del servizio e la latenza della sola PdD.

Il Modulo di Data Analisys

La possibilità di intercettare, classificare ed analizzare i contenuti applicativi in transito, mette a disposizione del gestore e dei responsabili dei servizi applicativi una piattaforma completa di analisi del comportamento dei servizi applicativi erogati o fruiti dal Dominio Applicativo di un Ente.

Estrazione dei Dati in Transito

L'estrazione delle informazioni rilevanti dai messaggi in transito, prerequisito per le successive attività di analisi, avviene ad opera in un interceptor integrato nella PdD per:

- Estrazione di contenuti del messaggio, anche in maniera condizionale (ad esempio, estrazione di una certa risorsa solo da messaggi di richiesta relativi a transazioni completate con un esito di errore ed uno specifico tipo di Fault).
- Possibilità di anonimizzare i dati estratti.
- Possibilità di compressione o cifratura dei dati estratti.
- Possibilità di personalizzare, tramite scripting Java, il processo di analisi dei dati, ad esempio per sollevare allarmi per particolari tipi di messaggi in transito o per estrarre dati di sintesi a partire dai dati inclusi nel messaggio originale.

Classificazione dei Dati in Transito

Permette di definire criteri per la classificazione dei messaggi in transito sulla base dei valori dei dati estratti. In dettaglio, è possibile:

- 'marcare' i messaggi in transito sulla base delle proprie caratteristiche (ad esempio: richieste per una specifica operation con esito negativo, richieste con un particolare valore di una risorsa di contenuto del messaggio di richiesta o di risposta, etc.);
- utilizzare la classificazione dei dati all'interno di altre funzionalità del prodotto: ricerca di transazioni di un certo tipo, estrazioni di dati solo per messaggi di un certo tipo, allarmi per numero eccessivo di transazioni di un certo tipo, etc.;
- personalizzare, tramite scripting Java, il processo di tipizzazione dei dati in transito sulla base di criteri arbitrari non gestibili da console (ad esempio: assegnare un tipo particolare ai messaggi con una risorsa di contenuto riconosciuta in base ad una tabella di decodifica disponibile su una base dati esterna).

Funzionalità di Ricerca sui Contenuti dei Messaggi

L'estrazione e la classificazione dei contenuti consentono di arricchire le modalità di ricerca dei messaggi:

- Disponibilità di filtri aggiuntivi per la ricerca nello storico delle transazioni, basati sui valori delle risorse di contenuto estratte nella fase di analisi dei dati.

- Disponibilità di filtri aggiuntivi per la ricerca nello storico delle transazioni, basati sul “tipo” di transazione, così come classificata nella fase di analisi dei dati.
- Possibilità di realizzare, tramite scripting Java, funzionalità custom di ricerca nello storico delle transazioni accessibili da Console. Le nuove ricerche potranno essere basate sulla combinazione arbitraria di filtri sulle caratteristiche e sui contenuti dei messaggi, anche accedendo a basi dati esterne per la decodifica dei dati originali inclusi nel messaggio.

Funzionalità di Reportistica dei Contenuti dei Messaggi

L'estrazione e la classificazione dei contenuti consentono di arricchire le modalità di reportistica:

- Modalità aggiuntive disponibili da Console per la generazione di report sullo storico delle transazioni, basate sui valori delle risorse di contenuto estratte nella fase di analisi dei dati (ad esempio sarà possibile produrre report che classificano i messaggi trattati sulla base della regione di provenienza del Cittadino oggetto di una specifica richiesta di servizio).
- Modalità aggiuntive disponibili da Console per la generazione di report sullo storico delle transazioni, basate sul “tipo” di transazione, così come classificata nella fase di analisi dei dati (ad esempio sarà possibile produrre report che classificano le diverse operazioni di un servizio sulla base dello stato del worflow applicativo al quale appartengono).
- Possibilità di realizzare, tramite scripting Java, report personalizzati basati sull'applicazione arbitraria di classificazioni sulle caratteristiche e sui contenuti dei report, anche accedendo a basi dati esterne per la decodifica dei dati originali inclusi nel datamart di monitoraggio.

L'Offerta OpenSPCoop Enterprise

L'offerta include i seguenti prodotti.

- La **Porta di Dominio OpenSPCoop Enterprise**, il software di base che fornisce le funzionalità di API Gateway per il protocollo SOAP 1.1 e 1.2 ed SPCoop. Il prodotto è commercializzato in 3 diverse versioni (Entry, Standard, Proactive), in funzione delle caratteristiche della Porta di Dominio del Cliente, dei Livelli di Servizio garantiti e dei prodotti software aggiuntivi disponibili rispetto alla distribuzione pubblica di OpenSPCoop.
- Il **Modulo eDelivery per la PdD OpenSPCoop Enterprise**, un modulo aggiuntivo che estende le funzionalità della Porta anche al paradigma RESTFul e fornisce un connettore per il protocollo eDelivery, permettendo alla PdD di operare come Access Point eDelivery.
- Il **Modulo di Monitoraggio Applicativo per la PdD OpenSPCoop Enterprise**, un modulo aggiuntivo che fornisce le funzionalità essenziali (sonde, gestione allarmi, rate limiting, controllo congestione) per il completo controllo del comportamento della Porta di Dominio e dei servizi applicativi erogati o fruiti dal Dominio Applicativo di un Ente.
- Il **Modulo di Data Analysis per la PdD OpenSPCoop Enterprise**, un modulo aggiuntivo che fornisce un insieme di strumenti mirati per l'analisi delle informazioni contenute nei messaggi in transito sulla Porta di Dominio.
- I **Kit di Integrazione OpenSPCoop Enterprise**, consistono nella fornitura di pacchetti di giornate specialistiche utilizzabili per l'integrazione del prodotto nell'ambiente del Cliente.

Il Software OpenSPCoop Enterprise viene commercializzato come “Subscription”, tipicamente di durata annuale o triennale, ed include:

- la licenza d’uso a tempo determinato del software OpenSPCoop Enterprise, come da condizioni nel “**Contratto di Licenza per l'uso del Software OpenSPCoop Enterprise**”, consultabile alla URL http://www.link.it/pddoe/subscription_lic.pdf; la durata della licenza decorre dalla data di attivazione della “Subscription” e rimane efficace per il periodo indicato nel relativo ordine di acquisto;
- il servizio di supporto, erogato in accordo alle “**Condizioni del Servizio di Manutenzione del Software OpenSPCoop Enterprise**”, consultabile alla URL http://www.link.it/pddoe/subscription_sla.pdf.

Tutta l'offerta è disponibile direttamente sul MEPA o rivolgendosi a LINK.IT (openspcoop@link.it).