Release Notes

Release 3.2.1

Link.it

14 nov 2019

Release Notes

1 Versione 3.2.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.2.1 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

1.1 Miglioramenti alla funzionalità di Autorizzazione

- *Informazione in Cache*: è stata aggiunta un'informazione nei diagnostici relativa all'esito dell'autenticazione, dell'autorizzazione e dell'autorizzazione per contenuti, indicando se sia stato prelevato dalla cache o sia stata elaborato durante la transazione stessa.
- *Autorizzazione dei Contenuti*: nelle autorizzazioni custom è adesso possibile utilizzare la cache relativa alle autorizzazioni, già disponibile sul gateway
- *Profilo SPCoop*: per le erogazioni è adesso possibile autenticare i soggetti mittenti. Nel caso sia abilitata l'autenticazione, il Gateway controlla che il soggetto identificato corrisponda al soggetto indicato nella busta.

1.2 Bug Fix

Sono stati risolti i seguenti bug:

- Non venivano verificati eventuali ruoli associati agli applicativi identificati durante l'invocazione dell'erogazione quando era abilitata l'autorizzazione per ruoli.
- L'autenticazione http-basic non funzionava con password che contenevano il carattere ":".
- Corretto un problema nella gestione di messaggi MTOM con struttura Multipart con solamente una singola "part". Il messaggio veniva processato correttamente ma poi veniva inoltrato verso il backend senza una struttura Multipart (veniva eliminato il boundary nello stream) lasciando inalterato il Content-Type che invece presentava sempre l'indicazione MultipartRelated. L'effetto di questa inconsistenza era che il backend non riusciva a processare il messaggio ottenuto generando un errore simile al seguente: "Unable to internalize message".
- Durante la validazione dei contenuti, in presenza di messaggi con elemento "xsi:type" definito con un prefisso non utilizzato da altri elementi, si otteneva il seguente errore: "The value of the attribute

«prefix=»xmlns»,localpart=»p»,rawname=»xmlns»» is invalid. Prefixed namespace bindings may not be empty.”

Sulla console di gestione sono stati risolti i seguenti bug:

- In presenza di multitenant attivo, durante la creazione di una erogazione o fruizione, se non era stato selezionato il soggetto del dominio in gestione (in alto a destra), la selezione della API reimpostava il soggetto erogatore scelto in precedenza nel form.
- Nella sezione di configurazione delle cache era presente un link errato che portava alla configurazione delle regole di proxy pass.
- Aggiunto controllo grafico che, avviata un'operazione, disabilita gli elementi grafici sulla console fino al completamento dell'operazione.
- Aggiunta finestra modale per indicare all'utente che non ha selezionato nessun elemento da esportare o eliminare.

Per l'API di monitoraggio sono stati risolti i seguenti bug:

- L'API utilizza adesso il time zone di default presente sul sistema dove è dispiegata.
- Le operazioni di accesso ad elenchi di transazioni ritornavano degli item che includevano elementi non previsti dall'interfaccia OpenAPI.
- È adesso possibile configurare un database delle transazioni differente da quello dove sono presenti le configurazioni.

2 Versione 3.2.0

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.2.0 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

2.1 Nuovo Profilo di Interoperabilità ModI PA

La 3.2 è la prima versione di GovWay a supportare completamente il profilo ModIPA, assicurando in maniera del tutto trasparente alle applicazioni interne al dominio, la conformità delle API (sia in fruzione che in erogazione) alle nuove *Linee Guida AGID di Interoperabilità* (https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/bozza/).

Il Modello di Interoperabilità di ModIPA mantiene sostanzialmente invariato il concetto di *dominio* di un'amministrazione rispetto a quanto prevedeva il precedente modello SPCoop, rendendo quindi le modalità di configurazione dei profili previsti da ModiPA del tutto analoghe a quelle già adottate per SPCoop.

Tramite la govwayConsole è quindi possibile gestire tutti gli aspetti previsti dalle Linee Guida.

- *Profili di Interazione*: definiscono la modalità con cui interagiscono fruitore ed erogatore di una API. Sono supportati i due profili previsti in ModIPA:
  - *Bloccante*: il fruitore invia la richiesta e resta bloccato in attesa di ricevere la risposta dall'erogatore;
  - *Non Bloccante*: il fruitore non resta in attesa dopo aver inviato la richiesta, se non per ricevere una notifica di presa in carico. Per ottenere la risposta sarà poi necessario effettuare una distinta interazione, esplicitamente prevista dallo scenario del servizio.
- *Sicurezza Canale*: gestione della sicurezza inerente il canale di comunicazione tra i domini fruitore ed erogatore. Sono supportati i due profili previsti in ModIPA:

  - *[IDAC01] Direct Trust Transport-Level Security*: comunicazione basata sul canale SSL con trust del certificato X509 fornito dal dominio erogatore.
  - *[IDAC02] Direct Trust mutual Transport-Level Security*: comunicazione basata sul canale SSL con mutua autenticazione, tramite trust dei certificati X509 del fruitore e dell'erogatore.
- *Sicurezza Messaggio*: gestione della sicurezza a livello di messaggio, inerente lo scambio di informazioni tra le applicazioni agli estremi del flusso di comunicazione. I profili di sicurezza previsti si distinguono per il caso SOAP e per quello REST:
  - *[IDAS01 o IDAR01] Direct Trust con certificato X.509 su SOAP o REST*: Tramite la validazione del certificato X509, inserito dall'applicazione mittente all'interno del token di sicurezza della richiesta, l'applicativo destinatario verifica la corrispondenza delle identità e la validità del messaggio, prima di procedere con l'invio della risposta.
  - *[IDAS02 o IDAR02] Direct Trust con certificato X.509 su SOAP o REST con unicità del token/messaggio*: estensione del profilo precedente con l'aggiunta di un meccanismo di filtro che impedisce il processamento di un messaggio di richiesta duplicato.
  - *[IDAS03 o IDAR03] Integrità del payload del messaggio SOAP o REST*: profilo che estende i profili precedenti aggiungendo la gestione della firma del payload come verifica di integrità del messaggio ricevuto.
- *URL di Invocazione API*: le linee guida richiedono una indicazione esplicita della tecnologia utilizzata (REST o SOAP) e la versione. Le url con cui vengono esposte le API su GovWay soddisfano entrambi i requisiti.

2.2 Nuova funzionalità per taggare le API

Alle API è adesso possibile associare uno o più tag al fine di raccoglierle in un gruppo tematico.

La creazione di un tag o l'associazione di un tag preesistente alle API avviene tramite la govwayConsole, direttamente in fase di registrazione dell'API stessa o, successivamente, accedendo all'elenco dei tag di una API.

Il raggruppamento in tag permette:

- tramite la govwayMonitor, di filtrare per tag le ricerche sulle transazioni o la generazione di report statistici;
- tramite la govwayConsole, di filtrare per tag le ricerche sulle configurazioni di API, erogazioni e fruizioni.

2.3 Miglioramenti alle Funzionalità di Sicurezza

Sono state introdotte le seguenti nuove funzionalità:

- *Connettore HTTPS*: è stata aggiunta la possibilità di indicare opzionalmente l'alias della chiave privata da utilizzare per l'autenticazione client; funzionalità utile quando il keystore contiene più chiavi private.
- *CRL*: è adesso possibile indicare una lista di CRL per la validazione dei certificati sia sul connettore https che nelle configurazioni relative alla sicurezza messaggio (es. WSSecurity, JOSE Signature, OAuth2 . . .).
- *Cache*: tutti i keystore e CRL acceduti da GovWay, sia per la sicurezza a livello trasporto che a livello messaggio, sono ora gestiti tramite cache.
- *Frontend HTTPS*: se la terminazione ssl viene gestita su un frontend (Apache httpd, IIS, etc) che inoltra su header http i certificati x.509 o il DN dei certificati client autenticati, GovWay può adesso essere configurato per processare le informazioni presenti in tali header.

2.4 Miglioramenti alla Console di Monitoraggio

Sono state introdotte le seguenti nuove funzionalità:

- *Ricerca delle Transazioni*: è stata riorganizzata, classificando in sezioni le diverse modalità di ricerca:
  - Ricerca generica: consente di effettuare ricerche tramite la selezione di valori in liste ("base") o campi liberi ("avanzata").
  - Ricerca per mittente: consente di selezionare il fruitore della richiesta in base a vari criteri:
    - Valori dei claims di un Token
    - Identità del Soggetto
    - Identità dell'applicativo
    - Principal del chiamante
    - Indirizzo IP del client
  - Ricerca per identificativo: consente di individuare una transazione tramite l'identificativo applicativo, l'id del messaggio o l'id di transazione.
- *Tipologia delle Transazioni*: è stata reintrodotta la possibilità di ricerca senza dover indicare obbligatoriamente la tipologia della transazione (erogazione/fruizione).
- *Indirizzo IP del Chiamante*: è stata aggiunta la possibilità di effettuare la ricerca di transazioni specificando l'indirizzo IP del chiamante. L'indirizzo IP può riferirsi all'indirizzo IP del client o al valore dell'header http "X-Forwarded-For". L'indirizzo IP può essere inoltre utilizzato per filtrare i risultati dei report statistici (Distribuzione per API, per Operazione, per Soggetto ...). Infine è stata introdotta un nuovo tipo di report basato sugli indirizzi IP dei chiamanti.
- *Ricerca per Identificativo di Collaborazione*: aggiunta la possibilità di effettuare ricerche per individuare tutte le transazioni correlate attraverso il medesimo *identificativo di collaborazione*.
- *Ricerca per Identificativo della Richiesta*: consente di invidivuare una transazione che è correlata ad una precedente richiesta, tramite l'"*id di riferimento richiesta*

2.5 Miglioramenti sulla Visualizzazione delle Url di Invocazione

Rivista la modalità di visualizzazione delle Url di Invocazione delle API esposte da GovWay per assicurare che, in presenza di un reverse proxy che media le comunicazioni https con GovWay, sia possibile configurare opportunamente le url di invocazione delle API esposte da GovWay allineandole con le eventuali configurazioni specifiche realizzate sul reverse proxy.

2.6 Miglioramenti all'Installer

Sono state apportati i seguenti miglioramenti all'installer binario:

- Aggiunto supporto per il nuovo profilo di interoperabilità "ModI PA".
- L'installer adesso genera, all'interno degli script sql, informazioni relative ai parametri di installazione selezionati. Tali informazioni sono poi consultabili tramite la sezione "Runtime" della "govwayConsole".
- Nella modalità di aggiornamento vengono adesso prodotte informazioni utili a individuare le modifiche intervenute sui file di configurazione (dist/cfg) rispetto alla versione precedente.

2.7 Bug Fix

Sono stati risolti i seguenti bug:

- *Riconoscimento Azione per API Soap*: risolto bug che causava il fallimento durante il riconoscimento dell'azione basato sull'interfaccia wsdl se vi erano più operazioni che condividevano la definizione di un medesimo header soap.
- *Token Policy*: sono stati corretti alcuni bug inerenti la gestione dei token OAuth2:
  - Malfunzionamento nella funzione di «Token Forward» tramite header http "Authorization" (https://github.com/link-it/govway/issues/45).
  - Malfunzionamento nella gestione di alcune funzioni delle TokenPolicy. Quando disabilitate, se già in uso nella configurazione delle API, la funzionalità rimaneva abilitata sull'API anche se non più visualizzata nella maschera di controllo degli accessi e quindi non più disabilitabile.
  - Il truststore per gestire le comunicazioni ssl verso Google conteneva un certificato scaduto che è stato rimosso lasciando nel truststore la sola CA che possiede una scadenza con data Dicembre 2021.
- *Dump Binario*: risolto malfunzionamento che si verificava nel caso di messaggi senza payload. Non venivano salvati gli header HTTP presenti se era stata abilitata la funzionalità di dump binario.
- *Informazioni Runtime* e *Verifica Connettività*: abilitando la configurazione in cluster delle console, l'accesso alla sezione "Runtime" e l'accesso alla funzionalità di "Verifica Connettività" di un connettore produceva il seguente errore: java.lang.NoClassDefFoundError: org/springframework/web/util/UriUtils ...
- *Profilo "Fatturazione Elettronica"*: la riconciliazione sulle notifiche descritta nell'Issue (https://github.com/link-it/govway/issues/27) non funzionava su database di tipo Oracle. Inoltre la riconciliazione specifica per la fatturazione attiva, riguardante il trasmittente e l'applicativo mittente non funzionava correttamente.

3 Versione 3.1.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.1.1 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

3.1 Miglioramenti alla funzionalità di Autorizzazione

Nella sezione "Controllo degli Accessi" di una erogazione o fruizione sono state introdotte le seguenti modifiche.

La funzionalità di autorizzazione per Token Claims è stata estesa in modo da supportare i seguenti controlli sui valori dei claim:

- valore non nullo
- valore corrispondente ad un'espressione regolare
- valore atteso contenente parti dinamiche, riferite a header http, parametri della url o parti del messaggio

La funzionalità di autorizzazione basata sui contenuti è stata estesa per effettuare controlli sulle seguenti risorse:

- header http
- parametri o porzioni della url di invocazione
- credenziali del chiamante (principal, username, subject ...)
- claim presenti in un token
- porzioni del messaggio individuate tramite espressioni xPath o jsonPath

- valori statici

3.2 Miglioramenti alla funzionalità di Trasformazione dei Messaggi

Sono state introdotte le seguenti nuove funzionalità nella trasformazione dei contenuti tramite i template engine "Freemarker" e "Velocity":

- *Archivio di Template*: è adesso possibile caricare, oltre al singolo file che individua il nuovo payload, anche un archivio zip contenente più template collegati tra loro tramite un file indice (index.ftl o index.vm).
- *ErrorHandler*: è possibile utilizzare un oggetto "errorHandler" che consente di generare una risposta immediata in funzione dei dati della richiesta, utile, ad esempio, nei casi in cui il template richiede dei dati prelevati dalla richiesta (dagli header http, dal messaggio, dalla url . . .) e tali dati non sono disponibili.

Sono stati introdotti nuovi tipi di trasformazione (ZIP, TGZ o TAR) per supportare la trasformazione di richieste e risposte in archivi compressi.

Sono state inoltre aggiunte nuove risorse accessibili dai template:

- *TransportContext*: è ora possibile accedere al contesto http della richiesta. Questa nuova risorsa permette ad esempio di poter ottenere l'informazione sull'identità ("principal") del richiedente.
- *Token Info*: permette di accedere ai claims di un token che ha superato la validazione effettuata durante il processo di autorizzazione.
- *Request / Response*: consente di accedere ai contenuti (payload o attachment) del messaggio di richiesta o di risposta.

Infine è stata aggiunta la possibilità di sospendere una regola di trasformazione.

3.3 Miglioramenti della funzionalità di estrazione dei contenuti JSON

L'estrazione dei contenuti da messaggi JSON, utilizzata nelle funzionalità di Correlazione Applicativa, Rate Limiting, Trasformazioni, Identificazione dell'azione etc. era possibile attraverso la definizione di espressioni JSONPath.

Essendo allo stato attuale, XPath più espressivo di JSONPath, è stata introdotta la possibilità di utilizzare espressioni XPath su di una rappresentazione xml dell'oggetto json in transito.

3.4 Nuova funzionaltà di esposizione dei WSDL

Aggiunta la funzionalità di esposizione dell'interfaccia WSDL di una API SOAP.

È adesso possibile ottenere il file wsdl attraverso una invocazione HTTP GET, utilizzando la url di invocazione dell'API, arricchita del prefisso "?wsdl".

Nota: Nell'installazione di default la gestione delle richieste HTTP GET con prefisso "?wsdl" è disabilitata e tali richieste ottengono un errore "HTTP 404 Not Found".

Per abilitare la funzionalità è possibile agire sul file esterno "/etc/govway/govway_local.properties" abilitando le proprietà "org.openspcoop2.pdd.pd.generateWsdl" e "org.openspcoop2.pdd.pa.generateWsdl"

3.5 Miglioramenti all'Installer

È stato aggiunto il supporto per la nuova versione dell'application server "WildFly" 17.x

3.6 Bug Fix

Sono stati risolti i seguenti bug:

- *Negoziazione Token sul Conettore*: nelle token policy di tipo «Negoziazione», in presenza di un "Authorization Header" nella richiesta originale, se questa non veniva consumata dal modulo di autenticazione, veniva erroneamente sovrascritto il token ottenuto dalla negoziazione.
- *Dump Binario*: abilitando il debug sul connettore, la funzionalità di dump binario non registrava gli header gestiti dal connettore (Authorization, Content-Type, SOAPAction. . .).
- *Validazione dei Contenuti tramite OpenAPI 3*: sono stati risolti i seguenti problemi:
  - non venivano validati gli elementi presenti nella richiesta o nella risposta se definiti tramite "$ref";
  - la validazione dei parametri (header, query, path) non considerava eventuali restrizioni sul tipo (es. minLength, pattern . . .).
- *Gestione Header HTTP case-insensitive*: gli heder non venivano gestiti completamente in maniera "case-insensitive" come richiesto dalla specifica rfc7230#page-22. Venivano processati correttamente se dichiarati nella forma standard (es. Content-Type) o in una forma completamente minuscola o maiuscola (es. content-type). Non venivano invece riconosciuti se possedevano un nome che non rientrava nei casi precedenti (es. Content-type o Soapaction).

Sulla console di monitoraggio sono stati risolti i seguenti bug:

- *Summary "Ultimo Anno"*: risolto problema presente nel report statistico relativo all'intervallo "Ultimo anno" visualizzato dopo il login alla console. Il report visualizzava un intervallo temporale errato dove il mese corrente invece di essere utilizzato come ultimo mese, era proposto come primo e venivano poi forniti mesi "futuri".
- *Dump Binario*: la console non visualizzava il contenuto del dump binario se differente da xml.
- *Modifica Password*: la modifica della password dell'utente non funzionava.

4 Versione 3.1.0

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.1.0 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

4.1 Nuove API di Gestione e Monitoraggio

Sono ora disponibili API REST per la gestione ed il monitoraggio di GovWay, utilizzabili in alternativa alle due console ("govwayConsole" e "govwayMonitor"):

- http://localhost:8080/govwayAPIConfig/openapi.yaml
- http://localhost:8080/govwayAPIMonitor/openapi.yaml

L'installer è stato adeguato per generare gli archivi relativi ai due nuovi servizi.

Nota: Entrambi i servizi sono definiti tramite una interfaccia OpenAPI v3.0.

4.2 Nuova funzionalità di Trasformazione dei Messaggi

Aggiunta la funzionalità di trasformazione dei messaggi in transito. È possibile intervenire sugli header http, sui parametri della url, sui contenuti scambiati e sul codice di risposta, tramite varie modalità di trasformazione:

- *Header HTTP*: è possibile aggiungere nuovi header oppure modificare o eliminare quelli esistenti sia sulla richiesta che sulla risposta. I valori forniti possono essere statici o possono contenere parti dinamiche risolte a runtime dal Gateway.
- *Parametri della URL*: è possibile aggiungere nuovi parametri oppure modificare o eliminare quelli esistenti. I valori forniti possono essere statici o possono contenere parti dinamiche risolte a runtime.
- *Payload HTTP*: la funzionalità consente di modificare il payload della richiesta e/o della risposta. È possibile indicare la generazione di un payload vuoto o fornire un nuovo payload definito tramite una delle seguenti modalità:
  - *GovWay Template*: file contenente parti dinamiche risolte a runtime in maniera analoga agli header http e ai parametri della url.
  - *Freemarker Template*: template dinamico che può utilizzare i costrutti supportati da "Freemarker" (https://freemarker.apache.org/).
  - *Velocity Template*: template dinamico che può utilizzare i costrutti supportati da "Velocity" (http://velocity.apache.org/).
  - *XSLT*: fogli di stile XSLT utilizzabili su messaggi di tipo XML o SOAP.
- *Trasformazione di Protocollo*: è possibile effettuare trasformazioni di protocollo da SOAP a REST o viceversa, permettendo anche di fruire o erogare lo stesso servizio in entrambe le modalità.

Le regole di trasformazione sono soggette ai seguenti criteri di applicabilità:

- *Elenco Risorse*: indicazione puntuale di una o più risorse a cui la trasformazione deve essere applicata.
- *Elenco Soggetti e/o Applicativi*: indicazione puntuale di uno o più soggetti e/o applicativi mittenti.
- *Content-Type*: indicazione del Content-Type della richiesta.
- *Espressione XPath o JsonPath*: espressione applicata sul messaggio di richiesta. La trasformazione viene applicata in caso di match.

All'interno di una regola di trasformazione, è possibile poi applicare trasformazioni diverse della risposta ottenuta in funzione di:

- *Codice Risposta*: codice di risposta http.
- *Content-Type*: indicazione sul Content-Type della risposta.
- *Espressione XPath o JsonPath*: espressione applicata sul messaggio di risposta. La trasformazione viene applicata in caso di match.

4.3 Nuova funzionalità di Negoziazione Token

Aggiunta la funzionalità di negoziazione di Bearer Token da inoltrare verso gli endpoint definiti nei connettori.

All'interno di Token Policy, funzionali alla negoziazione di un access token, vengono definiti tutti i parametri necessari per l'accesso all'Authorization Server, tra cui il flusso oauth selezionabile tra "Client Credentials Grant" o "Resource Owner Password Credentials Grant". La policy, una volta definita, deve essere associata ad un connettore per attivarla. La rinegoziazione del token avviene automaticamente una volta che il token è scaduto.

4.4 Miglioramenti alla funzionalità di RateLimiting

La gestione delle politiche di "Rate Limiting" è stata semplificata, introducendo la distinzione tra due diverse modalità di registrazione:

- *Basata su Criteri*: permette di indicare direttamente i criteri che la politica deve garantire; tra i criteri utilizzabili: la metrica (numero richieste, occupazione banda, tempi medi, ...), l'intervallo temporale (minuto, ora, giorno) e le condizioni di applicabilità (congestione, degrado prestazionale).
- *Basata su Policy Utente*: permette di utilizzare una politica arbitraria, precedentemente definita dall'utente.

È stato rivisto l'algoritmo di valutazione delle politiche di rate limiting, come segue:

- le policy vengono raggruppate «per metrica» e per ogni metrica vengono valutate nell'ordine di inserimento, per cui è ora possibile modificare la posizione della policy;
- per ogni metrica vengono valutate le policy applicabili, cioè per le quali risultano soddisfatti il filtro e le condizioni di applicabilità;
- se la policy viola i livelli di soglia previsti, la transazione viene bloccata (o segnalata se configurata come «warning only») e la valutazione delle policy viene terminata;
- se la policy non viola invece i livelli di soglia previsti, si prosegue nella valutazione di ulteriori policy per quella metrica, solo se la policy è marcata come «prosegui».

Sono state inoltre realizzate le seguenti modifiche:

- *Livelli di Soglia*: riviste le maschere per la gestione dei valori di soglia (con o senza criteri di raggruppamento).
- *Raggruppamento per Token*: aggiunti criteri di raggruppamento dei dati per token, dove è possibile selezionare i claim da utilizzare (subject, clientId ...).
- *Filtro*: riviste le maschere per la gestione dei criteri di applicabilità. Nelle politiche relative alle API è adesso possibile definire all'interno del filtro più risorse e il ruolo del richiedente.

4.5 Nuova modalità di gestione delle Credenziali SSL

Introdotta la possibilità di registrare le credenziali "ssl" di applicativi e soggetti anche tramite upload del corrispondente certificato (formati DER, PEM, PKCS12, JKS).

La verifica dei certificati client viene ora effettuata confrontando non solamente il Subject ma anche l'Issuer. Inoltre è possibile configurare opzionalmente la verifica anche degli altri campi del certificato tra cui il serial number.

La nuova modalità di gestione dei certificati risolve anche i seguenti problemi:

- I certificati che contengono molteplici campi "OU" vengono adesso gestiti correttamente.
- È possibile salvare anche i certificati che possiedono un subject con lunghezza superiore ai 255 caratteri.
- Corretta la gestione dei certificati in presenza di caratteri speciali.

4.6 Miglioramenti alla funzionalità di Caching della Risposta

Sono state introdotte le seguenti nuove funzionalità:

- *Digest*: aggiunta la possibilà di indicare quali header (per default nessuno) e quali parametri della url (per default tutti) concorrano alla generazione del digest .
- *Cache-Control*: aggiunta la gestione dell'header http "Cache-Control" per quanto concerne le direttive "no-cache", "no-store" e "max-age". Su ogni erogazione o fruizione di API è possibile disabilitare la gestione di qualcuna o di tutte le direttive.

- *Caching attivabile in funzione della Risposta*: la funzionalità di caching delle risposte è ora attivabile in funzione del return code http e del tipo di risposta ottenuta (fault).

4.7 Miglioramenti alla funzionalità di Autenticazione

Nella sezione "Controllo degli Accessi" di una erogazione o fruizione di API sono ora disponibili nuove modalità di accesso all'identità del client per l'autenticazione di tipo «principal»:

- *Container*: rappresenta l'unica modalità presente nelle precedenti versioni di GovWay.
- *Header HTTP*: il principal viene letto da un header http il cui nome viene indicato nella configurazione dell'erogazione o fruizione. La configurazione permette inoltre di indicare se l'header vada consumato dopo il processo di autenticazione o invece inoltrato.
- *Parametri della URL*: il principal viene letto da un parametro della url di invocazione il cui nome viene indicato nella configurazione dell'erogazione o fruizione. La configurazione permette inoltre di indicare se l'header vada consumato dopo il processo di autenticazione o invece inoltrato.
- *Indirizzo IP*: come principal viene utilizzato l'indirizzo IP del mittente.
- *Token*: il principal viene letto da uno dei claim presenti nel token.

Per quanto concerne invece l'autenticazione di tipo "http-basic" è stata aggiunta la possibilità di configurare se l'header http "Authorization" vada consumato dopo il processo di autenticazione o invece inoltrato.

4.8 Miglioramenti alla funzionalità di Sicurezza Messaggio

Sono state introdotte le seguenti nuove funzionalità riguardanti la sicurezza dei messaggi JSON:

- *JSON Web Signature - Unencoded Payload Option*: aggiunto il supporto per generare un JWS con il payload non codificato come descritto nel RFC 7797 (https://tools.ietf.org/html/rfc7797).
- *JSON Web Signature - Compact Detach*: aggiunto il supporto per generare un JWS con serializzazione "Compact" in modalità "Detach" come descritto nell'Appendice F del RFC 7515 (https://tools.ietf.org/html/rfc7515#appendix-F).
- *JWT Header per informazione sul certificato*: aggiunto supporto per la gestione degli header "x5c","x5u","jwk", "jku" sia per la Signature che per l'Encrypt.
- *JWT Header per custom e critical claim*: aggiunta possibilità di generare header custom e critical sia per la Signature che per l'Encrypt.
- *JWKSet*: aggiunta gestione dei keystore di tipo "jwk".

4.9 Miglioramenti alla Console di Gestione

Sono state introdotte le seguenti nuove funzionalità:

- *Connettività dei connettori*: è possibile verificare la connettività dei connettori http/https configurati. In caso di configurazione in cluster su più nodi, la connettività è verificabile sul singolo nodo che su tutti.
- *Restyling grafico della configurazione di una API*: migliorata la gestione delle informazioni relative alle funzionalità attive su una API (es. Controllo Accessi, Validazione ...) e alla suddivisione delle risorse in gruppi differenti.
- *Connettore di Default*: durante la creazione di una erogazione o di una fruizione, se è stata caricata un'interfaccia (OpenAPI, WSDL, WADL ...) che definisce un connettore, questo viene proposto come connettore di default da utilizzare.

- *CORS*: aggiunta possibilità di registrare gli "expose headers" tramite la modalità standard della console.
- *Informazioni*: sugli elementi relativi a funzionalità complesse (es. Correlazione Applicativa, Trasformazione, Connettore di tipo "file" ...) è stata introdotta la presenza di un elemento "info" che consente di ottenere maggiori informazioni.
- *Tempi di attesa durante la navigazione*: è stata ottimizzata l'acquisizione delle informazioni relative alle API sulle varie maschere della console, rendendo la navigazione sulle varie sezioni più veloce.
- *Selezione applicativo con differenti utenze*: risolto problema che non consentiva l'aggiunta di un applicativo o soggetto tra la lista degli autorizzati se alla console ci si collegava con una utenza differente da quella utilizzata per creare l'applicativo o il soggetto.

4.10 Miglioramenti alla Console di Monitoraggio

Sono state introdotte le seguenti nuove funzionalità:

- *Filtri di Ricerca*: effettuata riorganizzazione degli elementi presenti nel filtro di ricerca delle transazioni e di generazione delle statistiche.
- *Storico delle Transazioni*: le informazioni relative al Mittente (Soggetto e Applicativo) ed all'API (Nome, Versione, Soggetto Erogatore) sono state raggruppate per fornire una consultazione più immediata ed in linea con la riorganizzazione dei filtri di ricerca.
- *Distribuzione per Esito*: nel report visualizzato dopo aver effettuato il login, la legenda riportava un'ora errata (+1 rispetto all'ora corrente) per il periodo "Ultime 24 Ore". Il problema è stato risolto.

4.11 Miglioramenti al profilo di Fatturazione Elettronica

Sono state realizzate le seguenti nuove funzionalità al profilo di Fatturazione Elettronica:

- Nella Fatturazione Passiva è stata aggiunta alla traccia delle notifiche ricevute l'informazione sul Codice Destinatario della Fattura. Tale informazione è utile per smistare le fatture e notifiche ricevute per Codice Destinatario.
- Nella Fatturazione Attiva è stata aggiunta alla traccia delle notifiche ricevute l'informazione sull'IdTrasmittente (IdPaese + IdCodice) e l'identificativo dell'Applicativo che ha inviato la fattura. Le informazioni aggiunte possono essere utilizzate per collezionare le notifiche in base all'ApplicativoMittente o all'IdTrasmittente.
- Nella Fatturazione Passiva è stata aggiunta la possibilità di consegnare all'applicativo, oltre alla fattura, anche il file Metadati ricevuto dallo SDI. Il contenuto di tale file viene inserito, codificato in base64, nell'header HTTP "GovWay-SDI-FileMetadati".
- Aggiunta la possibilità di disabilitare la generazione, da parte di GovWay, dei nomi SDI da associare alle fatture da inviare (fatturazione attiva) e alle notifiche esito (fatturazione passiva). Se viene disabilitata la funzionalità (attiva per default), la gestione dei nomi dei file (correttezza sintattica, univocità, ...) è demandata all'Applicativo Client che deve obbligatoriamente fornire il nome del file attraverso un parametro della query ("NomeFile") o un header http ("GovWay-SDI-NomeFile").
- Realizzato adeguamento necessario per ricevere le notifiche nel nuovo formato "Fatturazione B2B".
- Corretto problema che causava un salvataggio errato dei dati presenti nella traccia della richiesta, nel caso in cui fossero rilevate eccezioni di livello "INFO". I dati della traccia della richiesta riportavano erroneamente i dati relativi alla risposta.

4.12 Miglioramenti al profilo eDelivery

E" stata introdotta la compatibilità con la versione 4 di Domibus

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus

4.13 Miglioramenti all'Installer

Sono state apportati i seguenti miglioramenti all'Installer binario:

- Aggiunta all'Installer la possibilità di indicare la generazione degli archivi relativi ai nuovi servizi di configurazione e monitoraggio tramite API.
- Non è più consentito installare GovWay senza la presenza del profilo "API Gateway".
- Aggiunto supporto per le nuove versioni dell'application server "WildFly" 15.x e 16.x

4.14 Continuous Integration

- *Introduzione dell'uso di Jenkins*: ogni commit sul master del progetto (https://github.com/link-it/govway) viene verificato tramite l'esecuzione di oltre 7000 test. Lo stato di ogni commit è verificabile accedendo alla pagina https://jenkins.link.it/govway/job/GovWay/
- *OWASP Dependency-Check*: tutte le dipendenze relative a jar 3parti vengono adesso verificate per sapere se esistono vulnerabilità conosciute (fase "verify" di Maven).

4.15 GovWay Docker

Le versioni rilasciate di GovWay sono disponibili su DockerHub: https://hub.docker.com/r/linkitaly/govway

Il progetto govway-docker (https://github.com/link-it/govway-docker) fornisce tutto il necessario per produrre un'ambiente di prova per GovWay funzionante in formato Docker, a partire dai sorgenti.

4.16 Sorgenti e Librerie 3Parti

Introdotto l'utilizzo di Maven (https://maven.apache.org/) per migliorare gli aspetti di gestone delle librerie esterne, di compilazione e di packaging. Ogni funzionalità introdotta, descritta di seguito, è attivabile con il relativo comando maven eseguibile nella radice del progetto:

- Le librerie 3parti non devono più essere reperite tramite un file statico esterno, ma vengono scaricate da rete nella fase "initialize". Per forzare il download è possibile utilizzare il comando "mvn initialize".
- Gli archivi jar sono ottenibili tramite il comando "mvn compile". Tutti i jar compilati saranno disponibili al termine della compilazione nella sottodirectory "dist".
- Il pacchetto di installazione può essere prodotto a partire dai sorgenti utilizzando il comando "mvn package".
- La documentazione presente all'interno del pacchetto di installazione viene prelevata dalla directory "resources/doc/pdf/". Per generarla a partire dai sorgenti (resources/doc/src/) è possibile utilizzare il comando "mvn package -Dpackage.doc.generate=true"

Nota: La generazione della documentazione, a partire dai sorgenti, richiede sphinx e latex.

4.17 Bug Fix

Sono stati risolti i seguenti bug:

- *Contatore Richieste Attive su Rate Limiting*: non venivano decrementati i contatori delle richieste attive di una policy di Rate Limiting, se la transazione aveva un esito per cui era stato disabilitato il tracciamento.
- *ProxyReverse*: gestita funzionalità ProxyReverse per header "Location" e "Content-Location" anche sui codici di risposta non inerenti il Redirect.
- *MultiTenant dopo aggiornamento*: l'aggiornamento dalla versione 3.0.0 alla versione 3.0.1 non permette di attivare il multi-tenant se nella precedente versione era stato creato più di un soggetto di dominio interno.

5 Versione 3.0.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.0.1 di GovWay. Per un elenco dettagliato dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al file ChangeLog di questa versione.

5.1 Nuova funzionalità Multi-Tenant

Semplificata drasticamente la gestione in modalità multi-tenant, prima possibile esclusivamente in maniera analoga alla precedente modalità di gestione della Console OpenSPCoop.

- *Attivazione*: è possibile attivare la modalità multi-tenant direttamente dalla console di gestione, tramite la sezione "Configurazione - Generale".
- *Selezione del dominio*: è possibile selezionare il soggetto su cui operare direttamente dalla testata delle console di configurazione e monitoraggio.
- *Comunicazioni interne al dominio gestito*: è possibile abilitare la gestione multi-tenant in modo da permettere interazioni tra soggetti fruitori ed erogatori entrambi appartenente al dominio interno.

5.2 Revisione dei formati di errore generati dal Gateway

I formati dei messaggi di errore generati dal Gateway sono ora conformi a quanto previsto dall'RFC 7807 e dalle specifiche AGID «MI 2018». Sono stati inoltre uniformati i messaggi di errore ritornati nelle erogazioni e nelle fruizioni.

Per le API di tipologia REST viene generato un oggetto *Problem Details* come definito nella specifica *RFC 7807* (https://tools.ietf.org/html/rfc7807). Le casistiche di errore supportate sono le seguenti:

- *401*: rientrano in questa castistica gli errori avenuti durante le fasi di autenticazione degli applicativi e di verifica del token OAuth
- *403*: identifica un'autorizzazione fallita
- *404*: richiesta una erogazione o fruizione inesistente
- *400*: l'errore occorso è imputabile ai dati forniti dal client (es. messaggio non valido in caso di validazione attiva)
- *429*: identifica una violazione della politica di Rate Limiting
- *503*: rientrano in questa casistica gli errori causati da una irraggiungibilità dell'applicativo indirizzato dal Gateway o una temporanea sospensione della erogazione/fruzione

- *500*: qualsiasi altro errore

Nell'elemento *detail* è presente il dettaglio dell'errore mentre nell'elemento *govway_status* una codifica in GovWay di tale errore.

Per le API di tipologia SOAP, sia in erogazione che in fruizione, viene generato un SOAPFault contenente un actor valorizzato con *http://govway.org/integration*. Nell'elemento *fault string* è presente il dettaglio dell'errore mentre nell'elemento *fault code* una codifica in GovWay di tale errore.

5.3 Revisione delle url di invocazione di una erogazione o fruizione

Sono state adottate le seguenti revisioni nelle url di invocazione di una erogazione e fruizione nel profilo "API Gateway" al fine di semplificarle ed adeguarle agli standard di mercato.

- *erogazione*: non è più obbligatorio specificare il protocollo *"api"* ed il canale di inbound *"in"*. La versione indicata nel path presenta inoltre il prefisso "v".
  - *precedente*: http://host/govway/**api/in/**Ente/API/1
  - *nuova*: http://host/govway/Ente/API/**v**1
- *fruizione*: sono state adottate le medesime revisioni dell'erogazione fatta eccezione per il canale di outbound *"out"* che rimane obbligatorio.
  - *precedente*: http://host/govway/**api/**out/Ente/EnteEsterno/API/1
  - *nuova*: http://host/govway/out/Ente/EnteEsterno/API/**v**1

5.4 Nuova funzionalità Gestione CORS

In GovWay è ora possibile gestire il *cross-origin HTTP request (CORS)* sia globalmente, in modo che sia valido per tutte le APIs, che singolarmente sulla singola erogazione o fruizione.

5.5 Nuova funzionalità Caching della Risposta

Per le API è adesso possibile abilitare la funzionalità di caching delle risposte in modo che successive richieste, con le medesimi caratteristiche (uri, http header, payload), vengono servite direttamente da GovWay. Per ogni api deve essere definito l'intervallo di tempo per cuì una risposta salvata in cache viene mantenuta.

5.6 Nuove funzionalità di Identificazione e Autorizzazione

Per le API erogate da Soggetti interni è ora permesso l'accesso anche da parte di applicativi (interni al dominio gestito) e non solo di Soggetti (esterni al dominio gestito).

5.7 Miglioramenti alle Console di Gestione e Monitoraggio

Sono state apportate le seguenti migliorie:

- *Restyling grafico del menù in testata*: perfezionata la gestione delle informazioni relative all'utente collegato, alle modalità di utilizzo e, se attivato il multi-tenant, al soggetto gestito.
- *Nuova presentazione delle API*: completo restyling delle modalità di visualizzazione e di editing delle API registrate.

5.8 Miglioramenti all'Installer

Sono state apportati i seguenti miglioramenti all'Installer binario:

- *Aggiornamento*; L'Installer può ora gestire anche l'aggiornamento del Software rispetto ad una precedente versione già installata.
- *SQL*; corretti gli script sql, prodotti dall'installer, che causavano errori se utilizzati sui seguenti database:
  - *SQLServer*, si otteneva il messaggio di errore: Introducing FOREIGN KEY constraint "fk_..." on table "..." may cause cycles or multiple cascade paths
  - *MySQL*, venivano segnalati diversi errori come il seguente: CONSTRAINT unique_... UNIQUE (...), - ERROR 1071 (42000): Specified key was too long; max key length is 767 bytes

6 Versione 3.0

Il software GovWay è l'evoluzione della Porta di Dominio OpenSPCoop, e riparte quindi dalla versione 3.0, riprendendo il precedente versionamento del software OpenSPCoop.

GovWay recepisce le tante innovazioni dell'interoperabilità applicativa intervenute nelle normative italiana ed europea e negli standard internazionali. Il cambio di nome del progetto da OpenSPCoop a GovWay è stato necessario per svincolare il prodotto da uno standard ormai deprecato come SPCoop, mantenendo però il focus sulle funzioni di API Gateway verticalizzato sulle forti peculiarità della Pubblica Amministrazione italiana.

Avremmo voluto pubblicare la nuova versione contestualmente al rilascio delle nuove linee guida di AGID, annunciate nel piano triennale per fine 2017. Il ritardo di questa specifica (alla data di rilascio sono disponibili i soli primi due capitoli introduttivi) ci ha convinti a rilasciare GovWay nella nostra «interpretazione» dell'attuale versione della nuova specifica, in attesa di poterci adeguare alla versione definitiva non appena disponibile.

Oltre al nuovo modello di interoperabilità (MI2018), Govway supporta nativamente:

- tutti i più recenti standard internazionali (i nuovi servizi RESTful, la gestione dei Token, in particolare per AUTH2 e OIDC, ed in generale tutte le ultime specifiche relative all'API Management);
- le normative dell'interoperabilità europea, basate sul «building block» eDelivery del progetto CEF (Connecting European Facilities), utilizzate per gli scambi applicativi trans-europei;
- la retrocompatibilità con SPCoop, ancora molto utilizzato e quindi per il momento sicuramente imprescindibile come protocollo di interoperabilità nella Pubblica Amministrazione Italiana.
- infine GovWay introduce infine il concetto di «govlet», connettori pronti per i principali servizi della PA italiana. Al momento sono disponibili govlet per SIOPE+, PagoPA e Fatturazione Elettronica, tutti scaricabili dal sito govway.org, ma la libreria di govlet è in rapida evoluzione.