Release Notes

Release 3.3.17

Link.it

08 lug 2025

Contents

1 Versione 3.3.17

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.17 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

1.1 Miglioramenti al Profilo di Interoperabilità "ModI"

In ottemperanza a quanto indicato nella segnalazione "https://github.com/AgID/specifiche-tecniche-DPR-160-2010/issues/198", è stata introdotta la possibilità di generare un token di integrità anche per richieste e/o risposte prive di payload, calcolando in questo caso il Digest su un body vuoto («»).

È stata inoltre migliorata la gestione della cache per i token di audit e per i token di autenticazione generati localmente dal fruitore. Un token viene adesso rigenerato prima della scadenza effettiva per evitare che il suo utilizzo prossimo alla scadenza risulti scaduto una volta ricevuto dall'erogatore.

1.2 Miglioramenti all'integrazione con la PDND

Per allinearsi alle modifiche introdotte dalla nuova versione delle Linee Guida AgID, la piattaforma è stata estesa con il supporto alle seguenti funzionalità.

Signal Hub

GovWay supporta l'integrazione dei soggetti erogatori di e-service, permettendo la configurazione diretta della funzionalità Signal Hub all'interno della piattaforma. In questo modo, tutte le funzionalità relative alla pseudoanonimizzazione dei dati e alla comunicazione con la PDND sono gestite automaticamente da GovWay, senza richiedere interventi sul backend dell'e-service.

L'integrazione trasparente è articolata in due componenti principali:

- Esposizione di un'operazione dedicata per il recupero delle informazioni crittografiche. GovWay espone automaticamente un'operazione REST/SOAP, conforme alle specifiche PDND, che consente ai fruitori di ottenere le informazioni crittografiche necessarie alla pseudoanonimizzazione degli identificativi relativi ai dati oggetto di variazione. L'implementazione è completamente gestita dalla piattaforma: l'e-service non deve sviluppare alcuna logica specifica, ma solo adeguare l'interfaccia pubblicata sulla PDND secondo le specifiche fornite da GovWay.
- Esposizione di un'interfaccia semplificata per l'invio dei segnali. GovWay fornisce un endpoint dedicato che l'e-service può invocare per pubblicare le variazioni di dato (segnali) senza doversi occupare della generazione dell'identificativo pseudoanonimizzato o della gestione delle complessità del protocollo Signal Hub (es. progressivi per ogni segnale). La piattaforma si occupa internamente di garantire la conformità alle specifiche PDND.

Tracing

In conformità con le nuove disposizioni, gli e-service devono trasmettere regolarmente alla PDND un report giornaliero in formato CSV contenente i log delle chiamate ricevute tramite l'interoperabilità.

GovWay gestisce in modo completamente trasparente questa funzionalità, occupandosi della raccolta, aggregazione e invio automatico dei tracciamenti attraverso le API messe a disposizione dalla PDND. In questo modo, il soggetto erogatore non deve implementare alcuna logica aggiuntiva né preoccuparsi degli aspetti tecnici legati al conferimento dei log.

Identificativi presenti nel Voucher PDND

Tra gli header di integrazione inoltrati al backend sono adesso presenti anche le informazioni relative al consumerId, producerId, eserviceId e descriptorId presenti nel voucher PDND.

API Interoperabilità

Le informazioni recuperate tramite le API di interoperabilità relative all'identificativo esterno (externalId) e all'identificativo di registro della PDND (consumerId) di una organizzazione sono adesso utilizzabili per:

- filtrare le transazioni nelle ricerche dello storico e nella generazione di report statistici;
- generare report "3D" che utilizzano gli identificativi come informazione da visualizzare;
- raggruppare le richieste nel criterio di conteggio di una policy di Rate Limiting.

Inoltre il consumerId viene adesso visualizzato tra le informazioni di dettaglio di una transazione.

Infine è stata migliorata la gestione delle informazioni parziali o non disponibili ottenute dalle API Interop in relazione al clientId. In tali casi, le informazioni vengono comunque memorizzate temporaneamente nella cache locale, al fine di evitare chiamate ripetute e non necessarie verso la PDND. Tuttavia, rispetto alle informazioni acquisite correttamente, la loro permanenza in cache è ora ridotta: il valore predefinito è fissato a 5 minuti, contro i 30 giorni previsti per i dati completi

Finalità

È adesso possibile effettuare ricerche nello storico delle transazioni tramite l'identificativo della finalità PDND (purposeId). Inoltre nel dettaglio di una transazione, nella sezione "Informazioni Mittente", viene adesso visualizzato anche l'identificativo della finalità.

Token Policy di negoziazione

È stato introdotto un valore di default per il campo "purposeId", che consente di definire e gestire purposeId differenti in funzione degli applicativi associati alla fruizione. Inoltre, il box informativo relativo al campo purposeId è stato arricchito con una descrizione dettagliata dei valori ammessi, fornendo indicazioni utili per l'implementazione di diversi scenari configurativi.

1.3 Introduzione supporto per l'integrazione con i servizi SUAP

Utilizzando GovWay per la gestione dell'interoperabilità ModI, non è possibile delegare direttamente al backend SUAP tutti i casi di errore previsti dalla Specifica Tecnica DPR-160.

Ciò è dovuto al fatto che alcune comunicazioni vengono gestite direttamente da GovWay stesso, in presenza di errori di interoperabilità (ad esempio, token PDND non valido) o di problematiche di connettività verso il backend (ad esempio, connection refused o timeout). Gli errori generati da GovWay (ad esempio errori di autenticazione o indisponibilità del backend) rispettano la specifica *RFC 7807* (https://tools.ietf.org/html/rfc7807), per la rappresentazione strutturata delle informazioni di errore, come previsto dalle Linee Guida di Interoperabilità. Al contrario, il formato degli errori previsto dalla specifica SUAP non risulta conforme, in quanto prevede la trasmissione degli errori attraverso oggetti JSON con una struttura differente, di cui si riporta di seguito un esempio:

```
{ "code": "ERROR_401_001", "message": "PDND token not found"}
```

Per garantire la conformità con i formati di errore attesi è stato quindi realizzato un plugin, attivabile all'interno della configurazione delle erogazioni dei servizi SUAP su GovWay, che consente di gestire i casi di errore e di trasformarli nella struttura JSON attesa, secondo quanto descritto nella Specifica Tecnica DPR-160.

Gli errori gestiti da GovWay sono i seguenti:

- *ERROR_400_001 - incorrect request input*: uno o più parametri e/o la forma del body dell'operation non rispettano la sintassi definita nell'IDL OpenAPI.
- *ERROR_401_001 - PDND token not found*: token di autorizzazione della PDND non presente nella richiesta.
- *ERROR_401_002 - Invalid PDND token*: token di autorizzazione della PDND non valido.
- *ERROR_401_003 - AgID-JWT-Signature* token not found: la richiesta non contiene l'header AgID-JWT-Signature.
- *ERROR_401_004 - invalid AgID-JWT-Signature token*: token nell'header AgID-JWT-Signature non valido.
- *ERROR_404_001 - resource not found*: risorsa richiesta non esistente.
- *ERROR_500_007 - response processing error*: copre solamente i due casi seguenti:

  - backend non disponibile: rappresenta la casistica in cui il backend non è raggiungibile per vari motivi (es. connection refused, connection timeout, read timeout).
  - backend torna una risposta 5xx senza content-type o con un un content-type differente da application/json.

Nota

Rimangono a carico dell'implementazione del backend SUAP gli altri codici di errore.

1.4 Bug Fix

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2025-48976: aggiornata libreria "commons-fileupload:commons-fileupload" alla versione 1.6.0
- CVE-2025-48734: aggiornata libreria "commons-beanutils:commons-beanutils" alla versione 1.11.0

Sono stati risolti i seguenti bug che avvenivano in alcune condizioni limite caratterizzate da un numero elevato di richieste simultanee:

- il contatore delle richieste in corso non veniva decrementato correttamente, causando il rifiuto delle richieste con errore 429, anche in assenza del numero effettivo di richieste simultanee previsto dal limite;
- in caso di elevato numero di richieste SOAP simultanee, in situazioni limite di blocco dovuto a interazione con componenti esterni nella gestione delle richiesta (es: autorizzazione verso servizi esterni), poteva essere saturato il pool dei SAX Parser utilizzati per la gestione dei messaggi, provocando il fallimento anche di richieste non coinvolte nel problema generando il seguente errore nei log: «Couldn't get a SAX parser while constructing a envelope».

Per la console di gestione sono stati risolti i seguenti bug:

- Aggiunto supporto, nel caricamento di un'interfaccia OpenAPI, per le seguenti casistiche, precedentemente segnalate erroneamente come anomalie:
  - utilizzo delle anchor YAML (&chiave) e dei relativi riferimenti (*chiave);
  - definizione di parametri con schema: {}
- Corretto un malfunzionamento relativo alla creazione di un utente amministratore in ambiente single-tenant con successiva abilitazione dei flag DR. Sebbene il sistema impedisse correttamente la selezione dei soggetti (non previsti in modalità single-tenant), l'utenza creata nella base dati risultava non conforme e non era utilizzabile per l'accesso alla console di monitoraggio;
- Risolto problema di paginazione: durante la creazione di un nuovo oggetto, se l'utente si trovava su una pagina successiva alla prima all'interno di una lista paginata, l'interfaccia presentava comportamenti anomali.
- Nella funzionalità "Importa", utilizzata per modificare i dati di una govlet mediante input acquisiti in fase di importazione, è stato corretto un malfunzionamento che impediva la corretta sostituzione dei segnaposto nelle proprietà associate ai profili di interoperabilità.

Per le API di configurazione sono stati risolti i seguenti bug:

- corretta un'anomalia relativa all'utilizzo del parametro "profilo_qualsiasi" impostato a true nelle chiamate che restituiscono la lista delle erogazioni, delle fruizioni o delle API. Gli oggetti presenti nella lista risultante venivano erroneamente associati al profilo di interoperabilità di default, anziché a quello effettivamente configurato.

2 Versione 3.3.16

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.16 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.16 utilizzare l'ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.16.p2*
- *Bug Fix 3.3.16.p1*

2.1 Miglioramenti alla gestione dei Certificati X.509

La funzionalità di validazione dei certificati tramite lista di revoca (CRL) è stata ampliata per consentire il download della CRL specificata nell'estensione "CRLDistributionPoints" anche tramite il protocollo LDAP, oltre ai protocolli HTTP già precedentemente supportati.

2.2 Miglioramenti alla gestione dei Keystore

Nota

Nuova Funzionalità introdotta nella versione "3.3.16.p1"

È adesso possibile utilizzare keystore PKCS12 e JKS senza password.

2.3 Miglioramenti alla funzionalità di Autenticazione

Il gestore delle credenziali, utilizzabile per l'autenticazione dei certificati client ottenuti tramite header HTTP, supporta adesso la possibilità di interpretare un header valorizzato con una stringa vuota come indicazione che il fruitore non ha presentato alcun certificato client.

2.4 Miglioramenti alla funzionalità di Gestione dei Token

Aggiunto un criterio di tolleranza per la validazione del claim "nbf" nei token di sicurezza ModI e nei token validati tramite Token Policy. La tolleranza predefinita è impostata a 5 secondi, con la possibilità di personalizzarla tramite la configurazione di GovWay.

2.5 Miglioramenti alla funzionalità di Validazione dei Contenuti

La funzionalità di validazione dei contenuti tramite OpenAPI è stata modificata per garantire che i payload contenenti elementi "date-time" non conformi a RFC 3339 (#section-5.6), come caratteri minuscoli (t, z) o spazi (" ") al posto del separatore T, vengano rifiutati.

Prima della modifica tali formati venivano accettati nei payload ma non negli header, nei parametri delle URL e nei path; adesso la validazione è uniforme su tutte le sorgenti.

È stata inoltre introdotta una configurazione parametrica che consente, se necessario, di ripristinare l'accettazione di formati non conformi.

2.6 Miglioramenti alla funzionalità di RateLimiting

Aggiunta una nuova metrica utilizzabile nelle politiche di Rate Limiting: «Numero Richieste Completate con Successo o Fault Applicativi».

Inoltre il controllo attuato dalla policy di rate limiting per dimensione messaggio è stato ottimizzato per utilizzare il valore dell'header HTTP "Content-Length" se presente.

Infine nella funzionalità di controllo del traffico con sincronizzazione distribuita tramite hazelcast, è stato introdotto un meccanismo di recupero in caso di eccezione "DistributedObjectDestroyedException" che può avvenire in casi limite in configurazioni del cluster che non utilizzano il CP Subsystem. Nell'intervento è stato reso configurabile il sistema di diagnostica di hazelcast e la validazione della configurazione utilizzata.

2.7 Miglioramenti alla funzionalità dei Connettori

Aggiunto un nuovo tipo di connettore, selezionabile tramite configurazione avanzata, che implementa la verifica dello stato di un servizio. Il nuovo connettore può essere utilizzato per supportare direttamente su GovWay la risorsa "/status" richiesta dalle linee guida ModI, nel caso in cui questa non sia nativamente disponibile nel backend dell'API.

2.8 Miglioramenti alla funzionalità di Trasformazione

In presenza di messaggi SOAPWithAttachments, è adesso possibile utilizzare una trasformazione per forzare la generazione del parametro "start" nel Content-Type.

2.9 Miglioramenti alla funzionalità "Header di Integrazione"

Nota
Nuova Funzionalità introdotta nella versione "3.3.16.p1"

È stata introdotta una nuova funzionalità che gestisce la riscrittura di eventuali header in ingresso con prefisso «GovWay-», producendo nuovi header HTTP con prefisso "GovWay-Peer-".

Questa funzionalità risulta particolarmente utile negli scenari di fruizione ModI o SPCoop, in cui anche la parte erogatrice è esposta tramite GovWay. In tali contesti, permette al client di ricevere entrambi gli identificativi generati dal GovWay locale e da quello dalla parte erogatrice, migliorando la tracciabilità e la gestione delle eventuali richieste di supporto.

2.10 Miglioramenti al Profilo di Interoperabilità "ModI"

Migliorata la gestione della registrazione di repository multipli delle chiavi PDND e/o di utilizzo di client interop differenti in ambiente Multi-Tenant:

- i repository multipli vengono ora rilevati automaticamente nella console di gestione e nei timer dedicati alla gestione delle interazioni con la PDND, eliminando la necessità di attivazione manuale nelle configurazioni dei vari tool;
- la proprietà "remoteStore.pdnd.baseUrl" può ora essere definita utilizzando esclusivamente la base URL, senza il suffisso "/keys";
- aggiunti ulteriori criteri di personalizzazione per le configurazioni Multi-Tenant.

È stata inoltre risolta un'anomalia nella funzionalità ModI relativa all'imbustamento delle fruizioni per applicativi identificati tramite autenticazione interna di tipo "token". Il keystore definito nell'applicativo non veniva correttamente utilizzato, generando le seguenti segnalazioni di errore:

- in caso di token generati senza PDND:

  «Il profilo di sicurezza richiesto “idam01” richiede l’identificazione di un applicativo».

- in caso di negoziazione del token tramite PDND:

  «Il tipo di keystore indicato nella token policy “PDND” richiede l’autenticazione e l’identificazione di un applicativo fruitore: Servizio applicativo anonimo».

2.11 Miglioramenti all’integrazione con la PDND

Nota

Nuova Funzionalità introdotta nella versione “3.3.16.p2”

È Stato adeguato il profilo di interoperabilità “ModI” alle nuove linee guida PDND indicate nell’issue “https://github.com/pagopa/pdnd-interop-frontend/issues/1215”:

- rivista la generazione dell’asserzione per la richiesta di voucher PDND, assicurando che includa esclusivamente i claim previsti dalla specifica;
- introdotta la possibilità di configurare l’ID Ente per i soggetti con profilo ModI; in fase di validazione del voucher viene ora verificata la corrispondenza tra il claim producerId e l’ID Ente dell’erogatore configurato;
- introdotta la possibilità di indicare “eserviceId” e/o “descriptorId” nella configurazione dell’erogazione; in fase di validazione del voucher viene ora verificata la corrispondenza tra il claim eserviceId e/o il claim descriptorId con i corrispettivi valori configurati;
- infine sono aggiunti controlli espliciti sulla presenza dei claim “iat”, “exp” e “nbf” durante la validazione dei voucher PDND.

2.12 Miglioramenti dei Log Applicativi

Nota

Nuova Funzionalità introdotta nella versione “3.3.16.p1”

Aggiunta la possibilità di personalizzare i log applicativi di debug prodotti dalle applicazioni di GovWay tramite variabili di sistema o parametri Java. Le nuove opzioni permettono di:

- abilitare il log su console;
- aggiungere un identificativo del nodo nel percorso di log, facilitando la condivisione dello stesso filesystem tra più istanze;
- abilitare il log in formato JSON.

2.13 Miglioramenti alla Console di Gestione

Migliorata l’usabilità con l’introduzione della funzionalità di copia negli appunti al passaggio del mouse su campi specifici, come ad esempio «URL Invocazione» e «Connettore» delle erogazioni o fruizioni.

Inoltre nella sezione «runtime» è stata introdotta la possibilità di effettuare il refresh della pagina mantenendo l’utente nella stessa sezione in cui è stato effettuato il refresh.

2.14 Bug Fix

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2025-23184:
  - aggiornata libreria "org.apache.cxf:*" alla versione 3.6.5
  - aggiornata libreria "org.ow2.asm:asm" alla versione 9.7.1
- CVE-2024-38827: aggiornata libreria "org.springframework.security:*" alla versione 5.8.16
- CVE-2024-38829: aggiornata libreria "org.springframework.ldap:*" alla versione 2.4.4
- CVE-2024-47535: aggiornata libreria "io.netty:*" alla versione 4.1.115
- Corrette nuove segnalazioni di vulnerabilità emerse in seguito all'aggiornamento dei seguenti tools di analisi statica:
  - SpotBugs alla versione 4.8.6;
  - SonarQube alla versione "10.7".

Sono stati risolti i seguenti bug:

- risolta anomalia presente nella funzionalità "FileTrace" per la registrazione delle transazioni, dove l'informazione "requester", se registrata con l'opzione "logBase64", veniva codificata in Base64 due volte;
- quando la funzionalità di proxy pass reverse per gli header HTTP è attiva, se un header Location contiene un'URL con query parameter che non corrisponde a quella del connettore (e quindi non viene tradotta), l'header veniva inoltrato al client senza i query parameters.

Per la console di gestione sono stati risolti i seguenti bug:

- utilizzando il database "SQLServer", si verificava un errore inatteso accedendo alla sezione "Handler" nelle opzioni avanzate di un'erogazione/fruizione e cliccando su una qualsiasi delle liste relative alla richiesta o alla risposta.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- il filtro utilizzato per la ricerca delle transazioni o per la generazione di report statistici non permetteva di selezionare una risorsa o un'azione semplicemente scegliendo l'API. Era necessario selezionare la voce Implementazione API. Ora, il filtro per risorse/azioni consente la selezione sia tramite l'API che tramite la sua implementazione, offrendo maggiore flessibilità.
- corretta anomalia che causava la registrazione di comandi SQL nel file di log "govway_monitor_core.log" invece che nel file "govway_monitor_sql.log".

Infine è stato aggiunto su tutti i tools un controllo dello stato della connessione al rilascio al datasource che consente di:

- verificare la presenza di transazioni aperte (autoCommit disabilitato);
- effettuare il log dello stack trace per identificare la classe responsabile;
- richiamare *setAutoCommit(true)* per ripristinare lo stato corretto.

Grazie all'introduzione del controllo sulla connessione è stato individuata e corretta un'anomalia presente in alcuni casi limite, in cui i driver per l'accesso al database delle configurazioni restituivano al pool una connessione con l'opzione autoCommit disabilitata.

2.15 Bug Fix 3.3.16.p1

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2025-22228: aggiornata libreria "org.springframework.security:spring-security-crypto" alla versione 5.8.16-gov4j-1;
- CVE-2025-25193: aggiornata libreria "io.netty:*" alla versione 4.1.118.Final.

Sono stati risolti i seguenti bug:

- Il token presente nell'header "Authorization" non veniva inoltrato al backend in caso di API SOAP, nonostante la configurazione ne prevedesse l'inoltro.
- I contatori delle policy di rate limiting non venivano aggiornati correttamente se si disabilitava il tracciamento su database.
- Migliorata la tracciabilità nei casi in cui una policy non veniva elaborata a causa di malfunzionamenti interni, configurazioni errate o altre anomalie. In queste circostanze viene ora assegnato un esito di errore generico, distinto da «Violazione Rate Limiting», consentendo il tracciamento e la diagnosi anche quando la registrazione delle policy violate è disabilitata.
- Nel profilo di interoperabilità "ModI" una configurazione della risposta che prevedeva la personalizzazione del claim "aud" veniva ignorata, impedendo l'assegnazione del valore configurato nei token di risposta generati.
- Nella funzionalità di validazione dei contenuti applicativi per API SOAP, sono state risolte le seguenti anomalie:
  - In caso di fallimento nella costruzione dello schema XSD, la collezione degli schemi veniva serializzata nella directory */tmp*, causando potenziali problemi di esaurimento dello spazio nella partizione temporanea. Ora la collezione degli schemi viene registrata in una directory interna alla directory di log associata a GovWay, migliorando la gestione dello spazio e facilitando il debug.
  - In presenza di schemi XSD con un grafo di import ciclico, l'applicazione andava in out of memory a causa della mancata gestione corretta di tale situazione.
  - In presenza di allegati contenenti uno spazio nel nome del file la validazione dei contenuti falliva.
  - Risolta l'anomalia «The prefix "xml" cannot be bound to any namespace other than its usual namespace; neither can the namespace for "xm"» be bound to any prefix other than "xml".» che poteva accadere se l'API contenente lo schema "http://www.w3.org/XML/1998/namespace" tra gli allegati caricati.
- La diagnostica di Hazelcast veniva mantenuta attiva per default, generando file di log nel percorso LOG_DIR/hazelcast con il formato diagnostics-#-.log. Sebbene fossero presenti meccanismi di rotazione basati sulla dimensione del file, il nome del log cambiava a ogni riavvio dell'application server, portando nel tempo all'accumulo di file e al rischio di esaurimento dello spazio su disco. Per prevenire questo problema, la diagnostica di Hazelcast viene adesso disabilitata di default.
- (https://github.com/link-it/govway/issues/191) Arricchite tabelle "statistiche" e "transazioni_info" con una colonna "id" definita come primary key.
- Nelle configurazioni dei Key Management Service utilizzati per le funzionalità "BYOK", veniva erroneamente utilizzata la keyword "ksm" al posto di "kms". È stata apportata la correzione, mantenendo tuttavia il supporto della vecchia keyword per motivi di retrocompatibilità, deprecandone l'utilizzo.
- Le funzionalità di lock basate su semafori sono state estese con uno scheduler che permette il rilascio automatico del lock dopo un timeout configurabile.
- Nel log applicativo "govway_core", in condizioni limite, avveniva il seguente errore: «Errore durante il dump del soap fault».
- Introdotta una gestione delle risposte Problem Details non conformi; ora il connettore intercetta e registra correttamente le risposte contenenti Problem Details con struttura non valida (es. {«code»:500,»status»:»internal

error»}), evitando la terminazione anomala della transazione. In questi casi, tuttavia, il codice di stato non può essere interpretato, quindi eventuali rispedizioni condizionate su tale informazione non saranno eseguite.

Per la console di gestione sono stati risolti i seguenti bug:

- Se il numero di regole di proxy pass definite superava le 9, l'ordinamento previsto non veniva mantenuto, causando un riordino errato. In particolare, le regole venivano ordinate in modo lessicografico anziché numerico.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- Corretto un problema nella risoluzione delle informazioni PDND nell'elenco delle transazioni e nei report statistici, che si verificava in presenza di più clientId associati alla stessa organizzazione. In tali casi, solo uno dei clientId veniva risolto correttamente, mostrando i dati dell'organizzazione, mentre per gli altri la risoluzione non avveniva come previsto.
- È stato corretto un comportamento anomalo nel filtro di ricerca delle azioni per le API SOAP nelle sezioni «Transazioni» e «Statistiche», che impediva la selezione delle azioni. Il filtro funzionava correttamente per le API di tipo REST.
- Nella ricerca per token, per principal o per indirizzo ip non veniva effettuato il trim del valore inserito in input.
- (https://gitlab.link.it/gitlab/linkit/dev/govway/govway/-/issues/1583) Aggiunto il suffisso ".rollingFile" ai RollingFile appender in monitor.log4j2.properties per uniformarli agli altri file di configurazione log4j del progetto.

Per le API di configurazione sono stati risolti i seguenti bug:

- aggiunto supporto per configurare un truststore di tipo PDND;
- introdotto controllo sul valore del claim "tipo_servizio" in modo da verificare che sia uno dei valori ammessi dal profilo di interoperabiltà.

2.16 Bug Fix 3.3.16.p2

Corretto malfunzionamento sulla console di gestione "govwayConsole" che impediva lo scorrimento di oltre 20 elementi nella cache PDND.

Risolto inoltre un bug nelle API di configurazione che non consentiva la creazione di un API con interfaccia "OpenApi3.0".

3 Versione 3.3.15

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.15 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.15 utilizzare l'ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.15.p2*
- *Bug Fix 3.3.15.p1*

3.1 Nuova funzionalità di cifratura delle informazioni confidenziali

È stato aggiunto il supporto alla gestione delle informazioni confidenziali memorizzate su database e delle chiavi/keystore presenti su filesystem attraverso la cifratura/decifratura dei dati mediante una master key, utilizzando uno dei seguenti approcci:

- HYOK (Hold Your Own Key): le operazioni di cifratura e decifratura avvengono utilizzando una master key presente in un keystore memorizzato su filesystem o all'interno di un HSM.
- BYOK (Bring Your Own Key): la master key viene depositata su un servizio remoto (es. in cloud). In questo caso, le operazioni di wrap-key e unwrap-key delle informazioni confidenziali vengono gestite tramite chiamate API esposte dal servizio remoto.

La console di gestione è stata modificata per:

- assicurare la cifratura dei campi contenenti informazioni confidenziali;
- consentire l'indicazione di una modalità "unwrap" di un keystore cifrato riferito nella configurazione di un connettore https o nella sicurezza messaggio (es. token ModI);
- consentire la registrazione di proprietà definite con un valore cifrato nei seguenti elementi di registro:
  - API erogata o fruita
  - soggetto
  - applicativo
  - configurazione globale

È stato inoltre realizzato il supporto per inizializzare una serie di variabili Java che potranno essere riferite in qualsiasi file di proprietà di GovWay presente nella "directory-lavoro" e nelle configurazioni di GovWay (es. all'interno di una trasformazione).

La definizione di una variabile può essere attuata all'interno di due file differenti:

- govway.map.properties: le variabili definite in questo file verranno caricate all'avvio di tutte le applicazioni GovWay (es. runtime, console, batch ecc.);
- govway.secrets.properties: a differenza del precedente file, i valori delle variabili potranno essere definiti cifrati e GovWay si occuperà di decifrarli prima del loro caricamento nel sistema.

3.2 Miglioramenti alla funzionalità di Tracciamento

Migliorata funzionalità di tracciamento introducendo la possibilità di personalizzare l'aggiornamento delle tracce su database e/o su file (FileTrace) in corrispondenza dei 4 eventi principali della gestione di una richiesta:

- Richiesta ricevuta
- Richiesta in consegna
- Risposta in consegna
- Risposta consegnata

La modalità di tracciamento può essere personalizzata sia a livello di configurazione generale che per le singole erogazioni o fruizioni. Inoltre, per ogni evento, GovWay può essere configurato per far terminare la richiesta con errore in caso di tracciamento fallito o proseguire segnalando l'anomalia solamente nei log.

Per il caso di richiesta terminata con un errore di tracciamento è stato aggiunto il nuovo esito di "Tracciamento Fallito".

Sono state introdotte le seguenti nuove funzionalità di tracciamento su file (FileTrace):

- possibilità di attivare il tracciamento rispetto all'esito di una transazione;
- è possibile modificare la configurazione di default per ogni singola erogazione o fruizione, nello specifico per:
  - il file di configurazione che definisce il formato del log;
  - l'attivazione o meno del buffer dei messaggi, che consente di registrare gli header HTTP e il contenuto del payload;

- possibilità di utilizzare una chiave/keystore cifrata e specificare la policy necessaria per decifrarla, prima di utilizzarla per la cifratura dei dati registrati nel log.

Nel menù principale la configurazione a livello globale del tracciamento e della registrazione messaggi è stata suddivisa in due voci distinte.

Infine è stato modificato il comportamento predefinito in modo che il tracciamento delle richieste che violano una politica di RateLimiting sia disabilitato.

3.3 Miglioramenti al Profilo di Interoperabilità "ModI"

È stato introdotta la gestione del "soggetto intermediario", che consente di autorizzare una richiesta proveniente da un soggetto identificato sul canale e da un applicativo appartenente a un soggetto differente, identificato tramite token di sicurezza.

Nell'occasione, è stato affinato il processo di autenticazione:

- Il processo di identificazione degli applicativi veniva inutilmente attivato per l'autenticazione MTLS delle erogazioni, anche se con tale profilo gli applicativi possono essere censiti solamente con credenziale di tipo "token" o con certificato di firma; tale controllo è stato pertanto eliminato.
- I controlli di esistenza di un applicativo già registrato con lo stesso certificato sono stati affinati al fine di escludere gli applicativi con profilo di interoperabilità "ModI" di un dominio esterno, poiché tali certificati non si riferiscono a credenziali TLS ma vengono utilizzati solo per firmare token di sicurezza.

Sono stati apportati i seguenti miglioramenti alla funzionalità di integrazione con la PDND:

- aggiunta, nelle politiche di Rate Limiting, la possibilità di conteggiare per nome dell'organizzazione ottenuta tramite le API di interoperabilità della PDND;
- aggiunta la possibilità di modificare sulla singola erogazione o fruizione il comportamento di default per far fallire la transazione nel caso in cui il recupero delle informazioni sul client o sull'organizzazione tramite API PDND fallisca;
- le informazioni sull'organizzazione, recuperate tramite le API PDND, vengono ora propagate al backend tramite gli header di integrazione: GovWay-Token-PDND-OrganizationName, GovWay-Token-PDND-OrganizationCategory e GovWay-Token-PDND-OrganizationExternal.

Sono infine stati apportati i seguenti miglioramenti:

- (https://github.com/link-it/govway/issues/161) aggiunta validazione dei campi contenenti codici crittografici come ad esempio il clientId o il KID relativo ai token pdnd;
- in una configurazione che prevedeva un access token PDND (ID_AUTH_REST_01), il claim "jti" presente all'interno del token non veniva utilizzato come identificativo messaggio della richiesta, alla quale veniva invece associato un identificativo generato da GovWay. L'anomalia comportava:
  - un doppio tracciamento sia del claim "jti" che dell'identificativo generato da GovWay;
  - una valorizzazione dell'header di integrazione "GovWay-Message-ID" con l'identificativo generato da GovWay invece del jti.

3.4 Miglioramenti al Profilo di Interoperabilità "SPCoop"

Nota

La funzionalità è stata introdotta nella versione "3.3.15.p2"

Se il gateway fruitore riceve dalla controparte erogatrice del servizio un messaggio di errore SPCoop come risposta, la busta viene validata e viene generato un messaggio applicativo di errore che viene ritornato all'applicativo mittente, come descritto nel documento «Sistema pubblico di cooperazione: PORTA DI DOMINIO v1.1», voce «PD_UR-5».

Anche con la voce «Sbustamento SPCoop» disabilitata, viene comunque restituito un messaggio applicativo di errore.

È stata aggiunta la possibilità di modificare il comportamento di default, precedentemente descritto, per inoltrare all'applicativo mittente esattamente il messaggio di errore SPCoop ricevuto dalla controparte.

3.5 Miglioramenti alla funzionalità dei Connettori

È adesso possibile specificare il metodo di autenticazione "Api Key" consentendo di inviare al backend una chiave di identificazione veicolata in un header http come descritto nella specifica "OAS3 API Keys" (https://swagger.io/docs/specification/authentication/api-keys/).

Viene supportata anche la modalità "App ID" che prevede oltre all'ApiKey un identificatore dell'applicazione, modalità denominata "Multiple API Keys" nella specifica "OAS3 API Keys".

La configurazione permette anche di personalizzare il nome degli header http, rispetto a quanto indicato nella specifica "OAS3 API Keys".

Inoltre è stata aggiunta la possibilità di abilitare o disabilitare la funzionalità di "encoded word" per i valori degli header HTTP, oltre alla possibilità di personalizzarne gli aspetti di codifica per singole erogazioni o fruizioni di API attraverso la definizione di proprietà specifiche.

3.6 Miglioramenti alla funzionalità di Gestione dei Token

È ora possibile definire una token policy di validazione tramite una "well-known URL" come descritto nella specifica "https://swagger.io/docs/specification/authentication/openid-connect-discovery".

Inoltre, è stata aggiunta la possibilità di definire il keystore contenente le chiavi necessarie per effettuare una "validazione JWT" del token, anche indicando un endpoint.

È stata aggiunta la possibilità di utilizzare policy OCSP nei connettori HTTPS riferiti nelle token policy di validazione e negoziazione.

Nella configurazione di una token policy di negoziazione, è ora possibile indicare di utilizzare direttamente il payload di risposta HTTP come access token.

Infine, è stato risolto un problema che si presentava selezionando un'autenticazione HTTPS client nella funzionalità specifica di introspection o userinfo, senza abilitare l'endpoint HTTPS nella sezione token. In questo scenario, la gestione personalizzata dei keystore utilizzati per la connessione HTTPS non veniva attivata.

3.7 Miglioramenti alla funzionalità di Sicurezza Messaggio

La funzionalità di verifica dei certificati, abilitabile tramite la console di gestione, include adesso anche la validazione dei keystore riferiti nella configurazione della sicurezza dei messaggi.

Inoltre, è stata aggiunta la possibilità di disabilitare la "Compliance BSP 1.1" nella validazione di un messaggio contenente WS-Security Username Token.

Infine sono state introdotte opzioni aggiuntive che consentono di modificare alcuni aspetti relativi alla sicurezza del messaggio attuata tramite la libreria "wss4j", al fine di renderlo interoperabile con altre librerie più datate:

- encoding in base64 dell'attachment prima o dopo aver applicato la sicurezza;
- gestione dell'elemento "InclusiveNamespace" in presenza di lista di prefissi vuota e all'interno dell'elemento "CanonicalizationMethod";
- gestione dell'elemento "KeyInfo" presente all'interno dell'elemento "EncryptedData";
- aggiunta o meno delle parentesi uncinate ("<" e ">") nei riferimenti agli allegati;

- aggiunta dell'header di un attachment all'interno del messaggio cifrato;
- aggiunto il supporto per lo scambio di chiavi simmetriche di cifratura usando un'altra chiave simmetrica condivisa, tramite la gestione di keystore di tipo "jceks".»

3.8 Miglioramenti alla Console e alle API di Monitoraggio

Sono stati apportati i seguenti miglioramenti alle funzionalità di reportistica:

- il report "heatmap" fornito con la distribuzione statistica in 3 dimensioni è stato migliorato per:
  - contenere una legenda che descriva la corrispondenza tra tonalità del colore e misura rappresentata;
  - possibilità di visualizzare in ogni quadratino la misura;
- è ora possibile produrre una distribuzione statistica in 3 dimensioni personalizzata, dove al posto della data è possibile selezionare l'informazione da includere nel report.

3.9 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- aggiunti i seguenti tools command line presenti nella directory *dist/tools* prodotta dall'installer:
  - *govway-vault-cli* consente:
    - la cifratura o decifratura di informazioni o chiavi tramite una master key;
    - l'aggiornamento di una base dati esistente, consentendo di cifrare le informazioni confidenziali precedentemente salvate in chiaro o di aggiornarle attraverso l'utilizzo di una differente master key.
  - *govway-config-loader* dispone delle medesime funzionalità presenti nella sezione "Importa" della console di gestione, che consentono di importare o eliminare le configurazioni memorizzate in un archivio ottenuto con la funzionalità "Esporta".
- i file relativi ai profili di interoperabilità (es. modipa_local.properties) presenti nella configurazione esterna (es. /etc/govway) non venivano configurati correttamente dall'installer se erano presenti archivi patch al suo interno;
- gli archivi "patch" relativi ai profili di interoperabilità (es. openspcoop2_modipa-protocol-<version>.jar) non venivano configurati nel file di proprietà interno (es. modipa.properties) per contenere la proprietà relativa alla directory di configurazione esterna indicata nell'installer (es. "org.openspcoop2.protocol.modipa.confDirectory=/etc/govway").

3.10 Bug Fix

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2024-32007, CVE-2024-41172:
  - aggiornata libreria "org.apache.cxf:*" alla versione 3.6.4
  - aggiornata libreria "org.ow2.asm:asm" alla versione 9.7
  - aggiornata libreria "com.fasterxml.woodstox:woodstox-core" alla versione 6.6.2
- CVE-2024-34447, CVE-2024-30172, CVE-2024-30171, CVE-2024-29857:
  - aggiornata libreria "org.bouncycastle:bcprov-ext-jdk18on" alla versione 1.78.1 (migrazione verso bcprov-jdk18on)
  - aggiornata libreria "org.bouncycastle:bcpkix-jdk18on" alla versione 1.78.1
  - aggiornata libreria "org.bouncycastle:bcutil-jdk18on" alla versione 1.78.1
- CVE-2024-31573: aggiornata libreria "org.xmlunit:*" alla versione 2.10.0

- CVE-2024-22262: aggiornata libreria “org.springframework:*” alla versione 5.3.34
- CVE-2024-28752:
  - aggiornata libreria “org.apache.cxf:*” alla versione 3.6.3
  - aggiornata libreria “org.ow2.asm:asm” alla versione 9.6
  - aggiornata libreria “org.codehaus.woodstox:stax2-api” alla versione 4.2.2
  - aggiornata libreria “com.fasterxml.woodstox:woodstox-core” alla versione 6.6.0
  - aggiornata libreria “org.apache.ws.xmlschema:xmlschema-core” alla versione 2.3.1
  - aggiornata libreria “org.springframework:*” alla versione 5.3.33
- CVE-2024-22257: aggiornata libreria “org.springframework.security:*” alla versione 5.8.11
- CVE-2024-21742: aggiornata libreria “org.apache.james:apache-mime4j-*” alla versione 0.8.10
- CVE-2024-22243: aggiornata libreria “org.springframework:*” alla versione 5.3.32
- CVE-2024-25710: aggiornata libreria “org.apache.commons:commons-compress” alla versione 1.26.0
- CVE-2023-52428: aggiornata libreria “com.nimbusds:nimbus-jose-jwt” alla versione 9.37.3

Sono stati risolti i seguenti bug:

- in caso di violazione della policy di Rate Limiting con raggruppamento per Token Claim, l’evento emesso non conteneva l’informazione puntuale sul valore del claim;
- (https://github.com/link-it/govway/issues/160) utilizzando un’architettura con database distinti per configurazione e runtime si otteneva un errore non bloccante riportato nei log del database, ad esempio su postgresql: «ERROR: relation «db_info_console» does not exist at character 15 STATEMENT: select * from db_info_console order by id DESC»;
- definendo una trasformazione in cui nella configurazione dell’area di applicabilità veniva impostato «Content-Type: application/json», la trasformazione non veniva applicata se nella richiesta o nella risposta era presente un header «Content-Type» con un valore contenente altre informazioni oltre al tipo base, ad esempio: «application/json; charset=utf-8»;
- nel profilo di interoperabilità “Fatturazione Elettronica”, la disabilitazione della validazione del nome della fattura tramite la proprietà “org.openspcoop2.protocol.sdi.validazione.nomeFile.enable” causava il seguente errore bloccante se il nome della fattura era conforme a una fatturazione europea che iniziava con il codice “UB” o “II”: “Elemento [File] decodifica non riuscita: formato non conosciuto”;
- nella funzionalità di consegna asincrona, in alcuni casi limite con connettori con consegna in errore, lo stato della transazione non veniva aggiornato correttamente.

Per la console di gestione sono stati risolti i seguenti bug:

- corretta un’anomalia presente durante il salvataggio di una policy di rate limiting con criterio di raggruppamento per Token Claim “subject”: l’impostazione del criterio non consentiva di entrare nuovamente in modifica della policy e nei log si poteva riscontrare un errore simile al seguente: “Enum with value [TOKEN_ISSUER] not found”;
- è stata risolta una problematica nella gestione degli allegati di una erogazione o API, in cui il pulsante “cestino” non funzionava correttamente, impedendo la rimozione di un file una volta caricato;
- la modifica del nome di un soggetto non veniva riflessa correttamente sul nome dell’erogazione: nella denominazione del componente “porta_applicativa”, veniva erroneamente aggiunto un carattere “/” finale, causando l’impossibilità di riconoscere l’erogazione al momento della sua invocazione e generando un errore “404 NotFound” restituito al chiamante;

- è stato corretto un problema nella funzionalità di export per il profilo di interoperabilità "SPCoop" che si verificava quando veniva selezionato un soggetto multi-tenant tra quelli disponibili. Il problema si presentava durante l'export di un'API o di una fruizione che faceva riferimento a un'API il cui soggetto era differente da quello selezionato; all'interno dell'archivio zip, l'API non veniva inclusa;
- corretta anomalia presente durante l'export di una erogazione o fruizione: il plugin riferito per l'autorizzazione dei contenuti non veniva esportato;
- in presenza di regole di proxy pass, nella maschera di visualizzazione dell'URL di invocazione di una API erogata o fruita, viene ora visualizzata anche l'URL di invocazione interna.
- apportate alcune migliorie prestazionali.

Infine è stato rivisto l'algoritmo di generazione delle statistiche poiché le transazioni da inserire in un intervallo temporale potrebbero non essere ancora tutte presenti nella base dati nel caso in cui il generatore di statistiche si avvii nell'intervallo prossimo successivo (es. calcolo intervallo orario 16-17 e generatore che si avvia alle 17:00:06). Transazioni che non rientrano nel calcolo dell'intervallo potrebbero essere relative ad eventi di "readTimeout" (scritte sulla base dati dopo 120 secondi e oltre) o di lettura dello storico delle transazioni su una base dati in replica (ritardo dovuto alla sincronizzazione). Per gestire correttamente queste casistiche, è stato introdotto un parametro di tradeoff per individuare anche le transazioni che vengono registrate sulla base dati in un tempo successivo alla data di avvio del batch. Il generatore continuerà ad aggiornare i dati aggregati fino a quando la data di esecuzione del generatore non supera l'intervallo temporale corrente aumentato del tradeoff. Per default viene utilizzato un tradeoff di 5 minuti. In questo scenario, ad esempio, il generatore continuerà ad aggiornare i dati dell'intervallo 16-17 fino a quando non verrà avviato dopo le 17:05, consentendo così alle transazioni scritte dopo le 17:00 ma facenti parte dell'intervallo 16-17 di essere incluse nel dato aggregato statistico.

3.11 Bug Fix 3.3.15.p1

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2024-38808, CVE-2024-38809: aggiornata libreria "org.springframework:*" alla versione 5.3.39;
- CVE-2024-45801 aggiornata libreria "org.webjars:swagger-ui" alla versione 4.19.1.

Sono stati risolti i seguenti bug:

- (https://github.com/link-it/govway/issues/170) abilitando la validazione degli header in una Token Policy di Validazione e inserendo i valori attesi solo per i claim "typ" e "alg", si otteneva uno dei seguenti errori inattesi:
  - «JWT header validation failed; null»
  - «JWT header validation failed; Expected claim "cty" not found»
- (https://github.com/link-it/govway/issues/171) utilizzando il profilo "Fatturazione Elettronica" su Tomcat, durante la validazione di una richiesta di notifica di decorrenza termini, nei log diagnostici si manifestava la seguente anomalia:
  - «Eccezione INFO con codice [GOVWAY-5] - EccezioneValidazioneProtocollo: Traccia di una precedente fattura inviata, con identificativo SDI [xxx], non rilevata: Errore durante la ricerca del datasource…»

Inoltre sono state aggiunte utility:

- per trattare gli attributi mustUnderstand e actor attraverso gli elementi request e response accessibili tramite trasformazioni;
- è stata aggiunta un'opzione che permette di disabilitare, su singola erogazione o fruizione, il controllo della validità (scadenza) del certificato X.509 utilizzato per firmare un token; la verifica può anche essere condizionata alla presenza o meno del certificato nel truststore.

Per la console di gestione sono stati risolti i seguenti bug:

- quando si navigava in liste interne a una singola erogazione o fruizione (ad esempio, gli applicativi autorizzati nel controllo degli accessi), il passaggio alla pagina successiva veniva erroneamente mantenuto anche quando si

accedeva a una lista di un'altra erogazione o fruizione comportando una visualizzazione scorretta: nella seconda pagina potevano non esserci dati e non era più possibile tornare indietro alla pagina precedente;

- la maschera di caricamento di un certificato in un applicativo o in un soggetto è stata rivista per rendere più chiaro cosa comporta disabilitare la verifica del certificato.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- nella distribuzione statistica a 3 dimensioni, personalizzata per esito, non venivano incluse le transazioni gestite con successo;
- in caso di transazioni fallite per indisponibilità del backend, veniva erroneamente riportata una dimensione per una risposta inesistente nei dettagli del messaggio di risposta, sia quando la richiesta era diretta verso il dominio interno che verso quello esterno, nonostante nessuna risposta potesse esistere a causa del fallimento della connessione.

Infine è stata corretta una anomalia presente all'interno del tool command line "govway-vault-cli" che ne impediva il funzionamento su database oracle.

3.12 Bug Fix 3.3.15.p2

Sono state risolte le seguenti vulnerabilità relative alle librerie di terza parte:

- CVE-2024-38821: aggiornate librerie "org.springframework.security:*" alla versione 5.8.15
- CVE-2024-38820: aggiornate librerie "org.springframework:*" alla versione 5.3.39-gov4j-1
- CVE-2024-47554:
  - aggiornata libreria "commons-io:commons-io" alla versione 2.15.1
  - aggiornata libreria "org.apache.velocity:velocity-engine-core" alla versione 2.4

  CVE-2024-45772: aggiornate librerie "org.apache.lucene:*" alla versione 9.12.0.

Sono stati risolti i seguenti bug:

- Quando si definivano erogazioni o fruizioni con gruppi di configurazioni specifiche per operazioni, eventuali modifiche alla configurazione CORS venivano applicate solo alle operazioni del gruppo predefinito. Di conseguenza, per le operazioni degli altri gruppi, continuava ad essere utilizzata la configurazione CORS di default.
- La validazione dei contenuti, successiva alla verifica di una firma WSSecurity, falliva se l'elemento da validare conteneva elementi tipizzati tramite «xsi:type» e la dichiarazione dei namespace dei prefissi associati era presente nell'elemento Envelope della busta SOAP. L'errore riscontrato era simile al seguente: «UndeclaredPrefix: Cannot resolve "test:EsempioType" as a QName: the prefix "test" is not declared.».
- La validazione di un certificato di firma utilizzato in un header WSSecurity, inclusa l'analisi delle CRL, veniva eseguita su tutti i certificati della catena, compresi quelli intermedi, anche se era stato fornito solo il file CRL relativo al certificato finale. Di conseguenza, durante la validazione di un certificato intermedio, compariva l'errore: «No CRLs found for issuer "cn=ExampleCA,ou=TEST,o=Example,c=IT"». Per risolvere il problema, era necessario fornire un file CRL per ogni certificato, inclusi quelli intermedi. Per evitare questa configurazione complessa e prevenire il fallimento della validazione quando viene fornito un solo file CRL, la configurazione predefinita ora presume che il file CRL sia relativo solo al certificato finale e non viene utilizzato per validare i certificati intermedi.

Inoltre sono state aggiunte utility:

- per la gestione dell'ora legale e solare, utilizzate nella funzionalità di riconsegna con presenza in carico dei messaggi.

Per la console di gestione sono stati risolti i seguenti bug:

- la pagina iniziale che consente di effettuare il login nella console (es. http://127.0.0.1:8080/govwayConsole/) restituiva un codice di risposta HTTP 500 invece di 200;
- nella configurazione di un'API ModI con pattern INTEGRITY_REST, la scelta dell'header HTTP «Custom-JWT-Signature» comporta che la gestione dell'integrità non venga eseguita in modo integrato, ma sia demandata all'applicazione. A causa di questo comportamento, la maschera di configurazione non era del tutto intuitiva e poteva far pensare che si stesse solo modificando il nome dell'header HTTP, mentre in realtà cambiava anche la modalità di gestione dell'integrità. È stata quindi aggiunta una nota esplicativa per chiarire meglio il funzionamento.

4 Versione 3.3.14

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.14 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

4.1 Miglioramenti al Profilo di Interoperabilità "ModI"

Sono stati apportati i seguenti miglioramenti alla gestione dei pattern "AUDIT_REST_01" e "AUDIT_REST_02":

- aggiunta la possibilità di definire dei criteri di validazioni sui claim attesi all'interno del token di audit; i criteri associabili ad ogni specifico claim sono:
  - una lista di valori ammessi;
  - una validazione tramite espressione regolare;
  - indicazione della lunghezza minima e/o massima di caratteri;
- nella definizione delle informazioni personalizzate da includere nel token di AUDIT è adesso possibile indicare per ogni singolo claim se l'informazione veicolata sia riutilizzabile o meno su differenti chiamate; l'intero token di audit verrà salvato in cache e riutilizzato su differenti chiamate solo se tutti i claim inseriti all'interno del token risultano configurati come riutilizzabili;
- attivando una configurazione opzionale per il token di audit, l'impostazione veniva ignorata e il token veniva obbligatoriamente richiesto; l'anomalia è stata risolta.

Sono stati apportati i seguenti miglioramenti alla funzionalità di integrazione con la PDND:

- è stato rivisto il concetto di richiedente di una richiesta di servizio al fine di considerare anche il nome dell'organizzazione recuperata tramite le API PDND, in modo da visualizzarla al posto del clientId durante la consultazione dello storico delle transazioni;
- sono stati introdotti i seguenti miglioramenti alla console e alle API di monitoraggio per utilizzare i dati individuati tramite le API PDND:
  - nello storico delle transazioni è adesso possibile effettuare una ricerca per nome dell'organizzazione individuata;
  - i dati dei report statistici possono essere filtrati per nome dell'organizzazione;
  - è possibile adesso ottenere una distribuzione per clientId contenente anche le informazioni recuperate tramite le API PDND (nome organizzazione, external-id, categoria);
- tramite la console di gestione è adesso possibile verificare o eliminare i dati presenti nella cache locale contenente le chiavi pubbliche (JWK) e le informazioni sui client raccolte tramite le API PDND;
- nella configurazione che consente l'invocazione delle API PDND è adesso possibile:
  - produrre header o parametri della url personalizzati da inoltrare verso la fruizione delle API;
  - disattivare l'invio di credenziali basic;

  - personalizzare le chiamate per tenant in una installazione multi-tenant.

Sono infine stati apportati i seguenti miglioramenti:

- aggiunto supporto per uno scenario di fruizione ModI in cui sia necessario utilizzare il materiale crittografico definito nella token policy per firmare i token di AUDIT e di INTEGRITY;
- la validazione dei token "ModI" non supportava token contenenti claim "aud" definiti come stringhe di array; è stato aggiunto il supporto in modo da rispettare entrambe le modalità (array of case-sensitive strings or single case-sensitive string) indicate nel RFC "https://datatracker.ietf.org/doc/html/rfc7519.html#section-4.1.3";
- la produzione e la validazione dell'header di integrità "Custom-JWT-Signature" è adesso attivabile anche per metodi senza payload.

4.2 Miglioramenti alla funzionalità di Tracciamento

Sono stati apportati i seguenti miglioramenti:

- anche per le richieste contenenti credenziali non valide, token scaduti o non autorizzati vengono adesso registrate:
  - le informazioni sui claim principali presenti nel token (clientId, subject/issuer, username, eMail);
  - le informazioni recuperate tramite le API PDND (es. nome e categoria dell'organizzazione);
  - l'identificativo autenticato a livello trasporto (principal);
- sono stati aggiunti nuovi esiti per le transazioni:
  - "Read Timeout": risposta non ricevuta entro il timeout specificato;
  - "Request Read Timeout": richiesta non ricevuta entro il timeout specificato;
  - "Connection Timeout": connessione non stabilita entro il timeout specificato;
  - "Negoziazione Token Fallita": indica degli errori emersi durante la negoziazione del token;
- le classi di appartenenza degli esiti sono state riviste al fine di includere il nuovo esito "Request Read Timeout" e l'esito "Connessione Client Interrotta" in una nuova classe "Errore Client Indisponibile";
- i nuovi esiti relativi a timeout concorrono alla generazione di eventi che consentono all'operatore di indivuare l'occorrenza di errori di timeout senza dove effettuare ricerche puntuali nello storico delle transazioni;
- le informazioni raccolte tramite le API PDND sono state aggiunte alla base dati di tracciamento in modo da consentirne l'estrazione tramite viste personalizzate;
- nella funzionalità "fileTrace" è adesso possibile accedere alle seguenti informazioni ModI:
  - informazioni del token ModI di audit "Agid-JWT-TrackingEvidence";
  - informazioni recuperate tramite le API PDND.

4.3 Miglioramenti alla funzionalità di Correlazione Applicativa

Sono state modificate le seguenti logiche di gestione.

- Una richiesta non intercettata da nessuna regola di correlazione applicativa, fino alla versione 3.3.13.p1, terminava con l'errore:

  «Identificativo di correlazione applicativa non identificato; nessun elemento tra quelli di correlazione definiti è presente nel body».

  È stato modificato il default in modo da accettare la richiesta. Il precedente comportamento è ripristinabile agendo sulle proprietà della singola fruizione o erogazione di API.

- Una correlazione applicativa configurata con una modalità d'identificazione basata su header HTTP e un comportamento in caso di identificazione fallita uguale al valore "accetta", provocava la terminazione con errore della transazione se la richiesta non presentava l'header HTTP configurato. L'errore riportato era il seguente:

  «Identificativo di correlazione applicativa non identificato; nessun elemento tra quelli di correlazione definiti è presente nel body».

  L'anomalia si presentava anche per altre modalità di identificazione nel caso in cui l'identificativo estratto risultasse null o una stringa vuota. È stato modificato il comportamento di default del gateway in modo da considerare entrambi i casi come una estrazione di correlazione applicativa fallita. Il precedente comportamento di accettare identificativi null o stringhe vuote è ripristinabile agendo sulle proprietà della singola fruizione o erogazione di API.

4.4 Miglioramenti alla funzionalità di Gestione dei Token

In una token policy di validazione, per un token JWS è adesso possibile aggiungere criteri di validazione dei "typ", "cty" e "alg" presenti nell'header.

È inoltre stata differenziata la cache che conserva i dati recuperati dalle Attribute Authority rispetto alla cache che conserva i token.

4.5 Miglioramenti alla funzionalità di Sicurezza Messaggio

Viene adesso consentito l'utilizzo di valori dinamici anche sul flusso di risposta per quanto concerne la funzionalità di sicurezza messaggio.

Inoltre per la funzionalità "WS-Security Username Token" è adesso possibile definire una mappa di credenziali attese.

4.6 Miglioramenti alla Console di Gestione

Su ogni oggetto del registro è adesso possibile indicare una descrizione contenente fino a 4000 caratteri.

Inoltre sono adesso consultabili le informazioni su chi e quando ha creato o modificato un oggetto tramite la nuova voce "Proprietà" utilizzabile tramite il menù «tre puntini» presente sia nell'elenco che nel dettaglio di un oggetto.

Infine sono state riviste le schede di visualizzazione dei dettagli di una API, di una erogazione o fruizione e di un gruppo di configurazioni per i seguenti aspetti:

- la descrizione viene visualizzata solo se definita ed è possibile aggiungerla tramite un'azione dedicata presente tra le informazioni sul nome dell'oggetto;
- vengono visualizzate le informazioni riguardanti la data di creazione, la data di ultima modifica e gli utenti che hanno effettuato tali operazioni.

4.7 Miglioramenti alla Console e alle API di Monitoraggio

Sono stati apportati i seguenti miglioramenti alle funzionalità di reportistica:

- nella funzionalità «Configurazione API» è adesso possibile esportare il report oltre che nel formato "csv" anche nel formato "xls";
- nella funzionalità «Analisi Statistica» è adesso possibile produrre anche una distribuzione statistica in 3 dimensioni: criterio di distribuzione, data e valore.

4.8 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- aggiunti script di svecchiamento delle tracce per tipo di database sqlserver;

- eliminata la generazione dell'archivio "govwaySec" prodotto per default tra gli archivi generati per l'application server WildFly; l'archivio è comunque generabile abilitando l'opzione specifica disponibile in modalità avanzata;
- gli artefatti prodotti dall'installer in caso di scelta del profilo di interoperabiltà "eDelivery" presentavano i seguenti errori:
  - nell'archivio govway.ear mancava il jar "openspcoop2_as4-protocol_ecodexBackendStub_cxf.jar";
  - il datasource per wildfly "domibus-ds.xml" non conteneva il nome jndi "org.govway.datasource.domibus" atteso.

4.9 Bug Fix

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2023-51074: aggiornata libreria "com.jayway.jsonpath:json-path" alla versione 2.9.0;
- CVE-2023-45860: aggiornata libreria "com.hazelcast:hazelcast" alla versione 5.3.5;
- CVE-2023-44483: aggiornata libreria "org.apache.santuario:xmlsec" alla versione 2.3.4;
- CVE-2023-5072: aggiornata libreria "org.json:json" alla versione 20231013;
- CVE-2023-4586: aggiornata libreria "io.netty:*" alla versione 4.1.100.Final, libreria "org.redisson:redisson" alla versione 3.23.5 e libreria "org.jboss.marshalling:*" alla versione 2.1.3.SP1
- CVE-2023-34042: aggiornata libreria "org.springframework.security:*" alla versione 5.8.7;
- CVE-2023-4759: aggiornata libreria "org.eclipse.jgit:org.eclipse.jgit" alla versione 6.7.0.202309050840-r;
- CVE-2023-40167: aggiornata libreria "org.eclipse.jetty:*" alla versione 10.0.16.

Sono stati risolti i seguenti bug:

- le richieste contenenti metodi http "PATCH", "LINK" e "UNLINK" venivano inoltrate al backend erroneamente come metodo POST se la connessione era https;
- non venivano utilizzati i tempi di connection e read timeout impostati a livello globale; l'anomalia è stata risolta e nell'occasione sono stati rivisti i tempi di default utilizzati a livello globale per una nuova installazione:
  - connection timeout: modificato da 10 a 5 secondi;
  - read timeout sulle erogazioni: modificato da 120 a 60 secondi;
  - read timeout sulle fruizioni: modificato da 150 a 65 secondi.
- risolta anomalia che si verificava in alcuni casi limite durante il tracciamento delle fruizioni di API con negoziazione token; l'errore segnalato nei log era: «PostOutResponseHandler [transazioni]Errore durante la scrittura della transazione sul database (Lettura dati Transazione): Caused by: java.util.ConcurrentModificationException … at org.openspcoop2.pdd.core.token.TokenUtilities.replaceTokenInMap(TokenUtilities.java)».

Sono stati risolti i seguenti bug relativi al profilo di interoperabilità «ModI»:

- in una fruizione ModI di una API definita tramite i pattern "ID_AUTH_REST via PDND" e "AUDIT_REST_01", se la fruizione risultava configurata per utilizzare un keystore definito nell'applicativo e quest'ultimo non veniva identificato durante la gestione della richiesta, GovWay emetteva un diagnostico malformato: «Il profilo di sicurezza richiesto "null" richiede l'identificazione di un applicativo»;
- in un contesto in cui risultava già attiva una erogazione definita senza pattern di sicurezza messaggio o con un pattern con generazione token "Authorization ModI", se veniva modificata l'API per utilizzare un pattern con token "Authorization PDND", la sezione controllo degli accessi dell'erogazione non consentiva di abilitare la token policy di validazione dei voucher PDND;

- la creazione di una erogazione di API con pattern di sicurezza canale “ID_AUTH_CHANNEL_02” veniva effettuata definendo un controllo accessi non corretto poichè l’autenticazione canale veniva configurata come opzionale;
- in un API definita con un pattern di sicurezza messaggio con generazione token “Authorization ModI” e con voce “Header HTTP del Token” impostata a “Custom-JWT-Signature”, se veniva modificata la voce di generazione token in “Authorization PDND” rimanevano inconsistenti le successive voci che consentono la configurazione dell’header custom;
- la verifica dei keystore/truststore di una fruizione o erogazione, da utilizzare per i token di risposta, viene adesso effettuata solamente se l’API prevede un token di sicurezza nella risposta;
- una fruizione ModI di una API definita con pattern “ID_AUTH_REST” e “Generazione Token via PDND” presentava le seguenti anomalie:
  - la verifica dei certificati non veniva effettuata: la console indicava che tutti i certificati erano validi anche quando non lo erano;
  - la configurazione fornita dalla funzionalità “Visualizza dettagli della configurazione”, presente nelle opzioni della fruizione, non visualizzava le informazioni corrette su eventuali keystore definiti nella fruizione stessa;
  - nel caso fosse configurata una API senza pattern di sicurezza messaggio e successivamente questa fosse stata modificata impostando il pattern “ID_AUTH_REST_01” e “Generazione Token” via PDND, entrando nella maschera di configurazione del connettore della fruizione si otteneva una informazione errata sulla token policy che risultava assegnata anche se in realtà non lo era;
- durante la registrazione di un applicativo con profilo di interoperabilità “ModI”, se nella sezione “ModI - Sicurezza Messaggio - KeyStore” veniva effettuato con modalità “Archivio” l’upload di un keystore pkcs12, creato importando un altro archivio pkcs12 al suo interno, si otteneva l’errore: «keystore password was incorrect». Si trattava dello stesso bug risolto nell’issue “https://github.com/link-it/govway/issues/128” la cui risoluzione non era stata riportata nella maschera di gestione della sicurezza ModI di un applicativo.

Per la console di gestione sono stati risolti i seguenti bug:

- durante la visualizzazione di una pagina, il componente «loading», che inibisce l’utilizzo della pagina stessa, terminava la sua funzione prima che il caricamento della pagina fosse completato;
- la creazione di una API tramite caricamento di un’interfaccia OpenAPI contenente la definizione di un parametro di tipo “header” falliva e dai log si poteva riscontrare il seguente errore: «Trovato parametro header “Authorization” senza tipo»;
- se veniva effettuata una configurazione dei nodi in cluster suddivisi per gruppi, l’operazione «Svuota le Cache dei nodi “<nomeGruppo>”» veniva ripetuta erroneamente più volte per ogni nodo;
- su una erogazione configurata per gestire gruppi di risorse differenti, in cui per ogni gruppo fosse ridefinito il connettore e attivata la consegna condizionale, il passaggio in visualizzazione tra gruppi diversi poteva mostrare dati dei connettori errati.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- la visualizzazione dei contenuti delle richieste e delle risposte su database SQLServer falliva se la dimensione dei messaggi era superiore a “250Kb”.

Per le API di monitoraggio sono stati risolti i seguenti bug:

- la distribuzione temporale non consentiva di ottenere report contenenti informazioni sull’occupazione della banda e sul tempo medio di risposta dei servizi;
- tra le informazioni restituite per un evento non era presente la sua descrizione.

5 Versione 3.3.13

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.13 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.13 utilizzare l'ultima patch version che risolve bug importanti descritti nella sezione:

- *Bug Fix 3.3.13.p1*

5.1 Miglioramenti al Profilo di Interoperabilità "ModI"

Il profilo di interoperabilità "ModI" è stato adeguato agli aggiornamenti AGID sulle Linee Guida di Interoperabilità indicati nella determina n.128 del 23 maggio 2023.

Sono ora supportati anche i seguenti nuovi pattern di sicurezza:

- "INTEGRITY_REST_02"
- "AUDIT_REST_01"
- "AUDIT_REST_02"

L'insieme dei claim da includere nel JWT di Audit "Agid-JWT-TrackingEvidence" è configurabile consentendo di definire insiemi differenti da associare alle API.

La validazione dei token di tipo AUDIT o INTEGRITY ricevuti può essere effettuata anche utilizzando una validazione "PDND" configurata per prelevare la chiave pubblica del mittente tramite le API di interoperabilità esposte dalla PDND. La chiave viene poi memorizzata in una cache locale e mantenuta aggiornata tramite gli eventi, emessi dalla PDND, relativi alle chiavi prelevate.

Sono inoltre stati apportati i seguenti miglioramenti:

- è stata rivista la definizione del pattern di sicurezza nella API al fine di indicare chi genera il token ID_AUTH tra il mittente e la PDND;
- aggiunta possibilità di arricchire la traccia di informazioni relative al client-id presente nel token "ID_AUTH" attraverso informazioni prelevate utilizzando le API della PDND;
- nella personalizzazione dei keystore è adesso possibile utilizzare una chiave privata, protetta da password o meno, nei formati pkcs1 o pkcs8 in codifica PEM o DER;
- aggiunta possibilità di utilizzare un keystore JWK sia come keystore che come truststore;
- migliorata diagnostica emessa in presenza di una richiesta con pattern "INTEGRITY_REST" che presenta l'header digest e un payload http vuoto. L'errore che veniva segnalato nel diagnostico era fuorviante poichè indicava: «Header HTTP "digest", dichiarato tra gli header firmati, non trovato». Adesso invece l'errore riportato è il seguente: «Header HTTP "Digest" presente in una risposta con http payload vuoto».
- risolto bug di verifica audience; l'anomalia avveniva in presenza di erogazioni configurate con un valore di audience di default e operazioni suddivise in gruppi di configurazione differente. Per le operazioni associate a gruppi di configurazione diverse da quello predefinito la verifica dell'audience falliva erroneamente.

5.2 Miglioramenti alla gestione degli archivi delle chiavi

Nelle Token Policy sia di validazione che di negoziazione e negli Attribute Authority è stato aggiunto il supporto per i seguenti archivi:

- "Key Pair": chiave pubblica e privata, protetta da password o meno, nei formati pkcs1 o pkcs8 in codifica PEM o DER;

- “Public Key”: chiave pubblica in codifica PEM o DER;
- “JWK Set”: l’archivio è adesso utilizzabile in tutti i contesti in cui è definibile un keystore o un truststore.

La funzionalità “Verifica Certificati” è stata migliorata al fine di:

- supportare i nuovi tipi di archivio;
- aggiungere la verifica di accesso alla chiave privata tramite la password fornita per i tipi di archivio già esistenti (JKS, PKCS12, . . .).

5.3 Miglioramenti alla funzionalità di Autenticazione

Il gestore delle credenziali, utilizzabile per l’autenticazione dei certificati client ottenuti tramite header HTTP, supporta adesso anche la decodifica HEX. È stata inoltre aggiunta la possibilità di decodificare i certificati ricevuti in qualsiasi modalità supportata, prima provando la decodifica “urlEncoded”, in caso di fallimento la decodifica “base64” e infine la decodifica “hex”.

5.4 Miglioramenti alla funzionalità di Registrazione dei Messaggi

È adesso possibile definire “white-list” o “black-list” per gli header HTTP da registrare sia a livello di singola erogazione o fruizione tramite le proprietà, sia a livello globale nel file govway_local.properties.

La funzionalità consente di specificare le liste sia sui singoli flussi (richiesta-ingresso, richiesta-uscita, risposta-ingresso, risposta-uscita) sia differenziando tra erogazione e fruizione.

5.5 Miglioramenti all’Installer

Sono stati apportati i seguenti miglioramenti all’installer binario:

- aggiunti script di svecchiamento delle tracce per tipo di database postgresql e oracle;
- l’esecuzione in modalità testuale (“./install.sh text”) rimaneva bloccata in caso di tipologia d’installazione “Aggiornamento” durante la selezione della “Versione Precedente”.

Inoltre la modalità «gestione dei nodi dinamica», indicata per le installazioni in cloud e selezionabile con una installazione in modalità avanzata, è stata modificata per rendere utilizzabile la soluzione anche in architetture cloud dove i nodi runtime (pod) non risultano invocabili tra di loro.

5.6 Nomenclatura

Il nome di un soggetto, escluso che per il profilo di interoperabilità SPCoop, può adesso essere definito anche tramite il carattere “-“.

5.7 Bug Fix

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2023-33201: aggiornata libreria “org.bouncycastle:*” alla versione 1.74;
- CVE-2023-34411: aggiornata libreria “com.fasterxml.woodstox:woodstox-core” alla versione 6.5.1, “org.apache.cxf:*” alla versione 3.6.1 e “org.ow2.asm:asm” alla versione 9.5;
- CVE-2020-8908: aggiornata libreria “com.google.guava:guava” alla versione 32.0.0-jre;
- CVE-2023-33264: aggiornata libreria “com.hazelcast:hazelcast” alla versione 5.3.0;
- CVE-2023-20862: aggiornata libreria “org.springframework.security:spring-security-*” alla versione 5.8;
- CVE-2017-9096, CVE-2022-24196 e CVE-2022-24197: sostituita libreria “com.lowagie:itext” versione 2.1.7.js7 con le librerie “org.apache.pdfbox:*” versione 2.0.27 e “com.github.dhorions:boxable” versione 1.7.0.

Sono stati risolti i seguenti bug:

- (https://github.com/link-it/govway/issues/133) tentando di avviare la piattaforma GovWay sotto Windows si otteneva un errore causato dal mancato supporto agli attributi posix: «java.lang.UnsupportedOperationException: "posix:permissions" not supported as initial attribute»;
- (https://github.com/link-it/govway/issues/128) l'accesso ad un keystore pkcs12 creato importando un archivio pkcs12 al suo interno falliva con il seguente errore: «keystore password was incorrect»;
- su database SQLServer veniva segnalato il seguente errore dovuto ad una colonna definita in minuscolo e riferita nella query in maiuscolo: «ERROR .... [GestoreCorrelazioneApplicativa.getCorrelazioniStoriche] errore, queryString[SELECT TOP 50 id,SCADENZA FROM CORRELAZIONE_APPLICATIVA WHERE (ORA_REGISTRAZIONE < ?)]: Invalid column name "ORA_REGISTRAZIONE".»;
- nella configurazione di default, su API SOAP, il riconoscimento dell'operazione avviene comparando il path indicato dopo la base-url rispetto alle operazioni della API. Il riconoscimento dell'operazione basata sulla url non funzionava correttamente in presenza di una url formata da molteplici endpoint come ad esempio: «http://host/govway/ente/service/v1/azione1,http://host/govway/ente/service/v1/azione3». L'operazione che veniva erroneamente individuata era "azione3". La problematica risiedeva nell'espressione regolare generata per default dalla console di configurazione e associata alla funzionalità di identificazione dell'operazione, nell'esempio:
  - .*/(?:gw_)?ente/(?:gw_)?service/v1/([^/|^?]*).*

  L'espressione è stata corretta in:
  - /(?:gw_)?ente/(?:gw_)?service/v1/([^/?]*).*

Per la console di gestione sono stati risolti i seguenti bug:

- l'apertura di un nuovo tab tramite le breadcump rendeva la console inutilizzabile sul nuovo tab. Per provocare l'anomalia si doveva procedere come segue:
  - aprire una lista di api, erogazioni, fruizioni, soggetti o applicativi;
  - entrare nel dettaglio di un oggetto;
  - cliccare con il tasto destro sulla breadcump che indica l'elenco degli oggetti ed aprire un nuovo tab;
  - spostarsi sul nuovo tab;
  - entrare nel dettaglio di un oggetto qualsiasi: la console andava in errore.
- la maschera di creazione di un soggetto con profilo di interoperabiltà "API Gateway" o "ModI" consente adesso di crearlo con una tipologia "Fruitore" senza dover obbligatoriamente fornire delle credenziali; lo scenario serve a definire il soggetto che verrà poi associato all'applicativo fruitore che possiede le credenziali.

5.8 Bug Fix 3.3.13.p1

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2023-2976: aggiornata libreria "com.google.guava:guava" alla versione 32.1.1-jre;
- CVE-2023-34034: aggiornata libreria "org.springframework.security:*" alla versione 5.8.5;
- CVE-2023-34462: aggiornata libreria "io.netty:*" alla versione 4.1.94.Final.

Sono stati risolti i seguenti bug:

- corrette le seguenti anomalie relative al profilo di interoperabilità "ModI":
  - risultavano le stesse informazioni sulle organizzazioni prelevate dalla PDND relativamente a chiamate (clientId) differenti;

  - dopo un upgrade all'ultima versione 3.3.13 si otteneva l'errore «[GOVWAY-6] - EccezioneProcessamento: per abilitare la proprietà è richiesto che sia abilitata la gestione delle chiavi PDND» se il file di proprietà esterno "govway_local.properties" non veniva aggiornato con le differenze introdotte nell'ultima versione riguardanti la gestione delle chiavi "PDND". La problematica è stata risolta in modo che l'errore non avvenga anche se non vengono aggiornati i file locali;

- nel profilo di interoperabilità "SPCoop" è stato rivisto l'utilizzo dell'identificativo numerico del nodo in modo da utilizzare il «padding» corretto in presenza di 2 cifre;
- utilizzando la configurazione di Apache suggerita per inoltrare il certificato TLS ("RequestHeader set SSL_CLIENT_CERT «%{SSL_CLIENT_CERT}s» «expr=-n %{SSL_CLIENT_CERT}»") avviene un inoltro dell'header in una formato che non veniva supportato da GovWay: PEM su una unica linea dove i ritorni a capo venivano sostituiti da spazi. È stato aggiunto il supporto.

Sono state corrette alcune anomalie riguardanti la consegna asincrona:

- i messaggi serializzati su database contenevano informazioni «inconsistenti» se utilizzati dopo un upgrade di versione di GovWay. In particolar modo l'identificativo di protocollo (trasparente, modi, spcoop...) non veniva risolto correttamente causando una mancata registrazione della diagnostica, dei messaggi e dei dati relativi alla consegna asincrona (nella transazione) per le nuove consegne effettuate con la versione del software aggiornata;
- l'informazione di contesto sul nome della porta invocata non era presente in un messaggio trasformato e causava un errore simile al seguente: «Errore avvenuto durante la consegna HTTP: Errore durante la raccolta delle informazioni necessarie alla funzione di proxy pass reverse: [getPortaApplicativa]: Parametro non definito (idPA.getNome() is null)».

Per la console di gestione sono stati risolti i seguenti bug:

- modificando la configurazione di una fruizione o di una erogazione (es. sicurezza messaggio) era necessario effettuare due volte l'operazione "Rimuovi dalla Cache" per far sì che la modifica venisse effettivamente vista dal runtime;
- in un ambiente multi-tenant la creazione di un applicativo con credenziali api-key, dove il soggetto di dominio interno non veniva selezionato attraverso le voci in alto a destra nella console ma utilizzando la select list presente nella form di creazione, non funzionava correttamente poichè le credenziali generate venivano assegnate al soggetto presente inizialmente nella maschera di creazione e non al soggetto successivamente selezionato;
- se su una API REST venivano caricati schemi XSD, il download della "XSD Schema Collection" produceva l'errore: «Content is not allowed in prolog.»;
- nella maschera di resoconto dei dati di una trasformazione della richiesta, dopo aver effettuato una operazione di salvataggio, i link sugli header http e/o sui parametri della url non riportavano il numero corretto di header/parametri precedentemente configurati e veniva sempre indicato il valore "0";
- corretti alcuni errori che procuravano il fallimento dell'importazione di configurazione tramite "wizard".

Per le API di monitoraggio sono stati risolti i seguenti bug:

- nel dettaglio di una transazione veniva restituito un elemento vuoto "informazioni_token:{}" nel caso in cui la gestione della richiesta non prevedesse un token; se non valorizzato adesso l'elemento non viene prodotto.

6 Versione 3.3.12

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.12 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

6.1 Miglioramenti alla funzionalità di Validazione Token

In una token policy di validazione è adesso possibile definire una validazione JWT che identifica il certificato all'interno del truststore, da utilizzare per la validazione, attraverso il "kid" presente nell'header del token.

6.2 Miglioramenti alla funzionalità dei Connettori

È adesso possibile configurare GovWay per utilizzare una configurazione https differente da quella ereditata dalla jvm, oltre che tramite la configurazione specifica di un connettore https, attraverso un repository di configurazioni definite tramite file di proprietà.

Il nome e la posizione del file di proprietà è configurabile a livello di singola API.

Il nome del file indicato può contenere delle macro, risolte a runtime dal gateway, per creare dei path dinamici (es. un keystore differente per ogni applicativo).

6.3 Miglioramenti alla funzionalità di Trasformazione

Tra le informazioni dinamiche utilizzabili all'interno di trasformazioni è adesso possibile riferire anche l'identificativo di correlazione applicativa.

Nelle consegna di una notifica asincrona, attivando una trasformazione, è adesso possibile accedere oltre che alla richiesta e alla risposta della transazione sincrona anche al contesto di tale transazione. È stata inoltre risolta un'anomalia che provocava la mancata esecuzione di una trasformazione se, tra i criteri di applicabilità, veniva utilizzato il connettore associato all'implementazione dell'API.

6.4 Bug Fix

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2023-20863: aggiornata libreria "org.springframework:spring-expression" alla versione 5.3.27
- CVE-2023-1436: aggiornata libreria "org.codehaus.jettison:jettison" alla versione 1.5.4
- CVE-2023-1370: aggiornata libreria "net.minidev:json-smart" alla versione 2.4.10
- CVE-2023-20861: aggiornata libreria "org.springframework:spring-*" alla versione 5.3.26
- CVE-2022-42003: aggiornata libreria "com.fasterxml.jackson.core:jackson-databind" alla versione 2.14.2

Per la console di gestione sono stati risolti i seguenti bug:

- l'accesso alle maschere di configurazione delle proprietà di sistema, delle regole di proxy pass, delle regole di response caching e dei canali produceva un errore inatteso;
- durante l'aggiornamento dell'interfaccia OpenAPI o WSDL di una API, se l'utente decideva di annullare l'aggiornamento la console andava in errore e nel log veniva riportato un errore simile al seguente: "Parametro [_csrf] Duplicato";
- caricando un'interfaccia OpenAPI 3 contenente una descrizione del corpo della richiesta, di una risposta o di un parametro superiore ai 255 caratteri si otteneva un errore inatteso sulla console;
- la verifica dei certificati, su erogazioni/fruizioni ModI, andava in errore se veniva impostata una OCSP Policy.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- i tempi medi di risposta riportati nei report statistici non venivano correttamente calcolati in presenza di campionamenti statistici che presentavano variazioni di risultati importanti tra un campionamento ed un altro come ad esempio in presenza di richieste terminate correttamente e richieste terminate con un "read timeout" (2 minuti).

7 Versione 3.3.11

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.11 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

7.1 Miglioramenti al Profilo di Interoperabilità "ModI"

Sono stati apportati i seguenti miglioramenti:

- viene adesso supportato una nuova modalità di fruizione ModI in cui il keystore utilizzato per la firma viene associato direttamente alla fruizione, in alternativa alla modalità già esistente in cui il keystore viene associato all'applicativo mittente;
- aggiunta la possibilità di definire una token policy di negoziazione in cui i dati relativi al keystore, al KID e al clientId possono essere configurati nelle fruizioni con connettore che utilizza token policy con tali caratteristiche;
- rivista la label "Contemporaneità Token Authorization e Agid-JWT-Signature" in "Coesistenza Token Authorization e Agid-JWT-Signature";
- aggiunta la possibilità di registrare nelle fruizioni proprietà relative ad uno specifico applicativo mittente. La funzionalità è utilizzabile per configurare in una fruizione purposeId differenti per ogni applicativo mittente. Analogamente è ora possibile registrare proprietà diverse per ogni applicativo rispetto all'api invocata.

7.2 Miglioramenti alla funzionalità di Negoziazione Token

In una token policy di negoziazione è adesso possibile personalizzare i seguenti parametri della chiamata verso l'authorization server:

- metodo http;
- eventuale content-type e payload;
- aggiunta di header http;
- definire credenziali http-basic, http-bearer e l'invio di un certificato tls client;
- personalizzazione del parsing della risposta.

Inoltre anche nelle modalità di negoziazione standard già esistenti è stata aggiunta la possibilità di aggiungere header http personalizzati nella richiesta.

Infine è stato migliorato il tooltip visualizzato sul connettore di una erogazione in modo da visualizzare l'eventuale token policy associata.

7.3 Miglioramenti alla funzionalità di Tracciamento

La traccia prodotta da GovWay è stata arricchita:

- delle date di acquisizione completata degli stream in ingresso e di completamento della spedizione dei messaggi in uscita;
- del token ricevuto in caso di validazione fallita;
- delle informazioni inviate e della risposta ricevuta in caso di negoziazione token fallita.

La diagnostica è stata arricchita al fine di individuare:

- negoziazione di un token;
- registrazione dei messaggi.

Le informazioni sui messaggi di richiesta e di risposta visualizzate nel dettaglio di una transazione, tramite la console "govwayMonitor", sono state riorganizzate per una migliore comprensione.

La latenza totale di una transazione viene adesso calcolata in base al momento in cui la spedizione dei messaggi in uscita verso il client sia stata completata.

Il termine "latenza servizio" è stato rinominato in "tempo di risposta servizio" in tutti i report statistici.

7.4 Miglioramenti alla Console di Gestione

Sono stati apportati i seguenti miglioramenti alla console di gestione:

- è adesso possibile effettuare ricerche di erogazioni e fruizioni rispetto allo stato della configurazione relativa alle seguenti funzionalità:
  - stato dell'API;
  - autenticazione token;
  - autenticazione trasporto;
  - rate limiting;
  - validazione;
  - response caching;
  - trasformazioni;
  - correlazione applicativa;
  - sicurezza messaggio;
  - gestione mtom;
  - registrazione dei messaggi;
  - gestione CORS;
- per i soggetti e per gli applicativi è stata aggiunta la possibilità di effettuare ricerche rispetto all'Issuer del certificato associato;
- aggiunta la possibilità di registrare le classi dei plugin che implementano funzionalità personalizzabili relative al parsing delle risposte in una Token Policy di validazione o negoziazione e in una Attribute Authority.

7.5 Bug Fix

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2022-45688: aggiornata libreria "org.json:json" alla versione 20230227;
- CVE-2023-24998: aggiornata libreria "commons-fileupload" alla versione 1.5 .

Sono stati risolti i seguenti bug:

- l'autorizzazione puntuale in una erogazione con profilo di interoperabilità "ModI" non veniva effettuata se la lista degli applicativi autorizzati veniva lasciata vuota;
- le regole di autorizzazione definite nell'autorizzazione dei contenuti o nell'autorizzazione per token claims non venivano controllate nell'ordine in cui erano state configurate;
- la validazione di un token che presentava date (exp,iat,nbf) serializzate in un formato numerico esponenziale falliva generando un errore simile al seguente: "Token non valido: For input string: «1.67»"

Per la console di gestione sono stati risolti i seguenti bug:

- il controllo dei certificati di una token policy di negoziazione andava in errore quando la modalità scelta era "Definito nell'applicativo ModI";
- non era più possibile creare una token policy in caso di servizi OCSP disabilitati (file ocsp.properties non presente o nessuna policy definita al suo interno);
- sono stati corretti i seguenti problemi relativi alla configurazione dell'autorizzazione per contenuti:
  - se nelle regole erano presenti commenti (#) potevano presentarsi segnalazioni errate dovuti a "commenti duplicati" quando la linea inserita era la stessa in due o più righe;
  - in alcuni casi l'ordine di inserimento delle regole non veniva preservato in fase di salvataggio;
  - non venivano gestite correttamente più entry con la stessa chiave (la stessa problematica è stata risolta anche nella configurazione dell'autorizzazione per token claims).

Per la console di monitoraggio sono stati risolti i seguenti bug:

- risolta problematica che non consentiva di visualizzare la scheda dei messaggi duplicati nel dettaglio di una transazione.

8 Versione 3.3.10

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.10 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

8.1 Miglioramenti alle funzionalità di Sicurezza

È stato introdotto il supporto al protocollo Online Certificate Status Protocol (OCSP), descritto nel RFC 2560, che consente di verificare la validità di un certificato senza ricorrere alle liste di revoca dei certificati (CRL).

GovWay consente di definire differenti molteplici policy OCSP, ad ognuna delle quali è possibile attribuire una modalità di validazione del certificato differente rispetto a vari parametri: dove reperire la url del servizio OCSP a cui richiedere la validità del certificato e il certificato dell'Issuer che lo ha emesso, come comportarsi se un servizio non è disponibile, eventuale validazione CRL alternativa etc.

Una policy OCSP è utilizzabile nelle seguenti funzionalità per attuare una validazione OCSP dei certificati presenti:

- *Profilo di Interoperabilità ModI*: certificato utilizzato all'interno dei token di sicurezza "ID_AUTH" e "INTEGRITY";
- *Connettore HTTPS*: certificato server;
- *WSSecurity* e *JOSE*: certificato utilizzato per firmare il messaggio;
- *Token OAuth*: certificato utilizzato per firmare il token;
- *Autenticazione HTTPS*: certificato client;
- *Frontend HTTPS*: certificati X.509 inoltrati a GovWay su header http dai frontend dove viene attuata la terminazione tls (Apache httpd, IIS, etc).

8.2 Miglioramenti alla gestione dei Certificati X.509

È adesso possibile caricare un certificato, da associare ad un applicativo o ad un soggetto, anche nei seguenti formati:

- pkcs7 (p7b);
- certificate chain.

Per ogni certificato è adesso possibile accedere anche alle seguenti informazioni:

- ottenere i "subject alternative names" presenti nel certificato;

- accedere all'oggetto "extensions" generico che raccoglie tutte le estensioni presenti nel certificato.

8.3 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- Nello script SQL generato per SQLServer è stata aggiunta una nota iniziale che indica il charset "UTF-8" e la collation "case sensitive" da utilizzare.

8.4 Bug Fix

Sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:

- CVE-2022-46364: aggiornate librerie "org.apache.cxf:cxf-*" alla versione 3.5.5 (e dipendenza org.ow2.asm:asm alla versione 9.4);
- CVE-2022-41915: aggiornate librerie "io.netty:netty-*" alla versione 4.1.86.Final.

Sono stati risolti i seguenti bug:

- le operazioni riguardanti richieste definite tramite WSDL con stile rpc, non venivano riconosciute dal processo di lettura delle informazioni SOAP in streaming;
- aggiunta proprietà "validation.rpc.rootElementUnqualified.accept", configurabile nell'erogazione o nella fruizione, che consente di indicare se devono essere accettate o meno richieste RPC il cui root-element non appartiene ad alcun namespace in modo da poter disattivare il comportamento di default del prodotto che consente di accettare le richieste al fine di essere compatibile con framework soap datati;
- un utilizzo di configurazioni che prevedono keystore PKCS12 o CRL in formato PEM su GovWay dispiegato nell'application server JBoss EAP 7.3 (aggiornato all'ultimo patch level) provocava il seguente errore: «java.lang.NoClassDefFoundError: org/bouncycastle/util/encoders/Base64 at org.bouncycastle.jcajce.provider.asymmetric.x509.PEMUtil.readPEMObject()»;
- La risoluzione dinamica di una risorsa che riferiva un metodo con un parametro contenente un punto non funzionava. Ad esempio supponendo di avere nella richiesta un header con nome "Header3.1", l'espressione "${transportContext:headerFirstValue(Header3.1)}" falliva con il seguente errore: «... resolution failed: method [org.openspcoop2.protocol.engine.URLProtocolContextImpl.getHeaderFirstValue(Header3()] not found ...».
- risolto problema di caching delle richieste su API SOAP, in alcune condizioni limite di errore, dove avveniva una inviduazione errata dell'azione;
- il timer che verifica la disponibilità delle risorse (connessione verso i database di runtime, tracciamento, configurazioni) è adesso configurabile per iterare il controllo x volte prima di segnalare l'anomalia (default: 5 iterazioni, una ogni 500ms). L'iterazione nel controllo serve ad evitare che una singola anomalia (es. di rete) possa bloccare tutta la gestione delle richieste fino al prossimo controllo che per default avviene dopo 30 secondi.

Per la console di gestione sono stati risolti i seguenti bug:

- la selezione di un numero di Entries da visualizzare differente dal default (20) provocava uno stato di attesa infinito della console causato dall'errore: «Uncaught ReferenceError: selectedIndex is not defined»;
- la verifica CSRF falliva erroneamente dopo un controllo dei riferimenti di un oggetto in 2 scenari d'uso differenti:
  - entrando nel dettaglio un soggetto (o applicativo o ruolo o scope), controllando i riferimenti dell'oggetto e successivamneto provandolo a salvare;
  - nelle liste controllando i riferimenti di un oggetto e successivamente provandolo ad eliminare;
- era erroneamente concesso modificare la token policy associata ad un applicativo anche se quest'ultimo risultava censito puntualmente nel controllo degli accessi di una erogazione o fruizione;

- la modifica delle credenziali di un applicativo di dominio esterno, per il profilo di interoperabilità “ModI”, non funzionava nel caso di credenziali di tipo “Authorization PDND” o “Authorization OAuth” nei seguenti casi:
  - modifica dell valore dell’identificativo;
  - aggiunta o eliminazione di un certificato X.509 all’autorizzazione per gestire l’integrità;
- sono stati corretti i seguenti problemi relativi all’importazione di una configurazione:
  - se l’archivio importato conteneva 2 applicativi con profilo di interoperabilità “ModI” di dominio esterno, uno definito con credenziale “Authorization ModI” tramite un certificato x.509 ed uno definito con credenziale “Authorization PDND + Integrity” contenente lo stesso certificato x.509, il caricamento falliva segnalando erroneamente la duplicazione dell’associazione del certificato x.509 ai due applicativi, mentre doveva essere permesso poichè uno dei due viene riconosciuto tramite l’identificativo della token policy e non tramite il certificato (poi utilizzato per la verifica dell’integrità);
  - dopo aver esportato una API, la successiva importazione dell’archivio in un’installazione in cui il soggetto di default indicato nell’installer differiva, provocava un fallimento dell’import poichè veniva erroneamente richiesta la presenza del soggetto originale da cui era stato fatto l’export.

9 Versione 3.3.9

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.9 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.9 utilizzare l’ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.9.p3*
- *Bug Fix 3.3.9.p2*
- *Bug Fix 3.3.9.p1*

9.1 Aggiornamento Librerie Terza Parte

Sono state aggiornate alle versioni più recenti tutte le librerie terza parte utilizzate al fine di risolvere tutte le vulnerabilità note.

9.2 Miglioramenti alla funzionalità di Correlazione Applicativa

Nota

Nuova funzionalità introdotta nella versione “3.3.9.p2”

Sono state aggiunte ulteriori modalità di estrazione dell’identificativo di correlazione applicativa:

- Template: l’id di correlazione è il risultato dell’istanziazione del template fornito rispetto ai dati della richiesta;
- Freemarker Template: l’id è ottenuto tramite il processamento di un Freemarker Template;
- Velocity Template: l’id è ottenuto tramite il processamento di un Velocity Template.

9.3 Miglioramenti alla funzionalità “Header di Integrazione”

Nota

Nuova Funzionalità introdotta nella versione “3.3.9.p2”

Oltre alle informazioni standard previste dagli header di integrazione di GovWay, i client applicativi possono adesso fornire informazioni custom al gateway tramite un json il cui formato può essere arbitrariamente definito dal client.

Il json può essere inviato nell’header http “GovWay-Integration” codificato in base64.

La presenza dell’header http non è obbligatoria ma se presente le informazioni contenute vengono rese disponibili per l’uso nelle varie funzionalità del gateway, come ad esempio la correlazione applicativa o l’utilizzo di claim custom nella generazione di token di sicurezza ModI, o nella generazione di asserzioni JWT per la negoziazione di token OAuth.

9.4 Miglioramenti alla modalità di generazione dei token JWT

Nota

Nuova Funzionalità introdotta nella versione “3.3.9.p2”

Per quanto concerne i claim aggiuntivi che possono essere aggiunti all’interno del payload dei JWT generati da GovWay è adesso possibile:

- aggiungere il claim solamente se la risoluzione dinamica del valore viene effettuata con successo utilizzando la forma opzionale «?{..}»;
- definire tipi primitivi json (boolean,int,long,float,double) effettuando un cast nella forma «cast(<valore> as <tipoPrimitivo>)»;
- convertire una lista json di tipi primitivi in lista di stringhe effettuando un cast nella forma «cast(<valore> as string array)».

9.5 Miglioramenti alla gestione dei Certificati X.509

Nota

Nuova Funzionalità introdotta nella versione “3.3.9.p3”

Per ogni certificato è adesso possibile accedere anche alle seguenti informazioni:

- verificare se una Certificate Policy è presente o meno sul certificato ed accedere alle informazioni interne della policy;
- verificare i basic constraints (CA, pathLen);
- ottenere le Authority Information Access presenti nel certificato:
  - CA Issuers;
  - OCSP.
- ottenere i CRL Distribution Points presenti nel certificato.

9.6 Bug Fix

Sono stati risolti i seguenti bug:

- una richiesta POST senza contenuto e senza ContentType veniva erroneamente riconosciuta come non valida dal filtro CORS e di conseguenza non veniva generato l'header http "Access-Control-Allow-Origin" nella risposta;
- corretto errore di parsing che si presentava con alcune SOAPEnvelope:

  > «Invalid content (</SOAP-ENV:Envelope/>): The markup in the document preceding the root element must be well-formed.».

Sono stati introdotti miglioramenti prestazionali minimizzando gli accessi concorrenti alle varie cache di configurazione tramite l'ausilio di una cache di secondo livello che contiene tutti i dati principali raccolti durante la gestione della prima richiesta.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- utilizzando il database SQLServer la ricerca base nello storico delle transazioni produceva il seguente errore SQL:

  > «ERROR <20-10-2022 14:03:03.969> org.openspcoop2.core.commons.search.dao.jdbc.JDBCAccordoServizioParteSpecific Ambiguous column name "tipo_soggetto".»

- era erroneamente possibile cancellare testo nel contenuto di un messaggio visualizzato nel dettaglio di una transazione;
- sono stati corrette le seguenti anomalie relative alla funzionalità di export CSV delle configurazioni:
  - l'export produceva risultati non deterministici e/o incompleti;
  - l'username associato ad una erogazione tramite servizio IntegrationManager/MessageBox non veniva riportato nel report.

9.7 Bug Fix 3.3.9.p1

Sono stati risolti i seguenti bug:

- nel profilo di interoperabilità "SPCoop" è stata eliminata la dichiarazione del namespace con prefisso "SOAP_ENV" che veniva inserito nell'header eGov generato senza poi essere effettivamente utilizzato;
- nelle informazioni salvate durante la negoziazione di un token non venivano memorizzati gli eventuali parametri indicati nella form: audience, scope, client_id, resource (PDND).

Per la console di gestione sono stati risolti i seguenti bug:

- perfezionata la gestione delle vulnerabilità di tipo CSRF;
- perfezionata la gestione dell'header http «Content Security Policy (CSP)»;
- la segnalazione "Visualizza Riferimenti" di un applicativo non visualizzava applicativi con ruoli compatibili con le erogazioni associate;
- l'associazione di credenziali di tipo basic/ssl/principal ai soggetti e agli applicativi viene adesso effettuata controllando l'univocità della credenziale su entrambi;
- nella sezione "sicurezza messaggio" di un applicativo con profilo di interoperabilità ModI, la configurazione relativa ai dati di accesso al keystore risultava eliminabile da console, ma l'operazione non comportava una effettiva pulizia nella base dati dove i dati rimanevano, anche se non più visualizzabili.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- perfezionata la gestione delle vulnerabilità di tipo CSRF.

9.8 Bug Fix 3.3.9.p2

È stata introdotta una politica di generazione automatica degli header HTTP indicati di seguito, se non ritornati dal backend che implementa l'API, con lo scopo di evitare alcune vulnerabilità a cui possono essere soggette le implementazioni delle API:

- X-Content-Type-Options: nosniff
- Cache-Control: no-cache, no-store, must-revalidate

  Pragma: no-cache

  Expires: 0

  Vary: *

> **Nota**
>
> Il caching viene disabilitato per evitare che delle risposte vengano inopportunamente messe in cache, come indicato nelle Linee Guida - raccomandazioni tecniche per REST "RAC_REST_NAME_010". Il mancato rispetto di questa raccomandazione può portare all'esposizione accidentale di dati personali.

Per la console di gestione sono stati risolti i seguenti bug:

- l'aggiornamento dell'interfaccia OpenAPI o WSDL di una API provocava un errore non atteso. Dal log si poteva riscontrare il bug introdotto con la gestione delle vulnerabilità di tipo CSRF nella versione 3.3.9.p1: "Parametro [_csrf] Duplicato".

9.9 Bug Fix 3.3.9.p3

Sono stati risolti i seguenti bug:

- con interfacce OpenAPI complesse di grandi dimensioni la validazione dei contenuti utilizzando la libreria «swagger-request-validator» impiegava diversi secondi ad inizializzare lo schema, anche per richieste successive alla prima dove le informazioni vengono salvate in cache;
- la negoziazione di un token in modalità "SignedJWT" utilizzando un keystore di tipo "JWK Set" falliva con il seguente errore: «Errore avvenuto durante la consegna HTTP: (Errore di Connessione) JWT Signature keystore password undefined»;
- sono state risolte le seguenti vulnerabilità relative ai jar di terza parte:
  - CVE-2021-37533: aggiornata libreria "commons-net" alla versione 3.9.0;
  - CVE-2022-40150: aggiornata libreria "jettison" alla versione 1.5.2.

Per la console di gestione sono stati risolti i seguenti bug:

- utilizzando il database SQLServer l'accesso alla pagina di configurazione di una erogazione o fruizione produceva il seguente errore SQL: «ERROR … org.openspcoop2.core.mapping.DBMappingUtils._mappingErogazionePortaApplicativaList: Ambiguous column name "descrizione"»;
- la selezione della modalità "interfaccia avanzata", tramite la voce presente nel menù in alto a destra, presentava le seguenti problematiche:
  - la modalità selezionata veniva erroneamente visualizzata anche accedendo al profilo dell'utenza, invece dei criteri configurati in maniera persistente per quell'utente;

  - anche se veniva selezionata la modalità “interfaccia avanzata”, la selezione di connettori differenti da http (jms, file, . . .) non era disponibile se il profilo persistente associato all’utente era definito come “interfaccia standard”;

- la modifica del keystore di un applicativo ModI, nella sezione “Sicurezza Messaggio”, provocava un errore e nel file di log era presente la segnalazione: «Parametro [confSSLCredWizStep] Duplicato.»;
- effettuando un export contenente la configurazione di un soggetto diverso dal soggetto di default dichiarato nell’installer, la successiva importazione dell’archivio in un’installazione in cui tale soggetto fosse stato definito come soggetto di default provocava una inconsistenza delle configurazioni, segnalata dalla console al momento del login.

10 Versione 3.3.8

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.8 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

10.1 Miglioramenti alla funzionalità di Identificazione degli Applicativi

È stata estesa la possibilità di censimento degli applicativi fornendo le seguenti nuove opzioni:

- registrare applicativi afferenti a domini esterni anche per il profilo APIGateway, con la possibilità di censirli puntualmente tra i criteri di autorizzazione per richiedente;
- registrare applicativi con credenziali di tipo “token”. La nuova funzione consente al processo di autenticazione tramite token di identificare anche questo tipo di client, che saranno quindi riconoscibili nei log e utilizzabili per le ricerche negli strumenti di monitoraggio.

Nel controllo degli accessi di erogazioni e fruizioni è stata aggiunta la possibilità di autorizzare per richiedente o per ruolo gli applicativi identificati tramite token, prima autorizzabili sono sulla base dei valori dei token presentati.

Nel profilo di interoperabilità “ModI” la nuova modalità consente:

- di identificare ed autorizzare puntualmente gli applicativi registrati su PDND;
- di attuare controlli di consistenza tra i certificati utilizzati dal chiamante nei casi di utilizzo simultaneo dell’header Authorization, generato dalla PDND, e dell’header Agid-JWT-Signature, generato dalla parte mittente.

10.2 Miglioramenti alla funzionalità di RateLimiting

Sono state ottimizzate le prestazioni in caso di utilizzo degli scenari di conteggio tramite storage distribuito tra i nodi del cluster. Vengono adesso utilizzati “atomic-long”, sia sull’implementazione “Hazelcast” che sull’implementazione “Redis”.

Per l’implementazione “Hazelcast” sono inoltre stati effettuate le seguenti ulteriori ottimizzazioni:

- aggiunta una tecnica di sincronizzazione basata sui “PN Counters”;
- aggiunta la possibilità di definire un’unica configurazione di rete condivisa tra tutte le istanze attivate per ogni tecnica.

10.3 Miglioramenti alla funzionalità di Gestione dei Token

Migliorata la validazione dei token:

- aggiunto controllo che verifica che la data indicata nel claim “iat” non rappresenti una data futura;
- aggiunta la possibilità di configurare una token policy di validazione che utilizzi, per la validazione del token, il certificato presente negli header x5c e x5t del JWT.

Migliorata la gestione degli access token negoziati con gli Authorization Server:

- aggiunto supporto per il parametro “resource” richiesto nella v4.1 della PDND;
- in una policy di tipo “Signed JWT”, se utilizzata con API registrate con profilo di interoperabilità ModI, è adesso possibile firmare l’asserzione e valorizzare i paramtri ClientId e KID utilizzando il keystore e i dati definiti sull’applicativo richiedente;
- i token JWT scambiati durante la negoziazione di un token vengono adesso salvati nella traccia escludendo la parte relativa alla signature.

10.4 Miglioramenti alla funzionalità di Autenticazione

Per l’autenticazione https è adesso possibile:

- associare un truststore per verificare i certificati client ricevuti;
- definire delle CRL per la verifica delle revoche.

Le stesse funzionalità sono state rese disponibili anche per il gestore delle credenziali utilizzabile per l’autenticazione tramite certificati client ottenuti tramite header HTTP. In quest’ultima modalità è stata aggiunta la possibilità di decodificare i certificati ricevuti in entrambe le modalità supportate, prima provando la decodifica “urlEncoded” ed in caso di fallimento la decodifica “base64”.

10.5 Miglioramenti alla funzionalità di Autorizzazione

Sia nell’autorizzazione per token claims che nell’autorizzazione per contenuti è adesso possibile:

- definire controlli di uguaglianza case insensitive;
- definire delle condizioni “not” in cui si indicano i valori che non devono essere posseduti da un claim o da una risorsa;
- utilizzare la negazione anche sulle verifiche effettuate tramite espressioni regolari.

10.6 Miglioramenti alla funzionalità di Correlazione Applicativa

E” stata aggiunta la possibilità di modificare l’attuale comportamento di govway, attivando il troncamento dell’identificativo estratto alla massima lunghezza consentita di 255 caratteri.

Il comportamento di default resta lo stesso della precedente versione: nel caso l’identificativo estratto superi la massima lunghezza consentita di 255 caratteri, la transazione termina con errore o senza estrarre l’identificativo a seconda della modalità di gestione della regola di estrazione configurata (blocca/accetta).

10.7 Miglioramenti alla funzionalità dei Connettori

Nella gestione del proxy pass reverse è stata aggiunta la gestione dei path e dei domini presenti negli header Set-Cookie delle risposte (disabilitata per default).

È stata inoltre aggiunta la possibilità di abilitare o disabilitare sulla singola erogazione o fruizione:

- la traduzione di entrambi gli attributi di un Set-Cookie o solamente di uno dei due;
- la traduzione dell’header “Location” e/o Content-Location.

Infine è adesso possibile abilitare la funzionalità di proxy pass reverse anche su API SOAP (disabilitata per default).

10.8 Miglioramenti alla funzionalità di Tracciatura su File

È adesso possibile configurare una “DenyList” o una “WhiteList” che consente di personalizzare gli header HTTP ottenibili tramite la chiamate delle primitive: “getInRequestHeaders”, “getOutRequestHeaders”, “getInResponseHeaders”, “getOutResponseHeaders”.

È inoltre stato corretto un bug presente nell'uso dell'istruzione "${logBase64:xx}" su tali primitive: il valore codificato in base64 restituito conteneva una lista di header in cui i nomi e i valori erano nuovamente codificati in base64.

È infine adesso possibile abilitare il dump binario solamente per gli headers o per il payload dei messaggi scambiati.

10.9 Miglioramenti alle funzionalità base dell'API Gateway

Sono stati introdotti significativi miglioramenti prestazionali:

- in presenza di stress test alcune comunicazioni terminavano con l'errore «Cannot assign requested address» dovuto ad un numero troppo basso (5) di connessioni http "keep-alive" mantenute aperte per una stessa destinazione (numero aumentato per default a 200);
- risolto degrado delle performance, che avveniva in presenza di trasformazione Freemarker o Velocity, attraverso il salvataggio dell'oggetto template istanziato in cache;
- è adesso possibile configurare una "DenyList" o una "WhiteList" che consente di personalizzare gli header HTTP che devono essere registrati su database tramite la funzionalità di registrazione messaggi;
- migliorata la latenza introdotta da GovWay (attualmente pochi millisecondi) durante la gestione di una prima richiesta non ancora in cache, su API Rest contenenti molte risorse (es. 600), in cui la latenza introdotta da GovWay era nell'ordine dei secondi (5,7 secondi);
- le richieste che richiedevano la validazione/negoziazione di un token, il recupero di attributi da un AttributeAuthority o l'invocazione di meccanismi di autenticazione/autorizzazione esterni acceduti via http (implementati tramite plugin) potevano far scaturire l'errore «Could not acquire semaphore after 30000ms», quando il servizio http esterno contattato (es. Authorization Server) non rispondeva mandando la richiesta in read timeout e nel frattempo continuavano ad accumularsi richieste che necessitavano dell'invocazione del servizio esterno poichè l'informazione richiesta non era in cache. L'errore si amplificava poichè per stessa funzionalità (es. Token Policy di Negoziazione) non vi era un lock dedicato alla singola policy ma un lock condiviso tra tutte le policy. La problematica è stata risolta:
  - dedicando un lock ad ogni Token Policy, AttributeAuthority o tipo di autenticazione/autorizzazione;
  - abbassando i tempi di read-timeout di default a 10 secondi;
  - consentendo un numero di richieste parallele verso il servizio esterno quando le informazioni non sono in cache (default 10), in modo da non rendere seriale l'inizializzazione della cache.

10.10 Miglioramenti al Profilo di Interoperabilità "ModI"

Sono stati apportati i seguenti miglioramenti:

- aggiunto controllo che verifica che la data indicata nel claim "iat" (API di tipo REST) e nell'elemento "Timestamp/Created" (API di tipo SOAP) non rappresenti una data futura (viene applicato un intervallo di tolleranza configurabile, con un default di 5 secondi);
- nel controllo degli accessi, è adesso possibile definire un criterio di autorizzazione basato sui ruoli dell'applicativo richiedente;
- è ora possibile personalizzare il comportamento del pattern "INTEGRITY_REST_01", delegando la parte relativa alla gestione dell'integrità (calcolo/verifica Digest, gestione claim "signed_header" o simile) alla componente applicativa. Con questa modalità è possibile anche personalizzare il nome dell'header HTTP utilizzato.

10.11 Miglioramenti alle Console

È stata migliorata la modalità di selezione dei profili di interoperabilità e dei soggetti operativi:

- a login effettuato, il profilo e il soggetto proposti sono quelli associati per default all'utente e sono modificabili accedendo al "Profilo Utente";

- la selezione dal menù a tendine, visualizzato in alto a destra nella console, ha un effetto immediato ma non viene più resa persistente dopo un logout;
- relativamente alla sola console di gestione, gli stessi criteri di selezione del profilo e del soggetto sono stati riportati anche nella selezione della modalità di utilizzo dell'interfaccia (standard/avanzata);
- relativamente alla sola console di monitoraggio è adesso possibile definire la sezione visualizzata al momento del login, selezionandola tra le seguenti due voci:
  - pagina di ricerca delle transazioni
  - report statistico; in questo caso viene consentito anche di definire l'intervallo temporale di default.

Infine è stato risolto un problema sulla console di gestione che non ne consentiva l'utilizzo in contemporanea su più tab di un browser.

10.12 Bug Fix

Sono stati risolti i seguenti bug:

- risolti i seguenti problemi relativi alla validazione di un'interfaccia OpenAPI 3.0:
  - non erano supportati parametri (path/header/query/cookie) definiti tramite complex type (anyOf/allOf/oneOf);
  - la validazione di un "path parameter", contenente caratteri che erano stati codificati per poter essere trasmessi nella url, falliva poichè non veniva attuata una decodifica prima della validazione del parametro;
- le invocazione di API REST con contenuti XML permettevano di sfruttare la vulnerabilità XXE descritta in:
  - https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html
  - https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing
- la keyword "securityToken.accessToken" era utilizzabile per accedere al certificato utilizzato nell'access token solamente alla prima invocazione;
- il certificato ottenuto tramite il "gestore delle credenziali" via header HTTP è adesso disponibile nel contesto per essere acceduto tramite la keyword "securityToken.channel";
- l'utilizzo dei metodi getJSONObject(...) e getJSONArray(...) dell'utility JsonPathExpressionEngine creava, in presenza di richieste parallele, dei messaggi inconsistenti per via di un utilizzo statico del parser JSONParser che non era "thread safe";
- risolti errori di validazione degli header HTTP che si presentavano utilizzando la libreria di validazione "swagger-request-validator" al posto di quella di default "Openapi4j":
  - se la richiesta presentava un header HTTP "Accept" contenente parametri "q" si otteneva un errore simile al seguente: «Request Accept header "*; q=.2" is not a valid media type»;
  - se l'OpenAPI definiva risposte con qualsiasi subtype (es. application/*), le richieste valide venivano erroneamente rifiutate con un errore simile al seguente: «Request Accept header "[application/xml]" does not match any defined response types. Must be one of: [application/*]»
- se per una API SOAP veniva configurata una trasformazione della richiesta (o della risposta) che rientrava nella seguente casistica:
  - il contenuto veniva ridefinito tramite una envelope soap di una versione differente da quello della richiesta originale (es. soap1.1 -> soap 1.2)
  - veniva definito il nuovo Content Type conforme alla nuova versione dell'envelope (es. application/soap+xml)

  l'applicazione della trasformazione a runtime produceva l'errore «Trasformazione richiesta fallita: Cannot add fragments which contain elements which are in the SOAP namespace».

Per la console di gestione sono stati risolti i seguenti bug:

- la creazione di una API REST, tramite l'upload di un openapi, presentava le seguenti problematiche:
  - non venivano create eventuali risorse definite con i metodi "HEAD" o "TRACE";
  - se venivano definiti erroneamente degli header senza schema, la console riportava un errore non corretto: «[Interfaccia OpenAPI 3] Documento non valido: java.lang.NullPointerException»;
- la validazione di un'interfaccia OpenAPI era troppo stringente per quanto concerne i valori definiti nella sezione "info" riguardanti:
  - indirizzo email dei contatti (info.contact.email)
  - url dei contatti e della licenza (info.contact.url e info.license.url)
- sono state risolte le seguenti problematiche relative al caricamento di un allegato in una API:
  - utilizzando Internet Explorer il nome del documento conteneva il path assoluto;
  - il tipo di specifica semiformale selezionato non veniva preservato quando si caricava un file e veniva riproposto il tipo UML (stesso problema era presente nel caricamento degli allegati di una erogazione o fruizione);
- nei campi "textarea" utilizzabili per indicare path su file system, url, audience e altri valori che rappresentano un identificativo, non veniva segnalata l'eventuale presenza errata di new-line o tab nel valore fornito;
- aggiornate le librerie che consentono di effettuare il parsing di un documento yaml (OpenAPI 3) al fine di non essere più vulnerabile a Denial of Service (DoS) per mancanza di limitazione sulla profondita dei nodi analizzati e collezionati durante il parsing;
- l'utilizzo di schede multiple all'interno del browser provocava errori durante l'utilizzo della console;
- la validazione del pattern speciale "XPath su messaggi JSON" (https://govway.readthedocs.io/it/latest/console/avanzate/contentBased.html) non era più configurabile sulla console dove veniva segnalato un errore di formato;
- utilizzando la funzionalità "Elimina" per caricare archivi contenenti Policy di Rate Limiting, l'operazione terminava con successo ma l'eliminazione lasciava policy "zombie" sulla base dati.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- l'esito "API Sospesa" è stato incluso nel gruppo "Richiesta Scartata";
- migliorata la documentazione della console di monitoraggio relativa alle informazioni Esito, Richiedente e Dettaglio Errore riportate nel dettaglio di una transazione;
- se veniva richiesto un download con la funzionalità "Estrai Contenuti Multipart", il successivo download di un messaggio non multipart andava in errore;
- risolta anomalia presente in tutte le distribuzioni statistiche eccetto quella temporale e per esiti. Quando si selezionava un periodo "personalizzato", se la scelta precedente del periodo era diversa da "ultime 12 ore", le date venivano resettate automaticamente dopo l'impostazione dell'ora all'intervallo inferiore o superiore a seconda della data iniziale o finale.

11 Versione 3.3.7

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.7 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

11.1 Miglioramenti alla funzionalità di Validazione dei Contenuti

Aggiunto supporto per le richieste "multipart/form-data" e "multipart/mixed":

- https://swagger.io/docs/specification/describing-request-body/multipart-requests/
- https://swagger.io/docs/specification/describing-request-body/file-upload/

È stata inoltre introdotta la possibilità di ottimizzare (su una singola erogazione o fruizione) la validazione dei messaggi ricevuti, sospendendo l'analisi dello stream dopo aver validato tutti i metadati non binari previsti dall'interfaccia OpenAPI.

Nota

Benchè l'ottimizzazione consenta di ottenere significativi benefici prestazionali, rappresentando tipicamente le parti binarie la maggior dimensione del messaggio, non viene attivata per default poichè non consente di individuare se esistano «part» non previste dalla specifica (in presenza di "additionalProperties=false") successive alle «part» non binarie.

11.2 Miglioramenti alla funzionalità di RateLimiting

Aggiunte nuove modalità di gestione delle policy di RateLimiting utilizzabili su un cluster di nodi:

- possibilità di suddividere le quote previste per il numero di nodi attivi; questa modalità permette, potendo sfruttare la collaborazione del load balancer, di ottenere il conteggio corretto delle quote previste anche senza bisogno di utilizzare uno storage distribuito tra i nodi del cluster;
- possibilità di gestire il conteggio tramite storage distribuito tra i nodi del cluster; per limitare il degrado prestazionale introdotto dalla gestione del conteggio distribuito, è possibile configurare opzioni di comunicazione asincrona tra i nodi del cluster, ottenendo performance migliori a discapito della precisione nei conteggi.

La modalità di configurazione del rate limiting può essere perfezionata per ogni erogazione o fruizione di API, permettendo quindi di adottare la soluzione più opportuna per ogni singola API gestita da GovWay.

È inoltre stata introdotta la possibilità di personalizzare gli header HTTP restituiti ai client, relativi alle informazioni sulle quote e sulle finestre temporali delle policy di rate limiting: è possibile disabilitarne del tutto la generazione o modificarne i valori indicati per quanto concerne la quota (indicazione o meno della finestra temporale) e gli intervalli di retry (utilizzo o meno di un tempo di backoff).

È infine stata aggiunta la possibilità di filtrare l'applicabilità di una policy rispetto ai valori presenti in un token OAuth2.

11.3 Miglioramenti alla funzionalità di Gestione dei Token

Migliorata la gestione degli access token negoziati con gli Authorization Server:

- un access token, precedentemente negoziato e disponibile in cache, viene adesso rinegoziato prima della scadenza effettiva (indicata in expireIn) per evitare che possa risultare scaduto una volta ricevuto dall'erogatore, quando utilizzato per richieste gestite in prossimità della scadenza;
- è adesso possibile configurare il criterio di generazione del claim "jti" inserito nell'asserzione JWT generata nella modalità "JWT Signed";
- i criteri di negoziazione (asserzione JWT, url, clientId) e l'access token ottenuto sono adesso consultabili tramite la console di monitoraggio, accedendo ai dati della transazione (Token Info).

Sono inoltre stati risolti i seguenti problemi:

- risolto problema di performance in cui l'accesso sincronizzato all'interno della gestione della cache per i token avveniva erroneamente per ogni richiesta anche se il token era già presente in cache;

- i token ottenuti venivano salvati in cache tramite una chiave formata dal solo nome della Token Policy di negoziazione, ignorando gli eventuali parametri dinamici risolti a runtime. In tale situazione, se una policy con parametri dinamici veniva utilizzata su più fruizioni, poteva succedere che il token negoziato in seguito all'invocazione di una prima fruizione, venisse erroneamente riutilizzato (disponibile in cache) per l'invocazione di una seconda fruizione. Scenario tipico in presenza di PDND dove il purposeId è rappresentato da un parametro dinamico ad esempio indicato dal client tramite un header HTTP.

Infine nelle policy di validazione dei token è adesso possibile indicare come formato dell'access token anche la struttura definita nel RFC 9068.

11.4 Miglioramenti alla gestione dei Certificati X.509

I certificati scambiati nelle richieste sono adesso accessibili dal contesto tramite le keyword:

- "transportContext": consente di accedere ai certificati TLS;
- "securityToken": consente di accedere ai certificati presenti nei token di sicurezza messaggio ModI e negli access token JWT.

Per ogni certificato è adesso possibile accedere alle seguenti informazioni:

- accedere ai singoli campi di un DN;
- verificare se una keyUsage è presente o meno sul certificato;
- verificare se un purpose (extendedKeyUsage) è presente o meno sul certificato.

L'oggetto associato alla keyword "securityToken" (org.openspcoop2.protocol.sdk.SecurityToken) consente di ottenere anche solamente la parte relativa all'header o al payload del token ModI (Authorization o Agid-JWT-Signature) o dell'access token JWT. Inoltre consente di accedere puntualmente ai singoli claim presenti nell'header o nel payload del token.

Le informazioni sopra descritte sono ora utilizzabili nella gestione delle seguenti funzionalità di GovWay:

- autorizzazione per Token Claims;
- autorizzazione per Contenuti;
- trasformazioni.

11.5 Miglioramenti alla funzionalità di Correlazione Applicativa

Aggiunto il supporto per applicare regole di correlazione applicativa su richieste multipart per API di tipo REST: l'identificativo viene ricercato all'interno del primo part che rappresenta un contenuto xml o json.

11.6 Miglioramenti alla funzionalità di Tracciatura su File

Tra le informazioni che possono essere riversate nei file di log associati ai topic di file trace, sono adesso disponibili anche le seguenti informazioni:

- Token negoziati con gli Authorization Server:
  - retrievedAccessToken: access token ottenuto dall'authorization server configurato nella Token Policy associata al connettore;
  - retrievedTokenClaim(nomeClaim): valore del claim indicato come parametro e presente nella risposta ritornata dall'authorization server;
  - retrievedTokenRequestTransactionId: identificativo della transazione che ha originato la richiesta verso l'authorization server;
  - retrievedTokenRequestGrantType: tipo di grant type utilizzato nella negoziazione del token (clientCredentials, usernamePassword, rfc7523_x509, rfc7523_clientSecret);

  - retrievedTokenRequestJwtClientAssertion: asserzione jwt generata durante una negoziazione con grant type «rfc7523_x509»;
  - retrievedTokenRequestClientId: clientId utilizzato durante la negoziazione del token;
  - retrievedTokenRequestClientToken: bearer token utilizzato durante la negoziazione del token;
  - retrievedTokenRequestUsername: username utilizzato durante una negoziazione del token con grant type «usernamePassword»;
  - retrievedTokenRequestUrl: endpoint dell'authorization server.
- Certificato TLS Client:
  - clientCertificateSubjectDN: distinguished name del subject relativo al certificato tls client;
  - clientCertificateSubjectCN: common name del subject relativo al certificato tls client;
  - clientCertificateSubjectDNInfo(String oid): ritorna l'informazione indicata come parametro relativa al subject del certificato tls client;
  - clientCertificateIssuerDN: distinguished name dell'issuer relativo al certificato tls client;
  - clientCertificateIssuerCN: common name dell'issuer relativo al certificato tls client;
  - clientCertificateIssuerDNInfo(String oid): ritorna l'informazione indicata come parametro relativa all'issuer del certificato tls client.
- Token OAuth2 validato come JWT:
  - tokenClaim(nomeClaim): consente di accedere ad un singolo claim di un token OAuth2 validato su GovWay;
  - tokenRaw: JWT token presente nella richiesta;
  - tokenHeaderRaw: porzione dell'header relativa al token JWT presente nella richiesta, in formato base64;
  - tokenPayloadRaw: porzione del payload relativa al token JWT presente nella richiesta, in formato base64;
  - tokenDecodedHeader: contenuto decodificato dell'header presente nel token JWT;
  - tokenDecodedPayload: contenuto decodificato del payload presente nel token JWT;
  - tokenHeaderClaim(nomeClaim): valore del claim indicato come parametro e presente nell'header del token JWT;
  - tokenPayloadClaim(nomeClaim): valore del claim indicato come parametro e presente nel payload del token JWT;
  - tokenHeaderClaims(): claims (nome=valore) presenti nell'header del token JWT;
  - tokenHeaderClaims(claimSeparator, nameValueSeparator): simile alla precedente opzione, consente di indicare i separatori utilizzati;
  - tokenPayloadClaims(): claims (nome=valore) presenti nel payload del token JWT;
  - tokenPayloadClaims(claimSeparator, nameValueSeparator): simile alla precedente opzione, consente di indicare i separatori utilizzati;
  - tokenCertificateSubjectDN: distinguished name del subject relativo al certificato con cui è stato firmato il token JWT;
  - tokenCertificateSubjectCN: common name del subject relativo al certificato con cui è stato firmato il token JWT;
  - tokenCertificateSubjectDNInfo(String oid): ritorna l'informazione indicata come parametro relativa al subject del certificato con cui è stato firmato il token JWT;

  - tokenCertificateIssuerDN: distinguished name dell'issuer relativo al certificato con cui è stato firmato il token JWT;
  - tokenCertificateIssuerCN: common name dell'issuer relativo al certificato con cui è stato firmato il token JWT;
  - tokenCertificateIssuerDNInfo(String oid): ritorna l'informazione indicata come parametro relativa all'issuer del certificato con cui è stato firmato il token JWT.

- Profilo Interoperabilità "ModI":
  - tokenModI<tokenType>Raw: security token presente nella richiesta;
  - tokenModI<tokenType>CertificateSubjectDN: distinguished name del subject relativo al certificato con cui è stato firmato il security token;
  - tokenModI<tokenType>CertificateSubjectCN: common name del subject relativo al certificato con cui è stato firmato il security token;
  - tokenModI<tokenType>CertificateSubjectDNInfo(String oid): ritorna l'informazione indicata come parametro relativa al subject del certificato con cui è stato firmato il security token;
  - tokenModI<tokenType>CertificateIssuerDN: distinguished name dell'issuer relativo al certificato con cui è stato firmato il security token;
  - tokenModI<tokenType>CertificateIssuerCN: common name dell'issuer relativo al certificato con cui è stato firmato il security token;
  - tokenModI<tokenType>CertificateIssuerDNInfo(String oid): ritorna l'informazione indicata come parametro relativa all'issuer del certificato con cui è stato firmato il security token.

  I tipi di token disponibili sono:
  - Authorization: security token ricevuto nell'header HTTP "Authorization";
  - Integrity: security token ricevuto nell'header HTTP "Agid-JWT-Signature";
  - Soap: security token ricevuto nell'header SOAP;

  Per i tipi di token "Authorization" e "Integrity", relativi ad API di tipo REST, sono disponibili anche le seguenti informazioni:
  - tokenModI<tokenType>HeaderRaw: porzione dell'header relativa al security token presente nella richiesta, in formato base64;
  - tokenModI<tokenType>PayloadRaw: porzione del payload relativa al security token presente nella richiesta, in formato base64;
  - tokenModI<tokenType>DecodedHeader: contenuto decodificato dell'header presente nel security token;
  - tokenModI<tokenType>DecodedPayload: contenuto decodificato del payload presente nel security token;
  - tokenModI<tokenType>HeaderClaim(nomeClaim): valore del claim indicato come parametro e presente nell'header del security token;
  - tokenModI<tokenType>PayloadClaim(nomeClaim): valore del claim indicato come parametro e presente nel payload del security token;
  - tokenModI<tokenType>HeaderClaims(): claims (nome=valore) presenti nell'header del security token;
  - tokenModI<tokenType>HeaderClaims(claimSeparator, nameValueSeparator): simile alla precedente opzione, consente di indicare i separatori utilizzati;

  - tokenModI<tokenType>PayloadClaims(): claims (nome=valore) presenti nel payload del security token;
  - tokenModI<tokenType>PayloadClaims(claimSeparator, nameValueSeparator): simile alla precedente opzione, consente di indicare i separatori utilizzati;

- Altro:
  - requesterIP: rappresenta l'indirizzo IP del richiedente e assumerà la prima informazione valorizzata, trovata nella richiesta, nel seguente ordine: forwardedIP, clientIP;
  - resultCode: consente di ottenere il codice numerico di GovWay che rappresenta l'esito della transazione.

Sono infine stati risolti i seguenti problemi:

- corretto valore ritornato dalla keyword "inUrl", dove è stato eliminato il prefisso "[in]" o "[out]" che rimane recuperabile tramite la keyword "inFunction";
- la tracciatura dell'informazione "${logBase64:errorDetail}" provocava un errore inatteso poichè venivano erroneamente serializzate in base64 le informazioni prima di interpretare il dettaglio dell'errore;
- le richieste errate (es. API not found) non venivano tracciate se la funzionalità veniva attivata tramite una configurazione globale.

11.7 Miglioramenti alla funzionalità dei Connettori

Nel connettore di tipo "file" è stata aggiunta la possibilità di definire i permessi (rwx) dei file creati in cui viene serializzato il contenuto della richiesta (payload e header).

11.8 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti alla console di monitoraggio:

- nel dettaglio di una transazione è adesso possibile ispezionare il contenuto multipart delle richieste relativamente ad API di tipo REST.

11.9 Bug Fix

Sono stati risolti i seguenti bug:

- aggiunto il timezone nella serializzazione delle date negli header HTTP inoltrati ai backend;
- migliorata diagnostica emessa in presenza di una richiesta SOAP vuota (senza http payload), rispetto al precedente errore che riportava un null pointer: «Riscontrato errore ... errore durante il controllo del namespace del soap envelope: null». La nuova diagnostica riporta invece la causa dell'errore: «Riscontrato errore ... errore durante il controllo del namespace del soap envelope: Invalid empty message»
- in presenza di una API SOAP con registrazione messaggi abilitata, se la risposta pervenuta conteneva un Content-Type non compatibile con quello della richiesta, GovWay segnalava l'anomalia correttamente nei diagnostici ma non registrava il contenuto della risposta e degli header HTTP;
- la funzionalità di lettura delle richieste SOAP in streaming veniva erroneamente attivata nel servizio di imbustamento Xml2Soap e causava, nel profilo di interoperabilità "Fatturazione Elettronica", una spedizione di fatture binarie (P7M/ZIP) corrotte;
- modificato nome della proprietà "topic.*.requestSended" in "topic.*.requestSent" nella tracciatura su file;
- la configurazione di default della funzionalità "GovWayProxy" per Token Policy e A.A. descritta nel file govway.properties veniva ignorata;

- negli header di integrazione “Backward Compatibility OpenSPCoop”, gli header che riportano il tipo dei soggetti e il tipo del servizio contengono adesso i valori che venivano utilizzati in OpenSPCoop2 (es. PROXY al posto di gw per il profilo “API Gateway”);
- sono stati risolti i seguenti problemi che avvenivano disabilitando il tracciamento delle transazioni:
  - la funzionalità di tracciatura su file non registrava le informazioni nei topic configurati;
  - la funzionaltà di consegna asincrona produceva un errore durante il tentativo di registrazione delle tracce e dei diagnostici.

Sono stati risolti i seguenti bug relativi al profilo di interoperabilità “ModI”:

- nel pattern “Integrity_REST_01” l’header Digest veniva erroneamente sia generato che atteso con una codifica “hex”. La codifica è stata rivista per utilizzare “base64” in modo da essere conformi al RFC 5843 (che estende il RFC 3230 indicato nelle Linee Guida). Per garantire la retrocompatibilità è possibile configurare la singola erogazione/fruizione per produrre un header Digest codificato in esadecimale, mentre in fase di validazione è possibile accettare entrambe le codifiche. Per default sia la codifica attesa che quella generata è sempre base64.
- risolta mancata rilevazione di identificativo duplicato quando sia il dominio fruitore che quello erogatore venivano gestiti sulla stessa instanza di GovWay. La mancata rilevazione avveniva solamente se le richieste duplicate venivano ricevute simultaneamente rispetto all’originale.

Per la console di gestione sono stati risolti i seguenti bug:

- risolti i seguenti problemi relativi alla validazione di un’interfaccia OpenAPI 3.0:
  - la validazione risultava esssere troppo stringente per quanto concerne i valori di default associati ai tipi primitivi (integer, number o boolean) definiti con gli apici (es. “65” invece di 65). Il validatore segnalava un errore simile al seguente: «Validation error(s) : paths./pets1.patch.parameters.schema.default: Value “65” is incompatible with schema type “integer” (code: 138)»
  - OpenAPI in formato YAML che possedevano anchor «merge key» (es. <<: *) non superavano la validazione dell’interfaccia;
  - il caricamento di un’interfaccia contenente una descrizione superiore a 255 caratteri, causava un errore inatteso in alcuni casi su database Oracle dove si otteneva l’errore: «Caused by: java.sql.SQLException: ORA-12899: value too large for column «GOVWAY334TESTBYSETUP».»ACCORDI».»DESCRIZIONE» (actual: 257, maximum: 255)».

Per la console di monitoraggio sono stati risolti i seguenti bug:

- i grafici (PieChart e BarChart) della distribuzione per errore non venivano visualizzati dalla console nel caso in cui tra le tipologie di errore individuate fosse presente un errore la cui descrizione presentava l’apice singolo;
- in una ricerca per identificativo (applicativo, messaggio o transazione), se la query impiega troppo tempo la console interrompe la ricerca visualizzando un popup che segnala di riprovare stringendo i parametri di ricerca. Il messaggio riportato è stato corretto non essendoci criteri temporali nella ricerca per identificativo.

12 Versione 3.3.6

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.6 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.6 utilizzare l’ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.6.p1*

12.1 Miglioramenti alla Console di Gestione

Sono stati apportati i seguenti miglioramenti alla console di gestione:

- per ogni entità del registro, sia dall'elenco che dal dettaglio, è adesso possibile:
  - rimuovere puntualmente dalla cache i dati relativi all'oggetto;
  - visualizzare i riferimenti agli utilizzi di quella entità;
  - visualizzare una scheda riassuntiva della configurazione di una erogazione o di una fruizione;
  - verificare la validità dei certificati inclusi nei keystore riferiti dai connettori http/https, dalla configurazione del profilo di interoperabilità ModI o riferiti negli applicativi e nei soggetti;
  - aggiunta la possibilità di verificare la connettività anche per gli endpoint configurati nelle Token Policy di validazione e negoziazione, nelle Attribute Authority e negli applicativi di tipo server.
- effettuato un restyling dell'elenco delle Token Policy di validazione e negoziazione e delle Attribute Authority;
- aggiunta la validazione delle espressioni regolari, degli xpath e dei jsonPath configurabili nelle varie funzionalità gestite da console;
- migliorata gestione e monitoraggio delle consegne asincrone (attivabili con una installazione in modalità avanzata):
  - aggiunta la possibilità di disabilitare lo scheduling delle consegne di un connettore, mantenendo i messaggi in coda fino alla riabilitazione;
  - nella funzionalità "Coda Messaggi" è adesso possibile avere una informazione di sintesi delle consegne in corso.

12.2 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti alla console di monitoraggio:

- aggiunto report statistico che consente di ottenere una distribuzione per tipo di errore;
- in caso di consegna multipla è stata aggiunta alla transazione l'informazione riguardante il nome del connettore selezionato, informazione ricercabile tramite la console attraverso la casella "Eventi" nello storico delle transazioni;
- aggiunto alle transazioni il nuovo stato «in coda», che identifica le consegne asincrone, permettendo di differenziare le richieste «in coda», su cui non è ancora stata effettuata alcuna consegna, rispetto a quelle «in corso», per le quali è già stata tentata almeno una consegna.

12.3 Miglioramenti alla funzionalità di Gestione dei Token

Nota

La funzionalità è stata introdotta nella versione "3.3.6.p1"

Nella negoziazione di un Token tramite la modalità JWT Signed è adesso possibile:

- configurare i parametri da inserire nell'header non firmato (kid, x5c, x5t ...);
- personalizzare i valori dei claim inseriti nel payload firmato tramite parti dinamiche che vengono risolte a runtime dal Gateway;
- aggiungere claim ulteriori oltre a quelli previsti dallo standard;

- possibilità di abilitare una modalità di compatibilità con la Piattaforma Digitale Nazionale Dati (PDND), che permette di configurare gli ulteriori campi richiesti dalla PDND (purposeId, sessionInfo).

Nella validazione dei token è stata introdotta la possibilità di configurare un formato di token definito tramite mapping puntuale tra il nome di un claim e l'informazione che GovWay cerca di estrarre dal token. Inoltre nel controllo degli accessi, in una autorizzazione per token claims (o per contenuti), è adesso possibile utilizzare la costante "${undefined}" per indicare che un claim non è atteso all'interno del token.

Infine la funzionalità di proxy applicativo è stata resa attivabile anche nelle comunicazioni verso gli authorization server indicati nelle token policy di negoziazione e validazione e nelle attribute authorities.

12.4 Miglioramenti alla funzionalità di Trasformazione

Nota

La funzionalità è stata introdotta nella versione "3.3.6.p1"

Sono state introdotte utility per la conversione da xml a json e viceversa, utilizzabili all'interno delle trasformazioni di protocollo SOAP->REST e REST->SOAP.

Nelle trasformazioni è inoltre adesso possibile:

- accedere agli allegati caricati nelle erogazioni/fruizioni e nelle API;
- indicare valori dinamici, contenenti parti che vengono risolte a runtime, per quanto concerne il codice http di risposta e i content-type utilizzati nelle richieste e nelle risposte.

12.5 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- aggiunto il supporto per le nuove versioni dell'application server "WildFly": 26.x;
- è stata uniformata la gestione dei nodi runtime in un unico file "govway.nodirun.properties".

12.6 Bug Fix

Sono stati risolti i seguenti bug:

- libreria "log4j2" aggiornata alla versione "2.17.1" per risolvere le vulnerabilità "CVE-2021-45105" e "CVE-2021-44832";
- il diagnostico «errore di trasporto, codice XXX», che poteva far pensare a problematiche inerenti il trasporto, è stato modificato in «errore HTTP XXX»;
- le richieste SOAP che contenevano prima della definizione dell'elemento Envelope un commento xml (<!– … –>) contenente al suo interno una definizione Envelope con versione soap differente, venivano interpretati erroneamente con la versione SOAP indicata nella dichiarazione commentata;
- i messaggi SOAP contenenti come rootElement del Body un child element vuoto con localName che iniziava con "Body", venivano erroneamente interpretati come messaggi SOAP con body vuoto;
- per le configurazioni di tipo "cluster dinamico", è stata aggiunta la possibilità di configurare lo schema utilizzato (https/http), la porta e i parametri del connettore https per il servizio proxy, da utilizzare per effettuare il forward della chiamata al servizio check dei nodi;
- una consegna condizionale basata su template, su richieste senza payload (es. HTTP GET), provocava un errore simile al seguente: «Selettore "Template" non supportato per il message-type "BINARY"»;

- l'identificativo di una consegna condizionale o l'id di sessione ottenuto tramite un template viene adesso normalizzato per eliminare spazi o ritorni a capo presenti nella parte iniziale o finale;
- differenziato diagnostico emesso in caso di consegna condizionale configurata per utilizzare un connettore di default, in modo da riconoscere un caso di estrazione della condizione fallita rispetto al caso di mancata individuazione di un connettore tramite la condizione estratta dalla richiesta;
- in caso di utilizzo della funzionalità Load Balancer con algoritmo "SourceIpHash", la transazione terminava in errore in presenza di indirizzi ip per cui il calcolo "hashCode" produceva un numero negativo;
- è stata corretta un'anomalia che si presentava durante una consegna di una notifica asincrona (in presenza di connettori multipli) se il backend restituiva un HTTP Redirect 3XX con header "Location". L'errore che veniva riportato nel diagnostico era simile al seguente: «Errore durante l'aggiornamento dell'header "Location" attraverso la funzione di proxy pass reverse: [getAccordoServizioParteComune]: Parametro non definito».

Per la console di gestione sono stati risolti i seguenti bug:

- non era consentito modificare la modalità di caricamento di una credenziale ssl relativa ad un applicativo;
- è stata rivista la gestione dei connettori multipli in modo che successivamente ad un'operazione di aggiunta o modifica (nome, descrizione, weight ...) si venga riposizionati nella lista dei connettori dove viene selezionato il connettore oggetto della precedente operazione;
- aggiunto controllo di assegnazione univoca di un filtro ad un connettore multiplo, nel caso di consegna condizionale;
- eliminata la possibilità di associare filtri al connettore di default, nel caso di consegna condizionale;
- nella maschera di creazione di una regola specifica per azione/risorsa di un connettore multiplo veniva riportata erroneamente la dicitura "Container" invece di "Contenuto";
- nella consegna con notifiche, se si impostava una configurazione delle risposte accettate con «Consegna Completata» su tutti i codici http e «Consegna Fallita» nel fault, si otteneva una segnalazione errata di configurazione non valida;
- nella maschera di configurazione dei parametri di riconsegna, per le consegne con notifiche, è stata eliminata l'opzione "3xx" nel caso di API SOAP;
- nel menù è adesso possibile utilizzare il tasto destro su tutta la voce e non solo sul testo;
- la funzionalità di verifica connettività riportava un errore non corretto di "Read timed out", invece di "connect timed out", quando veniva verificato un endpoint non raggiungibile ad esempio per problematiche di firewall. L'anomalia è stata risolta aumentando il tempo di attesa dello stato di verifica connettività recuperato dalla console interrogando i nodi run, portando l'attesa da 5 secondi a 60 secondi per default per questo tipo di operazione.
- nella maschera di modifica di un connettore, abilitando la funzionalità "IntegrationManager/MessageBox" veniva erroneamente riportato il checkbox "Modifica Password".

Per la console di monitoraggio sono stati risolti i seguenti bug:

- il download dei report statistici come immagine, non preservava il font visualizzato nella console;
- risolta anomalia presente in tutte le distribuzioni statistiche, eccetto quella temporale e per esiti, dove selezionando il periodo "personalizzato" compariva erroneamente la scelta dell'unità di tempo che non aveva senso per il tipo di distribuzione;
- in caso di registrazione dei contenuti abilitati, se veniva salvata una richiesta contenente un Content-Type Multipart che però nond conteneva effettivamente degli attachments, la consultazione tramite console dei contenuti multipart produceva un errore non atteso e una pagina bianca. Anche la funzionalità di export dei contenuti multipart generava un errore simile.

12.7 Bug Fix 3.3.6.p1

Sono stati effettuati i seguenti interventi migliorativi degli aspetti prestazionali:

- introdotta ottimizzazione nella gestione degli header SOAP: durante la gestione della richiesta o della risposta, se le funzionalità attivate richiedono solamente la gestione del SOAPHeader, viene costruito in memoria la sola rappresentazione DOM dell'header e non dell'intero messaggio mentre il contenuto presente nel body viene trattato in modalità streaming.

Sono stati risolti i seguenti bug:

- la serializzazione di un token malformato causava la mancata scrittura della transazione su database;
- i controlli di consistenza del formato di un content-type, già presenti per le richieste ricevute, sono stati introdotti anche per le risposte in modo da avere una diagnostica conforme per entrambi i casi.

Per la console di gestione sono stati risolti i seguenti bug:

- l'aggiornamento della configurazione ModI di una erogazione o fruizione andava in errore su InternetExplorer 11, per via della presenza di elementi contenenti caratteri che confondevano il visualizzatore di IE;
- il reset puntuale di una API non eliminava dalla cache la definizione dell'interfaccia OpenAPI o Wsdl;
- la funzionalità di download dei certificati server di una Token Policy di Negoziazione generava un errore;
- sono state risolte le seguenti anomalie presenti nella funzionalità di «consegna condizionale»:
  - eliminata la voce "SOAPAction" nell'impostazione del filtro di «consegna condizionale» per API di tipo REST;
  - aggiunta la possibilità di individuare una risorsa REST, nelle regole specifiche di una consegna condizionale, anche per metodo e path oltre che per identificativo;
  - migliorata la pagina di configurazione per la gestione delle notifiche;
  - differenziato diagnostico emesso in caso di «consegna condizionale non applicabile» e impostazione configurata per non inviare la notifica a nessun connettore registrato;
  - in presenza di regole di condizionalità specifiche per determinate azioni, una qualsiasi modifica della configurazione generale del connettore multiplo provocava la perdita delle regole precedentemente configurate.
- sono stati risolte le seguenti anomalie presenti nella funzionalità di «consegna con notifiche»:
  - il connettore indicato come "Connettore Implementa API" presentava accanto al nome l'indicazione di uno stato (abilitato/disabilitato) che non aveva senso poichè non è possibile disabilitarlo;
  - nella lista degli esiti con cui si configura l'invio delle notifiche, è stato escluso il gruppo "Richieste Scartate" essendo richieste non ancora accettate in ingresso;
  - nel connettore associato all'implementazione dell'API non è più possibile definire i criteri di consegna asincrona;
  - tra i connettori selezionabili, in caso di identificazione della condizione fallita o di individuazione del connettore non riuscita, non viene più presentato il connettore che implementa l'API;
  - selezionando un "Connettore che Implementa API" differente da quello iniziale, la maschera dei connettori non riportava correttamente il connettore scelto alla prima posizione dell'elenco.

Sull'installer è stato corretto il seguente bug:

- utilizzando l'installer in modalità avanzata, l'opzione che consente di abilitare le funzionalità di consegna delle notifiche generava artefatti non corretti se l'application server selezionato era Tomcat.

13 Versione 3.3.5

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.5 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.5 utilizzare l'ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.5.p2*
- *Bug Fix 3.3.5.p1*

13.1 Miglioramenti al Profilo di Interoperabilità "ModI"

Sono stati apportati i seguenti miglioramenti:

- *Contemporaneità degli Header "Authorization" e "Agid-JWT-Signature"*: su API REST, per quanto concerne la sicurezza messaggio, è stata aggiunta la possibilità di generare contemporaneamente gli header "Authorization" e "Agid-JWT-Signature" consentendo di agire sulle seguenti configurazioni:
  - è possibile indicare se la contemporaneità vale solo per la richiesta o in entrambi i flussi;
  - aspetti configurabili in fase di produzione del token:
    - generazione dei claim "jti" e "aud" identici o differenti nei 2 token;
    - possibilità di personalizzare ulteriori claim (compresi "sub" e "iss" e "client_id") anche solo in uno dei due header;
  - aspetti configurabili in fase di validazione del token:
    - selezione dell'header da cui estrarre l'identificativo "jti" utilizzato per filtrare le richieste duplicate;
    - indicare un audience atteso differente tra i due token.

  La generazione contemporanea dei 2 header nella richiesta e del solo header "Agid-JWT-Signature" nella risposta diventa il default proposto con un pattern di sicurezza "Integrity".
- *Custom Claims*: è adesso possibile aggiungere nel payload del token JWT, su API REST, ulteriori claims oltre a quelli standard generati da GovWay oltre a poter sovrascrivere i valori di default assegnati ai claims standard (es. "iss", "sub", "client_id") o disabilitarne la generazione;
- *PKCS11*: è stata aggiunta la possibilità di configurare un keystore HSM via "PKCS11" per accedere alla chiave privata da utilizzare per la firma del token di sicurezza; il keystore è associabile all'applicativo che deve firmare il token di richiesta e all'erogazione che deve firmare il token di risposta;
- *Validazione Audience Risposta*: come audience atteso per un token della risposta è adesso possibile configurare un valore statico sulla fruizione, invece di usare il valore associato ad ogni applicativo fruitore;
- *TTL in Validazione*: sulla singola erogazione (configurazione "ModI" della richiesta) o sulla fruizione (configurazione "Modi" della risposta) è adesso possibile configurare un intervallo temporale (in secondi) per cui i token creati precedentemente all'intervallo indicato verranno rifiutati; la nuova opzione consente di sovrascrivere la configurazione di default in cui i token vengono rifiutati se sono stati creati da più di 5 minuti;
- *Token Sicurezza nelle Tracce*: in accordo a quanto richiesto dalle linee guida ModI, è stato modificato il comportamento di default di GovWay il quale non salva più i token di sicurezza scambiati;
- *Multi-Tenant Intra-Dominio con modalità "FileSystem"*: nella registrazione degli applicativi client sul profilo ModI, nella sezione relativa alla sicurezza messaggio, è adesso possibile caricare il certificato anche con la

modalità “filesystem” e “hsm”. Il caricamento del certificato consente la corretta identificazione dell’applicativo su un altro dominio gestito sempre nella stessa installazione govway.

Sono inoltre stati risolti i seguenti problemi:

- la configurazione delle proprietà “org.openspcoop2.protocol.modipa.rest.securityToken.claims.iat.minutes” e “org.openspcoop2.protocol.modipa.soap.securityToken.timestamp.created.minutes” con valori superiori alle 3 settimane venivano ignorati.

Sono stati infine apportati i seguenti miglioramenti alla console di gestione:

- nei criteri di ricerca delle API, delle Erogazioni e delle Fruizioni è stata aggiunta una sezione dedicata al profilo “ModI” che consente di filtrare per pattern di sicurezza canale, sicurezza messaggio, digest della richiesta e informazioni utente. Inoltre nelle Erogazioni/Fruizioni è consentito filtrare per keystore e audience;
- nei criteri di ricerca degli Applicativi è stata aggiunta una sezione dedicata al profilo “ModI” che consente di individuare gli applicativi per i quali è stata abilitata la sicurezza messaggio. La sezione consente anche di filtrare per keystore e identificativo client inserito nel token di sicurezza ModI;
- è stato aggiunta la possibilità di espandere o richiudere le sezioni “Informazioni Utente” e “Contemporaneità Token Authorization e Agid-JWT-Signature” presenti nella configurazione ModI delle Erogazioni o delle Fruizioni.

13.2 Miglioramenti alla Console di Gestione

Sono stati apportati i seguenti miglioramenti alla console di gestione:

- nei filtri di ricerca delle Erogazioni, Fruizioni e Applicativi è stata aggiunta una sezione dedicata ai dati sui connettori tramite la quale è possibile filtrare per tipo di connettore, endpoint, token policy e keystore (solo in https);
- nei filtri di ricerca delle Erogazioni, Fruizioni, Applicativi e Soggetti è stata aggiunta una sezione dedicata alle proprietà che consente di filtrare selezionando una proprietà tra quelle configurate e/o indicandone un valore;
- il criterio di ricerca, nelle Erogazioni e Fruizioni, che consente di filtrare per nome API e soggetto erogatore è stato disaccoppiato in modo da poter effettuare una ricerca composta su entrambi i criteri;
- nei connettori multipli di una erogazione è adesso possibile effettuare ricerche usando come criterio il nome, un filtro e i dati del connettore;
- tra i criteri di ricerca, negli Applicativi e nei Soggetti, è adesso possibile indicare oltre al tipo di credenziale (https/http-basic/principal) anche il valore stesso della credenziale (es. CN del certificato X.509);
- la maschera di gestione del controllo degli accessi di una Erogazione o Fruizione è stata ottimizzata in modo da espandere solamente le sezioni per cui è stata abilitata una funzionalità;
- aggiunto al widget che consente di caricare un file sulla console la possibilità di rimuovere tale scelta;
- tra le informazioni visualizzate per il certificato associato ad un soggetto o ad un applicativo è adesso presente anche il serial number in formato Hex;
- nella maschera di dettaglio di una erogazione o fruizione, in presenza di un connettore di lunghezza superiore ai 150 caratteri viene visualizzata una informazione troncata contenente il suffisso “ . . . ”; lo stesso accorgimento è stato adottato nelle liste degli header HTTP e dei parametri della URL configurabili nelle trasformazioni.

13.3 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti alla console di monitoraggio:

- nelle ricerche che prevedono un intervallo temporale, è stata aggiunta la gestione del timeout, in modo da segnalare all’utente di restringere l’intervallo di ricerca quando i parametri indicati richiedono un tempo eccessivo di elaborazione;

- lo storico delle transazioni, dopo aver presentato i risultati della ricerca, fornisce adesso la possibilità di effettuare una nuova ricerca, con i medesimi criteri, senza dover riaprire il filtro. La nuova ricerca è attivabile attraverso un pulsante di refresh posto accanto alla lente che consente la riapertura del filtro;
- nelle ricerche puntuali per identificativo, un utente amministratore o un utente a cui sono stati associati più profili e/o soggetti può individuare una transazione appartenente ad un profilo o soggetto differente da quello selezionato in alto a destra nella console. L'anomalia viene segnalata all'utente tramite una finestra informativa visualizzata prima di poter accedere ai dettagli della transazione;
- la generazione dei report statistici è stata ottimizzata al fine di ridurre il numero di query effettuate sulla base dati statistica;
- migliorata funzionalità di export CSV tramite la console e l'API di monitoraggio dove sono state aggiunte le informazioni riguardanti: tipo API (rest/soap), gruppo, configurazione CORS, proprietà dell'autenticazione e dell'autorizzazione, attribute authority (attributi), configurazione dell'autorizzazione per contenuti, rate limiting, caching della risposta, trasformazioni, registrazione dei messaggi, metadati e handlers, configurazioni del profilo di interoperabilità ModI e Applicativo Server.

13.4 Nuova funzionalità per il supporto dei device pkcs11

È stata introdotta la possibilità d'uso di Keystore HSM via "PKCS11" per tutte le funzionalità gestite da GovWay: nella configurazione dei connettore "https", nelle funzionalità di sicurezza dei messaggi (WSSecurity, XMLSecurity e JOSE), nelle Token Policy di validazione e negoziazione, nelle Attribute Authority e nella gestione dei token di sicurezza previsti nel Profilo "ModI".

13.5 Nuova funzionalità di registrazione delle Attribute Authority

È adesso possibile censire Attribute Authority che consentono di definire politiche di controllo degli accessi basate sugli attributi.

13.6 Miglioramenti alle funzionalità base dell'API Gateway

- aggiunti i contesti "api-soap", limitata alla gestione di API SOAP e "api-rest" limitata alla gestione di API REST;
- i criteri dinamici, utilizzabili nelle trasformazioni, nei criteri di autorizzazione, nella definizione di endpoint dinamici dei connettori etc, consentono adesso di:
  - accedere alle proprietà definite negli applicativi e nei soggetti;
  - accedere alle proprietà indicate nella configurazione generale di GovWay;
  - leggere variabili di sistema e proprietà della jvm;
- la presenza dei file di configurazione esterna generati dall'installer, non è più necessaria per il corretto avvio di GovWay e possono essere quindi presenti solo nel caso di effettiva necessità di personalizzazione dei valori di default;
- in una installazione di tipo cluster dinamico, viene adesso utilizzato come id del nodo l'identificativo del gruppo;
- aggiunto il tipo di errore "ConnectorNotFound" utilizzato per identificare la casistica in cui non sia stato possibile individuare il connettore che implementa l'API, in configurazioni con connettori multipli (es. con consegna condizionale);
- miglioramenti prestazionali introdotti utilizzando il semaforo java.util.concurrent.Semaphore al posto dei blocchi synchronized.

13.7 Miglioramenti alle API di Gestione e Monitoraggio

Sono stati apportati i seguenti miglioramenti alle API di gestione:

- aggiunta la possibilità di abilitare Attribute Authority e registrare attributi nel Controllo degli Accessi delle erogazioni/fruizioni;
- è adesso possibile registrare Applicativi Server ed associarli ad un connettore;
- è infine possibile registrare connettori differenti da http.

13.8 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- aggiunto il supporto per le nuove versioni dell'application server "WildFly": 24.x e 25.x;
- il timer "Messaggi Inconsistenti" è stato disabilitato per default.

13.9 Bug Fix

Sono stati risolti i seguenti bug:

- Le richieste contenenti credenziali "http-basic", veicolate all'interno dell'header "Authorization" in un formato non corretto, non venivano registrate nello storico delle transazioni. Il client riceveva un codice http di risposta 404 insieme ad una pagina html contenente il codice di errore "GovWay-OP20000-0001".
- Risolto bug che non consentiva di processare SOAP Envelope 1.2 con WSSecurity quando la configurazione prevedeva l'utilizzo di un "role" o l'abilitazione dell'attributo "mustUnderstand".
- Aggiornate librerie bouncy castle alla versione 1.69 per risolvere la problematica che avveniva casualmente dopo aver aggiornato OpenJDK ad una versione superiore alla 11.0.8; la seguente eccezione occorreva di rado su invocazioni in https: «arraycopy: last source index 32 out of bounds for byte[31] at java.base/sun.security.ssl.Alert.createSSLException»
- È stato risolto un problema presente nella libreria xPath disponibile tra le funzioni built-in nelle trasformazioni. Quando si estraevano frammenti di elementi xml, eventuali entity reference presenti nei valori degli elementi estratti venivano erroneamente risolti. La risoluzione poteva comportare una generazione di un frammento xml sintatticamente non valido. Ad esempio se nella trasformazione si utilizzava il frammento xml "<descrizione>Esempio con <30</descrizione>" per comporre un nuovo xml, si otteneva un errore di parsing poichè l'entity reference presente nella descrizione "<30" veniva risolta con il carattere "<" comportando quindi la generazione di un elemento xml malformato: "<descrizione>Esempio con <30</descrizione>".
- La risoluzione dinamica dell'endpoint dei connettori http/https e dei path sul connettore "file" non consentiva di utilizzare i valori di header HTTP e/o parametri della url ricevuti, se questi non venivano serializzati verso il backend. È stata inoltre aggiunta la possibilità di utilizzare una espressione regolare applicata all'url di invocazione, nella definizione dell'endpoint di un connettore.
- Le richieste ricevute prima del completamento dello startup di GovWay, provocano una inizializzazione non corretta degli handler. Il problema è stato risolto facendo in modo che le richieste ricevute prima dello startup rimangano in attesa che il gateway sia completamente inizializzato prima di essere processate.
- La registrazione della transazione falliva, con l'errore riportato di seguito, se l'erogazione era configurata con diversi connettori multipli in cui la somma dei nomi superava i 2000 caratteri: org.openspcoop2.generic_project.exception.ServiceException: ERRORE: il valore è troppo lungo per il tipo character varying(2000)
- Migliorati log emessi in casi di errore avvenuti durante l'aggiornamento dell'esito della consegna di un connettore multiplo o durante l'aggiornamento della transazione che raggruppa le varie consegne multiple.
- Su API REST, se in un handler si aggiungeva alle proprietà del trasporto (direttamente e non tramite i metodi "forceHeader") un header http che non risiedeva in black list si

otteneva un errore simile al seguente: «java.util.ConcurrentModificationException: null at java.util.ArrayList$Itr.checkForComodification(ArrayList.java:1042)...»

- In una configurazione senza connettori multipli, dove era stato abilitato il salvataggio dei messaggi su MessageBox, in occasione dell'eliminazione di un messaggio via Integration Manager o per scadenza naturale, si otteneva un errore simile al seguente: ERROR <23-09-2021 16:03:00> [id:4eccbf4e-181a-11ec-b5a0-00505686878f][sa:gw_SOGGETTO/gw_SERVIZIO/v1][null] "aggiornaInformazioneConsegnaTerminata" non riuscta. Tutti gli intervalli di update non hanno comportato un aggiornamento della transazione.
- Le operazioni "getAllMessageIds", esposte dal servizio MessageBox via IntegrationManager, che non prevedono tra i parametri un limite massimo di id ritornati utilizzano adesso il limite di default di sistema (1000) per evitare OutOfMemory in presenza di una mole di messaggi considerevole.

Per quanto concerne il Profilo "Fatturazione Elettronica" sono stati risolti i seguenti bug:

- Nel caso di fatture P7M, nel formato PEM, contenenti i prefissi —-BEGIN e —-END il software non era in grado di parsare la fattura se si abilitavano i controlli che lo richiedevano (ad esempio abilitando la proprietà "org.openspcoop2.protocol.sdi.accesso.campiFattura.enable" nel file esterno "sdi_local.properties".

Per quanto concerne il Profilo "SPCoop" sono stati risolti i seguenti bug:

- Durante il restyling grafico delle liste accessibili dal menù principale, relativamente agli Applicativi e realizzato con il rilascio della versione 3.3.3, è venuta meno la possibilità di configurare i connettori relativi alla "Risposta Asincrona" richiesti dai profili asincroni. La problematica è stata risolta.
- In caso di ricezione di una busta con un soggetto mittente censito e registrato con delle credenziali differenti da quelle presenti nella richiesta, l'autenticazione non falliva se le credenziali non corrispondevano a nessun altro soggetto censito.

Per la console di gestione sono stati risolti i seguenti bug:

- Caricando un'interfaccia OpenAPI 3 in cui gli elementi principali (openapi, info, servers, paths ...) non erano posizionati sulla prima colonna, si otteneva il seguente errore (https://github.com/link-it/govway/issues/83): [Interfaccia OpenAPI 3] Documento non valido: org.openspcoop2.utils.rest.ProcessingException: Parse failed: mapping values are not allowed here in "reader", line 2, column 9: info: ^ at [Source: (StringReader); line: 2, column: 9]
- Utilizzando il browser IE11 quando si selezionava un filtro di ricerca, al momento del reload della pagina, l'applicazione si bloccava. La console del browser indicava il seguente errore: «Errore: L'oggetto non supporta la proprietà o il metodo "endsWith"».
- Risolto bug che non consentiva l'associazione di ruoli ad un applicativo server in cui era stata abilitata l'opzione "Utilizzabile come Client".
- La console terminava con un errore non atteso in caso di caricamento di certificati, sugli applicativi o sui soggetti, che non possedevano il campo "CN" nel subject o nell'issuer.
- La console non consentiva di aggiungere credenziali (es. un certificato x.509) ad un soggetto creato precedentemente senza.
- Il dialog informativo, che riporta le credenziali http-basic o api-key, non visualizzava correttamente credenziali che possedevano caratteri particolari come i doppi apici.
- La creazione di un nuovo gruppo, in un'erogazione, non andava a buon fine se durante la creazione veniva scelto di ereditare le configurazioni di un gruppo non predefinito, configurato per utilizzare un connettore ridefinito con consegna multipla.
- La funzionalità "Importa" non gestiva correttamente l'importazione di fruizioni in cui era stato ridefinito il connettore, per specifiche azioni/risorse, attraverso l'utilizzo della tipologia "https".
- L'eliminazione di un utente (o la modifica del permesso "S") comportava una riassegnazione degli oggetti appartenenti all'utente nella quale venivano erroneamente eliminate eventuali proprietà o credenziali presenti

nei soggetti aggiornati. La problematica è stata risolta, e l'attività di riassegnamento è stata eliminata se la visibilità degli oggetti risulta globale per tutte le utenze di gestione (comportamento di default).

Per la console di monitoraggio sono stati risolti i seguenti bug:

- gli applicativi server, utilizzabili anche come client, non erano selezionabili tra la lista degli applicativi fornita dalla tipologia di ricerca per applicativo;
- sono stati risolti i seguenti problemi relativamente alla funzionalità di export CSV:
  - nella colonna delle azioni/risorse non venivano riportate le risorse per le API di tipo REST;
  - risolto problema di conflitto di nome tra il nome dell'API e il nome della fruizione/erogazione dove per entrambi la colonna si chiamava con l'header "API";
  - risolto problema di ordine differente tra header e valori nelle fruizioni per quanto concerne i parametri dell'autenticazione dove venivano fornite informazioni errate;
  - la funzionalità di esportazione tramite la voce "seleziona tutti" non considerava gli eventuali filtri impostati su API e Tag;
  - non venivano riportati i dati del connettore se questo veniva ridefinito in un gruppo di una fruizione.

Per le API di gestione sono stati risolti i seguenti bug:

- il download di specifiche semiformali non funzionava e veniva generato un errore «404 Not Found» anche per specifiche esistenti sull'API;
- se tramite console veniva registrata una specifica semiformale in Linguaggio Naturale, la raccolta degli allegati via api terminava con errore;
- non era consentito allegare documenti i cui nomi contenevano spazi o iniziavano con un numero.

13.10 Bug Fix 3.3.5.p1

Sono stati effettuati i seguenti interventi migliorativi degli aspetti prestazionali:

- gli oggetti java.util.Hashtable e java.util.Vector sono stati sostituiti con strutture più efficienti;
- sostituiti i blocchi synchronized con l'uso di java.util.concurrent.Semaphore, relativamente alla negoziazione di connessioni e alla funzionalità di filtro dei duplicati;
- gli oggetti restituiti dalle factory dei profili di interoperabilità che contengono solamente configurazioni statiche, vengono adesso istanziate solamente una volta all'avvio del gateway;
- il recupero dell'identificativo della PrimaryKey di una nuova entry, avviene adesso, anche su postgresql, utilizzando la funzionalità "getGeneratedKeys" fornita dai driver jdbc postgresql con versione superiore alla 9.4;
- il provider "Bouncy Castle" viene adesso utilizzato per gestire i certificati (java.security.cert.CertificateFactory e java.security.cert.CertPathValidator) e per calcolare il digest di un messaggio (java.security.MessageDigest).

Sono stati risolti i seguenti bug:

- libreria "log4j2" aggiornata alla versione "2.15.0" per risolvere la vulnerabilità "CVE-2021-44228";
- nel profilo di interoperabilità "ModI" con API REST configurata con pattern "Integrity", la validazione degli header firmati non rilevava, in presenza di molteplici header HTTP con lo stesso nome, l'esistenza di un valore ulteriore rispetto a tutti quelli definiti all'interno del claim "signed_headers";
- se venivano ricevuti messaggi SOAP che iniziavano con il carattere ">" l'anomalia veniva correttamente segnalata al client, ma nel log veniva emessa un'eccezione relativa ad un caso non gestito (NullPointerException);
- aggiunta gestione del charset nella classe "OpenSPCoop2MessageSoapStreamReader" utilizzata per leggere le informazioni SOAP in streaming;

- risolto bug di serializzazione di un messaggio SOAP With Attachments, che si presentava quando il messaggio veniva acceduto per funzionalità read-only (es. correlazione applicativa), che provocava la generazione di un content-type con un mimepart differente da quello effettivamente serializzato;
- la normalizzazione dell'input stream "vuoto", viene adesso gestita tramite l'utilizzo di un buffer di lunghezza 2 compatibile con il charset "UTF-16";
- corretti problemi presenti sulla funzionalità "follow-redirect" che non consentivano di ottenere una risposta applicativa una volta seguito il flusso di redirect;
- risolti problemi presenti nella funzione di merge degli schemi OpenAPI:
  - l'import di file i cui nomi erano uno inclusivo dell'altro causavano una serializzazione di un path scorretto;
  - la serializzazione YAML dell'interfaccia generava alcune enumeration (es. in security schema) con i valori maiuscoli invece che minuscoli come atteso dalla specifica OpenAPI;
- in caso l'immagine del controllo del traffico, salvata durante uno shutdown dell'A.S., risultava corrotta, il gateway non ripartiva; è stata migliorata la gestione facendo in modo che il gateway riparta con stato iniziale vuoto e segnali l'anomalia su file di log.
- in presenza di richieste malformate che causavano la generazione di un diagnostico contenente il carattere "u0000", su ambienti con database di tipo Postgresql si otteneva un errore simile al seguente durante il tracciamento: Caused by: org.postgresql.util.PSQLException: ERROR: invalid byte sequence for encoding «UTF8»: 0x0.

È stato inoltre migliorato il sistema di log, relativamente alle seguenti casistiche:

- aggiunto diagnostico che evidenzia la ricezione di richieste o risposte con un charset differente da quello definito per default nel prodotto (qualsiasi charset per messaggi REST e solamente il charset UTF-8 per messaggi SOAP);
- aggiunta verifica che le connessioni prelevate dal datasource siano con autocommit disabilitato e con livello di serializzazione atteso (ReadCommitted);
- il file di log "govway_transazioni_slow.log" è stato arricchito con le seguenti informazioni:
  - dettaglio sulla fase in cui viene speso il tempo nella costruzione delle informazioni da salvare in fase di scrittura della transazione;
  - informazioni relative alla gestione del rate limiting applicabile in seguito al completamento della richiesta;
- migliorati i log di eventuali errori emersi durante la gestione degli handler.

Per la console di gestione sono stati risolti i seguenti bug:

- una connessione al database veniva acceduta dalla console anche per gestire risorse statiche non protette (es. js/autocomplete.js o css/linkit-base.css);
- corretto bug presente nella funzionalità di export e import di un'API che, in alcune configurazioni particolari, poteva non preservare la configurazione del profilo di collaborazione, del filtro duplicati, del riferimento alla richiesta e dell'id di conversazione;
- la ricerca delle operazioni effettuate sulla console, tramite la funzionalità di "Auditing", avviene adesso tramite criteri «contains case insensitive». Inoltre nella lista delle operazioni individuate è stata aggiunta la data di esecuzione dell'operazione.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- le pagine xhtml presentavano erroneamente campi "date" con un time zone "forzato" a "Europe/Rome";
- aggiunta la possibilità di selezionare in blocco gli elementi visualizzati nello storico delle transazioni;
- nell'export CSV delle transazioni sono stati aggiunte le seguenti informazioni mancanti:
  - richiedente;

  - dettaglio dell'errore o dell'anomalia;
  - informazioni principali estratte dal token: subject, issuer, clientId, username ed indirizzo eMail.

Sull'installer è stato corretto il seguente bug:

- nei binari prodotti dall'installer, il timer per la consegna dei messaggi presi in carico viene adesso disabilitato essendo la funzionalità considerata "sperimentale".

13.11 Bug Fix 3.3.5.p2

Sono stati risolti i seguenti bug:

- libreria "log4j2" aggiornata alla versione "2.16.0" per risolvere la vulnerabilità "CVE-2021-45046";
- nella console di gestione, se configurata in Load Balancing per gestire molteplici nodi, l'accesso alla sezione "Runtime" causava delle invocazioni verso i nodi gestiti ancor prima di averne selezionato qualcuno o aver richiesto operazioni di gestione (es. svuota cache).

14 Versione 3.3.4

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.4 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

Nota

Per la versione 3.3.4 utilizzare l'ultima patch version che risolve bug importanti descritti nelle sezioni:

- *Bug Fix 3.3.4.p2*
- *Bug Fix 3.3.4.p1*

14.1 Miglioramenti alle funzionalità base dell'API Gateway

Sono stati introdotti significativi miglioramenti prestazionali:

- la gestione dei messaggi di API SOAP è adesso equivalente a quella delle API REST: se non sono attive funzionalità che richiedono l'accesso al contenuto del messaggio, la gestione avviene in "Passthrough", senza introdurre nessun overhead nella trasmissione;
- per API SOAP, anche se viene richiesta la costruzione in memoria dell'oggetto DOM che rappresenta il messaggio, al backend verrà inoltrata esattamente la richiesta originale ricevuta dal client, preventivamente bufferizzata, se le funzionalità che hanno avuto bisogno di accedere all'oggetto DOM non lo hanno modificato;
- la connessione verso il database "runtime" viene adesso negoziata solamente se richiesta da funzionalità che ne necessitano;
- i connettori http preservano il "keep-alive";
- la SSLSocketFactory istanziata per i connettori https viene mantenuta in una apposita cache;
- le chiavi private accedute per funzionalità di firma e decrifratura vengono salvate in cache assieme ai keystore;
- sono adesso gestiti i seguenti generatori di UUID:
  - generatore uuid v4 che utilizza SecureRandom;
  - generatore uuid v1 con mac address configurabile (se non fornito viene utilizzato uno tra quelli appartenenti alle schede di rete disponibili sulla macchina);
  - per tutti i generatori è adesso possibile attivarne una versione "ThreadLocal";

  - il default del prodotto è stato modificato da UUIDv4 (java.util.UUID senza ThreadLocal) a UUIDv1 (com.fasterxml.uuid.impl.TimeBasedGenerator con ThreadLocal).

È stata migliorata la generazione delle informazioni statistiche:

- i criteri di generazione dei report statistici utilizzano adesso un'identificazione dell'intervallo temporale inclusivo del giorno di interesse del report (es. >=2021-02-10 00:00:00.000), soluzione che risulta maggiormente efficiente in presenza di partizionamento giornaliero delle transazioni;
- l'algoritmo di generazione delle statistiche è stato completamente rivisto:
  - le informazioni statistiche, comprensive di latenze, vengono adesso calcolate tramite un'unica query SQL in modo da essere maggiormente efficiente in presenza di grande mole di dati;
  - l'aggiornamento dell'intervallo corrente è adesso transazionale;
  - aggiunto refresh della connessione ogni 300 secondi.

Infine sono stati apportati i seguenti ulteriori miglioramenti:

- per API di tipo REST è stato arricchito il diagnostico di consegna, in presenza di codice di risposta http 3xx, per registrare anche il valore dell'header http "Location";
- la funzionalità "ID Collaborazione" è stata ridenominata in "ID Conversazione" e, se abilitata, l'header HTTP GovWay-Conversion-ID viene adesso sempre generato, anche nella richiesta capostipite della conversazione dove viene valorizzato con l'id di transazione della prima richiesta;
- aggiunti timeout per la lettura dello stream di dati relativo alla richiesta e alla risposta;
- aggiunta la possibilità di configurare ulteriori Content-Type associabili a richieste SOAP 1.2 (per default viene accettato solo "application/soap+xml");
- l'autenticazione "https", attivabile nel controllo degli accessi delle erogazioni e fruizioni, effettua adesso anche la verifica della validità temporale del certificato ricevuto;
- la lettura delle proprietà di configurazione dai file locali (es. govway_local.properties) è stata rivista per risolvere le variabili indicate nei file anche come variabile di sistema oltre che come variabili java;
- è stato rivisto il diagnostico relativo ad una richiesta duplicata al fine di fornire un messaggio più generico rispetto a quello precedente specifico per il profilo SPCoop;
- è stato modificata la configurazione di default del CORS per generare un header "Access-Control-Max-Age" valorizzato con "28800" (8 ore).

14.2 Miglioramenti al Profilo di Interoperabilità "ModI"

Sono stati apportati i seguenti miglioramenti:

- adeguamenti alla terminologia utilizzata dalla specifica finale del Modello di Interoperabilità:
  - ridenominato profilo "ModI PA" in "ModI";
  - adeguata terminologia da "profilo" a "pattern" per i pattern di Interazione, di Sicurezza Canale e di Sicurezza Messaggio;
- per API di tipo SOAP è adesso possibile attivare anche la firma degli allegati utilizzando il pattern di sicurezza "INTEGRITY_SOAP_01";
- è stato abilitato per default il controllo che rifiuta token scaduti (default 5 minuti): la verifica viene effettuata verificando la data presente nel claim "iat" del JWT per API REST o nell'elemento "Create" del WSSecurity Timestamp per API SOAP;
- nella configurazione relativa alla sicurezza messaggio ModI di un applicativo di dominio interno è adesso possibile configurare il keystore per la firma indicandolo anche tramite un path su filesystem;

- aggiunta la possibilità, su API SOAP, di configurare ulteriori header soap da aggiungere agli elementi inclusi nella firma (la configurazione è disponibile utilizzando la console in modalità avanzata);
- tra le informazioni ModI presenti nella traccia vengono adesso riportati anche gli header soap firmati.

Sono inoltre stati risolti i seguenti problemi:

- nei Pattern di Interazione la validazione dei codici http su API REST bloccanti e non bloccanti viene adesso effettuata esclusivamente su codici di risposta che rientrano nelle casistiche 2xx o 3xx;
- nella validazione di un token JWT Modi per API REST con pattern INTEGRITY_REST_01 non veniva verificato che tra gli header firmati vi fosse obbligatoriamente l'header HTTP "Digest" se la richiesta presentava un payload;
- la funzionalità "Verifica Audience", della sezione Sicurezza Messaggio Risposta di una fruizione, veniva ignorata e la validazione effettuata anche se l'opzione era disabilitata.

14.3 Miglioramenti alla Console di Gestione

Sono stati apportati i seguenti miglioramenti alla console di gestione:

- aggiunta la possibilità di modificare il soggetto erogatore nelle fruizioni e nelle erogazioni (https://github.com/link-it/govway/issues/63 e https://github.com/link-it/govway/issues/64);
- aggiunto supporto per il caricamento di file multipli nelle schermate di aggiunta degli allegati nelle API e nelle Erogazioni e Fruizioni;
- aggiunta la possibilità di filtrare per API sulle erogazioni e fruizioni;
- nellla sezione "Controllo degli Accessi":
  - l'autenticazione è adesso modificabile solamente se non sono stati indicati puntualmente degli applicativi o dei soggetti nel criterio di autorizzazione «per richiedente»;
  - se viene selezionata una autenticazione differente da quella precedentemente impostata, gli eventuali link "Applicativi" e "Soggetti" presenti nella sezione «autorizzazione per richiedente» non vengono più visualizzati fino a che non viene effettuato il salvataggio del nuovo tipo di autenticazione
- nella configurazione dei gruppi di risorse di una erogazione o fruizione è adesso possibile filtrare per metodo http e path;
- aggiunta la possibilità di registrare proprietà generiche sui soggetti e sugli applicativi;
- la funzionalità "In uso" per gli applicativi e per i soggetti mostra adesso anche per quali erogazioni e fruizioni sono compatibili rispetto al criterio di autorizzazione per ruoli impostato nel controllo degli accessi;
- durante la creazione di una erogazione o fruizione fino a che non viene selezionata una API non sono visualizzate le sezioni "Controllo Accessi", "Connettore" e "ModI";
- il parametro "Access-Control-Max-Age", per le richieste Preflight CORS, è adesso configurabile dalla console senza dover accedere alla modalità avanzata;
- aggiunta funzionalità di filtro per Tag nelle policy di Rate Limiting a livello di configurazione globale;
- nella configurazione del tracciamento, dove è possibile indicare gli esiti delle transazioni da registrare, viene adesso gestita tramite una voce dedicata l'esito relativo alla violazione di una policy di RateLimiting;
- nelle maschere di configurazione dei connettori:
  - è stata aggiunta la nota «Indicazione in millisecondi (ms)» nei campo relativi alla sezione «ridefinisci tempi di risposta»;
  - nella maschera di configurazione di un connettore multiplo vengono adesso proposti i valori di default nella sezione «ridefinisci tempi di risposta», se abilitata
- aggiunta funzionalità di export/import per:

  - Token Policy
  - Policy di Rate Limiting del Controllo del Traffico
  - Regole di Proxy Pass
- è adesso possibile attivare una scadenza temporale alle password associate alle utenze delle console.

14.4 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti alla console di monitoraggio:

- nella ricerca avanzata dello storico delle transazioni, se viene effettuata una ricerca che comprende qualsiasi profilo, le transazioni riportate nell'elenco visualizzano adesso anche il profilo di appartenenza;
- tra i criteri di generazione delle statistiche è adesso possibile filtrare per identificativo del cluster e del canale;
- corretto formato delle label dell'asse Y dei grafici: aggiunto separatore delle migliaia per una migliore visualizzazione delle label.

14.5 Miglioramenti alla funzionalità di Registrazione dei Messaggi

È stata rivista la registrazione dei messaggi in ingresso e in uscita per salvare direttamente lo stream dei dati.

L'analisi di eventuali strutture multipart viene demandata alla console di monitoraggio.

14.6 Miglioramenti alla funzionalità di Autenticazione degli Applicativi e dei Soggetti

È adesso possibile associare più di un certificato X.509 agli applicativi e ai soggetti in modo da poter gestire i periodi di transizione relativi all'aggiornamento di un certificato.

Modificata la configurazione di default, proposta durante la registrazione di un nuovo applicativo o soggetto, in modo da prevedere l'identificazione tramite confronto tra certificato caricato e certificato fornito durante l'autenticazione. È sempre possibile configurare la modalità in cui verrà controllato solamente che i DN del Subject e dell'Issuer siano identici.

14.7 Miglioramenti alla funzionalità di RateLimiting

Introdotta nuova metrica che consente di indicare la dimensione massima di un messaggio di richiesta o di risposta

14.8 Miglioramenti alla funzionalità di Correlazione Applicativa

È adesso possibile definire regole di correlazione applicativa che contengono nel campo "Elemento" il metodo http e il path di una risorsa, nel caso di API REST. In questo modo l'applicazione della regola avverrà solamente sulla risorsa dell'API che possiede il metodo e il path indicato.

Inoltre, sia tramite la console che tramite le API di monitoraggio, è stata aggiunta la possibilità di cercare transazioni fornendo come criterio di ricerca il solo identificativo applicativo. La funzionalità già esistente che consentiva di effettuare la ricerca tramite dei criteri più articolati (es. intervallo temporale, modalità di ricerca "contains" e "case-insensitive") rimane disponibile come "ricerca avanzata" dell'identificativo applicativo.

14.9 Miglioramenti alla funzionalità di Identificazione dell'Azione

La modalità di identificazione dell'azione "SOAPAction" è stata rivista:

- viene prima ricercata un'azione, all'interno dell'interfaccia dell'API invocata, contenente un soap binding con la SOAPAction presente nella richiesta (nuova feature);

- se la prima ricerca non va a buon fine viene verificato se il valore presente nella SOAPAction della richiesta corrisponde al nome di un'azione registrata sull'API (precedente comportamento).

14.10 Miglioramenti alla funzionalità di Negoziazione Token

Nota

La funzionalità è stata introdotta nella versione "3.3.4.p2"

È stata aggiunto il supporto per la negoziazione di token tramite la modalità di autenticazione descritta nella sezione 2.2 del RFC 7523 (https://datatracker.ietf.org/doc/html/rfc7523#section-2.2). È possibile configurare la policy per firmare l'asserzione JWT di autenticazione tramite un certificato X.509 o tramite un client secret.

È stata inoltre aggiunta la possibilità di configurare l'autenticazione server di una token policy per accettare qualsiasi certificato.

14.11 Miglioramenti alle API di Gestione e Monitoraggio

Sono stati apportati i seguenti miglioramenti alle API di gestione:

- aggiunta la possibilità di effettuare configurazione con il Profilo "ModI";
- è adesso possibile ottenere la lista degli oggetti presenti nel registro relativamente a qualsiasi profilo e/o soggetto;
- aggiunta la possibilità di filtrare per API sulle erogazioni e fruizioni;
- il parametro "Access-Control-Max-Age", per le richieste Preflight CORS, è adesso configurabile via API.

Sono stati apportati i seguenti miglioramenti alle API di monitoraggio:

- aggiunta la possibilità di ottenere report statistici filtrando per l'identificativo del cluster;
- è adesso possibile ricercare transazioni oltre che per IdMessaggio anche per id di conversazione o di riferimento alla richiesta.

14.12 Nuova funzionalità di registrazione dei Plugins

Aggiunta la possibilità di registrare, tramite la console di gestione, le classi dei plugin che implementano le funzionalità personalizzabili: autenticazione, autorizzazione, autorizzazione dei contenuti, connettori, rate-limiting, header di integrazione e handlers. Successivamente alla registrazione, il plugin risulta selezionabile nella configurazione dell'erogazione o della fruizione relativa alla funzionalità che il plugin implementa.

È inoltre possibile caricare tramite la console gli archivi jar che implementano le personalizzazioni; gli archivi caricati risultano subito disponibili al gateway essendo stato implementato un meccanismo di class loader dedicato a tali componenti.

14.13 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- aggiunto il supporto per le nuove versione dell'application server "WildFly" 22.x e 23.x;
- gli indici "Full", generabili utilizzando l'installer in modalità avanzata, vengono adesso generati anche per i tipi di database hsql e sqlserver;
- aggiunta all'installer in modalità avanzata, opzione per la configurazione del software in modalità "cluster dinamico", indicata per le installazioni in cloud.

14.14 Bug Fix

Sono stati risolti i seguenti bug:

- In presenza di parametri della query con lo stesso nome, veniva inoltrato all'API di backend solamente il primo. Analogo problema si verificava con gli header http (es. Set-Cookie).
- Le richieste contenenti Content-Type strutturalmente non corretti non venivano registrate nello storico delle transazioni e ai client veniva restituito una pagina html su codice di risposta 404. La problematica è stata risolta: tutte le richieste vengono adesso registrate e ai client viene ritornato un errore "Bad Request" conforme alla specifica REST o SOAP dell'API invocata.
- Risolte le seguenti anomalie presenti sulla validazione tramite OpenAPI 3:
  - se il Content-Type di una risposta veniva definito tramite placeholders */*, la validazione terminava con un errore «Content-Type non supportato»;
  - vengono adesso supportate le varie modalità di serializzazione dei parametri della query e degli header HTTP descritte in "https://swagger.io/docs/specification/serialization/";
  - se gli oggetti erano definito nell'OpenAPI con "nullable: true" e venivano quindi serializzati con il valore null la validazione sollevava erroneamente un problema di mancanza degli elementi obbligatori definiti per l'oggetto;
  - corretti i problemi che causavano una errata validazione delle interfacce OpenAPI 3.0.x contenenti il claim "allowEmptyValue" o security schema vuoti («security»: [{}]);
  - se uno degli oggetti indicati nell'enumerazione oneOf di un discriminator veniva dichiarato tramite costrutto "allOf" la validazione falliva erroneamente indicando un errore simile al seguente: «components.schemas.xxx.properties.xxx.discriminator: The discriminator "nomeDiscriminator" is not required or not a property of the allOf schemas (code: 133)».
- Risolte le seguenti anomalie presenti sul Rate Limiting:
  - durante la valutazione di una policy configurata per essere applicata solamente in presenza di degrado prestazionale, si verificava un errore inatteso dovuto ad un accesso fallito alla base dati statistica a causa di una inizializzazione errata;
  - in presenza di una policy con filtro basato su chiave estratta dal contenuto, la valutazione della policy terminava con errore, invece di essere semplicemente filtrata, nel caso la richiesta non contenesse un payload http (es. GET);
  - le politiche basate sulle richieste simultanee potevano bloccare un numero maggiore di richieste rispetto a quelle permesse;
  - risolto problema sull'aggiornamento dell'intervallo temporale corrente che in alcuni casi provocava una mancata generazione dell'header X-*-Reset;
  - le politiche con metrica "Numero Richieste Completate con Successo", "Numero Richieste Fallite" e "Numero Fault Applicativi" consentivano erroneamente il transito della N+1 richiesta, quando il limite era N;
  - utilizzando la metrica "Numero Richieste Fallite" o "Fault Applicativi" non veniva generato l'header HTTP "*-Limit" che segnala il numero massimo di richieste effettuabili;
  - con la metrica "Numero Richieste Completate con successo" venivano erroneamente conteggiate anche le richieste terminate con esito "Fault Applicativo";
  - sono stati riviste le pagine html generate insieme al codice HTTP 429 su API SOAP, in seguito a errori "Too Many Requests" e "Limit Exceeded"; è stato aggiunto l'header http "GovWay-Transaction-ErrorType" mancante;

  - risolta anomalia che poteva causare un deadlock nell'utilizzo delle connessioni se in una API veniva definita una policy applicabile solamente in presenza di degrado prestazionale.

- Risolto problema che si presentava durante la negoziazione di un token, se l'url dell'AuthorizationServer ritornava un codice http 3xx con header Location. L'errore segnalato nei diagnostici era il seguente: «Errore durante l'aggiornamento dell'header "Location" attraverso la funzione di proxy pass reverse: [getAccordoServizioParteComune]: Parametro non definito»
- La chiave utilizzata per l'aggiunta in cache di un'autorizzazione non teneva conto del token OAuth2.
- Su API SOAP, in alcuni casi di errore, non veniva individuato correttamente l'esito della transazione associando un errato esito "SOAPFault".
- Risolti problemi di serializzazione relativo all'elemento "details", per le fruizioni di API SOAP, in caso di errore generato tramite handler di ingresso.
- Su una installazione con più nodi in load balancer sono stati risolti i seguenti errori:
  - se arrivavano nel medesimo istante, ma su due nodi differenti, due richieste che presentano la stessa credenziale fino ad ora mai ricevuta sul gateway: «ERROR org.openspcoop2.generic_project.exception.ServiceException: Create not completed: insertAndReturnGeneratedKey failed: ORA-00001: violata restrizione di unicità (GOVWAY_TRAC.UNIQUE_CREDENZIALE_MITTENTE_1)»
  - al primo avvio del gateway, dopo l'installazione, se nell'avvio venivano fatti partire simultaneamente più nodi (installazione in cluster) avveniva un errore simile al seguente «org.openspcoop2.core.registry.driver.DriverRegistroServiziException: [DriverRegistroServiziDB::createAccordoServizioParteComune] SQLException [ERROR: duplicate key value violates unique constraint «unique_accordi_1»
- La funzione di filtro delle richieste duplicate poteva far scaturire un deadlock tra le richieste su architetture dove il tracciamento fosse dispiegato su un database differente da quello di runtime.
- È stata risolta una problematica relativa alla funzionalità "Riferimento della Richiesta" dove non veniva associata alla traccia l'identificativo correlato.
- Risolto Bug sul Timer "FileSystem Recovery" che tentava di ripristinare le transazioni aggiungendo un evento che causava l'errore: «il valore è troppo lungo per il tipo character varying(20)»
- Invocazioni GET che richiedevano un wsdl tramite il parametro "?wsdl" potevano causare un OutOfMemory sul Gateway. L'anomalia risiedeva nel fatto che tutte le richieste venivano registrate in memoria ma mai rilasciate e continuavano a crescere nel tempo. Si poteva individuare l'anomalia tramite la console di gestione, accedendo alla sezione "Runtime - Transazioni Attive", dove veniva riportata una crescita costante del numero di transazioni.
- Corretta anomalia che si verificava durante l'identificazione dell'esito in presenza di richieste parallele ricevute non appena veniva avviato il gateway: «Identificazione stato non riuscita: null … Caused by: java.util.ConcurrentModificationException»
- Modificato livello di serverità da ERROR a WARN per l'evento registrato nel file di log govway_core.log relativo all'invocazione di una API per la quale non esiste una specifica di interfaccia.
- Corretto problema presente su application server wildfly che non consentiva di accedere ai parametri di una richiesta "application/x-www-form-urlencoded" se i parametri erano un numero maggiore di uno.
- Risolto un problema di rilascio dell'input stream della risposta che si verificava se la richiesta presentava il medesimo identificativo; l'errore generato riportava il messaggio "stream is closed".
- La consegna con notifiche non propagava l'identità del servizio applicativo fruitore.
- Nella funzionalità di presa in carico dei messaggi (attivabile con una installazione in modalità avanzata):

  - i comandi che si occupavano di aggiornare lo stato della transazione sono stati ricondotti ad un unico comando di UPDATE con CASE e condizione di BEETWEEN per ottimizzare le query in presenza di partizioni,
  - i comandi che si occupano di selezionare i messaggi da consegnare sono stati rivisti al fine di smistare normalmente solamente i nuovi messaggi e ogni X secondi di provare a rispedire eventuali messaggio andati precedentemente in errore. È stata inoltre aggiunta una query che calcola, in caso di rispedizione dei messaggi in errore, la data del più vecchio messaggio che può essere rispedito.
- Rivisto il servizio di IntegrationManager (attivabile con una installazione in modalità avanzata): per:
  - ritornare identificativi, tramite il metodo "getAllIdMessages", che contengano anche la data (formato: YYYYMMDDHHMMSS.sss@UUID);
  - sono state ricondotte ad un'unica query il recupero di un messaggio tramite il metodo "getMessage";
  - aggiunto esito "Disponibile in MessageBox" ricercabile tramite la console di monitoraggio;
  - nel dettaglio di ogni transazione sono adesso disponibili le informazioni relative allo scaricamento e all'eliminazione;
  - sono infine state migliorate le query in generale di accesso al messaggio e di eliminazione e in ogni comando è stato aggiunta la condizione BEETWEEN per ottimizzare le query in presenza di partizioni.

Per la console di gestione sono stati risolti i seguenti bug:

- La creazione o l'aggiornamento di una API tramite il caricamento dell'interfaccia OpenAPI 3.x non rilevava alcuni tipi di errore presenti nell'interfaccia (es. negli schema) e terminava con la creazione dell'API correttamente senza segnalarli. Il problema è stato risolto, e adesso vengono segnalati anche eventuali anomalie non bloccanti (es. url scorrette definite nella sezione info).
- L'aggiornamento dell'interfaccia di una API sovrascriveva eventuali impostazioni "ModI" definite a livello della singola operazione aggiornata.
- Il semaforo che visualizza lo stato di una erogazione o fruizione considerava lo stato del gruppo "Predefinito" anche se tutte le azioni o risorse erano state riassegnate in altri gruppi. Il problema è stato risolto.
- Le policy di RateLimiting associate ad un'erogazione si perdevano se si effettuava la modifica del nome del soggetto erogatore.
- In presenza di una policy di RateLimiting con raggruppamento per risorsa/azione, se veniva abilitato un filtro sulla policy, l'impostazione del raggruppamento spariva.
- L'aggiornamento del nome di un soggetto generava un errore inatteso se esistevano erogazioni o fruizioni interessate dal soggetto modificato contenenti trasformazioni configurate con applicativi o soggetti nei criteri di applicabilità.
- L'aggiornamento del nome di un soggetto non veniva correttamente propagato nelle liste dei soggetti presenti tra i criteri di applicabilità delle trasformazioni attivate su erogazioni o fruizioni e nelle regole di proxy pass che lo contenevano come criterio di applicabilità.
- L'aggiornamento del nome di un soggetto, di un ruolo, o di una erogazione/fruizione (compresa la versione) non veniva propagata sulle policy di RateLimiting, sia attivate globalmente che puntualmente su una erogazione o fruizione (i filtri che contenevano l'oggetto di modifica risultavano erroneamente disabiliti).
- La modifica del nome del soggetto, se riferito da più di 1000 erogazioni, non veniva propagata sulle erogazioni successive alla 1000-esima.
- La modifica del tipo di credenziali di un soggetto da nessuna a basic o api-key comportava una mancata visualizzazione del dialog informativo che indica di copiare e custodire attentamente le credenziali generate.
- In una configurazione con Multitenant abilitato, accendendo in modifica ai dati di un soggetto definito con credenziali https, se si modificava il dominio, si avviava erroneamente il wizard di caricamento dei certificati.

- In una erogazione o fruizione, durante la creazione di un nuovo gruppo, se si sceglieva di ereditare la configurazione da un precedente gruppo, non venivano riportate le politiche di rate limiting esistenti sul vecchio.
- Se una erogazione conteneva nel gruppo "predefinito" un connettore multiplo non era possibile ridefinire il connettore su eventuali altri gruppi.
- Nel cambio di versione di una API venivano erroneamente proposte anche le versioni di API incomplete o che non contenevano lo stesso port-type nel caso di API SOAP. Inoltre non veniva verificato che la nuova versione possedesse tutte le operazioni riferite puntualmente nei gruppi, nei criteri di applicabilità delle trasformazioni o nei filtri di policy di RateLimiting.
- Durante la creazione di un nuovo gruppo, non veniva verificato se le azioni associate fossero già riferite puntualmente nei criteri di applicabilità delle trasformazioni del gruppo Predefinito.
- L'aggiornamento dell'interfaccia WSDL di una API SOAP provocava un errore inatteso della console se il WSDL possedeva i caratteri \r\n all'inizio del file.
- In seguito alla creazione di una API REST creata attraverso il caricamento di un'interfaccia OpenAPI contenente una descrizione maggiore di 255 caratteri, una qualsiasi modifica dell'API (del nome, tag, descrizione stessa, ...) terminava con un errore: "La descrizione supera i 255 caratteri ammessi". Il problema derivava dall'aggiunta dei caratteri "\r" dove erano presenti i caratteri "\n" nella descrizione. La correzione è stata effettuata per tutti gli elementi della console che vengono gestiti con lo stesso tipo di elemento html: "text-area".
- Se per un applicativo o soggetto veniva caricato un certificato con serial number più grande della dimensione massima di un long, la console visualizzava un numero negativo.
- Nella sezione "Configurazione - Cache" (disponibile in modalità avanzata) sono adesso configurabili tutte le cache del prodotto (anche registry e controllo del traffico).
- Corretta anomalia nella ridefinizione del connettore su un nuovo gruppo, che provocava errore in caso di annullamento/ripetizione della stessa operazione.
- L'eliminazione di un'entità del registro rimaneva nella cache interna dell'applicazione e in alcune circostanze veniva ripresentata erroneamente.
- Una volta impostato un filtro su un connettore multiplo, era possibile solamente modificarne il valore ma non eliminarlo.
- Durante l'aggiornamento del nome di un Tag veniva erroneamente generato un messaggio di livello ERROR nel file di log.
- Durante il salvataggio delle API (e dei Soggetti in Multitenant) associate ad un utente, quando si selezionava la checkbox "Tutti" nella pagina di configurazione dell'utente la precedente associazione continuava ad esistere a livello di base dati anche se non più visualizzate da console comportando anomalie durante l'utilizzo della console.
- Migliorato il messaggio di errore riportato dalla console se viene utilizzata la funzionalità "Importa" o "Esporta" senza fornire un archivio.
- Nei Connettori Multipli erano presenti i seguenti problemi relativi alle credenziali basic associate in una consegna tramite servizio IntegrationManager (funzionalità attivabile con una installazione "avanzata"):
  - le credenziali non venivano verificate ed era quindi possibile creare una configurazione di consegna senza credenziali
  - per le credenziali definite non veniva controllato se fossero già utilizzate in altri applicativi o erogazioni
  - se veniva prima abilitata la consegna tramite I.M. assegnando delle credenziali basic e poi successivamente disabilitata, le credenziali restavano erroneamente assegnate all'applicativo.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- La console non visualizzava il contenuto del messaggio, anche se salvato dal gateway, in presenza di header http con valore una stringa vuota.
- Risolto problema presente sui criteri di generazione di report statistici: quando veniva selezionata un'implementazione di API non era più possibile modificare il tipo delle informazioni visualizzate nel report (numero transazioni, dimensione e latenza).
- In presenza di una configurazione in Load Balancing, se la connessione verso un nodo andava in «read timed out», la console era accessibile allo scadere del timeout impostato a 120 secondi. Il valore di default del timeout è stato ridotto a 5 secondi.
- Risolto problema presente nella gestione dei permessi riguardanti gli utenti della console di monitoraggio con visibilità limitata per soggetti e/o API:
  - le ricerche puntuali tramite identificativo di transazione o di messaggio non verificavano che l'utente avesse i diritti per visualizzare i dati della transazione;
  - le liste contenenti le erogazioni o le fruizioni di API, impostabili nei criteri di ricerca, visualizzano adesso solamente le API associate all'utente.
- Il controllo dello stato dei nodi del cluster non avveniva ogni 60 secondi a causa di una problematica che resettava il counter ad ogni navigazione sulla console di monitoraggio e quindi una continua navigazione faceva si che l'aggiornamento dello stato non avvenisse mai.

Per le API di monitoraggio sono stati risolti i seguenti bug:

- In una configurazione multitenant, con opzione "multitenant.forzaSoggettoDefault" disabilitata (comportamento di default), la generazione di report statistici con filtro contenente il field "api_implementata", senza la definizione del soggetto referente (richiesta comune per il Profilo "API Gateway"), produceva il seguente errore: Parametro "api" fornito possiede un valore "NomeAPI:1" che non rispetta il formato atteso "^[a-z]{2,20}/[0-9A-Za-z]+:[_A-Za-z][\-\._A-Za-z0-9]*:\d$"
- Le interfacce generate tramite "CXF OpenApiFeature" presentavano erroneamente come risposta 2xx un problem detail.

14.15 Bug Fix 3.3.4.p1

Sono stati risolti i seguenti bug:

- corretto problema introdotto nella versione 3.3.4 con l'ottimizzazione dei messaggi soap: le richieste che presentavano un carattere "\n", "\r" o "\t" nel root-element causavano un fallimento del parser il quale riportava erroneamente un errore simile al seguente:

  > Caused by: org.xml.sax.SAXParseException: The end-tag for element type «rootElementName» must end with a ">" delimiter

- nei casi suddetti, in cui il parser andava in errore, la funzionalità di registrazione dei messaggi salvava un contenuto incompleto;
- l'header HTTP SOAPAction non risultava modificabile tramite una trasformazione;
- aggiunto file "govway_transazioni_slow.log" utilizzabile per registrare le operazioni effettuate sulla base dati del tracciamento (registrazione log, controllo duplicati) che impiegano un tempo maggiore di una soglia prefissata;
- resa possibile la personalizzazione del nome dell'header HTTP "GovWay-Transaction-ErrorType" e del namespace associato al faultCode su SOAPFault 1.2. Aggiunta inoltre la possibilità di non generare il claim "type" in un Problem Detail.

Per la console di gestione sono stati risolti i seguenti bug:

- il bottone "i" di informazione presente negli elementi "checkbox" veniva erroneamente visualizzato spostato sulla destra;

- su un'installazione Tomcat, la sezione "Runtime" non visualizzava correttamente le informazioni relative alle connessioni attive del database di configurazione;
- se nel controllo degli accessi veniva configurata un'autenticazione "plugin", non venivano visualizzati i link necessari a registrare puntualmente gli applicativi e i soggetti.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- risolta problematica che si presentava saltuariamente sul server.log dell'application server, riportando un errore simile al seguente:

  > SEVERE [facelets.viewhandler] (default task-5) Error Rendering View[/transazioni/pages/form/dettagliMessaggioTab.xhtml]: java.lang.IllegalArgumentException: could not find dataTable with id "diagnosticiTable_tbl"

Sull'installer è stato corretto il seguente bug:

- utilizzando la modalità avanzata con ambiente dedicato per la gestione e il monitoraggio, se veniva indicato l'utilizzo di uno schema dedicato per le informazioni statistiche, tra i datasource del runtime non veniva generato quello richiesto dal Controllo del Traffico per accedere alle informazioni statistiche.

14.16 Bug Fix 3.3.4.p2

Sono stati risolti i seguenti bug:

- gli scope presenti in un access token con formato JWT non venivano identificati se la Token Policy associata per la validazione utilizzata il parser "OpenID Connect - ID Token" comportando un errore di autorizzazione "AuthorizationMissingScope";
- in caso di installazione Multi-Tenant, gli applicativi interni "ModI" di un Tenant non venivano identificati sull'erogazione di un altro Tenant, facendo fallire eventuali autorizzazioni puntuali configurate nel controllo degli accessi;
- corretta un'anomalia presente nel connettore https, dove se veniva impostata una configurazione errata (es. path di un keystore inesistente), veniva segnalato un errore generico "no SSLSocketFactory specified" invece della motivazione puntuale;
- con l'introduzione della funzionalità di ottimizzazione delle connessioni, la consegna con connettore multipli "Più Destinatari" su API Soap con profilo "oneway" falliva con un errore simile al seguente: Riscontrato errore durante la gestione del messaggio [EJBUtils.sendToConsegnaContenutiApplicativi(RichiestaApplicativa)]: GESTORE_MESSAGGI, Errore di aggiornamento proprietario Messaggio INBOX/xxxx: null

Per la console di gestione sono stati risolti i seguenti bug:

- la console non consentiva l'aggiornamento delle chiavi private registrate in modalità "Archivio" (caricate su database), relativamente alla sezione "sicurezza messaggio" degli applicativi e delle erogazioni nel profilo ModI;
- risolta anomalia presente nella gestione degli allegati delle API e delle Erogazioni e Fruizioni:
  - il caricamento di allegati xml e xsd falliva segnalando erroneamente un contenuto scorretto;
  - il caricamento di allegati di altro tipo veniva completato con successo sulla console anche se poi i dati salvati risultavano corrotti;
- nella scheda di dettaglio di una erogaziono o fruizione, sull'informazione riportata per il connettore è stata aggiunta l'indicazione sull'eventuale policy di negoziazione token configurata;
- i connettori multipli, definiti su di un'erogazione, non venivano cancellati dalla base dati in seguito all'eliminazione dell'erogazione causando il fallimento di una eventuale nuova creazione della medesima erogazione appena eliminata.

Per la console di monitoraggio sono stati risolti i seguenti bug:

- risolto bug che visualizzava erroneamente la checkbox di selezione delle consegne avvenute con connettore multiplo;
- nei csv esportati tramite la funzionalità di reportistica delle configurazioni non venivano riportati i soggetti e gli applicativi autorizzati. Inoltre in presenza di connettori multipli non veniva riportato il nome del connettore.

15 Versione 3.3.3

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.3 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

15.1 Miglioramenti al Profilo di Interoperabilità "ModI PA"

Adeguato il profilo "ModI PA" alla versione finale delle Linee Guida di Interoperabilità rilasciate in data 15/09/2020: https://trasparenza.agid.gov.it/archivio19_regolamenti_0_5386.html

- *Nomenclatura*: le maschere di configurazione sono state allineate alla nuova terminologia riguardante i pattern di interazione e sicurezza.
- *Interazione CRUD*: alle risorse di una API REST viene adesso per default assegnato il pattern di interazione "CRUD_REST".
- *Interazione Bloccante e Non Bloccante su API REST*: i profili bloccanti e non bloccanti sono adesso assegnabili alle risorse solamente se compatibili con i metodi HTTP e i codici di risposta richiesti dalla specifica.
- *Firma del payload su API REST*: sostituito l'header "Authorization" con il nuovo header "Agid-JWT-Signature" per il pattern di sicurezza "INTEGRITY_REST_01".
- *Rate Limiting*: aggiunta gestione "window" come descritto in "https://datatracker.ietf.org/doc/draft-polli-ratelimit-headers/". La funzionalità è attivabile tramite la proprietà "org.openspcoop2.pdd.controlloTraffico.numeroRichieste.header.limit.windows=true" da registrare nel file govway_local.properties
- *X5U per Applicativo*: la url indicata nel claim "x5u" di un token di sicurezza per API REST deve adesso essere registrata sull'applicativo e non più sulla fruizione in modo da consentire url differenti per applicativi differenti.
- *Certificate Chain per API REST*: aggiunta la possibilità di inviare l'intera catena dei certificati anche per API REST all'interno del claim "x5c".
- *Sicurezza Messaggio su Richiesta/Risposta*: è adesso possibile attivare la sicurezza messaggio puntualmente solamente sulla richiesta o sulla risposta di una operazione. Per API REST è possibile anche definire dei criteri di applicabilità della sicurezza messaggio in base a Content-Type o codici di risposta HTTP.

15.2 Miglioramenti alle Console di Gestione

Sono stati apportati i seguenti miglioramenti alle funzionalità di ricerca della console di gestione:

- Restyling grafico delle liste accessibili dal menù principale relativamente per i Soggetti, gli Applicativi, i Ruoli e gli Scope.
- Introdotti nuovi criteri di filtro per la ricerca degli applicativi e dei soggetti. È adesso possibile ricercarli per il loro utilizzo in erogazioni o fruizioni, anche specializzando la ricerca per tag o singola implementazione di API.
- Per tutti i principali oggetti presenti nel Registro (api, applicativi, soggetti, ruoli, scope ...) è adesso possibile conoscere in dettaglio dove sono utilizzati nelle configurazioni delle erogazioni e fruizioni.
- Il filtro di ricerca "API / Soggetto Erogatore", presente tra i criteri di ricerca nella lista delle erogazioni o fruizioni, permetteva di individuare tutte le entità che contengono il parametro di ricerca indicato nel nome del soggetto erogatore o nel nome stesso associato alla erogazione o fruizione. Il parametro viene adesso utilizzato anche per

verificare una corrispondenza sul nome dell'API implementata che, soprattutto in API di tipo SOAP dove viene utilizzato il nome del port-type, può differire dal nome dell'erogazione o fruizione.

- Dopo aver creato un oggetto sul registro, il filtro di ricerca viene impostato automaticamente con il nome di tale oggetto al fine di poterlo visualizzare immediatamente nella lista.
- Il filtro per Tag presente nei criteri di ricerca presenta adesso solamente i tag assegnati alle API relative al Profilo di Interoperabilità selezionato.
- Durante l'aggiornamento dell'interfaccia di un API è adesso possibile:
  - indicare se aggiornare o meno le risorse/azioni esistenti;
  - indicare se eliminare le risorse non più esistenti nella nuova interfaccia.

15.3 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti alle funzionalità di ricerca della console di monitoraggio:

- È adesso possibile ricercare transazioni o ottenere report statistici filtrando per API implementata. La funzionalità è utile in presenza di molteplici erogazioni o fruizioni che implementano la stessa API, per ottenere un report che non distingua per la singola erogazione o fruizione ma li raggruppi per API implementata.
- Le transazioni visualizzate nello storico riportano anche il codice http oltre all'esito della transazione. È adesso inoltre possibile effettuare ricerche per codice http.
- La sezione "Reportistica - Configurazione API" consente adesso di filtrare per tag.
- Il filtro per Tag presente nei criteri di ricerca presenta adesso solamente i tag assegnati alle API relative al Profilo di Interoperabilità selezionato.

15.4 Miglioramenti alla funzionalità di Validazione dei Contenuti

Utilizzando le proprietà dell'API è adesso possibile:

- *API SOAP*: disabilitare la validazione della SOAPAction;
- *API REST*: disabilitare o abilitare la validazione su codici http e/o content-type definiti puntualmente; è inoltre possibile disabilitare la validazione su risposte vuote e/o su risposte contenenti problem details.

15.5 Miglioramenti alla funzionalità del CORS

Nella configurazione CORS, quando viene abilitato uno o più specifiche origin, è adesso possibile indicare di autorizzare qualsiasi metodo e/o header http della richiesta, senza dover definire l'elenco dei metodi e/o header autorizzati.

15.6 Miglioramenti alla funzionalità dei Connettori

Sul connettore https è adesso possibile effettuare una configurazione che accetta qualsiasi certificato venga ritornato dal server.

È stata inoltre aggiunta la possibilità di configurare, a livello di installazione, un utilizzo di un java.security.SecureRandom con algoritmo personalizzato rispetto al default di java.

Infine la lunghezza massima di un endpoint associabile ad un connettore è adesso di 4000 caratteri.

15.7 Miglioramenti alla funzionalità di Trasformazione

È stato aggiunto nella maschera di gestione di un header o di un parametro della url un campo "Identificazione Fallita" che consente di definire il comportamento del Gateway quando non riesce a risolvere le parti dinamiche contenute nel valore indicato:

- Termina con errore: la transazione termina con un errore che riporta la fallita risoluzione della parte dinamica indicata per il valore;
- Continua senza header: la transazione continua senza che l'header o il parametro venga aggiunto o modificato.

15.8 Miglioramenti alla funzionalità di Tracciatura su File

Aggiunte ulteriori informazioni, inerenti le comunicazioni gestite dal gateway, che possono essere riversate nei file di log associati ai topic di file trace:

- resultClass, resultClassOk, resultClassKo, resultClassFault: classe a cui appartiene l'esito della transazione tra OK, KO e FAULT;
- errorDetail: dettaglio dell'errore avvenuto durante la gestione della transazione;
- requester: rappresenta il richiedente della richiesta e assumerà la prima informazione valorizzata, trovata nella richiesta, tra tokenUsername, tokenSubject[@tokenIssuer], application, principal e tokenClientId;
- ipRequester: rappresenta l'indirizzo ip del richiedente e viene valorizzato con il forwardedIP se presente, o altrimenti con il clientIP;
- principalAuthType: tipo di autenticazione (basic/ssl/principal) con cui l'applicativo è stato autenticato;
- diagnostics e errorDiagnostics: consentono di accedere ai diagnostici emessi da GovWay durante la gestione della richiesta;
- senderId, providerId, apiId, apiInterfaceId, profileLabel: consentono di ottenere delle informazioni già accessibili in precedenza con un nuovo formato conforme al profilo di interoperabilità utilizzato.

15.9 Miglioramenti alle API di Gestione e Monitoraggio

Sono stati apportati i seguenti miglioramenti alle API di monitoraggio:

- È adesso possibile ricercare transazioni o ottenere report statistici filtrando per API implementata. La funzionalità è utile in presenza di molteplici erogazioni o fruizioni che implementano la stessa API, per ottenere un report che non distingua per la singola erogazione o fruizione ma li raggruppi per API implementata.

Sono stati apportati i seguenti miglioramenti alle API di gestione:

- Le risorse "/fruizioni/{erogatore}/{nome}/{versione}/url-invocazione" e "/erogazioni/{nome}/{versione}/url-invocazione" gestiscono adesso tutte le modalità supportate dal prodotto ("content-based", "header-based", "input-based", "interface-based", "soap-action-based", "url-based", "protocol-based"). È stata inoltre aggiunta la modalità "static" utilizzabile su API soap contenente un'unica azione.
- È adesso possibile registrare le proprietà di configurazione nelle erogazioni e fruizioni anche tramite api.

15.10 Nuova funzionalità di suddivisione delle API in Canali

Aggiunta la possibilità di attivare, in una installazione composta da più nodi in Load Balancing, una suddivisione delle API tra i vari nodi utilizzando il concetto di canale, al fine di suddividere il carico tra i nodi.

Abilitando la nuova funzionalità sarà possibile assegnare uno o più canali ad ogni nodo che compone il cluster ed un canale ad ogni API. Su ogni nodo saranno autorizzate ad essere invocate solamente le API che possiedono un canale corrispondente alla configurazione del nodo.

15.11 Miglioramenti al Profilo di Interoperabilità "Fatturazione Elettronica"

Aggiornati gli schemi xsd della fattura (versione 1.2.1) e della fattura semplificata (versione 1.0.1) come adeguamento al provvedimento del 28/02/2020 descritto in https://www.agenziaentrate.gov.it/portale/web/guest/-/provvedimento-del-28-febbraio-2020. Gli schemi utilizzati sono quelli presenti all'interno dell'archivio zip della versione 1.6 delle specifiche tecniche (Allegato A).

15.12 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- È stato aggiunto il supporto per la nuova versione dell'application server "WildFly" 21.x.
- Le patch SQL che modificano il tipo di una colonna da VARCHAR a CLOB, tramite il comando ALTER, sono state riviste al fine di utilizzare una versione più efficiente per i tipi di database che lo consentono (https://github.com/link-it/govway/issues/58).
- Modificato tipo della colonna "value" della tabella "tracce_ext_protocol_info" al fine di poter creare un indice su tale colonna. L'indice consente di migliorare le performance come descritto nell'issue https://github.com/link-it/govway/issues/60.
- Lo script SQL generato per MySQL, possedeva un vincolo "unique" non instanziabile su mysql: «ERROR 1071 (42000): Specified key was too long; max key length is 3072» (https://github.com/link-it/govway/issues/66).
- L'installer genera adesso un archivio govway.ear contenente nel file application.xml i "resource-ref" necessari all'A.S. per effettuare un shutdown corretto dei datasource.

15.13 Bug Fix

Sono stati risolti i seguenti bug:

- Sono stati corretti i seguenti problemi presenti sulla validazione tramite OpenAPI 3:
  - Un oggetto di tipo "string", definito con la restrizione basata su pattern (es. "^d{6}$"), non veniva correttamente validato se il valore presente nel messaggio json possedeva dei caratteri speciali come "\r\n" o "\n" o "\t". La validazione OpenAPI terminava con successo non rilevando i caratteri non ammessi dal pattern indicato.
  - Sulla validazione della risposta, per operazioni che non prevedevano una risposta applicativa, la validazione non rilevava un contenuto non ammesso se era compatibile con la risposta definita per il codice http "default".
  - La validazione trattava come "required" i contenuti delle richieste per cui nell'interfaccia non veniva definito l'attributo "required" nel request-body. Il comportamento è stato modificato per adeguarsi a quando descritto nella specifica "https://swagger.io/docs/specification/describing-request-body/": «Request bodies are optional by default. To mark the body as required, use required: true.»
  - Corretti problemi di validazione dei parametri definiti come "date-time" che presentavano il carattere "+" nell'offset.
- Corretto problema di identificazione fallita di un risorsa di API REST quando l'OpenAPI caricato conteneva lo "/" in fondo ad una risorsa.
- Corretto http status presente nel ProblemDetail generato dalle erogazioni in caso di "internalResponseError". Veniva indicato erroneamente 503, invece del corretto codice 502 utilizzato per la connessione http.
- La libreria di valutazione delle espressioni JsonPath, se queste contenevano la funzione concat (es. concat($.richiedente.codice_fiscale,»###»,$.richiedente.nome)), salvava in una cache interna il risultato; il salvataggio comportava che a fronte di messaggi differenti l'applicazione dell'espressione JsonPath forniva lo stesso risultato. Il comportamento errato della libreria comportava malfunzionamenti nelle funzionalità

di GovWay dove era possibile utilizzare espressioni JsonPath (es. nella correlazione applicativa, nelle trasformazioni).

- Sia nella funzionalità di negoziazione dei token che durante la verifica tramite servizio di introspection e userInfo, viene adesso utilizzata la modalità http "content-length" al posto della precedente modalità "transfer-encoding-chunked". Nella negoziazione del token è stato inoltre corretto il body della richiesta "application/x-www-form-urlencoded" eliminando il primo carattere "&" aggiunto erroneamente, es. &grant_type=client_credentials (https://github.com/link-it/govway/issues/69).
- Nella funzionalità di negoziazione dei token, in presenza di un token con expires_in = 9223372036854775 (il Long.MAX_VALUE portato ai secondi), il sistema segnalava erroneamente il token come scaduto. Invece da specifiche tale valore dovrebbe indicare un tempo «infinito» (https://github.com/link-it/govway/issues/70).
- Aggiunta generazione dell'header WWW-Authenticate in ogni tipo di autenticazione gestita su GovWay se l'autenticazione fallisce (codice http 401). Anche il gestore delle credenziali, da utilizzare in caso di frontend web, gestisce adesso la possibilità di generare tale header. È stato inoltre associato uno stato "autenticazione fallita" alle transazioni che non presentano le credenziali attese dal gestore.
- La funzione di ottenimento di un wsdl tramite l'invocazione dell'url di invocazione arricchita del prefisso "?wsdl", poteva generare un wsdl contenente schemi xsd in cui alcuni elementi riferivano prefissi non associati a dichiarazioni di namespace. Il problema è stato risolto.
- Il campionamento statistico mensile e settimanale, in ambienti con un elevato traffico, non era performante e quindi ne è stata disabilitata la generazione. I report di distribuzione statistica che riguardano un periodo superiore al giorno vengono adesso calcolati con il campionamento giornaliero. Durante la generazione delle statistiche è stato inoltre corretto il valore attribuito ai tempi di latenza per le transazioni che non possedevano le date dei quattro corner, utilizzando un valore null al posto di un fuorviante valore 0.
- Ottimizzato il diagnostico relativo ad una utenza errata, eliminando dalle informazioni tracciate la password utilizzata dal chiamante.
- Corretto timer che consente di verificare lo spazio disco occupato da un database.
- I timer e il batch di generazione delle statistiche registrano adesso gli eventi in log dedicati al tipo di intervallo gestito: orario,giornaliero,settimanale,mensile. Questo consente di evitare la sovrascrittura da parte degli intervalli più frequenti delle informazioni inerenti a intervalli maggiori durante la ruotazione dei log.
- Nelle installazioni in cluster, sono stati ridotti i tempi di verifica per l'ottenimento di un lock da parte del timer che consegna le notifiche ed è stato corretto un problema che sbilanciava l'acquisizione del lock sempre su un nodo. Inoltre è stata corretta la procedura di rilascio dei lock in fase di shutdown dell'A.S., ed è stata inserita anche una pulizia iniziale all'avvio. Sono inoltre stati rivisti l'utilizzo dei lock per quanto concerne i timer adibiti alla pulizia del repository messaggi.
- Aggiunta impostazione del Locale per il fault string del SOAPFault. Il locale utilizzato è adesso indicabile in govway.properties tramite le proprietà "org.openspcoop2.pdd.erroreApplicativo.faultString.language" e "org.openspcoop2.pdd.erroreApplicativo.faultString.country".
- Corretti i seguenti problemi presenti in uno scenario con profilo di interoperabilità ModI:
  - aggiunti gli header contenente gli identificatori anche sulle erogazioni (es. GovWay-Conversation-ID);
  - corretto digest salvato nelle tracce per i profili IDAS03: veniva erroneamente salvato in codifica hex invece che in codifica base64;
  - corrette utility JWT al fine di validare un certificato in un truststore verificandone anche l'uguaglianza con il certificato stesso oltre che tramite la CA;
  - aggiunto controllo che l'applicativo venga identificato, tramite uno dei meccanismi di autenticazione, per poter usare funzionalità di sicurezza;

  - corretto problema che non consentiva, in presenza di validazione dei contenuti attivi, la generazione dell'header SOAP "X-Correlation-ID", nel profilo di interazione PUSH, quando il backend server non generava di proprio conto tale header;
  - risolto problema che avveniva durante la creazione dell'header SOAP "X-Correlation-ID" se il messaggio di risposta di una Richiesta PULL non conteneva il SOAPHeader;
  - gestito aggiornamento del valore dell'header "ReplyTo", sia in REST che SOAP, sull'erogazione prima di contattare il backend in modo da tradurre il valore con la relativa url di invocazione del servizio di callback correlato;
  - corretta descrizione dell'errore ritornata al client in caso di header SOAP Correlation-ID non trovato;
  - risolto problema presente nella gestione della fase di Richiesta per il profilo PUSH e PULL SOAP: se il server non generava un header "X-Correlation-ID", GovWay creava un header valorizzandolo con l'id del messaggio invece che con l'id di transazione come descritto da documentazione;
  - corretti esiti riportati per la fase di imbustamento SOAP quando mancavano elementi obbligatori nel profilo PULL;
  - corretto esito della transazione, quando avveniva un errore di "protocollo" anche durante la fase di imbustamento;
  - aggiunto controllo sul codice http nella fase di imbustamento per il protocollo rest, profilo non bloccante;
  - aggiunto "IDCollaborazione" letto dalla risposta per generare l'header GovWay-Conversation-ID.

Per la console di gestione sono stati risolti i seguenti bug:

- Durante l'aggiunta di un applicativo di tipo server veniva visualizzata erroneamente la finestra di dialogo per la copia delle credenziali con delle credenziali vuote.
- Risolto malfunzionamento presente nella sezione del connettore che consente il download dei certificati server; il problema causava un errore inatteso sulla console quando il server non era raggiungibile (es. errore di connection refused o timed out).
- Durante la creazione di una API, se si caricava un wsdl e solo successivamente si impostava il tipo di API a SOAP, la console non consentiva di completare la creazione segnalando erroneamente un problema di sintassi relativo all'interfaccia caricata.
- La selezione di un "Servizio" in una erogazione o fruizione di API SOAP è adesso obbligatoria anche utilizzando la console in modalità avanzata.
- Corretta una errata visualizzazione delle informazioni presenti nella maschera di creazione di una fruizione, utilizzando la console in modalità avanzata: la scelta dell'erogatore risiedeva tra i dati dell'API e venivano quindi visualizzati due campi consecutivi con la stessa denominazione "Nome".
- Risolto problema che provocava uno stallo sulla console quando si selezionava ripetutamente da una select list il valore già scelto in precedenza.
- La creazione di una nuova erogazione/fruizione o l'aggiornamento del nome e/o dei parametri del profilo, richiedevano un tempo considerevole per presentare la maschera dei dati quando il numero delle API era elevato.
- L'aggiornamento del nome di una erogazione, che presentava connettori multipli, non veniva riportato sugli applicativi aggiuntivi a quello di default.
- L'aggiornamento dell'url di invocazione o delle "Opzioni Avanzate" di una erogazione, che presentava connettori multipli, comportava una perdita dei dati associati ai connettori.
- Corretti i seguenti problemi presenti in uno scenario con profilo di interoperabilità ModI:
  - se si modificava la configurazione del profilo in una fruizione, alcuni parametri del connettore quale l'eventuale abilitazione del debug e l'autenticazione http o token venivano erroneamente disabilitate;

  - il cambio di nome di una API di richiesta correlata tramite profilo PUSH, provocava un errore inatteso della console quando si accedeva all'API con ruolo "Risposta";
  - risolta anomalia che si presentava quando veniva creata una erogazione a partire da una API con sicurezza canale IDAC01, e successivamente veniva modificata la sicurezza del canale dell'API implementata a IDAC02, o veniva associata all'erogazione una API differente con sicurezza canale IDAC02. La configurazione riportava correttamente un warning nella sezione "Controllo degli Accessi" poichè l'autenticazione era opzionale (configurazione derivante dall'API indicata al momento della creazione dell'erogazione). Accedendo in modifica al controllo degli accessi non veniva però visualizzato e non era consentito modificare il criterio di opzionalità dell'autenticazione.
- Corretta funzionalità di import affinchè il controllo che verifica l'aderenza delle informazioni fornite con il WSDL sia effettuato solamente su API SOAP.
- Corretti i seguenti problemi relativi alla gestione delle proprietà binarie di un profilo di interoperabilità:
  - l'import di un servizio applicativo andava in errore se una proprietà binaria era valorizzata (es. keystore pkcs12 di un applicativo in ModI PA);
  - l'accesso al dettaglio di una proprietà binaria di una fruizione andava in errore;
  - la registrazione o l'aggiornamento di una proprietà binaria comportava un salvataggio corrotto di tale documento sul registro; il problema era presente anche per gli allegati di una API, di una erogazione e di una fruizione;
  - corrette breadcump errate presenti nelle sezioni di dettaglio di una proprietà binaria di una erogazione o di una fruizione;
  - corretta breadcump errata presente nella sezione "Modifica Profilo Interoperabiltà" di una fruizione.
- Nella sezione Runtime è adesso disponibile il dettaglio dei timer attivi e la possibilità di attivarli/disattivarli.
- Rivista la sezione "Coda Messaggi" nella govwayConsole al fine di visualizzare tutte le informazioni di interesse: nome dell'erogazione, nome dei connettori, data di rispedizione per ogni connettore, nome degli applicativi server. È stato inoltre aggiunta la funzionalità "Riconsegna Immediata" utilizzabile per forzare la consegna di un messaggio senza aspettarne la data di rispedizione (la presa in carico avviene tramite funzionalità ancora in versione alfa e quindi non attive per default).
- Il cookie generato dalla console di gestione è stato ridenominato in "JSESSIONID_GW_CONSOLE".

Per la console di monitoraggio sono stati risolti i seguenti bug:

- I dati delle configurazioni accedute tramite la console di monitoraggio vengono adesso salvati in una cache interna al fine di rendere più veloce la navigazione tra le maschere di ricerca.
- Nella Ricerca Avanzata delle transazioni è adesso consentito effettuare una ricerca che includa qualsiasi profilo di interoperabiltà; con questa scelta anche l'indicazione del soggetto locale diventa a campo libero.
- Nei report statistici che non riguardano distribuzioni temporali è stata eliminata la voce "Unità temporale" tra i criteri di ricerca; la scelta compare solamente, limitata ai valori "oraria" e "giornaliera", nel caso di impostazione di un periodo personalizzato poichè influenza il widget nel quale viene consentito o meno la possibilità di indicare l'orario desiderato.
- Corretto nullPointer che capitava dopo un utilizzo prolungato della console: «Caused by: javax.el.ELException: /commons/includes/menu.xhtml @33,58 rendered=»#{applicationBean.showTransazioniBase}»: java.lang.NullPointerException».
- Il cookie generato dalla console di monitoraggio è stato ridenominato in "JSESSIONID_GW_MONITOR".

Nell'utilizzo dell'Installer in modalità avanzata sono stati risolti i seguenti bug:

- L'indice "full INDEX_TR_SEARCH", generato dall'installer in modalità avanzata per i database di tipo postgresql e oracle, non venivano utilizzati dal db per soddisfare le query prodotte tramite la console di monitoraggio durante la ricerca nello storico a causa dei seguenti problemi:
  - la colonna "versione_servizio" non era presente nell'indice ma veniva utilizzata sia per la ricerca di una API Implementata che per la visualizzazione delle informazioni relative ad una singola transazione
  - nel comando SELECT venivano aggiunte ulteriori colonne non presenti nell'indice che non avevano però alcuna utilità durante la presentazione dei risultati in lista.
- Il file "consolePassword.properties" non veniva generato per l'ambiente runtime in caso di disaccoppiamento tra runtime e manager.
- È adesso possibile generare un batch che gestisce la pulizia dei messaggi presi in carico sul gateway (gestoreRuntimeRepository). La presa in carico avviene tramite due funzionalità ancora in versione alfa e quindi non attive per default (IntegrationManager e ConsegnaAsincrona) per le quali è stata introdotta la gestione delle priorità e la possibilità di assegnare una coda di pool di thread differente ad un connettore. Sono inoltre stati risolti i problemi che riguardavano la consegna (veniva incrementato erroneamente per 2 volte il numero di rispedizione del messaggio ad ogni consegna) e l'invocazione del servizio IntegrationManager (segnalazione non bloccante presente nel log: "Non abilitata la gestione delle transazioni stateful"). Nella consegna con notifiche, anche le url verso i server di notifica venivano erroneamente arricchiti con il contesto "rest" dell'invocazione: il problema è stato risolto. Infine sul database di runtime è stata aggiunta una colonna contenente l'informazione temporale di creazione dell'entry, nelle tabelle del runtime che non la possedevano, per poter effettuare il partizionamento del database "runtime".

16 Versione 3.3.2

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.2 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

16.1 Nuova funzionalità di Autenticazione "Api Key"

La nuova funzionalità consente di autenticare gli applicativi e i soggetti tramite una chiave di identificazione "Api Key" veicolata in un header http, un parametro della url o un cookie come descritto nella specifica "OAS3 API Keys" (https://swagger.io/docs/specification/authentication/api-keys/).

Viene supportata anche la modalità "App ID" che prevede oltre all'ApiKey un identificatore dell'applicazione; modalità denominata "Multiple API Keys" nella specifica "OAS3 API Keys".

È quindi possibile registrare applicativi e soggetti associandogli credenziali "api-key"; la registrazione comporta la generazione di una chiave univoca da utilizzare per accedere all'API su GovWay.

La configurazione dell'autenticazione consente di indicare la modalità di identificazione della chiave di accesso tra header http, parametro della url e cookie (viene supportata la scelta multipla), permettendo anche di personalizzare i nomi dei parametri, rispetto a quanto indicato nella specifica "OAS3 API Keys".

16.2 Miglioramenti alla funzionalità di Autenticazione

Introdotta la configurabilità del tipo di cifratura delle password utilizzato per:

- le utenze delle console di gestione e monitoraggio;
- gli applicativi e i soggetti registrati con credenziali "http-basic".

È stata adeguata la configurazione di default al fine di utilzzare un algoritmo di cifratura più recente: SHA-512-based Unix crypt (6).

Per garantire la retrocompatibilità con le utenze esistenti, la verifica delle password viene attuata anche usando il precedente algoritmo. La verifica in modalità "backward compatibility" può essere disattivata una volta migrate tutte le password al nuovo formato di cifratura.

16.3 Miglioramenti alla API di Monitoraggio

Sono stati apportati i seguenti miglioramenti alle funzionalità di monitoraggio delle transazioni:

- *Richiedente*: l'informazione sul richiedente dell'operazione è stata aggiunta sia nel dettaglio di una transazione che nelle informazioni generali presenti nella lista.
- *Client Id*: tra le informazioni generali presenti in ogni item della lista è stato aggiunto il client-id del token OAuth2.
- *Dettaglio Errore*: nel dettaglio di una transazione è stato aggiunto il dettaglio dell'errore nel caso la transazione non sia completata con successo.
- *Latenze*: nel dettaglio di una transazione sono state riportate le informazioni già presenti nella lista riguardanti la data e le latenze.
- *Escludi Richieste Scartate*: disabilitato come criterio di default il filtro "Escludi Richieste Scartate".

16.4 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- È stato aggiunto il supporto per la nuova versione dell'application server "WildFly" 20.x.
- Le password relative alle utenze delle console, indicate durante l'esecuzione dell'installer, vengono predisposte negli script SQL cifrate in SHA-512-based Unix crypt (6).

16.5 Bug Fix

Per la console di gestione sono stati risolti i seguenti bug:

- Introdotta una nuova modalità di gestione delle operazioni di delete ed export attraverso l'utilizzo di una form con method POST al posto dell'invocazione di una GET. La nuova modalità consente di evitare il formarsi di una url eccessivamente lunga che poteva essere bloccata dai frontend http.

Per la API di configurazione sono stati risolti i seguenti bug:

- Corretto http status, da 204 a 201, restituito in caso di operazione effettuata con successo per le risorse:
  - POST /erogazioni/{nome}/{versione}/gruppi/{nome_gruppo}/azioni
  - POST /fruizioni/{erogatore}/{nome}/{versione}/gruppi/{nome_gruppo}/azioni

17 Versione 3.3.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.1 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

17.1 Nuova Gestione degli Errori generati da GovWay

Sono state completamente riviste le informazioni di errore ritornate al client, in seguito ad anomalie rilevate da GovWay nella gestione della richiesta o della risposta.

Oltre agli errori già previsti nelle interfacce dell'API, gli applicativi client possono ricevere due tipi di errori generati direttamente da GovWay:

- *Errori Client*: identificabili da un codice http 4xx su API REST o da un fault code "Client" su API SOAP. Indicano che GovWay ha rilevato problemi nella richiesta effettuata dal client (es. errore autenticazione, autorizzazione, validazione contenuti...).
- *Errori Server*: identificabili dai codici http 502, 503 e 504 per le API REST o da un fault code "Server" generato dal Gateway e restituito con codice http 500 per le API SOAP.

La codifica degli errori prodotta dal Gateway permette alle applicazioni client di discriminare tra errori causati da una richiesta errata, per i quali è quindi necessario intervenire sull'applicazione client prima di effettuare nuovi invii, ed errori dovuti allo stato dei servizi invocati, per i quali è invece possibile continuare ad effettuare la richiesta.

Per ciascun errore GovWay riporta le seguenti informazioni:

- Un codice http su API REST o un fault code su API SOAP.
- Un codice di errore, indicato nell'header http "GovWay-Transaction-ErrorType", che riporta l'errore rilevato dal gateway (es. AuthenticationRequired, TokenExpired, InvalidRequestContent ...).
- Un identificativo di transazione, indicato nell'header http "GovWay-Transaction-ID", che identifica la transazione in errore, utile principalmente per indagini diagnostiche.
- Un payload http, contenente maggiori dettagli sull'errore, opportunamente codificato per API REST (Problem Details - RFC 7807) o SOAP (Fault).

Nella configurazione di default di GovWay, gli errori restituiti ai client non contengono dettagli che possano causare disclosure di informazioni relative al dominio interno. In alcuni casi, per facilitare il supporto alla risoluzione di problemi, è comunque possibile abilitare la generazione di codici più specifici di errore ritornati al client nell'header http "GovWay-Transaction-ErrorStatus".

17.2 Nuova funzionalità di Tracciatura su File

La nuova funzionalità consente il tracciamento su file di tutte le informazioni relative alle comunicazioni gestite da GovWay. Il successivo processamento del file da strumenti esterni (es. FileBeat) abilità così una facile integrazione con sistemi di tracciamento esterni (es. Logstash, Kafka, ...).

La funzionalità consente una completa personalizzazione delle informazioni da riportare su file di log, permettendo anche di definirne il formato e l'ordine in cui vengono salvate. È inoltre possibile suddividere le informazioni in più file di log in modo da facilitare l'invio di informazioni selezionate a destinazioni diverse.

17.3 Nuova funzionalità Gestione Proxy

Permette di gestire correttamente le situazioni in cui le comunicazioni tra GovWay e l'endpoint destinatario siano mediate dalla presenza di un proxy.

Nei casi più comuni si tratta di un «forward proxy». In questi casi l'indirizzo del proxy può essere censito sul connettore dell'Erogazione.

In scenari più complessi possono essere presenti reverse proxy che intervengono nella gestione delle connessioni https, utilizzando certificati client e/o trustStore differenti per diversi contesti applicativi. In queste situazioni l'endpoint indicato nella configurazione del connettore su GovWay non è l'indirizzo remoto dell'applicativo ma bensì l'indirizzo del reverse proxy il quale a sua volta si occuperà di inoltrare la richiesta agli indirizzi a lui noti.

In questa situazione, è necessario configurare gli endpoint delle API sia su GovWay (indirizzo del reverse proxy), che sul reverse proxy (indirizzo dell'Erogatore finale)

Per semplificare la gestione di questo scenario architetturale, dalla versione 3.3.1 GovWay può passare l'indirizzo remoto dell'applicativo al proxy tramite un header HTTP o un parametro della url. In questo modo il censimento degli applicativi viene effettuato esclusivamente su GovWay.

17.4 Miglioramenti al Profilo di Interoperabilità "ModI PA"

È adesso possibile estendere il profilo di sicurezza messaggio IDAR03/IDAS03 in modo che il token di sicurezza ModI PA contenga:

- *Digest Richiesta*: nel token di sicurezza della risposta viene incluso il digest della richiesta. La funzionalità consente di implementare la soluzione per la non ripudiabilità della trasmissione come suggerito nelle linee guida di interoperabilità (punto D): https://docs.italia.it/italia/piano-triennale-ict/lg-modellointeroperabilita-docs/it/bozza/doc/doc_04/soluzioni-di-sicurezza.html#soluzioni-per-la-non-ripudiabilita-della-trasmissione.
- *Informazioni Utente*: le informazioni sull'utente che ha effettuato la richiesta.

17.5 Miglioramenti alle Console

Sono stati apportati i seguenti miglioramenti:

- *Ricerca nelle liste a tendina*: aggiunta la possibilità di selezionare incrementalmente nelle liste a tendina, tramite digitazione di caratteri.
- *Highlight*: aggiunto il supporto dell'highlight della keyword di ricerca effettuata sia all'interno delle liste che nei campi con funzionalità di "autocomplete".

Relativamente alla sola console di gestione:

- *Risorse REST con qualsiasi path*: aggiunta la possibilità di registrare manualmente risorse in API REST con HttpMethod definito e Path Qualsiasi.
- *Modifica Risorsa*: è stata aggiunta la possibilità di accedere al dettaglio di una risorsa, dall'elenco presente in una API, cliccando anche sul metodo http.
- *Modifica Nome Applicativo*: aggiunta la possibilità di modificare il nome di un applicativo precedentemente registrato.
- *Modifica API di una Erogazione/Fruizione*: aggiunta la possibilità di modificare l'API implementata in una erogazione o fruizione.
- *Sospensione API*: la sospensione di una API (erogazione/fruizione), o la successiva riattivazione, non necessita più un'operazione di reset delle cache. L'operazione effettuata tramite console è immediatamente attiva.

Relativamente alla sola console di monitoraggio

- *Ricerca per ID Transazione*: è adesso il primo criterio di ricerca per identificativo
- *Pie Chart*: nei report a torta, sulla destra di ogni voce presente nella legenda viene adesso riportato anche il numero di record oltra la %.
- *Distribuzione Temporale*: aggiunta la possibilità di personalizzare il numero di label da visualizzare sull'asse X nei report con distribuzione temporale.
- *Nuovi esiti associati alle Transazioni*:
  - "Errore ModI PA": gli errori generati durante la validazione "ModI PA" vengono adesso classificati con un esito dedicato;
  - "Richiesta o Risposta già Elaborata": i nuovi esiti sono associati a transazioni riguadanti richieste o risposte duplicate.
- *Escludi Richieste Scartate*: il comportamento di default utilizzato nella sezione Transazioni e Statistiche può essere modificato tramite la proprietà "transazioni.escludiRichiesteScartate.defaultValue" nel file di configurazione esterno "/etc/govway/monitor_local.properties".
- *Volume di Traffico Iniziale*: il grafico che fornisce il volume di traffico complessivo, disponibile una volta collegati alla console, è adesso configurabile per restituire il volume complessivo di tutti i Profili di Interoperabilità abilitati sul gateway.

17.6 Miglioramenti alla funzionalità di Validazione dei Contenuti

- *Nuovo Engine*: la validazione dei contenuti, tramite interfaccia OpenAPI 3, utilizza adesso la libreria openapi4j (https://openapi4j.github.io/openapi4j/) che consente di validare correttamente messaggi definiti tramite strutture "oneOf" con discriminator.
- *Validazione solo per la Richiesta*: la validazione è adesso «disattivabile» sulla fase di richiesta o risposta utilizzando le proprietà dell'API.

17.7 Miglioramenti alla funzionalità Importa e Esporta

Nella funzionalità "Importa" della console è adesso possibile selezionare puntualmente se importare o meno nel registro di GovWay eventuali configurazioni o policy globali (Token, RateLimiting) presenti all'interno dell'archivio.

Anche per la funzionalità "Esporta" è possibile indicare se includere nell'archivio esportato le policy globali riferite.

17.8 Miglioramenti alla funzionalità "Header di Integrazione"

Aggiunte nuove modalità di interscambio delle informazioni che consentono di definire tramite un template «Freemarker» o «Velocity» come le informazioni di integrazione siano inserite nel messaggio inoltrato al backend (richiesta) o restituito al client (risposta).

17.9 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- È stato aggiunto il supporto per la nuova versione dell'application server "WildFly" 19.x

17.10 Bug Fix

Sono stati risolti i seguenti bug:

- Nella funzionalità di tracciamento con correlazione applicativa è adesso possibile definire regole multiple di correlazione anche per i messaggi JSON e non più solamente per messaggi XML. L'applicabilità di una regola è verificabile tramite l'utilizzo di un'espressione JSONPath.
- Le richieste "OPTIONS", identificate tramite una risorsa definita nell'API con HttpMethod "Qualsiasi", vengono adesso gestite come "Request Preflight" se il CORS è abilitato nell'API.
- Gli header HTTP di integrazione specifici di un Profilo di Interoperabilità (es. Fatturazione Elettronica) non venivano gestiti correttamente in caso di attivazione dei "metadati" di integrazione "backward compatibility" il cui scopo è quello di produrre header di integrazione uguali a quelli generati da "OpenSPCoop2" (es. x-openspcoop2-trasporto). Il problema è stato risolto e adesso tutti gli header generati sono stati allineati per essere retrocompatibili (es. X-SDI-*).
- L'accesso al database è stato ottimizzato per i seguenti casi:
  - Registrazione delle credenziali (trasporto, token) e dei tags/eventi nella transazione.
  - Funzionalità di arricchimento delle tracce, nel Profilo di Interoperabilità "Fatturazione Elettronica"
- Sono stati disattivati i log generati dai template engine "Freemarker" e "Velocity" sul server log dell'Application Server.
- Aggiunta la possibilità di gestire gli header HTTP e i parametri delle URL all'interno di una trasformazione.
- L'identificativo del cluster numerico assegnabile alla proprietà "org.openspcoop2.pdd.cluster_id.numeric" nel file "govway_local.properties", veniva erroneamente gestito come intero invece che come stringa; questo comportava nel caso di numeri a due cifre che non si potessero utilizzare le prime 9 cifre definite come "0X" poichè si perdeva lo 0 iniziale. Il problema è stato corretto.

- Modificato il livello di severità da “error” a “info” del diagnostico che riporta l’esito di una comunicazione terminata con codice http 3xx di una API REST.

Per la console di gestione sono stati risolti i seguenti bug:

- Risolto problema, per quanto concerne il profilo “ModI PA”, che non consentiva di registrare gli applicativi autorizzati in presenza di Multi-Tenant abilitato.
- Corretto messaggio di warning presente durante la modifica di un referente di API (Profilo SPCoop); veniva erronamente visualizzato un id numerico al posto del nome del soggetto.
- La configurazione sui connettori multipli veniva erroneamente persa se venivano effettuate modifica nella sezione “URL di Invocazione”.
- Corretto colore dei link visitati; veniva erroneamente utilizzato il colore associato all’hover.
- Se durante un aggiornamento veniva aggiunto un nuovo profilo di interoperabilità, senza che fosse stato creato sul database un soggetto di default associato, la console sollevava un errore generico. L’anomalia viene adesso segnalata correttamente.

Nelle funzionalità di “importa” e “esporta” sono stati risolti i seguenti bug.

- Aggiunti controlli di consistenza durante l’import di un archivio: vengono verificate la presenta di tutti gli elementi riferiti dalle configurazioni, compreso le Token Policy.
- Mediante il processo di importazione di una govlet era possibile creare un nuovo applicativo o soggetto con le stesse credenziali di uno già esistente.
- Revisione delle govlet per gestire correttamente il soggetto referente di “default” per il Profilo API Gateway.
- Risolto problema presente durante l’esportazione di una API con Multi-Tenant abilitato e un soggetto selezionato in testata; l’archivio esportato era vuoto.
- L’esportazione di una erogazione, sulla quale era associato nel connettore un applicativo “server”, non veniva effettuata correttamente poichè tra gli elementi esportati non veniva inserito l’applicativo interno associato all’erogazione stessa.
- Importando un’archivio contenente una erogazione in cui era stato registrato nel controllo degli accessi un applicativo non esistente, l’operazione terminava con un errore inatteso. Aggiungendo l’applicativo mancante l’operazione terminava correttamente ma veniva generata una erogazione con stato disabilitato contenente erroneamente due gruppi (nell’erogazione originale esisteva solamente il gruppo predefinito). Entrambe le problematiche sono stati risolte.
- L’import di un archivio, contenente una una erogazione con connettore definito tramite Integration Manager, comportava una errata registrazione di un applicativo “client”.
- Se su un connettore veniva prima abilitata la consegna su Integration Manager, definendo delle credenziali basic, e poi successivamente disabilitata, le credenziali rimanevano erroneamente assegnato all’applicativo. Il problema si evidenziava effettuando una esportazione ed una successiva importazione dell’erogazione. Terminato il processo di import veniva creato erroneamente un applicativo che possedeva il nome interno dell’erogazione e le credenziali che inizialmente erano state assegnate alla funzione I.M.

Sulla console di monitoraggio sono stati risolti i seguenti bug:

- Ritornando alla lista delle transazioni, dopo aver visionato il dettaglio di una transazione, viene adesso mantenuto chiuso il filtro di ricerca in modo da permettere una immediata consultazione di una transazione successiva presente nell’elenco.
- Risolto problema di visualizzazione dei contenuti di messaggi formato da solamente 2 caratteri (es. un semplice text/plain “ok”) che visualizzava erroneamente un messaggio vuoto.

- Il download dei contenuti applicativi utilizza adesso la corretta estensione del file, in relazione al Content-Type, anche per una registrazione avvenuto con la funzionalità di "Dump Binario". Prima del fix veniva utilizzata sempre l'estensione ".bin".
- L'accesso al database è stato ottimizzato per alcune voci della console di monitoraggio che portano a pagine statiche e quindi non necessitano di query:
  - le voci del menù principale "Transazioni" e "Analisi Statistica"
  - le modalità di ricerca "ID Transazione" e "ID Messaggio".
- Corretto colore dei link visitati; veniva erroneamente utilizzato il colore associato all'hover.
- L'export, di qualsiasi tipo, non conteneva le informazioni riguardanti il tipo di api (REST/SOAP) e i tags.

Per le API di configurazione e monitoraggio sono stati risolti i seguenti bug:

- Adeguate interfacce OpenAPI 3 per utilizzare un discriminator interno agli oggetti elencati nelle strutture oneOf, come richiesto dalla specifica OpenAPI «https://swagger.io/docs/specification/data-models/inheritance-and-polymorphism/». Nelle precedenti versioni il discriminator utilizzato era un claim esterno agli oggetti riferiti nella struttura oneOf.
- Aggiunta la possibilità, durante la creazione di una erogazione o fruizione, di ridefinire un nome o una versione differente da quella dell'API implementata.
- Ripristino log relativo all'http status code ritornato nel log govway_api[Config,Monitor]_transaction.log
- Aggiunti controlli di robustezza durante la creazione di una erogazione o fruizione di API SOAP, al fine di verificare la presenza obbligatoria del claim "api_soap_servizio".
- Corretta descrizione "TAg" in govway_core.yaml.

18 Versione 3.3.0

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.3.0 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

18.1 Nuova funzionalità di registrazione di un Applicativo Server

Gli applicativi registrati su GovWay, dalla versione 3.3.0, possono essere di due tipi:

- *Client*: si tratta degli applicativi presenti anche nelle precedenti versioni, censiti allo scopo di identificarli ed autorizzarli durante l'invocazione di erogazioni o fruizioni di API;
- *Server*: un nuovo tipo di applicativo che consente di censire una applicazione di backend alla quale associare quelle informazioni tipicamente indicate sinora nella sezione "Connettore" dell'erogazione della API (endpoint, credenziali, ...). In una erogazione è così possibile riferire un applicativo server già registrato come modalità alternativa a quella di indicare esplicitamente tutte le informazioni richieste.

18.2 Nuova funzionalità di Load Balancer

Per le erogazioni di API è possibile definire connettori multipli con finalità di bilanciamento delle richieste in arrivo. Vengono forniti differenti tipi di bilanciamento del carico:

- *Round Robin*: le richieste vengono distribuite in ordine tra i connettori registrati;
- *Weight Round Robin*: rispetto al Round Robin consente di riequilibrare eventuali server eterogenei tramite una distribuzione bilanciata rispetto al peso associato ad ogni connettore;
- *Random*: le richieste vengono distribuite casualmente tra i connettori registrati;

- *Weight Random*: rispetto al Random si ha una distribuzione casuale che considerà però il peso associato ad ogni connettore;
- *Source IP hash*: combina l'indirizzo IP del client e l'eventuale indirizzo IP portato nell'header "Forwarded-For" per generare una chiave hash che viene designata per un connettore specifico;
- *Least Connections*: la richiesta viene indirizzata verso il connettore che ha il numero minimo di connessioni attive.

La configurazione permette anche di abilitare una sessione sticky in modo che tutte le richieste che presentano lo stesso id di sessione vengano servite tramite lo stesso connettore. Se l'identificativo di sessione si riferisce ad una nuova sessione, viene selezionato un connettore rispetto alla strategia indicata. L'identificativo di sessione utilizzato è individuabile tramite una delle seguenti modalità:

- *Cookie*: nome di un cookie;
- *Header HTTP*: nome di un header http;
- *Url di Invocazione*: espressione regolare applicata sulla url di invocazione;
- *Parametro della Url*: nome del parametro presente nella url di invocazione;
- *Contenuto*: espressione (xPath o jsonPath) utilizzata per estrarre un identificativo dal body della richiesta;
- *Client IP*: indirizzo IP del client;
- *X-Forwarded-For*: header http appartenente alla classe di header «Forwarded-For» o «Client-IP»;
- *Template*: l'identificativo di sessione è il risultato dell'istanziazione del template fornito rispetto ai dati della richiesta;
- *Freemarker Template*: l'identificativo di sessione è ottenuto tramite il processamento di un Freemarker Template;
- *Velocity Template*: l'identificativo di sessione è ottenuto tramite il processamento di un Velocity Template;

È infine possibile attivare un "Passive Health Check" che verifica la connettività verso i connettori configurati. Un utilizzo di un connettore che provoca un errore di connettività comporta la sua esclusione dal pool dei connettori utilizzabili per un intervallo di tempo configurabile.

18.3 Nuova funzionalità di Consegna Condizionale

Per le erogazioni di API è possibile definire connettori diversi, selezionati dinamicamente al verificarsi di specifiche condizioni.

Il connettore da utilizzare può essere selezionato in base al nome o a un filtro associato al connettore stesso. Il nome o il valore del filtro può essere estratto dalla richiesta attraverso una delle seguenti modalità:

- *Header HTTP*: nome di un header http;
- *Url di Invocazione*: espressione regolare applicata sulla url di invocazione;
- *Parametro della Url*: nome del parametro presente nella url di invocazione;
- *SOAPAction*: individua una operazione SOAP;
- *Contenuto*: espressione (xPath o jsonPath) utilizzata per estrarre un identificativo dal body della richiesta;
- *Client IP*: indirizzo IP del client;
- *X-Forwarded-For*: header http appartenente alla classe di header «Forwarded-For» o «Client-IP»;
- *Template*: l'identificativo di sessione è il risultato dell'istanziazione del template fornito rispetto ai dati della richiesta;
- *Freemarker Template*: l'identificativo di sessione è ottenuto tramite il processamento di un Freemarker Template;
- *Velocity Template*: l'identificativo di sessione è ottenuto tramite il processamento di un Velocity Template;

È infine possibile configurare l'erogazione per utilizzare uno specifico connettore di default nel caso la condizione non permetta di identificare alcun connettore all'interno del pool, o in alternativa per restituire un errore.

18.4 Miglioramenti alla Console di Monitoraggio

Sono stati apportati i seguenti miglioramenti:

- *Restyling grafico dello storico delle Transazioni*: le informazioni sulle transazioni vengono riportate tramite una nuova veste grafica, con un approccio non più tabellare ma orientato all'ottimizzazione degli spazi e del posizionamento delle informazioni di interesse per l'operatore. È stata inoltre rivista anche la maschera di dettaglio di una transazione al fine di suddividere in maniera più razionale le numerose informazioni presenti.
- *Nuovi esiti associati alle Transazioni*:
  - Token non Presente: la richiesta non presenta un token;
  - Autenticazione Token Fallita: nel token ricevuto non sono presenti dei claim configurati come obbligatori per l'accesso alla API;
  - API non Individuata: la richiesta non indirizza una API registrata sul Gateway;
  - Operazione non Individuata: la richiesta non indirizza un'operazione prevista sulla API invocata.
- *Nuovi criteri di ricerca delle Transazioni basate sugli esiti*: sia le ricerche nello storico che le informazioni statistiche possono adesso essere ricercate per due nuovi raggruppamenti degli esiti:
  - Errori di Consegna: in questo gruppo sono collezionate tutte le transazioni con esiti che individuano un errore generato dal backend applicativo (Fault Applicativi e/o codici di ritorno 4xx e 5xx) o un errore di connettività verso il backend.
  - Richieste Scartate: in questo gruppo sono collezionate tutte le transazioni con esiti che riguardano richieste di erogazione o fruizione malformate (es. api non individuate, operazioni non individuate, errori di autenticazione . . .)

  Inoltre per gli altri criteri di ricerca è sempre possibile indicare se le richieste scartate devono essere prese in considerazione o meno; per default le richieste scartate non vengono considerate ai fini del risultato della ricerca.
- *Numero di Risultati*: nello storico delle transazioni è adesso possibile indicare il numero di risultati della ricerca che si desidera ottenere (default: 25).

18.5 Java 11, A.S. e Librerie 3Parti

Dalla versione 3.3.0, GovWay introduce nuovi vincoli sulle versioni minime dei prodotti parte dello stack tecnologico utilizzato:

- La versione 11 di Java, una release di tipo LTS (Long-Term Support).
- Application Server: v18 per WildFly e v9 per Apache Tomcat.

Sono state inoltre aggiornate alle versioni più recenti tutte le librerie 3parti utilizzate.

19 Versione 3.2.2

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 3.2.2 di GovWay. Per un maggior dettaglio si può invece far riferimento al file ChangeLog di questa versione.

19.1 Miglioramenti alla Console di Gestione

Sono state introdotte le seguenti nuove funzionalità:

- *Nuova Versione API*: nel dettaglio di una API è adesso disponibile il pulsante di creazione di una nuova versione dell'API. Durante la creazione della nuova versione è possibile scegliere se fornire una nuova specifica dell'interfaccia o ereditarla (insieme alle azioni/risorse e agli allegati) dalla precedente.
- *Generazione http-basic password per un Applicativo/Soggetto*: in caso di registrazione di un applicativo o di un soggetto, con autenticazione di tipo http-basic, è ora presente un pulsante per il fill del campo password con una password generata random in accordo a criteri minimi di qualità. È stato inoltre aggiunto un vincolo di univocità sull'username associato ad un applicativo o ad soggetto.
- *Trasformazione del Contesto di Invocazione*: per una API di tipo REST, all'interno della trasformazione della richiesta nella sezione "trasporto", è adesso possibile modificare sia il metodo http che il path concatenato alla base url utilizzata per invocare l'applicativo di backend.

19.2 Correzione Bug Critico su Profilo "Fatturazione Elettronica"

L'identificativo SDI per FatturaPA viene definito come xsd:integer con totalDigits=12. In GovWay è stato erroneamente utilizzato il tipo java Integer, non potendo gestire correttamente i messaggi SDI (fatture ed esiti) con identificativo oltre il numero limite di 2147483647. Il problema è stato risolto adeguando la gestione del tipo dell'Identificativo SDI da Integer a String allineandosi così con quanto previsto nella FatturaB2B nella quale l'identificativo SDI viene definito come xsd:string con lunghezza da 1 a 36.

19.3 Miglioramenti all'Installer

Sono stati apportati i seguenti miglioramenti all'installer binario:

- È stato aggiunto il supporto per la nuova versione dell'application server "WildFly" 18.x
- Le directory "controlloTraffico", "dumpNonRealTime", "resources" e "attachments" vengono adesso configurate per essere generate nella logDir e non più nella workDir

19.4 Bug Fix

Sono stati risolti i seguenti bug:

- Corretta sezione "Configurazione in Load Balancing" della Guida di Installazione che presentava nomi di proprietà errati.
- Risolti alcuni problemi presenti nella diagnostica emessa per le funzionalità di trasformazione e gestione dei token.

Per la console di gestione sono stati risolti i seguenti bug:

- Non era possibile eliminare un'azione da una API di tipo SOAP se esisteva un'azione con lo stesso nome in un'altra API.
- La console produceva un errore non gestito al momento di registrare una nuova regola di Proxy Pass. Il problema sussisteva solamente su nuove installazioni dove non era mai stato effettuato il salvataggio della configurazione.

Sulla console di monitoraggio sono stati risolti i seguenti bug:

- Nella ricerca transazioni, in ciascuna delle ricerche per mittente (Token Info, Soggetto ecc..), quando veniva cambiata la Tipologia (Fruzione,Erogazione,Qualsiasi), scomparivano gli input sotto la sezione «Dati Mittente».
- Sia per la ricerca di transazioni che per la generazione di report statistici, quando il valore della lista "Tipologia" era indefinito, non veniva visualizzato il campo per la scelta del Soggetto Remoto.

Per le API di configurazione e monitoraggio sono stati risolti i seguenti bug:

- Le liste vengono adesso correttamente valorizzate con gli elementi “next”, “prev”, “last” e “first” attraverso url relative che preservano i parametri della query e non contengono la base url.
- Migliorate validazioni degli oggetti oneOf dove è stata agganciata una validazione sintattica degli oggetti forniti rispetto al parametro discriminator.
- Per l’API di monitoraggio:
  - Nei metodi GET è adesso possibile indicare il soggetto erogatore di una api.
  - Nei metodi POST è adesso possibile indicare, con tipologia di ricerca qualsiasi, il soggetto remoto e/o il soggetto erogatore di una api.
  - Nell’interfaccia yaml sono stati aggiunti i criteri di obbligatorietà per i campi “data_inizio” e “data_fine” dell’oggetto FiltroTemporale e per il campo tipo dell’oggetto FiltroEsito. Inoltre il FiltroMittenteErogazioneDistribuzioneSoggettoRemoto è stato modificato per utilizzare una enumeration personalizzata, relativamente al tipo di ricerca, che non contiene il soggetto.
- Nella API di configurazione, l’opzione “forward” relativa all’autenticazione basic o principal di un applicativo/soggetto veniva salvata con valore invertito.

20 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.

20.1 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.

20.2 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.

21 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.

21.1 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.

21.2 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.

21.3 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.

21.4 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*

21.5 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.

21.6 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.

21.7 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.

22 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.

22.1 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

22.2 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.

22.3 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.

22.4 Nuova funzionaltà di esposizione dei WSDL

Deprecato dalla versione 3.3.0: Il WSDL generato risulta diverso da quello effettivamente esposto dal backend, comportando potenziali errori di interoperabilità.

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"

22.5 Miglioramenti all'Installer

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

22.6 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.

23 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.

23.1 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.

23.2 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.

23.3 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.

23.4 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.

23.5 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.

23.6 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).

23.7 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.

23.8 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".

23.9 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.

23.10 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.

23.11 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.

23.12 Miglioramenti al profilo eDelivery

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

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

23.13 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

23.14 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).

23.15 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.

23.16 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.

23.17 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.

24 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.

24.1 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.

24.2 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.

24.3 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

24.4 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.

24.5 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.

24.6 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).

24.7 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.

24.8 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

25 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.