Release Notes di OpenSPCoop2

Indice

1 Versione 2.3.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 2.3.1 di OpenSPCoop. Per un elenco dettagliato dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al file ChangeLog di questa versione.

1.1 Miglioramenti all'Installer

Sono state apportati i seguenti miglioramenti all'Installer binario:

- *Datasource JBoss7/WildFly*; Modificati i datasource prodotti dall'installer per usare il prefisso 'java:/' per i nomi JNDI, come richiesto dagli application server JBoss7 e WildFly per la registrazione da console.
- *Datasource Tomcat8*; Aggiornati i Datasource generati dall'installer per la versione di Tomcat 8 per adeguare i parametri all'aggiornamento delle librerie apache commons pool e commons dbcp usate da Tomcat8 (passaggio alla versione 2 delle librerie). I Warning sollevati dal servlet container erano i seguenti:
  - WARNING Property maxActive is not used in DBCP2, use maxTotal instead.
  - WARNING Property maxWait is not used in DBCP2 , use maxWaitMillis instead.

1.2 Nuove funzionalità di Autenticazione

Sono state apportate i seguenti miglioramenti alle funzionalità di autenticazione:

- *Principal*; Introdotta la nuova tipologia di autenticazione 'principal' associabile ad un servizio applicativo. Con questa modalità l'autenticazione va configurata sull'application server o con qualunque altra modalità che permetta alla Porta di Dominio di accedere al principal tramite la api HttpServletRequest.getUserPrincipal().
- *Nuovi parametri nella fruizione*; Durante l'aggiunta di una fruizione sulla parte specifica di un accordo di servizio è ora possibile specificare la modalità di autenticazione prescelta (basic/ssl/principal/disabilitata).
- *Autenticazione dei Soggetti*; E' ora possibile gestire l'autenticazione del soggetto fruitore (basic/ssl/principal) sulla porta applicativa, con le stesse modalità già previste per i servizi applicativi sulla porta delegata.
- *Nuovi parametri nell'erogazione*; Durante l'aggiunta di una erogazione (parte specifica di un accordo di servizio) è ora possibile specificare la modalità di autenticazione prescelta (basic/ssl/principal/disabilitata).
- *Opzionale*; Nella definizione delle porte delegate e applicative è ora possibile configurare l'obbligatorietà o meno dell'autenticazione.

1.3 Nuove funzionalità di Autorizzazione

Sono state apportate i seguenti miglioramenti alle funzionalità di autorizzazione:

- *Ruoli*; E' ora possibile attribuire un ruolo a servizi applicativi e soggetti fruitori. La gestione dei ruoli può essere effettuata direttamente sulla console della Porta di Dominio (ruoli locali) o delegata all'Application Server o a qualunque altra modalità che permetta alla Porta di Dominio di accedere ai ruoli tramite la api HttpServletRequest.isUserInRole().
- *Autorizzazione sulla Porta Applicativa*; E' ora possibile gestire l'autorizzazione del fruitore sulla porta applicativa, con le stesse modalità già previste per i servizi applicativi sulla porta delegata.
- *Nuovi criteri di Autorizzazione*; Riviste le modalità di gestione dell'autorizzazione sulle porte delegate e applicative:
  - *autorizzazione dei client autenticati*; prevede di elencare puntualmente i servizi applicativi (PD) o i soggetti (PA) abilitati all'accesso.
  - *autorizzazione basata sui ruoli*; prevede di elencare i ruoli richiesti per l'abilitazione all'accesso.

  - *xacmlPolicy*; prevede di limitare l'accesso ai soli servizi applicativi (PD) o soggetti fruitori (PA) che soddisfano la policy XACML associata al servizio.

- *Nuovi parametri nella fruizione*; Durante l'aggiunta di una fruizione sulla parte specifica di un accordo di servizio è ora possibile specificare la modalità di autorizzazione prescelta.
- *Nuovi parametri nell'erogazione*; Durante l'aggiunta di una erogazione (parte specifica di un accordo di servizio) è ora possibile specificare la modalità di autorizzazione prescelta.

1.4 Miglioramenti sui connettori http/s

Sono state apportate i seguenti miglioramenti sui connettori http e https della porta di dominio:

- *Proxy*; Aggiunta la possibilità di impostare l'utilizzo di un proxy http sul singolo connettore.
- *Redirect/TransferEncoding*; Aggiunta una sezione di configurazione 'Opzioni Avanzate' sul singolo connettore. Tale sezione, accessibile in modalità 'avanzata', consente di:
  - abilitare la gestione di un eventuale redirect http restituito da un servizio, specificando anche il massimo numero di hop accettati;
  - scegliere la modalità di trasferimento dei dati (transfer-encoding-chunked o con content length fisso).
- *SSL Type*; Migliorata la configurabilità del connettore HTTPS tramite pddConsole. Il default è stato modificato in modo da fornire l'implementazione più recente disponibile sulla jvm su cui è in esecuzione la PdD. Inoltre le versioni disponibili del protocollo SSL impostabili vengono recuperate dinamicamente leggendo i protocolli supportati dalla jvm.
- *Informazioni Runtime*; Aggiunta, nella sezione 'Configurazione - Runtime', la voce 'Informazioni SSL' che mostra, per ogni SSLType, gli effettivi protocolli abilitati nella jvm su cui la PdD è in esecuzione. Inoltre sempre nella sezione 'Configurazione - Runtime' vengono ora mostrate, oltre alla versione di java anche molte altre informazioni riguardanti la jvm tra cui gli algoritmi di cifratura e firma. In questo modo è ora possibile sapere quale protocollo SSL venga effettivamente utilizzato rispetto alla tipologia configurata sul connettore https. La scelta può infatti variare a seconda della JVM. Ad es. sulla versione 1.7.0_75 di Oracle, se si utilizza il tipo SSL 'SSLv3', la comunicazione https verrà instaurata tramite 'TLSv1' poichè associato al tipo 'SSLv3' risulta abilitato solamente 'TLSv1'.

1.5 Nuovo Connettore 'File'

Introdotto un nuovo tipo di connettore che permette la serializzazione del messaggio in arrivo su file system. Il path dove serializzare il messaggio può essere indicato dinamicamente, basandosi su id della transazione, data di elaborazione, etc.

1.6 Miglioramenti su WSSecurity

Sono state apportate i seguenti miglioramenti per quanto concerne la gestione della sicurezza dei messaggi:

- *Asserzioni SAML*; Aggiunta la possibilità di creare asserzioni SAML (1.1 e 2.0) senza dover implementare una classe java di Callback. Tutti i parametri dell'asserzione SAML (Subject, AuthnStatement e Attributi) possono essere specificati in un file di properties associabile alla singola Porta Delegata o Porta Applicativa tramite la proprietà 'samlPropFile'. In tal modo nella maggior parte dei casi in cui serve generare una asserzione SAML non è più necessario ricorrere all'implementazione di una classe java di Callback.

  Detach Header WSSecurity; Aggiunta la possibilità di non effettuare il detach dell'header WSSecurity dopo che la PdD ne ha effettuato la verifica della validità. Il detach è disabilitabile tramite l'opzione 'detachHeaderWSSecurity=false'.

  Password Callback; La classe di utility *org.openspcoop2.security.utils.ExternalPWCallback* è stata estesa in modo che attui la risoluzione di variabili Java indicate all'interno del file di proprietà (es. user.${ENV1}=${ENV2}). Inoltre è stato aggiunto il refresh automatico del file di properties ogni minuto; refresh configurabile tramite la proprietà 'refresh=true/false'.
- *Integrazione SAML con XACMLPolicy*; Integrazione della validazione di un'asserzione SAML in WS-Security, tramite l'applicazione di una policy XACML. La validazione può avvenire direttamente sulla Porta di Dominio o utilizzando un Policy Decision Point remoto.

1.7 Miglioramenti alla Console di Gestione

Sono state apportate le seguenti modifiche alla pddConsole:

- *Restyling grafico*; Completo restyling grafico della console.
- *Criteri di Sicurezza sulle Password*; Aggiunti criteri di sicurezza sulle password delle utenze della console.
- *Stato di una Porta Delegata e Applicativa*; Aggiunta la possibilità di disabilitare temporaneamente una fruizione od una erogazione di servizio agendo sul nuovo parametro 'stato' presente nella porta delegata e nella porta applicativa.
- *Vincoli sui nomi*; Introdotti vincoli sui nomi degli oggetti registrabili:
  - Soggetti: solo lettere e numeri
  - Pdd, Ruoli, Accordi, Servizi, Azioni: NCName
  - Servizi Applicativi, Porte Delegate e Porte Applicative: NCName + carattere '/'
- *Runtime*; Estesa la sezione 'Runtime' al fine di visualizzare le seguenti ulteriori informazioni:
  - lunghezza delle chiavi accettate per la cifratura
  - informazioni sull'internazionalizzazione (Locale)
  - informazioni sul TimeZone
  - possibilità di attivare o disabilitare completamente il servizio 'porta delegata' (PD) e/o 'porta applicativa' (PA).

  Molti dettagli sulle nuove informazioni aggiunte sono presenti solamente all'interno del file di report scaricabile da questa sezione.

1.8 Bug Fix Protocollo Trasparente

Risolto problema legato alla non corretta interpretazione dell'header di integrazione openspcoop fornito dall'applicativo client in SOAP 1.2.

1.9 Bug Fix Protocollo SPCoop

L'header di Integrazione 'soap', in modalità backward compatibility, veniva prodotto con alcune differenze rispetto a quello generato da una versione di OpenSPCoop di generazione 1.x. Gli attributi 'SPCoopPdd' e 'SPCoopPddDetails' non erano presenti ed al loro posto venivano generati i gli attributi 'OpenSPCoop2Pdd' e 'OpenSPCoop2PddDetails'. La stessa problematica era presente per le modalità di integrazione 'trasporto' e 'urlBased'.

1.10 Bug Fix

Sono state apportati i seguenti bug fix al runtime della Porta di Dominio:

- *MTOM*; Corretto un problema nella gestione dei messaggi MTOM. I messaggi in transito venivano erroneamente "sbustati" dal protocollo MTOM ed il messaggio inoltrato al nodo successivo presentava nella SOAPEnvelope il contenuto in base64 dell'allegato, pur continuando a possedere anche l'attachment mtom.
- *SOAPFault FaultCode qualificato*; Risolto problema che si verificava in presenza di un SOAPFault applicativo contenente un elemento 'faultcode' qualificato con un prefisso che non corrispondeva a nessuna dichiarazione di namespace. Un tale SoapFault provocava un errore interno della PdD simile al seguente: "org.openspcoop2.protocol.sdk.ProtocolException: Comprensione stato non riuscita: null"
- *SOAPFault Detail*; Risolto un problema nella gestione, da parte della PdD, dell'elemento 'detail' di un SOAPFault applicativo. Un testo presente direttamente all'interno dell'element 'detail' (senza essere contenuto in alcun elemento xml) non veniva correttamente ritornato al client.

- *Handshake SSL*; Nel caso di fallimento dell'handshake ssl, durante l'utilizzo di un connettore di tipo 'https', la transazione andava in errore con un 'NullPointerException'. Il problema è stato corretto e adesso viene riportata l'eccezione corretta.

Sono state apportati i seguenti bug fix alla Console di Gestione:

- *Connettore HTTPS*; Risolto problema nella maschera di configurazione del connettore https che, in alcuni casi, causava il reset dei dati già inseriti durante la compilazione della form.
- *Importa/Esporta*; Corrette alcuni malfunzionamenti presenti nelle funzionalità 'Importa' ed 'Esporta' delle configurazioni:
  - l'importazione non abilitava le regole sulla sicurezza del messaggio, se presenti su porte delegate o applicative.
  - Un nome di servizio contenente '-' o altri caratteri speciali non veniva gestito correttamente. Per correggere questa problematica è stato necessario modificare il formato degli archivi. Rimangono comunque compatibili i vecchi formati.
  - Risolto un problema che si verificava durante l'esportazione di un accordo di servizio parte specifica in formato CNIPA. L'errore che si otteneva era il seguente: "RegistroOpenSPCoopUtilities.setImportLocation error: Riscontrato errore durante la lettura del wsdl: null"

2 Versione 2.3

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 2.3 di OpenSPCoop. Per un elenco dettagliato dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al file ChangeLog di questa versione.

2.1 Versione Java

Dalla versione 2.3 viene richiesta una versione di java 1.7 o superiore.

2.2 Nuove versione supportate dell'Application Server

Sono supportate le seguenti nuove piattaforme di Application Server:

- **WildFly 10.x**
- **WildFly 9.x**
- **Apache Tomcat 9.x**

Sono invece state deprecate e non più gestite dall'installer binario le seguenti versioni:

- **JBoss 6.x**
- **JBoss 5.x**
- **JBoss 4.x**

2.3 Librerie Terze Parti

Sono state aggiornate alle ultime versioni disponibili tutte le librerie terze parti usate dal software OpenSPCoop. Alcune degli aggiornamenti più significativi sono i seguenti:

- **Apache CXF (http://cxf.apache.org)**; aggiornamento alla release 3.1.x la quale richiede una versione di java 1.7 o superiore.
- **WSSecurity (https://ws.apache.org/wss4j/)**; aggiornamento alla release 2.1.x la quale richiede una versione di java 1.7 o superiore e supporta molte nuove funzionalità come indicato nel sito del progetto alle pagine https://ws.apache.org/wss4j/migration/wss4j e in https://ws.apache.org/wss4j/migration/wss4j21.html.
- **OpenSAML (https://wiki.shibboleth.net/confluence/display/OS30/Home)**; aggiornamento alla release 3.x.
- **Log4J (http://logging.apache.org/log4j/2.x/)**; aggiornamento alla release 2.x. Tutti i log vengono creati attraverso il bridge SLF4J (http://www.slf4j.org/)

2.4 Miglioramenti all'Installer

Sono state apportati i seguenti miglioramenti all'Installer binario:

- *Utenza*; L'utenza utilizzabile per accedere alle console 'pddConsole' e 'pddLoader' sono configurabili durante l'installer.
- *Datasource*; aggiunte sui datasource di riferimento generati dall'installer binario le configurazioni necessarie al riconoscimento di connessioni verso il database inattive ('idle'). Tali configurazioni sono necessarie in presenza di un firewall tra l'application server ed un database.

2.5 Miglioramenti alla Console di Gestione

Sono state apportate le seguenti modifiche alla pddConsole:

- *XSD Schema Collection*; Aggiunta alla console, in modalità avanzata, la possibilità di effettuare il download degli schemi XSD utilizzati dalla PdD per la validazione dei messaggi.
- *WSDL Definitorio*; La visualizzazione/gestione del 'wsdl definitorio' è adesso disponibile solamente per i protocolli che lo richiedono. Nei protocolli built-in della PdD è presente solo per il protocollo 'spcoop'.

2.6 Bug Fix

Sono state apportati i seguenti bug fix al runtime della Porta di Dominio:

- *PA su Protocollo Trasparente*; Risolto problema che si presentava durante l'identificazione dell'azione di una PortaApplicativa con modalità wsdlBased su protocollo trasparente. Il malfunzionamento si presentava se il nome della PA invocata presentava uno '/' nel nome.
- *Validazione Contenuti Applicativi*;
  - Risolto problema nella validazione di tipo 'WSDL' che faceva ignorare erroneamente eventuali informazioni di binding presenti nei WSDL logici.
  - Risolto bug che causava errori simile al seguente "com.ctc.wstx.exc.WstxParsingException: Non-default namespace can not map to empty URI (as per Namespace 1.0 # 2) in XML 1.0 documents at [row,col {unknown-source}]"
  - Risolto bug che causava errori simile al seguente "org.w3c.dom.DOMException: NOT_FOUND_ERR: An attempt is made to reference a node in a context where it does not exist"
  - Risolto bug che causava errori simile al seguente "INUSE_ATTRIBUTE_ERR: An attempt is made to add an attribute that is already in use elsewhere"
- *Identificazione WsdlBased e Correlazione Applicativa*; Risolto malfunzionamento che si verificava durante il riconoscimento WsdlBased e/o la correlazione applicativa in presenza di richieste SOAP che contenevano tra i nodi figli del body dei commenti.
- *Header SOAP con mustUnderstand senza actor*; Risolto problema che si presentava in presenza di header SOAP con attributo mustUnderstand valorizzato a true e attributo actor non presente. La PdD generava un errorre di processamento che presentava una descrizione simile alla seguente: "Namespace URI may not be null".
- *Connettore HTTP*; Risolto problema "Found Illegal character(s) in message header value ..." che poteva avvenire durante la spedizione http.

Sono state apportati i seguenti bug fix alla Console di Gestione:

- *Creazione Accordo Parte Comune in modalità avanzata*; Risolto problema che si verificava durante la creazione di un accordo di servizio parte specifica in modalità avanzata su application server tomcat. L'errore si presentava quando veniva premuto il tasto invio; la console riportava il seguente messaggio: "L'ultima operazione effettuata ha provocato un errore che ha reso l'interfaccia non utilizzabile". Con la modalita' di visualizzazione standard il problema non si presentava.
- *Schemi interni alla sezione types di un WSDL*; Risolto problema nel caricamento dei WSDL. Gli schemi xsd che risiedevano all'interno dei WSDL concettuali o logici venivano ignorati dalla PdD. Il problema è stato risolto associando all'accordo di servizio come allegati gli schemi interni ai wsdl (nella sezione types).

3 Versione 2.2.1

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 2.2.1 di OpenSPCoop. Per un elenco dettagliato dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al file ChangeLog di questa versione.

3.1 Evoluzioni - Porta di Dominio

Sono state apportate le seguenti modifiche alla porta di dominio

- *Diagnostica Generale*; perfezionati i messaggi diagnostici emessi dalla Porta per quanto concerne:
  - analisi del messaggio in ingresso
  - processo di autenticazione
  - processo di autorizzazione
  - validazione dei contenuti
  - message security
  - processamento mtom

  Per ogni funzionalità sopra elencata viene emesso un messaggio diagnostico di livello lowDebug, se la funzionalità è in stato disabilitato, per segnalarlo. Se la funzionalità è invece abilitata viene emesso un messaggio diagnostico di livello infoIntegration che indica "funzionalità in corso ..." e successivamente un ulteriore messaggio diagnostico per segnalare l'esito "funzionalità completata", di livello infoIntegration, se non occorrono errori o un diagnostico di livello errorIntegration se viene rilevato un errore. Ogni diagnostico contiene anche il tipo di operazione che viene effettuata (ad es. il tipo di autenticazione basic/ssl, il tipo di message security signature/encrypt ...)
- *Diagnostica relativa alla risoluzione del nome di un host*; in presenza di un problema di risoluzione del nome dell'host durante la fase di consegna di un messaggio applicativo o di inoltro di una busta, veniva generato un messaggio generico non abbastanza esemplificativo della problematica. Ad esempio utilizzando una url di consegna 'http://serverDemo/service' si otteneva il diagnostico:
  - Errore avvenuto durante la consegna HTTP: serverDemo

  Con la nuova diagnostica si otterrà invece il seguente messaggio:
  - Errore avvenuto durante la consegna HTTP: unknown host 'serverDemo'
- *Dump binario nei servizi in ingresso*; aggiunta la possibilità di configurare un dump binario dei dati 'RAW' che vengono scambiati nei servizi in ingresso sulla Porta Delegata e Porta Applicativa. La configurazione (attivabile nella sezione Configurazione in modalità avanzata della pddconsole) permette di abilitare il dump in maniera selettiva sui due canali (PD o PA). I dati 'RAW' vengono registrati su un file di log dedicato al canale:
  - Canale PD: openspcoop2_dumpBinarioPD.log
  - Canale PA: openspcoop2_dumpBinarioPA.log
- *Envelope SOAP senza Fault su errore trasporto*; una risposta ben formata (envelope SOAP senza Fault) presente in un http-body di una risposta insieme ad un codice di trasporto 500 non è compatibile con quanto indicato nel basic profile (R1111, (http://www.ws-i.org/profiles/basicprofile-1.1.html#HTTP_Success_Status_Codes). Tale comportamento non veniva segnalato in alcun modo dalla PdD a parte la segnalazione del diagnostico di errore per quanto concere l'errore di trasporto. Questo provocava confusione, poichè si vedeva nei diagnostici un errore di consegna ma poi la transazione terminava correttamente. Con il fix è stato aggiunto un diagnostico che evidenzia il comportamento anomalo. Inoltre è attivabile tramite opzione su file di proprietà la possibilità di far terminare in errore le transazioni che presentano questo caso anomalo. Per backward compatibility è rimasto il comportamento di non far terminare con errore la transazione, ma però viene sollevato un opportuno diagnostico.
- *WS-Security*; Implementata una nuova classe 'org.openspcoop2.security.utils.ExternalPWCallback' con la funzione di PWCallback nel contesto WSSecurity, che legge la password dinamicamente da un file. Il file da utilizzare può essere indicato nella configurazione openspcoop2.properties tramite la proprietà 'org.openspcoop2.pdd.messageSecurity.externalPWCallback.propertiesFil
  Per default il file di properties è atteso in /etc/openspcoop2/wssPassword.properties.

3.2 Miglioramenti alla Console di Gestione

Sono state apportate le seguenti modifiche alla pddConsole:

- *Informazioni di Runtime*; rinominata la sezione 'Configurazione Sistema' in 'Runtime' e aggiunto un collegamento diretto sul menù a sinistra della console. Questa sezione visualizza le informazioni sull'ambiente runtime della PdD, accedendo alle informazioni JMX di ogni singolo nodo. Estese le informazioni visualizzate in modo da poter conoscere anche le connessioni http in uscita attivate dal modulo InoltroBuste, le connessioni http in uscita attivate dal modulo ConsegnaContenutiApplicativi, le connessioni attive verso il database, e le connessioni attive verso il broker jms. Inoltre in questa sezione è possibile modificare il livello di logging della PdD senza doverla riavviare.
- *Personalizzazione del Titolo e Favicon*; aggiunta la possiblità di personalizzare il titolo visualizzato sulla console, attraverso una proprietà nel file di configurazione 'console.properties' che indica il titolo da visualizzare. E' stata inoltre aggiunta una favicon associata alla pddConsole.

3.3 Identificativi Protocollo Trasparente

Identificativi della Richiesta e della Risposta; reso parametrico la generazione degli identificativi della richiesta e della risposta sul protocollo trasparente. La proprietà 'org.openspcoop2.protocol.trasparente.id.uuid' nel file trasparente.properties pilota tale gestione. In caso la proprietà sia abilitata vengono generati sempre nuovi UUID. Altrimenti gli identificativi vengono generati con il formato 'yyyyMMddHHmmssSSS-uuidDellaTransazione[-response]'. Il default è impostato per la generazione di identificativi come nuovi UUID.

3.4 Bug Fix

Sono state apportati i seguenti bug fix:

- *Creazione Accordo Parte Comune con wsdl contenente parte Implementativa*; quando si procedeva alla creazione di un accordo di servizio parte comune utilizzando un wsdl che conteneva la parte implementativa (Binding e Service), la creazione andava in errore. L'errore segnalava impropriamente che il wsdl dichiarava più volte uno stesso portType.
- *Nuova versione di un Accordo Parte Comune* Quando veniva registrata una nuova versione di un accordo di servizio parte comune, non era possibile attivarla attraverso un accordo di servizio parte specifica senza prima eliminare la parte specifica che implementava la vecchia versione. L'attivazione di una nuova parte specifica che implementava la nuova versione della parte comune non era possibile soprattuto se il nome del port-type rimaneva invariato, poichè non è permesso creare più di un servizio con stesso tipo e nome erogato dallo stesso soggetto identificato anch'esso con tipo e nome. Per continuare a soddisfare il vincolo di unicità tipo/nome servizio e tipo/nome soggetto, ma poter gestire il versionamento degli accordi di servizio parte comune, è stata aggiunta la possibilità di modificare la versione della parte comune implementata da un accordo di servizio parte specifica. Con questa nuova funzionalità si potrà censire tutte le versioni dell'accordo di servizio parte comune sul registro e modificare di volta in volta la parte specifica aggiornandola rispetto all'ultima versione della parte comune (o ritornando indietro ad una precedente versione).
- *Modifica Accordo Parte Comune*; la modifica di un servizio interno ad un accordo di servizio parte comune, creato a partire dal caricamento tramite wsdl, provocava un errore SQL (FK constraint violated). Il problema è stato risolto.
- *Eliminazione di un'azione da un servizio di un Accordo Parte Comune*; non era possibile eliminare le azioni definite in un servizio di un accordo parte comune. Se si selezionava un'azione e poi "Rimuovi selezionati", l'azione rimaneva presente senza segnalare alcun problema.
- *Creazione di un Accordo Parte Specifica*; durante la creazione di un accordo parte specifica, se non viene indicato un servizio applicativo erogatore viene adesso segnalato un messaggio di errore. Il workflow di creazione di un accordo parte specifica erogato da un soggetto operativo sulla PdD, richiede una creazione precedente del servizio applicativo erogatore.
- *Nome PA generata automaticamente*; alla creazione di un accordo parte specifica veniva generata una Porta Applicativa con un nome che non rispettava la convenzione indicata nei manuali, se l'utente sceglieva prima un servizio e poi cambiava accordo parte comune.

- *Eliminazione Accordo Parte Specifica*; corretto problema che non consentiva l'eliminazione di un'accordo di servizio parte specifica se il tipo di database era Oracle.
- *Informazioni visualizzate nell'elenco dei Servizi Applicativi*; nella visualizzazione in modalità avanzata non veniva riportata la tipologia del servizio applicativo nell'elenco
- *Ricerca nell'elenco dei Servizi Applicativi*; la funzionalità di ricerca all'interno dell'elenco dei servizi applicativi (in presenza di un numero maggiore di 10 elementi) non memorizzava l'ultima ricerca effettuata, in caso l'operazione di filtro avvenisse come prima operazione effettuata dopo il login.
- *Message Security*; se venivano create delle regole di message-security sulla richiesta o sulla risposta di una PD o PA, e successivamente lo stato veniva riportato a disabilitato, l'header WSSecurity veniva comunque generato dalla PdD. L'unica maniera per non far generare l'header era quello di eliminare tutte le proprietà precedentemente inserite, quando lo stato era ancora abilitato. La risoluzione del problema ha comportato che la PdD riconosca correttamente lo stato 'disabilitato'.
- *Internet Explorer*; su Internet Explorer 10 dopo aver effettuato il login su pddConsole veniva fornito un menù laterale con una formattazione scorretta. Selezionando uno qualsiasi dei link presenti sul menu la formattazione si correggeva.
- *Connettore custom*; La gestione dell'opzione di debug, utilizzabile con l'interfaccia avanzata, non veniva correttamente gestita. L'indicazione di debug veniva ulteriormente aggiunta tra le proprietà custom oltre che impostata sul connettore. Sono inoltre stati sistemati bug minori relativi alle breadcump visualizzate.
- *Connettore custom su Internet Explorer*; la modifica di un Connettore di un Servizio Applicativo per impostare il tipo custom non funzionava in InternetExplore 11.
- *Importazione Archivi*; Aggiunta funzionalità di download del resoconto di una importazione. E' stato inoltre aggiunto supporto per l'eliminazione degli oggetti presenti in un package precedentemente caricato.

4 Versione 2.2

In questa sezione sono descritte le principali nuove funzionalità e i problemi risolti nella versione 2.2 di OpenSPCoop. Per un elenco dettagliato dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al ChangeLog di questa versione.

4.1 Protocollo SDI per la Fatturazione Elettronica

E' stata aggiunta al protocollo, per quanto concerne la fatturazione passiva, la possibilità di ricevere fatture nel formato P7M. Vengono gestiti correttamente entrambi i formati P7M indicati nella delibera CNIPA numero 45 del 9 Novembre 2009 all'articolo 21, comma 3 dove viene indicato che la fattura può essere ricevuta direttamente come rappresentazione binaria o codificata in base64.

Nel caso di utilizzo del canale SPCoop (alternativo a SDICoop) le fatture o i messaggi di servizio che transitano sulla PdD vengono gestiti tramite due protocolli: spcoop e sdi. In questa nuova versione sono stati aggiunti gli identificativi di entrambi i protocolli tra le informazioni tracciate, in modo da poter riconciliare sulle tracce una transazione di fatturazione elettronica, sia partendo da un identificativo SDI che partendo da un identificativo eGov.

Per maggiori informazioni sulla gestione della Fatturazione Elettronica in OpenSPCoop è possibile consultare il documento La Fatturazione Elettronica in ambiente OpenSPCoop

4.2 Protocollo SPCoop

Sono stati risolti i seguenti problemi di importazione degli archivi in formato CNIPA tramite la pddConsole:

- La funzionalità di FiltroDuplicati (obbligatorio LineeGuidaBustaEGov_V11) non veniva abilitato nelle azioni create in seguita all'importazione di un accordo di servizio parte comune.
- Per gli archivi CNIPA che non possedevano il mapping delle informazioni eGov ('ProfiloDiCollaborazione.wscp') l'interfaccia non permetteva di passare alla modalita' di configurazione manuale della sezione 'Acquisizione informazioni di protocollo', rendendo quindi impossibile procedere con l'importazione.

4.3 FunzionalitàÂ generiche della PdD

Header HTTP di Integrazione. Adeguato il trattamento degli header HTTP alla specifica HTTP 1.1 (RFC 7230), per quanto concerne le informazioni di integrazione inviate agli applicativi. I valori degli headers HTTP vengono adesso codificati tramite MIME encoding definito nella specifica RFC 2047 se contengono dei caratteri che non appartengono al charset S_ASCII. Il Charset S_ASCII, più restrittivo dell'ISO-8859-1 definito dal RFC 7230, viene consigliato nella specifica HTTP 1.1. La nuova funzionalità appena descritta è attivabile (default) o disattivabile da file di proprietà.

Connettori in Modalità di Debug. Aggiunta la possibilità di configurare il funzionamento di un connettore in 'debug mode' (tramite pddConsole in modalità avanzata). In tale modalità vengono salvate tutte le operazioni effettuate dal connettore in un file di log dedicato: openspcoop2_connettori.log. In 'debug mode' vengono inoltre salvati tutti i contenuti inviati e ricevuti sullo stream (es. stream http).

Cache. I parametri delle cache utilizzate dalla PdD sono adesso gestibili tramite pddConsole. Inoltre nella cache contenente i dati di autorizzazione vengono adesso collezionati anche i risultati di autorizzazione delle invocazioni di una PortaDelegata.

Sono stati risolti i seguenti problemi di trattamento dei messaggi soap:

- Risolto errore 'Security processing failed. ; error constructing MAC: java.lang.SecurityException: JCE cannot authenticate the provider BC' che si verificava nell'application server jboss7 in presenza di configurazioni Message-Security, attivate sulle porte delegate o applicative, che utilizzavano un keystore di tipo p12.
- Nel caso in cui l'applicativo ritornava un SOAPFault 1.2 contenente l'elemento 'Node', la PdD non lo propagava al Client, non garantendo quindi la totale trasparenza. Il problema è stato risolto.
- Risolto errore 'Unable to internalize message' che si presentava con messaggi senza attachments che possedevano il Content-Type 'multipart/related; ...type="application/xop+xml"'. Adesso anche questi messaggi 'anomali' vengono comunque gestiti dalla Porta di Dominio.

4.4 Interfaccia Grafica PddConsole

Sull'interfaccia di gestione della PdD sono stati risolti i seguenti problemi:

Consultazione Tracce e Diagnostici

- Per motivi di performance, durante la ricerca è adesso obbligatorio selezionare almeno uno dei seguenti criteri di ricerca: Intervallo Iniziale, ID Messaggio, ID Applicativo.
- Risolto problema presente nella consultazione dello storico in cui veniva ignorato il filtro per ID Messaggio durante l'esportazione xml.
- Disattivata funzionalità di auto-focus della data che veniva presentata all'utente, durante la consultazione, anche quando veniva modificato uno dei parametri di ricerca.
- Risolto problema di visualizzazione del dettaglio di un diagnostico che non veniva presentata correttamente dalla Console se il testo del messaggio diagnostico conteneva del codice html.

Gestione Porte Delegate e Applicative

- Per la gestioneManifest sulla PortaDelegata e PortaApplicativa è stata aggiunta la voce 'default' tra le opzioni possibili selezionabili durante la creazione o modifica, allo scopo di indicare che viene utilizzata l'indicazione registrata nella configurazione generale.
- Risolta problematica sulla modificata del nome di una PortaDelegata. La modifica non aveva effetto sulla sua invocazione (tramite il nuovo nome).
- Risolto problema che consentiva la registrazione di più porte applicative che erogavano lo stesso servizio e la stessa azione per lo stesso soggetto erogatore. Adesso questa configurazione non è più consentita.
- Le informazioni presenti nelle liste Erogatori/Servizi/Azioni all'interno delle form di add/edit delle porte delegate/applicative vengono adesso correttamente ordinate.

- Risolto problema che non consentiva l'eliminazione delle proprietà Message-Security, una volta aggiunta la proprietà con nome 'action'.

Gestine dei Connettori

- Introdotta possibilità di configurare il connettore in 'debug mode' se si accede in modalità avanzata.
- Migliorata maschera di gestione del connettore JMS.

Consultazione Auditing

- Per motivi di performance, durante la visualizzazione dell'auditing è adesso obbligatorio selezionare almeno uno dei seguenti criteri di ricerca: Intervallo Iniziale, Identificativo, Id precedente alla modifica.
- Disattivata funzionalità di auto-focus della data che veniva presentata all'utente, durante la consultazione, anche quando veniva modificato uno dei parametri di ricerca.

Altro

- Risolto problema di importazione degli archivi in formato 'openspcoop' che si presentava a seconda del criterio di ordinamento utilizzato dal compressore zip durante la creazione dell'archivio. E' stato aggiunto un pre-ordinamento in modo da navigare lo zip nell'ordine atteso (lessicografico crescente).
- Risolto schianto che si verificata selezionando il servizio applicativo visualizzato nella lista di un fruitore di un Accordo Servizio Parte Specifica.
- Sistemata la breadcrumb nella schermata che presenta la lista dei soggetti associati all porta di dominio.

5 Versione 2.1

In questa sezione sono descritte le principali nuove funzionalità introdotte nella versione 2.1 di OpenSPCoop. Per un elenco dei problemi risolti e per maggiori dettagli sulle funzionalità si può invece far riferimento al file ChangeLog di questa versione.

5.1 Gestione del protocollo SDI per la Fatturazione Elettronica

Oltre ai protocolli SPCoop e Trasparente, la nuova versione include il supporto nativo al protocollo SDI utilizzato per gli scambi di fatture elettroniche nell'ambito della pubblica amministrazione italiana (http://www.fatturapa.gov.it). La Porta di Dominio supporta sia lo scenario passivo che attivo, e viene rilasciata con configurazioni pronte per vari scenari di utilizzo. Per maggiori informazioni sulla gestione della Fatturazione Elettronica in OpenSPCoop è possibile consultare il documento La Fatturazione Elettronica in ambiente OpenSPCoop

5.2 Modificati contesti di default dei protocolli 'spcoop' e 'trasparente'

Il protocollo 'spcoop' è adesso indirizzabile attraverso le seguenti alternative url:

- *http://host/openspcoop2/spcoop/SERVICE*
- *http://host/openspcoop2/SERVICE*

Il protocollo 'trasparente' è adesso indirizzabile attraverso la seguente url:

- *http://host/openspcoop2/proxy/SERVICE*

SERVICE può assumere i valori PD, PA e IntegrationManager.

5.3 Restyling dell'interfaccia grafica PddConsole

L'interfaccia di gestione della PdD è stata significativamente rinnovata nell'ottica di una drastica semplificazione dei processi di configurazione. Di seguito una sintesi delle principali modifiche:

- *Semplificazione del menu di navigazione*. Il menu principale per l'accesso alle funzionalità della console è stato ristrutturato in modo da avere una forma più compatta.
- *Switch rapido tra modalità standard ed avanzata*. Si può passare dalla modalità standard a quella avanzata e viceversa in modo rapido tramite un link posto nell'intestazione. Molti elementi di configurazione di uso non comune sono stati migrati all'interfaccia avanzata allo scopo di semplificare le maschere standard di configurazione.
- *Scelta del protocollo*. In vari contesti è stata aggiunta la possibilità di selezionare il protocollo (spcoop, trasparente, sdi, ...) in modo da semplificare la compilazione delle maschere eliminando gli elementi non applicabili o aggiungendo quelli applicabili in base ai vari casi.
- *Semplificazione Servizi Applicativi*. La configurazione dei servizi applicativi è stata semplificata introducendo la scelta del ruolo (fruitore o erogatore). In base al ruolo scelto vengono mostrati i campi necessari al completamento della configurazione in un unico passo.
- *Configurazione Accordo Parte Comune guidata dal WSDL*. L'inserimento del WSDL comporta la generazione automatica dei rimanenti elementi di configurazione (port-type ed operations).
- *Accordi Cooperazione*. Gli elementi di configurazione degli accordi di cooperazione, utilizzati nel contesto SPCoop, venono gestiti da un nuovo permesso utente 'P' (disabilitato per default).
- *Configurazione Sistema*. Aggiunta la voce 'Configurazione Sistema' alla sezione 'Configurazione' che riporta le informazioni sull'installazione e permette il reset delle Cache.
- *Download delle interfacce WSDL*. Aggiunta la possibilità di effettuare il download dei WSDL caricati negli accordi di servizio.

5.4 Nuovo meccanismo di importazione delle configurazioni

Questa nuova funzionalità della PddConsole consente di importare interi blocchi di configurazione invece dei soli accordi di servizio. Gli archivi di importazione utilizzabili in questo contesto sono differenziati in base al protocollo.

5.5 Supporto MTOM

Aggiunta la possibilità di far gestire alla Porta di Dominio le funzionalità di supporto al protocollo MTOM/XOP per l'ottimizzazione dei messaggi XML contenenti file binari. Tale supporto è disponibile sia sulle richieste di fruizione che di erogazione consentendo ai servizi applicativi di mantenere compatibilità con il mondo esterno in vari scenari, ad esempio:

- *PortaDelegata*. Servizio Applicativo fruitore che non supporta MTOM ed erogatore che lo richiede. La PdD effettua il packaging MTOM sui messaggi da inviare all'erogatore. Sull'eventuale risposta dell'erogatore la PdD effettua il processo inverso, unpackaging MTOM, per fornire al servizio applicativo fruitore il messaggio nel formato standard.
- *PortaApplicativa*. Servizio Applicativo erogatore che non supporta MTOM e fruitore che invece invia pacchetti serializzati in mtom. Al contrario del caso precedente la PdD effettua l'unpackaging MTOM dei messaggi da inviare all'erogatore. Sull'eventuale risposta dell'erogatore la PdD effettua il packaging per fornire al servzio applicativo fruitore il messaggio nel formato MTOM.
- *Verifica*. In entrambi i casi descritti in precedenza la Porta può essere configurata per effettuare solamente una verifica che il messaggio ricevuto sia stato serializzato tramite protocollo MTOM/XOP. In questo caso la Porta non effettua alcuna trasformazione del messaggio.

5.6 Modalità di identificazione dell'azione wsdlBased

Aggiunta la nuova modalità di identificazione dell'azione *wsdlBased* nella configurazione di una porta delegata. Con questa nuova modalità il servizio applicativo fruitore non è più tenuto a specificare l'azione invocata, infatti la porta delegata è in grado di identificarla dall'analisi della struttura del messaggio inviato e dalla sua corrispondenza con quanto specificato nel WSDL presente per l'accordo di servizio.

5.7 Aggiunto supporto alla piattaforma database DB2

È ora possibile installare OpenSPCoop utilizzando la piattaforma database DB2.

6 Novità di OpenSPCoop-v2 rispetto ad OpenSPCoop

OpenSPCoop-v2 è una completa reingegnerizzazione del software OpenSPCoop che recepisce gran parte delle esperienze maturate nei principali progetti di cooperazione applicativa in cui OpenSPCoop è stato impiegato.

Nel seguito elenchiamo le principali novità introdotte in OpenSPCoop-v2.

6.1 Protocollo di Cooperazione personalizzabile tramite plugin

A differenza di OpenSPCoop, abilitato ad operare esclusivamente secondo la logica del protocollo SPCoop, OpenSPCoop2 basa tutte le sue funzionalità su un'astrazione del protocollo di cooperazione applicativa. OpenSPCoop2 è così in grado di supportare un qualunque protocollo di cooperazione tramite la programmazione di specifici **plugin**, realizzati utilizzando un apposito Software Development Kit.

L'SDK include anche un package **basic** che funge da acceleratore per le implementazioni di nuovi plugin, mettendo a disposizione del programmatore interi moduli con logiche di default che possono essere estesi o semplicemente adattatti per l'implementazione di un nuovo protocollo.

Un'importante protocollo realizzato come plugin di OpenSPCoop-v2 è il protocollo PdC di Acquirente Unico, usato per la realizzazione della Porta di Comunicazione del SII, l'infrastruttura di cooperazione applicativa realizzata da Acquirente Unico per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica e del gas.

6.2 Supporto Web Services Standard non-SPCoop

OpenSPCoop-v2 è in grado di gestire il routing di messaggi di Web Service standard (specifica SOAP 1.1 o 1.2), erogati o fruiti dal proprio dominio, grazie alla disponibilità di un plugin di protocollo trasparente. In questo caso la configurazione dei servizi è analoga a quella necessaria per SPCoop con l'unica differenza relativa al tipo utilizzato per la definizione del Soggetto. Questo dovrà essere un tipo abbinato al protocollo trasparente (per default il tipo **PROXY**). Per i servizi afferenti a tale Soggetto, non ci sarà quindi trasformazione del messaggio tramite le fasi di imbustamento/sbustamento SPCoop, ma la Porta di Dominio manterrà tutte le altre proprie possibili funzioni.

6.3 Configurazione dei servizi in modalità "Local Forward"

Per le configurazioni di servizi in loopback (cioè nei casi in cui fruitore ed erogatore siano gestiti dalla stessa Porta di Dominio) è stata aggiunta la possibilità di abilitare l'inoltro locale dalla porta delegata a quella applicativa saltando il processamento interno che la PdD attua per il protocollo di cooperazione gestito (imbustamento, tracciamento, ecc). Questa configurazione consente quindi di inviare un messaggio diretto dal fruitore all'erogatore sfruttando, a livello della PdD, i soli meccanismi disponibili nei componenti di integrazione (autenticazione, autorizzazione, ws-security, ecc).

6.4 Middleware di gestione SOAP basato su CXF

OpenSPCoop-v1 utilizza Axis come SOAP Engine, un progetto di grande valore storico, ma ormai non più supportato e non conforme quindi ai più recenti standard Web Services. In OpenSPCoop-v2 questo limite è stato superato adottando il software del progetto CXF.

6.5 Drastico miglioramento del supporto di WS-Security

OpenSPCoop utilizzava la libreria wss4j per supportare le funzionalità dello standard WS-Security. In OpenSPCoop2, oltre a wss4j, è stato introdotto l'uso del software **SoapBox**, già in uso nel progetto *UltraUSB*, del quale è stata effettuata una completa personalizzazione per gli scopi della cooperazione applicativa:

- Firma/cifratura degli attachments.
- Cifratura con chiave simmetrica.
- Gestione delle Certificate Revocation List per la firma digitale.
- Possibilità di definire Keystore dinamicamente determinati tramite informazioni di protocollo.

6.6 Arricchimento dei dati di tracciamento

Le informazioni inserite dalla Porta di Dominio nelle tracce sono state arricchite con ulteriori dati:

- Identificativi delle Porte di Dominio mittente e destinataria.
- Identificativo del Servizio Applicativo che ha prodotto e consegnato alla Porta di Dominio il messaggio.
- Dump XML dell'intestazione di protocollo del messaggio gestito.
- Informazioni di dettaglio riguardanti gli allegati al messaggio (mime-type, dimensioni, ecc.)
- Informazioni di dettaglio estratte dai dati di sicurezza presenti nel messaggio (digest)

6.7 Nuove piattaforme RDBMS supportate: HSQL e SQLServer

Sono state ampliate le piattaforme database già supportate da OpenSPCoop (MySQL, PostgreSQL e Oracle), migliorando così le possibilità di integrazione del prodotto con gli ambienti standard preesistenti. Le nuove piattaforme supportate sono:

- **MS SQLServer (http://www.microsoft.com/sqlserver)**
- **HSQLDB (http://hsqldb.org/)**

6.8 Nuove versione supportate dell'Application Server

Sono state ampliate le piattaforme Application Server già supportate dall'installer binario di OpenSPCoop. Le nuove piattaforme supportate sono:

- **JBossAS 6.x**
- **JBossAS 7.x**
- **WildFly 8.x**
- **Apache Tomcat**