ALLEGATO *A*

REGOLE TECNICO-OPERATIVE
PER L'USO DI STRUMENTI INFORMATICI E TELEMATICI NEL PROCESSO CIVILE

INDICE

DEFINIZIONI E ACRONIMI

Nel presente capitolo è riportata la descrizione dei termini, degli acronimi e delle abbreviazioni usate nel documento.

Acronimo	*Descrizione*
CdO	Consiglio dell'Ordine
CPECPT	Casella di Posta Elettronica Certificata Processo Telematico
DTD	Document Type Definition
GC	Gestore Centrale
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MIME	Multipurpose Internet Mail Extensions
PCT	Processo Civile Telematico
PdA	Punto di Accesso
PIN	Personal Identification Number
RDPIC	Ricevuta di presa in carico
ReGIndE	Registro Generale degli Indirizzi Elettronici
ReLIndE	Registro Locale degli Indirizzi Elettronici
RPC	Remote Procedure Call
RUG	Rete Unica della Giustizia
RUPA	Rete Unitaria della Pubblica Amministrazione
S/MIME	Secure Multipurpose Internet Mail Extensions
SIC	Sistema Informativo Civile
SICC	Sistema Informatico del Contenzioso Civile
SIL	Sistema Informativo del Lavoro
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SPC	Servizio Pubblico di Connessione
SSLv3	Secure Sockets Layer version 3
UG	Ufficio Giudiziario
UNEP	Ufficio Notifiche e Protesti
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

1 DESCRIZIONE DELL'ARCHITETTURA DEL SISTEMA

1.1 SCENARIO COMPLESSIVO ED ATTORI COINVOLTI

Il Processo telematico prevede il seguente scenario operativo:

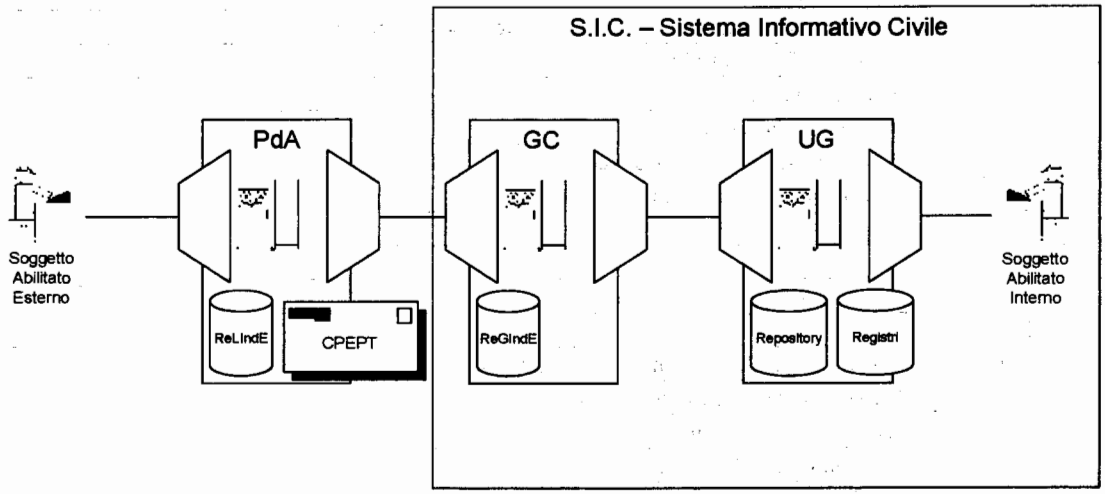

Figura 1 – Scenario operativo di riferimento

Dove:

- PdA = Punto di accesso
- GC = Gestore centrale
- UG = Ufficio Giudiziario

Nella fase 1.0 di sperimentazione, il contesto applicativo, oggetto di analisi e realizzazione, sarà limitato al solo Sistema Informativo del Contenzioso Civile (SICC) presso i Tribunali Ordinari; i Soggetti Abilitati Esterni saranno limitati ai soli Avvocati.

L'Avvocato può, già a partire dalla prima fase sperimentale (fase 1.0):

- redigere e firmare l'atto di parte: a tal fine si avvale di uno strumento di redazione (Redattore Atti) integrato con strumenti *software* per la firma, cifratura e imbustamento;
- depositare l'atto di parte (ricevendo la relativa attestazione temporale e successivamente la ricevuta elettronica di avvenuta presa in carico da parte dell'Ufficio Giudiziario);
- ricevere comunicazioni da parte dell'Ufficio Giudiziario nella propria "Casella di Posta Elettronica Certificata del Processo Telematico" (CPECPT);
- effettuare consultazioni dei fascicoli di propria pertinenza tramite l'evoluzione del PolisWeb (sito internet di consultazione disponibile agli avvocati abilitati).

L'Avvocato interagisce con il S.I.C. necessariamente per il tramite di un **Punto di Accesso Esterno** (PdA), presso cui è registrato come utente nel Registro Locale degli Indirizzi

Elettronici (ReLIndE).

Il PdA è quindi l'unico fornitore dei servizi di interfacciamento del "dominio giustizia" per gli Avvocati, autorizzato ad operare su provvedimento dell'Amministrazione. Questo in quanto offre ai propri Utenti una schermatura dei protocolli e dei formati di interfaccia previsti dal PCT per il colloquio con gli Uffici Giudiziari (UG), salvaguardando i principi di sicurezza e di riservatezza (tramite **autenticazione forte**) alla base della specifica problematica applicativa.

Presso il PdA è attivo un Registro Locale degli Indirizzi Elettronici (ReLIndE), che viene acceduto in fase di autenticazione, in fase di prelievo o consultazione dei messaggi provenienti dal SIC e in fase di deposito degli atti, per eseguire, se in possesso dell'albo elettronico del Consiglio dell'Ordine di appartenenza dell'Avvocato, la certificazione dello status del professionista.

Per quanto attiene alla ricezione di comunicazioni di cancelleria, il PdA fornirà all'avvocato una casella di posta elettronica certificata in aderenza alle specifiche dettate dal Centro Tecnico della RUPA, opportunamente adattate per il Processo Telematico.

Il **Gestore Centrale** (GC) svolge servizi di cooperazione allo scambio di dati che, pur non entrando nel merito delle richieste ricevute, consentono di assicurare la correttezza della composizione delle buste prodotte e di tracciare tutti i flussi applicativi, verificando il completamento dei relativi cicli logici.

Provvede cioè ad indirizzare le richieste inoltrate dai PdA, e originate dagli Avvocati, verso gli UG destinatari e viceversa a smistare ai relativi PdA le risposte o le comunicazioni provenienti dagli UG, sopperendo, grazie ad una architettura logica e fisica particolarmente robusta, alla eventuale indisponibilità temporanea dei relativi sistemi di colloquio.

Il GC associa automaticamente , ad ogni documento informatico pervenuto da un punto di accesso, un' attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti. Questa è inserita in un messaggio inviato alla casella di posta elettronica di servizio del Punto di Accesso, che provvede a renderla disponibile al mittente.

Il GC esegue inoltre, in fase di deposito di un atto, la certificazione sostitutiva del difensore, nei casi in cui il PdA mittente non sia tenuto, o non sia stato delegato, alla gestione dell'albo dell'Ordine professionale di appartenenza dell'Avvocato mittente. A tal fine è previsto che ciascun Consiglio dell'Ordine inoltri al GC l'elenco aggiornato dei propri iscritti all'albo.

L'entità rappresentata come Ufficio Giudiziario coincide tecnicamente con il cosiddetto **Gestore Locale**, ossia l'insieme di tutti i servizi applicativi del Processo Telematico esposti sia verso il Gestore Centrale sia verso i soggetti abilitati ed i sistemi interni.

In particolare all'interno di questa componente vengono realizzati tutti i sottosistemi per:

- la gestione delle fasi di controllo e accettazione dell'atto di parte;
- l'invio di eventuali eccezioni al mittente;
- la gestione dei diritti di visibilità sui dati;
- l'invio dei biglietti di cancelleria.

Il Gestore Locale gestisce, infine, l'interfacciamento tra il *Repository* Documentale (la base dati documentale, contenente tra l'altro il fascicolo informatico) e il SICC (gestione registri del Contenzioso Civile) per tutto ciò che concerne le operazioni a disposizione dei soggetti abilitati interni.

L'operatore di cancelleria e il Magistrato si interfacciano alle funzionalità del Processo Telematico attraverso l'applicativo SICC. Le evoluzioni del SICC permetteranno infatti l'accesso al fascicolo informatico non più solo come storico degli eventi, ma anche nel merito del contenuto degli atti di parte.

Il Cancelliere in particolare, potrà intervenire, attraverso componenti specifiche previste dalle evoluzioni del SICC, per gestire le eventuali situazioni di eccezione che si possono verificare in fase di ricezione, controllo e accettazione degli atti di parte.

1.2 BREVI CENNI ARCHITETTURALI

I flussi del Processo Telematico possono essere classificati per tipologia in invii documentali e consultazioni.

Dal punto di vista applicativo, la loro principale differenza è legata all'utilizzo di un differente protocollo di trasporto nella tratta tra PdA e GC. In particolare, per gli invii documentali, è previsto l'utilizzo di un meccanismo asincrono, basato sul protocollo SMTP, mentre per le consultazioni, si prevede l'utilizzo di soli meccanismi sincroni, basati su HTTPS.

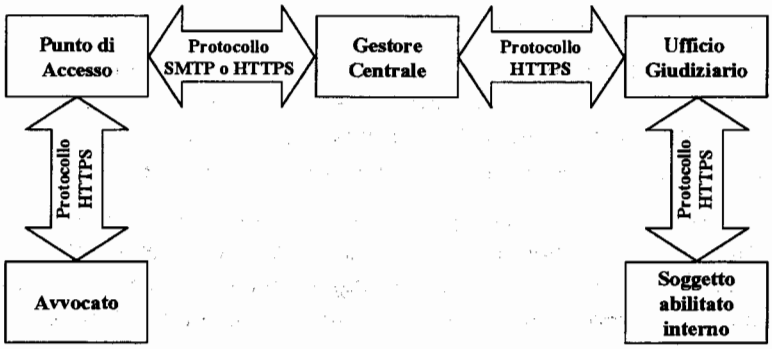

Figura 2 – Protocolli di trasporto

Gli Avvocati dovranno essere dotati di *smart card* contenenti:

- il certificato per la firma elettronica, rilasciato da un certificatore accreditato, in modo da garantire che quelle determinate credenziali siano riferite ad una persona fisica la cui identità è garantita dall'insieme dei processi di identificazione attuati dal certificatore stesso;
- il certificato di autenticazione, per la connessione al Punto di Accesso, rilasciato da una certification authority riconosciuta dal Punto di Accesso.

Sarà pertanto possibile l'utilizzo di una sola smart-card contenente entrambi i certificati oppure l'utilizzo di smart-card distinte. Sarà inoltre possibile dotarsi di più smart-card di autenticazione.

L'avvocato dovrà essere dotato inoltre di un certificato di crittografia necessario per decifrare gli atti criptati; questo dovrà avere lunghezza di chiave di almeno 1024 bit e potrà coincidere con il certificato di autenticazione.

Dal punto di vista pratico, dunque, gli Avvocati opereranno su *client* dotati di dispositivo di lettura della *smart card* e, nel momento di connessione al PdA, per il deposito o la consultazione, inseriranno il proprio PIN e presenteranno le proprie credenziali con cui verranno autenticati dal servizio, creando così un canale sicuro basato su protocollo SSLv3.

Gli UG saranno inoltre dotati di chiave e certificati di cifratura[1] per consentire che gli atti depositati vengano cifrati sul *client* dell'avvocato, con il certificato pubblico dell'UG destinatario, e che solo quest'ultimo possa procedere a decifrare e leggere gli atti stessi.

I PdA e il GC sono attestati su rete pubblica (SPC) e specificatamente su Interdominio RUPA; pertanto l'interazione tra le due entità, tanto in caso di utilizzo del protocollo sincrono (per le consultazioni dei procedimenti giudiziari) che asincrono (per gli invii documentali), fruisce delle garanzie di sicurezza offerta da tale rete. La tratta GC - UG sfrutta la Rete Unica della Giustizia (RUG).

In entrambi i casi si ipotizza comunque di instaurare sui protocolli sincroni una connessione sicura (SSLv3) mediante mutua autenticazione dei *server*.

1.3 SOTTOSISTEMI DISPONIBILI ALL'ESTERNO PER LA SPERIMENTAZIONE

Nel seguente paragrafo sono riportati i sottosistemi resi disponibili dall'Amministrazione ai soli fini di consentire la sperimentazione presso le sedi pilota.

Relativamente a tutti questi moduli software, l'Amministrazione, nell'ambito delle regole tecnico-operative, fornisce le necessarie specifiche (WSDL, DTD e quant'altro) per consentire a tutti i fornitori di software l'integrazione dei loro software con i servizi del Processo Telematico secondo la logica "application-to-application".

Stazione di lavoro dell' Avvocato È il sottosistema contenente l'insieme delle funzionalità fornite all'Avvocato al fine di consentirgli di compilare un atto, firmarlo digitalmente, criptarlo per l'UG di destinazione ed inoltrarlo al PdA di riferimento. A tale scopo si fornisce uno strumento di redazione atti, funzionalità per la firma e la crittografia e funzionalità per la spedizione, previa autenticazione ad un Punto di Accesso. Tale sottosistema consente di implementare i requisiti di strutturazione degli atti e la loro formattazione nello standard XML, secondo le specifiche che saranno riportate nelle Regole Tecniche.

Punto di Accesso (PdA) E' il sottosistema attraverso il quale l'Avvocato può interagire con il Sistema Informatico Civile. Per il tramite di apposite funzionalità, il PdA consente all'utente di:

- depositare atti presso un Ufficio Giudiziario e di ricevere i relativi messaggi di risposta da parte del SIC;
- ricevere nella CPECPT di un Avvocato un biglietto di cancelleria generato da un Ufficio Giudiziario, emettendo le ricevute previste dagli standard di posta certificata;
- accedere, tramite Polis Web, alle informazioni tenute dagli Uffici Giudiziari in termini di consultazione dei dati relativi ai fascicoli di competenza. Nell'ambito di tale sottosistema è oggetto di fornitura il solo front-end dell'applicazione PolisWeb, attivabile a seguito dell'autenticazione dell'utente al PdA.

[1] Si ipotizza che l'Amministrazione assuma in proprio la responsabilità della produzione e della distribuzione dei certificati server validi limitatamente alla operatività del Processo Telematico (in questo modo, ad esempio, potrebbero risultare più gestibili le problematiche di rinnovo dei certificati).

Sempre nella logica "application-to-application", le regole tecnico-operative forniscono le specifiche affinché ogni PdA fornito da terze parti possa costruirsi il proprio front-end per le consultazioni web, in eventuale sostituzione di PolisWeb (vedi sotto).

PolisWEB - Strumento di consultazione WEB E' il sottosistema costituito dall'applicazione per la consultazione Web delle informazioni contenute nei registri dei procedimenti, in ambiente SICC, e/o nei documenti afferenti ad un procedimento, in ambiente repository documentale. PolisWeb può essere utilizzato sia in ambiente Intranet (all'interno dell'UG, attraverso appositi "chioschi" informativi) che in ambiente Internet (attraverso il PdA).

1.4 FLUSSI PRINCIPALI

Il presente paragrafo descrive i principali flussi del sistema, rappresentando le interazioni tra le principali componenti di ciascun sottosistema, seguendo l'iter logico della redazione e del deposito di un atto.

1.4.1 Redazione dell'atto di parte

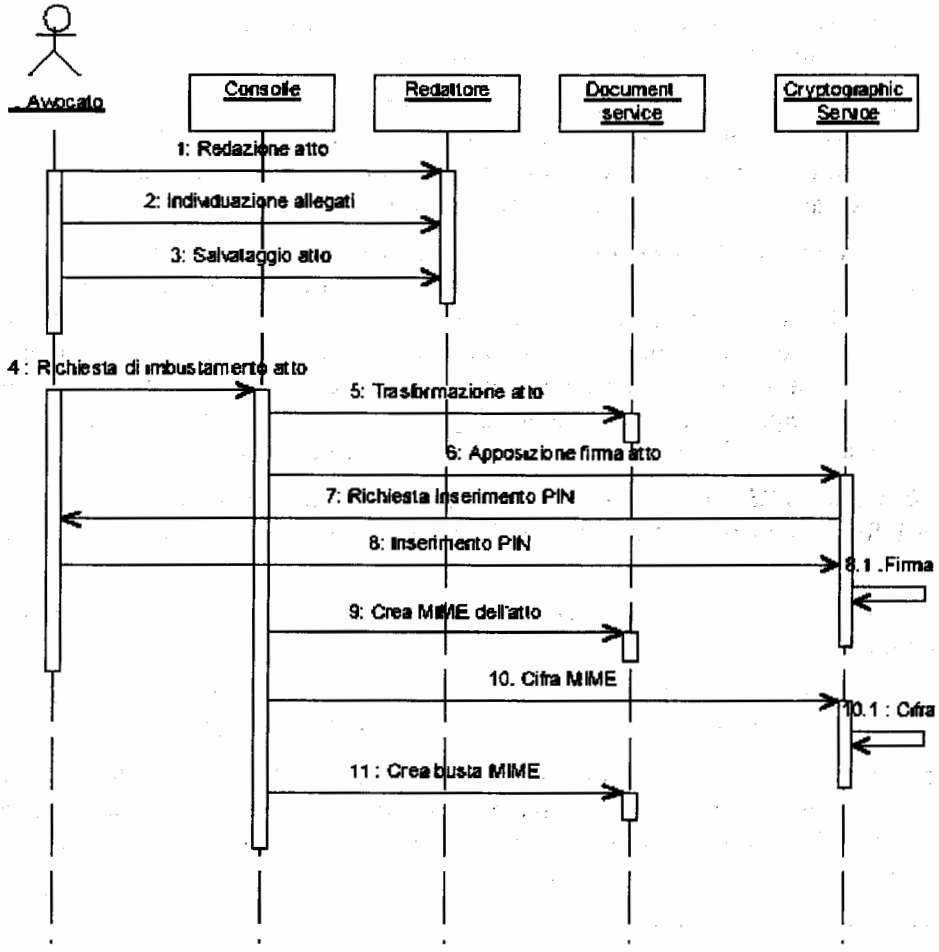

Figura 3 – Sequence diagram redazione e imbustamento atto

Nella Figura 3 è rappresentato il diagramma di sequenza relativo alla redazione dell'atto da parte dell'Avvocato e alla richiesta di imbustamento (necessario al successivo deposito dell'atto attraverso il PdA).

In particolare sono svolte le seguenti azioni:

1. L'avvocato scrive l'atto attraverso l'ambiente di redazione.
2. Individua i documenti da allegare all'atto.
3. Salva l'atto.
4. Al termine della redazione, dalla Consolle, l'Avvocato richiede l'imbustamento dell'atto.
5. L'atto viene convertito automaticamente in formato XML.

   L'atto potrà essere visualizzato e stampato, utilizzando un visualizzatore che aderisce allo standard Formatting Objects. È opportuno infatti far presente che questa sarà la visualizzazione "ufficiale", consigliata all'avvocato soprattutto per la stampa, in quanto la trasformazione da Word a XML potrebbe non essere fedele al 100%.
6. Viene richiesta l'operazione di firma dell'atto.
7. Viene richiesto all'Avvocato di inserire il PIN
8. L'Avvocato inserisce il PIN della Smartcard contenente il certificato digitale di firma.

   8.1 L'atto viene firmato
9. Viene creata la busta MIME dell'atto.
10. Viene richiesta l'operazione di cifratura del MIME dell'atto

    10.1 L'atto viene cifrato.
11. Viene creata la busta MIME contenente l'atto cifrato e le informazioni di instradamento all'UG.

A questo punto la busta è pronta per essere trasmessa attraverso la funzione di "deposito atto" messa a disposizione dal PdA.

Per attivare la funzione di "deposito atto" l'Avvocato si connette via internet con il proprio PdA, si autentica tramite smart-card e attiva la funzionalità di "deposito atto" che consente la trasmissione al PdA della busta memorizzata sulla postazione client.

La funzione di "deposito atto" prevede un flusso di trasmissione dell'atto informatico dal client dell'Avvocato che lo ha predisposto fino all'UG destinatario, cui farà seguito un messaggio di risposta da parte dell'UG per segnalare l'esito dell'atto depositato.

È inoltre previsto un ulteriore messaggio di risposta generato dal GC al momento della ricezione della richiesta di inoltro dell'atto all'UG. Tale risposta dipenderà dall'esito dei controlli eseguiti dal GC sulla busta inoltrata dal PdA. In caso di esito positivo detta risposta conterrà l'attestazione temporale dell'evento di ricezione della richiesta di deposito e la sua data di emissione avrà valore legale per la verifica dei termini di scadenza per la presentazione dell'atto, salvo verifica di buon fine dell'atto medesimo presso l'UG (verifica delle condizioni minime di accettabilità dell'atto). In caso di esito negativo, la risposta conterrà la segnalazione dell'errore riscontrato e bloccherà l'inoltro dell'atto all'UG.

A tale flusso collaborano:

- il PdA, che provvede all'inoltro materiale dell'atto informatico e alla ricezione e archiviazione del contenuto dei messaggi di risposta e alla contestuale emissione automatica di un messaggio di *Delivery Status Notification* (DSN);
- il GC, che provvede al deposito dell'atto presso l'UG indicato e, contestualmente, alla trasmissione del messaggio di attestazione temporale dell'evento di deposito;
- l'UG, che provvede alla acquisizione e pre-elaborazione dell'atto.

Le figure che seguono riassumono i flussi logici generati dalla funzione di "deposito atto":

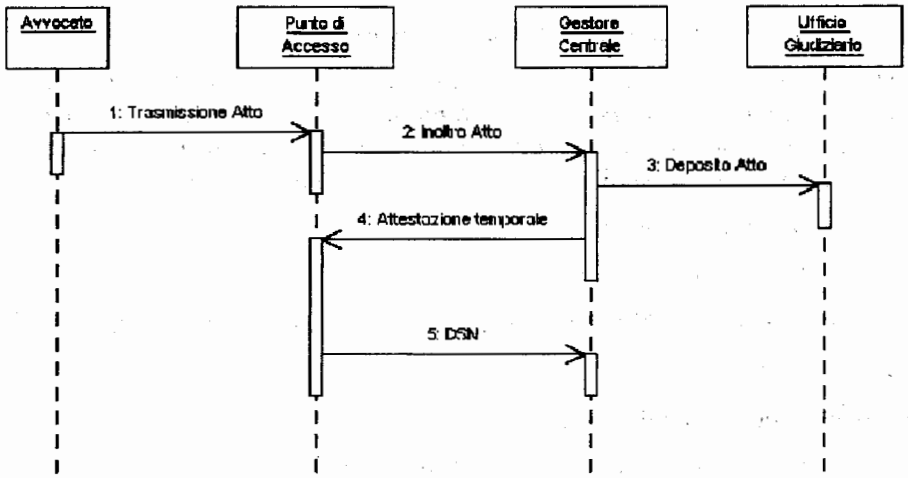

Figura 4 - Sequence diagram del deposito atto

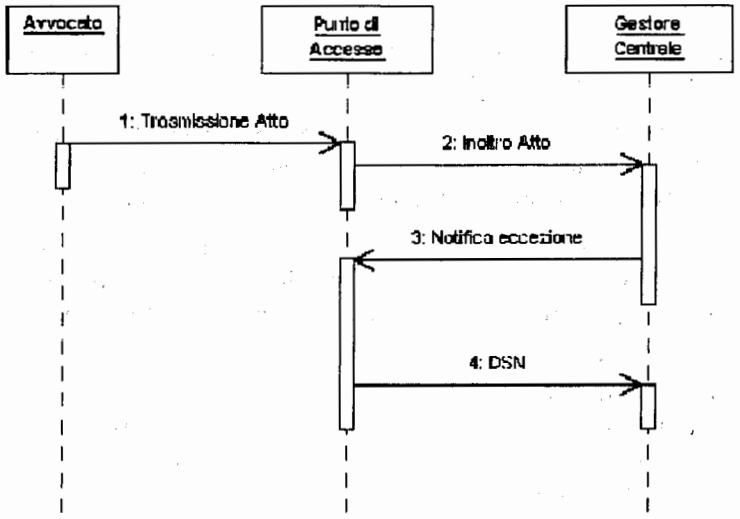

Figura 5 - Sequence diagram del deposito atto in caso di notifica di eccezione

1.4.2 Ricezione e accettazione dell'atto di parte

La Figura 6 mostra la sequenza delle operazioni eseguite nella fase di ricezione, da parte dell'UG, dell'atto di parte. Si vogliono qui evidenziare le interazioni di alto livello, le sequenze temporali, il ruolo del registro e del fascicolo informatico.

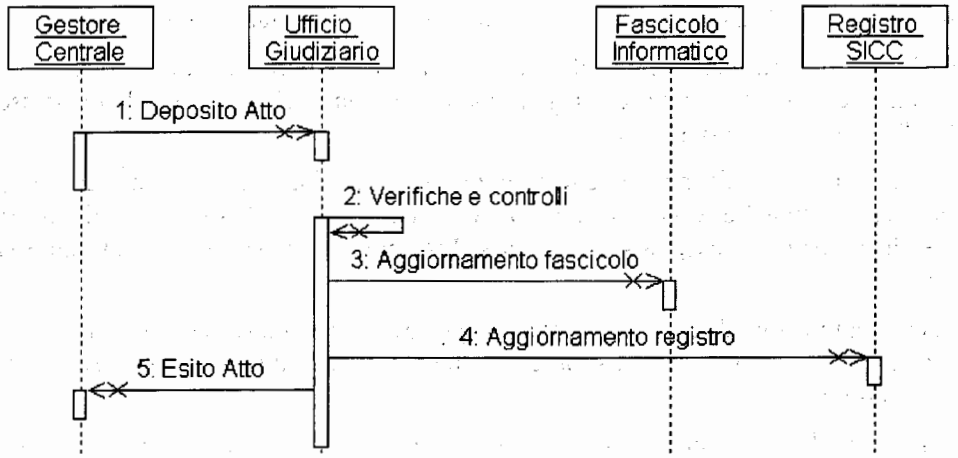

Figura 6 – Sequence diagram ricezione e accettazione atto di parte

Descrizione della figura:

1. Il Gestore Centrale invia i contenuti da depositare al sistema informatico dell'ufficio giudiziario.
2. In un istante temporale successivo alla ricezione, l'ufficio giudiziario attiva le procedure di verifica e controllo sui contenuti pervenuti.
3. I contenuti verificati vengono elaborati per l'aggiornamento del fascicolo informatico.
4. In base alle informazioni presenti nell'atto depositato si provvede all'aggiornamento del registro SICC.

A questo punto il deposito effettuato è visibile tramite i servizi di consultazione di Polis Web.

L'Ufficio giudiziario prepara ed invia una comunicazione di esito atto da far pervenire, tramite l'ausilio del Gestore Centrale, all'avvocato mittente.

1.4.3 Invio dell'esito di ricezione dell'atto all'Avvocato

L'invio della notifica di esito dell'atto prevede un flusso di risposta, di direzione opposta a quello del deposito, innescato dalla generazione di un messaggio di esito da parte dell'UG.

Il flusso si completa con il deposito nella casella di posta elettronica di servizio del Punto di Accesso del messaggio di notifica esito. A tale flusso collaborano:

- il GC, che provvede all'inoltro della notifica di esito;
- il PdA, che provvede all'emissione della ricevuta (DSN) per il GC ed a mettere a disposizione dell'Avvocato la notifica di esito.

1.4.4 Comunicazioni di cancelleria

La funzione di invio di un biglietto di cancelleria prevede un flusso di trasmissione di una comunicazione, prodotta dal Cancelliere, alle CPECPT di uno o più Avvocati, e di un flusso di risposta, di direzione opposta, innescato dalla emissione delle singole ricevute di presa in carico delle comunicazioni da parte dei PdA gestori delle CPECPT interessate.

Nella sua interezza il flusso nasce e si completa presso l'UG. A tale flusso collabora:

- il PdA, che genera una ricevuta di presa in carico per ogni messaggio ricevuto, ed una ricevuta breve di avvenuta consegna contestualmente al deposito dello stesso nella CPECPT dell'Avvocato indicato;
- il GC, che provvede all'inoltro delle comunicazioni ai destinatari indicati dall'UG (fase di invio), ed effettua l'attestazione temporale di ogni evento di ricezione di una ricevuta breve di avvenuta consegna da parte dei PdA, per restituirla all'UG mittente (fase di risposta).

Ai fini della valutazione di eventuali termini legali per la consegna della comunicazione, farà fede la data apposta dal GC in fase di attestazione temporale sulla ricevuta breve di avvenuta consegna prodotta dal PdA.

Nella fase 1.0 la funzione sarà limitata nell'invio ad un solo Avvocato. Pertanto, transitoriamente, l'UG dovrà generare tante comunicazioni, una per ogni Avvocato destinatario.

La creazione delle comunicazioni ad opera del cancelliere segue, in questa fase, le stesse modalità attualmente previste dal SICC. Tali comunicazioni, ed in particolare il loro contenuto, sono quindi costruite in maniera automatica dal client SICC evoluto per il processo telematico.

Le evoluzioni vanno nella direzione di gestire quali comunicazioni possono essere inoltrate per via telematica e quali devono essere cartacee mantenendo quindi piena compatibilità con le attuali modalità. Il sistema di cancelleria sarà in grado di gestire in maniera autonoma tali situazioni miste, evitando di chiedere all'utente di cancelleria un intervento manuale per discriminare cosa gestire in cartaceo e cosa in telematico.

La notifica attraverso il sistema del processo telematico prevede quindi che il client SICC crei il contenuto della comunicazione e lo depositi nel sistema di invio dell'UG includendo le informazioni necessarie ad identificare il destinatario (codice fiscale dell'avvocato).

Anche il biglietto di cancelleria, come gli atti di parte, è strutturato secondo il formato XML. La strutturazione data in questa prima fase è tuttavia molto semplice e si limita di fatto ad identificare l'oggetto della comunicazione, il contenuto della stessa e il riferimento al fascicolo di cui fa parte.

Dal punto di vista tecnico il sistema di cancelleria identifica ogni comunicazione con un identificatore univoco che permetterà di legare la comunicazione stessa alla ricevuta di deposito restituita dal GC. Il fascicolo informatico tiene infatti traccia di ogni comunicazione inviata e della relativa ricevuta di consegna.

1.4.5 Evoluzione PolisWeb: consultazione web delle informazioni SICC e del fascicolo informatico

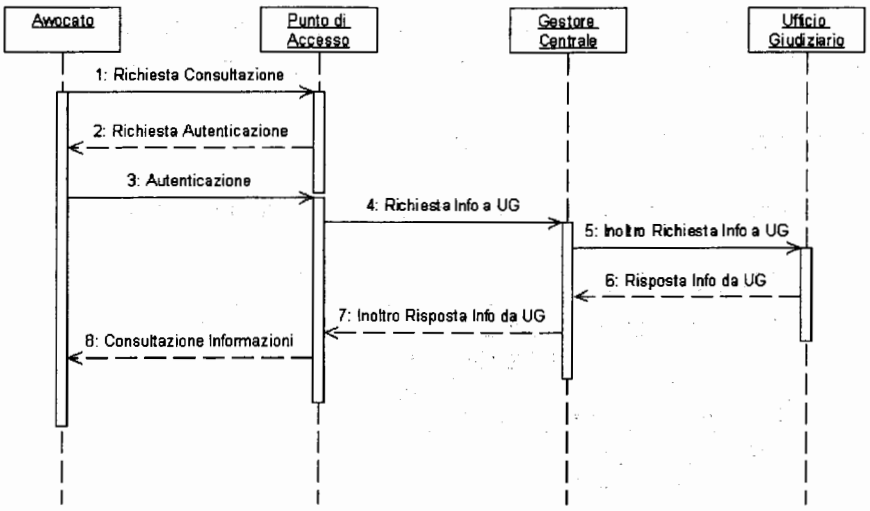

Figura 7 - Sequence diagram Consultazione Web

Nella Figura 7 è rappresentato il diagramma di sequenza relativo alla consultazione dei procedimenti personali e degli atti tramite l'applicazione Polis Web fornita sul Punto di accesso. In particolare sono svolte le seguenti azioni:

- L'avvocato sottopone a Polis Web, presente sul PdA, una richiesta di consultazione;
- Il PdA autentica l'utente, se questi non è gia stato precedentemente autenticato, e inoltra la richiesta all'Ufficio Giudiziario, per il tramite del Gestore Centrale;
- Un apposito sottosistema, all'interno dell'UG, predispone le informazioni ottenute a seguito dell'interrogazione del SICC e del sottosistema di gestione del fascicolo informatico (repository documentale) e le inoltra al PdA, per il tramite del GC;
- Polis Web presenta le informazioni in consultazione all'Avvocato.

2 DESCRIZIONE DELLE PRINCIPALI FUNZIONALITÀ

Si precisa che gli strumenti software a disposizione dell'avvocato, descritti in questo capitolo, sono forniti dal Ministero della Giustizia ai soli fini della sperimentazione.

2.1 ATTI DI PARTE COINVOLTI NELLA FASE 1.0

Di seguito è riportato l'elenco degli atti di parte di cui è possibile la redazione e il deposito in fase 1.0:

Atto di Citazione
Nota di Iscrizione a Ruolo
Atto di citazione in opposizione a d. i.
Ricorso per ingiunzione art. 633 cpc
Ricorso per ingiunzione artt. 633 e 642 cpc
Ricorso per consegna di cose fungibili
Ricorso per sequestro giudiziario *ante causam*
Ricorso per sequestro conservativo *ante causam*
Reclamo avverso provvedimento cautelare
Ricorso per separazione
Ricorso per divorzio
Comparsa di costituzione e risposta
Comparsa di costituzione con domanda riconvenzionale
Comparsa di costituzione con chiamata di terzo
Memoria generica
Comparsa ex art. 180 cpc
Memoria ex art. 183
Replica ex art. 183 cpc
Memoria ex art. 184
Replica ex art. 184
Comparsa conclusionale ex art. 190
Memoria conclusionale di replica ex art. 190

Il modello proposto per ciascun atto tiene conto della normativa di riferimento e su di esso è stata studiata una suddivisione strutturale basata sull'analisi dei principali formulari in commercio ulteriormente arricchiti, per i profili informativi in esame, dal lavoro svolto in sede di analisi.

È importante sottolineare che, la linea guida seguita in fase di analisi nella definizione di tali campi, è stata quella di optare comunque per il **carattere opzionale di ogni altro campo e sezione**, liberamente componibile dall'avvocato nella successione argomentativa dallo stesso ritenuta più idonea, qualora la valorizzazione del campo in oggetto non derivi da vincoli imposti dalla logica stati-eventi del sistema SICC, ossia in sostanza non sia necessaria per l'inserimento dell'evento.

La strutturazione dei modelli DTD (Document Type Definition) è pubblicata con apposito decreto ministeriale a parte.

2.2 L'AMBIENTE DEL REDATTORE SPERIMENTALE

L'ambiente di redazione è uno strumento integrato in *Microsoft Word* che consente la predisposizione dell'atto per la successiva trasformazione in formato XML.

Attraverso gli strumenti applicativi disponibili in Word, l'utente redige l'atto, nelle sue parti obbligatorie ed opzionali. Le funzionalità disponibili in fase di redazione, sono attivabili in diversi modi, per esempio attraverso una barra degli strumenti, un menù o abbreviazioni da tastiera.

Le funzionalità native di MS Word sono utilizzate, dove possibile, nell'ambiente di redazione, mentre quelle non consentite sono disabilitate all'utente.

L'ambiente di *editing* è lo stesso di un normale documento Word, e viene proposto all'utente dopo un apposito data-entry per i dati configurati come obbligatori nel modello di atto scelto.

Si ribadisce che tale obbligatorietà si riferisce ai dati necessari per registrare l'evento SICC.

Il Sistema, avendo a disposizione un modello ed un documento di default per l'atto che l'utente ha deciso di redigere, presenterà nell'ambiente di redazione un documento con:

- una intestazione contenente tutti i dati definiti come obbligatori nel modello stesso;
- una serie di sezioni (il cui ordine è definito nel modello, ma può essere modificato in fase di data-entry iniziale) riempibili opzionalmente a cura dell'utente Avvocato;
- una formula testuale pre-determinata per ogni sezione, che potrà essere modificata e/o cancellata dall'utente solo sull'Atto stesso senza lasciare parti di testo inconsistenti o righe vuote se non espressamente inserite.

Il Documento Word è, così, organizzato come un insieme gerarchico di Sezioni e Campi, secondo una struttura ad albero: l'intero documento costituisce il Campo radice (root, comune a tutti gli Atti) che può contenere testo e/o Campi figli, e così via, ricorsivamente, esattamente come avviene per i documenti XML. Pertanto ogni parte del Documento appartiene ad un Campo e ogni Campo ne può contenere altri. I Campi del Documento corrispondono biunivocamente ai nodi dell'XML.

Il Sistema permette inoltre all'utente Avvocato di inserire all'interno di ciascuna sezione uno o più campi strutturati (suggeriti dal sistema stesso), e di norma opzionali, la cui compilazione, nel caso di dati complessi, è guidata tramite una finestra di inserimento che controlla l'obbligatorietà o l'opzionalità dei dati stessi contenuti nel campo.

Durante la fase di redazione vera e propria, l'applicativo esercita un costante controllo sull'attività dell'utente al fine di sincronizzare il contesto alla posizione corrente di redazione nel Documento: in ogni istante, lo Strumento di Redazione abilita esclusivamente le funzioni valide nel nodo corrente. Inoltre, impedisce modifiche alla struttura, al fine di garantire la creazione di file XML validi rispetto ai requisiti definiti per il singolo Atto con l'ausilio dei DTD.

L'atto in formato XML, conforme ai DTD previsti dall'Amministrazione, è ottenuto a partire dal formato Word mediante l'esecuzione di procedure specifiche ed automatiche. Il formato dell'Atto XML include, oltre alle marcature "semantiche", ove previsto, anche le informazioni di formattazione del testo.

L'ambiente di redazione così strutturato ha carattere sperimentale e la sua progettazione tiene conto dell'esigenza di apertura verso eventuali indicazioni da parte degli utenti Avvocati che,

durante la sperimentazione, potranno validare le scelte funzionali fatte e contribuire ad un'evoluzione migliorativa dell'applicazione.

La logica progettuale sarà, in ogni caso, "application to application", ossia mira alla realizzazione di un'integrazione tra applicazioni in modo tale da consentire loro di interagire e scambiarsi dati in modo autonomo.

Si aggiunge infine che la scelta, operata per la fase di sperimentazione, è quella di ***non introdurre vincoli di alcun tipo*** *all'accettabilità dell'atto, fermo restando le informazioni essenziali che consentono di farlo pervenire all'ufficio giudiziario destinatario.*

2.3 CIFRATURA E FIRMA DELL'ATTO DI PARTE

L'atto redatto sulla postazione client deve essere firmato e cifrato per l'Ufficio Giudiziario di destinazione.

La modalità di apposizione della firma individuata, denominata **firme indipendenti (meccanismo "aggiungi una firma")**, prevede che uno o più soggetti firmano digitalmente lo stesso documento. L'ordine di apposizione delle firme degli N firmatari non è significativo, ed il file generato si presenta con un'unica estensione *p7m*.

La struttura è quindi PKCS#7 in cui sono contenute le N firme che si riferiscono quindi, al medesimo documento. Non è possibile utilizzare tale meccanismo per stabilire l'ordine in cui le firme stesse sono state apposte: una alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica PKCS#7.

Tale meccanismo è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

In Figura 8 è rappresenta la struttura PKCS#7 del file firmato.

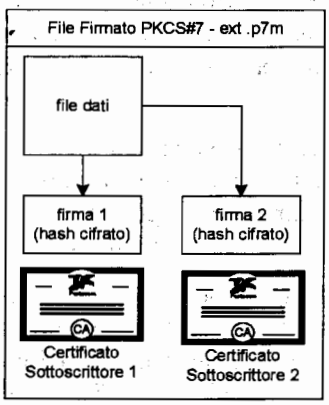

Figura 8 – Struttura del file firmato

Per la fase 1.0 del progetto si prevede l'apposizione della firma singola, ovvero effettuata da un unico firmatario.

Tali oggetti, creati sulla postazione dell'avvocato, vengono aggregati, ai fini del deposito, in un'opportuna struttura dati denominata "busta MIME" che contiene le informazioni di

instradamento, i riferimenti ai documenti atto ed allegati, l'atto firmato (*corpoatto.xml.p7m*) e gli eventuali allegati (nella figura che segue l'allegato è *AllegatoX.pdf.p7m*) .

Di seguito viene rappresentata la struttura dell'oggetto MIME, di cui è fornito apposito DTD.

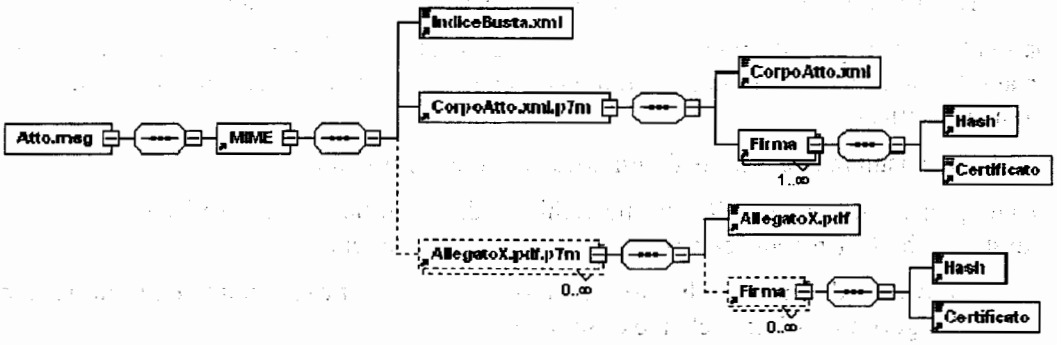

Figura 9 - Struttura MIME contenente l'atto i suoi allegati e l'indice degli stessi

La busta così composta è successivamente cifrata per l'ufficio giudiziario di destinazione, in modo che soltanto questo ufficio possa decifrarlo e quindi leggere il contenuto della busta.

Lo standard previsto è il PKCS #7.

"Atto.msg" è l'atto cifrato con chiave di sessione. "ChiaveSessione" è la chiave di sessione cifrata con il certificato del destinatario. "Issuer Dname" è il *Distinguished Name* della CA che ha emesso il certificato dell'ufficio giudiziario destinatario, "*Serial Number*" è il numero seriale del certificato dell'ufficio giudiziario destinatario. Tali dati sono necessari per il controllo successivo in fase di decifratura ed identificano il certificato con cui è stato cifrato l'oggetto.

Di seguito viene rappresentato lo schema della busta ottenuta a seguito del processo di cifratura dell'oggetto mime contenuto nell'oggetto Atto.msg.

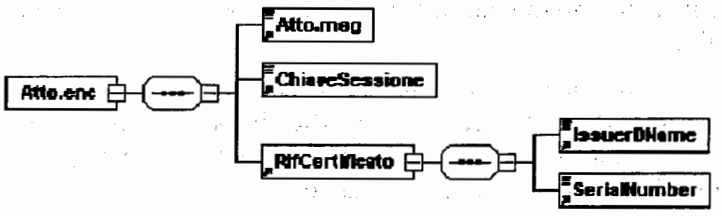

Figura 10 - Schema del risultato dell'operazione di cifratura di Atto.msg

L'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione vengono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario con il quale si intende corrispondere.

Tale busta sarà successivamente depositata presso l'Ufficio Giudiziario per il tramite del Punto di Accesso e del Gestore Centrale.

Relativamente alla cifratura degli atti in uscita, ossia cifrati a cura del gestore locale con la chiave pubblica del soggetto abilitato esterno (disponibile sul registro generale degli indirizzi presso il gestore centrale), si applicano le stesse specifiche sopra riportate.

In particolare, per gli atti inviati alla casella di posta certificata del destinatario, verrà utilizzata la medesima struttura di *atto.enc*, che verrà allegato al messaggio di posta elettronica certificata.

Ai fini della consultazione web degli atti, sarà valido quanto segue:

- il GL prepara la risposta SOAP alla richiesta di consultazione e inserisce all'interno di questa un "blob" (in codifica base64) che a sua volta contiene:
  - L'XML dell'atto richiesto, cifrato con crittografia simmetrica utilizzando l'algoritmo 3-DES e chiave di sessione;
  - la chiave di sessione cifrata con la chiave pubblica del certificato di cifratura dell'Avvocato;
  - il certificato utilizzato per la cifratura.
- Il Front-End di Polis Web riceve la risposta SOAP, estrae il "blob" e prepara la risposta HTML inserendo all'interno di essa il "blob".

2.4 RICEZIONE E ACCETTAZIONE DELL'ATTO DI PARTE

Nel presente paragrafo sono analizzate le funzionalità dei componenti tecnologici ad ausilio della cancelleria coinvolti nella fase di ricezione e accettazione dell'atto di parte. In particolare l'attenzione sarà posta sulla gestione delle potenziali situazioni di errore, sia di tipo strettamente tecnico che nel merito del contenuto dell'atto, sull'interfacciamento con il SICC, sulla gestione del fascicolo elettronico e infine sulla modalità con cui la cancelleria comunica all'avvocato mittente l'esito delle operazioni compiute a seguito della ricezione dell'atto.

L'analisi dell'intera infrastruttura dell'UG avrà come necessario punto di partenza la qualità progettata per il SICC che, come richiesto anche dal capitolato tecnico del presente progetto, non dovrà essere in alcun modo intaccata in quanto ha permesso di raggiungere un notevole livello di affidabilità.

Nel momento in cui l'atto viene ricevuto dalla cancelleria l'avvocato mittente ha già ricevuto l'attestazione temporale da parte del GC che ufficializza l'avvenuto deposito dell'atto nel dominio giustizia. E' infatti il GC che funge da "sportello virtuale" per l'avvocato verso il sistema informativo del Processo Civile Telematico.

E' quindi importante distinguere i tre momenti temporali di seguito definiti:

a) **il deposito**, scandito dal GC ed in riferimento al quale è necessario verificare le eventuali scadenze dei termini per il deposito stesso;

b) **la ricezione** da parte dell'UG;

c) **l'accettazione da parte del sistema di cancelleria** a seguito della quale viene scatenato l'evento del SICC e viene concessa visibilità dell'atto, a tutte le parti coinvolte nel procedimento giudiziario, inserendolo nel fascicolo elettronico.

Il ruolo del GC è definito dalle specifiche del presente progetto in sede di capitolato tecnico e quindi la distinzione tra i primi due punti è di fatto obbligata. L'introduzione dell'ultimo asincronismo, tra ricezione e accettazione, si è resa necessaria data la criticità del sistema dei controlli il quale potrebbe introdurre sensibili appesantimenti sul sistema di ricezione se con esso si trovasse a coincidere, con evidenti svantaggi sull'intera infrastruttura.

Si precisa comunque che i passi "b" e "c" sono di norma eseguiti uno di seguito all'altro, nel giro di qualche istante, a meno che non risulti impossibile scatenare l'evento del SICC.

Nel seguito si elenca la classificazione degli errori e degli allarmi così come individuata in fase di analisi:

- errore fatale: non è possibile innescare la catena di controlli. Due possibilità:
  - impossibilità di decifrare la busta contenente l'atto e i suoi eventuali allegati assemblati come messaggio MIME multipart;
  - la busta decifrata non è un messaggio MIME multipart.
- errore bloccante: non è possibile scaricare l'evento SICC e l'inserimento nel fascicolo informatico; varie possibilità:
  - IndiceBusta in formato non corretto e quindi non utilizzabile dal sistema.
  - Non è presente l'atto giudiziario.
  - Non è presente un allegato particolare, necessario per eseguire l'evento specifico (es. nota di iscrizione a ruolo nel caso di deposito di un atto di citazione).
  - Atto o allegato non conforme al formato del file richiesto dalle Regole Tecniche, per cui file in formato .pdf, .rtf, .txt, .jpg, .gif, .tiff, .xml, .zip, .rar.
  - Atto o allegato non integro rispetto alla firma elettronica apposta sullo stesso.
  - Il firmatario dell'atto non è costituito parte in causa nel procedimento a cui l'atto si riferisce (nel caso di atti depositati in corso di causa).
  - Il firmatario non è costituito nell'atto introduttivo.
  - Impossibilità di elaborare la struttura dell'atto (errore nel formato XML).
  - Numero di Ruolo non esistente nel SICC o non indicato.
  - Tipologia di atto non previsto.
  - Non completezza o non correttezza dei dati necessari ad innescare l'evento SICC.
  - Altro (eventuali errori che emergeranno dalla fase di sperimentazione)
- allarme: è stato possibile scaricare l'evento SICC ed effettuare l'inserimento nel fascicolo informatico, ma vengono segnalate anomalie nel contenuto dell'atto o nell'insieme degli eventuali allegati; varie possibilità:
  - Il mittente non è il firmatario dell'atto.
  - L'avvocato costituito nell'atto introduttivo non è abilitato. Questo tipo di controllo si rende necessario anche a livello di UG in quanto se il mittente non è il firmatario dell'atto l'abilitazione di quest'ultimo non è stata possibile da parte del PdA o GC in quanto l'atto è cifrato. Le verifiche delle credenziali di un avvocato a livello di UG avviene attraverso la chiamata ad un apposito servizio del GC.
  - Presenza di allegati non indicati nell'indice della busta.
  - Assenza di allegati indicati nell'indice della busta.
  - Atto depositato fuori termine.
  - Data in citazione non possibile (festivo, periodo feriale, fuori dai termini,...).
  - Struttura non conforme ai modelli ovvero ai DTD ministeriali, tipicamente manca una sezione, ad esempio non conformità rispetto alla strutturazione definita dall'articolo 163 per l'atto di citazione.
  - Altro (dipendente dalla strutturazione degli atti ed eventualmente emergente dalla fase di sperimentazione).

- informazione di esito positivo: viene registrato l'esito positivo della fase di controllo e innescato il sistema di accettazione.

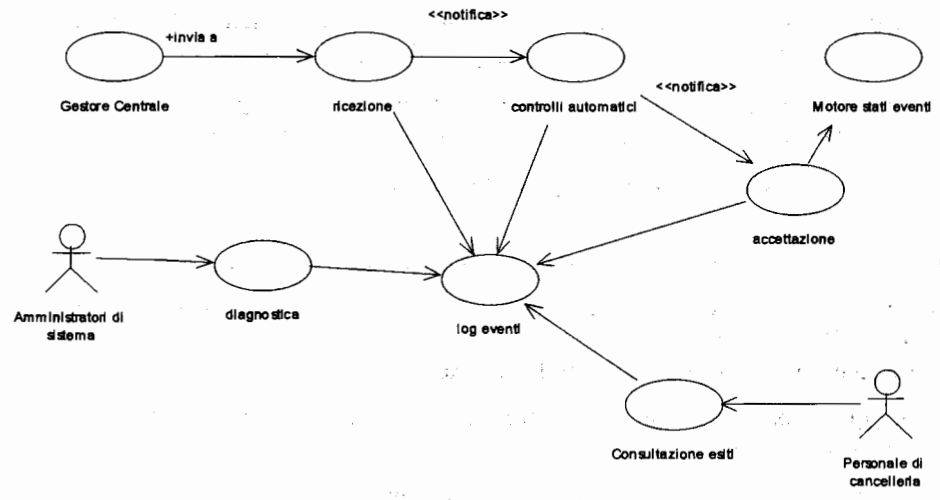

Figura 11 - Attori e componenti applicative coinvolte in fase di ricezione e accettazione

Descrizione della figura:

Come risulta evidente dalla figura la componente applicativa più importante dell'intero sistema è quella denominata ***Log Eventi***. Il log eventi è un'insieme persistente di informazioni che permettono di tracciare **tutte le operazioni** che, sia le componenti applicative sia gli operatori di cancelleria, effettuano sugli atti in ingresso all'UG. Il documento di analisi architetturale definirà in maniera più esplicita e tecnicamente esaustiva le caratteristiche di questa componente mentre nel contesto del presente documento è sufficiente indicare che viene utilizzata per registrare la tipologia di operazione che il sistema o l'operatore esegue (in forma codificata), la descrizione di tale operazione, il riferimento al documento (atto o allegato) oggetto dell'operazione e l'indicazione temporale del momento in cui viene eseguita.

Nel caso più semplice, ovvero di totale assenza di eccezioni, nel log eventi verrà tenuta traccia delle seguenti operazioni:

- data e ora di ricezione di un atto;
- data e ora dei controlli su di esso effettuati;
- data e ora in cui l'evento del SICC viene scaricato e il fascicolo elettronico aggiornato;
- data e ora di invio della notifica, al mittente, dell'avvenuta accettazione dell'atto da parte della cancelleria.

Il sistema di ricezione è l'interfaccia esposta dall'UG verso il GC e si occupa esclusivamente di ricevere attraverso una comunicazione sincrona l'atto giudiziario e i suoi allegati in una busta cifrata con chiave pubblica dell'UG. Il componente si occupa di gestire attraverso meccanismi tipici del protocollo di comunicazione (HTTP) eventuali problemi trasmissione a meno dei quali la busta viene memorizzata localmente in un'area del repository Documentale denominata *Area Buste*. La memorizzazione nell'area buste garantisce sicurezza

dell'avvenuta ricezione di una busta integra in tutte le sue componenti ovvero informazioni sul mittente, attestazione temporale e pacchetto dati cifrato contenente l'atto giudiziario e i suoi eventuali allegati.

Il sistema dei controlli è una componente altamente configurabile che permette di individuare eventuali errori bloccanti o semplici anomalie sull'atto depositato e comunicare le stesse all'operatore di cancelleria attraverso il log eventi. Verrà realizzato un vero e proprio sistema di *ruling* altamente personalizzabile con l'obiettivo di conferire al sistema un alto grado di flessibilità ed elasticità necessario soprattutto nella fase sperimentazione.

Il sistema di accettazione è in grado di utilizzare il motore stati eventi per lo scarico dell'evento corrispondente al deposito dell'atto e di memorizzare l'atto stesso nel fascicolo elettronico attraverso l'interfacciamento con il repository documentale. Il sistema di accettazione viene attivato solo nel caso in cui tutti i controlli diano esito positivo.

Il motore stati eventi è esattamente lo stesso che viene attualmente utilizzato dal SICC.

Il fascicolo elettronico indica quell'area del repository documentale utilizzata per la memorizzazione degli atti di parte e d'ufficio e dei relativi allegati.

Il sistema di diagnostica è utilizzato dagli amministratori di sistema dell'UG per individuare e intervenire a livello esclusivamente tecnico sull'atto pervenuto all'UG. Il sistema di diagnostica fornisce agli amministratori un'interfaccia attraverso la quale registrate gli interventi nel log eventi.

Il sistema per la consultazione del log eventi mette a disposizione degli operatori di cancelleria un'interfaccia grafica potente e flessibile che permette loro di verificare tutte le operazioni effettuate dal sistema in automatico. Nel caso di errori o anomalie tale interfaccia permetterà in maniera semplice di intervenire manualmente, laddove possibile, per riuscire comunque ad aggiornare il SICC e il fascicolo elettronico.

2.5 Il Fascicolo Informatico

Il Repository Documentale nasce per gestire il fascicolo informatico, conservare i documenti prodotti nell'ambito di un procedimento giudiziario ed esporre ai sistemi utilizzatori servizi informatici di alimentazione e fruizione delle informazioni. Tale servizio si configura come una piattaforma di gestione documentale che mette in comunicazione i diversi applicativi con la base dati documentale, per consentire l'interazione documentale ed informativa fra soggetti appartenenti a categorie diverse tra loro (Giudice, Cancelliere, Avvocato, CTU).

L'obiettivo principale del Repository Documentale è quello di potenziare le funzionalità delle Applicazioni di Gestione dei Registri, con capacità di Gestione Documentale ed *Information Retrieval* (queste ultime verranno introdotte nella fase 2 del progetto).

In questo modo il Repository Documentale funge da gestore centralizzato del patrimonio documentale, divenendo l'unità di archiviazione univoca e centrale a livello di UG dei documenti prodotti o ricevuti dall'Ufficio stesso, indipendentemente dalla loro natura originaria, analogica o digitale.

Nella fase sperimentale del Processo Telematico, il Repository Documentale esporrà un insieme limitato di servizi; sarà infatti compito del SICC, in questa prima fase, ricevere le richieste di accesso al patrimonio documentale, filtrarle sulla base dei criteri di visibilità insiti nelle proprie strutture dati e formulare specifiche richieste al Repository Documentale.

Il SICC, in questa fase, sarà il sistema tenutario di tutte le informazioni che riguardano la vita del Fascicolo; il Fascicolo Informatico gestito in ambito del Repository Documentale pertanto sarà limitato alla memorizzazione dei Documenti depositati da soggetti esterni ed interni all'Ufficio Giudiziario, provvedendo a mantenere il legame con il Procedimento corrispondente sul SICC.

Riguardo ai Documenti informatici, il legame tra SICC e Repository verrà assicurato attraverso l'implementazione della relazione Eventi – Atti, che associa a ciascun Evento che accade ad un Procedimento sul SICC il/i Documenti che lo hanno generato, memorizzati sul Repository. In questa prima fase progettuale il Repository Documentale, pertanto, si limiterà ad esporre le seguenti categorie di servizi:

- acquisizione dei documenti contenuti nelle Buste ricevute dal Gestore Centrale, confezionate allo scopo di depositare gli Atti, dagli Avvocati che partecipano alla fase sperimentale del progetto;
- acquisizione delle comunicazioni inviate dalla Cancelleria dell'Ufficio Giudiziario verso l'esterno, quali ad esempio i Biglietti di Cancelleria;
- consultazione di documenti.

A titolo esemplificativo, il seguente diagramma di sequenza illustra le modalità di interazione tra SICC e Repository Documentale nella fase sperimentale del Processo Telematico, relativamente alle richieste di consultazione documenti inoltrare da PolisWeb.

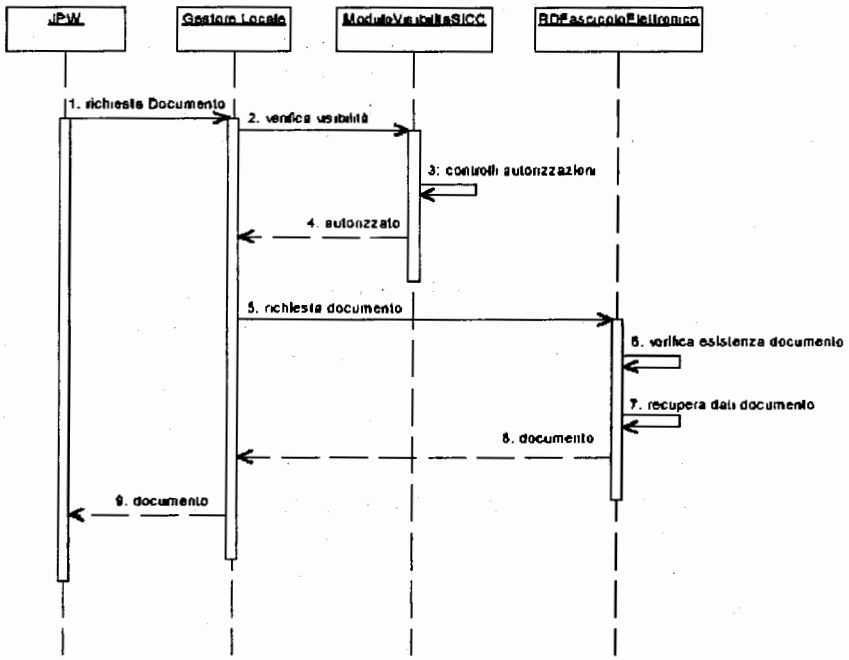

Figura 12 – Diagramma di sequenza "Interazioni SICC – repository documentale"

Spiegazione:

1. Il Sottosistema Polis Web (JPW) inoltra una richiesta di visualizzazione Documento;

2. Il Gestore Locale invia la richiesta di verifica dei diritti di visibilità al Modulo Visibilità del SICC;
3. Il SICC effettua i controlli sui diritti di visibilità inerenti la richiesta;
4. Il SICC restituisce al Gestore Locale l'informazione relativa alla presenza o assenza dell'autorizzazione;
5. A seguito dell'autorizzazione da parte del SICC, il Gestore Locale richiede il Documento al Repository Documentale;
6. Il Repository Documentale verifica l'esistenza del Documento;
7. Il Repository, trovato il documento, provvede a recuperarlo;
8. Il Repository invia il documento richiesto al Gestore Locale;
9. Il Gestore Locale invia il documento al Sottosistema JPW che ne aveva richiesto la visualizzazione.

Gli ambienti del Repository Documentale

Gli ambienti nei quali il Repository Documentale è suddiviso nella fase sperimentale del Progetto sono i seguenti:

Ambiente di Memorizzazione delle Buste; tale ambiente è demandato alla memorizzazione e conservazione delle Buste inoltrate dal Gestore Centrale all'Ufficio Giudiziario e, viceversa, delle Buste inoltrate dall'Ufficio Giudiziario al Gestore Centrale, le quali vengono conservate localmente per essere successivamente elaborate dalla componente di controllo (cfr. 2.4).

Ambiente di Pre-Accettazione; in questo ambiente sono memorizzati, in maniera temporanea, i documenti contenuti in ciascuna Busta scambiata con il Gestore Centrale; tali documenti verranno successivamente recepiti ai fini della accettazione dei Documenti in ingresso.

Ambiente Fascicolo Elettronico; contiene i documenti elettronici ricevuti dal Gestore Centrale e sottoposti al processo di accettazione da parte del SICC ed i documenti prodotti all'interno dell'Ufficio Giudiziario ed inoltrati al Gestore Centrale; tali documenti rappresentano gli Atti dei Procedimenti Giudiziari e sono raccolti in fascicoli, ricalcando le logiche applicative che legano un Procedimento Giudiziario al relativo fascicolo cartaceo.

2.6 Comunicazioni di Cancelleria

Allo stato attuale il SICC gestisce le comunicazioni in forma cartacea ed in particolare a seguito di un aggiornamento del fascicolo e quindi dello scarico di un evento viene proposto al cancelliere di stampare le comunicazioni, una per ogni parte, più un report riassuntivo da inserire nel fascicolo d'ufficio.

L'emissione del biglietto di cancelleria non è vincolata allo scarico di un evento e il suo contenuto può essere esplicitamente scritto dal cancelliere, è per questo che si è definita nel SICC la tipologia *comunicazione generica*.

A seguito della consegna al destinatario viene da questi rilasciata la ricevuta breve di avvenuta consegna che sarà anch'essa inserita nel fascicolo d'ufficio.

Viene di seguito riportato l'elenco delle comunicazioni di cancelleria considerate in questa fase di analisi:

- Nomina Giudice
- Sostituzione Giudice
- Fissazione data udienza
- Sostituzione sezione
- Nomina CTU
- Convocazione CTU
- Revoca CTU
- Liquidazione CTU
- Nomina o revoca di Tutore/Curatore
- Avviso di deposito sentenza
- Comunicazione generica

La funzione di invio di un biglietto di cancelleria prevede un flusso di trasmissione dall'UG verso le caselle di posta elettronica del processo telematico di tutti gli avvocati coinvolti nel procedimento giudiziario a cui la comunicazione è riferita. In seguito al deposito su tale casella di posta viene attivato il flusso di risposta, innescato dalla emissione delle singole ricevute di avvenuta consegna da parte dei PdA gestore delle caselle di posta interessate.

Nella sua interezza il flusso nasce e si completa presso l'UG e a tale flusso collabora:

- il GC, che provvede all'inoltro delle comunicazioni ai destinatari indicati dall'UG (fase di invio), ed effettua l'attestazione temporale di ogni evento di ricezione di una ricevuta di avvenuta consegna da parte dei PdA, per restituirla all'UG mittente (fase di risposta).
- il PdA, che genera una ricevuta di presa in carico per ogni messaggio ricevuto ed una ricevuta di avvenuta consegna contestualmente al deposito dello stesso nella CPECPT dell'avvocato indicato;

Ai fini della valutazione di eventuali termini legali per la consegna della comunicazione farà fede la data apposta dal GC, in fase di attestazione temporale, sulla ricevuta di avvenuta consegna prodotta dal PdA.

2.7 CONSULTAZIONE WEB (JPW)

Il sottosistema PolisWeb fornisce strumenti per la consultazione via Web delle informazioni contenute nei Registri dei Procedimenti e/o nei Documenti afferenti ad un Procedimento (Fascicolo Elettronico) o alla Base Dati Giurisprudenziale dei Provvedimenti pubblicati.

L'attuale sistema PolisWeb fornisce una serie di servizi informativi riguardanti sia la giurisprudenza che la gestione operativa dei fascicoli e delle udienze del Contenzioso Civile relative ad ogni singolo Ufficio Giudiziario.

L'applicazione PolisWeb è rivolta a ***tipologie di utenti*** distinti in base al proprio ruolo, identificabili come Utente di Consultazione, Utente di Cancelleria e Utente di Amministrazione.

- L'Utente di Consultazione è genericamente un Avvocato, abilitato all'utilizzo dell'applicazione da un Utente di Amministrazione dell'Ufficio Giudiziario. Il sistema PolisWeb è utilizzabile dall'Avvocato sia all'interno dell'Ufficio Giudiziario, tramite

delle postazioni di lavoro dedicate e definite "Chiosco" (Intranet), che dal proprio Studio Legale attraverso il proprio browser web con collegamento Internet.

- L'Utente di Cancelleria è un operatore di cancelleria che attraverso PolisWeb è in grado di utilizzare le funzionalità relative alla gestione delle richieste di copie di documenti effettuate dall'Avvocato tramite le specifiche funzioni messe a disposizione da PolisWeb.
- L'Utente di Amministrazione gestisce le richieste di Account e le relative attivazioni e abilitazioni per gli Utenti di Consultazione e di Cancelleria.

PolisWeb, potrà essere installato e configurato all'interno dell'UG, allo scopo di rispondere alle richieste informative provenienti dai cosiddetti "chioschi" presenti nelle sale degli UG (***Modalità Intranet***) e, allo stesso modo, essere installato su server esterni al confine del Sistema Informativo Civile, quali ad esempio i Punti di Accesso. In tale caso PolisWeb sarà capace di sfruttare i servizi offerti dagli Uffici Giudiziari attraverso il Punto di accesso ed il Gestore Centrale (***Modalità Internet***).

PolisWeb può quindi essere utilizzato all'interno dell'UG attraverso appositi "chioschi" informativi mentre dall'esterno attraverso i Punti di Accesso.

Di seguito viene rappresentato il diagramma di sequenza relativo alla autenticazione dell'utente al Punto di Accesso:

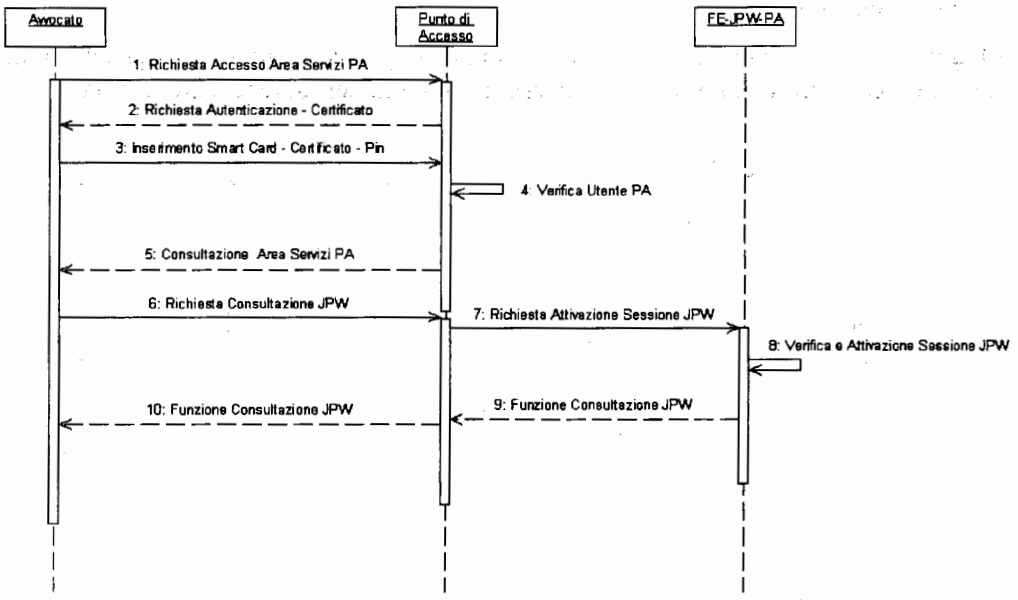

Figura 13- Flusso Autenticazione PolisWeb da internet

Descrizione della figura:

- La funzione prevede la richiesta da parte di un utente Avvocato di accedere ai servizi web forniti dal Punto di Accesso.

- Per l'accesso all'Area Servizi del Punto di Accesso all'Avvocato viene richiesto il Certificato di Autenticazione.
- L'Avvocato, utilizzando la propria Smart-Card, fornisce al Punto di Accesso il proprio certificato di autenticazione.
- Il Punto di Accesso verifica le informazioni di autenticazione fornite dall'utente Avvocato. La Verifica Utente accerta l'utente come appartenente agli utenti del Punto di Accesso e successivamente la validità del Certificato di Autenticazione ricevuto.
- L'utente Avvocato, a seguito della corretta autenticazione, accede all'area di consultazione dei servizi del Punto di Accesso.
- Dall'area dei servizi del Punto di Accesso l'Avvocato può richiedere l'accesso alle funzioni di consultazione di PolisWeb, installato presso il Punto di Accesso.
- Il Punto di Accesso, a seguito della richiesta dell'Avvocato di accedere alle funzioni di consultazione di PolisWeb, si l'interfaccia con il Front-End di PolisWeb per la richiesta attivazione della sessione utente.
- PolisWeb abilita la nuova sessione utente per l'accesso all'area riservata di PolisWeb, attraverso le informazioni fornite dal Punto di Accesso
- PolisWeb a seguito dell'attivazione della sessione utente, fornisce e permette al Punto di Accesso di presentare all'utente Avvocato la funzione di consultazione di default dell'area privata di PolisWeb.

Nella Figura 14 viene rappresentato il diagramma di sequenza relativo alla consultazione dei procedimenti personali in ambito SICC, attivabili a seguito dell'autenticazione al PdA.

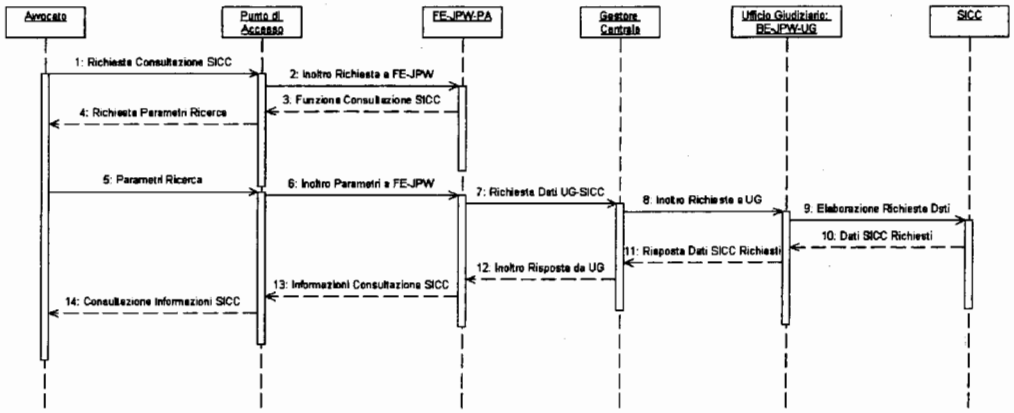

Figura 14- Flusso Consultazione PolisWeb Internet

Descrizione della figura:

- A seguito dell'autenticazione presso il Punto di Accesso un utente Avvocato può effettuare la richiesta di una funzione di consultazione fornita dal Punto di Accesso attraverso l'integrazione con il PolisWeb installato presso il Punto di Accesso stesso.
- La richiesta dell'Avvocato, di attivazione di una funzione di consultazione, viene inoltrata al Front-End di PolisWeb. PolisWeb fornisce la funzione richiesta per consentire all'Avvocato di indicare i parametri necessari alla ricerca delle informazioni a lui utili.
- I parametri di ricerca forniti dall'Avvocato possono essere ad esempio relativi ad una ricerca di consultazione di informazioni del SICC, fornite da un Ufficio Giudiziario specifico. I parametri sono inoltrati dal Punto di Accesso al Front-End di PolisWeb.
- Il Front-End di PolisWeb, in base ai parametri ricevuti, prepara il messaggio di richiesta (XML-Soap) da indirizzare al Gestore Centrale per l'inoltro all'Ufficio Giudiziario indicato dall'Avvocato.
- La richiesta di informazioni ricevuta dal Back-End di PolisWeb presso l'Ufficio Giudiziario (Servzi Soap dell'Application Server Comune) viene elaborata con l'interrogazione della base dati di interesse (SICC e/o Fascicolo Elettronico).
- Le informazione così individuate, sono fornite in risposta al Gestore Centrale per l'inoltro al Front-End di PolisWeb presso il Punto di Accesso richiedente.
- L'Utente Avvocato può consultare le informazioni di risposta, in base ai parametri di ricerca precedentemente forniti.

3 FLUSSO DI DETTAGLIO PER IL DEPOSITO DI UN ATTO

Il deposito di un atto prevede un flusso di trasmissione dell'atto informatico da un PdA, fino al GL destinatario, e un flusso di risposta, di direzione opposta, innescato dalla produzione di un messaggio di *esito atto*, automatico o su azione del Cancelliere, indirizzato al PdA mittente.

In fase di trasmissione dell'atto è inoltre prevista una risposta al momento della ricezione della richiesta di inoltro dell'atto, da parte del GC. Detta risposta, indirizzata al PdA mittente, consiste nella *attestazione temporale* dell'evento di ricezione e la sua data di emissione avrà valore legale per la verifica dei termini di scadenza per la presentazione dell'atto, salvo verifica di buon fine dell'atto medesimo presso l'UG (verifica delle condizioni minime di accettabilità dell'atto).

Si ricorda che il flusso di deposito atto è originato dall'attivazione da parte di un Avvocato di un apposito servizio offerto dal proprio PdA, e che è sempre compito del PdA presentare all'Avvocato i messaggi di risposta ricevuti dal SIC.

Inoltre per completezza delle casistiche che la funzione in oggetto può generare è necessario prendere in considerazione la possibilità, seppure remota e imputabile ad un errore software, che la busta inoltrata dal PdA possa contenere un errore o una anomalia che impedisce l'inoltro dell'atto al GL. In questo caso il GC genera e invia al PdA un messaggio di *notifica eccezione*. Sarà cura del PdA rimuovere l'errore che ha prodotto la non conformità della busta e provvedere ad una nuova trasmissione.

I messaggi SMTP relativi alla funzione di *deposito atto* vengono ricevuti dal GC all'indirizzo **gestorecentrale@processotelematico.giustizia.it** e spediti al PdA all'indirizzo **<codicePdA>@processotelematico.<dominioPdA>**.

Tali messaggi sono:

- il messaggio di inoltro atto trasmesso dal PdA al GC, contenente Atto.enc e InfoInoltro.xml;
- il messaggio contenente l'attestazione temporale inviato dal GC al PdA (vedi paragrafo 3.1.3);
- il messaggio di notifica eccezione inviato dal GC al PdA alternativo all'attestazione temporale (vedi paragrafo 3.1.4);
- il messaggio di esito deposito inviato dal GC al PdA contenente l'esito del deposito lato UG (vedi paragrafo 3.2.2).

I messaggi ricevuti dal GC hanno una testata SMTP standard in cui viene richiesto di impostare almeno i parametri "MSG-ID" e "FROM" (da utilizzare per individuare la provenienza del messaggio quando non è possibile procedere all'apertura della busta ricevuta).

I messagi inviati dal GC al PdA hanno una testata SMTP standard in cui il subject, in base al tipo di messaggio, ha uno dei seguenti valori: esito atto, attestazione, notifica eccezione.

Al PdA viene anche richiesto di implementare il servizio SMTP standard di Delivery Status Notification (DSN), che assume il valore di ricevuta *debole* dei messaggi di risposta trasmessi dal SIC. La ricezione del DSN da parte del GC consente di controllare il corretto completamento del flusso logico della funzione.

3.1 FASE DI TRASMISSIONE DELL'ATTO

Come anticipato precedentemente la sequenza dei messaggi scambiati tra PdA e GC nella fase di trasmissione dell'atto può dare luogo a diverse alternative in funzione dell'esito dei controlli operati dal GC.

Nel caso in cui il messaggio di inoltro atto ricevuto dal PdA sia corretto la sequenza e il tipo di messaggi scambiati è indicata nello schema seguente:

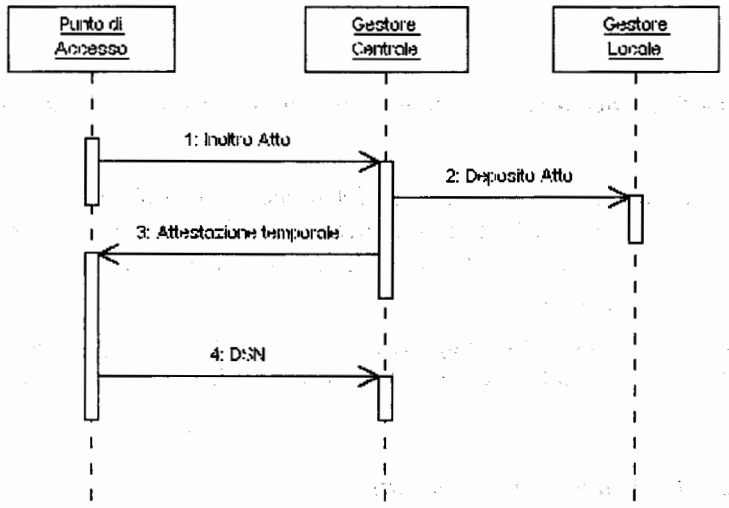

Figura 15 – Sequence diagram del deposito atto – Fase di trasmissione dell'atto

Nel caso in cui il GC riscontri un errore nel messaggio di inoltro dell'atto, oltre a non procedere al deposito presso il GL invia al PdA un messaggio di notifica eccezione:

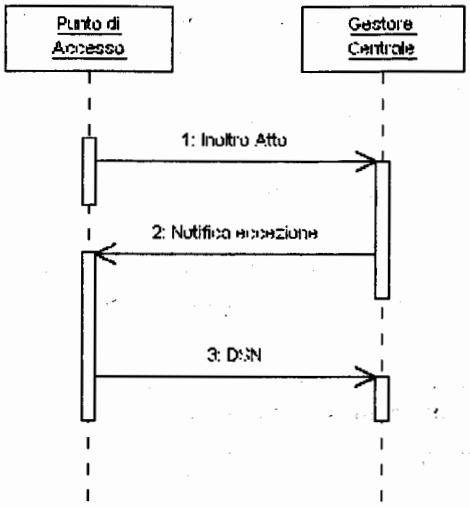

Figura 16 - Sequence diagram del deposito atto in caso di notifica di eccezione

Il GC svolge quindi una funzione di garante del processo di inoltro assicurando che gli atti informatici depositati presso i GL non contengano errori attribuibili alle attività svolte dai PdA, ma solo eventualmente ascrivibili ad operazioni svolte in locale dall'Avvocato in fase di formazione dell'atto informatico.

Nel seguito viene descritta la struttura applicativa di ciascun messaggio generato nella fase di trasmissione dell'atto e in allegato vengono forniti i DTD di ciascuna struttura XML utilizzata.

3.1.1 Struttura del messaggio di "inoltro atto"

La struttura del messaggio SMTP di *inoltro atto* proveniente da un PdA è illustrata nella figura che segue:

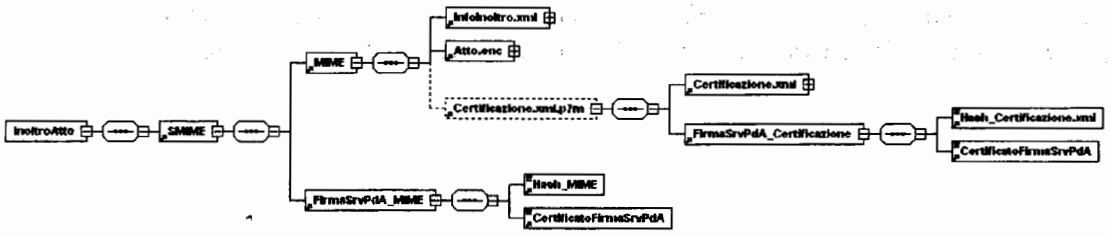

Figura 17 - S/MIME di Inoltro Atto

Essa è costituita da un S/MIME, cioè da una struttura MIME sottoscritta da parte del PdA con proprio certificato server, a titolo di verifica della integrità del messaggio.

Pertanto al suo interno è riconoscibile:

- una struttura MIME;

- l'hash del MIME, cioè la registrazione in formato binario che contiene l'*impronta* del documento, firmata secondo le modalità tecniche previste dal D.P.R. 513/97 e dalle relative regole tecniche (D.P.C.M. 8/02/99).
- il Certificato del PdA, ossia una struttura dati tipo X.509. I dati forniscono informazioni sul possessore del certificato, il firmatario del certificato, la versione, il numero seriale, l'algoritmo di firma, il periodo di validità, la corrispondente chiave pubblica e altri dati.

Le parti costituenti la struttura MIME sono appresso descritte.

1. File InfoInoltro.xml

Il file *InfoInoltro.xml* contiene le informazioni di servizio per il GC. Tali informazioni consentono il routing del messaggio e la verifica dei dati di certificazione.

Il file ha la seguente struttura:

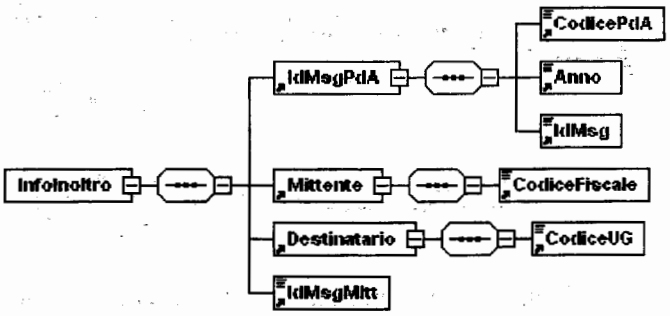

Figura 18 – Struttura del file InfoInoltro.xml

- IdMsgPdA.

  Riporta l'identificativo univoco del messaggio generato dal PdA. Tali dati sono:

  CodicePdA = E' il codice identificativo del PdA.

  Anno = E' l'anno di generazione del messaggio.

  IdMsg = E' un progressivo numerico univo nell'ambito dell'anno.

- Mittente.

  CodiceFiscale = È il codice fiscale dell'Avvocato che ha originato il messaggio.

  L'attributo *ruolo* indica il ruolo assunto dal mittente (al momento "Avvocato").

- Destinatario.

  CodiceUG = È il codice identificativo dell'UG destinatario.

  L'attributo *tipo* indica il tipo di destinatario (al momento "Ufficio"). Al momento è previsto un solo destinatario.

- IdMsgMitt.

  IdMsgMitt = È l'identificato assegnato dall'Avvocato all'atto informatico.

2. File Atto.enc

Il file Atto.enc è l'atto informatico prodotto dall'Avvocato, criptato utilizzando la chiave pubblica di cifratura dell'UG destinatario.

3. File Certificazione.xml.p7m

Il file Certificazione.xml.p7m può mancare nella busta di inoltro atto se il PdA non dispone delle informazioni atte a certificare l'Avvocato.

Se presente tale file è firmato dal PdA (firma server) ed ha la seguente struttura:

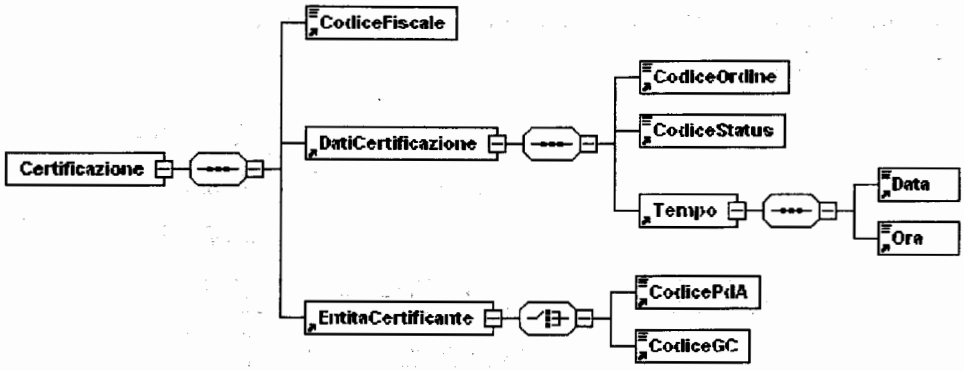

Figura 19 - Struttura del file Certificazione.xml

- CodiceFiscale.

  CodiceFiscale = È il codice fiscale dell'Avvocato che si certifica (deve coincidere con *InfoInoltro/Mittente/CodiceFiscale*).

- DatiCertificazione.

  Riporta i dati risultanti nell'albo elettronico all'atto della certificazione

  CodiceOrdine = E' l'organizzazione (CdO) che ha fornito i dati per la certificazione dello status dell'Avvocato.

  CodiceStatus = E' il codice dello status professionale dell'Avvocato risultante all'atto della certificazione (attivo, sospeso, radiato).

  Tempo = E' la data e ora in cui viene eseguita la certificazione.

- EntitaCertificante.

  EntitaCertificante = È il codice dell'entità che ha eseguito la certificazione (PdA o GC).

3.1.2 Struttura del messaggio di "deposito atto"

La busta di *Deposito atto* presenta la struttura appresso schematizzata:

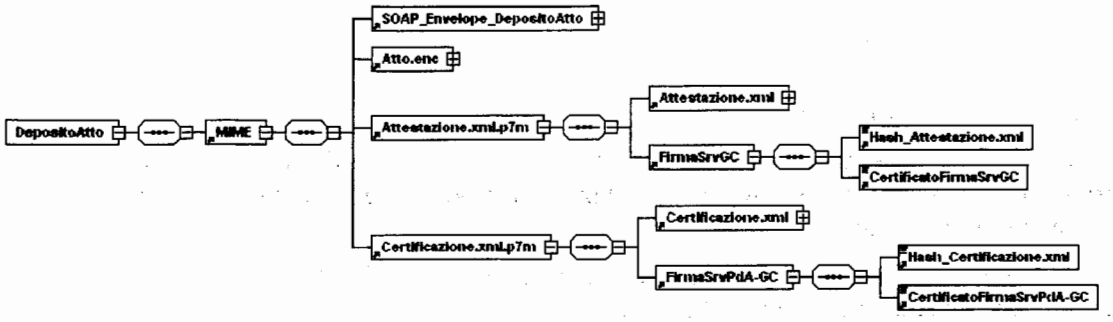

Figura 20 – MIME di Deposito Atto

dove la struttura SOAP_Envelope_DepositoAtto ha la seguente rappresentazione grafica:

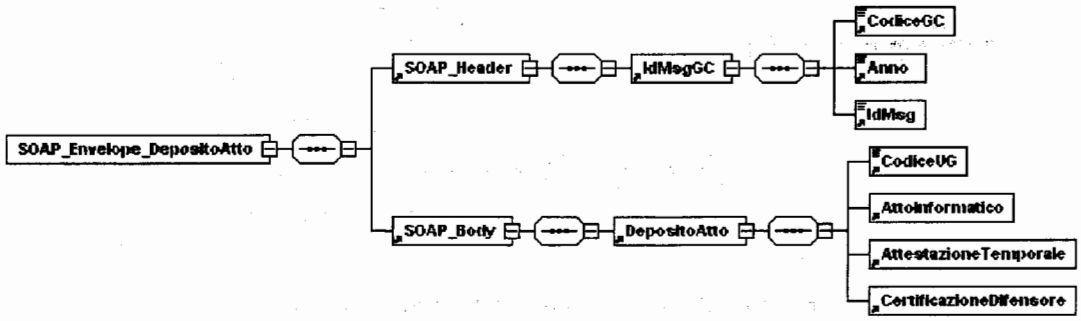

Figura 21 – Struttura SOAP_Envelope di DepositoAtto

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioDepositoAtto>.

La busta *DepositoAtto* contiene le seguenti strutture:

1. **SOAP:Envelope**
   La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto (in questo caso il messaggio di *Inoltro atto*).

   Il body della struttura ha un elemento, denominato *DepositoAtto* contenente:

CodiceUG	=	E' il codice dell'UG cui è destinato l'Atto informatico, ricavato da *InfoInoltro/Destinatario/CodiceUG*
Atto	=	Referenzia l'Atto informatico (file Atto.enc), generato dall'Avvocato, allegato nel MIME.
AttestazioneTemporale	=	Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME.
CertificazioneDifensore	=	Referenzia il file Certificazione.xml.p7m, ricevuto dal PdA o generato e firmato dal GC, allegato nel MIME.

2. File Atto.enc

Si veda il paragrafo 3.1.1.

3. File Attestazione.xml.p7m

All'atto della ricezione di un messaggio di *Inoltro atto* da parte del PdA, e dopo averne verificato la correttezza, il GC esegue l'attestazione temporale dell'evento di ricezione della richiesta di inoltro dell'atto.

L'attestazione temporale si sostanzia nella generazione del file *Attestazione.xml*, la cui struttura viene illustrata nella figura che segue:

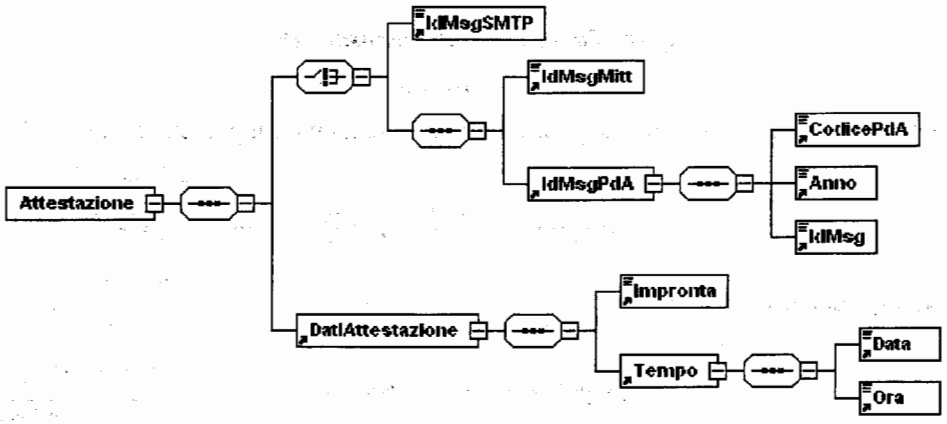

Figura 22 - Struttura del file Attestazione.xml

- IdMsgSMTP.

  In questo caso non è valorizzato (tale elemento è alternativo rispetto a i due successivi).

- IdMsgMitt.

  IdMsgMitt = È l'identificativo assegnato dall'Avvocato all'atto informatico (ricavato da *InfoInoltro/IdMsgMitt*)

- IdMsgPdA.

  IdMsgPdA = È l'identificato del messaggio generato dal PdA (ricavato da *InfoInoltro/IdMsgPdA*)

- DatiAttestazione.

  DatiAttestazione = Contiene l'impronta della busta ricevuta (nel formato S/MIME) e la data e ora dell'evento di attestazione temporale

4. File Certificazione.xml.p7m

Il file Certificazione.xml.p7m è lo stesso presente nella busta di Inoltro atto (si veda **Figura 19**). Qualora tuttavia il PdA non disponesse delle informazioni atte a certificare l'Avvocato, il GC deve eseguire la certificazione sostitutiva e sottoscrivere il file con la propria firma digitale (firma server).

3.1.3 Il messaggio di risposta "attestazione temporale"

Oltre al deposito dell'atto presso il GL destinatario, il GC genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto, un messaggio di *Attestazione temporale*.

Il messaggio contiene allegato all'interno della struttura MIME lo stesso file Attestazione.xml.p7m trasmesso all'UG.

Figura 23 – MIME di Attestazione temporale

3.1.4 Il messaggio di risposta "notifica eccezione"

Qualora il GC riscontri un errore nella formazione della busta di *inoltro atto*, oltre a non eseguire il deposito dell'atto, genera e trasmette al PdA da cui ha ricevuto la richiesta di inoltro dell'atto un messaggio di *Notifica eccezione*.

Il messaggio ha la seguente struttura:

Figura 24 – MIME di Notifica eccezione

All'interno della struttura MIME è presente in allegato il file *Eccezione.xml* che ha la seguente struttura:

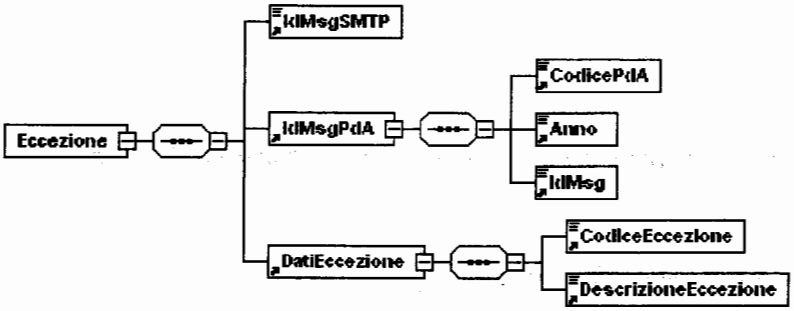

Figura 25 - Struttura del file Eccezione.xml

- IdMsgSMTP.

  IdMsgSMTP = È l'identificativo SMTP del messaggio ricevuto (parametro Message-ID). Tale identificativo potrebbe costituire l'unico modo di identificare il messaggio, qualora non fosse possibile eseguirne lo sbustamento.

- IdMsgPdA.

  IdMsgPdA = È l'identificativo del messaggio generato dal PdA (si veda il paragrafo 3.1.1).

- DatiEccezione.

  CodiceEccezione = È il codice identificativo dell'errore riscontrato.

  DescrizioneEccezione = È la descrizione dell'errore riscontrato.

3.2 FASE DI TRASMISSIONE DELL'ESITO DELL'ATTO

La sequenza e il tipo di messaggi scambiati in fase di trasmissione dell'esito dell'atto è indicata nello schema seguente:

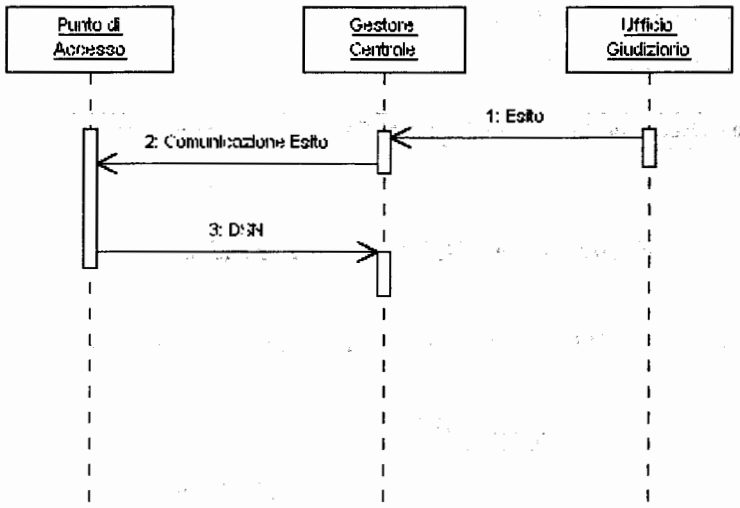

Figura 26 – Sequence diagram del deposito atto – Fase di trasmissione dell'esito dell'atto

3.2.1 Struttura del messaggio di esito atto

Il GL, in risposta alla ricezione di un atto informatico genera e inoltra al GC un messaggio di *Esito atto* che presenta la struttura appresso schematizzata:

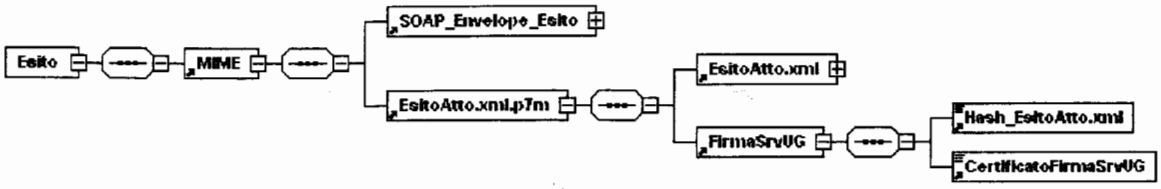

Figura 27 – MIME di Esito

dove la struttura SOAP_Envelope_Esito ha la seguente rappresentazione grafica:

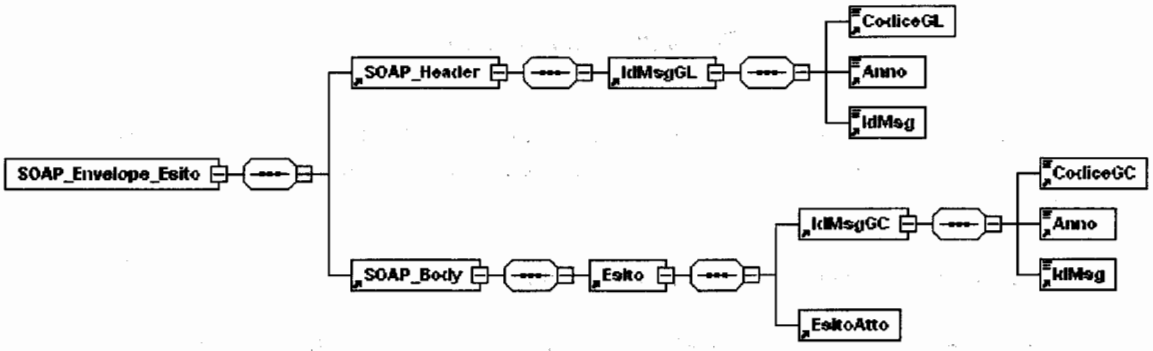

Figura 28 – Struttura SOAP_Envelope di Esito

Il messaggio viene ricevuto dal GC all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/esitoatto.asp.

1. SOAP:Envelope della busta di Esito

La struttura contiene a livello di header l'identificativo univoco del messaggio di *Esito* generato dall'GL.

Il body della struttura ha un elemento, denominato Esito, contenente:

IdMsgGC = È l'identificativo univoco del messaggio di *Deposito atto* generato dal GC.

EsitoAtto = Referenzia il file EsitoAtto.xml.p7m allegato nel MIME.

2. File EsitoAtto.xml.p7m

Il file *EsitoAtto.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni che comunicano all'Avvocato l'esito dell'atto.

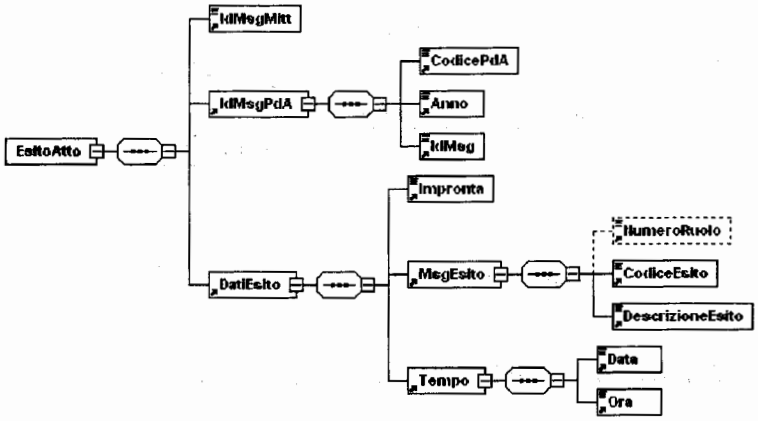

Figura 29 - EsitoAtto.xml

Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti, per il cui dettaglio si rimanda al documento di "Analisi funzionale del Processo Telematico".

3.2.2 Il messaggio di risposta "comunicazione esito"

Quando il GC riceve un messaggio di *esito atto*, attraverso l'identificativo del messaggio (*IdMsgGC*) ricava tutte le informazioni necessarie per recapitare il messaggio (Avvocato destinatario, PdA di appartenenza).

Il messaggio contiene allegato all'interno della struttura MIME il file EsitoAtto.xml.p7m firmato dall'UG.

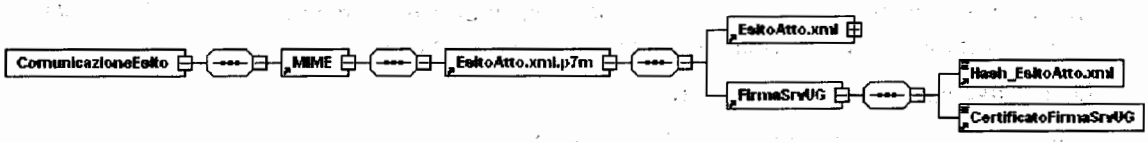

Figura 30 – MIME di Comunicazione esito

4 INVIO DI UNA COMUNICAZIONE DI CANCELLERIA

La funzione di *invio comunicazione (o biglietto) di cancelleria* prevede un flusso di trasmissione di una comunicazione da un GL, fino al dominio di Posta Certificata del Processo Telematico del PdA gestore della CPECPT dell'Avvocato destinatario, e un flusso di risposta, di direzione opposta, innescato dalla produzione automatica della *ricevuta breve di avvenuta consegna*, che viene restituita al GL mittente munita dell'attestazione temporale emessa dal GC al momento della sua ricezione.

Benché al di fuori del contesto di analisi del presente documento, giova ricordare che il flusso del biglietto di cancelleria è originato dall'azione di un cancelliere e che nell'ambito dei meccanismi di scambio previsti dalla Posta Certificata si generano ulteriori due ricevute:

- la *ricevuta di accettazione*, emessa dal server di dominio del sistema di Posta Certificata del Processo Telematico del GC, depositata nella casella di Posta Certificata dell'UG mittente, presso il GC;
- la *ricevuta di presa in carico*, emessa dal server di dominio del sistema di Posta Certificata del Processo Telematico del PdA, destinata al corrispondente server mittente del GC.

I messaggi di Posta Certificata del Processo Telematico relativi alla funzione di *invio biglietto di cancelleria* vengono spediti alle CPECPT degli Avvocati agli indirizzi **<CPECPT>@processotelematico.<dominiocertPdA>** e ricevuti sulle CPECPT degli UG presso il GC agli indirizzi **<codiceUG>@processotelematico.giustiziacert.it**.

I messaggi prodotti dal GC sono conformi allo standard previsto dal sistema di Posta Certificata.

La sequenza dei messaggi scambiati con il GC nella fase di trasmissione del biglietto di cancelleria e della relativa risposta è indicata nello schema seguente:

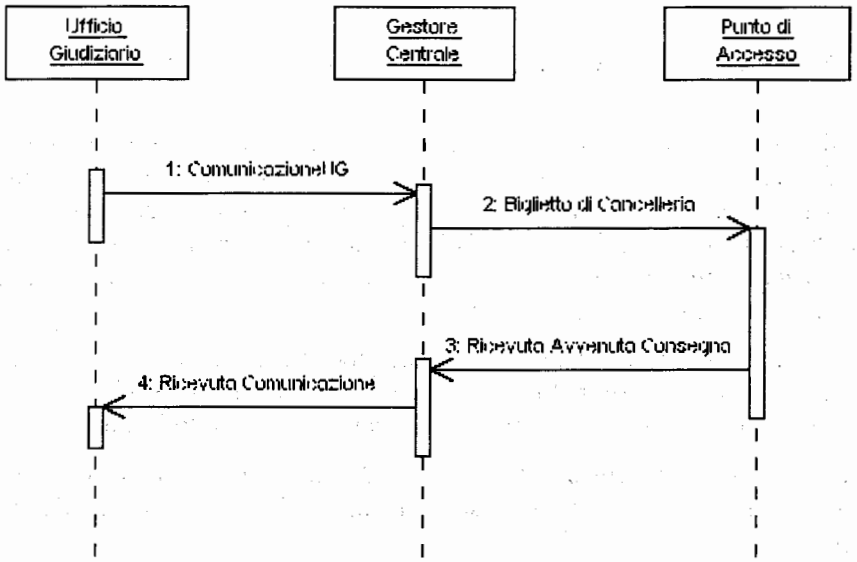

Figura 31 – Sequence diagram dell'invio di un biglietto di cancelleria

4.1 STRUTTURA DEI MESSAGGI RELATIVI ALL'INVIO DEL BIGLIETTO DI CANCELLERIA

Nel seguito del documento viene descritta la struttura applicativa di ciascun messaggio generato dalla funzione di invio di un biglietto di cancelleria e in allegato vengono forniti i DTD di ciascuna struttura XML utilizzata.

4.1.1 Struttura del messaggio di "comunicazione UG"

La struttura del messaggio di *comunicazione* proveniente da un GL è illustrata nella figura che segue:

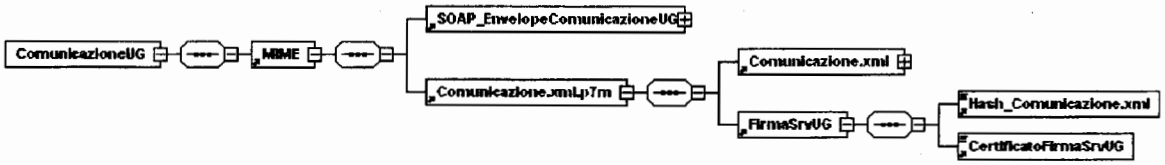

Figura 32 – MIME di Comunicazione UG

dove la struttura SOAP_EnvelopeComunicazioneUG ha la seguente rappresentazione grafica:

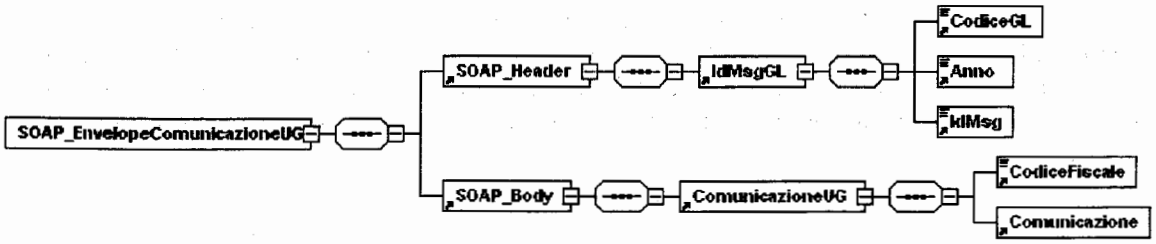

Figura 33 – Struttura SOAP_Envelope di ComunicazioneUG

Il messaggio viene ricevuto dal GC, all'indirizzo identificato dalla URI http://gestorecentrale.processotelematico.giustizia.it/comunicazioneUG.asp.

La transazione tra GL e GC termina con successo solo dopo che il GC ha effettuato i controlli formali sulla busta ricevuta ed ha controllato che il codice fiscale del destinatario sia presente nel ReGIndE.

La busta *ComunicazioneUG* contiene le seguenti strutture:

1. **SOAP:Envelope**

   La struttura contiene a livello di header l'identificativo univoco del messaggio generato dal GL (*IdMsgGL*).

   Il body della struttura ha un elemento, denominato ComunicazioneUG, contenente:

   CodiceFiscale = È l'identificativo del destinatario della comunicazione.

   Comunicazione = Referenzia il file Comunicazione.xml.p7m allegato nel MIME.

2. **File Comunicazione.xml.p7m**

   Il file *Comunicazione.xml.p7m* generato presso l'UG e firmato dall'UG stesso (firma server), trasporta le informazioni relative alla comunicazione da trasmettere all'Avvocato.

   Benché il file non sia cifrato, il GC non esegue alcun controllo sulla sua struttura e sui suoi contenuti, per il cui dettaglio si rimanda al documento di "Analisi funzionale del Processo Telematico".

4.1.2 Struttura del messaggio di "biglietto cancelleria"

Ricevuta la comunicazione da parte del GL, il servizio SMTP del GC genera un messaggio di Posta Certificata del Processo Telematico contenente in allegato il file Comunicazione.xml.p7m.

Il messaggio riporta come destinatario, la CPECPT dell'Avvocato corrispondente al codice fiscale trasmesso, e come mittente la CPECPT dell'UG dal quale è stata ricevuta la comunicazione.

Tale messaggio, secondo i meccanismi standard di Posta Certificata, viene acquisito dal server di dominio del GC, imbustato in un messaggio di trasporto e spedito al server di dominio di Posta Certificata del PdA. A seguito di tali operazioni il server SMTP di Posta Certificata del GC restituisce nella CPECPT dell'UG mittente una *ricevuta breve di accettazione* che segnala l'effettiva spedizione del messaggio la cui struttura è rappresentata di seguito:

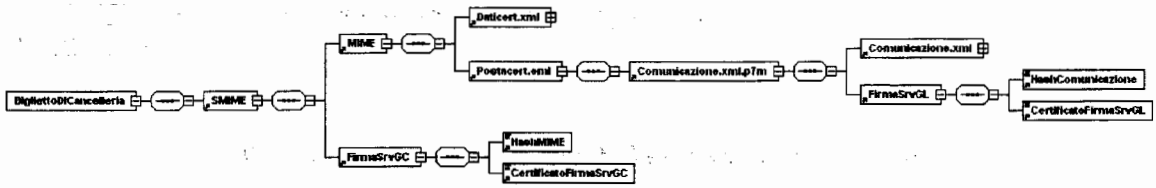

Figura 34 – S/MIME di Biglietto di cancelleria

4.1.3 Struttura del messaggio di "ricevuta comunicazione"

All'atto della ricezione nella CPECPT dell'UG mittente della *ricevuta breve di avvenuta consegna* il GC genera automaticamente l'attestazione temporale di tale evento.

Il file Attestazione.xml.p7m insieme con la *ricevuta breve di avvenuta consegna* viene imbustato in un messaggio di *Ricevuta comunicazione* che presenta la struttura appresso schematizzata:

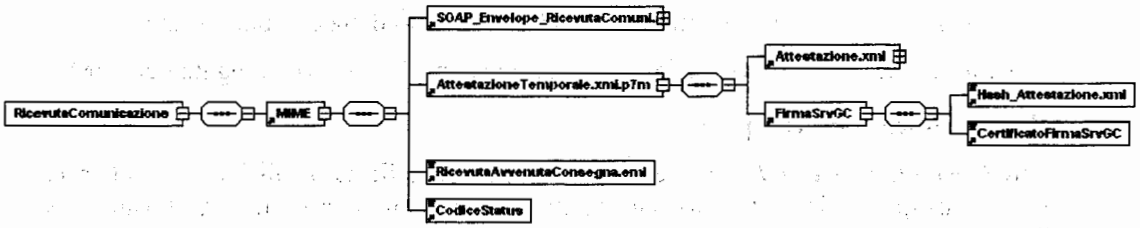

Figura 35 – MIME di Ricevuta comunicazione

dove la struttura SOAP_Envelope_RicevutaComunicazione ha la seguente rappresentazione grafica:

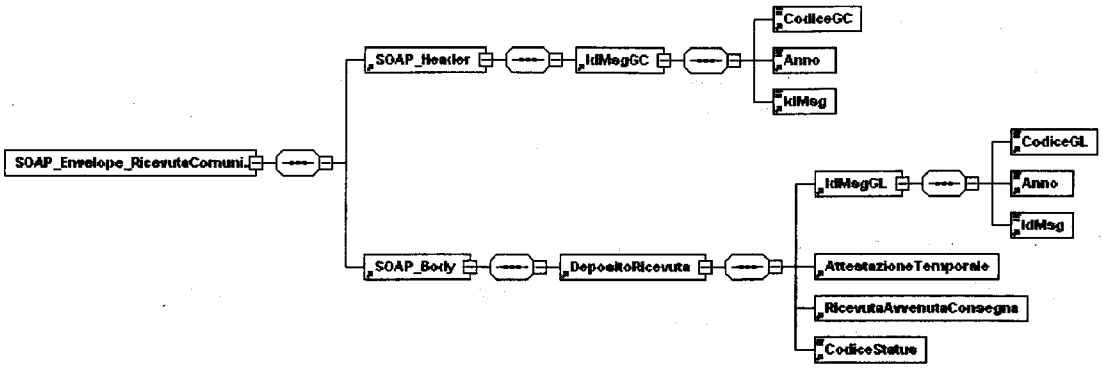

Figura 36 – Struttura SOAP_Envelope di RicevutaComunicazione

Il messaggio viene spedito dal GC all'indirizzo identificato dalla URI http://<codiceGL>.processotelematico.giustizia.it/<servizioRicevutaComunicazione>.

La busta *RicevutaComunicazione* contiene le seguenti strutture:

1. **SOAP:Envelope**

   La struttura contiene a livello di header il codice univoco generato dal GC per identificare il messaggio ricevuto.

   Il body della struttura ha un elemento, denominato *DepositoRicevuta* contenente:

   IdMsgGL = E' l'identificativo della comunicazione trasmessa dall'UG.

   AttestazioneTemporale = Referenzia il file Attestazione.xml.p7m, generato e firmato dal GC, allegato nel MIME.

   RicevutaAvvenutaConsegna = Referenzia il file RicevutaAvvenutaConsegna.eml ricevuto dal PdA, allegato nel MIME.

   CodiceStatus = Contiene il codice dello status professionale dell'Avvocato destinatario della comunicazione (attivo, sospeso, radiato).

2. **File Attestazione.xml.p7m**

   Il file Attestazione.xml.p7m ha la struttura presentata in ***Figura 22*** ed è firmato dal GC (firma server). Il contenuto informativo di tale file è il seguente:

- IdMsgSMTP.

  IdMsgSMTP = Contiene il valore del parametro SMTP Message-ID del messaggio di *ricevuta breve di avvenuta consegna*

- IdMsgMitt e IdMsgPdA.

  In questo caso non sono valorizzati (questi elementi sono alternativi rispetto al precedente).

- DatiAttestazione.

  DatiAttestazione = Contiene l'impronta della busta di *ricevuta breve avvenuta consegna* (nel formato S/MIME) e la data e ora dell'evento di attestazione temporale

3. File RicevutaAvvenutaConsegna.eml

E' il messaggio di *ricevuta breve di avvenuta consegna* così come ricevuta dal dominio di Posta Certificata del Processo Telematico del PdA.

5 CONSULTAZIONE WEB (POLISWEB)

Il sistema PolisWeb fornisce un'interfaccia applicativa per l'integrazione delle funzionalità di Consultazione per il Processo Telematico, presso un Punto di Accesso (Modalità Internet).

L'interfaccia applicativa permette l'attivazione di PolisWeb, installato presso un Punto di Accesso, a seguito dell'autenticazione effettuata e delegata al Punto di Accesso stesso.

A seguito dell'autenticazione di un utente da parte del Punto di Accesso, PolisWeb può essere attivato tramite l'interfaccia applicativa che espone e attraverso la quale riceve e condivide i parametri identificativi dell'utente e della sessione utente.

5.1 CARATTERISTICHE DI POLISWEB

PolisWeb per il Processo Telematico è costituita da un'applicazione Web basata sul modello J2EE.

La soluzione architetturale e tecnologica di PolisWeb prevede l'utilizzo del Web Server Apache e di Jakarta Tomcat come container per la tecnologia java utilizzata (Jsp, Servlet, Bean).

Per il progetto del Processo Telematico si è adottato Linux come sistema operativo dei sistemi server, e quindi anche per PolisWeb presso il Punto di Accesso è consigliata l'adozione di Linux.

PolisWeb integrato e configurato presso il Punto di Accesso, non necessita di un Database. Le informazioni di configurazione sono definite all'interno di file nel filesystem. Le informazioni relative agli utenti non sono gestite da PolisWeb ma ricevute, e ritenute valide, dall'interfaccia per il Punto di Accesso.

Si precisa comunque, date le caratteristiche open-source dei prodotti tecnologici utilizzati per PolisWeb, che il sistema operativo Microsoft Windows può essere valutato come ambiente server per il PolisWeb presso il Punto di Accesso.

La documentazione rilasciata dal'RTI relativa all'installazione e configurazione di PolisWeb per Processo Telematica sarà relativa al sistema operativo Linux.

Tra le caratteristiche di PolisWeb, si ricorda inoltre la sua configurabilità. La configurabilità di PolisWeb nella Fase 1 del Processo Telematico, permette al Punto di Accesso una minima personalizzazione dell'Interfaccia Grafica per l'utente. Con la personalizzazione dei loghi, delle intestazioni, dei colori è possibile, ad esempio, allineare l'interfaccia utente di PolisWeb con alcune preferenze adottate dal Punto di Accesso.

Nei paragrafi che seguono sono fornite le informazioni relative all'Interfaccia Applicativa tra Punto di Accesso e PolisWeb, con l'indicazione dei protocolli di comunicazione adottati.

Nella tabella seguente sono riepilogate le caratteristiche tecnologiche di PolisWeb.

CARATTERISTICA	DESCRIZIONE	
Tipo Applicazione	Applicazione Web Java	
Sistema Operativo	Linux (Windows 2000 Server)	SERVER
Java Virtual Machine	1.4.2	SERVER
Web Server	Apache.	SERVER
Web Container	Tomcat.	SERVER
Database	Non necessario.	SERVER
Configurabilità	Alcune caratteristiche del Front-End.	SERVER
Interfaccia Applicativa	Parametri Intestazione Richieste http Parametri Intestazione Risposte http	
Protocollo PA-PW	http	
Protocollo PW-GC	https con mutua autenticazione	
Browser supportati	Microsft Explorer, Netscape, Mozilla.	CLIENT
Configurazione browser	Utilizzati Coockie e java script lato client.	CLIENT

Tabella 1 - Caratteristiche di PolisWeb per il Punto di Accesso

5.2 ARCHITETTURA E FLUSSI DI COLLOQUIO TRA PUNTO ACCESSO E POLISWEB

PolisWeb presso il Punto di Accesso permette agli utenti del Processo Telematico di accedere alle informazioni di Back-End presso gli Uffici Giudiziari attraverso il Punto di Accesso e il Gestore Centrale (Modalità Internet).

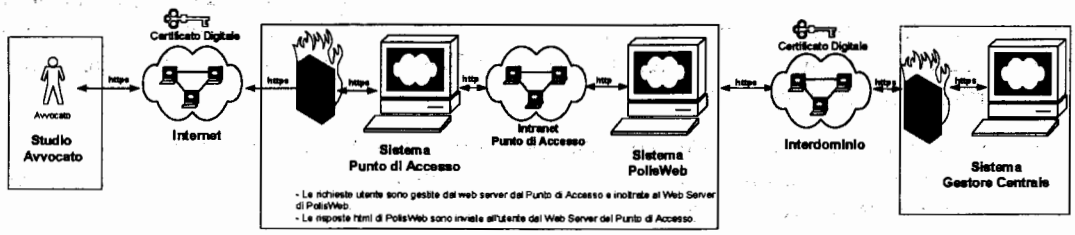

Figura 37 – Architettura per PolisWeb nel Punto di Accesso

Si precisa che il precedente schema è stato volutamente rappresentato con un'immagine e non attraverso un diagramma UML, per dare la percezione schematica della relazione tra il sistema del Punto di Accesso e PolisWeb. Si precisa che essendo Polis Web multipiattaforma, l'applicazione potrà essere opzionalmente installata sulla stessa macchina del Punto di Accesso. Nei paragrafi successivi è riportata la descrizione dei flussi tra PA e PW attraverso un diagramma di sequenza.

Il Punto di Accesso si interpone tra le richieste dell'utente e PolisWeb. Le richieste effettuate dall'utente, tramite browser web, sono autenticate dal Punto di Accesso (smart-card). A seguito dell'autenticazione dell'utente, il Punto di Accesso può attivare PolisWeb tramite l'interfaccia applicativa esposta.

PolisWeb è installato presso la "Server Farm" del punto di accesso e isolato verso l'esterno (Internet, Interdominio, altro).

Nell'analisi dei requisiti di colloquio tra il Punto di Accesso e PolisWeb si evidenziano le seguenti esigenze:

- Attivazione di una sessione utente di PolisWeb.
- Richiesta di Consultazione Informazioni di PolisWeb.
- Chiusura di una sessione utente di PolisWeb.
- Gestione delle eccezioni.

I diagrammi di sequenza, di seguito illustrati, permettono di definire il flusso di colloquio tra il Punto di Accesso e PolisWeb.

Attivazione Sessione Utente di PolisWeb

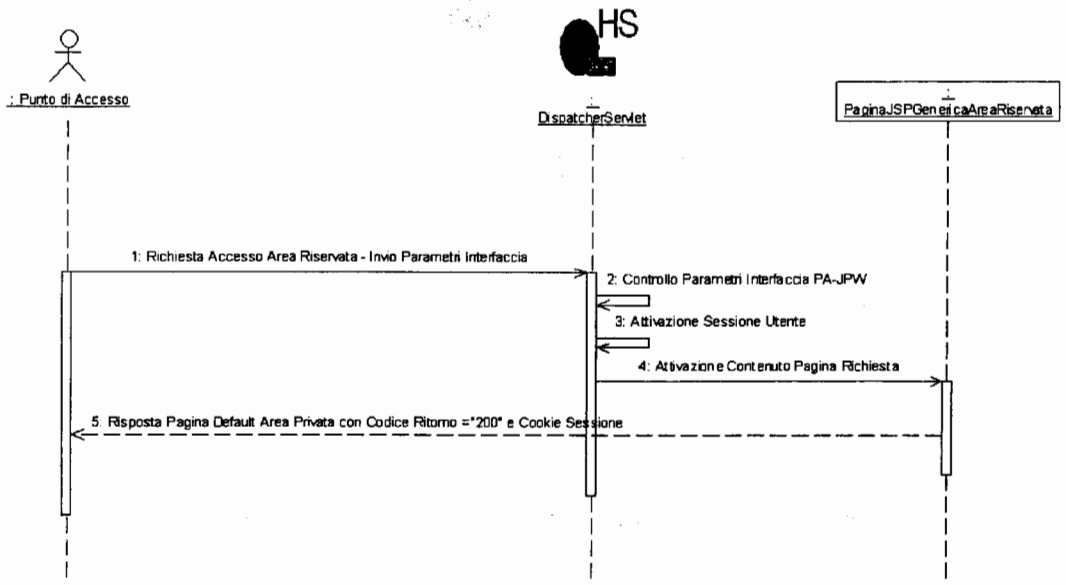

Figura 38 – Sequenza Messaggi PA / FE-PW-PA- Attivazione Sessione

Spiegazione:

- A seguito della richiesta di accesso all'area Privata di PolisWeb da parte di un utente autenticato dal Punto di Accesso, il Punto di Accesso si interfaccia a PolisWeb chiedendo l'attivazione di una sessione utente. L'interfaccia applicativa di PolisWeb per l'attivazione della sessione utente prevede una serie di parametri descritti in dettaglio nel seguito di questa sezione del documento.
- PolisWeb, a seguito della richiesta di attivazione di una sessione utente effettua il controllo dei parametri dell'interfaccia di attivazione, forniti dal Punto di Accesso. L'interfaccia di attivazione e i parametri di interscambio con PolisWeb sono descritti nel paragrafo 7.2.13. (JPW_COD_FISCALE, JPW_COGNOME, JPW_NOME, JPW_DT_ULTIMO_ACCESSO, JPW_INFO_PA).
- Superati i controlli dei parametri (in caso contrario è attivata un'eccezione applicativa da parte di PolisWeb trattata in particolare nell'ultimo diagramma), PolisWeb attiva la sessione utente in base all'utente identificato dal Codice Fiscale ricevuto come parametro.

L'attivazione della sessione prevede il controllo da parte di PolisWeb che, per il Codice Fiscale corrente, non risulti già attiva una sessione (eccezione).

- A seguito dell'attivazione della sessione utente, PolisWeb individua la pagina di default da presentare all'utente a seguito dell'attivazione nell'area privata.
- PolisWeb infine risponde al Punto di Accesso con la pagina html, indicando il Codice Ritorno 200 per la corretta attivazione della sessione utente e il cookie per le informazioni identificative della sessione di PolisWeb.

Consultazione Informazioni di PolisWeb

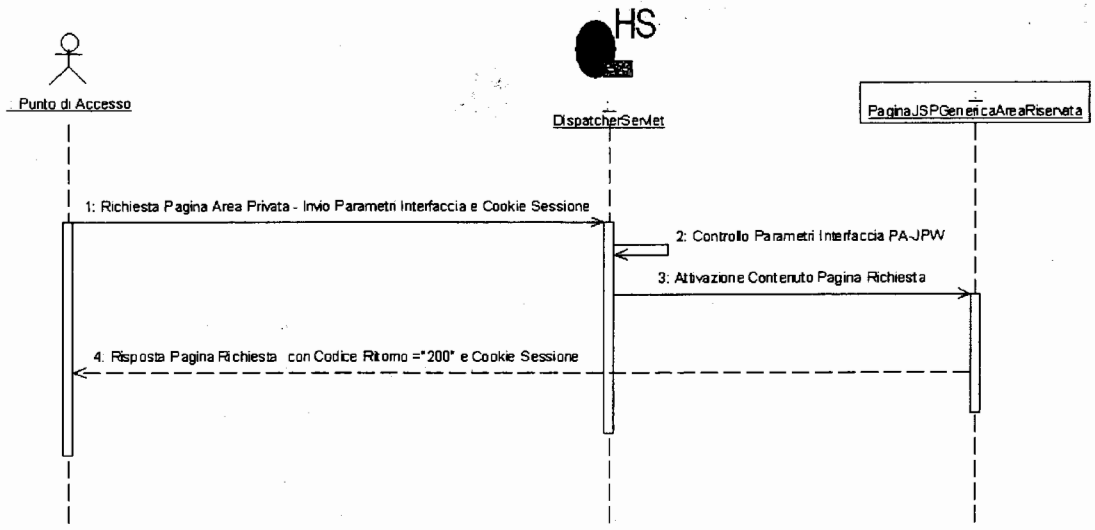

Figura 39 – Sequenza Messaggi PA / FE-PW-PA- Consultazione

Spiegazione:

- Il dialogo tra Punto di Accesso e PolisWeb è basato sullo scambio delle informazioni previste dall'interfaccia applicativa di PolisWeb per ogni richiesta effettuata dal Punto di Accesso. Il Punto di Accesso richiede una singola pagina di Consultazione di PolisWeb, fornendo i parametri dell'interfaccia e il Cookie di sessione ricevuto da PolisWeb dopo l'attivazione della sessione utente attiva.
- PolisWeb controlla i parametri di interfaccia, che prevedono anche il cookie di sessione utente. Il cookie deve determinare in PolisWeb una corrispondenza tra una sessione valida e associata in precedenza al Codice Fiscale, ricevuto nella richiesta corrente (altrimenti Eccezione).
- PolisWeb determina il contenuto html da fornire al Punto di Accesso, in base alla funzione richiesta.
- PolisWeb infine risponde al Punto di Accesso con la pagina html, indicando il Codice Ritorno 200 per la corretta attivazione della sessione utente e il cookie per le informazioni identificative della sessione di PolisWeb.

Chiusura Sessione Utente di PolisWeb

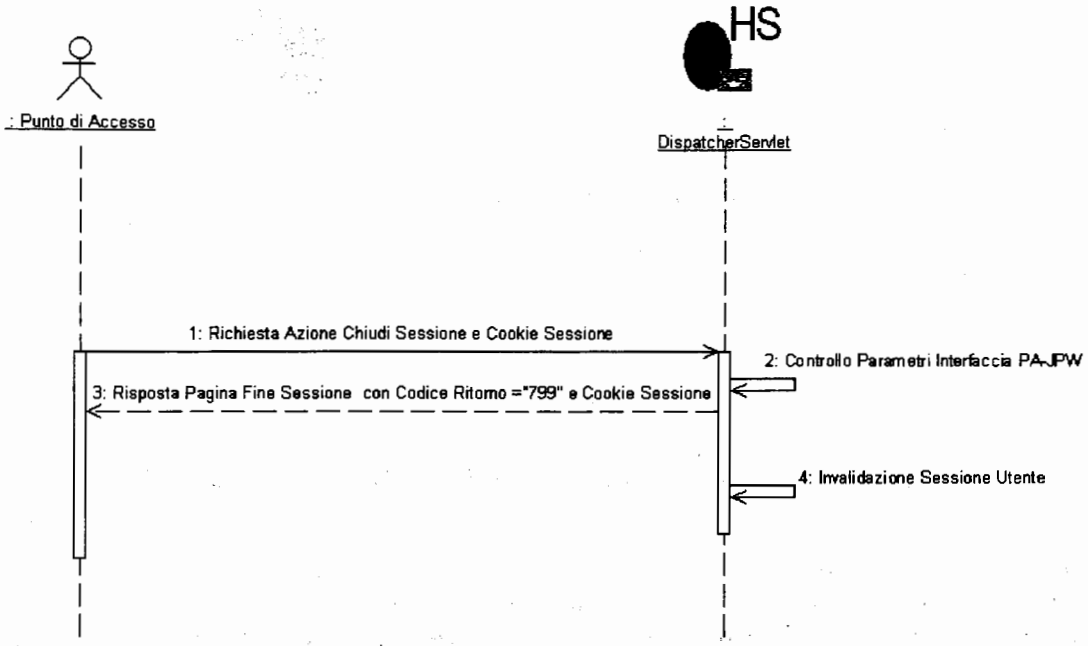

Figura 40 – Sequenza Messaggi PA / FE-PW-PA- Chiusura Sessione

Spiegazione:

- La chiusura della sessione utente in PolisWeb può avvenire attraverso la richiesta diretta della funzione di logout da parte dell'utente, attraverso l'interfaccia utente di PolisWeb fornita all'utente dal Punto di Accesso. PolisWeb espone al Punto di Accesso, un'interfaccia applicativa per richiedere direttamente a PolisWeb la chiusura della sessione utente. Questa funzionalità può risultare utile nel caso in cui il Punto di Accesso determini una propria chiusura di sessione con l'utente (timeout).
- PolisWeb a seguito della richiesta di chiusura di una sessione utente, da Parte del Punto di Accesso, controlla la corrispondenza tra cookie di sessione attivata e il codice fiscale corrispondente (Eccezione se non corrisponde).
- PolisWeb, a seguito della chiusura di una propria sessione utente (anche nel caso di richiesta da parte dell'utente), risponde al Punto di Accesso con un contenuto html, riportando il Codice Ritorno 799 ad indicare l'avvenuta chiusura della sessione utente.

Eccezione PolisWeb in caso di ricezione di parametri errati dal Punto di Accesso

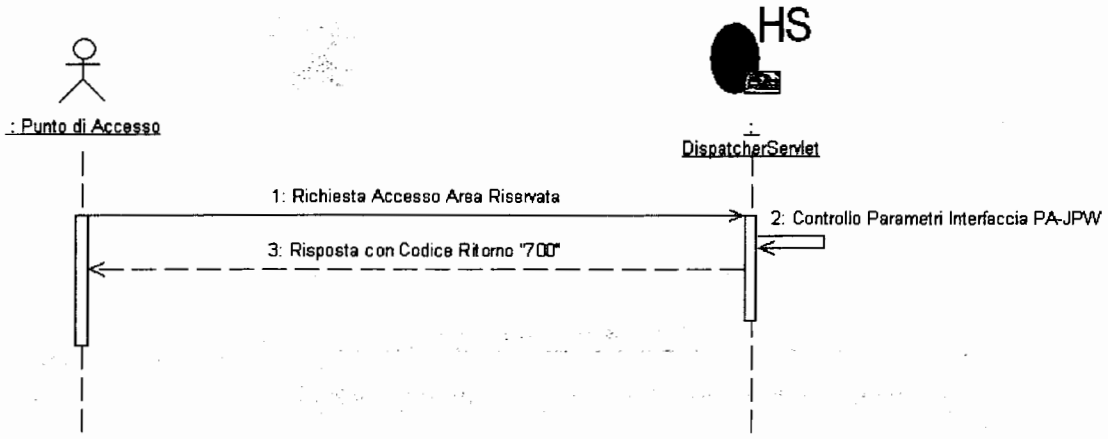

Figura 41 – Sequenza Messaggi PA / FE-PW-PA- Eccezione Parametri Errati

Come descritto nei diagramma di sequenza precedenti, in caso di controlli non validi PolisWeb determina una Eccezione segnalata al Punto di Accesso attraverso il Codice di Ritorno. L'elenco dei codici previsti è riportato successivamente, e nel caso dei parametri errati è impostato a 700.

Eccezione PolisWeb in caso di richiesta di attivazione di una sessione per utente connesso

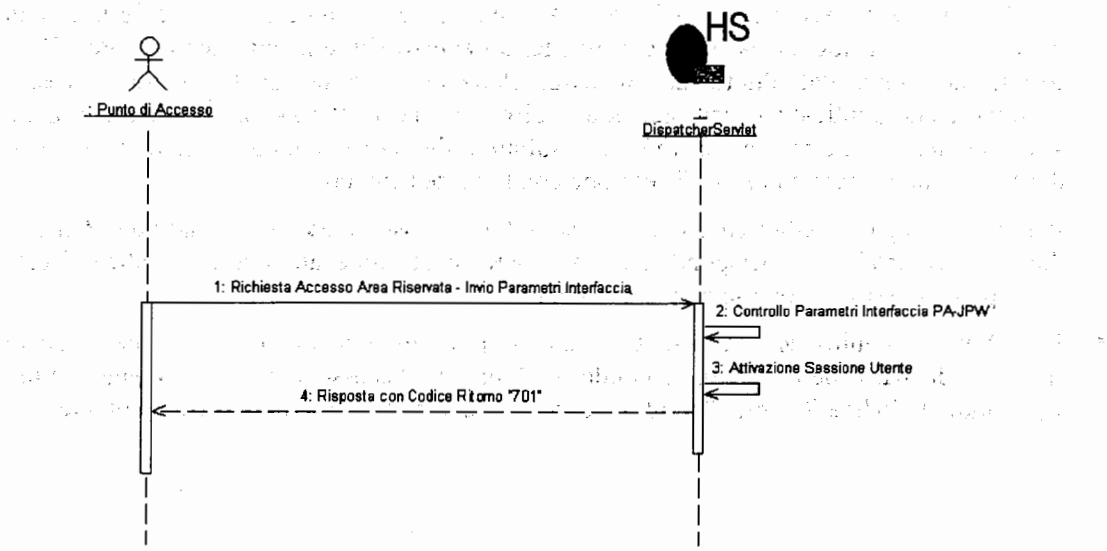

Figura 42 – Sequenza Messaggi PA / FE-PW-PA- Eccezione Utente Connesso

Nel caso di richiesta dell'attivazione per un utente che risulta già connesso il codice di ritorno impostato da PolisWeb per il Punto di Accesso è uguale a 701.

5.3 INTERFACCE PER IL PUNTO DI ACCESSO

Sono descritte le informazioni di interscambio tra il Punto di Accesso e PolisWeb, relative a:

- Richiesta attivazione di una sessione utente di PolisWeb da parte del Punto di Accesso.
- Risposta di PolisWeb al Punto di Accesso , alla richiesta di attivazione di una sessione utente.
- Richiesta a PolisWeb delle pagine del front-end di consultazione dell'area privata, da parte del Punto di Accesso.
- Risposta di PolisWeb alla richiesta da parte del Punto di Accesso delle pagine del front-end di consultazione dell'area privata.
- Richiesta di chiusura di una sessione utente di PolisWeb da parte del Punto di Accesso.
- Risposta di PolisWeb al Punto di Accesso, alla richiesta di chiusura di una sessione utente.
- Risposte di PolisWeb al Punto di Accesso, in caso di Eccezione.

5.3.1 Richiesta "Attivazione Sessione Utente PolisWeb"

Per l'attivazione di una sessione utente di PolisWeb, da parte del Punto di Accesso è fornita un'interfaccia applicativa che prevede l'utilizzo del protocollo http tra PA e PW.

Il PA (Client) invia la richiesta di login verso il server PolisWeb aggiungendo nella testata della richiesta client le informazioni dell'utente, individuate a seguito di un'autenticazione valida con smart-card.

Sono di seguito fornite le modalità di attivazione dell'interfaccia applicativa di PolisWeb e un esempio del relativo messaggio di richiesta http inviata dal PA a PW.

Richiesta http inviata dal Punto di Accesso a PolisWeb per l'attivazione della sessione utente:
http://hostpwpa/pwprivate?action=Login

Esempio di Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Attivazione Sessione

POST /pwprivate?action=Login HTTP/1.0 <CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*<CR><LF>
Accept-Language: it<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: jpolisweb:8081<CR><LF>
JPW_COD_FISCALE: CPRGRGXXXXXXXXX<CR><LF>
JPW_COGNOME: YYYYYYYY<CR><LF>
JPW_NOME: ZZZZZZZZZ<CR><LF>
JPW_DT_ULTIMO_ACCESSO: GG/MM/YYYY HH24:MI:SS<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

Spiegazione:

Il Punto di Accesso fornisce nell'intestazione del messaggio di richiesta http (Header Http_Request) inviato a PolisWeb i seguenti parametri:

- JPW_COD_FISCALE: rappresenta il Codice Fiscale dell'utente autentificato dal Punto di Accesso. Questo parametro è obbligatorio. Il Codice Fiscale dell'utente è utilizzato da

PolisWeb per l'attivazione della sessione utente. Per ogni richiesta di informazione è verificata la presenza di una sessione attiva valida in PolisWeb.

- JPW_COGNOME: rappresenta il Cognome dell'utente. Permette di visualizzare sull'Interfaccia Utente di PolisWeb il nominativo dell'utente attivo nella sessione visualizzata nel browser .
- JPW_NOME: rappresenta il Nome dell'utente. Vedi JPW_COGNOME.
- JPW_DT_ULTIMO_ACCESSO: rappresenta la data di ultimo accesso da parte dell'utente al sistema di consultazione PolisWeb per il Processo Telematica dal Punto di Accesso. Permette di visualizzare sull'Interfaccia Utente di PolisWeb la data di ultimo accesso dell'utente e di poter utilizzare correttamente la consultazione dell'Agenda relativa agli ultimi eventi.
- JPW_INFO_PA: rappresenta un parametro, utile al Punto di Accesso, per l'interscambio di informazioni con PolisWeb. Questo parametro non è necessario a PolisWeb, ma è reso disponibile al Punto di Accesso. Questa informazione è restituita, al Punto di Accesso, nel messaggio di risposta. Un utilizzo pratico può essere ad esempio ricevere e restituire una chiave della sessione utente del Punto di Accesso.

5.3.2 Risposta PolisWeb alla richiesta di "Attivazione Sessione Utente PolisWeb"

PolisWeb alla richiesta di attivazione di una nuova sessione utente risponde al client del Punto di Accesso con un messaggio riportante nella header http i parametri di interfaccia applicativa e il cookie relativo alla sessione utente attivata in PolisWeb.

Esempio di Risposta http resituita da PolisWeb al Punto di Accesso

HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: **JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/**
JPW_CODICE_RITORNO: 200<CR><LF>
JPW_DESCR_SEGNALAZIONE: OK<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

Spiegazione:

- Set-Cookie: JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/: rappresenta l'informazione identificativa della sessione utente di PolisWeb. Questa informazione deve essere ritornata a PolisWeb nelle successive richieste, per associare correttamente utente e sessione utente.
- JPW_CODICE_RITORNO: rappresenta il codice di ritorno previsto da PolisWeb, in base alla codifica riportata nella tabella ...vedi oltre. Nel caso di corretta attivazione della nuova sessione utente assume il valore "200". Per quanto riguarda le situazioni in cui PolisWeb non riesce ad attivare, o determinare, la sessione utente (ad. Es. già collegato) consultare il trattamento delle risposte "*Eccezioni*", analizzate in ultimo.
- JPW_DESCR_SEGNALAZIONE: rappresenta una stringa di descrizione del codice di ritorno. Nel caso di corretta attivazione della sessione utente assume il valore di "OK".

- JPW_INFO_PA: è il parametro ricevuto nella richiesta del Punto di Accesso. Questo parametro è restituito, senza nessun trattamento, in risposta.

Si precisa che la risposta http di PolisWeb contiene oltre ai parametri di interscambio previsti con il PA, anche l'html della prima pagina consultabile dall'utente a seguito dell'attivazione della sessione (pagina di default).

Di seguito vengono elencati i Codici di Ritorno individuati ad oggi:

JPW_COD_RITORNO	JPW_DESCR_SEGNALAZIONE	COMMENTI	PDA
200	OK		Si
700	Parametro invalido o non presente.	Un parametro fondamentale per l'elaborazione non e' presente o è invalido. Esempio mancanza del codice fiscale o dello username nella richiesta.	Si
701	Utente già connesso.	E' stata trovata un'altra sessione attiva per lo stesso Codice Fiscale.	Si
709	Sessione errata.	Le informazioni di sessione non corrispondono ad una sessione valida.	Si
710	Informazioni sessione errata.	Le informazioni di sessione non corrispondono con il Codice Fiscale associato.	Si
799	Chiusura sessione.	L'utente ha richiesto una chiusura della sessione.	Si

Tabella 2 - Codici Ritorno FE-PW-PA

5.3.3 Richiesta "Pagine Area Privata Consultazione PolisWeb"

Il Punto di Accesso successivamente all'attivazione della sessione di PolisWeb, deve inoltrare tutte le richieste dell'utente a PolisWeb dopo aver aggiunto all'intestazione della richiesta http (header http request) i parametri definiti dall'interfaccia di attivazione di PolisWeb.

Esempio Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Consultazione Informazioni

POST /forms/RicercaFascicoliPersonali;**jsessionid=A889EA5555C7A387F36A7A2892045FFD**?action=ElencoFascicoliPersonali HTTP/1.0<CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*<CR><LF>
Referer: http://localhost:8081/pwprivate?action=Login<CR><LF>
Accept-Language: it<CR><LF>
Content-Type: application/x-www-form-urlencoded<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: localhost:8081<CR><LF>
Content-Length: 33<CR><LF>
Pragma: no-cache<CR><LF>
Cookie: JSESSIONID=A889EA5555C7A387F36A7A2892045FFD<CR><LF>
JPW_COD_FISCALE: CPRGRGXXXXXXXXX<CR><LF>
JPW_COGNOME: YYYYYYYY<CR><LF>
JPW_NOME: ZZZZZZZZZ<CR><LF>
JPW_DT_ULTIMO_ACCESSO: GG/MM/YYYY HH24:MI:SS<CR><LF>

<CR><LF>

Spiegazione:

- Cookie: JSESSIONID=A889EA5555C7A387F36A7A2892045FFD: rappresenta l'informazione identificativa della sessione utente in PolisWeb, ricevuta in risposta dal PA dopo la richiesta di attivazione della sessione utente.

- JPW_COD_FISCALE: rappresenta il Codice Fiscale dell'utente. E' obbligatorio. PolisWeb controlla l'associazione del Codice Fiscale con la sessione utente identificata con le informazioni del cookie.
- JPW_COGNOME, JPW_NOME, JPW_DT_ULTIMO_ACCESSO: vedi descrizione fornita nella richiesta di attivazione della sessione.

5.3.4 Risposta di PolisWeb alla richiesta "Pagine Area Privata Consultazione PolisWeb".

La risposta fornita da PolisWeb è nello stesso formato della risposta descritta per la richiesta di attivazione della sessione utente. La risposta differisce nel contenuto l'html della pagina di consultazione richiesta.

5.3.5 Richiesta "Chiusura Sessione Utente PolisWeb"

Sono di seguito forniti le modalità di attivazione dell'interfaccia applicativa di PolisWeb per la chiusura di una sessione utente, e un esempio del relativo messaggio di richiesta http inviata dal PA a PW.

Richiesta http inviata dal Punto di Accesso a PolisWeb per la chiusura della sessione utente: http://hostpwpa/pwprivate?action=Logout

Esempio di Messaggio di Richiesta http inviata dal Punto di Accesso a PolisWeb – Chiusura Sessione

POST /pwprivate;**jsessionid=A889EA5555C7A387F36A7A2892045FFD**?action=Logout HTTP/1.0 <CR><LF>
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*<CR><LF>
Referer: http://localhost:8081/pwprivate?action=Login<CR><LF>
Accept-Language: it<CR><LF>
Content-Type: application/x-www-form-urlencoded<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0) <CR><LF>
Host: localhost:8081<CR><LF>
Content-Length: 33<CR><LF>
Pragma: no-cache<CR><LF>
Cookie: JSESSIONID=A889EA5555C7A387F36A7A2892045FFD<CR><LF>
JPW_COD_FISCALE: CPRGRGXXXXXXXXX<CR><LF>
JPW_COGNOME: YYYYYYYY<CR><LF>
JPW_NOME: ZZZZZZZZZ<CR><LF>
JPW_DT_ULTIMO_ACCESSO: GG/MM/YYYY HH24:MI:SS<CR><LF>
<CR><LF>

Analogamente ai messaggi di richiesta precedenti, per richiedere la chiusura forzata di una specifica sessione utente, occorre attivare l'azione di Logout indicando le informazioni relative all'utente (Cookie e Codice Fiscale).

5.3.6 Risposta PolisWeb per richiesta "Chiusura Sessione Utente PolisWeb"

PolisWeb alla richiesta di chiusura di una sessione utente, dopo aver chiuso la sessione utente, risponde al client del Punto di Accesso con un messaggio riportante nella header http i parametri di interfaccia applicativa previsti

Esempio di Risposta http restituita da PolisWeb al Punto di Accesso per Richiesta Chiusura Sessione

HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: **JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/**
JPW_CODICE_RITORNO: 799<CR><LF>
JPW_DESCR_SEGNALAZIONE: OK<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

Spiegazione:

JPW_COD_RITORNO: con il valore di Codice di Ritorno "799" il punto di accesso ha la conferma della chiusura della sessione e può redirigere l'utente in una funzionalità del Punto di Accesso.

5.3.7 Eccezioni

Con il concetto di eccezione, relativamente all'interfaccia tra PA e PW, si intendono situazioni in cui ad una precisa richiesta del Punto di Accesso PolisWeb non può rispondere come dovuto. Queste eccezioni possono essere dovute sia ad errate impostazione dei parametri di attivazione del Punto di Accesso che per condizioni di stato di PolisWeb. Le eccezioni ad oggi individuate sono le seguenti:

- 700 – Parametro invalido o non presente. Un parametro dell'interfaccia di attivazione di PolisWeb, fondamentale per l'elaborazione della richiesta, non è fornito o è invalido.
- 701 – Utente già connesso. Nell'elaborazione della richiesta di attivazione di una nuova sessione utente, è trovata un'altra sessione attiva per lo stesso Codice Fiscale.
- 709 – Sessione errata. Le informazioni di sessione fornite a PolisWeb attraverso l'interfaccia di attivazione, non corrispondono ad una sessione valida.
- 710 – Informazione sessione errata. Le informazioni di sessione fornite a PolisWeb attraverso l'interfaccia di attivazione, non corrispondono con il Codice Fiscale associato.

Esempio di Risposta http restituita da PolisWeb al Punto di Accesso in caso di Eccezione

HTTP/1.1 200 OK
Content-Type: text/html; charset=iso-8859-1
Connection: close
Date: Tue, 21 Oct 2003 16:03:01 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Set-Cookie: **JSESSIONID= A889EA5555C7A387F36A7A2892045FFD;Path=/**
JPW_CODICE_RITORNO: 700<CR><LF>
JPW_DESCR_SEGNALAZIONE: Parametro invalido o non presente.<CR><LF>
JPW_INFO_PA: XXXXXXXXXXXXXXXXXXXX<CR><LF>
<CR><LF>

Spiegazione:

JPW_COD_RITORNO: con il valore di Codice di Ritorno "700" il punto di accesso ha l'evidenza di una situazione di "Eccezione". In caso di un'eccezione il Punto di Accesso può intercettare e condizionare il flusso http. La risposta di PolisWeb contiene comunque l'html di visualizzazione dell'eccezione riscontrata.

5.3.8 Sicurezza Punto Di Accesso, PolisWeb e Gestore Centrale

Per quanto concerne gli aspetti di sicurezza tra il **Punto di Accesso e PolisWeb** si precisa quanto segue:

- Il sistema PolisWeb è installato e configurato all'interno della Intranet del Punto di Accesso.
- Il sistema PolisWeb non deve essere accessibile dall'esterno della Intranet del Punto di Accesso (Internet, Interdominio, altro).
- Il Punto di Accesso e PolisWeb utilizzano il protocollo di comunicazione http per lo scambio dei messaggi.
- PolisWeb delega l'autenticazione degli utenti al Punto di Accesso (Smart-Card).

Per quanto concerne gli aspetti di sicurezza tra il **PolisWeb e il Gestore Centrale**, si precisa che utilizzano il protocollo Https su SSL con autenticazione client per lo scambio delle informazioni. In particolare l'applicazione web PolisWeb, basata su tecnologia Java, sfrutta il plug-in "*JSSE – Java Security Socket Extention*" recentemente integrato nella distribuzione Java 2 SDK (a partire dalla 1.4.0).

Java Secure Socket Extension (JSSE) è un insieme di package Java che consentono comunicazioni Internet sicure. JSSE implementa una versione dei protocolli SSL e TLD e include funzionalità di cifratura dei dati, autenticazione server, integirtà dei messaggi e autenticazione client opzionale. Utilizzando JSSE, gli sviluppatori possono utilizzare, per il passaggio sicuro di dati tra client e server, qualsiasi protocollo applicativo su TCP/IP (come HTTP, Telnet, NNTP e FTP). Per ulteriori approfondimenti è possibile consultare la documentazione ufficiale disponibile sul sito http://java.sun.com/products/jsse.

5.3.9 Attivazione del Gestore Centrale

Per completare questa sezione relativa a PolisWeb presso un Punto di Accesso, si riporta la modalità di attivazione delle richiste al Gestore Centrale.

Richiesta http inviata da PolisWeb al Gestore Centrale per l'individuazione delle informazioni di back-end presso un Ufficio Giudiziario, fornite dal Gestore Locale:

https://hostgc/NomeLogicoUfficioGiudiziario/PathSoap

Si riporta una sintetica descrizione degli elementi che compongono la richiesta di attivazione di un servizio di back-end:

hostgc: indirizzo telematico del Gestore Centrale configurato in PolisWeb (jpolisweb.xml).

NomeLogicoUfficioGiudiziario: identificativo logico dell'Ufficio Giudiziario configurato in PolisWeb (UfficiGiudiziali.xml), in base all'Ufficio indicato dall'utente nell'impostazione dei parametri di ricerca.

PathSoap: url relativa del servizio di backend configurato in PolisWeb e definito univocamente per l'utilizzato del Gestore Locale (jpolisweb.xml).