

CONSIGLIO DELL'ORDINE DEGLI AVVOCATI DI BUSTO ARSIZIO

**PUNTO DI ACCESSO**  
PER IL PROCESSO CIVILE TELEMATICO

**MANUALE OPERATIVO**

---

*A norma dell'art. 33 del D.M. 17/07/2008 recante le regole tecnico-operative per l'uso di strumenti  
informatici e telematici nel processo civile*

VERSIONE 2.2

11/12/2008

## **Sommario**

Riferimenti.....	4
Acronimi.....	4
1 Premessa.....	5
1.1 Riepilogo dei servizi offerti agli avvocati.....	5
1.2 Concetti di base relativi alle smart card.....	5
2 Dati identificativi.....	6
3 Obblighi e responsabilità.....	6
3.1.1 Obblighi del titolare.....	6
3.1.2 Obblighi di coloro che vi accedono per l'utilizzo dei servizi.....	7
3.1.3 Definizione delle responsabilità e delle eventuali limitazioni agli indennizzi .....	7
4 Tariffe.....	8
5 Modalità operative .....	8
5.1 Funzioni consiglio dell'Ordine degli Avvocati di VigevanoBusto Arsizio .....	8
5.2 Modalità di autenticazione, registrazione e gestione degli utenti .....	8
5.2.1 Gestione degli utenti.....	8
5.2.2 Procedura di registrazione dell'utente (front-office) .....	9
5.2.3 Procedura di autenticazione dell'utente e fase di attivazione dei servizi.....	10
5.2.4 Procedura di Variazione dell'Utente.....	11
5.2.5 Procedura di Cancellazione delle Utenze .....	14
5.3 Modalità di attivazione e gestione degli indirizzi elettronici.....	15
5.4 Il Punto di Accesso rende disponibile agli utenti abilitati una copia operativa del ReLIndEModalità di accesso al registro degli indirizzi elettronici .....	16
6 Politiche e procedure di sicurezza. ....	16
7 Procedure per la fornitura dei servizi .....	17
7.1 Certificazione .....	17
7.2 Deposito atto.....	17
7.2.1 Ricezione dei messaggi di risposta all'inoltro di un atto.....	24
7.2.2 Gestione delle notifiche di eccezione.....	29
7.3 Visualizzazione dello stato degli atti depositati.....	31
7.4 Ricezione dei Biglietti di cancelleria destinati alle CPECPT degli avvocati .....	34
7.4.1 Visualizzazione dei Biglietti di cancelleria ricevuti da un avvocato .....	38
7.5 Accesso ai servizi di consultazione PolisWeb .....	39
7.6 Controllo antivirus.....	39
7.7 Conservazione dei messaggi inviati e ricevuti.....	39

7.7.1 Gestione messaggi scaduti nelle CPECPT.....	39
7.7.2 Storizzazione dei dati e archiviazione .....	40
7.7.3 Registrazione su Giornale di controllo .....	40
7.8 Servizio di distribuzione del software del Ministero .....	41
7.9 Tenuta del giornale di controllo .....	42
7.10 Connettività .....	42
7.11 Assistenza agli utenti .....	42
8 Altre indicazioni.....	42
9 Appendice.....	44
9.1 Architettura del PdA .....	44
9.2 Architettura di PolisWeb .....	44

## RIFERIMENTI

- [1] D.P.R. 13 febbraio 2001, n.123
- [2] D.M. 17 luglio 2008, (regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile) – articolato
- [3] Allegato A alle regole tecniche [2]
- [4] Specifiche di interfaccia tra Punto di Accesso e Gestore Centrale (Versione 2.0) pubblicato sul sito [www.processotelematico.giustizia.it](http://www.processotelematico.giustizia.it)

## ACRONIMI

<i>Acronimo</i>	<i>Descrizione</i>
DGSIA	Direzione Generale dei Sistemi Informativi Automatizzati del Ministero della Giustizia
GC	Gestore centrale
GL	Gestore locale
PCT	Processo civile telematico
PdA	Punto di accesso
PIN	Personal Identification Number
SICI	Sistema informatico civile
UG	Ufficio Giudiziario

## 1 PREMESSA

Il presente manuale operativo è relativo al Punto di Accesso del Consiglio dell'Ordine degli Avvocati di Busto Arsizio, ed è redatto in ottemperanza a quanto disposto dalle regole tecnico-operative [2].

### 1.1 RIEPILOGO DEI SERVIZI OFFERTI AGLI AVVOCATI

Il punto di accesso (PdA) è l'unica struttura tecnico-organizzativa che può rendere disponibile ai soggetti abilitati esterni (avvocati e ausiliari del giudice), previa autenticazione, i servizi del processo civile telematico<sup>1</sup>; tali servizi, forniti esclusivamente agli iscritti all'Ordine degli Avvocati di Busto Arsizio,<sup>2</sup> sono principalmente ed in sintesi:

- Trasmissione telematica degli atti giudiziari civili
- Consultazione web degli atti e delle informazioni (PolisWeb per PCT);<sup>3</sup>
- disponibilità di una casella di posta elettronica certificata del processo telematico, che costituisce l'unico indirizzo telematico, ove il soggetto riceve gli avvisi di cancelleria e (per i difensori) che usa per ricevere ed inviare notifiche telematiche a e da altri difensori; si precisa che detta casella è utilizzabile unicamente per il processo telematico e che non è possibile utilizzare una casella di posta elettronica certificata ordinaria. L'accesso a tale casella è consentito al solo utente proprietario (o agli eventuali rappresentanti legali dei CdO), esclusivamente in modalità applicativa attraverso un servizio offerto dal PdA. Non è prevista la possibilità da parte dell'utente di gestire il contenuto della casella, né di inviare messaggi se non attraverso funzionalità applicative espressamente realizzate.

Gli atti telematici depositabili, e quali Uffici Giudiziari sono abilitati all'accettazione, sono stabiliti con Decreto della D.G.S.I.A.,<sup>4</sup> e pubblicati sul sito [www.processotelematico.giustizia.it](http://www.processotelematico.giustizia.it).

L'indirizzo dell'area pubblica del punto di accesso, ove sono disponibili ulteriori informazioni, è il seguente: <https://busto.ul.consiglioordineavvocati.it>.

### 1.2 CONCETTI DI BASE RELATIVI ALLE SMART CARD

La smart card è lo strumento che assolve alle seguenti funzioni:

- apposizione della firma digitale;
- autenticazione via web: consente di identificare univocamente il possessore e di creare un canale sicuro (criptato) tra il PC che legge la smart card e il sistema (server) con il quale è stabilita la connessione, nel caso specifico tra il PC dell'avvocato e il punto di accesso;
- cifratura degli atti in uscita: consente all'avvocato (e solo tramite la sua smart card) di decifrare un atto, qualora questo sia cifrato.

---

<sup>1</sup> D.M. 17/07/2008 (Regole tecniche PCT), art. 2, comma 1, lettera e  
<sup>2</sup> D.M. 17/07/2008, art. 6, comma5, lettera b.  
<sup>3</sup> D.M. 17/07/2008, art.29, comma 1  
<sup>4</sup> D.M. 17/07/2008, art.62, comma 1

Per assolvere a queste funzioni, sulla smart card sono contenuti altrettanti *certificati*, che per essere utilizzati necessitano di un PIN.

## 2 DATI IDENTIFICATIVI

Codice identificativo <sup>5</sup>	PDACDOBUSTO
Descrizione PdA	Punto di Accesso del Consiglio dell'Ordine degli Avvocati di Busto Arsizio
Casella di posta elettronica di sistema	postmaster@busto.ul.consiglioordineavvocati.it
Dominio della posta elettronica ordinaria	@busto.ul.consiglioordineavvocati.it
Dominio della posta elettronica certificata	@pec.busto.ul.consiglioordineavvocati.it
Codice albo (in quanto gestito dal PdA)	CDO0120260097
Descrizione albo	Albo iscritti al Consiglio dell'Ordine degli Avvocati di Busto Arsizio.
Responsabile del manuale operativo	Avv. Brunella Cardani
Sede legale del soggetto titolare <sup>6</sup>	Largo Giardino Tel. 0331.635022 fax 0331.678602_
Nome secondo lo standard X.500 <sup>7</sup>	PDACDOBUSTO/CDO0120260097
Indirizzo internet <sup>8</sup>	<a href="https://busto.ul.consiglioordineavvocati.it">https://busto.ul.consiglioordineavvocati.it</a>
Dati legale rappresentante <sup>9</sup>	nome: Brunella cognome: Cardani codice fiscale: CRDBNL55D49D869E indirizzo elettronico: puntodiaccesso@busto.ul.consiglioordineavvocati.it numero di telefono: 0331791776 numero di fax: 0331705859
Elenco dei numeri telefonici di accesso <sup>10</sup>	Non applicabile

Il server e tutte le apparecchiature hardware del punto di accesso sono fisicamente dislocate presso la sede operativa della società ELSAGDATAMAT S.p.A., nello stabile di Via Laurentina 760.

## 3 OBBLIGHI E RESPONSABILITÀ

### 3.1.1 *Obblighi del titolare*

Gli obblighi del titolare del punto di accesso sono di:

- mantenere aggiornate le anagrafiche, con cadenza almeno settimanale;
- verificare il corretto funzionamento dei servizi (servizio svolto in deroga dalla società Net Service s.r.l. di Bologna).

<sup>5</sup> [2] Art. 31, comma 1, lettera a

<sup>6</sup> [2] Art. 31, comma 1, lettera b

<sup>7</sup> [2] Art. 31, comma 1, lettera c

<sup>8</sup> [2] Art. 31, comma 1, lettera d

<sup>9</sup> [2] Art. 31, comma 1, lettera e

<sup>10</sup> [2] Art. 31, comma 1, lettera f

### **3.1.2 Obblighi di coloro che vi accedono per l'utilizzo dei servizi**

È necessario, per coloro che intendono utilizzare i servizi del punto di accesso, dotarsi di smart-card con certificato di autenticazione, rilasciata da una Certification Authority (CA) accreditata dal CNIPA e compatibile con il PdA.

Le Smart card compatibili sono elencate nell'area pubblica del punto di accesso.

Per completezza, si riporta di seguito l'articolo 36 [2] "Postazioni di lavoro dei soggetti abilitati esterni", per quanto di pertinenza.

1. La postazione di lavoro dei soggetti abilitati esterni è l'insieme delle risorse hardware, software e di rete da loro utilizzate direttamente [...] per la consultazione del SICI.
2. La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario [...] all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi.

Il punto di Accesso non risponde di eventuali malfunzionamenti nei casi in cui le postazioni di coloro che accedono ai servizi non siano configurate come testé definito.

Ogni utente è tenuto ad informare tempestivamente il Consiglio dell'Ordine in caso di smarrimento o furto del dispositivo di autenticazione, di compromissione della segretezza della chiave privata.

L'utente prende inoltre atto di essere l'unico responsabile della protezione della propria chiave privata da danni, perdite, divulgazioni, modifiche o usi non autorizzati e si impegna a richiedere, in caso di smarrimento o sottrazione del dispositivo di autenticazione, la sospensione immediata del certificato, rivolgendosi alla Certification Authority.

### **3.1.3 Definizione delle responsabilità e delle eventuali limitazioni agli indennizzi**

Net Service Srl, quale operatore qualificato per conto del Consiglio dell'Ordine degli Avvocati di Busto Arsizio, e gestore del Punto di Accesso:

- non risponde di eventuali malfunzionamenti nei casi in cui le postazioni di coloro che accedono ai servizi non siano configurate come definito al punto 3.1.2;
- non risponde per l'ipotesi di utilizzo del servizio difforme da quanto descritto nel presente manuale;
- limita ogni ipotesi di responsabilità ai soli casi di dolo o colpa grave, ritenendo esclusa ogni responsabilità per danni, da chiunque subiti, causati da caso fortuito o forza maggiore.

La Net Service Srl renderà le eventuali documentazioni di disservizio dovute agli ISP Provider.

Le denunce per vizi o malfunzionamenti, nei limiti di cui ai precedenti punti, unitamente alle eventuali pretese risarcitorie, dovranno prevenire in forma raccomandata a.r. alla sede della Net Service Srl, e per conoscenza al Consiglio dell'Ordine di Busto Arsizio, a pena di decadenza, entro cinque giorni dal loro verificarsi.

L'utente dichiara di mantenere indenne e di malleverare il Consiglio dell'Ordine e la Net Service Srl da ogni richiesta di danni diretti e/o indiretti, da terzi eventualmente avanzata a qualsiasi titolo o ragione per fatti imputabili esclusivamente all'utente stesso.

## 4 TARIFFE

Allo stato non è previsto nessun onere di tipo economico per gli iscritti al Consiglio dell'Ordine degli Avvocati di Busto Arsizio relativamente ai servizi disponibili sul Punto di Accesso in oggetto.

## 5 MODALITÀ OPERATIVE

### 5.1 FUNZIONI CONSIGLIO DELL'ORDINE DEGLI AVVOCATI DI BUSTO ARSIZIO

Per la realizzazione del flusso di iscrizione e registrazione dei difensori, il Consiglio dell'Ordine degli avvocati ha a propria disposizione una casella di posta certificata del Processo Telematico (CPECPT), in modo da potere scambiare i messaggi di comunicazione dei dati degli iscritti con il gestore centrale.

L'accesso alla CPECPT è riservato al Presidente del Consiglio dell'Ordine e ad eventuali suoi rappresentanti.

La postazione di lavoro del Consiglio dell'Ordine è collegata alla rete Internet e dotata di lettore di smart card per l'autenticazione. L'autenticazione infatti viene effettuata con le stesse modalità (*strong authentication*) previste per i soggetti abilitati esterni.

La dotazione software delle postazioni del Consiglio dell'Ordine prevede:

- strumenti per creare il file XML nel formato previsto per le comunicazioni relative ai dati dei soggetti abilitati (in alternativa si potrà disporre del tool integrato al Punto di Accesso)
- software per la firma digitale dei file XML

### 5.2 MODALITÀ DI AUTENTICAZIONE, REGISTRAZIONE E GESTIONE DEGLI UTENTI

La gestione delle utenze relative ai soggetti abilitati ad operare nel Processo Telematico viene effettuata con un complesso di procedure, descritte nelle Regole tecnico-operative [2].

#### 5.2.1 Gestione degli utenti

I profili d'utenza applicativi gestiti dal PdA del CdO degli Avvocati di Busto Arsizio sono limitati a:

- difensori di parti private e avvocati iscritti presso il Consiglio dell'Ordine degli Avvocati di Busto Arsizio (d'ora in avanti avvocati o difensori);
- amministratore di PdA, per le funzioni di amministrazione delle utenze e le interazioni con il giornale di controllo;
- legale rappresentante di CdO, con funzionalità di gestione di una CPECPT, utilizzata per la creazione, aggiornamento e cancellazione delle utenze relative ai propri iscritti.

Il profilo d'utenza viene determinato dal PdA in base al ruolo associato all'utente connesso, a sua volta identificato mediante il processo di autenticazione; nel corso del processo di autenticazione si verifica la validità del certificato utilizzato.

Tutti gli utenti (con l'eccezione degli amministratori) dispongono di una casella di posta elettronica del processo telematico (CPECPT) in cui ricevere i documenti informatici trasmessi per il tramite del Gestore Centrale (GC).

Gli avvocati possono effettuare consultazioni dei dati processuali nei limiti dei profili funzionali definiti e dei privilegi determinati a livello di UG.

### **5.2.2 Procedura di registrazione dell'utente (front-office)**

Per la creazione di un utente è necessario seguire le procedure descritte dalle Regole tecnico-operative, allo scopo di generare la CPECPT del soggetto abilitato e ad inserire tutti i dati richiesti dalle Regole stesse.

Le Regole Tecniche stabiliscono, agli articoli 14, 16 e 17, un flusso abilitativo che viene di seguito schematizzato:

1. i soggetti esterni che desiderano registrarsi presso un punto di accesso, devono produrre una richiesta scritta, comunicando i seguenti dati (art. 14):
  - nome e cognome;
  - luogo e data di nascita;
  - codice fiscale;
  - residenza;
  - domicilio;
  - certificato digitale, relativo alla chiave pubblica, per la cifratura;
  - codice consiglio dell'ordine di appartenenza (Busto Arsizio);
  - inoltre è richiesto un certificato per i difensori, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine attesta l'iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati oppure la qualifica che legittima all'esercizio della difesa e l'assenza di cause ostantive allo svolgimento dell'attività difensiva;
2. (art. 14 comma 7) il punto di accesso acquisisce tutti i dati necessari all'inserimento nei registri degli indirizzi elettronici, genera l'indirizzo elettronico e invia i dati acquisiti al gestore centrale dell'accesso e al consiglio dell'ordine;
3. (art. 16, comma 4 e 5) gli avvocati comunicano, al consiglio dell'ordine i propri dati identificativi insieme all'indirizzo elettronico rilasciato dal PdA ed ai dati identificativi del punto di accesso.

Lo scambio di messaggi tra PdA, GC e CdO avviene per via telematica, e le comunicazioni sono strutturate in linguaggio XML, secondo il formato definito nel relativo decreto ministeriale.

Di seguito la descrizione del flusso relativo alla creazione di un'utenza (avvocati):

1. L'avvocato iscritto al Consiglio dell'Ordine degli Avvocati di Busto Arsizio si collega all'url messo a disposizione dal Consiglio dell'Ordine (nel vademecum,

- nel proprio sito internet, nel materiale divulgativo e presso la sede del Consiglio dell'Ordine);
2. L'avvocato inserisce la propria smart card nell'apposito lettore e procede alla compilazione della form di richiesta iscrizione inserendo i dati richiesti. Tra i dati richiesti vi è l'obbligatorietà della chiave pubblica del certificato di cifratura che risiede sulla smart card dell'avvocato (si veda al riguardo il paragrafo 1.2). Le modalità di estrazione di tale certificato dalla smart card sono indicate nel contesto della pagina web di registrazione;
  3. L'avvocato spedisce la form dopo aver verificato la congruenza dei dati;
  4. L'avvocato salva e stampa la lettera di richiesta iscrizione autostrutturata a seguito della fornitura dei dati inseriti;
  5. L'avvocato entro 3gg (oltre i quali la richiesta informatica viene cancellata) si presenta al CdO per depositare la lettera di richiesta iscrizione firmata nonché la copia del Codice Fiscale;
  6. La persona delegata del Consiglio dell'Ordine verifica ed accetta la documentazione cartacea certificando l'iscrizione all'Albo e l'abilitazione del richiedente;
  7. La persona delegata del Consiglio dell'Ordine, attraverso un'apposita sezione del Punto di Accesso, provvede quindi ad inoltrare al Gestore Centrale la richiesta in questione, una volta verificata la presenza della richiesta scritta; provvede inoltre a comunicare al Gestore Centrale la cancellazione delle richieste scadute;
  8. Il Punto di Accesso genera l'indirizzo elettronico dell'avvocato;
  9. Il Punto di Accesso verifica che l'avvocato non abbia già un indirizzo elettronico nel Registro Generale degli Indirizzi, e invia al Gestore Centrale una richiesta di abilitazione dell'avvocato, in un formato XML che comprende codice fiscale, indirizzo elettronico, chiave pubblica del certificato di cifratura e dati anagrafici dell'avvocato;
  10. Il Gestore Centrale effettua i controlli formali sul messaggio ed in caso di esito positivo invia un'attestazione temporale. In caso di errore nel formato del messaggio viene inviata una notifica di eccezione ed il flusso viene interrotto;
  11. Il Gestore Centrale verifica il merito della richiesta. In caso di esito positivo aggiorna il Registro Generale degli Indirizzi Elettronici con i dati dell'avvocato e invia al Punto di Accesso un file XML contenente gli indirizzi abilitati. In caso di esito negativo (ad esempio se l'avvocato è già presente nel ReGIndE) invia al Punto di Accesso un messaggio contenente l'anomalia;
  12. il Punto di Accesso del Consiglio dell'Ordine degli Avvocati di Busto Arsizio riceve il file XML, verifica i dati ottenuti, a sua volta aggiorna il Registro Locale degli Indirizzi, abilitando l'avvocato. All'avvocato è consentito l'accesso sul PdA a partire dal giorno successivo all'iscrizione sul Registro Generale degli indirizzi Elettronici.

I punti da 8 a 12 sono implementati in maniera automatica.

### **5.2.3 Procedura di autenticazione dell'utente e fase di attivazione dei servizi**

Il Punto di Accesso fornisce il servizio di autenticazione dei soggetti abilitati.

La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario alla gestione su smart card dell'autenticazione nei confronti del punto di accesso (*client authentication*).

Per accedere alla funzione di autenticazione, l'utente deve collegarsi dal browser alla pagina iniziale (*home page*) del Consiglio dell'Ordine degli Avvocati di Busto Arsizio (<https://busto.ul.consiglioordineavvocati.it>), inserendo la smart card contenente il certificato di autenticazione nel lettore.

Il Punto di Accesso per il CdO degli avvocati di Busto Arsizio accetta, per l'autenticazione dei soggetti abilitati, solo smart card compatibili (il cui elenco è riportato nell'area pubblica del punto di accesso).

Ciascun utente può utilizzare diversi certificati di autenticazione, registrati su supporti smart card separati, purché contengano il codice fiscale nel campo predeterminato. Il Punto di Accesso si limita quindi a verificare che il soggetto che richiede l'autenticazione, identificato tramite il codice fiscale, sia registrato nella base dati locale<sup>11</sup> ed abilitato ad operare.

#### **5.2.4 Procedura di Variazione dell'Utente**

Per effettuare la variazione dei dati di registrazione di un utente, le procedure da seguire ricalcano il flusso di inserimento.

Oltre alla modalità di variazione dei dati anagrafici richiesta dall'utente stesso (avvocato) è prevista la variazione dello stato dell'avvocato, comunicata dal Consiglio dell'Ordine (ad esempio per una sospensione o per la radiazione) con l'invio di un file XML di variazione dati dell'Albo.

Lo scambio di messaggi tra PdA, GC e CdO avviene sempre per via telematica, e le comunicazioni sono strutturate in linguaggio XML, secondo il formato definito nel relativo decreto ministeriale.

Per la procedura di variazione dell'Utente si possono considerare quindi due casistiche.

##### **Variazione generata dall'utente stesso (avvocato).**

I soggetti abilitati esterni iscritti al Punto di Accesso possono inviare richieste di variazione dei propri dati di registrazione.

Il Punto di Accesso mette a disposizione una form di registrazione, all'interno dell'area privata, per l'inserimento dei dati da modificare e l'invio della richiesta.

L'accesso a tale form è soggetto ai controlli di autenticazione richiesti per l'accesso all'area privata del PdA, basati sul controllo del certificato registrato nella smart card dell'utente, ed avviene in modalità SSL.

Il PdA controlla che il certificato contenuto nella smart card sia valido, ed esegue anche i seguenti controlli:

- controlla che la CA che ha emesso il certificato del soggetto sia abilitata sul PdA;
- verifica che il codice fiscale sia contenuto all'interno del certificato nella posizione prevista e che sia valido;

---

<sup>11</sup> È opportuno ricordare che tutti i soggetti che utilizzano il Punto di Accesso del CdO degli avvocati di Busto Arsizio devono aver completato la procedura di registrazione così come indicata nel paragrafo 5.2.2. Tale procedura si completa infatti con la registrazione del soggetto sulla base dati locale del punto di accesso.

- verifica che il CF dell'utente sia già iscritto sul PdA;
- verifica che il CF non abbia già una richiesta di modifica dati in corso di esecuzione sullo stesso PdA;
- verifica che il soggetto sia presente sul ReGInde del gestore centrale.

Nel caso in cui i controlli abbiano esito positivo, viene visualizzata una pagina che consente di inserire tutti i dati richiesti. I campi Codice Fiscale, Cognome e Nome sono riempiti dal sistema e non sono modificabili.

A seguito dell'inserimento dei dati anagrafici dell'utente, si richiede l'upload del certificato di cifratura, che deve essere caricato sul PdA per il successivo invio al gestore centrale e la registrazione sul ReGIndE. Questo passo può essere saltato nel caso in cui l'utente non desideri modificare il proprio certificato. Il certificato eventualmente inserito viene verificato per controllare che sia in corso di validità, che sia utilizzabile per la cifratura e che contenga la relativa chiave pubblica.

Successivamente viene visualizzata una pagina in cui sono evidenziati tutti i dati inseriti, e viene richiesta la conferma della modifica dei dati.

A seguito della ricezione della conferma, il PdA provvede ad inserire i dati nella tabella delle richieste ricevute.

Al termine delle operazioni viene visualizzata una pagina, in formato stampabile, che contiene tutti i dati dell'utente. Questa pagina deve essere stampata a cura dell'utente, firmata e consegnata al proprio CdO (solo per gli avvocati).

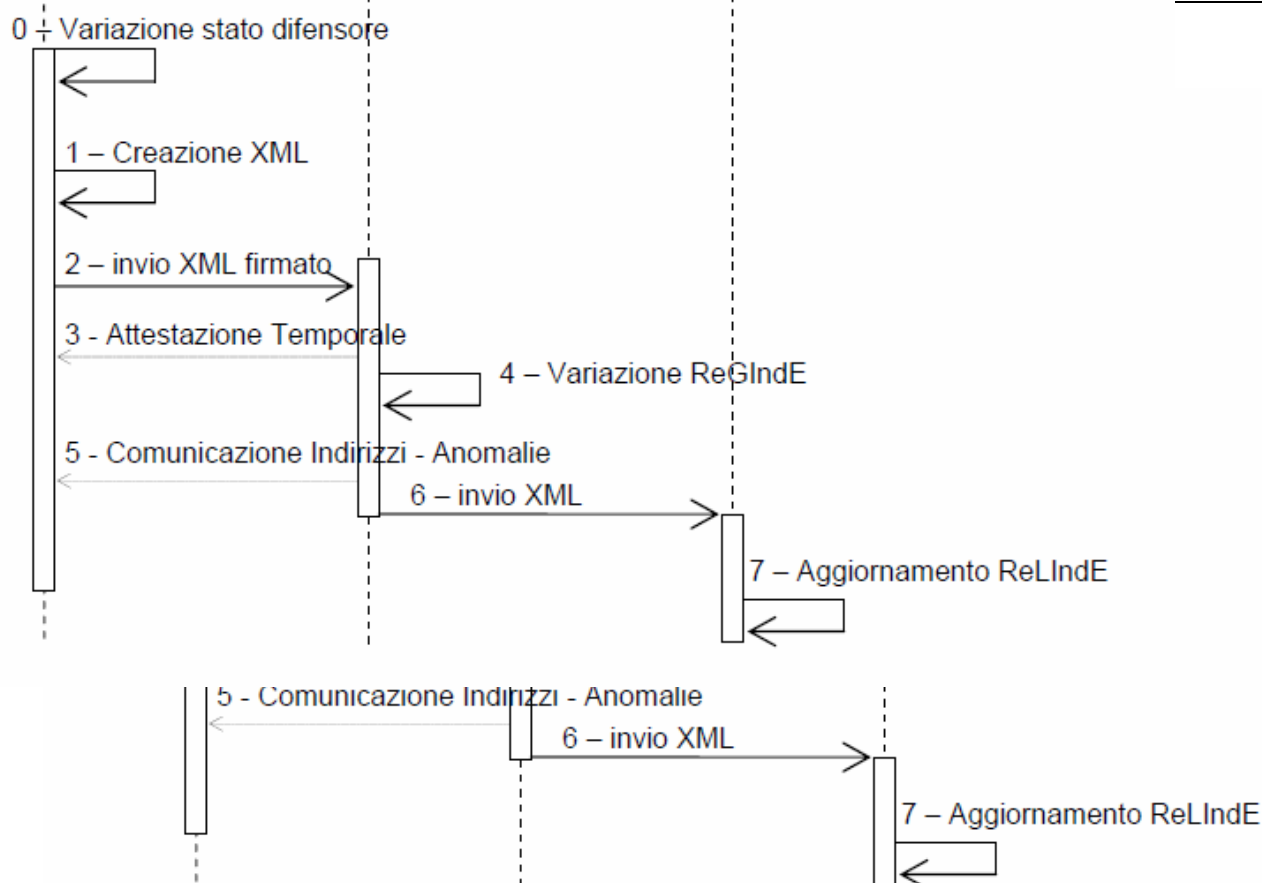
Le richieste accettate al punto precedente sono processate automaticamente dal PdA per eseguire le seguenti attività:

- preparazione di un file XML contenente le informazioni inserite nelle fasi precedenti (in base al DTD di registrazione dei soggetti, contenente tutti i dati necessari al trattamento della richiesta, vedi Decreto DTD)
- invio del file XML di cui al punto precedente al gestore centrale

La modifica dei dati ha effetto solo a seguito della ricezione della conferma dell'effettuazione della relativa modifica sul ReGIndE da parte del gestore centrale. Tale conferma viene inviata dal Gestore Centrale al CdO a seguito della corretta elaborazione della richiesta di variazione dei dati effettuata dall'utente attraverso il PdA.

### **Variazione dello stato del difensore generata dal Consiglio dell'Ordine**

Il flusso previsto è il seguente:



**Figura 3 – Flusso di variazione utenza – generata dal CdO**

Lo scambio di messaggi tra PdA, GC e CdO avviene sempre per via telematica, e le comunicazioni sono strutturate in linguaggio XML, secondo i formati definiti nel relativo decreto ministeriale.

Di seguito una descrizione del flusso:

- Il Consiglio dell'Ordine varia lo stato del difensore e crea il file XML contenente i dati dell'avvocato e il nuovo stato (attivo, sospeso, radiato, ecc.);
- il file XML viene firmato dal Presidente del CdO o dal Delegato Rappresentante ed inviato alla casella di posta certificata del Gestore Centrale;
- Il Gestore Centrale, dopo avere effettuato i controlli formali invia alla CPECPT del Consiglio dell'Ordine un'attestazione temporale in caso di esito positivo, una notifica di eccezione altrimenti. Quindi controlla il merito della richiesta e in caso positivo si predispose all'aggiornamento del ReGIndE (che sarà operativo il giorno lavorativo seguente) con i dati dell'avvocato ed invia all'Ordine un file XML con i dati modificati. In caso di esito negativo dei controlli il GC invia un messaggio contenente l'anomalia alla CPECPT dell'Ordine;
- Il Gestore Centrale inoltra al Punto di Accesso il file XML ricevuto dal Consiglio dell'Ordine;
- Il Punto di Accesso aggiorna il Registro Locale degli Indirizzi.

### **5.2.5 Procedura di Cancellazione delle Utenze**

I soggetti abilitati esterni iscritti al Punto di Accesso possono inviare richieste di cancellazione della propria utenza.

Il Punto di Accesso mette a disposizione una form, all'interno dell'area privata, per l'inserimento delle richieste di cancellazione.

L'accesso a tale form è soggetto ai controlli di autenticazione richiesti per l'accesso all'area privata del PdA, basati sul controllo del certificato registrato nella smart card dell'utente, ed avviene in modalità SSL.

Il PdA controlla che il certificato contenuto nella smart card sia valido, ed esegue anche i seguenti controlli:

- controlla che la CA che ha emesso il certificato del soggetto sia abilitata sul PdA;
- verifica che il codice fiscale sia contenuto all'interno del certificato nella posizione prevista e che sia valido;
- verifica che il CF dell'utente sia già iscritto sul PdA;
- verifica che il CF non abbia già una richiesta di cancellazione dell'utenza in corso di esecuzione sullo stesso PdA;
- verifica che il soggetto sia presente sul ReGInde del gestore centrale.

Nel caso in cui i controlli abbiano esito positivo, viene visualizzata una pagina in cui viene richiesta la conferma della cancellazione dell'utenza.

A seguito della ricezione della conferma, il PdA provvede ad inserire i dati nella tabella delle richieste ricevute.

Al termine delle operazioni viene visualizzata una pagina, in formato stampabile, che contiene tutti i dati della richiesta. Questa pagina deve essere stampata a cura dell'utente, firmata e consegnata al proprio CdO.

Le richieste accettate al punto precedente sono processate automaticamente dal PdA per eseguire le seguenti attività:

- preparazione di un file XML contenente le informazioni dell'utente (in base al DTD di registrazione dei soggetti, contenente tutti i dati necessari al trattamento della richiesta, vedi Decreto DTD) nel formato di richiesta cancellazione
- invio del file XML di cui al punto precedente al gestore centrale

La cancellazione viene eseguita a seguito della ricezione della conferma da parte del gestore centrale. Tale conferma viene inviata dal Gestore Centrale al CdO a seguito della corretta elaborazione della richiesta di variazione dei dati effettuata dall'utente attraverso il PdA.

La cancellazione non comporta l'eliminazione del soggetto abilitato all'interno dell'archivio anagrafico del PDA, a solo la revoca dell'accesso (stato dell'utenza = non attivo).

### 5.3 MODALITÀ DI ATTIVAZIONE E GESTIONE DEGLI INDIRIZZI ELETTRONICI

Il Punto di Accesso attiva un registro degli indirizzi elettronici che contiene l'elenco di tutti gli indirizzi elettronici emessi, revocati o sospesi dal punto di accesso.<sup>12</sup>

Il registro verrà di seguito chiamato come Registro Locale degli Indirizzi Elettronici (ReLIndE) per differenziarlo dal ReGIndE.

Il ReLIndE contiene i seguenti dati<sup>13</sup>:

1. Ad ogni indirizzo elettronico di persona fisica sono associate le seguenti informazioni:
  - a) nome e cognome;
  - b) luogo e data di nascita;
  - c) codice fiscale
  - d) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
  - e) residenza;
  - f) domicilio;
  - g) stato dell'indirizzo: attivo, non attivo;
  - h) certificato digitale relativo alla chiave pubblica, da utilizzare per la cifratura;
  - i) data, ora e minuti dell'ultimo aggiornamento del certificato digitale;
  - j) consiglio dell'ordine o ente di appartenenza;
  - k) stato del soggetto abilitato: attivo, non attivo;
  - l) codice del Punto di Accesso di appartenenza;
  - m) ruolo del soggetto abilitato: avvocato, CTU.
2. L'indirizzo elettronico di enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, associa le seguenti informazioni:
  - a) denominazione sociale;
  - b) codice fiscale;
  - c) data ed ora dell'ultima variazione dell'indirizzo elettronico;
  - d) sede legale;
  - e) certificato digitale relativo alla chiave pubblica da utilizzare per la cifratura;
  - f) data ed ora dell'ultimo aggiornamento del certificato digitale;
  - g) stato dell'indirizzo: attivo, non attivo.

Il registro viene alimentato e variato, da procedure automatiche, al termine delle operazioni di iscrizione di un soggetto esterno, di variazione e cancellazione del profilo utente, così come descritto nei paragrafi 5.2.2, 5.2.4 e 5.2.5.

---

<sup>12</sup> [2] Art. 16, comma 1.  
<sup>13</sup> [2] Art. 16, comma 2.

## 5.4 MODALITÀ DI ACCESSO AL REGISTRO DEGLI INDIRIZZI ELETTRONICI

L'accesso al registro degli indirizzi avviene in conformità al protocollo ldap (come definito nella specifica pubblica RFC 1777 e successive modificazioni).<sup>15</sup>

Relativamente all'autenticazione<sup>16</sup>, è prevista l'adozione di SSL e identificazione tramite username e password, rilasciati dal punto di accesso, e comunicati nel messaggio di posta elettronica certificata di avvenuta attivazione dell'avvocato.

## 6 POLITICHE E PROCEDURE DI SICUREZZA.

Per la descrizione delle politiche e procedure di sicurezza si rimanda al documento "piano per la sicurezza".

## 7 PROCEDURE PER LA FORNITURA DEI SERVIZI<sup>17</sup>

### 7.1 CERTIFICAZIONE

Il punto di accesso esegue la certificazione del difensore<sup>18</sup>; quando prevista questa viene effettuata dal sistema accedendo al database degli avvocati abilitati alle funzionalità del Processo Civile Telematico. (vedi paragrafo successivo)

### 7.2 DEPOSITO ATTO

La funzione di deposito atto consente ad un soggetto abilitato esterno (avvocato) di inviare al SICI un documento informatico. Le modalità di formazione del documento informatico e della busta che lo contiene non sono oggetto della presente analisi; dettagliate informazioni al riguardo possono essere reperite dal documento "Specifiche di interfaccia tra Punto di Accesso e Gestore Centrale" [4].

La funzione invia al client dell'avvocato una form per la selezione della busta predisposta localmente, che contiene le informazioni di instradamento dell'atto (file *Infolnltro.xml*) e l'atto informatico cifrato (file *Atto.enc*).

A seguito della scelta della busta e della conferma da parte dell'utente, viene attivato l'upload della busta stessa.

La struttura del file Infolnltro.xml è schematizzata nella figura che segue:

---

<sup>15</sup> [2] Art. 19.

<sup>16</sup> [2] Art. 16, comma 6.

<sup>17</sup> [2] Art. 30, comma 5. *Le procedure per la fornitura dei servizi attuate dal punto di accesso sono dettagliatamente documentate sul manuale operativo, previsto dall'art. 33*

<sup>18</sup> [2] Art. 7 e Art. 29, comma 2.

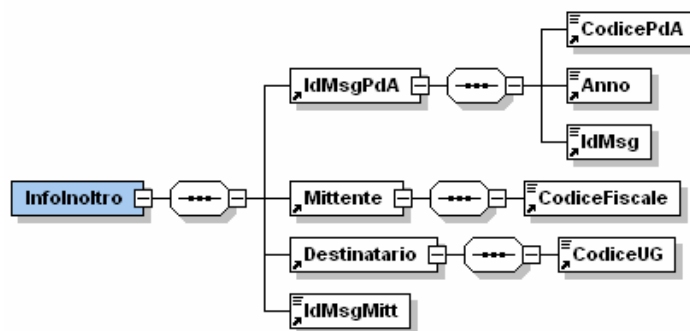


Figura 5 – Struttura del file InfoInoltro.xml

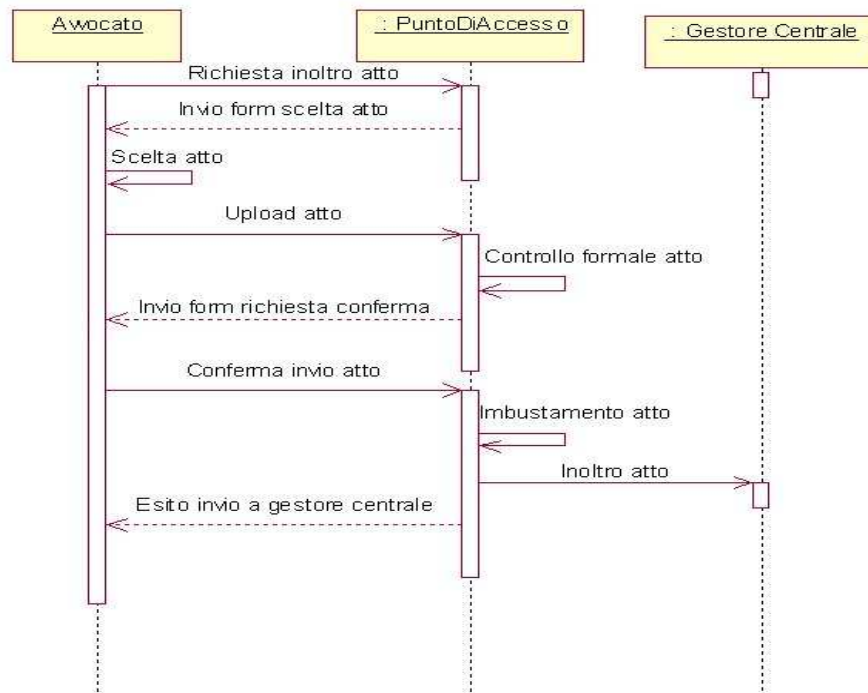
I controlli eseguiti dal PdA in fase di inoltro dell'atto sono di seguito elencati:

1. Apre la busta (MIME) e verifica la correttezza della sua struttura.
2. Verifica la validità formale di *InfoInoltro.xml*.
3. Verifica la validità dei contenuti dei tag Mittente e Destinatario. In particolare il Codice Fiscale del Mittente deve corrispondere a quello dell'utente connesso, mentre il codice dell'UG Destinatario deve essere validato con accesso all'elenco degli Uffici Giudiziari.
4. Verifica che il tag Mittente contenga anche l'attributo Ruolo, indispensabile per il controllo della certificazione del difensore da parte del PdA<sup>19</sup>.
5. Se tutti i controlli sono superati, crea un identificativo univoco (a livello PdA) dell'atto informatico da inoltrare (*IdMsgPdA*) e memorizza il file da inoltrare sul database.
6. Invia al client una form in cui sono visualizzati i dati ricevuti nel file *InfoInoltro.xml* e chiede conferma della richiesta.
7. Dietro conferma dell'utente il PdA aggiorna il file *InfoInoltro.xml* con l'identificativo univoco (a livello PdA) dell'atto informatico da inoltrare (*IdMsgPdA*).
8. Il PdA, certificato il difensore, crea il file *Certificazione.xml*, lo firma con il proprio certificato (server) di firma digitale (*Certificazione.xml.p7m*) e lo include nella busta per l'inoltro.
9. Compone la busta MIME da inviare al GC.
10. Firma il MIME con il certificato server di firma digitale (S/MIME).
11. Aggiorna la base dati locale con i dati di input ricevuti e il messaggio di output prodotto.
12. Invia il messaggio creato al GC all'indirizzo [gestorecentrale@processotelematico.giustizia.it](mailto:gestorecentrale@processotelematico.giustizia.it).
13. Segnala all'Utente l'avvenuta trasmissione del messaggio e termina la funzione.

<sup>19</sup>

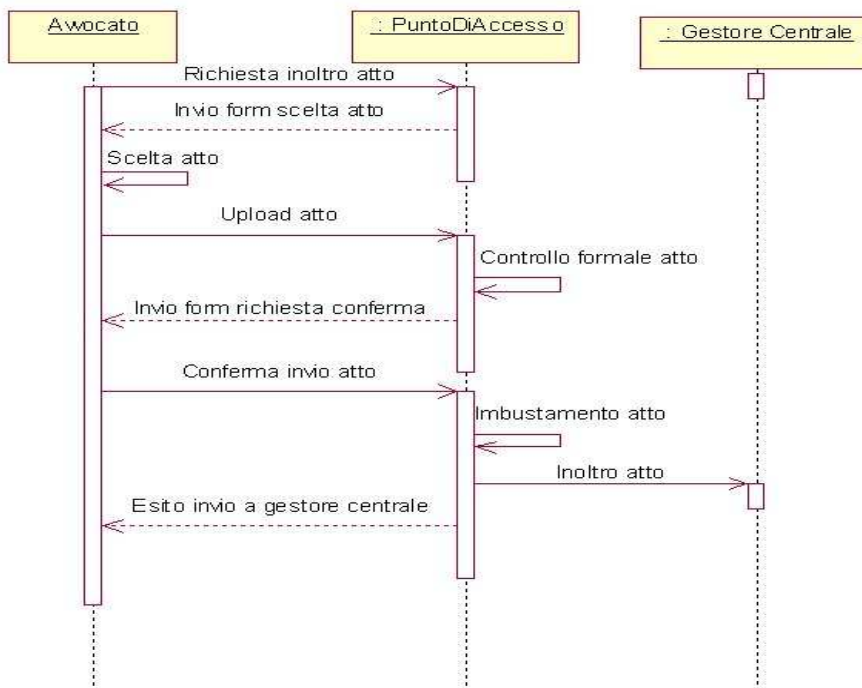
La certificazione del difensore è svolta dal PdA essendo quest'ultimo gestito direttamente dal CdO.

Il flusso sopra descritto è sintetizzato nella figura seguente.



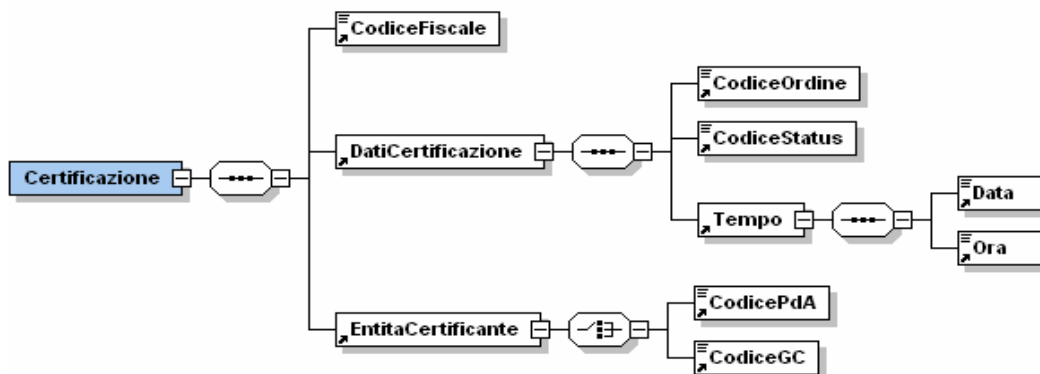
**Figura 6 – Richiesta di deposito atto**

La struttura della busta inoltrata al GC è schematizzata nella figura che segue:



**Figura 7 - S/MIME di Inoltro atto**

La struttura del file *Certificazione.xml* è schematizzata nella figura che segue:



**Figura 8 - Struttura del file Certificazione.xml**

Il contenuto dei tag del file *Certificazione.xml* è il seguente:

1. *CodiceFiscale* è il codice fiscale dell'avvocato certificato (corrispondente all'avvocato connesso con il PdA e al tag *Infolnoltro/Mittente/CodiceFiscale*);
2. *CodiceOrdine* è il codice del CdO dal cui Albo elettronico vengono estratte le informazioni per la certificazione;
3. *CodiceStatus* indica lo status del difensore all'atto della certificazione (attivo, sospeso, radiato);
4. *Tempo* indica la data e ora in cui è stata eseguita la certificazione del difensore;
5. *EntitaCertificante* contiene il codice del PdA.

### **7.2.1 Ricezione dei messaggi di risposta all'inoltro di un atto**

A seguito dell'inoltro di un atto dal PdA verso un Ufficio giudiziario, vengono emessi i seguenti messaggi di risposta:

- attestazione temporale (o notifica di eccezione), inviata dal gestore centrale
- comunicazioni relative all'esito del deposito atto, inviate dall'Ufficio Giudiziario al gestore centrale: un primo esito automatico ed un secondo esito a seguito dell'intervento di accettazione (o rifiuto) da parte del cancelliere.

Nel caso di esito negativo rilevato dal gestore centrale, questi invia una notifica di eccezione invece dell'attestazione temporale. La notifica di eccezione è trattata nel paragrafo successivo.

Il PdA riceve i messaggi di risposta all'inoltro di un atto in una casella di posta elettronica di sistema, all'indirizzo [postmaster@busto.ul.consiglioordineavvocati.it](mailto:postmaster@busto.ul.consiglioordineavvocati.it).

In entrambi i casi, le operazioni eseguite dal PdA sono:

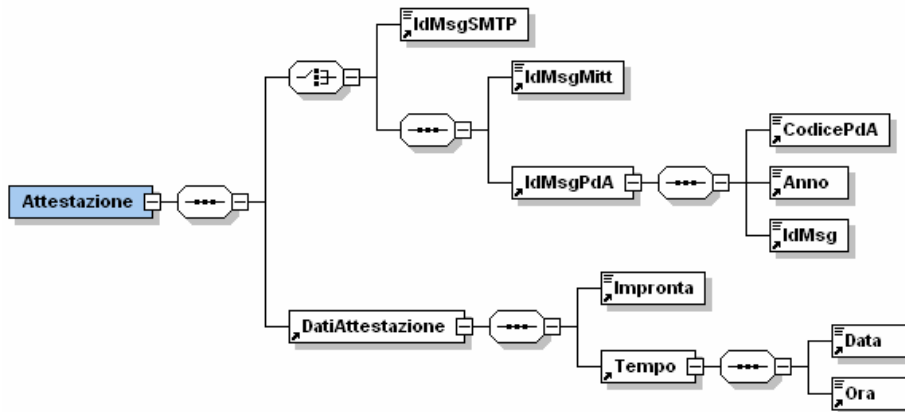
1. Memorizzazione del messaggio ricevuto e del file allegato.
2. Ricerca dell'identificativo (*IdMsgPdA*) del messaggio di *Inoltro atto* cui il messaggio di risposta è riferito.
3. Identificazione del messaggio ricevuto e verifica dell'integrità del file allegato (*Attestazione.xml.p7m* o *EsitoAtto.xml.p7m*)
4. Verifica della corrispondenza del campo *Impronta* con quanto trasmesso (hash della busta S/MIME di *Inoltro atto* nel caso del messaggio di *Attestazione temporale*, hash del file *Atto.enc* nel caso di *Comunicazione esito*).
5. Aggiornamento della base dati locale con i dati del messaggio ricevuto.

La struttura del MIME di *Attestazione temporale* è schematizzata nella figura che segue:



**Figura 1 - MIME di Attestazione temporale**

dove la struttura del file *Attestazione.xml* è la seguente:



**Figura 2 - Struttura del file Attestazione.xml**

Il contenuto dei tag del file *Attestazione.xml* è il seguente:

1. *IdMsgMitt* e *IdMsgPdA* contengono rispettivamente gli identificativi dell'Atto informatico generato dall'avvocato e l'identificativo del messaggio di *Inoltro atto* generato dal PdA. Il contenuto di tali tag deve corrispondere con quello del file *InfoInoltro.xml* precedentemente trasmesso al GC;
2. *Impronta* deve corrispondere all'hash della struttura S/MIME del messaggio di *Inoltro atto* precedentemente trasmesso al GC;
3. *Tempo* indica la data e ora in cui il GC ha eseguito l'attestazione temporale del messaggio di *Inoltro atto*.

La struttura del MIME di *Comunicazione esito* è schematizzata nella figura che segue:

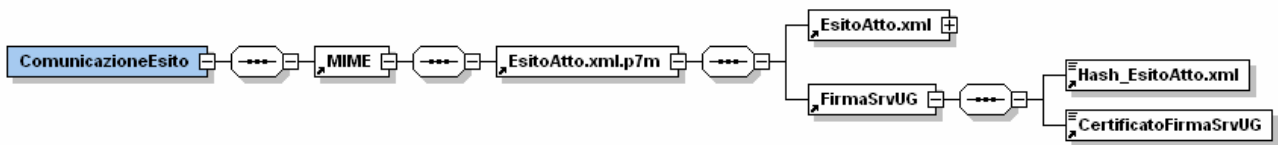


Figura 3 - MIME di Comunicazione esito

dove la struttura del file *EsitoAtto.xml* è la seguente:

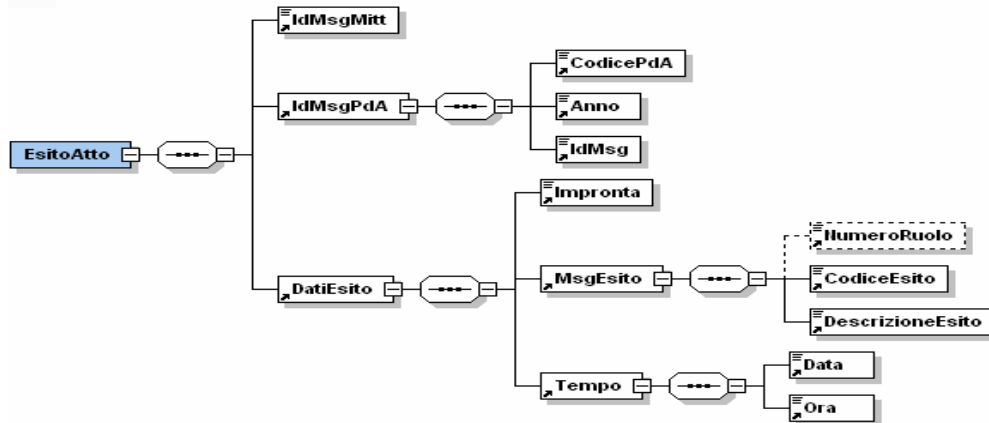


Figura 4 - Struttura del file *EsitoAtto.xml*

Il contenuto dei tag del file *EsitoAtto.xml* è il seguente:

1. *IdMsgMitt* e *IdMsgPdA* contengono rispettivamente gli identificativi dell'Atto informatico generato dall'avvocato e l'identificativo del messaggio di *Inoltro atto* generato dal PdA. Il contenuto di tali tag deve corrispondere con quello del file *InfoInoltro.xml* precedentemente trasmesso al GC;
2. *Impronta*, deve corrispondere all'hash del file *Atto.enc* del messaggio di *Inoltro atto* precedentemente trasmesso al GC;
3. *NumeroRuolo*, se presente, indica il numero di iscrizione a ruolo conseguente al deposito dell'atto;
4. *CodiceEsito* e *DescrizioneEsito* forniscono le indicazioni relative all'esito dell'atto;
5. *Tempo* indica la data e ora in cui è stato prodotto l'esito dell'atto.

### 7.2.2 Gestione delle notifiche di eccezione

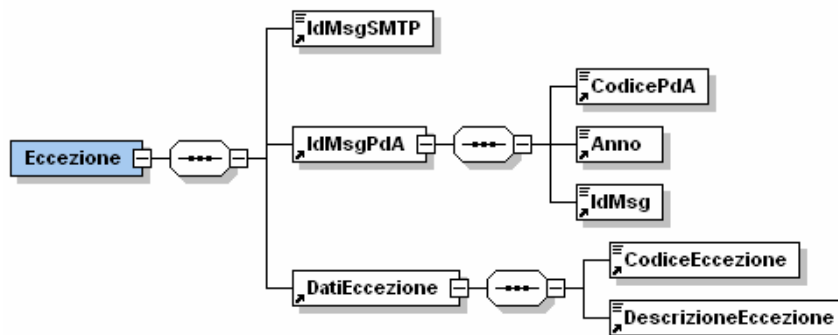
I messaggi di notifica eccezione sono inviati dal gestore centrale per segnalare un errore nella fase di invio del messaggio di *Inoltro atto*.

La struttura del messaggio è schematizzata nella figura che segue:



Figura 5 - MIME di Notifica eccezione

Il messaggio di *Notifica eccezione* trasporta in allegato il file *Eccezione.xml* la cui struttura è visualizzata nella figura che segue



**Figura 6 - Struttura del file *Eccezione.xml***

Il PdA riceve dal gestore centrale la notifica di eccezione nel caso in cui la busta inoltrata dal PdA possa contenere un errore o una anomalia che impedisce l'inoltro dell'atto al GL. La notifica viene inviata all'indirizzo [postmaster\\_cert@pec.busto.ul.consiglioordineavvocati.it](mailto:postmaster_cert@pec.busto.ul.consiglioordineavvocati.it).

Le operazioni eseguite dal PdA sono:

1. Verifica della correttezza formale della notifica.
2. Memorizzazione del messaggio ricevuto.
3. Ricerca dell'identificativo (*IdMsgPdA*) del messaggio di *Inoltro atto* cui il messaggio di risposta è riferito.
4. Identificazione del messaggio ricevuto e memorizzazione del codice e della descrizione dell'eccezione.
5. Memorizzazione dei dati della notifica di eccezione in una tabella dedicata e nella tabella riepilogativa dello stato degli atti inoltrati.

La visualizzazione da parte dell'utente avviene all'atto della richiesta di consultazione dello stato del deposito di un atto (cfr. paragrafo 7.3).

### 7.3 VISUALIZZAZIONE DELLO STATO DEGLI ATTI DEPOSITATI

Il PdA prevede una funzionalità che consente agli utenti abilitati di visualizzare lo stato degli atti depositati, per verificare che gli atti stessi siano stati correttamente inoltrati, ed abbiano quindi ricevuto l'attestazione temporale dal gestore centrale e i relativi esiti da parte dell'Ufficio Giudiziario destinatario (un primo esito automatico ed un secondo esito a seguito dell'intervento di accettazione (o rifiuto) da parte del cancelliere).

All'atto della richiesta di accesso alla funzionalità, viene presentata all'utente una form nella quale sono previsti alcuni campi per effettuare la ricerca dell'atto di cui si vuole verificare l'esito:

- ricerca ultimi *n* messaggi inoltrati (default 10)
- ricerca messaggi inoltrati negli ultimi *n* giorni
- ricerca per intervallo di date (formato data *gg/mm/aaaa*)

Nella ricerca per intervallo di date si utilizzano i seguenti criteri:

- qualora la data di *inizio* periodo non sia valorizzata, questa non viene considerata nell'interrogazione (sono selezionati tutti gli inoltri, senza considerare la data di inizio periodo)
- qualora la data di *fine* periodo non sia valorizzata, viene presa per default la data di esecuzione dell'interrogazione

Il risultato della ricerca viene visualizzato in pagine contenenti ciascuna al massimo 10 atti (questo numero può essere configurato), con la possibilità di scorrere le pagine di risultati qualora non entrassero in una sola pagina.

Il risultato della ricerca viene presentato all'utente in una tabella con i seguenti contenuti:

<b>ID Busta</b>	Contiene l'identificativo del documento fornito dall'avvocato ( <i>IdMsgMitt</i> ), al quale è associato un link, che punta ad informazioni di dettaglio sull'atto, ed in particolare all'attestazione temporale, al testo dell'esito ed all'eventuale numero di iscrizione a ruolo ( <i>EsitoAtto/DatiEsito/MsgEsito/DescrizioneEsito</i> ) oppure, in caso di ricezione di notifica eccezione, al relativo messaggio ( <i>Eccezione/DatiEccezione/DescrizioneEccezione</i> ). Si veda sotto la descrizione della videata contenente i dati di dettaglio.
<b>Data invio</b>	Contiene la data e l'ora di inoltro dell'atto al GC da parte del PdA
<b>Data ricezione</b>	Contiene la data e l'ora dell'attestazione temporale emessa dal GC ( <i>Attestazione/DatiAttestazione/Tempo/Data-Ora</i> ), oppure l'orario di ricezione della notifica di eccezione da parte del PdA.
<b>Data esito automatico</b>	Contiene la data e l'ora dell'esito automatico dei controlli di accettazione deposito atto da parte dell'UG ( <i>EsitoAtto/DatiEsito/Tempo/Data-Ora</i> )
<b>Data esito</b>	Contiene la data e l'ora dell'esito del deposito atto in cancelleria da parte dell'UG ( <i>EsitoAtto/DatiEsito/Tempo/Data-Ora</i> )
<b>Esito</b>	Contiene un'icona (di colore rosso in caso di ricezione di una notifica di eccezione o di esito negativo da parte dell'Ufficio Giudiziario, di colore verde in caso di esito positivo dall'UG). Tale campo non è valorizzato fino alla ricezione dell'esito dall'UG o di una notifica di eccezione.
<b>Visto</b>	Evidenzia un simbolo di spunta quando il dettaglio dell'atto è stato visualizzato dall'utente almeno una volta.

Per rendere visivamente immediato l'evento anomalo, viene inserita nella tabella un'icona, di colore verde nel caso di ricezione dell'esito positivo da parte dell'Ufficio Giudiziario, e di colore rosso nel caso di notifica di eccezione da parte del GC o di esito negativo da parte dell'UG. Un link sul campo ID Busta consente all'utente di richiedere informazioni aggiuntive sull'atto depositato e di visualizzare il messaggio di esito dell'UG o la descrizione del messaggio di errore per la notifica di eccezione.

Il risultato della richiesta di visualizzazione del dettaglio dell'atto, inviata cliccando sul link sopra descritto, viene presentato all'utente in una tabella con i seguenti contenuti:

<b>ID Busta</b>	Contiene l'identificativo integrale del documento fornito dall'avvocato ( <i>IdMsgMitt</i> )
<b>ID PDA</b>	Contiene l'identificativo assegnato al messaggio da parte del PdA al momento della spedizione. E' composto da 3 campi separati dal carattere '/': <ul style="list-style-type: none"> <li>• identificativo del PdA</li> <li>• anno</li> <li>• numero progressivo nell'anno</li> </ul>
<b>Data e ora inoltrato</b>	Contiene la data e l'ora di invio dell'atto verso il GC da parte del PdA
<b>Destinatario</b>	Contiene il nome dell'Ufficio Giudiziario cui è stato inviato l'atto
<b>Attestazione temporale</b>	
In questa sezione compaiono i dati dell'attestazione temporale o della notifica di eccezione, solo se pervenute.	
<b>Data e ora Attestazione temporale</b>	Presente solo se l'attestazione temporale (o la notifica di eccezione) è pervenuta. Contiene la data e l'ora dell'attestazione temporale emessa dal GC ( <i>Attestazione/DatiAttestazione/Tempo/Data-Ora</i> ), oppure l'orario di ricezione da parte del PdA della notifica di eccezione.
<b>Codice Eccezione</b>	Se presente, indica il codice della notifica di eccezione restituito dal GC ( <i>Eccezione/DatiEccezione/CodiceEccezione</i> ) o "DSN" in caso di Delivery Status Notification ricevuta dal server di posta.
<b>Esito</b>	
In questa sezione (valorizzata solo se l'esito dall'Ufficio Giudiziario è pervenuto) compaiono i dati contenuti nell'esito del messaggio.	
<b>Ricevuto da</b>	Contiene la descrizione dell'Ufficio Giudiziario che ha inviato l'esito
<b>Data e ora esito</b>	Contiene la data e l'ora dell'esito atto da parte dell'UG ( <i>EsitoAtto/DatiEsito/Tempo/Data-Ora</i> )
<b>Numero di iscrizione a ruolo</b>	Se presente, contiene il numero di iscrizione a ruolo generato a seguito dell'inoltro dell'atto ( <i>EsitoAtto/DatiEsito/MsgEsito/NumeroRuolo</i> )
<b>Descrizione Esito</b>	Contiene il testo in chiaro dell'esito atto ( <i>EsitoAtto/DatiEsito/MsgEsito/DescrizioneEsito</i> ) oppure, in caso di ricezione di notifica eccezione, al relativo messaggio ( <i>Eccezione/DatiEccezione/DescrizioneEccezione</i> )
<b>Codice Esito</b>	Codice numerico dell'esito pervenuto dall'Ufficio Giudiziario, e relativa descrizione <ul style="list-style-type: none"> <li>• 1 – Esito positivo generato in automatico dal sistema</li> <li>• 2 – Esito positivo generato manualmente dal Cancelliere</li> <li>• -1 – Esito negativo</li> </ul>

Lo stato del messaggio, in differenti momenti di visualizzazione, varia in funzione della ricezione dei messaggi di *Attestazione temporale* e successivamente di *Comunicazione esito*.

In questa tabella sono visualizzati anche i dati relativi alle anomalie operative<sup>20</sup> e alla eventuale ricezione di una notifica di eccezione, proveniente dal gestore centrale al posto di un messaggio di attestazione temporale, nel caso in cui si sia verificato un errore nell'esecuzione del deposito di un atto.

I dati relativi alle attestazioni temporali ed alle comunicazioni di esito rimangono memorizzati nella base dati locale per un periodo di cinque anni.

Per il momento non è prevista alcuna funzione di cancellazione, storicizzazione ed archiviazione di questi dati, che rimangono dunque accessibili per le interrogazioni da parte degli avvocati per tutto il periodo sopra ricordato.

#### 7.4 RICEZIONE DEI BIGLIETTI DI CANCELLERIA DESTINATI ALLE CPECPT DEGLI AVVOCATI

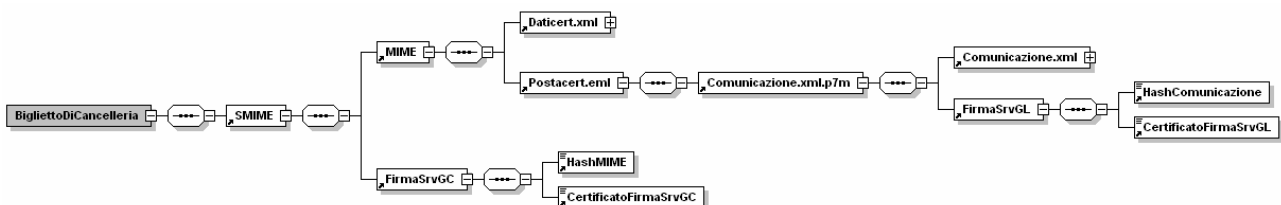
I messaggi relativi a *Biglietti di cancelleria* vengono prodotti dalla cancelleria di un Ufficio Giudiziario e sono indirizzati dal SICI alle CPECPT degli avvocati.

Al riguardo presso il PdA è implementato un dominio di Posta Certificata del Processo Telematico con una CPECPT per ogni avvocato utente del PdA, il cui indirizzo per il Punto di Accesso è  [<codicefiscale>@pec.busto.ul.consiglioordineavvocati.it](mailto:<codicefiscale>@pec.busto.ul.consiglioordineavvocati.it).

Secondo i meccanismi e le denominazioni previsti dallo standard di Posta Certificata del Processo Telematico, il messaggio in entrata subisce le seguenti elaborazioni:

- Il server di Posta Certificata del Processo Telematico presso il PdA riceve il messaggio in entrata e produce una *ricevuta di presa in carico* destinata al server di Posta Certificata mittente.
- Il messaggio di Posta Certificata viene depositato nella CPECPT dell'avvocato e viene prodotta una *ricevuta di avvenuta consegna* indirizzata alla CPECPT del GL mittente presso il GC (indirizzo  [<codiceGL>@processotelematico.giustiziacert.it](mailto:<codiceGL>@processotelematico.giustiziacert.it)).

La struttura del *messaggio di trasporto* generato dal sistema di Posta Certificata è schematizzata nella seguente figura:



**Figura 7 - Struttura del Biglietto di cancelleria**

I Biglietti di cancelleria non sono cifrati.

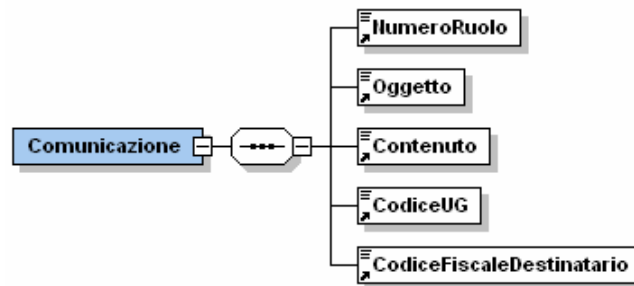
A seguito della ricezione del messaggio, il sistema di Posta certificata del Punto di Accesso provvede a depositare il messaggio in un repository temporaneo, da dove viene

<sup>20</sup> Ad esempio la verifica dell'hash di un messaggio (S/MIME) trasmesso al GC non corrisponde con l'hash contenuto nel messaggio di Attestazione temporale.

prelevato da un'apposita funzione. Questa funzione interpreta la struttura del biglietto di cancelleria ed effettua le seguenti operazioni:

- verifica della firma del gestore centrale;
- verifica dell'integrità della busta S/MIME composta dal gestore centrale;
- apertura dell'allegato *Comunicazione.xml.p7m*;
- verifica della firma del gestore locale;
- verifica dell'integrità della busta MIME composta dal gestore locale;
- controllo della struttura del file *Comunicazione.xml*;
- verifica della correttezza del destinatario;
- memorizzazione nella base dati locale dei dati del biglietto di cancelleria.

La struttura del file *Comunicazione.xml* è schematizzata nella figura seguente:



*Figura 8 - Struttura del file Comunicazione.xml*

#### **7.4.1 Visualizzazione dei Biglietti di cancelleria ricevuti da un avvocato**

La visualizzazione dei Biglietti di cancelleria avviene attraverso una funzionalità applicativa, che maschera all'utente la struttura della propria CPECPT e rende visualizzabili i dati in modo "user friendly".

La funzione è realizzata in modo da controllare che l'avvocato possa accedere in visualizzazione solamente ai dati della propria CPECPT.

All'atto della richiesta di accesso alla funzionalità, viene presentata all'utente una form nella quale sono previsti alcuni campi per effettuare la ricerca dei biglietti di cancelleria:

- ricerca biglietti di cancelleria non ancora visualizzati
- ricerca ultimi *n* biglietti di cancelleria ricevuti (default 10)
- ricerca biglietti ricevuti negli ultimi *n* giorni
- ricerca per intervallo di date

Il risultato della ricerca viene presentato all'utente in una tabella con i seguenti contenuti:

<b>Mittente</b>	Contiene l'Ufficio Giudiziario che ha inviato il biglietto di cancelleria
-----------------	---

<b>Oggetto</b>	Contiene il valore del campo oggetto del biglietto di cancelleria ( <i>Comunicazione/Oggetto</i> ), cui è associato un link, che punta al testo del contenuto del biglietto ( <i>Comunicazione/Contenuto</i> )
<b>Data ricezione</b>	Contiene la data e l'ora della ricezione del messaggio, rilevata dal sistema di posta certificata
<b>Num. Iscr. Ruolo</b>	Contiene il numero di ruolo cui si riferisce il biglietto di cancelleria ( <i>Comunicazione/NumeroRuolo</i> )
<b>Visto</b>	Evidenzia un simbolo di spunta quando il dettaglio del biglietto è stato visualizzato dall'utente.

Cliccando sul link contenuto nel campo Oggetto, l'utente può richiedere le informazioni di dettaglio del biglietto, che vengono visualizzate in una pagina con il seguente contenuto:

<b>Mittente</b>	Contiene l'Ufficio Giudiziario che ha inviato il biglietto di cancelleria
<b>Numero di iscrizione al ruolo</b>	Contiene il numero di ruolo cui si riferisce il biglietto di cancelleria ( <i>Comunicazione/NumeroRuolo</i> )
<b>Data e ora ricezione</b>	Contiene la data e l'ora della ricezione del messaggio, rilevata dal sistema di posta certificata
<b>Oggetto</b>	Contiene il valore del campo oggetto del biglietto di cancelleria ( <i>Comunicazione/Oggetto</i> )
<b>Contenuto</b>	Contiene il testo in chiaro del biglietto di cancelleria ( <i>Comunicazione/Contenuto</i> )

## 7.5 ACCESSO AI SERVIZI DI CONSULTAZIONE POLISWEB

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.

Il punto di accesso ospita il front-end del sistema PolisWeb nell'architettura descritta nell'allegato A delle Regole Tecniche e si collega a tutti i gestori locali attivati dal Ministero della Giustizia ed ai relativi sistemi di back-end al fine di consultare i registri di cancelleria abilitati (SICID per la cognizione ordinaria e SIECIC per le esecuzioni civili), man mano che il Ministero li rende disponibili.

Il punto di accesso si collega inoltre al "sito nazionale" PolisWeb per consultare i registri degli uffici caricati (il relativo elenco è disponibile su [www.processotelematico.giustizia.it](http://www.processotelematico.giustizia.it), sezione "Uffici Giudiziari").

Gli aspetti architettonici di PolisWeb sono descritti in appendice (paragrafo 9.2).

## 7.6 CONTROLLO ANTIVIRUS

Il controllo antivirus è realizzato avvalendosi del software ClamAV.

Tale software si incarica di effettuare il controllo per ogni messaggio in arrivo e in partenza.<sup>21</sup>

## 7.7 CONSERVAZIONE DEI MESSAGGI INVIATI E RICEVUTI

### 7.7.1 *Gestione messaggi scaduti nelle CPECPT*

Le Regole Tecniche prevedono all'articolo 12 che, dopo trenta giorni dalla ricezione, i messaggi di posta certificata contenuti nelle caselle utente siano archiviati e sostituiti da un avviso contenente i dati dei messaggi.

Le Regole non prevedono la possibilità di cancellazione dei messaggi, né da parte dell'utente, né da parte del sistema.

Il Punto di Accesso realizza una procedura, da attivare periodicamente in maniera automatica nei momenti di fermo delle attività del sistema (ore notturne e/o giorni festivi), che esamina le caselle di posta certificata degli utenti e le relative registrazioni nella base dati applicativa per ricercare i messaggi che siano stati ricevuti da oltre 30 giorni e sostituirli con un apposito avviso.

Si noti che dal punto di vista del dimensionamento delle caselle di posta, per le comunicazioni (es. Biglietti di cancelleria) c'è poca differenza tra il messaggio originale e l'avviso che lo sostituisce. Una riduzione significativa dello spazio occupato si ottiene invece nel caso delle *copie degli atti* o delle *notifiche tra difensori*, che possono essere di dimensioni notevoli.

Per quanto riguarda l'archiviazione dei messaggi, gli originali devono essere archiviati per un periodo di cinque anni, e devono quindi essere messi a disposizione degli strumenti che provvedono alla registrazione su appositi supporti. Sono esclusi dal processo di archiviazione i messaggi di risposta alla richiesta di copia degli atti. Le copie degli atti non sono quindi più disponibili all'utente sul Punto di Accesso dal momento della sostituzione del messaggio con l'avviso sopra menzionato.

La periodicità con cui la procedura viene attivata è settimanale.

### 7.7.2 *Storicizzazione dei dati e archiviazione*

Le Regole Tecniche stabiliscono, all'articolo 29, che il Punto di Accesso mantiene in linea i documenti informatici inviati fino a quando non riceve un avviso di consegna dal gestore centrale dell'accesso o dal punto di accesso di destinazione e che il Punto di Accesso garantisce, per un periodo non inferiore a cinque anni, la conservazione di tutti i messaggi inviati e ricevuti

Il Punto di Accesso provvede quindi alla realizzazione di procedure che mettono fuori linea tutti i dati relativi ai messaggi di cui sia stato ricevuto un avviso di consegna, inserendoli in archivi storici non accessibili dagli utenti.

Tali archivi storici sono poi periodicamente scaricati su idonei supporti, archiviati e conservati, per un periodo non inferiore a cinque anni.

I criteri utilizzati per mettere fuori linea i messaggi sono i seguenti:

---

<sup>21</sup> [2] Art. 29, comma 6.

- sono cancellati tutti i messaggi dalla tabella contenente i messaggi in uscita (cioè i messaggi caricati sul server per essere inoltrati, ma il cui invio non è stato effettuato)
- nella tabella contenente i messaggi inviati sono messi fuori linea tutti gli atti inviati ad uffici giudiziari che hanno ricevuto l'attestazione temporale e l'esito (tali eventi sono registrati a loro volta in una apposita tabella per la memorizzazione dello stato degli atti inviati)
- nella tabella contenente i messaggi inviati sono messi fuori linea tutti i messaggi inviati ad avvocati che hanno ricevuto la ricevuta di avvenuta consegna dal Punto di Accesso destinatario (evento registrato nella tabella per la memorizzazione dello stato degli atti inviati)
- Per quanto riguarda i messaggi ricevuti nelle caselle di posta certificata, le procedure di storicizzazione ed archiviazione sono descritte nel paragrafo 7.7.1.

### **7.7.3 Registrazione su Giornale di controllo**

Il punto di accesso attiva il giornale di controllo, contenente l'insieme delle registrazioni effettuate automaticamente allorché si verificano i seguenti eventi:

1. difformità tra la copia operativa e l'originale del Registro Locale degli Indirizzi Elettronici (art. 18, comma 2)
2. effettuazione di operazioni che modificano il contenuto del Registro Locale degli Indirizzi Elettronici (art. 18, comma 3)
3. ogni intervallo di tempo nel quale i registri non risultano accessibili dall'esterno, oppure sono indisponibili in una loro funzionalità (art. 18, comma 4)
4. eventi significativi nel funzionamento del punto di accesso (art. 30, comma 8),
5. nomina del responsabile della sicurezza (art. 34, comma 1)

In particolare il punto di accesso traccia il verificarsi dei seguenti eventi:

#### Responsabile della sicurezza

- Nomina di un responsabile

#### Registro Locale degli Indirizzi Elettronici

- difformità tra la copia operativa e l'originale del Registro Locale degli Indirizzi Elettronici
- attività che modificano il contenuto del Registro Locale degli Indirizzi Elettronici

#### Utenti e Accessi al PdA

- Creazione e aggiornamento di un soggetto
- Tentativi di accesso da parte di soggetti non abilitati

#### Anomalie operative

- Firme non conformi
- Autenticità dei messaggi
- Notifiche di Eccezioni

#### - Messaggi non previsti

Le registrazioni sono effettuate in modo indipendente dalle diverse componenti del Punto di Accesso, anche su distinti supporti e di diverso tipo.

Ogni registrazione associa la data, l'ora e i minuti in cui è effettuata.

Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e da consentire la ricostruzione accurata di tutti gli eventi rilevanti per la sicurezza.

L'integrità del giornale di controllo è verificata con frequenza almeno mensile.

Le registrazioni contenute nel giornale di controllo sono archiviate e conservate per un periodo non inferiore a cinque anni.

### 7.8 SERVIZIO DI DISTRIBUZIONE DEL SOFTWARE DEL MINISTERO

Presso un'apposita area è disponibile il link per il download del redattore atti per l'avvocato e del relativo manuale utente.

Selezionando il link viene attivato il download direttamente dal sito ufficiale del processo telematico messo a disposizione dal Ministero della Giustizia ([www.processotelematico.giustizia.it](http://www.processotelematico.giustizia.it)).

### 7.9 TENUTA DEL GIORNALE DI CONTROLLO

Il giornale di controllo è costituito al momento da un file in formato XML ove vengono effettuate le registrazioni relativamente a:

- Operazioni sui database (albo, utenti iscritti e registro ldap);
- Eventuali difformità tra la copia operativa e l'originale del registro ldap<sup>22</sup>;
- data, ora e minuti (iniziali e finali), di ogni intervallo di tempo nel quale il registro degli indirizzi non risulta accessibile dall'esterno<sup>23</sup>;

Il giornale riporta il nominativo del responsabile per la sicurezza.<sup>24</sup>

Fanno parte del giornale di controllo (come allegati esterni) i file di log relativi a tutte le operazioni effettuate dal sistema.

Il file XML viene firmato digitalmente dal responsabile dello staff tecnico ad ogni modifica; in tale circostanza vengono firmati anche i file di log come disponibili al momento della firma stessa.

L'integrità del giornale di controllo è verificata con frequenza almeno mensile dallo staff tecnico.<sup>25</sup>

### 7.10 CONNETTIVITÀ

Il servizio di connettività ad internet è assicurato dalla società Net Service s.r.l. attraverso una connessione a 4 Mb/sec fornita dall'ISP Fastweb.

---

<sup>22</sup> [2] Art. 18, comma 2.

<sup>23</sup> [2] Art. 18, comma 4.

<sup>24</sup> [2] Art. 34, comma 1.

<sup>25</sup> [2] Art. 35, comma 5.

## 7.11 ASSISTENZA AGLI UTENTI<sup>26</sup>

L'assistenza agli utenti viene fornita tramite l'apposito servizio al quale ha aderito il Consiglio dell'Ordine di Busto Arsizio, con sportello fisicamente dislocato presso il Tribunale distrettuale di Milano (lun-ven 10.00-13.00), raggiungibile al numero di telefono 0236504593 e all'indirizzo di posta elettronica infopct@ordineavvocatimilano.it oppure infopct@unionelombardaordiniforensi.it.

Sarà questo servizio di primo livello (e soltanto questo) ad interfacciarsi con il supporto tecnico fornito dalla società Net Service s.r.l.

## 8 ALTRE INDICAZIONI

Il punto di accesso garantisce un **livello di disponibilità del servizio** pari al 99,5 per cento, su base quadrimestrale, nei seguenti orari:

- dalle ore 8 alle ore 22, nei giorni feriali, dal lunedì al venerdì;
- dalle ore 8 alle ore 13 del sabato e dei giorni 24 e 31 dicembre.

Il punto di accesso è comunque attivo 24 ore su 24, 7 giorni su 7

Net Service s.r.l. garantisce il presidio tecnico durante le ore d'ufficio, ovvero dalle ore 9.00 alle ore 18.00, nei giorni feriali, dal lunedì al venerdì. Eventuali segnalazioni di malfunzionamento pervenute al di fuori di tale orari potranno quindi essere prese in carico unicamente alle ore 9 del successivo giorno feriale (escluso il sabato).

Tutti i **canali di autenticazione** instaurati dal punto di accesso con gli utenti abilitati e con il gestore centrale sono realizzati in SSL versione 3, con chiave a 1024 bit.<sup>27</sup>

È possibile il **download** del presente manuale operativo, in formato PDF, accedendo all'apposita area di download (<http://busto.ul.consiglioordineavvocati.it/download>).<sup>28</sup>

---

<sup>26</sup> [3] § 5.2, punto 4.

<sup>27</sup> [2] Art. 30, comma 9.

<sup>28</sup> [2] Art. 33, comma 2.

## 9 APPENDICE

### 9.1 ARCHITETTURA DEL PDA

Il PdA del Consiglio dell'Ordine degli Avvocati di Busto Arsizio si configura come un'infrastruttura hardware e software che fornisce servizi di autenticazione e di comunicazione tra la postazione utente e il Consiglio dell'Ordine.

La comunicazione tra PdA e soggetto esterno avviene sulla rete Internet.

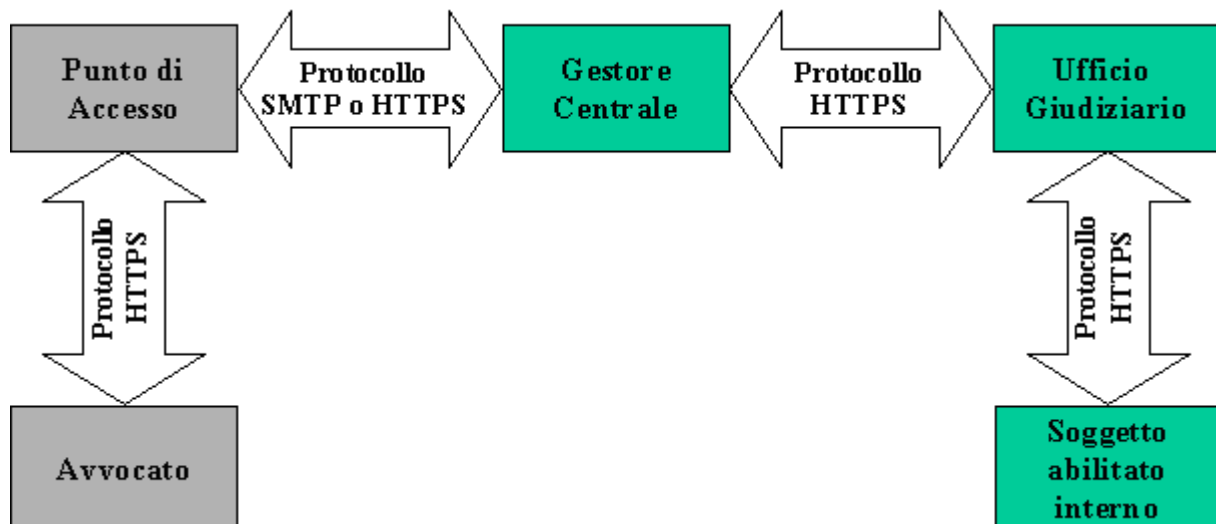
Dal punto di vista applicativo, i flussi del Processo Telematico possono essere classificati per tipologia in invii documentali e consultazioni.

Dal punto di vista trasmissivo, 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 meccanismi sincroni, basati su HTTPS. Per la consultazione del Registro Generale degli Indirizzi Elettronici e del Registro degli Uffici Giudiziari, residenti sul GC, le Regole Tecniche stabiliscono poi l'utilizzo del protocollo LDAP.

Protocollo HTTPS – Protocollo di comunicazione utilizzato in Internet (HyperText Transfer Protocol Secure, ovvero protocollo HTTP con supporto SSL: Secure Socket Layer)

Protocollo SMTP – Protocollo per la comunicazione diretta tra i server di posta elettronica (Simple Mail Transfer Protocol).

Protocollo LDAP - Protocollo lightweight per gestire servizi di directory, basato sui servizi di directory X.500 (Lightweight Directory Access Protocol).



*Figura 9 – Protocolli di trasporto*

### 9.2 ARCHITETTURA DI POLISWEB

Nel presente paragrafo vengono evidenziate le caratteristiche realizzative della specifica implementazione di PolisWeb per il Punto di Accesso, in particolare per quanto riguarda le fasi di autenticazione ed il flusso di consultazione.

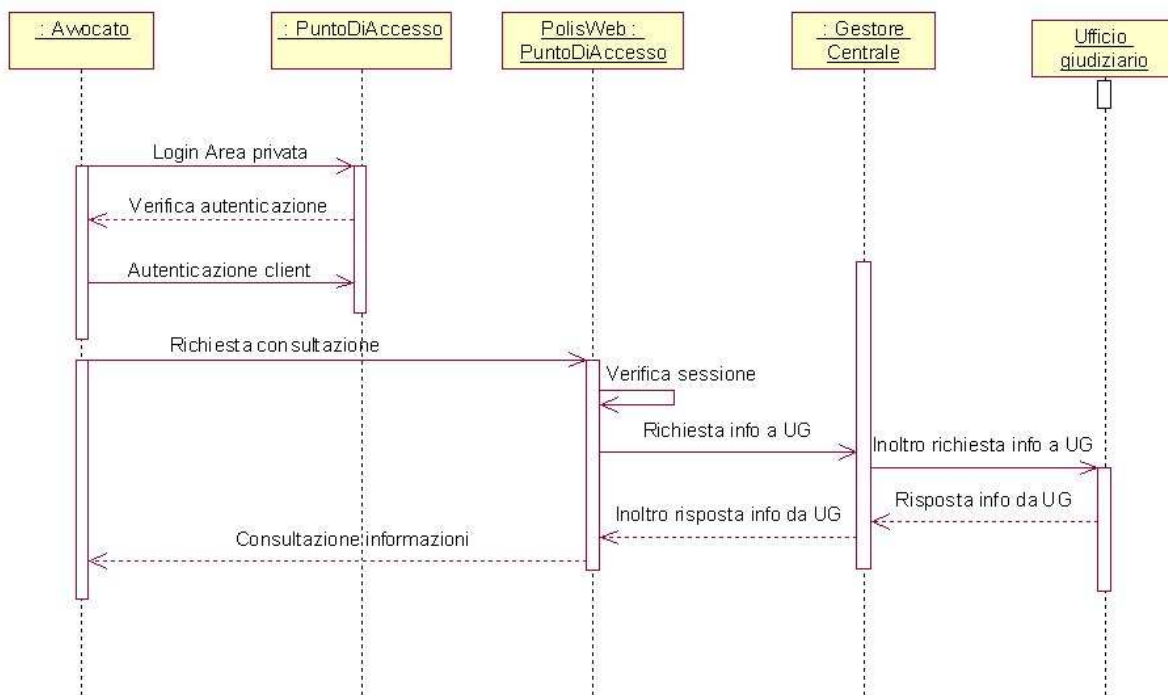
Il Punto di Accesso è realizzato, dal punto di vista architetturale e degli strumenti utilizzati, in modo da essere integrato con il *Front-End* dello strumento di consultazione di dati processuali PolisWeb ospitato sul PdA stesso. Le due componenti applicative, infatti, condividono lo stesso ambiente runtime, all'interno del container per applicazioni Java J2EE Jboss.

In questo modo le due applicazioni condividono l'ambiente e molte risorse. Inoltre tutte le fasi di comunicazione sono notevolmente semplificate, ricavando benefici sia in termini di utilizzo di risorse del sistema sia in termini di performance.

A seguito dell'autenticazione, infatti, per ciascun utente collegato viene creata una sessione SSL per l'instaurazione di un canale di comunicazione sicuro (gestita dal web server Apache con il modulo mod\_ssl), ed una sessione applicativa all'interno del container Jboss e dell'application server Tomcat. Entrambe le sessioni sono condivise dalle funzionalità del Punto di Accesso e da quelle di PolisWeb.

Quando l'utente richiede l'accesso alle funzionalità di consultazione messe a disposizione da PolisWeb all'interno del Punto di Accesso, l'autenticazione è già stata effettuata all'atto dell'ingresso nell'Area privata. Non è quindi necessario effettuare un'altra autenticazione e attivare un'altra sessione applicativa, ma è sufficiente verificare che le sessioni precedentemente instaurate siano ancora attive ed invocare le classi ed i metodi di PolisWeb con gli opportuni parametri.

Nella Figura 10 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.



**Figura 10 - Sequence diagram Consultazione Web**

Nella Figura 10 si evidenziano in particolare le seguenti azioni:

- L'utente sottopone a Polis Web, presente sul PdA, una richiesta di consultazione;
- Il PdA verifica che l'utente sia già stato precedentemente autenticato;
- I dati di autenticazione (smart card) sono inviati dal browser al PdA;
- La componente PolisWeb sul PdA inoltra la richiesta al Gestore Centrale;
- Il GC inoltra la richiesta all'Ufficio Giudiziario;
- Il GC acquisisce la risposta dall'UG;
- Il GC inoltra la risposta dell'UG alla componente PolisWeb sul PdA;
- L'utente consulta le informazioni tramite Polis Web.

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'utente.

Si noti inoltre che non sono effettuati controlli sull'univocità della sessione utente per i soggetti abilitati. Questo in quanto, come sopra ricordato, ciascun soggetto può avere a propria disposizione diversi certificati di autenticazione, ed utilizzarli contemporaneamente su diverse postazioni client.