



# *Ministero della Giustizia*

*Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi*

*Direzione generale per i sistemi informativi automatizzati*

*Sistemi informativi automatizzati per la giustizia civile e processo telematico*

## **PROCESSO CIVILE TELEMATICO**

---

***Piano delle verifiche  
per il rilascio dell'autorizzazione ai Punto di Accesso***

Versione 2.0



**PIANO DELLE VERIFICHE PER L’AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

**Sommario**

<b>1</b>	<b>INTRODUZIONE .....</b>	<b>6</b>
<b>2</b>	<b>ANALISI DELLA DOCUMENTAZIONE PREDISPOSTA DAL PDA .....</b>	<b>7</b>
2.1	MANUALE OPERATIVO E PIANO PER LA SICUREZZA. ....	7
2.2	RELAZIONE TECNICA SULLE MODALITÀ DI AUTENTICAZIONE DEGLI UTENTI. ....	8
<b>3</b>	<b>ISPEZIONE E VERIFICA DELLE FUNZIONALITÀ DEL SISTEMA .....</b>	<b>9</b>
3.1	PROCEDURE DI ABILITAZIONE E GESTIONE UTENZE.....	10
3.1.1	Procedura (completa) di registrazione di un nuovo soggetto.....	10
3.1.2	Procedura di variazione utenze .....	11
3.1.3	Procedura di cancellazione utenze .....	12
3.1.4	Verifica funzionalità per i Rappresentanti dei Consigli dell’Ordine.....	12
3.2	VERIFICA DELLE CREDENZIALI DI UN SOGGETTO ATTRAVERSO ALBO (SE APPLICABILE) .....	13
3.3	CONSULTAZIONI POLISWEB .....	14
3.4	FUNZIONALITÀ DI ACCESSO AI REGISTRI DEL GC.....	15
3.5	DEPOSITO DI ATTI E TRACCIABILITÀ DELLO STATO DEL DEPOSITO. ....	15
3.6	GESTIONE DI ECCEZIONI (ERRORI RICEVUTI DA GC).....	17
3.7	RICEZIONE DI NOTIFICHE NELLE CASELLE DI POSTA CERTIFICATA (BIGLIETTO DI CANCELLERIA).....	18
3.8	NOTIFICHE TRA DIFENSORI .....	18
3.8.1	Invio di notifiche tra difensori .....	18
3.8.2	Ricezione di notifiche tra difensori.....	19
3.9	RICHIESTA DI COPIA CONFORME .....	19
3.10	PROCEDURA (COMPLETA) DI DISABILITAZIONE DI UN SOGGETTO ABILITATO .....	20
3.11	SICUREZZA DEI LOCALI E DELLE PROCEDURE DI AMMINISTRAZIONE DEL SISTEMA .....	20
3.12	CORRETTA PROCEDURA DI CHIUSURA SESSIONE .....	20



PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

## STORIA DELLE MODIFICHE APPORTATE

<i>Versione</i>	<i>Data</i>	<i>Descrizione Modifica</i>
<b>1.0</b>	22/11/2004	Prima emissione
<b>1.1</b>	31/07/2006	<ul style="list-style-type: none"><li>▪ Inserito riferimento n° 3</li><li>▪ Inserita nota n° 2 sulla cifratura atti in uscita</li><li>▪ § 3.3, punto 3: adeguato a CNS</li><li>▪ Inserita precisazione alla nota 3</li><li>▪ Rivisto § 3.4, punto 2</li><li>▪ Inserito punto 7 nel § 3.4</li></ul>
<b>1.2 (bozza)</b>	16/03/2007	<ul style="list-style-type: none"><li>▪ Necessità di installare certificato di ispezione per modalità debug (§ 3)</li><li>▪ Allineamento orologio di sistema (§ 3)</li><li>▪ Rivisto § 3.4, punto 4</li><li>▪ Tracciabilità nel caso di attestazione temporale errata (§ 3.4, punto 6 a )</li><li>▪ Controllo validità data Attestazione Temporale (§ 3.4, punto 8 g )</li><li>▪ Eliminato punto 9 di § 3.4</li><li>▪ Inserito § 3.9</li></ul>
<b>2.0</b>	23/05/2007	<ul style="list-style-type: none"><li>▪ Riferimenti: inserito “Specifiche di Interfaccia tra Punto di Accesso e Gestore Centrale v. 2.0”</li><li>▪ § 3, Specificato che in fase di test il PdA sarà collegato al GC di pre-produzione</li><li>▪ § 3, Aggiornato l’elenco delle funzionalità e flussi oggetto di verifica</li><li>▪ § 3, Introdotto l’iter di messa in esercizio del PdA</li><li>▪ Rivisto § 3.1.1 <i>Procedura (completa) di registrazione di un nuovo soggetto</i>, punti 1.a, 1.b, 4</li><li>▪ Inseriti § 3.1.2, 3.1.3, 3.1.4</li><li>▪ § 3.2 <i>Verifica delle credenziali di un soggetto attraverso albo (se applicabile)</i>: inserita distinzione nel metodo di verifica in base alla tipologia del PdA (di un CdO/CNF o privato)</li><li>▪ Inserito § 3.4 Funzionalità di accesso ai registri del GC</li><li>▪ Rivisto § 3.5 <i>Deposito di atti e tracciabilità dello stato del deposito</i>, punti 1, 4, 6.b</li><li>▪ § 3.6 <i>Gestione di Eccezioni (errori ricevuti da GC)</i>: punto 2, inserito test in collegamento con il GC</li><li>▪ § 3.7 <i>Ricezione di notifiche nelle caselle di Posta Certificata</i>, inserito punto 5</li><li>▪ Inserito § 3.8 <i>Notifiche tra difensori</i></li><li>▪ Inserito § 3.9 <i>Richiesta di copia conforme</i></li></ul>



**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

## DEFINIZIONI E ACRONIMI

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

<b>Acronimo</b>	<b>Descrizione</b>
CdO	Consiglio dell'Ordine
CPC	Codice di Procedura Civile
CPECPT	Casella di Posta Certificata Processo Telematico (anche CPEPT)
DSN	Delivery Status Notification
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
RD	Repository Documentale
ReGIndE	Registro Generale degli Indirizzi Elettronici
ReLIndE	Registro Locale degli Indirizzi Elettronici
RPC	Remote Procedure Call
RUG	Rete Unitaria della Giustizia
RUPA	Rete Unitaria della Pubblica Amministrazione
S/MIME	Secure Multipurpose Internet Mail Extensions
SIC	Sistema Informativo Civile
SICI	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
UI	User Interface
UNEP	Ufficio Notifiche e Protesti
W3C	World Wide Web Consortium
XML	eXtensible Markup Language



**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

## RIFERIMENTI

<i>Progressivo</i>	<i>Descrizione</i>
1	Regole Tecnico-Operative per l'Uso di Strumenti Informatici e Telematici nel Processo Civile e relativi allegati (D.M. 14/10/2004).
2	Posta Elettronica Certificata “Allegato tecnico alle linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata” ( <a href="http://www.ctrupa.it/RETE-RUPA/Posta-Elet">http://www.ctrupa.it/RETE-RUPA/Posta-Elet</a> ).
3	“Linee guida per l'utilizzo e l'emissione delle CNS”, documento CNIPA disponibile on-line nella sezione CNS → Specifiche Tecniche del sito <a href="http://www.cnipa.it/">http://www.cnipa.it/</a>
4	Specifiche della strutturazione dei modelli DTD (Document Type Definition) D.M. 15/12/2005
5	Specifiche di Interfaccia tra Punto di Accesso e Gestore Centrale v. 2.0



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

### 1 INTRODUZIONE

Il soggetto che intende costituire un Punto di Accesso (PdA) inoltra, alla DGSIA, domanda di iscrizione nell'elenco pubblico dei punti di accesso. Il Ministero della Giustizia decide sulla domanda, con provvedimento motivato, anche sulla base di **apposite verifiche**, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente. Successivamente alla concessione di autorizzazione, il Ministero della Giustizia **può verificare l'adempimento degli obblighi assunti da parte del gestore del PdA**, di propria iniziativa oppure su segnalazione.

La verifica eseguita dal Ministero della Giustizia previo rilascio di prima autorizzazione prevede due fasi:

- Analisi della documentazione predisposta dal PdA
- Ispezione e verifica delle funzionalità del sistema

Le due fasi sono descritte nelle sezioni 2 e 3 del presente documento.



**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

## **2 ANALISI DELLA DOCUMENTAZIONE PREDISPOSTA DAL PdA**

Il gestore del PdA deve consegnare alla DGSIA, almeno quindici giorni prima dell'ispezione del sistema, i seguenti documenti:

- **manuale operativo** (art. 33 delle regole tecniche)
- **piano di sicurezza** (art. 34 delle regole tecniche)
- **relazione tecnica** sulle modalità di autenticazione degli utenti (nel seguito descritta).

### **2.1 MANUALE OPERATIVO E PIANO PER LA SICUREZZA.**

Gli articoli 33 e 34 delle regole tecniche (sotto riportati per comodità) obbligano il PdA a predisporre e mantenere Manuale Operativo e Piano della Sicurezza. I suddetti documenti saranno attentamente vagliati prima di concedere autorizzazione, con particolare riferimento alle parti qui in grassetto:

*Art. 33*

*(Manuale operativo)*

1. Il punto di accesso utilizza un manuale operativo in cui sono definite le procedure applicate per effetto del presente decreto.
2. Il manuale operativo è pubblicato a cura del punto di accesso, per la consultazione in via telematica.
3. Il manuale operativo contiene almeno le seguenti informazioni:
  - a) dati identificativi del punto di accesso e del relativo gestore;
  - b) dati identificativi della versione del manuale operativo;
  - c) responsabile del manuale operativo;
  - d) definizione degli obblighi del titolare del punto di accesso e di coloro che vi accedono per l'utilizzo dei servizi;
  - e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
  - f) tariffe;
  - g) **modalità di autenticazione, registrazione e gestione degli utenti;**
  - h) **modalità di attivazione e gestione degli indirizzi elettronici;**
  - i) modalità di gestione del registro degli indirizzi elettronici;
  - j) modalità di accesso al registro degli indirizzi elettronici;
  - k) **politiche e procedure di sicurezza.**

*Art. 34*

*(Piano per la sicurezza)*

1. Il punto di accesso individua ed iscrive nel giornale di controllo il responsabile per la sicurezza.
2. Il responsabile di cui al comma 1 definisce un piano per la sicurezza che contiene almeno i seguenti elementi:
  - a) **struttura generale, modalità operativa e struttura logistica dell'organizzazione;**
  - b) **descrizione dell'infrastruttura di protezione per ciascun immobile rilevante ai fini della sicurezza;**
  - c) collocazione dei servizi e degli uffici negli immobili dell'organizzazione;
  - d) elenco del personale e sua distribuzione negli uffici;
  - e) **ripartizione e definizione delle responsabilità;**



**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

- f) **descrizione delle procedure utilizzate nell'attività di attivazione delle utenze e, limitatamente ai punti di accesso, di rilascio di indirizzi elettronici;**
  - g) **descrizione dei dispositivi installati;**
  - h) **descrizione dei flussi di dati;**
  - i) **procedura di gestione delle copie di sicurezza dei dati;**
  - j) **procedura di gestione dei disastri;**
  - k) **analisi dei rischi;**
  - l) **descrizione delle contromisure;**
  - m) **specificazione dei controlli.**
3. Il piano per la sicurezza è conforme a quanto previsto dal decreto legislativo 30 giugno 2003, n.196.

**2.2 RELAZIONE TECNICA SULLE MODALITÀ DI AUTENTICAZIONE DEGLI UTENTI.**

L'autenticazione degli utenti è una delle operazioni più critiche al fine della sicurezza del sistema. Il manuale operativo (art 33, comma 3, punto g) prevede una descrizione delle modalità di autenticazione, registrazione e gestione degli utenti. Si richiede al gestore del PdA di predisporre (a parte rispetto al manuale operativo) una *relazione tecnica dettagliata* circa l'implementazione dei meccanismi di autenticazione e la loro aderenza rispetto a quanto previsto dalle regole tecniche. La relazione non dovrà far riferimento a generiche tecnologie ma dovrà indicare e descrivere nel dettaglio tutte le componenti del sistema che si occupano della gestione dell'autenticazione, e le loro interazioni.



### 3 ISPEZIONE E VERIFICA DELLE FUNZIONALITÀ DEL SISTEMA

Durante l'ispezione, pre-rilascio dell'autorizzazione, dovrà essere verificato che il PdA sia in grado di svolgere i servizi richiesti, interfacciandosi con un *ufficio giudiziario (UG) di test* attraverso il *gestore centrale (GC) di pre-produzione*.

In particolare saranno verificati i seguenti aspetti:

1. Procedure di abilitazione e gestione utenze
2. Verifica delle credenziali di un soggetto attraverso albo (se applicabile).
3. Consultazioni PolisWeb.
4. Funzionalità di accesso ai registri del Gestore Centrale
5. Deposito di atti e tracciabilità dello stato del deposito.
6. Gestione di Eccezioni (errori ricevuti da GC).
7. Ricezione di notifiche nelle caselle di Posta Certificata.
8. Invio e ricezione di notifiche tra difensori
9. Procedura di richiesta Copia Conforme
10. Procedura (completa) di disabilitazione di un soggetto abilitato.
11. Sicurezza dei locali e delle procedure di Amministrazione del sistema.
12. Procedura di chiusura sessione.

I punti 1..8 sopra elencati sono spiegati in maggiore dettaglio nel resto del documento.

Il gestore del PdA onde supportare l'amministrazione nell'esecuzione delle procedure di verifica deve:

- garantire, durante l'ispezione, la **presenza di figure tecniche** in grado di rispondere adeguatamente alle domande (anche di dettaglio) poste dalle persone incaricate della verifica.
- **prevedere che il sistema si possa configurare** in modalità tale che invece di inoltrare i messaggi SMTP al gestore centrale (ovvero a [gestorecentrale@processotelematico.giustizia.it](mailto:gestorecentrale@processotelematico.giustizia.it)) li invii a un indirizzo di posta elettronica specificato dal collaudatore (modalità *debug*). Inoltre in modalità debug il PdA deve poter ricevere messaggi SMTP da un mittente diverso dal GC (ovvero deve essere possibile inviare dall'esterno messaggi a <codicePdA>@processotelematico.<dominioPdA>, e alle caselle <CPCPT>@processotelematico.<dominiocertPdA> degli utenti registrati). Nel caso di pacchetti che prevedono la firma del GC il PdA deve essere in grado di riconoscere come validi pacchetti firmati con un certificato diverso, fornito appositamente per l'ispezione.

Il passaggio tra la modalità di funzionamento normale e quella di debug deve poter essere eseguita rapidamente possibilmente senza dover ricompilare applicativi e o dover riavviare il sistema.



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

*Per la simulazione di collegamenti di utenti esterni al PdA gli accessi verranno effettuati attraverso Internet evitando di connettersi direttamente alla LAN del PdA, in modo da simulare il più possibile una situazione reale (evitando problematiche relative a tempi di accesso, firewall, ecc.).*

- Il PdA deve prevedere una funzionalità di allineamento dell'orologio di sistema con quello di un server di riferimento della RUPA, o comunque garantire allineamento rispetto all'orologio di sistema del GC.

Per le specifiche dei flussi di comunicazione tra PdA e GC si faccia riferimento al documento “Specifiche di Interfaccia tra Punto di Accesso e Gestore Centrale v. 2.0” [5].

### 3.1 PROCEDURE DI ABILITAZIONE E GESTIONE UTENZE

Per le specifiche dei messaggi coinvolti si faccia riferimento a “3 Flusso di abilitazione e gestione utenze” [5].

#### 3.1.1 Procedura (completa) di registrazione di un nuovo soggetto

1. Eseguire almeno tre procedure di registrazione (possibilmente una per un **avvocato**, una per un **CTU** e una per un **ente collettivo**)<sup>1</sup> di un nuovo soggetto fornendo i dati di cui all'art. 13 delle regole tecniche, verificando che:
  - a. Il PdA invii la richiesta di abilitazione in formato xml (ComunicazioneIndirizzi.xml) creando una busta SMIME “RichiestaAggiornamentoUtenze”. Il PdA deve mettere a disposizione una funzionalità di amministrazione per specificare e modificare i dati di iscrizione all'albo di un CdO (in particolare lo status dell'avvocato).
  - b. Il PdA deve consentire la tracciabilità dello stato delle richieste di registrazione evidenziando in particolare:
    - L'evento di ricezione da parte del GC della richiesta di registrazione. Il GC a seguito della ricezione invia al PdA una attestazione temporale o una notifica di eccezione.
    - L'evento di avvenuta registrazione (l'utente deve poter correttamente accedere al PdA) o la comunicazione di rifiuto della registrazione da parte del GC. Il GC infatti a seguito di una richiesta di registrazione di indirizzi invia al PdA una busta *ComunicazioneIndirizzi* con le richieste accettate dal GC ed eventualmente una busta *AnomaliaIndirizzi* contenente le richieste rifiutate.
  - c. venga aggiornato il ReLIndE presso il punto di accesso (consultare in modalità LDAP da browser collegato a Internet).

---

<sup>1</sup> Nel caso un PdA fornisca i propri servizi a una sola (o due) categorie di soggetti i test saranno limitati a queste categorie. In ogni caso eseguire almeno tre procedure di abilitazione.



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

- d. venga aggiornato il ReGIndE presso il gestore centrale (consultare in modalità LDAP da browser collegato a gestore centrale attraverso la rete privata con il punto di accesso).
2. Verificare che venga effettivamente garantito il rispetto dei seguenti vincoli (ovvero che il software impedisca di eseguire le operazioni):
  - a. Inserimento codice fiscale non valido (in base ai campi nome, cognome, sesso, luogo e data di nascita)
  - b. Inserimento codice fiscale già esistente nel ReLIndE (inserire soggetto con stesso CF del precedente)
  - c. Inserimento indirizzo elettronico già esistente nel ReLIndE (provare ad assegnare stesso indirizzo elettronico precedentemente assegnato). **Attenzione:** *non deve essere possibile assegnare nemmeno indirizzi elettronici di soggetti non attivi, revocati, sospesi e/o non più gestiti dal punto di accesso.*
  - d. Inserimento indirizzo elettronico (e/o CF) non esistente nel ReLIndE ma esistente nel ReGIndE (provare ad assegnare indirizzo elettronico già esistente nel ReGIndE verificando la corretta gestione dell'errore segnalato). **Attenzione:** *dovendo l'unicità dell'indirizzo elettronico (e del CF) essere garantita a livello di gestore centrale, prima di assegnare un nuovo indirizzo il PdA dovrebbe interrogare il ReGIndE per accertarsi della non esistenza evitando di dover gestire a posteriori l'errore.*
3. Tra i dati di cui all'art. 13, al punto h è citato il certificato di cifratura<sup>2</sup>. Verificare che vengano accettati certificati validi rispetto a quanto previsto dalle regole tecniche, per evitare che successivamente l'ufficio giudiziario non sia in grado di cifrare un documento. In particolare verificare che la lunghezza di chiave sia di almeno 1024 bit e che tra gli "usage" previsti compaia cifratura (ovvero "Key Encipherment" e "Data Encipherment"). Il PdA deve impedire il caricamento di certificati non validi, pertanto in fase di caricamento del certificato deve eseguire parsing di quest'ultimo e verificarne la compatibilità. Provare a caricare almeno due certificati non validi (lunghezza di chiave 512 e usage non corretto). In caso di certificato non accettato il sistema deve segnalare la motivazione del rifiuto in gergo comprensibile.
4. Al gestore centrale dovranno pervenire tutti i messaggi previsti prodotti in automatico dai server di posta elettronica certificata del PdA.

### 3.1.2 Procedura di variazione utenze

Procedere all'invio di richiesta di modifica di dati da parte dell'utente secondo il flusso previsto, simile a quello di registrazione utenze.

1. Verificare che venga correttamente creata la busta S/MIME "AggiornamentoUtenze", in cui l'elemento *TipoOperazione* nell'XML *ComunicazioneIndirizzi* dovrà avere valore "M". La corretta composizione del messaggio può essere verificata (impostando il PdA in modalità debug) e analizzando i messaggi prodotti.

---

<sup>2</sup> Al momento di pubblicazione del presente documento questo tipo di test è sospeso, in quanto non è tuttora prevista la cifratura per le informazioni in uscita dall'UG.



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

2. Il PdA deve consentire la tracciabilità dello stato delle richieste di variazione delle utenze evidenziando in particolare:
  - o L'evento di ricezione da parte del GC della richiesta di variazione (attestazione temporale).
  - o L'evento di avvenuta variazione o la comunicazione di anomalia nella richiesta
3. venga aggiornato il ReLIndE presso il punto di accesso (consultare in modalità LDAP da browser collegato a Internet).
4. venga aggiornato il ReGIndE presso il gestore centrale (consultare in modalità LDAP da browser collegato a gestore centrale attraverso la rete privata con il punto di accesso).
5. Al gestore centrale dovranno pervenire tutti i messaggi previsti prodotti in automatico dai server di posta elettronica certificata del PdA.

### **3.1.3 Procedura di cancellazione utenze**

Procedere all'invio di richiesta di cancellazione di un utente da parte dell'utente stesso secondo il flusso previsto, simile a quelli di inserimento e cancellazione.

1. Verificare che venga correttamente creata la busta S/MIME "AggiornamentoUtenze" in cui l'elemento *TipoOperazione* nell'XML *ComunicazioneIndirizzi* dovrà avere valore "C". La corretta composizione del messaggio può essere verificata (impostando il PdA in modalità debug) e analizzando i messaggi prodotti.
2. Il PdA deve consentire la tracciabilità dello stato delle richieste di cancellazione delle utenze evidenziando in particolare:
  - o L'evento di ricezione da parte del GC della richiesta di cancellazione (attestazione temporale).
  - o L'evento di avvenuta variazione o la comunicazione di anomalia nella richiesta (esempio cancellazione di un utente non registrato)
3. venga aggiornato il ReLIndE presso il punto di accesso (consultare in modalità LDAP da browser collegato a Internet).
4. venga aggiornato il ReGIndE presso il gestore centrale (consultare in modalità LDAP da browser collegato a gestore centrale attraverso la rete privata con il punto di accesso).
5. a cancellazione registrata verificare che l'utente non abbia più il permesso di accesso all'area privata del PdA.
6. Al gestore centrale dovranno pervenire tutti i messaggi previsti prodotti in automatico dai server di posta elettronica certificata del PdA.

### **3.1.4 Verifica funzionalità per i Rappresentanti dei Consigli dell'Ordine**

Questo tipo di test è applicabile solo se il PdA è gestito da un consiglio dell'ordine o dal Consiglio Nazionale Forense. In questi casi è necessario verificare:



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

1. la disponibilità della funzionalità di invio al Gestore Centrale del file XML di richiesta di variazione utenze firmato dal Rappresentante del Consiglio dell'Ordine degli Avvocati o del consiglio Nazionale Forense, tramite la relativa CPECPT.
2. la disponibilità per il Rappresentante dell'Ordine degli Avvocati (o del Consiglio Nazionale Forense) ed eventuali suoi rappresentati di visualizzare tutti i messaggi di comunicazione indirizzi o notifiche eccezioni inviati dal GC, relativamente a tutte le richieste di iscrizione, modifica e cancellazione di utenti (difensori) che sono iscritti presso il CdO effettuate. Per testare la ricezione di Notifica Eccezione è possibile inviare una richiesta di variazione utente firmato da un Legale Rappresentante del CdO non censito nella base dati anagrafica del GC.
3. Al gestore centrale dovranno pervenire tutti i messaggi previsti prodotti in automatico dai server di posta elettronica certificata del PdA.

### 3.2 VERIFICA DELLE CREDENZIALI DI UN SOGGETTO ATTRAVERSO ALBO (SE APPLICABILE)

1. È necessario verificare la presenza e il funzionamento di un applicativo per le procedure di inserimento, modifica e visualizzazione dello status degli avvocati, eseguita dallo stesso sistema informativo del PdA da parte dell'amministratore o dal Rappresentante del CdO (se previsto).
2. Dalla CPECPT del CdO inviare al GC variazione dello status di un avvocato (abilitato → radiato, radiato → sospeso) e procedere alla verifica del comportamento del PdA. Ad ogni variazione dello status (ricezione da parte del PdA di *AggiornamentoUtenze*) verificare il corretto aggiornamento sul ReLIndE.

Nel caso di PdA di un Consiglio dell'Ordine o del Consiglio Nazionale Forense, il corretto funzionamento dell'applicativo di gestione delle utenze può essere verificato analizzando il pacchetto di certificazione allegato al flusso InoltroAtto ("*4.1.1.1 Struttura del messaggio di inoltro atto*" [5]) secondo la seguente procedura:

- a) impostare la modalità debug sul PdA (in modo da re-dirigere gli output a un indirizzo elettronico specificato).
- b) Inviare un atto utilizzando come mittente un avvocato "abilitato". Verificare nel messaggio S/MIME prodotto la corretta composizione del pacchetto *certificazione*.
- c) Modificare lo status dell'avvocato di cui al punto precedente da "abilitato" a "radiato".
- d) Inviare nuovamente l'atto utilizzando come mittente lo stesso avvocato (ora "radiato"). Verificare nel messaggio S/MIME prodotto la corretta composizione del pacchetto *certificazione*.
- e) Ripetere i due punti di cui sopra modificando lo status in "sospeso".

Nel caso di PdA privato sarà a carico del personale del PdA mostrare la correttezza e l'attendibilità dell'applicativo di gestione dello status delle utenze. Ad esempio mostrando in ReLIndE il valore dello status dell'avvocato prima e dopo una modifica, o impedendo a un avvocato l'accesso alle funzionalità critiche nel caso in cui gli sia stato attribuito uno status invalidante.



---

**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

### **3.3 CONSULTAZIONI POLISWEB**

Per le specifiche di accesso ai servizi di consultazione attraverso Polis Web si faccia riferimento a “5 Consultazioni” [5].

1. Le regole tecniche prevedono che il PdA stabilisca un canale sicuro con i browser esterni utilizzando SSL v.3 e chiavi di 1024 bit. Per la verifica di questi parametri è necessario collegarsi con un browser dall'esterno e:
  - a. verificare la lunghezza della chiave visualizzando il certificato (doppio click sul lucchetto nella barra di stato del browser IE 6).
  - b. verificare l'impossibilità di connettersi se non attraverso protocollo SSL v.3. Nel browser IE 6, entrare nelle impostazioni avanzate (Internet Option → Advanced) e disabilitare l'opzione “USE SSL 3.0”. Chiudere il browser e ritentare il collegamento, verificando che il sito non accetti la connessione.
2. Deve essere anche verificato che il PdA stabilisca un canale sicuro con il GC (SSL v.3 e chiavi di 1024 bit) durante la consultazione sincrona mediante polis web. Il PdA deve mettere a disposizione procedure per la verifica di queste specifiche.
3. Le regole tecniche stabiliscono che l'autenticazione avviene secondo le specifiche previste dalla Carta Nazionale dei Servizi (CNS); nel seguito con *certificato di autenticazione valido* si intende un certificato di autenticazione compatibile con le specifiche della CNS. Si identificano due casi: 1) Il PdA, a seguito di un accordo con una CA accreditata, rilascia direttamente in fase di registrazione dell'utente un token crittografico con il certificato di autenticazione valido; 2) Il PdA richiede all'utente di dotarsi prima della registrazione di un token crittografico contenente un certificato di autenticazione valido e compatibile con la propria architettura<sup>3</sup>. In entrambi i casi deve essere verificato durante la registrazione come avviene l'associazione tra il certificato di autenticazione e il record dell'utente nel PdA<sup>4</sup>. Verificare la procedura di connessione al PdA (da Internet) tramite browser e il funzionamento della procedura di autenticazione.
4. Nel caso 2) del punto precedente (si veda anche la nota 3), è facoltà di chi esegue l'ispezione, verificare la compatibilità di tutti i token crittografici previsti, o limitarsi a verificare la compatibilità di alcuni di questi.
5. La verifica delle funzionalità di accesso sincrono tramite PolisWeb (Front End) può essere fatta eseguendo attraverso browser una serie di interrogazioni. La completezza e il livello di dettaglio del test dipende anche dal livello di confidenza nell'implementazione di Polis Web nel PdA. Se ad esempio è stato utilizzato esattamente lo stesso front end (a livello di codice) già collaudato dall'Amministrazione in precedenti occasioni, la verifica sarà orientata a verificare aspetti relativi all'integrazione di questo modulo con il resto dell'architettura più che a una copertura funzionale totale.

---

<sup>3</sup> Il manuale operativo deve esplicitamente indicare quali token crittografici sono compatibili specificando modello/versione e CA emittitrice.

<sup>4</sup> Potrebbe essere una semplice associazione tramite Codice Fiscale oppure potrebbe venir associato SerialNumber + Issuer del certificato al Codice Fiscale dell'utente inserito solo nel sistema informativo del PdA.

## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

6. Al termine della deroga sulla cifratura (si veda a tale proposito la nota 2) è necessario prevedere la verifica delle funzionalità di cifratura in uscita dall'UG. La procedura di verifica dipende dalla soluzione tecnica adottata dal PdA. Il PdA deve mettere a disposizione una procedura per la verifica di queste specifiche.

### 3.4 FUNZIONALITÀ DI ACCESSO AI REGISTRI DEL GC

Il Punto di Accesso deve fornire una funzionalità di accesso ai registri sul Gestore Centrale attraverso un collegamento in modalità LDAP.

I registri di interesse sono:

- il Registro Generale degli Indirizzi utile per il reperimento degli indirizzi delle caselle di posta elettronica e dei certificati di cifratura degli avvocati
- il registro degli Uffici Giudiziari, in cui sono registrati i dati di tutti i Tribunali che partecipano al Processo Telematico.

### 3.5 DEPOSITO DI ATTI E TRACCIABILITÀ DELLO STATO DEL DEPOSITO.

Per le specifiche dei messaggi coinvolti nel flusso di deposito si faccia riferimento a “4.1 Il Deposito di un Atto” [5].

1. Il PdA deve accettare atti composti tramite il prototipo di redattore ministeriale. In particolare tutti i file del tipo *atto.enc* prodotti dal prototipo redattore ministeriale devono poter essere inviati tramite il PdA eventualmente estraendo le informazioni di inoltro dalla busta dell'avvocato. Ciascun PdA può definire autonomamente le procedure di caricamento degli atti a partire dalla postazione dell'utente esterno, automatizzando o meno la compilazione delle informazioni di spedizione, ecc. Durante il collaudo deve essere verificata la modalità di caricamento atti proposta dal PdA.
2. Verificare che nella modalità di caricamento proposta dal PdA, la cifratura dell'atto (passaggio da *atto.msg* a *atto.enc*) venga eseguita dalla postazione dell'avvocato e non dal PdA il quale non deve poter accedere al contenuto in chiaro degli atti.

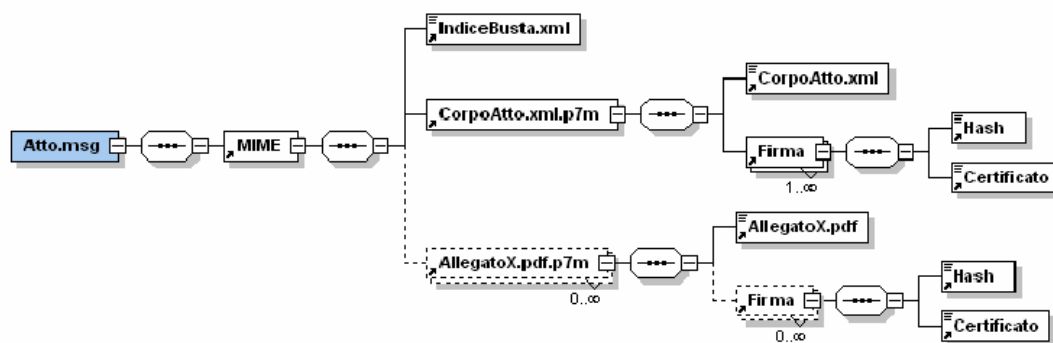


Figura 1 - Atto con indice e allegati, prima della crittazione

**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

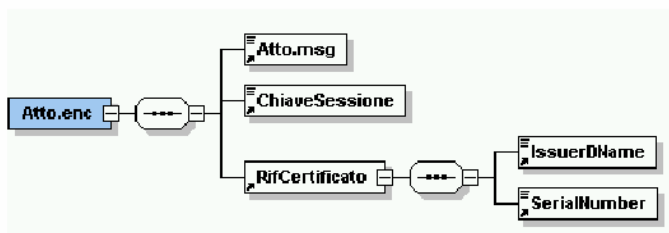


Figura 2 - pacchetto atto.enc già cifrato dalla postazione dell'Avvocato prima del caricamento sul PdA

3. Verificare l'effettiva presenza di controllo antivirus sui file *atto.enc* caricati, inserendo un file *atto.enc* affetto da virus (recente).
4. Verificare che il PdA controlli le informazioni contenute in InfoInoltro. In particolare il PdA dovrebbe controllare che la busta sia destinata ad un UG conosciuto che fa capo al PdA stesso e il relativo campo CodiceUG di InfoInoltro sia correttamente valorizzato.
5. Il PdA invia l'atto al GC creando un messaggio S/MIME secondo la struttura prevista di *InoltroAtto*. La corretta composizione del messaggio può essere verificata impostando il PdA in modalità debug e analizzando i messaggi prodotti. In particolare deve essere verificato il contenuto di ciascuno dei campi del messaggio e la corrispondenza di *atto.enc* con quanto utilizzato come input.
6. Il PdA deve consentire la tracciabilità dello stato del deposito evidenziando in particolare:
  - a. l'evento di ricezione da parte del GC dell'atto. Il GC a seguito della ricezione invia al PdA un messaggio di attestazione temporale, o di notifica di eccezione. Deve essere tracciato anche l'evento di ricezione di attestazione temporale non corretta (ad esempio campo *Impronta* sbagliato).
  - b. l'evento di accettazione da parte dell'UG dell'atto. L'UG a seguito dell'inoltro di un Atto dal Pda, invia al GC due messaggi di risposta:
    - comunicazione dell'esito automatico dei controlli di accettazione del deposito atto,
    - comunicazione dell'esito del deposito atto in Cancelleria.I messaggi vengono rielaborati dal GC e spediti al PdA (ComunicazioneEsito).  
Il PdA dovrà consentire la tracciabilità delle due fasi di accettazione del deposito distintamente (controlli automatici e accettazione in Cancelleria).
7. Ciascun PDA può proporre una diversa interfaccia per la visualizzazione dei messaggi di attestazione temporale e di accettazione dell'UG di cui sopra. Durante il collaudo deve essere comunque verificato che l'interfaccia del PdA sia sufficientemente semplice e che le informazioni presentate siano corrette e complete. A tal fine verificare il corretto funzionamento dell'intera procedura di deposito (con il vero GC e l'UG di test) e relativa tracciabilità per almeno 3 atti.
8. Il PdA deve verificare la validità e l'autenticità dei messaggi che riceve dal GC e in particolare:
  - a. verificare che non siano affetti da virus.



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

- b. che il messaggio *AttestazioneTemporale* sia stato firmato dal GC e non modificato (controllo di *HashAttestazione*).
- c. che l'*attestazione* del messaggio *AttestazioneTemporale* sia relativa al messaggio spedito dal PdA e che questo sia stato ricevuto correttamente dal GC (controllando *Impronta* all'interno di *DatiAttestazione*).
- d. che i messaggi di *ComunicazioneEsito* siano stati firmati dall'UG e non modificati (controllo di *Hash\_EsitoAtto*).
- e. che *DatiEsito* dei messaggi *ComunicazioneEsito* siano relativi al messaggio spedito dal PdA e che questo sia stato ricevuto correttamente dall'UG (controllando *Impronta* all'interno di *DatiEsito*).
- f. che tutti gli identificatori di messaggio, utente, PdA, ecc... siano corretti.
- g. che gli eventi temporali siano ragionevolmente corretti (allineamento rispetto all'orologio del PdA); in particolare deve essere controllata la validità della data di attestazione temporale (compresa tra la data di deposito e la data di ricezione dell'attestazione temporale stessa da parte del PdA).

L'effettiva verifica della presenza di questi controlli può essere fatta, trasmettendo in modo *debug* al PdA (impersonificando il GC) pacchetti preconfezionati che sono stati alterati introducendo inconsistenze.

9. Test di carico: il gestore del PdA deve mettere a disposizione, all'atto della verifica, un apposito strumento software che consenta di effettuare simulazioni di carico con l'obiettivo di verificare che il PdA sia in grado di gestire più utenti che inviano atti nello stesso istante temporale. Il software deve eseguire l'invio automatico (in parallelo) di un numero rilevante di buste (nell'ordine delle venti-trenta), preconfezionate in formato atto.enc.

### **3.6 GESTIONE DI ECCEZIONI (ERRORI RICEVUTI DA GC).**

Per le specifiche dei messaggi coinvolti si faccia riferimento a “4.1.1.3 Struttura del messaggio di Notifica Eccezione” [5].

1. Se il GC riscontra un errore nella formazione della busta di *InoltroAtto*, 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 dalla struttura prevista, che il PdA deve saper gestire e segnalare all'utente. Il test può essere eseguito inviando un atto dal PdA in modalità *debug* e restituendo al PdA un messaggio di eccezione preconfigurato.
2. Oltre alle simulazioni eseguire un deposito in collegamento con il Gestore Centrale che scateni l'emissione di una Notifica Eccezione (utilizzando ad esempio un codice fiscale dell'avvocato mittente non presente in base dati).
3. Deve essere simulato anche il caso di inoltro di un atto e assenza di risposta da parte del GC. Verificare come si comporta in questo caso il PdA, e che tipo di allarmi e procedure di re-invio automatico sono previste.



**PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

### **3.7 RICEZIONE DI NOTIFICHE NELLE CASELLE DI POSTA CERTIFICATA (BIGLIETTO DI CANCELLERIA)**

Per le specifiche dei flussi e dei messaggi coinvolti si faccia riferimento a “4.2 L'invio di un biglietto di cancelleria” [5].

1. Inviare al PdA, presso la casella di posta <CPECPT> di ciascuno degli utenti attivati al punto 3.1.1, una notifica (preconfezionata). Il PdA su ricezione del messaggio deve verificare:
  - a. che non sia affetto da virus.
  - b. la firma del GC sul MIME.
  - c. la firma e quindi l'integrità di *AttoUG.enc* attraverso controllo di *HashMIME*.
2. Il Server di dominio del PdA deve emettere la ricevuta di presa in carico per il GC.
3. La casella di posta certificata di destinazione deve emettere ricevuta di avvenuta consegna conforme alle specifiche della posta certificata.
4. Oltre alle simulazioni e analisi dei pacchetti in modo debug eseguire invio di comunicazioni dall'ufficio giudiziario di Test verso le caselle degli utenti creati al punto 3.1.1, verificando il funzionamento.
5. Verificare che il PdA metta a disposizione una funzionalità applicativa, che renda visualizzabili, in modo semplice e intuitivo, le diverse tipologie di messaggi ricevuti nella CPECPT dell'utente.

### **3.8 NOTIFICHE TRA DIFENSORI**

Per le specifiche dei flussi di comunicazione si faccia riferimento a “4.3 Flusso di notifiche tra difensori (tramite CPECPT)” [5].

#### **3.8.1 Invio di notifiche tra difensori**

1. Nel flusso di inoltro notifica ad avvocato, nella fase di upload ed inoltro della busta contenente la notifica (*InoltroNotificaAvvocato*) il PdA deve:
  - Verificare la correttezza della struttura MIME della busta
  - Verificare la validità formale di *InfoNotifica.xml*
  - Verificare la validità dei contenuti dei tag *Mittente* e *Destinatario*. In particolare il Codice Fiscale del Mittente deve corrispondere a quello dell'utente connesso, mentre deve essere controllato il formato del codice Fiscale dell'avvocato Destinatario.
  - Se tutti i controlli sono superati, deve aggiornare il file *InfoNotifica.xml* con un identificativo univoco (a livello PdA) dell'atto informatico da inoltrare (*IdMsgPdA*)



## PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO

---

- Comporre la busta MIME da inviare al GC firmandola con il certificato server di firma digitale (S/MIME).
- 2. Il PdA deve consentire inoltre la tracciabilità dello stato di invio notifiche in base alla ricezione di eccezioni o delle attestazioni temporali che il GC invia a seguito di:
  - ricezione della notifica da inoltrare
  - ricezione della ricevuta di avvenuta consegna dal PdA dell'avvocato destinatario; in questo caso l'attestazione temporale è accompagnata dalla RdAC.

Per ogni attestazione temporale ricevuta il PdA deve verificarne la validità e l'autenticità, in particolare:

- verificare che non siano affetti da virus.
- che il messaggio sia stato firmato dal GC e non modificato (controllo di *HashAttestazione*).
- che l'attestazione sia relativa al messaggio spedito dal PdA e che questo sia stato ricevuto correttamente dal GC (controllando *Impronta* all'interno di *DatiAttestazione*).
- che tutti gli identificatori di messaggio siano corretti.
- che la data di attestazione temporale sia valida

Per le verifiche si può procedere ad invio di notifiche ad avvocati iscritti sul registro generale degli indirizzi, ed invio di notifiche con allegato "*InfoNotifica.xml*" mal valorizzato (ad esempio codice fiscale destinatario non presente sul registro generale degli indirizzi).

### 3.8.2 Ricezione di notifiche tra difensori

Il punto di Accesso dell'avvocato destinatario alla ricezione di un messaggio di notifica nel sistema di posta certificata deve verificare provenienza ed integrità (firma digitale) dei messaggi, in particolare:

- all'atto della ricezione della notifica e della prima attestazione temporale, il PdA deve verificare la corrispondenza del campo *Impronta* con quanto trasmesso (hash della busta S/MIME di *ConsegnaNotifica*);
- verifica dell'integrità e della validità dell'attestazione temporale inviata dal GC a seguito dell'invio della RdAC dal sistema di gestione di Posta Certificata del PdA stesso.

## 3.9 RICHIESTA DI COPIA CONFORME

Per le specifiche dei messaggi coinvolti si faccia riferimento a "4.4 Funzione di richiesta e ricezione della copia conforme" [5].



## **PIANO DELLE VERIFICHE PER L'AUTORIZZAZIONE DEI PUNTI DI ACCESSO**

---

1. Verificare la possibilità di accedere alla funzionalità, messa a disposizione da PolisWeb, di richiesta di copia conforme di documenti rilasciati dall'Ufficio Giudiziario; il PdA dovrà fornire tracciabilità dello stato della richiesta.
2. Verificare che il PdA permetta all'utente di visualizzare copie di atti richieste, ricevute nella propria CPECPT, e di poterne attivare il download.

### **3.10 PROCEDURA (COMPLETA) DI DISABILITAZIONE DI UN SOGGETTO ABILITATO**

1. Si tratta di disabilitare i soggetti registrati al punto 3.1.1 revocando loro i permessi di accesso, attraverso le funzionalità messe a disposizione dell'amministratore del PdA. A seguito della disabilitazione verificare che vengano aggiornati il ReLIndE e il ReGIndE e che gli utenti non siano più in grado di accedere nemmeno disponendo delle relative smart card di autenticazione.

### **3.11 SICUREZZA DEI LOCALI E DELLE PROCEDURE DI AMMINISTRAZIONE DEL SISTEMA**

L'accesso ai locali e ai server che ospitano le macchine del PdA è un altro punto di primaria importanza. Nel piano di sicurezza devono essere precisamente indicate tecnologie e modalità operative utilizzate per la protezione delle macchine. Deve altresì essere precisamente indicato quali sono le modalità di amministrazione del sistema (upgrade, correzione bug, patch al sistema operativo, etc.) e se e come è possibile un'amministrazione remota delle macchine (operazione molto rischiosa).

Durante l'ispezione verrà verificato che quanto descritto nel piano di sicurezza corrisponda alla situazione reale.

### **3.12 CORRETTA PROCEDURA DI CHIUSURA SESSIONE**

Ogni accesso al PdA deve attivare il processo di autenticazione; deve quindi essere verificato il controllo di validità del certificato di autenticazione presente nella smart card in uso. Il PdA deve prevedere un meccanismo di scadenza o invalidamento della sessione in caso di inattività (es rimozione della carta o timeout).

La corretta procedura di chiusura sessione deve essere testata con browser diversi (Internet Explorer, FireFox,...)