

MINISTERO DELLA GIUSTIZIA
DECRETO 14 ottobre 2004

Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile.

Gazzetta Ufficiale 19-11-2004, n. 272, Serie Generale, S.O. 167

Capo I Principi generali

IL MINISTRO DELLA GIUSTIZIA

Visto il decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123;

Visto il decreto ministeriale 27 marzo 2000, n. 264;

Visto il decreto ministeriale 24 maggio 2001;

Vista la delibera del Centro nazionale per l'informatica nella pubblica amministrazione del 19 febbraio 2004, n. 11;

Sentito il Centro nazionale per l'informatica nella pubblica amministrazione, con il parere del 22 settembre 2004, dal quale parzialmente ci si discosta, ove si ravvisa la superfluità del certificato per la crittografia delle informazioni trasmesse, ritenendo opportuno garantire la massima sicurezza nei raccordi comunicativi, in particolare, nel punto d'accesso e nel gestore centrale; ritenuta, inoltre, l'opportunità di limitare

l'utilizzazione delle caselle di posta elettronica alle sole comunicazioni del processo telematico, in considerazione dell'inesperienza degli utenti, in fase di prima attuazione; Sentito il Garante per la protezione dei dati personali, con il parere del 23 luglio 2004, dal quale parzialmente ci si discosta, ove si ravvisa l'utilità di inserire ulteriori richiami, sostanziali e formali, al decreto legislativo n. 196 del 2003, trovando tale normativa, di rango superiore, comunque applicazione; ritenuta, inoltre, la non necessità di individuare i titolari del trattamento dei dati personali, esulando la problematica dal ristretto ambito delle regole tecniche; ritenuta la non opportunità di cumulare, necessariamente, il responsabile della sicurezza con il responsabile del trattamento dei dati personali, attese le diverse finalità che possono richiedere professionalità differenti ed, infine, di mantenere le ampie condizioni di accesso agli avvocati dello Stato, in ragione della loro rappresentanza, fissata dall'art. 1 del regio

decreto 30 ottobre 1933, n. 1611;

Decreta:

Art. 1.

Ambito di applicazione

1. Il presente decreto stabilisce le regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile di cui all'art. 3, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123.

Art. 2.

Definizioni

1. Ai fini del presente decreto si intendono per:

a) **SICI: sistema informatico civile** come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n. 123;

b) gestore centrale: struttura tecnico-organizzativa che, nell'ambito del dominio giustizia, come definito all'art. 1, comma 1, lettera e) del decreto ministeriale 13 febbraio 2001, n. 123, fornisce i servizi di accesso al SICI ed i servizi di trasmissione telematica dei documenti informatici processuali fra il SICI ed i soggetti abilitati, secondo le norme riportate nel presente decreto;

c) gestore locale: sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o **all'ufficio notifiche esecuzioni e protesti (G)**, ed i servizi di trasmissione telematica dei documenti informatici processuali fra il gestore centrale ed il singolo ufficio giudiziario o **UNEP**;

d) certificazione del difensore: attestazione al difensore di iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati ovvero di possesso della qualifica che legittima l'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva;

e) punto di accesso: struttura tecnico-organizzativa che fornisce ai soggetti abilitati, esterni al SICI, i servizi di connessione al gestore centrale e di trasmissione telematica dei documenti informatici relativi al processo, nonché la casella di posta elettronica certificata, secondo le regole tecnico-operative riportate nel presente decreto;

f) autenticazione: operazione di identificazione in rete del

titolare della carta nazionale dei servizi o di altro dispositivo crittografico, contenente un certificato di autenticazione, secondo la previsione dell'art. 62;

g) firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 23 gennaio 2002, n. 10;

h) fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, ovvero le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo;

i) soggetti abilitati: tutti i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:

1.1. soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;

1.2. soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali;

1.3. soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;

1.4. soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli **UNEP**;

j) casella di posta elettronica certificata per il processo telematico (CPECPT): indirizzo elettronico, per il processo telematico, dei soggetti abilitati.

Art. 3.

Gestore centrale

1. Il gestore centrale e' il punto unico di interazione, a livello nazionale, tra il SICI ed i soggetti abilitati esterni.

2. Il gestore centrale e' attivo presso il Ministero della giustizia.

Art. 4.

Gestore locale

1. Il gestore locale e' parte del sistema informatico dell'ufficio giudiziario e dell'**UNEP**, come definito nel decreto ministeriale del 24 maggio 2001, e rispetta i requisiti tecnici ed organizzativi definiti in tale ambito.

2. I gestori locali sono attivi presso gli uffici giudiziari e gli **UNEP**.

Art. 5.

Sistemi informatici di gestione della cancelleria e dell'**UNEP**

1. Il sistema informatico di gestione delle cancellerie civili e' costituito dall'infrastruttura hardware e software di gestione dei registri e dei fascicoli informatici.

2. Il sistema informatico di gestione degli UNEP e' costituito dall'infrastruttura hardware e software per la gestione delle notifiche.

Art. 6.

Punto di accesso

1. I soggetti abilitati esterni accedono al SICI tramite un punto di accesso, che puo' essere attivato esclusivamente dai soggetti pubblici, di cui al comma 5, e dai soggetti privati, di cui al comma 6. Ciascun soggetto puo' avvalersi di un solo punto di accesso.

2. I punti di accesso forniscono un'adeguata qualita' dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema ed a non comprometterne i livelli di servizio, nel rispetto dei requisiti tecnici di cui all'art. 30.

3. La violazione, da parte di un punto di accesso, dei livelli di sicurezza e di servizio, comporta la sospensione ad erogare i servizi fino al ripristino di tali livelli.

4. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.

5. I soggetti pubblici, che possono attivare e gestire uno o piu' punti di accesso, sono:

a) i consigli dell'ordine degli avvocati, ciascuno limitatamente ai propri iscritti;

b) il Consiglio nazionale forense, limitatamente ai propri iscritti e agli iscritti dei consigli dell'ordine degli avvocati;

c) il Consiglio nazionale del notariato, limitatamente ai propri iscritti;

d) l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;

e) il Ministero della giustizia, per i soggetti abilitati interni

e in via residuale, ove sussistano oggettive difficoltà per

l'attivazione del servizio da parte dei soggetti di cui ai punti a) e b);

f) il Ministero della giustizia, in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui al comma 6, al solo fine di garantire l'accesso agli esperti e ausiliari del giudice.

6. I soggetti privati, che attivano e gestiscono un punto di accesso, hanno i seguenti requisiti:

a) forma di società per azioni;

b) capitale sociale e requisiti di onorabilità di cui al decreto legislativo 1° settembre 1993, n. 385, art. 25, comma 1.

Art. 7.

Certificazione dei difensori

1. La certificazione del difensore è svolta dal punto di accesso, qualora questo sia gestito da un Consiglio dell'ordine degli avvocati o dal Consiglio nazionale forense, oppure dal gestore centrale sulla base di copia dell'albo fornita al Ministero della giustizia e dai consigli dell'ordine degli avvocati e dal Consiglio nazionale forense.

2. L'aggiornamento della copia dell'albo avviene entro 72 ore dalla comunicazione, dei provvedimenti di pertinenza, all'interessato.

3. Il Consiglio nazionale forense compie il servizio di certificazione dei difensori per i propri iscritti o, per gli iscritti dei consigli dell'ordine, su delega di questi ultimi.

Art. 8.

Accesso dei soggetti abilitati esterni privati

1. Per il difensore delle parti è necessaria, ai fini dell'accesso al SICI, l'autenticazione presso il punto di accesso di cui al capo quarto e la certificazione di cui all'art. 7.

2. Il SICI consente al difensore l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito e permette, negli altri casi, l'acquisizione delle informazioni necessarie per la costituzione in giudizio.

3. In caso di delega, rilasciata ai sensi dell'art. 9, regio decreto legislativo 27 novembre 1933, n. 1578, il SICI consente all'avvocato delegato l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dall'avvocato delegante, previa comunicazione, a cura di parte, di copia della delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della

revoca della delega.

4. La delega, sottoscritta con firma digitale, e' rilasciata in conformita' al modello previsto dall'art. 56.

5. Gli esperti e gli ausiliari del giudice accedono al SICI nel limite dell'incarico ricevuto e della autorizzazione, concessa dal giudice, alla consultazione e alla copia degli atti.

6. A seguito dell'autenticazione, viene trasmesso al gestore centrale il codice fiscale del soggetto abilitato esterno privato.

Art. 9.

Accesso dei soggetti abilitati esterni pubblici

1. Il punto di accesso autentica il soggetto abilitato esterno pubblico e trasmette il relativo codice fiscale al gestore centrale.

2. I dati, di cui al comma 1, sono utilizzati per individuare i privilegi di accesso alle informazioni contenute nel SICI.

3. Il SICI consente agli avvocati e procuratori dello Stato l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui e' parte una pubblica amministrazione.

Art. 10.

Accesso dei soggetti abilitati interni

1. I soggetti abilitati interni accedono al SICI attraverso la rete unica della giustizia (RUG) e attraverso il punto di accesso del Ministero della giustizia.

Capo II Gestione della posta elettronica

Art. 11.

Casella di posta elettronica certificata del processo telematico

1. I soggetti abilitati esterni, per utilizzare i servizi di trasmissione telematica dei documenti informatici, dispongono di un indirizzo elettronico e della relativa casella di posta elettronica, CPECPT, forniti e gestiti dal punto di accesso, nel rispetto dei requisiti di cui all'art. 12.

2. Ogni indirizzo elettronico, come definito nel decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, corrisponde ad una CPECPT.

3. Ad ogni soggetto, che interagisce per via telematica con il SICI, corrisponde un solo indirizzo elettronico.

4. Ogni CPECPT e' abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale.

Art. 12.

Requisiti del servizio di gestione della CPECPT

1. La CPECPT garantisce la ricezione dei messaggi e la loro

disponibilita' per trenta giorni, successivamente il messaggio e' archiviato e sostituito da un avviso contenente i seguenti dati: identificativo univoco del messaggio, mittente, data, ora e minuti di arrivo.

2. Il servizio di posta elettronica certificata restituisce al mittente una ricevuta breve di avvenuta consegna per ogni documento informatico reso disponibile al destinatario, cui e' associata l'attestazione temporale di cui all'art. 45.

3. Salvo quanto previsto nel presente decreto e nell'allegato B, la posta certificata del processo telematico si conforma alle linee guida stabilite dal Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA).

4. L'avviso di cui al comma 1 e' conservato, presso il punto d'accesso, per un periodo non inferiore a cinque anni.

Art. 13.

Registro generale degli indirizzi elettronici

1. Il registro generale degli indirizzi elettronici, attivo presso il gestore centrale, contiene l'elenco di tutti gli indirizzi elettronici attivati dai punti di accesso.

2. Il registro generale degli indirizzi elettronici e' accessibile a tutti i soggetti abilitati, secondo le modalita' previste dall'art. 19.

3. All'indirizzo elettronico delle persone fisiche, 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) consiglio dell'ordine o ente di appartenenza;
- j) stato del difensore: attivo, non attivo.

4. All'indirizzo elettronico degli enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, sono associate le seguenti informazioni:

- a) denominazione sociale;
- b) codice fiscale;
- c) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
- d) sede legale;

- e) certificato digitale relativo alla chiave pubblica da utilizzare per la cifratura;
- f) stato dell'indirizzo: attivo, non attivo.

Art. 14.

Registrazione dei soggetti abilitati esterni al SICI

1. L'accesso al SICI e la casella di posta elettronica si ottengono previa registrazione presso un punto di accesso.
2. La registrazione si ottiene con richiesta scritta, che il punto d'accesso conserva per almeno dieci anni.
3. Con la registrazione, il punto di accesso acquisisce i dati di cui all'art. 13, commi 3 e 4, e verifica l'identità del richiedente ed il relativo codice fiscale.
4. I difensori delle parti presentano, all'atto della registrazione, un certificato, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine di appartenenza 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 ostative allo svolgimento dell'attività difensiva.
5. Gli esperti e gli ausiliari del giudice presentano, all'atto della registrazione, il certificato della iscrizione all'albo dei consulenti tecnici o copia della nomina da parte del giudice dalla quale risulta che l'incarico non è esaurito.
6. Al momento della registrazione, i soggetti abilitati esterni comunicano al punto di accesso le seguenti informazioni:
 - a) nome e cognome;
 - b) luogo e data di nascita;
 - c) codice fiscale
 - d) residenza;
 - e) domicilio;
 - f) certificato digitale, relativo alla chiave pubblica, per la cifratura;
 - g) consiglio dell'ordine di appartenenza.

I soggetti abilitati esterni comunicano al punto di accesso ogni variazione delle informazioni di cui alle lettere d), e), f) e g).

7. Le informazioni di cui al comma 6, unitamente alla qualità di difensore delle parti, di esperto o ausiliario del giudice, ed all'indirizzo elettronico assegnato e ad eventuali variazioni del suo stato, sono trasmesse dal punto di accesso al gestore centrale e, per i difensori delle parti, al consiglio dell'ordine di appartenenza.

Art. 15.

Obbligo di informazione

1. I punti di accesso informano i titolari di indirizzi elettronici

degli obblighi assunti in relazione al servizio offerto.

Art. 16.

Registro degli indirizzi elettronici del punto di accesso

1. 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.
2. Ad ogni indirizzo elettronico di persona fisica sono associate le informazioni di cui all'art. 13, comma 3.
3. L'indirizzo elettronico di enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, associa le informazioni di cui all'art. 13, comma 4.
4. Il difensore comunica al consiglio dell'ordine di appartenenza il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso, unitamente al proprio codice fiscale e ai dati identificativi del punto di accesso.
5. Il difensore delle parti, l'esperto o l'ausiliario del giudice comunica alla cancelleria competente il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso.
6. Il registro degli indirizzi elettronici e' accessibile a tutti i soggetti abilitati, secondo le modalita' previste dall'art. 19.
7. Per i soggetti abilitati esterni pubblici, ciascun punto di accesso comunica al Ministero della giustizia, per via telematica, tutte le informazioni di cui all'art. 13, commi 3 e 4, ed ogni loro variazione, al fine dell'inserimento nel registro generale degli indirizzi elettronici.

Art. 17.

Comunicazioni dei consigli dell'ordine degli avvocati e del Consiglio nazionale forense

1. Al fine dell'inserimento nei registri degli indirizzi elettronici, i consigli dell'ordine degli avvocati e il Consiglio nazionale forense comunicano al Ministero della giustizia ed ai punti di accesso di riferimento, le seguenti informazioni e le loro variazioni, per via telematica, relative ai difensori:
 - a) nome e cognome;
 - b) luogo e data di nascita;
 - c) codice fiscale;
 - d) domicilio;
 - e) indirizzo elettronico, dichiarato e fornito dal punto di accesso;
 - f) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
 - g) stato dell'indirizzo: attivo, sospeso, non attivo;
 - h) dati identificativi del punto di accesso che fornisce il

servizio di posta elettronica;

i) stato del difensore: attivo, sospeso, cancellato, radiato; con indicazione di inizio efficacia del provvedimento e di fine efficacia nell'ipotesi di provvedimento temporaneo.

2. La comunicazione di cui al comma 1 e' sottoscritta, con firma digitale, dal presidente del consiglio dell'ordine ovvero del Consiglio nazionale forense, o da un loro delegato.

3. La comunicazione di cui al comma 1 e' strutturata in linguaggio XML, secondo il formato definito nel decreto ministeriale di cui all'art. 52.

Art. 18.

Requisiti tecnici dei registri degli indirizzi elettronici

1. Il gestore centrale ed i punti di accesso rendono disponibile una copia operativa dei propri registri degli indirizzi elettronici e mantengono l'originale inaccessibile dall'esterno.

2. Il gestore centrale ed i punti di accesso garantiscono la conformita' tra la copia operativa e l'originale dei propri registri e risolvono tempestivamente qualsiasi difformita', registrandola in un apposito giornale di controllo.

3. Le operazioni che modificano il contenuto dei registri sono consentite unicamente al personale espressamente autorizzato e sono registrate in un apposito giornale di controllo.

4. La data, l'ora e i minuti, iniziali e finali, di ogni intervallo di tempo nel quale i registri non risultano accessibili dall'esterno, oppure sono indisponibili in una loro funzionalita', sono registrate in un apposito giornale di controllo.

5. Almeno una copia dei registri e' conservata in locali di sicurezza, ubicati in luoghi diversi da quelli ove sono custoditi gli originali.

Art. 19.

Modalita' di accesso ai registri degli indirizzi elettronici

1. L'accesso ai registri degli indirizzi elettronici avviene secondo una modalita' compatibile con il protocollo LDAP, definito nella specifica pubblica RFC 1777 e successive modificazioni.

2. Il gestore centrale dell'accesso e i punti di accesso possono fornire modalita' di accesso al proprio registro aggiuntive, rispetto a quella prevista dal comma 1.

3. La struttura LDAP e' specificata nei decreti ministeriali di cui all'art. 62, comma 2.

Capo III Attivita' del SICI

Art. 20.

Funzionamento e gestione del SICI

1. La direzione generale per i sistemi informativi automatizzati del Ministero della giustizia (DGSIA) cura il funzionamento e la gestione del gestore centrale.
2. Il coordinamento interdistrettuale dei sistemi informativi automatizzati (CISIA) cura, attraverso l'amministratore di sistema, il funzionamento del gestore locale degli uffici di competenza.
3. **Il dirigente amministrativo dell'ufficio giudiziario e dell'UNEP curano e sono responsabili, per l'ufficio di propria competenza, della consistenza dei dati.**

Art. 21.

Attività del gestore centrale

1. Il gestore centrale fornisce il servizio di consultazione del SICI e il servizio di trasmissione telematica degli atti. I soggetti abilitati esterni accedono ai servizi del gestore centrale esclusivamente attraverso il proprio punto di accesso.
2. Il gestore centrale è connesso ai punti di accesso mediante canali sicuri.
3. Nelle **comunicazioni o notificazioni al difensore**, il gestore centrale controlla, mediante il registro generale degli indirizzi elettronici, la certificazione del difensore. **In caso di esito negativo del controllo, il gestore centrale inoltra la comunicazione o notifica, e trasmette all'ufficio giudiziario o all'UNEP un messaggio contenente l'esito del controllo.**
4. Il gestore centrale associa automaticamente, ad ogni documento informatico pervenuto da un punto di accesso, una attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti, che è inserita in un messaggio inviato all'indirizzo elettronico del mittente.
5. Il gestore centrale associa automaticamente, ad ogni ricevuta breve di avvenuta consegna pervenuta da un punto di accesso, una attestazione temporale, comprensiva di data, ora e minuti di ricezione del relativo documento informatico da parte del destinatario, e trasmette questi dati al gestore locale dell'ufficio giudiziario competente.
6. Il gestore centrale utilizza, per gli adempimenti di cui ai commi 4 e 5, un servizio di attestazione temporale basato, con una differenza non superiore ad un minuto primo, sulla scala di tempo UTC (IEN), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.
7. Il gestore centrale verifica l'assenza di virus informatici in ogni messaggio, in arrivo e in partenza.
8. Il gestore centrale, se riceve un messaggio privo dei dati necessari all'instradamento verso l'ufficio giudiziario o l'**UNEP**,

genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio e l'indicazione degli elementi mancanti.

9. Il gestore centrale inoltra automaticamente tutti i documenti informatici provenienti dall'esterno del SICI e diretti verso il gestore locale dell'ufficio giudiziario o dell'UNEP, ed associa la attestazione temporale.

10. Il gestore centrale fornisce un servizio di inoltro automatico di tutti i documenti informatici ricevuti dall'interno del SICI verso l'indirizzo elettronico di destinazione.

11. Il gestore centrale fornisce il servizio di conservazione di tutti i messaggi inviati e ricevuti, associati alle relative attestazioni temporali, con le modalita' previste dalla delibera CNIPA del 19 febbraio 2004, n. 11. I supporti sono inviati, con periodicit  mensile, ad un apposito centro di conservazione presso il Centro di gestione centralizzata del Ministero della giustizia, che ne assicura la conservazione per un periodo non inferiore a cinque anni.

12. Il gestore centrale esegue la certificazione del difensore, qualora non sia gi  stata compiuta dal punto d'accesso.

13. Il gestore centrale fornisce un servizio per verificare lo stato delle notifiche e delle relative ricevute brevi di avvenuta consegna.

Art. 22.

Attivit  del gestore locale

1. Il gestore locale fornisce il servizio di consultazione del sistema informatico dell'ufficio giudiziario, per i soggetti abilitati, collegati attraverso il gestore centrale.

2. Il gestore locale, mediante il sistema informatico di gestione della cancelleria, fornisce il servizio di consultazione, nei limiti dei privilegi di accesso dell'utente.

3. Il gestore locale trasmette i documenti tra i sistemi informatici dell'ufficio giudiziario o dell'**UNEP** ed il gestore centrale.

4. Il gestore locale fornisce una verifica della ricezione di tutti i documenti informatici ricevuti dal gestore centrale e delle relative attestazioni temporali.

5. Il gestore locale decifra i messaggi crittografati ricevuti, secondo le regole previste all'art. 42.

6. Il gestore locale cifra, con le modalita' di cui all'art. 43, i documenti in uscita, facenti parte del fascicolo informatico, quando sono destinati a soggetti abilitati esterni.

7. Il gestore locale verifica automaticamente, con il controllo della firma digitale, l'autenticita' e l'integrita' di ogni documento informatico ricevuto.

8. Il gestore locale verifica il rispetto dei formati e l'assenza di virus.

9. Il gestore locale rende disponibile il documento ricevuto al sistema informatico di gestione delle cancellerie civili o dell'UNEP, associandovi le informazioni dell'attivit  di verifica di cui al comma 8, per valutarne la ricevibilit .

Art. 23.

Attivit  del sistema informatico di gestione della cancelleria

1. Il sistema informatico di gestione delle cancellerie civili cura l'accettazione del documento ricevuto aggiornando il relativo registro ed il fascicolo informatico.

2. Il sistema informatico di gestione delle cancellerie civili invia, tramite il gestore locale ed il gestore centrale, all'indirizzo elettronico del mittente, una comunicazione di accettazione del documento informatico da parte della cancelleria oppure i motivi della mancata accettazione. La comunicazione contiene, se possibile, il numero di iscrizione a ruolo.

Art. 24.

Attivit  del sistema informatico di gestione dell'UNEP

1. Il sistema informatico di gestione degli UNEP acquisisce i documenti informatici da notificare, procede alla loro notifica e li restituisce con la relata di notifica.

Art. 25.

Orario di disponibilit  dei servizi

1. Il gestore centrale ed i gestori locali garantiscono la disponibilit  del servizio, nei giorni feriali, dalle ore otto alle ore ventitre', dal lunedi' al venerdi', e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 26.

Requisiti tecnici di sicurezza

1. Al gestore centrale si applicano le regole di sicurezza stabilite per il SICI e per la RUG.

2. Per il gestore locale e per il fascicolo informatico si applicano le norme sulla sicurezza previste dal decreto del Ministero della giustizia del 24 maggio 2001.

Art. 27.

Requisiti tecnici relativi all'infrastruttura di comunicazione

1. Il gestore centrale ed i gestori locali comunicano, tra loro, esclusivamente mediante la RUG.
2. Il gestore centrale utilizza l'infrastruttura tecnologica resa disponibile nell'ambito della rete unitaria della pubblica amministrazione (RUPA) per le comunicazioni con l'esterno del dominio giustizia.

Capo IV Accesso al SICI

Art. 28.

Funzionamento e gestione del punto di accesso

1. Il funzionamento e la gestione dei punti di accesso e' a carico dei soggetti pubblici o privati, in possesso dei requisiti di cui all'art. 6.

Art. 29.

Funzionalità del punto di accesso

1. Il punto di accesso fornisce ai soggetti abilitati esterni i servizi di consultazione del SICI e di trasmissione telematica degli atti.
2. Il punto di accesso fornisce il servizio di autenticazione dei soggetti abilitati, per l'accesso al SICI. Il punto di accesso, gestito dal consiglio dell'ordine degli avvocati di appartenenza o dal Consiglio nazionale forense, con l'autenticazione del difensore, esegue la certificazione di cui all'art. 7.
3. La comunicazione tra la postazione informatica del soggetto abilitato esterno e il punto di accesso avviene mediante canale sicuro.
4. Il punto di accesso mantiene in linea i documenti informatici inviati fino a quando non riceve un avviso di consegna dal gestore centrale o dal punto di accesso di destinazione.
5. Il punto di accesso fornisce il servizio di ricezione, inviando, in risposta ad ogni documento informatico ricevuto dal gestore centrale o da un altro punto di accesso, una ricevuta breve di avvenuta consegna.
6. Il punto di accesso verifica l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.
7. Il punto di accesso garantisce, per un periodo non inferiore a cinque anni, la conservazione di tutti i messaggi inviati e ricevuti.
8. Il punto di accesso fornisce il servizio di distribuzione del software, fornito come prototipo dal Ministero della giustizia, per la redazione dei documenti informatici in formato XML.

Art. 30.

Requisiti tecnici del punto di accesso

1. L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche previste dalla carta nazionale dei servizi.
2. I punti di accesso stabiliscono le connessioni con il gestore centrale esclusivamente mediante un collegamento diretto alla RUPA, autorizzato dal CNIPA.
3. Ciascun punto di accesso stabilisce con il gestore centrale un canale sicuro di comunicazione, che consente la reciproca autenticazione e riservatezza.
4. Il punto di accesso garantisce un livello di disponibilit  del servizio pari al 99,5 per cento, su base quadrimestrale, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.
5. Le procedure per la fornitura dei servizi attuate dal punto di accesso sono dettagliatamente documentate sul manuale operativo, previsto dall'art. 33.
6. Tutte le azioni e le procedure di sicurezza attivate dal punto di accesso sono dettagliatamente documentate nel piano per la sicurezza, previsto dall'art. 34.
7. La frequenza di salvataggio dei dati e' almeno giornaliera.
8. Gli eventi significativi nel funzionamento del punto di accesso, sono registrati sul giornale di controllo, di cui all'art. 35.
9. I canali di autenticazione del presente regolamento sono in SSL versione 3, con chiave a 1024 bit.

Art. 31.

Elenco pubblico dei punti di accesso

1. L'elenco pubblico dei punti di accesso, attivo presso il Ministero della giustizia, comprende le seguenti informazioni:
 - a) identificativo del punto di accesso;
 - b) sede legale del soggetto titolare del punto di accesso;
 - c) nome secondo lo standard X.500;
 - d) indirizzo Internet;
 - e) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo elettronico, numero di telefono e di fax;
 - f) elenco dei numeri telefonici di accesso;
 - g) manuale operativo;
 - h) data di cessazione dell'attivit .

Art. 32.

Iscrizione nell'elenco pubblico dei punti di accesso

1. Il soggetto che intende costituire un punto di accesso inoltra,

alla DGSIA, domanda di iscrizione nell'elenco pubblico dei punti di accesso.

2. Alla domanda sono allegati le dichiarazioni di:

- a) possesso dei requisiti di cui all'art. 6;
- b) attestazione di affidabilità organizzativa e tecnica necessaria per svolgere il servizio di punto di accesso;
- c) attestazione relativa all'impiego di personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti;
- d) obbligo di fornirsi di: manuale operativo, piano per la sicurezza e giornale di controllo, secondo quanto previsto dagli articoli 33, 34 e 35;
- e) obbligo di garantire la sicurezza e l'integrità del servizio e dei dati di propria competenza;
- f) obbligo di compiere il processo di autenticazione dei soggetti abilitati ad esso afferenti, su mandato del Ministero della giustizia, conformemente all'art. 30, comma 1;
- g) obbligo di comunicare, al Ministero della giustizia, la data di cessazione del servizio, con preavviso di sei mesi;
- h) informazione dei dati di cui all'art. 31.

3. 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.

4. Con il provvedimento di cui al comma 3, il Ministero della giustizia delega la responsabilità del processo di autenticazione dei soggetti abilitati esterni al punto di accesso.

5. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso, di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'art. 6, comma 3.

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 responsabilita' e delle eventuali limitazioni agli indennizzi;
 - f) tariffe;
 - g) modalita' di autenticazione, registrazione e gestione degli utenti;
 - h) modalita' di attivazione e gestione degli indirizzi elettronici;
 - i) modalita' di gestione del registro degli indirizzi elettronici;
 - j) modalita' 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 il piano per la sicurezza che contiene almeno i seguenti elementi:
 - a) struttura generale, modalita' 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 responsabilita';
 - f) descrizione delle procedure utilizzate nell'attivita' 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 e' conforme a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, e puo' essere adottato unitamente al documento programmatico per la sicurezza previsto dall'art. 34, comma 1, lettera g), del medesimo decreto legislativo.

Art. 35.

Giornale di controllo

1. Il punto di accesso attiva il giornale di controllo, contenente l'insieme delle registrazioni effettuate automaticamente allorché si verificano le condizioni previste dal presente decreto.
2. Le registrazioni possono essere effettuate in modo indipendente, anche su distinti supporti e di diverso tipo.
3. La registrazione associa la data, l'ora e i minuti in cui è effettuata.
4. 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.
5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo sono archiviate con le modalità previste dal presente decreto e conservate per un periodo non inferiore a cinque anni.

Art. 36.

Postazioni di lavoro dei soggetti abilitati esterni

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 formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del SICI.
2. La postazione di lavoro dei soggetti abilitati esterni è dotata

dell'hardware e del software necessario alla gestione della firma digitale su smartcard, e all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi.

3. La postazione di lavoro dei soggetti abilitati esterni è dotata di software idoneo a verificare l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

Capo V Trasmissione di documenti informatici tra il SICI ed entità esterne

Art. 37.

Principi normativi

1. Nella trasmissione di documenti informatici nell'ambito del processo civile, trovano applicazione tutte le prescrizioni contenute nel decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nel decreto legislativo 23 gennaio 2002, n. 10, e successive modificazioni.
2. I documenti informatici prodotti nel processo civile sono sottoscritti con firma digitale, nei casi previsti dall'art. 4, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n.123.

Art. 38.

Ricezione del documento informatico

1. Il documento informatico inviato da un soggetto abilitato esterno e' ricevuto dal SICI nel momento in cui il gestore centrale lo accetta e associa l'attestazione temporale di cui all'art. 21, comma 4.
2. Il documento informatico inviato da un soggetto abilitato interno e' ricevuto, dal soggetto abilitato esterno, nel momento in cui il gestore centrale riceve la ricevuta breve di avvenuta consegna relativa al documento e associa l'attestazione temporale di cui all'art. 21, comma 5.

Art. 39.

Orario dei servizi telematici di cancelleria

1. Il SICI fornisce i servizi telematici di cancelleria, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

Art. 40.

Iscrizione a ruolo generale

1. Il sistema informatico dell'ufficio giudiziario invia al difensore, che iscrive la causa a ruolo per via telematica, una comunicazione, recante il numero di ruolo del procedimento assegnato dall'ufficio.

Art. 41.

Dimensione del messaggio

1. La dimensione massima del messaggio e' di 10 Mb.

Art. 42.

Crittografia del messaggio

1. Al fine della riservatezza del documento da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia basato sulla chiave pubblica del gestore locale cui e' destinato il messaggio.
2. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato A del presente decreto.
3. Le chiavi pubbliche dei gestori locali sono pubblicate in un registro del gestore centrale dell'accesso.
4. Il registro di cui al comma 3 e' accessibile in modalita' LDAP.

Art. 43.

Trasmissione e consultazione dei fascicoli

1. Nel caso di richiesta di trasmissione o di consultazione, totale o parziale, di un fascicolo, il gestore locale, per garantire la riservatezza della comunicazione, utilizza un meccanismo di crittografia basato sulla chiave pubblica di cifratura del soggetto abilitato esterno di destinazione.
2. Nel caso di richiesta di copia conforme del fascicolo, totale o parziale, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.
3. Le chiavi pubbliche dei soggetti abilitati esterni sono disponibili nel registro generale degli indirizzi di cui all'art. 13.
4. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato A, del presente decreto.

Art. 44.

Trasmissione delle sentenze

1. L'originale della sentenza, redatta in formato elettronico dal giudice estensore o, ai sensi dell'art. 119 delle norme di attuazione del codice di procedura civile, dal cancelliere o dal dattilografo da questi incaricato, è sottoscritta con firma digitale dall'estensore, previa verifica della conformità dell'originale alla minuta.
2. In caso di giudice collegiale, l'originale della sentenza è sottoscritto con firma digitale anche dal presidente e, a tal fine, la sentenza gli è trasmessa, in formato elettronico, dal giudice estensore o dal cancelliere.
3. Il cancelliere attesta il deposito della sentenza apponendo la data e sottoscrivendo la sentenza con la propria firma digitale.

Art. 45.

Comunicazioni e notificazioni

1. La comunicazione per via telematica di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno avviene mediante inoltro del documento dal **gestore locale** al gestore centrale, che lo invia alla CPECPT del destinatario.
3. La notificazione telematica di documenti informatici tra difensori avviene, ove sussistano i presupposti di cui alla legge 21 gennaio 1994, n. 53, mediante inoltro del documento dal punto di accesso del mittente alla CPECPT del destinatario. A tale scopo il punto di accesso trasmette il messaggio con il documento da notificare al gestore centrale che, a sua volta, inoltra il messaggio ricevuto al punto di accesso di destinazione.
3. **Le richieste di un'attività di notifica telematica da parte di un ufficio giudiziario sono inoltrate, mediante la RUG, al sistema informatico dell'UNEP. Le richieste dei difensori sono inoltrate**

all'UNEP per il tramite del punto di accesso del mittente e del gestore centrale, nel rispetto dei requisiti dei documenti informatici provenienti dall'esterno. La notificazione di documenti informatici da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da ufficio giudiziario verso soggetti abilitati esterni.

4. Il sistema informatico dell'UNEP, eseguita la notifica, trasmette per via telematica, a chi ha richiesto il servizio, il documento informatico con la relata di notifica, costituita dalla ricevuta elettronica, sottoscritta dall'ufficiale giudiziario con firma digitale.

5. Nell'ipotesi di cui all'art. 6, comma 3, del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, **l'ufficiale giudiziario provvede a notificare il duplicato del documento informatico, su supporto ottico non riscrivibile.**

6. La consegna del documento informatico alla CPECPT del soggetto abilitato esterno e' assicurata dai punti di accesso mediante l'invio al mittente di una ricevuta breve di avvenuta consegna.

7. Il gestore centrale, nella trasmissione di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno, associa automaticamente ad ogni ricevuta breve di avvenuta consegna una attestazione temporale contenente data, ora e minuti della ricezione che inoltra al gestore locale per l'inserimento nel fascicolo informatico.

8. Nelle notifiche tra difensori, il gestore centrale, ricevuto dal mittente il messaggio da notificare, associa automaticamente ad esso una prima attestazione temporale, che viene spedita alla CPECPT del mittente e, unitamente al messaggio, alla CPECPT del destinatario. La CPECPT del destinatario, ricevuto il messaggio, invia al gestore centrale la ricevuta breve di avvenuta consegna; il gestore centrale associa a quest'ultima una seconda attestazione temporale, che viene spedita alla CPECPT del destinatario e, unitamente alla ricevuta breve di avvenuta consegna, alla CPECPT del mittente.

Capo VI Pagamenti

Art. 46.

Pagamenti

1. I pagamenti per via telematica, relativi agli atti giudiziari, si effettuano mediante il modello definito dal Ministero dell'economia e delle finanze.

2. Il pagamento puo' anche avvenire nelle forme di cui all'art. 1 del decreto del Presidente della Repubblica del 1° marzo 2001, n. 126.

3. Gli estremi del pagamento sono allegati alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio giudiziario.

4. Se il pagamento e' effettuato a norma del comma 2 e con sistemi non telematici, l'originale cartaceo dell'attestazione di pagamento deve, in ogni caso, essere presentato per la prima udienza.

Art. 47.

Diritto di copia

1. Il difensore nella richiesta di copia puo' chiedere l'indicazione dell'importo del diritto corrispondente che gli e' comunicato, senza ritardo, dall'ufficio giudiziario.
2. Alla richiesta di copia e' associato un numero identificativo che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel fascicolo informatico per consentire il versamento secondo le modalita' previste dal decreto del Presidente della Repubblica 1° marzo 2001, n. 126.

Art. 48.

Registrazione, trascrizione e voltura degli atti

1. La registrazione, la trascrizione e la voltura degli atti avvengono, in via telematica, nelle forme previste dall'art. 73 del decreto del Presidente della Repubblica 30 maggio 2002, n. 115.

Art. 49.

Pagamento dei diritti di notifica

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'art. 46.
2. **L'UNEP rende pubblici, attraverso il gestore locale dell'ufficio, gli importi dovuti a titolo di anticipazione. Eseguita la notifica, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previa definizione del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.**

Capo VII Archiviazione e conservazione delle informazioni

Art. 50.

Gestione del fascicolo informatico

1. Il sistema di gestione del fascicolo informatico e' la parte del sistema dell'ufficio giudiziario dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno dell'ufficio giudiziario.
2. Il fascicolo informatico contiene i documenti informatici e le relative informazioni quali: allegati, ricevute brevi di avvenuta consegna e attestazioni temporali.

Art. 51.

Archiviazione e conservazione dei documenti informatici degli uffici giudiziari e degli **UNEP**

1. I fascicoli informatici relativi ai procedimenti in corso sono archiviati, per tutta la durata del procedimento, nell'archivio in linea dell'ufficio giudiziario, secondo le modalita' previste dal decreto ministeriale del 24 maggio 2001 e dal decreto legislativo 30 giugno 2003, n. 196.

2. I fascicoli informatici relativi ai procedimenti esauriti sono soggetti a conservazione, presso il competente ufficio giudiziario, secondo le modalita' previste dalla deliberazione del CNIPA del 19 febbraio 2004, n. 11, per il periodo previsto dall'art. 41 del decreto legislativo 22 gennaio 2004, n. 42, fatte salve le operazioni di scarto ivi previste.

3. I documenti informatici degli **UNEP** sono soggetti a conservazione, presso il competente ufficio, secondo le modalita' e termini di cui al comma 2.

Capo VIII Standard e modelli di riferimento

Art. 52.

Formato dei documenti informatici

1. Gli atti del processo in forma di documenti informatici sono redatti in formato XML, le cui specifiche tecniche sono determinate a norma dell'art. 62, comma 2.

Art. 53.

Formato dei documenti informatici allegati

1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, ed hanno i seguenti formati: .pdf, .rtf, .txt, .jpg, .gif, .tiff, .xml.

2. E' consentito l'utilizzo dei formati compressi .zip, .rar. e .arj, purché contenenti file nei formati previsti dal comma precedente.

Art. 54.

Documenti probatori e allegati non informatici

1. I documenti probatori e gli allegati depositati in formato non elettronico, sono identificati e descritti in una apposita sezione del documento informatico, secondo la definizione del modello DTD (Document Type Definition) e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati: numero di ruolo della causa, progressivo dell'allegato e indicazione della prima udienza successiva al deposito.

Art. 55.

Servizio di posta elettronica

1. Il servizio di posta elettronica utilizzato dal gestore centrale dell'accesso e dai punti di accesso e' conforme agli standard dei sistemi di posta elettronica compatibili con il protocollo di trasporto SMTP ed il formato dei messaggi S/MIME.

Art. 56.

Modelli di documenti informatici prodotti dai difensori

1. I modelli dei documenti informatici prodotti dai difensori, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

- a) atto introduttivo (citazione, ricorso, ricorso cautelare, ricorso per decreto ingiuntivo);
- b) nota di iscrizione a ruolo;
- c) comparsa di costituzione e risposta con eventuale domanda riconvenzionale ed eventuale richiesta di rinvio della prima udienza per la chiamata in causa del terzo;
- d) deduzioni istruttorie a norma dell'art. 184 del codice di procedura civile;
- e) note autorizzate ex art. 183, comma 5, del codice di procedura civile;
- f) memorie autorizzate;
- g) chiamata in causa del terzo;
- h) istanza;
- i) reclamo;
- j) atti conclusivi (comparsa conclusionale, memoria di replica);
- k) atto di pignoramento;
- l) atto di intervento nell'esecuzione;
- m) osservazioni al progetto di distribuzione;
- n) istanza di fallimento;
- o) istanza di insinuazione al passivo;
- p) ricorso per insinuazione tardiva;
- q) ricorso per opposizione allo stato passivo;
- r) istanza di ammissione alla procedura di amministrazione controllata;
- s) istanza di ammissione alla procedura di concordato preventivo;
- t) istanza di concordato fallimentare;
- u) dichiarazione di voto nelle procedure di amministrazione controllata o di concordato;
- v) delega rilasciata ai sensi dell'art. 9 del regio decreto legislativo 27 novembre 1933, n. 1578.

Art. 57.

Modelli di documenti informatici prodotti dalla cancelleria

1. I modelli dei documenti informatici prodotti dalla cancelleria,

riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

- a) verbale di udienza;
- b) biglietto di cancelleria;
- c) richiesta di notifica;
- d) richiesta di informazione o ordine di esibizione.

Art. 58.

Modelli di documenti informatici prodotti dal giudice

1. I modelli dei documenti informatici prodotti dal giudice, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

- a) provvedimento (sentenza, ordinanza, decreto);
- b) dispositivo sentenza;
- c) verbale di conciliazione.

Art. 59.

Modelli di documenti informatici prodotti dal consulente tecnico di ufficio

1. I modelli dei documenti informatici prodotti dal consulente tecnico di ufficio, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:

- a) modello generico di consulenza;
- b) stima di beni mobili;
- c) stima di beni immobili;
- d) stima di azienda.

Art. 60.

Modelli di documenti informatici prodotti dall'UNEP

1. Il modello dei documenti informatici prodotti dall'UNEP, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi al seguente atto: **relata di notifica**.

Capo IX Disposizioni finali e transitorie

Art. 61.

Adeguamento delle regole tecnico-operative

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 62.

Disposizioni transitorie

1. L'attivazione del processo telematico e' preceduta da un decreto dirigenziale, che accerta l'installazione e l'idoneita' delle

attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.

2. Le caratteristiche specifiche della strutturazione dei modelli DTD (Document Type Definition) saranno pubblicate, con uno o più decreti ministeriali, entro 180 giorni dalla data di entrata in vigore del presente decreto.

3. Fino all'entrata in vigore delle regole tecniche relative alla carta nazionale dei servizi, l'autenticazione dei soggetti abilitati esterni avviene mediante dispositivo di crittografia contenente al suo interno un certificato di autenticazione e la corrispondente chiave privata protetta da PIN. La chiave privata, lunga almeno 1024 bit e generata all'interno del dispositivo crittografico, non deve essere estraibile dal dispositivo stesso.

4. L'art. 22, comma 6, e l'art. 43, comma 1, hanno efficacia a decorrere da sei mesi dalla data di entrata in vigore del presente decreto.

Roma, 14 ottobre 2004

Il Ministro: Castelli

Allegato A

----> in corso di inserimento <----

Allegato B

----> in corso di inserimento <----