Specifiche tecniche Digsia 16-4-2014 (gu 30 aprile 2014)

Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24

Direzione generale per i sistemi informativi automatizzati
Il responsabile per i sistemi informativi automatizzati

Visto il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44 (pubblicato sulla Gazzetta Ufficiale n. 89 del 18 aprile 2011), recante “Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell’articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24”, come modificato dal decreto ministeriale 15 ottobre 2012 n. 209 e dal decreto ministeriale 3 aprile 2013 n. 48;

Visto il decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221 e successivamente modificato dalla legge 24 dicembre 2012, n. 228;

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;

Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della L. 16 gennaio 2003, n. 3»;

Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2013;

Visto il decreto ministeriale 27 aprile 2009, recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»;

Rilevata la necessità di aggiornare le specifiche tecniche previste dall’articolo 34, comma 1, del citato decreto ministeriale 21 febbraio 2011, n. 44;

Acquisito il parere espresso in data 23 dicembre 2013 dal Garante per la protezione dei dati personali;

Acquisito il parere espresso in data 4 febbraio 2014 dall’Agenzia per l’Italia Digitale;

EMANA
IL SEGUENTE PROVVEDIMENTO:

Specifiche tecniche Digsia 16-4-2014 (gu 30 aprile 2014)

CAPO I – PRINCIPI GENERALI

Art. 1 Ambito di applicazione

Il presente provvedimento stabilisce le specifiche tecniche previste dall’articolo 34, comma 1, del regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell’articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24.

Art. 2 Definizioni

Ai fini del presente provvedimento, oltre alle definizioni contenute nell’articolo 2 del regolamento, si intende:
regolamento: il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, portante “Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell’articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24” e successive modificazioni;
CAD: codice dell’amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale” e successive modificazioni);
CNS: Carta Nazionale dei Servizi;
CSV: Comma-separated values;
DTD: Document Type Definition;
DGSIA: Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia;
GSU: Sistema di gestione informatizzata dei registri per gli uffici notifiche e protesti;
HSM: Hardware Security Module;
HTTPS: HyperText Transfer Protocol over Secure Socket Layer;
IMAP: Internet Message Access Protocol;
PdA: Punto di Accesso, come definito all’art. 23 del regolamento;
PEC: Posta Elettronica Certificata;
POP: Post Office Protocol;
PP.AA.: Pubbliche Amministrazioni;
RdA: Ricevuta di Accettazione della Posta Elettronica Certificata;
RdAC: Ricevuta di Avvenuta Consegna della Posta Elettronica Certificata;
ReGIndE: Registro Generale degli Indirizzi Elettronici, come definito all’art. 7 del regolamento;
SMTP: Simple Mail Transfer Protocol;
UU.GG.: Uffici Giudiziari;
WSDL: Web Services Definition Language;
XML; eXtensible Markup Language;
XSD: XML Schema Definition;
SPC: Sistema Pubblico di Connettività;
PKCS#11: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite apposita sequenza di chiamate al token per mezzo dell’interfaccia PKCS#11 è possibile implementare la procedura di identificazione;

CAdES (CMS Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 e basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni;
PAdES (PDF Advanced Electronic Signature): formato di busta crit-tografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;
OID (Object IDentifier): codice univoco basato su una sequenza ordi-nata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale;
Autenticazione a due fattori: metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia che combina un'informazione nota (ad esempio un nome utente e una password) con un oggetto a disposizione (ad esempio, una carta di credito, token o telefono cellulare).

CAPO II – SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Art. 3 Infrastrutture informatiche – art. 3 del regolamento

Il sistema informatico del Ministero della giustizia è articolato, salvo le infrastrutture unitarie e comuni, a livello nazionale, interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale (di circondario).
Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.
Il sistema di posta elettronica certificata è gestito dal fornitore presso la propria sala server, collegata ad SPC secondo le relative regole di interoperabilità e sicurezza, oppure presso una sala server del Ministero della giustizia.
Il dispiegamento di detti sistemi rispetta le disposizioni di cui al decreto del Ministro della giustizia in data 27 aprile 2009, recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".
Il Direttore Generale S.I.A. emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico, sentito il Garante per la protezione dei dati personali. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul sito internet dell'Amministrazione.
Le strutture elaborative serventi ed i dati sono allocati in corrispondenza delle componenti di cui ai commi precedenti.

Art. 4 Gestore della posta elettronica certificata del Ministero della giustizia – art. 4 del regolamento

Il Ministero della giustizia si avvale del proprio gestore di posta elettronica certificata, che rilascia e gestisce apposite caselle di PEC degli uffici giudiziari e degli UNEP da utilizzare esclusivamente per i servizi previsti dal regolamento, nel rispetto delle specifiche tecniche riportate nel presente provvedimento.
Le caselle appartengono ad apposito sotto-dominio (civi-le.ptel.giustiziacert.it e

penale.ptel.giustiziacert.it) e possono ricevere unicamente messaggi di posta elettronica certificata. I messaggi di posta elettronica ordinaria vengono automaticamente scartati.
Il gestore dei servizi telematici utilizza i protocolli POP3, POP3S, IMAP, IMAPS e SMTP per collegarsi al gestore di posta elettronica certificata del Ministero.
La codifica dei singoli uffici, comprensiva del relativo indirizzo di PEC, è contenuta nel catalogo dei servizi telematici di cui all'articolo 5, comma 3.
Non possono essere utilizzate caselle di PEC diverse da quelle di cui ai commi precedenti per la trasmissione e il deposito di atti processuali.
Il Ministero della giustizia conserva il log dei messaggi, transitati attraverso il proprio gestore di posta elettronica certificata, per cinque anni. A tal fine, il gestore di PEC del Ministero invia giornalmente, a una casella di posta di sistema, il log in formato CSV. Il log, sottoscritto con firma digitale o firma elettronica qualificata, è relativo a tutti gli indirizzi del sotto-dominio delle caselle del processo telematico e contiene tutti gli eventi relativi ai messaggi pervenuti, conservando le seguenti informazioni:
il codice identificativo univoco assegnato al messaggio originale;
la data e l'ora dell'evento;
il mittente del messaggio originale;
i destinatari del messaggio originale;
l'oggetto del messaggio originale;
il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
il gestore mittente.
Un apposito modulo nell'ambito del portale dei servizi telematici comprende i componenti funzionali necessari per l'acquisizione, il salvataggio e l'interrogazione dei log prodotti dal servizio di PEC.
I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.
Le comunicazioni di atti e documenti tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria nella fase delle indagini preliminari, avvengono mediante i gestori di posta elettronica certificata delle forze di polizia, le cui caselle sono rese disponibili unicamente agli utenti abilitati; in questo caso il gestore dei servizi telematici utilizza un canale sicuro protetto da un meccanismo di crittografia ai sensi di quanto previsto dall'articolo 20.

Art. 5 Portale dei servizi telematici – art. 6 del regolamento

Il portale dei servizi telematici è accessibile all'indirizzo http://pst.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".
L'"area pubblica", denominata "Servizi online Uffici Giudiziari", è composta da tutte le pagine web e i servizi del portale disponibili ad accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione; in essa sono disponibili le seguenti tipologie d'informazione:
Informazioni e documentazione sui servizi telematici del dominio giustizia;
Raccolte giurisprudenziali;
Informazioni essenziali sullo stato dei procedimenti pendenti, rese di-sponibili in forma anonima; in questo caso, i parametri e i risultati di ricerca riportano unicamente i dati identificativi dei procedimenti (numero di ruolo, numero di sentenza, ecc.), senza riferimenti in chiaro ai nomi o ai dati personali delle parti e tali per cui non sia possibile risalire all'identità dell'interessato. Il

canale di comunicazione per l’accesso a tali informazioni è cifrato (HTTPS).
Nell’area pubblica è consultabile il catalogo dei servizi telematici, che si compone di una serie di file aventi lo scopo di censire, in forma strutturata, tutte le informazioni relative ai servizi telematici, secondo gli XSD di cui all’Allegato 10.
Per “area riservata” s’intende il contenitore di tutte le pagine e i servizi del portale disponibili previa identificazione informatica, come disciplinata dall’articolo 6.
Nell’area riservata sono disponibili informazioni, dati e provvedimenti giudiziari in formato elettronico, secondo quanto previsto all’art. 27 del regolamento, nonché i servizi di pagamento telematico e di richiesta copie.

Art. 6 Identificazione informatica – art. 6 del regolamento

L’identificazione informatica per i soggetti abilitati esterni e gli utenti privati avviene sul portale dei servizi telematici mediante carta d'identità elettronica o carta nazionale dei servizi e sul punto di accesso mediante autenticazione a due fattori oppure tramite token crittografico (smart card, chiavetta USB o altro dispositivo sicuro) in conformità all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82; in caso si utilizzi il token crittografico, l’identificazione avviene nel rispetto dei seguenti requisiti:
Il certificato deve essere rilasciato da un certificatore accreditato dall’Agenzia per l’Italia Digitale ai sensi dell'art 29 del CAD, che si fa garante dell’identità del soggetto.
Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all’Appendice 1 del documento rilasciato dal CNIPA: “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”. L’estensione Certificate Policy (2.5.29.32) può essere valorizzata con un Object Identifier (OID) definito dalla CA.
In termini di sicurezza, i dispositivi ammessi sono i dispositivi personali consentiti per la firma elettronica qualificata e quindi smart card e token USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criteria EAL4+ con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie.
In termini d’interoperabilità, sono ammissibili dispositivi che consentano la disponibilità di entrambe le interfacce PKCS#11 e CSP; in particolare, entrambe le interfacce devono consentire l’accesso alla procedura d’identificazione forte mediante digitazione del PIN da parte dell’utente; il dispositivo deve inoltre rispettare la strutturazione del file system come da specifiche CNS.
In fase di identificazione tramite token crittografico, il punto di accesso o il portale dei servizi telematici verifica la validità del certificato presente nel token crittografico utilizzato dall’utente che accede; prima di consentire qualunque operazione, inoltre, il punto di accesso verifica che il token crittografico sia collegato alla postazione; in caso contrario, invalida e termina la sessione.
Il Ministero della giustizia verifica, anche attraverso opportune visite ispettive, che i punti di accesso rispettino i predetti requisiti.
La violazione di queste regole di sicurezza comporta per il punto di accesso la sospensione dell’autorizzazione a erogare i servizi, fino al definitivo rispetto dei requisiti.
L’identificazione informatica per i soggetti abilitati interni avviene ai sensi dell’articolo 10.

Art. 7 Registro generale degli indirizzi elettronici – art. 7 del regolamento

Il Registro Generale degli Indirizzi Elettronici (ReGIndE) è gestito dal Ministero della giustizia e contiene i dati identificativi nonché l’indirizzo di PEC dei soggetti abilitati esterni.

Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al presente regolamento.
I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l'inserimento manuale dei dati.
Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:
soggetti appartenenti ad un ente pubblico che svolgano uno specifico ruolo nell'ambito di procedimenti (ad esempio avvocati e funzionari dell'INPS e dell'Avvocatura dello Stato, avvocati e funzionari delle PP.AA.);
professionisti iscritti in albi ed elenchi istituiti con legge (ad esempio Consiglio dell'ordine degli avvocati o Consiglio nazionale del Notariato);
professionisti non iscritti ad alcun albo: tutti i soggetti nominati dal giudice come consulenti tecnici d'ufficio – o più in generale ausiliari del giudice – non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (ad eccezione degli avvocati).
Il ReGIndE non gestisce informazioni già presenti in registri disponibili alle PP.AA., qualora questi siano accessibili in via telematica ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008 n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009 n. 2, il cui contenuto occorre ai sistemi del dominio Giustizia; da tali registri – tra cui il registro delle imprese, l'indice nazionale delle imprese e dei professionisti (INI-PEC), l'anagrafe nazionale della popolazione residente (ANPR) e il domicilio digitale del cittadino di cui all'art 3-bis del CAD – sono recuperati gli indirizzi di PEC dei professionisti e delle imprese, nonché gli indirizzi dei cittadini ivi censiti.
Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.
Il ReGIndE è consultabile dai soggetti abilitati esterni tramite il proprio punto di accesso o tramite il Portale dei Servizi Telematici, su connessioni sicure (SSL v3), attraverso un apposito web service; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici.
Art. 8
Alimentazione del registro generale degli indirizzi elettronici – art. 7 del regolamento

L'alimentazione del ReGIndE avviene previo invio al responsabile per i sistemi informativi automatizzati di un documento di censimento contenente le informazioni necessarie ad identificare:
l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;
il nominativo e il codice fiscale del delegato all'invio dell'albo, che dovrà sottoscrivere con firma digitale o firma elettronica qualificata l'albo in trasmissione;
la casella di PEC utilizzata per l'invio dell'albo.
Il documento di censimento di cui al comma precedente aderisce al modello reperibile nell'area pubblica del portale e viene inviato all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: Questo indirizzo email è protetto dagli spambots. È necessario abilitare JavaScript per vederlo..
Terminate le operazioni di censimento da parte del responsabile per i si-stemi informativi automatizzati, l'ente mittente del documento di censimento riceve una risposta; in caso di esito positivo, l'ente può procedere all'invio dell'albo secondo le seguenti specifiche:
il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;
non vi sono vincoli sull'oggetto né sul corpo del messaggio;

l’indirizzo di PEC mittente deve essere censito tra quelli delegati all’invio e riportati nel documento di censimento;
deve essere allegato un solo file (ComunicazioniSoggetti.xml o, per le Pubbliche Amministrazioni, ComunicazioneSoggettiPPAA.xml), sotto-scritto con firma digitale o firma elettronica qualificata;
la firma digitale o firma elettronica qualificata deve appartenere al soggetto delegato di cui al comma 1, lettera b, sulla base del codice fiscale censito;
il file ComunicazioniSoggetti.xml o il file ComunicazioneSogget-tiPP.AA.xml deve essere conforme all’XML-Schema di cui all’Allegato 2;
il codice ente specificato nel file deve essere tra quelli censiti.
Il mancato rispetto di uno o più dei vincoli di cui all’articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l’allegato ComunicazioniSoggetti.xml viene scartato.
A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso “– Esito” e riporta in allegato l’esito dell’elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell’Allegato 3.
L’esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come ad esempio codice fiscale inesistente), sia ad errori legati a vincoli e prerequisiti che presuppongono la validità dell’invio di un albo (ad esempio: censimento dell’ente richiedente e dei soggetti abilitati all’invio dell’albo).
Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell’inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di PEC di cortesia in cui si attesta l’avvenuta registrazione.

Art. 9 Professionisti non iscritti in albi – art. 7 del regolamento

I professionisti non iscritti all’albo, oppure per i quali il proprio ordine di appartenenza non abbia provveduto all’invio di copia dell’albo (ad eccezione degli avvocati), si registrano al ReGIndE attraverso un Punto di Accesso (PdA) o attraverso il Portale dei Servizi Telematici, previa identificazione, effettuando altresì l’inserimento (upload) del file che contiene copia informatica, in formato PDF, dell’incarico di nomina da parte del giudice; tale file è sottoscritto con firma digitale o firma elettronica qualificata dal soggetto che intende iscriversi.
Il PdA provvede a trasmettere l’avvenuta registrazione con le medesime modalità di cui all’articolo precedente, con la differenza che il file ComunicazioniSoggetti.xml è digitalmente sottoscritto con firma digitale o firma elettronica qualificata dal PdA.
Qualora il professionista di cui al comma 1 s’iscriva ad un albo, oppure pervenga copia dell’albo da parte dell’ordine di appartenenza, prevalgono i dati trasmessi dall’ordine stesso; in questo caso il sistema cancella la prima iscrizione e invia un messaggio PEC di cortesia al professionista.

Art. 9 bis Indirizzi di posta elettronica certificata delle pubbliche amministrazioni

La pubblica amministrazione che deve comunicare il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni, ai sensi dell’articolo 16, comma 12, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, procede inserendo tale indirizzo sul portale dei servizi telematici.

Ai fini di cui al comma precedente, la pubblica amministrazione invia all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati (Questo indirizzo email è protetto dagli spambots. È necessario abilitare JavaScript per vederlo.) un documento contenente le seguenti informazioni:
descrizione e codice fiscale della pubblica amministrazione;
nominativo, codice fiscale e recapiti del soggetto incaricato di inserire o modificare gli indirizzi di PEC della pubblica amministrazione sul portale dei servizi telematici;
Il soggetto incaricato di cui al comma precedente accede ad un'apposita area riservata del portale dei servizi telematici, previa identificazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica:
l'indirizzo di PEC della pubblica amministrazione;
il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti tramite i quali la pubblica amministrazione sta in giudizio personalmente; tali soggetti alimentano il Registro Generale degli Indirizzi Elettronici.
L'elenco degli indirizzi di PEC delle pubbliche amministrazioni è consultabile dagli uffici giudiziari e dagli uffici NEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni.
L'elenco degli indirizzi di PEC di cui al comma 3, lettera a, è consultabile dagli avvocati tramite il proprio punto di accesso o tramite il portale dei servizi telematici (area riservata), su connessioni sicure (SSL v3), attraverso un apposito web service, che verifica la presenza dell'avvocato sul ReGIndE; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici. L'accesso è tracciato in appositi log, che il Ministero della giustizia conserva per cinque anni, recanti: il punto di accesso attraverso cui è stato effettuato l'accesso, la data e l'ora dell'accesso.

Art. 10 Sistemi informatici per i soggetti abilitati interni – art. 8 del regolamento

I sistemi informatici a disposizione dei soggetti abilitati interni sono conformi alle regole di cui al D.M. 27 aprile 2009 e mettono a disposizione le funzioni relative a:
ricezione, accettazione e trasmissione dei dati e dei documenti informatici;
consultazione e gestione del fascicolo informatico.
Per l'accesso ai sistemi di cui al comma precedente dall'interno degli uffici giudiziari, l'identificazione è effettuata mediante coppia di credenziali "nome utente/password" oppure mediante autenticazione a due fattori.
Per l'accesso ai sistemi di cui al comma 1 dall'esterno della Rete Giustizia, l'identificazione è effettuata dal portale dei servizi telematici sulla base del sistema "Active Directory Nazionale" (ADN) tramite autenticazione a due fattori; ai soli fini del recupero dall'esterno delle informazioni di registro da parte dei sistemi a disposizione dei magistrati in ambito civile, è sufficiente l'identificazione sulla base del sistema ADN purché l'interrogazione dei dati finalizzati al recupero preveda l'indicazione del numero di ruolo generale nonché del codice fiscale dell'attore principale e del convenuto principale del procedimento.

Art. 11 Fascicolo informatico – art. 9 del regolamento

Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.

Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutti i metodi – esposti attraverso appositi web service – necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione.
Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:
il codice fiscale del soggetto che ha effettuato l'accesso;
il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);
la data e l'ora dell'accesso.
Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni.

CAPO III – TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Art. 12 Formato dell'atto del processo in forma di documento informatico – art. 11 del regolamento

L'atto del processo in forma di documento informatico, da depositare telematicamente all'ufficio giudiziario, rispetta i seguenti requisiti:
è in formato PDF;
è privo di elementi attivi;
è ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;
è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata.
La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CA-dES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo "firme multiple indipendenti" o parallele, e prevede che uno o più soggetti firmino, ognuno con la propria chiave privata, lo stesso documento (o contenuto della busta). L'ordine di apposizione delle firme dei firmatari non è significativo e un'alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica; nel caso del formato CAdES il file generato si presenta con un'unica estensione p7m. Il meccanismo qui descritto è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.
Le applicazioni di generazione della firma digitale o qualificata per la sottoscrizione dei documenti informatici devono utilizzare la funzione di hash di cui all'art 4, comma 2, del Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013.

Art. 13 Formato dei documenti informatici allegati – art. 12 del regolamento

I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:
.pdf
.rtf
.txt
.jpg
.gif
.tiff
.xml
.eml, purché contenenti file nei formati di cui alle lettere precedenti.
.msg, purché contenenti file nei formati di cui alle lettere da a ad h.
È consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti al comma precedente:
.zip
.rar
.arj.
Gli allegati possono essere sottoscritti con firma digitale o firma elettronica qualificata; nel caso di formati compressi la firma digitale, se presente, deve essere applicata dopo la compressione.

Art. 14 Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati – art. 13 del regolamento

L'atto e gli allegati sono contenuti nella cosiddetta "busta telematica", ossia un file in formato MIME che riporta tutti i dati necessari per l'elaborazione da parte del sistema ricevente (gestore dei servizi telematici); in particolare la busta contiene il file Atto.enc, ottenuto dalla cifratura del file Atto.msg, il quale contiene a sua volta:
IndiceBusta.xml: il DTD è riportato nell'Allegato 4. Tale file deve essere omesso qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b).
DatiAtto.xml: gli XSD sono riportati nell'Allegato 5.
<nome file (libero)>: atto vero e proprio, in formato PDF, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 12 comma 2.
AllegatoX.xxx: uno o più allegati nei formati di file di cui all'articolo 13, eventualmente sottoscritti con firma digitale o firma elettronica qualificata; il nome del file può essere scelto liberamente.
La cifratura di Atto.msg è eseguita con la chiave di sessione (ChiaveSessione) cifrata con il certificato del destinatario; IssuerDname è il Distinguished Name della CA che ha emesso il certificato dell'ufficio giudiziario o dell'UNEP destinatario, SerialNumber è il numero seriale del certificato dell'ufficio giudiziario o dell'UNEP destinatario; l'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione sono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario; le chiavi di cifratura degli uffici giudiziari sono disponibili nell'area pubblica del portale dei servizi telematici (il relativo percorso e nome file è indicato nel catalogo dei servizi telematici).
La dimensione massima consentita per la busta telematica è pari a 30 Megabyte.
La busta telematica viene trasmessa all'ufficio giudiziario destinatario in allegato ad un

messaggio di posta elettronica certificata che rispetta le specifiche su mittente, destinatario, oggetto, corpo e allegati come riportate nell'Allegato 6.
Il gestore dei servizi telematici scarica il messaggio dal gestore della posta elettronica certificata del Ministero della giustizia ed effettua le verifiche formali sul messaggio; le eccezioni gestite sono le seguenti:
T001: l'indirizzo del mittente non è censito in ReGIndE;
T002: Il formato del messaggio non è aderente alle specifiche;
T003: la dimensione del messaggio eccede la dimensione massima consentita.
Il gestore dei servizi telematici, nel caso in cui il mittente sia un avvocato, effettua l'operazione di certificazione, ossia recupera lo status del difensore da ReGIndE; nel caso in cui lo status non sia "attivo", viene segnalato alla cancelleria.
Il gestore dei servizi telematici effettua i controlli automatici (formali) sulla busta telematica; le possibili anomalie all'esito dell'elaborazione della busta telematica sono codificate secondo le seguenti tipologie:
WARN (WARNING): anomalia non bloccante; si tratta in sostanza di segnalazioni, tipicamente di carattere giuridico (ad esempio manca la procura alle liti allegata all'atto introduttivo);
ERROR: anomalia bloccante, ma lasciata alla determinazione dell'ufficio ricevente, che può decidere di intervenire forzando l'accettazione o rifiutando il deposito (esempio: certificato di firma non valido o mittente non firmatario dell'atto);
FATAL: eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fondamentali per l'elaborazione).
La codifica puntuale degli errori indicati al comma precedente è pubblicata e aggiornata nell'area pubblica del portale dei servizi telematici.
All'esito dei controlli di cui ai commi precedenti, il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata riportante eventuali eccezioni riscontrate.
Il gestore dei servizi telematici, all'esito dell'intervento dell'ufficio, invia al depositante un messaggio di posta elettronica certificata contenente l'esito dell'intervento di accettazione operato dalla cancelleria o dalla segreteria dell'ufficio giudiziario destinatario.

Art. 15 Documenti probatori e allegati non informatici – art. 14 del regolamento

I documenti probatori e gli allegati depositati in formato analogico, sono identificati e descritti in un'apposita sezione dell'atto del processo in forma di documento informatico e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati:
numero di ruolo della causa;
progressivo dell'allegato;
indicazione della prima udienza successiva al deposito.

Art. 16 Deposito dell'atto del processo da parte dei soggetti abilitati interni – art. 15 del regolamento

I soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro trasmissione alla cancelleria o alla segreteria dell'ufficio giudiziario.
L'atto è inserito nella medesima busta telematica di cui all'articolo 14 e viene trasmesso su canale sicuro (SSL v3) al gestore dei servizi telematici, tramite collegamento sincrono

(http/SOAP); si applicano le disposizioni di cui all’articolo 10, comma 2.
Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell’ufficio giudiziario ne estrae copia per immagine in formato PDF, e lo sottoscrive con firma digitale o firma elettronica qualificata.

Art. 17 Comunicazioni e notificazioni per via telematica – art. 16 del regolamento

Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall’ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell’utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi ai sensi dell'art 16-ter del decreto legge del 30 ottobre 2012, n. 179 oppure ai sensi dell'art 16 comma 7 del medesimo decreto; il formato del messaggio è riportato nell’Allegato 8; la comunicazione o notificazione è riportata nel corpo del messaggio nonché nel file allegato Comunicazione.xml (il relativo DTD è riportato nell’Allegato 4).
La cancelleria o la segreteria dell’ufficio giudiziario, attraverso apposite funzioni messe a disposizione dai sistemi informatici di cui all’articolo 10, provvede ad effettuare una copia per immagine in formato PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.
Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni.

Art. 18 Comunicazioni e notificazioni contenenti dati sensibili – art. 16 del regolamento

La comunicazione o la notificazione che contiene dati sensibili è effettuata per estratto: in questo caso al destinatario viene recapitato l’avviso di disponibilità, secondo il formato riportato nell’Allegato 8; il destinatario effettua il prelievo dell’atto integrale accedendo all’indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso.
Il prelievo di cui al comma precedente avviene attraverso l’apposito servizio proxy del portale dei servizi telematici, su canale sicuro (protocollo SSL); tale servizio effettua l’identificazione informatica dell’utente, ai sensi dell’articolo 6; il prelievo è consentito unicamente se l’utente è registrato nel ReGIndE.
Il prelievo di cui al comma precedente avviene da un’apposita area di download del gestore dei servizi telematici, dove viene gestita e mantenuta un’apposita tabella recante le seguenti informazioni:
il codice fiscale del soggetto che ha effettuato il prelievo o la consultazione;
il riferimento al documento prelevato o consultato (codice univoco inserito nell’URL inviato nell’avviso di cui al comma 4);
la data e l’ora di invio dell’avviso;
la data e l’ora del prelievo o della consultazione.
Le informazioni di cui al comma precedente vengono conservate per cinque anni.
Nel caso in cui il destinatario sia un’impresa iscritta nel relativo registro o una Pubblica Amministrazione, la comunicazione o la notificazione che contiene dati sensibili è effettuata ai sensi del comma 1; l'utente che accede all’indirizzo (URL) contenuto nel messaggio di PEC di avviso, su canale sicuro (protocollo SSL), viene identificato ai sensi dell'art 6 ed è abilitato ad accedere all'atto integrale solo se appartiene all'impresa destinataria come risultante dal

registro delle imprese o se è un dipendente della Pubblica Amministrazione autorizzato.

Art. 19 Notificazioni per via telematica a cura degli uffici NEP – art. 17 del regolamento

Le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP in formato XML, attraverso un colloquio diretto, via web service, tra i rispettivi gestori dei servizi telematici, su canale sicuro (SSL v3), oppure tramite posta elettronica certificata.
Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tecnici di cui agli articoli 12, 13 e 14; all'interno della busta telematica è inserito il file RichiestaParte.xml, il cui XML-Schema è riportato nell'Allegato 5.
All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.
Alla notificazione per via telematica da parte dell'UNEP si applicano le specifiche della comunicazione per via telematica di cui all'articolo 17; il formato del messaggio di posta elettronica certificata è riportato nell'Allegato 7.
Ai fini della notificazione per via telematica, il sistema informatico dell'UNEP recupera l'indirizzo di posta elettronica del destinatario a seconda della sua tipologia:
soggetti abilitati esterni e professionisti iscritti in albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con legge del 28 gennaio 2009, n. 2: dal registro generale degli indirizzi elettronici, ai sensi dell'articolo 7, comma 6, nonché dall'indice nazionale delle imprese e dei professionisti (INI-PEC), sezione professionisti;
imprese iscritte nel relativo registro: ai sensi dell'articolo 7, comma 5;
cittadini: ai sensi dell'articolo 7, comma 5.
Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette - per via telematica a chi ha richiesto il servizio - il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale o firma elettronica qualificata e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata. La relazione di notificazione è in formato XML e rispetta l'XML-Schema riportato nell'Allegato 5; se il richiedente è un soggetto abilitato esterno, la trasmissione avviene via posta elettronica certificata; il formato del messaggio è riportato nell'Allegato 7.

Art. 19 bis Notificazioni per via telematica eseguite dagli avvocati – art. 18 del regolamento

Qualora l'atto da notificarsi sia un documento originale informatico, esso deve essere in formato PDF e ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è ammessa la scansione di immagini. Il documento informatico così ottenuto è allegato al messaggio di posta elettronica certificata.
Nei casi diversi dal comma 1, i documenti informatici o copie informatiche, anche per immagine, di documenti analogici, allegati al messaggio di posta elettronica certificata, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti in formato PDF.
Nei casi in cui l'atto da notificarsi sia l'atto del processo da trasmettere telematicamente all'ufficio giudiziario (esempio: atto di citazione), si procede ai sensi del precedente comma 1.
Qualora il documento informatico, di cui ai commi precedenti, sia sotto-scritto con firma digitale o firma elettronica qualificata, si applica quanto previsto all'articolo 12, comma 2.
La trasmissione in via telematica all'ufficio giudiziario delle ricevute previste dall'articolo 3-bis,

comma 3, della legge 21 gennaio 1994, n. 53, nonché della copia dell'atto notificato ai sensi dell'articolo 9, comma 1, della medesima legge, è effettuata inserendo l'atto notificato all'interno della busta telematica di cui all'art 14 e, come allegati, la ricevuta di accettazione e la ricevuta di avvenuta consegna relativa ad ogni destinatario della notificazione; i dati identificativi relativi alle ricevute sono inseriti nel file DatiAtto.xml di cui all'articolo 12, comma 1, lettera e.

Art. 20 Disposizioni particolari per la fase delle indagini preliminari – art. 19 del regolamento

Nelle indagini preliminari le comunicazioni tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria avvengono su canale sicuro protetto da un meccanismo di crittografia (SSL v3).
Il sistema di gestione del registro e il sistema documentale garantiscono la tracciabilità delle attività, attraverso appositi file di log, conservati nel sistema documentale stesso.
L'atto del processo rispetta le specifiche di cui agli articoli 12 e 13.
La comunicazione di atti e documenti nella fase di indagini preliminari avviene tramite posta elettronica certificata, secondo le specifiche di cui all'articolo 17; le caselle di PEC dell'ufficio del pubblico ministero sono attivate presso i gestori di posta elettronica certificata della forze di polizia.
Il gestore dei servizi telematici si collega alle caselle di cui al comma precedente su canale sicuro, utilizzando i protocolli POP3Ss o HTTPS, al fine di evitare la trasmissione in chiaro delle credenziali di accesso e dei messaggi.
La comunicazione degli atti del processo alle forze di polizia è effettuata per estratto, secondo le specifiche di cui all'articolo 18; l'atto è protetto da meccanismo di crittografia a chiavi asimmetriche, con le medesime specifiche di cui all'articolo 14 comma 2.
Gli atti contenuti nel fascicolo informatico, relativi alle indagini preliminari, sono custoditi in una sezione distinta del sistema documentale; ciascun atto potrà essere protetto da un meccanismo di crittografia basato su chiavi asimmetriche, custodite e gestite nell'ambito di un sistema HSM (hardware security module) appositamente dedicato alle operazioni di cifratura e decifratura, invocato dalle applicazioni di gestione dei registri. Ogni istanza della piattaforma di gestione documentale è dotata di apparati HSM dedicati.
La trasmissione telematica delle informazioni relative alle notizie di reato avviene tramite cooperazione applicativa tra il sistema di gestione informatizzata dei registri presso l'ufficio del pubblico ministero e il Sistema Informativo Interforze del Ministero dell'Interno, secondo le specifiche del Sistema Pubblico di Cooperazione (SPCoop), su canale cifrato attraverso l'uso di certificati server. Le informazioni contenute nella busta di e-Government prevista dalle specifiche SPCoop sono in formato XML.

Art. 21 Requisiti della casella di PEC del soggetto abilitato esterno – art. 20 del regolamento

La casella di posta elettronica certificata di un soggetto abilitato esterno deve disporre di uno spazio disco minimo pari a 1 Gigabyte.

Art. 22 Richiesta delle copie di atti e documenti – art. 21 del regolamento

Per la richiesta telematica di copie di atti e documenti relativi al procedimento è disponibile, sul punto di accesso e sul portale dei servizi telematici, un servizio sincrono attraverso il quale individuare i documenti di cui richiedere copia e, in seguito al perfezionamento del pagamento,

inoltrare la richiesta effettiva della copia stessa.
Il soggetto che ne ha diritto può richiedere:
copia semplice in formato digitale;
copia semplice per l'avvocato non costituito in formato digitale;
copia autentica in formato digitale;
copia esecutiva in formato digitale;
copia semplice in formato cartaceo;
copia autentica in formato cartaceo;
copia esecutiva in formato cartaceo.
I dati relativi alla richiesta sono inoltrati all'ufficio giudiziario attraverso l'invocazione di un apposito web service; al richiedente è restituito l'identificativo univoco della richiesta inoltrata. Tale identificativo univoco è associato all'intero flusso di gestione della richiesta e di rilascio della copia.
Nel caso in cui la copia non possa essere rilasciata il sistema, in maniera automatica, comunica al richiedente l'impossibilità di evadere la richiesta.

Art. 23 Rilascio delle copie di atti e documenti – art. 21 del regolamento

Il rilascio della copia informatica di atti e documenti viene eseguito secondo le specifiche di cui all'articolo 16 del regolamento e dell'art. 23-bis del CAD; la copia è inviata al richiedente in allegato ad un messaggio di posta elettronica certificata, secondo il formato riportato nell'Allegato 9.
Nel caso di copia di documenti contenenti dati sensibili o nel caso di copia di documenti che eccedono il massimo consentito dalla posta elettronica certificata, il messaggio di cui al comma precedente contiene l'avviso di disponibilità della copia, secondo il formato riportato nell'Allegato 9; il prelievo avviene secondo le specifiche di cui all'articolo 18, commi 2, 3 e 4.

CAPO IV – CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Art. 24 Requisiti di sicurezza – art. 26 del regolamento

L'architettura dei servizi di consultazione aderisce al modello MVC (Model View Controller) e prevede il disaccoppiamento del front-end, localizzato sul punto di accesso o sul portale dei servizi telematici, dal back-end, localizzato sul gestore dei servizi telematici, incaricato di esporre i servizi sottoforma di web service (http/SOAP).
Il portale dei servizi telematici espone, attraverso un apposito servizio proxy, i web service forniti dal gestore dei servizi telematici, a beneficio dei punti di accesso e di applicazioni esterne.
I punti di accesso realizzano autonomamente la parte di front-end, che deve essere localizzata all'interno della intranet del PdA stesso e non deve essere accessibile direttamente dall'esterno.
I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne.
Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.
Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del portale dei servizi telematici.
L'accesso ai servizi di consultazione avviene su canale sicuro (protocollo SSL) previa

identificazione informatica su di un punto di accesso o sul portale dei servizi telematici, secondo le specifiche di cui all'articolo 6; a seguito di tale identificazione, il punto di accesso o il portale dei servizi telematici attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice fiscale del soggetto che effettua l'accesso (nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy trasmette la richiesta al web service del gestore dei servizi telematici.
In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal regolamento.
In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche dell'Agenzia per l'Italia Digitale; in questo caso, il Direttore Generale S.I.A., valutata la soluzione proposta e opportunamente descritta nel piano della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.
Il punto di accesso può consentire l'accesso a soggetti delegati da un utente registrato (soggetto delegante), con le stesse modalità di cui ai commi 7, 8 e 9, purchè il soggetto delegante abbia predisposto un atto di delega, sottoscritto con firma digitale, che il punto di accesso conserva per cinque anni unitamente alla tracciatura di ogni accesso effettuato su delega; le informazioni e gli atti di cui sopra sono forniti su richiesta al Ministero della giustizia.
Fuori dai casi previsti ai commi 1 e 10, l'architettura dei servizi di consultazione prevede in via residuale che il punto di accesso o il portale dei servizi telematici effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che rende disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati identificativi del soggetto vengono inseriti nell'header HTTP della richiesta.
I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
L'elenco dei punti di accesso autorizzati è pubblicato nell'area pubblica del portale dei servizi telematici e nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
Il punto di accesso si dota di un piano della sicurezza, depositato al re-sponsabile per i sistemi informativi automatizzati unitamente all'istanza di iscrizione all'elenco pubblico dei punti di accesso, che prevede la trattazione, esaustiva e dettagliata, dei seguenti argomenti:
struttura logistica e operativa dell'organizzazione;
ripartizione e definizione delle responsabilità del personale addetto;
descrizione dei dispositivi installati;
descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);
descrizione delle procedure di registrazione delle utenze;
descrizione relativa all'implementazione dei meccanismi di identificazione informatica;
qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;
procedura di gestione delle copie di sicurezza dei dati;
procedura di gestione dei disastri;
analisi dei rischi e contromisure previste;
descrizione dell'eventuale processo di delega di cui al comma 10 nonché delle modalità di conservazione dell'elenco dei soggetti delegati e delle eventuali revoche delle deleghe;
descrizione della modalità di verifica dell'effettiva funzionalità e adeguatezza del sistema di

sicurezza del punto di accesso.
Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi in-formativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.
Il punto di accesso abilita i propri iscritti unicamente a usufruire dei servizi esplicitamente autorizzati dal responsabile per i sistemi informativi automatizzati e riportati nel catalogo dei servizi telematici.
Il punto di accesso si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della giustizia.
Il punto di accesso fornisce al Ministero della giustizia, su richiesta, i dati di censimento sul ReGIndE di cui articolo 8 comma 1 per i casi di iscrizione dei professionisti non iscritti in albi di cui articolo 9 comma 1.
Il punto di accesso verifica l'effettiva funzionalità e adeguatezza del sistema di sicurezza almeno una volta l'anno e provvede ad inviare l'esito delle stesse, unitamente ad eventuali variazioni nei contenuti del piano, all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: Questo indirizzo email è protetto dagli spambots. È necessario abilitare JavaScript per vederlo..

Art. 25 Registrazione dei soggetti abilitati esterni e degli utenti privati – art. 28 del regolamento

L'utente accede ai servizi di consultazione previa registrazione presso un punto di accesso autorizzato o presso il portale dei servizi telematici.
Il punto di accesso o il portale dei servizi telematici effettuano la registrazione del soggetto abilitato esterno o dell'utente privato, prelevando il codice fiscale dal token crittografico dell'utente; attraverso un'apposita maschera web, l'utente (senza poter modificare il codice fiscale) completa i propri dati, inserendo almeno le seguenti informazioni:
nome e cognome
luogo e data di nascita
residenza
domicilio
ruolo
consiglio dell'ordine o ente di appartenenza.
I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per cinque anni.
Gli esperti e gli ausiliari del giudice, non iscritti ad alcun albo professionale o per i quali il proprio ordine non abbia provveduto all'invio dell'albo, presentano, all'atto della registrazione, copia elettronica in formato PDF dell'incarico di nomina da parte del giudice; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
Qualora il professionista sia iscritto ad un albo dei consulenti tecnici, istituito presso un tribunale (ai sensi del Capo II, sezione 1, delle disposizioni di attuazione del codice di procedura civile), al PdA viene presentata copia elettronica in formato PDF del provvedimento di iscrizione all'albo stesso da parte del comitato; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
Il punto di accesso è tenuto a conservare i documenti informatici di cui ai commi precedenti, e a renderli disponibili, su richiesta, al Ministero della giustizia.

I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all’allegato 11.

CAPO V – PAGAMENTI TELEMATICI

Art. 26 Requisiti relativi al processo di pagamento telematico – art. 30 del regolamento

Al fine di comunicare in via telematica all’ufficio giudiziario l’avvenuto pagamento delle spese, dei diritti e del contributo unificato, la ricevuta di versamento è inserita come allegato della busta telematica nel caso di inoltro via PEC, oppure è associata alla richiesta telematica nel caso di istanza gestita tramite un flusso sincrono.
Il servizio di pagamento in modalità telematica è messo a disposizione dei soggetti abilitati nell’ambito delle funzionalità del punto di accesso e del portale dei servizi telematici, con lo scopo di permettere il pagamento attraverso strumenti telematici e di ottenere la ricevuta di pagamento attraverso il medesimo canale telematico; l’accesso ai servizi di pagamento avviene previa identificazione informatica di cui all’articolo 6.
Le regole per l'esecuzione del pagamento, le modalità di interconnessione tra i sistemi nonchè le modalità di rendicontazione e riconciliazione dei pagamenti rispettano le Linee Guida emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal decreto legge del 30 ottobre 2012, n. 179.
Il portale dei servizi telematici si avvale dell'infrastruttura e della piattaforma tecnologica messa a disposizione dall'Agenzia per l'Italia Digitale, attraverso il Sistema Pubblico di Connettività, (Nodo dei Pagamenti-SPC) allo scopo di garantire l'interconnessione e l'interoperabilità tra le Pubbliche Amministrazioni e i Prestatori di Servizi di Pagamento;
Il portale dei servizi telematici espone ai punti di accesso servizi web per l'esecuzione dei pagamenti telematici utilizzando le funzionalità messe a disposizione dal Nodo dei Pagamenti-SPC. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull’area pubblica del portale dei servizi telematici.
I punti di accesso possono mettere a disposizione dei propri utenti il servizio di pagamento telematico, definendo opportuni accordi con uno o più prestatori di servizi di pagamento, nel rispetto di quanto indicato al comma 3.
Nei casi di cui al precedente comma, il punto di accesso è garante nei confronti del Ministero della Giustizia del rispetto delle Linee Guida di cui al comma 3, relativamente alle modalità di riversamento verso la banca tesoriera e alla rendicontazione; il punto di accesso rispetta quanto indicato nelle Linee Guida relativamente al flusso di rendicontazione nei confronti del Ministero della Giustizia.
Il processo di pagamento consente all’utente di scegliere tra diverse modalità di pagamento messe a sua disposizione da una molteplicità di prestatori di servizi di pagamento che aderiscono all'infrastruttura del Nodo dei pagamenti-SPC.
La ricevuta di pagamento restituita all’utente a fronte del pagamento effettuato in via telematica costituisce prova del trasferimento dell’importo versato sul conto corrente intestato alla Tesoreria dello Stato
Per il recupero delle somme erroneamente versate si procede secondo le modalità previste dalla legge.

Art. 27 Oggetti informatici interessati nel pagamento telematico – art. 30 del regolamento

La Richiesta di Pagamento Telematico (RPT), relativa al versamento di una o più spettanze legate ad un medesimo servizio, è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
definisce gli elementi necessari a caratterizzare i pagamenti, in particolare qualifica il versamento attraverso un identificativo univoco di cui al successivo comma 5;
contiene i dati identificativi del soggetto che esegue il pagamento, contiene una parte riservata (Dati Specifici Riscossione) per inserire informazioni elaborabili automaticamente dai sistemi della Giustizia;
viene predisposta dal soggetto che procede al pagamento ed inviata dal portale dei servizi telematici al Nodo dei Pagamenti-SPC;
La Ricevuta Telematica (RT) è restituita al soggetto che ha eseguito il pagamento a fronte di ogni singola RPT: essa è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
definisce gli elementi necessari a qualificare il pagamento, tra cui l'esito del pagamento stesso e, in caso positivo, l'identificativo univoco del pagamento assegnato dal sistema del prestatore dei servizi di pagamento (Psp);
trasferisce inalterate le stesse informazioni ricevute in ingresso (RPT) relative alla parte riservata (Dati Specifici Riscossione) a disposizione della PA
Il soggetto che emette la Ricevuta Telematica (RT) di cui al comma 2, la sottoscrive- ai sensi dell'art 30, comma 5 del regolamento- con firma digitale o firma elettronica qualificata in formato CAdES; a tal fine possono essere utilizzati certificati emessi da una autorità di certificazione allo scopo messa a disposizione dell'Agenzia per l'Italia Digitale.
Al fine di qualificare in maniera univoca il pagamento all'interno del dominio giustizia, è definito l'identificativo univoco di pagamento (IUV)) secondo i formati previsti dalle Linee Guida emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal decreto legge del 30 ottobre 2012, n. 179.
Lo IUV (identificato con il nome CRS nell'ambito Giustizia) è generato esclusivamente dal portale dei servizi telematici attraverso l'invocazione di un web service di cui all'art 26, comma 5 e ha il seguente formato: <check digits> <identificatore univoco>, dove:
<check digit> costituisce il codice numerico di controllo (2 posizioni);
<identificatore univoco> è rappresentato da 33 posizioni alfanumeriche così strutturate: <codice PdA richiedente><codice Sistema Gestore><codice univoco operazione>; la sezione <codice PdA richiedente> (4 caratteri alfanumerici) assicura flessibilità nella emissione del CRS; la sezione <codice Sistema Gestore> (4 caratteri alfanumerici) rappresenta il sistema a cui è destinata la ricevuta; la sezione <codice univoco operazione> (25 caratteri alfanumerici) contiene un codice 'non ambiguo' all'interno del dominio entro il quale viene generato.
Lo IUV viene inserito nella struttura RPT (elemento identificativoUnivocoVersamento) e viene restituito invariato al punto di accesso o al portale dei servizi telematici all'interno della RT (elemento identificativoUnivocoVersamento).
Al momento dell'accettazione della ricevuta di pagamento, il sistema informatico dell'ufficio giudiziario controlla, attraverso l'identificativo univoco, che la ricevuta telematica non sia stato già utilizzata per altri servizi di pagamento e, in caso di esito positivo del controllo, la ricevuta viene marcata al fine di non permetterne il riutilizzo.

Art. 28 Riscontro del pagamento telematico – art. 30 del regolamento

Allo scopo di permettere all'Amministrazione di verificare e riscontrare le ricevute generate a seguito di pagamento telematico, nell'ambito del dominio giustizia è configurato un

sottosistema per la memorizzazione e gestione delle Ricevute Telematiche di cui all'articolo 27; il sottosistema è denominato Repository Ricevute Telematiche (RRT) ed è accessibile a tutte le applicazioni e ai sistemi del dominio Giustizia interessate dai pagamenti telematici.
Il punto di accesso o il portale dei servizi telematici provvede a registrare la RT nel sistema RRT contestualmente al rilascio della stessa al soggetto abilitato esterno richiedente; la registrazione si conclude con esito positivo solo se lo IUV presente nella RT è stato generato dal portale dei servizi telematici
Per la registrazione della RT nel al sistema RRT, il portale dei servizi telematici espone un apposito web service il cui WSDL è pubblicato nell'area pubblica del portale dei servizi telematici.
Il sistema RRT permette la gestione delle RT e dei relativi identificativi univoci di pagamento secondo le modalità indicate nell'articolo 27.
Le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1 sono messe a disposizione, sulla base di specifica convenzione da sottoscriversi con il Direttore Generale S.I.A., degli enti e delle agenzie pubbliche per l'adempimento dei propri compiti di verifica, controllo e contrasto all'evasione ed elusione.
I soggetti abilitati che hanno effettuato i versamenti in via telematica possono consultare sul portale dei servizi telematici, previa identificazione informatica di cui all'articolo 6, le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1.

Art. 29 Diritto di copia – art. 31 del regolamento

Il sistema informatico del Ministero della giustizia comunica all'interessato l'importo da versare per i diritti di copia; tale importo è calcolato, sulla base delle vigenti disposizioni normative e regolamentari, in base alle indicazioni fornite dall'interessato al momento dell'individuazione dei documenti di cui richiedere copia. L'informazione è messa a disposizione dell'interessato attraverso il servizio di richiesta copie attivo sul punto di accesso e sul portale dei servizi telematici; unitamente all'importo dei diritti ed oneri viene comunicato all'interessato anche l'identificativo univoco associato associato al flusso di gestione della richiesta e rilascio della copia.
La richiesta di copia è soddisfatta solo dopo che è pervenuta la ricevuta telematica di pagamento di cui all'articolo 27, comma 2.

CAPO VI – DISPOSIZIONI FINALI E TRANSITORIE

Art. 30 Gestione del transitorio – art. 35 del regolamento

Al momento dell'attivazione, sul ReGIndE di cui all'articolo 7, dell'indirizzo di posta elettronica certificata del soggetto abilitato esterno, il portale dei servizi telematici invia un messaggio di PEC al medesimo soggetto comunicando l'avvenuta attivazione. La comunicazione riporta espressa avvertenza che il soggetto abilitato esterno dovrà usare per le successive trasmissioni unicamente la casella PEC.
A decorrere dalla comunicazione di cui al comma 1, il soggetto abilitato esterno utilizza unicamente il sistema di trasmissione della posta elettronica certificata, così come disciplinato nel presente provvedimento.
A decorrere dalla comunicazione di cui al comma 1, il gestore dei servizi telematici:
Invia comunicazioni e notificazioni solamente alla casella di PEC ivi indicata;

Consente la ricezione di atti solo tramite PEC, rifiutando automatica-mente il deposito tramite altro canale.
Le pubbliche amministrazioni comunicano il proprio indirizzo di posta elettronica certificata ai sensi dell'articolo 9-bis del presente provvedimento entro il novantesimo giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana; le pubbliche amministrazioni possono comunicare detto indirizzo anche successivamente alla scadenza di detto termine; l'indirizzo sarà reso consultabile dagli uffici giudiziari a partire dal 91° giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana.

Art. 31 Efficacia

Fatto salvo quanto indicato dall'articolo 30 comma 4, il presente provvedimento acquista efficacia decorsi 15 giorni dalla sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana e sostituisce l'analogo provvedimento del 18 luglio 2011.
Roma, addì 16 aprile 2014

IL DIRETTORE GENERALE PER I SISTEMI INFORMATIVI AUTOMATIZZATI
Daniela Intravaia

ALLEGATO 1 - BANCHE DATI E SISTEMI DI CUI ALL'ARTICOLO 3, COMMA 2

Costituiscono infrastrutture unitarie e comuni:

le banche dati e i relativi sistemi informativi del personale (inclusi i sistemi di misurazione e monitoraggio dela performance), delle risorse finanziarie, strumentali e materiali, del protocollo e di gestione documentale degli atti amministrativi e delle attività amministrative anche presso gli uffici giudiziari;
le banche dati e i relativi sistemi informativi di statistica, anche giudiziaria, delle spese di giustizia;
le banche dati e i relativi sistemi informativi dell'amministrazione penitenziaria (inclusi gli archivi anagrafici di identificazione), del dipartimento della giustizia minorile, inclusa la banca dati delle adozioni, del casellario giudiziale (inclusi i carichi pendenti), dell'esecuzione penale, delle misure di prevenzione e dei beni confiscati, il Registro Generale dei Testamenti;
il portale web istituzionale www.giustizia.it e siti internet istituzionali dell'amministrazione centrale, il portale dei servizi telematici, il registro generale degli indirizzi elettronici, il gestore dei servizi telematici, il sistema di gestione delle notificazioni e comunicazioni e relativi sistemi di gestione documentale;
le banche dati e i relativi sistemi informativi degli uffici giudiziari a competenza nazionale (Corte di Cassazione e relativa Procura Generale, Tribunale superiore delle acque pubbliche, Direzione Nazionale Antimafia), nonché le banche dati e i sistemi informativi del Centro Elettronico di Documentazione;
il sistema di autenticazione al dominio giustizia e di gestione e monitoraggio delle infrastrutture, della sicurezza, della rete e dei servizi, inclusi i sistemi di salvataggio dei log di accesso.

Allegati
omissis