ALLEGATO 2

PIANO DELLE VERIFICHE

Premessa

Nel prosieguo si intende:

- Regole Tecniche (o anche Regolamento): D.M. 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».
- Specifiche Tecniche: Provvedimento del responsabile per i sistemi informativi automatizzati del Ministero della giustizia del 18 luglio 2011 recante « Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44»

Vengono inoltre utilizzati i seguenti acronimi:
- PdA: Punto di Accesso
- CF: Codice Fiscale

Prerequisiti

Il PdA deve essere in grado di svolgere le verifiche richieste, riportate in questo allegato, interfacciandosi con un ***Ufficio Giudiziario (UG) di test***, attestato presso il Model Office.

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

- Garantire, durante l'ispezione, la **presenza di figure tecniche** in grado di rispondere adeguatamente alle domande tecniche, anche di dettaglio, poste dalle persone incaricate della verifica.
- Fornire una **connessione Internet** per la simulazione di collegamenti di utenti esterni, evitando di connettersi direttamente alla LAN del PdA, in modo da riprodurre il più possibile una situazione reale (evitando problematiche relative a tempi di accesso, firewall, ecc.).

Per le specifiche dei flussi di comunicazione tra PdA e dominio Giustizia e del formato dei messaggi coinvolti si faccia riferimento alle Regole Tecniche e alle Specifiche Tecniche.

Verifiche

1. Procedura di autenticazione dell'utente

Ogni accesso al PdA deve attivare il processo di identificazione informatica, secondo quanto disciplinato dall'art. 6 delle specifiche tecniche e conformemente a quanto indicato nella relazione tecnica sulle modalità di identificazione degli utenti di cui all'articolo 2, comma 3, del presente decreto.

A. A riguardo deve essere verificato il controllo di validità del certificato di autenticazione presente nel token crittografico in uso (smart card, chiavetta USB o altro dispositivo sicuro). In particolare il PdA deve verificare che il certificato:
    i. rispetti il profilo del certificato di autenticazione previsto dalla CNS[1], secondo quanto indicato alla lettera b, comma 1 dell'articolo 6 sopra citato;
    ii. sia stato rilasciato da una CA accreditata DigitPA;
    iii. sia in corso di validità.

[1] Linee guida per l'emissione e l'utilizzo della Carta Nazionale dei Servizi (CNS)", documento disponibile on-line nella sezione Specifiche Tecniche del sito di DigitPA al seguente indirizzo http://www.digitpa.gov.it/carta_nazionale_servizi

I tecnici del PdA dovranno mostrare i controlli adottati per il rispetto delle specifiche indicate; in fase di test si procederà al tentativo di autenticazione con token contenenti certificati non conformi, che il PdA dovrà opportunamente rifiutare.

B. Deve essere verificato il metodo di associazione tra il certificato di autenticazione e il record dell'utente nel PdA, attraverso la procedura di estrazione del codice fiscale dell'utente dal certificato in uso. Verificare la procedura di connessione al PdA (da Internet) tramite browser e il funzionamento della procedura di autenticazione.

C. Il PdA, prima di consentire qualunque operazione, deve verificare la presenza del token crittografico collegato alla postazione dell'utente; nel caso non sia rilevata deve prevedere un meccanismo di invalidamento e terminazione della sessione. La corretta procedura di chiusura sessione deve essere testata con browser diversi (Internet Explorer, FireFox…).

2. Procedure di abilitazione e gestione utenze

L'utente esterno accede ai servizi di consultazione previa registrazione presso un Punto di Accesso autorizzato o presso il portale dei servizi telematici. Il metodo di registrazione è disciplinato all'articolo 25 delle specifiche tecniche.

Procedura di registrazione utenze

Eseguire almeno una procedura di iscrizione di un professionista il cui ordine/ente abbia già inviato l'albo e di almeno un professionista non ancora presente su ReGIndE, verificando che:

A. il PdA richieda i dati di cui all'art. 25, comma 2 delle specifiche tecniche;

B. per i soggetti indicati ai punti 4 e 5 dell'articolo 25 delle specifiche tecniche metta a disposizione una funzionalità di upload della copia elettronica di nomina del giudice o copia provvedimento iscrizione all'albo dei consulenti tecnici, firmata digitalmente dal soggetto stesso. In fase di upload del documento il PdA deve verificare:
   - che sia in formato PDF
   - che il firmatario sia il soggetto al momento autenticato
   - la validità della firma secondo le "Regole per il riconoscimento e la verifica del documento informatico"[2];

   I tecnici del PdA dovranno mostrare i controlli adottati per il rispetto delle specifiche indicate, e/o gli strumenti/software esterni adottati.

C. Per i soggetti appartenenti alle categorie indicate al comma 4 dell'art. 7 delle specifiche tecniche, che non sono ancora iscritte su ReGIndE, invii tramite PEC il file *ComunicazioniSoggetti.xml* conforme alle specifiche, firmato digitalmente dal PdA. Nota: il codice ente deve essere quello fittizio e non deve prevedere modalità di invio integrale.

D. il PdA memorizzi i dati di registrazione (con garanzia di conservazione per almeno 10 anni), come indicato al comma 3 dell'articolo 25. Deve essere inoltre verificata la conservazione dei documenti informatici di cui al punto precedente.

E. Il PdA deve garantire la tracciabilità di ogni risposta ricevuta via PEC e gestire opportunamente ogni eventuale comunicazione di errore/anomalia, come indicato nell'allegato 2 delle specifiche tecniche (si procederà ad esempio ad iscrizione di soggetto già registrato in ReGIndE, associato al suo ordine/ente di appartenenza oppure a ordine/ente di appartenenza diverso).

Procedura di variazione e cancellazione utenze

A. Il PdA dovrà mettere a disposizione, per i soli soggetti non iscritti ad alcun albo, o il cui albo non sia stato ancora inviato, anche la procedura di modifica dati anagrafici e cancellazione da parte dell'utente stesso.

B. Verificare che le richieste siano inviate tramite PEC utilizzando la struttura *ComunicazioniSoggetti.xml* conforme alle specifiche, firmato digitalmente.

---

[2] "Regole per il riconoscimento e la verifica del documento informatico": Deliberazione n. 45 del 21 maggio 2009 - Testo coordinato con le modifiche apportate dalla Determinazione DIGITPA 28 luglio 2010, pubblicata su Gazzetta Ufficiale della Repubblica Italiana serie generale n. 191 del 17 agosto 2010.

C. Il PdA deve garantire la tracciabilità di ogni risposta ricevuta via PEC e gestire opportunamente ogni eventuale comunicazione di errore/anomalia, come indicato nell'allegato 2 delle specifiche tecniche (si procederà ad esempio a cancellazioni o modifiche di soggetti per cui è stato inviato l'albo al ReGIndE).

3. Consultazioni delle informazioni

A. La verifica delle funzionalità di accesso sincrono ai servizi esposti dal proxy del Portale dei Servizi Telematici può essere fatta eseguendo attraverso browser una serie di interrogazioni. Il PdA è tenuto a fornire una interfaccia chiara e intuitiva che permetta di accedere a tutte le informazioni relative alla consultazione dei web service forniti dal gestore dei servizi telematici attraverso l'apposito servizio proxy.

B. Per procedere alle funzionalità di consultazione, il PdA deve inviare una richiesta, secondo i WSDL pubblicati sull'area pubblica del Portale dei Servizi Telematici, con indicazione di:

- codice fiscale del soggetto al momento autenticato
- ruolo di consultazione, che il PdA associa all'utente a seconda del registro di cancelleria.

I tecnici del PdA dovranno mostrare in particolare la procedura adottata per l'assegnazione del ruolo.

A. Deve essere verificato che il PdA garantisca la tracciabilità delle risposte inviate dal web service di back-end.

B. Nel caso in cui il PdA esponga a sua volta i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne, i tecnici del PdA dovranno mostrare i meccanismi adottati per garantire la sicurezza nell'accesso ai servizi. Questo aspetto dovrà essere esposto in modo dettagliato anche nel Piano della Sicurezza.

4. Richiesta copie

A. Verificare la possibilità di accedere al web service che espone la funzionalità di richiesta di copie di atti e documenti rilasciati dall'Ufficio Giudiziario, in tutti i formati elencati al comma 2 art. 22 delle specifiche tecniche.

B. Il PdA dovrà fornire tracciabilità dello stato della richiesta e ogni risposta inviata all'Ufficio Giudiziario.

C. Se l'interfaccia del PdA fornisce accesso alla casella PEC del soggetto iscritto, verificare che permetta di visualizzare la copia richiesta e di poterne attivare il download, o l'avviso di disponibilità della copia.

5. Flussi di invii documentali e comunicazioni tramite PEC

Qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, la verifica ha come oggetto la corretta implementazione di quanto riportato nel Piano della sicurezza ai sensi dell'art. 24, comma 13.g delle specifiche tecniche, soprattutto con riferimento ad eventuali modalità di gestione delle credenziali di accesso alla casella di PEC.

6. Accesso al ReGIndE

Il Punto di Accesso deve fornire una funzionalità di accesso al Registro Generale degli Indirizzi Elettronici attraverso interrogazione di un apposito web service (su connessioni sicure – SSL v3).

7. Sicurezza delle connessioni

A. Le specifiche tecniche prevedono che il PdA stabilisca un canale sicuro con i browser esterni utilizzando SSL v.3 e chiavi di almeno 1024 bit. Per la verifica di questi parametri è necessario collegarsi con un browser dall'esterno e:

i. Verificare la lunghezza della chiave visualizzando il certificato.

ii. Verificare l'impossibilità di connettersi se non attraverso protocollo SSL v.3. Ad esempio, nel browser IE, entrare nelle impostazioni avanzate (Internet Option → Advanced) e abilitare la sola opzione "USE SSL 2.0". Chiudere il browser e ritentare il collegamento, verificando che il sito non accetti la connessione.

B. Deve essere anche verificato che il PdA stabilisca un canale sicuro con il Portale dei Servizi Telematici mediante un collegamento sicuro con mutua autenticazione (SSL v.3 e chiavi di almeno 1024 bit). Il PdA deve mettere a disposizione procedure per la verifica di queste specifiche.

C. Se il PdA mette a disposizione un servizio di pagamento in modalità telematica, secondo quanto disciplinato nelle specifiche tecniche, deve dimostrare la garanzia di sicurezza del servizio (su protocolli sicuri), ed in particolare tra PdA e PsP.

8. Sicurezza dei locali e delle procedure di amministrazione del sistema

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

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