ALLEGATO 1

PUNTO DI ACCESSO

PER IL PROCESSO TELEMATICO

RELAZIONE TECNICA

Relativa al sistema di autenticazione

VERSIONE 1.0

23/12/2019

Sommario

RIFERIMENTI

[1] Provvedimento 16 aprile 2014 del responsabile per i sistemi informativi automatizzati del Ministero della giustizia

[2] D.M. n.44 21/02/2011: regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile

ACRONIMI

Acronimo	*Descrizione*
PCT	Processo civile telematico
PdA	Punto di Accesso
SICI	Sistema Informatico Civile
PSP	Prestatore servizi pagamento

Premessa

La presente relazione ha lo scopo di illustrare in modo dettagliato le modalità di registrazione e autenticazione degli utenti del Punto di Accesso di Lepida S.c.p.A., come richiesto dal Provvedimento 16 aprile 2014 [1].

1 LA REGISTRAZIONE DEGLI UTENTI

Come previsto dall'ART. 28 del DM 21 febbraio 2011 [2]: "L'accesso ai servizi di consultazione resi disponibili dal dominio giustizia si ottiene previa registrazione presso il punto di accesso autorizzato o presso il portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1".

L'utilizzo del Punto di Accesso sarà consentito ai seguenti ruoli:

- Legale rappresentante degli Enti soci e loro delegati;
- Avvocati appartenenti alle avvocature degli Enti soci;
- Funzionari pubblici appartenenti agli Enti soci;
- Amministratore di sistema[1]

L'utente, dopo la verifica da parte del sistema della correttezza del certificato, accedere alla funzionalità di iscrizione. Tale funzionalità prevede la compilazione di un modulo on-line affinchè siano disponibili, sull'utente, i seguenti dati:

a) nome e cognome

b) luogo e data di nascita

c) residenza

d) domicilio

e) ruolo[2]

f) ordine o ente di appartenenza[3]

La comunicazione dell'utente Amministratore da parte di Lepida S.P.A.al fornitore, che lo registra sul PdA, avviene via PEC e prevede l'invio dei dati sopra riportati.

Le richieste di registrazione sono verificate dall'Amministratore del Punto di Accesso. Gli utenti sono abilitati dall'Amministratore del Punto di Accesso.

Non sono previsti invii al ReGIndE di alcun soggetto. I soggetti autorizzati sono il legale rappresentante della società intestataria del PdA, i soggetti da lui delegati ed, eventualmente, avvocati iscritti ad altri fori, la cui iscrizione al ReGIndE è gestita dall'Ordine di appartenenza.

[1] Soggetto delegato da Lepida S.P.A. per la gestione degli utenti del Punto di Accesso
[2] Come sopra riportato
[3] Consiglio dell'Ordine di appartenenza per avvocati, Ente rappresentato per i legali rappresentanti

2 L'AUTENTICAZIONE DEGLI UTENTI

Per una migliore comprensione del testo si riporta, come introduzione, un breve richiamo di quanto indicato nel contesto delle specifiche tecniche ART. 6 del Provvedimento 16 Aprile 2014 in merito all'identificazione informatica degli utenti:

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.

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

2.1 AUTENTICAZIONE CON TOKEN CRITTOGRAFICO (SMART CARD)

Nel caso si utilizzi il token crittografico, l'identificazione avviene nel rispetto dei seguenti requisiti:

a) 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.

b) Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all'Appendice 1 del documento rilasciato dal AgID (ex 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.

c) 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.

d) In termini di 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.

e) In fase di identificazione tramite token crittografico, il punto di accesso 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 certificato di autenticazione deve contenere il **codice fiscale** del possessore della smart card. La circolare 19 giugno 2000 n. AIPA/CR/24, contenente le linee guida per l'interoperabilità tra i certificatori, stabilisce la posizione in cui si deve trovare il codice fiscale per i certificati di firma. La prassi utilizzata dalle Certification Authority in molti casi non rispetta tale standard. Il Punto di Accesso fornirà quindi la possibilità di configurare per ciascuna CA il campo, la posizione e il carattere separatore dei campi utilizzati per contenere il codice fiscale. Questa attività di configurazione deve essere effettuata prima che un utente possa autenticarsi con una smart card emessa da una nuova CA. Inoltre, il certificato della CA emittente deve essere registrato dal PdA.

Di seguito sono dettagliati i passi dell'autenticazione degli utenti.

2.1.1 Verifica del certificato

A seguito della richiesta di apertura sessione, viene effettuato l'handshake SSL, in aderenza al protocollo.

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

La connessione instaurata con il client avviene su canale sicuro SSL v3 con chiave a 1024 bit.

2.1.2 Verifica delle credenziali utente

Effettuato l'handshake SSL, vengono verificate le credenziali dell'utente contenuto nell'apposito database. La chiave di ricerca è costituita dal codice fiscale.

Vengono autorizzati i soli utenti che risultano registrati e non disabilitati.

Se l'utente è autorizzato il punto di accesso permette la connessione ai servizi resi disponibili così come previsto dalle specifiche tecniche [1].

2.1.3 Controllo CRL

Il Punto di Accesso effettua il controllo delle CRL in fase di autenticazione utente. Il controllo viene effettuato sulla base di file delle CRL memorizzati in locale.

Nel caso in cui il Punto di Accesso non trovi in locale il file della CRL indicato nel relativo campo del certificato di autenticazione presente nella smart card dell'utente, l'autenticazione viene rifiutata. Questa eventualità si può verificare nel caso in cui l'utente stia utilizzando una nuova smart card, il cui certificato di autenticazione è emesso da una CA appena inclusa tra quelle accreditate oppure che stia utilizzando un nuovo Distribution Point della CRL (CDP).

La fase di autenticazione utente gestita dal Punto di Accesso prevede le attività così come di seguito riportate.

All'atto della richiesta di accesso all'area riservata (login), il Punto di Accesso verifica:

- che la smart card sia inserita nel lettore e che il relativo certificato di autenticazione sia formalmente corretto;
- che il certificato sia emesso da una Certification Authority riconosciuta presso il Punto di Accesso[4];
- che il certificato sia in corso di validità (non scaduto e non revocato).

In caso di esito negativo dei controlli viene inviata al client una pagina contenente il messaggio di errore.

Il controllo che la smart card sia inserita nel lettore viene eseguito alla ricezione di ogni richiesta da parte del client.

Il PdA verifica che il certificato non sia stato revocato o sospeso, accedendo ai dati della CRL (Certificate Revocation List) pubblicata dalla Certification Authority che ha emesso la smart card. Il controllo della CRL è effettuato su file locale, che viene aggiornato periodicamente.

È anche possibile configurare il PdA per verificare o meno che la CRL a disposizione sia in corso di validità o sia scaduta.

In caso di esito negativo del controllo viene inviata al client una pagina contenente il messaggio di errore.

Il PdA estrae i dati identificativi dell'utente registrati nel certificato di autenticazione.

Il PdA verifica che l'utente cui appartiene la smart card, identificato dal codice fiscale, sia registrato sul PdA e sia abilitato ad operare.

Il controllo che il certificato di autenticazione registrato nella smart card appartenga ad un soggetto abilitato ad operare viene effettuato nel seguente modo:

- il PdA estrae dai dati del certificato il codice fiscale;
- verifica che l'utente identificato dal codice fiscale sia registrato nel database del PdA;
- verifica che l'utente cui appartiene il certificato sia abilitato ad operare (stato dell'utenza = attivo);
- associa i dati dell'utente (codice fiscale, cognome, nome, data ultimo accesso, ruolo, ecc.) alla sessione.

In caso di esito negativo del controllo viene inviata al client una pagina contenente il messaggio di errore.

La data di ultimo accesso dell'utente viene aggiornata nel database.

[4] Il modulo di autenticazione per effettuare le opportune verifiche deve avere installato in locale il certificato server della CA che ha emesso il certificato di autenticazione. I certificati server delle CA devono essere preventivamente caricati sul Punto di Accesso dall'Amministratore.

Al termine delle suddette verifiche viene inviata all'utente una home page dove sono presenti i dati dell'utente (cognome, nome, data ultimo accesso, ecc.) e le funzionalità disponibili.

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

Il flusso sopra descritto viene sintetizzato nella figura seguente.

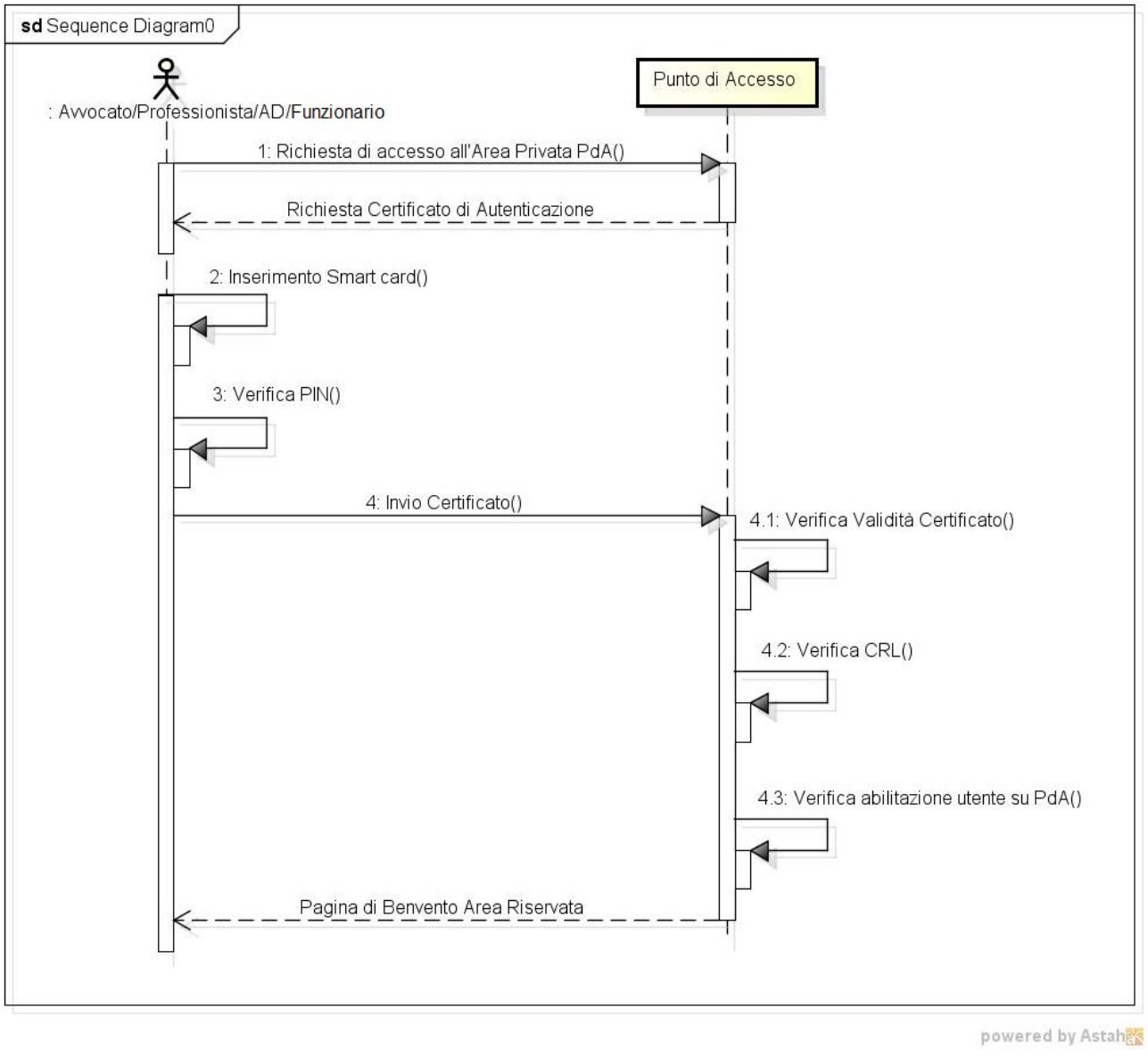

Figura 1 – Autenticazione utente

Dettagli sul flusso

L'entrata nell'Area Privata del Punto di Accesso da parte dell'utente prevede l'utilizzo del protocollo http con SSL e richiede la mutua autenticazione tramite certificati digitali.

Il diagramma che segue illustra le componenti del Punto di Accesso coinvolte nell'elaborazione.

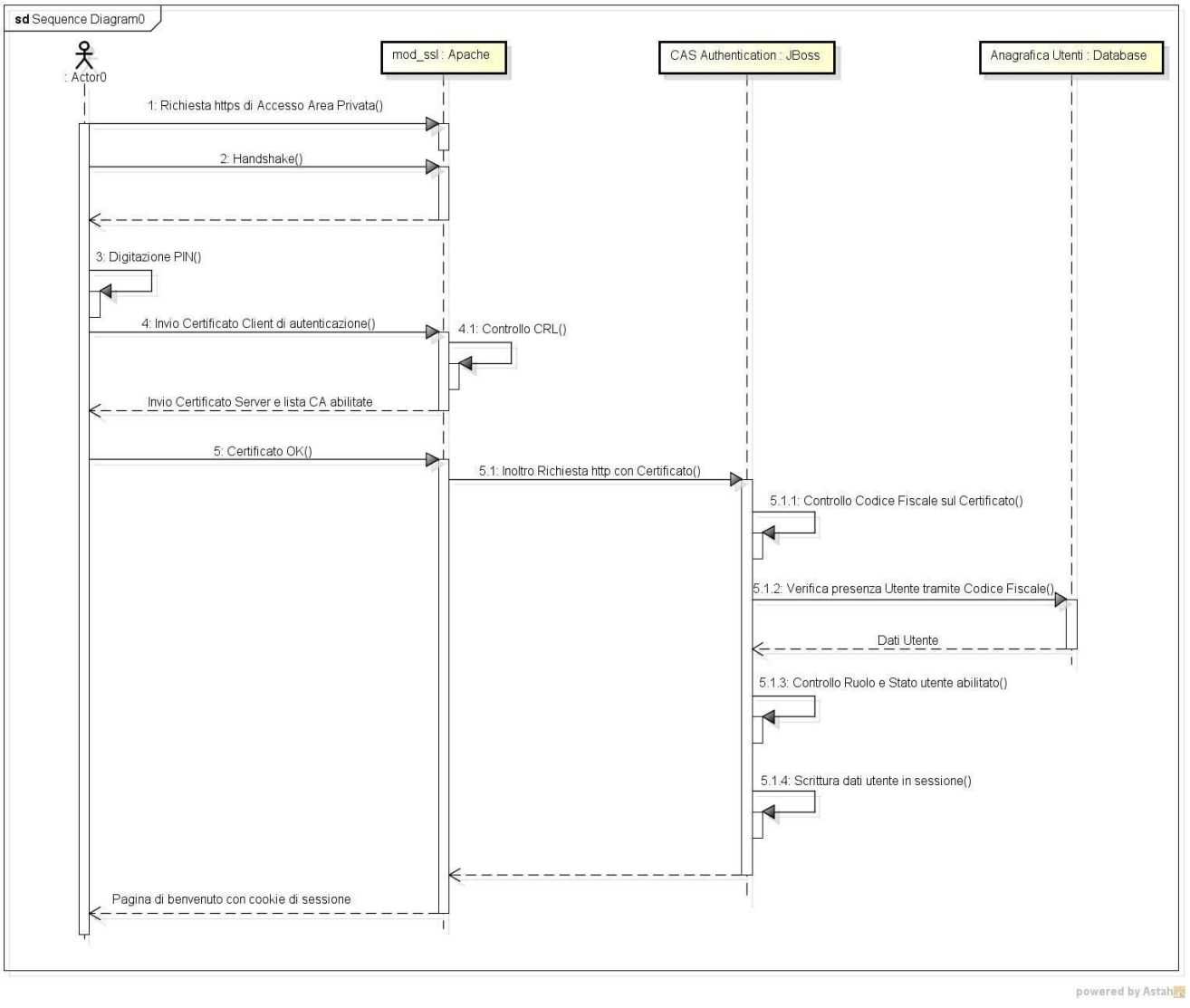

Figura 2 – Sequence Diagram della richiesta di Autenticazione con Smart Card

Spiegazione:

Il diagramma si riferisce agli oggetti che vengono utilizzati durante l'attivazione della sessione dell'utente che accede all'area privata del punto di accesso.

L'utente, con la propria smart card inserita nel lettore, seleziona la URL relativa al punto di accesso (https://pda.lepida..net). L'opzione richiama una risorsa web protetta del web server Apache il cui accesso avviene attraverso il

protocollo https ed è soggetto a mutua autenticazione con l'uso di certificati digitali.

A questo punto inizia l'operazione di *handshake* tra il browser ed il modulo mod_ssl di Apache, il cui ruolo è quello di occuparsi della gestione delle chiamate con protocollo https. Il web server Apache rimanda al browser il proprio certificato pubblico e l'elenco delle Certification Authority abilitate all'utilizzo delle funzionalità del punto di accesso.

L'utente seleziona il proprio certificato di autenticazione sul browser e digita il PIN che viene richiesto per il suo utilizzo. Il certificato pubblico viene inviato al modulo mod_ssl del web server Apache che si occupa di effettuarne la validazione, controllando la sua struttura, la data di scadenza e la presenza del flag che indichi che il certificato è abilitato all'utilizzo per Autenticazioni Client.

Ogni eventuale errore che possa verificarsi nelle fasi sopra descritte, oppure nel caso in cui l'utente tolga dal lettore la Smart Card in qualsiasi fase di utilizzo dell'applicazione PdA dopo aver acceduto all'Area Privata, viene intercettato dal modulo mod_ssl. Il messaggio di errore generato viene interpretato in modo diverso da ciascun browser. Nella figura seguente viene riportata la pagina di errore generata dal browser Internet Explorer. Altri browser (es. Mozilla Firefox) non generano alcun messaggio di errore.

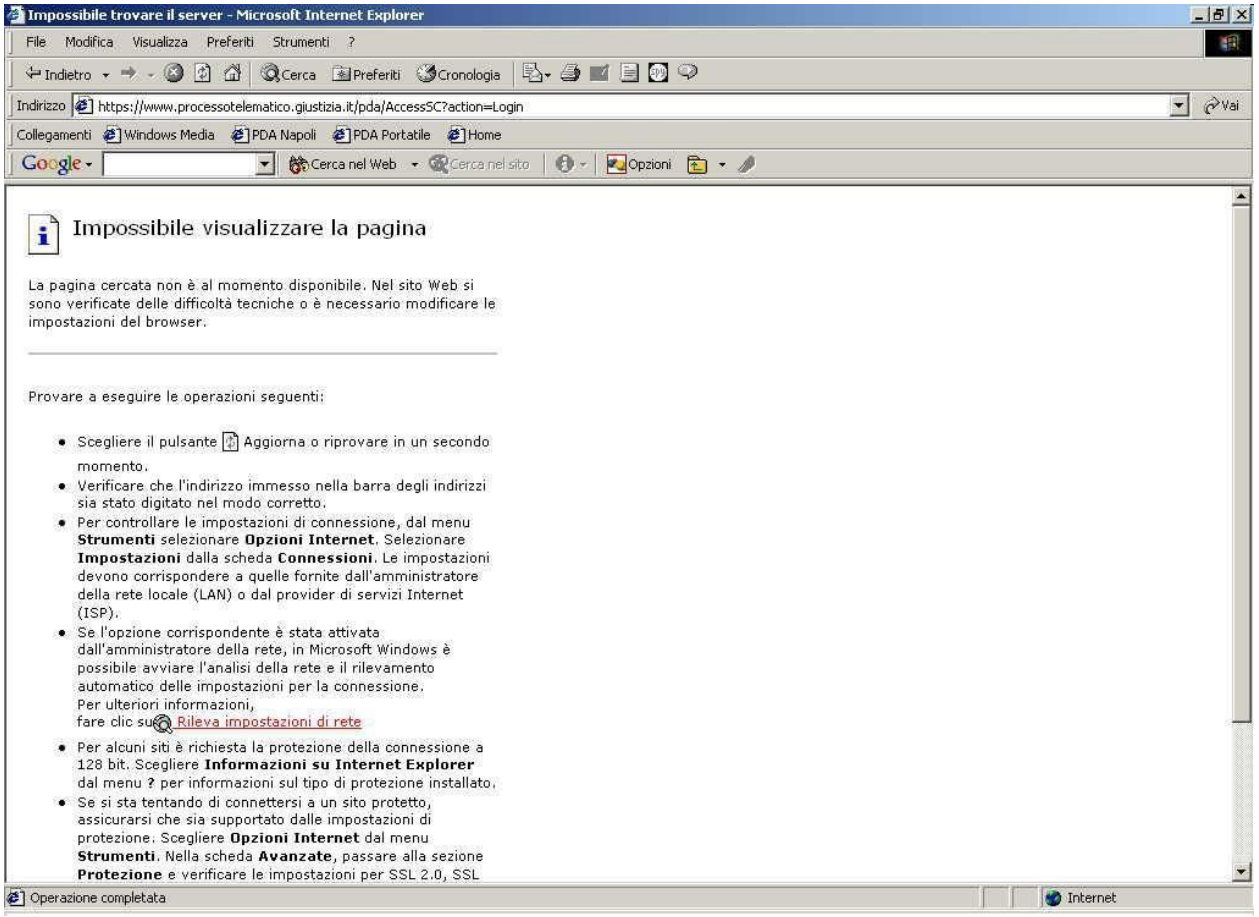

Figura 3 - Pagina di errore generata da IE in fase di Autenticazione SSL

Se tutti i controlli sono superati, ovvero viene verificata la validità del certificato digitale verso le liste di revoca (CRL) della CA emittente e che la CA che ha emesso il certificato sia abilitata ad operare sul PdA, Apache crea un proprio identificativo di sessione e la richiesta http, insieme col certificato digitale utente, prosegue verso il modulo CAS installato sull'application server JBoss dell'applicazione PdA.

Il modulo CAS ricerca e preleva dal Certificato Digitale contenuto nella richiesta http il Codifice Fiscale dell'utente e verifica che l'utente sia iscritto e abilitato all'accesso al PdA.

Nel caso in cui i controlli non siano superati l'utente viene rediretto su una pagina di errore.

Nel caso in cui i controlli diano esito positivo, l'utente viene rediretto alla Pagina di Benvenuto del PdA.

Nella richiesta http contenente la pagina di risposta viene anche inserito un cookie contenente un ID univoco della sessione JBoss. Tale cookie verrà utilizzato dal browser nelle chiamate successive verso il Punto di Accesso per poter identificare la sessione corrente.

2.2 Autenticazione a due fattori (One Time Password)

L'autenticazione a due fattori si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia 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).

La scelta operata è di effettuare l'autenticazione forte tramite l'utilizzo congiunto dei seguenti due fattori di autenticazione individuale:

- "Una cosa che conosci": una password
- "Una cosa che hai": un dispositivo mobile

Non si sono introdotte informazioni biometriche "qualcosa che sei" in quanto critiche sia per l'utilizzo (device specifici) sia per la tutela della privacy nell'utilizzo di informazioni biometriche.

2.2.1 Flusso di autenticazione

L'autenticazione viene effettuata da una specifica applicazione mobile (disponibile per tutte le piattaforme mobili: Android, iOS, Windows Phone).

Il meccanismo di autenticazione è basato su una applicazione specifica per Punto di Accesso ovvero una specifica app autenticherà solo e soltanto gli utenti del Punto di Accesso cui è espressamente dedicata.

Tale applicazione genera le chiavi OTP (One Time Password), ovvero codici dinamici di autenticazione che cambiano ad ogni utilizzo rendendo praticamente impossibile la sottrazione di credenziali. Ciascuna chiave generata ha una durata entro la quale la chiave deve essere utilizzata. Tale durata viene configurata nell'ottica di limitare la finestra di vulnerabilità del sistema.

La generazione dei codici è univoca per ciascun dispositivo attivato, in quanto i dati relativi al dispositivo vengono utilizzare per la generazione delle chiavi. In questo modo si garantisce che la chiave generata sia indissolubilmente legata allo specifico dispositivo che quindi viene a costituire il fattore di autenticazione "Una cosa che hai".

La generazione dell'OTP richiede l'inserimento di un PIN code, obbligatorio e scelto dall'utente. Questa informazione rappresenta il fattore di autenticazione "Una cosa che conosci". L'applicazione richiede obbligatoriamente l'inserimento del PIN, senza permetterne il salvataggio, ad ogni avvio per evitare furti di identità dovuti a sottrazione di dispositivi altrui.

Si precisa che:

- Il PIN non rimane all'interno del dispositivo e non viene conosciuto, nemmeno in parte, dal servizio di erogazione
- La verifica del PIN avviene attraverso meccanismi di hashing (SHA-256)
- Il PIN rappresenta inoltre una chiave crittografica che permette la generazione di un OTP valido
- La lunghezza del PIN deve essere di minimo 8 caratteri
- È possibile effettuare al massimo tre tentativi di inserimento del PIN, se errato. Al terzo tentativo fallito l'istanza dell'applicazione sul dispositivo mobile viene resettata ed è necessario una nuova attivazione del dispositivo con autenticazione forte sul PdA (token crittografico)

Al fine di garantire la massima sicurezza agli utenti occorre proteggere il device: il rischio è che il dispositivo possa essere stato "aperto" permettendo alle applicazioni l'accesso al sistema operativo. Tale scenario potrebbe portare all'implementazione di un'applicazione "malvagia" che implementi il classico "man in the middle" tra l'applicazione di generazione delle chiavi OTP ed il sistema operativo impossessandosi di chiavi "buone". Si è reso necessario integrare all'interno dell'applicazione specifici meccanismi che rilevano "jailbreak" e "rootkit", se vengono rilevati l'applicazione avverte e non genera alcuna chiave.

Si sono implementati meccanismi specifici per evitare attacchi con tecnica di "forza bruta" ovvero quando il backend rileva tentativi ravvicinati nel tempo per il medesimo utente.

Di seguito il flusso di autenticazione così come descritto:

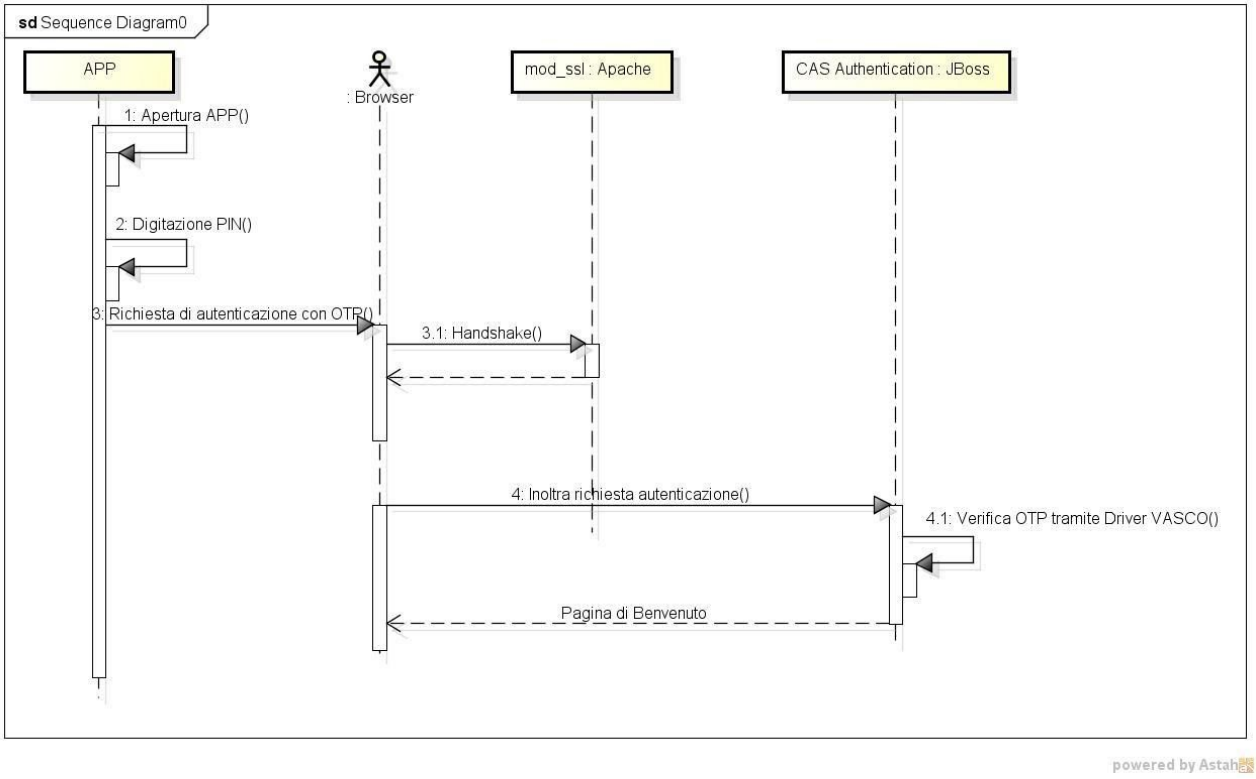

Figura 3 – Sequence Diagram della richiesta di Autenticazione con OTP

2.2.2 Meccanismo di Provisioning

Un momento particolarmente critico è il provisioning del meccanismo di autenticazione ovvero stabilire la relazione tra dispositivo ed utente del Punto di Accesso.

L'attivazione avviene solamente dal PdA a valle dell'autenticazione forte come da regole tecniche per smart card e/o USB token. Questa modalità assicura che sia certificata la titolarità dell'utente che collega il dispositivo alla propria utenza.

Il "seme" di autenticazione viene incapsulato all'interno di un QR-CODE che sarà reso disponibile all'interno del PdA a seguito di autenticazione forte. Tale QR-CODE è accessibile tramite una funzionalità dedicata che permette all'utente di fotografarlo per completare la procedura di attivazione del dispositivo mobile. Attraverso l'inserimento del codice di 25-26 caratteri ottenuto a seguito della fotografia del QR-CODE dalla APP installata sul dispositivo mobile, è possibile l'associazione del dispositivo al token di autenticazione.

Visto il meccanismo di cui sopra, ne deriva che il "seme" di autenticazione non sia facilmente leggibile e/o duplicabile nemmeno da un utente che "veda il medesimo schermo".

2.2.3 Meccanismo di revoca

Al fine di assicurare un altro grado di sicurezza anche nella malaugurata ipotesi di smarrimento del dispositivo (inizializzato come descritto in precedenza) basterà effettuare il login secondo le modalità standard al Punto di Accesso (Smart card CNS/ USB token) dove si troverà un'apposita funzionalità utente che disattiva, con effetto immediato, il dispositivo che da quel preciso istante non potrà più autenticarsi.

Per facilitare il processo di revoca nell'ipotesi in cui l'utente non sia in grado di effettuare login con autenticazione forte sul PdA è possibile contattare il supporto tecnico del PdA per richiedere l'immediata revoca del dispositivo.

2.2.4 Meccanismo di Rinnovo

Il meccanismo di attivazione ha una durata nota all'utente. Alla scadenza del servizio il dispositivo mobile non sarà più in grado di autenticare l'utente. L'utente sarà avvisato tramite email ed un'indicazione sul Pda, a partire dal mese precedente la scadenza.

Il rinnovo avviene introducendo una nuova chiave nel registro delle abilitazioni con la nuova scadenza ed invalidando la precedente chiave. Si noti che per il rinnovo non è necessario procedere ad una nuova operazione di provisioning (prevista nel caso si sostituzione del dispositivo abilitato).

L'utente procede al rinnovo nell'ambito delle funzioni di amministrazione personale del Punto di Accesso ovvero a valle di un'autenticazione forte (eventualmente anche da piattaforma mobile se si dispone di altro dispositivo abilitato).

2.2.5 Registro delle abilitazioni

Il registro delle abilitazioni è una "estensione" della base dati del Punto di Accesso e ne eredita tutti gli oneri di sicurezza (si faccia riferimento al documento Piano della sicurezza per i dettagli).

Tale registro lega a ciascun token di autenticazione il Codice Fiscale dell'utente che accede al PdA.

3 Funzionalità esposte dal PdA

Le funzionalità esposte dal PdA sono riconducibili ai servizi esposti dal Ministero della Giustizia così come previsto nella documentazione presente nel portale dei servizi telematici:

http://pst.giustizia.it/PST/resources/cms/documents/Documentazione_servizi_web_v1.16.pdf

Sono inoltre previste funzionalità specifiche del PdA che non prevedono alcun interfacciamento con i servizi esposti da Giustizia.

L'applicazione client interagisce con i web services esposti dal PDA previa autenticazione forte, cioè l'accesso a tali funzionalità viene autorizzato secondo quanto previsto al capitolo 2. Inoltre, per i soggetti diversi dal legale

rappresentante e dai suoi delegati, viene effettuata la verifica della presenza del soggetto sul ReGIndE.

Gli utenti del PdA autorizzati possono accedere alle informazioni afferenti ai fascicoli giudiziari di Lepida S.c.p.A. o degli Enti Controllanti sia per PARTE sia attraverso il proprio ruolo di Avvocato/Funzionario dell'Ente per la consultazione dei fascicoli di propria competenza.

Sono previste inoltre le funzionalità Consultazione dei soggetti iscritti a ReGIndE o la ricerca delle PEC delle PP.AA.

La funzionalità di Pagamento Telematico è disponibile utilizzando i servizi messi a disposizione dal nodo dei pagamenti telematici-SPC. Sono utilizzati tutti i metodi di pagamento esposti dal PSP, demandano allo stesso la gestione in base ai prestatori dei servizi di pagamento.

Il PdA tiene traccia dell'accesso ai servizi esposti da Giustizia da parte degli utenti del PdA senza alcuna tracciatura dei contenuti di richiesta o risposta.

Le informazioni registrate nei log delle varie componenti del sistema sono le seguenti:

- Codice fiscale dell'utente
- Codice fiscale dell'utente delegato e del delegante (se la consultazione è per delega)
- Client di invocazione, distinguendo tra PdA Web e Desktop Client
- Gestore locale di destinazione

4 DELEGA DI UN SOGGETTO AI SERVIZI DI CONSULTAZIONE

Il PdA, conformemente a quanto specificato nelle regole tecniche [Rif. 2] ART. 7 comma 2, consente l'accesso ai servizi di consultazione offerti da Giustizia sia nella forma di soggetto abilitato sia come soggetto delegato, ai soggetti presenti sul ReGIndE, al legale rappresentante della Società intestataria del PdA e ai soggetti da lui delegati.

Le modalità di accesso al sistema sono le medesime previste al capitolo 2.

Il desktop client del PdA espone la funzionalità di delega FASCICOLO attraverso la quale un utente registrato al PdA può delegare un altro soggetto, sia iscritto che non al PdA. Nel caso in cui il soggetto delegato non sia iscritto al PdA, viene censito tra i soggetti iscritti con ruolo SOGGETTO DELEGATO. Tale ruolo consentirà la visibilità dei soli fascicoli del soggetto delegante. Il PdA inibisce, quindi, al soggetto delegato non iscritto al PdA qualsiasi accesso alle funzionalità di consultazione offerte da Giustizia con il proprio codice fiscale. Nel caso in cui il soggetto delegato sia un iscritto al PdA, le funzionalità di consultazione saranno disponibili con entrambi i profili (CF delegato e delegante).

Si sottolinea che l'attivazione del meccanismo di delega FASCICOLI, attraverso il desktop client del PdA, prevede che il soggetto delegante firmi digitalmente l'atto di delega che sarà archiviato all'interno del PdA per 5 anni. È prevista la

funzionalità di revoca della delega che comporta il caricamento di un documento firmato sul PdA, archiviato per 5 anni sul PdA, e l'inibizione all'accesso ai fascicoli del soggetto delegante.

È possibile la delega anche da parte del legale rappresentante a soggetti cui vuole consentire la consultazione di fascicoli per PARTE, in cui la parte è rappresentata dalla società intestataria del PdA. In questo caso l'Amministratore si occupa di inserire una o più deleghe ad un soggetto, verifica che siano firmate da un legale rappresentante, quindi è tenuto a firmarle digitalmente e a caricarle sul PdA affinchè siano salvate; il PdA ne verifica la firma. È possibile la revoca di una o più deleghe date all'utente, attività sempre in carico all'Amministratore che prevede sempre il caricamento sul PdA del documento di revoca firmato e l'attribuzione della revoca.