

MANUALE TECNICO RELATIVO AL PROCESSO DI FIRMA ELETTRONICA AVANZATA RELATIVO AI SERVIZI "MANPOWER ON LINE"

SISTEMA DI FIRMA ELETTRONICA AVANZATA

Il sistema di firma elettronica utilizzato dal Portale è basato su HSM CoSign ed è esclusivamente dedicato al Portale stesso. HSM CoSign è un sistema di firma ad alta sicurezza certificato FIPS 140-2 level 3 ed in via di certificazione Common Criteria EAL4+. E' un prodotto conforme alla normativa Italiana per la generazione di firme elettroniche avanzate, firme elettroniche qualificate e firme digitali: DPCM 19 luglio 2012 sugli HSM ed il DPCM 22 febbraio 2013 (Regole tecniche sulla firma elettronica)

Ogni chiamata del portale verso il sistema di firma è autenticata e protetta con protocollo HTTPS.

Il sistema di firma è costituito da due HSM CoSign in cluster (in modo conforme all'art. 8 comma 4 DPCM 22 febbraio 2013) e da un front end securizzato di gestione del servizio di firma (FirmaRemota Virtual Box).

La sicurezza del sistema di autenticazione per la firma elettronica avanzata è basata sulla password che autentica il firmatario ed una One Time Password (OTP) a 6 cifre generata con il protocollo standard OATH HOTP (RFC 4226). L'OTP viene inviato al cellulare del firmatario. Per eseguire la firma è necessario che il firmatario digiti l'OTP ricevuto nella form. La chiave privata, generata all'interno di HSM CoSign ed il certificato di firma vengono utilizzati in modalità ONE SHOT, ovvero generati on the fly al momento della sessione di firma ed automaticamente distrutti al termine della sessione. Il periodo di validità del certificato è di soli 5 minuti. E' quindi garantito che lo stesso certificato non può essere usato in sessioni differenti. L'HSM CoSign viene anche utilizzato per la sottoscrizione del documento da parte di Manpower con una firma elettronica qualificata erogata nella modalità di sottoscrizione con procedura automatica (art. 35 comma 3 del Codice dell'Amministrazione Digitale).

ATTIVAZIONE DEL SERVIZIO E REVOCA

I candidati interessati al servizio di Missioni On Line si potranno recare in una filiale Manpower, dove un operatore di filiale, adeguatamente formato sulle procedure, esporrà loro il contratto di servizio e il relativo contratto di attivazione della firma elettronica avanzata.

Il candidato sarà quindi attivato come da procedura di attivazione descritta nel paragrafo seguente.

L'operatore di filiale stamperà la documentazione per l'attivazione di firma elettronica avanzata e la farà sottoscrivere al candidato in duplice copia. Una copia verrà consegnata al candidato, mentre l'altra copia sarà archiviata da Manpower sia attraverso il sistema documentale Docsweb attualmente in uso nelle filiali, sia attraverso il sistema fisico di archiviazione.

I clienti che vogliono aderire al servizio di Missioni On Line di Manpower potranno recarsi in filiale, oppure potranno richiedere una visita presso la propria sede di un agente di Manpower.

Il cliente definirà per il servizio di firma elettronica avanzata gli account che potranno firmare i contratti. Gli account saranno quindi attivati come da procedura di attivazione descritta nel paragrafo seguente.

L'operatore di filiale stamperà la documentazione per l'attivazione di firma elettronica avanzata per ogni account e la farà sottoscrivere agli account in duplice copia. Una copia verrà consegnata all'account, mentre l'altra copia sarà archiviata da Manpower sia attraverso il sistema documentale Docsweb attualmente in uso nelle filiali, sia attraverso il sistema fisico di archiviazione.

ATTIVAZIONE UTENTI DEL PORTALE E DEL SISTEMA DI FIRMA

Il processo di attivazione, di seguito descritto, è il medesimo sia per il candidato sia per l'account del cliente.

L'utente di filiale riconosce l'utente (candidato o referente del cliente) attraverso un documento di identità in corso di validità e ne richiede una copia da archiviare contestualmente al contratto di attivazione. Se non presente nell'anagrafica di PowerBase, inserisce la nuova anagrafica di contatto con i relativi servizi sottoscritti e stampa i contratti di servizio e di attivazione della firma elettronica avanzata su cui è riportato l'indirizzo e-mail e il cellulare utilizzati per il servizio. Il sistema PowerBase genererà per ogni utente uno username (codice generato casualmente) e una password temporanea (generazione casuale).

Attraverso un web service PowerBase invierà al sistema portale i seguenti dati per ogni utente:

- Username personale
- Password temporanea
- Cellulare (presente sul contratto di accettazione d'uso della Firma Elettronica Avanzata FEA)
- E-mail (presente sul contratto di accettazione d'uso della FEA)
- Anagrafica (es. IDCliente, IDLavoratore, flag servizi attivati, ecc)

Il portale creerà nella tabella degli utenti una nuova riga, impostando il campo 'Primo accesso' a zero e il campo 'Data scadenza password' su scaduta e invierà all'utente tramite e-mail le credenziali di primo accesso.

Al primo accesso l'utente inserirà sul portale Username personale e Password temporanea. Il portale richiederà il cambio password. La password è un campo obbligatorio per poter proseguire.

La nuova password dovrà rispettare le seguenti regole semantiche:

- Deve essere lunga almeno 8 caratteri.
- Deve contenere almeno una lettera Maiuscola.
- Deve contenere almeno una lettera Minuscola.
- Deve contenere almeno un numero.

La validità della password è di 30 gg ed al rinnovo non potranno essere utilizzate le precedenti 13 password già utilizzate. La nuova password non sarà memorizzata in nessun punto del portale ma verrà archiviata l'impronta HASH della stessa. Non è possibile quindi recuperare la password dimenticata ma verrà rinnovata con la procedura di "Password Dimenticata". Per cambiare la password al primo accesso il portale invierà un'e-mail all'utente con un link. Solo quando l'utente accederà al link in oggetto, la nuova password sarà attivata e l'utente sarà effettivamente attivo per i servizi sopra descritti.

E-mail e numero di Cellulare di ogni account sono gli unici dati che potranno essere modificati solo dall'utente sul portale e validati (attraverso mail + link di validazione) prima di essere inseriti in anagrafica e trasferito a PowerBase.

Ad ogni modifica di anagrafica, PowerBase e il Portale comunicheranno le variazioni tramite web services, nei due sensi, ad esclusione di e-mail e cellulare le cui modifiche saranno scambiate solo dal Portale verso Powerbase

Accessi successivi al primo, potranno essere effettuati dall'account utilizzando a scelta il proprio Username personale, o l'indirizzo mail registrato.

L'utente nella pagina di login ha la possibilità di cliccare su "password dimenticata". Il portale richiede quindi di inserire Username e indirizzo e-mail. Il portale quindi controlla:

- 1) Che esista lo username.
- 2) Che l'e-mail inserita sia uguale a quella in anagrafica per lo username specificato.

In caso di errore restituisce un messaggio che riporta "La Username o l'email non sono corrette"

Se invece le due condizioni sono vere il portale invia un'e-mail con un link che mi porta alla pagina di modifica password.

Gli utenti del portale che hanno aderito al servizio di firma elettronica avanzata, saranno attivati anche sul sistema di firma. Il portale attraverso un web service invia al sistema di firma i dati anagrafici dell'utente. L'utente viene attivato sul sistema di firma e viene rilasciato un certificato di firma temporaneo associato ad un indirizzo e-mail e al cellulare specifico a cui saranno inviati le OTP (One Time Password).

REVOCA DEL SERVIZIO DI FIRMA ELETTRONICA AVANZATA

L'utente potrà revocare in ogni momento il consenso all'utilizzo della firma elettronica avanzata mediante richiesta da inviare per iscritto agli indirizzi in calce alle Condizioni Generali dei Servizi "Manpower on Line" tramite raccomandata A.R o fax. La Società provvederà a disattivare la modalità di firma entro il giorno lavorativo successivo a quello in cui ha ricevuto la comunicazione di revoca. Nel caso in cui l'utente revocherà il servizio di firma elettronica avanzata non potrà più utilizzare i servizi "Manpower On Line" e quindi sarà disabilitata l'utenza sul portale.

ARCHIVIAZIONE DEI DOCUMENTI FIRMATI

I documenti sottoscritti tramite firma elettronica avanzata saranno archiviati nel sistema documentale Docsweb centralizzato e consultabili tramite browser da Manpower.

I dati a corredo dei documenti per poterli ricercare in modo semplice ed efficace seguiranno le logiche attualmente in uso per i documenti cartacei.

Il sistema documentale non permette agli utenti la modifica dei dati o dei documenti inseriti nello stesso, in quanto sono in sola lettura.

ARCHIVIAZIONE DIGITALE DEI DOCUMENTI FIRMATI

I documenti sottoscritti tramite firma elettronica oltre ad essere archiviati sul documentale, saranno trasmessi al sistema di archiviazione digitale.

Il pacchetto di documenti corredati dai dati identificativi, saranno trasmessi via FTPS all'outsourcer che, una volta validato il pacchetto, provvederà mensilmente alla conservazione digitale degli stessi secondo il manuale di conservazione digitale.