SERVIZIO DI CERTIFICAZIONE TERNA
MANUALE UTENTE INTERNET - ISTRUZIONI TECNICHE PER L'UTILIZZO DEL SERVIZIO

Storia delle revisioni

Rev. n°	Data	Descrizione
01	23/08/2010	Prima emissione del documento.
02	24/09/2010	Aggiornamento printscreen emissione certificati e paragrafo Firma Digitale
03	25-02-2021	Aggiornamento printscreen nuovo portale

Redatto	Verificato	Verificato	Verificato	**Approvato**
Innovery S.p.A.	D. Guida (DSC-TSP-ESM)	F. De Sanctis (DSC-TSP-ESM)		P. Vaccaro (SA-IS-CSI)

INDICE

1. SCOPO DEL DOCUMENTO

Il presente manuale contiene le istruzioni tecniche per l'utilizzo del Portale del Certificatore di Terna S.p.A. per un utente INTERNET.

2. DEFINIZIONI E ACRONIMI

SIGLA	DEFINIZIONE	RIFERIMENTO
CA	Certification Authority	
DES	Data Encryption Standard, è un algoritmo di cifratura.	American National Standards Institute, ANSI X3.106, "American National Standard for Information Systems - Data Link Encryption"
DM	Directory Master	Server LDAP Master usato come repository principale dei certificate
DS	Directory Shadow	Server LDAP Shadow, usato come copia del repository dei certificate
DSA	Directory Server Agent	
E.E.S.P.	Entrust Entelligence Security Provider	
FE	Front End	
IESG	Internet Engineering Steering Group. Il gruppo che sovrintende a IETF e determina quali proposte diventano standard.	http://www.ietf.org/iesg.html
IP	Internet Protocol	
LDAP	Lightweight Directory Access Protocol. Protocollo di accesso alle directory X.500	RFC 1777 – RFC 2251
PKI	Public Key Infrastructure.	
PKIX	Internet X.509 Public Key Infrastructure. Il nome del gruppo di lavoro IETF che crea standard per la PKI in Internet.	http://www.imc.org/ietf-pkix/
RFC	Request For Comments. Il metodo utilizzato da IETF per pubblicare documenti	
RSA	Rivest-Shamir-Adelman. Nome di un algoritmo di cifratura a chiave pubblica. E' anche il nome della società che controlla i diritti di utilizzo dell'algoritmo	RFC 2313
SAN	Storage Are Network	
SAS	Self Administration Server	Prodotto Entrust per la Gestione del ciclo di vita dei titolari
SDK	Software Development KIT	
S.M.A.	Security Manager Administration	Prodotto Entrust per l'amministrazione della Certification Authority
SNMP	Simple Network Management Protocol	
SP	Security Policy	
SSL	Secure Sockets Layer. Protocollo di cifratura e d autenticazione per le connessioni Internet	Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., Feb 9, 1995. A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.
TLS	Transport Layer Security. La versione standard di SSL	RFC 2246
TP	True Pass	Prodotto Entrust per la gestione delle procedure di Autenticazione alle applicazioni

		Web.
URI	Uniform Resource Identifier	RFC 2396
URL	Uniform Resource Locator. Metodo per identificare una risorsa in Internet.	RFC 1738, 1808, 2368, 2396
X.500	Specifiche per server di directory e modalità di accesso alle stesse	ITU-T Recommendation X.500 (1997), ISO/IEC 9594-1:1997, Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services
X.509	Specifiche per il formato dei certificati digitali.	ITU-T Recommendation X.509 (1997), ISO/IEC 9594-8:1997, Information technology - Open Systems Interconnection - The Directory: Authentication framework.
VPN	Virtual Private Network	

3. PORTALE DI CERTIFICAZIONE

3.1. PREREQUISITI

Di seguito sono elencati i requisiti richiesti per l'utilizzo del Portale di Certificazione:

- Sistema operativo:
  - Microsoft Windows XP Pro SP1, SP1a or SP2
  - Microsoft Windows XP Home
  - Microsoft Windows Svr 2003 Ent
  - Microsoft Windows 2000 Server
  - Microsoft Windows 2000 Pro
- Browser internet e java runtime

Browser	**JVM**
Mac Safari 1.2 (OSX 10.3)	Apple Java Plugin 1.4.2*
Microsoft Internet Explorer 5.5-6.0 SP1/SP2	Sun Java Plugin 1.4.2/1.5**, MS JVM*****
Microsoft Internet Explorer 6.0 SP1/SP2 and 7.0 (on Microsoft XP only)	IBM JRE versions 1.4.2 and 1.5.0
Microsoft Internet Explorer 7.0****	Sun Java Plugin 1.4.2+/1.5.0_04+, MS JVM*****
Netscape Navigator 7.0	Sun Java Plugin 1.4.2, Browser Built in JVM
Mozilla FireFox	Sun Java Plugin 1.4.2
Mozilla 1.7.2 (Fedora Core 2)***	Sun Java Plugin 1.5**
Mozilla 1.7.2	Sun Java Plugin 1.4.2

1- Apple Java Plugin 1.4.2_05 (Update 1) is not supported
2- Apple Java Plugin 1.4.2_05 (Update 2) requires a workaround from Apple due to a problem introduced in the Update 2 release. Please contact Apple support for additional information (i.e. Signed Applet initialization problems).
**Note:Our testing currently indicates that Sun Plugin 1.5 is unstable when used with Netscape Navigator 7.0, Mozilla 1.7.2, and Mozilla FireFox 0.9.3. As such, Sun Plugin 1.5 will only be supported with IE 6.0 on Windows and Mozilla 1.7.2 on Fedora Core 2.
***Note:Alternative Linux distributions (RedHat, SuSe, Debian, etc.) may work with Mozilla 1.7.2 and the Sun Plugin 1.5, but they have not been tested by Entrust. Customers at their descretion can deploy Entrust credentials to these different Linux distributions, but will need to reproduce any problems experienced on a supported client platform before Entrust Customer Service can provide assistance. Alternatively, Entrust Professional Services can be engaged to perform validation on a particular Linux distribution.
**** Please read: Deploying Entrust products containing Java applets on Microsoft Windows Vista with Internet Explorer 7
Note: What are the known issues with Entrust products containing Java applets and the Sun Java 6 JVM?
***** Microsoft JVM will no longer be supported as of December 31st, 2007. http://www.microsoft.com/mscorp/java/

3.2. HOME PAGE

Il Certificatore Terna ha messo a disposizione su Internet il portale descritto nel presente manuale al fine di semplificare i servizi connessi all'utilizzo dei certificati digitali.

Per utilizzare i servizi di certificazione offerti da Terna ad aziende esterne, è sufficiente seguire le istruzioni messe a disposizione all'interno del portale, la cui home page, mostrata in Figura 7.1., è raggiungibile all'indirizzo https://secureproc.terna.it/PortaleDiCertificazione/

Figura 7.1: Home Page

Il portale dà la possibilità di consultare i manuali contenenti la descrizione delle procedure operative da seguire per acquisire un certificato digitale.

Inoltre, dai link elencati nel menu a destra della home page è possibile accedere alle procedure e alla parte operativa per l'emissione e recovery dei certificati digitali.

I servizi offerti dal Portale di certificazione vengono descritti nei paragrafi successivi.

3.3. SERVIZIO DI CERTIFICAZIONE

Cliccando sul link **INFO** posizionato centralmente in fondo alla home page del Portale del Certificatore, si apre una pagina (Figura 7.2) che elenca i servizi forniti da Terna mediante il Portale di Certificazione:

- generazione delle coppie di chiavi di cifratura;
- recovery delle chiavi di cifratura;
- pubblicazione delle Liste dei Certificati Revocati (CRL).

Figura 7.2: Servizio di Certificazione

3.4. CERTIFICATORE

Selezionando il link **Certificatore** nel menu a destra della home page del Portale del Certificatore si apre una pagina (Figura 7.3) che mostra i dati identificativi del Certificatore.

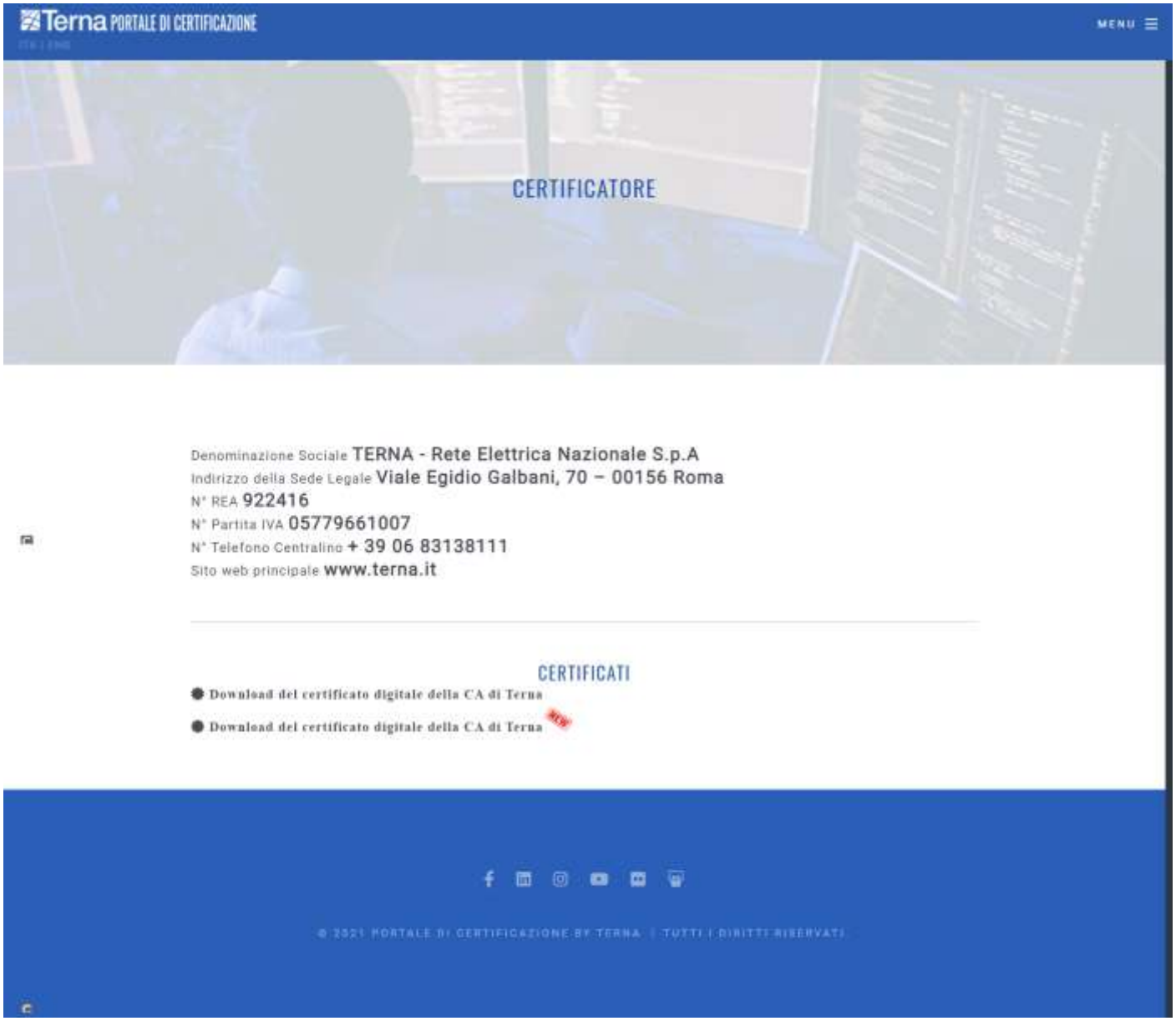

Figura 7.3: Dati identificativi del Certificatore

3.5. MANUALE OPERATIVO

Selezionando il link **Manuale Operativo** nel menu a destra della home page del Portale del Certificatore si apre una pagina (Figura 7.4) che consente di scaricare i manuali operativi che descrivono le regole che governano l'emissione e l'uso dei Certificati sottoscritti dal Certificatore Terna e l'insieme delle procedure operative per l'erogazione dei relativi servizi di certificazione digitale.

Le procedure operative vere e proprie sono poi dettagliate in documenti specifici.

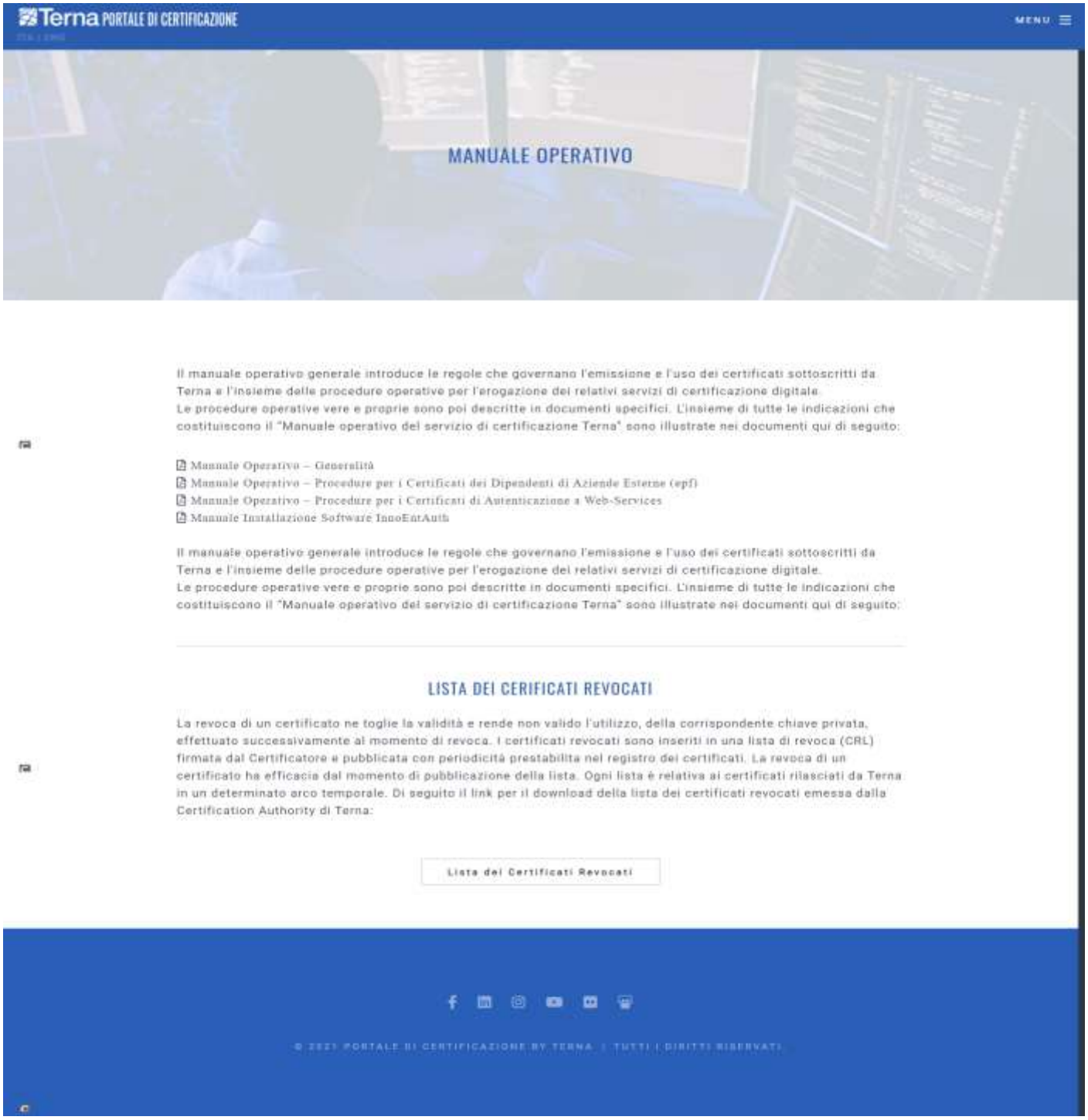

Figura 7.4: Manuali Operativi

3.5.1 LISTA DEI CERTIFICATI REVOCATI

Selezionando il link **Lista dei Certificati Revocati** nella pagina **Manuale Operativo** del Portale del Certificatore (Figura 7.5) e cliccando su **Lista dei certificati revocati** in fondo alla pagina, sarà possibile scaricare la lista dei certificati revocati dalla Certification Authority di Terna.

Figura 7.5: Lista dei Certificati Revocati

3.6. PROCEDURE PER I CERTIFICATI DEI DIPENDENTI DI AZIENDE ESTERNE

Selezionando il link **Procedure per i certificati dei dipendenti di aziende esterne** nel menu a destra della home page del Portale del Certificatore si apre una pagina (Figura 7.6) suddivisa in tre sezioni:

- **Procedure per i Certificati dei Dipendenti di Aziende Esterne**. Da questa sezione è possibile scaricare le procedure operative per l'acquisizione dei certificati da parte dei dipendenti di aziende esterne.
- **Modulistica**. Da questa sezione è possibile scaricare i moduli per la richiesta di Rilascio/ Revoca/Sospensione/Recovery di certificati digitali e per la richiesta di Rilascio dei codici di attivazione per i certificati digitali.
- **Operazioni Automatiche sui certificati**. Da questa sezione è possibile accedere ad ulteriori pagine che consentono di eseguire le procedure per l'emissione/recovery dei certificati digitali.
- **Call Center.** Da questa sezione è possibile reperire i riferimenti utilizzabili per inoltrare eventuali richieste al Certificatore

Figura 7.6: Emissione Certificati EPF per dipendenti di aziende esterne

3.6.1. EMISSIONE DEL CERTIFICATO CON CODICI DI ATTIVAZIONE

Per ottenere l'emissione del certificato con i codici di attivazione, nella pagina mostrata in Figura 7.6 procedere come segue:

1. Selezionare il link **Operazioni Certificati**.
2. Nella pagina visualizzata (Figura 7.7) selezionare il link **Emissione Certificato con codici di attivazione**.

Figura 7.7: Procedure per i certificati per i dipendenti di aziende esterne

3. Inserire (Figura 7.8) *Numero di Riferimento* e *Codice di Autorizzazione*, quindi premere **Conferma** per avviare la richiesta di emissione del certificato.

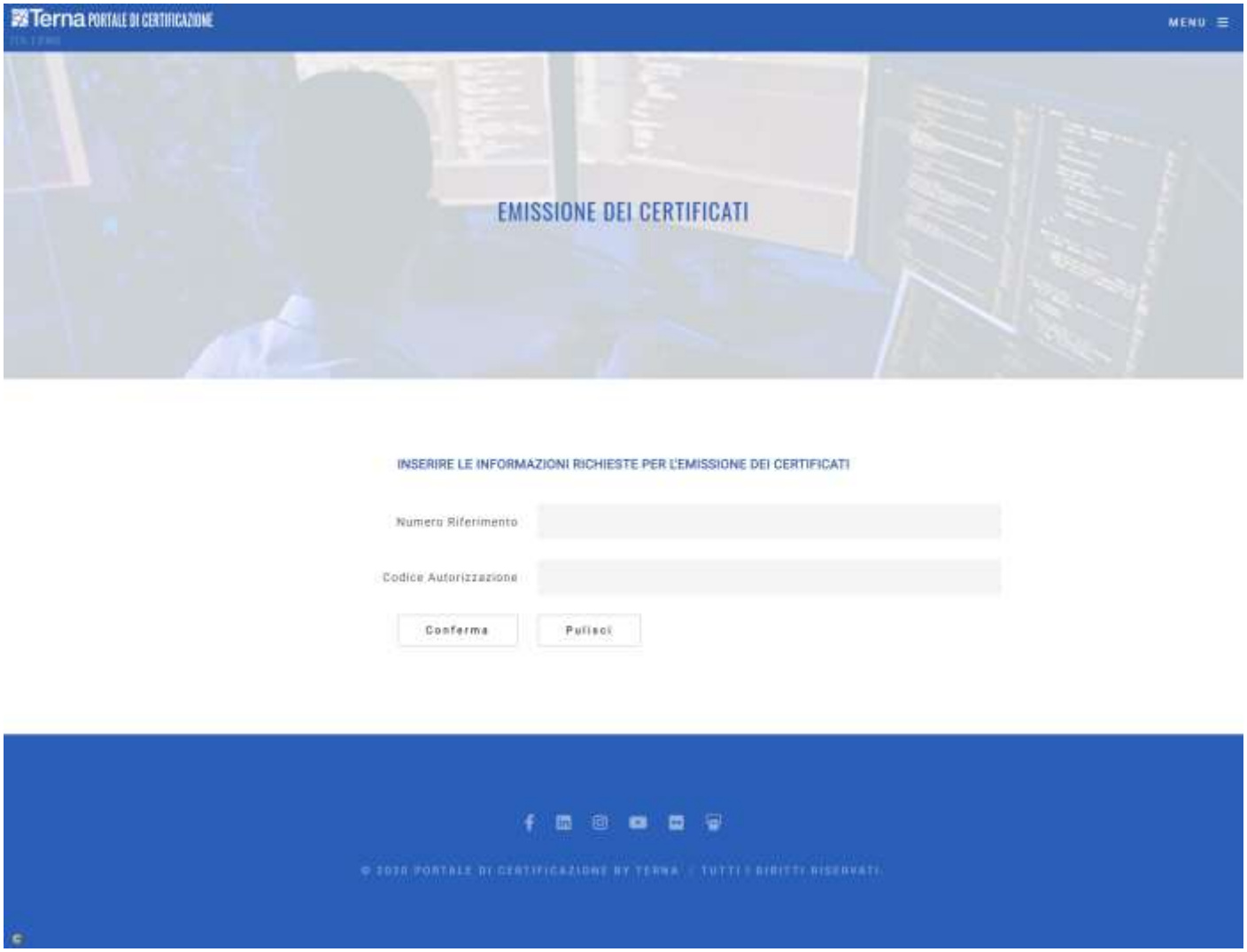

Figura 7.8: Richiesta emissione certificato per i dipendenti di aziende esterne

4. Scegliere il nome del **nuovo** file ".epf" che si sta generando e inserire due volte la password, infine premere **Conferma** (figura 7.9).

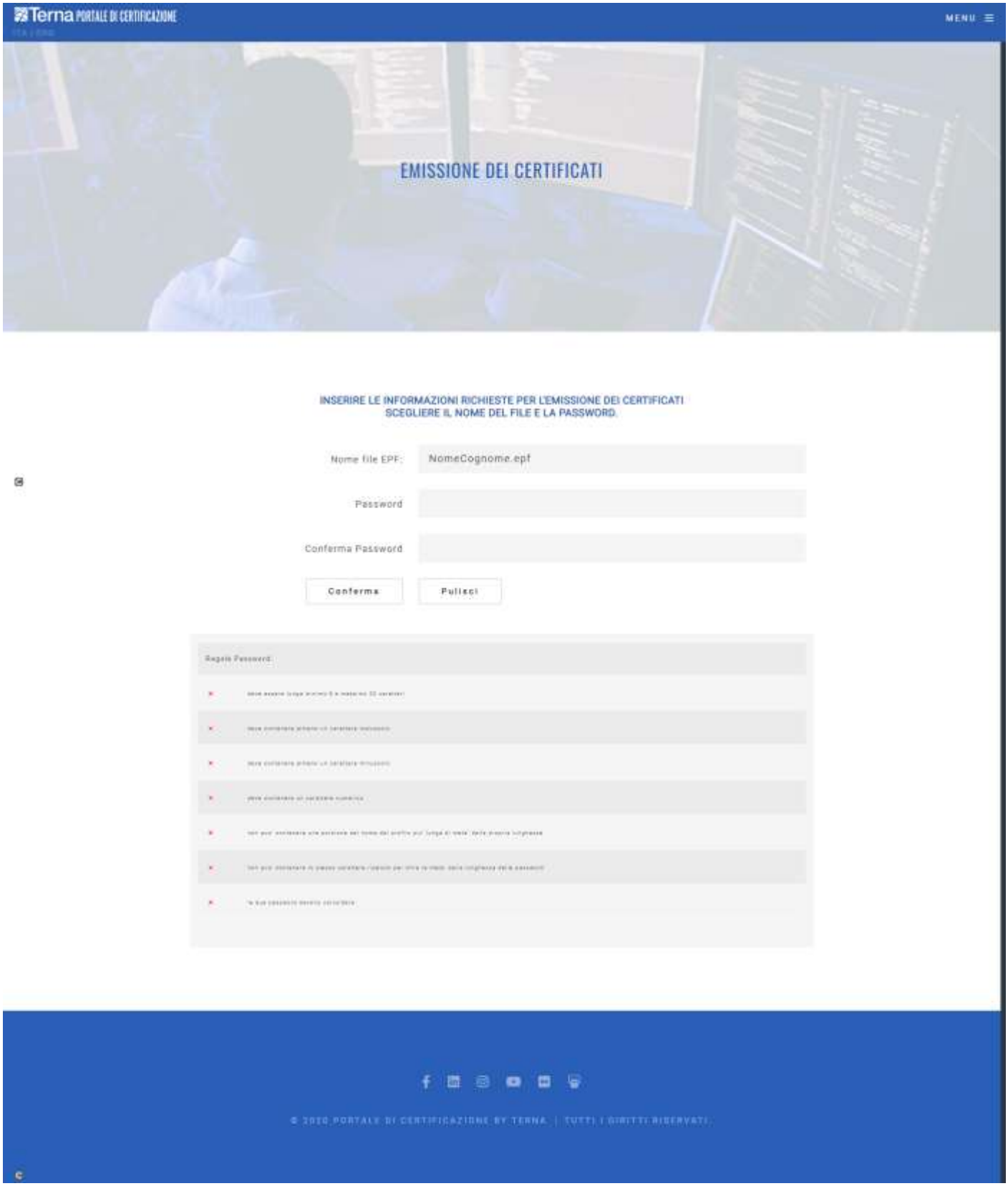

Figura 7.9: inserimento informazioni per la creazione del file .epf

3.6.2. RECOVERY DEL CERTIFICATO CON CODICI DI ATTIVAZIONE

Per ottenere la recovery del certificato con i codici di attivazione, nella pagina mostrata in Figura 7.7 procedere come segue:

1. Selezionare il link **Operazioni Certificati**.
2. Nella pagina visualizzata (Figura 7.8) selezionare il link **Recovery Certificato con codici di attivazione**.
3. Inserire (Figura 7.10) *Numero di Riferimento* e *Codice di Autorizzazione*, quindi premere **Conferma** per avviare la richiesta di recovery del certificato.

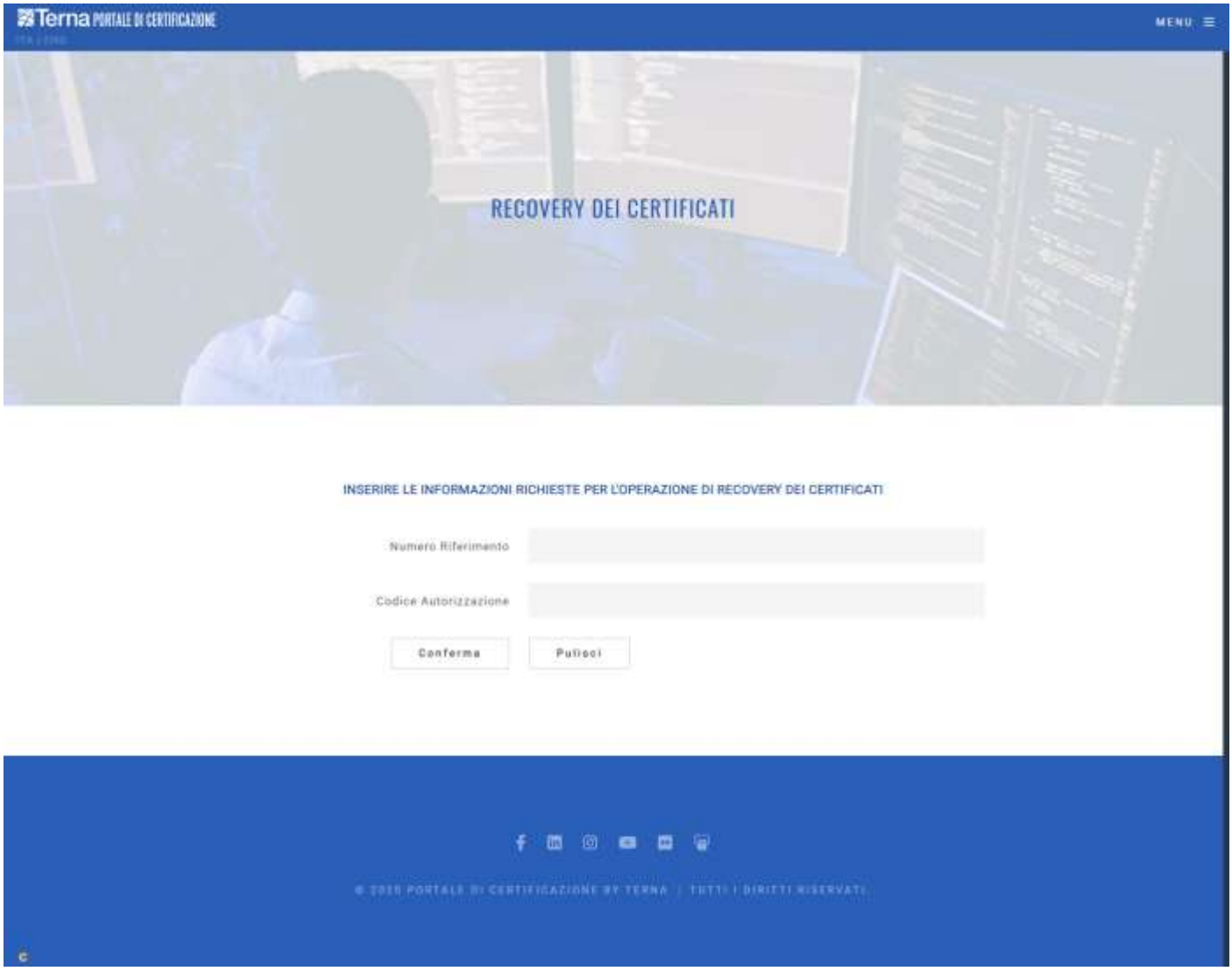

Figura 7.10: Richiesta recovery del certificato per i dipendenti di aziende esterne

4. Scegliere il nome del **nuovo** file ".epf" che si sta generando e inserire due volte la password, infine premere **Conferma** (figura 7.11).

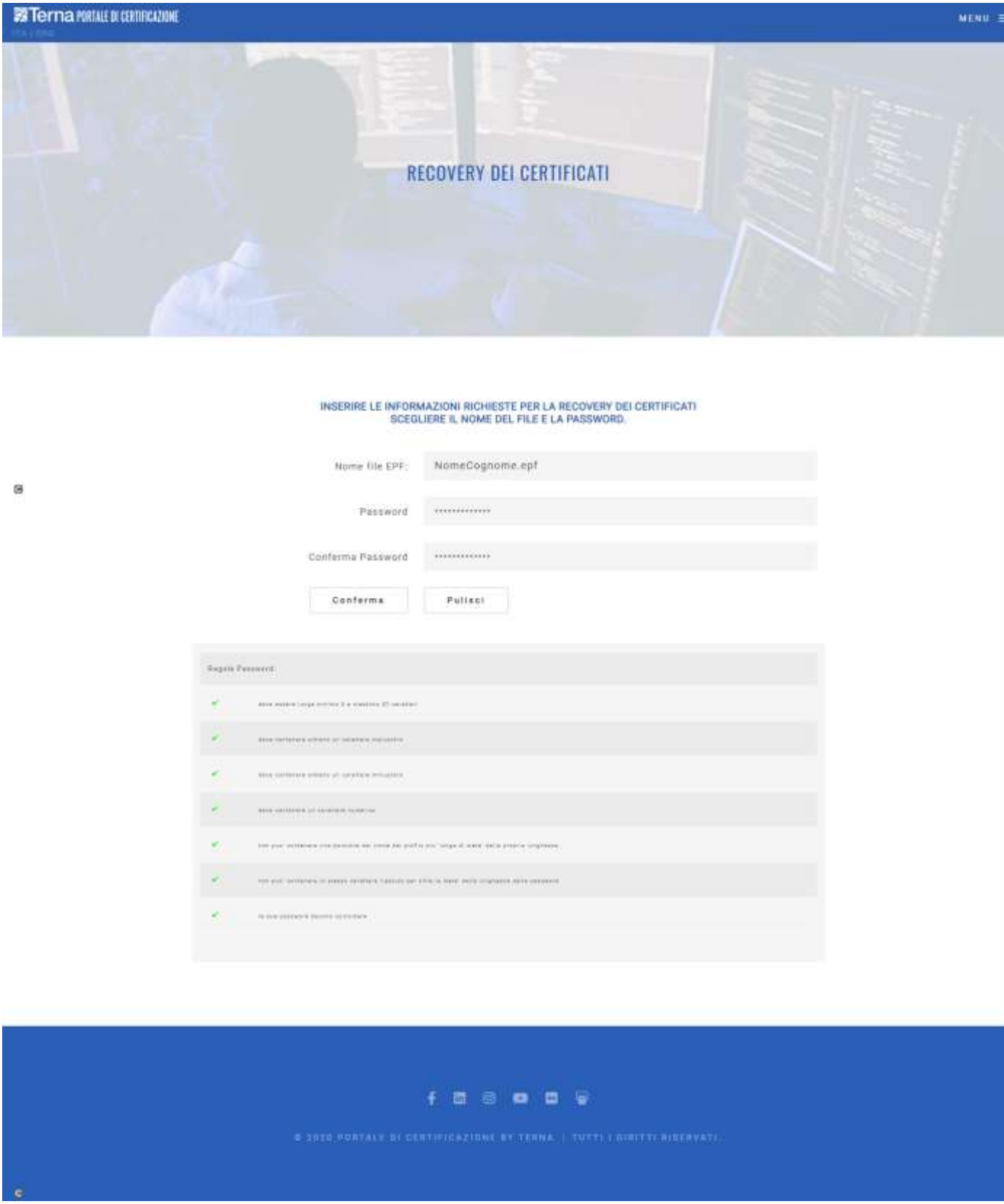

Figura 7.11: inserimento informazioni per la creazione del file .epf

3.6.3 FIRMA DIGITALE DEL MODULO DI RICHIESTA

Attraverso queste funzioni l'utente, utilizzando il proprio certificato EPF, può firmare digitalmente il modulo di richiesta e inviarlo automaticamente a Terna in accordo con le procedure del manuale operativo.

Nella pagina mostrata in Figura 7.7 procedere come segue:

1. Selezionare il link **Operazioni Certificati**.
2. Nella pagina visualizzata (Figura 7.8) selezionare il link **Firma Digitale del Modulo di Richiesta**
3. Sarà visualizzata la scherma in (Figura 7.12) nella quale è necessario inserire nuovamente la password dell'epf con il quale ci si è autenticati al Portale del Certificatore.

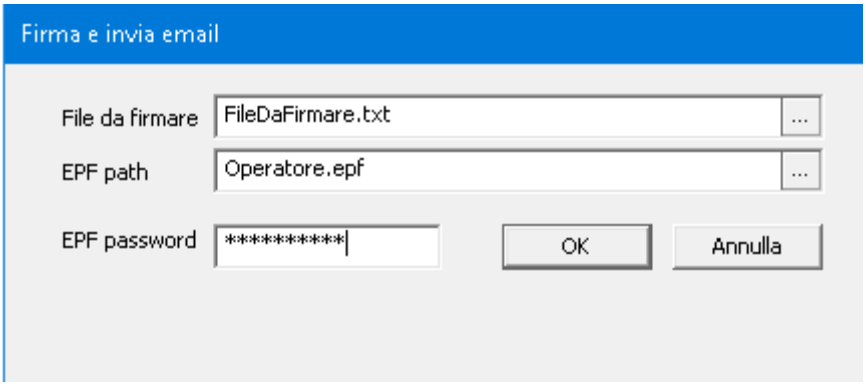

Figura 7.12: Inserimento password .epf e selezione file da firmare

4. Premendo sul pulsante con i tre puntini viene visualizzata una finestra di dialogo (Figura 7.13), attraverso la quale è possibile selezionare da file system il file da firmare.

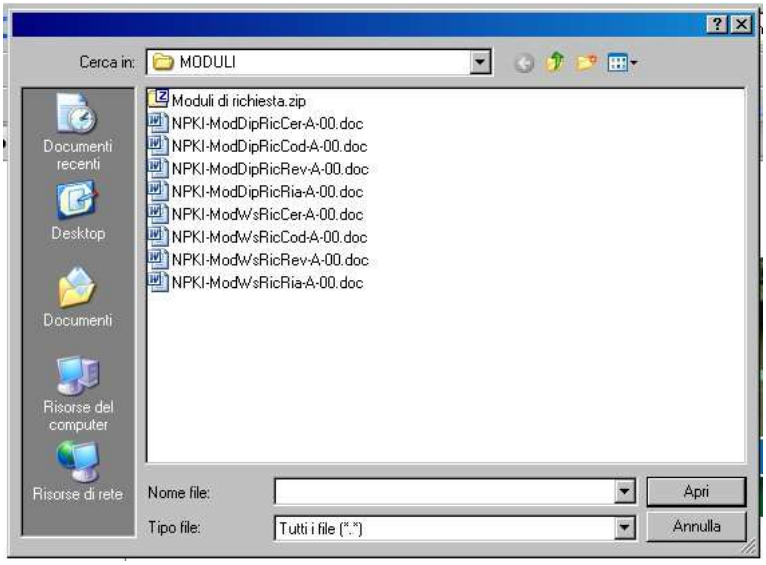

Figura 7.13: selezione del file da firmare

Una volta selezionato il file da firmare, l'applicazione processa automaticamente il file, inviandolo direttamente, tramite posta elettronica a Terna.

Al termine delle operazioni viene presentata la finestra di dialogo in Figura 7.14, attraverso la quale è possibile salvare localmente, per usi successivi, il file appena firmato.

Figura 7.14: memorizzazione in locale del file firmato

3.6.4 CALL CENTER

TERNA è responsabile della definizione, pubblicazione e aggiornamento dei Manuali Operativi e del Portale del Certificatore. Domande, osservazioni e richieste di chiarimento al riguardo dovranno essere rivolte al Call Center utilizzando i riferimenti indicati in questa sezione.

Figura 7.15: Riferimenti Call Center

3.7. PROCEDURE PER I CERTIFICATI DI AUTENTICAZIONE A WEB SERVICE TERNA

Selezionando il link **Procedure per i Certificati di Autenticazione a Web Service Terna** nel menu a destra della home page del Portale del Certificatore si apre una pagina (Figura 7.16) suddivisa in tre sezioni:

- **Procedure per i Certificati di Autenticazione a Web-Services Terna.** Da questa sezione è possibile scaricare le procedure operative che governano l'emissione e l'uso dei Certificati sottoscritti dal Certificatore Terna per l'autenticazione alle applicazioni Web Services Terna. Le indicazioni fornite hanno validità per le attività relative a Terna, nel ruolo di Certificatore, per l'Ufficio di Registrazione, per gli Amministratori di Sistema di quelle Applicazioni di Aziende Esterne che dovranno essere abilitate all'utilizzo degli Web Services Terna.
- **Modulistica**. Da questa sezione è possibile scaricare i moduli per la richiesta di Rilascio/ Revoca/Sospensione/Recovery di certificati digitali di autenticazione a Web Services Terna e per la richiesta di Rilascio dei codici di attivazione per i certificati digitali di autenticazione a Web Services Terna.
- **Operazioni Automatiche sui certificati**. Da questa sezione è possibile accedere ad ulteriori pagine che consentono di eseguire le procedure per applicativi web che fanno uso di file in formato PKCS#12 ovvero per l'emissione/recovery dei certificati di autenticazione a Web Services Terna.
- **Call Center.** Da questa sezione è possibile reperire i riferimenti utilizzabili per inoltrare eventuali richieste al Certificatore

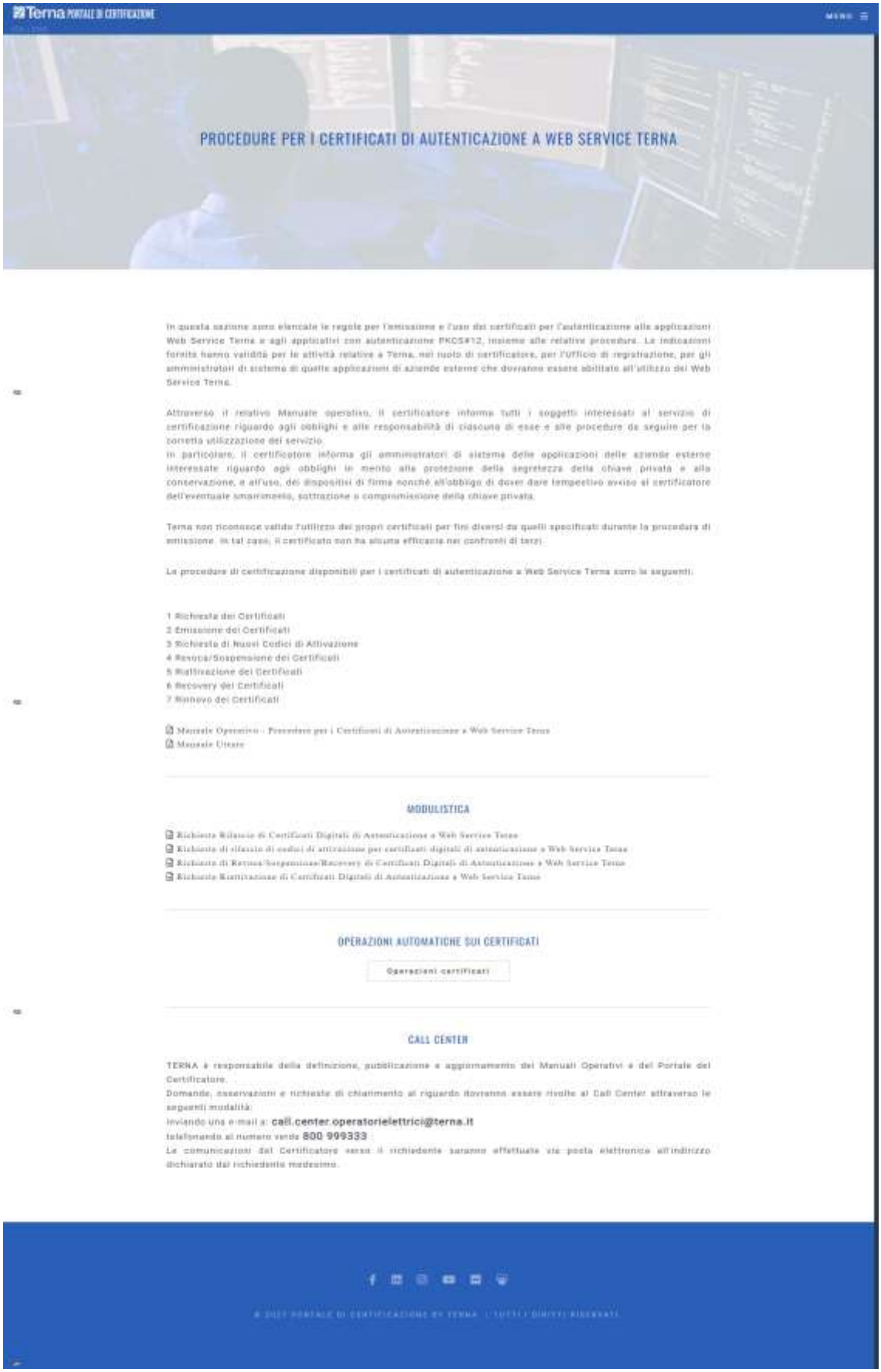

Figura 7.16: Emissione Certificati per i Clienti BDE

3.7.1 EMISSIONE DEL CERTIFICATO CON CODICI DI ATTIVAZIONE

Per ottenere l'emissione del certificato con i codici di attivazione, nella pagina mostrata in Figura 7.17 procedere come segue:

1. Selezionare il link **Operazioni Certificati**.
2. Nella pagina visualizzata (Figura 7.18) selezionare il link **Emissione Certificato con codici di attivazione**.

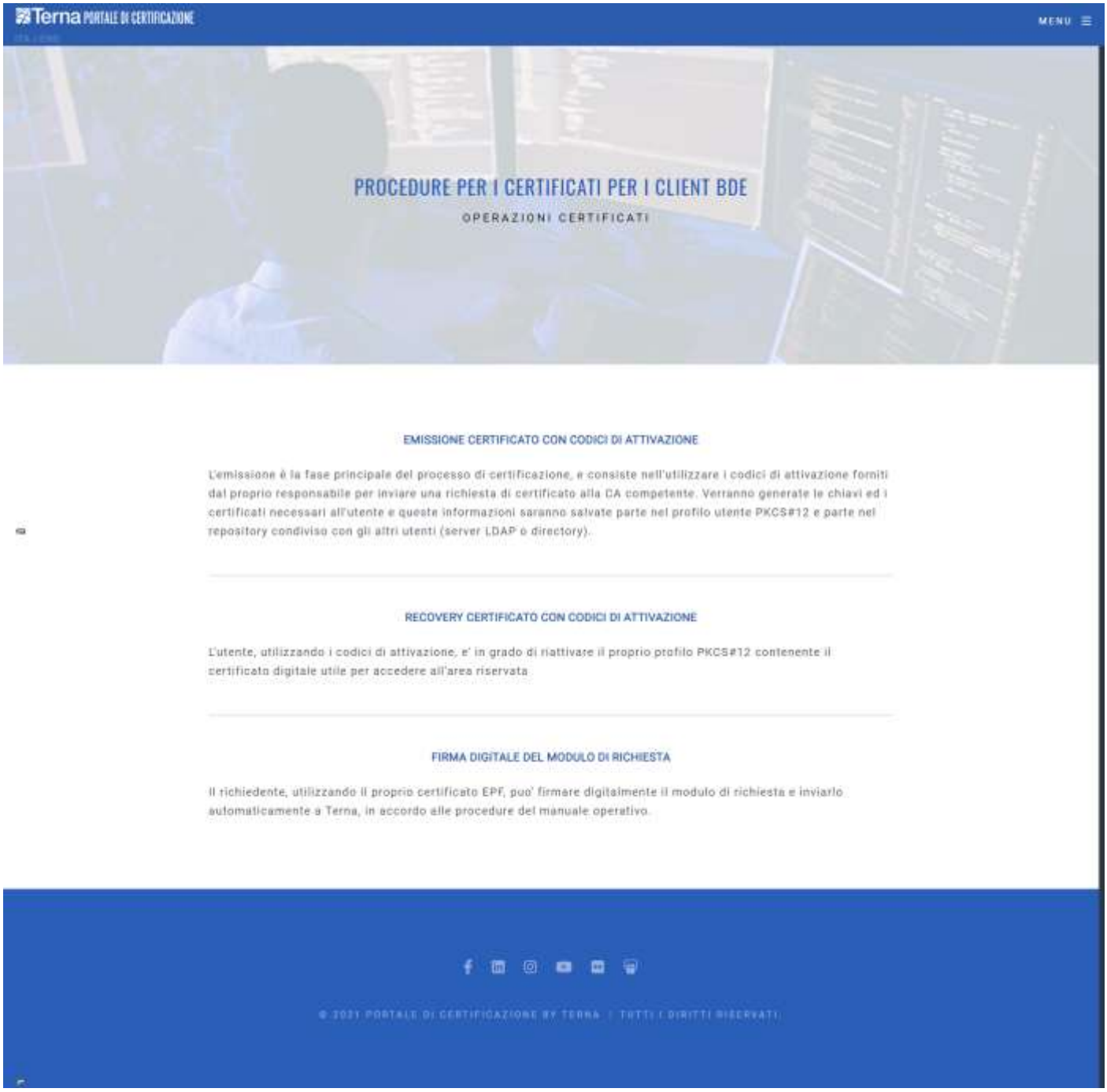

Figura 7.17: Procedure per i certificati di autenticazione a Web Services Terna

3. Inserire (Figura 7.18) *Numero di Riferimento*, *Codice di Autorizzazione e Password file PKCS12*, quindi premere **Conferma** per avviare la richiesta di emissione del certificato.

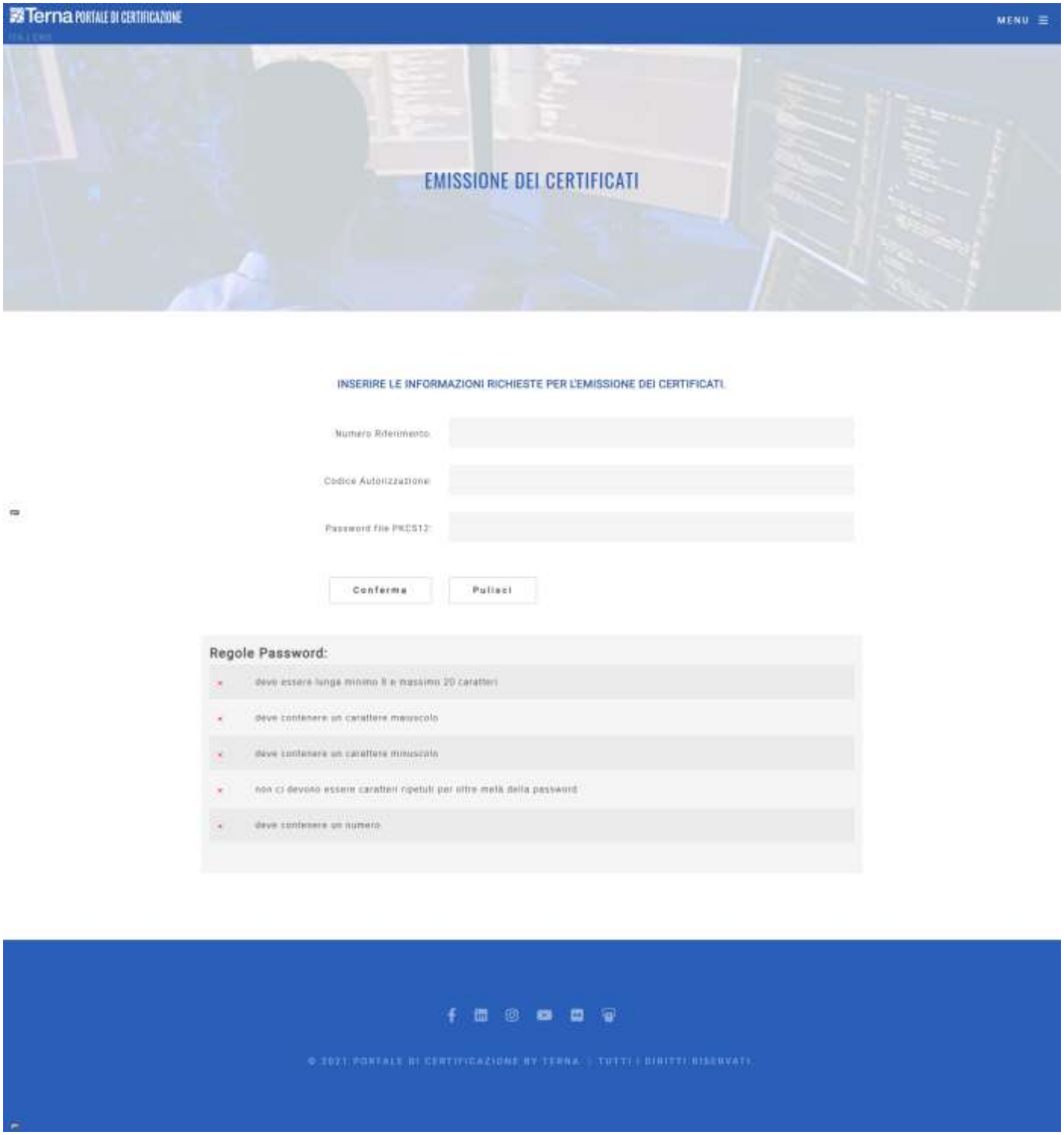

Figura 7.18: Richiesta emissione certificato di autenticazione a Web Services Terna

4. Salvare il file.

3.7.2 RECOVERY DEL CERTIFICATO CON CODICI DI ATTIVAZIONE

Per ottenere la recovery del certificato con i codici di attivazione, nella pagina mostrata in Figura 7.16 procedere come segue:

1. Selezionare il link **Operazioni Certificati**
2. Nella pagina visualizzata (Figura 7.17) selezionare il link **Recovery Certificato con codici di attivazione**
3. Inserire (Figura 7.19) *Numero di Riferimento*, *Codice di Autorizzazione e Password file PKCS12*, quindi premere **Conferma** per avviare la richiesta di recovery del certificato.

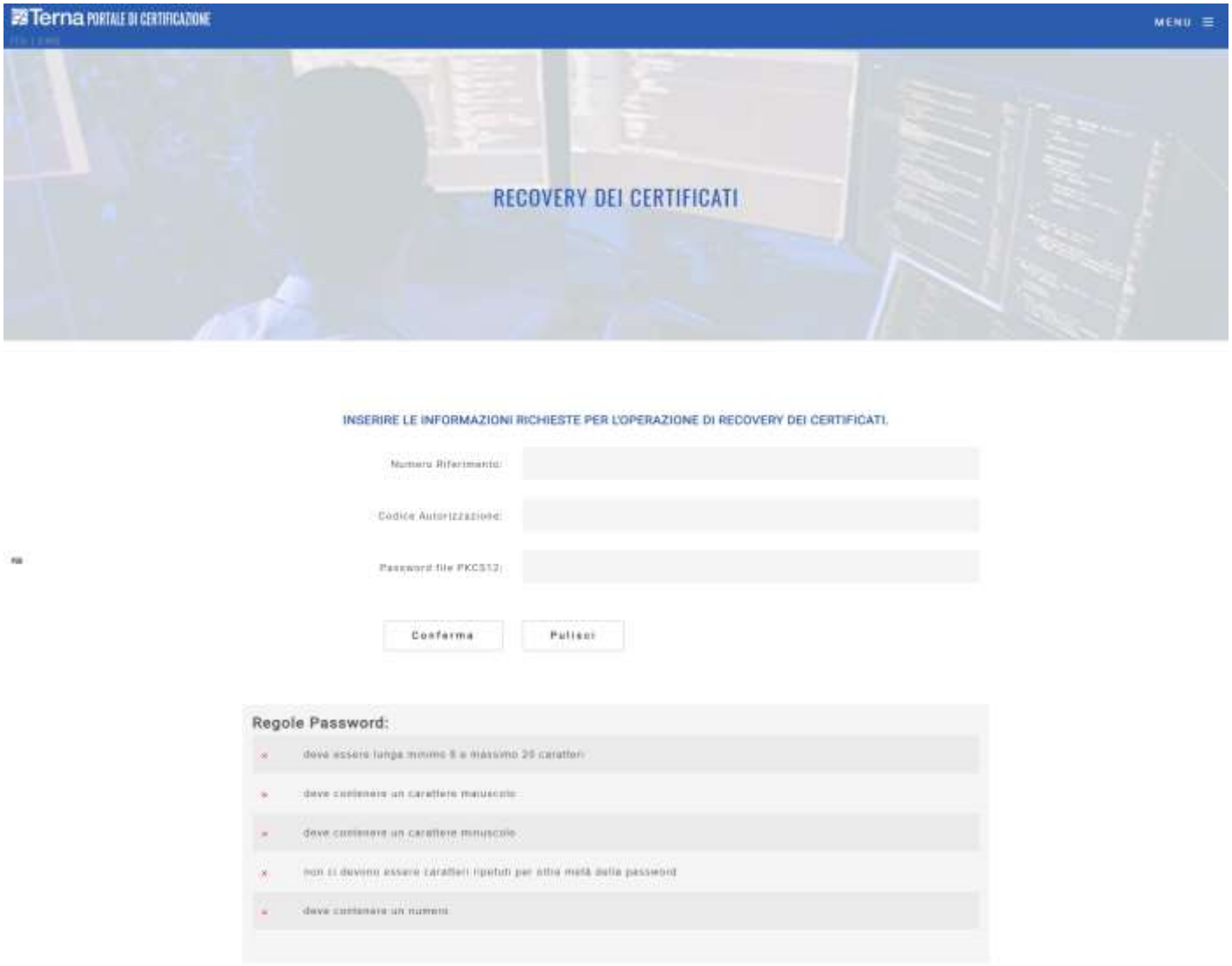

Figura 7.19: Richiesta recovery certificato di autenticazione a Web Services Terna

4. Salvare il file.

(Fine documento)