SERVIZIO DI CERTIFICAZIONE TERNA - AZIENDE

ISTRUZIONE OPERATIVA - GENERALITÀ

Storia delle revisioni

Rev. n°	Data	Descrizione
00	31/08/2010	Prima versione del documento (nuova codifica).

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

INDICE GENERALE

1. GENERALITÀ

TERNA eroga un SERVIZIO DI CERTIFICAZIONE per l'emissione e l'esercizio di CERTIFICATI DIGITALI al personale delle AZIENDE che hanno sottoscritto, con TERNA, specifici accordi.

I CERTIFICATI DIGITALI TERNA consentono:

- l'AUTENTICAZIONE sicura ad applicazioni informatiche TERNA;

Il SERVIZIO DI CERTIFICAZIONE erogato consiste in:

- emissione di CERTIFICATI DIGITALI al personale dipendente di AZIENDE che hanno preventivamente sottoscritto specifici accordi di collaborazione con TERNA;
- emissione di CERTIFICATI DIGITALI per applicazioni informatiche e dispositivi elettronici specifici;
- pubblicazione dei CERTIFICATI delle CHIAVI PUBBLICHE di CIFRATURA;
- generazione delle coppie di CHIAVI DI CIFRATURA;
- RECOVERY delle CHIAVI DI CIFRATURA;
- RECOVERY dei PROFILI DI CERTIFICAZIONE;
- pubblicazione delle liste dei CERTIFICATI REVOCATI o SOSPESI (CRL).

I CERTIFICATI DIGITALI TERNA non rientrano nella tipologia dei CERTIFICATI QUALIFICATI conformi alla Direttiva europea 1999/93/CE e nazionale in materia.

1.1. SCOPO

Il presente documento introduce le regole che governano l'emissione e l'uso dei CERTIFICATI sottoscritti dal CERTIFICATORE e l'insieme delle procedure operative per l'erogazione dei relativi servizi di certificazione digitale.

Le procedure operative sono dettagliate nei seguenti documenti:

- NPKI-IOAzGen-A-00 – "Istruzione Operativa - Generalità" (questo documento);
- NPKI-IOAzDip-A-00 – "Istruzione Operativa per i CERTIFICATI dei dipendenti di AZIENDE ESTERNE";
- NPKI-IOAzWS-A-00 – "Istruzione Operativa per i CERTIFICATI per WEB SERVICES- APPLICATIVI".

Tutte le indicazioni fornite hanno validità per le attività riguardanti TERNA, nel ruolo di CERTIFICATORE, per l'UFFICIO DI REGISTRAZIONE, per i soggetti incaricati ad effettuare l'identificazione/registrazione dei TITOLARI e per gli stessi TITOLARI.

Attraverso tale documentazione, il CERTIFICATORE informa tutti i soggetti interessati al SERVIZIO DI CERTIFICAZIONE, riguardo agli obblighi e alle responsabilità di ciascuno di essi e alle procedure da seguire per la corretta utilizzazione del servizio.

In particolare, il CERTIFICATORE informa il TITOLARE del CERTIFICATO, riguardo agli obblighi, da quest'ultimo assunti, in merito alla protezione della segretezza della chiave privata ed alla conservazione, ed all'uso, dei dispositivi di firma, nonché all'obbligo di dover dare tempestivo avviso al CERTIFICATORE, dell'eventuale smarrimento, sottrazione o compromissione della chiave privata.

TERNA non riconosce valido l'utilizzo dei propri CERTIFICATI per fini diversi da quelli specificati durante la procedura di emissione. In tal caso, il CERTIFICATO non ha alcuna efficacia nei confronti di terzi.

1.2. ORGANIZZAZIONE DEL DOCUMENTO

Questo documento è organizzato nei seguenti capitoli:

1. GENERALITÀ – Fornisce informazioni di carattere generale sulla ISTRUZIONE OPERATIVA e sulla sua organizzazione.

2. SOGGETTI INTERESSATI AL SERVIZIO DI CERTIFICAZIONE – Definisce le caratteristiche dei principali soggetti interessati, a diverso titolo, dal SERVIZIO DI CERTIFICAZIONE.
3. DISPOSIZIONI GENERALI – Definisce il ruolo e le responsabilità di ciascuno dei soggetti interessati al sistema di Certificazione.
4. OPERATIVITÀ DEL SISTEMA DI CERTIFICAZIONE – Introduce le procedure fondamentali che regolano il funzionamento dell'intero sistema di certificazione.

1.3. DEFINIZIONI E ACRONIMI

TERMINE O ACRONIMO	SIGNIFICATO
AMMINISTRATORE DI SISTEMA	In ambito informatico, figura professionale finalizzata alla gestione tecnica ed alla manutenzione di un sistema di elaborazione o di sue componenti. Ricadono in questo ruolo anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di applicazioni.
AZIENDA	ENTE che ha stipulato con TERNA uno specifico accordo (e.g. Operatore Elettrico) che prevede l'utilizzo di CERTIFICATI DIGITALI TERNA.
CALL CENTER	Unità organizzativa TERNA a cui è stato attribuito il ruolo d'interfaccia di erogazione del SERVIZIO DI CERTIFICAZIONE nei confronti di tutti gli utilizzatori.
CERTIFICATORE	TERNA come erogatore di Servizi di Certificazione.
CERTIFICATO DIGITALE	Il risultato di un processo mediante il quale la chiave pubblica del TITOLARE, e altre informazioni, vengono associate univocamente al TITOLARE della chiave privata. L'autenticità e l'integrità di tale associazione vengono assicurate tramite la FIRMA DIGITALE da parte del CERTIFICATORE.
CHIAVI DI CIFRATURA	La coppia di chiavi utilizzate dall'operazione di CIFRATURA per rendere segrete delle informazioni.
CHIAVI DI SOTTOSCRIZIONE	La coppia di chiavi destinate alla generazione ed alla verifica di firme digitali.
CHIAVE PRIVATA	L'elemento della coppia di chiavi destinato ad essere utilizzato e conosciuto dal solo soggetto TITOLARE.
CHIAVE PUBBLICA	L'elemento della coppia di chiavi destinato ad essere reso pubblico.
CIFRATURA	Il processo di trasformazione di dati in un formato che garantisca la riservatezza dei dati stessi. Tale operazione prevede l'utilizzo delle chiavi pubbliche dei sogogetti a cui sono destinate le informazioni.
CODICI DI ATTIVAZIONE	I codici riservati concordati tra UTENTE e il CERTIFICATORE per stabilire un'identificazione sicura dell'UTENTE all'atto della sua certificazione.
CODICE DI AUTENTICAZIONE E NUMERO DI RIFERIMENTO	CODICI DI ATTIVAZIONE.

TERMINE O ACRONIMO	SIGNIFICATO
COPPIA DI CHIAVI	L'insieme costituito dalla chiave pubblica e dalla chiave privata ad essa associata.
CRL	Vedi LISTA DEI CERTIFICATI REVOCATI O SOSPESI
DECIFRATURA	Il processo di trasformazione inverso a quello di CIFRATURA. Tale operazione prevede l'utilizzo della chiave privata da parte del TITOLARE che intende decifrare il messaggio.
EESP	Il software per l'utilizzo delle operazioni di crittografia da installare sulle postazioni di lavoro degli Utenti.
FIRMA DIGITALE	Firma elettronica basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al TITOLARE tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
INFORMATION SYSTEM OWNER	Con riferimento a §[8], deve garantire che adeguati metodi di identificazione e autenticazione siano implementati per i *Sistemi Informativi* di sua pertinenza, in funzione della classificazione e del livello di rischio assegnato.
LISTA DEI CERTIFICATI REVOCATI O SOSPESI	E' una lista di CERTIFICATI che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata REVOCA se definitiva, SOSPENSIONE se temporanea. Quando un CERTIFICATO viene revocato o sospeso il suo numero di serie viene aggiunto e pubblicato attraverso la CRL (Certificate Revocation List).
ISTRUZIONE OPERATIVA	Manuale che definisce le procedure che il CERTIFICATORE applica nello svolgimento del servizio.
OPERATORE DI REGISTRAZIONE	Operatore dell'UFFICIO DI REGISTRAZIONE TERNA.
PORTALE DI CERTIFICAZIONE	Portale che Terna ha predisposto al fine di semplificare i servizi connessi all'utilizzo dei certificati digitali: • fornisce le istruzioni per utilizzare i servizi di certificazione; • consente di consultare i manuali contenenti la descrizione delle procedure operative da seguire per dotarsi di un certificato digitale; • fornisce gli strumenti di accesso alle procedure per l'emissione e la gestione dei certificati digitali.
PROFILO DEL TITOLARE (EPF)	È un file cifrato con una password conosciuta solo dal TITOLARE che contiene l'insieme delle informazioni crittografiche del TITOLARE stesso. Queste informazioni gli consentono di eseguire le principali operazioni di crittografia, come quelle di firma, di CIFRATURA, di verifica, di DECIFRATURA e di autenticazione. Il file EPF (ENTRUST PROFILE FILE) è rilasciato dal CERTIFICATORE direttamente al TITOLARE e contiene anche il CERTIFICATO di Firma, il CERTIFICATO di CIFRATURA, il CERTIFICATO di Autenticazione e le relative Chiavi.

TERMINE O ACRONIMO	SIGNIFICATO
REVOCA/SOSPENSIONE DEL CERTIFICATO	È l'operazione con cui il CERTIFICATORE annulla la validità del CERTIFICATO prima della naturale scadenza. Vedi LISTA DEI CERTIFICATI REVOCATI O SOSPESI - CRL.
SERVIZIO DI CERTIFICAZIONE	Il servizio erogato dal CERTIFICATORE ai soggetti interessati attraverso le proprie strutture organizzative;
TERNA	TERNA S.p.A. e Società controllate.
TERZO INTERESSATO AZIENDA	La persona designata dall'organizzazione dell'AZIENDA, che ha una relazione contrattuale con TERNA, la quale può autorizzare, in virtù dello stesso contratto, l'emissione dei CERTIFICATI per il Personale Dipendente dell'AZIENDA stessa. Ha il diritto/dovere di richiedere la revoca o sospensione del CERTIFICATO DIGITALE in caso di necessità.
TERZO INTERESSATO TERNA	La figura designata dall'organizzazione Aziendale TERNA che ha la facoltà di autorizzare l'emissione dei CERTIFICATI per il Personale Dipendente TERNA, a lui afferente, e richiederne la revoca.
TITOLARE	La persona fisica per la quale è stato emesso un CERTIFICATO da parte del CERTIFICATORE, contenente la sua chiave pubblica. E' responsabile dell'utilizzo della chiave privata corrispondente alla chiave pubblica.
UFFICIO DI REGISTRAZIONE	Unità Organizzativa del CERTIFICATORE che svolge un ruolo di servizio nei confronti di tutti i soggetti che ricorrono al servizio stesso.
UTENTE	Soggetto, persona o applicazione informatica, che riceve un CERTIFICATO DIGITALE e/o che fa affidamento sul CERTIFICATO medesimo o sulla FIRMA DIGITALE basata su quel CERTIFICATO.

1.4. RIFERIMENTI

1.4.1 Documenti Utilizzati per la Stesura del Documento

[1] NPKI-CP-A-01 – "Policy dei CERTIFICATI"
[2] NPKI-CPS-A-01 – "Certification Practice Statement"
[3] NPKI-TC-A-03 – "Profilo dei CERTIFICATI"
[4] NPKI-PR-A-00 – "Processi e Ruoli"
[5] DPS – "Documento Programmatico sulla Sicurezza"
[6] LG018 – "Information Security Policy – Indirizzi strategici"
[7] IO001SG – "Gestione della Documentazione"
[8] R04LG018 – "Controllo degli Accessi Logici alle Risorse informatiche di TERNA"

1.4.2 Documenti Complementari all'Utilizzo del Documento

I seguenti documenti sono reperibili sul sito TERNA nella sezione Portale di Certificazione:

[9] NPKI-MANUTEINTER-A-00 – "Manuale Utente Internet"

1.5. DATI IDENTIFICATIVI DEL CERTIFICATORE

Denominazione Sociale	Terna - Rete Elettrica Nazionale S.p.A
Indirizzo della Sede Legale	Viale Egidio Galbani, 70 – 00156 Roma
Legale Rappresentante	Flavio Cattaneo
N°REA	922416
N°Iscrizione al Registro delle Imprese	05779661007 del 05/07/1999
N°Partita IVA	05779661007
N°Telefono Centralino	+39 06 8313 8111
N°Fax	+39 06 8313 8389
Sito Web Principale	http://www.terna.it
Sito Web per i Servizi di Certificazione	http://www.terna.it /ServizidiCertificazione
X500	ldap://ldap.terna.it

1.6. CONTATTI PER GLI UTENTI

TERNA è responsabile della definizione, pubblicazione e aggiornamento della presente ISTRUZIONE OPERATIVA.

Domande, osservazioni e richieste di chiarimento circa l'utilizzo di questo documento dovranno essere rivolte al CALL CENTER attraverso le seguenti modalità:

- inviando una e-mail a call.center.operatorielettrici@terna.it
- telefonando al numero verde **800 999 333**

1.7. CONVENZIONI TIPOGRAFICHE

All'interno del Manuale, le parole scritte intenzionalmente in MAIUSCOLETTO sono utilizzate secondo il significato riportato in §1.3.

Tutti i collegamenti ipertestuali utilizzati possono essere distinti all''interno del testo attraverso le seguenti peculiarità grafiche:

- il simbolo "§" seguito da una stringa alfanumerica;
- un numero racchiuso nelle parentesi [];
- la parola "Facsimile" seguita da un numero all'interno di parentesi tonde;
- la parola "Figura" seguita da un numero all'interno di parentesi tonde.

2. SOGGETTI INTERESSATI AL SERVIZIO DI CERTIFICAZIONE

Un CERTIFICATO DIGITALE è l'associazione tra una chiave pubblica di crittografia e un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata, chiamato anche TITOLARE della coppia di chiavi asimmetriche (pubblica e privata).

Il CERTIFICATO è utilizzato da altri soggetti, gli UTENTI, per ricavare la chiave pubblica, contenuta e distribuita con il CERTIFICATO, e verificare, tramite questa, il possesso della corrispondente chiave privata, identificando in tal modo il TITOLARE della stessa.

Il CERTIFICATO garantisce la corrispondenza tra la chiave pubblica e il TITOLARE.

Gli Utenti del servizio di certificazione Terna, dettagliati nei corrispondenti paragrafi sono:

1. CERTIFICATORE
2. UFFICIO DI REGISTRAZIONE
3. CALL CENTER
4. TERZO INTERESSATO
5. AMMINISTRATORE DI SISTEMA
6. TITOLARE
7. UTENTE

2.1 CERTIFICATORE

Il CERTIFICATORE:

- è il responsabile della corretta erogazione dell'intero SERVIZIO DI CERTIFICAZIONE;
- emette, pubblica nel registro e revoca i CERTIFICATI, operando in conformità a quanto descritto nella presente ISTRUZIONE OPERATIVA.
- eroga il proprio servizio attraverso l'utilizzo di un'idonea infrastruttura tecnologica e del personale addetto al suo funzionamento.

2.2 UFFICIO DI REGISTRAZIONE

L'UFFICIO DI REGISTRAZIONE è il soggetto TERNA che ha la responsabilità di attivare la procedura di certificazione per conto del CERTIFICATORE, in seguito alla richiesta del CALL CENTER.

2.3 CALL CENTER

Il CALL CENTER:

- è il soggetto cui è stato attribuito il ruolo d'interfaccia nei confronti di tutti gli utilizzatori del SERVIZIO DI CERTIFICAZIONE.
- ha la responsabilità di verificare la completezza dei dati forniti dal TERZO INTERESSATO durante la procedura di richiesta di certificazione.
- fornisce anche supporto nell'applicazione delle procedure operative e nell'utilizzo degli strumenti informatici messi a disposizione dal CERTIFICATORE.

2.4 TERZO INTERESSATO

TERZO INTERESSATO è la persona designata dall'AZIENDA, che ha stipulato con TERNA uno specifico accordo, cui è stato formalmente assegnato, dall''AZIENDA stessa, il mandato di richiedere l'emissione di CERTIFICATI DIGITALI per un determinato gruppo di suoi dipendenti o collaboratori.

Il TERZO INTERESSATO AZIENDA può anche richiedere:

- la REVOCA o la SOSPENSIONE dei CERTIFICATI dei TITOLARI a lui afferenti;
- il RECOVERY delle Chiavi di CIFRATURA e dei CERTIFICATI dei TITOLARI a lui afferenti.

2.5 AMMINISTRATORE DI SISTEMA

L'AMMINISTRATORE DI SISTEMA è il dipendente TERNA che, in base al suo ruolo aziendale, può richiedere l'emissione e ricevere un CERTIFICATO DIGITALE per i sistemi informativi, o gli asset, di sua pertinenza.

L'AMMINISTRATORE DI SISTEMA può richiedere anche:

- la REVOCA o la SOSPENSIONE dei CERTIFICATI per i sistemi informativi di propria pertinenza;
- il RECOVERY delle CHIAVI DI CIFRATURA e dei CERTIFICATI DIGITALI per i sistemi informativi di propria pertinenza.

2.6 TITOLARE

Il TITOLARE è la persona fisica per la quale è stato emesso un CERTIFICATO DIGITALE TERNA, è identificata nel CERTIFICATO come titolare della chiave privata corrispondente alla chiave pubblica contenuta nel CERTIFICATO stesso; al TITOLARE è attribuita la FIRMA DIGITALE generata con la chiave privata della coppia.

Il TITOLARE può richiedere anche:

- REVOCA o la SOSPENSIONE dei propri CERTIFICATI;
- il RECOVERY dei propri CERTIFICATI e delle relative chiavi di CIFRATURA.

2.7 UTENTE

Soggetto, persona o applicazione informatica, che riceve un CERTIFICATO DIGITALE e/o che fa affidamento sul CERTIFICATO medesimo o sulla FIRMA DIGITALE basata su quel CERTIFICATO.

Affinché un UTENTE possa fare affidamento sull'utilizzo di una chiave privata, il CERTIFICATO corrispondente deve essere valido, cioè non scaduto, sospeso o revocato.

3 DISPOSIZIONI GENERALI

Questa sezione specifica in dettaglio gli obblighi e le responsabilità del CERTIFICATORE, dell'UFFICIO DI REGISTRAZIONE, dei TITOLARI di CERTIFICATI DIGITALI e di tutti gli altri soggetti che concorrono alla realizzazione del SERVIZIO DI CERTIFICAZIONE TERNA.

3.1 OBBLIGHI E RESPONSABILITÀ DEL CERTIFICATORE

Il CERTIFICATORE è tenuto a garantire:

- che il TITOLARE sia espressamente informato riguardo alla necessità di protezione della segretezza della chiave privata;
- l'associazione tra il TITOLARE e la chiave pubblica certificata;
- di non rendersi depositario di chiavi private relative ai corrispondenti Certificati;
- il rilascio e il rinnovo di un CERTIFICATO richiesto secondo le procedure indicate nella presente ISTRUZIONE OPERATIVA;
- la revoca o la sospensione del CERTIFICATO dandone pubblicazione secondo le tempistiche indicate nella presente ISTRUZIONE OPERATIVA;
- la protezione accurata delle proprie chiavi private mediante dispositiviadeguati a garantire i necessari criteri di sicurezza;
- la gestione delle operazioni e dell'infrastruttura tecnologica, relativa al SERVIZIO DI CERTIFICAZIONE, secondo le regole e le procedure indicate nella presente ISTRUZIONE OPERATIVA;
- che le operazioni relative al SERVIZIO DI CERTIFICAZIONE, da lui stesso affidate all'Ufficio di Registrazione e al CALL CENTER, siano effettuate secondo le regole e le procedure indicate nella presente ISTRUZIONE OPERATIVA;
- la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, Decreto Legislativo 30 giugno 2003, n.196, attraverso l'attuazione delle disposizioni di cui al §[5].

3.2 OBBLIGHI E RESPONSABILITÀ DELL'UFFICIO DI REGISTRAZIONE

L'Ufficio di Registrazione è tenuto a garantire:

- la registrazione dei dati del TITOLARE;
- la comunicazione al CERTIFICATORE di tutti i dati del TITOLARE acquisiti allo scopo di attivare la procedura di emissione del CERTIFICATO.

3.3 OBBLIGHI E RESPONSABILITÀ DEL CALL CENTER

Il CALL CENTER è tenuto, a:

- verificare la completezza dei dati di un TITOLARE, e, richiedere all'UFFICIO DI REGISTRAZIONE di attivare la procedura di certificazione;
- verificare e inoltrare al CERTIFICATORE le richieste di REVOCA o di SOSPENSIONE attivate dal TITOLARE o dal suo TERZO INTERESSATO.

3.4 OBBLIGHI E RESPONSABILITÀ DEL TERZO INTERESSATO

Il TERZO INTERESSATO ha la responsabilità oggettiva per l'uso improprio o abusivo dei CERTIFICATI DIGITALI assegnati ai TITOLARI a lui afferenti.

Nella fase di richiesta del CERTIFICATO, il TERZO INTERESSATO ha l'obbligo di:

- verificare e garantire l'identità del TITOLARE;
- controllare la veridicità, l'accuratezza e la completezza dei dati e delle informazioni fornite dal TITOLARE a lui afferente;
- fornire in modo corretto al CALL CENTER i dati e le informazioni del TITOLARE a lui afferente;
- informare il TITOLARE sugli obblighi e le responsabilità inerenti l'utilizzo del CERTIFICATO.

Quando necessario, il TERZO INTERESSATO ha inoltre la responsabilità di richiedere al CALL CENTER la REVOCA o la SOSPENSIONE dei CERTIFICATI.

Infine, il TERZO INTERESSATO deve comunicare al CALL CENTER ogni eventuale variazione dei dati che riguardano il TITOLARE.

3.5 OBBLIGHI E RESPONSABILITÀ DELL'AMMINISTRATORE DI SISTEMA

L'AMMINISTRATORE DI SISTEMA ha la responsabilità di fornire tutti i dati necessari alla richiesta di CERTIFICATI digitali per i sistemi informativi aziendali di sua pertinenza.

Quando necessario, ha anche la responsabilità di richiedere la REVOCA o la SOSPENSIONE dei CERTIFICATI utilizzati dai sistemi informativi aziendali di sua pertinenza.

3.6 OBBLIGHI E RESPONSABILITÀ DEL TITOLARE

Il TITOLARE ha l'obbligo di:

- prendere accurata visione della presente ISTRUZIONE OPERATIVA, relativamente ad ogni suo aspetto, e di assumersi tutti i doveri e le responsabilità in esso previste;
- accettare di conformarsi a quanto indicato nei MANUALI OPERATIVI IN 1.1 e osservare scrupolosamente tutte le procedure riportate;
- fornire, nella fase di richiesta del CERTIFICATO, dati e informazioni idonee a consentirne la sua corretta identificazione.
- utilizzare il CERTIFICATO DIGITALE e gli altri dispositivi di sicurezza TERNA soltanto per gli scopi per i quali è stato rilasciato ed autorizzato;
- garantire la segretezza del codice di abilitazione all'uso delle proprie CHIAVI PRIVATE, conservandolo in un luogo diverso da quello delle chiavi stesse;
- non tentare di estrarre la CHIAVE PRIVATA dal dispositivo che la contiene o di duplicare il dispositivo;
- non rendere disponibile ad altri le proprie CHIAVI PRIVATE;
- non utilizzare una CHIAVE PRIVATA di firma che si presuma compromessa;
- non utilizzare una CHIAVE PRIVATA relativa a un CERTIFICATO revocato o scaduto;
- non utilizzare un CERTIFICATO di CIFRATURA revocato o scaduto;
- distruggere la propria CHIAVE PRIVATA di firma qualora non abbia più titolo a possederla;
- rispettare i diritti di proprietà TERNA sui dati trattati e sui marchi da essa registrati o utilizzati, nonché i diritti di proprietà TERNA o di terzi sui programmi software utilizzati;
- rispettare le disposizioni aziendali sulla riservatezza delle informazioni;
- richiedere nei casi previsti la REVOCA o la SOSPENSIONE del proprio CERTIFICATO;
- comunicare tempestivamente al CALL CENTER ogni cambiamento delle informazioni e dei dati precedentemente forniti.

3.7 OBBLIGHI E RESPONSABILITÀ DELL'UTENTE

L'UTENTE, che accede al servizio di verifica delle firme o di cifratura di dati per un TITOLARE, è tenuto a accertarsi della validità dei CERTIFICATI avvalendosi delle LISTE DI REVOCA O SOSPENSIONE (CRL) gestite dal CERTIFICATORE.

In particolare, l'UTENTE deve:

- conoscere l'ambito di utilizzo del CERTIFICATO;
- verificare le informazioni contenute nel CERTIFICATO relative alla chiave pubblica della coppia di chiavi utilizzata;
- verificare la data di scadenza del CERTIFICATO;
- verificare lo stato del CERTIFICATO, prima di usare la chiave pubblica in esso contenuta.

Qualora le liste di revoca non fossero valide, l'UTENTE non è autorizzato a ritenere valido il CERTIFICATO in esame. Di conseguenza non è autorizzato ha ritenere valida la FIRMA DIGITALE associata al CERTIFICATO stesso o a effettuare operazioni di CIFRATURA.

L'UTENTE deve inoltre prendere visione delle caratteristiche e delle limitazioni relative all'uso del CERTIFICATO contenute in questo manuale.

3.8 DISPONIBILITÀ DEL SERVIZIO DI CERTIFICAZIONE

I requisiti di disponibilità del servizio sono:

TIPO DI SERVIZIO	GIORNI	ORARIO
Registrazione ed emissione di CERTIFICATI	LUN – VEN	08:00 – 17:00
Revoca/Sospensione	LUN – DOM	H24
Servizio di Verifica della Validità dei CERTIFICATI – CRL	LUN – DOM	H24
CALL CENTER	LUN – VEN	08:00 – 17:00

Le CRL vengono pubblicate periodicamente almeno ogni 24 ore.

La richiesta di revoca di un CERTIFICATO viene verificata ed elaborata nel più breve tempo possibile e comunque non superiore ad 1 (una) ora dal momento in cui la richiesta perviene al CERTIFICATORE.

3.9 TRATTAMENTO DEI DATI PERSONALI E TUTELA DELLA PRIVACY

Tutte le informazioni riservate raccolte, generate, trasmesse e gestite dal CERTIFICATORE devono essere considerate come tali e trattate secondo quanto definito nel documento programmatico della Sicurezza TERNA §[5].

In particolare, sono da considerare riservate tutte le informazioni relative a dati personali e, ove presenti, sensibili ai sensi della legge 196/2003, n. 196.

In particolare, il CERTIFICATORE - Titolare del Trattamento dei dati Personali, forniti dal TITOLARE (del certificato) mediante la compilazione della Richiesta di Certificazione - informa lo stesso, ai sensi e per gli effetti di cui all'art. 13 del Decreto Legislativo 30.06.2003, n. 196, che i predetti dati personali saranno trattati, con l'ausilio di archivi cartacei e di strumenti informatici e telematici idonei a garantire la massima sicurezza e riservatezza.

Il conferimento dei dati indicati nella richiesta è obbligatorio da parte del TITOLARE ai fini dello svolgimento del servizio, e un'eventuale rifiuto o un conferimento parziale comporterà l'impossibilità di fornire il servizio richiesto. Parte di essi, appositamente indicati nella richiesta, verranno pubblicati attraverso il loro inserimento nel CERTIFICATO DIGITALE.

I dati forniti saranno trattati al fine di fornire il servizio previsto e potranno essere comunicati alle società che forniscono consulenza ed assistenza tecnica al CERTIFICATORE.

In particolare, il CERTIFICATORE si riserva, su richiesta espressa da parte di terzi, di comunicare la documentazione fornita dal TITOLARE al momento dell'inoltro della richiesta di emissione del CERTIFICATO nonché quella relativa all'esito delle verifiche effettuate.

Un TITOLARE può esercitare in qualunque momento i diritti di cui all'art. 7 del Decreto Legislativo 30.06.2003, n. 196 scrivendo a *privacy@terna.it*.

4 OPERATIVITÀ DEL SISTEMA DI CERTIFICAZIONE

L'operatività dell'intero sistema di certificazione è garantita da alcune procedure fondamentali oggetto di una descrizione introduttiva nell'ambito del seguente paragrafo:

Ciascuna delle suddette procedure è argomento di una successiva e più dettagliata descrizione, nell'ambito delle altre parti della ISTRUZIONE OPERATIVA in 1.1,che ne indirizza e caratterizza l'utilizzo in funzione del tipo di TITOLARE.

4.1 RICHIESTA DEI CERTIFICATI

La procedura di richiesta dei CERTIFICATI è propedeutica alla loro emissione.

È effettuata da parte di un richiedente autorizzato, il cosiddetto TERZO INTERESSATO, che si assume la responsabilità di verificare l'identità del TITOLARE del CERTIFICATO.

Questa procedura termina con la registrazione dei dati del TITOLARE negli archivi del CERTIFICATORE.

4.2 EMISSIONE DEI CERTIFICATI

La procedura di emissione dei CERTIFICATI è la procedura che consente l'emissione dal CERTIFICATORE al TITOLARE dei CERTIFICATI, di cui è stata fatta richiesta.

4.3 RICHIESTA DI NUOVI CODICI DI ATTIVAZIONE

Ove applicabile, questa procedura consente al TITOLARE di richiedere nuovi CODICI DI ATTIVAZIONE, eventualmente scaduti o smarriti, necessari all'emissione del CERTIFICATO.

4.4 REVOCA O SOSPENSIONE DEI CERTIFICATI

La REVOCA o la SOSPENSIONE di un CERTIFICATO ne tolgono la validità e rendono non validi gli utilizzi della corrispondente CHIAVE PRIVATA.

I CERTIFICATI revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal CERTIFICATORE e pubblicata con periodicità prestabilita nel registro dei CERTIFICATI.

La revoca e la sospensione di un CERTIFICATO hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso, e degli utilizzi della corrispondente CHIAVE PRIVATA effettuati successivamente a tale momento.

E' fatto obbligo di richiedere la REVOCA nel caso in cui:

- la CHIAVE PRIVATA sia stata compromessa, ed in particolare:
  - sia stato smarrito o rubato il dispositivo che contiene la Chiave Privata di firma;
  - sia venuta meno la segretezza della Chiave Privata o del codice di attivazione per accedervi;
  - sia compromesso il livello di affidabilità della Chiave Privata;

- il TITOLARE non riesce più ad utilizzare il dispositivo sicuro contenente la CHIAVE PRIVATA in suo possesso;
- si verifichi un cambiamento dei dati del TITOLARE presenti nel CERTIFICATO;
- termina il rapporto tra il TITOLARE e il CERTIFICATORE;
- viene verificata una condizione di non conformità della presente ISTRUZIONE OPERATIVA.

Il TITOLARE ha anche facoltà di richiedere la REVOCA di un CERTIFICATO per un qualunque motivo dallo stesso ritenuto valido e in qualsiasi momento.

Il CERTIFICATORE esegue la SOSPENSIONE del CERTIFICATO su propria iniziativa o su richiesta del TITOLARE o del suo TERZO INTERESSATO.

La SOSPENSIONE tutela il TITOLARE del CERTIFICATO quando non vi sia la possibilità di accertare in tempo utile l'autenticità di una richiesta di REVOCA e ragioni di urgenza impongano la cautelativa inefficacia del CERTIFICATO.

La SOSPENSIONE deve essere effettuata nel caso in cui:

- è stata effettuata una richiesta di REVOCA senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il TITOLARE o il CERTIFICATORE acquisiscano elementi di dubbio sulla validità del CERTIFICATO;
- è necessaria un'interruzione temporanea della validità del CERTIFICATO.

La SOSPENSIONE del CERTIFICATO determina l'immediata cessazione della validità del CERTIFICATO stesso.

4.5 RIATTIVAZIONE DEI CERTIFICATI

Questa procedura consente la riattivazione dei CERTIFICATI di cui è stata in precedenza effettuata la sospensione.

La riattivazione di un CERTIFICATO sospeso può essere richiesta soltanto dalla stessa persona che ha in precedenza richiesto la sospensione del CERTIFICATO.

4.6 RECOVERY DEI CERTIFICATI

Ove applicabile, questa procedura consente al TITOLARE il RECOVERY dei CERTIFICATI eventualmente danneggiati o compromessi.

4.7 RINNOVO DEI CERTIFICATI

I CERTIFICATI hanno una durata stabilita, oltre la quale il CERTIFICATO non è più valido.

Ove applicabile, questa procedura consente al TITOLARE di rinnovare i propri CERTIFICATI al momento della loro imminente scadenza.

(Fine documento)