IN.TE.S.A. S.p.a.
Qualified Trust Service Provider

Manuale operativo
per le procedure di firma elettronica qualificata remota
ai sensi del Regolamento (UE) 910/2014 (eIDAS)
delle ricevute di consegna di NEXIVE S.p.A.

Codice documento: MO_NXV

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 13/03/2018

Versione: 01

REVISIONI

Revisione n°:	***01***	***Data Revisione:***	***13 marzo 2018***
Descrizione modifiche:	**Nessuna**		
Motivazioni:	**Prima emissione**		

Riferimenti di legge

Testo Unico - DPR 445/00 e successive modificazioni e integrazioni	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*". Nel seguito indicato anche solo come *TU*.
DLGS 196/03 e successive modificazioni e integrazioni	Decreto Legislativo n. 196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali*". Nel seguito indicato anche solo come *DLGS196/03*
CAD - DLGS 82/05 e successive modificazioni e integrazioni	Decreto Legislativo 7 marzo 2005, n. 82. "*Codice dell'amministrazione Digitale*". Nel seguito indicato anche solo come *CAD*.
DELIBERAZIONE CNIPA n. 45 e successive modificazioni e integrazioni	Deliberazione CNIPA 21 maggio 2009, n. 45. *"Regole per il riconoscimento e la verifica del documento informatico"*. Nel seguito indicato anche solo come *DELIBERAZIONE*
DPCM 22/02/2013 *Nuove Regole Tecniche* e successive modificazioni e integrazioni	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, ndr).* Nel seguito indicato anche solo come *DPCM*
DPCM 19/07/2012 e successive modificazioni e integrazioni	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma*".
Regolamento (UE) N. 910/2014 (eIDAS) e successive modificazioni e integrazioni	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *eIDAS*

Definizioni & Acronimi

Termine o acronimo	***Significato***
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigitPA): www.agid.gov.it. Nel seguito anche solo *Agenzia*.
Certificato Qualificato	Attestato elettronico, che contiene un insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. È rilasciato da un Certificatore Accreditato
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*) Persona fisica o giuridica che presta uno o più servizi fiduciari.
Certificatore Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID. (nelle more del Regolamento (UE) N. 910/2014).
CP	Certificate Policy - Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore / TSP che li ha emessi.

Termine o acronimo	*Significato*
Doc. Informatico	Documento Informatico: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Doc. Analogico	Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA	Firma elettronica Avanzata – ex Art.26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
Firma Digitale	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, 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
Firma remota	Particolare procedura di firma qualificata o di firma digitale che consente di garantire il controllo esclusivo del dispositivo di firma;
Firma automatica	Particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
HSM	Hardware Security Module - Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PKI	Public Key Infrastructure - Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA	Certification Authority: Entità della PKI che rilascia i certificati
RA Registration Authority	Autorità di Registrazione che su incarico del TSP esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al TSP. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del TSP (INTESA S.p.A.).
Validazione temporale	Informazione elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel momento
Terzo Interessato	Il terzo interessato è il terzo dal quale derivino i poteri del Titolare medesimo.
Titolare	Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.
TSA	Time Stamping Authority - Autorità che rilascia marche temporali.

A. Introduzione

A.1. Proprietà intellettuale

Questo documento è il *Manuale operativo per le procedure di firma elettronica qualificata remota delle ricevute di consegna di NEXIVE S.p.A.*, società con Sede Sociale in Via Fantoli 6/3, 20138 Milano - Capitale *Sociale 120'000 euro interamente versato - Iscrizione al Registro Imprese di Milano nr. 1551131, Codice Fiscale e P.IVA n. 12383760159 - direzione e coordinamento di PostNL N.V.*

A.2. Il Manuale Operativo

Il Manuale Operativo descrive le procedure e le relative regole utilizzate dal Certificatore Accreditato In.Te.S.A. S.p.A. (di seguito anche solo *INTESA* o *Certificatore*) per l'emissione dei Certificati Qualificati e la generazione e la verifica della firma elettronica qualificata nell'ambito dei servizi di Nexive (di seguito anche solo *Nexive* oppure *LRA – Local Registration Authority*).

Il contenuto di questo Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (di seguito anche solo "DPCM") e dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione Digitale", come successivamente modificato e integrato (di seguito anche solo "CAD") e in particolare:

- il capo II, Sez. II del CAD che disciplina le firme elettroniche e i certificatori;
- il capo VII del CAD, che prevede le modalità con le quali vengono dettate le regole tecniche.

Le attività descritte sono svolte in conformità con il Regolamento (UE) 910/2014 (eIDAS).

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme tempo per tempo vigenti.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dalla stessa Nexive che, in virtù di specifico accordo con il Certificatore, è autorizzata a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare una procedura di Firma Remota di documenti.

A.3. Validità

Quanto descritto in questo documento si applica al Certificatore, cioè alle sue infrastrutture logistiche e tecniche e al suo personale, alla Local RA Nexive, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti sui quali sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'art. 5 del DPCM, al comma 4. Ai fini previsti dal presente manuale, le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali;

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e relative regole utilizzate dal certificatore accreditato INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei certificatori accreditati.

Pertanto, in funzione delle normative menzionate, vengono coinvolte più entità che saranno meglio identificate nel proseguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n. 03 del *Manuale Operativo del Certificatore Accreditato INTESA per le procedure di firma remota nell'ambito dei servizi di Nexive* rilasciata il 13/12/2017, in conformità con l'art. 40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.50.9***.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica anche presso l'indirizzo Internet

http://e-trustcom.intesa.it/DOCS/mo_nexive.pdf

La pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire sul sito sopra indicato solo successivamente al loro inoltro all'Agenzia per l'Italia Digitale.

Lo stesso manuale operativo viene pubblicato e aggiornato in simultanea anche sul sito di Nexive.

B.2. Dati identificativi del Certificatore

Il Certificatore, ai sensi dell'art. 29 del CAD, è la società INTESA, di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289** **10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**n. Iscrizione 1692/87**
n. di Partita I.V.A.	**05262890014**
n. di telefono (centralino)	**+39.011.19216.111**
Sito Internet	**www.intesa.it**
n. di fax	**+39.011.19216.375**
Indirizzo di posta elettronica	**marketing@intesa.it**
Indirizzo (URL) registro dei certificati	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'art. 40 comma 3 lett. c) del DPCM è di INTESA, nella persona di Antonio Raia, il quale ne cura la stesura, la pubblicazione, l'aggiornamento e ogni eventuale revisione, in accordo e in collaborazione con Nexive.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, INTESA ha predisposto i seguenti strumenti:

un recapito di posta elettronica:	***e-trustcom@intesa.it***
un recapito telefonico:	+39 011.192.16.111
un recapito fax:	+39 011.192.16 375
un servizio di HelpDesk	per le chiamate dall'Italia 800.80.50.93 per le chiamate dall'estero +39 02.871.193.396

B.4. Entità coinvolte nei processi

All'interno della struttura del certificatore vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal Certificatore espletando, per la parte di loro competenza, le attività a loro attribuite.

B.5. Certification Authority

INTESA, operando in ottemperanza con quanto previsto dal DPCM, dal CAD e dal Reg. eIDAS, espleta le attività di TSP Qualificato Accreditato. Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per la firma digitale remota.

I dati identificativi del certificatore accreditato INTESA sono riportati al precedente paragrafo B.2.

B.6. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (Firma Remota nell'ambito delle applicazioni di Nexive descritte in questo Manuale Operativo), il Certificatore ha rilasciato mandato a svolgere le funzioni di Local Registration Authority a Nexive. In particolare, la LRA svolge le seguenti attività:

- Identificazione del Richiedente e/o Titolare.
- Registrazione del Richiedente.

Nexive, nello svolgimento della propria funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente.

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dalla normativa vigente (vedi Riferimenti di legge).

In particolare, INTESA:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- identifica con certezza la persona che fa richiesta della certificazione;
- specifica nel certificato qualificato, su richiesta dell'istante e con il consenso del Terzo Interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi secondo quanto indicato nel cap. F.1;
- informa i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali;
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
- garantisce il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- non copia, nè conserva le chiavi private di firma del soggetto cui il TSP ha fornito il servizio di certificazione;
- assicura che il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra queste citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il TSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- raccoglie i dati personali direttamente dalla persona cui si riferiscono o, previo suo esplicito consenso, attraverso personale esterno da lui delegato. I dati così raccolti saranno soltanto quelli necessari al rilascio e al mantenimento del certificato, accompagnati dall'informativa prevista dalla disciplina in materia di dati personali.

La generazione dei certificati qualificati è conforme all'Art.18 del DPCM e secondo quanto disposto dalla Deliberazione 45/2009. Quindi:

- prima di emettere il certificato qualificato il TSP deve:

a) accertarsi dell'autenticità della richiesta
b) verificare il possesso della chiave privata e il corretto funzionamento della coppia delle chiavi;

- il certificato qualificato deve essere generato con un sistema conforme a quanto previsto dall'art.33 del DPCM;
- il termine del periodo di validità del certificato qualificato precede di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verifi carne l'autenticità;
- l'emissione dei certificati qualificati è registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione;

Secondo quanto stabilito dall'Art.14 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il Certificatore:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati (Art.42 DPCM);
- garantisce l'interoperabilità del prodotto di verifica (DPCM, Art.42, comma 2);
- mantiene copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione e la rende rende accessibile per via telematica (DPCM, Art.42, comma 3).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato qualificato per i servizi descritti nel presente Manuale Operativo è un postino o driver di Nexive, la quale opera da Registration Authority.

In quanto Titolare, potrà utilizzare il proprio certificato qualificato per la Firma Digitale Remota per sottoscrivere documenti relativi ai servizi erogati da Nexive.

Il Titolare è tenuto a conservare le informazioni necessarie all'utilizzo della chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, art. 32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al Certificatore, tramite Nexive, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- dare immediata comunicazione alla LRA, in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma; Nexive provvederà all'immediato blocco degli stessi e dei canali di accesso ai servizi di firma digitale;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

Coloro che si avvalgono di un Certificato Qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a verificare:

- la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio e il momento della sua emissione;
- l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e il momento della sua emissione;
- la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori e su eventuali certificati derivanti da accordi di mutua certificazione tra il proprio Certificatore e quelli altrui;
- l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del Certificatore che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato nei servizi descritti dal presente Manuale Operativo è Nexive spa.

Pertanto, il terzo interessato deve verificare che il richiedente il certificato sia in possesso di tutti i requisiti necessari e lo autorizza a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota.

Nexive, nella sua veste di Terzo Interessato, svolge un'attività di supporto al Titolare; in particolare sarà Nexive ad indicare al Certificatore:

- eventuali ulteriori limitazioni d'uso del Certificato Qualificato per la Firma Digitale oltre a quelle previste al paragrafo *F.3*;
- informazioni specifiche relative al Titolare, quali a titolo esemplificativo, ma non esaustivo, eventuali poteri di rappresentanza del Titolare.

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente inoltrata quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato il certificato qualificato.

C.5. Obblighi della Local Registration Authority

Il Certificatore, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale di ulteriori soggetti (nel seguito denominati RA esterne) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. In particolare, le RA esterne espletano le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- registrazione del Titolare;
- consegna al Titolare dei codici che gli permettano di accedere alla propria chiave di firma nel rispetto degli artt. 8 e 10 comma 2 del DPCM.

Il Certificatore ha rilasciato mandato a svolgere la funzione di Local Registration Authority a Nexive mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere la LRA alla quale INTESA assegna l'incarico di RA e sui quali il Certificatore ha l'obbligo di vigilare; in particolare si richiede di:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente (CAD e successive modificazioni, DPCM, eIDAS);
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il Dlgs. 196/03;
- rendere disponibile per il Certificatore il materiale raccolto nella fase di identificazione e l'autorizzazione all'uso dei dati personali.

Il personale della LRA svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

La documentazione relativa alle attività di cui sopra, necessaria all'emissione del Certificato Qualificato, viene inviata alla RA INTESA e conservata dal TSP, secondo gli obblighi di legge, per 20 (venti) anni.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore - Limitazione agli indennizzi

Conformemente a quanto previsto dal CAD, dal DPCM e dal D. Lgs. 196/03, INTESA è responsabile, verso i Titolari per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal D. Lgs 196/03 e dal CAD e successive modificazioni e integrazioni (vedi Capitolo C, paragrafo C.1, "Obblighi del Certificatore Accreditato").

INTESA, fatto salvo i casi di negligenza, dolo o colpa grave, non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'art. 5 del DPCM, e, in particolare, dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Parimenti, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano

anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

Il Certificatore non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al paragrafo *F.3*.

D.2. Assicurazione

In base a quanto previsto dall'art. 15, comma 1, lettera i) del DPCM, il Certificatore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e degli eventuali danni causati a terzi, derivanti dall'erogazione del servizio di certificazione, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è stata inviata all'Agenzia per l'Italia Digitale apposita copia.

I massimali della copertura Assicurativa sono conformi alla normativa vigente.

E. .Tariffe

Il Servizio viene fornito da Nexive S.p.A. ai Titolari senza oneri e non è pertanto soggetto a tariffazione.

F. Modalità di identificazione e registrazione degli utenti per il rilascio del Certificato Qualificato

F.1. Identificazione degli utenti

Il Certificatore deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

Questa operazione viene demandata alla LRA Nexive che identificherà *de visu, in presenza,* il Titolare e ne opererà la registrazione ai fini dell'emissione del certificato.

Per i successivi rinnovi, anche se effettuati prima che il certificato qualificato già rilasciato sia scaduto, tale attività dovrà essere ripetuta. Sarà inoltre cura del Titolare comunicare al Certificatore attraverso la LRA gli eventuali cambiamenti relativi ai propri dati di registrazione.

Fra i dati di registrazione necessari all'avviamento del servizio, ricordiamo:

- nome e cognome;
- data di nascita;
- comune o stato estero di nascita;
- codice fiscale;
- numero di telefono cellulare;
- indirizzo di posta elettronica;
- tipo e numero del documento d'identità esibito;
- autorità che ha rilasciato il documento e data di scadenza.

F.1.1. Modalità operative

L'operatore della Local RA (Capo filiale delle sedi di partenza dei postini / driver Nexive) si collegherà in prima istanza al portale di censimento dei titolari (i postini / driver).

L'operatore, durante la compilazione del form, richiederà al futuro titolare di esibire:

- Documento di riconoscimento (carta d'identità, Passaporto)
- Codice Fiscale (opzionale)

Ne farà una fotocopia da allegare alla documentazione.

Quindi, con i documenti a portata di mano, immetterà nel form:

- Cognome
- Nome
- Codice Fiscale (inserito dalla documentazione fornita)

- Riferimento Documento: la scansione del codice a barre che apporrà nella documentazione
- Data di scadenza del documento (il documento deve essere valido)

Compilerà anche la parte relativa alla funzione del titolare del certificato e l'area di competenza.

A fronte dell'immissione dei dati di registrazione, saranno prodotte due copie del modulo di richiesta di certificazione, una da trattenere e l'altra da consegnare al Titolare.

Sul modulo saranno apposte tre firme da parte del futuro Titolare su ciascun modulo nelle sezioni apposite allo scopo di raccogliere:

- Il consenso all'informativa sulla privacy
- La conferma della presa visione del manuale operativo
- Il consenso alla pubblicazione del certificato su x.500

Nell'ultima sezione del modulo, l'operatore di LRA certificaherà l'avvenuto riconoscimento.

I dati di registrazione dell'utente e la copia del proprio documento d'identità verranno inviati in conservazione a norma e conservati da Nexive (in qualità di LRA) come da normativa vigente fino al completamento delle attività di conservazione sostitutiva.

F.2. Certificato Qualificato per la Firma Digitale

Il Certificato Qualificato per la Firma Digitale sarà rilasciato, previa richiesta al Certificatore, al Titolare in possesso del palmare a lui assegnato e utilizzato per le attività connesse al servizio fornito da Nexive.

F.2.1. Modalità operative

All'assegnazione del palmare, il postino / driver eseguirà come prima attività il cambio password del profilo del dispositivo.

Successivamente gli verrà chiesto di scegliere il PIN di sblocco del certificato: questo PIN, conosciuto esclusivamente dal titolare del certificato, garantisce il titolare da utilizzi a sua insaputa.

Sono previste, inoltre, *domande di sicurezza*, che potranno permettere il recupero del PIN nel caso in cui il titolare non lo ricordi in modalità autonoma.

Con quest'operazione termina il processo di emissione del certificato di firma qualificata.

F.3. Limitazioni d'uso

Nel Certificato Qualificato emesso nell'ambito dei servizi descritti nel presente Manuale, è inserito il seguente limite d'uso:
"***Il presente certificato e' valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti per Nexive S.p.A.*** ".

"This certificate may only be used for unattended/automatic digital signature for the signature of documents for Nexive S.p.A.".

G. Modalità operative per la sottoscrizione di documenti

Il Certificatore rende disponibile ai Titolari un'applicazione di firma conformemente a quanto previsto dalla normativa vigente.

I documenti sottoscritti con tale applicazione di firma, come richiesto dall'art. 4 comma 3 del DPCM, non conterranno macro istruzioni o codici eseguibili, tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati.

I documenti sottoscritti con firma elettronica qualificata sono le ricevute di consegna già sottoscritte con firma elettronica semplice dal Destinatario della corrispondenza Nexive.

Il processo di firma viene innescato in presenza dell'azione di recapito di una raccomandata:

- La ricevuta di consegna è un file PDF composto da un template, alcuni dati anagrafici del Destinatario e del Postino/Driver e tratto grafico generato dal destinatario in fase di consegna, inserendo all'interno del documento (in modalità nascosta) i dati di contesto raccolti al punto

precedente e viene apposta un Firma Elettronica Semplice utilizzando un Certificato Digitale non qualificato intestato a Nexive, volto a garantire garantire l'integrità del documento firmato.

- Il documento firmato con Firma Elettronica Semplice viene salvato all'interno dell'applicazione, in attesa di essere inviato ai server per l'apposizione della Firma Elettronica Qualificata da parte del Postino/Driver (Titolare).
- Il documento firmato con firma semplice, viene inviato ai sistemi di INTESA, contestualmente all'identificativo del Postino/Driver e al suo PIN di sblocco del Certificato Digitale, per la validazione temporale e la Firma Elettronica Qualificata, apposta mediante un Certificato Digitale Qualificato a lui intestato e residente sui dispositivi sicuri di INTESA (HSM).
- Il documento firmato con Firma Elettronica Qualificata viene restituito a Nexive, che si occuperà poi di inviarlo eventualmente presso il proprio sistema di Conservazione a norma.

G.1. Processo di Firma

Entrato in possesso dei necessari codici durante la fase d'identificazione, il postino potrà attivare la procedura di Firma di un documento secondo le modalità sotto descritte.

- Il postino / driver, al momento della partenza dalla sede Nexive, ritira uno dei dispositivi disponibili, che non sono univocamente assegnati, effettua il login con le proprie credenziali e inserisce una password di autenticazione personale.
- E' richiesto inoltre l'inserimento del PIN di sblocco del Certificato Digitale Qualificato necessario per le firme applicate (con procedura automatica) durante il turno di lavoro.
- Al temine del turno di lavoro, è prevista la riconsegna del dispositivo palmare, con contestuale log-out dal sistema e perdita delle informazioni relative allo sblocco del certificato qualificato (PIN).

I documenti che verranno sottoscritti con le modalità indicate in precedenza saranno esclusivamente in formato PDF (Deliberazione, art. 21, comma 8 e 15) e, pertanto, potranno essere verificati utilizzando il software Acrobat Reader DC scaricabile gratuitamente dal sito *www.adobe.com*.

H. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione

H.1. Generazione delle chiavi di certificazione

La generazione delle chiavi di Certificazione all'interno dei dispositivi di firma custoditi nei locali del TSP avviene in presenza del *Responsabile dei servizi di certificazione*, come previsto dal DPCM all'art. 7 comma 1, ed è preceduta dall'inizializzazione dei dispositivi di firma.

Il tutto avviene inoltre alla presenza di un numero di responsabili aziendali ritenuto adeguato e sufficiente ad evitare operazioni illecite.

Una volta generate le coppie di chiavi, quelle private vengono suddivise in più parti, ciascuna delle quali viene trascritta su più dispositivi di backup (token USB), secondo una logica *m di n*: gli n dispositivi sono suddivisi e consegnati alle n figure aziendali presenti, le quali vi associeranno una propria password.

I dispositivi sono conservati in modo sicuro, così come sono conservate in modo sicuro le relative password.

La lunghezza delle chiavi del sistema di certificazione è di 2048 bit.

H.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'art. 49 del DPCM.

La lunghezza delle chiavi del sistema di validazione temporale è di 2048 bit.

H.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore, è possibile procedere alla generazione delle chiavi di sottoscrizione.

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato autenticandosi al sistema fornitogli da Nexive nella modalità precedentemente descritta.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è di 2048 bit) vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa vigente.

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta al paragrafo *H.1*, sono generati i certificati delle chiavi pubbliche conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia per l'Italia Digitale attraverso il sistema di comunicazione di cui all'art. 16 comma 1 del DPCM.

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, art. 42, commi 1 e 3).

I.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema di generazione conforme con l'art. 33 del DPCM .

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel paragrafo *H.3*, è possibile generare una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione di Nexive al Certificatore.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, art. 18, comma 4).

I.3. Informazioni contenute nei certificati

I certificati INTESA, emessi nell'ambito del presente manuale, sono certificati qualificati ai sensi del Regolamento UE 910/2014 (eIDAS) e che, pertanto, ne è garantita la loro interoperabilità e riconoscimento a livello comunitario.

Il Certificato Qualificato definisce con certezza il Certificatore che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

Ogni Certificato Qualificato per la Firma Digitale contiene, a titolo esemplificativo ma non esaustivo, le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del Certificatore;
- codice identificativo unico del Titolare presso il Certificatore;
- nome, cognome, codice fiscale del Titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale, contengono almeno il limite d'uso riportato al par. *F.3*:

I.4. Codice di Emergenza

Il Certificatore garantisce un codice di emergenza da utilizzarsi per richiedere la sospensione del Certificato (DPCM, art. 21).

Nelle applicazioni descritte dal presente Manuale Operativo, il codice di emergenza è definito e assegnato al Titolare come segue: NEXIVEXXXX, dove XXXX corrisponde al codice numerico del postino.

J. Modalità di revoca e sospensione dei certificati

J.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista CRL (art. 22 DPCM).

Il profilo delle CRL/CSL è conforme con lo standard RFC 3280.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

Ai sensi della Determinazione Commissariale 119/2016 e del regolamento eIDAS, le informazioni di revoca e sospensione sono anche disponibili attraverso il protocollo OCSP.

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato (artt. 23, 25, 27 e 29 del DPCM), il Certificatore notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato (art. 24 comma 1 DPCM).

J.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca mettendosi in contatto diretto con la LRA Nexive.

Il Certificatore, avvertito dalla LRA, provvederà alla immediata revoca del certificato.

J.1.2. Revoca su richiesta del Terzo Interessato

Nexive, in qualità di Terzo Interessato può richiedere la revoca del certificato.

Il Certificatore, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso e inserirà il certificato nella lista di revoca, che sarà emessa il prima possibile.

J.1.3. Revoca su iniziativa del Certificatore

Il Certificatore, salvo i casi di motivata urgenza, potrà revocare il certificato dandone preventiva comunicazione al Titolare all'indirizzo di posta certificata comunicato in fase di registrazione specificando i motivi della revoca e data e ora a partire dalle quali tale revoca sarà efficace.

Una comunicazione analoga verrà inviata dal Certificatore anche al Terzo Interessato.

J.1.4. Revoca dei certificati relativi a chiavi di certificazione

Nei casi di:

1. compromissione della chiave di certificazione,
2. guasto del dispositivo di firma (HSM),
3. cessazione dell'attività,

il Certificatore procede con la revoca dei certificati di certificazione corrispondenti e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione.

Entro 24 ore, il Certificatore notificherà la revoca all'Agenzia per l'Italia Digitale e ai Titolari.

J.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al capitolo J.1.

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba effettivamente essere revocato.

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli artt. 23, 24 e 25 (Certificatore, Titolare, Terzo Interessato).

In assenza di comunicazioni da parte del Titolare, il certificato verrà automaticamente revocato dopo un periodo di sospensione di 90 (novanta) giorni o comunque entro la data di scadenza del certificato stesso.

La data di decorrenza della revoca coinciderà, in ogni caso, con la data di decorrenza della sospensione.

J.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione del certificato mettendosi in contatto diretto con la LRA Nexive.

Il Certificatore, avvertito dalla LRA, provvederà alla immediata revoca del certificato.

Il Titolare successivamente potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre dalla LRA.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione.

J.2.2. Sospensione su richiesta del Terzo Interessato

Nexive, in qualità di Terzo Interessato, potrà richiedere la sospensione del certificato.

Il Certificatore, accertata la correttezza della richiesta, sospenderà immediatamente il certificato e darà notizia della sospensione ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso.

J.2.3. Sospensione su iniziativa del Certificatore

Il Certificatore salvo i casi di motivata urgenza potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo di posta certificata comunicato in fase di registrazione specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

Una comunicazione analoga verrà inviata dal Certificatore anche al Terzo Interessato.

K. Modalità di sostituzione delle chiavi

K.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare

I certificati digitali emessi dal Certificatore hanno validità di 60 (sessanta) mesi dalla data di emissione.

Al termine dei cinque anni si renderà necessaria l'emissione di un nuovo certificato e la sostituzione delle chiavi precedentemente utilizzate dal Titolare con una procedura del tutto simile a quella seguita per l'emissione di un nuovo certificato (primo rilascio).

K.2. Sostituzione delle chiavi del Certificatore

K.2.1. Sostituzione pianificata delle chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alla coppia di *Chiavi di certificazione*, in presenza del *Responsabile del servizio di certificazione* e di responsabili aziendali in numero sufficiente a garantire la sicurezza dell'operazione, si procederà alla generazione di nuove chiavi di certificazione.

L'attività è pianificata in modo da garantire la continuità dei servizi, compatibilmente al fatto che Il termine del periodo di validità di un certificato qualificato deve precedere di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità (DPCM, art.18, comma 3).

Quanto fatto sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza del certificato.

K.2.2. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati

Il procedimento utilizzato in caso di guasto del dispositivo di firma o di disastro presso la sede centrale è trattato alla sezione 0.

K.2.3. Sostituzione pianificata delle chiavi del sistema di validazione temporale

In conformità con quanto indicato all'art. 49 comma 2 del DPCM, al fine di limitare il numero di marche temporali generate con la medesima coppia di chiavi di marcatura temporale, queste sono sostituite entro 90 (novanta) giorni dalla data della loro creazione. Contestualmente, un nuovo certificato è emesso relativamente alla nuova coppia di chiavi, senza revocare il certificato corrispondente alla chiave precedentemente in uso *H.2*.

K.2.4. Sostituzione in emergenza delle chiavi del sistema di validazione temporale

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) o di disastro presso la sede centrale è descritto alla sezione 0.

L. Registro dei certificati

L.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

1. I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
2. I certificati delle chiavi di certificazione.
3. I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
4. Certificati per le chiavi di firma dell'Agenzia.
5. Le liste di revoca e sospensione.

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno: questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

L.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL.

L'accesso è possibile all'indirizzo ***ldap://x500.e-trustcom.intesa.it*** secondo il protocollo LDAP. Il Certificatore consente l'accesso alle CRL anche via Internet attraverso il protocollo http.

L.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se presenti almeno nel numero ritenuto adeguato ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

M. Modalità di protezione dei dati personali

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal D. Lgs 196/03 e successive modificazioni e integrazioni.

N. Procedura di gestione della copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato alla sezione L.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del TSP (DPCM, Art.36).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (DPCM, art. 49 comma 1).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (DPCM, art. 52).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

O. Procedura di gestione degli eventi catastrofici

Il *Responsabile della sicurezza* gestisce un piano di gestione degli eventi catastrofici che prevede le seguenti fasi:

- gestione dell'emergenza: in questa fase è garantita la continuità di accesso alle CRL/CSL; la loro emissione può subire ritardi derivanti dalla necessità di attivare il server di back up della CA, situato nel sito di back up;
- gestione del transitorio: in questo periodo è assicurata l'emissione dei certificati e il ripristino di ulteriori soluzioni di disaster recovery;
- ritorno dell'esercizio a regime: nel medesimo sito originale o in un altro alternativo, ma definitivo.

La presenza di repliche della copia operativa del registro dei certificati distribuite in più punti consente comunque, in caso di interruzione di funzionamento della sede principale, di accedere al contenuto del registro dei certificati aggiornato fino al momento dell'interruzione.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL/CSL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e dello HW, anche della situazione di emergenza. È previsto inoltre l'intervento entro il medesimo lasso di tempo dei depositari delle componenti la chiave privata della CA ai fini di ricostruirla nel dispositivo di firma del sito di backup.

In tutte le località interessate dalla gestione degli eventi catastrofici è depositata copia cartacea del piano di emergenza.

P. Modalità per l'apposizione e la definizione del riferimento temporale

Tutte le macchine del sistema di PKI del TSP INTESA sono sincronizzate con l'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata da un software specifico installato su ogni server che, mediante il protocollo NTP (Network Time Protocol), si collega al server remoto configurato.

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per passare l'informazione di tempo e di data sulla rete Internet. Esso permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.

L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il software installato presso il TSP INTESA si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l'ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (GG/MM/YYYY HH:MM:SS), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM, art. 51.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (DPCM, art. 41).

P.1. Modalità di richiesta e verifica marche temporali

Il Certificatore appone una marca temporale su tutti i documenti sottoscritti dal Titolare nell'ambito dei servizi descritti da questo Manuale Operativo.

L'apposizione di detta marca è un processo integrato con l'operazione di firma e non richiede nessuna attività specifica da parte del Titolare.