

IN.TE.S.A. S.p.A.
Manuale Operativo:
Certificati qualificati di sottoscrizione
& validazione temporale

Codice documento: MO

Redazione: Antonio Raia

Approvazione: Franco Tafini

Revisione: 10

Data di rilascio: 21/11/2016

Firmato da:

ANTONIO RAIA

Certificato emesso da: IN.TE.S.A. Certification Authority, IN.TE.S.A. S.p.A., IT



REVISIONI

Revisione n°:	01	Data Revisione:	12 Ottobre 2000
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		
Revisione n°:	02	Data Revisione:	20 Giugno 2002
Descrizione modifiche:	Aggiornamenti		
Motivazioni:	Riorganizzazione aziendale; recepimento nuove normative; revisione procedure di emissione e gestione certificati; modifica URL dei servizi INTESA; aggiornamento Riferimenti di Legge; aggiornamento Definizioni e Acronimi; termini assicurativi; prezzo certificati.		
Revisione n°:	03	Data Revisione:	07 Ottobre 2002
Descrizione modifiche:	Correzioni o integrazioni in: pag. 6: eliminato riferimento al DL 23/01/2002; pag. 17: integrazione al 5° elenco puntato; pag. 23: penultimo capoverso; pag. 25: terzo capoverso; pag. 27: punto "d"; pag. 34: paragrafo K.2.2 primo capoverso.		
Motivazioni:	Aggiornamenti		
Revisione n°:	04	Data Revisione:	02 Febbraio 2005
Descrizione modifiche:	<ol style="list-style-type: none"> Aggiunti capitoli: <ul style="list-style-type: none"> Modalità per l'apposizione e la definizione del riferimento temporale Modalità operative per l'utilizzo del sistema di verifica delle firme Modalità operative per la generazione della firma digitale. Sostituiti i riferimenti al DPCM 08/02/99 con riferimenti al TU e DPCM 13/01/04. Modificati i dati identificativi del Certificatore nel Cap. B.2 Sostituiti i dati del Responsabile del Manuale Operativo nel Cap. B.3 Estensione dell'utilizzo delle chiavi di certificazione per l'emissione di certificati di CNS e di Crittografia Rivisto e completato il Par. I.1.2 Revoca su richiesta del Terzo Interessato 		
Motivazioni:	Adeguamento alla normativa vigente Aggiornamento delle procedure interne Cambiamento indirizzo sede legale dell'azienda		
Revisione n°:	05	Data Revisione:	22 Febbraio 2005
Descrizione modifiche:	<ol style="list-style-type: none"> In "Riferimenti di Legge" modificato "DL 196 30/06/03" con "DLGS 196 30/06/03" In "Definizioni e acronimi" aggiunte definizioni di "OID" e "ObjectIdentifier" In "Riferimenti tecnici" aggiunto RFC3039 Nel Cap. B.1 "Dati Identificativi della versione del Manuale Operativo" aggiunto OID Nel Par. H.3 "Informazioni contenute nei certificati" aggiunti dettagli sui contenuti dei certificati qualificati. Nel Par. O.1 "Servizio di validazione temporale" eliminato l'ultimo punto relativo alla verifica della marca temporale. Aggiunto Par. O.2 "Modalità di richiesta e verifica marche temporali" Nel Cap. P "Modalità per l'apposizione e la definizione del riferimento temporale" dichiarata la conformità al DPCM 13/01/04 Art.39.2. Aggiunto Par. O "Formati dei documenti" 		
Motivazioni:	Recepimento delle osservazioni di CNIPA sulla precedente versione		
Revisione n°:	06	Data Revisione:	30 Novembre 2006
Descrizione modifiche:	<ol style="list-style-type: none"> Introdotti i "Riferimenti di Legge" al Codice dell'Amministrazione Digitale 		
Motivazioni:	Adeguamento alla normativa vigente		
Revisione n°:	07	Data Revisione:	10 Luglio 2007
Descrizione modifiche:	<ol style="list-style-type: none"> Variato indirizzo sede Variati recapiti telefonici Nel Par.A.3.Validità, aggiunta l'autorizzazione all'utilizzo delle chiavi di certificazione per la generazione e la verifica delle firme associate a certificati destinati 		

- all'autenticazione dei server
4. Nel Cap.G.Modalità di generazione delle chiavi, inserite indicazioni circa la lunghezza delle chiavi di certificazione, di validazione temporale e di sottoscrizione
 5. Nel Par.H.3.*Informazioni contenute nei certificati*, eliminato il periodo <<L'indicazione del fatto che un certificato sia qualificato è attestato dalla presenza di un'apposita estensione "QcStatements" (OID 1.3.6.1.5.5.7.1.3) impostata al valore "QcStatement-1".>>

Motivazioni:	Trasloco in nuova sede Precisazioni tecniche	
	Revisione n°: 08	Data Revisione: 30 Novembre 2009
Descrizione modifiche:	Variati i riferimenti di legge: aggiornamenti al DPCM 30/03/09 e alla Deliberazione CNIPA 21/05/2009 Cambio Amministratore delegato	
Motivazioni:	Adeguamento alla nuova normativa vigente Variazioni organizzative	
	Revisione n°: 09	Data Revisione: 13 Giugno 2012
Descrizione modifiche:	Variazione riferimenti al software di Verifica Variazione dati Amministratore Delegato Sostituzione CNIPA con DigitPA	
Motivazioni:	Sostituzione del software di firma e verifica Variazioni organizzative DL 177 – 01/12/2009	
	Revisione n°: 10	Data Revisione: 21 novembre 2016
Descrizione modifiche:	Variazione dati societari e logo Aggiornamento definizioni e riferimenti normativi Aggiornamento cap. E - Tariffe Inserimento procedura per Riconoscimento a Distanza (F.1.5) Aggiornamento cap. R - Modalità operative per la generazione della firma digitale Formattazione Documento	
Motivazioni:	Aggiornamenti normativi: Regolamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 Variazioni organizzative Variazioni operative Aggiornamento tariffe Revisione documentale	

Sommario

Introduzione – Riferimenti Normativi & Acronimi	6
<i>Riferimenti di legge</i>	6
<i>Definizioni & Acronimi.....</i>	7
A. Il Manuale Operativo.....	8
A.1. Proprietà intellettuale	8
A.2. Applicabilità	8
A.3. Validità.....	8
B. Generalità.....	8
B.1. Dati identificativi della versione del Manuale Operativo.....	9
B.2. Dati identificativi del Prestatore di Servizi Fiduciari.....	9
B.3. Responsabilità del Manuale Operativo	9
B.4. Entità coinvolte nei processi	9
B.4.1. Certification Authority.....	10
B.4.2. Registration Authority (Ufficio RA).....	10
C. Obblighi	10
C.1. Obblighi del Prestatore di Servizi Fiduciari.....	10
C.2. Obblighi del Titolare.....	12
C.3. Obblighi degli utilizzatori dei certificati	12
C.4. Obblighi del Terzo Interessato	13
C.5. Obblighi delle LRA esterne	13
D. Responsabilità e limitazioni agli indennizzi.....	13
D.1. Responsabilità del Prestatore di Servizi Fiduciari	13
D.2. Assicurazione	14
D.3. Limitazioni agli indennizzi.....	14
E. Tariffe	14
E.1. Dispositivo di firma individuale	14
E.1. Dispositivo di firma remota.....	15
F. Modalità di identificazione e registrazione degli utenti.....	15
F.1. Identificazione degli utenti.....	15
F.1.1. Titoli e abilitazioni professionali	16
F.1.2. Poteri di rappresentanza	16
F.1.3. Limitazioni d'uso.....	16
F.1.4. Uso di pseudonimi	17
F.1.5. Riconoscimento remoto	17
F.2. Contratto di servizio tra INTESA ed Ente cliente.....	18
F.3. Registrazione degli utenti.....	18
G. Modalità di generazione delle chiavi	18
G.1. Generazione delle chiavi di certificazione.....	18
G.2. Generazione delle chiavi del sistema di validazione temporale	18
G.3. Generazione delle chiavi di sottoscrizione	19
G.3.1. Chiavi generate dal TSP.....	19
G.3.2. Chiavi generate dal Richiedente	19
H. Modalità di emissione dei certificati.....	19
H.1. Procedura di emissione dei Certificati di certificazione	19
H.2. Procedura di emissione dei Certificati di sottoscrizione	19
H.2.1. Emissione certificato per chiavi generate dal TSP	20
H.2.2. Emissione certificato per chiavi generate dal Richiedente	20
H.3. Informazioni contenute nei certificati.....	20
I. Modalità di revoca e sospensione dei certificati	20
I.1. Revoca dei certificati.....	20
I.1.1. Revoca su richiesta del Titolare.....	21

I.1.2. Revoca su richiesta del Terzo Interessato	22
I.1.3. Revoca su iniziativa del TSP	23
I.1.4. Revoca dei certificati relativi a chiavi di certificazione	23
I.2. Sospensione dei certificati	23
I.2.1. Sospensione su richiesta del Titolare	23
I.2.2. Sospensione su richiesta del Terzo Interessato	23
I.2.3. Sospensione su iniziativa del TSP	24
J. Modalità di sostituzione delle chiavi	24
J.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare	24
J.2. Sostituzione delle chiavi del Certificatore	24
J.2.1. Sostituzione pianificata delle chiavi di certificazione	24
J.2.2. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati	24
J.2.3. Sostituzione pianificata delle chiavi del sistema di validazione temporale	24
J.2.4. Sostituzione in emergenza delle chiavi del sistema di validazione temporale	25
K. Registro dei certificati	25
K.1. Modalità di gestione del Registro dei certificati	25
K.2. Accesso logico al Registro dei certificati	25
K.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati	25
L. Modalità di protezione della riservatezza	25
M. Procedura di gestione delle copie di sicurezza	25
N. Procedura di gestione degli eventi catastrofici	26
O. Procedure per la validazione temporale	26
O.1. Servizio di validazione temporale	26
O.2. Modalità di richiesta e verifica marche temporali	26
P. Modalità per l'apposizione e la definizione del riferimento temporale	27
Q. Modalità operative per l'utilizzo del sistema di verifica delle firme	27
R. Modalità operative per la generazione della firma digitale	28
R.1. Firma mediante dispositivo di firma individuale	28
R.1.1. Software di firma e verifica – DigitalSign	29
R.1.2. Software di firma e verifica – firma4ng	29
R.2. Firma con procedure automatiche	29
R.3. Firma Digitale Remota	29
R.3.1. Dispositivo di Firma Remota presso Terzi	30
R.4. Firma con certificato di validità temporale limitata	30
R.5. Firma con certificato “one-shot”	30
R.6. Autenticazione Biometrica	30
R.7. Formato dei documenti	31
ALLEGATO A	31

Introduzione – Riferimenti Normativi & Acronimi

Riferimenti di legge

Testo Unico DPR 445/00	Decreto del Presidente della Repubblica del 28 dicembre 2000, n.445. <i>"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"</i> . (G.U. n.42 del 20 febbraio 2001). Nel seguito indicato anche solo come <i>TU</i> .
DLGS 196/03	Decreto Legislativo n.196 del 30 giugno 2003 <i>"Codice in materia di protezione dei dati personali"</i> . (G.U. n.174 del 29 luglio 2003, suppl. ord.). Nel seguito indicato anche solo come <i>DLGS196/03</i>
CAD DLGS 82/05	Decreto Legislativo 7 Marzo 2005, n. 82. <i>"Codice dell'amministrazione Digitale"</i> . (G.U. n.112 del 16 Maggio 2005). Nel seguito indicato anche solo come <i>CAD</i> .
DLGS 235/2010	Decreto Legislativo 30 dicembre 2012, n. 235 <i>"Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n.69"</i> . (G.U. n.3 del 4 Gennaio 2013)
DELIBERAZIONE CNIPA n.45	Deliberazione CNIPA 21 Maggio 2009, n.45. <i>Regole per il riconoscimento e la verifica del documento informatico</i> . (G.U. n.282 del 3 dicembre 2009) Modificata dalla Determ. DigitPA n.69/2010. Nel seguito indicato anche solo come <i>DELIBERAZIONE</i>
DETERMINAZIONE COMMISSARIALE DIGITPA, n.69	Determinazione commissariale DigitPA 28/07/2010, n.69 <i>Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante Regole per il riconoscimento e la verifica del documento informatico, pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 282.</i>
DPCM 22/02/2013 Nuove Regole Tecniche	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 <i>"Regole tecniche in materia di generazione, apposizione e verifiche 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)</i> . (G.U. n.117 del 21 maggio 2013). Nel seguito indicato anche solo come <i>DPCM</i>
DPCM 19/07/2012	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 <i>"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."</i> (G.U. n. 237 del 10 ottobre 2012)
DPCM 05/02/2015	Decreto del Presidente del Consiglio dei Ministri 5 febbraio 2015 <i>"Modifiche al decreto del Presidente del Consiglio dei Ministri 19 luglio 2012."</i>
Regolamento (UE) N. 910/2014 (eIDAS)	Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, 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 <i>eIDAS</i>
D.Lgs 26 agosto 2016, n. 179	DECRETO LEGISLATIVO 26 agosto 2016, n. 179 <i>"Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche."</i> (GU Serie Generale n.214 del 13-9-2016)

Definizioni & Acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

Termine o acronimo	Significato
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigitPA): www.agid.gov.it Nel seguito anche solo <i>Agenzia</i> .
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. E' rilasciato da un Certificatore Accreditato
TSP	Trust service provider – Prestatore di servizi fiduciari (già <i>Certificatore</i>) 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.
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
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. Il Manuale Operativo

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di Prestatore di servizi fiduciari è coperto da diritti sulla proprietà intellettuale.

A.2. Applicabilità

Il presente documento costituisce il Manuale Operativo del Prestatore di Servizi Fiduciari In.Te.S.A. S.p.A., al quale d'ora in poi si farà riferimento anche solo come *INTESA* ovvero *TSP* (Trust Service Provider) o anche *TSP INTESA*.

Il contenuto del Manuale Operativo è conforme con quanto definito nelle regole tecniche contenute nel DPCM e nel CAD (e relative modifiche e integrazioni).

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

Questo documento descrive le regole e le procedure operative del TSP INTESA per l'emissione dei certificati qualificati, la generazione e la verifica della firma digitale e le procedure del servizio di validazione temporale, in conformità con la vigente normativa in materia.

A.3. Validità

Quanto descritto in questo documento si applica al TSP INTESA, cioè alle sue infrastrutture logistiche e tecniche, al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma digitale 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, che, al comma 4, distingue le chiavi e i correlati servizi 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 e alle loro liste di revoca (CRL) o sospensione (CSL), 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 TSP 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 tenuto da AgID.

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.10 del Manuale Operativo del Prestatore di Servizi Fiduciari INTESA, rilasciata il 21/11/2016 in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è 1.3.76.21.1.50.100.

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

http://e-trustcom.intesa.it/ca_pubblica/manuale_operativo.pdf

La pubblicazione di versioni aggiornate del Manuale Operativo avverrà sul sito sopra indicato solo successivamente al loro inoltro all'Agenzia.

INTESA ha adottato, come propria Certificate Policy, quanto indicato all'interno del documento ETSI 101 456 (OID 0.4.0.1456.1.1). Tale decisione è stata confortata dal fatto che la maggior parte dei certificatori europei hanno adottato tali indicazioni per le proprie certificate policy. Inoltre, tale certificate policy è stata riconosciuta comparabile alla US Federal Bridge CA Certificate Policy, Medium Level. L'adozione di tale policy permetterà quindi una più facile interoperabilità in sede europea e un'eventuale più agevole interazione con le amministrazioni del governo USA.

B.2. Dati identificativi del Prestatore di Servizi Fiduciari

Il TSP di cui il presente documento costituisce il "Manuale Operativo" ai sensi dell'Art.40 del DPCM è la società INTESA, di cui di seguito sono forniti 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 è di INTESA, nella persona di Antonio Raia (DPCM Art.40, comma 3.c), il quale ne cura la stesura, la pubblicazione e l'aggiornamento.

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 TSP INTESA 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 TSP INTESA espletando, per la parte di loro competenza, le attività a loro attribuite.

Pertanto saranno di seguito descritti gli ambiti nei quali il TSP opera e, di conseguenza, le entità coinvolte.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti:

- a) Responsabile della sicurezza.
- b) Responsabile del servizio di certificazione e validazione temporale
- c) Responsabile della conduzione tecnica dei sistemi
- d) Responsabile dei servizi tecnici e logistici.
- e) Responsabile delle verifiche e delle ispezioni (auditing).

Le figure sopra elencate sono tutte appartenenti all'organizzazione del TSP INTESA.

B.4.1. Certification Authority

INTESA, operando nell'ottemperanza di quanto previsto nelle Regole Tecniche (DPCM) e al Codice dell'Amministrazione Digitale (CAD) e del Regolamento eIDAS, espleta le attività di Prestatore di Servizi Fiduciari per le attività di emissione, pubblicazione, revoca e sospensione di certificati qualificati.

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

B.4.2. Registration Authority (Ufficio RA)

INTESA ha costituito al suo interno un'entità denominata *Ufficio RA* che ha funzioni di Registration Authority. In particolare, essa espleta le seguenti attività:

- Identificazione dei titolari.
- Registrazione dei titolari.
- Inizializzazione dei dispositivi sicuri di firma.
- Distribuzione dei dispositivi di firma.
- Gestione dell'inventario dei dispositivi di firma.
- Supporto al titolare.

L'Ufficio RA, all'interno di specifici accordi, ha inoltre l'incarico d'istruire il personale di entità esterne per la costituzione di Local Registration Authority (LRA). Queste ultime operano sul territorio svolgendo, anche solo in parte, le attività sopra elencate su incarico di INTESA.

C. Obblighi

C.1. Obblighi del Prestatore di Servizi Fiduciari

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 verificare 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 accessibile per via telematica (DPCM, Art.42, comma 3).

C.2. Obblighi del Titolare

Il Titolare è tenuto 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 TSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- indicare esplicitamente nella richiesta di certificazione le informazioni che egli desidera non siano inserite nel certificato;
- comunicare al TSP eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici o di Internet, ecc.;
- utilizzare dispositivi di firma conformi all'Art.11 del DPCM, nel caso in cui non sia il TSP a fornirli. Le informazioni relative a tale dispositivo dovranno comunque essere comunicate al TSP, in quanto INTESA intende conservare il controllo delle caratteristiche di sicurezza dei dispositivi di firma utilizzati dai Titolari e mantiene la corrispondenza tra certificato qualificato e dispositivo;
- conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza (DPCM, Art.8, comma 5);
- non duplicare la chiave privata né il dispositivo che la contiene (DPCM Art.8, comma 1), fatto salvo quanto disposto al medesimo Articolo, ai commi 2.3 e 4;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave (DPCM, Art.8, comma 5, lett. b);
- conservare con la massima diligenza i codici segreti, ricevuti dal TSP al fine di garantirne la massima riservatezza;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (DPCM, Art.5, comma 5);
- utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso nel caso la firma venga apposta per mezzo di una procedura automatica (DPCM, Art.5, comma 5);
- utilizzare esclusivamente il dispositivo fornito dal TSP, ovvero un dispositivo scelto tra quelli indicati dal TSP stesso (DPCM, Art.7, comma 6);
- richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso. chiave (DPCM, Art.8, comma 5, lett. C);
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua durata (DPCM, Art.28, comma 1);
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua decorrenza (DPCM, Art.24, comma 1);
- sporgere denuncia alle Autorità competenti in caso di smarrimento o sottrazione del dispositivo di firma.

C.3. Obblighi degli utilizzatori dei certificati

Coloro che utilizzino messaggi elettronici e/o evidenze informatiche firmati digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato allo standard ISO 9594-8, e il momento della sua emissione;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e il momento della sua emissione;
- verificare 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 TSP e quelli altrui;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del TSP che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, si tratti di persona fisica o di organizzazione (impresa, associazione di categoria, ente, ecc.), ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato, previa sua autorizzazione, al Titolare.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza;
- variazione dei dati identificativi dell'azienda (es. denominazione sociale, sede legale, etc.), cessazione dell'attività da parte dell'organizzazione e ogni altro dato rilevante o che influisca ai fini dell'uso del certificato.

La richiesta di revoca o sospensione da parte del Terzo Interessato deve essere inoltrata per iscritto e corredata di documentazione giustificativa. Inoltre, il Terzo Interessato è tenuto a porre a conoscenza dei Titolari, che a lui afferiscono, delle tematiche di sicurezza concernenti l'uso della firma digitale: custodia del dispositivo, accesso ai sistemi, nonché a quanto esposto nel presente Manuale Operativo.

C.5. Obblighi delle LRA esterne

Il TSP INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale, ai sensi dell'Art.1717 del codice civile, di ulteriori soggetti (nel seguito denominati LRA esterne) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. In particolare, le LRA esterne espletano le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- raccolta della richiesta di registrazione e certificazione compilata e sottoscritta dal Titolare;
- consegna del dispositivo di firma.

La documentazione raccolta deve essere trasmessa all'Ufficio RA di INTESA ovvero, previo accordo, trattenuta e conservata dalla LRA con le stesse modalità.

Le LRA esterne sono attivate dal TSP a seguito di un adeguato addestramento del personale indicato dall'Azienda o Ente con il quale viene stipulato un regolare Contratto di Mandato sottoscritto da entrambe le parti. In tale contratto sono esplicitati gli obblighi cui si deve attenere l'Azienda o Ente cui INTESA assegna l'incarico di LRA; in particolare deve:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente;
- impedire ai propri dipendenti la prosecuzione dell'attività di riconoscimento e curare l'immediato ritiro di ogni materiale qualora, per qualsiasi causa, si interrompa il rapporto in essere tra l'Azienda e il dipendente stesso, dandone tempestivamente notizia per iscritto a INTESA;
- custodire i dispositivi di firma fino alla consegna degli stessi ai Titolari destinatari, rispondendo direttamente della loro sottrazione o perdita per qualsiasi causa, con obbligo di comunicare senza ritardo tali eventi all'Ufficio di Registrazione di INTESA;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il Dlgs. 196/03.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Prestatore di Servizi Fiduciari

INTESA è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle proprie attività, come previsto dalla normativa vigente (vedi [C.1](#)).

INTESA non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dal DPCM, e in particolare, dal mancato rispetto da parte del Titolare, degli utilizzatori dei

certificati e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e dalla mancata osservanza da parte degli stessi della normativa vigente.

Si ricorda pertanto di conservare con speciale diligenza il dispositivo di firma per garantirne l'integrità e la massima riservatezza e di conservare sempre separatamente dal dispositivo stesso le informazioni di abilitazione all'uso dello stesso.

Per quanto non esplicitamente riportato si fa specifico riferimento a quanto espresso nel CAD, *Capo II, Sezione II Firme elettroniche e Certificatori, Art.32 Obblighi del Titolare e del Prestatore di servizi di firma elettronica qualificata.*

INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo di esempio: calamità naturali, 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.

D.2. Assicurazione

INTESA ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è stata inviata ad AgID apposita dichiarazione di stipula.

La copertura Assicurativa prevede i seguenti massimali:

- 250.000,00 (duecentocinquantamila) euro per singolo sinistro.
- 1.500.000,00 (unmilione cinquecentomila) euro per annualità.

D.3. Limitazioni agli indennizzi

Il TSP INTESA, fatto salvo i casi di dolo e colpa grave, esclude ogni responsabilità per danni subiti dagli utenti o da terzi in conseguenza di:

- mancato rispetto delle procedure e delle regole stabilite dal TSP;
- danno causato da disservizio;
- uso improprio dei certificati di sottoscrizione da parte di applicazioni di terze parti.

INTESA non si ritiene, peraltro, responsabile dei danni causati agli utenti Titolari e utilizzatori o a terzi conseguenti al non rispetto, da parte del Titolare, delle regole definite nel presente Manuale Operativo.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal certificatore accreditato.

E. Tariffe

E.1. Dispositivo di firma individuale

Si riportano le tariffe per l'emissione e il primo rinnovo del certificato qualificato su **dispositivo di firma individuale** (smartcard / token usb).

Le tariffe indicate non comprendono il servizio di riconoscimento del Titolare, quando questo non è effettuato nei locali della Registration Authority INTESA.

- Emissione di un certificato con validità di 2 anni su token USB: 70,00 euro
- Emissione di un certificato con validità di 2 anni su smartcard: 25,00 euro
- Software di firma, licenza annuale: 90,00 euro
- Revoca e/o Sospensione: gratuita

Le tariffe sopra indicate sono valide alla data di rilascio del presente MO e sono soggette a variazioni in funzione delle quantità trattate.

Per ulteriori informazioni: marketing@intesa.it

E.1. Dispositivo di firma remota

Per quanto riguarda la **firma remota**, le tariffe saranno concordate su base progettuale tra INTESA e il Cliente (Ente/Azienda) committente il servizio. Sarà cura di quest'ultimo indicare al Titolare (utilizzatore finale) un'eventuale tariffazione a suo carico.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

Il TSP verifica con certezza, *de visu* (in presenza o a distanza - cfr. [F.1.5](#)), l'identità del richiedente alla prima richiesta di emissione di certificato qualificato. Per i successivi rinnovi tale attività non sarà più ripetuta: sarà cura del Titolare comunicare al TSP eventuali cambiamenti relativi ai propri dati di registrazione.

L'attività di identificazione del richiedente viene effettuata:

- da INTESA, tramite le persone del proprio Ufficio RA;
- da LRA esterne; ad es. personale dell'Azienda o dell'Ente Cliente oppure di terze parti appositamente autorizzate dal TSP (vedi anche [C.5 Obblighi delle LRA esterne](#));
- da INTESA, ovvero da LRA esterne, tramite sistemi di riconoscimento a distanza (cfr. [F.1.5](#))

In ogni caso la persona che fa richiesta della certificazione viene identificata con certezza e viene archiviata da INTESA la fotocopia di almeno un documento ufficiale per lo Stato di appartenenza.

Il Titolare ovvero il Terzo Interessato, sottoscrivono:

- Il contratto di servizio, in duplice copia, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Digitale*, in duplice copia, in cui riporta i propri dati, tra cui:
 - Ente richiedente.
 - Cognome e nome.
 - Data e luogo di nascita.
 - Codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano).
 - Numero di telefono (fisso o cellulare).
 - Indirizzo di posta elettronica.
 - Tipo, numero ed Ente di rilascio del documento di identità esibito.
- Il documento *Presa visione del Manuale Operativo INTESA*, in duplice copia, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del DLgs 196/03.

Nel caso la chiave debba essere utilizzata da dispositivi HW con procedura automatica (DPCM, Art.5, comma 2 e 3), saranno notificati al richiedente gli estremi di detti apparati (es. produttore, modello e numero di serie).

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il TSP (che non verifica la validità dell'indirizzo) userà in seguito tale indirizzo per comunicare con il richiedente.

La documentazione precedentemente descritta, relativa alla registrazione dei Titolari, viene conservata da INTESA per 20 (venti) anni dalla scadenza del certificato a cura del *Responsabile dei servizi tecnici e logistici*.

Prima di avviare le procedure di richiesta, il richiedente dovrà munirsi del dispositivo di firma richiedendolo ad INTESA, ovvero acquistandolo da un terzo fornitore a patto che il dispositivo sia conforme alle specifiche di utilizzo di INTESA e dalla stessa approvato, nonché conforme all'Art.11 del DPCM.

Durante la fase di consegna del materiale, il personale INTESA addetto provvederà ad aggiornare il proprio database elettronico riportando i dati identificativi del dispositivo di firma (serial number, numero di lotto, ecc.).

F.1.1. Titoli e abilitazioni professionali

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a dimostrazione dell'effettiva sussistenza di tali abilitazioni professionali o documentazione equivalente (es. autocertificazione), così come indicato nella Deliberazione CNIPA n.45. Una copia di tale documentazione viene conservata dal TSP.

La documentazione atta a supportare la richiesta d'inserimento di titoli o abilitazioni professionali all'interno del certificato qualificato non può essere antecedente a 10 (dieci) giorni dalla data di presentazione della richiesta di emissione del suddetto certificato.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative ad abilitazioni professionali.

INTESA, in caso di autocertificazione, non si assume alcuna responsabilità, salvo i casi di dolo o colpa grave, per l'eventuale inserimento nel certificato d'informazioni autocertificate dal titolare.

F.1.2. Poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di poteri di rappresentanza (es. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un Cliente, etc.), il richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza di tali poteri di rappresentanza.

Per la rappresentanza di persone fisiche, il richiedente dovrà produrre una copia autentica della delega o procura notarile sottoscritta dalla persona rappresentata insieme all'attestazione di consenso di quest'ultima all'inserimento del ruolo nel certificato.

Nel caso in cui sia richiesta l'indicazione nel certificato di un ruolo relativo alla rappresentanza di organizzazioni o enti di diritto privato, il titolare dovrà presentare documentazione atta a comprovare il ruolo di cui si chiede l'inserimento nel certificato ed una dichiarazione dell'ente di appartenenza nel quale l'organizzazione autorizza il TSP all'inserimento dello specifico ruolo nel certificato. Quest'ultimo documento non dovrà essere antecedente 20 (venti) giorni rispetto alla data di richiesta di emissione del certificato qualificato.

L'inserimento nel certificato qualificato d'informazioni relative all'esercizio di funzioni pubbliche o poteri di rappresentanza in enti od organizzazioni di diritto pubblico sarà subordinato a specifici accordi con gli enti stessi. Sulla base di tali accordi sarà possibile specificare il ruolo del titolare all'interno dell'ente o organizzazione pubblica.

La documentazione prodotta sarà conservata dal TSP per un periodo di 20 (venti) anni.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative a poteri di rappresentanza.

F.1.3. Limitazioni d'uso

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di limiti d'uso ovvero di valore per i negozi per i quali può essere usato il certificato stesso, il richiedente deve sottoscrivere idonea documentazione attestante la richiesta. Una copia di tale documentazione viene conservata dal TSP.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.1.3.1. Limiti d'uso

Specifici limiti d'uso possono essere concordati con il Cliente, fermo restando che restano garantiti agli utenti i limiti d'uso ai sensi dell'art.12, comma 6, lett.c della DELIBERAZIONE indicati da AgID con specifica Circolare (www.agid.gov.it).

Inoltre, uno specifico limite d'uso deve essere utilizzato per indicare esplicitamente nel certificato qualificato che questo è utilizzato per apporre la firma digitale per mezzo di procedure automatiche (DPCM, Art. 5, comma 2).

F.1.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti un pseudonimo in alternativa ai propri dati reali. Anche in questo caso, poiché comunque ci si riferisce a certificati qualificati, il TSP conserverà le informazioni relative alla reale identità dell'utente per 20 (venti) anni dopo la scadenza del certificato stesso.

F.1.5. Riconoscimento remoto

Il servizio di identificazione potrà essere gestito, remotamente, come sotto descritto

Requisito necessario è la disponibilità di utilizzare un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante.

Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di RA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.

L'intera sessione viene registrata in modalità audio e video (sia lato richiedente che lato operatore) e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.

La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa distinguibile del documento di riconoscimento inquadrato). L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione.

- **Il Richiedente:**

1. si connette al sito della Registration Authority (RA), dove sono riportate tutte le istruzioni necessarie per eseguire la procedura di riconoscimento e dove sono indicati i documenti necessari per l'identificazione;
2. compila, sul sito della RA, una richiesta di certificato digitale compilando un form in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione;
3. prende visione del presente *Manuale Operativo*, che dovrà essere aperto in lettura. Lo stesso Manuale Operativo sarà anche disponibile al download dal sito stesso;
4. autorizza il consenso al trattamento dei dati personali;
5. esegue, tramite l'apposita funzione del sito, l'upload della copia scansionata dei documenti di identità (carta d'identità, passaporto, tesserino sanitario nazionale). L'invio preventivo di tali documenti conferma la volontà del Richiedente di completare la procedura di identificazione finalizzata all'emissione di un certificato qualificato utilizzabile esclusivamente nell'ambito dei servizi di firma qualificata forniti dal TSP;
6. Decide, eseguiti gli step precedenti, se continuare la sessione attivando appena possibile il collegamento via web cam oppure se continuare fissando un successivo appuntamento con gli operatori di RA, per completare in un momento successivo a lui più comodo la procedura;

- **L'operatore di RA:**

1. esegue controlli sui documenti ricevuti;
2. domanda, durante la sessione on-line (via web cam), al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi, verificando che nella foto del documento sia riconoscibile il Richiedente;
3. chiede all'utente, durante la registrazione, di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del soggetto richiedente

L'operatore deve essere libero di rifiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.

Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie per permettergli di utilizzare il certificato qualificato che sta per essergli emesso e di firmare digitalmente.

Si precisa che il Certificatore, in ottemperanza con il CAD (Art.35, comma 5), prevede esclusivamente l'impiego di dispositivi di autenticazione che abbiano ottenuto una valutazione positiva da parte di AgID.

La documentazione precedentemente citata, relativa alla registrazione dei Titolari, viene conservata dal TSP INTESA per 20 (venti) anni dalla scadenza del certificato, ovvero, in caso di specifici accordi, dalla Local RA che ha ricevuto mandato per operare come tale.

F.2. Contratto di servizio tra INTESA ed Ente cliente

Nel caso in cui il Cliente sia un Ente o una Azienda, i cui dati identificativi saranno definiti a contratto, si applicano anche le norme seguenti, fermo restando quanto specificato al paragrafo F.1, dal punto 2 in poi, per l'identificazione e la registrazione dei singoli Titolari.

1. Le persone delegate ad indicare il personale del Cliente abilitato ad essere certificato da INTESA faranno pervenire al TSP gli elenchi delle persone alle quali INTESA sarà autorizzata a rilasciare i certificati qualificati. In tali elenchi sarà possibile anche indicare eventuali limitazioni all'uso delle coppie di chiavi, poteri di rappresentanza o abilitazioni professionali.
2. Questi elenchi saranno resi disponibili agli addetti interessati: il personale dell'Ufficio RA e dell'Help Desk.
3. Le persone autorizzate esibiranno alle LRA documenti analoghi a quelli indicati al paragrafo F.1.
4. La LRA verificherà che la persona sia autorizzata ad essere certificata e opererà in conformità a quanto indicato al paragrafo F.1.

F.3. Registrazione degli utenti

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi del TSP. Questa operazione viene sempre eseguita dal personale dell'Ufficio RA di INTESA.

Durante la registrazione dei dati del Titolare viene generato l'identificativo univoco del Titolare presso il TSP.

G. Modalità di generazione delle chiavi

G.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 assoceranno 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.

G.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.

G.3. Generazione delle chiavi di sottoscrizione

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

Questa operazione può avvenire in due diverse modalità:

1. Chiavi generate dal TSP.
2. Chiavi generate dal Richiedente.

In ogni caso, avendo a disposizione il dispositivo di firma, il Titolare o gli operatori di RA INTESA potranno generare una nuova coppia di chiavi mediante la funzione di generazione di chiavi asimmetriche dello stesso dispositivo. Le chiavi vengono generate in conformità con il DPCM, Artt. 5 e 6.

I dispositivi di firma utilizzati rispondono ai requisiti di sicurezza previsti dall'Art.9 del DPCM. La lunghezza delle chiavi di sottoscrizione è di almeno 2048 nel caso di dispositivi di firma remota.

G.3.1. Chiavi generate dal TSP

Questa procedura viene effettuata dagli operatori di RA presso i locali del TSP INTESA.

Sono effettuate le seguenti operazioni:

1. L'operatore si autentica all'applicazione, seleziona i dati di registrazione del Richiedente e attiva la procedura di richiesta di certificato.
2. L'applicazione accede al dispositivo di firma con il PIN di default e genera la coppia di chiavi.

G.3.2. Chiavi generate dal Richiedente

Questa procedura può essere effettuata nei casi in cui il Richiedente disponga di un proprio dispositivo di firma e di un'applicazione in grado di generare sia la coppia di chiavi sullo stesso dispositivo, sia la richiesta di certificato in formato PKCS#10. La procedura può essere utilizzata per l'operazione di rinnovo di un precedente certificato generato dal TSP o per la prima emissione in base agli accordi con il personale INTESA.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo **G.1**, vengono 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 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 chiavi di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

H.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel paragrafo **G.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.

A seconda della modalità adottata per la generazione della coppia di chiavi, la richiesta di certificato sarà generata dalle diverse applicazioni attivate dall'operatore di RA di INTESA, ovvero dal Richiedente.

In ogni caso, la CA elabora immediatamente la richiesta ricevuta, in conformità con quanto previsto dal DPCM all'Art.18.

In particolare:

- si accerta dell'autenticità della richiesta (comma 1.a);
- si accerta che il Titolare sia effettivamente in possesso della chiave privata e verifica il corretto funzionamento della coppia di chiavi (comma 1.b).

Il certificato così generato è pubblicato sul registro dei certificati, dietro consenso del Titolare.

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

Il TSP mantiene le informazioni per l'identificazione del Titolare di un dispositivo sicuro di firma e dei certificati in esso contenuti, per un periodo pari a 20 (venti) anni dalla data di emissione del certificato qualificato, salvo quanto previsto dall'Art.11 del decreto legislativo n. 196/03.

Al termine del processo, sul dispositivo del Titolare saranno stati registrati, oltre alla chiave privata di firma:

- il certificato di sottoscrizione;
- il certificato elettronico relativo alla chiave pubblica del Certificatore Accreditato la cui corrispondente chiave privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del Titolare, come da Art.11, comma 5, del DPCM.

I seguenti paragrafi descrivono le operazioni effettuate per l'emissione dei certificati nelle due modalità previste dal TSP per la generazione delle chiavi.

H.2.1. Emissione certificato per chiavi generate dal TSP

In questo caso devono essere effettuate le seguenti operazioni:

1. L'applicazione attivata dall'operatore di RA, dopo la generazione delle chiavi secondo la procedura descritta al punto [G.3.1](#), genera la richiesta di certificato.
2. La richiesta viene direttamente inoltrata alla CA, firmata elettronicamente dall'operatore e trasmessa su canale sicuro.
3. Il certificato emesso viene ricevuto dall'applicazione e inserito sul dispositivo di firma con le dovute verifiche.
4. L'applicazione blocca il PIN di accesso al dispositivo di firma. Al Titolare sarà consegnata, separatamente, una busta contenente il PUK del dispositivo per l'attivazione del medesimo.

H.2.2. Emissione certificato per chiavi generate dal Richiedente

In questo caso devono essere effettuate le seguenti operazioni:

1. Il Richiedente, dopo aver generato la richiesta in formato PKCS#10 come sommariamente descritto al punto [G.3.2](#), invia la richiesta all'Ufficio RA INTESA su canale di comunicazione sicuro.
2. La richiesta pervenuta e debitamente verificata, viene inviata alla CA che emette il nuovo certificato di sottoscrizione.
3. INTESA invia il certificato di sottoscrizione al Richiedente, utilizzando un canale di comunicazione sicuro.
4. Il Richiedente importa il certificato sul dispositivo di firma.

H.3. Informazioni contenute nei certificati

I certificati qualificati emessi dal TSP INTESA sono conformi a quanto indicato nella deliberazione CNIPA n.45 del 21/05/09 e successive modificazioni e sono conformi al regolamento eIDAS.

I. Modalità di revoca e sospensione dei certificati

I.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista di revoca CRL (DPCM, Art.20).

Il profilo delle CRL/CSL è conforme con lo standard RFC 5280.

La CRL, firmata dalla CA, viene aggiornata con periodicità prestabilita (24h) e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

Informazioni circa la validità del certificato saranno rese disponibili anche via 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.

Un certificato può essere revocato nei seguenti casi, ad ognuno dei quali corrisponde un codice detto CRLReason indicato tra parentesi:

1. sostituzione del certificato senza compromissione della chiave privata (*CRLReason: Superseded*);
2. compromissione (perdita delle caratteristiche di sicurezza e univocità) della chiave privata del Titolare (*CRLReason: Key Compromise*);
3. i dati del certificato sono modificati o obsoleti; in questo caso ricade anche l'eventualità che un Titolare non accetti i certificati emessi a suo nome in quanto i dati sono errati (*CRLReason: Affiliation Changed*);
4. cessazione repentina, in condizioni di conflittualità o non, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati (*CRLReason: Cessation of Operation*);
5. mancato rispetto da parte del Titolare degli obblighi specificati nel Manuale Operativo, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata (*CRLReason: Unspecified*);
6. altri casi, che non ricadono nei precedenti (*CRLReason: Unspecified*); tuttavia, l'utilizzo di tale causale è deprecato e se ne sconsiglia l'utilizzo

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato e il motivo della revoca.

I.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca del proprio certificato secondo tre diverse modalità:

1. Qualora il Titolare disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo uff_ra@intesa.it contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata (il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'indirizzo internet http://e-trustcom.intesa.it/ca_pubblica/mod_revoca.doc). Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che permettano di identificare univocamente il certificato da revocare - vedi più sotto) e il motivo della richiesta (eventualmente facendo riferimento a quelli indicati al paragrafo [I.1](#)).
2. Nei casi in cui il Titolare non disponga di un proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente:
 - a. via fax, al numero indicato all'URL <http://www.hda.intesa.it/> nell'orario di servizio ivi riportato.
 - b. via posta ordinaria, all'indirizzo sempre indicato all'URL di cui al punto a.
3. Eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia *Key Compromise*, il Titolare potrà telefonare al numero fornito dal TSP al momento del rilascio del primo certificato qualificato a lui intestato. Egli dovrà fornire i dati relativi al certificato e il *Codice di Emergenza* (DPCM, Art.21). In questo caso il certificato indicato sarà temporaneamente sospeso in attesa della richiesta scritta del Titolare.

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'Art.24, comma 1, del DPCM.

Al di fuori degli orari di assistenza indicati all'URL <http://www.hda.intesa.it/>, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente, per quanto riguarda il Titolare interessato:

- generalità (es. nome, cognome, email, telefono, ente di riferimento)

- motivazione della richiesta
- momento di decorrenza del provvedimento.

Altri dati aggiuntivi possono essere utili al fine di identificare univocamente il certificato da revocare. Tali dati possono essere recuperati dal Titolare dalla documentazione rilasciata in fase di emissione, se ancora disponibile (es. tipo di dispositivo e numero seriale, organizzazione di riferimento, numero seriale del certificato, data di rilascio...).

Il TSP, accertata la correttezza della richiesta, darà notizia della revoca al Titolare tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca (CRL).

I.1.2. Revoca su richiesta del Terzo Interessato

Il Terzo Interessato può richiedere la revoca del certificato del Titolare.

Il TSP INTESA dispone tre diverse modalità per la richiesta di revoca da parte del Terzo Interessato:

1. Qualora il Terzo Interessato disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo **uff_ra@intesa.it** contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata (il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'URL http://e-trustcom.intesa.it/ca_pubblica/mod_revoca.doc). Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che permettano di risalire univocamente al certificato da revocare) e il motivo della richiesta (eventualmente facendo riferimento a quelli indicati al paragrafo. **I.1**).
2. Nei casi in cui il Terzo Interessato non disponga del proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente:
 - a. via fax, al numero indicato all'URL <http://www.hda.intesa.it/> nell'orario di servizio ivi riportato;
 - b. via posta ordinaria, all'indirizzo sempre indicato all'URL di cui al punto precedente.
3. Eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia *Key Compromise*, il Terzo Interessato potrà telefonare al numero fornito dal TSP al momento del rilascio del primo certificato qualificato a lui intestato. Egli dovrà fornire i dati relativi al certificato e il Codice di Emergenza (DPCM, Art.21). In questo caso il certificato indicato sarà temporaneamente sospeso in attesa della richiesta scritta del Titolare.

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'Art.25 comma 1 del DPCM.

Al di fuori degli orari di assistenza indicati all'URL <http://www.hda.intesa.it/>, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente:

- per quanto riguarda il Terzo Interessato:
 - Azienda di appartenenza
 - generalità
 - riferimenti al documento che lo autorizza a chiedere l'emissione, la revoca o la sospensione del certificato del Titolare interessato
 - suoi recapiti: telefonici e di posta elettronica
- per quanto riguarda il Titolare interessato:
 - generalità
 - estremi del certificato di cui si chiede la revoca o la sospensione
 - tipo (revoca o sospensione) e motivazione della richiesta, come indicato al par. **I.1** (CRLReason).
 - momento di decorrenza del provvedimento.

Il TSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca, che sarà emessa immediatamente.

1.1.3. Revoca su iniziativa del TSP

Il TSP INTESA può revocare i certificati dei Titolari nei casi indicati al par. [1.1](#) (CRLReason), in aggiunta ai motivi riportati al paragrafo seguente.

In ogni caso informerà della revoca i Titolari interessati tramite posta elettronica, altrimenti tramite posta ordinaria.

1.1.4. Revoca dei certificati relativi a chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- malfunzionamento del dispositivo sicuro per la generazione delle firme,
- cessazione dell'attività,

il TSP 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 TSP notificherà la revoca all'Agenzia e ai Titolari.

1.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al capitolo [1.1](#).

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 (ad esempio nei casi in cui si tema la compromissione della chiave privata o lo smarrimento/furto del dispositivo di firma, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

Per una sospensione, il codice di CRLReason è *certificateHold* e ha come conseguenza l'inserimento del certificato nella lista aggiornata di revoca (CRL).

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli Artt. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

Sarà cura del richiedente comunicare all'Ufficio RA di INTESA, con modalità analoghe a quelle utilizzate per la richiesta di sospensione, la richiesta di riattivazione o di revoca del certificato precedentemente sospeso.

In assenza di comunicazioni, il certificato verrà automaticamente revocato dopo il periodo di sospensione indicato dal Titolare nella richiesta, con la CRLReason indicata al momento della richiesta stessa (vedi [1.2.1](#)) e con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione).

1.2.1. Sospensione su richiesta del Titolare

Le modalità da seguire in questo caso sono le medesime indicate al capitolo [1.1.1](#), cui si aggiunge la possibilità di richiedere la sospensione immediata, che può essere inoltrata utilizzando il numero telefonico fornito dal TSP al momento del rilascio del primo certificato qualificato. Il Titolare comunicherà il *Codice di Emergenza* stabilito al momento dell'emissione del certificato (vedi paragrafo [H.2](#)) e specificherà il motivo della richiesta di sospensione, facendo riferimento a quelli indicati al par. [1.1](#) (CRLReason): durante la conversazione telefonica si farà comunicare il numero di fax o l'indirizzo postale, cui invierà la medesima richiesta su lettera a conferma della comunicazione telefonica.

Il Titolare specificherà nella richiesta la durata del periodo di sospensione, che in ogni caso non potrà superare i 90 (novanta) giorni.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione, con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione).

1.2.2. Sospensione su richiesta del Terzo Interessato

Le modalità da seguire in questo caso sono le medesime indicate al capitolo [1.1.1](#).

Il Terzo interessato specificherà nella richiesta la durata del periodo di sospensione, che in ogni caso non potrà superare i 90 (novanta) giorni.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione, con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione)..

1.2.3. Sospensione su iniziativa del TSP

Il TSP INTESA notifica la sospensione ai Titolari tramite posta elettronica oppure, in casi particolari, tramite posta ordinaria.

J. Modalità di sostituzione delle chiavi

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

I certificati digitali emessi dalla CA INTESA hanno validità 24 (ventiquattro) mesi dalla data di emissione, salvo accordo diverso con i singoli clienti.

Entro la data di scadenza del certificato, al Titolare del dispositivo di firma sarà spedito, all'indirizzo di posta elettronica comunicato, un avviso di prossima scadenza.

Il Titolare che intende rinnovare il proprio certificato deve darne comunicazione tempestiva all'Ufficio RA, in modo da garantire la continuità del servizio.

Le procedure per l'ottenimento di un nuovo certificato differiscono dalla prima emissione in quanto non vengono più ripetute le attività di identificazione e di registrazione dei dati del Titolare.

Se il Titolare è provvisto di dispositivo di firma e di un'applicazione in grado di generare la nuova coppia di chiavi e la corrispondente richiesta in formato PKCS#10, è possibile procedere al rinnovo del certificato nella modalità descritta al paragrafo [G.3.2](#).

Nel caso il Titolare non sia provvisto di dispositivo di firma o esso sia inutilizzabile (per esempio: saturazione della memoria), l'Ufficio RA provvederà a far pervenire un nuovo dispositivo contenente il nuovo certificato, utilizzando un canale di comunicazione sicuro.

J.2. Sostituzione delle chiavi del Certificatore

J.2.1. Sostituzione pianificata delle chiavi di certificazione

Almeno 90 (novanta) giorni prima della scadenza del certificato relativo alla coppia di chiavi utilizzate dal sistema di emissione dei certificati, in presenza del *Responsabile del servizio di certificazione* e di responsabili aziendali in numero adeguato e sufficiente a garantire la sicurezza dell'operazione, si procederà all'esecuzione degli eventi sotto descritti, conformi con il DPCM, Artt. 17 e 30.

Sarà eseguita la procedura descritta al paragrafo [G.1](#).

J.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 [N](#).

J.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 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 il certificato corrispondente alla chiave precedentemente in uso.

L'operazione è svolta in presenza del Responsabile del Servizio.

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

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

K. Registro dei certificati

K.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.

K.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.

K.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.

L. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal DLgs 196/03.

M. Procedura di gestione delle 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 K.

- 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.

N. 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.

Va premesso che 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.

O. Procedure per la validazione temporale

O.1. Servizio di validazione temporale

Il TSP INTESA offre un servizio di validazione temporale di documenti informatici.

Data e ora certa sono garantite dalla sincronizzazione con l'ora campione italiana fornita dal servizio NTP di INRIM (vedi cap. P)

O.2. Modalità di richiesta e verifica marche temporali

Il TSP INTESA mette a disposizione dei propri Clienti un'applicazione per la richiesta e la verifica di marche temporali.

Tale applicazione effettua la richiesta di marca temporale con la seguente procedura:

1. Selezione, da parte dell'utente, del documento a cui associare la marca temporale.
2. Generazione dell'impronta da parte dell'applicazione.
3. Invio alla TSA della richiesta di marca temporale con la stessa impronta.

4. Ricezione della risposta da parte della TSA con il risultato della richiesta e, in caso di successo, la marca temporale che viene memorizzata nel file specificato dall'utente.

Mediante la stessa applicazione l'utente può, in qualsiasi momento, visualizzare e verificare le marche temporali ricevute.

Il comando di visualizzazione fornisce le seguenti informazioni relative alla marca temporale contenuta nel file selezionato:

- data ed ora di generazione della marca;
- versione del protocollo di Time Stamping utilizzato dal server che ha generato la marca temporale;
- identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- valore dell'impronta dell'evidenza informatica;
- numero di serie della marca temporale;
- identificativo della policy di sicurezza implementata dalla TSA.

La verifica di una marca temporale richiede l'indicazione del file originale e del file contenente la marca temporale associata.

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.R.I.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.R.I.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.R.I.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).

Q. Modalità operative per l'utilizzo del sistema di verifica delle firma

Come previsto dall'Art.14, comma 1, del DPCM, al fine di effettuare la verifica delle firme digitali, il Certificatore fornisce l'applicazione "**DigitalSign Reader**". Il software è disponibile per il download, assieme alla relativa documentazione, all'indirizzo:

<http://e-trustcom.intesa.it/softwarediverifica.html>

L'utilizzo del software è gratuito.

L'applicazione permette di verificare qualunque archivio informatico firmato e di visualizzarne il contenuto, qualora la stazione di lavoro sia dotata del software adatto a processare quella tipologia d'archivio. A titolo d'esempio, l'applicazione sarà in grado di visualizzare i documenti caratterizzati dall'estensione ".pdf" qualora sia stata preventivamente installata l'applicazione Acrobat Reader.

Per l'utilizzo dell'applicazione non è necessario disporre di alcun dispositivo di firma.

La procedura di verifica della firma digitale apposta ad un documento informatico esegue i seguenti controlli:

1. verifica della struttura della busta PKCS#7;
2. verifica che il certificato del firmatario non sia scaduto;
3. verifica che il certificato del firmatario non sia stato revocato o sospeso;
4. verifica che il certificato del firmatario sia stato emesso da una Autorità di Certificazione inclusa nell'elenco pubblico dei certificatori accreditati;
5. verifica le informazioni presenti nel certificato qualificato, nonché le estensioni obbligatorie (DPCM, Art.14, comma 2b);
6. consente l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori accreditati (DPCM, Art.14, comma 2c);
7. verifica della validità del certificato di certificazione;
8. se presente all'interno del PKCS#7, verifica della marca temporale associata.

Per ulteriori dettagli relativi all'applicazione, si rimanda al manuale utente disponibile sull'applicazione stessa.

R. Modalità operative per la generazione della firma digitale

Il TSP INTESA mette a disposizione dei propri Clienti strumenti per la generazione della firma digitale sia su documenti singoli che in modalità massiva mediante l'utilizzo di procedure automatiche. Tali strumenti sono conformi a quanto previsto dagli Artt. 4 e 11 del DPCM.

R.1. Firma mediante dispositivo di firma individuale

Presso il TSP INTESA è possibile acquistare il prodotto **PKI Smart Kit**. Questa è la soluzione ideale in un kit completo che consente, con facilità d'uso, di eseguire tutte le operazioni relative alla firma digitale: generazione delle chiavi, richiesta di un certificato digitale, sottoscrizione di documento e verifica dello stesso. Grazie a tale tecnologia è possibile apporre la firma digitale a qualunque tipo di documento informatico.

Il package PKI Smart Kit offre una soluzione completa per l'impiego della firma digitale. In particolare, nel kit sono inclusi i seguenti prodotti e servizi:

- Identificazione personale dell'utente
- Un dispositivo di firma (smartcard oppure token USB)
- Un lettore di smartcard da collegare al PC
- Un certificato qualificato per firma digitale
- Il software di firma **DigitalSign (R.1.1)** o **firma4NG (R.1.2)**
- Un CD-ROM contenente:
 - I driver per l'installazione dell'hardware fornito
 - I manuali d'uso.

La smartcard e il relativo lettore sono forniti in alternativa al token USB.

Il kit è facilmente installabile su un personal computer, sul quale deve essere disponibile una porta di connessione USB.

R.1.1. Software di firma e verifica – DigitalSign

DigitalSign è l'applicazione fornita dal per la generazione e la verifica di firme digitali e l'apposizione di marche temporali.

Alla prima attivazione, occorre procedere alla configurazione del dispositivo di firma e aggiornare l'elenco dei certificati di CA con le relative CRL. Queste informazioni vengono reperite dalla lista dei Certificati di certificazione tenuta da AgID.

Attivando la funzione di Firma, è richiesto di selezionare il documento da sottoscrivere e di inserire il dispositivo di firma (smartcard ovvero token USB), se non ancora presente. Il documento selezionato viene visualizzato mediante l'applicazione e viene quindi richiesto di digitare il codice PIN del dispositivo di firma. Finalmente, all'utente è richiesto di salvare il documento firmato (Cades o Pades) e/o marcato temporalmente, se richiesto.

Nel processo di generazione della firma digitale vengono effettuate le seguenti operazioni:

- Verifica che il certificato di sottoscrizione indicato dall'utente non sia scaduto.
- Verifica della corrispondenza tra chiave privata presente sul dispositivo di firma e certificato del Titolare.

L'applicazione *DigitalSign* permette anche l'apposizione di firme multiple allo stesso documento.

Alla firma può associata una marca temporale generata dal servizio di validazione temporale del TSP INTESA, descritto alla sezione [O – Procedure per la validazione temporale](#).

Oltre alla funzioni di generazione di firme, il prodotto offre le seguenti funzionalità:

- Verifica firma: tale funzione è analoga a quella descritta nella sezione Q.
- Cifra: tale funzione permette di cifrare un documento, disponendo di un certificato utilizzabile per la cifratura di dati.
- Decifra: tale funzione permette la decifrazione di dati precedentemente cifrati.

Per ulteriori dettagli relativi all'applicazione *DigitalSign* si rimanda al manuale utente, disponibile nel prodotto stesso.

R.1.2. Software di firma e verifica – firma4ng

Il TSP INTESA distribuisce anche il software di firma e verifica **firma4ng**, un'applicazione professionale di firma digitale, compatibile con i sistemi operativi Windows, Linux e Mac OS X. Permette la firma e la verifica di qualsiasi tipo di documento elettronico.

Per ulteriori dettagli relativi all'applicazione *firma4ng* si rimanda al manuale utente, disponibile nel prodotto stesso

R.2. Firma con procedure automatiche

Il TSP INTESA offre un servizio di generazione automatica delle firme digitali da utilizzare per la gestione di grossi volumi di documenti. In questo caso i certificati di sottoscrizione generati dal Certificatore risiedono, con le rispettive chiavi private, su di un dispositivo di firma di tipo Hardware Security Module (HSM). Tale metodologia garantisce migliori prestazioni e maggiore sicurezza rispetto ad una smartcard o ad un token USB. Il servizio è conforme a quanto stabilito dalla normativa (DPCM, Art.5, comma 2 e 3) e il formato delle firme elettroniche generate è conforme alla normativa vigente.

Alla firma è associata una marca temporale generata dal servizio di validazione temporale, descritto alla sezione [O – Procedure per la validazione temporale](#).

R.3. Firma Digitale Remota

Il TSP INTESA offre un servizio Firma Digitale Remota, generata su HSM, conforme alla normativa vigente. Essa è generata su di un HSM custodito e gestito sotto la responsabilità del Certificatore accreditato ovvero dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi. Il Certificatore è in grado, dato un certificato qualificato, di individuare il dispositivo afferente la corrispondente chiave privata

Conformemente alla normativa vigente, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto alla sezione [O – Procedure per la validazione temporale](#).

R.3.1. Dispositivo di Firma Remota presso Terzi

La Firma Remota può essere generata su HSM custoditi e gestiti dall'Organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'Organizzazione che richiede al TSP di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi (Art.3, comma 4 del DPCM)

In questo caso, il TSP deve essere in grado di:

- individuare agevolmente il dispositivo afferente la corrispondente chiave di un dato certificato;
- mettere in essere quanto previsto dall'Art.3, comma 5, del DPCM.

Nel caso in cui il TSP venga a conoscenza dell'inosservanza di quanto ivi esposto, procede alla revoca dei certificati afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.

R.4. Firma con certificato di validità temporale limitata

Il TSP INTESA offre un servizio Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato a validità temporale limitata (30 minuti dall'emissione o come altrimenti concordato con il cliente / terzo interessato). Essa è generata su di un HSM custodito e gestito sotto la responsabilità del TSP INTESA.

Il Titolare attiva la procedura di firma mediante sistemi di autenticazione consentiti dalla normativa vigente in materia.

Per questa tipologia di certificato, non è prevista la revoca o la sospensione. E' previsto uno specifico limite d'uso, da concordare con il cliente.

Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto alla sezione [O – Procedure per la validazione temporale](#).

R.5. Firma con certificato "one-shot"

Il TSP INTESA offre un servizio Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato "one-shot". Essa è generata su di un HSM custodito e gestito sotto la responsabilità del TSP INTESA. Al termine della procedura di firma, il certificato utilizzato è immediatamente revocato.

Il Titolare attiva la procedura di firma mediante sistemi di autenticazione consentiti dalla normativa vigente in materia.

E' prevista uno specifico limite d'uso, da concordare con il cliente.

Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto alla sezione [O – Procedure per la validazione temporale](#).

R.6. Autenticazione Biometrica

Il servizio fornito dal TSP INTESA prevede che il Titolare di un certificato di firma digitale possa avviare il processo di firma utilizzando una procedura di riconoscimento *biometrico*.

Perché ciò avvenga, nel rispetto della normativa vigente e garantendo la massima sicurezza della procedura, è previsto che, durante l'identificazione del Titolare, queste nuove tecniche siano utilizzate per registrare dati e parametri specifici del Titolare.

Al momento della firma, al posto dei tradizionali PIN e OTP (OneTime Password) solitamente utilizzati in questa tipologia di servizi, al Titolare è richiesto di autenticarsi al servizio utilizzando specifici dispositivi biometrici.

La firma digitale è poi realizzata tramite un sistema di coppie di chiavi asimmetriche, una pubblica e una privata, che consentono al Titolare di rendere manifesta l'autenticità e l'integrità di un documento informatico ad uno o più destinatari che ne possono verificare la validità.

In linea con quanto previsto dall'Art.8 del DPCM, le chiavi di firma sono conservate, su dispositivi HSM.

L'uso esclusivo di tali chiavi, come specificato dall'Art.11, comma 2, del DPCM, è garantito dall'utilizzo del sistema di autenticazione di tipo biometrico.

Per maggiori dettagli, è disponibile un Manuale Operativo dedicato, reperibile all'URL seguente:

http://e-trustcom.intesa.it/ca_pubblica/manuale_operativo_grfmtr.pdf.

R.7. Formato dei documenti

Le applicazioni fornite dal TSP INTESA permettono l'apposizione della firma digitale su tutti i formati di documenti informatici.

È tuttavia importante sottolineare che alcune tipologie di documento informatico sottoscritti con firma digitale non potrebbero comunque ottenere gli effetti descritti nell'Art.21 del CAD, poiché potrebbero contenere macroistruzioni o codice eseguibile tali da attivare funzionalità che possano modificare gli atti o i dati nello stesso rappresentati.

Nell'**ALLEGATO A** del presente manuale è data una breve descrizione relativa alle principali fonti di macroistruzioni o codice eseguibile

ALLEGATO A

Attualmente, i prodotti di Office Automation consentono l'uso di procedure automatizzate all'interno dei documenti prodotti (come ad esempio Macro e /o inserimento di codici di controllo)

A tal proposito, la normativa vigente afferma che l'apposizione della firma digitale su documenti che contengano al loro interno "microistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti previsti per la firma elettronica qualificata.

Oggetti e/o procedure che possono essere presenti all'interno dei documenti sono, a titolo di esempio:

- MACRO: script automatizzati presenti nel documento ed invisibili sul Layout di stampa
- REVISIONI: traccia delle modifiche riportate all'interno del documento
- Script (VBS, JS, ecc.): codici inseriti realizzati tramite linguaggi di alto livello
- Formule e Codici campo, Codici automatici: oggetti specifici che aggiungono funzionalità particolari come ad esempio la numerazione automatica delle pagine
- Oggetti e/o link ad essi: parti di documenti differenti da quello preso in considerazione o link a documenti esterni (ad esempio un grafico MS-Excel all'interno di un documento MS-Word).

Si rimanda ai manuali utente degli specifici prodotti per una descrizione dettagliata e aggiornata su come evidenziare le funzionalità di cui sopra e sul come annullarle.