

LISIT S.p.A.
Manuale Operativo per il Servizio di Certificazione Digitale

Codice documento:	LISIT-CA-PRC#01		
Revisione:	8	Stato:	Emesso
Data di revisione:	25/08/2010		

	NOME	DATA
Redatto da:	Gianluca Gallia	23/08/2010
Approvato da:	Marina Vianello	25/08/2010

INDICE DEI CONTENUTI

1	STORIA DELLE MODIFICHE APPORTATE	4
1.1	DATI IDENTIFICATIVI DELLA VERSIONE DEL MANUALE OPERATIVO.....	4
1.2	REGOLE PER LA PUBBLICAZIONE DEGLI AGGIORNAMENTI AL MANUALE OPERATIVO.....	4
2	INTRODUZIONE	5
2.1	SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO.....	5
2.2	REQUISITI PER LA LETTURA	5
3	ACRONIMI E DEFINIZIONI	6
4	RIFERIMENTI	9
4.1	RIFERIMENTI NORMATIVI.....	9
4.2	STANDARD DI RIFERIMENTO	9
4.2.1	<i>Sistema di qualità del Certificatore</i>	9
5	MODALITÀ GENERALI DEL SERVIZIO	10
5.1	IDENTIFICAZIONE DEL DOCUMENTO.....	10
5.2	IDENTIFICAZIONE DELLA TIPOLOGIA DEI CERTIFICATI EMESSI	10
5.3	RESPONSABILE DEL DOCUMENTO	11
5.4	ENTE CERTIFICATORE.....	11
5.5	ENTE DI REGISTRAZIONE	11
5.6	UTENTI TITOLARI	11
5.7	REGISTRO DEI CERTIFICATI.....	12
5.8	PUBBLICAZIONE ED ARCHIVIAZIONE STORICA DEI DATI DEGLI UTENTI	12
5.8.1	<i>Modalità di protezione della riservatezza</i>	12
5.9	SERVIZIO DI MARCATURA TEMPORALE	12
5.10	TARIFFE.....	13
5.11	ORARI DEL SERVIZIO ED ENTI PREPOSTI	13
5.12	ASSISTENZA.....	13
6	OBBLIGHI	14
6.1	OBBLIGHI DEL CERTIFICATORE	14
6.2	OBBLIGHI DELL'ORGANISMO DI REGISTRAZIONE.....	14
6.3	OBBLIGHI DEGLI UTENTI TITOLARI	15
6.4	OBBLIGHI DEGLI UTENTI UTILIZZATORI	15
7	RESPONSABILITÀ DEL CERTIFICATORE	16
7.1	CONDIZIONI DI FORNITURA DEL SERVIZIO DI CERTIFICAZIONE DIGITALE	16
8	MODALITÀ OPERATIVE	20
8.1	MODALITÀ DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI TITOLARI.....	20
8.1.1	<i>Procedure di adesione al servizio</i>	20
8.1.2	<i>Procedure di identificazione e registrazione dell'Utente Titolare</i>	20
8.2	MODALITÀ DI GENERAZIONE DELLE CHIAVI E EMISSIONE DEI CERTIFICATI.....	21
8.2.1	<i>Generazione delle chiavi di firma e richiesta del certificato</i>	21
8.2.2	<i>Generazione della chiave di cifra e richiesta certificato cifra</i>	22
8.2.3	<i>Verifica delle richieste</i>	22
8.2.4	<i>Generazione dei certificati e loro pubblicazione</i>	22
8.2.5	<i>Personalizzazione del dispositivo di firma (Acquisizione Certificati)</i>	23
8.3	VALIDITÀ DEI CERTIFICATI	23
8.4	TIPOLOGIA E STRUTTURA DEI CERTIFICATI	23
8.5	MODALITÀ DI SOSTITUZIONE DELLE COPPIE DI CHIAVI E DEI CERTIFICATI DELL'UTENTE TITOLARE.....	23
8.6	MODALITÀ DI SOSPENSIONE E REVOCA DEI CERTIFICATI.....	23
8.6.1	<i>Motivi validi per la revoca e per la sospensione dei certificati</i>	24
8.6.2	<i>Procedura di revoca su richiesta del Titolare</i>	24
8.6.3	<i>Procedura di revoca su iniziativa del Terzo interessato</i>	25
8.6.4	<i>Procedura di revoca su iniziativa del Certificatore</i>	25
8.6.5	<i>Procedura di sospensione dei certificati su richiesta del Titolare</i>	25
8.6.6	<i>Sospensione su richiesta del Terzo interessato</i>	26
8.6.7	<i>Sospensione su iniziativa del Certificatore</i>	26
8.6.8	<i>Durata massima della sospensione dei certificati</i>	26
8.6.9	<i>Procedura di annullamento della sospensione</i>	26

8.6.10	Procedura di revoca dopo la sospensione	26
8.7	PROCEDURA DI CERTIFICAZIONE SUCCESSIVA ALLA REVOCA	26
8.8	ARCHIVIAZIONE DELLA CHIAVE PRIVATA DI CIFRA E SUE PROCEDURE DI RECUPERO	26
8.9	REGISTRO DEI CERTIFICATI.....	27
8.9.1	Frequenza delle pubblicazioni.....	27
8.9.2	Procedura di gestione del Registro dei certificati	27
8.9.3	Modalità di accesso al Registro dei certificati.....	27
8.10	MODALITÀ OPERATIVE PER LA GENERAZIONE DELLA FIRMA DIGITALE.....	27
8.10.1	Corretta rappresentazione dei documenti.....	28
8.11	INFORMAZIONI SUI FORMATI DEI DOCUMENTI.....	28
8.11.1	Il formato PDF.....	28
8.11.2	Formati di Microsoft Office	29
8.11.3	Formati per le immagini	29
8.11.4	Generazione della firma digitale	29
8.11.5	Verifica della firma digitale.....	30
8.11.6	Verifica della firma digitale tramite DigitalSign ® – Edizione Lisit	30
8.11.7	Verifica della firma digitale da parte di soggetti che non dispongono di DigitalSign ® – Edizione Lisit	30
9	SERVIZI INTERNI ALLA CA	31
9.1	GENERAZIONE DELLA CHIAVE PRIVATA DELLA CA	31
9.2	GENERAZIONE DEL CERTIFICATO DELLA CA	31
9.3	SOSTITUZIONE DELLA CHIAVE PRIVATA DELLA CA	31
9.4	REVOCA DEL CERTIFICATO DELLA CA.....	31
9.5	TERMINE DELL' ATTIVITÀ DELLA CA	32
9.6	IL GIORNALE DI CONTROLLO.....	32
10	SERVIZIO DI VALIDAZIONE TEMPORALE	33
10.1	GENERAZIONE DELLA CHIAVE PRIVATA DELLA TIME STAMPING AUTHORITY	33
10.2	GENERAZIONE DELLE CHIAVI DI MARCATURA TEMPORALE	33
10.3	ARCHIVIAZIONE DELLE MARCHE TEMPORALI	34
10.4	RIFERIMENTO TEMPORALE	34
10.5	VALIDAZIONE TEMPORALE	34
10.6	MODALITÀ DI EMISSIONE O VERIFICA DI MARCHE TEMPORALI.....	35
10.6.1	Algoritmo di richiesta di marche temporali.....	35
10.6.2	Marche Temporali	35
10.6.3	Validità delle marche temporali	35
10.7	IL SISTEMA DI VALIDAZIONE TEMPORALE.....	35
11	MISURE DI SICUREZZA	37
11.1	PROCEDURE DI GESTIONE DEGLI EVENTI CATASTROFICI	37
12	PROTEZIONE DEI DATI	38
12.1	MODALITÀ DI PROTEZIONE DEI DATI.....	38
12.2	DEFINIZIONE E IDENTIFICAZIONE DI “DATI PERSONALI”	39
12.3	TUTELA E DIRITTI DEGLI INTERESSATI	39
12.4	APPLICAZIONE DEL CODICE PER LA PROTEZIONE DEI DATI PERSONALI	39
12.4.1	Adempimenti generali.....	39
12.4.2	Adempimenti tecnici ed organizzativi	39
12.4.3	Registrazione	40
12.4.4	Elaborazione.....	40
12.4.5	Conservazione.....	40
12.4.6	Cancellazione/Distruzione.....	40
12.4.7	Protezione.....	40
12.5	CIRCOSTANZE DI RILASCIO DI DATI PERSONALI	41

1 STORIA DELLE MODIFICHE APPORTATE

Numero versione	Data di emissione	Sintesi delle variazioni
1.0	14/05/2004	Prima emissione
2.0	14/06/2006	Seconda emissione: adeguamenti richiesti dal DPCM 2004
3.0	31/10/2008	Terza emissione: modificato il par. 5.2 relativo all'identificazione della tipologia dei certificati emessi
4.0	10/02/2009	Quarta emissione: modificato il par. 5.2: corretti i policyOID dei Certificati Qualificati di Firma Digitale, dei Certificati Qualificati di Firma Digitale CRS-SISS e dei Certificati di Autenticazione e Cifra da 1.3.6.1.4.1.7790.8.*.** 1.3.6.1.4.1.7790.1.*.** in quanto errati
5.0	28/08/2009	Quinta emissione: modificato il par. 5.2 relativo all'identificazione della tipologia dei certificati emessi; aggiornati il nr. di fax e l'indirizzo email del certificatore (par. 5.4); inserita deroga, per operatori sanitari aderenti al Progetto CRS-SISS della Regione Lombardia, dell'obbligo di revoca dei certificati digitali per cessazione del servizio (par. 8.6.1); eliminato il riferimento alla Legge n.675 del 31 dicembre 1996
6.0	20/07/2010	Sesta emissione: rivisto l'intero documento per conformità a DPCM 30 Marzo 2009 e Deliberazione CNIPA 45/2009
7.0	03/08/2010	Settima emissione: modificato il par. 9.3 relativo alla sostituzione della chiave privata della CA e il par. 10.6.3 relativo alla validità delle marche temporali
8.0	25/08/2010	Modificato par. 5.2: introdotti nuovi policy OID per i certificati di firma digitale conformi alla Deliberazione CNIPA 45/2009

1.1 Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione 8.0, emessa in data 25/08/2010, del Manuale Operativo per il Servizio di Certificazione Digitale di Lombardia Integrata S.p.A. Servizi Infotelematici per il Territorio (nel seguito: LISIT o Certificatore).

1.2 Regole per la pubblicazione degli aggiornamenti al Manuale Operativo

LISIT si riserva di apportare modifiche al presente Manuale Operativo per esigenze tecniche o modifiche procedurali intervenute durante la gestione del servizio.

Al verificarsi di ogni variazione LISIT ne darà notifica a DigitPA (ex CNIPA) e, previa ratifica della stessa, il manuale modificato verrà pubblicato sul sito di DigitPA e sul sito del Certificatore.

2 INTRODUZIONE

La firma digitale può considerarsi l'equivalente elettronico della tradizionale firma autografa apposta su carta, essa ha ormai assunto piena validità legale come da art. 21 ex D.lgs n°82/2005 e successive modifiche ed integrazioni.

La firma digitale è il risultato di una operazione di crittazione; le tecnologie di crittazione riconosciute sono quelle a chiave asimmetrica basate su una coppia di chiavi, chiave privata e relativa chiave pubblica: la chiave privata deve essere tenuta rigorosamente segreta dal possessore, quella pubblica in quanto tale può essere resa nota. Apporre una firma digitale ad un documento significa compiere una operazione di crittazione dell'impronta del documento con la propria chiave privata (diversa è la cifratura che è il risultato di una operazione di crittazione eseguita con la chiave pubblica del destinatario; la decifratura avviene da parte del destinatario con l'utilizzo della corrispondente chiave privata). Le due chiavi sono infatti complementari, l'operazione di crittazione compiuta con la chiave privata può essere annullata solo ricorrendo alla relativa chiave pubblica e viceversa.

Il certificato digitale è quell'elemento che lega una chiave pubblica ad un insieme di dati anagrafici ed elettronici (tra i quali la stessa chiave pubblica) che identificano il soggetto che possiede ed usa la corrispondente chiave privata.

La veridicità dei dati contenuti nel certificato e l'attendibilità del legame univoco tra una coppia di chiavi ed il suo possessore è garantita dalla Certification Authority (CA), una terza parte fidata che emette il certificato digitale e vi appone la propria firma digitale quale sigillo di affidabilità. L'emissione del certificato dalla competente Autorità di Certificazione avviene previa identificazione sicura del titolare e registrazione dei suoi dati personali.

Il Certificatore inoltre si occupa della gestione dell'intero ciclo di vita dei certificati e della loro pubblicazione così da consentire in ogni momento ad altri soggetti la verifica della validità della firma e dell'integrità e provenienza di uno o più documenti informatici.

L'Autorità di Certificazione di LISIT nell'espletamento del suo ruolo di Certificatore opera in conformità alle regole tecniche in vigore in materia di firma digitale e secondo quanto richiesto per l'accreditamento presso DigitPA.

2.1 Scopo e campo di applicazione del documento

Lo scopo del presente documento è quello di fornire la descrizione delle procedure, delle misure di sicurezza, delle garanzie, degli obblighi e delle responsabilità adottate da LISIT nell'emissione di certificati Qualificati per sottoscrizione. In particolare il presente documento contiene le informazioni richieste e soddisfa i requisiti previsti nelle regole tecniche di attuazione della legge sulla firma digitale per il "Manuale Operativo" del Certificatore accreditato.

Questo documento verrà chiamato d'ora in poi con la sola sigla *Manuale Operativo*, per esso esiste uno standard di riferimento definito dall'IETF "RFC3647" a cui questo documento resta conforme. Il nome per esteso col quale si deve citare questo documento è uno dei seguenti:

Manuale Operativo per il Servizio di Certificazione Digitale;
Certification Practice Statement (CPS) di LISIT Servizio di Certificazione per la firma digitale.

In ottemperanza all'obbligo di informazione (DPCM 30 Marzo 2009, art. 36 e successive modifiche ed integrazioni) è richiesto dalla legge; LISIT come struttura di certificazione digitale, pubblica il presente manuale operativo in modo da permettere ad ogni singolo utente di valutare il grado di affidabilità del servizio offerto.

2.2 Requisiti per la lettura

Per una comprensione piena e corretta del documento, prima di procedere oltre con la lettura, riteniamo essenziale invitare il lettore a prendere visione degli strumenti esplicativi forniti di seguito.

3 ACRONIMI E DEFINIZIONI

Vengono di seguito elencati gli acronimi introdotti nella stesura del presente Manuale Operativo, nonché le definizioni utili alla comprensione di molti termini tecnici in esso utilizzati. Consigliamo la lettura di questa sezione prima di prendere visione dell'intero documento.

Certification Authority (CA)

La CA è un'entità pubblica o privata che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. In particolare la CA LISIT svolge le attività generazione, emissione, conservazione revoca e sospensione dei certificati:

Certificate Revocation List o lista dei certificati revocati (CRL)

Elenco in formato standard ITU-T X.509 dei certificati revocati o sospesi. La CRL è pubblicata nel Registro dei certificati (Directory Service) della CA firmata digitalmente ed è aggiornata dalla CA e asseverata temporalmente.

Certification Practice Statement (CPS) o Manuale Operativo (MO)

La CPS definisce le metodologie utilizzate dalla CA nell'applicazione delle Policy. La CPS può essere utilizzata dall'utente per valutare l'affidabilità delle procedure utilizzate dalla CA per emettere un certificato. La CPS deve essere resa pubblica.

Certificato digitale

Il certificato digitale è un insieme di dati elettronici, firmato dalla CA con la propria chiave privata di certificazione, che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi. Il formato del certificato ed i dati in esso contenuti sono definiti dallo standard ITU-T X.509. Il certificato contiene le informazioni richieste dalla normativa applicabile, e in particolare:

- Numero di serie del certificato
- Informazioni sul Certificatore
- Codice Identificativo del Titolare presso il Certificatore
- Informazioni sul titolare
- Valore della Chiave pubblica del titolare
- Algoritmi di generazione e verifica utilizzabili
- Periodo di validità del certificato
- Algoritmo di sottoscrizione del certificato
- eventuali campi facoltativi denominati estensioni.

La presenza e le caratteristiche di una particolare estensione dipendono dalla tipologia del certificato.

Chiavi asimmetriche

La coppia di chiavi crittografiche, una privata e una pubblica, correlate tra loro, utilizzate nei sistemi di validazione dei documenti informatici.

Chiave privata

L'elemento della coppia di chiavi asimmetriche, destinato ad essere utilizzato soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico.

Chiave e pubblica

L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche.

Codice di Sospensione

Codice segreto attribuito all'utente e utile alla sua identificazione durante la procedura di sospensione dei certificati.

Crittografia

Meccanismo che rende comprensibile l'informazione cifrata solo a chi è autorizzato attraverso l'operazione opposta (decifratura).

Cross-certification

E' il processo attraverso cui le CA si certificano l'una con l'altra. La Cross-certification si esercita tra CA che appartengono a domini diversi. Condizione necessaria affinché possa avvenire la Cross-certification è che le CA accettino le rispettive CPS.

Codice unico presso il Certificatore

Codice utile all'identificazione univoca dell'utente all'interno del dominio del certificatore; questo codice viene generato e consegnato all'utente durante la fase di registrazione, è inoltre contenuto nel Common Name del certificato relativo al titolare.

Directory Service (DS)

Archivio elettronico conforme allo standard ITU-T X.500 dove la CA pubblica i certificati emessi e la lista dei certificati revocati o sospesi. E' un database pubblico che fornisce la possibilità di disporre "on-line", tramite protocollo LDAP, delle informazioni necessarie alla verifica della firma.

Distinguished Name (DN)

Nome univoco secondo lo standard ITU-T X.500.(esempio: c=IT,o=LISIT S.p.A.,cn=Mario Rossi)

Firma Elettronica

L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;

Firma Elettronica Qualificata

La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

Firma Digitale

La firma digitale è un particolare tipo di firma elettronica qualificata basata su una coppia di chiavi asimmetriche, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Funzione di hash

Funzione matematica standard che genera, a partire da una sequenza di simboli binari, un'impronta specifica di tale sequenza in modo tale che risulti di fatto impossibile, a partire da questa, determinare la sequenza di simboli binari da cui è stata generata.

HSM

Hardware Security Module nota anche come crypto machine. Dispositivo hardware di firma veloce.

IETF - Internet Engineering Task Force

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori, e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet. E' aperta a chiunque sia interessato.

Impronta

Sequenza di simboli binari, di lunghezza predefinita, generata mediante l'applicazione di una opportuna funzione di hash al documento che si vuole sottoscrivere digitalmente.

ISO – International Organization for Standardization

Abbreviazione di "International Organization for Standardization" (Associazione Internazionale per la Standardizzazione). Non è che l'ISO non sia un acronimo; al contrario, il nome deriva dalla parola greca iso, che significa uguale. Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione provenienti da più di 75 paesi. Ad esempio, l'ANSI (American National Standards Institute) è un membro ISO. L'ISO ha definito numerosi ed importanti standard per i computer. Di questi, il più significativo è forse l'OSI (Open Systems Interconnection), un'architettura standard per progettare le reti.

ITU – International Telecommunication Union

Acronimo di International Telecommunication Union (Unione Internazionale per le Telecomunicazioni), un organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni. In precedenza, le attività di standardizzazione venivano effettuate da un gruppo interno all'ITU chiamato CCITT, ma dopo la riorganizzazione del 1992 il CCITT come corpo separato non esiste più.

Key Archive Server

Data base contenente le chiavi di cifra dei Titolari.

Key Recovery Server

Servizio di gestione e recupero delle chiavi di cifra dei Titolari.

LDAP – Lightweight Directory Access Protocol

Protocollo utilizzato per accedere alla directory contenente i certificati ed effettuare tutte le operazioni di prelievo certificato, verifica CRL eccetera.

OID – Object Identifier

Valore numerico univoco che identifica un oggetto nell'ambito della gerarchia ITU-T X.500.

PIN

Personal Identification Number, codice associato ad un dispositivo di firma (Smart Card o altro supporto), utilizzato dall'utente per accedere alle sue funzioni.

PdR

I Punti di Registrazione sono Registration Authority Locali preposte alle operazioni di identificazione e di registrazione alla CA degli utenti, di emissione dei dispositivi sicuri di firma e di revoca/sospensione/annullamento sospensione dei certificati digitali.

PKCS – Public Key Cryptography Standard

Serie di specifiche crittografiche sviluppate dalla RSA Data Security Inc.

PKI

PKI è acronimo per Public Key Infrastructure ossia una infrastruttura che fornisce servizi di certificazione e crittografici. Una PKI è formata da CA (legate tra loro da un modello gerarchico o di cross-certification), RA, prodotti software (applicazioni, database) ed hardware che consentono ad applicazioni esterne di usufruire dei servizi della PKI.

Policy

Un insieme di regole che indica l'applicabilità di un certificato ad una particolare comunità e/o classe di applicazioni con comuni necessità di sicurezza.

Puk

Pin Unblocking Key, codice per lo sblocco e la ridefinizione dei PIN.

Registration Authority (RA)

La RA è un'entità pubblica o privata che esegue la procedura di registrazione, durante la quale viene eseguita la validazione e l'autenticazione di tutti i

dati che fornisce l'utente, l'identificazione fisica degli utenti basata su documenti a valore legale.

Revoca/Sospensione di un certificato

Sono le operazioni con cui la CA annulla/sospende la validità del certificato prima della naturale scadenza. Vengono registrate sulla Certificate Revocation List (CRL).

RFC – Request For Comments

Sigla con la quale si indicano gli standard di Internet emanati dall'IETF.

RSA (Rivest-Shamir-Adleman algorithm)

Algoritmo per la generazione e verifica delle firme digitali alla base della crittografia a coppia di chiavi asimmetriche.

Serial Number

Numero intero attribuito dalla CA per identificare in modo univoco un certificato o una CRL all'interno del proprio dominio.

Terzo interessato

Il terzo interessato è rappresentato da persona fisica o Pubblica Amministrazione il cui consenso è necessario per specificare la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite dal richiedente l'emissione del certificato digitale, ai sensi dell'art. 29 bis del DPR 445/2000 e successive modificazioni e integrazioni. Il terzo interessato può richiedere la revoca o la sospensione dei certificati digitali di un utente titolare, supportandola con adeguata documentazione giustificativa.

TSA

Time Stamping Authority. Certification Authority preposta all'emissione di certificati per il Time Stamping Service (TSS).

TSS

Time Stamping Service. Servizio di emissione di marche temporali con valore legale.

URL –Uniform Resource Locator

Modalità semantica per indirizzare un oggetto su INTERNET. (esempio: <http://www.lisit.it/ca>).

Utente titolare

L'utente titolare di un certificato è una persona fisica o giuridica che richiede al Certificatore la certificazione di una chiave pubblica.

Utente utilizzatore

L'utente utilizzatore è una persona fisica o giuridica che accede alla directory pubblica del Certificatore per consultare e verificare certificati digitali e CRL.

Validazione Temporale

La validazione temporale è il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

X.509 e X.509 v3

Raccomandazioni ITU-T che definiscono la struttura e la semantica dei certificati e della CRL; X.509 è equivalente allo standard ISO 9594-8. La terza edizione (1997) dello standard X.509, che permette l'uso di estensioni, è denominata X.509 v3.

4 RIFERIMENTI

4.1 Riferimenti normativi

D.Lgs n.196 del 30 giugno 2003	“Codice in materia di protezione dei dati personali”.
D.lgs n° 82/2005 [CAD] 7 marzo 2005	Codice dell’amministrazione digitale
Circolare n° 48 del 6 settembre 2005	Circolare n. 48 del 13 settembre 2005 ”Modalità per presentare domanda di iscrizione nell’elenco pubblico dei certificatori di cui all’articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n° 445”
D. lgs 159/2006 Del 4 aprile 2006	Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n° 82 recante codice dell’amministrazione digitale
DPCM 30 marzo 2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
Deliberazione CNIPA n. 45 del 21/05/2009	Regole per il riconoscimento e la verifica del documento informatico

I riferimenti si intendono a tutte le fonti normative sopra elencate, anche successivamente modificate, e ad ulteriori disposizioni normative e regolamentari non ancora emanate, ma comunque pertinenti per competenza.

4.2 Standard di riferimento

I certificati descritti nel presente documento sono conformi agli standard di riferimento internazionali (X509), agli standard individuati dalla normativa italiana in materia di Firma Digitale ed agli standard dalla Commissione Europea.

Per quanto concerne i dispositivi di firma si indica il “CWA 14169 (March 2002): Secure Signature-Creation Devices ‘EAL 4+’” che definisce i requisiti ai quali deve aderire un dispositivo sicuro di firma per l’utilizzo nella firma digitale.

4.2.1 Sistema di qualità del Certificatore

Il sistema di qualità del Certificatore è conforme alla norma UNI EN ISO 9001:2008 con certificato CERT-13614-2003-AQ-MIL-SINCERT emesso da Det Norske Veritas il 23/12/2003. Il Sistema di Gestione della Sicurezza dell’informazione è conforme alla la norma ISO/IEC 27001:2005 con certificato CERT-012-2005-AIS-MIL-SINCERT emesso da Det Norske Veritas il 16/05/2005

5 MODALITÀ GENERALI DEL SERVIZIO

In questo capitolo vengono fornite informazioni utili all'identificazione del documento, dell'Ente Certificatore e dei vari attori coinvolti nella sua Infrastruttura a Chiave Pubblica (PKI), nonché le modalità generali seguite da LISIT nell'espletamento del ruolo di Certificatore.

5.1 Identificazione del documento

Questo documento è pubblicato e liberamente scaricabile in formato PDF dal sito del Certificatore, al seguente indirizzo (URL):

<http://www.lisit.it/firmadigitale>

Del documento pubblicato a questo indirizzo viene garantita l'integrità e l'autenticità.

L'URL dove questo documento è pubblicato e l'OID che lo identifica, è reperibile nell'estensione standard dei certificati che fanno riferimento alla CPS descritta in questo documento.

Il presente documento è depositato presso DigitPA e consegnato, su richiesta, al richiedente il certificato presso gli sportelli dell'Ente di Registrazione al momento della registrazione.

Sul sito del certificatore sono riportate altre informazioni di dettaglio del servizio di certificazione.

5.2 Identificazione della tipologia dei certificati emessi

Le policy del Certificatore LISIT sono descritte in appositi documenti pubblicati sul sito del servizio di Firma Digitale <http://www.lisit.it/firmadigitale/documentazione/index.php> e sono identificate dagli OID presenti nell'attributo policy identifier dell'estensione certificatePolicy (OID 2.5.29.32) riportati di seguito:

- | | |
|---|-------------------------|
| - Certificati Qualificati di Firma Digitale CRS-SISS ¹ | 1.3.6.1.4.1.7790.1.2.11 |
| - Certificati Qualificati di Firma Digitale ² | 1.3.6.1.4.1.7790.1.2.12 |
| - Certificati Qualificati di Firma Digitale CRS-SISS 2 ³ | 1.3.6.1.4.1.7790.1.2.13 |
| - Certificati Qualificati di Firma Digitale 2 ⁴ | 1.3.6.1.4.1.7790.1.2.14 |
| - Certificati di Marcatura Temporale | 1.3.6.1.4.1.7790.4.2 |

Le policy sono parte integrante del Manuale Operativo e delle condizioni contrattuali del servizio.

Il policy OID 1.3.6.1.4.1.7790.1.2.10 presente nei Certificati Qualificati di Firma Digitale fa riferimento al presente Manuale Operativo.

La Certification Authority LISIT è registrata presso IANA (www.iana.org) come sotto riportato:

1.3.6.1.4.1.7790 - LISIT Certification Authority Submitted by from host (213.140.9.174) on Wed Jun 4 11:44:10 CEST 2003 using a WWW entry form.

OID value: 1.3.6.1.4.1.7790.

¹ Conforme alla Deliberazione CNIPA n. 4/2005

² Conforme alla Deliberazione CNIPA n. 4/2005

³ Conforme alla Deliberazione CNIPA n. 45/2009

⁴ Conforme alla Deliberazione CNIPA n. 45/2009

5.3 Responsabile del documento

Il responsabile del presente documento è Gianluca Gallia contattabile tramite:

e-mail:	gianluca.gallia@lispa.it
Telefono:	+39 02-39331.1
Fax:	+39 02-93660225

5.4 Ente Certificatore

Il servizio di certificazione digitale è erogato dalla seguente organizzazione:

Denominazione sociale:	LOMBARDIA INTEGRATA S.p.A. SERVIZI INFOTELEMATICI PER IL TERRITORIO
Indirizzo della sede legale:	via Don Minzoni, 24 20158 Milano
Rappresentante legale:	Giovanni Catanzaro
N° di partita IVA:	12922020156
N° di telefono:	+39 02-39331.1
N° di fax	+39 02-93660225
ISO Object Identifier (OID):	1.3.6.1.4.1.7790
e-mail:	ca@lisit.it
PEC:	ca@pec.lisit.it

5.5 Ente di Registrazione

L'Ente di Registrazione o Registration Authority (RA) è l'organismo che nell'ambito di un'Autorità di Certificazione è preposto a gestire il rapporto ed il contatto con l'utente titolare del certificato digitale ed a espletare le preliminari procedure di identificazione e registrazione dello stesso verificando la sua abilitazione a proseguire nel processo di certificazione.

LISIT per il servizio di registrazione si avvale di una RA interna e dei Punti di Registrazione (PdR) distribuiti sul territorio presso le sedi di riferimento delle Strutture Clienti del Certificatore; questi rispondono per le attività svolte a LISIT e ne condividono le regole di erogazione e gestione del servizio.

LISIT si dichiara responsabile verso terzi delle attività svolte dai suddetti Punti di Registrazione.

Oltre alle attività di identificazione e registrazione, presso la RA è possibile effettuare le operazioni di:

- personalizzazione del dispositivo di firma;
- richiesta di revoca dei certificati;
- richiesta di sospensione e annullamento della sospensione dei certificati.

Questi compiti sono svolti dal personale di PdR tramite il Portale del Certificatore. L'accesso al Portale avviene in seguito ad autenticazione con dispositivo di firma; tutte le operazioni del PdR sopra riportate sono firmate dall'Addetto PdR.

5.6 Utenti Titolari

I clienti del Certificatore LISIT sono persone fisiche, Pubbliche Amministrazioni o enti privati che si rivolgono ad esso per ottenere certificati per persone fisiche a loro afferenti.

Questi soggetti hanno il compito di svolgere le procedure finalizzate alla gestione degli stessi, essendo di fatto i titolari dei certificati.

Agli utenti vengono erogate due coppie di chiavi, con i relativi certificati, l'una per le operazioni di firma digitale, l'altra per le operazioni di cifra e autenticazione.

Chiavi e certificati dell'utente vengono memorizzati su un dispositivo che viene definito, dalla normativa sulla firma digitale, dispositivo sicuro di firma.

5.7 Registro dei certificati

La lista dei certificati revocati e sospesi sono pubblicati sul registro dei certificati.

Il registro dei certificati di LISIT è mantenuto su un archivio elettronico (Directory Service X.500), accessibile in sola lettura a tutta l'utenza mediante protocollo LDAP, la possibilità di modificarne il contenuto è riservata a personale autorizzato e competente.

L'indirizzo del Directory Server sul quale LISIT pubblica le CRL è: ldap.crs.lombardia.it.

5.8 Pubblicazione ed archiviazione storica dei dati degli utenti

Durante le procedure di identificazione e registrazione, l'Autorità di Certificazione entra in possesso di informazioni riguardanti l'utente richiedente i certificati.

Queste informazioni sono quelle che secondo la normativa debbono contenere i certificati. Queste informazioni saranno pubblicate dalla CA nel certificato dell'utente.

I dati depositati presso il Punto di Registrazione e raccolti su supporto cartaceo, o altri strumenti equivalenti, (nella stessa fase di registrazione o in altre successive) sono conservati in contenitori muniti di serratura di sicurezza, situati in locali protetti per un periodo di 20 anni a partire dalla data di emissione dei certificati.

Il trattamento dei dati avviene nel rispetto delle misure di sicurezza emanate ai sensi dell'art. 33, del D.Lgs. del 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e sue successive modifiche e integrazioni.

5.8.1 Modalità di protezione della riservatezza

Tutti i dati che risiedono sui database del Certificatore sono protetti da strumenti che implementano politiche di autorizzazione per l'accesso ai dati legati a meccanismi di autenticazione degli utenti.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali emanate con Decreto Legislativo 196 del 2003 allegato B (disciplinare tecnico in materia di misure minime di sicurezza), per l'esecuzione delle seguenti attività:

- individuazione degli incaricati;
- assegnazione dei codici identificativi;
- protezione degli elaboratori;
- modalità di designazione degli incaricati del trattamento.

5.9 Servizio di Marcatura Temporale

Oltre al servizio di Certification Authority, il Certificatore LISIT dispone del servizio di Validazione Temporale. Questo servizio permette di attribuire ad uno o più documenti informatici un riferimento temporale opponibile a terzi mediante la generazione di una marca temporale costituita da una data ed ora certe.

Ciascuna marca temporale apposta ad un documento informatico è indissolubilmente legata ad esso con riferimenti certi come impronta del documento, numero seriale della marca ed identificativo della CA di Marcatura Temporale. Con la marca temporale associata ad un documento un utente titolare può dimostrare l'esistenza del documento e darne validità legale con l'operazione di sottoscrizione.

I dettagli del servizio di marcatura temporale sono riportati sul sito del Certificatore.

5.10 Tariffe

Le tariffe applicate dal Certificatore LISIT sono pubblicate e aggiornate sul sito web del Certificatore, all'indirizzo www.lisit.it/firmadigitale.

5.11 Orari del Servizio ed Enti preposti

La tabella che segue riporta gli orari dei servizi di registrazione degli utenti e gestione dei certificati digitali svolti dalla Registration Authority di LISIT.

SERVIZIO	ENTE	GIORNI ED ORARIO
Registrazione alla CA	RA di Lisit	○ Dal lunedì al venerdì dalle 9 alle 17.30
Sospensione dei certificati	○ RA di Lisit, ○ numero verde Help Desk del Certificatore ○ Portale del Certificatore	○ La Registration Authority è attiva dal lunedì al venerdì dalle 9 alle 17.30. ○ L'Help Desk è contattabile h24, 7 giorni su 7 ○ Il portale è disponibile h24, 7 giorni su 7
Annullamento Sospensione	RA di Lisit	○ La Registration Authority è attiva dal lunedì al venerdì dalle 9 alle 17.30.
Revoca dei certificati	RA di Lisit	○ Dal lunedì al venerdì dalle 9 alle 17.30

Analogamente gli orari degli stessi servizi presso i Punti di Registrazione (PdR) distribuiti sul territorio, saranno disponibili presso i PdR stessi.

5.12 Assistenza

Per ogni problematica legata al servizio ed alle procedure descritte in questo documento e per ottenere informazioni, è a disposizione dell'utente un servizio di Help Desk attivo dal lunedì al sabato dalle ore 8,00 alle ore 20,00.

6 OBBLIGHI

Questa sezione tratta degli obblighi di LISIT nell'esercizio delle funzioni di CA ed RA, degli utenti titolari e degli utenti utilizzatori dei certificati.

6.1 Obblighi del Certificatore

Nello svolgimento della propria attività di Certificatore, LISIT dichiara di rimanere conforme a quanto richiesto dalla normativa vigente:

- attenersi alle regole tecniche definite nel DPCM 30 Marzo 2009 e successive modifiche e integrazioni;
- identificare con certezza la persona che fa richiesta della certificazione;
- accertare la corrispondenza univoca fra chiave pubblica e utente titolare;
- verificare che la chiave pubblica che si deve certificare non sia già stata certificata nel proprio dominio, né da uno dei Certificatori iscritti nell'Elenco pubblico quando gli accordi di interoperabilità lo consentiranno;
- emettere il certificato e notificare la sua emissione al richiedente;
- specificare nel certificato, su richiesta dell'istante e con il consenso del terzo interessato, la sussistenza di poteri di rappresentanza o altri titoli relativi all'attività professionale o alle cariche rivestite, previa verifica della sussistenza degli stessi;
- non rendersi depositario di dati per la creazione della firma del titolare;
- procedere tempestivamente alla revoca/sospensione dei certificati dell'utente in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, 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;
- notificare all'utente titolare la revoca o la sospensione dei certificati nel caso queste avvengano su iniziativa del Certificatore o su richiesta del terzo interessato;
- aggiornare tempestivamente la CRL in caso di revoca/sospensione di un certificato;
- garantire l'interoperabilità del prodotto di verifica come definito nell'art. 38 del DPCM 30 Marzo 2009 e successive modifiche e integrazioni ai documenti informatici sottoscritti con firma;
- mantenere e rendere accessibile per via telematica copia della lista sottoscritta dal dipartimento, dei certificati relativi alle chiavi di certificazione di cui all'art. 39 del DPCM 30 Marzo 2009 e successive modifiche e integrazioni;
- dare comunicazione agli utenti e a DigitPA, con un preavviso di almeno sessanta (60) giorni, in caso di cessazione della propria attività;
- proteggere le proprie chiavi private con i necessari criteri di sicurezza;
- rispettare le misure minime di sicurezza previste per il trattamento dei dati personali D.lgs 196 del 2003 allegato B (disciplinare tecnico in materia di misure minime di sicurezza).

6.2 Obblighi dell'Organismo di Registrazione

Gli obblighi dell'Organismo di Registrazione sono i seguenti:

- incaricare gli Addetti PdR mediante Lettera di Incarico, con cui viene garantito al Certificatore LISIT che le persone incaricate sono idonee a svolgere il compito loro assegnato nonché il rispetto da parte degli incaricati delle procedure previste dal Manuale Operativo della CA LISIT, ferma restando la responsabilità del certificatore stesso;
- fornire la formazione e le istruzioni operative a cui gli incaricati devono attenersi per il trattamento dei dati personali;
- comunicare a LISIT la revoca dell'incarico agli Addetti PdR;
- effettuare la revoca e la sospensione dei certificati da parte del Terzo Interessato in caso di mancato rispetto, da parte dell'Utente Titolare, delle condizioni di utilizzo previste dal Manuale Operativo della CA LISIT;
- conservare la documentazione utente raccolta dagli Addetti PdR per 20 anni. L'Organismo di Registrazione deve garantire che tale documentazione venga archiviata in armadi ignifughi e blindati o con sistemi di archiviazione che garantiscano un livello di sicurezza non inferiore a quello dell'armadio ignifugo e durata nel tempo.

Gli Obblighi dell'Addetto PdR sono i seguenti:

- verificare con certezza l'identità del richiedente i certificati e registrare i dati dello stesso;
- far firmare la richiesta cartacea di registrazione al servizio di certificazione ;
- archiviare le richieste cartacee di registrazione per almeno 20 anni;
- comunicare alla CA tutti i dati acquisiti durante la registrazione;
- informare il richiedente la registrazione riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle chiavi private, al trattamento dei dati personali ed al rispetto delle normative contenute nel presente manuale;
- consegnare al richiedente i codici identificativi personali generati durante la procedura di registrazione ;
- verificare e inoltrare alla CA le richieste di revoca, di sospensione o di annullamento della sospensione attivate presso il punto di registrazione dal titolare;
- rispettare le misure minime di sicurezza previste per il trattamento dei dati personali D.lgs 196 del 2003 allegato B (disciplinare tecnico in materia di misure minime di sicurezza);
- rispettare le necessarie procedure di sicurezza nell'esercizio delle sue funzioni.

6.3 Obblighi degli Utenti Titolari

Gli utenti titolari della PKI LISIT hanno i seguenti obblighi:

- consultare preventivamente il Manuale Operativo ;
- comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione al servizio di certificazione;
- comunicare al Certificatore eventuali variazioni dei dati dichiarati al momento della registrazione;
- conservare con la massima diligenza i codici riservati ricevuti durante la fase di registrazione per evitare la conoscenza di questi da parte di altri soggetti;
- custodire in modo diligente le proprie chiavi private e il dispositivo sul quale sono state archiviate, al fine di garantire la massima riservatezza delle prime e l'integrità dello stesso dispositivo di archiviazione;
- provvedere a cambiare i PIN provvisori del proprio dispositivo di firma per realizzare un ulteriore livello di sicurezza;
- conservare i PIN in luogo diverso da quello in cui è conservato il dispositivo contenente le chiavi;
- richiedere tempestivamente la revoca dei certificati al verificarsi delle condizioni enunciate nel paragrafo "Motivi per la revoca e per la sospensione dei certificati";
- richiedere la sospensione dei certificati nei casi e con le modalità previste dal paragrafo "Procedura di sospensione dei certificati";
- utilizzare le chiavi private personali ed il corrispondente certificato nel pieno rispetto delle funzioni previste dalla sua tipologia e secondo le modalità enunciate nel presente Manuale Operativo.

6.4 Obblighi degli Utenti Utilizzatori

Gli utenti utilizzatori che intendono verificare la firma digitale apposta ai documenti sottoscritti con chiavi emesse dal Certificatore LISIT hanno l'obbligo di verificare la validità dei relativi certificati attenendosi alle modalità descritte in questo documento al par. "Modalità operative per la generazione della firma digitale".

Con il riferimento al art. 36, comma 3, lett. D del DPCM 30 Marzo 2009 chiunque intende accedere al registro dei certificati per verificare una firma digitale è tenuto a:

- attenersi alle modalità indicate dal Certificatore per l'operazione di verifica firma;
- verificare attentamente il contenuto del certificato relativo alla chiave pubblica;
- avvalersi di mezzi tecnici idonei a consentire la corretta consultazione del registro dei certificati;
- verificare ed utilizzare i certificati e le relative informazioni solo per le finalità in relazione alle quali i certificati sono rilasciati.

E' inoltre vietato a chiunque utilizzare i certificati emessi dal Certificatore LISIT per fini differenti da quelli previsti dal presente Manuale Operativo e dalla vigente normativa (art. 15, comma 2 e art. 30, comma 3 del DPCM 30 Marzo 2009).

E' allo stesso modo vietato a chiunque di accedere al registro dei certificati per finalità differenti dalla sua consultazione, pena le sanzioni previste dalle leggi vigenti.

7 RESPONSABILITÀ DEL CERTIFICATORE

Il Certificatore è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dalla Direttiva 1999/93/CE, dal DPCM 30 Marzo 2009 e successive modifiche ed integrazioni, dalle regole tecniche previste e dalla Legge sulla tutela della privacy.

Il Certificatore è altresì responsabile nei confronti di qualunque soggetto faccia ragionevolmente affidamento sui certificati emessi dallo stesso, nei limiti della normativa applicabile. L'esistenza e la validità del certificato non dispensano tuttavia l'utente dall'eseguire ogni altra verifica che appaia opportuna secondo i criteri di oculata prudenza, anche in relazione al rilievo, economico o d'altra natura, degli interessi coinvolti.

Il Certificatore non sarà responsabile per danni di qualsiasi natura, diretti o indiretti, da chiunque patiti nella misura in cui tali danni derivino dalla violazione di obblighi che, in virtù di quanto previsto dal presente Manuale Operativo ovvero dalle vigenti disposizioni di legge, incombono al titolare, al terzo interessato e/o a quanti accedono al registro dei certificati per la verifica della firma, ovvero dallo svolgimento di attività illecite.

Il Certificatore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

Il Certificatore non assume alcun obbligo, garanzia e responsabilità ulteriori rispetto a quelle previste dal presente Manuale o dalle vigenti disposizioni normative.

Ogni responsabilità è comunque esclusa laddove il Certificatore provi di aver agito senza colpa, ed in ogni caso in cui la responsabilità è esclusa da quanto previsto dall'art. 30 del D.lgs n°82/2005 (CAD) e successive modifiche ed integrazioni.

A copertura dei rischi connessi all'attività di certificazione e dei danni causati a terzi, il Certificatore ha stipulato un contratto assicurativo secondo le seguenti modalità:

€ 258.228,00 (Lit. 500.000.000) per singolo sinistro

€ 1.549.000,00 (Lit. 3.000.000.000) per annualità assicurativa.

7.1 Condizioni di Fornitura del Servizio di Certificazione Digitale

Premesso che:

Il rilascio al pubblico di certificati qualificati è regolata da un'apposita normativa e da regole tecniche emanate dal DigitPA (ex CNIPA);

Tutto quanto ciò premesso, si riportano le seguenti CONDIZIONI di Fornitura del Servizio (CONDIZIONI).

Articolo 1 Soggetti del SERVIZIO

Nell'ambito del SERVIZIO si identificano i soggetti di seguito indicati:

- CERTIFICATORE: Lombardia Integrata S.p.A (LISIT S.P.A.), che opera in qualità di Certificatore Accreditato iscritto nell'Elenco Pubblico di DigitPA;
- TITOLARE: la persona fisica che richiede al CERTIFICATORE la certificazione di una chiave pubblica; cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
- TERZO INTERESSATO: Il terzo interessato è rappresentato da persona fisica o Pubblica Amministrazione il cui consenso è necessario per specificare la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite dal TITOLARE che richiede l'emissione del certificato digitale.

Articolo 2 Acronimi e definizioni

Certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime

- Punto di Registrazione (PdR): ufficio preposto alle operazioni di identificazione e di registrazione dei TITOLARI, di emissione dei dispositivi sicuri di firma e di revoca, sospensione, annullamento sospensione dei certificati digitali dei TITOLARI;

- Certificate Revocation List (CRL): elenco in formato standard ITU-T X.509 dei certificati revocati o sospesi. La CRL è pubblicata nel Registro dei certificati (Directory Service) del CERTIFICATORE;
- Registro dei Certificati o Directory Service (DS): archivio elettronico conforme allo standard ITU-T X.500 dove il CERTIFICATORE pubblica i certificati emessi e la lista dei certificati revocati o sospesi. E' un servizio pubblico che fornisce la possibilità di disporre "on-line", tramite protocollo ldap, delle informazioni necessarie alla verifica della firma;
- Certification Practice Statement (CPS) o Manuale Operativo (MO): definisce le metodologie utilizzate dal CERTIFICATORE nell'applicazione delle policy. La CPS può essere utilizzata dai TITOLARI e dagli UTENTI UTILIZZATORI per valutare l'affidabilità delle procedure utilizzate dal CERTIFICATORE per emettere i certificati digitali. La CPS deve essere resa pubblica;
- Certificato Digitale: il certificato digitale è un insieme di dati elettronici che collegano i dati utilizzati per verificare le firme elettroniche all'identità del TITOLARE;
- Certificato Qualificato: il certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
- Chiavi Asimmetriche: la coppia di chiavi crittografiche, una privata e una pubblica, correlate tra loro, utilizzate nei sistemi di validazione dei documenti informatici;
- Chiave Privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal TITOLARE, mediante il quale si appone la firma digitale sul documento informatico;
- Chiave Pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal TITOLARE delle chiavi asimmetriche;
- Codice di Sospensione: codice segreto attribuito al TITOLARE utile alla sua identificazione durante la procedura di sospensione telefonica dei certificati digitali;
- Firma Elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
- Firma Elettronica Qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;
- Firma Digitale: la firma digitale è un particolare tipo di firma elettronica qualificata basata su una coppia di chiavi asimmetriche, una pubblica e una privata, che consente al TITOLARE tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Articolo 3 Obblighi del CERTIFICATORE

A norma dall'art.32 del D.lgs. n. 82/2005 (Codice dell'amministrazione digitale) e successive modifiche ed integrazioni, il CERTIFICATORE fornirà il SERVIZIO conformemente a quanto stabilito dalla normativa vigente in materia, con le modalità indicate nel Manuale Operativo e secondo le presenti CONDIZIONI. In particolare, il CERTIFICATORE nello svolgimento della propria attività assume i seguenti obblighi:

- attenersi alle regole tecniche definite nel DPCM 30 Marzo 2009 e successive modifiche e integrazioni;
- identificare con certezza il TITOLARE che fa richiesta di certificazione;
- accertare la corrispondenza univoca fra chiave pubblica e TITOLARE;
- verificare che la chiave pubblica che si deve certificare non sia già stata certificata nel proprio dominio, né da uno dei Certificatori iscritti nell'Elenco Pubblico quando gli accordi di interoperabilità lo consentiranno;
- emettere il certificato digitale e notificare la sua emissione al TITOLARE;
- specificare nel certificato digitale, su richiesta del TITOLARE e con il consenso del TERZO INTERESSATO, la sussistenza di poteri di rappresentanza o altri titoli relativi all'attività professionale o alle cariche rivestite, previa verifica della sussistenza degli stessi;
- non rendersi depositario di dati per la creazione della firma del TITOLARE;
- procedere tempestivamente alla revoca/sospensione dei certificati digitali del TITOLARE in caso di richiesta da parte del TITOLARE stesso o del TERZO INTERESSATO dal quale derivino i poteri di quest'ultimo, 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;
- notificare al TITOLARE la revoca o la sospensione dei certificati digitali nel caso queste avvengano su iniziativa del CERTIFICATORE o su richiesta del TERZO INTERESSATO;
- aggiornare tempestivamente la CRL in caso di revoca/sospensione di un certificato digitale;

- garantire l'interoperabilità del prodotto di verifica delle firme digitali come definito nell'art. 38 del DPCM 30 Marzo 2009 e successive modifiche e integrazioni e nel D.lgs. n. 82/2005 e successive modifiche ed integrazioni;
- mantenere e rendere accessibile per via telematica copia della lista sottoscritta da DigitPA, dei certificati relativi alle chiavi di certificazione di cui all'art. 39 del DPCM 2009 e successive modifiche e integrazioni;
- dare comunicazione ai TITOLARI ed a DigitPA, con un preavviso di almeno sessanta (60) giorni, in caso di cessazione della propria attività;
- proteggere le proprie chiavi private di certificazione con i necessari criteri di sicurezza;
- rispettare le misure minime di sicurezza previste per il trattamento dei dati personali D.lgs n. 196/2003 allegato B (disciplinare tecnico in materia di misure minime di sicurezza).

Il CERTIFICATORE si riserva il diritto di modificare le specifiche tecniche di erogazione del SERVIZIO in base all'evoluzione tecnologica e/o normativa, rendendole note attraverso la pubblicazione del Manuale Operativo. Ove tali modifiche risultassero essere di rilevante entità, ne verrà data informazione al Titolare, che ha la facoltà di recedere dal presente contratto.

Articolo 4 Esclusioni

Il CERTIFICATORE non sarà in alcun modo responsabile per quanto di seguito indicato:

- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti per eventi derivanti da atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile al CERTIFICATORE (quali, in via puramente esemplificativa e non esaustiva, mancato o erroneo funzionamento di reti, apparecchiature o strumenti di carattere tecnico al di fuori della sfera di controllo del CERTIFICATORE, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi), esclusi i casi di dolo o colpa grave;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti nella misura in cui tali danni derivino dalla violazione di obblighi che, in virtù di quanto previsto dal Manuale Operativo del CERTIFICATORE ovvero dalle vigenti disposizioni di legge, incombono sul TITOLARE o sull'UTENTE UTILIZZATORE, a quanti intendono verificare la firma digitale apposta ai documenti sottoscritti con chiavi emesse dal CERTIFICATORE;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti dall'erroneo utilizzo di codici identificativi (userid e password) da parte del TITOLARE;
- danni di qualsiasi natura, diretti od indiretti, o pregiudizi da chiunque patiti derivanti da ritardi, interruzioni, errori o malfunzionamenti del SERVIZIO non imputabili al CERTIFICATORE o derivanti dall'errata utilizzazione del SERVIZIO da parte del TITOLARE.

Il CERTIFICATORE non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelle scaturenti dalle presenti CONDIZIONI, da quelle espresse nel Manuale Operativo e dalla normativa vigente.

Articolo 5 Obblighi del TITOLARE

A norma dell'art.32 del D.lgs. n. 82/2005 (Codice dell'amministrazione digitale), con l'accettazione di quanto stabilito in queste CONDIZIONI di Fornitura il TITOLARE assume gli obblighi seguenti:

- conservare e custodire con la massima diligenza la sua smart card, al fine di garantire l'integrità e la riservatezza delle chiavi private in essa contenute;
- conservare le informazioni di abilitazione all'uso della smart card (PIN e PUK) in luogo diverso dalla smart card stessa;
- cambiare i PIN provvisori della propria smart card;
- comunicare informazioni esatte e veritiere rispetto ai propri dati personali nell'ambito delle iniziali procedure di registrazione al servizio di certificazione;
- informare il Certificatore (recandosi presso il Punto di Registrazione di riferimento) di ogni variazione delle informazioni fornite durante la procedura di identificazione e registrazione;
- informare il Certificatore (recandosi presso il Punto di Registrazione di riferimento) in caso di cessazione del servizio per cui sono stati richiesti i certificati digitali (ove previsto cfr. art. 6);
- conservare con la massima diligenza la userid, la password e il codice di sospensione ricevuti durante la fase di registrazione per evitare la conoscenza di questi da parte di altri soggetti;
- richiedere tempestivamente al PdR di riferimento la revoca dei propri certificati digitali al verificarsi delle condizioni enunciate nel paragrafo "Motivi per la revoca e per la sospensione dei certificati";
- richiedere tempestivamente al PdR di riferimento o al numero verde del CERTIFICATORE la sospensione dei propri certificati digitali al verificarsi delle condizioni enunciate nel paragrafo "Motivi per la revoca e per

la sospensione dei certificati” e in particolare nei casi di furto, smarrimento o sospetta compromissione della propria smart card;

- utilizzare le chiavi private personali ed il corrispondente certificato digitale nel pieno rispetto delle funzioni previste dalla sua tipologia e secondo le modalità enunciate nelle “Condizioni di Fornitura del Servizio di Certificazione Digitale” e nel Manuale Operativo del Certificatore LISIT S.P.A.

In caso di furto o smarrimento della Sua smart card contatti immediatamente il numero verde 800-287524, attivo tutti i giorni 24 ore su 24, per richiedere il blocco della smart card stessa comunicando il codice di sospensione stampato sulla busta oscurata che Le verrà consegnata insieme alla carta.

Articolo 6 Motivi per la revoca e sospensione dei certificati

Si elencano le condizioni al verificarsi delle quali si rende necessaria, da parte del TITOLARE o del TERZO INTERESSATO, la richiesta di sospensione o revoca dei certificati digitali:

- per compromissione della chiave privata del TITOLARE; una chiave privata si intende compromessa quando:
 - sia venuta meno la sua segretezza;
 - si sia verificato un qualunque evento che ne abbia compromesso il livello di affidabilità
- in caso di furto o smarrimento del dispositivo di firma;
- in caso di guasto del dispositivo di firma;
- in caso di furto o smarrimento dei PIN e/o del PUK del dispositivo di firma;
- non ci sia più corrispondenza tra i dati del TITOLARE e quelli riportati sui suoi certificati;
- per cessazione dell’utilizzo del servizio per il quale il TITOLARE aveva richiesto i certificati;
- per riscontro da parte del CERTIFICATORE o del TERZO INTERESSATO di un sostanziale mancato rispetto, da parte del TITOLARE, delle condizioni di utilizzo previste dal Manuale Operativo del CERTIFICATORE.

Articolo 7 Responsabilità del CERTIFICATORE

Il CERTIFICATORE è responsabile verso i Titolari, per l’adempimento di tutti gli obblighi discendenti dall’espletamento delle attività previste dalla Direttiva 1999/93/CE, dal DPCM 30 Marzo 2009 e successive modifiche ed integrazioni, dal D.lgs. n. 82/2005 e successive modifiche ed integrazioni e dal D.lgs n. 196/2003.

Il CERTIFICATORE è altresì responsabile nei confronti di qualunque soggetto faccia ragionevolmente affidamento sui certificati emessi dallo stesso, nei limiti della normativa vigente in materia. L’esistenza e la validità del certificato digitale non dispensano tuttavia il TITOLARE dall’eseguire ogni altra verifica che appaia opportuna secondo i criteri di oculata prudenza, anche in relazione al rilievo, economico o d’altra natura, degli interessi coinvolti.

Il CERTIFICATORE non sarà responsabile per danni di qualsiasi natura, diretti o indiretti, da chiunque patiti nella misura in cui tali danni derivino dalla violazione di obblighi che, in virtù di quanto previsto dal Manuale Operativo del CERTIFICATORE ovvero dalle vigenti disposizioni di legge, incombono al TITOLARE, al TERZO INTERESSATO e/o a quanti accedono al registro dei certificati per la verifica della firma, ovvero dallo svolgimento di attività illecite.

Il CERTIFICATORE non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

Il CERTIFICATORE non assume alcun obbligo, garanzia e responsabilità ulteriori rispetto a quelle previste dal presente documento o dalle vigenti disposizioni normative.

Ogni responsabilità è comunque esclusa laddove il CERTIFICATORE provi di aver agito senza colpa, e nei casi previsti dall’art. 30 del D.lgs n°82/2005 e successive modifiche ed integrazioni.

Articolo 8 Clausola risolutiva espressa

Il mancato rispetto dell’art. 5 del contratto dà luogo all’applicazione dell’art. 1456 c.c.

Articolo 9 Rinvio al Manuale Operativo

Per quanto non espressamente indicato negli articoli precedenti in tema di attività ed obblighi, si rinvia a quanto dispone il Manuale Operativo del CERTIFICATORE, che costituisce parte integrante e sostanziale del presente documento.

Articolo 10 Foro Competente

Per ogni e qualsiasi controversia relativa all’esecuzione o interpretazione del contratto di fornitura del servizio è competente in via esclusiva il foro di Milano.

8 MODALITÀ OPERATIVE

Questo capitolo descrive le modalità di rilascio dei certificati relativi a chiavi di sottoscrizione e di cifra e autenticazione, nonché le procedure di sospensione, revoca e riemissione degli stessi.

Agli utenti vengono erogate due coppie di chiavi, con i relativi certificati, una per le operazioni di firma digitale (sottoscrizione), l'altra per le operazioni di cifra e autenticazione.

Chiavi e certificati dell'utente vengono memorizzati su un dispositivo che viene definito, dalla normativa sulla firma digitale, dispositivo sicuro di firma.

La coppia di chiavi di sottoscrizione dell'utente è generata all'interno del dispositivo di firma, la chiave privata non è estraibile da esso e non è conservata in nessun altro luogo. La coppia di chiavi di cifratura è generata dal Certificatore all'esterno del dispositivo di firma e conservata, oltre che sul dispositivo di firma dell'utente, anche in apposito sistema di gestione sicura delle chiavi (Key Archive/Key Recovery Service). Tale accorgimento è utilizzato per consentirne il recupero sicuro a fronte di una eventuale perdita, e permettere così all'utente, che avesse documenti cifrati con tali chiavi, di decifrare comunque gli stessi (vd. Procedure di recupero chiave privata di cifra ai par. "Modalità di sostituzione delle coppie di chiavi e dei certificati dell'utente titolare" e par. "Modalità di sostituzione delle coppie di chiavi e dei certificati dell'utente titolare").

Le procedure di richiesta ed acquisizione certificati, revoca certificati, sospensione ed annullamento della sospensione certificati, riemissione certificati, descritte di seguito nel presente Manuale, fanno sempre riferimento ad entrambi i certificati ed alle relative coppie di chiavi.

La procedura di recupero della/e chiave/i private di cifra fa riferimento solo a questa tipologia di chiavi.

8.1 Modalità di Identificazione e Registrazione degli Utenti Titolari

Questa sezione descrive le modalità operative che portano all'identificazione del richiedente e alla registrazione dei dati personali necessari all'emissione dei certificati.

8.1.1 Procedure di adesione al servizio

L'utente che intende aderire al servizio per ottenere la funzionalità di firma digitale compie un iniziale processo di adesione durante il quale personale incaricato effettua il riconoscimento e l'identificazione dello stesso. Questo processo genera la richiesta di produzione del dispositivo sicuro di firma e dei codici di sicurezza ad esso associati (PIN utente, PIN firma e relativo PUK di sblocco).

La busta con i codici PIN e PUK sarà recapitata tramite servizio postale al richiedente all'indirizzo da lui specificato (ufficio, studio o abitazione) al momento dell'adesione; il dispositivo di firma sarà invece inviato al PdR di riferimento, cioè quello a cui il richiedente fa capo e dove si recherà per ritirarlo. Il dispositivo di firma sarà inviato presso la struttura di appartenenza se si tratta di HSM.

8.1.2 Procedure di identificazione e registrazione dell'Utente Titolare

L'utente che intende richiedere alla CA di LISIT certificati digitali per la firma e la cifra di documenti in formato elettronico si deve rivolgere ad un Punto di Registrazione portando con sé i codici di sicurezza del dispositivo sicuro di firma di cui è titolare; i punti di registrazione svolgono il compito di acquisizione e registrazione nel sistema dei dati dell'utente necessari alla procedura di certificazione, previa identificazione certa del richiedente.

Questi compiti vengono svolti dal personale di PdR tramite il Portale del Certificatore LISIT. L'accesso al Portale è possibile solo in seguito ad autenticazione tramite Smart Card personale, di seguito la Smart Card sarà usata anche per firmare digitalmente le transazioni di dati attivate verso la CA.

L'utente munito di documento di identità valido (sono accettati tutti i documenti previsti dall'art. 35 del DPR445/2000) e di Codice Fiscale si reca al Punto di Registrazione.

L'addetto del Punto di Registrazione riconosce l'utente che si vuole registrare attraverso il documento di identità da questo fornito. Recupera i suoi dati anagrafici e compila il modulo elettronico di richiesta di registrazione con i dati ottenuti dall'identificazione; la richiesta di registrazione e i dati anagrafici dell'utente sono archiviati nel data base del Certificatore.

Per ottenere la certificazione il titolare deve sottoscrivere una richiesta cartacea di registrazione che riporta, oltre ai dati personali del richiedente la registrazione:

- una dichiarazione di presa visione del presente Manuale Operativo;
- una dichiarazione di condivisione degli obblighi e delle responsabilità enunciate nel presente manuale;
- una dichiarazione di consenso all'utilizzo dei propri dati personali e alla pubblicazione dei certificati digitali emessi a proprio nome.

La stampa in formato cartaceo del modulo elettronico è firmata dal richiedente in presenza dell'addetto che la controfirma.

Questa documentazione cartacea e copia del documento esibito per l'identificazione sarà archiviata dal responsabile del punto di registrazione in appositi contenitori muniti di serratura di sicurezza siti in locali protetti e custodita per un periodo di 20 anni dalla data di scadenza dei certificati emessi.

I dati acquisiti dalla CA di LISIT, attraverso le operazioni di registrazione, sono:

- Codice Fiscale
- Nome
- Cognome
- Ruolo
- Data di nascita
- Luogo di nascita
- Indirizzo E-mail
- Tipo, numero e data di emissione del documento di identità esibito
- Ente che ha emesso il documento

In caso di variazioni di uno o più dati raccolti durante la registrazione, il titolare dovrà prontamente comunicare le modifiche al Certificatore.

Se la registrazione è andata a buon fine vengono generati tre codici per la futura identificazione dell'utente; si tratta di:

- ID Utente e password di accesso al portale del Certificatore;
- Codice di Sospensione per l'autenticazione delle richieste di sospensione.

Ogni individuo può possedere più certificati relativi a ruoli diversi con cui firmare, il rilascio di ogni certificato avverrà previa procedura di identificazione indipendente e con l'assegnazione di altrettanti dispositivi di firma quanti sono i certificati di firma digitale di cui è titolare.

Eventuali poteri di rappresentanza e titoli professionali devono essere dichiarati al momento della registrazione e supportati con adeguata documentazione.

L'informazione relativa al ruolo del titolare è trattata nei certificati in conformità con le regole tecniche in vigore.

8.2 Modalità di generazione delle chiavi e emissione dei certificati

Questa sezione descrive le modalità seguite dal Certificatore per la generazione delle coppie di chiavi crittografiche, la verifica delle relative richieste di certificazione e l'emissione dei certificati.

8.2.1 Generazione delle chiavi di firma e richiesta del certificato

Terminata la fase di registrazione l'addetto PdR avvia, per conto dell'utente ed in sua presenza la procedura di richiesta dei certificati.

In questa fase viene registrata negli archivi del Certificatore l'associazione tra i dati dell'utente e quelli del dispositivo di firma di cui è titolare e assegnato all'utente un Codice Unico presso il Certificatore, codice utile all'identificazione univoca dell'utente all'interno del dominio del Certificatore.

La coppia di chiavi per le operazioni di firma digitale è generata all'interno del dispositivo sicuro di firma sotto il controllo del Certificatore prima che il dispositivo stesso sia recapitato al PdR. Le chiavi generate sono di tipo RSA con lunghezza almeno pari a 1024 bit, tali da garantire un elevato livello di sicurezza.

Durante la procedura di generazione della richiesta di certificati alla CA, l'utente digita dapprima il *PIN Firma* per abilitare l'uso del dispositivo e successivamente inserisce il *PIN Utente*. La richiesta di certificato, in formato standard PKCS#10, è firmata con la chiave privata di Firma dell'utente ed inviata alla CA. Il formato della richiesta è tale da fornire la prova del possesso della chiave e la verifica del corretto funzionamento della coppia di chiavi e del dispositivo nel rispetto di quanto definito nell'art. 5 del DPCM 30 Marzo 2009.

I PIN provvisori utilizzati in questa fase per la personalizzazione del dispositivo di firma possono essere cambiati dal titolare in qualsiasi momento.

8.2.2 Generazione della chiave di cifra e richiesta certificato cifra

Alla ricezione della richiesta di certificato per chiavi di firma, è generata dal Certificatore, esternamente al dispositivo di firma, in modo del tutto automatico, un'ulteriore coppia di chiavi per operazioni di cifratura e la conseguente richiesta di certificazione alla CA. Le chiavi private di cifratura sono trasferite mediante un canale protetto nel dispositivo di firma e contemporaneamente sono custodite in maniera sicura all'interno di un apposito sistema di archiviazione dedicato (Key Archive Server) presso il Certificatore. Questo permette al Titolare di richiedere eventualmente il Key Recovery delle sue chiavi di cifratura anche a distanza di tempo.

8.2.3 Verifica delle richieste

Prima di inoltrare le richieste alla CA, viene verificata la corrispondenza fra l'identificativo del dispositivo di firma (s/n) che si vuole personalizzare e quello raccolto in fase di registrazione.

Superata questa fase di verifica le richieste vengono inoltrate alla CA, qui viene controllata l'appartenenza del dispositivo e delle chiavi che si vogliono certificare al dominio di LISIT; successivamente le richieste sono sottoposte ad un processo di verifica della firma, ossia la firma digitale apposta sulla richiesta è verificata con la chiave pubblica presente all'interno della richiesta stessa; questa verifica costituisce la prova di possesso della chiave privata da parte dell'utente richiedente e la prova di corretto funzionamento della coppia di chiavi come richiesto dalla normativa vigente.

Le richieste vengono sottoposte ad un ulteriore controllo di unicità della chiave. La CA si accerta che la chiave pubblica da certificare non sia già stata certificata in precedenza a favore di un titolare diverso dal richiedente, all'interno del proprio dominio. L'eventuale esistenza di una chiave pubblica uguale a quella generata dal richiedente darà luogo, su iniziativa della CA, al rigetto della richiesta di certificazione.

La CA, in relazione all'esito delle verifiche legate alla richiesta di emissione del certificato, procede all'invio all'utente di eventuali messaggi di errore o di presa in carico della richiesta stessa.

Nel caso in cui le verifiche di cui sopra, evidenzino incongruenze rispetto all'identità del titolare ovvero la presenza di certificati relativi alla stessa chiave di cui viene richiesta la certificazione, il Certificatore è obbligato a:

- procedere tempestivamente al rigetto della richiesta;
- informare il titolare della chiave già certificata e procedere alla revoca del certificato;
- conservare la richiesta respinta per un periodo di 20 anni.

8.2.4 Generazione dei certificati e loro pubblicazione

La CA, in relazione con l'esito positivo delle verifiche legate alle richieste di emissione dei certificati provvede ad effettuare le operazioni previste dal regolamento vigente. Nel dettaglio:

- registrare nei log di sistema il momento della generazione dei certificati;
- inviare al titolare copia dei certificati emessi (i certificati verranno scritti nel dispositivo di firma del titolare);
- conservare i dati relativi alla richiesta di certificato per un periodo di 20 anni.

Le informazioni contenute nei certificati soddisfano quanto richiesto dalla normativa vigente.

La presenza e le caratteristiche delle estensioni dipendono dalla tipologia del certificato e comunque vengono trattate in conformità con le disposizioni normative e regolamentari vigenti.

8.2.5 Personalizzazione del dispositivo di firma (Acquisizione Certificati)

Se l'inoltro della richiesta di certificazione è andata a buon fine, nel dispositivo di firma viene trasferito il certificato relativo alla chiave di firma, il certificato di cifra e relativa chiave privata di cifra, il certificato della CA relativo alle chiavi di sottoscrizione (secondo quanto previsto dalla normativa vigente) ed il certificato della CA di marcatura temporale, completando così la fase di personalizzazione.

Da questo momento l'utente è abilitato alle operazioni di firma e cifra.

8.3 Validità dei certificati

La durata dei certificati utente emessi dalla CA di LISIT è pari a 6 anni a partire dalla data di emissione. Al termine naturale di tale periodo i certificati andranno riemessi e le chiavi sostituite; la riemissione comporta la personalizzazione di un nuovo dispositivo di firma.

8.4 Tipologia e struttura dei certificati

La struttura dei certificati emessi dal Certificatore LISIT è conforme allo standard X.509 versione 3. I certificati emessi da LISIT, oggetto del presente Manuale Operativo sono inoltre conformi alla normativa secondo quanto previsto dall'art. 28 comma 1 del CAD.

Si veda il par 5.2 per le modalità di identificazione dei certificati emessi.

8.5 Modalità di sostituzione delle coppie di chiavi e dei certificati dell'utente titolare

In prossimità della data di scadenza dei certificati, verrà inviata una comunicazione d'ufficio all'utente. Da questo momento, l'utente potrà ripresentarsi al PdR di riferimento per effettuare la procedura di personalizzazione del nuovo dispositivo di firma secondo modalità analoghe a quanto previsto per la prima emissione.

I certificati scaduti saranno conservati da parte del Certificatore per un periodo di 20 anni. La firma elettronica basata su un certificato qualificato scaduto non costituisce valida sottoscrizione.

8.6 Modalità di Sospensione e Revoca dei certificati

La sospensione è l'operazione con cui la CA sospende la validità del certificato; la sospensione è una operazione temporanea e reversibile che può evolvere in una revoca definitiva o in un annullamento della sospensione stessa con contemporanea riattivazione del certificato. La sospensione può avvenire su richiesta dell'utente titolare nei casi in cui questo lo ritenga necessario, ma anche su richiesta del terzo interessato o su iniziativa della CA.

La revoca è l'operazione irreversibile con la quale la CA LISIT annulla la validità del certificato prima della sua naturale scadenza. La revoca può avvenire su richiesta dell'utente titolare, su iniziativa della CA o su richiesta del terzo interessato.

La revoca o la sospensione tolgono validità al certificato e rendono non valide le firme emesse successivamente al momento di revoca o sospensione.

Ogni certificato sospeso o revocato è pubblicato immediatamente nella Certificate Revocation List o lista dei certificati revocati (CRL) la quale è firmata digitalmente dalla CA e pubblicata sul Registro dei Certificati; l'attività di pubblicazione della CRL ed in generale tutte le attività di CA sono registrate nel log dei sistemi del Certificatore.

La CRL contiene sia i certificati revocati che quelli sospesi così come consentito dalla normativa vigente; per ogni registrazione presente nella CRL è indicato se si tratta di certificato sospeso o revocato.

La sospensione o la revoca di un certificato diviene effettiva dal momento della sua pubblicazione sulla CRL (CAD, art. 36, comma 3, e successive modifiche ed integrazioni).

Per la disponibilità del servizio di sospensione e di revoca si consulti il paragrafo "Orari del Servizio ed Enti preposti".

8.6.1 Motivi validi per la revoca e per la sospensione dei certificati

Si elencano le condizioni al verificarsi delle quali si rende necessaria la richiesta di revoca dei certificati relativi ad un utente:

- per compromissione della chiave privata (una delle due o tutte e due) dell'utente; una chiave si intende compromessa quando:
 - o sia venuta meno la sua segretezza;
 - o si sia verificato un qualunque evento che ne abbia compromesso il livello di affidabilità;
- sia stato smarrito o distrutto il dispositivo di firma;
- sia diventata impossibile, a causa di un guasto, l'utilizzo del dispositivo di firma;
- siano stati smarriti il PIN ed il PUK necessario per sbloccare il dispositivo di firma e ridefinire il relativo PIN;
- non ci sia più corrispondenza tra i dati dell'utente e quelli riportati sui suoi certificati;
- per cessazione dell'utilizzo del servizio per il quale l'utente titolare aveva richiesto i certificati (*);
- per riscontro da parte della CA di LISIT o dal terzo interessato di un sostanziale mancato rispetto, da parte dell'utente, delle condizioni di utilizzo previste dal presente Manuale Operativo.

(*) Questa clausola non si applica agli operatori socio sanitari aderenti al Progetto CRS-SISS della Regione Lombardia nel caso in cui, pur avendo cessato il servizio o la convenzione con una Struttura Sanitaria, intendano continuare ad operare nell'ambito del Servizio Sanitario Regionale. In tali circostanze, per ragioni di contenimento dei costi e per la razionalizzazione delle procedure operative, è data facoltà al Titolare di non richiedere la revoca dei propri certificati digitali. Il Terzo Interessato è esentato dall'obbligo di procedere alla revoca d'ufficio, a meno di gravi motivi.

8.6.2 Procedura di revoca su richiesta del Titolare

L'utente può richiedere la revoca dei propri certificati presentandosi allo sportello del Punto di Registrazione munito di documento di identità valido.

L'addetto del Punto di Registrazione identificherà il richiedente secondo modalità simili a quelle seguite durante la fase di registrazione.

L'utente dovrà compilare e sottoscrivere un apposito modulo cartaceo di richiesta di revoca, controfirmato dall'addetto che effettua il riconoscimento, nel quale si specificano chiaramente:

- i dati identificativi dell'utente titolare;
- la motivazione precisa che ha indotto la richiesta di revoca;
- la data di revoca.

Copia elettronica della richiesta di revoca così generata è inviata alla CA firmata digitalmente dallo stesso addetto PdR.

La CA procede alla revoca del certificato immediatamente o comunque nel più breve tempo tecnicamente possibile dalla ricezione della richiesta.

Qualora la richiesta di revoca sia dovuta alla possibile compromissione della chiave privata, il Certificatore deve provvedere tempestivamente all'effettuazione della revoca e alla pubblicazione della lista di revoca aggiornata secondo quanto previsto dalla normativa vigente in materia.

In ogni caso, l'utente, se è impossibilitato ad andare al Punto di Registrazione, può richiedere, in via cautelativa, la sospensione tramite il servizio di Help Desk telefonico oppure mediante il Portale del Certificatore (per le modalità di questi servizi vd. par. "Procedura di sospensione dei certificati su richiesta del Titolare"), entrambi i servizi sono fruibili

h24, 7 giorni su 7. Il titolare dovrà, non appena possibile, trasformare la sospensione in revoca seguendo la procedura sopra descritta.

8.6.3 Procedura di revoca su iniziativa del Terzo interessato

La revoca dei certificati di un utente può avvenire anche su iniziativa del terzo interessato. Il terzo interessato per poter inoltrare richiesta di revoca deve recarsi ad un Punto di Registrazione. Presso il Punto di Registrazione il terzo interessato, dopo essere stato identificato, deve fornire precisa motivazione della causale di revoca supportandola con adeguata documentazione giustificativa.

Il terzo interessato dovrà inoltre sottoscrivere un modulo cartaceo di revoca nel quale verranno specificati:

i dati identificativi del richiedente la revoca;

- i dati identificativi del Titolare del certificato che si vuole revocare;
- la causale della richiesta di revoca;
- la data della revoca.

Il modulo verrà controfirmato dall'addetto del Punto di Registrazione che, dopo aver effettuato l'identificazione e verificato l'attendibilità della documentazione presentata a suffragio, inoltrerà la richiesta al Certificatore.

La CA, fatte le necessarie verifiche, provvederà ad effettuare la revoca nel più breve tempo possibile ed invierà comunicazione all'utente titolare dell'avvenuta revoca dei suoi certificati tramite posta prioritaria specificando la motivazione della revoca e la data e l'ora a partire dalla quale i certificati risultano revocati.

8.6.4 Procedura di revoca su iniziativa del Certificatore

La revoca dei certificati di un utente può avvenire anche su iniziativa del Certificatore LISIT, soprattutto in caso di riscontro di un sostanziale mancato rispetto, da parte dell'utente, delle condizioni previste dal presente Manuale Operativo e nei casi previsti dall'art. 36 del CAD e successive modifiche ed integrazioni.

La CA provvederà alla revoca dei certificati ed alla sua pubblicazione sulla CRL, inviando comunicazione all'utente titolare dell'avvenuta revoca dei suoi certificati tramite posta prioritaria, specificando la motivazione della revoca e la data e l'ora a partire dalla quale i certificati risultano revocati.

8.6.5 Procedura di sospensione dei certificati su richiesta del Titolare

Per attivare la procedura di sospensione dei propri certificati, l'utente titolare può presentarsi personalmente agli sportelli del Punto di registrazione munito di documento di identità valido o contattare telefonicamente il numero verde del Help Desk di riferimento (procedura di emergenza) oppure utilizzare l'apposito servizio fruibile accedendo al Portale del Certificatore.

Procedura presso il PdR

La procedura di sospensione, attivata agli sportelli del punto di registrazione, prevede l'identificazione del richiedente secondo modalità simili a quelle seguite durante la fase di registrazione e la successiva trasmissione alla CA della richiesta di sospensione.

Dopo essere stato identificato, al richiedente verrà richiesto di sottoscrivere un apposito modulo cartaceo di sospensione dove verranno specificati:

- i dati identificativi del richiedente la sospensione;
- la causale della richiesta di sospensione;
- la data di inizio del periodo di sospensione.

La richiesta di sospensione firmata digitalmente dallo stesso addetto di Registrazione è inviata alla CA. La CA provvederà a renderla esecutiva immediatamente o comunque nel più breve tempo possibile.

Procedura telefonica

La sospensione del proprio certificato può essere innescata anche telefonicamente contattando il numero verde del Help Desk del Certificatore (800.28.75.24); in questo caso il richiedente è identificato fornendo tre su sei caratteri scelti a caso del suo Codice di Sospensione. Effettuata l'identificazione e raccolte le informazioni sulla causale della richiesta di sospensione, la richiesta verrà trasferita alla CA che provvederà a renderla esecutiva. In caso di dimenticanza o smarrimento della Chiave Segreta di Sospensione, per recuperarla, l'addetto di HD chiederà al titolare la risposta alla domanda segreta che l'utente stesso ha inserito tramite Portale. Qualora l'utente non ricordasse neppure questa o non

l'avesse mai inserita, l'HD aprirà un ticket alla CA o al PdR LISIT che provvederà a verificare l'attendibilità della richiesta e in caso di riscontro positivo ad evaderla nel più breve tempo possibile.

Procedura web

Per richiedere la sospensione l'utente può infine accedere al Portale del Certificatore identificandosi tramite la digitazione dell'ID Utente e della password oppure utilizzando la propria smart card se ne è ancora in possesso.

8.6.6 Sospensione su richiesta del Terzo interessato

La richiesta di sospensione deve essere inoltrata dal terzo interessato per iscritto presso un Ente di Registrazione secondo modalità simili a quanto descritto per la richiesta di revoca (vd. Par. "Procedura di revoca su iniziativa del Terzo interessato").

La CA invierà comunicazione al titolare tramite posta prioritaria dell'avvenuta sospensione dei suoi certificati, specificando la data e l'ora a partire dalla quale i certificati risultano sospesi.

8.6.7 Sospensione su iniziativa del Certificatore

La sospensione del certificato può essere innescata anche dalla CA stessa; sarà dovere della CA dare comunicazione all'utente titolare dell'avvenuta sospensione del suo certificato, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale il certificato risulta sospeso. La CA darà comunicazione all'utente tramite posta prioritaria.

8.6.8 Durata massima della sospensione dei certificati

Un certificato può rimanere nello stato di sospensione per un tempo massimo di 60 giorni. Oltre questa data il Certificatore provvederà ad effettuare un'operazione di revoca dello stesso. La CA darà comunicazione dell'operazione all'utente tramite posta prioritaria.

8.6.9 Procedura di annullamento della sospensione

Dopo aver sospeso i propri certificati l'utente titolare può richiedere l'annullamento della sospensione in ogni momento.

L'annullamento della sospensione può essere richiesto presentandosi presso gli sportelli del punto di registrazione identificandosi con un documento valido; inoltre al richiedente verrà richiesto di sottoscrivere un apposito modulo.

Con l'annullamento della sospensione viene ripristinata la validità dei certificati con la rimozione degli stessi dalla lista di revoca/sospensione.

8.6.10 Procedura di revoca dopo la sospensione

Al verificarsi di una delle condizioni elencate al par. "Motivi validi per la revoca e per la sospensione dei certificati", l'utente potrà invece tramutare la sospensione in revoca effettiva. Questa operazione può avvenire solo presentandosi personalmente presso gli sportelli del Punto di Registrazione ed espletando l'intera procedura di revoca (vd. par. "Procedura di revoca su richiesta del Titolare").

8.7 Procedura di certificazione successiva alla revoca

In caso di revoca dei suoi certificati per propria iniziativa o per iniziativa di terzi, per riottenere nuovi certificati l'utente dovrà ripetere nuovamente l'intera procedura di certificazione presentandosi al Punto di Registrazione per una nuova identificazione e registrazione alla CA.

8.8 Archiviazione della chiave privata di cifra e sue procedure di recupero

In caso di smarrimento/furto del dispositivo di firma oppure di guasto dello stesso, l'utente potrà ottenere la restituzione delle vecchie chiavi private di cifra, con cui potrà decifrare eventuali documenti cifrati in passato con le vecchie chiavi non più a sua disposizione. La procedura sarà disponibile collegandosi al Portale del Certificatore con la nuova smart card. Direttamente nella propria area personale il Titolare si troverà a disposizione la funzione di recupero chiavi di cifra.

8.9 Registro dei certificati

Sul Registro dei certificati vengono registrati i seguenti elementi:

- la lista dei certificati revocati;
- la lista dei certificati sospesi.

La lista dei certificati revocati e la lista dei certificati sospesi coincidono nella stessa CRL.

La CRL emessa rispetta la versione v2, definita dallo standard ITU-T X.509.

Oltre alla CRL relativa a tutti i certificati emessi dalla CA che siano sospesi o revocati, verranno prodotte altre CRL parziali relative a sottoinsiemi di tali certificati allo scopo di facilitare l'acquisizione delle informazioni sulla revoca e sulla sospensione dei certificati da parte delle applicazioni client.

All'interno dei certificati è presente un riferimento alla CRL parziale ad esso relativa in modo da ridurre il tempo necessario al suo download.

Come disposto dal comma 3 dell'art. 18 della Deliberazione 45/2009, i certificati revocati o sospesi permangono nella CRL, anche dopo la loro naturale scadenza, fino alla scadenza del relativo certificato di certificazione.

8.9.1 Frequenza delle pubblicazioni

La frequenza con cui le informazioni di cui al precedente paragrafo sono pubblicate dipende dalla tipologia dell'informazione stessa e comunque avviene secondo i seguenti criteri:

- la CRL è aggiornata e pubblicata ogni volta che viene revocato o sospeso un certificato e comunque almeno due volte al giorno (in assenza di nuove revoche o sospensioni).

8.9.2 Procedura di gestione del Registro dei certificati

La gestione del registro dei certificati avviene su un archivio elettronico (Directory Service) in standard ITU-T X.500, la copia di riferimento del registro dei certificati è inaccessibile dall'esterno e allocata su un sistema presso il locale a più alta protezione del sito della CA.

La gestione del registro dei certificati produce automaticamente due copie operative identiche, rese disponibili alla consultazione tramite protocollo LDAP v2 e v3 su Internet e su Extranet.

È compito del Certificatore verificare periodicamente la conformità fra la copia operativa e la copia di riferimento.

La copia di riferimento del registro di controllo è sottoposta a back-up giornaliero.

Solo le procedure autorizzate possono modificare il contenuto del registro; ogni modifica così come ogni momento di indisponibilità del registro verso l'esterno trova registrazione nei log di sistema.

8.9.3 Modalità di accesso al Registro dei certificati

L'accesso al registro dei certificati avviene con modalità conformi a quanto previsto dall'art. 32 comma 3 lett. M, del CAD e successive modifiche ed integrazioni.

Il registro dei certificati di LISIT è accessibile in sola lettura a tutta l'utenza mediante protocollo LDAP v3 all'indirizzo <ldap://ldap.crs.lombardia.it>.

8.10 Modalità operative per la generazione della firma digitale

In questo paragrafo vengono descritte, le modalità operative per la generazione della firma digitale come previsto dal art. 36, comma 3, lett. S del DPCM 30 Marzo 2009, maggiori informazione sono riportate sul sito del Certificatore LISIT.

Ai sensi dell'art. 6, commi 4 e 5 del DPCM 30 Marzo 2009, il Certificatore fornisce al Titolare un dispositivo sicuro di firma conforme con la normativa vigente e compatibile con le tecnologie utilizzate dal Certificatore; il Titolare a sua volta ha l'obbligo di utilizzare questo dispositivo esclusivamente per le operazioni previste dal servizio del Certificatore.

Il Certificatore LISIT si riserva di verificare la compatibilità di dispositivi alternativi qualora i Titolari ne facessero richiesta motivata.

8.10.1 Corretta rappresentazione dei documenti

I documenti elettronici sono redatti mediante elaboratori di testi, posta elettronica, fogli elettronici ecc. Molti di questi prodotti offrono la possibilità di inclusione di contenuti multimediali, di collegamenti ipertestuali e di oggetti dinamici. Queste funzionalità che possono risultare molto utili in alcuni contesti, possono risultare pericolose se usate in modo malizioso su documenti che si intende sottoscrivere con firma digitale. Di fatto quanto si firma un documento informatico con questi contenuti, non si sta firmando un documento vero e proprio ma un file di dati. Un utente esperto potrebbe ad esempio inserire macro o campi nascosti che alterano il documento magari facendo riferimento a file esterni o a condizioni di contorno differenti che ne variano dinamicamente il contenuto.

Per evitare questi rischi è dovere del Titolare assicurarsi che il documento non contenga macroistruzioni o codici eseguibili tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati nello stesso rappresentati (art. 3, comma 3 del DPCM 30 Marzo 2009). Si invita pertanto il Titolare, al momento della firma, a verificare che siano disattivate tutte le opzioni del programma in uso che portino ad una modificazione dinamica non desiderata⁵ al contenuto del documento da sottoscrivere. Per facilitare questo controllo è opportuno fare riferimento alle istruzioni d'uso dei programmi usati per produrre i documenti informatici da sottoscrivere.

E' opportuno per tanto che il Titolare tenga presente le seguenti indicazioni:

- il rischio di ottenere una presentazione ambigua dei dati è particolarmente elevato nel caso di documenti informatici composti da un elaboratore di testi a causa della natura di tali software, non progettati per ottenere visualizzazioni assolutamente univoche dello stesso documento in diversi contesti;
- il Certificatore LISIT distribuisce, nell'ambito del proprio servizio di Certificazione, il prodotto DigitalSign – Edizione Lisit, che visualizza al suo interno documenti di questo tipo in modo da ridurre il rischio di alterazione dei dati durante la visualizzazione. Nonostante questa funzionalità, è altamente consigliabile configurare opportunamente il word processor;
- per quanto riguarda i formati di salvataggio e memorizzazione dei documenti elettronici è opportuno non utilizzare i formati tipici dei singoli strumenti software ma i formati di interscambio che generalmente sono meno ricchi di funzionalità di modificazione dinamica del contenuto. In ogni caso è utile consultare le guide alla configurazione dei singoli prodotti utilizzati.

8.11 Informazioni sui formati dei documenti

8.11.1 Il formato PDF

Il formato PDF (Portable Document Format) è stato progettato appositamente per l'interscambio dei documenti in modo che il ricevente veda esattamente il documento come è stato creato, indipendentemente dalle diverse elaborazioni fatte su di esso. E' da considerare sicuro se usato come base per i documenti informatici firmati digitalmente tramite DigitalSign – Edizione Lisit. Anche documenti in formato PDF di ultima generazione tuttavia possono avere problemi di macro, codici ecc che possono variare il contenuto in modo dinamico per questo motivo anche in questo caso si consiglia al Titolare di verificare le impostazioni di programma che possono portare ad una modificazione dinamica non desiderata.

Il formato PDF può anche essere ottenuto in seguito alla stampa virtuale su stampanti PDF (come ad es. PDFCreator) di documenti prodotti con altri software. In questo caso il documento ottenuto a video è identico di quello ottenuto su carta. Questo ultimo documento prodotto può essere sottoscritto con ragionevole tranquillità.

⁵ A puro titolo esemplificativo: una data, un'ora, un numero di pagina oppure un richiamo del valore di una somma di un foglio di calcolo ecc

8.11.2 Formati di Microsoft Office

Purtroppo non sono disponibili metodi certi per la verifica della presenza di tutti gli elementi in grado di alterare i contenuti del documento presentato tramite uno degli applicativi MS Office, pertanto finché possibile si sconsiglia l'uso dei formati DOC, DOT, RTF, XLS, per i documenti particolarmente critici. Dove fosse indispensabile l'utilizzo di tali formati, prima di procedere alla sottoscrizione è indispensabile bloccare la dinamicità dei campi disattivando tutte le apposite funzioni oppure anche in questo caso ricorrere alla trasformazione del documento in formato PDF con una stampante virtuale e poi procedere alla sua sottoscrizione del documento PDF ottenuto tramite DigitalSign – Edizione Lisit. Si danno di seguito alcune informazioni specifiche sui principali formati MS Word utilizzati per la creazione di documenti:

- DOC/DOCX: è il formato predefinito di un documento di MS Word e può contenere macro istruzioni
- DOT: è il formato di un modello di MS Word e contiene le istruzioni per l'applicazione della formattazione e degli attributi contenuti a tutti i nuovi documenti basati su tale modello.
- RTF: converte la formattazione in istruzioni che possono essere lette ed interpretate da altri programmi e può contenere macro istruzioni.
- TXT: non contiene informazioni sulla formattazione del testo e non consente l'utilizzo di macro istruzioni
- XLS/XLSX: è il formato principale di MS Excel per memorizzare ed elaborare dati mediante funzioni di varia natura.

8.11.3 Formati per le immagini

Vi sono numerosi formati disponibili per l'utilizzo di immagini come documenti elettronici e si possono dividere tra:

- formati non compressi: (o a bassa compressione) che vengono utilizzati per le applicazioni di stampa o per conservare copie ad alta fedeltà di immagini;
- formati compressi: che generano documenti con dimensioni minori rispetto a quelli di partenza. A questo proposito è opportuno considerare che esistono due tipologie di compressione:
 1. senza perdita di dati: la compressione è reversibile e dall'informazione compressa è possibile ricostruire esattamente l'informazione originale.
 2. con perdita di dati: la compressione è irreversibile e non è più possibile ricostruire esattamente l'informazione originale.

Fra i formati non compressi o a bassa compressione (comunque senza perdita di dati) rientrano BMP (BitMaP - standard di Microsoft Windows® che permette compressioni senza perdita di dati) e TIFF (Tagged Image File Format - formato bitmap supportato da quasi tutte le applicazioni grafiche e molto utilizzato perché consente di scambiare file tra programmi e piattaforme diverse).

Tra i formati compressi con perdita di dati si segnala il comune JPEG (Joint Photographic Experts Group), mentre tra quelli compressi senza perdita, il GIF (Graphic Interchange Format) ed il PNG (Portable Network Graphics).

Sebbene sul piano tecnico la compressione può essere visivamente impercettibile, è opportuno evitare l'utilizzo di immagini sottoposte a procedimenti di compressione con perdita di dati per la creazione di documenti informatici, preferendo in assoluto i formati non compressi o i formati compressi senza perdita. Per l'individuazione di queste caratteristiche, è opportuno fare riferimento alle specifiche informazioni fornite dal produttore del software utilizzato per il trattamento delle immagini o agli standard pubblicati dagli organismi competenti.

8.11.4 Generazione della firma digitale

La firma digitale fa riferimento in maniera univoca ad un documento o insieme di documenti ed al Titolare che l'ha apposta in modo univoco. Compito del Titolare è di accertarsi che il proprio certificato qualificato non risulti scaduto temporalmente o non valido in quanto revocato o sospeso (CAD, art. 24).

L'apposizione della firma digitale ad un documento informatico si basa essenzialmente nella sequenza di operazioni matematiche cui il documento stesso viene sottoposto che per linee generali possiamo così riassumere:

- dal documento viene calcolata un'impronta tramite funzione HASH;
- l'impronta viene sottoposta alla funzione crittografica di firma tramite algoritmo asimmetrico RSA utilizzando la chiave privata del Titolare contenuta nel dispositivo sicuro di firma.

Il risultato dell'operazione crittografica descritta è la firma digitale. I documenti firmati digitalmente sono riconoscibili per l'estensione p7m.

Queste operazioni sono fatte in maniera trasparente per il Titolare tramite DigitalSign ® – Edizione Lisit che LISIT distribuisce quale strumento per la generazione della firma digitale di documenti.

Maggiori informazioni sulle funzionalità del prodotto sono riportate nella documentazione del prodotto stesso per il quale LISIT ha richiesto solo alcune pre-configurazioni.

8.11.5 Verifica della firma digitale

La verifica della firma digitale è l'operazione cardine dell'intero processo crittografico di sottoscrizione, e per questo motivo vanno verificate tutte le operazioni al contorno. Se la verifica della firma digitale ha esito positivo:

- si è certi che il documento sottoscritto non è stato alterato;
- si è certi che il certificato del firmatario è valido e garantito dal Certificatore;
- il Titolare della firma non può negare di averla emessa (non ripudio).

Tramite DigitalSign ® – Edizione Lisit è possibile verificare le firme digitali emesse dai titolari di certificati del Certificatore LISIT e da titolari di certificati emessi da altri certificatori.

L'operazione di verifica della firma digitale non richiede l'uso di smart card o lettore ma viene effettuata tramite personal computer collegato ad Internet. Il collegamento ad Internet è richiesto per la verifica dello stato del certificato tramite il controllo della lista di revoca pubblicata dal Certificatore. Queste operazioni sono svolte da DigitalSign ® – Edizione Lisit in modo del tutto automatico. E' invece richiesta la verifica di eventuali limitazioni dipendenti dalla natura del certificato o del documento da sottoscrivere, in particolare il Certificatore LISIT emette certificati per titolari appartenenti alla pubblica amministrazione, ne consegue che utilizzi esterni a questo ambito non sono da considerarsi validi.

8.11.6 Verifica della firma digitale tramite DigitalSign ® – Edizione Lisit

La verifica della firma digitale apposta ad un documento viene svolta in automatico da DigitalSign ® – Edizione Lisit. L'operazione di verifica compie una serie di operazioni crittografiche che si possono così riassumere:

- la firma digitale viene decifrata utilizzando la chiave pubblica corrispondente alla chiave privata che era stata usata per generarla (tramite algoritmo RSA). Questa operazione permette di ottenere l'impronta da cui si è partiti per l'operazione crittografica di sottoscrizione;
- il documento originale viene sottoposto alla stessa funzione di HASH impiegata all'origine, ottenendo così un'impronta calcolata che era stata ottenuta dal Titolare al momento della sottoscrizione del documento;
- le due impronte, originale e calcolata vengono confrontate, se esse coincidono la firma è verificata ed è da considerarsi autentica, si ha infatti la certezza che nulla è stato alterato.

Questa verifica garantisce l'integrità del documento ma non prova l'identità del Titolare, ma poiché il certificato del sottoscrittore è firmato dalla Certification Authority che lo ha emesso, occorre verificare la validità del certificato della CA e la validità del certificato del Titolare stesso andando a controllare la Certificate Revocation List.

Queste operazioni sono svolte in automatico da DigitalSign ® – Edizione Lisit in modo assolutamente trasparente per l'utilizzatore.

Allo stesso modo è possibile verificare tramite DigitalSign ® – Edizione Lisit firme digitali generate da titolari di certificati emessi da un altro Certificatore iscritto nella "Lista dei certificati delle chiavi di certificazione" pubblicata sul sito di DigitPA (www.cnipa.gov.it).

Con la permanenza nelle CRL delle informazioni di sospensione e revoca dei certificati scaduti, diventa possibile determinare la validità di un documento in una qualsiasi data compresa nel periodo di validità nominale del certificato di sottoscrizione (con l'esclusione di certificati scaduti prima del 3/12/2009).

Come disposto dal comma 3 dell'art.27 della Deliberazione 45/2009, DigitalSign ® – Edizione Lisit consente all'utente di verificare la validità della firma nel periodo di validità del corrispondente certificato. Se il documento è marcato temporalmente, la verifica alla data viene effettuata automaticamente utilizzando il riferimento temporale contenuto nella marca stessa. In alternativa, DigitalSign ® – Edizione Lisit consente di effettuare verifiche di firme digitali riferite ad una data qualsiasi, diversa da quella attuale, che deve essere inserita dall'utente tramite un'apposita funzione.

8.11.7 Verifica della firma digitale da parte di soggetti che non dispongono di DigitalSign ® – Edizione Lisit

I soggetti che necessitano di verificare una firma digitale ma che non dispongono di DigitalSign possono effettuare l'operazione utilizzando DigitalSign Lite disponibile sul sito www.comped.it o altro software indicato sul sito di DigitPA sulle linee guida per l'utilizzo della firma digitale pubblicate sul sito www.cnipa.gov.it.

9 SERVIZI INTERNI ALLA CA

9.1 Generazione della chiave privata della CA

La chiave privata della CA, con la quale essa firma tutti i certificati emessi, viene generata dal Responsabile della CA su dispositivo di firma dotato di requisiti di sicurezza e robustezza conformi a quanto richiesto dalla normativa vigente. Le chiavi generate sono di tipo RSA con lunghezza almeno pari a 2048 bit.

La chiave privata della CA è salvata, cifrata e suddivisa su diversi supporti di archiviazione affidati a responsabili diversi. Al fine di un suo ripristino in seguito al guasto del dispositivo di firma, è necessaria la compresenza di tutti i responsabili e di un sottoinsieme dei supporti di archiviazione loro affidati.

Per attivare i supporti di archiviazione sopra citati, è necessario inoltre conoscere i PIN di sblocco dei rispettivi dispositivi.

9.2 Generazione del certificato della CA

La generazione del certificato della CA avviene nel rispetto delle modalità stabilite dalla normativa vigente e secondo severe misure di sicurezza.

Il certificato è generato su sistema dedicato, sito nei locali del Certificatore a più elevata protezione protetti da meccanismi di controllo accessi che consentono la registrazione di ogni entrata ed uscita del personale sul giornale di controllo e monitorati da un sistema di videosorveglianza; l'accesso è altresì consentito solo a personale preventivamente autorizzato e qualificato per accedere ai sistemi di elaborazione.

Il certificato della CA, firmato con la chiave privata di certificazione stessa, ha una durata pari a 12 anni a partire dalla sua data di emissione, è pubblicato nel registro dei certificati, depositato presso DigitPA e da questa reso pubblicamente disponibile nell'elenco pubblico dei Certificatori accreditati.

9.3 Sostituzione della chiave privata della CA

La scadenza del certificato della CA implica la generazione di nuove coppie di chiavi di certificazione. Almeno 6 anni prima dell'effettiva scadenza della chiave della CA viene avviata la procedura di rinnovo della vecchia chiave privata di CA.

Si procede alla generazione della nuova chiave secondo modalità identiche a quelle descritte nel paragrafo "Generazione della chiave privata della CA". Durante la procedura di rinnovo viene emesso un certificato contenente la nuova chiave pubblica firmato con la nuova chiave privata.

Il certificato generato verrà inviato a DigitPA come previsto dal comma 2 dell'art. 26 del DPCM 30 Marzo 2009.

9.4 Revoca del certificato della CA

In caso di provata compromissione della sua chiave privata di certificazione, la CA procederà alla revoca del proprio certificato.

Seguiranno alla revoca le seguenti azioni del Certificatore:

- notifica, entro 24 ore, l'avvenuta revoca a DigitPA e a tutti i titolari di certificati sottoscritti con la chiave privata di certificazione appartenente alla coppia revocata;
- revoca di tutti i certificati sottoscritti con la chiave compromessa.

9.5 Termine dell'attività della CA

In caso di termine dell'attività, la notifica dell'eventuale cessazione del servizio di Certificazione sarà comunicata agli utenti titolari almeno 60 giorni prima rispetto alla data prevista per la cessazione.

Gli utenti titolari verranno inoltre informati che tutti i certificati ancora validi al momento di termine del Servizio di Certificazione saranno revocati, assicurando tuttavia la conservazione dei dati relativi per un periodo di almeno 20 anni a partire da tale data.

Con lo stesso preavviso, il Certificatore notifica a DigitPA la data della cessazione, dando indicazione dell'eventuale altro depositario del registro dei certificati e della relativa documentazione.

9.6 Il giornale di controllo

I sistemi utilizzati presso il Certificatore registrano automaticamente i diversi eventi che si verificano; l'insieme di queste registrazioni costituisce il giornale di controllo secondo quanto richiesto dalla normativa vigente. Ogni evento viene registrato apponendo la data e l'ora di registrazione. Al termine della giornata i log vengono consolidati mediante l'apposizione di una marca temporale.

Le informazioni che compongono il giornale di controllo sono salvate su supporto non riscrivibile e custodite nei locali a più alta protezione della CA allo scopo di garantirne l'autenticità e la loro non alterabilità.

Periodicamente le registrazioni vengono verificate e poi archiviate in ambienti distinti da quelli del Certificatore per un periodo non inferiore a 20 anni.

Le informazioni raccolte comprendono:

- la generazione dei certificati;
- la personalizzazione dei dispositivi di firma;
- il rigetto delle richieste di certificazione;
- la revoca dei certificati;
- la sospensione dei certificati;
- l'annullamento della sospensione dei certificati;
- gli orari di entrata ed uscita dai locali protetti della CA del personale addetto alla funzione di generazione dei certificati;
- gli orari di inizio e fine delle sessioni di lavoro dedicate alla generazione dei certificati;
- qualunque modifica del contenuto del registro dei certificati;
- qualsiasi discordanza rilevata relativamente al contenuto del registro dei certificati tra la copia operativa e la copia di riferimento;
- la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

10 SERVIZIO DI VALIDAZIONE TEMPORALE

Il Servizio di Validazione Temporale (Time Stamping) di LISIT si rifà alle norme per la validazione temporale contenute nelle regole tecniche previste dalla normativa vigente.

La normativa prevede l'utilizzo di chiavi differenti per le operazioni di certificazione di chiavi di sottoscrizione da quelle utilizzate per la certificazione di chiavi di Marcatura Temporale, è stata quindi implementata una Certification Authority destinata a certificare le sole chiavi utilizzate per il Servizio di Validazione Temporale.

Il servizio di Time Stamping di LISIT consente di generare e conservare marche temporali da apporre ad un qualsiasi documento, quando questo venga richiesto dall'utente attraverso un'applicazione che supporta il servizio.

Per ottenere l'apposizione di una marca temporale dal servizio di Validazione Temporale di LISIT, l'utente può utilizzare le funzioni o gli strumenti messi a disposizione degli utenti da LISIT, come DigitalSign® – Edizione Lisit, oppure implementare in modo autonomo le funzioni necessarie per inoltrare adeguata richiesta di marca temporale in formato conforme allo standard di riferimento RFC 3161 “*Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)*”.

10.1 Generazione della chiave privata della Time Stamping Authority

Le chiavi di certificazione destinate alla sottoscrizione di certificati relativi a chiavi di marcatura temporale hanno lunghezza almeno pari a 2048 bit e sono generate dal Responsabile del servizio su dispositivi sicuri conformi ai requisiti richiesti dalla normativa vigente.

Il certificato relativo alle chiavi della Time Stamping Authority è pubblicato sul registro dei certificati all'atto della sua emissione.

Il certificato della Time Stamping Authority ha validità pari a 12 anni, 90 giorni prima della scadenza vengono avviate le procedure di rinnovo secondo modalità di certificazione incrociata identiche a quelle seguite per la sostituzione delle chiavi di certificazione della CA (vd. par. “Sostituzione della chiave privata della CA”).

10.2 Generazione delle chiavi di marcatura temporale

La procedura di generazione dei certificati utilizzati dai moduli di validazione temporale (Time Stamping Service o TSS) per l'emissione delle marche temporali è compiuta da personale specializzato della CA in ambienti ad elevato profilo di sicurezza e all'interno di sistemi dedicati (HSM).

Le chiavi di marcatura temporale certificate hanno lunghezza almeno pari a 1024 bit, prodotte con l'applicazione di algoritmi RSA.

All'atto della sua emissione il certificato è pubblicato nel registro dei certificati, consultabile in ogni momento per le operazioni di verifica delle marche temporali. Le chiavi prodotte sono quindi univocamente associate ai moduli di validazione temporale utilizzati dal servizio di marcatura temporale.

La validità del certificato di marcatura temporale è pari almeno a 6 anni, tuttavia in conformità a quanto stabilito nella normativa in vigore, per limitare il numero di marche temporali emesse con le stesse chiavi, il certificato del servizio di validazione temporale è rinnovato dopo non più di un mese di utilizzazione, indipendentemente dalla durata del suo periodo di validità e senza tuttavia essere revocato.

Il rinnovo del certificato implica la generazione di una nuova copia di chiavi secondo modalità del tutto identiche rispetto alla prima emissione.

10.3 Archiviazione delle marche temporali

Le marche temporali prodotte vengono conservate nel DB del servizio di Validazione Temporale di LISIT per un periodo pari alla durata del certificato corrispondente alle chiavi utilizzate per la loro sottoscrizione (6 anni); sono anche conservate per almeno 20 anni su supporto ottico non riscrivibile.

10.4 Riferimento temporale

I certificati relativi a chiavi di marcatura temporale sono regolamentati allo stesso modo dei certificati di firma digitale.

In base a quanto previsto dal art 37 comma 2 del DPCM 30 Marzo 2009, il Certificatore è tenuto a redigere un giornale di controllo contenente le registrazioni effettuate automaticamente dai dispositivi installati associate ad un riferimento temporale per la sua opponibilità verso terzi.

Il livello di precisione richiesto stabilisce che la differenza rispetto alla scala di tempo UTC (IEN) non deve superare il minuto primo.

Ai fini della sicurezza il Certificatore garantisce l'autenticità delle annotazioni contenuto nel giornale di controllo così da permetterne la ricostruzione di tutti gli eventi rilevanti annotati.

Il Certificatore si fa carico di verificare l'integrità del giornale di controllo con cadenza mensile ed assicura la conservazione delle annotazioni per un periodo non inferiore a 20 anni.

Tutti i sistemi del Certificatore LISIT sono allineati periodicamente con i suddetti riferimenti temporali tramite script schedulati sui sistemi stessi.

10.5 Validazione temporale

Vengono discusse in questo paragrafo le modalità di utilizzo del servizio di Marcatura Temporale del Certificatore LISIT.

Il processo di marcatura temporale permette di attribuire un riferimento temporale opponibile a terzi ad uno o più documenti informatici. Un riferimento temporale è inteso come una data ed un'ora certe validate mediante la generazione di una marca temporale (art. 1, comma 1, lett. f, g, h, i ed art. 43, comma 1 del DPCM 30 Marzo 2009).

Ciascuna marca temporale generata ed apposta su un documento è ad esso legata in modo indissolubile grazie ai seguenti riferimenti certi:

- impronta del documento (con l'indicazione dell'algoritmo impiegato) che rende univoca l'associazione dello stesso con la marca temporale;
- il numero progressivo seriale della marca che stabilisce l'univocità della stessa;
- la data e l'ora della richiesta della marca da parte dell'utente.

La procedura di validazione ha termine con la firma del TSS alla struttura dei dati sopra indicati e l'invio della stessa al richiedente. Tramite questo servizio, gli utenti possono associare ai loro documenti un riferimento temporale così da dimostrare la loro esistenza e con l'utilizzo della firma digitale darne validità legale.

Il servizio permette inoltre:

- di estendere la validità legale di un documento firmato digitalmente nel tempo oltre il periodo di validità del certificato di sottoscrizione utilizzato al momento (art. 51 del DPCM 30 Marzo 2009);
- di verificare la validità delle marche temporali presenti su documenti informatici in suo possesso.

Le marche temporali richieste vengono generate da un apposito servizio sicuro (Time Stamping Service) del Certificatore LISIT.

10.6 Modalità di emissione o verifica di marche temporali

Le richieste di emissione o verifica di marche temporali arrivano al TSS del certificatore tramite appositi applicativi software. Le marche temporali sono emesse con un tempo di risposta, calcolato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

Mediante DigitalSign ® – Edizione Lisit, l'utente può richiedere e verificare marche temporali direttamente al servizio TSS del Certificatore. Il servizio di TSS verificate le credenziale del richiedente genera le marche temporali e le invia al richiedente, allo stesso modo le marche temporali emesse sono verificate insieme alla correttezza della richiesta.

Il certificatore LISIT dispone inoltre di un toolkit software, conforme allo standard RFC 3161, con cui è possibile richiedere e verificare marche temporali. Questo toolkit permette l'integrazione delle funzionalità di richiesta e verifica di marche temporali in applicazione che ne hanno necessità.

Sia per l'applicativo client che per il toolkit, l'utente od il servizio possono richiedere la verifica della marca temporale associata ad un documento con estensione MIME.

Il processo di verifica predisposto dal Certificatore LISIT consente di verificare la firma del TSS (con la chiave pubblica corrispondente alla chiave privata usata per la generazione della marca) e il valore dell'impronta del documento contenuta nella marca attraverso il confronto con il valore dell'impronta inviato in fase di richiesta al TSS.

Il sistema di validazione temporale del Certificatore LISIT garantisce la conservazione delle marche temporali emesse in un archivio digitale non modificabile per un periodo di 20 anni.

10.6.1 Algoritmo di richiesta di marche temporali

Attraverso un apposito algoritmo di hash, l'utente può calcolare con il suo applicativo client l'impronta relativa all'evidenza informatica da sottoporre a validazione temporale ed inviare la sua richiesta al TSS del Certificatore LISIT.

10.6.2 Marche Temporali

In coerenza con la normativa vigente, il Certificatore si è basato sulle specifiche tecniche IETF (Request for Comment 3161), per le tematiche legate al protocollo di comunicazione TSP (Time Stamp Protocol) con il TSS e per definire il formato delle marche temporali nell'ambito del suo servizio di Validazione Temporale.

Riguardo al contenuto delle stesse marche temporali, di seguito si riportano tutte le informazioni presenti nei relativi certificati (art. 44, comma 1 del DPCM 30 Marzo 2009):

- identificativo della CA emittente: LISIT Time Stamp Authority;
- numero di serie della marca;
- algoritmo impiegato per la sottoscrizione della marca: RSA;
- identificativo del certificato relativo alla chiave pubblica di verifica della marca;
- data ed ora di generazione della marca;
- identificatore dell'algoritmo di hash impiegato per la generazione dell'impronta dell'evidenza informatica sottoposta a validazione temporale;
- valore dell'impronta dell'evidenza informatica.

10.6.3 Validità delle marche temporali

Le marche temporali hanno validità sino alla scadenza del certificato ad esse associato e per l'intero periodo di conservazione negli archivi del certificatore (art 49, comma 2 del DPCM 30 Marzo 2009).

10.7 Il sistema di Validazione Temporale

Il sistema di Validazione Temporale viene verificato dal personale del Certificatore attraverso un sistema di monitoraggio interno che consente un continuo controllo delle fonti di riferimento temporale. Mediante un dispositivo di TIME CHECK tramite protocollo SMNP viene confrontato il riferimento temporale dell'elemento di rete monitorato con quelli provenienti da terze parti come lo IEN Galileo Ferraris. Eventuali anomalie o correzioni sono annotate su supporto non riscrivibile (art. 48, comma 1 e 2 del DPCM 30 Marzo 2009), le anomalie possono essere:

- asincronismo con la fonte esterna di riferimento (IEN);
- differenza oraria maggiore o uguale ad un minuto primo;

- indisponibilità o manomissione del supporto non riscrivibile;
- tentativo di sabotaggio del sistema.

Al verificarsi dei suddetti accadimenti, il personale autorizzato provvede al blocco del sistema ed alla sua pronta risoluzione (art. 48, comma 2 del DPCM 30 Marzo 2009).

Il sistema di Validazione Temporale del Certificatore è conforme ai requisiti di sicurezza previsti dal livello di valutazione E2 e di robustezza HIGH dell'ITSEC (art. 48, comma 3 DPCM 30 Marzo 2009).

11 MISURE DI SICUREZZA

Il Servizio di Certificazione di LISIT è erogato nel rispetto dei più elevati standard di sicurezza; LISIT ha approntato un sistema di sicurezza che prevede la protezione della rete, la protezione delle macchine, la protezione dei locali, la protezione e l'integrità dei dati nonché la continuità del servizio grazie al ricorso a misure di sicurezza di tipo tecnologico e organizzativo.

L'intera infrastruttura tecnologica interessata per l'erogazione del servizio di certificazione è sita in locali dotati di speciali sistemi di controllo accessi e di videosorveglianza. L'ingresso ai locali della CA è consentito solo a personale dedicato e specializzato, previa sua identificazione. Ogni ingresso ed uscita è registrato sul giornale di controllo.

La CA si avvale di personale qualificato e con provata esperienza, dotato di requisiti di onorabilità così come richiesto dall'attuale legislazione ed organizzato secondo una precisa ripartizione delle competenze e delle responsabilità.

L'insieme delle procedure operative del Certificatore e delle misure di sicurezza da questo adottate sono soggette a periodiche visite ispettive: il fine è quello di verificare la reale e corretta applicazione delle procedure dichiarate, il rispetto di misure essenziali di sicurezza, il grado di affidabilità e stabilità offerto dal servizio.

11.1 Procedure di gestione degli eventi catastrofici

Per ovviare al rischio di malfunzionamento dell'intera infrastruttura e assicurare continuità al servizio erogato, è stato predisposto un piano di gestione delle situazioni di emergenza con particolare attenzione alle contromisure adottabili in caso di calamità naturali o dolo per il ripristino e la salvaguardia del servizio.

Nell'eventualità di un disastro che renda inutilizzabile il sito principale, si è previsto di predisporre, in un sito fisicamente separato, un'infrastruttura dotata di misure di sicurezza e apparecchiature analoghe a quelle della PKI LISIT da utilizzare fino al ripristino dell'ambiente principale per minimizzare i rischi di ritardo o di indisponibilità del servizio.

Allo scopo, in funzione dell'impatto derivante da un eventuale disastro, sono stati individuati alcune funzionalità del servizio di certificazione che rappresentano e/o assolvono a funzioni critiche irrinunciabili, quali:

- la sospensione/annullamento sospensione e la revoca dei certificati emessi;
- l'emissione e la pubblicazione delle CRL/CSL.

In considerazione dell'evento verificatosi verrà predisposto un piano per ripristinare l'operatività delle altre funzionalità.

In ossequio alle disposizioni della normativa vigente è stato redatto un Piano della Sicurezza consegnato a DigitPA, nel quale vengono dettagliate le procedure di gestione dei disastri, l'analisi dei rischi possibili e delle contromisure adottate per vanificarne l'impatto.

12 PROTEZIONE DEI DATI

In considerazione della grande importanza attribuita alla tematica della sicurezza nel trattamento dei dati in Lombardia Integrata è operativo un sistema organizzativo e normativo interno che garantisce riservatezza, integrità e disponibilità delle informazioni, inoltre assicura anche che tutti i trattamenti di dati personali si svolgano nel rispetto delle disposizioni di legge vigenti e dei principi di correttezza e liceità dichiarati nel codice etico di LISIT.

Nell'ambito delle policy di sicurezza aziendale sono state sviluppate soluzioni tecniche ed organizzative per la protezione dei dati trasmessi e conservati sulla rete e sui sistemi aziendali, fra cui rientrano:

- sviluppo sicuro di servizi e architetture;
- gestione dei backup;
- tracciamento dell'operatività del personale;
- gestione e profilazione dell'utenza;
- gestione del personale;
- gestione delle terze parti;
- classificazione e gestione della documentazione;
- gestione della rete e dei sistemi;
- gestione dell'operatività dei sistemi e capacity planning;
- sicurezza fisica;
- metodologie di vulnerability assessment e risk analysis;
- monitoraggio della rete e dei sistemi per la prevenzione ed il contrasto degli incidenti di sicurezza;
- gestione della continuità del business.

Il complesso delle misure di sicurezza previste e messe in atto dal sistema implementato da Lombardia Integrata incorpora anche le misure minime previste dal D.Lgs. 196/03 Codice per la protezione dei dati personali.

Tale sistema si caratterizza per alcune importanti elementi di base, fra i quali si ricordano i seguenti:

- i dipendenti che hanno ricevuto la nomina di incaricati ai sensi dell'art. 30 del DL 196/03, hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali;
- il trattamento dei dati personali avviene sotto la supervisione del responsabile del trattamento;
- apposite funzioni aziendali hanno il compito di definire le policy per la sicurezza delle informazioni e di verificare, con l'ausilio di funzioni di auditing interno, che esse siano effettivamente applicate;
- il sistema di policy si basa sulla corretta classificazione degli asset. Con l'ausilio di strumenti di risk assessment, sono individuate le misure di sicurezza più idonee alla tutela dei singoli asset, alla definizione dei controlli e all'applicazione dei sistemi di monitoraggio e verifica più appropriati;
- la tutela dei dati personali non si configura come un processo indipendente, ma risulta del tutto integrato nella gestione corrente della sicurezza degli asset aziendali;
- le politiche di sicurezza fisica e di tutela del patrimonio materiale dell'azienda e le politiche di gestione degli incidenti di sicurezza e delle crisi sono definite tenendo presenti i principi di tutela dei dati personali e le necessità di protezione di questi dati fissate dalla legge.

12.1 Modalità di Protezione dei Dati

Il presente capitolo del Manuale Operativo ha lo scopo di illustrare le procedure e le modalità operative adottate dal Certificatore per il trattamento dei dati personali, nello svolgimento della propria attività di certificazione. I dati personali, relativi al richiedente la registrazione, al titolare di certificati, al terzo interessato e a chiunque acceda al servizio, sono trattati, conservati e protetti dal Certificatore conformemente a quanto previsto dal Decreto legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali".

La terminologia utilizzata nel presente capitolo è conforme a quella adottata dal DL 196/03, e parzialmente difforme da quella utilizzata nel D.lgs 82/2005 e nel DPCM 30 Marzo 2009. In particolare:

- per Titolare, si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza (ovvero il Certificatore);
- per Responsabile si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal Titolare al trattamento di dati personali;
- per Incaricato si intende la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile;

- per “Interessato”, si intende la persona fisica, la persona giuridica, l’ente o l’associazione cui si riferiscono i dati personali (ovvero il richiedente la registrazione, il titolare di certificati, il terzo interessato o chiunque acceda al servizio).

In particolare, il Certificatore:

- individua e nomina i funzionari Incaricati del trattamento dei dati (ovvero gli Incaricati dell’Identificazione e quanti altri tratteranno i dati attinenti il servizio del Responsabile del Servizio, attenendosi alle istruzioni impartite, ai sensi dell’Art. 30 del DL 196/03;
- nomina eventuali Responsabili esterni per il trattamento dei dati specificando analiticamente i compiti per iscritto ed effettua, anche tramite verifiche periodiche, controlli sulla puntuale osservanza delle disposizioni di legge e delle proprie istruzioni.

12.2 Definizione e identificazione di “Dati personali”

Ai sensi dell’Art. 1, comma 2, lett. b) del DL 196/03, per dato personale si intende “qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”; pertanto sono dati personali anche i codici identificativi forniti dal Certificatore, i puntatori e i PIN. Dati personali potranno inoltre essere quelli relativi all’utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi - elettronici o cartacei - di registrazione, di richiesta di sospensione e di riabilitazione, di revoca, di cambio anagrafica e nei certificati, di cui ai relativi capitoli del presente Manuale Operativo. Al fine di garantirne un trattamento adeguato, le misure di sicurezza predisposte dal Certificatore e analiticamente descritte nel Piano per la Sicurezza, sono realizzate conformemente a quanto previsto dal DL 196/03.

12.3 Tutela e diritti degli interessati

In materia di trattamento dei dati personali il Certificatore garantisce la tutela degli interessati in ottemperanza al DL 196/03. In particolare:

- agli interessati sono fornite le necessarie informazioni ai sensi dell’Art. 13 (quali ad esempio il titolare, le modalità e finalità del trattamento, l’ambito di comunicazione e di diffusione, nonché i diritti di accesso ai suoi dati ai sensi dell’Art. 7);
- agli interessati viene richiesto, laddove necessario, il consenso scritto al trattamento dei propri dati personali.

12.4 Applicazione del Codice per la protezione dei dati personali

12.4.1 Adempimenti generali

Dal punto di vista generale il Certificatore:

- predisporre, conserva e aggiorna, nell’ambito delle attività di certificazione, un Registro degli Archivi Informatici e Cartacei contenenti dati personali di cui è titolare e/o responsabile e che vengono utilizzati nella gestione di tutte le fasi dell’attività di certificazione;
- definisce e aggiorna i compiti dei suoi incaricati in relazione al trattamento degli archivi suddetti, in conformità con le misure minime di sicurezza previste dal DL 196/03 (Titolo V, capi I e II) e riportate nel Piano per la Sicurezza, nonché con le policy aziendali in materia di sicurezza e di tutela della riservatezza dei dati.

12.4.2 Adempimenti tecnici ed organizzativi

Dal punto di vista tecnico il Certificatore, tramite i suoi incaricati, adotta gli opportuni provvedimenti in relazione alla registrazione, elaborazione, conservazione, protezione dei dati personali, cancellazione/distruzione, secondo le modalità indicate qui di seguito.

12.4.3 Registrazione

- garantisce la conservazione dei dati tecnici relativi a struttura e formato degli archivi informatici e cartacei contenenti dati personali, nonché alla loro locazione fisica;
- supervisiona l'organizzazione e classificazione in maniera univoca degli archivi, nonché delle loro copie di sicurezza (backup) curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Certificatore. In proposito, si precisa che, a fronte di eventi che dovessero compromettere la capacità operativa del Certificatore presso la principale sede di attività, è definito un Piano Operativo che garantisce la disponibilità del registro dei certificati e le funzionalità di revoca e sospensione dei certificati in corso di validità;
- supervisiona l'organizzazione e classificazione in maniera univoca dei moduli di registrazione, accettazione, richiesta sospensione e riabilitazione, richiesta revoca, cambio anagrafica e qualsivoglia altro documento contenente dati personali, curando di ridurre al minimo indispensabile le copie, totali o parziali, di ciascun archivio secondo le modalità descritte nel Piano per la Sicurezza del Certificatore.

12.4.4 Elaborazione

- controlla che l'elaborazione dei suddetti archivi e dei dati personali in essi contenuti sia effettuata esclusivamente per le finalità indicate nell'informativa resa ai sensi dell'Art. 13 del DL 196/03;
- verifica, in funzione del tipo di elaborazione, i formati di output e la destinazione finale dei dati al fine di garantirne la protezione, secondo quanto previsto nel seguito;
- rileva l'eventuale generazione di nuovi archivi nell'ambito delle fasi di elaborazione, supervisionando la loro classificazione.

12.4.5 Conservazione

- supervisiona la classificazione degli eventuali archivi – e dei dati in essi contenuti - soggetti a pura e semplice conservazione (archivi storici e/o di backup), riportando la durata della conservazione (inclusa data iniziale e finale), la natura del supporto e la sede di conservazione;
- si assicura che siano trattati come archivi di conservazione dei dati personali tutti gli archivi appartenenti a procedure temporaneamente bloccate o sospese;
- verifica che le procedure di conservazione di tutti i documenti utilizzati all'interno dell'attività di certificazione siano coerenti con la tutela dei dati personali.

12.4.6 Cancellazione/Distruzione

- verifica la registrazione - eventualmente in maniera automatizzata - della cancellazione/distruzione di singoli dati personali dagli archivi, riportando la tipologia dei dati, l'archivio interessato, la data di cancellazione/distruzione, nonché l'origine della cancellazione/distruzione (su richiesta dell'interessato, procedurale, accidentale, ecc.);
- verifica la registrazione della cancellazione/distruzione di archivi interi, secondo le modalità illustrate al punto precedente ed in conformità a quanto previsto dal DL 196/03, curando inoltre l'aggiornamento del Registro degli Archivi Informatici e Cartacei.

12.4.7 Protezione

- protegge la confidenzialità dei dati personali stabilendo le modalità di accesso agli archivi informatici e cartacei da parte dei soggetti abilitati appartenenti all'organizzazione del Certificatore. In particolare:
 - o classifica i soggetti abilitati all'accesso in funzione delle loro mansioni. In particolare, si precisa che il Certificatore ha definito ed attua specifiche policy di gestione delle credenziali di autenticazione e per la costruzione e l'utilizzo delle password;
 - o registra le modalità di protezione dei dati, sia per quanto concerne la sicurezza logica degli archivi informatici (software di sicurezza, modalità di generazione del log delle elaborazioni, ecc.) che fisica (vigilanza dei locali, archiviazione documenti, gestione delle copie di sicurezza);
 - o assicura la confidenzialità dei dati personali contenuti nei diversi formati di output delle fasi di elaborazione (cartacei, su terminale, ecc.) stabilendo le modalità operative necessarie, sia manuali che automatizzate;
 - o supervisiona la circolazione interna delle informazioni contenute negli stampati (tabulati) o in altri supporti;
 - o assicura la distribuzione degli output su terminale in accordo con i profili utente designati dal responsabile della sicurezza;
- protegge l'integrità dei dati singolarmente considerati e degli archivi nel loro insieme, durante tutte le fasi di trattamento, stabilendo le modalità operative necessarie, sia manuali che automatizzate;

- garantisce la disponibilità dei dati, affinché il titolare possa adempiere alle richieste di consultazione/verifica da parte degli interessati previste dalla normativa vigente.

Ulteriori modalità di trattamento dei dati, oltre quella prevista dal DL 196/03, potranno essere previste a livello contrattuale tra il Certificatore e l'organizzazione, pubblica o privata che richieda il rilascio di più certificati, per conto di sottoscrittori a lei afferenti. In questo caso, tali accordi sono riportati all'interno del contratto di acquisto dei certificati da parte dell'organizzazione medesima.

12.5 Circostanze di rilascio di dati personali

Fermo restando il diritto dell'interessato di richiedere ed ottenere dal Certificatore informazioni relative ai propri dati personali, secondo quanto previsto dall'Art. 7 del DL 196/03, il Certificatore, nello svolgimento delle proprie attività di certificazione, può effettuare operazioni di comunicazione e diffusione dei dati personali.

In particolare:

- i dati personali possono essere comunicati all'Autorità Giudiziaria, in conformità con quanto previsto dalla normativa vigente;
- ad esclusione di quanto previsto dal CAD e dal DPCM 30 Marzo 2009 in merito alla pubblicazione delle liste di revoca dei certificati, le motivazioni della revoca o sospensione dei certificati possono essere diffuse solo con il consenso esplicito dell'interessato.