Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.

Manuale Operativo per i Servizi Fiduciari di Firma Elettronica Qualificata

(Certification Practice Statement)

Revisione del Documento: **1.0**

Codice del Documento: **ARIA-CA-CPS#01**

Data revisione: **01-07-2019**

	Ruolo	Nome	Firma
Redatto da:	Responsabile dei Servizi di CA	Luigi Bongiorni	
	Responsabile del Servizio di Identificazione e Registrazione degli utenti	Doriana Pepoli	
Verificato da:	Responsabile del Servizio di Certificazione	Gianluca Gallia	
	Responsabile Auditing	Luigia Barile	
	Responsabile della Sicurezza	Alberto Gazzoli	
Approvato da:	Responsabile del Dipartimento Piattaforme Applicative	Simona Sabadei	
	Direttore Centrale Operations	Luigi Pellegrini	
	Direttore Servizi ICT	Roberto Soj	
	Presidente	Francesco Ferri	
Emesso da:	Responsabile dei Servizi di CA	Luigi Bongiorni	Firmato da: LUIGI BONGIORNI Codice fiscale: BNGLGU67B18G388A Valido da: 19-09-2017 15:57:53 a: 19-09-2020 02:00:00 Riferimento temporale: Marca Temporale (vedi le proprietà della firma)

Firmato da:
AgID
Email: it_tsl@agid.gov.it
Codice fiscale: VATIT-9773502058
Valido da: 01-12-2020 10:34:41 a: 14-01-2026 10:34:41
Certificato emesso da: AgID, Agenzia per l'Italia Digitale, IT
Riferimento temporale 'SigningTime': 13-01-2021 17:30:36
Approvo il documento

Indice dei Contenuti

1. Storia delle modifiche apportate

Numero versione	Data di emissione	Sintesi delle variazioni
1.0	**01/07/2019**	Prima emissione

1.1 Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione 1.0, emessa in data 01/07/2019, del Manuale Operativo per i Servizi Fiduciari di Firma Elettronica Qualificata dell'Azienda Regionale per l'Innovazione e gli Acquisti S.p.A. (nel seguito ARIA).

1.2 Regole per la pubblicazione degli aggiornamenti al Manuale Operativo

ARIA 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 ARIA ne darà notifica ad AgID e, previa ratifica della stessa, il Manuale Operativo aggiornato verrà pubblicato sul sito di AgID e sul sito di ARIA stessa.

Il presente documento, unitamente alle Policy dei Certificati, è comunque soggetto ad aggiornamento annuale.

2. Introduzione

La Firma Elettronica Qualificata (o Firma Digitale) è l'equivalente informatico della tradizionale firma autografa apposta su carta e, come disposto dall'art. 25 del Regolamento eIDAS, assume piena validità legale sia a livello nazionale che in tutti gli stati membri della Comunità Europea.

La firma elettronica qualificata è il risultato di un'operazione di cifratura e le tecnologie di crittazione utilizzate 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 elettronica qualificata 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 di firma elettronica qualificata 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 dall'Autorità di Certificazione (Certification Authority - CA), una terza parte fidata che emette il certificato di firma elettronica qualificata e vi appone la propria firma elettronica quale sigillo di affidabilità. L'emissione del certificato di firma elettronica qualificata da parte della CA avviene previa identificazione sicura del richiedente e registrazione dei suoi dati personali.

L'Autorità di Certificazione, inoltre, si occupa della gestione dell'intero ciclo di vita dei certificati emessi e della pubblicazione delle informazioni sulla situazione di validità o revoca dei certificati da esso rilasciati, così da consentire in ogni momento ad altri soggetti la verifica della validità delle firme e dell'integrità e provenienza di uno o più documenti informatici.

Ai soggetti che richiedono il rilascio di un certificato di firma elettronica qualificata viene attivato il servizio di validazione temporale, che consente di asseverare temporalmente le firme elettroniche qualificate e, in generale, qualunque tipo di documento elettronico.

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 ARIA nell'erogazione del servizio di firma elettronica qualificata.

Questo documento, definito nel seguito Manuale Operativo, è conforme allo standard di riferimento definito dall'IETF "RFC3647". Il nome per esteso col quale si deve citare questo documento è uno dei seguenti:

Manuale Operativo per i Servizi Fiduciari di Firma Elettronica Qualificata - Certification Practice Statement (CPS) dell'Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.

ARIA, in qualità di Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata, pubblica il presente Manuale Operativo in modo da permettere ai propri utenti di valutare il grado di affidabilità dei servizi offerti.

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.

Addetto PdA/PdR
Incaricato della Identificazione e della Registrazione degli Utenti Titolari.

Addetto PKI o Incaricato RA del Certificatore
Personale del Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata, incaricato all'amministrazione di tutte le utenze della CA.

AgID
Agenzia per l'Italia Digitale, Organismo di Vigilanza ai sensi dell'articolo 17 del regolamento (UE) N. 910/2014, che è responsabile dei compiti di vigilanza sui prestatori di servizi fiduciari qualificati italiani.

ARIA
Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.

ASST
Aziende Socio-Sanitarie Territoriali.

ATS
Agenzie di tutela della salute.

Autorità di Certificazione (CA)
Soggetto che presta servizi fiduciari di certificazione (creazione e assegnazione di certificati elettronici) ed altri servizi correlati (per es. gestione del ciclo di vita dei certificati). In particolare, la CA di ARIA svolge le attività di gestione del ciclo di vita (sospensione, revoca, riattivazione) e conservazione dei certificati emessi.

Autorità di Validazione Temporale (TSA)
Soggetto che presta il servizio fiduciario di validazione temporale (emissione di marche temporali).

Banca Dati dei Certificati o Directory Service (DS)
Archivio elettronico conforme allo standard ITU-T X.500 dove la CA pubblica i certificati elettronici emessi e la lista dei certificati revocati o sospesi. È un servizio pubblico che fornisce la possibilità di disporre 'on-line', tramite protocollo ldap o http, delle informazioni necessarie alla verifica della validità dei certificati elettronici a norma dell'art. 24, comma 2, lettera k del Regolamento (UE) n. 910/2014.

Carta Nazionale dei Servizi (CNS) o Carta Regionale dei Servizi (CRS)
Tessera personale in possesso di tutti i cittadini iscritti al Servizio Sanitario Nazionale. Si tratta di una carta elettronica che garantisce il riconoscimento on-line dell'utente e che può essere usata per eseguire operazioni crittografiche quali la firma elettronica e la cifratura/decifratura dei documenti.

Carta SISS o carta operatore
Smartcard di firma elettronica qualificata rilasciata agli utenti Titolari.

Certificate Revocation List o lista dei certificati revocati (CRL)
Elenco in formato standard ITU-T X.509 dei certificati elettronici rilasciati dalla CA che risultano revocati o sospesi, e che quindi non sono considerati più validi dalla stessa autorità emittente. La CRL è pubblicata sulla Banca Dati dei certificati (Directory Service) della CA, è firmata elettronicamente e aggiornata dalla CA, che si occupa anche di asseverarla temporalmente.

Certification Practice Statement (CPS)
Definito anche *Manuale Operativo (MO)*, è il documento che definisce le metodologie e le politiche impiegate dal Prestatore dei Servizi Fiduciari nell'erogazione dei servizi di Firma Elettronica Qualificata. Il Manuale Operativo può essere utilizzato dai TITOLARI e dagli UTENTI UTILIZZATORI per valutare l'affidabilità delle procedure utilizzate dal Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata nell'emettere e gestire le chiavi e i certificati di firma elettronica qualificata. Il MO deve essere reso pubblico.

Certificate Policy (CP)
Un insieme di regole che descrivono l'applicabilità di una classe di certificati, identificati da un unico Policy OID, aventi requisiti di sicurezza comuni. Le policy dei certificati possono essere utilizzate dagli Utente Utilizzatore per decidere se fidarsi o meno di quel dato certificato, della chiave pubblica ad esso associata, o di qualsiasi firma elettronica apposta tramite l'utilizzo della corrispondente chiave privata.

Certificato di autenticazione e cifratura
Attestato elettronico che collega una persona fisica ad altri dati elettronici utilizzati come metodo di autenticazione o cifratura informatica.

Certificato di firma elettronica
Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona.

Certificato qualificato di firma elettronica
Certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del regolamento (UE) N. 910/2014.

Certificato CNS
Certificato di autenticazione e firma elettronica emesso su Carta Nazionale dei Servizi (CNS/CRS) da un Prestatore di Servizi Fiduciari iscritto nella TSL nazionale e corrispondente al Policy OID "1.3.76.16.2.1".

Conformity Assessment Body (CAB)
Organismo di valutazione di conformità accreditato da Organismi di accreditamento riconosciuti dagli Stati membri (ETSI EN 319 403). Per l'Italia l'organismo di accreditamento è Accredia.

Chiavi asimmetriche
Coppia di chiavi crittografiche, una privata e una pubblica, correlate tra loro, utilizzate nei sistemi di validazione dei documenti informatici.

Chiave privata
Elemento della coppia di chiavi asimmetriche, destinato ad essere utilizzato soltanto dal soggetto Titolare, mediante il quale si appone la firma elettronica su documenti elettronici.

Chiave e pubblica
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/Emergenza
Codice segreto attribuito all'utente Titolare e utile alla sua identificazione durante la procedura di sospensione dei certificati.

Conservazione digitale a norma
Insieme delle attività finalizzate alla conservazione dei documenti informatici atte a garantirne l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità nel tempo, come previsto dall'articolo 44 del D.lgs. n° 82/2005 Codice dell'Amministrazione Digitale [2].

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

Codice unico presso il Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata
Codice utile all'identificazione univoca dell'utente all'interno del dominio del Prestatore dei Servizi Fiduciari; questo codice viene generato e consegnato all'utente durante la fase di registrazione, è inoltre contenuto nel *dnQualifier* del certificato di firma elettronica qualificata.

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. È un database pubblico che fornisce la possibilità di disporre "on-line", tramite protocollo LDAP, delle informazioni necessarie alla verifica della firma.

Distinguished Name (DN)
Insieme di attributi conformi allo standard ITU-T X.500 che identificano univocamente un'entità.

Documento Elettronico
Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.

eIDAS
electronic IDentification, Authentication and Signature, ovvero l'insieme di tutti i servizi fiduciari disciplinati a livello europeo attraverso il Regolamento (UE) N. 910/2014.

Elenco di Fiducia
Elenco istituito, mantenuto e pubblicato dall'Organismo di Vigilanza di ciascun Stato membro, che riporta informazioni relative ai Prestatori di Servizi Fiduciari Qualificati e non Qualificati per cui lo Stato membro è responsabile, unitamente alle informazioni relative ai Servizi Fiduciari Qualificati e non Qualificati da essi prestati.

EEPA
Ente Erogatore Privato Accreditato

Firma Elettronica
Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

Firma Elettronica Avanzata
Firma elettronica che soddisfi i requisiti di cui all'articolo 26 del regolamento (UE) N. 910/2014.

Firma Elettronica Qualificata
Firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. La firma digitale è una firma elettronica qualificata.

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.

HD
Help Desk

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. È 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.

IRCCS
Istituti di Ricovero e Cura a Carattere Scientifico.

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 contente 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 banca dati dei certificati ed effettuare tutte le operazioni di prelievo certificato, verifica CRL eccetera.

LISIT
Lombardia Integrata - Servizi Infotelematici per il Territorio

LISPA
Lombardia Informatica S.p.A.

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

PEC - Posta Elettronica Certificata
Sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi.

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

Policy dei Certificati
Documento, o l'insieme dei documenti, che definisce le caratteristiche e l'affidabilità dei certificati corrispondenti all'identificativo della policy stessa. Scopo del documento è quello di fornire all'UTENTE UTILIZZATORE le informazioni necessarie alla verifica dell'idoneità dei certificati utilizzati in un determinato cotesto applicativo.

Portale CA o Portale PdR
Servizio erogato in modalità Web-Browsing attraverso cui vengono rese disponibili funzioni relative alla gestione del materiale crittografico e delle utenze CA degli Utenti Titolari.

Portale PdA o Servizio di Provisioning
Servizio erogato in modalità Web-Browsing attraverso cui gli Addetti PdA PdR registrano gli Utenti Titolari alla CA, gestiscono il ciclo di vita dei certificati (revoche, sospensioni e riattivazioni).

Punti di Adesione e Registrazione (PdA/PdR) o Registration Authority (RA)
Uffici preposti alle operazioni di identificazione e registrazione dei TITOLARI, di emissione dei dispositivi sicuri per la creazione di firme elettroniche qualificate, e all'invio verso la CA delle richieste di revoca, sospensione e annullamento della sospensione dei certificati elettronici dei TITOLARI.

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.

PKI Disclosure Statement (PDS) o Dichiarazione di Trasparenza dell'Autorità di Certificazione
Documento a supporto degli utenti per il reperimento di tutte le informazioni necessarie alla verifica delle procedure operative e politiche di sicurezza adottate dal Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata nell'erogazione dei servizi di Certificazione.

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

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.

Servizi Fiduciari di Firma Elettronica Qualificata
Servizi di Firma Elettronica Qualificata che soddisfano i requisiti pertinenti stabiliti nel regolamento (UE) N. 910/2014. Tali servizi consistono nella creazione, verifica e convalida di firme elettroniche, verifica e convalida di sigilli elettronici, validazioni temporali e certificati relativi a tali servizi.

Servizi PdA PdR
Si intendono l'insieme dei servizi erogati attraverso il Portale CA e il Servizio di Provisioning.

SSCD Secure Signature-Creation Device
Dispositivo sicuro per la creazione di firme elettroniche qualificate conforme all'allegato III della Direttiva 1999/93/CE.

QSCD Qualified Signature-Creation Device
Dispositivo sicuro per la creazione di firme elettroniche qualificate conforme all'allegato I del Regolamento (UE) n. 910/2014.

Terzo Interessato
La persona fisica o giuridica il cui consenso è necessario per autorizzare il Titolare a richiedere i servizi fiduciari e che, eventualmente, può specificare la sussistenza di poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite dal Titolare nell'ambito di propria competenza.

TSA
Time Stamping Authority. Autorità di Validazione Temporale Elettronica che emette le marche temporali.

TSU
Time Stamping Unit, ovvero HSM contenente la coppia di chiavi di firma ad uso del sistema di Validazione Temporale.

URL –Uniform Resource Locator
Modalità semantica per indirizzare un oggetto su INTERNET.

Utente Titolare o Titolare
Persona fisica che usufruisce dei servizi fiduciari di Firma Elettronica Qualificata.

Utente utilizzatore
«Parte facente affidamento sulla certificazione», ovvero una persona fisica o giuridica che fa affidamento su un servizio fiduciario.

Marca Temporale o Validazione Temporale Elettronica
È il risultato di una procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibile a terzi entro i confini nazionali.

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

[1] Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e successive modifiche ed integrazioni.

[2] Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[3] D.Lgs. n° 82/2005 [CAD]: Codice dell'amministrazione digitale e successive modifiche ed integrazioni.

[4] D.Lgs. n.196 del 30 giugno 2003: Codice in materia di protezione dei dati personali e s.m.i.

[5] D.P.C.M. del 22 febbraio 2013: Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71.

[6] Deliberazione CNIPA 45/2009 del 21 maggio 2009: Regole per il riconoscimento e la verifica del documento informatico e successive modifiche ed integrazioni.

[7] Determinazione AgID 121/2019 del 4 giugno 2019: "Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate." come modificata dalla Determinazione AgID 147/2019 del 17 maggio 2019 e successive modifiche ed integrazioni.

[8] Determinazione AgID 185/2017 del 23 giugno 2017: "Emanazione del regolamento recante le modalità con cui i soggetti che intendono avviare la prestazione di servizi fiduciari qualificati presentano all'AgID domanda di qualificazione ai sensi dell'art. 29 del decreto legislativo 7 marzo 2005, n. 82." che sostituisce la Circolare n.48/2005.

[9] Atto esecutivo (UE) 2015/1506 dell'8 settembre 2015: DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[10] Atto esecutivo (UE) 2015/1505 dell'8 settembre 2015: DECISIONE DI ESECUZIONE (UE) 2015/1505 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[11] Atto esecutivo (UE) 2015/1502 dell'8 settembre 2015: REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

[12] Atto esecutivo (UE) 2015/1501 dell'8 settembre 2015: REGOLAMENTO DI ESECUZIONE (UE) 2015/1501 DELLA COMMISSIONE dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

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 Documentazione di riferimento

[1] Dichiarazione di Trasparenza o PKI Disclosure Statement - PDS di ARIA.
[2] Condizioni di Fornitura dei Servizi Fiduciari di Firma Elettronica Qualificata.
[3] Policy dei Certificati di Firma Elettronica Qualificata emessi su Carte Firma - OID: 1.3.6.1.4.1.7790.1.4.22
[4] Policy dei Certificati di Firma Elettronica Qualificata emessi su Carte SISS - OID: 1.3.6.1.4.1.7790.1.4.32
[5] Policy dei Certificati di Firma Elettronica Qualificata emessi su Carte SISS - OID: 1.3.6.1.4.1.7790.1.4.33
[6] Policy dei Certificati di Firma Elettronica Qualificata emessi su CRS/CNS - OID: 1.3.6.1.4.1.7790.1.4.23

4.3 Standard di riferimento

I certificati descritti nel presente documento sono conformi agli standard di riferimento internazionali (X509, RFC 5280) e agli standard individuati dalla Commissione Europea in materia di Firma Elettronica Qualificata:

[7] ETSI EN 319 401 - General Policy Requirements for Trust Service Providers.
[8] ETSI EN 319 411-1 - Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
[9] ETSI EN 319 411-2 - Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
[10] ETSI EN 319 412-1 - Certificate Profiles; Part 1: Overview and common data structures.
[11] ETSI EN 319 412-2 - Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;
[12] ETSI EN 319 412-5 - Certificate Profiles; Part 5: QCStatements.
[13] ETSI TS 119 312 - Cryptographic Suites.
[14] CA/Browser Forum Guidelines (http://www.cabforum.org)

Per quanto concerne i requisiti di sicurezza specifici dei dispositivi sicuri per la firma elettronica qualificata (SSCD) si indica la conformità allo standard “CWA 14169 (March 2002) Secure Signature-Creation Device EAL 4+”. I dispositivi di firma elettronica qualificata rilasciati agli utenti sono considerati anche QSCD a norma dell’art 51, comma 1 del Regolamento (UE) N. 910/2014.

4.4 Sistema di gestione per la Qualità e la Sicurezza delle Informazioni

ARIA mantiene attivo, aggiornato e documentato un **Sistema di Gestione per la Qualità e per la Sicurezza delle Informazioni** certificato secondo gli standard **ISO 9001** e **ISO 27001** per il campo di applicazione “*Progettazione, gestione ed assistenza del servizio di certificazione e firma digitale*“, al fine di assicurarne la conformità ai requisiti specificati e che le attività vengano svolte nel rispetto della Sicurezza delle Informazioni.

5. Generalità dei Servizi Fiduciari

A partire dal primo luglio 2019, in seguito all'approvazione della Legge Regionale della Regione Lombardia N°27 del 27/03/2019 che ha decretato il **cambio di denominazione del Certificatore Qualificato Lombardia Informatica** S.p.A. in **ARIA - Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.** e la conseguente incorporazione per fusione dell'Azienda Regionale Centrale Acquisti S.p.A. (ARCA), **ARIA subentra a Lombardia Informatica nella gestione dei servizi fiduciari di Firma Elettronica Qualificata** che soddisfano i requisiti stabiliti nel Regolamento (UE) N. 910/2014 (detto anche "Regolamento eIDAS").

Tali servizi consistono nella creazione di firme elettroniche qualificate, verifica e convalida di firme elettroniche e validazioni temporali elettroniche, gestione del ciclo di vita dei certificati relativi a tali servizi.

ARIA, come certificatore qualificato subentrato a Lombardia Informatica, **non eroga i servizi fiduciari di emissione certificati e di generazione marche temporali**, ma in ottemperanza alle vigenti disposizioni di legge, garantisce:

- la gestione del ciclo di vita di tutti i certificati digitali emessi da Lombardia Informatica sino alla scadenza o alla revoca degli stessi;
- la conservazione delle marche generate da Lombardia Informatica fino alla cessazione del servizio per almeno 20 anni a partire dalla loro emissione, in modo da preservarne la validità nel tempo;
- la custodia e la gestione di tutte le informazioni necessarie al mantenimento del corretto funzionamento dei servizi erogati (banca dati dei certificati e relativa documentazione) per il periodo di tempo prescritto dalla normativa vigente in materia, adempiendo agli obblighi e alle responsabilità previste dalle condizioni di fornitura dei servizi.

In questo capitolo vengono fornite informazioni utili all'identificazione del Manuale Operativo di ARIA e di tutte le parti interessate, nonché le modalità operative e le politiche di sicurezza adottate da ARIA nell'erogazione dei servizi fiduciari.

Nel seguito del presente documento, ci si riferirà ad ARIA in qualità di Prestatore dei servizi fiduciari di Firma Elettronica Qualificata a norma del regolamento eIDAS.

5.1 Identificazione del Manuale Operativo

Questo documento è pubblicato e liberamente scaricabile in formato PDF/A dal sito di ARIA, ai seguenti indirizzi (URL): *https://www.ariaspa.it/CA/CPS* e *https://www.lispa.it/CA/CPS* ed è reso disponibile h24, 7 giorni su 7.

In caso di indisponibilità del servizio di pubblicazione causato da guasti o anomalie di sistema, ARIA ne garantisce il ripristino entro le 8 ore successive alla rilevazione del disservizio.

Del documento pubblicato a questi indirizzi viene garantita l'integrità e l'autenticità. L'URL dove questo documento è pubblicato, è reperibile nell'estensione **certificatePolicies** (OID: 2.5.29.32) dei certificati che fanno riferimento a questa Certification Practice Statement – CPS.

Il presente documento è depositato anche presso AgID.

5.2 Identificazione della tipologia dei certificati

5.2.1 Certificati di firma elettronica qualificata

Le policy (CP) dei certificati di firma elettronica qualificata sono conformi alla Deliberazione CNIPA n. 45/2009 e sono descritte in appositi documenti pubblicati ai seguenti indirizzi (URL) *https://www.ariaspa.it/CA/CPS* e *https://www.lispa.it/CA/CPS* e sono identificate dagli OID presenti nell'attributo policy identifier dell'estensione **certificatePolicy** (OID 2.5.29.32) dei certificati stessi.

Di seguito si riporta l'elenco dei policy OID dei certificati di firma elettronica qualificata in gestione ad ARIA:

Certificati di Firma Elettronica Qualificata emessi su Carte Firma	1.3.6.1.4.1.7790.1.4.22
Certificati di Firma Elettronica Qualificata emessi su Carte Operatore SISS	1.3.6.1.4.1.7790.1.4.32

Certificati di Firma Elettronica Qualificata emessi su Carte Operatore SISS	1.3.6.1.4.1.7790.1.4.33
Certificati di Firma Elettronica Qualificata emessi su CRS/CNS	1.3.6.1.4.1.7790.1.4.23

Queste policy sono parte integrante del Manuale Operativo di ARIA e delle Condizioni Contrattuali del servizio di Firma Elettronica Qualificata.

Il Prestatore di Servizi Fiduciari ARIA è registrato presso IANA (www.iana.org) con l'OID**: 1.3.6.1.4.1.54110** (mentre l'OID con cui è registrata Lombardia Informatica è 1.3.6.1.4.1.7790).

I certificati di certificazioni delle CA gestite da ARIA sono contenuti nella Trusted List (TL) Italiana gestita da AgID e pubblicata alla seguente URL: *https://eidas.agid.gov.it/TL/TSL-IT.xml*.

5.3 Responsabile del documento

Il responsabile del presente documento è il Dott. Luigi Bongiorni contattabile tramite i riferimenti di seguito riportati:

e-mail	*luigi.bongiorni@ariaspa.it*
PEC	*luigi.bongiorni@pec.ariaspa.it*
Telefono	+39 02-39331296
Fax	+39 02-93660225

5.4 Prestatore dei Servizi Fiduciari

Si riportano di seguito i riferimenti del Prestatore dei Servizi Fiduciari:

Denominazione sociale	Azienda Regionale per l'Innovazione e gli Acquisti S.p.A.
Indirizzo della sede legale	Via Torquato Taramelli, 26 20124, Milano
Rappresentante Legale	Il Presidente *pro tempore*
N° Partita IVA	05017630152
N° di telefono	+39 02-39331.1
N° di fax	+39 02-93660225
ISO Object Identifier (OID)	1.3.6.1.4.1.54110
e-mail	*ca@ariaspa.it*
PEC	*ca@pec.ariaspa.it*

5.5 Le Registration Authority

L'Autorità 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 e ad espletare le procedure di **identificazione** e **registrazione** dello stesso e ad inoltrare le eventuali richieste di **revoca**, **sospensione** e **annullamento della sospensione** dei certificati su richiesta dei soggetti autorizzati verso l'Autorità di Certificazione.

ARIA per l'erogazione di questi servizi si avvale di una RA interna e dei **Punti di Adesione e Registrazione (PdA/PdR)** distribuiti sul territorio presso le sedi delle Strutture Clienti; questi rispondono per le attività svolte ad ARIA e ne condividono le regole di erogazione.

ARIA si dichiara responsabile verso terzi delle attività svolte dai suddetti Punti di Adesione e Registrazione, le cui attività sono svolte da personale incaricato (Addetti PdA/PdR) attraverso i Servizi PdA PdR di ARIA. L'accesso ai Servizi PdA PdR avviene in seguito ad autenticazione forte con smart card e tutte le operazioni eseguite sono firmate digitalmente dall'Addetto PdA/PdR.

5.6 Utenti Titolari

Gli Utenti Titolari sono **persone fisiche** afferenti a

- Regione Lombardia
- Agenzie, Aziende ed Enti Pubblici del Sistema Regionale
- Enti Locali Lombardi
- Amministrazioni Pubbliche Lombarde ed Enti Erogatori Privati Convenzionati con il Servizio Socio Sanitario Regionale
- ARIA stessa

che si rivolgono al Certificatore per la fruizione dei servizi fiduciari di firma elettronica qualificata.

5.7 Banca Dati dei certificati

La lista dei certificati revocati e sospesi è pubblicata nella banca dati (o registro) dei certificati.

La banca dati dei certificati di ARIA è mantenuta su un archivio elettronico (Directory Service X.500), accessibile in rete h24x 7, in sola lettura mediante protocollo LDAP.

La possibilità di modificarne il contenuto è riservata esclusivamente a personale autorizzato e competente.

L'indirizzo del Directory Server sul quale ARIA pubblica le CRL è il seguente:

ldap://ldap.crs.lombardia.it

La URL di pubblicazione in HTTP delle CRL invece è la seguente: *http://ca.lispa.it*

Il sistema della banca dati è progettato per garantire un tempo di scaricamento delle CRL entro il tempo stabilito dalla normativa (10 secondi) in condizioni normali di operatività.

In caso di indisponibilità del servizio di pubblicazione causato da guasti o anomalie di sistema, ARIA ne garantisce il ripristino entro le 8 ore successive alla rilevazione del disservizio.

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. Parte di queste informazioni sono quelle pubblicate dalla CA nel certificato dell'utente.

La documentazione elettronica firmata digitalmente dal Titolare viene posta in conservazione digitale a norma ed è mantenuta da ARIA per un periodo di almeno 20 anni.

I dati raccolti dai Punti di Adesione e Registrazione su supporto cartaceo, in fase di registrazione o in altre successive, sono conservati per un periodo di 20 anni a partire dalla data di emissione dei certificati.

Il trattamento dei dati avviene nel rispetto del Regolamento UE 2016/679 e 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 di ARIA 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 per l'esecuzione delle seguenti attività:

- individuazione degli incaricati,
- assegnazione dei codici identificativi,
- protezione degli elaboratori.

sono conformi alle misure di sicurezza adeguate e, comunque, nel rispetto del principio di accountability di cui al Regolamento UE 2016/679.

5.9 Tariffe

ARIA, nella sua qualità di Ente strumentale della Regione Lombardia, non può esercitare il ruolo di rivenditore nei confronti di soggetti terzi.

5.10 Orari del Servizio ed Enti preposti

La tabella che segue riporta gli orari del servizio di gestione dei certificati digitali svolti dalla Registration Authority di ARIA.

Servizio	Ente	Giorni ed Orari
Sospensione dei certificati	**RA** del Prestatore dei Servizi Fiduciari	Dal lunedì al venerdì 9:00-13:00 e 14:00-17:00, festivi esclusi
	Numero verde per il blocco cautelativo della smartcard	Help Desk del Prestatore dei Servizi Fiduciari 800.030.101 attivo dal lunedì al sabato dalle 8 alle 20 oppure via mail: supporto.fdcns@lispa.it tutti i giorni 24 ore su 24
Annullamento della Sospensione o Riattivazione dei certificati	**RA** del Prestatore dei Servizi Fiduciari	Dal lunedì al venerdì 9:00-13:00 e 14:00-17:00, festivi esclusi
Revoca dei certificati	**RA** del Prestatore dei Servizi Fiduciari	Dal lunedì al venerdì 9:00-13:00 e 14:00-17:00, festivi esclusi

Analogamente gli orari degli stessi servizi presso i Punti di Adesione e Registrazione (PdA/PdR) distribuiti sul territorio, sono disponibili presso i PdA/PdR stessi.

5.11 Assistenza

Per ogni problematica legata ai servizi e per ottenere informazioni, è a disposizione dell'utente un servizio di assistenza.
I contatti e gli orari del servizio di assistenza sono pubblicati e resi disponibili ai seguenti indirizzi (URL) http://www.ariaspa.it/CA/FirmaDigitale e http://www.lispa.it/CA/FirmaDigitale all'interno della sezione "*Riferimenti Assistenza Tecnica*".

Di seguito se ne riportano i dettagli per ogni tipologia di utente.

Tipologia di utenti	Tipologia di Assistenza	Riferimento di Assistenza	Giorni ed Orari
Utenti afferenti a: • ATS, • ASST, • EEPA, • IRCCS, • Farmacie.	Problematiche tecniche legate a • l'applicazione di firma (DigitalSign - Edizione Lombardia Informatica/ARIA) • il servizio PdA/PdR • malfunzionamenti dispositivi di firma	**Service Provider di riferimento**	Variano in relazione al Service Provider
Medici di Medicina Generale e Pediatri di Famiglia (MMG/PdF)	Problematiche tecniche legate a • l'applicazione di firma (DigitalSign - Edizione Lombardia Informatica/ARIA) • malfunzionamenti dispositivi di firma	**numero verde 800.070.090** attivo dal lunedì al sabato, dalle 8:00 alle 20:00, festivi esclusi, oppure **scrivere una mail a** ***spoc_siss@lispa.it***	Dal lunedì al sabato dalle 8 alle 20, festivi esclusi
Utenti afferenti agli Enti Locali lombardi (Comuni, Province, Unioni di Comuni, Comunità Montane, ecc.)	Problematiche tecniche legate al servizio di firma elettronica qualificata caricato su CRS/CNS	**numero 02.39331.800** attivo dal lunedì al venerdì 9:00-13:00 e 14:00-17:00, festivi esclusi, oppure **scrivere una email a** ***supporto.fdcns@lispa.it***	Dal lunedì al venerdì dalle 9 alle 13 e dalle 14 alle 17, festivi esclusi
	Problematiche tecniche legate al malfunzionamenti dei dispositivi CRS/CNS	**Call Center CRS/CNS numero verde 800.030.606** attivo dal lunedì al sabato, dalle 8.00 alle 20.00, festivi esclusi.	Dal lunedì al sabato dalle 8 alle 20, festivi esclusi
Utenti afferenti a • Regione Lombardia • Enti del Sistema Regionale • ARIA stessa	Problematiche tecniche legate a • l'applicazione di firma (DigitalSign - Edizione Lombardia Informatica/ARIA) • malfunzionamenti dispositivi di firma	**Sistemi informativi interni**	Variano in relazione all'Ente

6. Obblighi

Questa sezione tratta degli obblighi di ARIA, in qualità di Prestatore di Servizi Fiduciari di Firma Elettronica Qualificata, nei confronti degli utenti Titolari e degli utenti Utilizzatori dei certificati di firma elettronica qualificata emessi dalle CA di Lombardia Informatica.

6.1 Obblighi del Prestatore di Servizi Fiduciari

ARIA, nello svolgimento della propria attività, dichiara di essere conforme a quanto stabilito dalla normativa vigente in materia e di erogare i servizi secondo le modalità descritte nel presente documento, nelle policy dei certificati e secondo quanto stabilito nel Contratto di Fornitura dei servizi fiduciari di Firma Elettronica Qualificata.

In particolare, ARIA assume i seguenti obblighi:

- attenersi alle specifiche tecniche, norme e procedure applicabili, relative al pertinente livello di garanzia, definite all'interno delle Decisioni e Regolamenti di Esecuzione della Commissione Europea in materia di Servizi Fiduciari a norma del Regolamento (UE) n. 910/2014;
- identificare con certezza il Titolare che fa richiesta dei servizi fiduciari di Firma Elettronica Qualificata;
- garantire la correttezza delle informazioni contenute all'interno del certificato di firma elettronica qualificata in relazione alle informazioni fornite dal Titolare;
- non copiare, né conservare, le chiavi private di firma del soggetto a cui siano stati forniti i servizi fiduciari di Firma Elettronica Qualificata;
- procedere tempestivamente alla revoca/sospensione del certificato di firma elettronica qualificata 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 delle chiavi private, 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 del certificato di firma elettronica qualificata nel caso queste avvengano su iniziativa del Certificatore o su richiesta del Terzo Interessato;
- garantire un aggiornamento delle CRL tempestivo in caso di compromissione delle chiavi private del Titolare;
- garantire l'interoperabilità del prodotto di convalida delle firme elettroniche qualificate come definito nell'art. 32 del Regolamento (UE) n. 910/2014 e successive modifiche ed integrazioni e nella Decisione di Esecuzione (UE) n. 1506/2015 e successive modifiche ed integrazioni;
- utilizzare sistemi affidabili per la gestione della banca dati dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sui certificati;
- mantenere e rendere accessibile per via telematica copia dell'elenco di fiducia sottoscritto da AgID di cui all'art. 22, paragrafo 1 del Regolamento (UE) n. 910/2014 e successive modifiche ed integrazioni;
- mantenere e rendere accessibile per via telematica copia delle condizioni di fornitura dei servizi fiduciari erogati al fine di consentirne la consultazione a tutti i soggetti interessati;
- dare comunicazione ai Titolare e ad AgID, 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 di sicurezza previste per il trattamento dei dati personali e, comunque, in modo conforme al principio di accountability di cui al Regolamento UE 2016/679.
- conservare i log degli eventi rilevanti ai fini della sicurezza per almeno 20 anni a partire dalla data di registrazione del singolo evento.
- conservare il contratto firmato elettronicamente dal Titolare con firma elettronica qualificata per almeno 20 anni, registrandone la data di sottoscrizione e garantendone l'integrità e la leggibilità nel tempo.

ARIA si riserva il diritto di modificare le specifiche tecniche di erogazione dei servizi fiduciari in base all'evoluzione tecnologica e/o normativa, rendendole note attraverso la pubblicazione del presente documento e delle Policy dei Certificati (CP) sul proprio sito https://www.ariaspa.it/CA/CPS all'interno della sezione "*Documentazione*". Ove tali

modifiche risultassero essere di rilevante entità, ne verrà data informazione al Titolare, che ha la facoltà di recedere dal contratto.

6.2 Obblighi delle Registration Authority

Gli obblighi delle Registration Authority, o dei Punti di Adesione e Registrazione, sono i seguenti:

- nominare almeno un Responsabile i cui compiti sono:
  - attuare quanto previsto dalle procedure di incarico/delega, rinnovo o cessazione dell'incarico degli Addetti PdA/PdR;
  - provvedere allo smaltimento delle smart card malfunzionanti o ritirate perché revocate;
  - verificare il rispetto delle procedure e del codice etico di ARIA da parte degli Addetti PdA/PdR;
  - verificare che la documentazione utente sia archiviata conformemente a quanto previsto nel presente documento;
  - verificare periodicamente (almeno una volta all'anno) le abilitazioni degli Addetti PdA/PdR;
- pubblicare e diffondere agli Addetti PdA/PdR le procedure che disciplinano
  - le modalità autorizzative per l'attribuzione di specifici ruoli applicativi sulle smart card emesse;
  - le procedure di verifica periodica circa la sussistenza dei requisiti degli utenti titolari per il mantenimento dei ruoli applicativi ad essi assegnati;
  - le condizioni ove si preveda la revoca delle autorizzazioni rilasciate;
- incaricare gli Addetti PdA PdR mediante Lettera di Incarico, con cui viene garantito al Prestatore dei Servizi Fiduciari 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 di ARIA, ferma restando la responsabilità del Prestatore dei Servizi Fiduciari stesso;
- incaricare gli Addetti PdA PdR al trattamento dei dati personali inerenti il Servizio Punto di Adesione e Registrazione (identificazione e registrazione del titolare, richiesta/revoca/sospensione/riattivazione dei certificati digitali);
- fornire la formazione e le istruzioni operative a cui gli incaricati devono attenersi per il trattamento dei dati personali;
- comunicare al Prestatore dei Servizi Fiduciari la revoca dell'incarico agli Addetti PdA 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 di ARIA;
- effettuare la revoca dei certificati da parte del Terzo Interessato in caso di decesso del Titolare;
- conservare la documentazione utente raccolta dagli Addetti PdA PdR fino alla consegna della stessa ad ARIA secondo le modalità indicate da ARIA stessa. L'Organismo di Registrazione deve comunque garantire che la documentazione gestita sia 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 (almeno 20 anni);
- smaltire conformemente alle norme anti-inquinamento le smart card risultate difettose, non consegnate oppure ritirate perché revocate, producendone un'evidenza documentale;
- definire e attuare opportune azioni correttive a seguito delle rilevazioni effettuate da parte del Prestatore dei Servizi Fiduciari;
- comunicare tempestivamente ad ARIA la violazione delle procedure operative previste dal Manuale Operativo da parte di un Addetto PdA PdR;
- garantire che il trattamento dei dati personali dei Titolari avvenga nel rispetto delle misure di sicurezza richieste dal D.Lgs. del 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" e s.m.i., nonché di quelle previste dal Regolamento UE 2016/679 e di quelle previste da ARIA nella lettera di nomina a Responsabile dei trattamenti inerenti i Punti di Adesione e Registrazione.

Gli Obblighi dell'Addetto PdA/PdR sono i seguenti:

- attenersi scrupolosamente alle procedure allegate alla Lettera di Delega fornita da ARIA per quanto riguarda le funzioni di Revoca, Sospensione e Riattivazione dei Certificati Digitali;
- verificare con ragionevole certezza l'identità del richiedente il servizio fiduciario e registrare i dati dello stesso;
- verificare e inoltrare alla CA le richieste di revoca, di sospensione o di annullamento della sospensione utilizzando le corrispondenti funzioni del Servizio PdA PdR;

- archiviare le richieste di revoca, sospensione e annullamento sospensione e tutta la documentazione accessoria fino alla consegna della stessa ad ARIA;
- non ritirare né conservare codici personali degli utenti Titolari (user-id, password e codice di sospensione/emergenza) o codici di utilizzo (PIN Utente, PIN Firma, PUK) di carte risultate difettose e non consegnate oppure ritirate perché revocate.
- rispettare le misure minime di sicurezza nel trattamento dei dati personali secondo le istruzioni operative e la formazione ricevuta dalla struttura di appartenenza;
- rispettare le misure di sicurezza consigliate da ARIA fornite in allegato alle lettere di incarico e delega nell'esercizio delle sue funzioni;
- adottare, nello svolgimento del suo incarico, comportamenti conformi alle previsioni contenute nel Codice Etico di ARIA e nel Dlgs. 231/2001;
- comunicare tempestivamente ad ARIA tutti i casi di mancato rispetto delle condizioni di fornitura del servizio da parte del Titolare (per es. se è venuto a conoscenza che un Titolare ha ceduto anche temporaneamente la propria smart card ad un altro).

6.3 Obblighi degli Utenti Titolari

A norma del Regolamento (UE) n. 910/2014 e s.m.i. e della normativa nazionale applicabile in materia (D.Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale e s.m.i.), con l'accettazione di quanto stabilito nel Contratto di Fornitura dei servizi fiduciari di Firma Elettronica Qualificata, il Titolare assume gli obblighi seguenti:

- conservare e custodire con la massima diligenza il proprio dispositivo sicuro per la creazione di firme elettroniche qualificate (smart card), al fine di garantire l'integrità e la riservatezza della chiave privata in esso contenuta;
- conservare le informazioni di abilitazione all'uso del dispositivo (PIN e PUK) in luogo diverso dal dispositivo stesso;
- cambiare i codici PIN provvisori del proprio dispositivo;
- comunicare informazioni esatte e veritiere rispetto ai propri dati personali, nell'ambito delle procedure di identificazione e registrazione ai servizi fiduciari di Firma Elettronica Qualificata;
- informare ARIA di ogni variazione delle informazioni fornite durante le procedure di identificazione e registrazione (recandosi presso il PdA PdR di riferimento, ove applicabile, oppure inviando opportuna comunicazione tramite i canali preposti - cfr. paragrafo 5.11 "Assistenza");
- verificare la correttezza delle informazioni contenute all'interno del proprio certificato di firma elettronica qualificata;
- informare ARIA (recandosi presso il PdA PdR di riferimento, ove applicabile, oppure inviando opportuna comunicazione tramite i canali preposti - cfr. paragrafo 5.11 "Assistenza") in caso di cessazione del servizio per cui è stato richiesto il servizio fiduciario di Firma Elettronica Qualificata (ove previsto - cfr. paragrafo 8.3.1 "Motivi validi per la revoca e per la sospensione dei certificati");
- cessare immediatamente di utilizzare il certificato di firma elettronica qualificata, e la chiave privata ad esso associata, nel momento in cui non ci sia più corrispondenza tra i dati del Titolare e quelli riportati sul certificato, oppure nel caso di compromissione della chiave privata o di sospensione/revoca;
- richiedere tempestivamente la revoca o la sospensione del proprio certificato di firma elettronica qualificata al verificarsi di una delle condizioni enunciate nel paragrafo 8.3.1 "Motivi per la revoca e per la sospensione dei certificati", in particolare nei casi di furto, smarrimento o sospetta compromissione del proprio dispositivo sicuro per la creazione di firme elettroniche qualificate, secondo le modalità definite nel presente documento;
- conservare con la massima diligenza il codice di sospensione/emergenza ricevuto durante le procedure di registrazione al fine di evitare la conoscenza di questo codice da parte di altri soggetti;
- utilizzare la chiave privata personale ed il corrispondente certificato di firma elettronica qualificata nel pieno rispetto delle funzioni previste dalla sua tipologia e secondo le modalità enunciate nel Contratto, nel Manuale Operativo e nelle Policy dei Certificati di ARIA;
- non fare usi non consentiti dei servizi fiduciari (ivi compresi gli utilizzi espressamente vietati in base all'articolo 8 del Contratto).

Il Titolare è tenuto anche ad eseguire le verifiche descritte nel paragrafo 6.4 "Obblighi degli Utenti Utilizzatori" del presente documento.

Per quanto non espressamente previsto si applicano le disposizioni del codice civile.

6.4 Obblighi degli Utenti Utilizzatori

Gli Utenti Utilizzatori devono verificare la validità dei certificati relativi ai servizi fiduciari erogati da ARIA attenendosi alle modalità descritte nel paragrafo 8.8 "Modalità operative per la verifica della firma elettronica qualificata" del presente documento.

Inoltre, chiunque intenda accedere alla banca dati dei certificati per verificare la validità dei certificati è tenuto a:

- verificare attentamente il contenuto del certificato relativo alla chiave pubblica;
- avvalersi di mezzi tecnici idonei a consentire la corretta consultazione della banca dati dei certificati;
- verificare ed utilizzare i certificati e le relative informazioni solo per le finalità in relazione alle quali i certificati sono rilasciati.

Nell'ambito del servizio fiduciario di Firma Elettronica Qualificata, è vietato a chiunque utilizzare i certificati per fini differenti da quelli previsti dal presente documento e dalla vigente normativa.

Allo stesso modo, è vietato a chiunque di accedere alla banca dati dei certificati per finalità differenti dalla sua consultazione, pena le sanzioni previste dalle leggi vigenti.

7. Responsabilità del Prestatore dei Servizi Fiduciari

ARIA è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e successive modifiche ed integrazioni, dalla normativa italiana di settore, ove applicabile, (D.Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale e s.m.i., D.P.C.M. 22 febbraio 2013 e s.m.i., e ulteriori disposizioni normative e regolamentari pertinenti per materia), dal D.Lgs. n. 196/2003 nonché di quelle previste dal Regolamento UE 2016/679.

ARIA è altresì responsabile nei confronti di qualunque soggetto faccia ragionevolmente affidamento sui servizi fiduciari erogati dallo stesso, nei limiti della normativa vigente in materia. L'esistenza e la validità dei certificati relativi a tali servizi non dispensano tuttavia il Titolare e gli Utenti Utilizzatori 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.

ARIA non sarà in alcun modo responsabile, né sarà tenuta ad alcuna forma di indennizzo o risarcimento, in relazione a quanto di seguito indicato:

- danni di qualsiasi natura, diretti od indiretti, pregiudizi o inadempimenti, da chiunque patiti per eventi derivanti da atti della Pubblica Autorità, caso fortuito, forza maggiore ovvero da altra causa non imputabile ad ARIA (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 di ARIA, interruzioni nella fornitura di energia elettrica, terremoti, esplosioni, incendi), esclusi i casi di dolo o colpa grave;
- danni di qualsiasi natura, diretti o indiretti, o pregiudizi, da chiunque patiti nella misura in cui tali danni derivino dalla violazione di obblighi che, in virtù di quanto previsto dal presente documento e dalle Policy dei Certificati di ARIA ovvero dalle vigenti disposizioni di legge, incombono sul Titolare, sull'utente Utilizzatore, sul Terzo Interessato e/o su quanti accedono alla banca dati dei certificati per la convalida o la verifica delle firme elettroniche e delle validazioni temporali elettroniche e dei relativi certificati, da usi non consentiti dei servizi fiduciari (ivi compresi gli utilizzi espressamente vietati in base all'art. 8 del Contratto), ovvero dallo svolgimento di attività illecite;
- 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 dei servizi fiduciari non imputabili ad ARIA o derivanti dall'errata utilizzazione dei servizi fiduciari da parte del Titolare.

ARIA non assume nessun obbligo, garanzia o responsabilità ulteriori rispetto a quelli scaturenti dal Contratto, da quelli espressi nel presente documento, nelle Policy dei Certificati e dalla normativa vigente.

Ogni responsabilità è comunque esclusa laddove ARIA provi di aver agito senza colpa, e nei casi previsti dall'articolo 13 del Regolamento (UE) n. 910/2014 e dalla normativa italiana applicabile in materia per quanto riguarda tematiche inerenti la giurisdizione nazionale.

A copertura dei rischi connessi all'attività di certificazione e dei danni causati a terzi, ARIA ha stipulato una polizza assicurativa secondo le seguenti modalità:

A. Responsabilità civile degli organi di amministrazione e controllo di società: massimale 10.000.000,00 € per sinistro;

B. Responsabilità civile patrimoniale: massimale 5.000.000,00 € per sinistro;

C. Responsabilità civile professionale: massimale 5.000.000,00 € per sinistro;

D. Responsabilità civile verso terzi: massimale 5.000.000,00 € per sinistro e responsabilità civile verso prestatori d'opera: massimale 5.000.000,00 € per sinistro.

Il massimale aggregato per le sezioni A, B e C è pari ad euro 20.000.000,00.

A copertura dei rischi connessi alla perdita o alterazione di archivi informatici e non informatici, ARIA ha stipulato una polizza assicurativa secondo le seguenti modalità:

- Ricostruzione archivi informatici: 5.000.000 € per sinistro e per periodo di assicurazione, diminuiti ad Euro 50.000 per sinistro per i danni causati da cestinatura per svista, cancellatura per errore ed errata registrazione;
- Ricostruzione archivi non informatici: 50.000 € per sinistro.

Tutti i massimali si intendono per annualità assicurativa.

7.1 Condizioni di Fornitura dei Servizi Fiduciari

Le Condizioni di Fornitura dei servizi di Firma Elettronica Qualificata sono pubblicate sul sito *https://www.ariaspa.it/CA/CPS* h24, 7 giorni su 7.

In caso di indisponibilità del servizio di pubblicazione delle Condizioni di Fornitura dei servizi causati da guasti o anomalie di sistema, ARIA ne garantisce il ripristino entro le 8 ore successive dalla rilevazione del disservizio.

8. Modalità Operative

Questo capitolo descrive le procedure operative adottate dal Certificatore ARIA nella gestione del ciclo di vita (sospensione, revoca e annullamento della sospensione) dei certificati emessi dalla CA di Lombardia Informatica. Per conoscere le modalità operative di emissione dei certificati, servizio cessato in data 28 aprile 2017 ed erogato dal Certificatore Lombardia Informatica, si rimanda al Manuale Operativo di quest'ultimo, reso disponibile sul sito *https://www.ariaspa.it/CA/CPS*.

Le procedure operative di ARIA si diversificano a seconda del dispositivo sicuro per la creazione della firma sul quale l'utente ha richiesto di installare il materiale crittografico necessario per usufruire del servizio di firma elettronica qualificata.

Le tipologie di dispositivi sicuri (Qualified Signature Creation Device – QSCD) per la creazione della firma su cui risultano installati i certificati di firma elettronica qualificata gestiti da ARIA, si possono classificare in due gruppi:

1. Smart Card rilasciata dall'Autorità di Certificazione Lombardia Informatica, denominata anche Carta SISS o Carta Operatore;
2. Carta Regionale dei Servizi (CRS) o Carta Nazione dei Servizi (CNS) di Regione Lombardia.

Nei paragrafi seguenti si definiscono le procedure di gestione del ciclo di vita degli stessi per le due tipologie di dispositivi sicuri sopra indicati.

Agli Utenti Titolari in possesso di Carta SISS (Smart Card), invece, oltre alla coppia di chiavi, e relativo certificato, per le operazioni di firma elettronica qualificata, è stata rilasciata anche una coppia di chiavi, con relativo certificato, per le operazioni di autenticazione e cifratura. Le procedure descritte nel seguito per la gestione dei certificati intestati ai Titolari di Smart Card, pertanto, fanno sempre riferimento ad entrambi i certificati ed alle relative coppie di chiavi.

Agli Utenti Titolari che usufruiscono del servizio fiduciario di firma elettronica qualificata su CRS/CNS è stata rilasciata una sola coppia di chiavi, con relativo certificato, ad uso delle operazioni di firma elettronica qualificata.

8.1 Validità dei certificati

La durata dei certificati utente emessi dalla CA di Lombardia Informatica, e gestiti dal Certificatore ARIA a seguito del cambio di denominazione, varia a seconda della policy specifica del certificato. In generale la validità dei certificati emessi può variare dai 2 ai 6 anni a partire dalla data di emissione. In prossimità della data di fine validità dei certificati, al Titolare in possesso di Firma Elettronica Qualificata su Carta SISS viene inviata una comunicazione d'ufficio per notificarne la prossima scadenza. Al termine naturale di tale periodo i certificati non sono più validi e non possono più essere utilizzati.

I certificati scaduti sono conservati dal Prestatore dei Servizi Fiduciari per un periodo di 20 anni a partire dalla data di emissione.

8.2 Tipologia e struttura dei certificati per la firma elettronica qualificata

La struttura dei certificati è conforme allo standard X.509 versione 3. I certificati oggetto del presente Manuale Operativo e le informazioni contenute negli stessi soddisfano quanto richiesto dalla normativa vigente in materia.

La presenza e le caratteristiche delle estensioni dipendono dalla tipologia del certificato e sono descritte nel dettaglio all'interno delle relative Policy dei Certificati.

All'interno delle Policy dei Certificati è definita anche la lunghezza della coppia di chiavi di sottoscrizione, che è di tipo RSA, cui è associato il certificato dell'utente. La generazione della coppia di chiavi avviene sempre internamente al dispositivo sicuro di firma e la relativa chiave privata risulta non esportabile, pertanto non ne esistono copie conservate in altri luoghi.

Per le modalità di rilascio dei certificati, servizio cessato in data 28 aprile 2017 ed erogato dal Certificatore Lombardia Informatica, si rimanda al Manuale Operativo di quest'ultimo, reso disponibile sul sito https://www.ariaspa.it/CA/CPS.

8.3 Modalità di Sospensione e Revoca dei certificati

La sospensione è l'operazione con cui la CA sospende la validità del certificato; la sospensione è un'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 del Prestatore dei Servizi Fiduciari.

La revoca è l'operazione irreversibile con la quale la CA 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 viene pubblicato nella Certificate Revocation List (CRL) o lista dei certificati revocati che è firmata con firma elettronica qualificata dalla CA e pubblicata sulla banca dati dei certificati ogni 60 minuti; la pubblicazione della CRL è registrata nei log dei sistemi della CA. 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 nella CRL.

Per la disponibilità del servizio di richiesta di sospensione e di revoca si consulti il paragrafo 5.10 "Orari del Servizio ed Enti preposti".

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

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

- compromissione della chiave privata (una delle due o tutte e due) dell'utente; una chiave si intende compromessa quando:
  - sia venuta meno la sua segretezza;
  - si sia verificato un qualunque evento che ne abbia compromesso il livello di affidabilità e sicurezza;
- sia stato smarrito, rubato o distrutto il dispositivo di firma;
- sia diventato impossibile, a causa di un guasto, l'utilizzo del dispositivo di firma;
- sia stato smarrito o bloccato il PUK, necessario per sbloccare il dispositivo di firma e cambiarne i PIN;
- non ci sia più corrispondenza tra i dati dell'utente e quelli riportati sui suoi certificati;
- cessazione dell'utilizzo del servizio per il quale l'Utente Titolare aveva richiesto i certificati (*);
- riscontro da parte del Certificatore ARIA 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 Sistema Informativo Socio Sanitario (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.

Si precisa che il Prestatore di Servizi Fiduciari può procedere autonomamente a revocare o sospendere, ove applicabile, i certificati oltre che per i motivi sopra elencati anche al verificarsi di uno dei seguenti eventi:

- i certificati siano stati emessi tramite procedure non conformi a quelle descritte nel presente documento;
- sia venuto a conoscenza che i certificati contengono informazioni inesatte o non veritiere;
- sia venuta meno la conformità alle specifiche tecniche/normative dei certificati;
- per avvenuta cessazione dell'attività o perdita della certificazione del Prestatore dei Servizi Fiduciari;
- per compromissione delle chiavi di CA del Prestatore dei Servizi Fiduciari;
- per obsolescenza dei formati e/o dei requisiti tecnici degli strumenti crittografici forniti, considerati quindi non più accettabili perché rischiosi (ad esempio algoritmi crittografici e lunghezza delle chiavi non più sicuri).

In tutti questi casi il Prestatore di Servizi Fiduciari procederà a revocare, o sospendere ove applicabile, i certificati oggetto della violazione entro le 24 ore successive all'individuazione della circostanza che rende necessaria la revoca/sospensione.

Nei paragrafi seguenti si definiscono le modalità di revoca e sospensione dei certificati, specificatamente per le due tipologie di dispositivi sicuri per la creazione di firma individuati (Carta SISS e CNS/CRS).

8.3.2 Procedura di revoca su richiesta del Titolare

8.3.2.1 Revoca dei certificati su SmartCard

L'Utente Titolare di Carta SISS può richiedere la revoca dei propri certificati presentandosi di persona presso un Punto di Adesione e Registrazione munito di un documento di riconoscimento in corso di validità (sono accettati tutti i documenti previsti dall'art. 35 del DPR445/2000) e di Tessera Sanitaria o tesserino del Codice Fiscale.

L'incaricato all'identificazione del Punto di Adesione e Registrazione, detto anche Addetto PdA/PdR, effettua il riconoscimento e l'identificazione dell'utente richiedente con lo scopo di identificare in maniera certa l'Utente Titolare e contestualmente avviare il processo di richiesta revoca dei certificati.

Completata la procedura di identificazione, per avviare la procedura di revoca l'Addetto PdA/PdR dovrà accedere, attraverso autenticazione forte con Smart Card personale, al servizio messo a disposizione dal Prestatore dei Servizi Fiduciari, denominato Servizio di Provisioning o anche Portale PdA. Di seguito la Smart Card sarà usata anche per firmare digitalmente la richiesta di revoca da inviare alla CA.

L'Addetto PdA/PdR recupera i dati registrati dell'utente riconosciuto dal Portale PdA, quindi stampa due copie cartacee del modulo di richiesta di revoca che l'utente dovrà compilare e sottoscrivere. Nel modulo sono specificati chiaramente:

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

Una copia del modulo cartaceo è consegnata al richiedente mentre l'altra copia sarà archiviata a cura dell'Addetto PdA/PdR unitamente alla fotocopia del documento di riconoscimento dell'Utente Titolare.

Tramite il Servizio di Provisioning l'Addetto PdA/PdR genera la richiesta di revoca elettronica, firmata con firma elettronica qualificata dallo stesso Addetto PdA/PdR, e la invia alla CA tramite canale sicuro.

Ricevuta la richiesta e la documentazione elettronica di cui sopra, la CA procede alla revoca del certificato nel più breve tempo tecnicamente possibile dalla ricezione della richiesta e ne fornisce comunicazione all'Addetto PdA/PdR tramite il Portale PdA. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

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

L'Addetto PdA/PdR informa il Titolare circa l'esito dell'operazione. Inoltre, i sistemi del Certificatore ARIA invieranno una notifica automatica dell'avvenuta revoca dei certificati dell'utente ai riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della revoca e la data e l'ora a partire dalla quale i certificati risultano revocati.

Nel caso in cui l'utente sia impossibilitato ad andare di persona al Punto di Adesione e Registrazione per eseguire la revoca, può richiedere la sospensione del certificato tramite il servizio telefonico di blocco cautelativo della smartcard oppure tramite l'invio di una richiesta scritta (per la descrizione di questi servizi fare riferimento al par. 8.3.5 "Procedura di sospensione dei certificati su richiesta del Titolare"). Il Titolare dovrà, non appena possibile, trasformare la sospensione in revoca seguendo la procedura sopra descritta.

Tutta la documentazione elettronica prodotta in fase di revoca o sospensione dei certificati (per es. la Richiesta di revoca firmata dall'Addetto PdA/PdR) viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Addetto PdA/PdR che all'Utente Titolare su richiesta puntuale e viene sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi. Una copia cartacea originale della richiesta di

revoca sottoscritta dal richiedente, inoltre, viene archiviata a cura del Punto di Adesione e Registrazione (PdA/PdR) e successivamente inoltrata ad ARIA, secondo modalità prescritte da quest'ultima.

8.3.2.2 Revoca dei certificati su CNS/CRS

L'Utente Titolare di un certificato qualificato di firma su CNS/CRS che intende richiederne la revoca, dovrà compilare e sottoscrivere un apposito modulo di richiesta di revoca scaricabile dal sito del Prestatore dei Servizi Fiduciari all'interno della sezione dedicata alle procedure di gestione dei certificati di firma su CNS/CRS ***www.ariaspa.it/CA/FirmaDigitaleCNS***.

Copia del modulo di richiesta di revoca compilato e sottoscritto in ogni sua parte dovrà essere poi inviato via fax al numero indicato all'interno del modulo stesso, unitamente alla fotocopia di un documento di riconoscimento in corso di validità. Qualora l'utente fosse in possesso di una casella di posta elettronica certificata, può inviare il modulo in formato elettronico all'indirizzo PEC del Certificatore, indicato nel modulo stesso.

Il modulo di richiesta di revoca sarà archiviato e conservato per 20 anni a cura del Prestatore dei Servizi Fiduciari.

Al ricevimento della richiesta di revoca, l'incaricato RA del Certificatore, dopo aver verificato la documentazione ricevuta, procede immediatamente all'invio alla CA della richiesta di revoca del certificato dell'utente, dopo averla firmata con firma elettronica qualificata, e ne fornisce comunicazione all'Utente Titolare attraverso i riferimenti da quest'ultimo forniti. L'invio della richiesta di revoca avviene tramite il Portale CA, a cui l'incaricato RA accede tramite autenticazione forte con Smart Card personale.

La CA procede alla revoca del certificato nel più breve tempo tecnicamente possibile dalla ricezione della richiesta. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti. Qualora la richiesta di revoca sia dovuta alla possibile compromissione della chiave privata, il Prestatore dei Servizi Fiduciari provvede 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 inviare tempestivamente il fax di richiesta di revoca, può richiedere la sospensione del certificato tramite il servizio telefonico di blocco cautelativo della smartcard oppure tramite l'invio di una richiesta scritta (per la descrizione di questi servizi fare riferimento al par. 8.3.5 "Procedura di sospensione dei certificati su richiesta del Titolare"). Il Titolare dovrà, non appena possibile, trasformare la sospensione in revoca seguendo la procedura sopra descritta.

La procedura di revoca sopra descritta annulla la validità del solo certificato qualificato di firma installato sulla CNS/CRS.

Tutta la documentazione elettronica prodotta in fase di revoca dei certificati (per es. la Richiesta di revoca firmata dall'Incaricato RA del Certificatore) viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Incarico RA che all'Utente Titolare su richiesta puntuale e viene sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi.

8.3.3 Procedura di revoca su iniziativa del Terzo Interessato

8.3.3.1 Revoca dei certificati su SmartCard

La revoca dei certificati di un Utente Titolare di Carta SISS può avvenire anche su iniziativa del Terzo Interessato. Il Terzo Interessato, per poter inoltrare la richiesta di revoca, deve recarsi di persona presso un Punto di Adesione e Registrazione munito di un documento di riconoscimento in corso di validità. Il Terzo Interessato, dopo essere stato identificato da un Addetto PdA/PdR, deve fornire precisa motivazione della causale di revoca supportandola con adeguata documentazione giustificativa.

Il Terzo Interessato compila e sottoscrive in duplice copia un apposito modulo cartaceo di richiesta revoca nel quale sono 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.

Una copia del modulo cartaceo è consegnata al richiedente mentre l'altra copia è archiviata a cura dell'Addetto PdA/PdR che, dopo aver effettuato l'identificazione e verificata l'attendibilità della documentazione presentata a suffragio, inoltrerà ad ARIA la richiesta di revoca firmata con firma elettronica qualificata dello stesso Addetto PdA/PdR.

Nel caso in cui il Terzo Interessato non avesse la possibilità di recarsi di persona presso un Punto di Adesione e Registrazione, è data facoltà a quest'ultimo di inoltrare un apposito modulo di richiesta revoca, firmato digitalmente dal Legale Rappresentante o da un suo delegato munito di apposita delega, via Posta Elettronica Certificata intestata all'organizzazione di appartenenza. Il template del modulo di richiesta è reso disponibile sul sito del Prestatore dei Servizi Fiduciari.

Al modulo di richiesta di revoca, deve essere allegata adeguata documentazione giustificativa che fornisca:

- evidenza circa l'appartenenza all'Organizzazione del Titolare cui si richiede la revoca dei certificati,
- evidenza circa la causale di revoca.

Tutta la documentazione dovrà essere inviata in formato elettronico all'indirizzo PEC del Certificatore, il quale provvederà ad archiviarla e conservarla a norma per 20 anni.

La CA provvederà ad effettuare la revoca nel più breve tempo possibile, previa verifica della correttezza della documentazione inoltrata dal Terzo Interessato.

A seguito della revoca l'incaricato della identificazione (Addetto PdA/PdR o incaricato RA del Certificatore, a seconda della modalità di presentazione della richiesta di revoca effettuata dal Terzo Interessato) invierà, ove possibile, comunicazione all'Utente Titolare dell'avvenuta revoca dei suoi certificati tramite i riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, fornendo motivazione precisa della revoca e la data e l'ora a partire dalla quale i certificati risultano revocati.

Nel caso in cui l'Addetto PdA/PdR o l'incaricato RA del Certificato non sia in grado di verificare immediatamente l'attendibilità della richiesta di revoca presentata dal Terzo Interessato, procede in via cautelativa, e solo nel caso di sospetta compromissione della chiave privata o di gravi motivi addotti alla richiesta di revoca stessa, ad eseguire un'operazione di sospensione dei certificati (vd. par. 8.3.6 "Sospensione su richiesta del Terzo Interessato"), in modo da poter eventualmente ripristinare in un secondo momento la validità dei certificati qualora non sia confermata la veridicità della richiesta.

Tutta la documentazione elettronica prodotta in fase di revoca o sospensione dei certificati viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Addetto PdA/PdR/Incaricato RA che all'Utente Titolare su richiesta puntuale, ed è sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi. L'eventuale originale cartaceo della richiesta di revoca o sospensione, sottoscritta dal richiedente, viene archiviata a cura del Punto di Adesione e Registrazione (PdA/PdR) e successivamente inoltrata ad ARIA, secondo modalità prescritte da quest'ultima.

8.3.3.2 Revoca dei certificati su CNS/CRS

Nel caso in cui la richiesta di revoca di un certificato qualificato caricato su CNS/CRS avvenga su iniziativa del Terzo Interessato, la procedura prevede che quest'ultimo inoltri via Posta Elettronica Certificata, intestata all'organizzazione di appartenenza, un apposito modulo di richiesta revoca, firmato digitalmente dal Legale Rappresentante o da un suo delegato munito di apposita delega. Il template del modulo di richiesta è reso disponibile sul sito del Prestatore dei Servizi Fiduciari all'interno della sezione dedicata alle procedure di gestione dei certificati di firma su CNS/CRS ***www.ariaspa.it/CA/FirmaDigitaleCNS***.

Unitamente al modulo di richiesta di revoca, deve essere allegata adeguata documentazione giustificativa che fornisca:

- evidenza circa l'appartenenza all'Organizzazione del Titolare cui si richiede la revoca dei certificati,
- evidenza circa la motivazione della causale di revoca.

Tutta la documentazione deve essere inviata in formato elettronico all'indirizzo PEC del Certificatore, il quale provvederà ad archiviarla e conservarla a norma per 20 anni.

Al ricevimento della richiesta di revoca, l'incaricato RA del Certificatore, dopo aver verificato l'attendibilità e la correttezza della documentazione ricevuta, procede tempestivamente all'invio alla CA della richiesta di revoca del certificato dell'utente, dopo averla firmata con firma elettronica qualificata.

L'invio della richiesta di revoca avviene tramite il Portale CA, a cui l'incaricato RA accede tramite autenticazione forte con Smart Card personale.

La CA procede alla revoca del certificato nel più breve tempo tecnicamente possibile dalla ricezione della richiesta. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

A seguito della revoca, l'incaricato RA del Certificatore invierà, ove possibile, comunicazione all'Utente Titolare dell'avvenuta revoca del suo certificato tramite i riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, fornendo motivazione precisa della revoca e la data e l'ora a partire dalla quale il certificato risulta revocato.

Nel caso in cui, invece, l'incaricato RA non sia in grado di verificare immediatamente l'attendibilità della richiesta di revoca presentata dal Terzo Interessato, l'incaricato procede in via cautelativa, solo nel caso di sospetta compromissione della chiave privata o di gravi motivi addotti alla richiesta di revoca stessa, ad eseguire un'operazione di sospensione dei certificati (vd. par. 8.3.6 "Sospensione su richiesta del Terzo Interessato"), in modo da poter eventualmente ripristinare in un secondo momento la validità dei certificati qualora non sia confermata la veridicità della richiesta.

Tutta la documentazione elettronica prodotta in fase di revoca o sospensione viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Incaricato RA che all'Utente Titolare su richiesta puntuale ed è sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi.

La procedura di revoca/sospensione qui descritta annulla la validità del solo certificato qualificato di firma installato sulla CNS/CRS.

8.3.4 Procedura di revoca su iniziativa del Prestatore dei Servizi Fiduciari

La revoca dei certificati di un utente può avvenire anche su iniziativa del Prestatore dei Servizi Fiduciari, soprattutto in caso di riscontro di un sostanziale mancato rispetto, da parte dell'Utente Titolare, delle condizioni previste dal presente Manuale Operativo e nei casi previsti dalla normativa vigente in materia.

L'incaricato, verificata la veridicità del motivo per cui è necessario annullare la validità dei certificati dell'utente, procede tempestivamente all'invio alla CA della richiesta di revoca dei certificati, dopo averla firmata con firma elettronica qualificata. Subito dopo l'incaricato invia comunicazione all'Utente Titolare dell'avvenuta revoca tramite i riferimenti comunicati dal Titolare in fase di registrazione, specificando la motivazione della revoca e la data e l'ora a partire dalla quale i certificati risultano revocati.

La CA procede alla revoca dei certificati nel più breve tempo tecnicamente possibile dalla ricezione della richiesta. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

Nel caso in cui, invece, l'incaricato non sia in grado di verificare nell'immediato la veridicità del motivo che indurrebbe ad effettuare l'operazione di revoca, l'incaricato procede in via cautelativa ad eseguire un'operazione di sospensione dei certificati (vd. par. 8.3.7 "Sospensione su iniziativa del Prestatore dei Servizi Fiduciari"), in modo da poter eventualmente ripristinare in un secondo momento la validità dei certificati qualora non sia confermata la veridicità della richiesta.

Tutta la documentazione elettronica prodotta in fase di revoca o sospensione viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Incaricato che all'Utente Titolare su richiesta puntuale ed è sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi.

8.3.5 Procedura di sospensione dei certificati su richiesta del Titolare

8.3.5.1 Sospensione dei certificati su SmartCard

Per attivare la procedura di sospensione dei propri certificati, l'Utente Titolare di Carta SISS può presentarsi personalmente presso un Punto di Adesione e Registrazione munito di documento di identità valido o contattare telefonicamente il numero verde 800.030.101 per il blocco cautelativo della smartcard (procedura di emergenza) oppure inviare una richiesta scritta al Prestatore dei Servizi Fiduciari.

Sospensione presso un Punto di Adesione e Registrazione

La procedura di sospensione presso il Punto di Adesione e Registrazione prevede l'identificazione dell'Utente Titolare di Carta SISS, secondo modalità simili a quelle effettuate per la procedura di revoca (par. 8.3.2.1 "Revoca dei certificati su SmartCard"), e la successiva trasmissione alla CA della richiesta di sospensione.

Dopo essere stato identificato, al richiedente verrà richiesto di compilare e sottoscrivere in duplice copia un apposito modulo cartaceo di richiesta 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.

Una copia del modulo cartaceo è consegnata al richiedente mentre l'altra copia sarà archiviata a cura dell'Addetto PdA/PdR unitamente alla fotocopia del documento di riconoscimento dell'Utente Titolare.

Tramite i servizi messi a disposizione dal Prestatore dei Servizi Fiduciari l'Addetto PdA/PdR genera la richiesta di sospensione elettronica, firmata con firma elettronica qualificata dallo stesso Addetto PdA/PdR, e la invia alla CA.

La CA procede alla sospensione dei certificati nel più breve tempo tecnicamente possibile dalla ricezione della richiesta. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

L'Addetto PdA/PdR informa il Titolare circa l'esito dell'operazione. Inoltre, i sistemi del Certificatore ARIA invieranno una notifica automatica dell'avvenuta sospensione dei certificati dell'utente ai riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale i certificati risultano sospesi.

Tutta la documentazione elettronica prodotta in fase di sospensione dei certificati (per es. la Richiesta di sospensione firmata dall'Addetto PdA/PdR) viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Addetto PdA/PdR che all'Utente Titolare su richiesta puntuale e viene sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi. Una copia cartacea originale della richiesta di sospensione sottoscritta dal richiedente, inoltre, viene archiviata a cura del Punto di Adesione e Registrazione (PdA/PdR) e successivamente inoltrata ad ARIA, secondo modalità prescritte da quest'ultima.

Procedura telefonica

La sospensione dei propri certificati può essere richiesta anche telefonicamente contattando il numero verde **800.030.101** (**selezione 2**) del Prestatore dei Servizi Fiduciari per il blocco cautelativo della smartcard; in questo caso l'Utente Titolare di Carta SISS è identificato fornendo tre su sei caratteri scelti a caso del suo Codice di Sospensione/Emergenza (rilasciato dal Certificatore in fase di emissione certificato per l'autenticazione delle richieste di sospensione dei certificati personali).

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 del Codice Sospensione/Emergenza, l'operatore di HD aprirà un ticket ai servizi di assistenza specialistica del Prestatore dei Servizi Fiduciari, che provvederà a verificare l'attendibilità della richiesta e, in caso di riscontro positivo, ad evaderla nel più breve tempo possibile.

L'operatore HD o i servizi di assistenza specialistica di ARIA informano il Titolare circa l'esito dell'operazione. Inoltre, i sistemi della CA invieranno una notifica automatica dell'avvenuta sospensione dei certificati dell'utente ai riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale i certificati risultano sospesi.

Procedura tramite posta elettronica

Per richiedere la sospensione, l'Utente Titolare può scrivere una mail all'indirizzo **supporto.fdcns@lispa.it** indicando nella richiesta i propri dati anagrafici: nome, cognome, codice fiscale e un recapito telefonico. Gli operatori del servizio di assistenza specialistica del Prestatore dei Servizi Fiduciari provvederanno a verificare l'attendibilità della richiesta e, in caso di riscontro positivo, ad evaderla nel più breve tempo possibile fornendone comunicazione al Titolare.

8.3.5.2 Sospensione dei certificati su CNS/CRS

Per attivare la procedura di sospensione del certificato qualificato di firma installato sulla CNS/CRS, l'Utente Titolare può contattare telefonicamente il numero verde **800.030.101** secondo le stesse modalità descritte nel sottoparagrafo "Procedura telefonica" del par. 8.3.5.1 "Sospensione dei certificati su SmartCard", oppure inviare una richiesta scritta al

Prestatore dei Servizi Fiduciari. Tale richiesta può essere inoltrata tramite e-mail, secondo le modalità descritte nel sottoparagrafo "Procedura tramite posta elettronica" del par. 8.3.5.1 "Sospensione dei certificati su SmartCard", oppure tramite l'invio **via fax** o **via posta elettronica certificata** di un apposito modulo, scaricabile dal sito del Prestatore dei Servizi Fiduciari all'interno della sezione dedicata alle procedure di gestione dei certificati di firma su CNS/CRS ***www.ariaspa.it/CA/FirmaDigitaleCNS***.

Gli operatori del servizio di assistenza specialistica di ARIA provvederanno a verificare l'attendibilità della richiesta e, in caso di riscontro positivo, ad evaderla nel più breve tempo possibile, fornendone comunicazione al Titolare.

8.3.6 Sospensione su richiesta del Terzo Interessato

8.3.6.1 Sospensione dei certificati su SmartCard

La sospensione dei certificati di un Utente Titolare di Carta SISS può essere effettuata dal Terzo Interessato presso un Punto di Adesione e Registrazione, secondo modalità simili a quanto descritto per la richiesta di revoca (vd. par. 8.3.3.1 "Revoca dei certificati su SmartCard").

La CA invierà comunicazione all'Utente Titolare dell'avvenuta sospensione dei suoi certificati, ove applicabile, tramite i riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale i certificati risultano sospesi.

8.3.6.2 Sospensione dei certificati su CNS/CRS

La sospensione di un certificato qualificato caricato su CNS/CRS può essere richiesta anche dal Terzo Interessato tramite l'invio al Prestatore dei Servizi Fiduciari del modulo di richiesta di sospensione, secondo modalità simili a quanto descritto per la richiesta di revoca (vd. par. 8.3.3.2 "Revoca dei certificati su CNS/CRS").

La CA invierà comunicazione all'Utente Titolare dell'avvenuta sospensione dei suoi certificati, ove applicabile, tramite i riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale i certificati risultano sospesi.

8.3.7 Sospensione su iniziativa del Prestatore dei Servizi Fiduciari

La sospensione dei certificati di un utente può essere effettuata anche su iniziativa del Prestatore dei Servizi Fiduciari secondo modalità simili a quanto descritto per la richiesta di revoca (vd. par. 8.3.4 "Procedura di revoca su iniziativa del Prestatore dei Servizi Fiduciari");

La CA invierà comunicazione all'Utente Titolare dell'avvenuta sospensione dei suoi certificati, ove applicabile, tramite i riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la motivazione della sospensione e la data e l'ora a partire dalla quale i certificati risultano sospesi.

8.3.8 Durata massima della sospensione dei certificati

Un certificato può rimanere nello stato di sospensione per un tempo massimo di 90 giorni. Oltre questa data il Prestatore dei Servizi Fiduciari provvederà ad effettuare un'operazione di revoca dello stesso. Il Certificatore ARIA darà comunicazione dell'operazione all'Utente Titolare tramite i riferimenti forniti in fase di registrazione o di richiesta modifica dei suoi contatti.

8.3.9 Procedura di annullamento della sospensione

Dopo aver sospeso i propri certificati, l'Utente Titolare può richiedere l'annullamento della sospensione entro 90 giorni dalla data di sospensione. Con l'annullamento della sospensione viene ripristinata la validità dei certificati con la rimozione degli stessi dalla lista di revoca/sospensione.

L'annullamento della sospensione può essere richiesto solamente dall'Utente Titolare. Tale procedura si differenzia a seconda del dispositivo in uso dall'Utente Titolare.

8.3.9.1 Annullamento della sospensione dei certificati su SmartCard

Per richiedere l'annullamento della sospensione o riattivazione dei certificati, l'utente in possesso di Carta SISS deve presentarsi di persona presso un Punto di Adesione e Registrazione identificandosi con un documento di riconoscimento valido; all'utente viene richiesto di compilare e sottoscrivere in duplice copia un apposito modulo cartaceo di richiesta di riattivazione, nel quale si specificano chiaramente:

- i dati identificativi dell'Utente Titolare;
- la data di riattivazione dei certificati.

Una copia del modulo cartaceo è consegnata all'Utente Titolare mentre l'altra copia sarà archiviata a cura dell'Addetto PdA/PdR. Tramite i servizi messi a disposizione dal Prestatore dei Servizi Fiduciari, l'Addetto PdA/PdR genera la richiesta di annullamento della sospensione elettronica, firmata con firma elettronica qualificata dallo stesso Addetto PdA/PdR, e la invia alla CA.

La CA procede alla riattivazione dei certificati attraverso la rimozione degli stessi dalla CRL. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

L'Addetto PdA/PdR informa il Titolare circa l'esito dell'operazione. Inoltre, i sistemi di ARIA invieranno una notifica automatica dell'avvenuta riattivazione dei certificati dell'utente ai riferimenti comunicati dal Titolare in fase di registrazione o di richiesta modifica dei suoi contatti, specificando la data e l'ora a partire dalla quale i certificati risultano essere stati riattivati.

Tutta la documentazione elettronica prodotta in fase di annullamento della sospensione dei certificati (per es. la richiesta firmata dall'Addetto PdA/PdR) viene archiviata nel data base del Prestatore dei Servizi Fiduciari, viene resa disponibile alla consultazione sia all'Addetto PdA/PdR che all'Utente Titolare su richiesta puntuale e viene sottoposta a conservazione digitale per almeno 20 anni dalla data di emissione dei certificati emessi. Una copia cartacea originale della richiesta di riattivazione sottoscritta dal richiedente, inoltre, viene archiviata a cura del Punto di Adesione e Registrazione (PdA/PdR) e successivamente inoltrata ad ARIA, secondo modalità prescritte da quest'ultima.

8.3.9.2 Annullamento della sospensione dei certificati su CNS/CRS

L'utente in possesso di un certificato qualificato di firma su CNS/CRS che intende richiederne la riattivazione, deve compilare e sottoscrivere un apposito modulo di richiesta di annullamento della sospensione, scaricabile dal sito del Prestatore dei Servizi Fiduciari all'interno della sezione dedicata alle procedure di gestione dei certificati di firma su CNS/CRS ***www.ariaspa.it/CA/FirmaDigitaleCNS***.

Copia del modulo di richiesta di annullamento, compilato e sottoscritto in ogni sua parte, dovrà essere poi inviato via fax al numero indicato all'interno del modulo stesso, unitamente ad una copia di documento di identità in corso di validità. Qualora l'utente fosse in possesso di una casella di posta elettronica certificata, può inviare il modulo in formato elettronico all'indirizzo PEC del Certificatore, indicato nel modulo stesso.

Il modulo di richiesta di annullamento sarà archiviato e conservato per 20 anni a cura del Prestatore dei Servizi Fiduciari.

Al ricevimento della richiesta di annullamento della sospensione, l'incaricato RA del Certificatore verifica l'attendibilità e la correttezza della documentazione ricevuta e procede ad inviare la richiesta di annullamento della sospensione alla CA, dopo averla firmata con firma elettronica qualificata. L'invio della richiesta di annullamento della sospensione avviene sempre tramite il Portale CA, a cui l'incaricato RA accede tramite autenticazione forte con Smart Card personale.

La CA procede alla riattivazione del certificato attraverso la rimozione dello stesso dalla CRL. Il tempo che intercorre tra due aggiornamenti successivi di una lista di revoca è pari a 60 minuti.

L'incaricato RA invierà comunicazione al Titolare dell'avvenuta riattivazione del suo certificato tramite i riferimenti comunicati dal Titolare in fase di richiesta, specificando la data e l'ora a partire dalla quale il certificato risulta essere stato riattivato.

La procedura di annullamento della sospensione sopra descritta riattiva la validità del solo certificato qualificato di firma installato sulla CNS/CRS.

8.3.10 Procedura di revoca dopo la sospensione

Al verificarsi di una delle condizioni elencate al par. 8.3.1 “Motivi validi per la revoca e per la sospensione dei certificati”, l’utente potrà invece tramutare la sospensione in revoca effettiva. Questa operazione avviene espletando l’intera procedura di revoca (vd. par. 8.3.2 “Procedura di revoca su richiesta del Titolare”). In tal caso la data e l’ora di revoca dei certificati riportati nella lista di revoca (CRL) risulteranno coincidenti con la data e l’ora di sospensione dei certificati eseguita dalla CA prima della revoca, conformemente alla normativa vigente.

8.4 Conservazione della documentazione

Durante la gestione del ciclo di vita dei certificati, e dei servizi fiduciari correlati, vengono prodotti, o ricevuto, sia documenti elettronici, firmati dall’Utente Titolare e/o dall’addetto/incaricato che esegue l'operazione, sia documenti cartacei, firmati in maniera autografa dall'addetto/incaricato, dal Titolare o dal Terzo Interessato.

In base a quanto sopra riportato, pertanto, la documentazione utente si suddivide in due categorie:

- documentazione elettronica firmata con firma elettronica avanzata o qualificata; tale documentazione viene posta in conservazione a norma ed è mantenuta dal Prestatore dei Servizi Fiduciari per un periodo di almeno 20 anni;
- documentazione cartacea firmata in maniera autografa; tale documentazione viene raccolta ed archiviata dagli Addetti PdA/PdR o dagli Incaricati RA in appositi armadi ignifughi muniti di serratura di sicurezza (o sistema equivalente che garantisca lo stesso livello di sicurezza) e siti in locali protetti in moda da garantire la durata nel tempo della documentazione custodita. Periodicamente il Punto di Adesione e Registrazione provvede alla trasmissione della documentazione cartacea, custodita presso le sedi dei propri PdA/PdR, verso l’Azienda che gestisce l’Archivio Documentale del Prestatore dei Servizi Fiduciari, previo accordo con ARIA e secondo le modalità definite da quest’ultima. Il Prestatore dei Servizi Fiduciari garantisce il mantenimento della documentazione cartacea per un periodo di almeno 20 anni dalla data di emissione dei certificati emessi.

8.5 Banca Dati dei certificati

Sulla Banca Dati dei certificati vengono pubblicati 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 del profilo definito dallo standard ITU-T X.509 della RFC IETF 5280.

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.

I certificati revocati o sospesi permangono nella CRL, anche dopo la loro naturale scadenza, fino alla scadenza del relativo certificato di certificazione.

8.5.1 Frequenza delle pubblicazioni

La frequenza con cui le informazioni di cui al precedente paragrafo sono pubblicate dipende dalla tipologia dell’informazione stessa. Le CRL sono aggiornate e pubblicate ogni 60 minuti.

8.5.2 Procedura di gestione della Banca Dati dei certificati

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

La gestione della banca dati 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 Prestatore dei Servizi Fiduciari verificare periodicamente la conformità fra la copia operativa e la copia di riferimento.

La copia di riferimento della Banca Dati dei certificati è sottoposta a back-up giornaliero.

Solo le procedure autorizzate possono modificare il contenuto della banca dati dei certificati; ogni modifica così come ogni momento di indisponibilità della banca dati verso l'esterno trova registrazione nei log di sistema.

8.5.3 Modalità di accesso alla Banca Dati dei certificati

La banca dati dei certificati gestiti dal Certificatore ARIA, in precedenza Lombardia Informatica, è accessibile in sola lettura mediante protocollo LDAP v3 all'indirizzo **ldap://ldap.crs.lombardia.it** oppure in http all'indirizzo **http://ca.lispa.it**.

8.6 Modalità operative per la generazione della firma elettronica qualificata

In questo paragrafo vengono descritte, le modalità operative per la generazione della firma elettronica qualificata. Maggiori informazioni sono riportate sul sito del Prestatore dei Servizi Fiduciari.

ARIA eroga all'Utente Titolare un servizio di firma elettronica qualificata su un dispositivo sicuro per la creazione della firma conforme alla normativa vigente in materia di firma elettronica qualificata e compatibile con le tecnologie utilizzate dal Prestatore dei Servizi Fiduciari; il Titolare a sua volta ha l'obbligo di utilizzare questo dispositivo secondo le modalità descritte nel presente documento ed esclusivamente per le operazioni previste dalle policy del certificato.

8.6.1 Generazione della firma elettronica qualificata

La firma elettronica qualificata fa riferimento in maniera univoca ad un documento, o insieme di documenti, ed al Titolare che l'ha apposta. Compito del Titolare è di accertarsi che il proprio certificato qualificato non risulti scaduto o non valido in quanto revocato o sospeso e che eventuali limitazioni d'uso del certificato di firma siano compatibili con la documentazione cui la firma deve essere apposta.

Durante il periodo di validità del certificato di firma elettronica qualificata il Titolare deve inoltre accertarsi che non venga meno la veridicità dei dati riportati all'interno del certificato stesso (per es. Organizzazione di appartenenza, eventuali poteri di rappresentanza, dati anagrafici, ecc.).

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

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

Il risultato dell'operazione crittografica descritta è la firma elettronica, che diventa qualificata quando eseguita tramite strumenti informatici (dispositivo di tipo QSCD, certificato di firma e software di apposizione della firma) aventi specifici requisiti tecnico-normativi.

I documenti firmati con firma elettronica qualificata più comunemente utilizzati hanno estensione p7m o pdf.

Per eseguire queste operazioni l'Utente Titolare deve utilizzare le funzioni apposite dell'applicazione di firma **DigitalSign® - Edizione Lombardia Informatica/ARIA**, adottato dal Prestatore dei Servizi Fiduciari quale strumento principale per la generazione della firma elettronica qualificata di documenti.

Maggiori informazioni sulle funzionalità del prodotto sono riportate nella documentazione dell'applicazione stessa disponibili sul sito del Prestatore dei Servizi Fiduciari ARIA.

8.6.2 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 elettronica qualificata. Di fatto quando 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 possano modificare gli atti, i fatti o i dati nello stesso rappresentati. 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 desiderata 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.

È opportuno, pertanto, 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 ARIA distribuisce, nell'ambito del proprio servizio fiduciario di Firma Elettronica Qualificata, il prodotto DigitalSign® – Edizione Lombardia Informatica/ARIA, che visualizza al suo interno documenti di questo tipo in modo da ridurre il rischio di alterazione dei dati durante la visualizzazione, anche mediante l'utilizzo di messaggi di warning;
- 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.

8.7 Informazioni sui formati dei documenti

8.7.1 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. È da considerare sicuro se usato come base per i documenti informatici firmati con firma elettronica qualificata tramite DigitalSign® – Edizione Lombardia Informatica/ARIA. 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 a quello ottenuto su carta. Il documento così prodotto può essere sottoscritto con ragionevole tranquillità.

8.7.2 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 sottoscrizione del documento PDF ottenuto tramite DigitalSign® – Edizione Lombardia Informatica/ARIA. Si danno di seguito alcune informazioni specifiche sui principali formati MS Office utilizzati per la creazione di documenti:

- DOC/DOCX: è il formato predefinito di un documento di MS Word e può contenere macroistruzioni;
- 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 macroistruzioni;
- XLS/XLSX: è il formato principale di MS Excel per memorizzare ed elaborare dati mediante funzioni di varia natura;
- PPT/PPTX: è il formato principale di MS Powerpoint.

8.7.3 Open Document Format

L'Open Document Format, (ODF) è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Le estensioni utilizzate da questo formato sono: .ods, .odp, .odg, .odb.

8.7.4 XML

XML (Extensible Markup Language) è un linguaggio che consente la rappresentazione di documenti e dati strutturati su supporto digitale sviluppato dal World Wide Web Consortium (W3C). XML è uno strumento potente e versatile per la creazione, memorizzazione e distribuzione di documenti digitali in formato testo (ASCII) e utilizza la codifica dei caratteri UNICODE. XML è indipendente dal tipo di piattaforma hardware e software e permette la rappresentazione di qualsiasi tipo di documento indipendentemente dai dispositivi di archiviazione e visualizzazione. L'estensione utilizzata da questo formato è: .xml.

8.7.5 TXT

L'estensione .txt denota semplici file di testo e il tipo di file TXT. Un file TXT è un file che contiene solo caratteri stampabili con caratteri di controllo end-of-line (EOL) e, facoltativamente, caratteri di controllo end-of-file (EOF).

I file TXT non contengono metadati, ma possono avere solo una formattazione semplice e sono normalmente codificati in ASCII, ANSI, o UNICODE. Sono direttamente leggibili e convenzionalmente indicati come file di "testo normale".

8.7.6 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.

8.8 Modalità operative per la verifica della firma elettronica qualificata

La verifica della firma elettronica qualificata è l'operazione cardine dell'intero processo crittografico di sottoscrizione, e per questo motivo vanno verificate tutte le condizioni al contorno. Se la verifica della firma elettronica qualificata 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 Prestatore del Servizio Fiduciario di Firma Elettronica Qualificata;
- il Titolare della firma non può negare di averla emessa (non ripudio).

Tramite DigitalSign® – Edizione Lombardia Informatica/ ARIA, è possibile verificare le firme elettronica qualificate emesse dagli Utenti Titolari di certificati emessi dalla CA di Lombardia Informatica, gestita dal Certificatore ARIA, e dagli Utenti Titolari di certificati emessi da altri Prestatori di Servizi Fiduciari di Firma Elettronica Qualificata.

L'operazione di verifica della firma elettronica qualificata non richiede l'uso di smart card o lettore, ma viene effettuata tramite personal computer collegato ad Internet. Il collegamento ad Internet è necessario affinché l'applicazione di verifica firma possa eseguire:

- il controllo della validità dei certificati tramite l'aggiornamento delle liste di sospensione/revoca (CRL) pubblicate dall'Autorità di Certificazione che ha emesso i certificati;
- l'aggiornamento dell'Elenco di Fiducia pubblicato dall'Organismo di Vigilanza dello Stato Membro di riferimento che contiene i certificati delle CA dei Prestatori di Servizi Fiduciari conformi alla vigente normativa italiana ed europea in materia;
- la verifica della presenza di aggiornamenti software dell'applicazione stessa.

L'utente è tenuto a verificare periodicamente che l'applicazione installata sulla propria postazione di lavoro sia aggiornata all'ultima versione rilasciata dal Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata. Tale informazione è resa disponibile sul sito del Certificatore ARIA.

Ogni eventuale modifica apportata dall'utente sulle configurazioni di sicurezza dell'applicazione consigliate, deve essere eseguita consapevolmente in merito agli effetti che tali modifiche possono comportare sull'esito della verifica delle firme elettroniche (ad. es. la disabilitazione della verifica delle CRL).

All'utente è richiesta un'attenta verifica delle informazioni contenute nei certificati in relazione al contenuto dei documenti firmati, al fine di assicurarsi che i certificati siano utilizzati per le finalità cui sono destinati (ad es. limitazioni d'uso, utilizzo della chiave, ecc.).

Qualora l'utente utilizzi altro software di verifica delle firme, non rilasciato dal Prestatore dei Servizi Fiduciari di Firma Elettronica Qualificata ARIA, deve accertarsi che tale strumento sia idoneo per la corretta consultazione della banca dati dei certificati.

8.8.1 Verifica della firma elettronica qualificata tramite DigitalSign ® – Edizione Lombardia Informatica/ARIA

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

- la firma elettronica qualificata 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 e si ha 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 Lombardia Informatica/ARIA in modo trasparente per l'utilizzatore.

Allo stesso modo è possibile verificare tramite DigitalSign® – Edizione Lombardia Informatica/ARIA firme elettroniche qualificate apposte da Titolari di certificati emessi da altri Prestatori di Servizi Fiduciari presenti negli Elenchi di Fiducia pubblicati dagli Organismi di Vigilanza dei singoli Stati Membri. Per i Prestatori di Servizi Fiduciari italiani, l'Elenco di Fiducia di riferimento è pubblicato da AgID (https://eidas.agid.gov.it/TL/TSL-IT.xml).

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).

DigitalSign® – Edizione Lombardia Informatica/ARIA 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 Lombardia Informatica/ARIA consente di effettuare verifiche di firme elettroniche qualificate riferite ad una data qualsiasi, diversa da quella attuale, che deve essere inserita dall'utente tramite un'apposita funzione.

8.8.2 Verifica della firma elettronica qualificata da parte di soggetti che non dispongono di DigitalSign® – Edizione Lombardia Informatica/ARIA

I soggetti che necessitano di verificare una firma elettronica qualificata ma che non dispongono di DigitalSign® – Edizione Lombardia Informatica/ARIA possono effettuare l'operazione utilizzando DigitalSign® Reader disponibile sul sito www.comped.it o altro software indicato nelle linee guida per l'utilizzo della firma elettronica qualificata pubblicate sul sito di AgID www.agid.gov.it.

9. Servizi interni alla CA

9.1 Generazione delle chiavi private di CA

Le chiavi private di CA vengono generate dal Responsabile della CA su dispositivi di firma dotati di requisiti di sicurezza e robustezza conformi a quanto richiesto dalla normativa vigente.

La coppia di chiavi della CA di Lombardia Informatica, con la quale il Certificatore ARIA firma le CRL emesse da questa CA, sono di tipo RSA con lunghezza pari a 2048 bit.

Invece, la coppia di chiavi della CA di ARIA è di tipo RSA con lunghezza pari a 4096 bit. La CA di ARIA non emette e non firma certificati o liste di revoca.

Il backup delle chiavi private di CA è salvato cifrato e suddiviso su più supporti di archiviazione affidati a diversi responsabili e conservati presso tre siti distinti. Per questo motivo, per ripristinare una chiave privata di CA in seguito al guasto del dispositivo di firma su cui risiede, è necessaria la compresenza di almeno due responsabili e del materiale di backup di due siti.

9.2 Generazione dei certificati di CA

La generazione dei certificati di CA avviene nel rispetto delle modalità stabilite dalla normativa vigente e secondo severe misure di sicurezza.

I certificati sono generati su sistema dedicato, sito nei locali dell'Autorità di Certificazione a più elevata protezione, protetti da meccanismi di controllo accessi che consentono la registrazione di ogni entrata ed uscita del personale sui Log di sistema (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.

I certificati di CA (sia della CA di Lombardia Informatica che della CA di ARIA, entrambi in gestione al Prestatore di Servizi Fiduciari di Firma Elettronica Qualificata ARIA subentrato a Lombardia Informatica) sono firmati con la chiave privata di certificazione dei certificati stessi (certificati self-signed), sono depositati presso AgID e da questa resi pubblicamente disponibili nel proprio elenco di fiducia (Trusted List o Trusted Service Status List - TSL).

Il certificato della CA di Lombardia Informatica ha una durata pari a 12 anni a partire dalla data di emissione ed è anche pubblicato nella banca dati dei certificati gestita dal Prestatore dei Servizi Fiduciari, mentre il certificato della CA ARIA ha una durata pari a 5 anni a partire dalla data di emissione.

9.3 Scadenza dei certificati di CA

Allo scadere dei certificati di certificazione delle CA in gestione al Prestatore dei Servizi Fiduciari, **non verranno generate nuove coppie di chiavi di certificazione** poiché ARIA, così come Lombardia Informatica a cui è subentrata in qualità di certificatore qualificato, **ha intrapreso un percorso di cessazione graduale dei servizi**, non emettendo più certificati digitali di firma elettronica qualificata ma gestendo esclusivamente il ciclo di vita dei certificati emessi fino al 28 aprile 2017 da Lombardia Informatica.

Il Prestatore dei Servizi Fiduciari continua comunque a garantire la custodia e la gestione di tutte le informazioni necessarie al mantenimento del corretto funzionamento dei servizi erogati (banca dati dei certificati e relativa documentazione) per il periodo prescritto dalla normativa vigente in materia, adempiendo agli obblighi e alle responsabilità previste dalle condizioni di fornitura dei servizi.

9.4 Revoca dei certificati di CA

In caso di compromissione della chiave privata di certificazione, il Prestatore dei Servizi Fiduciari procederà alla revoca del proprio certificato dandone notifica, entro 24 ore dall'essere venuti a conoscenza dell'accadimento, ad AgID e al CAB.

Seguiranno alla revoca del certificato di CA, le seguenti azioni:

- revoca di tutti i certificati sottoscritti con la chiave privata di certificazione compromessa.
- notifica a tutti gli Utenti Titolari coinvolti riguardo la revoca avvenuta dei certificati digitali a loro intestati a causa della compromissione della chiave privata di certificazione.

9.5 Il Giornale di Controllo

I sistemi utilizzati presso il Prestatore di Servizi Fiduciari registrano automaticamente tutti gli eventi che si verificano e che sono rilevanti ai fini della sicurezza secondo quanto richiesto dalla normativa vigente; l'insieme di queste registrazioni costituisce il Giornale di Controllo. Tutte le informazioni associate ad un evento vengono registrate in modo da consentire la ricostruzione di quest'ultimo, in particolare la data e l'ora in cui l'evento si è verificato. L'accuratezza della data e l'ora degli eventi è garantita dal fatto che tutti i sistemi di CA vengono sincronizzati alla scala di tempo UTC con una frequenza non superiore ai 1.064 secondi.

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 mediante un sistema di backup centralizzato.

Periodicamente le registrazioni vengono verificate e poi archiviate in ambienti a più alta protezione dell'Autorità di Certificazione per un periodo non inferiore a 20 anni a partire dal momento di emissione del certificato cui si riferiscono.

Inoltre, ad integrazione di quanto detto sopra, le informazioni che fanno parte del Giornale di Controllo vengono poste in Conservazione Digitale a norma dal Prestatore di Servizi Fiduciari.

Le informazioni raccolte comprendono i seguenti eventi:

- (*) personalizzazione dei dispositivi sicuri per la creazione di firma, ovvero l'inserimento nei medesimi dei relativi certificati;
- entrata e uscita dai locali protetti del personale;
- (*) inizio e fine di ciascuna sessione di lavoro dedicata alla generazione dei certificati;
- (*) generazione dei certificati;
- revoca e sospensione dei certificati;
- annullamento della sospensione dei certificati;
- operazioni che modificano il contenuto della banca dati dei certificati;
- intervallo di tempo nel quale la banca dati dei certificati non risulta accessibile dall'esterno o una sua funzionalità interna non risulta disponibile;
- (*) anomalie del servizio di Validazione Temporale;
- (*) emissione di marche temporali.

Gli eventi contrassegnati con (*) afferiscono a servizi cessati, pertanto in questi casi non si intende la raccolta delle relative informazioni ma si intende la conservazione e il mantenimento delle registrazioni relative a tali eventi, occorsi fino al 28 aprile 2017.

Ai fini della sicurezza il Prestatore di Servizi Fiduciari garantisce l'autenticità delle annotazioni contenute nel giornale di controllo così da permettere la ricostruzione di tutti gli eventi rilevanti annotati.

ARIA 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 dalla data di emissione dei certificati a cui si riferiscono.

10. Audit interni e verifiche ispettive

Il Prestatore di Servizi Fiduciari attua periodicamente audit interni e verifiche ispettive per monitorare lo stato della qualità e della sicurezza dei servizi fiduciari da esso erogati al fine di evitare la compromissione dei servizi. Le procedure di verifica vengono svolte in maniera strutturata e secondo metodologie derivanti dal sistema di gestione per la qualità e per la sicurezza delle informazioni e dalle ultime versioni delle linee guida emesse dal CA/Browser Forum per la gestione dei certificati, pubblicate su http://www.cabforum.org, cui il Prestatore dei Servizi Fiduciari è conforme, ove applicabile.

Oltre alle verifiche previste dal sistema di gestione della qualità e della sicurezza, vengono effettuati controlli periodici sulla conformità alla normativa vigente applicabile ai servizi erogati e sul mantenimento dei requisiti dichiarati all'interno della documentazione di certificazione (CPS, CP, PDS, ecc.), in particolare vengono svolte le seguenti verifiche:

- verifica sullo stato di certificazione dei dispositivi sicuri per la creazione della firma utilizzati dagli Utenti Titolari su cui è presente almeno un certificato per la firma elettronica qualificata, in corso di validità, emesso dalla CA di Lombardia Informatica. Nel caso in cui venissero meno le condizioni di sicurezza per una specifica tipologia di dispositivo, con la conseguente perdita della certificazione del dispositivo, il Prestatore dei Servizi Fiduciari procederà con la revoca dei certificati emessi su suddetti dispositivi secondo le modalità descritte nel par. 8.6.4 "Procedura di revoca su iniziativa del Prestatore dei Servizi Fiduciari" fornendone comunicazione preventiva agli Utenti Titolari;
- verifiche ispettive per il controllo dei requisiti tecnico-normativi dell'infrastruttura dell'Autorità di Certificazione;
- verifiche ispettive per il controllo della corretta applicazione delle procedure operative e di sicurezza svolte dalle RA Locali del Prestatore di Servizi Fiduciari;
- audit interni per la verifica della corretta applicazione delle procedure operative del personale di gestione dei servizi;
- verifiche sul rispetto dei requisiti dichiarati dei certificati emessi;
- controlli periodici sulla registrazione dei log di sistema rilevanti ai fini della sicurezza sia per la verifica del corretto funzionamento delle applicazioni e dei sistemi durante la loro operatività sia per il controllo del corretto funzionamento delle registrazioni stesse.

11. Cessazione dell'attività del Prestatore dei Servizi Fiduciari

Qualora il Prestatore dei Servizi dovesse cessare di erogare uno o più dei Servizi Fiduciari prestati, verrà data comunicazione, con un preavviso di almeno 60 (sessanta) giorni, agli Utenti Titolari, all'Agenzia per l'Italia Digitale (AgID), all'Organismo di valutazione di conformità (CAB) nonché ad ogni eventuale ulteriore soggetto interessato e legittimato a venire a conoscenza di tale accadimento.

Se il processo di cessazione intrapreso prevede la revoca di tutti i certificati digitali non ancora scaduti degli Utenti Titolari, nella comunicazione sarà chiaramente specificato che al momento della cessazione dell'attività saranno revocati i certificati degli utenti, assicurando tuttavia la conservazione dei dati relativi per un periodo di almeno 20 anni.

In adempimento alle vigenti disposizioni di legge e al fine di garantire la continuità dei servizi, ARIA provvederà

- a revocare le autorizzazioni verso tutti i propri Punti di Adesione e Registrazione (PdA PdR) di procedere ad ulteriori operazioni di gestione del ciclo di vita dei certificati digitali per la Firma Elettronica Qualificata ancora attivi per conto del Prestatore dei Servizi Fiduciari;
- a custodire e a gestire tutte le informazioni necessarie al corretto funzionamento dei servizi (banca dati dei certificati e relativa documentazione) per il periodo di tempo prescritto dalla normativa vigente in materia, adempiendo agli obblighi e alle responsabilità previste dal contratto tramite anche l'eventuale trasferimento degli stessi ad altro Prestatore di Servizi Fiduciari Qualificato che abbia i requisiti di affidabilità e sicurezza almeno pari a quelli di ARIA;
- a distruggere, o a rendere non più utilizzabili, tutte le chiavi private, ed eventuali copie di backup, custodite in modo che queste non possano più essere recuperate e utilizzate da terzi;
- a trasferire, ove possibile, la fornitura dei servizi fiduciari ad altro Prestatore di Servizi Fiduciari Qualificato che abbia i requisiti di affidabilità e sicurezza almeno pari a quelli di ARIA.

12. Misure di Sicurezza

I Servizi Fiduciari di Firma Elettronica Qualificata erogati da ARIA rispettano i più elevati standard di sicurezza; il Prestatore di Servizi Fiduciari 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 dei servizi fiduciari è sita in locali dotati di avanzati sistemi di controllo accessi e di videosorveglianza. L'ingresso ai locali dell'Autorità di Certificazione è consentito solo a personale dedicato e specializzato, previa sua identificazione. Ogni ingresso ed uscita è registrato sul Giornale di Controllo.

Il Prestatore di Servizi Fiduciari 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 Prestatore di Servizi Fiduciari e delle misure di sicurezza adottate sono soggette a periodiche analisi dei rischi: 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 dei servizi fiduciari offerti.

12.1 Procedure di gestione degli eventi catastrofici

Per ovviare al rischio di malfunzionamento dell'intera infrastruttura e assicurare continuità ai servizi fiduciari erogati, 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 dei servizi.

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 del sito primario, da utilizzare fino al ripristino del sito principale per minimizzare i rischi di indisponibilità del servizio.

A tale scopo sono state individuate, in funzione dell'impatto derivante da un eventuale disastro, alcune funzionalità dei servizi fiduciari che rappresentano e/o assolvono a funzioni critiche irrinunciabili, quali:

- la sospensione dei certificati digitali;
- l'emissione e la pubblicazione delle CRL.

In considerazione dell'evento verificatosi verrà predisposto un piano per ripristinare l'operatività delle altre funzionalità (revoca e annullamento della sospensione dei certificati).

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

13. Protezione dei Dati

In considerazione della grande importanza attribuita alla tematica della sicurezza nel trattamento dei dati, all'interno di ARIA è operativo un sistema organizzativo e normativo che garantisce riservatezza, integrità e disponibilità delle informazioni, e assicura 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 ARIA.

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 analisys;
- 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 ARIA, incorpora anche le misure minime previste dal D.Lgs. 196/03 Codice per la protezione dei dati personali e s.m.i., nonché di quelle previste dal Regolamento UE 2016/679. Tale sistema si caratterizza per alcuni 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 nonché delle norme previste dal Regolamento UE 2016/679, hanno ricevuto dettagliate istruzioni circa le modalità e le misure di sicurezza da adottare per il trattamento dei dati personali;
- 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.

13.1 Modalità di Protezione dei Dati

Il presente paragrafo ha lo scopo di illustrare le procedure e le modalità operative adottate da ARIA per il trattamento dei dati personali, nello svolgimento della propria attività di erogazione dei servizi fiduciari oggetto del presente documento. I dati personali relativi all'Utente Titolare di certificati, al Terzo Interessato e a chiunque acceda ai servizi, sono trattati, conservati e protetti da ARIA conformemente a quanto previsto dal Regolamento UE 2016/679 e dalla normativa italiana vigente.

La terminologia utilizzata nel presente paragrafo è conforme a quella adottata dal DL 196/03 nonché di quella prevista dal Regolamento UE 2016/679, e parzialmente difforme da quella utilizzata nel resto del documento, che è invece aderente alla terminologia derivante dalla normativa sulla firma elettronica qualificata. 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 Prestatore di Servizi Fiduciari);
- per Responsabile si intende la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo nominati dal Titolare al trattamento di dati personali;
- per Amministratore di Sistema si intende, nell'ambito della terminologia privacy, una figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Sono inclusi in questa categoria anche figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
- 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 l'Utente Titolare di certificati, il Terzo Interessato o chiunque acceda al servizio).

In particolare, il Prestatore di Servizi Fiduciari:

- individua e nomina gli Incaricati del trattamento dei dati (ovvero gli Incaricati dell'Identificazione e quanti altri tratteranno i dati attinenti ai servizi fiduciari di Firma Elettronica Qualificata), attenendosi alle istruzioni impartite, ai sensi dell'Art. 30 del DL 196/03 nonché delle norme applicabili previste dal Regolamento UE 2016/679;
- individua e nomina, con designazioni individuali, gli Amministratori di Sistema, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato e ne riporta gli estremi con l'elenco delle funzioni attribuitegli all'interno di un documento interno cosi come richiesto dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008.
- nomina i 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.

13.2 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 da considerare dati personali anche i codici identificativi forniti dal Prestatore di Servizi Fiduciari 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 riattivazione, 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 Prestatore di Servizi Fiduciari, e analiticamente descritte nel Piano per la Sicurezza, sono realizzate conformemente a quanto previsto dal DL 196/03 e dal Regolamento UE 2016/679.

13.3 Tutela e diritti degli interessati

In materia di trattamento dei dati personali il Prestatore di Servizi Fiduciari garantisce la tutela degli interessati in ottemperanza al D.Lgs. 196/03 ed al Regolamento UE 2016/679. 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 degli artt. 13 e 14 del Regolamento UE 2016/679;
- agli interessati viene richiesto il consenso scritto al trattamento dei propri dati personali.

13.4 Applicazione del Codice per la protezione dei dati personali

13.4.1 Adempimenti generali

Dal punto di vista generale il Prestatore di Servizi Fiduciari:

- predispone, conserva e aggiorna, nell'ambito delle attività di erogazione dei servizi fiduciari, un Registro degli Archivi Informatici e Cartacei contenenti i dati personali di cui è Titolare e che vengono utilizzati nella gestione di tutte le fasi delle attività inerenti ai servizi;
- 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, nonché del Regolamento UE 2016/679.

13.4.2 Adempimenti tecnici ed organizzativi

Dal punto di vista tecnico il Prestatore di Servizi Fiduciari, 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.

13.4.3 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 Prestatore di Servizi Fiduciari. In proposito, si precisa che, a fronte di eventi che dovessero compromettere la capacità operativa del Prestatore di Servizi Fiduciari presso la principale sede di attività, è definito un Piano Operativo che garantisce la disponibilità della banca dati dei certificati e le funzionalità del servizio considerate critiche dal punto di vista della sicurezza e del business (sospensione dei certificati e pubblicazione delle CRL);
- supervisiona l'organizzazione e la classificazione dei moduli di richiesta sospensione, riattivazione e 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 Prestatore di Servizi Fiduciari.

13.4.4 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 degli artt. 13 e 14 del Regolamento UE 2016/679;
- 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.

13.4.5 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 erogazione e gestione dei servizi fiduciari siano coerenti con la tutela dei dati personali.

13.4.6 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 Regolamento UE 2016/679 e dalla normativa italiana vigente, curando inoltre l'aggiornamento del Registro degli Archivi Informatici e Cartacei.

13.4.7 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 Prestatore di Servizi Fiduciari. In particolare:
  - classifica i soggetti abilitati all'accesso in funzione delle loro mansioni. In particolare, si precisa che ARIA ha definito ed attua specifiche policy di gestione delle credenziali di autenticazione e per la costruzione e l'utilizzo delle password;
  - 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);
  - 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;
  - supervisiona la circolazione interna delle informazioni contenute negli stampati (tabulati) o in altri supporti;
  - assicura la distribuzione degli output su terminale in accordo con i profili utente designati dal responsabile della sicurezza;
- protegge l'integrità dei dati considerati singolarmente 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 per poter adempiere alle richieste di consultazione/verifica da parte degli interessati previste dalla normativa vigente.

13.5 Comunicazione dei dati personali a soggetti terzi

Fermo restando il diritto dell'interessato di richiedere ed ottenere dal Prestatore di Servizi Fiduciari informazioni relative ai propri dati personali, secondo quanto previsto dall'informativa resa ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679, il Prestatore di Servizi Fiduciari, nello svolgimento delle proprie attività di erogazione e gestione dei servizi fiduciari, può effettuare operazioni di comunicazione e diffusione dei dati personali.

In particolare, in caso di cessazione dell'attività da parte di ARIA e al solo fine di assicurare la continuità dei servizi fiduciari, i dati personali possono essere comunicati per le medesime finalità di trattamento del Prestatore dei Servizi Fiduciari

- ad altri Prestatori di Servizi Fiduciari attivi presenti nell'elenco di fiducia sottoscritto da AgID, di cui all'art. 22, paragrafo 1 del Regolamento (UE) n. 910/2014,
- ad AgID.

Escludendo ogni finalità di trattamento per scopi diversi da quelli dichiarati dal Prestatore dei Servizi Fiduciari e direttamente e tecnicamente connessi all'erogazione dei servizi fiduciari, i dati personali possono essere comunicati anche a Pubbliche Amministrazioni, ai sensi di legge, o trasferiti al di fuori del territorio nazionale alle condizioni e con le garanzie di cui al RGPD. I dati personali possono essere comunicati, inoltre, all'Autorità Giudiziaria, in conformità con quanto previsto dalla normativa vigente.
Ad esclusione di quanto previsto dalla normativa vigente in materia 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.