Sede legale: Via Magellano, 1 – 10128 TORINO
Tel. +39 011.508.1111
www.mauriziano.it

REGOLAMENTO AZIENDALE
PER LE ATTIVITA' DI REGISTRAZIONE E RILASCIO DI CERTIFICAZIONE DIGITALE

Indice generale

(aggiornamento settembre 2019)

1. SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dall'A.O. Ordine Mauriziano per l'emissione dei certificati per chiavi di sottoscrizione, in conformità con la vigente normativa in materia di firma digitale.

2. CONTESTO NORMATIVO

Nell'ordinamento giuridico italiano il primo atto normativo che ha stabilito la validità della firma digitale per la sottoscrizione dei documenti elettronici è stato il DPR n. 513 del 1997, emanato in attuazione dell'articolo 15 della legge 15 marzo 1997, n. 59 (legge Bassanini), a norma del quale "gli atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge".
Successivamente, tale normativa è stata trasposta nel DPR n. 445 del 2000, recante il Testo Unico sulla documentazione amministrativa, più volte modificato per conformare la disciplina italiana alla normativa comunitaria contenuta nella Direttiva 99/93 in materia di firme elettroniche.
Da cui, la normativa in materia di firma digitale è contenuta nel D.Lgs. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" (nel prosieguo del documento denominato CAD), così come modificato dal D.Lgs. 4 aprile 2006, n. 159, dalla cui entrata in vigore (il 1 Gennaio 2006) scaturisce un insieme di nuovi adempimenti per le PA basati sull'utilizzo e l'integrazione delle tecnologie dell'ICT al fine di innovare, semplificare e snellire i servizi ed i procedimenti amministrativi.
Da tenere presente:

- il Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, recante «Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali», pubblicato nella Gazzetta Uffi ciale 21 maggio 2013, n. 117;
- il Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013, recante «Regole tecniche in materia di sistema di conservazione», pubblicato nel Supplemento ordinario n. 20 alla Gazzetta Ufficiale - serie generale - 12 marzo 2014, n. 59;
- il Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014, recante «Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni», pubblicato sulla Gazzetta Ufficiale Serie Generale n.8 del 12-1-2015
- Regolamento UE n° 910/2014 – eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull'identità digitale - ha l'obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.

Il Regolamento eiDAS (articolo 25, comma 3) prescrive che:

"Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.".
I formati che queste firme elettroniche qualificate devono possedere sono definiti nella Decisione di

esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015: fra quelli previsti, anche il formato PDF

L'obiettivo della normativa è, da un lato consentire al cittadino di interagire in modo più rapido ed efficiente attraverso internet, Posta Elettronica, reti, dall'altra, fare in modo che le PA si organizzino per gestire e rendere disponibili tutte le informazioni in modalità digitale, ovvero rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini, imprese e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'eBusiness e del commercio elettronico.

Da sottolineare anche la normativa in materia di Fascicolo Sanitario Elettronico (FSE), Fatturazione Elettronica, Nodo di Smistamento degli Ordini, che impongono la firma digitale dei documenti amministrativi e sanitari:

- DPCM n.178 del 29 settembre 2015 "Regolamento in materia di fascicolo sanitario elettronico"
- Decreto 4 agosto 2017 "Modalita' tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilita' del Fascicolo sanitario elettronico (FSE) di cui all'art. 12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221"
- Decreto del 25 ottobre 2018 "Modifica del decreto ministeriale 4 agosto 2017, concernente le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)".
- D.G.R. n.27-6517 del 23/2/2018 "Attuazione del piano triennale per l'informatica nella P.A. 2017-2019 e degli adempimenti in materia di sanità digitale. Linee di indirizzo della sanità digitale piemontese – Progetti regionali 2018-2020".
- Decreto del Ministero dell'Economia e delle Finanze del 7 dicembre 2018. Modalità e tempi per l'attuazione delle disposizioni in materia di emissione e trasmissione dei documenti attestanti l'ordinazione degli acquisti di beni e servizi effettuata in forma elettronica da applicarsi agli enti del Servizio sanitario nazionale, ai sensi dell'articolo 1, comma 414, della legge 27 dicembre 2017, n. 205
- Decreto Ministeriale del 3 aprile 2013, n. 55. Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 . Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005

3. PREMESSA

Nell'ambito del processo di *e-government*, avviato negli ultimi anni nella pubblica amministrazione, un importante traguardo è segnato dalla **firma digitale**, che consente di sottoscrivere documenti

informatici assicurando loro lo stesso valore giuridico di documenti sottoscritti con firma autografa.
Le Pubbliche Amministrazioni sono state chiamate, quindi, a dotarsi di opportune infrastrutture organizzative, informatiche e tecnologiche per adeguarsi alle novità normative, gestendo, in modo graduale ma deciso, la progressiva dematerializzazione dei documenti cartacei e la gestione dei documenti informatici, al fine di rendere più efficiente e trasparente l'azione amministrativa.
Il presente Regolamento persegue l'obiettivo prioritario di fornire le indicazioni operative per l'utilizzo del servizio di firma digitale nell'ambito dell'A.O. Ordine Mauriziano; a tal fine, appare indispensabile offrire preliminarmente una panoramica generale riportando alcune definizioni tratte dal Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) così come modificato dal D.Lgs. 235/ 2010:

- **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **firma elettronica avanzata**: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
- **firma elettronica qualificata**: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
- **firma digitale**: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
- **Firma digitale remota:** è una tipologia di firma digitale, accessibile via rete, la cui chiave privata del firmatario viene conservata assieme al certificato di firma, all'interno di un server remoto sicuro (basato su un HSM - Hardware Security Module) da parte di un certificatore accreditato.
- **Documento informatico**: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Se il comma 1 dell'art. 21 del CAD prevede che "*Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità*", il successivo comma 2 continua affermando che "*il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del Codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*".
La normativa primaria, quindi, mentre riconosce ai documenti sottoscritti con firme elettroniche "*semplici*" un valore giuridico e probatorio assodato ma difficilmente valutabile a priori, riconosce ai documenti sottoscritti con firme elettroniche avanzate (e in questa macro categoria rientrano

anche le firme digitali e le altre firme qualificate) un valore probatorio ben preciso, ovvero quello riconosciuto alle scritture private che, secondo quanto previsto dall'art. 2702 del nostro Codice civile, fanno piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.
La sottoscrizione, quindi, di un documento elettronico con una firma elettronica avanzata equivale pienamente alla sottoscrizione "analogica" su carta.

Inoltre il Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del CAD di cui al decreto legislativo n. 82 del 2005. (15A00107" pubblicato sulla GU n.8 del 12-1-2015, fornisce le seguenti indicazioni sul "documento informatico" (art. 3)

Il documento informatico è formato mediante una delle seguenti principali modalità:

- redazione tramite l'utilizzo di appositi strumenti software;
- acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il suddetto Decreto specifica inoltre che, nel caso di documento informatico formato ai sensi della lettera a), le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
b) l'apposizione di una validazione temporale;
c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
d) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
e) il versamento ad un sistema di conservazione.

Fatte queste premesse legislative si può affermare che per sostituire la documentazione cartacea con il documento informatico, quest'ultimo dovrebbe disporre di un sistema di firma digitale certificata o, almeno, di un sistema di firma elettronica con caratteristiche di sicurezza tali da presupporre una valutazione positiva da parte del giudice in caso di contenziosi.

Le soluzioni di firma elettronica avanzata devono assicurare:

- l'identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati

biometrici eventualmente utilizzati per la generazione della firma medesima;
- la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
- la connessione univoca della firma al documento sottoscritto.

Relativamente al tema delle firme elettroniche dei Documenti Clinici Elettronici (DCE), ogni Azienda sanitaria deve, pertanto, definire: quali sono i DCE da sottoscrivere e il formato con cui sono rappresentati, quale tipologia di firma elettronica usare, quale formato nel caso di firma digitale.
È opportuno evidenziare che non vi sono norme che danno risposte precise in tal senso e, pertanto, ogni realtà deve trovare le risposte in funzione del suo specifico livello tecnologico-organizzativo.
L'obiettivo è **g**arantire la regolarità e la trasparenza della firma digitale e il rispetto della normativa vigente.
In particolare, il documento informatico valido legalmente e con efficacia probatoria - e, quindi, sostitutiva del cartaceo - deve necessariamente assicurare non solo la tracciabilità di tutte le registrazioni informatiche effettuate in ogni fase del processo diagnostico-terapeutico-assistenziale, ovvero consentire di risalire a chi e quando ha effettuato ogni singola registrazione, ma anche garantire l'autenticità, l'integrità e l'immodificabilità dei documenti che vi afferiscono.
Questi particolari requisiti possono essere soddisfatti solo attraverso un adeguato utilizzo della firma elettronica che, come è noto, costituisce un supporto sia per garantire la tracciabilità in fase di inserimento e modifica di dati sia per garantire l'integrità di documenti prodotti.

4. ATTORI

Certificazione	il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato

1	**Certificatore accreditato**	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, **dall' Agenzia per l'Italia digitale**, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
2	**Ufficio di Registrazione**	Ente incaricato dal *Certificatore* a svolgere le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale nonché alla consegna del dispositivo sicuro di firma.
3	**Incaricato Registrazione**	La/le persone fisiche che hanno dichiarato la propria disponibilità a svolgere una parte delle funzioni dell'Ufficio di Registrazione, su delega dell'Azienda

4	**Titolare di firma**	La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso ovvero soggetto a favore del quale è stato emesso normativa vigente e del presente Regolamento

4.1 CERTIFICATORE ACCREDITATO

Il ***Certificatore Accreditato*** (ai sensi dell'art. 29 del **CAD**) emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle Regole Tecniche.
L'Ente Certificatore è abilitato ad emettere il "certificato digitale di sottoscrizione", intendendosi per tale "*l'insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la chiave pubblica del soggetto certificato*".

4.2 UFFICIO DI REGISTRAZIONE

Presupposto dell'emissione del certificato è il completamento della procedura di registrazione, durante la quale vengono acquisiti i dati forniti dall'utente e viene eseguita l'identificazione fisica dello stesso.

E' compito dell'***Ufficio di Registrazione*** svolgere l'attività di raccolta dei dati relativi ai richiedenti i certificati, la loro identificazione nonché il successivo eventuale rilascio del certificato digitale emesso dal *Certificatore Accreditato*, ovvero l'*Ufficio di Registrazione* svolge per conto del *Certificatore Accreditato* le suddette preliminari operazioni

Il Certificatore quindi si avvale sul territorio di *Uffici di Registrazione* per svolgere principalmente le funzioni di:

- identificazione e registrazione del ***Titolare***,
- validazione della richiesta del certificato,
- distribuzione ed inizializzazione del dispositivo sicuro di firma,
- attivazione della procedura di certificazione della chiave pubblica,
- supporto al ***Titolare*** e al ***Certificatore*** nel rinnovo/revoca/sospensione dei certificati.

L'Ufficio di Registrazione, anche tramite suoi incaricati (RAO Registration Authority Officer autorità preposta all'emissione della firma digitale), svolge in sostanza tutte le attività di interfaccia tra il ***Certificatore*** ed il ***Titolare***.
L'Ufficio di Registrazione ha la facoltà di nominare soggetti, persone fisiche o persone giuridiche, conferendo loro l'incarico di svolgere parte delle attività ad essa demandate e facendo loro accettare gli obblighi conseguenti.

4.3 INCARICATO DELLA REGISTRAZIONE

L'**Incaricato della Registrazione e più brevemente "I.R.",** dichiara la propria disponibilità a svolgere una parte delle funzioni dell'Ufficio di Registrazione ed in particolare quella relativa alle attività comprendenti:

- identificazione certa dell'utente;
- raccolta della richiesta di registrazione e certificazione da questo compilata e sottoscritta in modalità cartacea;
- rilascio della ricevuta (firmata dall'utente e dall'incaricato);

- consegna dei Manuale Operativi;
- consegna di copia delle condizioni generali di contratto e dei codici segreti di emergenza in busta sigillata;
- trasmissione all'Ufficio Registrazione della relativa documentazione per il rilascio dei certificati digitali di sottoscrizione e di autenticazione e del dispositivo di firma digitale (come dettagliato nel modello "Mandato per lo svolgimento di attività di incaricato per il rilascio di servizi di certificazione digitale")
- trasmissione all'Ufficio Registrazione della relativa documentazione per la revoca/sospensione dei certificati digitali di sottoscrizione

L'**I.R.** dovrà svolgere le attività previste nel mandato con la diligenza del mandatario di cui all'art. 1710 cod. civ.

In particolare l'**I.R.** dovrà:

- svolgere l'attività di registrazione nel rispetto della normativa vigente con particolare riferimento all'identificazione personale certa di coloro che sottoscrivono la richiesta di certificazione digitale;
- interrompere l'attività di registrazione e riconsegnare immediatamente ogni materiale a tal fine utilizzato, qualora, per qualsiasi causa, si interrompa il rapporto in essere dandone tempestivamente notizia per iscritto al Certificatore Accreditato;
- provvedere ad informare i richiedenti sulle modalità di utilizzo della firma digitale, con particolare riferimento alle modalità di revoca, sospensione e rinnovo dei certificati digitali, nonché sugli aspetti normativi e sulle conseguenze giuridiche derivanti dall'utilizzo della stessa;
- provvedere all'eventuale ritiro presso l'Ufficio di Registrazione dei dispositivi di firma degli Utenti Titolari che suo tramite hanno inoltrato la richiesta, rendendosi custode degli stessi dispositivi fino alla consegna agli Utenti, che si impegna ad effettuare entro trenta giorni dal ritiro, e rispondendo direttamente della loro sottrazione, perdita o deterioramento per qualsiasi causa, con obbligo di comunicare senza ritardo tali eventi all'Ufficio di Registrazione ed al Certificatore Accreditato;
- a non utilizzare né trattare i dati personali acquisiti in violazione del d.l.vo n. 196/2003.

La violazione di uno qualsiasi degli obblighi sopra riportati, costituirà giusta causa di revoca del mandato da parte dell'Ufficio di Registrazione, che sarà esercitata a mezzo di apposita comunicazione, fatto salvo il diritto al risarcimento dei danni eventualmente subiti e subendi. In caso di revoca l'**I.R.** è obbligato a cessare qualsiasi attività posta in essere in base al mandato ricevuto ed a restituire i materiali ricevuti al fine dell'espletamento dell'incarico.

4.4 TITOLARE DI FIRMA

All'interno dell'Azienda svolgono la propria attività amministrativa e sanitaria diverse figure professionali, che a seconda delle proprie competenze, debbono firmare documenti amministrativi e/o sanitari.

Per poter firmare digitalmente i documenti il dipendente deve essere dotato di dispositivo di firma e quindi diventa il ***Titolare*** del certificato, ovvero il possessore della chiave privata corrispondente

alla chiave pubblica contenuta nel certificato stesso

5. SOLUZIONE ADOTTATA DALL'A.O. ORDINE MAURIZIANO

La soluzione individuata dall'A.O. Ordine Mauriziano prevede di individuare responsabilità e competenze secondo quanto sotto riportato.

In qualità di ***Titolare*** sono nominati tutti i dipendenti per cui l'A.O. autorizza l'uso di un certificato qualificato per la firma digitale. In prima istanza i dirigenti amministrativi e i dirigenti sanitari autorizzati alla firma del referto.

L'*Ente certificatore* scelto dall'A.O. Ordine Mauriziano è InfoCert in quanto Certificatore per chiavi di firma digitale iscritto nell'elenco pubblico tenuto dall'organismo di controllo designato dal Dipartimento per l'Innovazione e le Tecnologie: con delibera del 19 luglio 2007 il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (ora Agenzia per l'Italia Digitale) ha iscritto InfoCert S.p.A. nell'elenco pubblico dei certificatori;
I dati completi dell'organizzazione che svolge la funzione di ***Certificatore*** sono i seguenti:

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Piazza Sallustio 9 00187 Roma**
Sede operativa	**Via G.B. Morgagni 30H 00161 Roma**
N° telefono	**06-442851**
N° fax	**06-44285255**
N° Iscrizione Registro Imprese	**Codice Fiscale 07945211006**
N° partita IVA	**07945211006**
Sito web	http://www.firma.infocert.it/
PEC	infocert@legalmail.it
Referente	Maurizio Carniello

L'A.O. Ordine Mauriziano ha stipulato con Infocert una "Convenzione per lo svolgimento di attività di **Ufficio di Registrazione** e rilascio di servizi di certificazione digitale" (allegata al presente Regolamento come parte integrale e sostanziale), che disciplina il rapporto tra InfoCert tramite l'Ufficio di Registrazione e l'Organizzazione, in virtù del quale è erogato a favore dei Titolari il servizio di certificazione, con generazione di chiavi asimmetriche all'interno del Dispositivo ed emissione dei relativi certificati, in conformità al Dlgs 82/2005 e s.m.i., alla normativa secondaria vigente in materia, nonché secondo le caratteristiche e modalità dettagliatamente descritte nel presente Regolamento e nel Manuale Operativo Infocert (depositato presso l'Agenzia per l'Italia Digitale e disponibile on line all'indirizzo web http://www.infocert.it).

L'Ufficio di Registrazione è l'Azienda Ospedaliera Mauriziano, nella persona del Direttore Generale, in qualità di rappresentante legale dell'Azienda

In particolare l'Ufficio di Registrazione:

- ha stipulato apposita convenzione con InfoCert, con la quale sono state affidate le funzioni

di Ufficio di Registrazione come previsto dal Manuale Operativo ICERT-INDI-MO per il rilascio del certificato di sottoscrizione di InfoCert;

- con la stessa Convenzione sono state affidate all'A.O. Ordine Mauriziano le funzioni di Ufficio di Registrazione previste nel Manuale Operativo ICERT-INDI-MOCA per il rilascio dei certificati di autenticazione di InfoCert;
- effettua le operazioni necessarie al rilascio degli ulteriori servizi di certificazione che verranno predisposti e forniti da InfoCert, attenendosi a quanto stabilito nei Manuali Operativi disciplinanti i singoli servizi e secondo le eventuali ulteriori istruzioni e condizioni comunicate da InfoCert medesima;
- secondo quanto stabilito all'art. 8 della Convenzione, ha facoltà di operare anche attraverso propri incaricati, previa comunicazione ad InfoCert dei loro dati identificativi ed accettazione da parte degli stessi degli obblighi conseguenti.

La fase di il riconoscimento è sotto l'esclusiva competenza e responsabilità dell'Ufficio di registrazione, escludendosi sin da subito ogni attività in capo ad InfoCert.

L'Ufficio di Registrazione ha dato per iscritto "Mandato per lo svolgimento di attività di ***Incaricato*** per il rilascio di servizi di certificazione digitale" alla S.C. ICT & Sistemi Informativi, nelle persone di:

- Sig.ra Rosa Strano

Tale mandato è stato comunicato per iscritto ad InfoCert.
Il rapporto tra l'Ufficio di Registrazione e l'I.R. è disciplinato esclusivamente dall'apposito contratto di mandato, che l'Ufficio di Registrazione ha sottoscritto con ciascun I.R
L'Ufficio di Registrazione si impegna, altresì, a mantenere costantemente aggiornata la lista dei suddetti nominativi, comunicando ad InfoCert ogni variazione entro e non oltre tre giorni dalla stessa.

6. FIRMA DIGITALE REMOTA

La firma remota è definita nel DPCM 22 febbraio 2013 (articolo 1, comma 1, lettera q) come "*particolare procedura di firma elettronica qualificata o firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse"*.

Il servizio di "firma digitale remota" consente alle Amministrazioni di dare efficacia probatoria ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.
Il servizio deve essere configurato come un servizio online nel quale la chiave privata del firmatario viene generata e conservata assieme al certificato di firma rilasciato da parte di un Certificatore accreditato, all'interno di un server remoto sicuro (basato su un HSM conforme alla normativa vigente in materia). E' quindi richiesto che venga utilizzato un sistema di autenticazione forte che preveda l'uso, oltre alla conoscenza di un codice segreto (es. PIN), di sistemi OTP fisici o logici, eliminando in tal modo i problemi e i rischi relativi all'utilizzo delle sole password statiche.
Nello specifico sono state fornite da Infocert Firme digitali Remote da utilizzare in modalità utente, utilizzate per la sottoscrizione dei documenti da parte dell'operatore sanitario all'interno

dell'applicazione Babele che gestisce tutto il processo di contatto del paziente dall'accettazione alla dimissione.
Al fine di ottimizzare i flussi relativi alla gestione della firma è stata prevista l'installazione presso l'A.O. Mauriziano di un Server virtuale che espone le funzionalità di Firma Remota su cui è stato installato il software Proxy Sign.

7. TIPI DI SOTTOSCRIZIONE DIGITALE

Gli standard europei (Decisione della Commissione europea 2011/130/EU) prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi
CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia. Ai fini del presente documento si tratteranno solo i primi due tipi.

La firma CAdES

La busta CAdES è un file con estensione *.p7m*, il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.
Per il formato CAdES l'apposizione di due o più firme può essere effettuata in due modi:

- re-imbustando in una nuova busta CAdES la busta generata dalla sottoscrizione precedente (c.d. controfirma o "firma matrioska")
- oppure aggiungendo nella busta ulteriori firme, accompagnate dai relativi certificati (c.d. firme congiunte)

In entrambi i casi è presente un'unica versione del documento, che pertanto può solo essere oggetto di ulteriori firme digitali senza modificarne il contenuto.
Nel caso di documenti sottoscritti in formato CAdES, non è possibile gestire diverse versioni di uno stesso documento all'interno della busta crittografica, pertanto, nell'ipotesi in cui si voglia riportare sul documento delle annotazioni successive alla sottoscrizione (ad esempio i dati della segnatura di protocollo), sarà necessario esportare il documento nel formato originario, ossia non firmato, per apportarvi le annotazioni. Tali modifiche, infatti, sarebbero apportate nell'unica versione del documento presente all'interno della busta CAdES, operazione questa che renderebbe le firme invalide

La firma PAdES

La firma digitale in formato PAdES è un file con estensione *.pdf*, leggibile con i comuni *reader* disponibili per questo formato.
Questa tipologia di firma, nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni, rende il documento più facilmente accessibile, ma consente di firmare solo documenti di tipo PDF.
Il formato PDF consente inoltre di gestire diverse versioni dello stesso documento senza invalidare le firme digitale apposte.
Tale caratteristica della busta PAdES rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso.

Ad una prima analisi, un documento sottoscritto sul quale sono riportate tali annotazioni potrebbe apparire corrotto in quanto modificato dopo la firma, tuttavia nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento, che pertanto conserva piena efficacia giuridica.

Allo stato attuale i documenti firmati attraverso applicativi utilizzati dal personale dell'AO Ordine Mauriziano risultano con la seguente sottoscrizione:

Tipologia Documento	Applicativo	Tipologia Sottoscrizione
Documenti sanitari (referti, lettere di dimissione, verbale di Pronto Soccorso, ...)	Babele	PADES (firma remota)
Referti di Laboratorio Analisi	Concerto	PADES (firma remota)
Referti di Anatomia Patologica	Winsap	PADES (firma remota)
Fatture , Ordini	DigitGo	CADES (utilizzando dispositivi di firma quali smart card o businessKey)
Atti Deliberativi - determinazioni	Auriga	CADES (utilizzando dispositivi di firma quali smart card o businessKey)
Lettere Protocollate, Contratti, Convenzioni	Auriga	PADES (utilizzando dispositivi di firma quali smart card o businessKey)
Registri di repertorio atti/protocollo	Auriga	PADES (utilizzando dispositivi di firma quali smart card o businessKey)

La scelta di frmare PADES i documenti sanitari è stata indotta dalla Regione Piemonte nell'ambito del progetto FSE (Fascicolo sanitario Elettronico).

8. DISPOSITIVI HARDWARE E SOFTWARE

Dispositivo di firma	Insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici

Nel caso di utilizzo di firma digitale con dispositivi hardware di firma (utilizzati per tutti i documenti non sanitari), per poter generare firme digitali è necessario essere dotati di un dispositivo sicuro per la generazione delle firme (costituito da una smartcard o da una businessKey USB), un lettore di smartcard (nel caso in cui non si utilizzi la businessKey USB), un software in grado di

interagire con il dispositivo per la generazione di firme digitali e per la gestione del dispositivo stesso (es. per il cambio del PIN che ne consente l'uso).
L'A.O. Ordine Mauriziano ha, allo stato attuale adottato:

- Smart card conformi alla normativa vigente in materia
- Business Key conformi alla normativa vigente in materia

Il lettore di smart card utilizzato, se necessario, è uno dei seguenti modelli:

- NILOX 10NXCR12SM001 USB 2.0
- miniLECTOR-piano bit4id USB full speed
- Gemalto PC USB-SW Reader

già a disposizione dell'A.O. Mauriziano con collegamento al computer tramite porta USB 2.0.
Tutti i lettori suddetti sono conformi allo standard ISO-7816.

Per quanto riguarda il software è utilizzato DiKe versione 6 e successive per le seguenti funzionalità:

- apporre firma e verifica delle firme di documenti elettronici;
- la verifica/visualizzazione di marche temporali e la richiesta di marche temporali da parte dei soli utenti attivati al servizio di marche temporali
- attivazione e verifica del dispositivo;
- verifica dei certificati;
- cambio/sblocco/impostazione del PIN;
- rinnovi dei certificati digitali.

Per quanto riguarda le Business Key, il software necessario a gestire i certificati ed apporre la firma digitale è memorizzato nel dispositivo stesso.
Nel caso di firma digitale remota l'accesso al certificato viene effettuato direttamente dall'applicativo BABELE al server Proxy Sign, installato presso il Mauriziano.

9. OBBLIGHI

Chiunque intenda utilizzare un sistema di chiavi asimmetriche o di firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

9.1 OBBLIGHI DELL'ENTE CERTIFICATORE (INFOCERT)

Nello svolgimento della sua attività il Certificatore:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
2. si attiene alle normativa vigente in materia di Firma Digitale;
3. genera e pubblica, nel proprio registro dei certificati, un certificato qualificato per ciascuna delle chiavi di firma elettronica avanzata, utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'Elenco Pubblico dei Certificatori Accreditati;
4. rende accessibile, per via telematica, la copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di Certificazione di cui al DPCM 13/01/2004;
5. predispone le informazioni relative all'uso del certificato, quali i termini e le condizioni di rilascio, le procedure di reclamo e di risoluzione delle controversie;
6. informa i richiedenti sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi e sulle caratteristiche delle firme emesse sulla base del servizio di certificazione;

7. richiede, quando previsto e prima di emettere il certificato, la prova del possesso della chiave privata; verifica il corretto funzionamento della coppia di chiavi;
8. genera la coppia di chiavi mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
9. registra, nel giornale di controllo, l'emissione dei certificati qualificati, con la specificazione della data e dell'ora di generazione;
10. attesta il momento della generazione dei certificati tramite un riferimento temporale;
11. non copia, né conserva le chiavi private di sottoscrizione dei Titolari;
12. adotta le misure di sicurezza per il trattamento dei dati personali ai sensi del D.Lgs. 196/2003;
13. procede alla pubblicazione della revoca e della sospensione del certificato qualificato, in caso di richiesta da parte del Titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
14. garantisce il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché un servizio di revoca e sospensione dei certificati qualificati tempestivo;
15. tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione per venti (20) anni (si considerano 20 anni a partire dalla scadenza del certificato, quindi in totale sono 23 anni; le informazioni valide sono SOLO relative al certificato qualificato e NON alla firma digitale);
16. assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei propri certificati;
17. utilizza sistemi affidabili per la gestione del registro dei certificati, con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato;
18. fornisce un sistema che consenta di effettuare la verifica delle firme digitali;
19. fornisce tutte le caratteristiche delle apparecchiature hardware e il software necessario per l'espletamento dell'attività di registrazione e di rilascio dei servizi;
20. dà consulenza ed assistenza sulle problematiche connesse all'espletamento dell'attività previste nella Convenzione stipulata;
21. addestra ed aggiorna adeguatamente il proprio personale, i propri addetti e/o incaricati mediante opportuni corsi di formazione specifica.

9.2 OBBLIGHI DELL'UFFICIO DI REGISTRAZIONE (A.O. Ordine Mauriziano)

L'Ufficio di Registrazione è tenuto a garantire:

1. che il ***Titolare*** sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma;
2. che il ***Titolare*** sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;

3. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196 e relativo allegato B ;
4. l'autenticità della richiesta di certificazione;
5. la verifica d'identità del ***Titolare*** del certificato, il controllo e la registrazione dei dati dello stesso, secondo le procedure di identificazione e registrazione previste;
6. la comunicazione al ***Certificatore*** di tutti i dati e documenti acquisiti, durante l'identificazione allo scopo di attivare la procedura di emissione del certificato, entro 30 gg;
7. la verifica e inoltro al ***Certificatore*** delle richieste di revoca, sospensione e rinnovo attivate dal ***Titolare*** presso l'Ufficio di Registrazione;
8. l'esecuzione, ove prevista a suo carico della revoca o sospensione dei certificati.
9. l'attività di vigilanza sui propri incaricati affinché le attività svolte ai sensi della convenzione siano eseguite nel rispetto della normativa vigente e di quanto previsto nei Manuali Operativi di InfoCert;
10. a tenere un registro aggiornato di carico e scarico dei dispositivi di firma di cui dispone e della loro allocazione territoriale.

9.3 OBBLIGHI DELL'INCARICATO DELLA REGISTRAZIONE

L'Incaricato della Registrazione, terrà direttamente i rapporti con il Certificatore e con i Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Regolamento.

Gli Incaricati della Registrazione, nello svolgimento della loro attività, sono tenuti a:

1. eseguire l'identificazione dei Titolari previa esibizione di un valido documento di riconoscimento nel rispetto della normativa vigente in materia;
2. raccogliere i contratti e le schede di registrazione, firmati dagli stessi Titolari, completarne la compilazione,
3. consegnare i Dispositivi ed il codice segreto ai Titolari;
4. informare il Titolare in merito agli accordi di certificazione stipulati con il certificatore;
5. accettare le eventuali richieste di revoca/sospensione formulate dai Titolari;
6. consegnare a Infocert gli originali dei documenti di richiesta firmati su supporto cartaceo, entro 30 giorni

9.4 OBBLIGHI DEL TITOLARE

Il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri. Il Titolare del certificato di firma digitale deve inoltre:

1. prendere visione del presente Regolamento;
2. fornire tutte le informazioni richieste dal Certificatore garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR 445/2000,
3. comunicare agli Incaricati della Registrazione ogni variazione dei dati forniti in fase di registrazione;
4. conservare con la massima diligenza la chiave privata e il dispositivo che la contiene, al fine di garantirne l'integrità e la massima riservatezza;
5. conservare con la massima diligenza i codici riservati ricevuti dal Certificatore, al fine di

garantirne l'integrità e la massima riservatezza;
6. conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
7. non apporre firme digitali su documenti contenenti macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che ne renderebbero, quindi, nulla l'efficacia;
8. richiedere l'immediata revoca dei certificati contenuti nei dispositivi di firma di cui si abbia perduto il possesso o difettosi;
9. richiedere l'immediata revoca dei certificati contenuti nei dispositivi di firma qualora cessi il rapporto di lavoro con l'A.O. Ordine Mauriziano di Torino, restituendo contestualmente il dispositivo stesso;
10. inoltrare, con le modalità indicate dal presente Regolamento, la richiesta di revoca munita della sottoscrizione e specificandone la motivazione e la sua decorrenza;
11. inoltrare, con le modalità indicate dal presente Regolamento, la richiesta di sospensione munita della sottoscrizione e specificando la motivazione ed il periodo durante il quale la validità del certificato deve essere sospesa;
12. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle autorità competenti.

10. VALIDITA' DEL CERTIFICATO

L'inizio e la fine del periodo di validità delle chiavi sono contenute all'interno dei relativi certificati.
Il periodo di validità dei certificati qualificati è determinato in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati.
Nel caso dell'A.O. Ordine Mauriziano il certificato ha validità 3 anni con un rinnovo ulteriore di 3 anni.
Si evidenzia che il documento firmato digitalmente eredita la medesima validità del certificato digitale di sottoscrizione, a meno che non vengano utilizzati sistemi di marcatura temporale o sistemi di archiviazione sostitutiva, che rendono di fatto valido il documento per un periodo maggiore.

11. MODALITA' DI IDENTIFICAZIONE E REGISTRAZIONE DEGLI UTENTI

L'utente (medico/amministrativi/ecc), a seguito della richiesta di essere dotato di firma digitale, si reca presso l'Ufficio degli Incaricati della Registrazione portando con sé i documenti necessari all'identificazione, l'eventuale ulteriore documentazione necessaria alla registrazione.

L'Incaricato della Registrazione addetto all'identificazione ritira la documentazione presentata dal Richiedente e:
- controlla la validità del documento di identità prodotto in originale;
- verifica la presenza e la correttezza dei dati di registrazione in base alle informazioni acquisite attraverso i documenti.

L'Incaricato della Registrazione, dopo aver compiuto le verifiche descritte:
- fa sottoscrivere, in duplice copia, i moduli al Titolare che è tenuto a verificare puntualmente la

correttezza delle informazioni di registrazione;
- firma e timbra due copie dei moduli;
- invia una copia della documentazione originale raccolta a Infocert entro 30 giorni;
- consegna una copia del contratto al Titolare e ne archivia un'immagine scannerizzata.

11.1 DOCUMENTI RICHIESTI AI FINI DELL'IDENTIFICAZIONE E REGISTRAZIONE

L'identificazione dell'utente avviene attraverso l'esibizione di uno dei seguenti documenti di riconoscimento:
- Carta di identità;
- Passaporto;
- Patente di guida;

I suddetti documenti devono essere validi e presentati in originale, corredati della relativa fotocopia.

11.2 MODALITA' DI EMISSIONE DEI CERTIFICATI

La documentazione prevista sarà inoltrata dagli Incaricati della Registrazione all'Ufficio di Registrazione, seguendo le istruzioni fornite per la specifica modalità operativa.
Il RAO (Registration Authority Officer), verificata la congruità dei dati, effettua la personalizzazione del dispositivo di firma e l'emissione del certificato qualificato.
Il dispositivo di firma e la busta contenente le credenziali segrete di accesso e sblocco della carta (PIN/PUK) e il codice di emergenza (codice di sospensione immediata), sono consegnate direttamente ai Titolari.
Analogamente per la firma remota, il RAO invia la documentazione al titolare del nuovo certificato richiedendo la sua compilazione e restituzione insieme alla copia di un documento di riconoscimento. A seguito il RAO emette il certificato e comunica al titolare via email di recarsi presso l'ufficio RAO per la sua identificazione e la conseguente attivazione del certificato e modifica del PIN.

11.3 REVOCA E SOSPENSIONE DEI CERTIFICATI QUALIFICATI

La revoca di un certificato qualificato è l'operazione con cui il RAO (Registration Authority Officer), annulla la validità di un certificato, da un dato momento, non retroattivo, in poi.

Il **Titolare** deve procedere alla richiesta di revoca nei seguenti casi:
- perdita del possesso del dispositivo di firma (smarrimento, furto);
- guasto o malfunzionamento del dispositivo di firma;
- compromissione della segretezza della chiave privata;
- variazione di uno qualunque dei dati presenti nel certificato (ad esempio, fine del rapporto di lavoro con l'Organizzazione o perdita del ruolo dichiarato nel certificato).

11.3.1 Revoca in caso di smarrimento / furto

Il Titolare, in caso di smarrimento o sottrazione del dispositivo di firma, deve richiedere la sospensione immediata avvertendo l'Incaricato della Registrazione e sporgendo denuncia alle autorità competenti, che deve essere consegnata tempestivamente al suddetto Incaricato.
Il richiedente è tenuto a sottoscrivere la richiesta di revoca scritta, corredata di un documento di

identità in corso di validità e consegnarla all'Incaricato della Registrazione, secondo le modalità concordate e mediante i moduli di revoca individuati.

L'Incaricato della Registrazione integrerà le operazioni di revoca dei certificati e provvederà alla richiesta di emissione di una nuova coppia di certificati, inoltrando richiesta scritta di revoca o di riattivazione del certificato, ricevuta dal Titolare e copia della denuncia. Qualora il Titolare ometta di presentarsi presso degli Incaricati della Registrazione, il certificato rimane sospeso fino alla naturale scadenza dello stesso.
La richiesta di revoca e sospensione deve essere inoltrata, munita di sottoscrizione del Titolare, con la specificazione della sua decorrenza (revoca).

In caso di smarrimento/furto o danneggiamento del dispositivo per un uso non appropriato che comporti l'acquisto di un nuovo dispositivo di firma (smartcard/businessKey), ***il costo sarà addebitato al Dipendente Titolare del dispositivo***.

11.3.2 Revoca in caso di cessazione attività o cambio funzione lavorativa

Il Titolare, in caso di cessazione attività o cambio funzione lavorativa, deve avvisare immediatamente l'Incaricato della Registrazione, compilare il modulo di revoca, corredato di documento di identità e restituire il dispositivo di firma.

L'Incaricato della Registrazione provvederà a inoltrare la richiesta di revoca, munita di sottoscrizione del Titolare, con la specificazione della sua decorrenza (revoca).

11.4 RINNOVO DEL CERTIFICATO QUALIFICATO

Il rinnovo del certificato deve essere effettuato prima che sia scaduto. A seguito di un avviso di scadenza tramite email da parte del Certificatore Accreditato, il Titolare trasmette la richiesta agli Incaricati dell'Ufficio di Registrazione, che, dopo averne verificato la legittimità e la validità, provvede al rinnovo del certificato.
Tale modalità è valida esclusivamente per il primo rinnovo. Successivamente, il Titolare che intende continuare ad avvalersi del servizio di certificazione, dovrà richiedere un nuovo dispositivo.
Qualora il certificato risulti già scaduto o revocato sarà necessario effettuare una nuova emissione e il costo sarà addebitato al **Titolare.**

11.5 CONSEGNA

La consegna dei dispositivi avverrà presso l'Ufficio degli Incaricati della Registrazione.