Certificatore InfoCert

Certificati di Sottoscrizione per Agos Ducato SpA
Addendum Manuale Operativo ICERT-INDI-MO

Codice Documento: ICERT-INDI-MO-AGOS

Questa pagina è lasciata
intenzionalmente bianca

1 Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.2	**Data Versione/Release**:	15/02/2016
Descrizione modifiche:	Modifica indirizzi, numeri di telefono e altri dati aziendali		
Motivazioni:			

Versione/Release n°:	1.1-	**Data Versione/Release**:	04/09/2013
Descrizione modifiche:	§ 1.2, § 1.4, § 2; § 2.2.3, § 2.2.4, § 2.4, § 3.1.2, § 3.1.3, § 3.1.4, § 3.1.5; § 3.1.6, § 3.2, § 3.3.1, § 3.4.1, § 3.7.1, § 4, § 4.1, § 4.1.1, § 4.1.2, § 4.1.2.1, § 4.1.3, § 4.1.4, § 4.1.5, § 4.1.6, § 4.1.7, § 4.1.7.1, § 4.1.7.2, § 4.1.7.3, § 4.1.7.4, § 4.2, § 4.3, § 4.3.1, § 4.3.2, § 4.3.3, § 5.1, § 5.1.2, § 5.2, § 5.2.1, § 5.2.2, § 5.2.3, § 5.3, § 5.3.1, § 5.3.2, § 5.3.2.1, § 5.3.3, § 5.3.4, § 5.3.5, § 5.3.6, § 5.3.7, § 5.4, § 7		
Motivazioni:	Miglioramento coerenza delle relazioni tra Addendum Agos Ducato e Manuale Operativo ICERT-INDI-MO. Sostituzione “DigitPA” con “AgID”		

Versione/Release n°:	1.0-	**Data Versione/Release**:	30/07/2012
Descrizione modifiche:	Prima Elaborazione		
Motivazioni:	Rilascio di certificati nell’ambito dei processi di contrattualizzazione di Agos Ducato S.p.A.		

1.2 Scopo campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCert per l’emissione dei certificati per chiavi di sottoscrizione nell’ambito dei processi di contrattualizzazione a distanza adottati da Agos Ducato S.p.A., in conformità con la vigente normativa in materia di firma digitale.
Il presente documento costituisce un addendum al Manuale Operativo ICERT-INDI-MO che ne è da questi integrato o disapplicato, secondo quanto descritto.

Per i processi di emissione dei certificati per chiavi di sottoscrizione eventualmente messi in opera da Agos Ducato S.p.A. con meccanismi differenti da quelli descritti dal presente Addendum si applica esclusivamente e solamente il Manuale Operativo ICERT-INDI-MO.

1.3 Riferimento normativi e tecnici

Trova piena applicazione il paragrafo 1.3 del Manuale Operativo ICERT-INDI-MO, cui si aggiungono i riferimenti normativi numerati come [24] e [25] specificati oltre.

Riferimenti normativi

[24] Decreto Legislativo 1 settembre 1993, n. 385, Testo unico delle leggi in materia bancaria e creditizia (nel seguito referenziato come TUB);

[25] Decreto legislativo 13 agosto 2010, n. 141, Attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonché modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi.

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Si intendono richiamate espressamente le definizioni già indicate nel Manuale Operativo ICERT-INDI-MO al paragrafo 1.3. Per i termini definiti dal **TU**, dal **CAD** e dal **DPCM** si rimanda alle definizioni in essi stabilite.
Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici o il codice identificativo assegnato all'oggetto dal Certificatore o da Agos Ducato.

Addendum Agos Ducato

Il presente documento, il quale integra o disapplica il Manuale Operativo ICERT-INDI-MO del Certificatore relativamente alle specifiche procedure di rilascio da remoto dei certificati qualificati di firma digitale adottati nei processi di contrattualizzazione di Agos Ducato. Per quanto non previsto nell'Addendum Agos Ducato si applica il Manuale Operativo ICERT-INDI-MO.

Agos Ducato

La **Agos Ducato S.p.A.** - Via Bernina, 7 - 20158 Milano - www.agosducato.it - Capitale Sociale Euro 338.655.200,00 I.V. Registro delle Imprese di Milano n. di C.F./P.IVA 08570720154 - Società autorizzata all'esercizio dell'attività finanziaria ai sensi dell'art. 106 del Dlgs. 385/93 n°iscr. all'elenco 5373 e sottoposta alla Vigilanza della Banca d'Italia ai sensi dell'art. 107 del Dlgs. 385/93 - N. di iscr. all'elenco 19309.4 - Iscritta all'albo degli istituti di pagamento di cui all'art. 114-septies del T.U.B. - Intermediario assicurativo iscritto al Registro degli Intermediari Assicurativi Sezione D. n° di iscr. D000200619

Autorità per la marcatura temporale [Time-stamping authority]

È il sistema software/hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale.

Certificato, Certificato Digitale, Certificato X.509 [Digital Certificate]

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.
Nel certificato compaiono altre informazioni tra cui:

- il Certificatore che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificato Qualificato – cfr. CAD

Certificatore [Certification Authority] – cfr. CAD

Certificatore Accreditato – cfr. CAD

Certificatore Qualificato – cfr. CAD

Chiave Privata e Chiave Pubblica – cfr. CAD

Cliente

Il soggetto che ha o intende instaurare rapporti contrattuali con Agos Ducato. Sono individuate tre categorie:

- ***Cliente Attivo***: un soggetto che, alla data di richiesta del certificato è parte di un contratto vigente con Agos Ducato e ha un rapporto continuativo in corso;
- ***Cliente non Attivo***: un soggetto censito nell'anagrafica Agos Ducato ma che, alla data di richiesta del certificato, non ha un rapporto contrattuale vigente con Agos Ducato;
- ***Prospect***: un soggetto non censito nell'anagrafica di Agos Ducato e che, al momento della richiesta del certificato, non ha un rapporto contrattuale vigente con Agos Ducato.

Codice di emergenza - ERC

Codice consegnato in busta elettronica sicura dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di sospensione di un certificato.

Dati per la creazione di una firma – cfr. CAD

Dati per la verifica della firma – cfr. CAD

Documento informatico

La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Nell'ambito della modalità prevista dal presente Addendum Agos Ducato, documenti informatici sono le clausole contrattuali sottoscritte dal Titolare con il Certificatore Qualificato InfoCert e la documentazione contrattuale Agos Ducato oggetto di sottoscrizione.

Evidenza Informatica

Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica e che attesta l'avvenuta elaborazione delle informazioni binarie.

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

Firma digitale [digital signature] – cfr. CAD

Giornale di controllo

Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche [5].

Lista dei Certificati Revocati o Sospesi [Certificate Revocation List - CRL]

E' una lista di certificati che non possono essere utilizzati per firmare in quanto scaduti, sospesi o revocati. Se il certificato è sospeso, la presenza nella CRL è temporanea e transitoria, la presenza è definitiva se il certificato è revocato.
L'inserimento nella lista è effettuato mediante inserimento del numero di serie del certificato nella CRL, che viene quindi pubblicata nel registro pubblico.

Manuale Operativo – cfr. art. 40 DPCM

Il Manuale Operativo definisce le procedure che il Certificatore applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Agenzia per l'Italia Digitale e quelle della letteratura internazionale. Nel presente documento il Manuale Operativo del Certificatore Accreditato InfoCert è codificato come ICERT-INDI-MO.

OTP - One Time Password

Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Titolare in un momento immediatamente antecedente all'apposizione della firma digitale.

Procedure Alert Antifrode

Procedure adottate da Agos Ducato al fine di prevenire le frodi ed accertare l'identità del ***Titolare***.

Procedure per la Certificazione del numero di cellulare

Procedure adottate da Agos Ducato al fine di accertare il presidio in capo al ***Titolare*** del numero di telefono cellulare dichiarato.

RAO – Registration Authority Officer

Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un ***Titolare***, nonché ad attivare la procedura di certificazione per conto del ***Certificatore***. Ai fini del presente Addendum Agos Ducato il RAO è Agos Ducato.

Registro dei Certificati

Il Registro dei Certificati è un archivio che contiene tutti i certificati validi emessi dal ***Certificatore***.

Registro pubblico [Directory]
Il Registro pubblico è un archivio che contiene:

- tutti i certificati validi emessi dal ***Certificatore*** per i quali sia stata richiesta dal titolare la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Revoca o sospensione di un Certificato
È l'operazione con cui il ***Certificatore*** annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

Richiedente [Subscriber]
E' il soggetto che richiede all'***Ente Certificatore*** il rilascio di certificati digitali. Ai fini del presente Addendum Agos Ducato il ***Richiedente*** è Agos Ducato.

Titolare [Subject]– cfr. CAD
La persona fisica, cliente di Agos Ducato, identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al ***Titolare*** è attribuita la firma digitale generata con la chiave privata della coppia.

Utente [Relying Party]
Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma digitale basata su quel certificato

1.5 Acronimi e abbreviazioni

ACBI – Associazione per il Corporate Banking Interbancario

AgID – Agenzia per l'Italia Digitale

CAD – Codice dell'amministrazione digitale
Ci si riferisce al D. Lgs n. 82/2005 e sue successive modificazioni, *"Codice dell'amministrazione digitale"*.

CIE – Carta di Identità Elettronica

CNS – Carta Nazionale dei Servizi

CRL – Certificate Revocation List

DN – Distinguished Name
Identificativo del ***Titolare*** di un certificato di chiave pubblica; tale codice è unico nell'ambito dei Titolari che abbiano un certificato emesso dal ***Certificatore***.

DPCM - Decreto del Presidente del Consiglio dei Ministri

Ci si riferisce al DPCM [5]

ETSI - European Telecommunications Standards Institute

HSM – Hardware Secure Module

insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche (DPCM, art 1, comma 1, lettera p)

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.

ISO - International Organization for Standardization

Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union

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.

IUT – Identificativo Univoco del Titolare

E' un codice associato al ***Titolare*** che lo identifica univocamente presso il ***Certificatore***; il ***Titolare*** ha codici diversi per ogni certificato in suo possesso.

LDAP – Lightweight Directory Access Protocol

Protocollo utilizzato per accedere al registro dei certificati.

OID – Object Identifier

E' costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

OTP – One Time Password

Meccanismo per l'autenticazione informatico basato sull'utilizzo non ripetibile di password. Può essere basato su dispositivi hardware o su procedure software.

PIN – Personal Identification Number

Codice associato ad un dispositivo sicuro di firma, utilizzato dal ***Titolare*** per accedere alle funzioni del dispositivo stesso.

SSCD – Secure Signature Creation Device

cfr. Dispositivo sicuro per la creazione della firma.

TSA – Time Stamping Authority

L'autorità di certificazione registrata presso l'Agenzia per l'Italia Digitale che certifica le chiavi dei sistemi (cfr. TSU) che firmano le marche temporali (Time Stamp Token).

TST – Time-Stamp Token

Termine usato nella pubblicistica internazionale per la marca temporale.

TSU – Time Stamp Unit

Il componente fidato, le cui chiavi, certificate dalla TSA, firmano le marche temporali.

TU – Testo Unico

Ci si riferisce al DPR n. 445/2000 e sue successive modificazioni, "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*".

Altri acronimi ed abbreviazioni sono utilizzati all'interno del testo con indicazione del loro significato.

2 Generalità

Come indicato nel Manuale Operativo ICERT-INDI-MO, un certificato lega la chiave pubblica ad un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata: tale soggetto è il "***Titolare***" del certificato. Il certificato è usato da altri soggetti, definiti "***Utenti***" per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma digitale apposta o associata ad un documento.

Ancora, il certificato garantisce la corrispondenza tra la chiave pubblica ed il ***Titolare*** del certificato. Il grado d'affidabilità di quest'associazione è legato a diversi fattori: la modalità con cui il ***Certificatore*** ha emesso il certificato, le misure di sicurezza adottate, gli obblighi assunti dal ***Titolare*** per la protezione della propria chiave privata, le garanzie offerte dal ***Certificatore***.

Questo documento evidenzia le regole generali e le procedure seguite dal **Certificatore Accreditato** InfoCert (nel proseguo semplicemente indicato come il ***Certificatore***) per l'emissione e l'utilizzo di **Certificati Qualificati** (nel proseguo riferiti semplicemente come Certificati) di sottoscrizione **esclusivamente** nell'ambito delle procedure di contrattualizzazione a distanza adottate da Agos Ducato. Per i processi di emissione dei certificati per chiavi di sottoscrizione eventualmente messi in opera da Agos Ducato S.p.A. con meccanismi differenti da quelli descritti dal presente Addendum si applica esclusivamente e solamente il Manuale Operativo ICERT-INDI-MO.

Il presente Addendum Agos Ducato integra le pratiche seguite dal ***Certificatore*** nell'emissione del certificato, delle misure di sicurezza adottate, degli obblighi, delle garanzie e delle responsabilità, ed in generale di tutto ciò che rende affidabile un certificato, già indicate nel Manuale Operativo ICERT- INDI-MO. Per quanto non espressamente richiamato o disapplicato dal presente Addendum Agos Ducato devono intendersi valide ed operanti le previsioni del Manuale Operativo ICERT-INDI-MO.

Pubblicando tale Addendum Agos Ducato ed inserendo i riferimenti a tale documento nei certificati, il ***Certificatore*** consente ai ***Clienti*** e agli ***Utenti*** di valutare le caratteristiche e l'affidabilità del servizio di certificazione svolto nell'ambito dei processi di contrattualizzazione adottati da Agos Ducato.

2.1 Identificazione del documento

Questo documento è denominato "Certificati di sottoscrizione per Agos Ducato– Addendum al Manuale Operativo ICERT-INDI-MO" ed è caratterizzato dal codice documento: **ICERT-INDI-MO-AGOS**.
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.
Al documento è associato un *object identifier,* referenziato nell'estensione CertificatePolicy dei certificati .
Il significato degli OID è il seguente:

L'*object identifier* (OID) **1.3.76.36.1.1.30** identifica:

InfoCert	1.3.76.36
certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
Manuale-operativo-firma-remota basata su HSM c/o InfoCert per Agos Ducato	1.3.76.36.1.1.30

I certificati riportano l'ulteriore OID **1.3.76.24.1.1.2**, che indica l'aderenza delle procedure InfoCert alle regole previste da ACBI e recepite dall'accordo quadro con AssoCertificatori.
OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo § 4.1.5 del Manuale Operativo ICERT-INDI-MO. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del suddetto Manuale Operativo.

Questo documento è pubblicato in formato elettronico presso il sito Web del ***Certificatore*** all'indirizzo: http://www.firma.infocert.it/doc/manuali.htm.

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCert S.p.A. è il ***Certificatore Accreditato*** (ai sensi dell'art. 29 del **CAD**) che emette, pubblica nel registro e revoca i Certificati Qualificati, operando in conformità alle Regole Tecniche [5] e secondo quanto prescritto dal **CAD**. In questo documento si usa il termine ***Certificatore Accreditato***, o per brevità ***Certificatore***, per indicare InfoCert.
I dati completi dell'organizzazione che svolge la funzione di ***Certificatore*** sono riportati nel Manuale Operativo ICERT-INDI-MO.

2.2.2 Uffici di registrazione

Le funzioni ed attività degli Uffici di Registrazione sono indicate al paragrafo 2.2.2. del Manuale Operativo ICERT-INDI-MO.
Nell'ambito del presente Addendum Agos Ducato, le funzioni di Ufficio di Registrazione sono svolte **esclusivamente** da Agos Ducato, che le svolge per mezzo di suoi incaricati nell'ambito della propria organizzazione.

2.2.3 Registro dei Certificati

Come previsto per le regole generali e le procedure indicate nel Manuale Operativo ICERT-INDI-MO, anche per quelle riferite al presente Addendum Agos Ducato, le liste di revoca e di sospensione dei certificati sono pubblicate in un ***registro pubblico*** che contiene anche i certificati dei ***Titolari*** che ne hanno fatto espressa richiesta.
Il ***registro dei certificati***, che contiene **tutti** i certificati emessi dal ***Certificatore***, **non** è pubblico.
Il ***Certificatore*** utilizza sistemi affidabili per la gestione del **registro pubblico** e del **registro dei certificati** con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal ***Titolare*** del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza.

2.2.4 Applicabilità

I certificati emessi dal ***Certificatore*** Accreditato InfoCert nelle modalità indicate dal presente Addendum Agos Ducato sono ***Certificati Qualificati*** ai sensi dell'art. 28 del CAD.
L'utilizzo dei certificati di sottoscrizione (***Certificati Qualificati***) è il seguente:

- il certificato emesso dal ***Certificatore*** sarà usato per verificare la Firma Digitale del ***Titolare*** cui il certificato appartiene.

Il ***Certificatore*** InfoCert mette il certificato a disposizione del ***Titolare*** e degli ***Utenti*** per consentire la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Deliberazione CNIPA [4];
Il prodotto messo a disposizione per la verifica è descritto al §6 del Manuale Operativo ICERT-INDI-MO. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.
In presenza di accordi di certificazione, il ***Certificatore*** riconosce la validità delle regole del ***Certificatore*** accreditato con cui stipula l'accordo e viceversa. Pertanto il certificato emesso per l'altro ***Certificatore*** sarà usato unicamente per verificare la firma di tale ***Certificatore*** sui certificati qualificati da questi emessi.

2.3 Contatto per utenti finali e comunicazioni

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.
Domande, reclami, osservazioni e richieste di chiarimento in ordine al presente Addendum Agos Ducato dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto 3
35131 Padova

Telefono: 06836691
Fax : 049 0978914
Call Center Firma Digitale: 199.500.130

Web: http://www.firma.infocert.it/
e-mail: firma.digitale@legalmail.it

Il ***Titolare*** può richiedere copia della documentazione a lui relativa, compilando e inviando il modulo disponibile sul sito www.firma.infocert.it e seguendo la procedura ivi indicata.
La documentazione verrà inviata in formato elettronico all'indirizzo di email indicato nel modulo.

2.4 Rapporti con AgID

Il presente ***Addendum Agos Ducato***, in quanto integrativo del Manuale Operativo ICERT-INDI-MO compilato dal ***Certificatore*** nel rispetto delle indicazioni legislative, è stato consegnato, in copia, ad AgID (ex DigitPA) che lo rende disponibile pubblicamente.
I rapporti con AgID sono regolati secondo quanto indicato nel Manuale Operativo ICERT-INDI-MO al § 2.4.

3 Regole Generali

In questo capitolo si descrivono le condizioni generali con cui il ***Certificatore*** eroga il servizio di certificazione descritto in questo ***Addendum Agos Ducato***.

3.1 Obblighi e Responsabilità

3.1.1 Obblighi del Certificatore

Gli obblighi cui è soggetto il ***Certificatore*** sono riportati nella corrispondente sezione del Manuale Operativo ICERT-INDI-MO.

3.1.2 Obblighi dell'Ufficio di Registrazione Agos Ducato

Nella realizzazione delle regole e delle procedure previste dal presente ***Addendum Agos Ducato***, 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 codici di attivazione (***PIN*** di firma) e del dispositivo utilizzato per la ricezione dei codici ***OTP*** (telefono cellulare);
2. che il ***Titolare*** sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. che il ***Titolare*** sia informato in merito agli accordi di certificazione stipulati con altri ***Certificatori***, se presenti e comunicati dal ***Certificatore***;
4. 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;
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 concordate e previste nel presente ***Addendum Agos Ducato***;
6. la custodia con la massima diligenza delle proprie chiavi private ai fini di preservarne la riservatezza e l'integrità;
7. la comunicazione al ***Certificatore*** di tutti ***i dati e documenti informatici*** acquisiti durante l'identificazione allo scopo di attivare la procedura di emissione del certificato, rappresentati nella documentazione prodotta e sottoscritta durante il processo di emissione del certificato qualificato InfoCert (clausole contrattuali accettate dal ***Titolare***);
8. la verifica e inoltro al ***Certificatore*** delle richieste di revoca, sospensione, riattivazione e rinnovo attivate dal ***Richiedente*** secondo le modalità condivise;
9. l'esecuzione, ove prevista a suo carico, della revoca o sospensione dei certificati;
10. il mantenimento della correlazione univoca tra in numero di telefono cellulare e il ***Titolare,*** anche mediante il ricorso alle procedure alert antifrode referenziate in 1.3 .

L'***Ufficio di Registrazione*** terrà direttamente i rapporti con i ***Titolari*** ed è tenuto ad informarli circa le disposizioni contenute nel presente ***Addendum Agos Ducato*** e nel Manuale Operativo ICERT-INDI-MO, per le parti di sua applicazione.

3.1.3 Obblighi dei Titolari

Per i certificati qualificati di firma digitale emessi nell'ambito delle regole e delle procedure previste dal presente ***Addendum Agos Ducato***, il ***Titolare*** deve:

1. garantire la correttezza, veridicità e completezza delle informazioni fornite, al momento della richiesta del certificato, ad Agos Ducato che raccoglie la richiesta ed effettua l'identificazione;

2. garantire di proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
3. garantire l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo ICERT-INDI-MO, nel presente ***Addendum Agos Ducato*** e dalle vigenti leggi nazionali e internazionali;
4. garantire la richiesta di revoca o di sospensione dei certificati di cui è ***Titolare*** nei casi previsti dal presente ***Addendum Agos Ducato*** al § **Errore. Il segnalibro non è definito.**;
5. garantire la protezione della segretezza e conservazione del codice di attivazione (PIN) utilizzato per l'abilitazione del certificato di firma in luogo sicuro;
6. garantire la protezione della segretezza e conservazione del codice di emergenza per richiedere la sospensione del proprio certificato;
7. garantire l'utilizzo esclusivo della propria chiave privata, tramite il controllo delle credenziali di cui al successivo punto 8;
8. garantire di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato;
9. garantire l'uso esclusivo della procedura per la generazione delle firma fornita dal ***Certificatore***;
10. garantire l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e la custodia e l'utilizzo personale del certificato di firma;
11. garantire di non apporre firme elettroniche avvalendosi di chiavi private basate su un certificato emesso in base ad un certificato di certificazione che a lui sia noto essere stato revocato;
12. garantire la corretta ed univoca identificazione del dispositivo su cui viene generata/inviata la OTP, nonché la protezione della segretezza dell'OTP ricevuta e l'esclusivo utilizzo del suddetto dispositivo.

Non trovano applicazione gli obblighi del ***Titolare*** indicati al § 3.1.3 del Manuale Operativo ICERT-INDI-MO.

3.1.4 Obblighi degli Utenti

Gli obblighi degli ***Utenti*** sono specificati al paragrafo 3.1.4 del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

3.1.5 Obblighi del Terzo Interessato

Nell'ambito delle modalità previste dal presente ***Addendum Agos Ducato*** la previsione in questione non è applicabile.

3.1.6 Obblighi del Richiedente

Non trova applicazione il paragrafo 3.1.6 del Manuale Operativo ICERT-INDI-MO, che è sostituito dal seguente testo:

1. attenersi a quanto disposto dal presente Addendum Agos Ducato e al Manuale Operativo ICERT-INDI-MO per le parti di applicazione
2. provvedere tempestivamente all'inoltro, con le modalità descritte ai paragrafi 5.3.2, 5.3.4, 5.3.5, della richiesta di revoca, sospensione o riattivazione nei casi previsti ai paragrafi 5.3.1 e 5.3.3 del presente Addendum Agos Ducato.

3.2 Clausola risolutiva espressa ai sensi dell'art. 1456 c.c.

Si applica ai certificati rilasciati in base al presente ***Addendum Agos Ducato*** la clausola risolutiva espressa di cui al paragrafo 3.2. del Manuale Operativo ICERT-INDI-MO, nonché le clausole eventualmente previste nei contratti con tra ***Certificatore*** e ***Richiedente***.
In particolare, per le modalità previste dall'***Addendum Agos Ducato***, l'inadempimento da parte dell'***Ufficio di Registrazione***, del ***Titolare*** e del ***Richiedente*** dei rispettivi obblighi descritti nei precedenti punti 3.1.2, 3.1.3, e 3.1.6 costituisce inadempimento essenziale ai sensi dell'art. 1456 c.c. e dà facoltà al ***Certificatore*** di risolvere il contratto eventualmente intercorso con tali soggetti.

3.3 Limitazioni e indennizzi

3.3.1 Limitazioni della garanzia e limitazioni degli indennizzi

Il ***Certificatore*** ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato trattato ed accettato dall'Agenzia per l'Italia Digitale, che ha come massimali:

- 1.500.000 euro per singolo sinistro
- 1.500.000 euro per annualità.

Il ***Certificatore*** si assume le responsabilità previste dal ***CAD*** per i soggetti che svolgono funzione di ***Ufficio di Registrazione***.

3.4 Pubblicazione

3.4.1 Pubblicazioni di informazioni relative al Certificatore

Il presente ***Addendum Agos Ducato*** è reperibile in formato elettronico presso il sito web del ***Certificatore*** e presso l'elenco AgID dei ***Certificatori.***

Il Manuale Operativo ICERT-INDI-MO, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative al ***Certificatore*** previste dal **DPCM** sono pubblicate presso l'elenco AgID dei ***Certificatori***.

3.4.2 Pubblicazione dei certificati

I certificati emessi in conformità al presente ***Addendum Agos Ducato*** non sono pubblicati.

3.4.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: **ldap://ldap.infocert.it**
Tale accesso può essere effettuato tramite i software messi a disposizione dal ***Certificatore*** e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP.
Il ***Certificatore*** potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

3.5 Verifica di conformità

Con frequenza non superiore all'anno, il ***Certificatore*** esegue un controllo di conformità di questo ***Addendum Agos Ducato*** al proprio processo di erogazione del servizio di certificazione.

3.6 Tutela dei dati personali

Le informazioni relative al ***Titolare*** e al ***Richiedente*** di cui il ***Certificatore*** viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico {chiave pubblica, certificato (se richiesto dal ***Titolare***), date di revoca e di sospensione del certificato}.
In particolare i dati personali vengono trattati dal ***Certificatore*** in conformità con il Decreto Legislativo 30 giugno 2003, n. 196.

3.7 Tariffe

3.7.1 Rilascio, rinnova, revoca e sospensione

La tariffe dei certificati rilasciati in base al presente ***Addendum Agos Ducato*** sono coperte secondo quanto previsto negli accordi intercorsi tra ***Certificatore*** e ***Agos Ducato***.

3.7.2 Accesso al certificato e alle liste di revoca

L'accesso al **registro pubblico** (lista dei certificati revocati o sospesi) è libero e gratuito.

4 Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per l'identificazione del cliente che intende diventare ***Titolare*** del certificato qualificato di sottoscrizione nell'ambito delle regole e delle procedure previste dal presente ***Addendum Agos Ducato*** per i certificati qualificati emessi nell'ambito delle procedure di vendita a distanza Agos Ducato.

4.1 Identificazione ai fini del primo rilascio

Il ***Certificatore*** deve verificare l'identità del ***Titolare*** del certificato di sottoscrizione richiesto.

4.1.1 Abilitazione di Agos Ducato all'identificazione

Ferma restando la responsabilità del ***Certificatore*** (§3.1.1), ***Agos Ducato***, in qualità di ***Ufficio di Registrazione*** è abilitata ad accertare l'identità del ***Cliente*** che richiede il certificato digitale di sottoscrizione con la seguente modalità:

Modalità 2
Tramite le procedure applicate ai sensi del D.L.vo n. 231/2007.

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 2

Nella modalità 2 l'Ufficio di Registrazione, nella sua qualità di Intermediario finanziario, provvede al riconoscimento del Titolare (Attivo, Non Attivo e Prospect) sulla base delle procedure adottate ai sensi degli articoli 19, co. 1 lettera a) (identificazione e verifica dell'identità del cliente in sua presenza), 22 (modalità di attuazione degli obblighi di adeguata verifica nei confronti dei nuovi clienti e della clientela già acquisita) 28 (identificazione e verifica dell'identità del cliente, anche in sua assenza, mediante l'adozione di misure rafforzate di adeguata verifica) 29 e 30 (identificazione e verifica dell'identità del cliente, anche in sua assenza, in quanto dette attività vengono effettuate da parte di terzi) del D.Lgs. 231/2007, e ss.mm.ii.; ovvero alle analoghe procedure adottate secondo la normativa antiriciclaggio vigente alla data del riconoscimento al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale).
I dati identificativi del Titolare raccolti da Agos Ducato all'atto del riconoscimento vengono utilizzati direttamente per l'emissione dei certificati, previa accettazione da parte del Titolare delle condizioni contrattuali per il rilascio del certificato e degli strumenti per l'apposizione della firma (siano essi SSCD o credenziali e strumenti per il controllo dei propri dati per la creazione della firma) nonché approvazione e conferma dei dati anagrafici registrati.
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.3 Modalità operative per la richiesta di rilascio del certificato di sottoscrizione

Nell'ambito delle regole e delle procedure previste dal presente ***Addendum Agos Ducato***, i passi principali a cui il ***Titolare*** deve attenersi per ottenere un certificato di sottoscrizione dall'***Ufficio di Registrazione Agos Ducato*** sono:

a) in generale, prendere visione del Manuale Operativo ICERT-INDI-MO e, in particolare del presente ***Addendum Agos Ducato*** e dell'eventuale ulteriore documentazione informativa;
b) seguire le procedure di identificazione adottate dal ***Certificatore*** come descritte nel presente paragrafo;
c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
d) inoltrare la richiesta di registrazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio.

Nell'ambito delle modalità previste dal presente ***Addendum Agos Ducato*** in accordo con il § 4.1.3 del Manuale Operativo ICERT-INDI-MO, nella richiesta di registrazione sono contenute sia i dati relativi all'identità del ***Cliente*** che le informazioni che consentono di gestire in maniera efficace il rapporto tra il ***Certificatore*** ed il ***Titolare***. Il modulo di richiesta è inoltrato dal ***Titolare*** e di esso viene conservata apposita evidenza informatica.

4.1.4 Informazioni che il Titolare deve fornire

Sono considerate **obbligatorie** le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale o analogo codice identificativo[1]
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso
- e-mail per l'invio delle comunicazioni dal ***Certificatore*** al ***Titolare***, anche attraverso l'Ufficio di Registrazione
- numero di telefonia mobile per la trasmissione della OTP.

Opzionalmente il ***Titolare*** può fornire un altro nome, con il quale è comunemente conosciuto, che sarà inserito in un apposito campo denominato *commonName* (nome comune) del SubjectDN del certificato.
Il commonName, nel caso in cui non venisse fornito alcun ulteriore nome dal ***Titolare***, sarà valorizzato con nome e cognome del ***Titolare*** stesso.

4.1.5 Uso di pseudonimi

Nell'ambito delle modalità previste dal presente ***Addendum Agos Ducato***, non è previsto l'uso di pseudonimi. Non si applica quindi la previsione di cui al § 4.1.4 del Manuale Operativo ICERT-INDI-MO.

4.1.6 Limiti d'uso e limiti di valore

Nei certificati emessi in conformità al presente manuale è inserito il seguente limite d'uso: "Questo certificato può essere utilizzato solo nei rapporti tra il Titolare ed il Richiedente Agos Ducato"

Inoltre il controllo applicativo svolto dal Certificatore nell'ambito dei sistemi di gestione dell'HSM garantisce che le chiavi private associate a certificati emessi in conformità al presente Manuale Operativo possono essere utilizzate solo nei rapporti tra il Titolare ed il Richiedente Agos Ducato.

L'inserimento di ulteriori limiti d'uso e di valore non è consentito: non trovano applicazione le previsioni di cui al paragrafo 4.1.5 del Manuale Operativo ICERT-INDI-MO.

4.1.7 Inserimento del Ruolo e dell'Organizzazione nel certificato

Per i certificati emessi in base al presente ***Addendum Agos Ducato*** non è prevista la facoltà di inserimento del Ruolo nel certificato. Non trovano applicazione le previsioni di cui al paragrafo § 4.1.6 del Manuale Operativo ICERT-INDI-MO.

[1]Per i cittadini stranieri che non fossero in possesso del codice fiscale nè di alcun altro codice identificativo nazionale, deve essere presentato il passaporto, il cui identificativo sarà inserito nel certificato nello spazio predisposto per il codice fiscale nel formato PASSPORTXXXXX

4.1.7.1 Titoli e/o Abilitazioni Professionali

Per i certificati emessi in base al presente ***Addendum Agos Ducato*** non è prevista la facoltà di inserimento di Titoli e/o Abilitazioni professionali. Non trovano applicazione le previsioni di cui al paragrafo § 4.1.6.1 del Manuale Operativo ICERT-INDI-MO.

4.1.7.2 Poteri di rappresentanza di persone fisiche

Per i certificati emessi in base al presente ***Addendum Agos Ducato*** non è prevista la facoltà di inserimento di poteri di rappresentanza di persone fisiche. Non trovano applicazione le previsioni di cui al paragrafo § 4.1.6.2 del Manuale Operativo ICERT-INDI-MO.

4.1.7.3 Poteri di rappresentanza di enti di diritto privato o appartenenza agli stessi

Per i certificati emessi in base al presente ***Addendum Agos Ducato*** non è prevista la facoltà di inserimento nel certificato di poteri di rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi. Non trovano applicazione le previsioni di cui al paragrafo § 4.1.6.3 del Manuale Operativo ICERT-INDI-MO.

4.1.7.4 Esercizio di Funzioni Pubbliche, Poteri di Rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi.

Per i certificati emessi in base al presente ***Addendum Agos Ducato*** non è prevista la facoltà di inserimento nel certificato di informazioni sull'esercizio di Funzioni Pubbliche, su poteri di rappresentanza di organizzazioni ed enti di diritto pubblico o appartenenza agli stessi. Non trovano applicazione le previsioni di cui al paragrafo § 4.1.6.4 del Manuale Operativo ICERT-INDI-MO.

4.2 Autenticazione per rinnovo delle chiavi e certificati

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (*validity*) con gli attributi "valido dal" (*not before*) e "valido fino al*" (not after).*

NOTA

le date indicate negli attributi suddetti sono espresse nel formato

anno-mese-giorno-ore-minuti-secondi-timezone
{AAAAMMGGHHMMSSZ}

nella rappresentazione UTCTime prevista dallo standard di riferimento [20]

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

4.3 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire esclusivamente su richiesta del ***Titolare,*** del ***Richiedente*** ovvero su iniziativa del ***Certificatore***.
Il ***Certificatore*** autentica chi fa richiesta di revoca e sospensione.

4.3.1 Richiesta da parte del Titolare

Nell'ambito delle modalità dell'***Addendum Agos Ducato***, se la richiesta viene effettuata per telefono o via Internet, il ***Titolare***, esclusivamente per la funzione di sospensione, si autentica fornendo il codice di emergenza, consegnato assieme al certificato che intende sospendere.

4.3.2 Richiesta da parte del Terzo Interessato

Nell'ambito delle modalità previste dal presente ***Addendum Agos Ducato***, la previsione in questione non è applicabile. Non trovano applicazione le previsioni di cui al paragrafo § 4.3.2 del Manuale Operativo ICERT-INDI-MO.

4.3.3 Richiesta da parte del Richiedente

Nell'ambito delle modalità previste dal presente ***Addendum Agos Ducato***, il ***Richiedente*** che, nelle ipotesi contrattualmente previste con il ***Certificatore***, richiede la revoca o sospensione del certificato del ***Titolare*** esegue la revoca e la sospensione, in qualità di ***RAO***.
La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 5.3.2 dell'***Addendum Agos Ducato***.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca o sospensione del ***Richiedente*** in apposite convenzioni da stipulare con lo stesso.

5 Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato secondo le procedure descritte nel presente ***Addendum Agos Ducato*** è necessario eseguire una procedura di registrazione durante la quale i dati dei ***Titolari*** vengono validati dall'***Ufficio di Registrazione*** Agos Ducato e memorizzati negli archivi del ***Certificatore***.

La registrazione iniziale è effettuata dall' ***Ufficio di Registrazione***, anche telematicamente.

Conclusasi la fase di registrazione iniziale, il rilascio del certificato digitale è previsto in unica modalità, ossia con chiavi generate su dispositivi HSM.

Per la conferma delle operazioni di rilascio al Titolare verrà richiesto l'utilizzo di un dispositivo ***OTP*** le cui caratteristiche (SMS su cellulare) sono verificate mediante la ***Procedura di Certificazione del Cellulare*** che si aggiunge alle ***Procedure Alert Antifrode*** in essere presso l'Ufficio di Registrazione.

Le modalità di registrazione del ***Titolare*** e di identificazione dello stesso sono diverse in base ai rapporti tra ***Titolare*** ed ***Ufficio di Registrazione***.

Qualora il ***Titolare*** sia un ***Cliente Attivo***, i dati identificativi sono attestati dall'***Ufficio di Registrazione*** sulla base del riconoscimento precedentemente svolto ai sensi del D.L.vo n. 231/2007 e dell'esistenza di un rapporto contrattuale continuativo con il ***Titolare*** al momento della richiesta di rilascio del certificato.

Qualora il ***Titolare*** sia un ***Cliente non Attivo*** o un ***Prospect*** deve essere effettuato il riconoscimento ai fini del rilascio del certificato. L'***Ufficio di Registrazione*** procede pertanto a svolgere tale riconoscimento sulla base del D.L.vo n. 231/2007.

1. Il ***Titolare***, utilizzando un sito dell'***Ufficio di Registrazione***, richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici;
2. Il ***Titolare*** inserisce i propri dati;
3. Successivamente, il ***Titolare*** è reindirizzato su una procedura web sviluppata dalla ***Certification Authority***, si autentica e conferma i propri dati manifestando la volontà di ottenere il rilascio di un certificato digitale mediante conferma sulla procedura web. L'***Ufficio di Registrazione*** raccoglie la richiesta e la trasmette al ***Certificatore,*** insieme ai dati del ***Titolare***;
4. il ***Certificatore*** provvede a rilasciare al ***Titolare*** un certificato digitale;
5. L'***Ufficio di Registrazione*** avvia, dove necessario, le procedure di identificazione certa del ***Titolare*** ai sensi del D. L.vo n. 231/2007. Attraverso le ***Procedure di Alert Antifrode***, l'***Ufficio di Registrazione*** verifica l'identità del ***Titolare*** e l'effettivo presidio del numero di cellulare comunicato, comunicando l'esito al ***Certificatore***, per l'attivazione o l'eventuale revoca del certificato.

Non trovano applicazione le disposizioni di cui ai paragrafi 5.1 e 5.2 del Manuale Opertivo ICERT-INDI-MO, che continuano ad applicarsi solamente ai certificati digitali eventualmente rilasciati da Agos Ducato al di fuori del perimetro del presente ***Addendum Agos Ducato.***

5.1.1 Generazione delle chiavi

Le chiavi asimmetriche sono generate all'interno del Dispositivo Sicuro per la Creazione della Firma (SSCD) utilizzando le funzionalità native offerte dai dispositivi stessi.
L'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è di 1024 bit.

5.1.2 Protezione delle chiavi private

La chiave privata del ***Titolare*** è generata e memorizzata in un'area protetta del dispositivo HSM che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione cancella la propria memoria, a protezione dei dati in essa contenuti.

Non trova applicazione il paragrafo 5.2.8 del Manuale Operativo ICERT-INDI-MO.

5.2 Emissione del certificato

L'emissione del certificato viene effettuata in modo automatico dalle procedure del ***Certificatore*** secondo i seguenti passi:

1. viene verificata la correttezza della richiesta di certificato controllando che:
   - il ***Titolare*** sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - al ***Titolare*** sia stato assegnato un codice identificativo unico nell'ambito degli utenti del ***Certificatore*** (IUT);
   - la coppia di chiavi funzioni correttamente;
2. viene controllata la validità della firma dell'***Ufficio di Registrazione*** che ha inviato l'evidenza informatica della richiesta
3. si procede alla generazione del certificato;
4. viene attestato il momento di generazione del certificato utilizzando quale riferimento temporale la data fornita dal sistema della ***Certification Authority*** e tale registrazione viene riportata sul giornale di controllo.
5. viene inviato al ***Titolare*** il codice di sicurezza ERC, in busta cifrata, da utilizzare per le richieste di sospensione;
6. il certificato viene memorizzato nei server del sistema di emissione;
7. il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati.

Non trova applicazione il paragrafo 5.3 del Manuale Operativo ICERT-INDI-MO.

5.2.1 Formato e contenuto del certificato

Si rimanda a quanto previsto dal paragrafo 5.3.1 del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

5.2.2 Pubblicazione del certificato

Si rimanda a quanto previsto dal paragrafo 5.3.2 del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

5.2.3 Validità del certificato

Si rimanda a quanto previsto dal paragrafo 5.3.3 del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

5.3 Revoca e sospensione di un certificato

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e rendono **non valide** le firme apposte successivamente al momento della pubblicazione della revoca.

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal ***Certificatore***, emessa e pubblicata nel registro dei certificati con periodicità prestabilita.
Il ***Certificatore*** può forzare un'emissione non programmata della CRL in circostanze particolari.
L'efficacia della revoca e della sospensione si ha dal momento di pubblicazione della lista, attestato dalla data apposta alla registrazione dell'evento nel Giornale di Controllo del ***Certificatore***.

5.3.1 Motivi per la revoca di un certificato

Secondo le modalità previste dal presente ***Addendum Agos Ducato***, il ***Certificatore*** esegue la revoca del certificato su propria iniziativa o per richiesta del ***Titolare*** o del ***Richiedente.***
Le condizioni per cui **DEVE** essere effettuata la richiesta di revoca sono le seguenti:

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
    a. sia venuta meno la segretezza della chiave o del suo codice d'attivazione (***PIN***) o il possesso del dispositivo indicato per la ricezione della ***OTP***;
    b. si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
2. si verifica un cambiamento dei dati del ***Titolare*** presenti nel certificato tale da rendere detti dati non più corretti e/o veritieri;
3. termina il rapporto tra il ***Titolare*** e il ***Certificatore***;
4. viene verificata una sostanziale condizione di non rispetto del presente ***Addendum Agos Ducato*** e/o del Manuale Operativo ICERT-INDI-MO, per le parti applicabili.

Il ***Titolare*** ha facoltà di richiedere la revoca di un certificato per un **qualunque** motivo dallo stesso ritenuto valido ed in qualsiasi momento.

5.3.2 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del soggetto che la pone in essere. Sono previsti i seguenti casi:

Revoca su iniziativa del *Titolare*

Il Titolare deve richiedere la revoca direttamente al ***Certificatore***, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede ad eseguire la revoca.

Chi richiede la revoca è tenuto a sottoscrivere la richiesta di revoca e inviarla al ***Certificatore*** per lettera o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

Non trova applicazione il caso "Revoca su iniziativa del Titolare" presente al paragrafo 5.4.2 del Manuale Operativo ICERT-INDI-MO.

Revoca su iniziativa del *Certificatore*

Trova piena applicazione il caso "Revoca su iniziativa del ***Certificatore***" presente al paragrafo 5.4.2 del Manuale Operativo ICERT-INDI-MO.

Revoca su iniziativa del *Terzo Interessato*

Non trova applicazione il caso "Revoca su iniziativa del Terzo Interessato" presente al paragrafo 5.4.2 del Manuale Operativo ICERT-INDI-MO.

Revoca su iniziativa del *Richiedente*

Agos Ducato, in qualità di ***Richiedente***, può revocare il certificato del ***Titolare***, rivolgendosi direttamente al ***Certificatore***.

La richiesta di revoca su iniziativa del ***Richiedente*** deve essere effettuata secondo la seguente modalità:

1. il ***Richiedente*** si autentica alle applicazioni del ***Certificatore*** e richiede la revoca del certificato, fornendo la motivazione della richiesta e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare***, eventualmente a mezzo dell'***Ufficio di Registrazione***, secondo le modalità di comunicazione stabilite all'atto dell'identificazione e procede alla revoca del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

Modalità aggiuntive per la richiesta di revoca da parte del ***Richiedente*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

Non trova applicazione il caso "Revoca su iniziativa del Richiedente" presente al paragrafo 5.4.2 del Manuale Operativo ICERT-INDI-MO.

5.3.2.1 Procedura per la revoca immediata

Nel caso di compromissione della chiave è necessario attivare la procedura di revoca immediata. Il ***Titolare*** è tenuto ad effettuare la richiesta di revoca specificando l'avvenuta o sospetta compromissione della chiave, dando luogo così alla revoca immediata.
Il processo di revoca segue i passi descritti nei casi precedenti con la particolarità che la pubblicazione della lista dei certificati revocati (CRL) avviene immediatamente.

5.3.3 Motivi per la sospensione di un certificato

Il ***Certificatore*** esegue la sospensione del certificato su propria iniziativa o per richiesta del ***Titolare***, o del ***Richiedente***.
La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il ***Titolare*** o il ***Certificatore*** acquisiscano elementi di dubbio sulla validità del certificato;
3. siano insorti dubbi sulla sicurezza del dispositivo OTP;
4. è necessaria un'interruzione della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato specificandone la durata; alla scadenza di tale periodo, alla sospensione seguirà o una revoca definitiva oppure la ripresa di validità del certificato.

5.3.4 Procedura per la richiesta di sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda del soggetto che la pone in essere.
La sospensione ha **sempre** una durata limitata nel tempo.
La sospensione termina alle ore 24:00:00 dell'ultimo giorno del periodo richiesto.

NOTA BENE:
il giorno di termine della sospensione non può essere successivo al giorno di scadenza del certificato.

Sono previsti i seguenti casi:

Sospensione su iniziativa del *Titolare*

Il ***Titolare*** deve richiedere la sospensione con una delle seguenti modalità:

1. utilizzando la funzione di sospensione disponibile nel sito Web del ***Certificatore***. Per effettuare la richiesta il ***Titolare*** **deve** comunicare:
2. i propri dati identificativi,
3. l'identificativo univoco a lui assegnato (IUT),
4. la motivazione,
5. la data di fine sospensione,
6. il codice di emergenza;
7. telefonando al Call Center del ***Certificatore*** e fornendo le informazioni di cui al punto precedente.

In assenza del codice di emergenza e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una **sospensione immediata** del certificato per una durata di **10 (dieci) giorni solari** in attesa della richiesta scritta del ***Titolare***; qualora il ***Certificatore*** non riceva la richiesta sottoscritta entro il termine indicato, il certificato verrà riattivato.

Il ***Titolare*** è tenuto a sottoscrivere la richiesta di sospensione e inviarla direttamente al ***Certificatore*** per lettera o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

Non trova applicazione il caso "Sospensione su iniziativa del Titolare" presente al paragrafo 5.4.5 del Manuale Operativo ICERT-INDI-MO.

Sospensione su iniziativa del *Certificatore*

Si rimanda al paragrafo 5.4.5 del Manuale Operativo MO-INDI-ICERT per la procedura per la sospensione del certificato su iniziativa del Certificatore, che trova piena applicazione.

Sospensione su iniziativa del Terzo Interessato

Non trova applicazione il caso "Sospensione su iniziativa del Terzo Interessato" presente al paragrafo 5.4.5 del Manuale Operativo ICERT-INDI-MO.

Sospensione su iniziativa del Richiedente

Agos Ducato, in qualità di ***Richiedente***, può sospendere il certificato del ***Titolare***, rivolgendosi direttamente al ***Certificatore***.

La richiesta di sospensione su iniziativa del ***Richiedente*** deve essere effettuata secondo la seguente modalità:

1. il ***Richiedente*** si autentica alle applicazioni del ***Certificatore*** e richiede la sospensione del certificato, fornendo la motivazione della richiesta, la data di fine sospensione (eventualmente coincidente con la data di scadenza del certificato) e specificando i dati del ***Titolare*** del certificato comunicati dal ***Certificatore*** al momento dell'emissione del certificato;
2. il ***Certificatore***, verificata l'autenticità della richiesta, la comunica al ***Titolare***, eventualmente a mezzo dell'***Ufficio di Registrazione***, secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla sospensione del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

Modalità aggiuntive per la richiesta di sospensione da parte del ***Richiedente*** potranno essere specificate negli eventuali accordi stipulati tra quest'ultimo ed il ***Certificatore***.

Non trova applicazione il caso "Sospensione su iniziativa del Richiedente" presente al paragrafo 5.4.5 del Manuale Operativo ICERT-INDI-MO.

5.3.5 Ripristino di validità di un certificato sospeso

Si rimanda al Manuale Operativo della CA InfoCert MO-INDI-ICERT, § 5.4.6 per il dettaglio delle modalità di riattivazione del certificato.

In aggiunta, per le modalità previste dall' ***Addendum Agos Ducato***, ***Agos Ducato*** in qualità di ***Richiedente*** può richiedere la riattivazione del certificato precedentemente posto in stato di sospensione.

5.3.6 Pubblicazione e frequenza di emissione della CRL

La Pubblicazione e frequenza di emissione della CRL è disciplinata al paragrafo 5.4.7. del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

5.3.7 Tempistica

La tempistica di emissione della CRL è disciplinata al paragrafo 5.4.8. del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

5.4 Sostituzione delle chiavi e rinnovo del Certificato

La procedura di sostituzione delle chiavi e rinnovo del certificato è disciplinata al paragrafo 5.5. del Manuale Operativo ICERT-INDI-MO, che trova piena applicazione.

6 Strumenti e modalità per l'apposizione e la verifica della firma digitale

La soluzione di firma digitale adottata da ***Agos Ducato*** si configura come un servizio di firma remota ai sensi dell'art. 1 comma 1 lettera q) del CAD, accessibile via rete (Internet).
La coppia delle chiavi crittografiche e il certificato digitale, risiede in modalità sicura nell'HSM sito presso il ***Certificatore*** e accessibile da remoto con modalità sicure.

Il certificato digitale è limitato applicativamente all'utilizzo esclusivo dello stesso nell'ambito dei rapporti tra il ***Titolare*** e ***Agos Ducato***, e solamente per sottoscrivere documenti presentati mediante la applicazioni ***Agos Ducato*** .

Il ***Titolare*** viene identificato dal servizio ed autorizza l'apposizione della firma tramite un meccanismo di sicurezza: all'atto della firma del documento il ***Titolare*** utilizza una One Time Password (***OTP***) ricevuta in tempo reale sul telefono cellulare e di un PIN di firma scelto in fase di rilascio del certificato, noto a lui solo noto.

Il codice ***OTP*** è di fatto una password "usa e getta", integralmente inserito dal firmatario nell'apposito box di firma del documento; il codice PIN è composto di 8 cifre, scelte dal ***Titolare*** al momento del rilascio.

Tutte le chiamate di firma sono inoltrate con modalità sicura da Agos Ducato al servizio del ***Certificatore,*** secondo le modalità tecniche concordate e contrattualizzate.

NOTA BENE: Alcuni formati permettono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che questo ne alteri la struttura binaria e tali da attivare funzionalità che possono modificare gli atti, i fatti o i dati rappresentati nel documento medesimo. I file firmati digitalmente che contengono tali strutture non producono gli effetti di cui all'articolo 21, comma 2 del CAD. Agos Ducato presenta per la firma al ***Titolare*** solo documenti in un formato privo di tale codice eseguibile.

7 Rinvio

Per quanto non espressamente previsto si vedano i paragrafi 7, 8, 9, 10, 11, 12, 13 e 14 del Manuale Operativo ICERT-INDI-MO, che trovano piena applicazione e a cui espressamente si rinvia.