Certificatore InfoCert

Certificati di Sottoscrizione per il Gruppo Findomestic
Addendum Manuale Operativo ICERT-INDI-MO

Codice Documento: ICERT-INDI-MO-FIND

1 Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.1	Data Versione/Release:	09/10/13
Descrizione modifiche:	Specificazione perimetro di utilizzabilità del certificato qualificato Allineamento riferimenti normativi		
Motivazioni:	Revisione periodica annuale del documento.		

Versione/Release n°:	1.0	Data Versione/Release:	15/05/12
Descrizione modifiche:	Prima elaborazione		
Motivazioni:	Rilascio di certificati nell'ambito dei processi di contrattualizzazione di Findomestic Banca S.p.A.		

1.2 Scopo e 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 adottati dalle società del Gruppo Findomestic, in conformità con la vigente normativa in materia di firma digitale.
Il presente documento costituisce un addendum al Manuale Operativo ICERT-INDI-MO e, per quanto in esso non richiamato, si applicano le regole e le procedure descritte nel suddetto Manuale Operativo.

1.3 Riferimenti normativi e tecnici

1.3.1 Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 – Codice dell'amministrazione digitale (nel seguito referenziato come **CAD**) e successive modifiche e integrazioni;
[2] --- non utilizzato ---
[3] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 e sue modificazioni secondo DPR 137/2003 – Disposizioni legislative in materia di documentazione amministrativa (nel seguito referenziato come **TU**);
[4] Deliberazione CNIPA 45/2009 – Regole per il riconoscimento e la verifica del documento informatico;
[5] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013. Referenziato nel seguito come **DPCM**;
[6] Decreto Legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali;
[7] Circolare CNIPA n. 48 del 6 settembre 2005;
[8] Legge 15 Marzo 1997, n. 59 (c.d. legge Bassanini);
[9] Legge 24 Dicembre 1993, n. 537;
[10] Legge 23 Dicembre 1993, n. 547;
[11] Legge 5 luglio 1991, n. 197 e successive modificazioni;
[12] Decreto del Ministero del Tesoro del 19 dicembre 1991; [13] Ufficio Italiano Cambi: parere del 14 giugno 2001;
[14] CIRCOLARE 19 giugno 2000 n. AIPA/CR/24;

[15] D.Lgs. 21 novembre 2007, n. 231 - Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione;
[16] Decreto del Presidente del Consiglio dei Ministri ottobre 2007 - Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'articolo 13, comma 4, del decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003;
[17] Decreto Legislativo 1 settembre 1993, n. 385, Testo unico delle leggi in materia bancaria e creditizia (nel seguito referenziato come **TUB**);
[18] 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.

1.3.2 Riferimenti tecnici

[19] Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" - Aprile 2002
[20] RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile [21] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
[22] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
[23] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

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 Findomestic.

Addendum Findomestic
Il presente documento, il quale integra il Manuale Operativo ICERT-INDI-MO del Certificatore relativamente alle procedure di rilascio dei certificati adottati nei processi di contrattualizzazione delle società del Gruppo Findomestic. Per quanto non previsto nell'Addendum Findomestic si applica il Manuale Operativo ICERT-INDI-MO.

Cliente
Il soggetto che ha o intende instaurare rapporti contrattuali con una società del Gruppo Findomestic. Sono individuate tre categorie:

- ***Cliente Identificato***: un soggetto che, alla data di richiesta del certificato è parte di un contratto vigente con Findomestic;
- ***Cliente non Identificato***: un soggetto censito nell'anagrafica Findomestic ma che, alla data di richiesta del certificato, non ha un rapporto contrattuale vigente con una società del Gruppo Findomestic;
- ***Prospect***: un soggetto non censito nell'anagrafica di Findomestic e che, al momento della richiesta del certificato, non ha un rapporto contrattuale vigente con una società del Gruppo Findomestic.

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

Findomestic
Una società del Gruppo Findomestic, iscritto all'albo dei Gruppi Bancari al N° 3115.3, e costituito da: Findomestic Banca S.p.A. in qualità di capo gruppo, Credirama S.p.A., BF5 S.p.A., Findomestic Banka a.d. Beograd.

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 Findomestic Banca, codificate come "*DO 10/12 DRC - processo di verifica delle alerts antifrode generate da telefoni sospetti*", al fine di prevenire le frodi ed accertare l'identità dei Clienti.

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***.

1.5 Acronimi e abbreviazioni

ACBI – Associazione per il Corporate Banking Interbancario

AgID– Agenzia per l'Italia Digitale
Già DigitPA, è stata istituita con decreto legge n. 83, convertito nella legge n. 134/2012 ed è l'ente preposto al coordinamento delle iniziative dell'Agenda 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 –

HSM - Hardware Secure Module
E' un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

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 AgID 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

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 per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma digitale apposta o associata ad un documento.

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 adottate dalle società del Gruppo Findomestic per la collocazione dei prodotti propri e dei partner.

Il presente Addendum Findomestic 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 derogato dal presente Addendum Findomestic devono intendersi valide ed operanti le previsioni del Manuale Operativo ICERT-INDI-MO.

Pubblicando tale Addendum Findomestic il ***Certificatore*** consente ai Clienti ed ai terzi di valutare le caratteristiche e l'affidabilità del servizio di certificazione svolto nell'ambito dei processi di contrattualizzazione adottati dalle società del Gruppo Findomestic.

2.1 Identificazione del documento

Questo documento è denominato "Certificati di sottoscrizione per Findomestic – Addendum al Manuale Operativo ICERT-INDI-MO" ed è caratterizzato dal codice documento: **ICERT-INDI-MO- FIND**.
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) **1.3.76.36.1.1.27** 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-automatica basata su HSM c/o InfoCert per Findomestic	1.3.76.36.1.1.27

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 §4.1.7 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 Findomestic, le funzioni di Ufficio di Registrazione sono svolte **esclusivamente** da Findomestic Banca S.p.A., sia per le altre società del Gruppo, in qualità di capogruppo, sia per le società con le quali il Gruppo Findomestic ha stretto rapporti di collaborazione.

2.2.3 Registro dei Certificati

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 Findomestic 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 a disposizione per la verifica delle firme il prodotto 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 Findomestic dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile Certificazione Digitale Corso Stati Uniti 14

35127 Padova
Telefono: 06836691
Fax : 049 8288 406

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 Findomestic in quanto integrativo del Manuale Operativo ICERT-INDI-MO, compilato dal ***Certificatore*** nel rispetto delle indicazioni legislative, è stato consegnato, in copia, all'Agenzia per l'Italia Digitale che lo rende disponibile pubblicamente.
I rapporti con AgID sono regolati secondo quanto indicato nel Manuale Operativo ICERT-INDI-MO.

3 Regole Generali

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

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 Findomestic

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;
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 previste nel Manuale Operativo ICERT-INDI-MO e nel presente Addendum Findomestic;
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 acquisiti durante l'identificazione allo scopo di attivare la procedura di emissione del certificato;
8. la verifica e inoltro al ***Certificatore*** delle richieste di revoca, sospensione e rinnovo attivate dal ***Titolare*** presso l'Ufficio di Registrazione;
9. l'esecuzione, ove prevista a suo carico, della revoca o sospensione dei certificati;
10. l'invio tempestivo al Certificatore delle evidenze informatiche relative alle richieste di certificazione;
11. il mantenimento della correlazione univoca tra in numero di telefono cellulare e il ***Titolare,***
12. anche mediante il ricorso alle procedure alerts antifrode referenziate in 1.4

L'Ufficio di Registrazione terrà direttamente i rapporti con i Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Addendum Findomestic e nel Manuale Operativo ICERT-INDI-MO.

3.1.3 Obblighi dei Titolari

Il ***Titolare*** deve garantire:

1. la correttezza, veridicità e completezza delle informazioni fornite al momento della richiesta del certificato al soggetto che raccoglie la medesima ed effettua l'identificazione;
2. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo ICERT-INDI-MO, nel presente Addendum Findomestic e dalle vigenti leggi nazionali e internazionali;
3. la richiesta di revoca o di sospensione dei certificati di cui è Titolare nei casi previsti dal Manuale Operativo ICERT-INDI-MO ai §§ 5.4.1 e 5.4.4 e dal presente Addendum Findomestic al § 5.3 ;
4. la protezione della segretezza e conservazione del codice di emergenza per richiedere la sospensione del proprio certificato;

5. l'utilizzo esclusivo della propria chiave privata, tramite il controllo delle credenziali di cui al successivo punto 8;
6. di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato o sospeso il certificato;
7. 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;
8. la protezione della segretezza e la conservazione del dispositivo e/o dei codici utilizzati per l'attivazione della procedura di firma;
9. 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.

3.1.4 Obblighi degli Utenti

Gli obblighi degli Utenti sono specificati al paragrafo 3.1.4 del Manuale Operativo ICERT-INDI-MO.

3.1.5 Obblighi del Terzo Interessato

Non applicabile.

3.1.6 Obblighi del Richiedente

Il ***Richiedente*** Findomestic che, avendo presa visione del Manuale Operativo ICERT-INDI-MO, acquisisce i certificati qualificati è tenuto a:

1. attenersi a quanto disposto dal Manuale Operativo ICERT-INDI-MO;
2. attenersi a quanto previsto nel presente Addendum Findomestic;
3. provvedere tempestivamente all'inoltro, con le modalità descritte ai paragrafi 5.4.2 e 5.4.5 del Manuale Operativo ICERT-INDI-MO, della richiesta di revoca o sospensione nei casi previsti ai paragrafi 5.4.1 e 5.4.4 del medesimo Manuale Operativo ICERT-INDI-MO.

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

Si applica ai certificati rilasciati in base al presente Addendum Findomestic 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.

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'AgID (all'epoca denominato CNIPA), 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 Pubblicazione di informazioni relative al Certificatore

Il presente Addendum Findomestic è reperibile: in formato elettronico presso il sito web del ***Certificatore***.
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 a questo Addendum 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 Findomestic 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, rinnovo, revoca e sospensione del certificato

I costi dei certificati rilasciati in base al presente Addendum Findomestic sono coperti secondo quanto previsto negli accordi intercorsi tra Certificatore e Findomestic.

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.
Le procedure di autenticazione del ***Titolare*** nel caso di rinnovo, revoca e sospensione del certificato qualificato di sottoscrizione e dell'eventuale ***Richiedente***, in caso di sua richiesta di revoca o sospensione del certificato qualificato del ***Titolare*****,** sono disciplinate ai paragrafi 4.2. e 4.3. del Manuale Operativo ICERT-INDI-MO.

4.1 Identificazione ai fini del primo rilascio

Il ***Certificatore*** deve verificare l'identità del ***Titolare*** del certificato di sottoscrizione richiesto.
La procedura di identificazione comporta che il ***Titolare*** sia riconosciuto personalmente da uno dei soggetti di cui al §4.1.1 del presente Addendum Findomestic, che ne verificherà l'identità secondo le procedure e la normativa applicabile.

4.1.1 Abilitazione di Findomestic Banca all'identificazione

Ferma restando la responsabilità del ***Certificatore*** (§3.1.1), Findomestic Banca S.p.A., capogruppo del Gruppo Findomestic e Ufficio di Registrazione, è abilitata ad accertare l'identità del ***Cliente*** che richiede il certificato digitale di sottoscrizione con le seguenti modalità:

1. **Modalità 1**

Direttamente o tramite suoi Incaricati.

2. **Modalità 2**

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

3. **Modalità 3**

Identificazione tramite firma digitale.

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 1

L'identificazione è effettuata da uno dei soggetti indicati al §4.1.1 (**Modalità 1**) ed è richiesta la **presenza fisica** del ***Cliente***.
Il soggetto che effettua l'identificazione verifica l'identità del ***Cliente*** tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato.

Il ***Cliente*** provvede a dichiarare i propri dati necessari al rilascio del certificato digitale ed il numero di utenza telefonica mobile su cui intende ottenere la comunicazione dell'OTP per l'apposizione della firma

digitale e per l'autenticazione nel sistema di comunicazione sicuro tra ***Certificatore*** e ***Titolare*** (cfr. art. 21 **DPCM**).

4.1.2.2 Riconoscimento effettuato secondo la modalità 2

Nella **modalità 2** l'Ufficio di Registrazione, nella sua qualità di Intermediario finanziario, provvede al riconoscimento del Cliente (Identificato, Non Identificato 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 ***Cliente*** raccolti dalla società del Gruppo Findomestic 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.

4.1.2.3 Riconoscimento effettuato secondo la modalità 3

Nella **modalità 3** il ***Certificatore*** si basa sul riconoscimento già effettuato da un altro ***Certificatore.*** Il ***Cliente*** è già in possesso di un dispositivo di firma con un certificato qualificato a bordo ancora in corso di validità. Il riconoscimento avviene in maniera analoga a quanto previsto dalla procedura di rinnovo.
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

I passi principali a cui il ***Cliente*** deve attenersi per ottenere un certificato di sottoscrizione sono:

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

4.1.4 Informazioni che il Titolare deve fornire

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.

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

Non è previsto l'uso di pseudonimi.

4.1.6 Limiti d'uso e limiti di valore

L'inserimento di limiti d'uso e di valore è disciplinato al paragrafo 4.1.6 del Manuale Operativo ICERT-INDI-MO.

I certificati emessi in conformità al presente Manuale Operativo potranno essere utilizzati solo nei rapporti tra il Titolare e le società del Gruppo Findomestic, per la sottoscrizione di contratti relativi a prodotti delle società del Gruppo e prodotti di altre società con cui il Gruppo ha stipulato appositi accordi di collaborazione. Tale limitazione viene garantita dal controllo applicativo svolto dal Certificatore nell'ambito dei sistemi di gestione dell'HSM.

4.1.7 Inserimento del Ruolo e dell'Organizzazione nel certificato

Per i certificati emessi in base al presente Addendum Findomestic non è prevista la facoltà di inserimento del Ruolo nel certificato.

4.1.8 Titoli e/o Abilitazioni Professionali

Per i certificati emessi in base al presente Addendum Findomestic non è prevista la facoltà di inserimento di Titoli e/o Abilitazioni professionali.

4.1.9 Poteri di rappresentanza di persone fisiche

Per i certificati emessi in base al presente Addendum Findomestic non è prevista facoltà di inserimento di poteri di rappresentanza di persone fisiche.

[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

4.1.10 Poteri di Rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi

Per i certificati emessi in base al presente Addendum Findomestic non è prevista la facoltà di inserimento nel certificato di poteri di rappresentanza di organizzazioni ed enti di diritto privato o appartenenza agli stessi.

4.1.11 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 Findomestic 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.

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.

Il ***Titolare*** del certificato può, tuttavia, rinnovarlo, prima della sua scadenza, facendone richiesta all'Ufficio di Registrazione.

4.3 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire 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

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, oppure altro sistema di autenticazione descritto nella documentazione contrattuale consegnata all'atto della registrazione.
Se la richiesta viene fatta presso l'Ufficio di Registrazione, l'autenticazione del ***Titolare*** avviene con le modalità previste per l'identificazione.

4.3.2 Richiesta da parte del Terzo Interessato

Non applicabile.

4.3.3 Richiesta da parte del Richiedente

Il ***Richiedente*** Findomestic 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 5.4.2.
Il ***Certificatore*** si riserva di individuare ulteriori modalità di inoltro della richiesta di revoca/sospensione del ***Richiedente*** in apposite convenzioni da stipulare con lo stesso.

5 Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione durante la quale i dati dei Titolari vengono validati dall'Ufficio di Registrazione e memorizzati negli archivi del ***Certificatore***.

La registrazione iniziale è effettuata presso l' 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.
Questa procedura viene effettuata con procedure automatizzate, sviluppate e supervisionate da personale specializzato del ***Certificatore*** o da quest'ultimo debitamente autorizzato, che si interfacciano con i sistemi siti presso i locali che ospitano l'HSM ed i server collegati.
Le modalità di registrazione del ***Titolare*** e di identificazione dello stesso sono diverse in base ai rapporti tra ***Titolare*** ed ***Ufficio di Registrazione***.

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 le Procedure Alert Antifrode in essere presso l'***Ufficio di Registrazione***.

5.1.1 Caso A: Cliente Identificato

Qualora il ***Titolare*** sia un Cliente Identificato, i dati identificativi sono attestati dall'***Ufficio di Registrazione*** sulla base del riconoscimento 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.

1. Il ***Titolare*** si collega al sito dell'***Ufficio di Registrazione*** e richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici (se autenticato con credenziali precedentemente fornite il form risulta precompilato con i dati);
2. Il ***Titolare*** conferma i propri dati e manifesta la volontà di ottenere il rilascio di un certificato digitale mediante procedura web;
3. L'***Ufficio di registrazione*** verifica la rispondenza dei dati inseriti dal ***Titolare*** con quelli presenti presso i propri archivi e comunica l'esito al ***Certificatore***, che provvede al rilascio del certificato;
4. attraverso le Procedure Alert Antifrode, l'***Ufficio di Registrazione*** verifica l'identità del ***Titolare*** e il presidio del numero di cellulare comunicato e comunica l'esito al ***Certificatore***, per l'eventuale revoca del certificato.

5.1.2 Cliente non Identificato/Prospect

Qualora il ***Titolare*** sia un Cliente non Identificato 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*** si collega al sito dell'***Ufficio di Registrazione*** e richiama una procedura web che presenta un form per l'inserimento dei dati anagrafici;
2. Il ***Titolare*** inserisce i propri dati;
3. Il ***Titolare*** manifesta 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 nei confronti del Cliente non Attivo/Prospect le procedure di identificazione ai sensi del D. L.vo n. 231/2007 e verifica l'identità del ***Titolare*** e il presidio del numero di cellulare comunicato attraverso le Procedure di Alert Antifrode, comunicando l'esito al ***Certificatore***, per l'eventuale revoca del certificato.

5.1.3 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.

5.1.4 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.

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. il certificato viene memorizzato nei server del sistema di emissione;
6. il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati;
7. in seguito all'eventuale esito negativo dell'identificazione da parte dell'***Ufficio di Registrazione*** viene revocato il certificato

5.2.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni relative al ***Titolare*** ed indicate nella richiesta di certificazione.
Il formato del certificato prodotto è conforme a quanto specificato nella Deliberazione CNIPA [4]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.
Il certificato contiene un'apposita estensione [Qualified Certificate Statements - esi4-qcStatement-1 (OID: 0.4.0.1862.1.1)] la quale indica che il certificato è qualificato.

5.2.2 Pubblicazione del certificato

Al buon esito della procedura di certificazione il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico.

5.2.3 Validità del certificato

Il periodo di validità del certificato è determinato sulla base:

- dello stato della tecnologia;
- dello stato dell'arte delle conoscenze crittografiche;
- dell'utilizzo previsto per il certificato stesso.

L'intervallo di validità del certificato è espresso al suo interno nella modalità indicata al paragrafo §4.2.

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 o sospensione.
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***.
La revoca della sospensione rende valide retroattivamente le firme digitali apposte anche nel periodo in cui il certificato era sospeso.

5.3.1 Motivi per la revoca di un certificato

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;
    c. si verifica un cambiamento dei dati del ***Titolare*** presenti nel certificato tale da rendere detti dati non più corretti e/o veritieri;
2. termina il rapporto tra il ***Titolare*** e il ***Certificatore***;
3. viene verificata una sostanziale condizione di non rispetto del presente Addendum Findomestic e/o del Manuale Operativo ICERT-INDI-MO.

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

5.3.3 Revoca su iniziativa del Titolare

Il ***Titolare*** può richiedere la revoca del certificato sia accedendo ai servizi messi a disposizione dall'***Ufficio di Registrazione***, sia rivolgendosi direttamente al ***Certificatore***.

Il ***Titolare*** che richiede la revoca accedendo ai servizi messi a disposizione dall'***Ufficio di Registrazione*** Findomestic si collega ai servizi nell'area riservata del portale Findomestic, stampa, compila e e sottoscrive l'apposito modulo.
La richiesta firmata dal ***Titolare***, in forma scritta, è raccolta dall'***Ufficio di Registrazione***, che effettua tutte le verifiche del caso e procede a richiedere la revoca al ***Certificatore*****,** secondo le modalità concordate.

Il ***Certificatore***, anche a mezzo dell'***Ufficio di Registrazione***, provvede a comunicare l'avvenuta revoca al ***Titolare*** e al ***Richiedente*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***.

5.3.4 Revoca su iniziativa del Certificatore

Le procedure per le revoca su iniziativa del Certificatore sono riportate nel Manuale Operativo ICERT-INDI-MO.

Il ***Certificatore***, anche mezzo dell'***Ufficio di Registrazione***, provvede a comunicare l'avvenuta revoca al ***Titolare*** e al ***Richiedente*** che abbia all'uopo stipulato apposita convenzione con il ***Certificatore***.

5.3.5 Revoca su iniziativa del Richiedente

Findomestic, 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*** e al ***Richiedente***, anche a mezzo dell'***Ufficio di Registrazione***, secondo le modalità di comunicazione stabilite all'atto della 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***.

5.3.6 Procedura per la revoca immediata

Le procedure per le richieste di revoca immediata sono riportate nel Manuale Operativo ICERT-INDI-MO.

5.3.7 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. 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.

5.3.8 Procedura per la richiesta di Sospensione

Il ***Titolare*** può sospendere il certificato accedendo ai servizi messi a disposizione da Findomestic sui propri portali, in area riservata:

1. Il ***Titolare*** accede al portale dell'***Ufficio di Registrazione*** mediante i codici personali a sua disposizione e richiede la sospensione del certificato, validandola con il codice di emergenza (OTP ricevuta a mezzo SMS);

2. L'***Ufficio di Registrazione*** invia al ***Certificatore*** la richiesta di sospensione.
3. il ***Certificatore*** sospende il certificato e comunica al titolare l'avvenuta sospensione direttamente, o attraverso l'***Ufficio di Registrazione***.

5.3.9 Ripristino di validità di un Certificato sospeso

Alla scadenza del periodo di sospensione richiesto, o su richiesta del ***Titolare*** o del ***Richiedente***, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL).
La riattivazione avviene nell'arco delle 24 ore successive alla data di termine della sospensione.

Qualora la scadenza della sospensione coincida con la scadenza del certificato o sia a questa successiva, la sospensione viene invece tramutata in revoca, con effetto dall'inizio della sospensione.

5.3.10 Pubblicazione e frequenza di emissione della CRL

La Pubblicazione e frequenza di emissione della CRL è disciplinata al paragrafo 5.3.7. del Manuale Operativo ICERT-INDI-MO.

5.3.11 Tempistica

La tempistica di emissione della CRL è disciplinata al paragrafo 5.3.7. del Manuale Operativo ICERT-INDI-MO.

5.4 Sostituzione delle chiavi e rinnovo del Certificato

La procedura di sostituzione delle chiavi e rinnovo del certificato è disciplinata al paragrafo 5.4. del Manuale Operativo ICERT-INDI-MO.

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

La soluzione di firma digitale adottata dalle società del Gruppo Findomestic si configura come un **servizio online**, accessibile via rete (Internet).
La coppia delle chiavi crittografiche e il certificato digitale, risiede in modalità sicura nel SSCD 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 il Gruppo Findomestic o società partner del Gruppo Findomestic e solamente per sottoscrivere documenti presentati dai portali delle società del Gruppo.

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" di 6 cifre, integralmente inserite dal firmatario nell'apposito box di firma del documento; il codice PIN è composto da 5 cifre, delle quali 2 (randomiche) sono inserite dal firmatario nel medesimo box di firma.

Tutte le chiamate di firma sono inoltrate con modalità sicura da Findomestic 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. Findomestic Banca 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 a cui espressamente si rinvia.