Certificatore InfoCert

Certificati di Sottoscrizione CCard

Addendum Manuale Operativo ICERT – INDI-MO

Codice documento: ICERT-INDI-MO-CCard

Questa pagina è lasciata
intenzionalmente bianca

Indice

1 Introduzione al documento

Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.0	**Data Versione/Release**:	25/07/12
Descrizione modifiche:	Prima elaborazione		
Motivazioni:	Rilascio di certificati nell'ambito dei processi di contrattualizzazione a distanza, con l'avvalimento del riconoscimento effettuato da un soggetto Emittente di carte di pagamento (Issuer).		

1.1 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 a seguito dei processi di identificazione dei richiedenti con strumenti di pagamento quali carte di credito.
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.

1.2 Riferimenti normativi e tecnici

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 30 marzo 2009. 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.

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

1.3 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***.

Addendum CCard

Il presente documento, il quale integra il Manuale Operativo ICERT-INDI-MO del ***Certificatore*** relativamente alle procedure di rilascio dei certificati in seguito a processi di riconoscimento dei richiedenti a mezzo strumenti di pagamento quali carte di credito. Per quanto non previsto nell'Addendum CCard si applica il Manuale Operativo ICERT-INDI-MO.

Carta di credito

Strumento che abilita il titolare, in base a un rapporto contrattuale con l'emittente, ad effettuare acquisti di beni o servizi oppure prelievi di contante con pagamento differito presso qualsiasi esercizio convenzionato con l'emittente stesso. Viene emessa da un soggetto Emittente, che può essere una banca, un intermediario finanziario (carte travel and entertainment – T&E) o un fornitore di beni e servizi (fidelity card). In quest'ultimo caso, la carta può essere utilizzata esclusivamente per il pagamento di acquisti effettuati presso lo stesso Emittente.

Circuito di pagamento

L'azienda che si occupa di veicolare, attraverso una propria rete di comunicazione, le richieste e le corrispondenti autorizzazioni alla spesa. Il circuito si occupa anche delle operazioni di settlement, ossia di contabilizzazione e pareggio delle partite, nonché di verifica del codice di sicurezza 3-D Secure.

Cliente

Il soggetto che, alla data di richiesta del certificato, è titolare della carta di credito in forza di un contratto con l'Ente Emittente, e in quanto tale è già stato riconosciuto ai sensi del D. Lgs. 21 novembre 2007, n. 231 [15].

Ente Emittente (Issuer)

L'Intermediario finanziario che provvede ad emettere la carta di pagamento in base ad un contratto stipulato con il Cliente.

Ente Esercente (Merchant)

L'esercizio commerciale che, aderendo ad un Circuito di pagamento, permette ai propri clienti di pagare attraverso lo strumento di pagamento convenzionato.

Evidenza Informatica

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

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.

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***.

3-D Secure

E' una procedura aggiuntiva di autenticazione richiesta dall'Ente Emittente. Il Cliente deve inserire delle credenziali di autenticazione, secondo i criteri definiti dal Circuito di Pagamento e dall'Issuer, al fine di autorizzare ogni singola transazione effettuata a mezzo della carta di credito.

1.4 Acronimi e abbreviazioni

ACBI – Associazione per il Corporate Banking Interbancario

CNIPA – Centro Nazionale per l'informatica nella Pubblica Amministrazione . Dal Dicembre 2009 ha assunto la denominazione **DigitPA**

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
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 il CNIPA 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 (definiti ***Utenti***) 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 emessi sulla base dei processi di identificazione dei richiedenti con strumenti di pagamento quali carte di credito.

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

Pubblicando tale Addendum CCard 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 identificazione a mezzo carta di credito.

2.1 Identificazione del documento

Questo documento è denominato "Certificati di sottoscrizione CCard – Addendum al Manuale Operativo ICERT-INDI-MO" ed è caratterizzato dal codice documento: **ICERT-INDI-MO-CCard**.
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) **1.3.76.36.1.1.28** 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 con identificazione del Titolare conforme al presente addendum	1.3.76.36.1.1.29

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 CCard, le attività e le responsabilità di identificazione del Richiedente a mezzo della transazione con carta di credito e le attività e responsabilità di raccolta e comunicazione al ***Certificatore*** dei suddetti dati e della richiesta di registrazione e certificazione potranno essere affidate a soggetti differenti, che operano di concerto tra loro e con il ***Certificatore***.

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 CCard 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.

-I certificati emessi in base al presente Addendum contengono limiti d'uso ed hanno validità limitata nel tempo secondo quanto meglio specificato nel paragrafo 4.2

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 CCard 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 DIGITPA

Il presente Addendum CCard in quanto integrativo del Manuale Operativo ICERT-INDI-MO, compilato dal ***Certificatore*** nel rispetto delle indicazioni legislative, è stato consegnato, in copia, a DigitPA (ex-CNIPA) che lo rende disponibile pubblicamente.
I rapporti con DigitPA 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 CCard.

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

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 per l'attivazione della firma;
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 CCard, assicurando il corretto svolgimento delle attività ad esso affidate dalla Convenzione RAO sottoscritta tra le parti;
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 presidio e la gestione delle procedure e degli strumenti di autenticazione al servizio di firma da parte dei Titolari, ove gestite nel proprio dominio.

Ai fini del presente Addendum CCard, il ruolo di ***Ufficio di Registrazione*** è assegnato all'***Ente Emittente*** (Issuer) e all'***Ente Esercente*** (Merchant), ciascuno per la parte di processo ad esso affidato e dettagliato dall'atto di nomina (Convenzione RAO).

3.1.3 Obblighi dei Titolari

Il ***Titolare*** deve garantire:

1. la correttezza, veridicità e completezza delle informazioni fornite al momento della richiesta della carta di pagamento all'***Ente Emittente*** che effettua l'identificazione ai sensi antiriciclaggio;

2. la correttezza, veridicità e completezza delle informazioni fornite al momento della richiesta del certificato al soggetto che raccoglie la medesima ed effettua l'identificazione;
3. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo ICERT-INDI-MO, nel presente Addendum CCard e dalle vigenti leggi nazionali e internazionali;
4. la richiesta di revoca o di sospensione dei certificati di cui è ***Titolare*** nei casi previsti dal presente Addendum CCard al § 5.3;
5. la protezione della segretezza e conservazione del codice di emergenza per richiedere la sospensione del proprio certificato, che corrisponde al valore dell'OTP al momento della richiesta;
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 conservazione dei codici utilizzati per l'attivazione della procedura di firma;
9. la protezione della segretezza e conservazione del codice 3-D Secure associato alla Carta di Pagamento utilizzata per la validazione dell'identificazione, ai fini del rilascio del certificato qualificato;
10. 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*** 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 CCard;
3. provvedere tempestivamente all'inoltro, della richiesta di revoca o sospensione nei casi e nelle modalità descritte al paragrafo 5.3 del presente Addendum CCard. .

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

Si applica ai certificati rilasciati in base al presente Addendum Ccard 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 dal 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 ***Certificatore***.

3.4 Pubblicazione

3.4.1 Pubblicazione di informazioni relative al Certificatore

Il presente Addendum Ccard è reperibile:

- in formato elettronico presso il sito web del ***Certificatore***;
- in formato elettronico presso il sito web dell'***Ente Esercente***.

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 DigitPA 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 CCard al proprio processo di erogazione del servizio di certificazione.

3.6 Tutela dei dati personali

Le informazioni relative al ***Titolare*** 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 CCard sono coperti secondo quanto previsto negli accordi intercorsi tra ***Certificatore*** e ***Richiedente***.

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 revoca e sospensione del certificato qualificato di sottoscrizione e del ***Richiedente***, in caso di sua richiesta di revoca o sospensione del certificato qualificato del ***Titolare*****,** sono disciplinate al paragrafo 5.3 dell'Addendum CCard.

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 in base alla procedura descritta al §4.1.1 del presente Addendum CCard.

4.1.1 Abilitazione dell'Ufficio di Registrazione all'identificazione

Ferma restando la responsabilità del ***Certificatore*** (§3.1.1), l'***Ufficio di Registrazione*** è abilitato ad accertare l'identità del ***Cliente*** che richiede il certificato digitale di sottoscrizione con le seguenti modalità:

Modalità 1
Identificazione tramite transazione online con carta di credito.

4.1.2 Procedure per l'identificazione

4.1.2.1 Riconoscimento effettuato secondo la modalità 1

L'identificazione del Cliente è effettuata dall'***Ente Esercente*** (Merchant), il quale opera nella sua qualità di ***Ufficio di Registrazione***, nell'ambito di una transazione on-line con pagamento a mezzo di carta di credito.

Il Cliente sul sito Internet dell'***Ente Esercente*** provvede ad inserire i propri dati anagrafici ed identificativi al fine dell'acquisto di un prodotto/servizio offerto. Al momento del pagamento il Cliente inserisce il proprio nominativo, i dati relativi alla carta di credito ed il codice di sicurezza 3-D Secure sul sistema del Circuito di Pagamento. In caso di esito positivo della transazione l'***Ente Esercente*** riceve conferma di tale risultato e provvede a trasmettere la richiesta di registrazione al ***Certificatore***, considerando valido il riconoscimento del Cliente.

Il riconoscimento si basa:

1) Sull'identificazione effettuata dall'***Ente Emittente***, ai sensi del D.Lgs. n. 231/2007 e ss.mm.ii. al momento del rilascio della carta di credito al Cliente, e da questi confermata all'***Ente Esercente***;
2) Sulla previsione di cui all'art. 28, 3° comma, lett. b) del D.Lgs. n. 231/2007 e ss.mm.ii. in merito agli obblighi di identificazione ed adeguata verifica della clientela;
3) Sui seguenti elementi di sicurezza:
    a. possesso della materialità della carta di credito da parte del Cliente, il quale inserisce i dati richiesti per effettuare la transazione;
    b. conoscenza esclusiva da parte del Cliente del codice di sicurezza 3-D Secure gestito dal Circuito di Pagamento e rilasciato dall'***Ente Emittente***;

I dati identificativi del Cliente, confermati dall'***Ente Emittente*** in qualità di ***Ufficio di Registrazione*** e raccolti dall'***Ente Esercente*** 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 (dispositivo OTP via SMS) 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

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

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

4.1.4 Informazioni che il Titolare deve fornire

Nella richiesta di registrazione sono contenuti 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 accettato dal ***Titolare*** e di esso viene conservata apposita Evidenza Informatica firmata digitalmente dal RAO.

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
- numero di telefonia mobile per la trasmissione della OTP e per l'invio delle comunicazioni dal ***Certificatore*** al ***Titolare***.

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.

[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

4.1.6 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 base al presente Addendum CCard possono essere utilizzati per la sottoscrizione di atti giuridici validi tra *Titolare* e *Ente Esercente* e tra *Titolare* e *Certificatore*, con esclusione di ulteriori loro utilizzi al di fuori di tale ambito.

Tale limitazione è implementata applicativamente ed è resa nota tramite l'OID identificante il presente Addendum.

4.1.7 Inserimento del Ruolo e dell'Organizzazione nel certificato

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

4.1.8.1 Poteri di rappresentanza di persone fisiche

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

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

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

4.1.8.3 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 CCard 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 Validità dei 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.
I certificati emessi in base al presente Addendum CCard, in considerazione della funzione svolta dagli stessi che ne limita ad un breve lasso di tempo la validità, hanno durata non superiore a 7 (sette) giorni.

Per i certificati disciplinati dal presente Addendum CCard non è prevista la possibilità di rinnovo da parte del ***Titolare***.

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 i codici di autenticazione descritti nella documentazione contrattuale consegnata all'atto della registrazione.
Se la richiesta viene fatta presso l'***Ufficio di Registrazione***, l'autenticazione del ***Titolare*** avviene utilizzando il valore del codice OTP al momento della richiesta.

4.3.2 Richiesta da parte del *Terzo Interessato*

Non applicabile

4.3.3 Richiesta da parte del *Richiedente*

L'***Ente Esercente*** che, in virtù della sua qualifica di ***Richiedente*** e nelle ipotesi contrattualmente previste con il ***Certificatore***, richiede la revoca o sospensione del certificato del ***Titolare***, si autentica sottoscrivendo l'apposito modulo di richiesta di revoca o sospensione messo a disposizione dal ***Certificatore*** e munendolo, qualora si tratti di un ente, di timbro o altra segnatura equivalente.
La richiesta dovrà essere inoltrata con le modalità indicate al paragrafo 5.3 .
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***, a mezzo dell'applicazione web dal medesimo predisposta e della convalida dei dati della carta di pagamento effettuata dal Circuito di pagamento.

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 da personale specializzato del ***Certificatore*** o da quest'ultimo debitamente autorizzato, presso i locali che ospitano l'HSM ed i server collegati.

Per la conferma delle operazioni di rilascio al ***Titolare*** verrà richiesto l'utilizzo di un dispositivo **OTP** fisico, software o SMS.

5.1.1 Rilascio del Certificato

Il Cliente ai fini del rilascio del certificato digitale è identificato dall'***Ente Esercente***, che si basa sui dei dati anagrafici inseriti sulla procedura on-line, validati dall'***Ente Emittente*** mediante l'esito positivo della transazione di pagamento a mezzo carta di credito.

1. L'***Ente Esercente*** – in qualità di ***Ufficio di Registrazione*** - in occasione dell'acquisto di un prodotto/servizio da parte del Cliente che abbia scelto quale strumento di pagamento la carta di credito, sottopone al Cliente medesimo la Richiesta di Registrazione che dovrà essere compilata dal Cliente con i dati necessari al rilascio del certificato;
2. L'***Ente Esercente*** provvede a formalizzare i dati ricevuti nella richiesta in un apposito file;
3. Il Cliente procede nella procedura di acquisto del servizio/prodotto e viene indirizzato sulla procedura del Circuito di pagamento che gli richiede i dati necessari ad autorizzare la transazione (Nome, Cognome, Numero carta, Scadenza, codice CVV2). Inseriti i dati il Cliente viene reindirizzato sulla procedura che gli richiede l'inserimento del codice di sicurezza 3-D Secure per l'autorizzazione della transazione[2];
4. Attraverso la transazione con carta di credito, attraverso le modalità operative definite dal Circuito di Pagamento, l'***Ente Emittente*** valida i dati identificativi ad esso sottoposti. L'esito della validazione è fornito insieme all'esito della transazione con carta di pagamento. Se gli esiti sono positivi, il Circuito di pagamento comunica tale esito all'***Ente Esercente*** che, in qualità di ***Ufficio di Registrazione***, considera validamente effettuata l'identificazione del Cliente[3];
5. L'***Ufficio di Registrazione*** comunica al ***Certificatore*** la corretta identificazione del Cliente;
6. Il ***Certificatore*** verifica la corrispondenza dei dati del Cliente relativi all'identificazione dello stesso trasmessi dall'***Ufficio di Registrazione*** e provvede al rilascio del certificato, con cui il Cliente sottoscrive il documento di conferma di emissione del certificato ed il contratto

[2] Il possesso del codice di sicurezza 3-D Secure è prerequisito per l'emissione dei certificati disciplinati dal presente Addendum CCard. Non è prevista la possibilità di emettere certificati digitali per le transazioni online con carta di credito che non utilizzano il codice 3-D Secure per l'autenticazione del titolare della carta.

[3] Ulteriore prerequisito per poter considerare correttamente effettuata l'identificazione del Cliente è che il nominativo del medesimo coincida con quello del titolare della carta di credito utilizzata per il pagamento.

relativo ai servizi di certificazione digitale ai fini dell'archiviazione di tali documenti da parte del ***Certificatore***.

5.1.2 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.

5.1.3 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 emissione del certificato controllando che:
   a) il ***Titolare*** sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   b) al ***Titolare*** sia stato assegnato un codice identificativo unico nell'ambito degli utenti del ***Certificatore*** (IUT);
   c) 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 di emissione;
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.

5.2.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni relative al ***Titolare*** ed indicate nella richiesta di emissione.
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, secondo quanto indicato al paragrafo §4..

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:
    - sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN) o del dispositivo indicato per la ricezione della OTP;
    - 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 CCard 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

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

Il ***Titolare*** che richiede la revoca accedendo ai servizi messi a disposizione dall'***Ufficio di Registrazione*** si collega al portale dell'***Ente Esercente***, stampa, compila e e sottoscrive l'apposito modulo.
La richiesta firmata dal ***Titolare***, in forma scritta, è raccolta dall'***Ente Esercente***, 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***.

5.3.3 Procedura per la revoca immediata

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

5.3.4 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.

5.3.5 Procedura per la richiesta di Sospensione

Il ***Titolare*** può sospendere il certificato accedendo ai servizi messi a disposizione dall'***Ente Esercente*** sul proprio portale:

1. Il ***Titolare*** si collega al portale dell'***Ente Esercente***, che opera in qualità di ***Ufficio di Registrazione*** richiede la sospensione del certificato mediante i servizi esposti, validandola con il codice di emergenza (OTP ricevuta a mezzo SMS);
2. L'***Ente Esercente***, in qualità di ***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***.

5.3.6 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.

5.3.7 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.

5.3.8 Tempistica

La tempistica di emissione della CRL è disciplinata al paragrafo 5.4.7. del Manuale Operativo ICERT-INDI-MO.
In caso di revoca o sospensione immediata il tempo di attesa è al massimo di 1 ora.

5.4 Sostituzione delle chiavi e rinnovo del Certificato

Per i certificati emessi secondo le procedure del presente Addendum CCard non è prevista l'opzione di sostituzione delle chiavi e rinnovo del Certificato.

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

La soluzione di firma digitale adottata nell'ambito del presente Addendum CCard 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 (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 ***Ente Esercente*** (Merchant), e solamente per sottoscrivere documenti presentati dai servizi dell'***Ente Esercente***.

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 di 8 cifre, inserite dal firmatario nel medesimo box di firma.

Tutte le chiamate di firma sono inoltrate con modalità sicura dall'***Ente Esercente*** 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. L'***Ente Esercente*** 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.

