Certificatore InfoCert

Certificati di Sottoscrizione One-Shot

Manuale Operativo

Codice documento: ICERT-INDI-MO-SHOT

Firmato digitalmente da:
Alfredo Esposito
Stato=IT
Organization=NON PRESENTE
Nome=ALFREDO Cognome=ESPOSITO
CF=SPSLRD56L26F839T
Motivo:
Data: 04/12/2014 - 10:22:42

Questa pagina è lasciata
intenzionalmente bianca

Indice

Table of Contents

1. Introduzione al documento

Versione/Release n°:	2.0	**Data Versione/Release**:	03/12/14
Descrizione modifiche:	§§4.1.2.1, 4.1.2.2, 5.2.1, 5.2.2, 5.2.3, 6.2		
Motivazioni:	Estensione delle modalità di emissione; riconoscimento anche ai sensi della normativa antiriciclaggio francese; riduzione dei documenti usabili solo a quelli di valenza internazionale; eliminazione dei limiti d'uso; lunghezza delle chiavi; associazione al documento firmato del riferimento temporale		

Versione/Release n°:	1.0	**Data Versione/Release**:	15/04/2014
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		

1.1 Proprietà Intellettuale

1.2 Cos'è il Manuale Operativo

Il presente documento descrive le regole e procedure adottate da InfoCert, in qualità di Certificatore Autorizzato, per l'emissione di certificati digitali qualificati denominati "One-Shot".
La caratteristica di detti certificati qualificati One-Shot è quella di avere una breve durata di validità, non superiore a 60 (sessanta) minuti dal momento di emissione.
Il presente documento, inoltre, identifica i soggetti coinvolti nel procedimento di rilascio dei certificati qualificati One-Shot, gli obblighi e le responsabilità di detti soggetti e degli utenti, i presupposti e le modalità di rilascio dei certificati, quelle di loro utilizzo e le procedure di sospensione e revoca degli stessi.
Il Manuale Operativo deve essere osservato dai soggetti che provvedono al rilascio dei certificati qualificati One-Shot, dai titolari dei medesimi e dagli utenti.
Il contenuto si basa sulle norme vigenti alla data di emissione e recepisce le raccomandazioni del documento *"Request for Comments: 2527 – Certificate Policy and certification practices framework"* © Internet Society 1999.

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – 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 (G.U. n. 42 del 20/2/2001) e sue modificazioni secondo DPR 137/2003 (nel seguito referenziato come **TU**)

[4] Deliberazione CNIPA 45/2009 (G.U. del 3-12-2009) – Regole per il riconoscimento e la verifica del documento informatico

[5] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (G.U. n. 117 del 21-5-2013)]. Referenziato nel seguito come **DPCM**

[6] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003)

[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 19 luglio 2012 - Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma. (Gazzetta Ufficiale n. 237 del 10-10-2012);

[17] Decreto Legislativo 6 settembre 2005, n.206 - Codice del Consumo

[18] Provvedimento Garante per la protezione dei dati personali 26 marzo 2003 [1053753]

[19] InfoCert - Manuale Operativo ICERT-INDI-MO per i certificati di sottoscrizione, disponibile su www.firma.infocert.it

[20] Decree 2009-1087 « Code monétaire et financier - Article D561-32-1"

Riferimenti tecnici

[21] Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" - Aprile 2002

[22] RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[23] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

[24] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[25] 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. 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.

Accreditamento facoltativo – cfr CAD – art 29
Il riconoscimento del possesso, da parte del ***Certificatore*** che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Autorità per la marcatura temporale *[Time-stamping authority]*
È il sistema software/hardware, gestito dal ***Certificatore***, che eroga il servizio di marcatura temporale.

Certificato, Certificato Digitale, Certificato X.509 *[Digital Certificate]*
Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.
Nel certificato compaiono altre informazioni tra cui:
- il ***Certificatore*** che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificato Qualificato – cfr. CAD

Certificato One-Shot
Il certificato digitale qualificato disciplinato nel presente Manuale Operativo avente durata limitata nel tempo per un periodo non superiore a 60 (sessanta) minuti a decorrere dal momento della sua emissione.

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD – art 27

Certificatore Qualificato – cfr. CAD – art 29

Chiave Privata e Chiave Pubblica – cfr. CAD

Dati per la creazione di una firma – cfr. DPCM

Dati per la verifica della firma – cfr. CAD – art 28

Dispositivo sicuro per la creazione della firma (SSCD)– cfr.CAD
Il dispositivo sicuro di firma utilizzato dal ***Titolare*** è un dispositivo crittografico rispondente a requisiti di sicurezza determinati dalla legge. Per il Certificato One-Shot è un HSM.

Evidenza Informatica
Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

Firma digitale *[digital signature]* – cfr. CAD

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

Lista dei Certificati Revocati o Sospesi *[Certificate Revocation List - CRL]*
E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea.
Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla CRL, che viene quindi pubblicata nel **registro pubblico**.

Marca temporale *[Time Stamp Token]* – cfr. DPCM

Manuale Operativo – cfr. [5]

Il Manuale Operativo definisce le procedure che il ***Certificatore*** applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse da AgID e quelle della letteratura internazionale

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. Può essere basato su dispositivi hardware o su procedure software.

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***.

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

Registro pubblico *[Directory]*
Il Registro pubblico è un archivio che contiene:
- tutti i certificati emessi dal ***Certificatore*** per i quali sia stata richiesta dal ***Titolare*** la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Regole tecniche
Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, [5].

Revoca o sospensione di un Certificato
È l'operazione con cui il ***Certificatore*** annulla la validità del certificato prima della naturale scadenza. Questo concetto non è applicabile ai certificati One-Shot emessi in conformità al presente Manuale Operativo.

Tempo Universale Coordinato *[Coordinated Universal Time]*
Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

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

Uffici di Registrazione *[Registration Authority]*
Ente incaricato dal ***Certificatore*** a svolgere le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale nonché alla consegna del dispositivo sicuro di firma.

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

1.5 Acronimi e abbreviazioni

AgID – Agenzia per l'Italia Digitale (ex-CNIPA, ex-DigitPA). Autorità di Vigilanza sui Certificatori Accreditati

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***.

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.

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.

2. Generalità

2.1 Identificazione del Manuale Operativo

Questo documento è denominato "Certificatore InfoCert – Manuale Operativo Certificati One-Shot" ed è caratterizzato dal codice documento: **ICERT-INDI-MO-SHOT**.
La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.
Al documento sono associati tre *object identifier,* referenziati nell'estensione CertificatePolicy dei certificati secondo l'utilizzo cui gli stessi sono destinati.
Il significato degli OID è il seguente:

L'*object identifier* (OID) 1.3.76.36.1.1.34 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-applicata tramite HSM (**CAD** Art. 35 comma 3, [16]) – certificati One-Shot	1.3.76.36.1.1.34

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo 4.1.5. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del 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 Soggetti coinvolti nei processi

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 i seguenti:

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Piazza Sallustio 9 00187 Roma**
Sede operativa	**Via Marco e Marcelliano 45, 00147 Roma** **Corso Stati Uniti 14bis, 35127 Padova** **Via Franco Russoli n. 5, 20143, Milano**
Rappresentante legale	**Fernando Zilio** In qualità di Presidente del Consiglio d'Amministrazione
Amministratore Delegato	
N° telefono	**06836691**
N° Iscrizione Registro Imprese	**07945211006**
Codice Fiscale	**07945211006**
N° partita IVA	**07945211006**
Sito web	http://www.firma.infocert.it/

2.2.2 Uffici di Registrazione

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

- identificazione e registrazione del ***Titolare***,
- validazione della richiesta del certificato,
- attivazione della procedura di certificazione della chiave pubblica,

L'Ufficio di Registrazione, anche tramite suoi incaricati, svolge in sostanza tutte le attività di interfaccia tra il ***Certificatore*** ed il ***Titolare***.
Gli Uffici di Registrazione sono attivati dal ***Certificatore*** a seguito di un adeguato addestramento del personale impiegato, che potrà svolgere le funzioni di identificazione, ed eventualmente registrazione, anche presso il ***Titolare***.
Il ***Certificatore*** verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo Manuale.

2.2.3 Titolare

E' il soggetto a cui è rilasciato il Certificato One-Shot e che risulta intestatario dello stesso all'interno del medesimo.

2.3 Applicazione e comunicazioni

2.3.1 Applicabilità

I certificati emessi dal ***Certificatore*** Accreditato InfoCert nelle modalità indicate dal presente manuale operativo 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. Possono essere disponibili sul mercato altri prodotti di verifica con funzionalità e limitazioni secondo le indicazioni del fornitore.

AVVERTENZA 1: per le particolari caratteristiche di rilascio e durata del Certificato One-Shot non è prevista la possibilità di specificare all'interno dello stesso i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite dal Titolare. Tale facoltà è consentita dal certificatore mediante richiesta di emissione di un certificato qualificato disciplinato dal Manuale Operativo ICERT-INDI-MO [19].

AVVERTENZA 2: per le particolari caratteristiche di rilascio e durata del Certificato One-Shot l'HSM è l'unico SSCD previsto per l'utilizzo dello stesso. Non è prevista inoltre la possibilità di rinnovo del Certificato One-Shot.

2.4 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 Manuale Operativo 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.

2.5 Rapporti con l'Autorità di Vigilanza

Il presente Manuale Operativo, compilato dal Certificatore nel rispetto delle indicazioni legislative, è stato consegnato, in copia, all'Autorità di Vigilanza che lo rende disponibile pubblicamente.
Al momento della richiesta d'iscrizione, il Certificatore fornisce all'autorità di vigilanza sui certificatori i dati identificativi richiesti, che vengono da quest'ultima sottoscritti, conservati e pubblicati.

Almeno 90 giorni prima della scadenza del periodo di validità delle proprie chiavi di certificazione, il Certificatore avvierà la procedura di sostituzione.
Il Certificatore si attiene alle regole emanate dall'Autorità di Vigilanza al fine dello scambio delle informazioni attraverso un sistema sicuro di comunicazione.

Il certificato relativo alle chiavi con cui viene firmato l'elenco pubblico dei certificatori accreditati è caratterizzato dall'OID 1.3.76.36.1.1.26.

3. Obblighi

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

3.1 Obblighi dei soggetti

3.1.1 Obblighi del Certificatore

Il ***Certificatore*** è tenuto a garantire che (cfr. artt. 30 e 32 del CAD):

1. siano soddisfatte tutte le regole tecniche specificate nel DPCM [5];
2. siano soddisfatte le modalità di riconoscimento del ***Titolare*** ai sensi delle norme [11], [12], [13] e [15], con particolare riguardo all'identificazione dello stesso;
3. il Sistema Qualità sia conforme alle norme ISO 9001;
4. la richiesta di certificazione abbia caratteristiche di autenticità;
5. la chiave pubblica di cui si richiede la certificazione non sia già stata certificata, per un altro soggetto ***Titolare***, nell'ambito del proprio dominio. Per la verifica nel dominio degli altri certificatori accreditati, il ***Certificatore*** si impegna a stabilire accordi con gli altri certificatori presenti nell'Elenco dell'Autorità di Vigilanza, in base alle attuali conoscenze tecnologiche, per l'attivazione di tali controlli;
6. sia rilasciato e reso pubblico, se esplicitamente richiesto dal ***Titolare***, il certificato qualificato secondo quanto stabilito all'art. 32, comma 3, lett. b) del **CAD**;
7. i Titolari siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi nonché riguardo agli obblighi da essi assunti in merito alla protezione della segretezza della chiave privata;
8. il proprio sistema di sicurezza dei dati sia rispondente alle misure minime di sicurezza per il trattamento dei dati personali, secondo il Decreto Legislativo 30 giugno 2003, n. 196 ;
9. sia certa l'associazione tra chiave pubblica e ***Titolare***;
10. il codice identificativo assegnato a ciascun ***Titolare*** sia univoco nell'ambito dei propri utenti;
11. le proprie chiavi private siano accuratamente protette mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
12. siano conservate per almeno 20 (venti) anni dalla data di scadenza del certificato le informazioni ottenute in fase di registrazione, di richiesta di certificazione, di revoca e di rinnovo;
13. siano custoditi per 20 (venti) anni in forma accessibile i certificati delle proprie chiavi pubbliche di certificazione;
14. alla data del rilascio siano esatte e complete le informazioni necessarie alla verifica della firma contenute nel certificato e rispetto ai requisiti fissati per i certificati qualificati
15. i dati per la creazione della firma siano sotto il controllo esclusivo del ***Titolare***.

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;
2. che il ***Titolare*** sia informato in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
3. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, secondo quanto previsto dal Decreto Legislativo 30 giugno 2003, n. 196 e relativo allegato B;
4. le caratteristiche di autenticità della richiesta di certificazione, la verifica dell'identità del ***Titolare*** del certificato, il controllo e la registrazione dei dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;
5. la comunicazione al ***Certificatore*** di tutti i dati e documenti acquisiti durante l'identificazione allo scopo di attivare la procedura di emissione del certificato;
6. l'invio tempestivo al Certificatore delle richieste di certificazione;

7. 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.

L'Ufficio di Registrazione terrà direttamente i rapporti con Titolari ed è tenuto ad informarli circa le disposizioni contenute nel presente Manuale Operativo.
Per il corretto riconoscimento, effettuato secondo la modalità 5 (cfr. §4.1.1), l'Ufficio di registrazione è tenuto a dotare la postazione dei propri incaricati del *client* per videoconferenza, necessario allo svolgimento delle procedure di riconoscimento a distanza.

3.1.3 Obblighi dei Titolari

Il ***Titolare*** deve garantire:
1. la correttezza, veridicità e completezza delle informazioni fornite al soggetto che effettua l'identificazione, per la richiesta di certificato;
2. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo e dalle vigenti leggi nazionali e internazionali;
3. l'uso esclusivo dei dati per la generazione delle firme;
4. l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
5. di non apporre firme elettroniche avvalendosi di chiavi private per le quali sia stato revocato il certificato;
6. 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;
7. la protezione della segretezza e la conservazione dei codici e dei dispositivi utilizzati per l'attivazione della procedura di firma.

3.1.4 Obblighi degli Utenti

L'utente che riceve e utilizza un documento informatico firmato dal Titolare, che quindi contiene il certificato, ha i seguenti obblighi:
1. conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del ***Certificatore***, riportati nel Manuale Operativo del ***Certificatore*** stesso;
2. verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta. Deve verificare con particolare attenzione il periodo di validità e che il certificato non risulti sospeso o revocato controllando le relative liste nel registro dei certificati;
3. Verificare il rispetto dei limiti d'uso eventualmente inseriti nel certificato;
4. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.2 Limitazioni e indennizzi

3.2.1 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***.

3.3 Pubblicazione

3.3.1 Pubblicazione di informazioni relative al Certificatore

Il presente Manuale Operativo è reperibile:
- in formato elettronico presso il sito web del ***Certificatore*** (cfr. § 2.1)
- in formato elettronico presso l'Ufficio di Registrazione

- in formato cartaceo, richiedibile sia al ***Certificatore*** sia al proprio Ufficio di Registrazione.

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative al ***Certificatore*** previste dal **DPCM** sono pubblicate presso l'Autorità di Vigilanza.

3.3.2 Pubblicazione dei certificati

I certificati emessi usualmente non sono pubblicati.
L'utente che voglia rendere pubblico il proprio certificato può farne richiesta inviando l'apposito modulo (disponibile sul sito www.firma.infocert.it), firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione. L'invio deve avvenire via e-mail indirizzata a **richiesta.pubblicazione@cert.legalmail.it** seguendo la procedura descritta sul sito stesso.

3.4 Verifica di conformità

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

3.5 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.

3.6 Tariffe

Le tariffe per l'acquisizione di questi certificati saranno incluse nel contratto del servizio ai cui fini questi certificati vengono rilasciati.

3.6.1 Accesso al certificato e alle liste di revoca

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

4. Modalità di identificazione e registrazione

Questo capitolo descrive le procedure usate per l'identificazione del ***Titolare*** ai fini del rilascio del Certificato One-Shot.

4.1 Modalità di identificazione

Il ***Certificatore*** deve verificare l'identità del ***Titolare*** prima di procedere al rilascio del certificato di sottoscrizione richiesto.

4.1.1 Soggetti abilitati ad effettuare l'identificazione

Ferma restando la responsabilità del ***Certificatore*** (§3.1.1), l'identità del soggetto ***Titolare*** viene accertata da:

Modalità 1
1. Il ***Certificatore***, anche tramite suoi Incaricati;
2. L'Ufficio di Registrazione, anche tramite suoi Incaricati;

Modalità 2
Intermediari finanziari e altri soggetti esercenti attività finanziaria.

Modalità 3
Identificazione tramite firma digitale.

Modalità 4
Identificazione tramite CNS/CIE.

Modalità 5
1. Il ***Certificatore***, anche tramite i suoi incaricati, supportati da un sistema di videoconferenza;
2. L'***Ufficio di registrazione***, anche tramite i suoi incaricati, supportati da un sistema di videoconferenza.

Modalità 6
Identificazione tramite le credenziali rilasciate per l'emissione di un precedente certificato one shot.

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 ***Titolare***.

Il soggetto che effettua l'identificazione verifica l'identità del ***Titolare*** 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

4.1.2.2 Riconoscimento effettuato secondo la modalità 2

Nella **modalità 2** il ***Certificatore*** si avvale del riconoscimento già effettuato da un Intermediario finanziario o da altro Soggetto Esercente Attività Finanziaria, che, ai sensi delle norme antiriciclaggio tempo per tempo vigente, è obbligato al riconoscimento dei propri clienti.

I dati utilizzati per il riconoscimento sono rilasciati dal ***Titolare*** ai sensi del D.Lgs. 231/07, a norma del quale i clienti sono tenuti a fornire - sotto la propria responsabilità - tutte le informazioni necessarie e aggiornate per consentire agli Intermediari e agli altri Soggetti Esercenti Attività Finanziaria di adempiere agli obblighi di identificazione della clientela.
Gli Intermediari e gli altri Soggetti Esercenti Attività Finanziaria acquisiscono i Dati in base alle procedure alle 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).
In questo caso, previo apposito accordo con l'Intermediario finanziario, **che agisce da Ufficio di Registrazione**, i dati identificativi del ***Titolare*** raccolti da quest'ultimo 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.
Analoga procedura si applica per i riconoscimenti antiriciclaggio effettuati in ossequi alla normativa francese di cui al [20].

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 ***Titolare*** è già in possesso di un dispositivo di firma con un certificato qualificato a bordo ancora in corso di validità. Il ***Titolare*** inoltra alla CA la richiesta di emissione del Certificato One-Shot, firmata digitalmente, tramite l'Ufficio di Registrazione.
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.2.4 Riconoscimento effettuato secondo la modalità 4

Nella **modalità 4** il ***Certificatore*** si basa sul riconoscimento già effettuato da un Ente Emettitore di CNS o dal Comune che ha rilasciato la CIE**.** Il ***Titolare,*** già in possesso di un dispositivo sicuro con un certificato CIE o CNS ancora in corso di validità, si autentica al portale del Certificatore o dell'Ufficio di Registrazione ed inoltra la richiesta di emissione del Certificato One-Shot.
I dati di registrazione sono conservati, in questo caso, esclusivamente in formato elettronico.

4.1.2.5 Riconoscimento effettuato secondo la modalità 5

Nella **modalità 5** l'identificazione è effettuata da uno dei soggetti indicati al §4.1.1 (Modalità 1) e sono richiesti, da parte del ***Titolare,*** il possesso di un PC, una webcam ad esso collegata e un sistema audio PC funzionante.
Il soggetto che effettua l'identificazione verifica l'identità del ***Titolare*** tramite il riscontro con documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile del ***Titolare***, firma autografa del ***Titolare*** e di timbro, rilasciato da un'Amministrazione dello Stato. E' facoltà del soggetto che effettua l'identificazione escludere l'ammissibilità del documento utilizzato dal ***Titolare*** se ritenuto carente delle caratteristiche elencate.
I dati identificativi del ***Titolare***, confermati all'atto del riconoscimento, vengono utilizzati per l'emissione del certificato, previa accettazione da parte del ***Titolare*** delle condizioni contrattuali e del trattamento dei dati personali, per il rilascio del certificato e degli strumenti per l'apposizione della firma nonché approvazione e conferma dei dati anagrafici registrati. I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati in forma protetta per una durata ventennale, secondo quanto indicato nell'art. 32, comma 1, lettera j) del CAD.
La procedura in uso soddisfa quanto richiesto dall'art. 32, comma 1, lettera a) del CAD.

4.1.2.6 Riconoscimento effettuato secondo la modalità 6

Nella **modalità 6** il ***Certificatore*** si basa sul riconoscimento già da esso stesso effettuato in occasione dell'emissione del primo certificato One Shot**.** Il ***Titolare,*** già in possesso delle credenziali per lo sblocco della firma, si autentica al portale del Certificatore o dell'Ufficio di Registrazione richiede l'emissione di un nuovo certificato, confermando o aggiornando i dati di registrazione.
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 ***Titolare*** deve attenersi per ottenere un certificato di sottoscrizione sono:

a) prendere visione del presente Manuale Operativo e dell'eventuale ulteriore documentazione informativa;
b) seguire le procedure di identificazione adottate dal ***Certificatore*** come descritte nel presente paragrafo;
c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
d) accettare 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 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 deve essere inviato dal ***Titolare***.

Sono considerate **obbligatorie** le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, ove presente, quali tipo, numero, ente emittente e data di rilascio dello stesso
- e-mail 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 Limiti d'uso e limiti di valore

Il Certificatore, per i Certificati One-Shot, può prevedere l'inserimento nel certificato di limiti di valore che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. **I valori sono espressi come numeri interi positivi, senza indicazione di cifre decimali.**

5. Operatività

5.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del ***Certificatore***.

La registrazione iniziale è effettuata presso il ***Certificatore*** oppure presso un Ufficio di Registrazione, anche telematicamente.

Conclusasi la fase di registrazione iniziale, il rilascio del Certificato One-Shot è previsto in unica modalità, ossia con chiavi generate su dispositivi HSM.

Questa procedura viene effettuata sotto la responsabilità di personale specializzato del ***Certificatore*** o da quest'ultimo debitamente autorizzato, 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***.

5.2 Rilascio del certificato

5.2.1 Caso A: Rilascio in presenza del Titolare

La procedura si applica nei casi in cui il Titolare è identificato da un Ufficio di Registrazione in presenza, ai sensi della Modalità 1 o 2 di identificazione. In questo secondo caso l'Ufficio di Registrazione è un Intermediario Finanziario o un Soggetto Esercente Attività Finanziaria.

1. Il Titolare si reca fisicamente presso l'Ufficio di Registrazione, che procede ad attestarne l'identità sulla base dei documenti di identità;
2. L'addetto dell'Ufficio di Registrazione richiama la procedura di inserimento dei dati anagrafici del Titolare;
3. Il ***Titolare***, utilizzando un tablet PC o interagendo con l'applicazione attraverso un monitor touch ovvero un monitor tradizionale e un mouse messi a sua disposizione, conferma i propri dati ed inserisce eventuali aggiornamenti dei medesimi relativamente ai dati accessori (indirizzo, casella mail);
4. Il ***Titolare*** manifesta la volontà di ottenere il rilascio di un certificato digitale mediante conferma ed accettazione della richiesta di registrazione sulla procedura, interagendo attraverso la strumentazione messa a disposizione . L'Ufficio di Registrazione produce un'evidenza informatica, con cui attesta le caratteristiche di veridicità della richiesta di rilascio, e la trasmette al Certificatore;
5. L'***Ufficio di registrazione*** comunica la corretta identificazione del Titolare al certificatore, che provvede al rilascio del certificato.

5.2.2 Caso B: Rilascio da remoto

La procedura si applica nei casi in cui il **Titolare** si collega da remoto alla procedura dell'Ufficio di Registrazione, che provvede all'identificazione ai sensi della Modalità 2 qualora sia un Intermediario Finanziario o un Soggetto Esercente Attività Finanziaria, ovvero si avvale alternativamente delle Modalità di identificazione 3, 4, 5 o 6:

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 del Titolare);
2) Il ***Titolare*** conferma i propri dati ed inserisce eventuali aggiornamenti dei medesimi;
3) L'***Ufficio di Registrazione*** inizia la procedura di identificazione da remoto tramite le Modalità da 2 a 6;Il Tit***olare*** manifesta la volontà di ottenere il rilascio di un certificato digitale mediante conferma sulla procedura web. L'Ufficio di Registrazione produce un'evidenza informatica, con cui attesta le caratteristiche di veridicità della richiesta di rilascio, e la trasmette al Certificatore;
5) Dopo il corretto completamento della procedura di identificazione, il **Certificatore** provvede all'emissione del Certificato One-Shot.

5.2.3 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 2048 bit.

5.2.4 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.

5.3 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 chiave pubblica che si intende certificare sia una chiave valida, della lunghezza prevista e non sia già stata certificata per un altro ***Titolare***;
   - la coppia di chiavi funzioni correttamente;
2) si procede alla generazione del certificato
3) 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.
4) il certificato viene pubblicato nel registro di riferimento (non accessibile da Internet) dei certificati;
5) il certificato viene memorizzato nei server del sistema di emissione.

5.3.1 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.

5.3.2 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. Il ***Titolare*** che volesse rendere pubblico il proprio certificato potrà richiederlo tramite la procedura descritta al §3.4.2.

5.3.3 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. 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 [16]

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato e da considerarsi non valido.
Il ***Titolare*** del certificato non può rinnovare il Certificato One-Shot il quale ha validità di non oltre 60 (sessanta) minuti dalla data ed ora di emissione.

6. Modalità per la sottoscrizione di documenti e verifica della firma

Il Certificato One-Shot è memorizzato all'interno di un HSM gestito dal Certificatore. I dati per la creazione della firma sono suddivisi in modo che unicamente attraverso la componente nota al Titolare possa essere apposta la firma digitali su documenti informatici.

6.1 Modalità di autenticazione per l'attivazione della firma remota.

Il Certificatore mette a disposizione due modalità di autenticazione da parte del Titolare per l'attivazione della procedura di firma remota. La firma può essere apposta unicamente tramite l'inserimento della componente di credenziale nota al Titolare.

6.1.1 Credenziali gestite dal Certificatore.

Il Certificatore ha predisposto per il Certificato One-Shot un sistema di gestione dinamico delle credenziali che richiede, per l'apposizione della firma remota, l'utilizzo di una OTP.

L'OTP è generata randomicamente dal sistema del Certificatore al momento dell'attivazione da parte del Titolare della procedura di firma remota.

La OTP viene trasmessa al Titolare tramite lo strumento hardware o software dallo stesso prescelto al momento della registrazione.

Con l'inserimento della OTP il Titolare avvia la procedura di firma remota provvedendo ad trasmettere il dato per la creazione della firma di sua esclusiva conoscenza, avviando così la procedura di Firma Digitale.

6.1.2 Credenziali gestite dall'Ufficio di Registrazione.

Il dato per la creazione della firma, necessario per l'attivazione della firma remota, può coincidere con delle componenti di un sistema di autenticazione gestito e verificato dall'Ufficio di Registrazione.

In tale ipotesi il Certificatore provvede a verificare la rispondenza dei requisiti di sicurezza del sistema gestito dall'Ufficio di Registrazione, assicurandosi che tale sistema garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del Titolare.

Il titolare, in questo caso, utilizza la componente di credenziale o il sistema di autenticazione già in essere presso l'Ufficio di Registrazione, provvedendo ad avviare la procedura di firma remota mediante l'inserimento di tale componente direttamente sul sistema dell'Ufficio di Registrazione che trasmette l'informazione alla procedura di firma remota, avviando così la procedura di Firma Digitale.

6.2 Modalità di verifica della firma.

I documenti sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF, formato di sottoscrizione previsto dall'Art.21 comma 8 e 15 della Deliberazione CNIPA n. 45.

Il formato di firma è conforme allo standard PadES (PDF Advanced Electronic Signatures) il quale non richiede la variazione dell'estensione del file ".pdf". La verifica può pertanto essere effettuata utilizzando il software Adobe Reader scaricabile gratuitamente dal sito www.adobe.com/it.

Ad un documento firmato è sempre collegato un riferimento temporale opponibile a terzi ai sensi della normativa vigente.

La verifica dei documenti sottoscritti potrà inoltre essere eseguita con il prodotto Dike gratuitamente scaricabile dai Titolari dal sito www.firma.infocert.it. Dike consente:

- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Deliberazione CNIPA [4].
- la verifica della firma apposta a documenti firmati digitalmente secondo il formato definito dalla Circolare AIPA 24/2000 [14].

Gli ambienti in cui Dike opera, i prerequisiti hardware e software nonché tutte le indicazioni per l'installazione del prodotto sono reperibili all'indirizzo web sopra indicato.

Le istruzioni per l'utilizzo del prodotto sono incluse nel prodotto stesso e consultabili tramite la funzione di help. Nel documento denominato "Manuale d'uso di Dike", facente parte integrante del presente Manuale Operativo, sono riportate le modalità operative per effettuare la generazione e la verifica della firma digitale.

7. Revoca e sospensione di un certificato

Essendo la durata del certificato minore o uguale del tempo minimo (60 (sessanta) minuti) previsto per rendere pubblica l'informazione sulla subentrata invalidità del certificato, per i certificati oggetto del presente Manuale Operativo non è prevista la possibilità di revoca e sospensione.

8. Rinvio

Per quanto non espressamente previsto si vedano i paragrafi 7, 8, 9, 10, 11, 12, 13, 14, 15 e 16 del Manuale Operativo ICERT-INDI-MO [[19]] a cui espressamente si rinvia.

9. Appendice: Macroistruzioni

A.2 Acrobat Reader

Sebbene il formato PDF sia giustamente noto per la produzione di materiale di stampa, l'introduzione di un interprete Javascript in Acrobat e Acrobat Reader permette di realizzare documenti con contenuti ipertestuali e dinamici.
Per disattivare la possibilità di esecuzione di codice javascript in file pdf si possono seguire i seguenti passi:

1. Fare clic sul menu **Modifica**, scegliere **Preferenze...**
2. Nella listbox a sinistra della finestra **Preferenze** selezionare con un clic la voce **Javascript**
3. **Deselezionare la checkbox Abilita Javascript di Acrobat;**
4. da questo momento l'eventuale presenza di Javascript verrà segnalata da un messaggio.