Schema D.P.C.M. dd mmmm 2011

Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici.

IL PRESIDENTE

DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il codice dell'amministrazione digitale e, in particolare, il capo II, che disciplina le firme elettroniche ed i certificatori, e l'art. 71, comma 1;

Visto il decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante codice in materia di protezione dei dati personali;

Visto il decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici, pubblicato nella Gazzetta Ufficiale 6 giugno 2009, n. 129;

Visto il decreto del Presidente della Repubblica in data 7 maggio 2008, con il quale l'on. prof. Renato Brunetta è stato nominato Ministro senza portafoglio;

Visto il decreto del Presidente del Consiglio dei Ministri dell'8 maggio 2008, con il quale al predetto Ministro senza portafoglio è stato conferito l'incarico per la pubblica amministrazione e l'innovazione;

Visto il decreto del Presidente del Consiglio dei ministri 13 giugno 2008, recante delega di funzioni del Presidente del Consiglio dei Ministri in materia pubblica amministrazione ed innovazione al Ministro senza portafoglio on. prof. Renato Brunetta;

Acquisito il parere tecnico di DigitPA di cui al decreto legislativo 12 febbraio 1993, n. 39 e successive modificazioni;

Sentito il Garante per la protezione dei dati personali;

Sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281 nella seduta del ;

Espletata la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con decreto legislativo 23 novembre 2000, n. 427;

Decreta:

TITOLO I

DISPOSIZIONI GENERALI

Art. 1. Definizioni

1. Ai fini delle presenti regole tecniche si applicano le definizioni contenute nell'art. 1 del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni. Si intende, inoltre, per:
a) codice: il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82;
b) chiavi: la coppia di chiavi asimmetriche come definite all'articolo 1, comma 1, lettere h) e i), del codice;
c) DigitPA: ente pubblico non economico istituito con D.Lgs 1 dicembre 2009, n. 177;
d) compromissione della chiave privata: la sopravvenuta assenza di affidabilità nelle caratteristiche di sicurezza della chiave crittografica privata;
e) dati per la creazione della firma: l'insieme dei codici personali e delle altre quantità di sicurezza, quali le chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica qualificata o una firma digitale;
f) evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
g) funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti;
h) impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;
i) marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;
l) registro dei certificati: la combinazione di uno o più archivi informatici, tenuto dal certificatore, contenente tutti i certificati emessi;
m) riferimento temporale: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
n) dispositivi sicuri per la generazione della firma elettronica qualificata: mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art. 12;
o) dispositivi sicuri per la generazione della firma digitale: mezzi sui quali il firmatario può conservare un controllo esclusivo la cui conformità è accertata ai sensi dell'art.13;
p) HSM: insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche;
q) firma remota: particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse;

r) firma automatica: particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, ma in assenza di presidio puntuale e continuo da parte di questo.

Art. 2. Ambito di applicazione

1. Il presente decreto stabilisce, ai sensi degli articoli 20, 24 comma 4, 27, 28, 29, 30, 32, 33, 35 comma 2 e 36 del codice, le regole tecniche per la generazione, apposizione e verifica della firma elettronica avanzata, qualificata e digitale, per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati.

2. Le disposizioni di cui al titolo II si applicano ai certificatori che rilasciano al pubblico certificati qualificati in conformità al codice.

3. Ai certificatori accreditati o che intendono accreditarsi ai sensi del codice, si applicano, oltre a quanto previsto dal comma 2, anche le disposizioni di cui al titolo III.

4. I certificatori accreditati rendono disponibile ai propri titolari un sistema di validazione temporale conforme alle disposizioni di cui al titolo IV.

5. Le disposizioni di cui al titolo V si applicano ai soggetti che intendono realizzare soluzioni di firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis) del codice. Non si applicano a soluzioni di firma elettronica qualificata e digitale.

6. Ai prodotti sviluppati o commercializzati in uno degli Stati membri dell'Unione europea e dello spazio economico europeo in conformità alle norme nazionali di recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, pubblicata nella Gazzetta Ufficiale dell'Unione europea, Serie L, n. 13 del 19 gennaio 2000, è consentito di circolare liberamente nel mercato interno.

Art. 3. Disposizioni generali

1. La firma elettronica qualificata è generata esclusivamente con i dispositivi di cui all'art. 1, comma 1, lettere n) e p).

2. La firma digitale è generata con i dispositivi di cui all'art. 1, comma 1, lettera n) o con i dispositivi di cui all'art. 1, comma 1, lettere o) e p).

3. La firma elettronica qualificata generata ai sensi delle presenti regole tecniche produce i medesimi effetti stabiliti dal codice per la firma digitale.

4. Fermo restando quanto prescritto dal codice per la firma elettronica avanzata, il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale ai sensi delle presenti regole tecniche, possiede caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità tali da soddisfare la valutazione prevista all'art. 20, comma 1-bis, del codice.

5. La firma remota di cui all'art. 1, comma 1, lettera q), è generata su un HSM custodito e gestito sotto la responsabilità del certificatore accreditato ovvero dell'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dell'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi. Il certificatore deve essere in grado, dato un certificato qualificato, di individuare agevolmente il dispositivo afferente la corrispondente chiave privata.

6. Nel caso in cui il dispositivo di cui al comma 5 non sia custodito dal certificatore, questo deve:
a) indicare al soggetto che custodisce il dispositivo le procedure operative, gestionali e le misure di sicurezza fisica e logica che tale soggetto è obbligato ad applicare
b) effettuare delle verifiche periodiche sulla corretta applicazione delle indicazioni di cui alla lettera a), che il soggetto che custodisce il dispositivo ha l'obbligo di consentire ed agevolare;
c) redigere dei verbali dell'attività di verifica di cui alla lettera b) che potranno essere richiesti in copia da DigitPa ai fini dell'attività di cui all'art. 31 del codice;
d) comunicare a DigitPA il luogo ove i dispositivi sono custoditi;
e) effettuare ulteriori verifiche su richiesta di DigitPA consentendo, se richiesto, a incaricati della stessa di parteciparvi;
f) assicurare che il soggetto che custodisce il dispositivo si impegni al fine di consentire le verifiche di cui alle lettere b) ed e).

7. Nel caso in cui il certificatore venga a conoscenza dell'inosservanza di quanto previsto al comma precedente, procede alla revoca dei certificati afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.

8. La firma remota di cui all'art. 1, comma 1, lettera q), è realizzata con misure tecniche ed organizzative, esplicitamente approvate per le rispettive competenze da DigitPA, nell'ambito delle attività di cui agli articoli 29 e 31 del codice e da OCSI per quanto concerne la sicurezza del dispositivo ai sensi dell'art. 35 del codice, tali da garantire al titolare il controllo esclusivo della chiave privata.

TITOLO II

REGOLE TECNICHE DI BASE

Art. 4. Norme tecniche di riferimento

1. I dispositivi sicuri per la generazione delle firme di cui all'art. 35 del codice sono conformi alle norme generalmente riconosciute a livello internazionale.

2. Gli algoritmi di generazione e verifica della firma elettronica qualificata e della firma digitale, le caratteristiche delle chiavi utilizzate, le funzioni di hash, i formati e le caratteristiche dei certificati qualificati, le caratteristiche della firma elettronica qualificata e della firma digitale, delle marche temporali, le caratteristiche delle applicazioni di verifica di cui all'articolo 14, il formato dell'elenco di cui all'art. 43 del presente decreto, le modalità con cui rendere disponibili le informazioni sullo stato dei certificati, sono definiti, anche ai fini del riconoscimento e della

verifica del documento informatico, con provvedimenti DigitPA e pubblicati sul sito internet dello stesso Ente. Nelle more dell'emanazione di tali provvedimenti continua ad applicarsi la Deliberazione del Centro Nazionale per l'Informatica nella Pubblica Amministrazione n. 45 del 21 maggio 2009 e successive modificazioni.

3. Il documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21, comma 2, del codice, se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Art. 5. Caratteristiche generali delle chiavi

1. Una coppia di chiavi per la creazione e la verifica della firma elettronica qualificata o della firma digitale può essere attribuita ad un solo titolare.

2. Se il soggetto appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del codice, deve utilizzare una coppia di chiavi destinata a tale scopo diversa da tutte le altre in suo possesso. L'utilizzo di tale procedura deve essere indicato esplicitamente nel certificato qualificato.

3. Se la procedura automatica di cui al comma 2 fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

4. Ai fini del presente decreto, le chiavi afferenti i certificati qualificati ed i correlati servizi, si distinguono secondo le seguenti tipologie:
a) chiavi di sottoscrizione, destinate alla generazione e verifica della firma elettronica qualificata o della firma digitale apposta o associata ai documenti;
b) chiavi di certificazione, utilizzabili per la generazione e verifica delle firme apposte o associate ai certificati qualificati, per la sottoscrizione delle informazioni sullo stato di validità dei certificati, per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali;
d) chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati.

5. Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste per ciascuna tipologia dal comma 4, salvo che, con riferimento esclusivo alle chiavi di cui al medesimo comma 4, lettera b), DigitPA non ne autorizzi l'utilizzo per altri scopi.

6. Le caratteristiche quantitative e qualitative delle chiavi sono tali da garantire un adeguato livello di sicurezza in rapporto allo stato delle conoscenze scientifiche e tecnologiche, in conformità con quanto indicato nei provvedimenti di cui all'art. 4, comma 2.

7. L'uso delle chiavi di cui al comma 4 lettera d), il loro uso e il profilo del certificato alle stesse associato, sono definiti con il provvedimento di cui all'art. 4, comma 2. A tali chiavi dovrà essere associato un certificato sottoscritto con le stesse chiavi di certificazione con cui sono sottoscritti i certificati di cui si forniscono informazioni sullo stato di validità.

Art. 6. Generazione delle chiavi

1. La generazione della coppia di chiavi è effettuata mediante dispositivi e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e un adeguato livello di sicurezza della coppia generata, nonché la segretezza della chiave privata.

2. Il sistema di generazione della coppia di chiavi comunque assicura:
a) la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
b) l'utilizzo di algoritmi che consentano l'equiprobabilità di generazione di tutte le coppie possibili;
c) l'autenticazione informatica del soggetto che attiva la procedura di generazione.

Art. 7. Modalità di generazione delle chiavi

1. Le chiavi di cui all'art. 5, comma 4, lettere b) e d) possono essere generate esclusivamente in presenza del responsabile del servizio.

2. Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.

3. La generazione delle chiavi di sottoscrizione effettuata autonomamente dal titolare, avviene all'interno del dispositivo sicuro per la generazione delle firme, che è rilasciato o indicato dal certificatore, con modalità atte ad impedire che la medesima chiave possa essere associata a più certificati.

4. Il certificatore è tenuto ad assicurarsi che il dispositivo sicuro per la generazione della firma elettronica qualificata, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 35 del codice e agli articoli 11 e 12 del presente decreto e a fornirne evidenza a DigitPa ai fini dell'attività di cui all'art. 31 del codice.

5. Il certificatore è tenuto ad assicurarsi che il dispositivo sicuro per la generazione della firma digitale, da lui fornito o indicato, presenti le caratteristiche e i requisiti di sicurezza di cui all'art. 35 del codice e agli articoli 11 e 13 del presente decreto e a fornirne evidenza a DigitPa ai fini dell'attività di cui all'art. 31 del codice.

6. Il titolare è tenuto ad utilizzare esclusivamente il dispositivo sicuro per la generazione delle firme fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

Art. 8. Conservazione delle chiavi e dei dati per la creazione della firma

1. Fatto salvo quanto disposto ai commi 2, 3 e 4, è vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

2. Per fini particolari di sicurezza, è consentito che le chiavi di certificazione vengano esportate, purché ciò avvenga con modalità tali da non ridurre il livello di sicurezza e di riservatezza delle chiavi stesse.

3. E' consentita l'esportazione sicura delle chiavi private di cui all'art.5, comma 4, lettera a) per la firma remota presenti su HSM al di fuori del dispositivo stesso, esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento del dispositivo in uso, purché protette con algoritmi crittografici ritenuti adeguati ai fini della certificazione e purché le operazioni di esportazione e importazione delle chiavi siano effettuate mediante funzionalità di sicurezza certificate implementate dai dispositivi sicuri di firma. La conservazione delle chiavi esportate deve avvenire nell'ambiente operativo del dispositivo sicuro di firma, sottoposta a opportune misure di sicurezza di tipo fisico e procedurale che debbono essere descritte, in forma di obiettivi o ipotesi per l'ambiente, nel relativo Traguardo di Sicurezza.

4. E' consentita la replicazione in sicurezza delle chiavi private di cui all'art.5, comma 4, lettera a) per la firma remota presenti su HSM al fine di realizzare una configurazione ad alta affidabilità del dispositivo sicuro di firma a condizione che tale configurazione rientri tra quelle sottoposte a certificazione ai sensi degli articoli 12 o 13. L'operazione di replicazione deve prevedere la protezione delle chiavi con algoritmi crittografici ritenuti adeguati ai fini della certificazione ed essere effettuata mediante funzionalità di sicurezza certificate implementate dal dispositivo sicuro di firma. Le chiavi replicate debbono essere conservate all'interno di dispositivi certificati con le stesse caratteristiche di sicurezza e controllati dal dispositivo certificato di origine, collocati nello stesso ambiente operativo o in altro ambiente con equivalente livello di sicurezza. Solo uno dei dispositivi fisici in questa configurazione deve essere abilitato ad effettuare le operazioni di firma.

5. Il titolare della coppia di chiavi:
a) assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal certificatore al fine di adempiere agli obblighi di cui all'art. 32, comma 1, del codice;
b) conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore;
c) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale inutilizzabili o di cui abbia perduto il possesso o il controllo esclusivo;
d) mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma;
e) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale qualora abbia il ragionevole dubbio che essi possano essere usati da altri.

Art. 9. Generazione delle chiavi di sottoscrizione al di fuori del dispositivo di firma

1. Il certificatore, se la certificazione del dispositivo di firma lo consente, può utilizzare un sistema diverso da quello destinato all'uso della chiave privata per la generazione delle chiavi di sottoscrizione.

2. Il certificatore descrive dettagliatamente il sistema di cui al comma 1 nel piano della sicurezza.

Art. 10. Sicurezza del sistema di generazione delle chiavi diverso dal dispositivo di firma

1. Se la generazione delle chiavi di sottoscrizione avviene su un sistema di cui all'art. 9, il sistema di generazione assicura:
a) l'impossibilità di intercettazione o recupero di qualsiasi informazione, anche temporanea, prodotta durante l'esecuzione della procedura;
b) il trasferimento della chiave privata, in condizioni di massima sicurezza, nel dispositivo di firma in cui verrà utilizzata.

2. Il sistema di generazione è isolato, dedicato esclusivamente a questa attività ed adeguatamente protetto.

3. L'accesso al sistema è controllato e ciascun utente è preventivamente identificato per l'accesso fisico e autenticato per l'accesso logico. Ogni sessione di lavoro è registrata nel giornale di controllo.

4. Il sistema è dotato di strumenti di controllo della propria configurazione che consentano di verificare l'autenticità e l'integrità del software installato e l'assenza di programmi non previsti dalla procedura e di dati residuali provenienti dalla generazione di coppie di chiavi precedenti che possano inficiare l'equiprobabilità della generazione di quelle successive.

Art. 11. Dispositivi sicuri e procedure per la generazione delle firme elettroniche qualificate e delle firme digitali

1. La generazione delle firme elettroniche qualificate e delle firme digitali avviene all'interno di un dispositivo sicuro per la generazione delle firme, così che non sia possibile l'intercettazione della chiave privata utilizzata.

2. Il dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale deve poter essere attivato esclusivamente dal titolare mediante sistemi di autenticazione ritenuti adeguati, secondo le rispettive competenze, dall'OCSI e da DigitPA, prima di procedere alla generazione della firma.

3. DigitPA, nell'ambito dell'attività di cui agli articoli 29 e 31 del codice, valuta l'adeguatezza tecnologica dei sistemi di autenticazione per quanto concerne l'interazione fra il titolare e il dispositivo sicuro per la generazione della firma, tenuto conto del traguardo di sicurezza di cui al DPCM 30 ottobre 2003 e del contesto di utilizzo.

4. La personalizzazione del dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale garantisce almeno:
a) l'acquisizione da parte del certificatore dei dati identificativi del dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale utilizzato e la loro associazione al titolare;
b) la registrazione nel dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale del certificato qualificato, relativo alle chiavi di sottoscrizione del titolare.

5. La personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali può prevedere, per l'utilizzo nelle procedure di firma, la registrazione, nel dispositivo medesimo, del certificato elettronico relativo alla chiave pubblica del certificatore la cui corrispondente privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del titolare.

6. La personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali è registrata nel giornale di controllo.

7. Il certificatore adotta, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme elettroniche qualificate e digitali, procedure atte ad identificare il titolare del dispositivo medesimo e dei certificati in esso contenuti.

8. I certificatori che rilasciano certificati qualificati forniscono almeno un sistema che consenta la generazione delle firme elettroniche qualificate e digitali.

Art. 12. Ulteriori requisiti per i dispositivi sicuri per la generazione della firma elettronica qualificata

1. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma elettronica qualificata, anche remota o automatica, prevista dall'art. 35 del codice è effettuata secondo criteri non inferiori a quelli previsti:
a) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai Profili di Protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni;
b) dal livello EAL 4+ della norma ISO/IEC 15408, in conformità ai Profili di Protezione o traguardi di sicurezza giudicati adeguati ai sensi dell'art. 35, commi 5 e 6 del codice, e successive modificazioni.

Art. 13. Ulteriori requisiti per i dispositivi sicuri per la generazione della firma digitale

1. Salvo quanto disposto al comma 2, la certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma digitale è effettuata ai sensi dell’articolo 12.

2. Fermo restando quanto disposto al comma 1, ulteriori modalità di verifica della conformità ai requisiti di sicurezza dei dispositivi sicuri per la creazione di una firma digitale remota previsti dall'art. 35, commi 1 e 2 del codice potranno essere individuate dal preposto organismo.

3. I certificati qualificati afferenti chiavi private custodite nei dispositivi di cui al comma 2, non devono contenere l’estensione qcStatements id-etsi-qcs-QcSSCD.

Art. 14. Verifica delle firme elettroniche qualificate e digitali

1. I certificatori che rilasciano certificati qualificati forniscono ovvero indicano almeno un sistema che consenta di effettuare la verifica delle firme elettroniche qualificate e delle firme digitali, conforme a quanto stabilito con i provvedimenti di cui all’art. 4, comma 2.

2. Il sistema di verifica delle firme elettroniche qualificate e digitali deve quantomeno:
a) presentare, almeno sinteticamente, lo stato di aggiornamento delle informazioni di validità dei certificati di certificazione presenti nell'elenco pubblico;
b) visualizzare le informazioni presenti nel certificato qualificato, in attuazione di quanto stabilito nell'art. 28, comma 3, del codice, nonché le estensioni obbligatorie nel certificato qualificato (qcStatements), indicate nei provvedimenti di cui all'art. 4, comma 2;
c) consentire l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori;
d) in caso di firme multiple, visualizzare l'eventuale dipendenza tra queste;
e) visualizzare chiaramente l'esito della verifica dello stato del certificato qualificato;
f) rendere evidente l'esito della verifica delle firme;
g) consentire di salvare il risultato dell'operazione di verifica su un documento informatico.

3. DigitPA, ai sensi dell'art. 31 del codice, accerta la conformità dei sistemi di verifica di cui al comma 1 alle norme del codice e alle presenti regole tecniche.

4. DigitPA, al fine di fornire garanzie di attendibilità nelle operazioni di verifica e di rendere effettivamente interoperabili le firme elettroniche qualificate e le firme digitali, anche in base all'evoluzione delle normative europee ed all'evoluzione degli standard tecnici, definisce e diffonde Regole Operative o Linee Guida per la verifica della firma elettronica qualificata e della firma digitale apposte a documenti informatici cui i certificatori accreditati hanno l'obbligo di attenersi.

Art. 15. Informazioni riguardanti i certificatori

1. I certificatori che rilasciano al pubblico certificati qualificati ai sensi del codice forniscono a DigitPA le seguenti informazioni e documenti a loro relativi:
a) dati anagrafici ovvero denominazione o ragione sociale;
b) residenza ovvero sede legale;
c) sedi operative;
d) rappresentante legale;
e) certificati delle chiavi di certificazione;
f) piano per la sicurezza di cui al successivo art. 35;
g) manuale operativo di cui al successivo art. 40;
h) relazione sulla struttura organizzativa;
i) copia di una polizza assicurativa a copertura dei rischi dell'attività e dei danni causati a terzi.

2. DigitPA rende accessibili, in via telematica, le informazioni di cui al comma 1, lettere a), b), e), g) al fine di rendere pubbliche le informazioni che individuano il certificatore qualificato. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.

Art. 16. Comunicazione tra certificatore e DigitPA

1. I certificatori che rilasciano al pubblico certificati qualificati comunicano a DigitPA la casella di posta elettronica certificata da utilizzare per realizzare un sistema di comunicazione attraverso il quale scambiare le informazioni previste dal presente decreto.

2. DigitPA rende disponibile sul proprio sito internet l'indirizzo della propria casella di posta elettronica certificata.

Art. 17. Generazione e uso delle chiavi del certificatore

1. La generazione delle chiavi di certificazione avviene in modo conforme a quanto previsto dalle presenti regole tecniche.

2. Per ciascuna chiave di certificazione il certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

3. I valori contenuti nei singoli campi del certificato delle chiavi di certificazione sono codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

4. La certificazione di sicurezza dei dispositivi sicuri per la creazione di una firma utilizzati per le chiavi di cui all'art. 5, comma 4, lettere b), c) e d), è effettuata secondo criteri non inferiori a quelli previsti:
a) dal livello EAL 4+ della norma ISO/IEC 15408 in conformità ai Profili di Protezione indicati nella decisione della Commissione europea 14 luglio 2003 e successive modificazioni;
b) dal livello di certificazione e in conformità ai Profili di Protezione o traguardi di sicurezza giudicati adeguati dagli organismi di cui all'art. 11, comma 1, lettera b) della Direttiva Europea 1999/93/EU.

5. La certificazione di sicurezza di cui al comma 4 può inoltre essere effettuata secondo i criteri previsti dal livello di valutazione E3 e robustezza HIGH dell'ITSEC, o superiori, con un traguardo di sicurezza giudicato adeguato dal DigitPA nell'ambito dell'attività di cui agli articoli 29 e 31 del codice.

Art. 18. Generazione dei certificati qualificati

1. In aggiunta agli obblighi previsti per il certificatore dall'art. 32 del codice, emettendo il certificato qualificato il certificatore:
a) si accerta dell'autenticità della richiesta;
b) nel caso di chiavi generate dal certificatore, assicura la consegna al legittimo titolare ovvero, nel caso di chiavi non generate dal certificatore, verifica il possesso della chiave privata da parte del titolare e il corretto funzionamento della coppia di chiavi.

2. Il certificato qualificato è generato con un sistema conforme a quanto previsto dall'art. 33.

3. Il termine del periodo di validità del certificato qualificato precede di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità.

4. L'emissione dei certificati qualificati è registrata nel giornale di controllo specificando il riferimento temporale relativo alla registrazione.

Art. 19. Informazioni contenute nei certificati qualificati

1. Fatto salvo quanto previsto dall'art. 28 del codice, i certificati qualificati contengono almeno le seguenti ulteriori informazioni:
a) codice identificativo del titolare presso il certificatore;
b) tipologia della coppia di chiavi in base all'uso cui sono destinate.

2. Le informazioni personali contenute nel certificato ai sensi di quanto previsto nell'art. 28 del codice sono utilizzabili unicamente per identificare il titolare della firma elettronica qualificata o della firma digitale, per verificare la firma del documento informatico, nonché per indicare eventuali qualifiche specifiche del titolare.

3. I valori contenuti nei singoli campi del certificato qualificato sono codificati in modo da non generare equivoci relativi al nome, ragione o denominazione sociale del certificatore.

4. Le informazioni e le qualifiche di cui all'art. 28, comma 3, lettera a) del Codice, codificate secondo le modalità indicate dai provvedimenti di cui all'art. 4, comma 2, del presente decreto, sono inserite d'ufficio dal certificatore nel certificato qualificato, nel caso in cui l'organizzazione di appartenenza abbia autorizzato la richiesta di emissione del certificato medesimo. In quest'ultimo caso l'organizzazione richiedente assume l'impegno di richiedere la revoca del certificato qualificato qualora venga a conoscenza della variazione delle informazioni contenute nello stesso.

5. Il certificatore, salvo quanto disposto al comma 6, determina il periodo di validità dei certificati qualificati anche in funzione della robustezza crittografica delle chiavi impiegate.

6. DigitPA, ai sensi dell'art. 4, comma 2, determina il periodo massimo di validità del certificato qualificato in funzione degli algoritmi e delle caratteristiche delle chiavi.

7. Il certificatore custodisce le informazioni di cui all'art. 32, comma 3, lettera j) del codice, per un periodo pari a 20 (venti) anni dalla data di emissione del certificato qualificato, salvo quanto previsto dall'art. 11 del decreto legislativo n. 196 del 2003.

Art. 20. Revoca e sospensione del certificato qualificato

1. Fatto salvo quanto previsto dall'articolo 36 del codice, il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme elettroniche qualificate o digitali.

2. Il certificatore conserva le richieste di revoca e sospensione per lo stesso periodo previsto all'art. 19, comma 7.

Art. 21. Codice di emergenza

1. Per ciascun certificato qualificato emesso il certificatore fornisce al titolare almeno un codice riservato, da utilizzare per richiedere la sospensione del certificato nei casi di emergenza indicati nel manuale operativo e comunicati al titolare.

2. La richiesta di cui al comma 1 è successivamente confermata utilizzando una delle modalità previste dal certificatore.

3. Il certificatore adotta specifiche misure di sicurezza per assicurare la segretezza del codice di emergenza.

Art. 22. Revoca dei certificati qualificati relativi a chiavi di sottoscrizione

1. La revoca del certificato qualificato relativo a chiavi di sottoscrizione viene effettuata dal certificatore mediante l'inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL).

2. Se la revoca avviene a causa della possibile compromissione della chiave privata, il certificatore deve procedere tempestivamente alla pubblicazione dell'aggiornamento della lista di revoca.

3. La revoca dei certificati è annotata nel giornale di controllo con la specificazione della data e dell'ora della pubblicazione della CRL.

4. Il certificatore comunica tempestivamente l'avvenuta revoca al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta revocato.

Art. 23. Revoca su iniziativa del certificatore

1. Salvo i casi di motivata urgenza, il certificatore che intende revocare un certificato qualificato ne dà preventiva comunicazione al titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

Art. 24. Revoca su richiesta del titolare

1. La richiesta di revoca è inoltrata al certificatore munita della sottoscrizione del titolare e con la specificazione della sua decorrenza.

2. Le modalità di inoltro della richiesta sono indicate dal certificatore nel manuale operativo di cui al successivo art. 40.

3. Il certificatore verifica l'autenticità della richiesta e procede alla revoca entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal precedente comma 2.

4. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 25. Revoca su richiesta del terzo interessato

1. La richiesta di revoca da parte del terzo interessato da cui derivano i poteri di firma del titolare è inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua decorrenza.

2. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca di cui al comma 1 è inoltrata non appena il terzo venga a conoscenza della variazione di stato.

3. Se il certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato.

Art. 26. Sospensione dei certificati qualificati

1. La sospensione del certificato qualificato è effettuata dal certificatore mediante l'inserimento del suo codice identificativo in una delle liste dei certificati revocati e sospesi (CRL).

2. Il certificatore comunica tempestivamente l'avvenuta sospensione al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato qualificato risulta sospeso.

3. Il certificatore indica nel manuale operativo, ai sensi dell'art. 40, comma 3, lettera l), la durata massima del periodo di sospensione e le azioni intraprese al termine dello stesso in assenza di diverse indicazioni da parte del soggetto che ha richiesto la sospensione.

4. In caso di revoca di un certificato qualificato sospeso, la data della stessa decorre dalla data di inizio del periodo di sospensione.

5. La sospensione e la cessazione della stessa sono annotate nel giornale di controllo con l'indicazione della data e dell'ora di esecuzione dell'operazione.

6. La cessazione dello stato di sospensione del certificato, che sarà considerato come mai sospeso, è tempestivamente comunicata al titolare e all'eventuale terzo interessato specificando la data e l'ora a partire dalla quale il certificato ha cambiato stato.

Art. 27. Sospensione su iniziativa del certificatore

1. Salvo casi d'urgenza, che il certificatore è tenuto a motivare contestualmente alla comunicazione conseguente alla sospensione di cui al comma 2, il certificatore che intende sospendere un certificato qualificato ne dà preventiva comunicazione al titolare e all'eventuale terzo interessato specificando i motivi della sospensione e la sua durata.

2. Se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il certificatore procede tempestivamente alla pubblicazione della sospensione.

Art. 28. Sospensione su richiesta del titolare

1. La richiesta di sospensione è inoltrata al certificatore secondo le modalità indicate nel manuale operativo previa approvazione di DigitPA e con la specificazione della sua durata.

2. Il certificatore verifica l'autenticità della richiesta e procede alla sospensione entro il termine richiesto. Sono considerate autentiche le richieste inoltrate con le modalità previste dal precedente comma 1.

Art. 29. Sospensione su richiesta del terzo interessato

1. La richiesta di sospensione da parte del terzo interessato, da cui derivano i poteri di firma del titolare, è inoltrata al certificatore munita di sottoscrizione e con la specificazione della sua durata.

Art. 30. Sostituzione delle chiavi di certificazione

1. La procedura di sostituzione delle chiavi, generate dal certificatore in conformità all'art. 17 del presente decreto, assicura il rispetto dei termini di cui all’art. 18, comma 3.

2. I certificati generati a seguito della sostituzione delle chiavi di certificazione sono inviati al DigitPA.

Art. 31. Revoca dei certificati relativi a chiavi di certificazione

1. La revoca del certificato relativo ad una coppia di chiavi di certificazione è consentita solo nei seguenti casi:
a) compromissione della chiave privata;
b) malfunzionamento irrecuperabile del dispositivo sicuro per la generazione delle firme;
c) cessazione dell'attività.

2. La revoca è comunicata entro ventiquattro ore a DigitPA e resa nota a tutti i titolari di certificati qualificati sottoscritti con la chiave privata la cui corrispondente chiave pubblica è contenuta nel certificato revocato.

3. La revoca di certificati di cui al comma 1, pubblicati da DigitPA nell'elenco pubblico dei certificatori di cui all'art. 43, è resa nota attraverso il medesimo elenco.

Art. 32. Requisiti di sicurezza dei sistemi operativi

1. I sistemi operativi dei sistemi di elaborazione utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati qualificati e la gestione del registro dei certificati qualificati, devono essere stati oggetto di opportune personalizzazioni atte a innalzarne il livello di sicurezza (hardening) a cura del certificatore.

2. Ai sensi dell'art. 31 del codice, DigitPA verifica l'idoneità delle personalizzazioni di cui al comma 1 e indica al certificatore eventuali azioni correttive.

3. Il comma 1 non si applica al sistema operativo dei dispositivi di firma.

Art. 33. Sistema di generazione dei certificati qualificati

1. La generazione dei certificati qualificati avviene su un sistema utilizzato esclusivamente per la generazione di certificati, situato in locali adeguatamente protetti.

2. L'entrata e l'uscita dai locali protetti è registrata sul giornale di controllo.

3. L'accesso ai sistemi di elaborazione è consentito, limitatamente alle funzioni assegnate, esclusivamente al personale autorizzato, identificato attraverso un'opportuna procedura di riconoscimento da parte del sistema al momento di apertura di ciascuna sessione.

4. L'inizio e la fine di ciascuna sessione sono registrati sul giornale di controllo.

Art. 34. Accesso del pubblico ai certificati

1. Le liste dei certificati revocati e sospesi sono rese pubbliche.

2. I certificati qualificati, su richiesta del titolare, possono essere accessibili alla consultazione del pubblico nonché comunicati a terzi, al fine di verificare le firme digitali, esclusivamente nei casi consentiti dal titolare del certificato e nel rispetto del decreto legislativo 30 giugno 2003, n. 196.

3. Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati eventualmente resi accessibili alla consultazione del pubblico, sono utilizzabili da chi li consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità delle firme elettroniche qualificate e digitali.

4. Chiunque ha diritto di sapere se a proprio nome sia stato rilasciato un certificato qualificato. Le modalità per ottenere l'informazione di cui al periodo precedente sono definite con il provvedimento di cui all'art. 42, comma 10 del presente decreto.

Art. 35. Piano per la sicurezza

1. Il certificatore definisce un piano per la sicurezza nel quale sono contenuti almeno i seguenti elementi:
a) struttura generale, modalità operativa e struttura logistica;
b) descrizione dell'infrastruttura di sicurezza fisica rilevante ai fini dell'attività di certificatore;
c) allocazione dei servizi e degli uffici negli immobili rilevanti ai fini dell'attività di certificatore;
d) descrizione delle funzioni del personale e sua allocazione ai fini dell'attività di certificatore;
e) attribuzione delle responsabilità;
f) algoritmi crittografici o altri sistemi utilizzati;
g) descrizione delle procedure utilizzate nell'attività di certificatore;
h) descrizione dei dispositivi installati;
i) descrizione dei flussi di dati;
l) procedura di gestione delle copie di sicurezza dei dati;
m) procedura di continuità operativa del servizio di pubblicazione delle liste di revoca e sospensione;
n) analisi dei rischi;
o) descrizione delle contromisure;
p) descrizione delle verifiche e delle ispezioni;
q) descrizione delle misure adottate ai sensi degli articoli 32, comma 1 e 47, comma 2;
r) procedura di gestione dei disastri.
s) descrizione della procedura di cui all'articolo 8, comma 3, ponendo in rilievo le modalità di conservazione e protezione dei supporti contenenti le chiavi esportate;
t) misure di sicurezza per la protezione dei dispositivi di firma remota, ivi comprese le modalità di custodia;
u) limitatamente a quanto previsto all'articolo 11, comma 3, modalità con cui è assicurato il controllo esclusivo delle chiavi private custodite sui dispositivi di firma remota;
v) le misure procedurali e tecniche applicate per la distruzione dei dispositivi HSM e delle chiavi che contengono in caso di guasto del dispositivo HSM che non consente l'applicazione delle funzionalità di sicurezza certificate implementate dai dispositivi medesimi

2. Quanto previsto dalle lettere t) e u) del comma precedente può essere oggetto di dichiarazioni separate da parte del certificatore, ad integrazione del piano per la sicurezza.

3. DigitPA, a seguito dell'analisi di quanto dichiarato alle lettere t) e u) del comma 1, può imporre al certificatore di inserire nei certificati qualificati afferenti la firma remota limitazioni d'uso e di valore.

4. Il piano per la sicurezza, sottoscritto dal legale rappresentante del certificatore, ovvero dal responsabile della sicurezza da questo delegato, è consegnato a DigitPA in busta sigillata o cifrato, al fine di garantirne la riservatezza, in base alle indicazioni fornite da DigitPA.

5. Il piano per la sicurezza si attiene almeno alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'art. 33 del decreto legislativo 30 giugno 2003, n. 196.

Art. 36. Giornale di controllo

1. Il giornale di controllo è costituito dall'insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il certificatore, allorché si verificano le condizioni previste dal presente decreto.

2. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.

3. A ciascuna registrazione è apposto un riferimento temporale.

4. Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.

5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.

6. Le registrazioni contenute nel giornale di controllo sono conservate per un periodo pari a venti anni, salvo quanto previsto dall'art. 11 del decreto legislativo n. 196 del 2003.

Art. 37. Sistema di qualità del certificatore

1. Entro un anno dall'avvio dell'attività di certificazione, il certificatore dichiara la conformità del proprio sistema di qualità alle norme ISO 9000, successive modifiche o a norme equivalenti.

2. Il manuale della qualità è depositato presso DigitPA e reso disponibile presso il certificatore.

Art. 38. Organizzazione del personale addetto al servizio di certificazione

1. Fatto salvo quanto previsto al comma 3, l'organizzazione del certificatore prevede almeno le seguenti figure professionali:
a) responsabile della sicurezza;
b) responsabile del servizio di certificazione e validazione temporale;
c) responsabile della conduzione tecnica dei sistemi;
d) responsabile dei servizi tecnici e logistici;
e) responsabile delle verifiche e delle ispezioni (auditing).

2. Non è possibile attribuire al medesimo soggetto più funzioni tra quelle previste dal comma 1.

3. Ferma restando la responsabilità del certificatore, l'organizzazione dello stesso può prevedere che alcune delle suddette responsabilità siano affidate ad altre organizzazioni. In questo caso il

responsabile della sicurezza o altro dipendente appositamente designato gestisce i rapporti con tali figure professionali.

4. In nessun caso quanto previsto al comma 3 si applica per le figure professionali di cui al comma 1, lettere a) ed e).

Art. 39. Requisiti di competenza ed esperienza del personale

1. Il personale cui sono attribuite le funzioni previste dall'art. 38 del presente decreto deve aver maturato una esperienza professionale nelle tecnologie informatiche e delle telecomunicazioni almeno quinquennale.

2. Per ogni aggiornamento apportato al sistema di certificazione è previsto un apposito addestramento.

Art. 40. Manuale operativo

1. Il manuale operativo definisce le procedure applicate dal certificatore che rilascia certificati qualificati nello svolgimento della sua attività.

2. Il manuale operativo è depositato presso DigitPA e pubblicato a cura del certificatore in modo da essere consultabile per via telematica.

3. Il manuale contiene almeno le seguenti informazioni:
a) dati identificativi del certificatore;
b) dati identificativi della versione del manuale operativo;
c) responsabile del manuale operativo;
d) definizione degli obblighi del certificatore, del titolare e dei richiedenti le informazioni per la verifica delle firme;
e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f) indirizzo del sito web del certificatore ove sono pubblicate le tariffe;
g) modalità di identificazione e registrazione degli utenti;
h) modalità di generazione delle chiavi per la creazione e la verifica della firma;
i) modalità di emissione dei certificati;
l) modalità di inoltro delle richieste e della gestione di sospensione e revoca dei certificati;
m) modalità di sostituzione delle chiavi;
n) modalità di gestione del registro dei certificati;
o) modalità di accesso al registro dei certificati;
p) modalità per l'apposizione e la definizione del riferimento temporale;
q) modalità di protezione dei dati personali;
r) modalità operative per l'utilizzo del sistema di verifica delle firme di cui all'art. 14, comma 1 del presente decreto;
s) modalità operative per la generazione della firma elettronica qualificata e della firma digitale.

Art. 41. Riferimenti temporali opponibili ai terzi

1. I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del codice.

2. I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del codice.

3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo.

4. Costituiscono inoltre validazione temporale:
a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272;
b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del codice;
d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il decreto del Presidente della Repubblica 12 gennaio 2007, n. 18.

TITOLO III

CERTIFICATORI ACCREDITATI

Art. 42. Obblighi per i certificatori accreditati

1. Il certificatore accreditato genera un certificato per ciascuna delle chiavi di firma utilizzate dal DigitPA per la sottoscrizione dell'elenco pubblico dei certificatori, lo pubblica nel proprio registro dei certificati e lo rende accessibile per via telematica al fine di verificare la validità delle chiavi utilizzate dal DigitPA. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge.

2. Il certificatore accreditato garantisce l'interoperabilità del prodotto di verifica di cui all'art. 14 del presente decreto con i documenti informatici sottoscritti mediante firme elettroniche qualificate e digitali ad opera di DigitPA, nell'ambito delle attività di cui all'art. 31 del codice.

3. Il certificatore accreditato mantiene copia della lista, sottoscritta da DigitPA, dei certificati relativi alle chiavi di certificazione di cui all'art. 43, comma 1, lettera e) del presente decreto, che

rende accessibile per via telematica per la specifica finalità della verifica delle firme elettroniche qualificate e digitali.

4. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 29, comma 1 del codice, svolgono la propria attività in conformità con quanto previsto dai provvedimenti emanati da DigitPA ai sensi dell'art. 4, comma 2. Fino all'emanazione di tali provvedimenti continua ad applicarsi la deliberazione CNIPA, 21 maggio 2009, n. 45, recante regole per il riconoscimento e la verifica del documento informatico e successive modificazioni.

5. I certificatori accreditati, al fine di ottenere e mantenere il riconoscimento di cui all'art. 29, comma 1 del codice assicurano la valorizzazione dell'estensione qcStatements id-etsi-qcs-QcSSCD esclusivamente nei certificati qualificati la cui corrispondente chiave privata sia custodita nei dispositivi di cui all'articolo 12.

6. I sistemi di generazione e verifica delle firme elettroniche qualificate e delle firme digitali, forniti o indicati dal certificatore accreditato ai sensi degli articoli 11, comma 8 e 14, comma 1, non devono consentire a quest'ultimo di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione o verifica.

7. Al fine dell'attività di cui all'art. 31 del codice, il certificatore deve consegnare a DigitPA un esemplare dei dispositivi di firma elettronica qualificata e di firma digitale forniti ai titolari. Il periodo precedente non si applica in relazione ai dispositivi di firma HSM.

8. Al fine dell'attività di cui all'art. 31 del codice, il certificatore deve consegnare a DigitPA copia delle applicazioni di generazione e verifica delle firme elettroniche qualificate o delle firme digitali fornite ai titolari per uso personale.

9. Al fine del mantenimento dell'accreditamento di cui all'articolo 29 del codice, il certificatore è obbligato a partecipare alle sessioni di test di interoperabilità indicate da DigitPA.

10. I certificatori rendono disponibile a DigitPA un servizio che consenta, ai fini dell'art. 34, comma 4 del presente decreto, di conoscere se per un determinato codice fiscale sia stato emesso un certificato qualificato e, in caso affermativo, la sua scadenza. DigitPA, sentite le associazioni di categoria e il Garante per la protezione dei dati personali, indica in un proprio provvedimento le caratteristiche del servizio, le modalità e i vincoli per la sua fruizione.

Art. 43. Elenco pubblico dei certificatori accreditati

1. L'elenco pubblico dei certificatori accreditati tenuto da DigitPA ai sensi dell'art. 29, comma 6, del codice, e del D.Lgs 1 dicembre 2009, n. 177, contiene per ogni certificatore accreditato almeno le seguenti informazioni:
a) denominazione;
b) sede legale;
c) indirizzo della sede legale;
d) indirizzi internet ove il certificatore pubblica in lingua italiana e lingua inglese informazioni inerenti all'attività svolta.
e) lista dei certificati delle chiavi di certificazione;
f) indirizzo di posta elettronica;
g) data di accreditamento volontario;

h) eventuale data di cessazione;
i) eventuale certificatore sostitutivo.

2. L'elenco pubblico è sottoscritto e reso disponibile per via telematica da DigitPA al fine di verificare le firme elettroniche qualificate e digitali e diffondere i dati dei certificatori accreditati. Tali informazioni sono utilizzate, da chi le consulta, solo per le finalità consentite dalla legge. DigitPA stabilisce il formato dell'elenco pubblico attraverso propria deliberazione.

3. L'elenco pubblico è sottoscritto elettronicamente dal Presidente DigitPA o dai soggetti da lui designati.

4. DigitPA pubblica sul proprio sito istituzionale i manuali operativi di cui all'art. 40, sottoscritti ai sensi del comma 3.

5. Nella Gazzetta Ufficiale della Repubblica italiana è dato avviso:
a) dell'indicazione dei soggetti preposti alla sottoscrizione dell'elenco pubblico di cui al comma 3;
b) del valore dei codici identificativi del certificato relativo alle chiavi utilizzate per la sottoscrizione dell'elenco pubblico, generati attraverso gli algoritmi di cui all'art. 4 del presente decreto;
c) con almeno sessanta giorni di preavviso rispetto alla scadenza del certificato, della sostituzione delle chiavi utilizzate per la sottoscrizione dell'elenco pubblico;
d) della revoca dei certificati utilizzati per la sottoscrizione dell'elenco pubblico sopravvenuta per ragioni di sicurezza.

Art. 44. Rappresentazione del documento informatico

1. Il certificatore indica nel manuale operativo i formati del documento informatico e le modalità operative a cui il titolare deve attenersi per evitare le conseguenze previste dall'art. 4, comma 3.

Art. 45. Limitazioni d'uso

1. Il certificatore, su richiesta del titolare, del terzo interessato o di DigitPA, è tenuto a inserire nel certificato qualificato eventuali limitazioni d'uso.

2. La modalità di rappresentazione dei limiti d'uso e di valore di cui all'articolo 28, comma 3, del codice è definita da DigitPA con uno dei provvedimenti di cui all'art. 4, comma 2 del presente decreto.

3. Il certificatore è tenuto ad indicare, in lingua italiana e lingua inglese, la limitazione d'uso dei certificati utilizzati per la verifica delle firme di cui all'art. 35, comma 3 del codice.

Art. 46. Verifica delle marche temporali

1. I certificatori accreditati forniscono ovvero indicano almeno un sistema, conforme al successivo comma 2, che consenta di effettuare la verifica delle marche temporali.

2. DigitPA con i provvedimenti di cui all'art. 4, comma 2, del presente decreto stabilisce le regole di interoperabilità per la verifica della marca temporale, anche associata al documento informatico cui si riferisce.

TITOLO IV

REGOLE PER LA VALIDAZIONE TEMPORALE MEDIANTE MARCA TEMPORALE

Art. 47. Validazione temporale con marca temporale

1. Una evidenza informatica è sottoposta a validazione temporale mediante generazione e applicazione di una marca temporale alla relativa impronta.

2. Le marche temporali sono generate da un apposito sistema di validazione temporale, sottoposto ad opportune personalizzazioni atte a innalzarne il livello di sicurezza, in grado di:
a) garantire l'esattezza del riferimento temporale conformemente a quanto richiesto dal presente decreto;
b) generare la struttura dei dati temporali secondo quanto specificato negli articoli 48 e 51 del presente decreto;
c) sottoscrivere elettronicamente la struttura di dati di cui alla lettera b).

3. L'evidenza informatica da sottoporre a validazione temporale può essere costituita da un insieme di impronte.

Art. 48. Informazioni contenute nella marca temporale

1. Una marca temporale contiene almeno le seguenti informazioni:
a) identificativo dell'emittente;
b) numero di serie della marca temporale;
c) algoritmo di sottoscrizione della marca temporale;
d) certificato relativo alla chiave utilizzata per la verifica della marca temporale;
e) riferimento temporale della generazione della marca temporale;
f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
g) valore dell'impronta dell'evidenza informatica.

2. La marca temporale può inoltre contenere un codice identificativo dell'oggetto a cui appartiene l'impronta di cui al comma 1, lettera g).

Art. 49. Chiavi di marcatura temporale

1. Dal certificato relativo alla coppia di chiavi utilizzate per la validazione temporale deve essere possibile individuare il sistema di validazione temporale.

2. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite ed un nuovo certificato è emesso, in relazione alla robustezza delle chiavi crittografiche utilizzate, dopo non più di tre mesi di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il certificato corrispondente alla chiave precedentemente in uso. Detto periodo è indicato nel manuale operativo e, previa valutazione, ritenuto congruente alla presente disposizione da DigitPA.

3. Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale sono utilizzate chiavi di certificazione appositamente generate.

4. Le chiavi di certificazione e di marcatura temporale possono essere generate esclusivamente in presenza dei responsabili dei rispettivi servizi.

Art. 50. Gestione dei certificati e delle chiavi

1. Alle chiavi di certificazione utilizzate, ai sensi dell'art. 49, comma 3 del presente decreto, per sottoscrivere i certificati relativi a chiavi di marcatura temporale, si applica quanto previsto per le chiavi di certificazione utilizzate per sottoscrivere certificati relativi a chiavi di sottoscrizione.

2. I certificati relativi ad una coppia di chiavi di marcatura temporale, oltre ad essere conformi a quanto stabilito ai sensi dell'art. 4, comma 2, contengono l'identificativo del sistema di marcatura temporale che utilizza le chiavi.

Art. 51. Precisione dei sistemi di validazione temporale

1. Il riferimento temporale assegnato ad una marca temporale coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.

2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC).

Art. 52. Sicurezza dei sistemi di validazione temporale

1. Qualsiasi anomalia o tentativo di manomissione che possa modificare il funzionamento del sistema di validazione temporale in modo da renderlo incompatibile con i requisiti previsti dal presente decreto, ed in particolare con quello di cui all'art. 51, comma 1, è annotato sul giornale di controllo e causa il blocco del sistema medesimo.

2. Il blocco del sistema di validazione temporale può essere rimosso esclusivamente con l'intervento di personale espressamente autorizzato.

3. I sistemi operativi dei sistemi di elaborazione utilizzati nelle attività di validazione temporale devono essere stati oggetto di opportune personalizzazioni atte a innalzarne il livello di sicurezza (hardening).

4. Ai sensi dell'art. 31 del codice, DigitPA verifica l'idoneità delle personalizzazioni di cui al comma 3 e indica al certificatore eventuali azioni correttive.

Art. 53. Registrazione delle marche generate

1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.

2. La marca temporale è valida per il periodo di conservazione, stabilito o concordato con il certificatore, di cui al comma 1.

Art. 54. Richiesta di marca temporale

1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'invio della richiesta di marca temporale.

2. La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale.

3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'articolo 4, comma 2, del presente decreto.

4. La generazione delle marche temporali garantisce un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

TITOLO V

FIRMA ELETTRONICA AVANZATA

Art. 55
Disposizioni generali

1. La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.

2. I soggetti che erogano o realizzano soluzioni di firma elettronica avanzata si distinguono in soggetti che:
a) erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nel processo di dematerializzazione dei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti di cui alla lettera b);
b) realizzano soluzioni di firma elettronica avanzata per fornirle ai soggetti di cui alla lettera a), quale scopo dell'attività di impresa.

Art. 56
Caratteristiche delle soluzioni di firma elettronica avanzata

1. Le soluzioni di firma elettronica avanzata devono garantire:

a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
d) la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati.

2. La firma elettronica avanzata generata in violazione di quanto disposto da una o più disposizioni di cui alle lettere a), b), c), d), g) del comma precedente, non soddisfa i requisiti previsti dall'art.21, comma 2, del codice.

Art. 57
Obblighi per i soggetti che erogano per proprio conto soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a) devono:

a) identificare in modo certo l'utente, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
b) conservare per almeno venti anni la dichiarazione di cui al punto a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;
c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;
d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;
e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1, specificando le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto, pubblicandole anche sul proprio sito internet;
f) consentire l'uso della firma elettronica qualificata e della firma digitale, ove applicabile, in alternativa alla firma elettronica avanzata per i procedimenti per i quali è previsto l'uso della firma elettronica avanzata;
g) assicurare la disponibilità di un servizio di revoca relativo alla firma elettronica avanzata, ove applicabile, e un servizio di assistenza. Il presente comma non si applica alle soluzioni di cui all'art. 61 commi 1 e 3, per le quali si applicano le norme vigenti in materia;

2. Al fine di proteggere i firmatari e i terzi da eventuali danni cagionati da una non adeguata soluzione di firma elettronica avanzata, i soggetti di cui all'art. 55, comma 2, lettera a), devono poter rispondere di eventuali danni derivanti dall'attività svolta per almeno cinquecentomila euro. A tale scopo è anche possibile dotarsi di una copertura assicurativa rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali.

3. Le modalità scelte per ottemperare a quanto disposto al comma precedente devono essere rese note ai soggetti interessati, pubblicandole anche sul proprio sito internet.

4. Quanto stabilito al comma 2 del presente articolo non si applica alle persone giuridiche pubbliche che erogano soluzioni di firma elettronica avanzata per conto di pubbliche amministrazioni.

5. In ambito sanitario, limitatamente alla categoria di utenti rappresentata dai cittadini fruitori di prestazioni sanitarie, la dichiarazione di accettazione delle condizioni del servizio prevista al comma 1, lettera a) del presente articolo, può essere fornita oralmente dall'utente all'esercente la professione sanitaria il quale la raccoglie in un documento informatico che sottoscrive con firma elettronica qualificata o firma digitale.

Art. 58
Soggetti che realizzano per terzi soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera b) per offrire una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni a supporto di tale soluzione, alla norma ISO/IEC 27001 ottenuta tramite una terza parte indipendente autorizzata allo scopo secondo le norme vigenti in materia.

2. I soggetti di cui all'art. 55, comma 2, lettera b) per offrire soluzioni di firma elettronica avanzata alle pubbliche amministrazioni, ovvero le società che li controllano, devono avere la certificazione di conformità del proprio sistema di qualità alla norma ISO 9001 e successive modifiche o a norme equivalenti.

3. Quanto stabilito ai commi 1 e 2 del presente articolo non si applica alle persone giuridiche private possedute o controllate dalla pubblica amministrazione al fine di realizzare per le stesse soluzioni di firma elettronica avanzata.

4. Quanto stabilito ai commi 1 e 2 del presente articolo non si applica alle persone giuridiche pubbliche che rendono disponibili soluzioni di firma elettronica avanzata a pubbliche amministrazioni.

5. I soggetti di cui all'art. 55, comma 2, lettera b), al fine di dare evidenza del grado di conformità della soluzione di firma elettronica avanzata a quanto previsto dalle presenti regole tecniche, su base volontaria, possono far certificare la propria soluzione secondo la norma ISO/IEC 15408, livello EAL 1 o superiore, da una terza parte indipendente autorizzata allo scopo secondo le norme vigenti in materia.

Art. 59
Affidabilità delle soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a), al fine di dare evidenza del grado di conformità alla norma ISO/IEC 27001 del proprio sistema di gestione per la sicurezza delle informazioni a supporto della soluzione di firma elettronica avanzata proposta, possono, su base volontaria, richiederne la certificazione ad una terza parte indipendente autorizzata allo scopo secondo le norme vigenti in materia.

2. I soggetti di cui all'art. 55, comma 2, lettera a), al fine di dare evidenza del grado di conformità della soluzione di firma elettronica avanzata a quanto previsto dalle presenti regole tecniche, su base volontaria, possono far certificare la propria soluzione secondo la norma ISO/IEC 15408, livello EAL 1 o superiore da una terza parte indipendente autorizzata allo scopo secondo le norme vigenti in materia.

Art. 60
Limiti d'uso della firma elettronica avanzata

1. La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a).

Art. 61
Soluzioni di firma elettronica avanzata

1. L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del

Decreto 2 novembre 2005 recante “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata”, costituisce, nei confronti della pubblica amministrazione, firma elettronica avanzata del messaggio spedito ai sensi delle presenti regole tecniche.

2. La firma elettronica avanzata di cui al comma 1 soddisfa quanto prescritto all’art. 56, comma 1. Alla stessa, fermo restando quanto prescritto dalle norme in materia di posta elettronica certificata, non si applica quanto previsto dalla lettera a) alla lettera e) del comma 1 dell’art. 57, dai commi 1 e 2 dell’art. 58 e dall’art.60.

3. La Carta d’Identità Elettronica, la Carta Nazionale dei Servizi e gli altri strumenti ad esse conformi, sono utilizzabili dalle pubbliche amministrazioni per realizzare sistemi di firma elettronica avanzata.

4. I formati della firma di cui al comma 3 sono gli stessi previsti ai sensi dell’art. 4, comma 2.

5. La firma elettronica avanzata di cui al comma 3 soddisfa quanto prescritto all’art. 56, comma 1. Alla stessa, fermo restando quanto prescritto dalle norme in materia di Carta d’Identità Elettronica e di Carta Nazionale dei Servizi, non si applica quanto previsto dalla lettera a) alla lettera e) del comma 1 dell’art. 57, dai commi 1 e 2 dell’art. 58 e dall’art. 60.

6. Le applicazioni di verifica della firma generata ai sensi del comma 3 devono accertare che il certificato digitale utilizzato nel processo di verifica sia afferente ad una Carta d’Identità Elettronica, ad una Carta Nazionale dei Servizi o ad altri strumenti ad esse conformi.

7. Qualunque altra soluzione conforme alle regole tecniche del presente Titolo costituisce soluzione di firma elettronica avanzata.

8. Fermo restando quanto disposto dall’art. 55, comma 1, al fine di favorire la realizzazione di soluzioni di firma elettronica avanzata, DigitPa pubblica delle linee guida attenendosi alle quali sia possibile realizzare soluzioni di firma elettronica avanzata conformi alle presenti regole tecniche.

TITOLO VI

DISPOSIZIONI FINALI

Art. 62. Valore delle firme elettroniche qualificate e digitali nel tempo

1. Le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Art. 63. Disposizioni finali e transitorie

1. Dall'entrata in vigore del presente decreto è abrogato il decreto del Presidente del Consiglio dei Ministri 30 marzo 2009, recante “Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.” pubblicato nella Gazzetta Ufficiale 6 giugno 2009, n. 129.

2. I certificatori accreditati ai sensi dell’art. 29 del codice, aggiornano la documentazione prevista per lo svolgimento di tale attività entro centoventi giorni dall’entrata in vigore del presente decreto.

Il presente decreto sarà inviato ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.