diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

D.P.C.M. 6 novembre 2015 - Firma digitale

Autore: Redazione

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 6 novembre 2015

Disciplina della firma digitale dei documenti classificati. (Decreto n. 4/2015).

(GU n.284 del 5-12-2015 - Suppl. Ordinario n. 65)

Capo I
PRINCIPI GENERALI

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI
Vista la legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto";
Visto il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
Viste le disposizioni in materia di protezione e tutela delle informazioni classificate;
Visto il decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445, recante "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa";
Visto il decreto legislativo del 7 marzo 2005, n. 82, e successive modificazioni, recante "Codice dell'amministrazione digitale" (CAD);
Visto il decreto del Presidente del Consiglio dei ministri dell'11 aprile 2002 recante "Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato";
Visto il decreto del Presidente del Consiglio dei ministri del 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71; Visto il decreto del Presidente del Consiglio dei ministri 12 giugno 2009, n. 7, recante "Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonche' dei modi di accesso nei luoghi militari o

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

definiti di interesse per la sicurezza della Repubblica";
Visto il decreto del Presidente del Consiglio dei ministri 22 luglio 2011, n. 4, recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate";
Visto l'art. 7, comma 1, lettera g), del suddetto decreto del Presidente del Consiglio dei ministri, che attribuisce la funzione di autorita' di certificazione all'Ufficio centrale per la segretezza, nonche' l'art. 75 concernente l'emanazione di nuove disposizioni tecniche al fine di adeguare la disciplina applicativa in materia di tutela amministrativa del segreto di Stato e delle informazioni classificate ai principi del suddetto decreto;
Vista la deliberazione del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) n. 45/2009 del 21 maggio 2009 concernente le "Regole per il riconoscimento e la verifica del documento informatico" cosi' come modificata dalla "Determinazione Commissariale 28 luglio 2010"; Visto l'art. 2, comma 6, del decreto legislativo del 7 marzo 2005, n. 82, secondo cui le disposizioni del CAD non si applicano limitatamente all'esercizio delle attivita' e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale;
Considerato che le classifiche di segretezza sono attribuite per limitare la circolazione di informazioni la cui eventuale diffusione non autorizzata sia idonea ad arrecare un pregiudizio agli interessi fondamentali della Repubblica;
Visto il decreto del Presidente del Consiglio dei ministri 22 febbraio 2013 recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 28, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71";
Visto il decreto del Presidente del Consiglio dei ministri 13 novembre 2014, recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonche' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al citato decreto legislativo n. 82 del 2005"; Visto l'art. 4, comma 3, lettera l), della legge 3 agosto 2007, n. 124, cosi' come modificato con decreto-legge 1° luglio 2009, n. 78, convertito con legge 3 agosto 2009 n. 102, il quale prevede che il Dipartimento delle informazioni per la sicurezza assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei ministri con apposito regolamento adottato ai sensi dell'art. 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresi' sulla loro corretta applicazione;
Visto il decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali"; Visto l'art. 43 della legge 3 agosto 2007, n. 124, che consente l'adozione di regolamenti in

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

deroga alle disposizioni dell'art. 17 della legge 23 agosto 1998, n. 400, e successive modificazioni e, dunque, in assenza del parere del Consiglio di Stato; Ravvisata la necessita' di regolamentare l'impiego delle procedure di firma digitale per i documenti informatici classificati;
Acquisito il parere tecnico dell'Agenzia per l'Italia digitale di cui alla legge 7 agosto 2012, n. 134;
Consultato il Garante per la protezione dei dati personali; Acquisito il parere del Comitato parlamentare per la sicurezza della Repubblica; Sentito il Comitato interministeriale per la sicurezza della Repubblica;

A d o t t a

il seguente regolamento:

Art. 1
Definizioni

1. Ai fini del presente regolamento sono definiti:
a) "Autorita' nazionale per la sicurezza (ANS)", il Presidente del Consiglio dei ministri nell'esercizio delle funzioni di tutela amministrativa del segreto di Stato e delle informazioni classificate;
b) "Autorita' di certificazione (CA)", l'ente nazionale che effettua la certificazione, rilascia il certificato qualificato, pubblica e aggiorna gli elenchi dei certificati sospesi e revocati. La CA si avvale di altre entita' chiamate Autorita' Locali di Registrazione (LRA), per garantire che l'utente richiedente un certificato sia esattamente quello riportato nel certificato stesso;
c) "Autorita' di registrazione locale (LRA)", l'ente responsabile della verifica in modo affidabile delle identita' dei titolari istituita presso tutti i soggetti, pubblici e privati, in possesso delle previste abilitazioni di sicurezza;
d) "CAD", il decreto legislativo del 7 marzo 2005 n. 82 e successive modificazioni, recante "Codice dell'amministrazione digitale";
e) "certificate revocation list (CRL)", la lista conseguente alle operazioni con cui la CA annulla la validita' di un certificato da un dato momento, non retroattivo, in poi. Tale elenco e' firmato digitalmente, aggiornato e pubblicato dalla CA; f) "certificate suspension list (CSL)", la lista conseguente alle operazioni con cui la CA sospende temporaneamente la validita' di un certificato da un dato momento, non retroattivo, in poi. Tale elenco e' firmato digitalmente, aggiornato e pubblicato dalla CA;
g) "certificato elettronico", attestato elettronico che collega all'identita' del titolare i dati utilizzati per verificare le firme elettroniche;

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

h) "certificato qualificato", un certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
i) "certificazione", il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza univoca tra chiave pubblica e soggetto titolare, si identifica quest'ultimo, si attesta il periodo di validita' della predetta chiave e il termine di scadenza del relativo certificato;
l) "chiavi asimmetriche", la coppia di chiavi crittografiche, una pubblica e una privata, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione e di generazione della firma;
m) "chiave privata", elemento della coppia di chiavi asimmetriche,utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
n) "chiave pubblica", l'elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;
o) "codici personali", codici alfanumerici o caratteristiche biometriche in possesso del titolare e necessarie per attivare le procedure di firma digitale;
p) "copia per immagine su supporto informatico di documento analogico", il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui e' tratto;
q) "copia informatica di documento informatico", il documento informatico avente contenuto identico a quello del documento da cui e' tratto su supporto informatico con diversa sequenza di valori binari;
r) "crittografia", metodo di codifica e protezione dei dati, definito per impedire ad estranei di accedere alle informazioni senza essere dotati di autorizzazione;
s) "Dipartimento delle informazioni per la sicurezza" (DIS), l'organismo di cui all'art. 4 della legge;
t) "dispositivo di firma", insieme dei dispositivi hardware e software che consentono di sottoscrivere con firma digitale i documenti informatici;
u) "Direttiva", il provvedimento in materia di documenti informatici classificati adottato ai sensi dell'art. 75 del decreto del Presidente del Consiglio dei ministri 22 luglio 2011, n. 4;
v) "Disciplinare Tecnico" documento che contiene le regole tecniche che disciplinano la sottoscrizione digitale del documento informatico;
z) "documento", rappresentazione in formato analogico o informatico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica;
aa) "documento analogico", il documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (ad esempio i documenti cartacei), le immagini su film (microfilm), le

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

magnetizzazioni su nastro (cassette e nastri magnetici audio);
bb) "documento informatico", la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, formata e gestita su un sistema per l'elaborazione automatica dei dati;
cc) "documento informatico classificato", un documento informatico, formato e gestito su un sistema per l'elaborazione automatica dei dati omologato dall'UCSe, a cui e' stata apposta una classifica di segretezza in conformita' a quanto stabilito dalle vigenti norme in materia di protezione e tutela delle informazioni classificate;
dd) "duplicato informatico", il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;
ee) "esibizione", l'operazione che consente di visualizzare un documento conservato e di ottenerne, eventualmente, copia; ff) "firma digitale", un particolare tipo di firma elettronica:
1) basata su un certificato qualificato;
2) basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrita' di un documento informatico o di un insieme di documenti informatici, nonche' eventualmente il momento dell'apposizione della firma medesima;
3) realizzata mediante un dispositivo sicuro per la creazione della firma;
gg) "firma elettronica", l'insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
hh) "firme multiple", firme digitali apposte da diversi sottoscrittori allo stesso documento informatico;
ii) "integrita'", caratteristica dei dati che si riferisce al loro livello di alterazione o danno;
ll) "formato di un file", un modo particolare col quale le informazioni sono codificate per la memorizzazione su un dispositivo di memoria;
mm) "legge", la legge 3 agosto 2007, n. 124; nn) "Manuale Operativo", documento che contiene le regole tecniche che disciplinano l'attivita' della CA;
oo) "Organo nazionale di sicurezza (ONS)", il Direttore generale del Dipartimento delle informazioni per la sicurezza di cui all'art. 4 della legge nell'esercizio delle funzioni di direzione e coordinamento dell'Organizzazione nazionale di sicurezza, di cui all'art. 5 del decreto del Presidente del Consiglio dei ministri 22 luglio 2011, n. 4, e secondo le direttive impartite dall'ANS;
pp) "public key infrastructure (PKI)", l'insieme di tecnologie, politiche, processi e persone utilizzate per gestire (generare, distribuire, archiviare, utilizzare, revocare) chiavi di crittografia e certificati digitali in sistemi di crittografia a chiave pubblica;

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

qq) "registrazione di protocollo", l'operazione con cui si attribuisce ai documenti prodotti o ricevuti da un soggetto una numerazione univoca secondo un ordine cronologico progressivo e si annotano informazioni descrittive idonee all'identificazione di ciascun documento;
rr) "revoca di un certificato", l'operazione con cui la CA annulla la validita' del certificato da un dato momento, non retroattivo, in poi;
ss) "riferimento temporale", l'informazione, contenente la data, che viene associata ad uno o piu' documenti informatici;
tt) "riservatezza", garanzia che le informazioni vengano utilizzate unicamente dalle persone o dalle organizzazioni autorizzate;
uu) "segnatura di protocollo", l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso; consente di individuare ciascun documento in modo univoco ed e' effettuata congiuntamente all'operazione di registrazione di protocollo;
vv) "sospensione del certificato", l'operazione con cui la CA sospende la validita' del certificato per un determinato periodo di tempo;
zz) "titolare", persona fisica titolare di un certificato, ossia il legittimo possessore e utilizzatore della chiave privata associata alla chiave pubblica che compare nel certificato;
aaa) "Ufficio centrale per la segretezza" (UCSe), l'Ufficio istituito dall'art. 9 della legge;
bbb) "validazione temporale", il risultato della procedura informatica, con cui si attribuisce, ad uno o piu' documenti informatici, un riferimento temporale opponibile ai terzi;
ccc) "validita' del certificato", l'efficacia e opponibilita' al titolare della chiave pubblica, dei dati contenuti nel certificato stesso.

Art. 2
Oggetto e ambito di applicazione

1. Le disposizioni del presente regolamento si applicano a tutti i soggetti, pubblici e privati, in possesso delle previste abilitazioni di sicurezza per il trattamento di informazioni classificate e disciplinano le modalita' di generazione, apposizione e verifica delle firme digitali nonche' la validazione temporale di documenti informatici classificati.
2. Quanto previsto al precedente comma 1 si applica anche ai documenti informatici non classificati, quando formati, sottoscritti e gestiti su sistemi omologati in conformita' a quanto previsto dalla normativa

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

vigente in materia di tutela delle informazioni classificate.

Capo II
DOCUMENTO INFORMATICO
CLASSIFICATO E FIRMA DIGITALE

Art. 3
Documenti informatici classificati

1. Ai documenti informatici di cui all'art. 2, si applica l'art. 20, comma 1, del CAD, in relazione alla validita' e rilevanza agli effetti di legge, se formati secondo quanto previsto dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.
2. I documenti informatici di cui all'art. 2, comma 1, sottoscritti con firma digitale, devono essere corredati di:
a) riferimento temporale opponibile a terzi secondo quanto previsto dall'art. 13;
b) classifica di segretezza, qualifica di sicurezza e altre informazioni, secondo quanto previsto dalle disposizioni in materia di protezione e tutela delle informazioni classificate.
3. I documenti informatici di cui all'art. 2, comma 2, sottoscritti con firma digitale, devono essere corredati di riferimento temporale opponibile a terzi secondo quanto previsto dall'art. 13.
4. Per la sottoscrizione di documenti informatici di cui all'art. 2, aventi rilevanza esclusivamente interna, ciascun soggetto, pubblico e privato, puo' adottare nella propria autonomia specifiche modalita' tecniche, organizzative e procedurali, nel rispetto di quanto previsto dalle norme in materia di protezione e tutela delle informazioni classificate e di quanto definito dal Disciplinare Tecnico di cui all'art. 33.
5. Ai documenti informatici di cui all'art. 2 non si applica il comma 1 se contengono macroistruzioni o codici eseguibili, tali da attivare funzionalita' che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.
6. L'apposizione di una firma digitale basata su un certificato qualificato revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione delle liste di sospensione e revoca di cui all'art. 22.
7. Ai documenti informatici di cui all'art. 2 si applica quanto previsto dall'art. 21, comma 2-bis, del CAD, in relazione alle scritture private ed al requisito della forma scritta, se formati secondo quanto stabilito dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.
8. Ai documenti informatici di cui al comma 4, ove sottoscritti con modalita' diverse dalla firma digitale, si applica quanto previsto dall'art. 20, comma 1-bis, del CAD, in relazione al requisito della forma scritta ed

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

al valore probatorio.
9. Ai documenti informatici di cui all'art. 2 si applica l'art. 21, comma 2, del CAD, se formati secondo quanto stabilito dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.
10. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Art. 4
Copie per immagine su supporto informatico di documenti analogici

1. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico o, comunque, non informatico, sono prodotte mediante processi e strumenti, secondo le modalita' stabilite dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33 che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui sono tratte.
2. Alle copie per immagine di cui al comma 1 si applica l'art. 22, commi 1 e 2, del CAD, in relazione all'efficacia ai sensi degli articoli 2714 e 2715 del codice civile, alla loro esibizione e produzione, nonche' all'efficacia probatoria, se la loro conformita' agli originali da cui sono estratte e' attestata da un pubblico ufficiale a cio' autorizzato, con dichiarazione allegata al documento informatico ed asseverata secondo le modalita' stabilite dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.

Art. 5
Copie analogiche di documenti informatici

1. Alle copie su supporto analogico o, comunque, non informatico di documenti informatici di cui all'art. 2, si applica l'art. 23, comma 1, del CAD, se la loro conformita' all'originale da cui sono tratte e' attestata da un pubblico ufficiale a cio' autorizzato, secondo le modalita' stabilite dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.

Art. 6
Copie informatiche di documenti informatici e duplicati informatici

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

1. A condizione che la conformita' all'originale sia attestata da un pubblico ufficiale a cio' autorizzato ed asseverata secondo le modalita' stabilite dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33, l'art. 23-bis, comma 2, del CAD si applica:
a) alle copie informatiche di documenti informatici di cui all'art. 2, se prodotte con un processo che ne assicuri la distinguibilita' rispetto all'originale o ad altra copia da cui sono tratte, secondo quanto previsto dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33;
b) agli estratti informatici di documenti informatici di cui all'art. 2, prodotti secondo quanto previsto dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33.
2. I duplicati informatici di documenti informatici di cui all'art. 2 sono prodotti mediante processi e strumenti, secondo le modalita' stabilite dalla Direttiva e dal Disciplinare Tecnico di cui all'art. 33, che assicurino che i documenti informatici ottenuti contengano la stessa sequenza di bit dei documenti informatici di origine.

Art. 7
Firma digitale

1. La firma digitale garantisce l'identificabilita' dell'autore, l'integrita' e l'immodificabilita' del documento.
2. La firma digitale dei documenti informatici di cui all'art. 2 deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui e' apposta o associata.
3. Per la generazione della firma digitale di documenti informatici di cui all'art. 2, deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validita' ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare la validita' del certificato stesso, nonche' gli elementi identificativi del titolare e della CA e gli eventuali limiti d'uso.
5. Le modalita' di apposizione della firma digitale ai documenti informatici di cui all'art. 2 sono definite nel Disciplinare Tecnico di cui all'art. 33.

Art. 8
Caratteristiche generali delle chiavi per la generazione e la verifica della firma

1. Ai fini del presente decreto, le chiavi di generazione e verifica della firma si distinguono secondo le

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

seguenti tipologie:
a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti informatici;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte o associate ai certificati relativi alle chiavi di sottoscrizione e alle informazioni sullo stato di validita' del certificato.
2. Non e' consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, dal comma 1, salvo che, con riferimento esclusivo alle chiavi di cui al medesimo comma 1, lettera b), la CA non ne autorizzi l'utilizzo per altri scopi.
3. La CA puo' individuare ulteriori tipologie di coppie di chiavi rispetto a quelle indicate nel comma 1, determinandone l'ambito d'impiego e disciplinandone l'utilizzo nel Disciplinare Tecnico di cui all'art. 33.
4. Se il soggetto appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso.
5. Se la procedura automatica di cui al comma 3 fa uso di un insieme di dispositivi sicuri per la generazione delle firme del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

Art. 9
Modalita' di generazione delle chiavi

1. Le chiavi di certificazione sono generate in presenza del responsabile del servizio di certificazione di cui all'art. 28, comma 1, lettera b).
2. Le chiavi di sottoscrizione sono generate dalla CA secondo le modalita' indicate nel Manuale Operativo di cui all'art. 32.
3. La generazione delle chiavi di sottoscrizione avviene all'interno di un dispositivo sicuro per la generazione delle firme approvato dall'UCSe e che presenti le caratteristiche di cui all'art. 11 del presente regolamento.

Art. 10
Conservazione delle chiavi e dei dati per la generazione della firma

1. E' vietata la duplicazione della chiave privata e la duplicazione dei dispositivi che la contengono.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

2. E' vietata l'esportazione, dal dispositivo sicuro di firma, della chiave privata relativa alle chiavi di sottoscrizione.
3. E' consentito che le chiavi di certificazione vengano esportate, purche' cio' avvenga con modalita' tali da non ridurre il livello di sicurezza e di riservatezza delle chiavi stesse.
4. Con modalita' descritte nel Disciplinare Tecnico e' possibile eseguire il back up e restore dei dati contenuti nel cryptoprocessore per le chiavi digitali denominato Hardware Security Module.
5. Il titolare della coppia di chiavi:
a) assicura la custodia del dispositivo di firma e l'adozione di tutte le misure organizzative e tecniche idonee in ottemperanza a quanto definito nel Manuale Operativo di cui all'art. 32;
b) conserva i codici personali di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
c) richiede immediatamente, secondo quanto indicato nel Manuale Operativo di cui all'art. 32, la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso, o qualora abbia il ragionevole dubbio che essi siano stati usati abusivamente da persone non autorizzate.

Art. 11
Dispositivi sicuri e procedure per la generazione della firma

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I documenti informatici di cui all'art. 2 devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguita', e si deve richiedere conferma della volonta' di generare la firma secondo quanto previsto nel Disciplinare Tecnico di cui all'art. 33.
3. Il comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica e' valida se apposta previo consenso del titolare all'adozione della procedura medesima. Il titolare che appone la sua firma mediante una procedura automatica deve utilizzare un certificato diverso da tutti gli altri in suo possesso.
4. La generazione della firma avviene all'interno di un dispositivo sicuro per la generazione delle firme

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

ovvero su un sistema informatico che realizza un dispositivo sicuro per la generazione delle firme secondo le modalita' stabilite dal Disciplinare Tecnico di cui all'art. 33, cosi' che non sia possibile l'intercettazione della chiave privata utilizzata.
5. Il dispositivo sicuro per la generazione delle firme deve poter essere attivato esclusivamente dal titolare mediante codici personali prima di procedere alla generazione della firma.
6. La personalizzazione del dispositivo sicuro di firma garantisce:
a) l'acquisizione da parte della CA dei dati identificativi del dispositivo sicuro utilizzato e della loro associazione al titolare;
b) la registrazione nel dispositivo sicuro del certificato relativo alle chiavi di sottoscrizione del titolare.
7. Nel dispositivo sicuro di firma e' ammessa la memorizzazione di altri certificati oltre quello di firma digitale e altri oggetti atti ad assicurare ulteriori funzionalita' di sicurezza, secondo le modalita' riportate nel Disciplinare Tecnico di cui all'art. 33.
8. La personalizzazione del dispositivo sicuro per la generazione delle firme puo' prevedere, per l'utilizzo nelle procedure di firma, la registrazione nel medesimo dispositivo del certificato elettronico relativo alla chiave pubblica della CA, la cui corrispondente privata e' stata utilizzata per sottoscrivere il certificato relativo alle chiavi di sottoscrizione del titolare.
9. La personalizzazione del dispositivo sicuro per la generazione delle firme e' registrata nel giornale di controllo di cui all'art. 26.
10. La CA di cui all'art. 15, avvalendosi delle LRA di cui all'art. 16, adotta, nel processo di personalizzazione del dispositivo sicuro per la generazione delle firme, procedure atte ad identificare il titolare di un dispositivo sicuro per la generazione delle firme e dei certificati in esso contenuti.
11. Le modalita' di personalizzazione del dispositivo sicuro per la generazione delle firme sono indicate nel Manuale Operativo di cui all'art. 32.
12. La procedura di firma deve generare, come risultato, un file il cui formato rientri tra quelli elencati nel Disciplinare Tecnico di cui all'art. 33.
13. Le modalita' per l'apposizione di firme multiple sono indicate nel Disciplinare Tecnico di cui all'art. 33.

Art. 12
Verifica delle firme digitali

1. I sistemi di verifica delle firme digitali devono essere conformi a quanto indicato nel Disciplinare Tecnico di cui all'art. 33.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

2. L'UCSe accerta la conformita' dei sistemi di verifica di cui al comma 1.

Art. 13
Riferimenti temporali opponibili ai terzi

1. Costituisce validazione temporale opponibile ai terzi il riferimento temporale contenuto nella segnatura di protocollo informatico.
2. Eventuali ed ulteriori modalita' per l'apposizione di un riferimento temporale opponibile ai terzi saranno indicate nel Disciplinare Tecnico di cui all'art. 33.
3. I riferimenti temporali apposti sul giornale di controllo, secondo quanto indicato nel Manuale Operativo di cui all'art. 32, sono opponibili ai terzi.

Art. 14
Valore della firma digitale nel tempo

1. La firma digitale apposta ad un documento informatico di cui all'art. 2, ancorche' sia scaduto, revocato o sospeso il connesso certificato qualificato relativo alle chiavi di sottoscrizione, e' valida se alla stessa e' associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma digitale in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.

Capo III
INFRASTRUTTURA A CHIAVE PUBBLICA
(PUBLIC KEY INFRASTRUCTURE)

Art. 15
Autorita' di certificazione

1. Presso l'UCSe e' istituita la CA, quale certificatore nazionale per i servizi di certificazione relativi alla firma digitale di documenti informatici di cui all'art. 2.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

2. La CA, di cui al comma 1:
a) rilascia certificati qualificati sulla base delle richieste autenticate dalle LRA di cui all'art. 16, secondo le modalita' riportate nel Manuale Operativo di cui all'art. 32;
b) revoca e sospende i certificati in accordo a quanto disposto dall'art. 22;
c) aggiorna e distribuisce le liste di revoca/sospensione dei certificati secondo le modalita' descritte nel Manuale Operativo di cui all'art. 32.

Art. 16
Autorita' locali di registrazione

1. Presso gli enti e le organizzazioni che intendono avvalersi delle procedure di sottoscrizione digitale dei documenti informatici di cui all'art. 2 viene istituita, nell'ambito delle rispettive organizzazioni di sicurezza, una LRA.
2. La LRA e' accreditata da parte della CA secondo le modalita' e le procedure operative descritte nel Manuale Operativo di cui all'art. 32.
3. La LRA procede al riconoscimento fisico delle persone, raccoglie i dati di interesse al fine di stabilirne le generalita' ed il possesso delle abilitazioni di sicurezza ed invia l'insieme delle informazioni necessarie al rilascio del Certificato alla CA, secondo quanto indicato nel Manuale Operativo di cui all'art. 32.
4. La LRA deve comunicare tempestivamente alla CA le variazioni dei dati relativi al personale gestito ai fini dell'eventuale aggiornamento delle liste di dei certificati revocati e sospesi.
5. La LRA nell'ambito della propria organizzazione: a) gestisce le richieste di certificazione;
b) gestisce le richieste di revoca e sospensione dei certificati; c) distribuisce i dispositivi sicuri di firma che contengono i certificati qualificati generati dalla CA ai titolari accreditati unitamente alle credenziali.
6. La LRA e' responsabile, per dolo o colpa grave, del danno cagionato a chi abbia fatto ragionevole affidamento sulla corretta procedura di riconoscimento delle persone, della raccolta dell'aggiornamento dei dati e del possesso delle necessarie autorizzazioni.
7. La LRA e' responsabile, per dolo o colpa grave, nei confronti di terzi dei danni provocati per effetto della mancata o non tempestiva comunicazione degli aggiornamenti relativi alla perdita dei requisiti di firma.

Art. 17

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Comunicazione tra CA e LRA

1. Le comunicazioni tra CA ed LRA avvengono secondo le modalita' indicate nel Manuale Operativo di cui all'art. 32.

Art. 18
Generazione delle chiavi di certificazione

1. La generazione delle chiavi di certificazione da parte della CA avviene in modo conforme a quanto indicato nel Disciplinare Tecnico di cui all'art. 33.

Art. 19
Certificati qualificati relativi alle chiavi di sottoscrizione

1. Per i certificati qualificati si fa riferimento a quanto previsto dal regolamento (UE) n. 910/2014.
2. L'emissione di certificati qualificati relativi alle chiavi di sottoscrizione avviene a seguito di una richiesta della LRA che ha l'obbligo di:
a) accertare l'autenticita' della richiesta secondo quanto previsto dall' art. 16 comma 3;
b) assicurare la consegna al legittimo titolare.
3. Il termine del periodo di validita' del certificato qualificato relativo alle chiavi di sottoscrizione e' anteriore al termine del periodo di validita' del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticita'.
4. L'emissione dei certificati qualificati e' registrata nel giornale di controllo di cui all'art. 26 specificando il riferimento temporale relativo alla registrazione.
5. I certificati qualificati relativi alle chiavi di sottoscrizione devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato e' un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) denominazione e nazionalita' della CA;
d) nome, cognome o uno pseudonimo chiaramente identificato come tale del titolare del certificato;
e) dati per la verifica della firma, cioe' i dati peculiari, come codici o chiavi crittografiche pubbliche,

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

utilizzati per verificare la firma elettronica corrispondenti ai dati per la generazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validita' del certificato;
g) firma digitale della CA, realizzata in conformita' alle regole tecniche definite nel Disciplinare Tecnico di cui all'art. 33 ed idonea a garantire l'integrita' e la veridicita' di tutte le informazioni contenute nel certificato medesimo.
6. Il certificato qualificato puo' inoltre contenere:
a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonche' poteri di rappresentanza;
b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarita' delle qualifiche e dai poteri di rappresentanza di cui alla precedente lettera a) ai sensi dell'art. 20, comma 3;
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato puo' essere usato, ove applicabili.
7. Il titolare, ovvero il terzo dal quale derivano i poteri del titolare, comunicano tempestivamente alla CA per il tramite della LRA il modificarsi o venir meno delle circostanze oggetto delle informazioni personali di cui ai precedenti commi 4 e 5. 8. Le informazioni personali contenute nel certificato sono utilizzabili unicamente per identificare il titolare della firma digitale e per verificare la firma del documento informatico.
9. La CA determina il periodo di validita' del certificato qualificato relativo alle chiavi di sottoscrizione in funzione della robustezza crittografica delle chiavi impiegate.
10. La CA determina, riportandolo nel Disciplinare Tecnico di cui all'art. 33, il periodo massimo di validita' del certificato relativo alle chiavi di sottoscrizione in funzione degli algoritmi e delle caratteristiche delle chiavi impiegate.
11. Le modalita' di formazione del certificato qualificato sono riportate nel Disciplinare Tecnico di cui all'art. 33.
12. La CA e la LRA conservano tutte le informazioni relative al certificato qualificato, per un periodo pari a venti anni, dal momento della sua emissione.

Art. 20
Responsabilita' della CA

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

1. La CA che rilascia un certificato qualificato e' responsabile, ove sia provato che abbia agito per dolo o colpa grave, del danno cagionato a chi abbia fatto ragionevole affidamento:
a) sull'esattezza e sulla completezza delle informazioni necessarie per la verifica della firma in esso contenute alla data del rilascio e per il rispetto dei requisiti fissati per i certificati qualificati;
b) sulla garanzia della corrispondenza, al momento del rilascio del certificato, tra i dati comunicati dalla LRA per la creazione della firma ed i dati per la verifica della firma riportati o identificati nel certificato.
2. La CA che rilascia un certificato qualificato e' responsabile, ove sia provato che abbia agito per dolo o colpa grave, nei confronti dei terzi che facciano affidamento sul certificato qualificato da essa rilasciato, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o sospensione del certificato, secondo quanto previsto dal Disciplinare Tecnico di cui all'art. 33.
3. Il certificato qualificato puo' contenere limiti d'uso ovvero un valore limite per i negozi per i quali puo' essere usato il certificato stesso, purche' i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dal Disciplinare Tecnico di cui all'art. 33. La CA non e' responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Art. 21
Codice di emergenza

1. Per ciascun certificato qualificato emesso, la CA fornisce al titolare, per il tramite della LRA, almeno un codice riservato, da utilizzare per richiedere la sospensione del certificato relativo alle chiavi di sottoscrizione nei casi di emergenza indicati nel Manuale Operativo di cui all'art. 32 e comunicati al titolare.
2. La richiesta di cui al comma 1 e' successivamente confermata utilizzando una delle modalita' descritte nel Manuale Operativo di cui all'art. 32.

Art. 22
Revoca e sospensione di certificati qualificati relativi alle chiavi di sottoscrizione

1. La CA revoca o sospende il certificato, di iniziativa o su richiesta della LRA, nei seguenti casi:
a) il soggetto ovvero la sua organizzazione di appartenenza non sono piu' abilitati a trattare dati

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

classificati;
b) a seguito di richiesta, per il tramite della LRA, del titolare o del terzo dal quale derivano i poteri del titolare ovvero dalla LRA stessa, secondo le modalita' previste nel Manuale Operativo di cui all'art. 32;
c) in presenza di abusi o falsificazioni;
d) per la compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme.
2. La CA e la LRA conservano le richieste di revoca e sospensione per 20 anni.
3. La CA effettua la sospensione e/o la revoca del certificato mediante l'inserimento del suo codice identificativo nella lista dei certificati sospesi o revocati (CSL/CRL). 4. La CA comunica, per il tramite della LRA, al titolare e all'eventuale terzo interessato, l'avvenuta sospensione e/o la revoca specificando la data e l'ora a partire dalla quale il certificato risulta sospeso o revocato.
5. La CA indica, nel Manuale Operativo di cui all'art. 32, 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. 6. In caso di revoca di un certificato sospeso, la data della stessa decorre dalla data di inizio del periodo di sospensione.
7. La sospensione e la cessazione della stessa sono annotate nel giornale di controllo di cui all'art. 26 con l'indicazione della data e dell'ora di esecuzione dell'operazione.
8. La CA comunica, per il tramite della LRA, al titolare e all'eventuale terzo interessato la cessazione dello stato di sospensione del certificato, che sara' considerato come mai sospeso, specificando la data e l'ora a partire dalla quale il certificato ha cambiato stato.
9. Tutte le comunicazioni relative alle operazioni di sospensione e/o revoca dei certificati qualificati avvengono secondo le modalita' indicate nel Manuale Operativo di cui all'art. 32.

Art. 23
Sostituzione delle chiavi di certificazione e dei certificati qualificati relativi alle chiavi di sottoscrizione

1. La procedura di sostituzione delle chiavi, generate dalla CA in conformita' all'art. 18, deve assicurare che non siano stati emessi certificati qualificati con data di scadenza posteriore al periodo di validita' del certificato relativo alla coppia sostituita.
2. La sostituzione dei certificati qualificati, generati in conformita' all'art. 19, avviene in conformita' con quanto indicato nel Manuale Operativo di cui all'art. 32.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Art. 24
Revoca dei certificati relativi a chiavi di certificazione

1. La CA procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione in caso di compromissione della chiave privata.
2. Nel caso di cui al comma 1, vengono revocati d'ufficio tutti i certificati sottoscritti con detta chiave secondo quanto indicato nel Manuale Operativo di cui all'art. 32.

Art. 25
Piano per la sicurezza

1. La CA definisce un piano per la sicurezza nel quale sono contenuti almeno i seguenti elementi:
a) struttura generale, modalita' operativa e struttura logistica;
b) descrizione dell'infrastruttura di sicurezza per ciascun immobile rilevante ai fini della sicurezza;
c) allocazione dei servizi e degli uffici negli immobili;
d) elenco del personale e sua allocazione negli uffici;
e) attribuzione delle responsabilita';
f) algoritmi crittografici o altri sistemi utilizzati;
g) descrizione delle procedure utilizzate nell'attivita' di certificazione;
h) descrizione dei dispositivi installati;
i) descrizione dei flussi di dati;
l) procedura di gestione delle copie di sicurezza dei dati;
m) procedura di gestione dei disastri;
n) analisi dei rischi;
o) descrizione delle contromisure;
p) specificazione dei controlli;
q) procedura di continuita' operativa del servizio di pubblicazione delle liste di revoca e sospensione.
2. Il piano per la sicurezza si attiene anche 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 ed al decreto del Presidente del Consiglio dei ministri 2 dicembre 2014, adottato ai sensi dell'art. 58, comma 3, del decreto legislativo 30 giugno 2003, n. 196.

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Art. 26
Giornale di controllo

1. Il giornale di controllo e' costituito dall'insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso la CA, allorche' 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 e' apposto un riferimento temporale generato con le modalita' descritte dal Disciplinare tecnico di cui all'art. 33.
4. Il giornale di controllo e' tenuto in modo da garantire l'autenticita' delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza.
5. L'integrita' del giornale di controllo e' verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo non sono soggette a distruzione o cancellazione.

Art. 27
Sistema di qualita'

1. La CA operera' in conformita' a quanto previsto delle norme della serie ISO 9000 in materia di qualita' con procedure descritte nel Manuale della Qualita' che sara' emesso congiuntamente al Manuale Operativo ed al Disciplinare Tecnico di cui all'art. 33.

Art. 28
Organizzazione del personale della CA

1. L'organizzazione del personale, in possesso delle necessarie abilitazioni di sicurezza, addetto al servizio di certificazione e' composto da:
a) un responsabile della sicurezza del sistema informativo;
b) un responsabile del servizio di certificazione;
c) un responsabile della conduzione tecnica dei sistemi;
d) un responsabile dei servizi tecnici e logistici;
e) un responsabile delle verifiche e delle ispezioni (auditing).

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

2. I compiti e le mansioni attribuiti alle figure professionali di cui al comma 1 sono indicati nel Manuale Operativo di cui all'art. 32.

Art. 29
Organizzazione del personale della LRA

1. L'organizzazione del personale, in possesso delle necessarie abilitazioni di sicurezza, addetto al servizio della LRA e' composto da:
a) un responsabile del servizio di registrazione e validazione temporale;
b) un responsabile dei servizi tecnici.
2. Compiti e mansioni attribuiti alle figure professionali di cui al precedente comma sono indicate nel Manuale Operativo di cui all'art. 32.

Art. 30
Cessazione della LRA

1. Nel caso di cessazione della LRA quest'ultima, salvo diverse prescrizioni contenute nel Manuale Operativo di cui all'art. 32, deve consegnare alla CA la documentazione attinente l'attivita' svolta. La CA diventa depositaria di tale documentazione.

Art. 31
Rappresentazione del documento informatico

1. Il Disciplinare tecnico di cui all'art. 33 indica i formati e le modalita' operative da adottare per la rappresentazione dei documenti informatici di cui all'art. 2 .

Art. 32
Manuale operativo

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

1. La CA per svolgimento della sua attivita' si avvale di un Manuale Operativo che deve contenere almeno le seguenti informazioni:
a) dati identificativi della versione del Manuale Operativo;
b) definizione degli obblighi di CA, di LRA e del titolare;
c) modalita' di comunicazione fra CA ed LRA;
d) modalita' di identificazione e registrazione degli utenti;
e) modalita' di creazione delle chiavi per la generazione e la verifica della firma;
f) modalita' di emissione dei certificati;
g) modalita' di sospensione e revoca dei certificati;
h) modalita' di sostituzione delle chiavi;
i) modalita' di gestione del registro dei certificati;
l) modalita' di accesso al registro dei certificati;
m) modalita' per l'apposizione e la definizione del riferimento temporale;
n) modalita' operative per l'utilizzo del sistema di verifica delle firme;
o) modalita' operative per la generazione della firma digitale.

Capo IV
DISPOSIZIONI FINALI

Art. 33
Norme Tecniche

1. Il Disciplinare Tecnico e' redatto in conformita' con quanto disposto dalla normativa in materia di protezione e tutela delle informazioni classificate.
2. Gli algoritmi crittografici utilizzati, la specifica delle chiavi, la precisione dei riferimenti temporali e tutti i dettagli tecnico-operativi relativi alle procedure di sottoscrizione dei documenti informatici classificati saranno descritti nei documenti di cui al comma 1.
3. L'organo nazionale di sicurezza emana con propria direttiva, entro 12 mesi dall'adozione del presente regolamento, il Disciplinare Tecnico e il Manuale Operativo recante la disciplina applicativa dei principi e le procedure applicate dalla CA nello svolgimento della sua attivita' di cui al presente regolamento, e ne cura l'aggiornamento.

Art. 34

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887
Diritto & Diritti ISSN 1127-8579

Entrata in vigore

1. Il presente regolamento non e' sottoposto al visto e alla registrazione della Corte dei conti in quanto adottato ai sensi dell'art. 43 della legge, in deroga alle disposizioni di cui all'art. 17, della legge 23 agosto 1988, n. 400. 2. Il presente regolamento entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 6 novembre 2015

Il Presidente: Renzi

https://www.diritto.it/normativa/d-p-c-m-6-novembre-2015-firma-digitale/

© 2017 Diritto.it s.r.l. - Tutti i diritti riservati
Fondatore Francesco Brugaletta
P.I. 01214650887

Diritto & Diritti ISSN 1127-8579