Come cambia il testo unico sulla documentazione amministrativa

26.06.03

Questa tabella mostra, punto per punto, le modiche subite dal DPR 445/00 (testo unico sulla documentazione amministrativa) ad opera del DLgv 10/02 e del DPR 137/03. In caratteri blu le modifiche introdotte dal DLgv 10/02.

Versione originaria	Nuovo testo
Articolo 1 (R) - *Definizioni*	
n) FIRMA DIGITALE il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.	n) FIRMA DIGITALE è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, 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'integrità di un documento informatico o di un insieme di documenti informatici;
	t) CERTIFICATI ELETTRONICI ai sensi dell'articolo 2, comma 1, lettera d), del decreto legislativo 23 gennaio 2002, n. 10, gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;
	u) CERTIFICATORE ai sensi dell'articolo 2, comma 1, lettera b), del decreto legislativo 23 gennaio 2002, n. 10, il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisco altri servizi connessi con queste ultime;
	v) CERTIFICATORE QUALIFICATO il certificatore che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel presente testo unico e nelle regole tecniche di cui all'articolo 8, comma 2;
	z) CERTIFICATORE ACCREDITATO ai sensi dell'articolo 2, comma 1, lettera c), del decreto legislativo 23 gennaio 2002, n. 10, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva n. 1999/93/CE, nonché ai sensi del presente testo unico;
	aa) CERTIFICATI QUALIFICATI ai sensi dell'articolo 2, comma 1, lettera e), del decreto legislativo 23 gennaio 2002, n. 10, certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva n. 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
	cc) FIRMA ELETTRONICA ai sensi dell'articolo 2, comma 1, lettera a), del decreto legislativo 23 gennaio 2002, n. 10, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autentificazione informatica;
	dd) FIRMA ELETTRONICA AVANZATA ai sensi dell'articolo 2, comma 1, lettera g), del decreto legislativo 23 gennaio 2002, n. 10, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati:

	ee) FIRMA ELETTRONICA QUALIFICATA la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;
	ff) TITOLARE la persona fisica cui è attribuita la firma elettronica e che ha accesso al dispositivo per la creazione della firma elettronica;
	gg) DATI PER LA CREAZIONE DI UNA FIRMA i dati peculiari, come codici o chiavi crittografiche private, utilizzati dal titolare per creare la firma elettronica;
	hh) dispositivo per la creazione della firma: il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica;
	ii) DISPOSITIVO SICURO PER LA CREAZIONE DELLA FIRMA ai sensi dell'articolo 2, comma 1, lettera f), del decreto legislativo 23 gennaio 2002, n. 10, l'apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'articolo 10 del citato decreto n. 10 del 2002, nonché del presente testo unico;
	ll) DATI PER LA VERIFICA DELLA FIRMA i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica;
	mm) DISPOSITIVO DI VERIFICA DELLA FIRMA il programma informatico (software) adeguatamente configurato o l'apparato strumentale (hardware) usati per effettuare la verifica della firma elettronica;
	nn) ACCREDITAMENTO FACOLTATIVO ai sensi dell'articolo 2, comma 1, lettera h), del decreto legislativo 23 gennaio 2002, n. 10, il riconoscimento del possesso, da parte del certificatore che la richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza;
	oo) PRODOTTI DI FIRMA ELETTRONICA i programmi informatici (software), gli apparati strumentali (hardware) e i componenti di tali sistemi informatici, destinati ad essere utilizzati per la creazione e la verifica di firme elettroniche o da un certificatore per altri servizi di firma elettronica.
Articolo 8 (R) - *Documento informatico*	
2. Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definite con decreto del Presidente del Consiglio dei Ministri sentita l'Autorità per l'informatica nella pubblica amministrazione e sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con decorrenza almeno biennale a partire dalla data di entrata in vigore del presente testo unico.	2. Le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici sono definite con decreto del Presidente del Consiglio dei Ministri , o, per sua delega del ministro per l'innovazione e le tecnologie, sentiti il ministro per la funzione pubblica e sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con decorrenza almeno biennale a partire dalla data di entrata in vigore del presente testo unico.
Articolo 9 (R) - *(Documenti informatici delle pubbliche amministrazioni)*	
4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dall'Autorità per l'informatica nella pubblica amministrazione d'intesa con l'amministrazione degli archivi di Stato e, per il materiale classificato, con le Amministrazioni della difesa, dell'interno e delle finanze, rispettivamente competenti.	4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dalla Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, d'intesa con il Dipartimento della funzione pubblica ed il Ministero per i beni e le attività culturali, sentito il Garante per la protezione dei dati personali e, per il materiale

	classificato d'intesa con le Amministrazioni della difesa, dell'interno e dell'economia e delle finanze, rispettivamente competenti.
Articolo 10 (R) - *Forma ed efficacia del documento informatico*	
1. Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, soddisfa il requisito legale della forma scritta e ha efficacia probatoria ai sensi dell'articolo 2712 del Codice civile.	1. Il documento informatico ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate.
4. Il documento informatico redatto in conformità alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.	2. Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta. Sul piano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli articoli 2214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare.
3. Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 23, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile.	3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.
	4. Al documento informatico, sottoscritto con firma elettronica, in ogni caso non può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del fatto che è sottoscritto in forma elettronica ovvero in quanto la firma non è basata su di un certificato qualificato oppure non è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma non è stata apposta avvalendosi di un dispositivo per la creazione di una firma sicura.
	5. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su di un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni: a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro; b) il certificato qualificato è garantito da un certificatore stabilito nella Comunità europea, in possesso dei requisiti di cui alla medesima direttiva; c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra la Comunità e Paesi terzi o organizzazioni internazionali.
2. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro delle finanze.	6. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con decreto del Ministro dell'economia e delle finanze.
Articolo 11 (R) - *Contratti stipulati con strumenti informatici o per via telematic*a	
1. I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente testo unico sono validi e rilevanti a tutti gli effetti di legge.	1. I contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma elettronica qualificata secondo le disposizioni del presente testo unico sono validi e rilevanti a tutti gli effetti di legge.
Articolo 12 (R) - *Pagamenti informatici*	

1. Il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche definite col decreto di cui all'articolo 8, comma 2.	1. Il trasferimento in via telematica di fondi tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo regole fissate con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.
Articolo 20 (R) - *Copie di atti e documenti informatici*	
2. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente testo unico.	2. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma elettronica qualificata.
Capo II Sez. V **FIRMA DIGITALE**	**Capo II Sez. V** **FIRME ELETTRONICHE**
Articolo 22 (R) - *Definizioni*	
1. Ai fini del presente Testo unico si intende: a) per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;	1. Ai fini del presente Testo unico si intende: a) per sistema di validazione, il sistema informatico e crittografico in grado di generare e apporre la firma digitale o di verificarne la validità;
b) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;	b) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata e una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;
c) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.	c) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
d) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;	d) per 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;
f) per certificazione, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;	ABROGATA
g) per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;	f) per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, a uno o più documenti informatici, una data e un orario opponibili ai terzi;
h) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;	g) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;
i) per certificatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della	ABROGATA

chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;	
l) per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;	l) per revoca del certificato elettronico, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;
m) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.	m) per sospensione del certificato elettronico, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;
n) per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;	n) per validità del certificato elettronico, l'efficacia e l'opponibilità al titolare dei dati in esso contenuti.
o) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.	ABROGATA
Articolo 23 (R) - *Firma digitale*	
1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale.	1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.	2. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
3. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.	3. L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata.	4. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.
5. L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.	5. Attraverso il certificato elettronico si devono rilevare, secondo le regole tecniche di cui all'articolo 8, comma 2, la validità del certificato elettronico stesso, nonché gli elementi identificativi del titolare e del certificatore.
6. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.	ELIMINATO
7. Attraverso la firma digitale devono potersi rilevare gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.	ELIMINATO
Articolo 26 (R) - *Deposito della chiave privata*	**Art. 26 (R)** - *Certificatori*
1. Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata presso un notaio o altro pubblico depositario autorizzato.	1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva, ai sensi dell'articolo 3 del decreto legislativo 23 gennaio 2002, n. 10. Detti certificatori o, se persone giuridiche, i loro

	legali rappresentanti ed i soggetti preposti all'amministrazione, devono inoltre possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385.
2. La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e deve essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni.	2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili.	3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente decreto e le relative norme tecniche di cui all'articolo 8, comma 2, e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.
Articolo 27 (R) - *Certificazione delle chiavi*	**Art. 27 (R)** - *Certificatori qualificati*
1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 8, comma 1 deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.	1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro valultabili in forma telematica.	2. I certificatori di cui al comma 1 devono inoltre: a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione; b) impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2; c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate; d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10; e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi.
3. Salvo quanto previsto dall'articolo 29, le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati con il decreto di cui all'articolo 8: a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati; b) possesso da parte dei rappresentanti legali e dei	3. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente testo unico, ai sensi dell'articolo 4, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche; c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole tecniche di cui all'articolo 8; d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.	
4. La procedura di certificazione di cui al comma 1 può essere svolta anche da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione europea o dello Spazio economico europeo, sulla base di equivalenti requisiti.	4. Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente testo unico e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.
	Art. 27-bis (R) - *Certificati qualificati*
	1. I certificati qualificati devono contenere almeno le seguenti informazioni: a) indicazione che il certificato elettronico rilasciato è un certificato qualificato; b) numero di serie o altro codice identificativo del certificato; c) nome, ragione o denominazione sociale del certificatore e lo Stato nel quale è stabilito; d) nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale; e) dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare; f) indicazione del termine iniziale e finale del periodo di validità del certificato; g) firma elettronica avanzata del certificatore che ha rilasciato il certificato.
	2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.
	3. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto: a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza; b) limiti d'uso del certificato, ai sensi dell'articolo 28-bis, comma 3; c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.
Articolo 28 (R) - *Obblighi dell'utente e del certificatore*	**Art. 28 (R)** - *Accreditamento*
1. Chiunque intenda utilizzare un sistema di chiavi	1. Ai sensi dell'articolo 5 del decreto legislativo 23

asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.	gennaio 2002, n. 10, i certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, che a tali fini può avvalersi delle strutture pubbliche di cui all'articolo 29.
2. Il certificatore è tenuto a: a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 8; c) specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite; d) attenersi alle regole tecniche di cui all'articolo 8; e) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi; f) attenersi alle misure minime di sicurezza per il trattamento dei dati personali,emanate ai sensi dell'articolo 12, comma 2 della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di chiavi private; h) procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche; l) dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.	2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27 ed allegare alla domanda il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole di tecniche.
	3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre: a) avere natura giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385; b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti il collegio sindacale, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 citato del decreto legislativo 1° settembre 1993, n. 385.
	4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
	5. Il termine di cui al comma 4 può essere interrotto una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o

	completino la documentazione presentata e che non siano già nella disponibilità del Dipartimento per l'innovazione e le tecnologie o che questo non possa acquisire autonomamente. In tal caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
	6. A seguito dell'accoglimento della domanda, il Dipartimento per l'innovazione e le tecnologie dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal Dipartimento stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
	7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
	Art. 28-bis (L) *Responsabilità del certificatore*
	1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento: a) sull'esattezza delle informazioni in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati; b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato; c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi.
	2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato, salvo che provi d'aver agito senza colpa.
	3. Il certificatore può indicare, in un certificato qualificato, i limiti d'uso di detto certificato ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.
Articolo 29 (R) - *Chiavi di cifratura della pubblica amministrazione*	**Art. 29 (R)** - *Vigilanza sull'attività di certificazione*
1. Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.	1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, svolge funzioni di vigilanza e controllo sull'attività di certificazione, ai sensi dell'articolo 3, comma 2, del decreto legislativo 23 gennaio 2002, n. 10, anche attraverso le strutture di cui si avvale il Ministro per l'innovazione e le tecnologie.
2. Con il decreto di cui all'articolo 8 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni.	2. Fatto salvo quanto previsto dal comma 1, il Dipartimento per l'innovazione e le tecnologie provvede al controllo periodico dei certificatori accreditati.
3. Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente in conformità	ELIMINATO

alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici.	
4. Le chiavi pubbliche di ordini ed albi professionali legalmente riconosciuti e dei loro legali rappresentanti sono certificate e pubblicate a cura del Ministro di grazia e giustizia o suoi delegati.	ELIMINATO
	Art. 29-bis (R) - *Obblighi del titolare e del certificatore*
	1. Il titolare e il certificatore sono tenuti ad adottare tutte le misure organizzative e tecniche idonee a evitare danno ad altri.
	2. Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati è tenuto inoltre a: a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'articolo 8, comma 2, nel rispetto della legge 31 dicembre 1996, n. 675, e successive modificazioni; c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi; d) attenersi alle regole tecniche di cui all'articolo 8, comma 2; e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione; f) adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di dati per la creazione della firma del titolare; h) procedere alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo; l) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici; m) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari; n) non copiare, nè conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione; o) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure

	di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore; p) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.
	3. Il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.
	Art. 29-ter (R) - *Uso di pseudonimi*
	1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.
	Art. 29-quater (R) - *Efficacia dei certificati qualificati*
	1. La firma elettronica, basata su un certificato qualificato scaduto, revocato o sospeso non costituisce valida sottoscrizione.
	Art. 29-quinquies (R) - *Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati*
	1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni: a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati; b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
	2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente

	interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 8, comma 2.
	3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.
	4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche di cui all'articolo 8, comma 2.
	Art. 29-sexies (R) - *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 dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.
	3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.
	4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.
	Art. 29-septies (R) - *Revoca e sospensione dei certificati qualificati*
	1. Il certificato qualificato deve essere a cura del certificatore: a) revocato in caso di cessazione dell'attività del certificatore; b) revocato o sospeso in esecuzione di un provvedimento dell'autorità; c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente decreto; d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni;
	2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 8, comma 2.
	3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere

	attestato mediante adeguato riferimento temporale.
	4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 8, comma 2.
	Art. 29-octies (R) - *Cessazione dell'attività*
	1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al Dipartimento per l'innovazione e le tecnologie, informando senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
	2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. l'indicazione di un certificatore sostitutivo non impone la revoca di tutti i certificati non scaduti al momento della cessazione.
	3. Il certificatore di cui al comma 1 deve indicare altro depositario del registro dei certificati e della relativa documentazione.
	4. Il dipartimento rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 28, comma 6.
Articolo 36 (L) *Carta d'identità e documenti elettronici*	
1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e del documento d'identità elettronico sono definite con decreto del Presidente del Consiglio dei Ministri su proposta del Ministro dell'interno, di concerto con il Ministro della funzione pubblica, sentito il Garante per la protezione dei dati personali.	1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica, del documento d'identità elettronico e della carta nazionale dei servizi sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali
e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti ivi compresa la chiave biometrica, occorrenti per la firma digitale;	e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.
4. La carta d'identità elettronica può altresì essere utilizzata per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni.	4. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate ai fini dei pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con decreto del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.
5. Con decreto del Ministro dell'interno, sentiti l'Autorità per l'informatica nella pubblica amministrazione, il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione delle carte di identità e dei documenti di riconoscimento di cui al presente articolo. Le predette regole sono adeguate con cadenza almeno biennale in relazione alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche.	5. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi.
Articolo 38 (L-R) - *Modalità di invio e sottoscrizione delle istanze*	
2. Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale o quando il sottoscrittore è identificato	2. Le istanze e le dichiarazioni inviate per via telematica sono valide: a) se sottoscritte mediante la firma digitale, basata su

dal sistema informatico con l'uso della carta d'identità elettronica.	di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura; b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (L).