Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003

Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del D.Lgs. 23 gennaio 2002, n. 10.
(G. U. 27 aprile 2004, n. 98)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Visto il decreto legislativo 23 gennaio 2002, n. 10 di recepimento della direttiva 1999/93/CE sulle firme elettroniche, ed in particolare l'art. 10, comma 1, che prevede la definizione con decreto del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie dello Schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione;

Visto il decreto del Presidente del Consiglio dei Ministri 9 agosto 2001, pubblicato nella Gazzetta Ufficiale n. 198 del 27 agosto 2001, concernente la delega di funzioni del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie al Ministro senza portafoglio, Lucio Stanca;

Visto il decreto-legge 12 giugno 2001, n. 217, convertito, con modificazioni, dalla legge 3 agosto 2001, n. 317, recante: «Modificazioni al decreto legislativo 30 luglio 1999, n. 300, nonché alla legge 23 agosto 1988, n. 400, in materia di organizzazione del Governo»;

Visto il decreto-legge 1° dicembre 1993, n. 487, convertito, con modificazioni, dalla legge 29 gennaio 1994, n. 71, recante: «Trasformazione dell'Amministrazione delle poste e delle telecomunicazioni in ente pubblico economico e riorganizzazione del Ministero»;

Visto il decreto del Presidente della Repubblica 24 marzo 1995, n. 166, concernente: «Regolamento recante riorganizzazione del Ministero delle poste e delle telecomunicazioni»;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni, recante: «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»;

Visto il decreto del Presidente della Repubblica 28 luglio 1999, n. 318, recante: «Regolamento per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali»;

Visto il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante: «testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa», come modificato dal decreto legislativo 23 gennaio 2002, n. 10;

Visto l'art. 41, comma 2, della legge 16 gennaio 2003, n. 3;

Vista la Dir.Min. 16 gennaio 2002 del Ministro per l'innovazione e le tecnologie, di intesa con il Ministro delle comunicazioni, sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;

Vista la direttiva 1999/93/CE del 13 dicembre 1999, del Parlamento europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche;

Vista la risoluzione del Consiglio dell'Unione europea del 6 dicembre 2001 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione;

Vista la decisione della Commissione europea 6 novembre 2000 (2000/709/CE) relativa ai criteri minimi di cui devono tener conto gli Stati membri all'atto di designare gli organismi di cui all'art. 3, paragrafo 4, della direttiva 1999/93/CE del Parlamento europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche;

Viste le norme UNI CEI EN ISO/IEC 17025:2000 concernente i requisiti generali per la competenza dei laboratori di prova e di taratura e UNI CEI EN 45011 concernente i requisiti generali relativi agli organismi che gestiscono sistemi di certificazione di prodotti;

Visti i criteri di cui agli Information Technology Security Evaluation Criteria (ITSEC), giugno 1991, e al Information Technology Security Evaluation Manual (ITSEM), settembre 1993;

Vista la raccomandazione del Consiglio dell'Unione europea (95/144/CE) in data 7 aprile 1995, concernente l'applicazione dei criteri per la valutazione della sicurezza della tecnologia dell'informazione (ITSEC - Information Technology Security Evaluation Criteria);

Visto l'atto del Comitato di gestione dell'ISO (International Standard Organization) che definisce come International Standard ISO/IEC n. 15408, la versione 2.1 dei «Common Criteria for Information Technology Security Evaluation» dell'agosto 1999;

Visto il Codice di buona pratica per la gestione della sicurezza dell'informazione di cui a ISO/IEC n. 17799, del 2000;

Considerato che l'informazione, nell'attuale società, costituisce un bene essenziale e si rende necessario garantirne l'integrità, la disponibilità e la riservatezza con misure di sicurezza che costituiscano parte integrante di un sistema informatico;

Considerato che da tempo i produttori offrono sistemi e prodotti dotati di funzionalità di sicurezza, per la quale dichiarano caratteristiche e prestazioni al fine di orientare gli utenti nella scelta delle soluzioni più idonee a soddisfare le proprie esigenze;

Considerato che in molte applicazioni caratterizzate da un elevato grado di criticità, le predette dichiarazioni potrebbero risultare non sufficienti, rendendo necessaria una loro valutazione e certificazione della sicurezza, condotte da soggetti indipendenti e qualificati, sulla base di standard riconosciuti a livello nazionale ed internazionale;

Considerato che le garanzie concernenti l'adeguatezza, la qualità e l'efficacia dei dispositivi di sicurezza di un sistema informatico possono essere fornite solo da certificatori e valutatori indipendenti ed imparziali;

Considerata la necessità di favorire, a livello comunitario e internazionale, la cooperazione tra gli organismi di certificazione e il mutuo riconoscimento dei certificati di valutazione della sicurezza nel settore della tecnologia dell'informazione;

Considerata la necessità di individuare un organismo di certificazione e di definire uno Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione, definendo altresì le competenze e le responsabilità degli organismi preposti alla sua applicazione;

Ritenuto che l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCTI) del Ministero delle comunicazioni possiede i requisiti di indipendenza, affidabilità e competenza tecnica richiesti dalla decisione della Commissione europea 6 novembre 2000 (2000/709/CE);

Di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze;

Adotta il seguente decreto:

1. Definizioni.

1. Ai fini del presente decreto si intende per:

a) COMMITTENTE: la persona fisica, giuridica o altro organismo o associazione che commissiona e sostiene gli oneri economici della valutazione e certificazione e che può anche rivestire il ruolo di fornitore;

b) FORNITORE: la persona fisica, giuridica o altro organismo o associazione che fornisce l'oggetto della valutazione e che può rivestire anche il ruolo di committente;

c) VALUTAZIONE: l'analisi di un sistema, prodotto, profilo di protezione o traguardo di sicurezza condotta in base a predefiniti criteri applicati secondo una predefinita metodologia;

d) LABORATORIO PER LA VALUTAZIONE DELLA SICUREZZA (LVS): l'organizzazione indipendente che ha ottenuto l'accreditamento e che pertanto è abilitata ad effettuare valutazioni e a fornire assistenza;

e) ACCREDITAMENTO: il riconoscimento formale dell'indipendenza, affidabilità e competenza tecnica di un centro per la valutazione della sicurezza;

f) OGGETTO DELLA VALUTAZIONE (ODV): il sistema o prodotto sottoposto alla valutazione;

g) PRODOTTO: l'elemento software, hardware o firmware idoneo a fornire una determinata funzionalità, progettato per essere utilizzato o incorporato in uno o più sistemi;

h) SISTEMA: gli elementi software, firmware o hardware funzionalmente o fisicamente interconnessi, destinati al trattamento automatico delle informazioni ed operanti in un ambiente definito;

i) PIANO DI VALUTAZIONE: il documento che descrive le attività che saranno svolte dal centro per la valutazione della sicurezza durante il processo di valutazione, i tempi di esecuzione e le risorse necessarie;

l) RAPPORTO DI ATTIVITÀ: il documento che il LVS invia all'organismo di certificazione, nel quale sono indicati dettagliatamente i risultati raggiunti e le attività svolte dal centro stesso durante le varie fasi della valutazione;

m) RAPPORTO DI OSSERVAZIONE il rapporto dell'organismo di certificazione o il LVS finalizzato alla richiesta di chiarimenti o variazioni inerenti l'oggetto cui si riferisce; può contenere informazioni riservate;

n) RAPPORTO FINALE DI VALUTAZIONE: il rapporto del LVS, contenente i risultati della valutazione, che costituisce la base per la certificazione dell'ODV, profilo di protezione o traguardo di sicurezza, contenente informazioni riservate;

o) RAPPORTO DI CERTIFICAZIONE: il documento emesso dall'organismo di certificazione, che conferma i risultati della valutazione e la corretta applicazione dei criteri;

p) CERTIFICAZIONE: l'attestazione da parte dell'organismo di certificazione che conferma i risultati della valutazione e la corretta applicazione dei criteri adottati e della relativa metodologia;

q) FIDUCIA: la fiducia che si può riporre nel soddisfacimento degli obiettivi di sicurezza da parte dell'oggetto della valutazione considerando le minacce e l'ambiente descritti nel traguardo di sicurezza;

r) LIVELLO DI FIDUCIA: la misura della fiducia espressa mediante identificatori alfanumerici la cui parte numerica cresce con il crescere della fiducia (in ITSEC da E0 a E6; nei Common Criteria da EALO a EAL7);

s) FUNZIONI DI SICUREZZA: le contromisure di tipo tecnico di cui è dotato l'oggetto della valutazione;

t) MECCANISMO DI SICUREZZA: le componenti hardware, software e firmware che realizzano le funzioni di sicurezza di cui è dotato l'oggetto della valutazione;

u) MATERIALE PER LA VALUTAZIONE: la documentazione tecnica o le componenti software, hardware, firmware realizzati durante lo sviluppo del sistema o del prodotto e contenente informazioni riservate;

v) PROFILO DI PROTEZIONE: il documento che descrive per una certa categoria di ODV ed in modo indipendente dalla realizzazione, gli obiettivi di sicurezza, le minacce, l'ambiente ed i requisiti funzionali e di fiducia, definiti secondo i Common Criteria;

z) ROBUSTEZZA DEI MECCANISMI DI SICUREZZA E DELLE FUNZIONI DI SICUREZZA DELL'ODV: la misura della capacità di contrastare attacchi diretti condotti con risorse predefinite;

aa) TRAGUARDO DI SICUREZZA: Il documento, utilizzato come base per la valutazione di un ODV, che contiene gli obiettivi di sicurezza, la descrizione dell'ambiente in cui l'ODV è utilizzato e le minacce alle quali è soggetto, i requisiti funzionali e di fiducia, la specifica delle funzioni di sicurezza.

2. Oggetto e àmbito di applicazione.

1. Il presente decreto definisce lo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, di seguito denominato «Schema nazionale», recante l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione, in conformità ai criteri europei ITSEC o agli standard internazionali ISO/IEC IS-15408 (Common Criteria), emanati dall'ISO (Organizzazione internazionale per la standardizzazione).

2. Le procedure relative allo Schema nazionale devono essere osservate dall'organismo di certificazione, dai LVS, nonché da tutti coloro, persone fisiche, giuridiche e qualsiasi altro organismo o associazione, cui competono le decisioni in ordine alla richiesta, acquisizione, progettazione, realizzazione, installazione ed impiego di sistemi e prodotti nel settore della tecnologia dell'informazione, per i quali la sicurezza costituisce uno dei requisiti e che necessitano di una certificazione di sicurezza conforme ai criteri di cui al comma 1.

3. Lo Schema nazionale non si applica per i sistemi e prodotti che trattino informazioni classificate.

4. Nell'àmbito dello Schema nazionale, la sicurezza nel settore della tecnologia dell'informazione è la protezione della riservatezza, integrità, disponibilità delle informazioni mediante il contrasto delle minacce originate dall'uomo o dall'ambiente, al fine di impedire, a coloro che non siano stati autorizzati, l'accesso, l'utilizzo, la divulgazione, la modifica delle informazioni stesse e di garantirne l'accesso e l'utilizzo a coloro che siano stati autorizzati.

3. Finalità dell'attività di valutazione e di certificazione.

1. La procedura di valutazione è finalizzata all'emissione di un rapporto in cui viene dichiarato se:

a. l'ODV soddisfa il traguardo di sicurezza con il livello di fiducia richiesto;

b. il profilo di protezione è completo, consistente e tecnicamente corretto;

c. il traguardo di sicurezza è completo, consistente e tecnicamente corretto ed adatto ad essere usato come base per la valutazione del corrispondente ODV.

2. La certificazione stabilisce che la valutazione è stata condotta conformemente ai criteri necessari a verificare il soddisfacimento del livello di fiducia, della robustezza dei meccanismi o delle funzioni di sicurezza dichiarati e conseguentemente garantisce i risultati della valutazione stessa.

3. La certificazione effettuata dall'ISCTI avviene a titolo oneroso. Le relative tariffe e modalità di versamento sono stabilite dal Ministro delle comunicazioni di concerto con il Ministro dell'economia e delle finanze, da emanarsi entro trenta giorni dall'entrata in vigore del presente decreto, secondo le disposizioni di cui all'art. 7 del decreto del Presidente della Repubblica 29 marzo 1973, n. 156.

4. Organismo di certificazione,

1. L'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCTI) del Ministero delle comunicazioni è l'organismo di certificazione della sicurezza informatica nel settore della tecnologia dell'informazione, anche ai sensi dell'art. 10 del decreto legislativo 23 gennaio 2002, n. 10 e dell'art. 3, paragrafo 4 della direttiva 1999/93/CE.

2. L'organismo di certificazione sovrintende alle attività operative di valutazione e certificazione nell'àmbito dello Schema nazionale attraverso:

a) la predisposizione di regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie ed internazionali di riferimento, ai fini dell'approvazione 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 delle comunicazioni;

b) il coordinamento delle attività nell'àmbito dello Schema nazionale in armonia con i criteri ed i metodi di valutazione;

c) la predisposizione delle linee guida per la valutazione di prodotti, traguardi di sicurezza, profili di protezione e sistemi, ai fini dell'approvazione 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 delle Comunicazioni;

d) la divulgazione dei princìpi e delle procedure relative allo Schema nazionale;

e) l'accreditamento, la sospensione e la revoca dell'accreditamento dai LVS;

f) la verifica del mantenimento dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte dei LVS accreditati;

g) l'approvazione dei piani di valutazione;

h) l'ammissione e registrazione delle valutazioni;

i) l'approvazione dei rapporti finali di valutazione;

l) l'emissione dei rapporti di certificazione sulla base delle valutazioni eseguite dai LVS;

m) l'emissione e la revoca dei certificati di sicurezza;

n) la definizione, l'aggiornamento e la diffusione, su base semestrale, di una lista di prodotti, sistemi e profili di protezione certificati;

o) la predisposizione, la tenuta e l'aggiornamento dell'elenco dai LVS accreditati;

p) la promozione delle attività per la diffusione della cultura della sicurezza nel settore della tecnologia dell'informazione;

q) la formazione, abilitazione e addestramento dei certificatori, personale dipendente dell'organismo di certificazione, nonché dei valutatori, dipendenti dei LVS e assistenti, ai fini dello svolgimento delle attività di valutazione;

r) la predisposizione, tenuta e aggiornamento dell'elenco dei certificatori valutatori e assistenti.

3. L'organismo di certificazione riferisce semestralmente sull'attività al Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri.

4. Sulla base degli indirizzi stabiliti dal Presidente del Consiglio dei Ministri o, per sua delega, dal Ministro per l'innovazione e le tecnologie e dal Ministro delle comunicazioni, l'organismo di certificazione cura i rapporti con organismi di certificazione esteri congiuntamente con l'Autorità Nazionale di Sicurezza, nonché partecipa alle altre attività in àmbito internazionale e comunitario riguardanti il mutuo riconoscimento dei certificati di sicurezza.

5. Alle predette attività l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCTI) farà fronte senza oneri aggiuntivi per il bilancio dello Stato.

5. Laboratori per la valutazione della sicurezza.

1. I laboratori per la valutazione della sicurezza (LVS) sono accreditati dall'organismo di certificazione ed effettuano le valutazioni di ODV secondo lo Schema nazionale e sotto il controllo dell'organismo di certificazione medesimo.

2. Ai fini dell'accreditamento, il LVS deve possedere i seguenti requisiti:

a) capacità di garantire l'imparzialità, l'indipendenza, la riservatezza e l'obiettività, che sono alla base del processo di valutazione;

b) disponibilità di locali e mezzi adeguati ad effettuare valutazioni ai fini della sicurezza nel settore della tecnologia dell'informazione;

c) organizzazione in grado di controllare il rispetto delle misure di sicurezza e della qualità previste per il processo di valutazione;

d) disponibilità di personale sufficiente dotato delle necessarie competenze tecniche e iscritto nell'elenco dell'organismo di certificazione;

e) conformità ai requisiti specificati nelle norme UNI CEI EN ISO/IEC 17025:2000 e UNI CEI EN 45011 per quanto applicabili;

f) capacità di mantenere nel tempo i requisiti in virtù dei quali è stato accreditato.

3. Il LVS deve garantire la massima riservatezza su tutte le informazioni acquisite relative all'oggetto della valutazione. A tal fine il committente può chiedere la sottoscrizione di un documento nel quale il LVS si impegna a mantenere la riservatezza su informazioni tecniche acquisite durante le attività di valutazione.

4. Oltre alle valutazioni di cui al comma 1, il LVS, previa formale comunicazione all'organismo di certificazione, può svolgere le seguenti attività:

a) assistenza al committente per la stesura della documentazione di sicurezza, nonché, durante la preparazione alla valutazione, per la determinazione della valutabilità del traguardo di sicurezza, ODV o profilo di protezione, assicurando che siano strutture e persone separate da quelle che effettuano la valutazione;

b) formazione sulle problematiche della sicurezza nel settore della tecnologia dell'informazione in generale e, in particolare, sulle tecniche di valutazione.

5. I valutatori devono essere indipendenti nello svolgimento delle loro attività. Qualora uno o più valutatori di un LVS diano assistenza ad un fornitore o committente per un ODV o parte di esso, gli stessi non potranno partecipare alla valutazione dello stesso ODV.

6. Responsabile della valutazione.

1. L'organismo di certificazione, il LVS e il committente devono rispettivamente designare un responsabile per ogni valutazione.

7. Accesso alle informazioni e garanzie di riservatezza.

1. Il committente deve garantire al LVS e all'organismo di certificazione il libero accesso ad ogni tipo di informazione, inerente il sistema, profilo di protezione, prodotto o traguardo di sicurezza, che risulti necessaria per lo svolgimento delle attività di valutazione e certificazione. L'organismo di certificazione e il LVS devono garantire che le informazioni a cui hanno accesso non siano divulgate a soggetti non autorizzati.

8. Attività preparatorie della valutazione.

1. Le attività di preparazione della valutazione sono svolte dal LVS e dal committente.

2. Il committente chiede l'intervento del LVS, specificando il traguardo di sicurezza o il profilo di protezione richiesto.

3. Il LVS esamina il traguardo di sicurezza o il profilo di protezione al fine di accertare, sulla base anche di eventuale ulteriore documentazione richiesta al committente, che lo stesso costituisca una solida base per la conduzione del processo di valutazione; ove necessario richiede modifiche.

4. Il LVS, in ragione delle informazioni di cui dispone, verifica l'assenza di elementi che possano pregiudicare il buon esito della valutazione.

5. Al fine di ottenere la certificazione il LVS comunica all'organismo di certificazione l'avvio dell'attività di valutazione.

9. Valutazione.

1. Il LVS effettua la valutazione impiegando il materiale per la valutazione, le risorse e i tempi indicati nel piano di valutazione, sottoposto all'approvazione dell'organismo di certificazione.

2. L'organismo di certificazione sovrintende alla valutazione mediante l'analisi dei rapporti di attività e dei rapporti di osservazione, le riunioni di aggiornamento ed eventualmente la partecipazione alle attività di valutazione.

3. Il LVS invia all'organismo di certificazione rapporti di attività per l'aggiornamento sullo stato della valutazione.

4. Il LVS può inviare al committente rapporti di osservazione finalizzati alla richiesta di chiarimenti o modifiche all'oggetto della valutazione, profilo di protezione, traguardo di sicurezza o al materiale per la valutazione. In tal caso, il committente è tenuto a fornire chiarimenti attraverso le risposte ai rapporti di osservazione, eventualmente apportando modifiche, entro il termine fissato.

5. Il LVS invia all'organismo di certificazione il rapporto finale di valutazione, allegandovi i verdetti intermedi e finali emessi con le relative motivazioni. In tale rapporto il LVS indica le risorse impiegate, le attività svolte, le osservazioni formulate e le relative risposte.

6. L'organismo di certificazione approva il rapporto finale di valutazione entro sessanta giorni dalla sua ricezione, qualora ne riscontri la conformità con i criteri e la metodologia adottati e lo Schema nazionale.

7. Qualora vengano individuate nel rapporto finale di valutazione delle anomalie risolvibili, l'organismo di certificazione richiede al LVS, nello stesso termine di cui al comma 6, il perfezionamento del rapporto finale di valutazione. In tal caso, il LVS è tenuto a perfezionare il rapporto entro i successivi quindici giorni. La richiesta di cui al presente comma sospende, fino al relativo esito, il decorso del termine di cui al comma 6.

8. Decorso inutilmente il termine di cui al comma 6, il rapporto finale di valutazione si intende approvato.

10. Certificazione.

1. Entro trenta giorni dall'approvazione del rapporto finale di valutazione, l'organismo di certificazione redige uno schema di rapporto di certificazione, contenente le indicazioni di cui al comma 2, che invia al LVS e al committente per avere conferma dell'assenza di errori materiali e della volontà dello stesso di ottenere il rilascio del rapporto di certificazione e del relativo certificato, nonché dell'assenza di elementi che consentano la divulgazione di informazioni riservate. Il LVS e il committente si pronunciano sulla richiesta entro i successivi 5 giorni.

2. Acquisita la conferma da parte del LVS e del committente, o decorso inutilmente il termine per la loro pronuncia, l'organismo di certificazione emette entro i successivi trenta giorni il rapporto di certificazione, in cui deve:

a) motivare l'eventuale emissione di giudizi in contrasto con quelli LVS;

b) dichiarare se la valutazione è stata condotta secondo i criteri e la metodologia previsti dallo Schema nazionale;

c) dichiarare se l'ODV o il traguardo di sicurezza o il profilo di protezione è conforme ai criteri di valutazione;

d) dichiarare se l'ODV o il profilo di protezione soddisfa il livello di fiducia dichiarato;

e) dichiarare che l'ODV è caratterizzato da meccanismi critici o funzioni di sicurezza la cui robustezza è conforme alla dichiarazione del committente.

3. Il rapporto di certificazione non deve contenere informazioni riservate, può essere utilizzato esclusivamente dall'organismo di certificazione e dal committente e reso pubblico solo integralmente.

4. In caso di valutazione positiva, l'organismo di certificazione allega al rapporto di certificazione il relativo certificato.

5. In relazione alla valutazione di sistemi, i termini di cui ai commi 1 e 2 possono essere differiti, d'intesa con le parti, in ragione della complessità del sistema stesso. Ai fini del decorso dei predetti termini non è computato il tempo richiesto per il riscontro ad eventuali osservazioni e chiarimenti.

11. Validità della certificazione.

1. I risultati delle attività di valutazione e certificazione sono riferibili esclusivamente ad una specifica e determinata configurazione dell'ODV e il certificato è valido ed efficace limitatamente a tale configurazione.

2. La commercializzazione di un sistema o prodotto certificato è vincolata a tale configurazione.

12. Controversie.

1. Nelle linee guida di cui all'art. 13 sono stabilite le procedure di risoluzione extragiudiziale delle controversie insorte in ordine alle attività di valutazione e certificazione svolte secondo lo Schema nazionale, nel rispetto dei princìpi di imparzialità, trasparenza, efficacia ed equità della procedura, nonché nel rispetto del principio del contraddittorio.

13. Norme transitorie e finali.

1. Entro 2 mesi dalla pubblicazione del presente decreto nella Gazzetta Ufficiale, l'organismo di certificazione predispone le «Linee guida provvisorie» per l'applicazione dello Schema nazionale, da approvare con decreto del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro delle comunicazioni, valevoli fino all'adozione delle «Linee guida definitive».

2. L'organismo di certificazione predispone, altresì, entro 12 mesi dalla pubblicazione del presente decreto, le «Linee guida definitive», recanti indicazioni dettagliate relative allo svolgimento delle attività di valutazione e certificazione, da approvare con la medesima procedura di cui al comma 1, esperita la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del 22 giugno 1998, del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE, del 20

luglio 1998, del Parlamento europeo e del Consiglio, attuata con decreto legislativo 23 novembre 2000, n. 427.

3. Per le valutazioni dei dispositivi di firma già effettuate, ai sensi delle vigenti regole tecniche, prima dell'entrata in vigore del presente decreto da centri di valutazione rispondenti ai requisiti di cui al presente decreto, ciascun LVS invia all'organismo di certificazione il rapporto finale di valutazione. L'organismo di certificazione procede ai sensi dei commi 6 e seguenti dell'art. 9.

4. Per un periodo di nove mesi decorrente dall'entrata in vigore del presente decreto, i certificatori di firma elettronica attestano la rispondenza dei propri prodotti e dispositivi di firma elettronica ai requisiti di sicurezza previsti dalla vigente normativa mediante autodichiarazione. Decorso il periodo indicato, si ricorre alla certificazione ai sensi del presente decreto, come prescritto dall'art. 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

5. Le autodichiarazioni rese ai sensi del D.P.C.M. 7 dicembre 2000, del D.P.C.M. 20 aprile 2001 e del D.P.C.M. 3 ottobre 2001, continuano a spiegare ininterrottamente i propri effetti fino al termine del periodo di cui al comma 4.

6. Il presente decreto non reca oneri aggiuntivi per il bilancio dello Stato ed è pubblicato nella Gazzetta Ufficiale della Repubblica italiana.