Ministero dello Sviluppo Economico

Dipartimento per le Comunicazioni

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE

OCSI/ACC/01/2010/PROC

Versione 1.0

2 novembre 2010

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	02/11/10

2 Indice

3 Riferimenti

[R01] DPCM del 10 febbraio 2010, G.U. n. 98 del 28 aprile 2010, recante “Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza”.

[R02] “Commission Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council”, Official Journal L 175, 15 luglio 2003.

[R03] “Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures”, Official Journal L 13, 19 gennaio 2000.

[R04] “Common Criteria for Information Technology Security Evaluation”, <www.commoncriteriaportal.org/thecc.html>.

[R05] “Documento di Supporto alla Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall’Allegato III della Direttiva 1999/93/CE”, OCSI/ACC/02/2010/DDS, versione 1.0, 2 novembre 2010

[R06] “Individuazioni delle prestazioni, eseguite dal Ministero delle Comunicazioni per conto terzi, ai sensi dell’articolo 6 del Decreto Legislativo 30 dicembre 2003, n. 366”, Decreto Interministeriale 15 febbraio 2006, G.U. n. 82, 7 aprile 2006.

[R07] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”, ETSI TS 102 176-1 V2.0.0 (2007-11), Technical Specification.

[R08] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices”, ETSI TS 102 176-2 V1.2.1 (2005-07), Technical Specification.

[R09] “Common Criteria Recognition Arrangement”, <www.commoncriteriaportal.org/theccra.html>.

[R10] “Certificate Authorizing Schemes”, <www.commoncriteriaportal.org/schemes.html>.

[R11] SOGIS-MRA “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 3.0, gennaio 2010.

4 Premessa

A. La Procedura di Accertamento in oggetto è valida esclusivamente per dispositivi per la creazione di firme elettroniche soddisfacenti i seguenti requisiti:

   i. al dispositivo deve essere applicabile il DPCM 10 febbraio 2010, recante "Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza" [R01];

   ii. per l'Accertamento di Conformità del dispositivo non è applicabile la Decisione Europea 2003/511/CE [R02] relativa al soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE [R03].

B. Per i dispositivi che superano con successo la Procedura di Accertamento in oggetto si rilascia un Attestato di Conformità la cui validità è soggetta alle condizioni e alle ipotesi esplicitate nel relativo Rapporto di Accertamento.

C. Il rilascio dell'Attestato di Conformità richiede, per il dispositivo di interesse, una certificazione di sicurezza ritenuta adeguata dall'OCSI ai fini del soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE:

   i. condizione necessaria ma non sufficiente per l'adeguatezza di cui sopra è che i criteri adottati per la certificazione di sicurezza siano riconosciuti dall'OCSI adeguati ai fini dell'Accertamento di Conformità;

   ii. i criteri di certificazione noti come *Common Criteria* [R04] sono riconosciuti dall'OCSI adeguati ai fini dell'Accertamento di Conformità;

   iii. nel seguito si descrive l'Accertamento di Conformità basato su certificazione di sicurezza rilasciata in accordo ai *Common Criteria*;

   iv. l'Accertamento di Conformità basato su certificazione di sicurezza rilasciata in accordo a criteri diversi dai *Common Criteria* non è escluso a priori ma necessita di una definizione caso per caso che deve essere richiesta all'OCSI dal soggetto interessato e che comporta per questi l'onere di fornire evidenza dell'equivalenza, ai fini dell'Accertamento di Conformità, tra la certificazione di interesse e quella ritenuta adeguata dall'OCSI.

D. La Procedura di Accertamento può essere soggetta ad aggiornamenti a causa di mutamenti di carattere normativo, scientifico e tecnologico del contesto di riferimento. In caso di aggiornamento, l'OCSI pubblica sul proprio sito Web istituzionale, nella sezione dedicata ai dispositivi di firma, all'indirizzo <www.ocsi.isticom.it/index.php/dispositivi-di-firma>, la versione aggiornata della Procedura, mantenendo l'archivio storico delle versioni precedenti.

E. Per i soggetti interessati all'Accertamento di Conformità in oggetto è disponibile il

Documento di Supporto [R05], in cui sono forniti ulteriori dettagli e approfondimenti aventi il fine di agevolare la comprensione e l'applicazione della Procedura.

F. Per i costi si applica il Decreto Interministeriale del 15 febbraio 2006 [R06].

5 Introduzione all'Accertamento basato su certificazione Common Criteria

A. La Procedura di Accertamento in oggetto si basa sui seguenti elementi del modello di certificazione *Common Criteria*:

   i. il Traguardo di Sicurezza (TDS), che fornisce la caratterizzazione di sicurezza dell'Oggetto della Valutazione (ODV) e quella dell'ambiente dell'ODV e, in particolare, identifica gli obiettivi di sicurezza a carico dell'ODV e quelli a carico dell'ambiente dell'ODV;

   ii. il Certificato, che fornisce evidenza che una certificazione *Common Criteria* è stata eseguita per un dato dispositivo come realizzazione dell'ODV di un dato TDS, nell'ipotesi che l'ambiente del dispositivo soddisfi gli obiettivi di sicurezza a carico dell'ambiente dell'ODV.

B. Ai fini del soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE [R03], la Procedura di Accertamento in oggetto definisce i requisiti fondamentali per il TDS (cap. 6, punto B.) e per il riconoscimento del Certificato (cap. 6, punto C.).

C. L'OCSI è disponibile, su richiesta, a considerare la possibilità di adattamento dei vincoli di cui al punto B. a casi specifici. Gli adattamenti ritenuti possibili dall'OCSI saranno comunque riportati, in caso di rilascio dell'Attestato di Conformità, nel corrispondente Rapporto di Accertamento di cui al cap. 10, punto B.

D. All'adeguatezza di un TDS concorrono congiuntamente:

   i. la caratterizzazione di sicurezza dell'ODV;

   ii. la caratterizzazione di sicurezza dell'ambiente dell'ODV.

E. Si noti che la Procedura di Accertamento in oggetto:

   i. analizza direttamente le caratterizzazioni di sicurezza di cui al punto D.;

   ii. non analizza direttamente la rispondenza di un dato dispositivo reale alla caratterizzazione di sicurezza dell'ODV e si basa per questo aspetto sull'evidenza del Certificato di cui al punto A.ii.;

   iii. non analizza, né direttamente né indirettamente, la rispondenza di un dato ambiente reale alla caratterizzazione di sicurezza dell'ambiente dell'ODV.

F. Le caratteristiche dell'Attestato di Conformità sono indicate nel cap. 10.

G. La Procedura di Accertamento in oggetto prevede due modalità alternative:

i. Procedura in Modalità 1: la prima modalità è indicata per i casi in cui il Certificato sia disponibile all'avvio della Procedura e prevede un'unica fase che produce un responso da parte dell'OCSI, consistente nel rilascio dell'Attestato di Conformità o nella motivazione per il mancato rilascio. La prima modalità copre quindi i casi in cui il richiedente cerca di dare valore a una certificazione la cui spendibilità ai fini dell'accertamento non sia stata precedentemente formalizzata in alcun modo dall'OCSI.

ii. Procedura in Modalità 2: la seconda modalità è indicata per i casi in cui il Certificato non è disponibile all'avvio della Procedura e il relativo processo di Certificazione non è ancora stato avviato o si trova in una fase iniziale. La seconda modalità mira quindi a produrre, seppure con i limiti precisati nel cap. 9, una formalizzazione della spendibilità che un Certificato non ancora ottenuto avrà ai fini dell'accertamento. La seconda modalità prevede una prima fase che produce un primo responso da parte dell'OCSI, consistente in un Pronunciamento (Positivo o Negativo) sul materiale analizzato. In caso di Pronunciamento Positivo, la Procedura nella seconda modalità prevede una seconda fase, da avviare alla consegna del Certificato, che dovrà avvenire entro un tempo prefissato; la seconda fase produce un secondo responso consistente nel rilascio dell'Attestato di Conformità o nella motivazione per il mancato rilascio.

6 Adeguatezza della certificazione Common Criteria

A. I requisiti seguenti si riferiscono al caso di dispositivo con generazione di chiavi al suo interno (l'OCSI è disponibile, su richiesta, a considerare eccezioni all'impostazione adottata: per un approfondimento si veda il Documento di Supporto [R05]).

B. Requisiti per l'adeguatezza del TDS:

   i. gli obiettivi di sicurezza dell'ODV, congiuntamente agli obiettivi di sicurezza dell'ambiente dell'ODV, devono garantire il soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE [R03];

   ii. la ripartizione tra obiettivi di sicurezza dell'ODV e obiettivi di sicurezza dell'ambiente dell'ODV deve essere tale che l'ODV includa tutte le funzioni di sicurezza che coinvolgono chiavi di firma per qualsiasi operazione connessa al loro intero ciclo di vita;

   iii. le funzioni di sicurezza di tipo crittografico incluse nell'ODV devono utilizzare algoritmi, protocolli, chiavi e parametri di sicurezza conformi a ETSI TS 102 176-1 V2.0.0 [R07] e successive edizioni;

   iv. se il TDS include il trasferimento attraverso canale sicuro, realizzato con strumenti crittografici, di chiavi di firma e/o di verifica della firma dall'ODV verso l'esterno e/o viceversa, allora tale canale deve essere conforme allo standard ETSI TS 102 176-2 V1.2.1 [R08] e successive edizioni;

   v. se la versione dichiarata dei *Common Criteria* è la 3.1, il livello di garanzia (*assurance*) dichiarato deve essere almeno EAL4 con l'aggiunta (*augmentation*) della componente di garanzia AVA_VAN.5 o di componenti a questa equivalenti;

   vi. se la versione dichiarata dei *Common Criteria* è precedente alla 3.1:

      a. il livello di garanzia (*assurance*) dichiarato deve essere almeno EAL4 con l'aggiunta (*augmentation*) della coppia di componenti di garanzia AVA_VLA.4 e AVA_MSU.3 o di componenti a questa coppia equivalenti;

      b. il valore dichiarato di *Strength of Function* (SOF) deve essere HIGH.

C. Requisiti per il riconoscimento del Certificato ai fini della Procedura di Accertamento:

   i. l'OCSI accetta un certificato emesso da un Paese che, nell'ambito dell'accordo CCRA [R09], ha ottenuto il ruolo di *Certificate Authorizing Scheme* [R10] in data non posteriore a quella di emissione del certificato

stesso (per un approfondimento si veda il Documento di Supporto [R05]);

ii. l'OCSI accetta un certificato emesso da un Paese che, nell'ambito dell'accordo SOGIS-MRA [R11], ha ottenuto il ruolo di *Certificate Authorising Participant* in data non posteriore a quella di emissione del certificato stesso (per un approfondimento si veda il Documento di Supporto).

7 Richiesta di Accertamento di Conformità

A. I materiali da presentare in prima istanza per l'Accertamento di Conformità di un dato dispositivo sono:

   i. Richiesta di Accertamento di Conformità nella quale siano specificati:

      a. il soggetto richiedente l'accertamento e il suo ruolo;

      b. l'ambito dell'Accertamento di Conformità stesso (DPCM 10 febbraio 2010 [R01]);

      c. il dispositivo per cui si richiede l'Accertamento di Conformità identificato tramite l'identificativo utilizzato nel TDS;

      d. la modalità della Procedura di Accertamento che si intende attivare (modalità 1 o 2), di cui ai capp. 8 e 9;

      e. la dichiarazione che per il dispositivo oggetto dell'Accertamento di Conformità, identificato esplicitamente tramite l'identificativo utilizzato nel TDS, non è applicabile la Decisione Europea 2003/511/CE [R02] relativa al soddisfacimento dei requisiti di sicurezza dell'Allegato III della Direttiva Europea 1999/93/CE [R03].

   ii. TDS relativo al dispositivo per cui si richiede l'Accertamento di Conformità;

   iii. evidenza della inapplicabilità della Decisione Europea 2003/511/CE;

   iv. evidenza che il TDS è adeguato, nel senso precisato al cap. 6, punto B. (per una guida alla produzione della evidenza richiesta si veda il Documento di Supporto [R05]);

   v. copia del versamento a titolo di acconto, effettuato secondo le modalità indicate nel Documento di Supporto.

8 Procedura in Modalità 1

A. L’attivazione della Procedura richiede i seguenti elementi:

   i. i materiali di cui al cap. 7;

   ii. il Certificato di cui al cap. 5, punto A.ii.

B. La Procedura consiste di una sola fase della durata massima prevista di sette mesi a partire dall’attivazione, al termine della quale si rilascia l’Attestato di Conformità o la motivazione per il mancato rilascio.

C. Nei casi in cui l’OCSI, nel corso dell'analisi degli elementi di cui al punto A., riscontri che questi risultano insufficienti per esprimersi sull’adeguatezza della certificazione in oggetto, potrà richiedere la loro integrazione con ulteriori evidenze. In tali casi l'OCSI si riserva la facoltà di ridefinire i tempi per l'applicazione della Procedura, la cui conclusione potrà eccedere la durata prevista.

D. L’OCSI è disponibile, su richiesta del soggetto richiedente e per uno specifico dispositivo, ad applicare la Procedura in modalità 1 anche in assenza del Certificato, purché il relativo processo di certificazione sia prossimo alla conclusione. In tal caso il Certificato dovrà comunque essere consegnato all'OCSI entro sei mesi dall'attivazione della Procedura. L’OCSI si riserva di definire una gestione adeguata del mancato rispetto di questo termine.

9 Procedura in Modalità 2

A. L'attivazione della Procedura richiede i materiali di cui al cap. 7.

B. La Procedura richiede la consegna del Certificato, di cui al cap. 5, punto A.ii., entro trenta mesi dall'attivazione. L'OCSI si riserva di definire una gestione adeguata del mancato rispetto di questo termine di scadenza.

C. La Procedura consiste di una prima fase della durata massima prevista di sei mesi a partire dall'attivazione, al termine della quale l'OCSI emetterà un Pronunciamento Positivo o Negativo circa l'adeguatezza, ai fini dell'Accertamento di Conformità, degli elementi di cui al punto A.

D. Nei casi in cui l'OCSI, nel corso dell'analisi degli elementi di cui al punto A., riscontri che questi risultano insufficienti per emettere il Pronunciamento, potrà richiedere la loro integrazione con ulteriori evidenze. In tali casi l'OCSI si riserva la facoltà di ridefinire i tempi per l'applicazione della prima fase della Procedura, la cui conclusione potrà eccedere la durata prevista.

E. In caso di emissione di Pronunciamento Negativo, la Procedura termina. Si noti che un Pronunciamento Negativo è accompagnato dalle motivazioni per la sua emissione.

F. In caso di emissione di Pronunciamento Positivo, la Procedura prosegue con una seconda fase che inizia alla data di consegna del Certificato di cui al punto B. Si noti che un Pronunciamento Positivo è accompagnato dalle condizioni per la sua validità ai fini della seconda fase. In particolare, la sostanza del TDS rilevante per l'accertamento viene congelata dal Pronunciamento Positivo (vedi anche punto I.)

G. La seconda fase della Procedura ha una durata massima prevista di un mese e termina con il rilascio dell'Attestato di Conformità o delle motivazioni per il mancato rilascio.

H. Nei casi in cui l'OCSI, anche sulla base delle condizioni di validità di cui al punto F., ritenga gli elementi di cui ai punti A. e B. insufficienti per esprimersi sull'adeguatezza della certificazione in oggetto, potrà richiedere la loro integrazione con ulteriori evidenze. In tali casi l'OCSI si riserva la facoltà di ridefinire i tempi per l'applicazione della Procedura, la cui conclusione potrà eccedere la durata prevista.

I. Si noti che l'emissione di un Pronunciamento Positivo non garantisce che il TDS incluso nei materiali soggetti a Pronunciamento sia approvato nell'ambito del processo di certificazione di interesse ed esiste la possibilità che ai fini del processo di certificazione si richiedano modifiche del TDS stesso. L'OCSI è disponibile, con modalità definite caso per caso, a interagire con il processo di certificazione per minimizzare il rischio che, tentando di raggiungere

separatamente gli obiettivi del Processo di Accertamento e quelli del processo di certificazione, si producano effetti negativi per il richiedente l'accertamento.

10 Caratteristiche dell'Attestato di Conformità

A. Nell'Attestato di Conformità si specificano:

   i. l'ambito dell'Accertamento di Conformità stesso (DPCM 10 febbraio 2010 [R01]);

   ii. il dispositivo di riferimento, tramite identificativo utilizzato nel TDS;

   iii. il TDS e il Certificato di riferimento, tramite i loro identificativi ufficiali di certificazione *Common Criteria*;

   iv. la modalità della Procedura utilizzata (modalità 1 o 2);

   v. il riferimento univoco al relativo Rapporto di Accertamento di cui al punto B.;

   vi. la data di rilascio dell'Attestato di Conformità.

B. All'Attestato di Conformità è associato il Rapporto di Accertamento contenente le ipotesi di rilascio dell'Attestato di Conformità stesso e tutte le informazioni integrative necessarie per ottenere un quadro completo dell'accertamento eseguito (per maggiori dettagli si veda il Documento di Supporto [R05]).

11 Registro degli Accertamenti

A. L'OCSI mantiene un registro pubblicamente consultabile contenente la lista dei dispositivi per i quali è stato rilasciato l'accertamento.