Ministero dello Sviluppo Economico

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 e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

OCSI/ACC/01/2016/PROC

Versione 1.0

21 dicembre 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	21/12/2016

2 Indice

1 Revisioni del documento 3
2 Indice 4
3 Elenco degli acronimi 5
4 Riferimenti 6
5 Premessa 8
6 Introduzione all'Accertamento di Conformità 9
7 Adeguatezza della certificazione Common Criteria 11
8 Attivazione della Procedura di Accertamento di Conformità 13
9 Procedura in Modalità 1 14
10 Procedura in Modalità 2 15
11 Caratteristiche dell'Attestato di Conformità 16
12 Registro degli Accertamenti 17

3 Elenco degli acronimi

EAL Evaluation Assurance Level

HSM Hardware Security Module

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PP Profilo di Protezione (Protection Profile)

SCD Signature Creation Data

TDS Traguardo di Sicurezza (Security Target)

USB Universal Serial Bus

4 Riferimenti

[R01] “Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014.

[R02] Decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179, G.U. n. 214 del 13 settembre 2016.

[R03] CCRA, “Common Criteria Recognition Arrangement”, 2 luglio 2014.

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

[R05] CCMB-2009-07-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 3, July 2009.

[R06] CCMB-2009-07-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 3, July 2009.

[R07] CCMB-2009-07-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 3, July 2009

[R08] “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.

[R09] Legge 7 agosto 1990, n. 241, “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, G.U. n. 19, 18 agosto 1990 e s.m.i.

[R10] “Decisione di esecuzione (UE) 2016/650 della Commissione, del 25 aprile 2016, che stabilisce norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno”, Gazzetta ufficiale dell’Unione Europea L 109/40, 26 aprile 2016.

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

[R12] “SOGIS Portal”, <www.sogisportal.eu>.

[R13] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.1.1 (2014-11).

[R14] “OCSI – Organismo di certificazione della Sicurezza Informatica”, <www.ocsi.isticom.it>

5 Premessa

A. L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014 sull'identità digitale – eIDAS (*Electronic IDentification, Authentication and Signature*) [R01] (nel seguito indicato come "Regolamento eIDAS") e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica qualificata e di un sigillo elettronico qualificato ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento eIDAS.

B. L'affidamento all'OCSI dell'accertamento di cui sopra è specificato dal comma 5 dell'articolo 35 del decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179 [R02].

C. La Procedura di Accertamento in oggetto si applica a tutti i dispositivi per la creazione di una firma elettronica qualificata e di un sigillo elettronico qualificato (nel seguito indicati per brevità come "dispositivi di firma" o "dispositivi"), così come definiti all'articolo 3 del Regolamento eIDAS, e copre tutti i casi previsti al comma 3 dell'articolo 30 dello stesso Regolamento.

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

E. 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 II al Regolamento eIDAS.

F. Condizione necessaria ma non sufficiente per l'adeguatezza di cui al punto E è che la certificazione di sicurezza sia ottenuta secondo lo standard di valutazione noto come *Common Criteria* [R04] (ISO/IEC 15408).

G. La presente 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 [R14], nella sezione "Dispositivi di firma", la versione aggiornata della Procedura, mantenendo l'archivio storico delle versioni precedenti.

H. Per determinare i costi della Procedura di Accertamento dovuti all'OCSI, si applica il Decreto Interministeriale del 15 febbraio 2006 [R08].

I. L'applicazione della Procedura di Accertamento è regolata dalla vigente normativa Italiana in materia di procedimento amministrativo [R09].

6 Introduzione all'Accertamento di Conformità

A. Sulla base di quanto indicato nella Decisione di esecuzione (UE) 2016/650 [R10], si prevedono due tipologie principali di dispositivi di firma:

   i. **Dispositivi di Tipo 1**: i dispositivi utilizzabili in un ambiente gestito integralmente, ma non necessariamente in via esclusiva, dal titolare delle chiavi di firma (ad es. *smartcard*, *token* USB e simili);

   ii. **Dispositivi di Tipo 2**: i dispositivi gestiti per conto dell'utilizzatore (firmatario o creatore di un sigillo) da un prestatore di servizi fiduciari qualificati (ad es. HSM o server di firma nei quali sono custoditi in maniera sicura i dati per la creazione delle firme o dei sigilli e ai quali l'utilizzatore accede da remoto, previa autenticazione).

B. Per entrambe le tipologie di dispositivi di cui al punto precedente è richiesta una certificazione *Common Criteria* ritenuta adeguata dall'OCSI.

C. 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.

D. Ai fini del soddisfacimento dei requisiti di sicurezza dell'Allegato II al Regolamento eIDAS [R01], la Procedura di Accertamento in oggetto definisce i requisiti fondamentali per il TDS (cap. 7, punti A, B e C) e per il riconoscimento del Certificato (cap. 7, punto D).

E. L'OCSI è disponibile, su richiesta, a considerare la possibilità di adattamento dei vincoli di cui al punto D 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. 11, punto B.

F. All'adeguatezza di un TDS concorrono congiuntamente:

   i. la caratterizzazione di sicurezza dell'ODV;

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

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

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

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 C.ii;

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

H. Le caratteristiche dell'Attestato di Conformità sono indicate nel cap. 11.

I. 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 si conclude con il rilascio dell'Attestato di Conformità ovvero con la comunicazione del mancato rilascio con addotte le relative motivazioni.

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 e prevede una prima fase che si conclude con un Pronunciamento preliminare (Positivo o Negativo) sul materiale analizzato. In caso di Pronunciamento Positivo si prevede una seconda fase, da avviare alla consegna del Certificato, che si conclude con il rilascio dell'Attestato di Conformità ovvero con la comunicazione del mancato rilascio con addotte le relative motivazioni.

7 Adeguatezza della certificazione Common Criteria

A. Per i **Dispositivi di Tipo 1** di cui al cap. 6, punto A.i, ai fini dell'Accertamento di Conformità il TDS deve dichiarare conformità ad uno o più, a seconda delle necessità, dei *Protection Profile* (PP) indicati nell'Allegato alla Decisione di esecuzione (UE) 2016/650 [R10].

B. Per i **Dispositivi di Tipo 2** di cui al cap. 6, punto A.ii, ai fini dell'Accertamento di Conformità il TDS deve soddisfare i seguenti requisiti di adeguatezza:

   i. la versione di riferimento dei *Common Criteria* non deve essere inferiore alla 3.1, Revision 3 ([R05], [R06], [R07]);

   ii. il TDS deve essere conforme al livello di garanzia (*assurance package*) EAL4 con l'aggiunta (*augmentation*) della componente AVA_VAN.5;

   iii. gli obiettivi di sicurezza dell'ODV, congiuntamente agli obiettivi di sicurezza dell'ambiente operativo, devono garantire il soddisfacimento dei requisiti di sicurezza dell'Allegato II al Regolamento eIDAS [R01];

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

   v. con riferimento al punto precedente, l'ODV deve includere al suo interno la funzionalità di generazione delle chiavi di firma (SCD);

   vi. ai fini del soddisfacimento del requisito 1, lettera d) dell'Allegato II al Regolamento eIDAS, l'ODV deve contenere specifiche funzioni di sicurezza che, unitamente alle ipotesi e agli obiettivi di sicurezza per l'ambiente operativo, contribuiscono a garantire il "controllo esclusivo" del firmatario sull'uso delle chiavi di firma (SCD) di cui è titolare;

   vii. nel caso di un dispositivo multi-utente e multi-chiave (ossia il dispositivo gestisce SCD multipli, attribuiti a diversi titolari) l'ODV deve prevedere meccanismi di identificazione, autenticazione e controllo di accesso "user-based", descritti nel TDS in forma di obiettivi per l'ODV ed SFR, che gli consentano di:

      a. distinguere gli utenti firmatari da altri utenti autorizzati (ad es. utenti amministratori);

      b. distinguere i diversi utenti firmatari;

      c. associare in maniera univoca ed esclusiva gli SCD ai loro legittimi titolari e consentire l'accesso agli SCD per l'operazione di firma esclusivamente ai legittimi titolari.

C. Per tutti i tipi di dispositivi, ai fini dell'Accertamento di Conformità le funzioni di sicurezza di tipo crittografico dell'ODV descritte nel TDS devono utilizzare algoritmi

crittografici, lunghezze di chiavi, funzioni *hash*, protocolli e parametri conformi a ETSI TS 119 312 V1.1.1 [R13] e successive edizioni.

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

   i. il Certificato è emesso dallo Schema Italiano (OCSI);

   ii. il Certificato è emesso da uno Schema partecipante all'accordo CCRA [R03] con il ruolo di *Certificate Authorizing Scheme* (l'elenco è disponibile sul portale dei *Common Criteria* [R04], nella sezione "Certificate Authorizing Schemes");

   iii. il Certificato è emesso da uno Schema partecipante all'accordo SOGIS-MRA [R11] con lo status di *Qualified/Authorising Participant* (l'elenco degli Schemi partecipanti, con il relativo status, è disponibile sul portale del SOGIS [R12], nella sezione "Status of Participants").

E. Con riferimento al punto precedente, si precisa che, in considerazione della particolare natura tecnologica dei dispositivi di firma e dello specifico ambito normativo di riferimento (Regolamento eIDAS), l'OCSI ha stabilito di riconoscere, esclusivamente ai fini dell'Accertamento di Conformità di tali dispositivi, certificati Common Criteria senza limitazioni sul livello di garanzia in deroga alle regole per il mutuo riconoscimento imposte dagli accordi di cui ai punti D.ii e D.iii.

8 Attivazione della Procedura di Accertamento di Conformità

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

   i. Richiesta di Accertamento di Conformità, redatta utilizzando l'apposito modulo, disponibile sul sito Web istituzionale dell'OCSI [R14], nella sezione "Dispositivi di firma", nella quale vanno specificati:

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

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

      c. la modalità della Procedura di Accertamento che si intende attivare (modalità 1 o 2), di cui ai capp. 9 e 10;

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

B. Entro 30 giorni dalla ricezione della Richiesta di Accertamento di Conformità, l'OCSI effettua un esame preliminare dei materiali consegnati allo scopo di verificarne la completezza e l'idoneità ai fini della Procedura. In caso di esito positivo, l'OCSI invia al richiedente un preventivo in cui sono specificati la durata minima prevista, l'impegno del personale OCSI e il costo della Procedura, calcolato in base al Decreto Interministeriale del 15 febbraio 2006 [R08].

C. Nel caso in cui l'OCSI rilevi la presenza di potenziali problemi nei materiali consegnati, provvede ad informare il richiedente, specificando le motivazioni che rendono la Richiesta di Accertamento non accoglibile e richiedendo le necessarie integrazioni e correzioni.

D. La Procedura si attiva con la ricezione del preventivo firmato per accettazione dal richiedente corredato, ove previsto, dalla prova del versamento dell'acconto, effettuato secondo le modalità indicate nel preventivo stesso.

E. I termini massimi per l'applicazione della Procedura sono indicati, per le due modalità previste, rispettivamente nei capp. 9 e 10.

9 Procedura in Modalità 1

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

   i. i materiali di cui al cap. 8;

   ii. il Certificato di cui al cap. 6, punto C.ii.

B. La Procedura consiste in una sola fase della durata massima di 180 giorni a decorrere dall’attivazione, durante la quale l’OCSI analizza i materiali presentati al fine di verificare il soddisfacimento dei requisiti di sicurezza dell’Allegato II al Regolamento eIDAS. Al termine di questa fase l’OCSI rilascia l’Attestato di Conformità ovvero la comunicazione del mancato rilascio con addotte le relative motivazioni.

C. Nei casi in cui l’OCSI, nel corso dell'analisi degli elementi di cui al punto A, riscontri che i suddetti elementi risultano insufficienti per esprimersi sull’adeguatezza della certificazione in oggetto, potrà richiedere la loro integrazione con ulteriori evidenze. Tale richiesta sospende, fino al relativo esito, il decorso dei termini per l'applicazione della Procedura specificati nel preventivo.

10 Procedura in Modalità 2

A. L’attivazione della Procedura richiede i materiali di cui al cap. 8.

B. La Procedura consiste in una prima fase della durata massima di 180 giorni a decorrere dall’attivazione, durante la quale l’OCSI analizza i materiali presentati al fine di verificare il soddisfacimento dei requisiti di sicurezza dell’Allegato II al Regolamento eIDAS. Al termine di questa fase l’OCSI emette un Pronunciamento Positivo o Negativo in merito all’adeguatezza, ai fini dell’Accertamento di Conformità, degli elementi di cui al punto A.

C. Nell’ipotesi in cui l’OCSI, nel corso dell'analisi degli elementi di cui al punto A, riscontri che i suddetti elementi risultano insufficienti ai fini dell’adozione di un Pronunciamento (Positivo o Negativo), potrà richiederne l’integrazione con ulteriori evidenze. La suddetta richiesta sospende, fino al relativo esito, il decorso dei termini per l'applicazione della Procedura specificati nel preventivo.

D. In caso di Pronunciamento Negativo, la Procedura termina. Nel Pronunciamento Negativo sono trascritte le motivazioni che non hanno consentito il rilascio dell’Attestato di Conformità.

E. In caso di Pronunciamento Positivo, la Procedura prevede una seconda fase che decorre dalla data di consegna del Certificato di cui al cap. 6, punto C.ii. Il Pronunciamento Positivo è accompagnato dalle condizioni per la sua validità ai fini dell’avvio della seconda fase. In particolare, tutti gli elementi del TDS ritenuti rilevanti ai fini dell’Accertamento di Conformità si intendono congelati dal Pronunciamento Positivo.

F. La seconda fase della Procedura ha una durata massima di 30 giorni durante i quali l’OCSI verifica la rispondenza della versione certificata del TDS alle condizioni di validità di cui al punto E. Al termine di questa fase l’OCSI rilascia l’Attestato di Conformità ovvero la comunicazione del mancato rilascio con addotte le relative motivazioni.

11 Caratteristiche dell'Attestato di Conformità

A. Nell'Attestato di Conformità si specificano:

   i. l'ambito dell'Accertamento di Conformità stesso (Regolamento eIDAS [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 condizioni e le ipotesi per la validità dell'Attestato di Conformità stesso e tutte le informazioni integrative necessarie per ottenere un quadro completo dell'accertamento eseguito.

12 Registro degli Accertamenti

A. L'OCSI mantiene un registro pubblicamente consultabile contenente la lista dei dispositivi per i quali è stato rilasciato l'accertamento, disponibile sul proprio sito Web istituzionale [R14], nella sezione "Dispositivi di firma".