Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)
Organismo designato, ai sensi del comma 4 dell'articolo 3 della Direttiva 1999/93/CE sulla firma elettronica, e notificato, ai sensi del punto b) del comma 1 dell'articolo 11 della Direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma ai requisiti di sicurezza espressi nell'Allegato III alla suddetta direttiva.

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

Attestato di Conformità n. 2/14

Dispositivo: CoSign v7.1

Sviluppato da: ARX

Il dispositivo per la creazione di firme elettroniche indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE

Il Direttore
(Dott.ssa Rita Forsi)

Prima emissione: 10 settembre 2014
Revisione: 23 luglio 2015

Il presente Attestato di Conformità è stato emesso dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) in conformità al comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", modificato ed integrato dal DL 30 dicembre 2010, n. 235.
La validità del presente Attestato di Conformità è soggetta alle condizioni e alle ipotesi esplicitate nel Rapporto di Accertamento (OCSI/ACC/ARX/01/2010/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

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 Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE

Rapporto di Accertamento

ARX CoSign v7.1

OCSI/ACC/ARX/01/2010/RA

Versione 1.1

23 luglio 2015

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	30/09/2014
1.1	OCSI	Revisione	23/07/2015

2 Indice

3 Elenco degli acronimi

CC Common Criteria

DL Decreto Legislativo

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

OCSI Organismo di Certificazione della Sicurezza Informatica

ODV Oggetto della Valutazione

PP Profilo di Protezione (Protection Profile)

SSCD Secure Signature Creation Device

TDS Traguardo di Sicurezza (Security Target)

TLS Transport Layer Security

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, G.U. n. 112 del 16 maggio 2005, Suppl. Ordinario n. 93, recante "Codice dell'amministrazione digitale", modificato ed integrato dal decreto legislativo 30 dicembre 2010, n. 235, G.U. n. 6 del 10 gennaio 2010, Suppl. Ordinario n. 8

[CD] "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, July 15, 2003.

[DEL] **"**Deliberazione CNIPA n. 45 del 21 maggio 2009, modificata dalla Determinazione DigitPA n. 69 del 28 luglio 2010", G.U. n. 191 del 17 agosto 2010

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

[DPCM] 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".

[DS] "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.

[PR] "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.

[RC] Rapporto di Certificazione, "ARX CoSign v.7.1", OCSI/CERT/IMQ/01/2011/RC, versione 1.1, 23 luglio 2015

[RT] **"**Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", DPCM del 22 febbraio 2013, G.U. n. 117 del 21 maggio 2013

[TDS] ARX CoSign Security Target, v.1.19, 15 June 2015

5 Ambito dell'Accertamento di Conformità

L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 4 dell'articolo 3 della Direttiva 1999/93/CE sulla firma elettronica [DIR] (nel seguito indicata come Direttiva), e notificato, ai sensi del punto b) del comma 1 dell'articolo 11 della Direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma ai requisiti di sicurezza espressi nell'Allegato III alla suddetta direttiva.

L'affidamento all'OCSI dell'accertamento di cui sopra è specificato dal comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" [CAD], modificato ed integrato dal DL 30 dicembre 2010, n. 235.

L'oggetto dell'Accertamento di Conformità è il dispositivo denominato "CoSign v7.1", prodotto dalla società ARX (nel seguito indicato come CoSign o "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Al dispositivo si applica, alla data di avvio della procedura di Accertamento (vedi cap. 6.2), 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" [DPCM].

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

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo denominato “CoSign v7.1”, prodotto dalla società ARX, ed è finalizzato a fornire indicazioni ai potenziali acquirenti ed utilizzatori di tale dispositivo circa la sua conformità ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per l'apposizione di firme elettroniche qualificate (automatiche e remote).

L'Accertamento è stato condotto dall’OCSI in accordo a quanto indicato nei documenti di riferimento “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 [PR] (nel seguito indicata come Procedura) e “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 [DS] (nel seguito indicato come Documento di Supporto).

In particolare, poiché all'avvio della Procedura di Accertamento non era ancora disponibile il Certificato Common Criteria né risultava avviato il relativo processo di Certificazione, è stata applicata la Procedura in Modalità 2. Pertanto, in una prima fase, l'OCSI ha esaminato il Traguardo di Sicurezza del dispositivo, emettendo il Pronunciamento positivo sulla sua adeguatezza in data 13 settembre 2010.

In data 31 ottobre 2011, veniva avviato presso lo stesso OCSI il Processo di valutazione e certificazione CC: le attività di valutazione da parte dell'LVS si sono concluse con esito positivo il 25 giugno 2014, mentre il Rapporto di Certificazione e il relativo Certificato CC sono stati rilasciati dall'OCSI il 10 settembre 2014.

Successivamente, in seguito alla sostituzione, da parte del Fornitore ARX, del modello di chip usato come generatore hardware di numeri casuali, è stato necessario procedere a una ri-valutazione dell'ODV da parte dello stesso LVS, che ha confermato i risultati della precedente valutazione.

Pertanto, l’OCSI ha provveduto a revisionare il Rapporto di Certificazione e conseguentemente a emettere, in data 23 luglio 2015, anche la versione aggiornata del presente Rapporto di Accertamento.

Si noti che la modifica effettuata ha comportato anche la revisione del Traguardo di Sicurezza [TDS]. Gli utenti della precedente versione dell’ODV sono quindi invitati a prendere visione anche del nuovo TDS.

Il dispositivo oggetto dell'Accertamento, così come descritto nel relativo Traguardo di Sicurezza [TDS], è risultato quindi conforme ai requisiti di sicurezza espressi nell’Allegato III alla Direttiva, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura, ovvero ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per l'apposizione di firme elettroniche qualificate (automatiche e remote).

Il presente Rapporto di Accertamento deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto e al relativo Rapporto di Certificazione [RC].

La validità dell'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento è soggetta alle condizioni e alle ipotesi esplicitate nel presente Rapporto di Accertamento (vedi cap. 7), che ne costituisce parte integrante e sostanziale.

Il rilascio dell'Attestato di Conformità da parte dell'OCSI non rappresenta alcun tipo di sostegno o promozione all'uso del dispositivo accertato da parte di questo Organismo.

6.2 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	ARX
Nome del dispositivo	CoSign
Versione del dispositivo	7.1
Traguardo di Sicurezza	ARX CoSign Security Target, v.1.19, 15 June 2015
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Versione dei CC	3.1 Rev.2
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	26 febbraio 2010
Data di inizio della valutazione	31 ottobre 2011
Data di fine della valutazione	25 giugno 2014
Data di inizio della ri-valutazione	15 giugno 2015
Data di fine della ri-valutazione	15 luglio 2015
Data di rilascio Certificato CC	10 settembre 2014
Data di rilascio Accertamento	30 settembre 2014
Data di revisione Certificato CC	23 luglio 2015
Data di revisione Accertamento	23 luglio 2015

6.3 Descrizione del dispositivo accertato

Il dispositivo "CoSign v7.1" (nel seguito anche indicato semplicemente come CoSign), è un dispositivo progettato per essere utilizzato come "Dispositivo sicuro di firma elettronica (Secure Signature-Creation Device, SSCD)" all'interno di un'organizzazione, fisicamente installato in un ambiente sicuro nel data-center dell'organizzazione e connesso alla rete dell'organizzazione stessa.

Il dispositivo certificato (ODV) è costituito da un apparato fisico e da svariati moduli software che consentono agli utenti di connettersi al dispositivo da remoto ed effettuare operazioni di firma. L'accesso all'apparato CoSign è possibile attraverso l'applicativo CoSign client, installato sulla postazione dell'utente finale, che consente di instaurare una sessione TLS tra il client e l'apparato stesso. È anche possibile accedere all'apparato CoSign mediante l'interfaccia REST (Representational State Transfer), tramite un REST-based client, che permette all'utente Firmatario di effettuare le stesse operazioni eseguibili mediante l'applicativo CoSign client, sempre attraverso una sessione TLS. Nel seguito, ogni riferimento al CoSign client sottintende il riferimento anche al REST-based client.

Un singolo dispositivo può gestire in modo sicuro molti utenti, e per ogni account di utente è possibile generare diverse chiavi di firma e i relativi certificati.

Tre diverse tipologie di utenti sono autorizzate ad operare sull'ODV: l'utente semplice (*Firmatario*) e due diversi profili di utente amministratore:

- *Appliance Administrator*: installa il dispositivo e ne gestisce le funzionalità;
- *Users Administrator*: gestisce gli account degli utenti.

Ad ogni utente Firmatario è fornito un dispositivo OTP (One Time Password) univocamente identificato e univocamente associato ad un utente. Un firmatario si autentica fornendo una password statica e una password dinamica che viene visualizzata sul display del dispositivo OTP. Quando un utente desidera firmare digitalmente un documento, il CoSign client apre una sessione utente protetta utilizzando un canale di comunicazione sicuro dedicato realizzato tramite il protocollo TLS v.1.0. Questo canale sicuro è utilizzato per ogni comunicazione tra il CoSign client e il dispositivo CoSign.

CoSign registra in un audit log ciclico tutte le attività amministrative e ogni utilizzo di una qualsiasi chiave di firma di un utente. L'audit log non può essere cancellato e può essere letto da un amministratore autorizzato.

Le funzioni di sicurezza implementate dall'ODV sono:

- Controllo d'accesso
- Identificazione e autenticazione
- Operazioni crittografiche
- Audit di sicurezza
- Comunicazioni sicure e gestione delle sessioni
- Rilevamento delle manomissioni
- Self test

Per maggiori informazioni sulle caratteristiche dell'ODV e sulla sua politica di sicurezza si faccia riferimento al Traguardo di Sicurezza [TDS] e al Rapporto di Certificazione [RC].

6.3.1 Configurazioni valutate dell'ODV

Il Traguardo di Sicurezza del dispositivo CoSign descrive due diverse possibili configurazioni:

1) PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (HA-PRI-REPL-INC-SIGKEY)

2) ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (HA-ALT-REPL-INC-SIGKEY)

Le due configurazioni permettono di utilizzare l'ODV in **Alta Disponibilità con replica delle chiavi private del firmatario**: nell'ambiente operativo è installato un solo dispositivo PRIMARY in configurazione HA-PRI-REPL-INC-SIGKEY e uno o più dispositivi ALTERNATE in configurazione HA-ALT-REPL-INC-SIGKEY.

Per ulteriori dettagli si rimanda a [TDS], par. 1.3.2.

7 Condizioni di validità dell'Attestato di Conformità

L'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento deve essere ritenuto valido ed efficace unicamente sotto le seguenti ipotesi:

i. la certificazione di sicurezza ottenuta (v. [RC]) è in corso di validità, ovvero il Certificato non è stato revocato;

ii. il dispositivo reale è conforme a quello certificato e descritto nel TDS;

iii. l'ambiente di utilizzo reale del dispositivo è conforme a quello descritto nel TDS;

iv. sono rispettate tutte le condizioni aggiuntive di utilizzo del dispositivo riportate nel cap. 8 del presente Rapporto di Accertamento.

La violazione dell'ipotesi (i) comporta la perdita di validità dell'Attestato di Conformità.

La violazione di una o più delle ipotesi (ii), (iii) e (iv) ha come conseguenza la perdita di efficacia dell'Attestato di Conformità, che mantiene comunque la sua validità.

Eventuali situazioni che comportano la perdita di validità del presente Attestato di Conformità, siano esse rilevate direttamente dall'Organismo di Certificazione (OCSI) emettitore o portate a conoscenza di quest'ultimo da soggetti esterni, saranno rese note ai soggetti interessati attraverso i canali di informazione ufficiali dell'Organismo stesso.

Nel caso si verifichino situazioni che comportano la perdita di efficacia del presente Attestato, sarà cura dell'ente preposto alla vigilanza sui prestatori di servizi di firma elettronica qualificata provvedere alle misure correttive necessarie.

8 Condizioni di utilizzo del dispositivo accertato

Il dispositivo CoSign deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS] e nel Rapporto di Certificazione [RC].

In particolare, la consegna, l'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo devono avvenire in accordo agli obiettivi di sicurezza indicati in [TDS] e seguendo le indicazioni riportate anche in [RC], cap. 8 Appendice A.

Inoltre, per quanto riguarda l'uso del dispositivo in conformità alla vigente normativa italiana in materia di firma elettronica, si raccomanda di porre particolare attenzione ai seguenti aspetti:

- **Algoritmi crittografici**: per quanto riguarda le funzioni di hash, la generazione di coppie di chiavi crittografiche e i metodi di sottoscrizione, fare riferimento a quanto indicato nella Deliberazione CNIPA n. 45/2009, modificata dalla Determinazione DigitPA n. 69/2010 [DEL].

- **Backup e ripristino di chiavi di sottoscrizione**: quanto alla possibilità di esportare chiavi private al di fuori del dispositivo di firma, esclusivamente per motivi di ripristino in caso di guasto o di aggiornamento del dispositivo in uso, nonché per la conservazione delle chiavi esportate, assicurarsi di rispettare quanto prescritto dalle "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" ([RT], art. 8, comma 3).

- **Configurazione ad alta affidabilità**: per quanto riguarda la possibilità di realizzare una configurazione ad alta affidabilità del dispositivo di firma, prevista nella configurazione certificata (cfr. par. 6.3.1), assicurarsi di rispettare quanto prescritto dalle suddette regole tecniche ([RT], art. 8, comma 4).

Infine, considerato che la normativa di riferimento in materia di firma elettronica è soggetta a naturali aggiornamenti o modifiche nel tempo, si raccomanda di seguirne l'evoluzione e di fare quindi riferimento all'ultima versione disponibile dei documenti sopra citati o delle loro eventuali integrazioni.