



Ministero dello Sviluppo Economico
Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione



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. 2/16

Dispositivo: CoSign v8.2

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)
Rita Forsi

Roma, 12 settembre 2016

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/01/2016/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota



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 v8.2

OCSI/ACC/ARX/01/2016/RA

Versione 1.0

12 settembre 2016

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	12/09/2016

2 Indice

1	Revisioni del documento	5
2	Indice.....	6
3	Elenco degli acronimi	7
4	Riferimenti	8
5	Ambito dell'Accertamento di Conformità.....	9
6	Riepilogo dell'accertamento	10
6.1	Introduzione	10
6.2	Descrizione del dispositivo accertato.....	10
6.3	Identificazione sintetica dell'accertamento.....	12
7	Condizioni di validità dell'Attestato di Conformità	13
8	Condizioni di utilizzo del dispositivo accertato.....	14

3 Elenco degli acronimi

CC	Common Criteria
DL	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
eIDAS	electronic IDentification Authentication and Signature
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
PP	Profilo di Protezione (Protection Profile)
QSCD	Qualified electronic Signature Creation Device
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 January 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
- [eIDAS] “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”, Official Journal L 257, 28 August 2014
- [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
- [RA] Rapporto di Accertamento, “ARX CoSign v7.5”, OCSI/CERT/IMQ/01/2015/RA, versione 1.0, 6 ottobre 2015
- [RC] Rapporto di Certificazione, “ARX CoSign v8.2”, OCSI/CERT/IMQ/04/2016/RC, versione 1.0, 12 settembre 2016
- [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, Version 2.6, Revision 2.6, ARX, 27 April 2016

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.

Si noti che, a decorrere dal 1° luglio 2016, con la definitiva entrata in vigore del Regolamento UE n. 910/2014 [eIDAS], la Direttiva 1999/93/CE è stata abrogata. Tuttavia, in base alle disposizioni transitorie del nuovo Regolamento (art. 51 comma 1) "i dispositivi sicuri per la creazione di una firma la cui conformità sia stata determinata a norma dell'articolo 3, paragrafo 4, della Direttiva 1999/93/CE sono considerati dispositivi per la creazione di una firma elettronica qualificata a norma del presente regolamento." Pertanto il dispositivo "CoSign v8.2", oggetto del presente Accertamento come Dispositivo sicuro per la creazione di firme elettroniche (SSCD), è da considerarsi anche un Dispositivo per la creazione di firme elettroniche qualificate (QSCD).

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 v8.2", 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. 6.3), 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].

Si noti che il dispositivo oggetto dell'Accertamento è una versione aggiornata del dispositivo denominato "CoSign v7.5", già accertato dall'OCSI (Attestato di Conformità n. 1/15 del 6 ottobre 2015 [RA]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore ARX, nonché all'adozione della Revision 4 dei Common Criteria Versione 3.1 ed all'aggiunta del componente di garanzia ATE_DPT.2, è stato necessario procedere a una ri-certificazione dell'ODV, i cui risultati sono riportati nel Rapporto di Certificazione [RC].

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente dispositivo, per facilità di lettura il presente Rapporto di Accertamento è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo dispositivo "CoSign v8.2".

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 v8.2”, 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).

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 Descrizione del dispositivo accertato

Il dispositivo “CoSign v8.2” è costituito dall'appliance CoSign progettata da ARX per essere utilizzata come Dispositivo sicuro di firma elettronica/firma elettronica qualificata (SSCD/QSCD) o come Dispositivo per la creazione di sigilli elettronici qualificati (Qualified Electronic Seal Creation Device).

Nel corso del presente Accertamento sono state considerate solo le configurazioni come SSCD/QSCD, tralasciando quella come Dispositivo per la creazione di sigilli elettronici qualificati, in quanto fuori dell'ambito dell'Accertamento stesso.

L'appliance CoSign è utilizzata all'interno di un'organizzazione, fisicamente installata in un ambiente sicuro nel data-center dell'organizzazione e connessa alla rete dell'organizzazione stessa.

Una singola appliance 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 l'appliance e ne gestisce le funzionalità;
- *Users Administrator*: gestisce gli account degli utenti.

Ad ogni utente Firmatario è fornito un dispositivo OTP (One Time Password) con un suo Profilo del dispositivo OTP univocamente associato. Il dispositivo OTP (OTP-Device) e il Profilo associato non fanno parte dell'ODV. 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, mediante il CoSign client o l'interfaccia REST, apre una sessione utente protetta utilizzando un canale di comunicazione sicuro dedicato realizzato tramite il protocollo TLS (v.1.0, 1.1 o 1.2). Questo canale sicuro è utilizzato per ogni comunicazione tra il client e l'appliance CoSign.

Nel caso di installazione dell'ODV come SSCD/QSCD è possibile configurare l'ODV per permettere all'utente di firmare, mediante il client CoSign, diversi documenti o transazioni, dopo una sola autenticazione a due fattori, entro un periodo di tempo fissato (configurabile fino ad un tempo massimo di 10 minuti equivalente a 600 secondi).

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].

6.2.1 Configurazioni valutate dell'ODV

Il Traguardo di Sicurezza del dispositivo CoSign v8.2 descrive quattro diverse possibili configurazioni, due delle quali realizzano un Dispositivo per la creazione di sigilli elettronici qualificati, e non sono state qui considerate in quanto fuori dell'ambito del presente Accertamento.

Si riportano quindi soltanto le due configurazioni del dispositivo “CoSign v8.2” installato come SSCD/QSCD:

- 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.

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	ARX
Nome del dispositivo	CoSign
Versione del dispositivo	8.2
Traguardo di Sicurezza	ARX CoSign Security Target, Version 2.6, Revision 2.6, ARX, 27 April 2016
Livello di garanzia	EAL4 con l’aggiunta di AVA_VAN.5, ALC_FLR.1 e ATE_DPT.2
Versione dei CC	3.1 Rev.4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della Procedura	29 febbraio 2016
Data di inizio della valutazione	29 febbraio 2016
Data di fine della valutazione	27 luglio 2016
Data di rilascio Certificato CC	12 settembre 2016
Data di rilascio Accertamento	12 settembre 2016

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 ([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 emittitore (OCSI) 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 verificano 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], 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. 6.2.1), 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.