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)

Certificato n. 2/14

(Certification No.)

Prodotto: **CoSign v.7.1**
(Product)

Sviluppato da: **ARX**
(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(AVA_VAN.5)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 10 settembre 2014

Common Criteria

SOGIS
IT SECURITY CERTIFIED

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

Rapporto di Certificazione

ARX CoSign v.7.1

OCSI/CERT/IMQ/01/2011/RC

Versione 1.0

10 settembre 2014

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	10/09/2014

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disk - Read-Only Memory
CEA	Certificate Enrollment Application
CEM	Common Evaluation Methodology
CGA	Certificate Generation Application
COTS	Commercial Off The Shelf
CSCI	Computer Software Configuration Item
CSP	Certificate Service Provider
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTBS/R	Data To Be Signed/Representation
EAL	Evaluation Assurance Level
HW	Hardware
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One Time Password
PP	Profilo di Protezione
RADIUS	Remote Authentication Dial-In User Service
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SFR	Security Functional Requirement

SSCD	Secure Signature-Creation Device
SVD	Signature Verification Data
SW	Software
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

4 Riferimenti

[ADM] ARX CoSign Administrator Guide, v.7.1, 23 March 2014

[CC1] CCMB-2006-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 1, September 2006

[CC2] CCMB-2007-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 2, September 2007

[CC3] CCMB-2007-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 2, September 2007

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, Version 1.0, May 2000

[CEM] CCMB-2007-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 2, September 2007

[CMS] ARX CoSign-ALC-CM Scope, v.1.19, 23 June 2014

[ETSI1] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”, ETSI TS102 176-1 V2.1.1 2011-07

[ETSI2] “Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices”, ETSI TS102 176-2 V1.2.1 2005-07

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[PRE] ARX CoSign Preparative Procedures, v.7.1, June 2014

[RFV] Rapporto Finale di Valutazione del prodotto “ARX CoSign v.7.1”, Versione 1.0, 25 giugno 2014

[TDS] ARX CoSign Security Target, v.1.18, 25 June 2014

[USR] ARX CoSign User Guide, v.7.1, March 2014

5 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto "CoSign v.7.1", sviluppato dalla società ARX.

La valutazione è stata di tipo concomitante, cioè effettuata durante lo sviluppo dell'ODV, ed è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo per la Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

6 Riepilogo della valutazione

6.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "CoSign v.7.1" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

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

6.2 Identificazione sintetica della certificazione

Nome dell'ODV	CoSign v.7.1
Traguardo di Sicurezza	ARX CoSign Security Target, v.1.18, 25 June 2014
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Fornitore	ARX
Committente	ARX
LVS	IMQ/LPS
Versione dei CC	3.1 Rev. 2
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	31 ottobre 2011
Data di fine della valutazione	25 giugno 2014

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

6.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "CoSign v.7.1" (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.

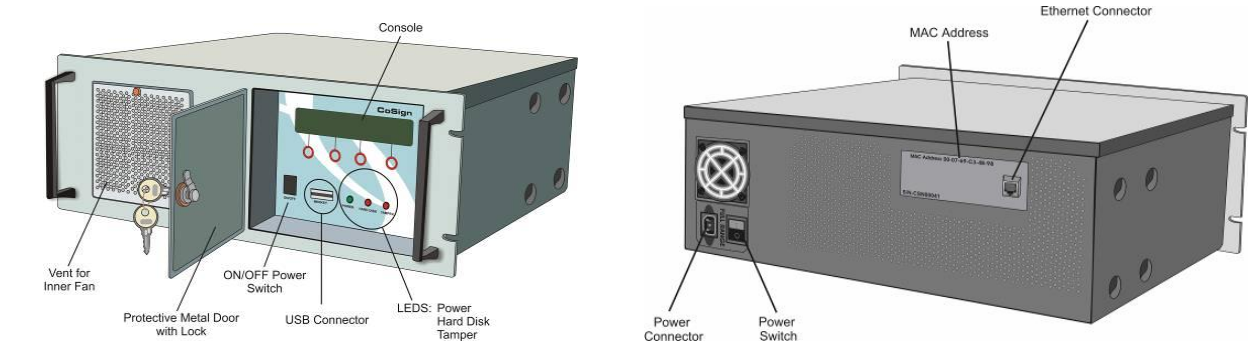

Figura 1 – Il dispositivo CoSign (fronte e retro)

Un singolo dispositivo può gestire in modo sicuro molti utenti, e per ogni account d'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.

Le funzionalità a disposizione degli amministratori sono descritte in [TDS], par. 1.4.2.2.4, mentre le funzionalità offerte ad utenti non di tipo amministrativo sono descritte in [TDS], par. 1.4.2.2.1.

Nella Figura 2 sono mostrate le entità esterne con cui interagisce l'ODV. Un firmatario interagisce usando il modulo software "CoSign client" per eseguire la registrazione dei certificati e per effettuare le operazioni di firma. L'amministratore interagisce con l'ODV per eseguire le varie attività amministrative previste.

Dal punto di vista della sicurezza, ad ogni utente è fornito un dispositivo OTP (One Time Password) univocamente identificato e univocamente associato ad un utente. Il dispositivo OTP e l'OTP RADIUS server non fanno parte dell'ODV.

Oltre all'OTP ed all'OTP RADIUS server, non fanno parte dell'ODV, ma sono da esso richiesti (maggiori dettagli in [TDS], par. 1.3.3): l'applicazione per la creazione della firma (SCA); l'applicazione per la registrazione dei certificati (CEA) e l'applicazione per la generazione dei certificati (CGA).

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.

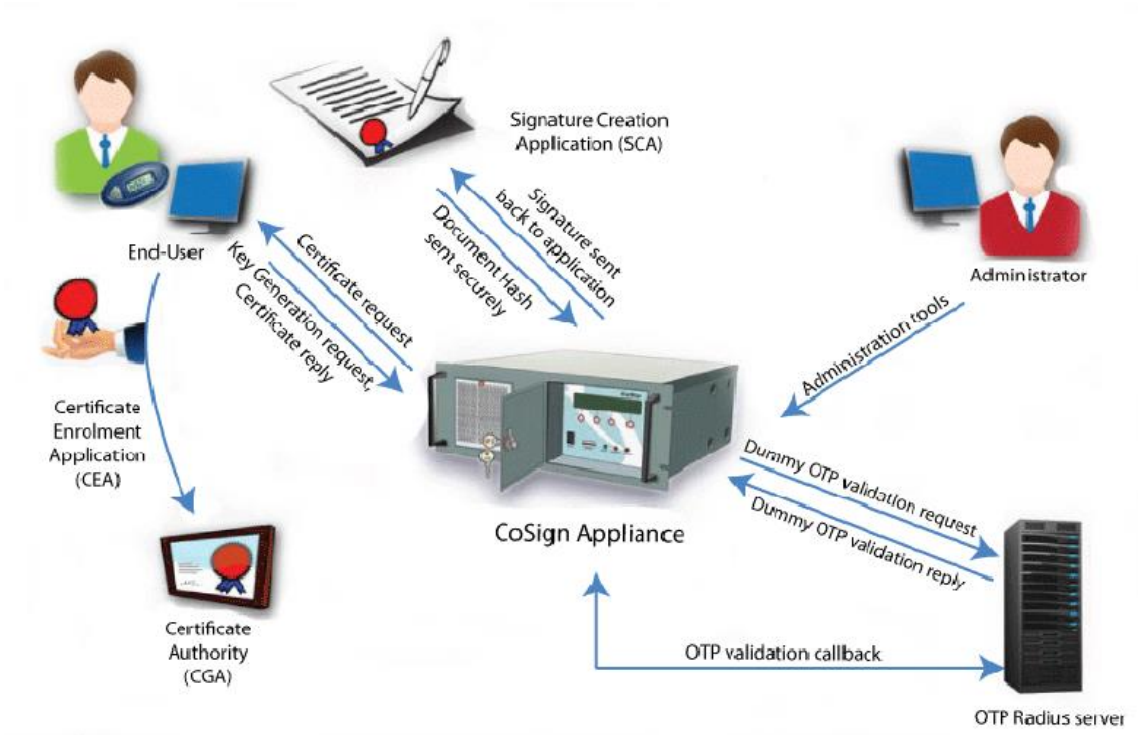

Figura 2 – Entità con cui si interfaccia il dispositivo CoSign

6.3.1 Architettura dell'ODV

6.3.1.1 Hardware

La descrizione dell'ambito fisico dell'ODV è fornita in [TDS], par. 1.4.2.1.

6.3.1.2 Software

La descrizione dell'ambito logico dell'ODV è fornita in [TDS], par. 1.4.2.2.

Il software di CoSign può trovarsi in uno dei seguenti stati:

- *Factory settings:* è lo stato in cui il prodotto arriva dalla fabbrica. Il prodotto non è ancora installato e non può essere utilizzato dagli utenti finali;
- *Operational State:* il prodotto è installato e pronto per gestire nuovi account utenti e per eseguire operazioni di firma digitale;
- *Tamper state:* il dispositivo è stato manomesso; in questo stato gli utenti finali non possono eseguire operazioni di firma digitale.

Nella Figura 3 è riportato il ciclo di vita dell'ODV. Maggiori dettagli sulla descrizione dei suddetti stati e delle operazioni permesse ad utenti ed amministratori nei diversi stati sono riportati in [TDS], par. 1.4.2.2.6.

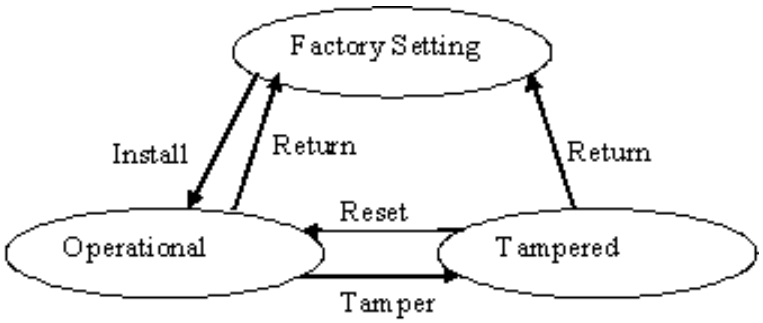

Figura 3 – Ciclo di vita del dispositivo CoSign

Le seguenti operazioni sono eseguite automaticamente da CoSign nello stato Operational:

- Tamper detection & protection (rilevamento manomissioni e protezione anti manomissione) in caso di apertura del coperchio del dispositivo. La protezione antimanomissione è garantita con il dispositivo sia acceso sia spento.
- Memorizzazione sicura delle chiavi di firma.
- Memorizzazione dei dati applicativi (certificati e immagini delle firme grafiche).

6.3.2 Caratteristiche di Sicurezza dell'ODV

6.3.2.1 Ipotesi

Le ipotesi definite nel Traguardo di Sicurezza [TDS] ed alcuni aspetti delle minacce e delle politiche di sicurezza organizzative non sono coperte direttamente dall'ODV stesso; ciò implica che specifici obiettivi di sicurezza debbano essere soddisfatti dall'ambiente operativo. In particolare in tale ambito i seguenti aspetti sono da considerare di rilievo:

- La CGA protegge l'autenticità del nome del firmatario e la chiave pubblica (SVD) nel certificato (qualificato) con una firma elettronica avanzata del Certificate Service Provider (CSP).
- Il firmatario utilizza solo una SCA affidabile; la SCA genera e invia la rappresentazione dei dati che il firmatario intende firmare (DTBS/R) in una forma appropriata per la firma da parte dell'ODV.
- Le guide di configurazione dell'ODV danno indicazioni chiare all'amministratore del dispositivo per consentirgli di verificare il rigoroso rispetto delle raccomandazioni incluse in [ETSI1], in tutti i casi in cui è richiesto, sulla robustezza delle funzioni hash e sulla resistenza nel tempo degli algoritmi di firma utilizzati.
- Le guide di configurazione dell'ODV danno indicazioni chiare all'amministratore del dispositivo al fine di garantire il rigoroso rispetto delle raccomandazioni incluse nell'ultima versione aggiornata di [ETSI2], in tutti i casi in cui è richiesto, o, in alternativa, al fine di verificare che sono applicate altre funzionalità crittografiche con livello di sicurezza equivalente.

- Si assume che l'ambiente operativo fornisca misure sufficienti per proteggere l'ODV da manomissioni fisiche che consentano accessi non autorizzati alla rete.

- Si assume che un amministratore autorizzato sia responsabile della conservazione in un luogo sicuro (cassaforte) di entrambi i token USB di backup generati durante l'installazione dell'ODV.

- Si assume che i dispositivi OTP vengano gestiti in modo sicuro dalla fase di produzione fino a quando il dispositivo OTP è consegnato al firmatario dall'organizzazione. Inoltre, si assume che le informazioni inerenti i dispositivi OTP siano gestite in maniera adeguata nell'OTP RADIUS Server, considerando anche lo stato dell'account di utente.

- Si assume che il firmatario manterrà il proprio dispositivo OTP sotto il suo controllo e ne segnalerà all'organizzazione l'eventuale perdita o manomissione, al fine di revocare l'account del firmatario stesso e il relativo dispositivo OTP.

- Si assume che tutti gli utenti dell'ODV siano sufficientemente addestrati per gestire l'ODV in modo sicuro. Si assume inoltre che gli amministratori dell'ODV siano fidati e sufficientemente addestrati per installare e configurare l'ODV e il suo ambiente operativo in modo sicuro. Ciò implica che gli amministratori dell'ODV sono anche responsabili per l'installazione, la configurazione e il funzionamento in modo sicuro del RADIUS Server.

6.3.2.2 Funzioni di sicurezza

Le funzioni di sicurezza implementate dall'ODV sono descritte in dettaglio in [TDS], par. 7. Di seguito sono riassunti alcuni aspetti ritenuti rilevanti:

- **Controllo d'accesso**: l'ODV autorizza l'accesso degli utenti assegnando i diritti in base al loro ruolo: Firmatario, Appliance Administrator e User Administrator.

- **Identificazione e autenticazione**: l'ODV identifica univocamente e autentica gli utenti. Gli amministratori si autenticano con una password statica: per alcune operazioni, come l'attivazione dell'account e le operazioni di generazione ed uso delle chiavi crittografiche, i firmatari si autenticano, oltre che con una password statica, anche con una dinamica (One Time Password).

- **Operazioni crittografiche**: l'ODV permette di effettuare operazioni crittografiche, quali generazione chiavi, firma digitale, verifica della firma, oltre che di gestione di chiavi a scopo di protezione dei dati dell'utente.

- **Audit di sicurezza**: l'ODV registra una serie di eventi relativi alla sicurezza; l'ODV permette all'Appliance Administrator di verificare i log registrati.

- **Comunicazioni sicure e gestione delle sessioni**: le comunicazioni tra ODV e RADIUS Server, tra ODV Primary e ODV Alternate e tra ODV e Client avvengono in modo sicuro, garantendo la confidenzialità e l'integrità dei dati trasmessi e la separazione delle sessioni d'utente.

- **Rilevamento delle manomissioni**: l'ODV implementa meccanismi di verifica dell'integrità del software e anti-tampering fisico.

- **Self test**: l'ODV fornisce una suite di test automatici di controllo eseguiti sia all'avvio sia durante la normale operatività, compresa la fase di creazione delle firme.

6.3.3 Configurazioni dell'ODV

Il Traguardo di Sicurezza di CoSign descrive 2 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 al [TDS], par. 1.3.2.

6.4 Documentazione

La documentazione specificata nel capitolo 8 (Appendice A) viene fornita al cliente finale insieme al prodotto. Questa documentazione contiene le informazioni richieste per l'installazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguiti gli ulteriori obblighi o note per l'utilizzo sicuro dell'ODV contenuti nel par. 7.2 di questo rapporto.

6.5 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione e le note applicative, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

Tutti gli SFR sono stati derivati direttamente o ricavati per estensione dai CC Parte 2 [CC2].

6.6 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement (CCRA).

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si

raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS IMQ/LPS.

L'attività di valutazione è terminata in data 25 giugno 2014 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 17 luglio 2014. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

6.7 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

7 Esito della valutazione

7.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "CoSign v.7.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Complete functional specification	ADV_FSP.4	Positivo
Implementation representation of the TSF	ADV_IMP.1	Positivo
Basic modular design	ADV_TDS.3	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Production support, acceptance procedures and automation	ALC_CMC.4	Positivo
Problem tracking CM coverage	ALC_CMS.4	Positivo

Classi e componenti di garanzia		Verdetto
Delivery procedures	ALC_DEL.1	Positivo
Identification of security measures	ALC_DVS.1	Positivo
Developer defined life-cycle model	ALC_LCD.1	Positivo
Well-defined development tools	ALC_TAT.1	Positivo
Test	**Classe ATE**	Positivo
Analysis of coverage	ATE_COV.2	Positivo
Testing: security enforcing modules	ATE_DPT.2	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing - sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Advanced methodical vulnerability analysis	AVA_VAN.5	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

7.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 5 - Dichiarazione di certificazione.

Si raccomanda ai potenziali acquirenti del prodotto "CoSign v.7.1" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel capitolo 3 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti di verificare la rispondenza ai requisiti identificati e di prestare attenzione alle raccomandazioni contenute in questo Rapporto.

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, le cui modalità di installazione e configurazione sono descritte nelle Procedure preparative [PRE] e nelle Guide per l'amministratore [ADM] e per l'utente [USR], fornite insieme all'ODV.

Si raccomanda l'utilizzo dell'ODV in accordo con quanto descritto nella documentazione citata. In particolare, l'Appendice A del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'installazione e all'utilizzo sicuro del prodotto.

Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte in [TDS], par. 3.2 e 3.3, in particolare quelle relative al personale ed ai locali all'interno dei quali andrà ad operare l'ODV.

8 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

8.1 Consegna

La consegna del dispositivo CoSign avviene direttamente presso la sede del cliente. Al momento della consegna, il prodotto si trova nello stato "Factory Settings", cioè non è stato ancora installato e non è accessibile dagli utenti finali ([TDS], par. 1.4.2.2). La sicurezza fisica è assicurata da sigilli metallici, identificati da numeri univoci indicati nella lettera di consegna, che risulterebbero danneggiati in caso di apertura illecita, rendendo così evidente al destinatario se l'involucro è stato manomesso durante il tragitto.

Nella stessa confezione dell'ODV, viene consegnato anche un CD-ROM contenente il software client (CoSign client software) e il manuale in formato PDF; i file eseguibili e la documentazione contenuti nel CD-ROM sono firmati digitalmente dal produttore ARX a garanzia dell'integrità del CD-ROM stesso e quindi della sicurezza logica dell'ODV.

Alla ricezione della confezione, il ricevente, in particolare l'Appliance Administrator, deve verificare l'integrità del dispositivo e la correttezza dei dati inclusi nel CD-ROM, seguendo le indicazioni fornite nel documento che descrive le procedure di preparazione [PRE].

8.2 Installazione e utilizzo sicuro dell'ODV

L'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo in accordo agli obiettivi di sicurezza indicati nel [TDS], devono avvenire seguendo le istruzioni contenute nelle apposite sezioni dei seguenti documenti:

- [PRE] ARX CoSign Preparative Procedures, v.7.1, June 2014;
- [ADM] ARX CoSign Administrator Guide, v.7.1, 23 March 2014;
- [USR] ARX CoSign User Guide, v.7.1, March 2014.

9 Appendice B – Configurazione valutata

Nel seguito sono elencati i componenti HW/SW, con le rispettive versioni, costituenti la configurazione valutata dell'ODV, come riportato in [CMS], a cui si applicano i risultati della valutazione.

9.1 Hardware

La Tabella 2 riporta gli HardWare Configuration Items dell'ODV valutato.

COMPONENTI HW	Descrizione
CoSign Appliance Ver. 7.0	Intera Appliance dell'ODV CoSign-GEN-HW_V7_0_SW_V7_1

Tabella 2 – Componenti HW dell'ODV

9.2 Software

9.2.1 CSCI

La Tabella 3 che segue riporta la versione dei Computer SoftWare Configuration Items (CSCI) dell'ODV valutato.

CSCI	Descrizione	Versione
ARX CryptoKit	Il prodotto fornisce le interfacce PKCS#11 e Microsoft CAPI (utilizzate internamente all'ODV)	4.20
ARX PrivateWire Firewall	Controlla le comunicazioni da/verso CoSign	3.4
ARX CoSign Appliance	Software dell'appliance CoSign	7.1
CoSign SAPI Component – ARX SignatureAPI.msi	Permette al componente Web Services di firmare e verificare firme	7.1
ARX CoSign Client Core component – ARX CoSign Client.msi	Componente del CoSign client interno all'ODV	7.1
CoSign Web Services DLL - Algorithmic Research - ARX	Utilizza il "CoSign SAPI Component" per preparare i contenuti digitali che devono essere firmati	7.1

Tabella 3 – Configurazione valutata dei CSCI dell'ODV

9.2.2 COTS

La Tabella 4 riporta la versione dei prodotti commerciali (COTS) dell'ODV valutato.

COTS	Descrizione	Versione
Microsoft Windows	Sistema operativo dell'ODV	XP SP3 Embedded
Microsoft SQL Server	DBMS	2008 R2
Mozilla NSS	Network Security Services	3.12
Vasco Vacman Controller	Modulo per la validazione degli OTP utilizzati dai token Vasco	3.11.2
Apache HTTP Server	Web server open source della Apache Software Foundation	2.2.21
OpenSSL	Librerie SSL (prodotto open source)	0.9.8

Tabella 4 – Configurazione valutata dei COTS dell'ODV

9.3 Ambiente operativo dell'ODV

Di seguito si riportano gli elementi HW e SW che devono essere presenti nell'ambiente operativo dell'ODV (TDS], par. 1.3.3 e 1.4.2.2.3):

- OTP-Device: sono utilizzabili token Vasco compatibili con Vacman Controller v.3.11.2 (cfr. Tabella 4) oppure token che implementano l'algoritmo OATH HOTP
- OTP RADIUS Server
- SCA (Signature Creation Application)
- CEA (Certificate Enrollment Application
- CGA (Certificate Generation Application)
- Smart Card in formato Token USB per funzioni di backup

10 Appendice C – Attività di Test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL4, con l'aggiunta di AVA_VAN.5, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

10.1 Configurazione per i Test

Per l'esecuzione dei test è stato predisposto un apposito ambiente di test presso la sede dell'LVS con il supporto del Committente/Fornitore, che ha fornito le risorse necessarie. In particolare, sono stati forniti due dispositivi CoSign (Primary e Alternate) col relativo software dell'ODV, un PC con il RADIUS server e alcuni token di autenticazione (token Vasco compatibile con Vacman Controller v.3.11.2 e token Yubico, come esempio di implementazione dell'algoritmo OATH HOTP).

Prima dell'esecuzione dei test il software è stato installato e configurato seguendo le istruzioni contenute nei documenti [PRE], [ADM] e [USR], come indicato nel par. 8.2.

10.2 Test funzionali svolti dal Fornitore

10.2.1 Copertura dei test

Il piano di test presentato dal Fornitore e la definizione dei casi di test necessari sono stati predisposti come segue:

- sono stati identificati i requisiti che i test devono soddisfare;
- tali requisiti sono stati identificati univocamente con un codice identificativo;
- ogni requisito corrisponde a una TSFI, evidenziata all'interno del titolo del requisito;
- per ogni requisito, sono stati indicati i test progettati per verificare il requisito stesso, cioè la TSFI associata;
- per ogni test, associato a un identificativo numerico, è stata specificata la procedura di test, con tutti i passi previsti, la descrizione degli stessi e i risultati attesi;
- la descrizione del test permette di evincere gli obiettivi del test e le condizioni iniziali dello stesso;
- ad ogni test è stato anche associato lo stato, ovvero se il test è stato eseguito con successo o meno;

- i test sono tra loro indipendenti, cioè la loro esecuzione non deve seguire un ordine prestabilito;

- per il modulo crittografico è stato indicato un elenco di test effettuati in modo automatico.

10.2.2 Risultati dei test

Per l'esecuzione dei test funzionali proposti dal Fornitore, e per la riesecuzione degli stessi da parte dei Valutatori, non è stato utilizzato nessuno strumento specifico.

In una prima fase, i Valutatori hanno eseguito una serie di test, scelti a campione tra quelli del Fornitore, mirati ai individuare il corretto comportamento delle TSFI, in modo da rilevare in tempi brevi eventuali problemi macroscopici sull'ODV.

Durante questa prima sessione di test effettuati dai Valutatori sono stati effettivamente riscontrati alcuni problemi che hanno reso necessario produrre da parte del Fornitore una nuova versione del software dell'ODV, che è stata installata sui due dispositivi CoSign dell'ambiente di test. Su tale versione aggiornata i Valutatori hanno eseguito ulteriori test, oltre a ripetere quelli già svolti in precedenza, stavolta con esito positivo.

10.3 Test funzionali ed indipendenti svolti dai Valutatori

Successivamente, i Valutatori hanno progettato dei test indipendenti per la verifica della correttezza delle TSFI.

Non sono stati utilizzati strumenti di test particolari oltre all'applicativo client (CoSign client software) a corredo dell'ODV, che ha consentito di sollecitare tutte le TSFI selezionate per i test indipendenti.

Per ogni test è stata predisposta una scheda apposita; tali schede sono state utilizzate sia come piano dei test dei Valutatori sia come rapporto dei test stessi, opportunamente compilate con i risultati.

Nella progettazione dei test indipendenti, i Valutatori hanno considerato aspetti che nei test del Fornitore erano non presenti o ambigui o eseguiti inizialmente non verificati con esito positivo o inseriti in test più complessi che interessavano più interfacce contemporaneamente ma con un livello di dettaglio non ritenuto adeguato.

I Valutatori, infine, hanno anche progettato ed eseguito alcuni test in modo indipendente da analoghi test del Fornitore, sulla base della sola documentazione di valutazione. Questo approccio ha portato a rilevare delle anomalie, che sono state poi risolte dal Fornitore nella nuova versione del software rilasciato.

I test indipendenti definiti dai Valutatori hanno avuto i seguenti principali obiettivi:

- verificare la correttezza della procedura di installazione di CoSign e preparare i dispositivi CoSign utilizzati per i test, compresa la funzione di Reset to Factory Settings;

- verificare le operazioni consentite a un utente firmatario: attivazione, operazioni di firma, inserimento, aggiornamento e cancellazione di firme grafiche, blocco dopo N tentativi di login errati;

- verificare le operazioni consentite a un utente amministratore: creazione, abilitazione/disabilitazione e sblocco degli utenti, cambio password, imputabilità delle azioni eseguite.

10.4 Analisi delle vulnerabilità e test di intrusione

Per l'esecuzione di queste attività è stato utilizzato lo stesso ambiente di test già utilizzato per le attività dei test funzionali: sui due dispositivi CoSign è stata installata la versione aggiornata del software dell'ODV, come risultato dalle attività stesse (cfr. par. 10.2.2).

I Valutatori hanno innanzitutto verificato che le configurazioni di test fossero congruenti con la versione dell'ODV in valutazione, cioè quelle indicate nel [TDS], par. 1.2:

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

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

In una prima fase, i Valutatori hanno effettuato delle ricerche tramite internet al fine di individuare eventuali vulnerabilità note applicabili all'ODV, con esito negativo.

In una seconda fase, è stata effettuata la ricerca di vulnerabilità di rete, utilizzando strumenti di scansione automatica; anche questa attività ha avuto esito negativo.

I Valutatori hanno poi esaminato i documenti di valutazione (TDS, specifiche funzionali, progetto dell'ODV, architettura di sicurezza e documentazione operativa) al fine di evidenziare eventuali vulnerabilità potenziali dell'ODV. Da questa analisi, congiuntamente a quella del codice sorgente, i Valutatori hanno effettivamente determinato la presenza di nove vulnerabilità potenziali.

Sulla base di questi risultati, i Valutatori hanno progettato dei test di intrusione per verificare la sfruttabilità delle vulnerabilità potenziali individuate. I test di intrusione sono stati descritti con un dettaglio sufficiente per la loro ripetibilità avvalendosi a tal fine delle schede di test, utilizzate in seguito, opportunamente compilate con i risultati, anche come rapporto dei test stessi.

Dall'esecuzione dei test di intrusione, i Valutatori hanno effettivamente riscontrato la sfruttabilità di alcune delle vulnerabilità individuate, determinando inoltre che solo alcune di esse, se sfruttate da un attaccante con potenziale di attacco High, avrebbero potuto compromettere la disponibilità dei servizi e l'integrità dell'ODV, mentre le altre sono risultate non sfruttabili. Non sono invece state individuate vulnerabilità residue, cioè vulnerabilità che, pur non essendo sfruttabili nell'ambiente operativo dell'ODV, potrebbero però essere sfruttate solo da attaccanti con potenziale di attacco superiore a High.

Tali risultati sono stati prontamente segnalati al Fornitore, che ha provveduto a rilasciare una terza versione del software dell'ODV, che è stata installata sui due dispositivi CoSign dell'ambiente di test.

La riesecuzione dei test di intrusione su questa nuova versione dell'ODV e l'esame del corrispondente codice sorgente ha permesso ai Valutatori di verificare che le vulnerabilità precedentemente riscontrate non erano più presenti nell'ODV. Pertanto, a seguito della conclusione con esito positivo dei test di intrusione, tale versione aggiornata dell'ODV è diventata la versione definitiva del prodotto.

I Valutatori, avvalendosi di opportuni strumenti software, hanno anche effettuato un'analisi statica del codice sorgente e una ricerca sistematica di eventuali vulnerabilità. I risultati ottenuti hanno mostrato che il codice sorgente dell'ODV non presenta problemi di sicurezza.