Ministero dello Sviluppo Economico

Dipartimento per le Comunicazioni

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)

Certificato n. 1/13

(Certification No.)

Prodotto: **Advanced E-Signature ENsoft v.1.1**

(Product)

Sviluppato da: **Euronovate SA**

(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:

EAL1+

(ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 18 settembre 2013

Common Criteria

SOGIS

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Dipartimento per le Comunicazioni

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Advanced E-Signature ENsoft v.1.1

OCSI/CERT/TEC/01/2013/RC

Versione 1.0

28/08/2013

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	Giacinto Dammicco	Prima emissione	28/08/13

2 Indice

3 Elenco degli acronimi

CAD Codice dell'Amministrazione Digitale

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DPCM Decreto della Presidenza del Consiglio dei Ministri

EAL Evaluation Assurance Level

FEA Firma Elettronica Avanzata

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

PP Profilo di Protezione (Protection Profile)

RFV Rapporto Finale di Valutazione

SFR Security Functional Requirement (Requisito Funzionale di Sicurezza)

SAR Security Assurance Requirement (Requisito di Garanzia)

TDS Traguardo di Sicurezza (Security Target)

4 Riferimenti

[CAD] "Codice dell'Amministrazione Digitale", DL 7 marzo 2005, n. 82, con le integrazioni introdotte dal DL 30 dicembre 2010, n. 235, Supplemento ordinario n. 8 alla Gazzetta Ufficiale n. 6 del 10 gennaio 2010

[CC1] CCMB-2012-09-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 4, September 2012

[CC2] CCMB-2012-09-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 4, September 2012

[CC3] CCMB-2012-09-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 4, September 2012

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

[CEM] CCMB-2012-09-004, "Common Methodology for Information Technology Security Evaluation – Evaluation methodology", Version 3.1, Revision 4, September 2012

[DPCM] "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", DPCM del 22 febbraio 2013, Gazzetta Ufficiale Serie Generale n.117 del 21 maggio 2013

[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. 1/07 – Modifiche alla LGP1, versione 1.0, Marzo 2007

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/07 – Modifiche alla LGP2, versione 1.0, Marzo 2007

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/07 – Modifiche alla LGP3, versione 1.0, Marzo 2007

[POIN] “Procedura operativa installazione Suite Ensoft”, EURONOVATE SA

[RFV] Rapporto Finale di Valutazione del prodotto “Advanced E-Signature ENsoft v.1.1”, versione 1, 25 giugno 2013

[TDS] Traguardo di sicurezza del prodotto “Advanced E-Signature ENsoft v.1.1”, versione 1.5, 19 giugno 2013

5 Dichiarazione di certificazione

[1] L'oggetto della valutazione (ODV) è l'applicazione software "Advanced E-Signature ENsoft v.1.1", progettata e prodotta dalla società EURONOVATE SA per realizzare una soluzione di Firma Elettronica Avanzata (FEA), definita nella vigente normativa italiana:

- Codice dell'Amministrazione Digitale [CAD];
- Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali [DPCM].

[2] La valutazione 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).

[3] 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].

[4] L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL1, con l'aggiunta di ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B di questo Rapporto di Certificazione.

[5] 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 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

[6] Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza dell'applicazione software "Advanced E-Signature ENsoft v.1.1", 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.

[7] 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	Advanced E-Signature ENsoft v.1.1
Traguardo di Sicurezza	Traguardo di Sicurezza per il prodotto "Advanced E-Signature ENsoft v.1.1", versione 1.5, 19 giugno 2013
Livello di garanzia	EAL1 con aggiunta di ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1
Fornitore	EURONOVATE SA
Committente	EURONOVATE SA
LVS	Technis Blu S.r.l.
Versione dei CC	3.1 (Rev. 4)
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	27 marzo 2013
Data di fine della valutazione	25 giugno 2013

[8] 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

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

[10] L'ODV è l'applicazione software "Advanced E-Signature ENsoft v.1.1", progettata e prodotta dalla società EURONOVATE SA per eseguire il processo di firma elettronica di un documento.

[11] L'ODV è strettamente connesso a un dispositivo *tablet*, che ha la funzione di ricevere la firma dell'utente e permettere l'utilizzazione dell'ODV. La società EURONOVATE produce un proprio dispositivo *tablet*, denominato “Ensign 10”, ma l'ODV può funzionare con altri dispositivi *tablet* aventi caratteristiche simili.

[12] L’ODV, insieme al suo ambiente operativo, realizza una soluzione di Firma Elettronica Avanzata (FEA), definita nella vigente normativa italiana:

- Codice dell’Amministrazione Digitale [CAD];
- Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali [DPCM].

[13] L'ODV offre all'utente una gestione completa del processo di firma, dalla creazione del documento in formato PDF fino alla restituzione del documento firmato non modificabile.

[14] Prima di apporre la propria firma, il firmatario viene identificato dall'operatore preposto al servizio di firma elettronica, tramite un documento di identità, analogamente a quanto avviene per un documento cartaceo.

[15] L'ODV realizza l'*hash* del documento PDF, tramite l'algoritmo SHA-1, prima di inviarlo al *tablet*.

[16] Il firmatario controlla sul *tablet* il documento PDF che gli viene mostrato, e che ha le stesse caratteristiche del documento cartaceo; se conforme a quanto atteso, l'utente appone la firma sul *tablet* e conferma l'operazione.

[17] Il *tablet*, all'atto delle firma, provvede a registrare alcuni parametri grafometrici caratteristici del firmatario, quali accelerazione, velocità, pressione e interruzioni, creando un vettore grafometrico che viene inviato all'ODV.

[18] L'ODV unisce il vettore grafometrico con l’*hash* del documento PDF; il blocco grafometrico (*hash* del documento + vettore) così costruito viene cifrato da una chiave pubblica fornita da una Certification Authority; la corrispondente chiave privata (necessaria per decifrare il documento in caso di disconoscimento della firma da parte del firmatario ed intervento della magistratura) è custodita presso un pubblico ufficiale o in un HSM (Hardware Security Module).

[19] Sul blocco grafometrico viene apposta un'ulteriore firma di integrità a livello software, al fine di rilevare e segnalare eventuali modifiche successive al documento firmato. Il dato grafometrico, cifrato insieme all’*hash* del documento originale e l’immagine stessa della firma, sono parti integranti della firma di integrità apposta dall'ODV sul documento PDF a fronte di ogni firma utente. Nel caso venga modificato anche solo un bit di quel documento, all’apertura dello stesso verrà visualizzato un messaggio che indica che il documento è stato modificato in data posteriore all’apposizione della firma.

[20] Alla fine del processo di firma, l'ODV cancella i dati temporanei di ciascuna sessione di firma, per evitare che siano usati in modo improprio per altre operazioni.

[21] Le funzioni di sicurezza dell'ODV sono:

- cifratura e decifratura per lo scambio dei dati col *tablet*;
- cancellazione dei dati al termine di ciascuna sessione di firma, al fine di proteggere i dati e la firma del firmatario;
- generazione dell'*hash* dei documenti con l'algoritmo SHA-1;
- firma di integrità sul documento alla fine dell'operazione di firma.

6.4 Politiche di sicurezza dell'organizzazione

[22] Per l'ODV non è richiesta alcuna conformità ad alcuna politica di sicurezza dell'organizzazione.

6.5 Requisiti funzionali e di garanzia

[23] Pur trattandosi di una valutazione a livello di garanzia EAL1, il Committente ha scelto di non limitarsi a indicare, nel Traguardo di Sicurezza [TDS], i Requisiti Funzionali di Sicurezza (RFS) e le funzioni di sicurezza che realizzano gli obiettivi di sicurezza, ma di descrivere completamente il problema di sicurezza per l'ODV, cioè tutti gli obiettivi di sicurezza e le minacce che questi devono contrastare.

[24] Tutti gli SFR sono stati selezionati dai CC Parte 2 [CC2].

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

6.6 Conduzione della valutazione

[26] 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].

[27] 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 TDS 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 TDS stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

[28] L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS Technis Blu S.r.l.

[29] La valutazione è terminata in data 25 giugno 2013 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV]. Tale Rapporto è stato analizzato dall'Organismo di Certificazione e approvato il 30 luglio 2013. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

6.7 Considerazioni generali sulla validità della certificazione

[30] 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.

[31] 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

[32] 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 "Advanced E-Signature ENsoft v.1.1" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL1, con l'aggiunta di ASE_OBJ.2, ASE_REQ.2 E ASE_SPD.1, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B.

[33] 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 EAL1, con l'aggiunta di ASE_OBJ.2, ASE_REQ.2 E ASE_SPD.1, oltre a quelli della classe ASE per la valutazione del TDS.

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 for the operational environment	ASE_OBJ.2	Positivo
Stated security requirements	ASE_REQ.2	Positivo
Security problem definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Basic functional specification	ADV_FSP.1	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
Labelling of the TOE	ALC_CMC.1	Positivo
TOE CM coverage	ALC_CMS.1	Positivo
Tests	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo

Classi e componenti di garanzia		Verdetto
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 - Verdetti finali per i requisiti di garanzia

7.2 Raccomandazioni

[34] Le conclusioni dell'Organismo di Certificazione sono riassunte nella Dichiarazione di certificazione riportata nel par. 5.

[35] Si raccomanda ai potenziali acquirenti del prodotto "Advanced E-Signature ENsoft v.1.1", di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto di Certificazione in riferimento al Traguardo di Sicurezza [TDS].

[36] L'ODV deve essere utilizzato in accordo all'ambiente di sicurezza specificato nel 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 di Certificazione.

[37] Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV valutato, configurato come riportato in Appendice B.

[38] Poiché l'ODV viene distribuito da Euronovate ai propri clienti prevalentemente per via telematica, si raccomanda agli utenti di seguire attentamente le procedure di installazione e configurazione, secondo quanto riportato in Appendice A.

[39] Al fine di preservare l'ambiente di utilizzo da rischi di manipolazione indebita del software, si suggerisce al Committente di effettuare periodicamente e volontariamente i test di vulnerabilità.

[40] L'ODV è un'applicazione che realizza una soluzione di Firma Elettronica Avanzata (FEA), definita nella vigente normativa italiana. Poiché nel tempo tale normativa potrebbe essere soggetta a revisioni, si consiglia il Committente di verificare periodicamente la conformità dell'ODV a tale normativa e, nel caso, valutare l'opportunità di un aggiornamento della certificazione o la necessità di una rivalutazione.

[41] Si assume che gli operatori preposti al servizio di firma elettronica siano adeguatamente addestrati al corretto utilizzo dell'ODV e scelti tra il personale fidato dell'organizzazione. L'ODV non è realizzato per contrastare minacce provenienti da operatori inesperti, malfidati o negligenti.

[42] Occorre inoltre notare che la sicurezza dell'operatività dell'ODV è condizionata al corretto funzionamento del sistema operativo di cui è dotata la workstation su cui è installato l'ODV, e delle cui funzionalità questo si serve. Le specifiche dell'ambiente IT sono descritte nel Traguardo di Sicurezza [TDS].

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

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

8.1 Predisposizione e Consegna dell'ODV

[44] Il prodotto viene distribuito da Euronovate ai propri clienti prevalentemente per via telematica, oppure spedendo un CD su richiesta specifica, insieme al documento "Procedura operativa installazione Suite Ensoft" [POIN].

[45] Tale documento contiene sia la parte relativa alle procedure preparatorie sia la parte propria di un manuale utente e sintetizza le operazioni da svolgere per scaricare il software dal sito di Euronovate, per installarlo su un normale PC, e per effettuare prove di corretta installazione, funzionamento, verifica.

[46] Nelle istruzioni che vengono fornite al cliente sono chiaramente indicate anche le caratteristiche della stazione di lavoro su cui deve essere installato l'ODV.

8.2 Documentazione per l'utilizzo sicuro dell'ODV

[47] I documenti di guida rilevanti ai fini della valutazione o referenziati all'interno dei documenti prodotti e disponibili ai potenziali acquirenti, sono i seguenti:

- Traguardo di sicurezza del prodotto "Advanced E-Signature ENsoft v.1.1", versione 1.5, 19 giugno 2013 [TDS];

- Procedura operativa installazione Suite Ensoft [POIN].

9 Appendice B - Configurazione valutata

[48] L'ODV, il software “Advanced E-Signature ENsoft v.1.1”, è un'applicazione che viene installata su un PC client, utilizzato dagli operatori per le attività aziendali di propria competenza. L’applicazione è indipendente dalle altre applicazioni ospitate dal PC, ma si appoggia al sistema operativo ed utilizza i supporti di memorizzazione del PC stesso. Analogamente si avvale di programmi di utilità del PC e delle funzioni di sicurezza predisposti sul PC (antivirus) e dall’ambiente IT in cui opera (firewall).

[49] L’ODV è stato installato, utilizzando il software scaricato dal sito di Euronovate, seguendo le istruzioni fornite insieme al software, su una workstation dotata di sistema operativo Windows 7 Enterprise 64bit, SP1 aggiornato.

[50] E' stata utilizzato anche il dispositivo *tablet* denominato “Ensign 10”, fornito dalla stessa società Euronovate, strumento indispensabile per utilizzare l'ODV.

[51] Gli utenti dell'ODV dovranno verificare la corrispondenza della versione scaricata o ricevuta su CD con quella valutata, cioè “Advanced E-Signature ENsoft v.1.1”.

10 Appendice C - Attività di Test

[52] Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL1 tali attività non prevedono l'esecuzione di test funzionali da parte del Fornitore, ma soltanto test funzionali indipendenti da parte dei Valutatori.

10.1 Configurazione per i Test

[53] I test indipendenti e le prove di intrusione sono stati eseguiti dai Valutatori dell'LVS presso la propria sede, simulando un ambiente operativo reale.

[54] L'ODV utilizzato è quello descritto in Appendice B, cioè il software scaricato dal sito di Euronovate, installato su una workstation dotata di sistema operativo Windows 7 Enterprise 64bit, SP1 aggiornato, secondo la procedura descritta nelle istruzioni, il dispositivo *tablet* "Ensign 10" e il relativo cavo di connessione USB.

10.2 Test funzionali ed indipendenti svolti dai Valutatori

[55] Nella predisposizione del programma dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS] e le specifiche funzionali.

[56] I Valutatori hanno quindi esaminato le funzioni di sicurezza dell'ODV, così come rappresentate nel TDS e, sulla base della propria esperienza, hanno predisposto un insieme di test, con l'obiettivo di verificare l'adeguatezza delle funzioni di sicurezza dell'ODV, nel rispetto di quanto previsto dalla CEM.

[57] In particolare, i Valutatori hanno deciso di verificare:

- che il documento informatico sottoscritto non possa subire modifiche dopo l'apposizione della firma, e che, in caso di modifiche, se ne possa avere evidenza;
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
- il controllo esclusivo del firmatario sul sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima.

[58] I Valutatori hanno dimostrato che l'ODV si comporta come descritto nella documentazione di progetto e che realizza i requisiti funzionali di sicurezza descritti nel TDS.

[59] L'ODV ha quindi superato con verdetto positivo la fase di test indipendenti.

10.3 Analisi delle vulnerabilità e test di intrusione

[60] Considerato che l'ODV viene dichiarato dal Committente strumento di Firma Elettronica Avanzata (FEA), definita nella normativa italiana nelle “Regole tecniche in materia di firme elettroniche” [DPCM], la ricerca di informazioni pubbliche sulle potenziali vulnerabilità dell'ODV ha portato i Valutatori ad assumere quanto riportato a tale proposito in tale [DPCM].

[61] Dalla suddetta documentazione e dall’analisi condotta dallo sviluppatore, i Valutatori hanno individuato alcune vulnerabilità potenzialmente rilevanti ai fini della valutazione dell'ODV.

[62] I Valutatori hanno quindi esaminato le vulnerabilità così individuate, tenendo presenti la tracciabilità e la chiarezza delle giustificazioni addotte dallo sviluppatore per contrastare attacchi potenziali. Con queste informazioni i valutatori hanno determinato un insieme di prove di intrusione appropriato per il livello di valutazione EAL1, cioè assumendo che l'ODV deve resistere ad un ipotetico attaccante con potenziale di attacco *Basic*, nel rispetto di quanto previsto dalla CEM (cfr. [CEM], appendice B.4).

[63] Le prove di intrusione condotte dai Valutatori hanno confermato che le potenziali vulnerabilità non possono essere sfruttate nell’ambiente operativo dell'ODV.