Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

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. 6/22

(Certification No.)

Prodotto: ENSoft version 2.0

(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 Eva Spina)

Firmato digitalmente da
Eva Spina
Data: 2022.02.02 09:22:16
+01'00'

Roma, 2 febbraio 2022

Common Criteria

SOGIS
IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

ENSoft version 2.0

OCSI/CERT/TEC/09/2021/RC

Versione 1.0

2 febbraio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	02/02/2022

2 Indice

3 Elenco degli acronimi

AES Advanced Encryption Standard

CA Certification Authority

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DLL Dynamic-Link Library

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

FEA Firma Elettronica Avanzata

HSM Hardware Security Module

HTTPS HyperText Transfer Protocol Secure

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

PC Personal Computer

PDF Portable Document Format

PP Profilo di Protezione

RFV Rapporto Finale di Valutazione

RSA Rivest, Shamir, Adleman

SAR Security Assurance Requirement

SDK Software Development Kit

SFR Security Functional Requirement

SHA Secure Hash Algorithm

TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[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

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

[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

[SOGIS] "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", Version 3, January 2010

4.2 Documenti tecnici

[GUI] "Euronovate Software Suite - Guida per l'installazione ed utilizzo di ENSoft v.2", Euronovate SA, 5 luglio 2021

[RC] "Rapporto di Certificazione Advanced E-Signature ENsoft v.1.1", OCSI/CERT/TEC/01/2013/RC, versione 1.0, 28 agosto 2013

[RFV] Rapporto Finale di Valutazione del prodotto "advanced Ensoft v.2.0", Versione 1.2, Technis Blu S.r.l., 20 gennaio 2022

[TDS] Security Target "Advanced E-Signature ENsoft v.2", versione 1.3, Euronovate SA, 13 gennaio 2022

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia indicati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia indicati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è l'applicazione software "ENSoft version 2.0", sviluppata dalla società Euronovate SA.

L'ODV, unitamente al suo ambiente operativo, realizza una soluzione di Firma Grafometrica mediante una gestione completa del processo di firma, dalla produzione dei documenti richiesti dagli utenti, fino alla gestione del documento PDF firmato e reso immodificabile. Al termine delle operazioni, l'ODV provvede alla cancellazione sicura dei dati temporanei generati, in modo da evitarne riutilizzi dolosi o involontari.

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 di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (Advanced E-Signature ENsoft v.1.1), già certificato dall'OCSI (Certificato n. 1/13 del 18 settembre 2013 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore Euronovate SA è stato necessario procedere a una ri-certificazione dell'ODV.

In considerazione del tempo trascorso dalla precedente certificazione, l'LVS Technis Blu S.r.l., in accordo con l'OCSI e col Committente, ha ripetuto tutte le attività di valutazione senza tenere conto delle evidenze e dei risultati ottenuti in precedenza.

Si noti che le modifiche effettuate hanno 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.

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 e/o utilizzatori. 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 EAL1, con l'aggiunta di ASE_OBJ.2, ASE_REQ.2 e ASE_SPD.1, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata 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.

Inoltre, si precisa che l'emissione del Certificato per l'ODV non costituisce in alcun modo attestazione da parte dell'OCSI di conformità dell'applicazione software denominata "ENSoft version 2.0" ai requisiti di sicurezza di una soluzione di firma elettronica avanzata (FEA) di cui all'art. 26 del Regolamento (UE) n. 910/2014 [eIDAS] e all'art. 56 del DPCM 22 febbraio 2013 [DPCM].

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "ENSoft version 2.0" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori 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.

7.2 Identificazione sintetica della certificazione

Nome dell'ODV	ENSoft version 2.0
Traguardo di Sicurezza	Security Target "Advanced E-Signature ENsoft v.2", versione 1.3 [TDS]
Livello di garanzia	EAL1 con l'aggiunta di ASE_OBJ.2, ASE_REQ.2 e ASE_SPD.1
Fornitore	Euronovate SA
Committente	Euronovate SA
LVS	Technis Blu S.r.l.
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	26 luglio 2021
Data di fine della valutazione	20 gennaio 2022

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].

7.3 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 è l'applicazione software "ENSoft version 2.0" la quale, unitamente al suo ambiente operativo, realizza una soluzione di Firma Grafometrica, un particolare tipo di Firma Elettronica Avanzata (FEA) che si ottiene rilevando i dati biometrici del firmatario nel

momento in cui appone la sua firma su un *tablet* legando gli stessi in maniera indissolubile al documento elettronico firmato.

L'ODV offre una gestione completa del processo di firma, dalla produzione dei documenti richiesti dagli utenti, fino alla gestione del documento PDF firmato e reso immodificabile. L'ODV riconosce e accetta documenti PDF o PDF/A.

L'ODV esegue l'*hash* del documento PDF con l'algoritmo SHA-256, prima di inviarlo al *tablet*. Gli utenti finali, dopo aver esaminato il documento, firmano sul *tablet* e confermano la firma. L'ODV effettua la registrazione dei parametri biometrici (accelerazione, velocità, pressione e tratti aerei) e crea un vettore grafometrico che viene unito all'*hash* del documento.

Successivamente, il blocco grafometrico (*hash* del documento + vettore grafometrico) creato viene prima cifrato mediante l'algoritmo AES e poi con una chiave pubblica RSA rilasciata da una CA, la cui 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.

Inoltre, al blocco grafometrico viene apposta un'ulteriore firma di integrità a livello software. I dati grafometrici, cifrati insieme all'*hash* del documento originale e all'immagine della firma, sono parte integrante della firma di integrità. 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 una data successiva all'apposizione della firma.

Al termine delle operazioni, l'ODV provvede alla cancellazione sicura dei dati temporanei generati in ogni sessione di firma, per evitare che siano usati in modo improprio per altre operazioni.

7.3.1 Architettura dell'ODV

I componenti della soluzione di FEA Euronovate sono:

- il software di firma "ENSoft version 2.0" (ODV);
- un *tablet* da 10 pollici (ad es., ENSign 11).

ENSoft version 2.0 è un *plugin* di processo e include le seguenti parti:

- driver di basso livello per le comunicazioni con il dispositivo;
- *layer* per la manipolazione dei file PDF e la gestione del vettore biometrico;
- visualizzatore PDF;
- canali di comunicazione (HTTPS, TCP/IP, WebSocket) che consentono l'utilizzo della suite di firma da parte di qualsiasi applicazione dotata di un SDK adeguato.

La piattaforma ENSoft version 2.0 è composta dai seguenti moduli:

- *ENLibPDF*: una libreria sviluppata internamente che manipola il PDF a basso livello. Questo componente aggiunge il campo della firma, applica il blocco biometrico cifrato nei campi della firma con il flusso della firma incrementale.

- *ENPdfUtils*: una libreria di strumenti che consente di utilizzare ENLibPDF all'interno del *plugin* di processo.

- *ENSoftServerHelper*: una libreria di strumenti preposta alla gestione della comunicazione con il server di firma remota (SoftServer).

- *ENDocumentModel*: una libreria di strumenti che descrive il modello del documento firmato (quante firme ci sono, dove si trovano le firme, quanti firmatari ci sono, ecc.).

- *ENViewerNet*: una libreria di strumenti incaricata di presentare il PDF all'utente finale all'interno del *tablet* e di gestire clic e gesti su di esso. Questo è il "nucleo" dell'esperienza utente del processo di firma. È un lettore PDF personalizzato che permette di visualizzare il PDF per la firma, mostra i campi firma per renderli più identificabili da parte del cliente, gestisce lo scroll del documento, lo zoom e la navigazione in generale.

L'ODV è strettamente legato ad un *tablet* che ha la funzione di ricevere la firma dell'utente e di consentirne l'utilizzo. Euronovate produce un *tablet* adeguato a questo scopo, denominato ENSign 11, ma l'ODV può funzionare con altri dispositivi aventi caratteristiche simili.

La soluzione ENSoft version 2.0 è stata sviluppata per sistemi Windows. Attualmente è compatibile con Windows 7, 8 e 10.

7.3.2 Caratteristiche di Sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nei cap. 5 e 6 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il cap. 10 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- l'ODV esegue la decifratura dei dati scambiati con il *tablet* utilizzando l'SDK fornito dal produttore del *tablet* e la loro cifratura mediante gli algoritmi AES e RSA prima di aggiungerli al file PDF.

- l'ODV, al fine di proteggere i dati e le firme dei firmatari, distrugge i dati di ogni sessione di firma al termine dell'operazione.

- l'ODV genera valori di *hash* mediante l'algoritmo SHA-256.

- l'ODV appone una firma di integrità sul documento al termine delle operazioni.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto. viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per 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. 8.2 di questo rapporto.

7.5 Conformità a Profili di Protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

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

Tutti i Requisiti Funzionali di Sicurezza (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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, gli SFR e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 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 e/o utilizzatori. 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 Technis Blu S.r.l.

L'attività di valutazione è terminata in data 20 gennaio 2022 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 26 gennaio 2022. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 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 – Configurazione valutata. I potenziali acquirenti e/o utilizzatori 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 e/o utilizzatori (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.

8 Esito della valutazione

8.1 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 "ENSoft version 2.0" 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 – Configurazione valutata.

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.

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
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
Test	**Classe ATE**	Positivo
Independent testing - conformance	ATE_IND.1	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability survey	AVA_VAN.1	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti e/o utilizzatori del prodotto "ENSoft version 2.0" 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 agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 6.2 e nel par. 6.3 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le ipotesi descritte nel par. 5.5 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, descritta in Appendice B – Configurazione valutata. In particolare, l'Appendice A – Indicazioni per l'uso sicuro del prodotto del presente Rapporto include una serie di raccomandazioni relative alla consegna, all'inizializzazione, all'installazione e all'utilizzo sicuro del prodotto, in accordo con la documentazione di guida fornita con l'ODV ([GUI]).

L'ODV è un'applicazione progettata per realizzare, unitamente al proprio ambiente operativo, una soluzione di Firma Elettronica Avanzata (FEA), definita nella vigente normativa ([eIDAS], [DPCM]). 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.

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

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

9.1 Consegna dell'ODV

La procedura di distribuzione dell'ODV prevede che lo stesso venga scaricato dal sito del Fornitore mediante identificazione dell'utente attraverso credenziali individuali (userid e password) fornite da Euronovate. Analogamente vengono distribuiti i driver.

Il *tablet* ENSign 11, se acquistato assieme all'ODV, viene spedito da Euronovate etichettato con un numero di serie di 8 caratteri alfanumerici.

Maggiori dettagli sulla procedura di download dell'ODV sono descritti nella documentazione di guida fornita con il prodotto al cliente.

9.2 Installazione, inizializzazione e utilizzo sicuro dell'ODV

L'ODV è una applicazione che viene generalmente installata su un PC client, utilizzato dagli utenti 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 e dall'ambiente IT in cui opera. Per l'utilizzo dell'ODV è indispensabile installare un *tablet* supportato, che ha lo scopo di raccogliere la firma dell'utente.

L'installazione, la configurazione e l'operatività dell'ODV devono essere eseguite secondo le istruzioni riportate nelle sezioni appropriate della documentazione di guida fornita con il prodotto al cliente.

In particolare, il seguente documento contiene informazioni dettagliate per l'inizializzazione sicura dell'ODV, la preparazione del suo ambiente operativo e il funzionamento sicuro dell'ODV in conformità con gli obiettivi di sicurezza specificati nel Traguardo di Sicurezza [TDS]:

- "Euronovate Software Suite - Guida per l'installazione ed utilizzo di ENSoft v. 2" [GUI]

10 Appendice B – Configurazione valutata

L'ODV è il prodotto software "ENSoft version 2.0". Il nome e il numero di versione identificano univocamente l'unica configurazione prevista dell'ODV a cui si applicano i risultati della valutazione.

L'ODV richiede per l'installazione e l'operatività un PC client con le seguenti caratteristiche minime:

- sistema operativo Microsoft Windows 7, 8, o 10;
- .NET Framework 4.5.2;
- interfaccia USB v2.2 o superiore per la connessione con il *tablet*;
- interfaccia USB o PS/2 per la connessione di mouse e tastiera.

Per il suo corretto funzionamento, l'ODV richiede un *tablet* a 10 pollici compatibile, con una penna inclusa.

11 Appendice C – Attività di Test

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 e test di intrusione da parte dei Valutatori.

11.1 Configurazione per i Test

Le attività relative ai test indipendenti e alle prove di intrusione sono state eseguite dai Valutatori presso la sede dell'LVS, su un ambiente di test predisposto secondo le specifiche contenute nel Traguardo di Sicurezza [TDS] e nella Guida per l'installazione ed utilizzo dell'ODV [GUI].

L'ODV utilizzato è stato scaricato dal sito di Euronovate e installato su una workstation dotata di sistema operativo Windows 10 Home Edition aggiornato. È stato utilizzato anche il dispositivo *tablet* denominato ENSign 11, fornito dalla stessa società Euronovate.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Nella predisposizione dell'insieme dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS], il documento di specifiche funzionali e la Guida per l'installazione ed utilizzo dell'ODV [GUI].

I Valutatori hanno quindi esaminato le funzioni di sicurezza dell'ODV e le TSFI descritte nella documentazione del Fornitore e, sulla base della propria esperienza, hanno predisposto un insieme di test con l'obiettivo di verificare la corretta implementazione delle funzioni di sicurezza dell'ODV, nel rispetto di quanto previsto dalla CEM.

Particolare attenzione è stata svolta nel controllo che l'ODV e l'ambiente di test si trovassero nello stato descritto nella documentazione di valutazione prima, durante e dopo le attività di test. In particolare, è stato verificato che il *tablet* venisse correttamente riconosciuto dal sistema operativo per poter essere utilizzato con l'ODV e che, in caso di mancato collegamento all'avvio dell'ODV o di disconnessione a caldo, venisse segnalata correttamente l'anomalia.

I test funzionali progettati e svolti dai Valutatori hanno coperto i seguenti aspetti di sicurezza:

- verifica che l'ODV gestisce solo documenti completati con la firma e confermati dal firmatario, al fine di assicurarne l'integrità;
- verifica che l'ODV mantiene l'integrità del documento firmato non consentendo l'apposizione della firma fuori dall'area appositamente prevista;
- esame del processo di acquisizione di un documento verificando l'integrità del documento e delle componenti che assicurano l'integrità del documento stesso;
- esecuzione di firma su un documento sprovvisto di campi firma verificando che l'ODV mantiene l'integrità del documento firmato;

- esame della consistenza del PDF firmato verificando che il PDF prodotto contenga il documento originale più la firma grafometrica cifrati con la chiave pubblica e il blocco che garantisce l'inalterabilità del documento;

- verifica dell'impossibilità di introdurre modifiche ad un documento informatico sottoscritto dopo l'apposizione della firma da parte dell'ODV;

- verifica che l'ODV consente l'acquisizione di un solo documento per volta, al fine di mantenerne la riservatezza;

- verifica che l'ODV mantiene l'integrità del documento quando è in corso la firma e per qualche motivo si interrompe la comunicazione tra il *tablet* e il PC;

- verifica che l'ODV esegue correttamente il processo di firma multipla di un documento PDF conforme;

- verifica che l'ODV esegue correttamente il processo di scelta di un documento PDF conforme;

- verificare che l'ODV esegue correttamente il processo di zoom in di un documento PDF;

- verifica che l'ODV esegue correttamente il processo di firma e viene registrata la chiave privata della firma.

I test effettuati hanno altresì consentito di verificare implicitamente il corretto utilizzo e l'aderenza agli standard delle funzioni crittografiche utilizzate dall'ODV.

Tutti i test effettuati dai Valutatori hanno dato esito positivo, dimostrando che l'ODV si comporta come descritto nella documentazione tecnica messa a disposizione dal Fornitore e realizza correttamente i requisiti funzionali di sicurezza descritti nel Traguardo di Sicurezza [TDS].

11.3 Analisi delle vulnerabilità e test di intrusione

Le attività di analisi delle vulnerabilità e test di intrusione sono state svolte nello stesso ambiente già utilizzato per le attività dei test funzionali. Le fasi di verifica dell'ambiente operativo e della corretta installazione e configurazione dell'ODV sono state ripetute anche in sede di test di intrusione.

In considerazione del fatto che l'ODV viene dichiarato dal Fornitore come strumento che realizza una soluzione di Firma Elettronica Avanzata (FEA), i Valutatori hanno condotto la ricerca di informazioni pubbliche sulle potenziali vulnerabilità dell'ODV tenendo conto principalmente dei requisiti di sicurezza definiti nella vigente normativa sulla FEA ([eIDAS], [DPCM]).

È stata altresì effettuata un'analisi veloce del codice e dei file .exe per verificare la presenza di vulnerabilità sfruttabili da un attaccante malevolo dotato di una dimestichezza base con l'ambiente operativo. Da questa analisi non sono emerse anomalie evidenti.

Sulla base della documentazione disponibile e dell'analisi preliminare condotta, i Valutatori hanno predisposto e condotto test di penetrazione relativamente alle seguenti vulnerabilità potenzialmente rilevanti ai fini della valutazione dell'ODV:

- l'attaccante si identifica al posto dell'utente destinatario del processo di firma;
- l'attaccante si sostituisce al soggetto che firma durante la procedura di apposizione;
- l'attaccante si sostituisce al soggetto che firma dopo la procedura di apposizione;
- l'attaccante acquisisce il sistema di generazione della firma di un altro soggetto; in particolare prende possesso del *tablet* da remoto;
- l'attaccante modifica il documento informatico già firmato senza che tale modifica venga rilevata;
- il firmatario nega di aver avuto la possibilità di controllare/visualizzare il documento successivamente sottoscritto;
- l'attaccante inserisce nell'oggetto della sottoscrizione del codice che può modificare l'oggetto stesso;
- il firmatario nega di aver firmato lo specifico documento che risulta sottoscritto (ripudio);
- l'attaccante si impossessa del vettore biometrico del sottoscrittore "sniffando" i dati sulla connessione USB;
- l'attaccante si impossessa dei file temporanei generati dall'ODV che permettono di ottenere i dati biometrici del sottoscrittore;
- vengono generate chiavi di firma non sufficientemente robuste;
- l'attaccante entra in possesso delle chiavi pubblica e privata utilizzate per garantire l'integrità del documento;
- l'attaccante tenta di accedere a zone protette del processo in esecuzione alterandone il funzionamento mediante un file PDF malformato;
- possibilità di estrarre i dati biometrici da un documento PDF firmato senza certificato;
- assenza di *timeout* a segnalare la conclusione dell'evento di firma, rendendo in questo modo vulnerabile il processo che contiene i buffer e aree di memoria contenenti i dati biometrici raccolti fino a quel momento;
- possibilità di forzare l'applicazione sostituendo le DLL o provocando comportamenti anomali;
- introduzione di codice malevolo nell'applicativo di firma.

Per i test sono stati utilizzati i seguenti strumenti di analisi in un ambiente Windows 10 a 64 bit non connesso ad una rete:

- analizzatore di traffico USB (Free USB Analyzer);
- analizzatore di processi Windows (Sysinternals Process Monitor);
- analizzatore delle attività dei processi (Sysinternals Process Explorer, Task Manager);
- strumento per il calcolo di valori di *hash*.

Durante i test è emerso che alcuni componenti del software dell'ODV vengono rilevati come malevoli dall'antivirus standard di Windows (Microsoft Defender). In effetti, viene espressamente richiesto dalle istruzioni contenute nel documento di guida [GUI] di disabilitare la scansione antivirus sulle cartelle in cui viene installato l'ODV.

Inoltre, non è presente una firma del codice dei componenti eseguibili dell'ODV. In assenza di un controllo di integrità sull'installazione all'avvio del PC, queste circostanze potrebbero potenzialmente consentire la modifica fraudolenta di componenti dell'ODV senza che questo venga rilevato dall'ambiente operativo. Questa vulnerabilità è considerata residua.

Al termine delle sessioni di test di intrusione, i Valutatori hanno quindi concluso che l'ODV, nel suo ambiente operativo, è in grado di resistere ad un attaccante che possiede un potenziale di attacco di livello Basic. Non sono state individuate vulnerabilità sfruttabili.

Ad ogni modo, per garantire una maggiore sicurezza dell'applicativo, si raccomanda al Fornitore di verificare ed eliminare la non compatibilità con l'antivirus di Windows e di abilitare la firma del codice in fase di sviluppo dell'ODV.