Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/15

(Certification No.)

Prodotto: **Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0**

(Product)

Sviluppato da: **CheBanca! S.p.A.**

(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)

Rita Forsi

Roma, 5 marzo 2015

Common Criteria

SOGIS

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

Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0

OCSI/CERT/TEC/04/2014/RC

Versione 1.0

5 marzo 2015

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	05/03/2015

2 Indice

3 Elenco degli acronimi

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

DBMS Database Management System

DPCM Decreto del Presidente del Consiglio dei Ministri

DTBS/R Data To Be Signed/Representation

EAL Evaluation Assurance Level

FEA Firma Elettronica Avanzata

HSM Hardware Security Module

HTTPS HyperText Transfer Protocol over Secure Socket Layer

LDAP Lightweight Directory Access Protocol

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

PDF Portable Document Format

PIN Personal Identification Number

PP Profilo di Protezione

RFV Rapporto Finale di Valutazione

SAR Security Assurance Requirement

SFR Security Functional Requirement

TDS Traguardo di Sicurezza

TOE Target of Evaluation

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 2011

[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

[GUI] "Guida Utente FEA - Applicazione Firma Elettronica Avanzata di CheBanca! Versione 1.0", versione 1.1, 17 luglio 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

[RFV] Rapporto Finale di Valutazione del prodotto “Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0”, Versione 1.3, 12 gennaio 2015

[TDS] Security Target “Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0”, v. 3.4, 16 dicembre 2014

5 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è l'applicazione software denominata "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", sviluppata da CheBanca! S.p.A. e progettata per rispondere, unitamente al proprio ambiente operativo, ai requisiti della Firma Elettronica Avanzata previsti dalla 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].

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).

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, 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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" ai requisiti generali di sicurezza definiti nelle Regole Tecniche emesse da AgID ([DPCM]) per le soluzioni di FEA.

6 Riepilogo della valutazione

6.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" 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.

6.2 Identificazione sintetica della certificazione

Nome dell'ODV	Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0
Traguardo di Sicurezza	Security Target "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", v. 3.4, 16 dicembre 2014
Livello di garanzia	EAL1 con aggiunta di ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1
Fornitore	CheBanca! S.p.A.
Committente	CheBanca! S.p.A.
LVS	Technis Blu S.r.l.
Versione dei CC	3.1 Rev. 4
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	20 marzo 2014
Data di fine della valutazione	12 gennaio 2015

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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", è un'applicazione software integrata nei servizi di *home banking* offerti attraverso il sito Web www.chebanca.it. L'ODV è accessibile da un qualsiasi dispositivo fisso o mobile sul quale sia possibile utilizzare un *browser* Web per accedere ad Internet con protocollo sicuro HTTPS.

L'ODV è progettato per realizzare, insieme al suo ambiente operativo, 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].

Mediante le funzionalità fornite dall'ODV i clienti CheBanca! possono richiedere l'attivazione dei servizi di Firma Elettronica Avanzata divenendo così "Utenti FEA". Successivamente, attraverso l'ODV, un "Utente FEA" ha la facoltà di firmare elettronicamente nuovi contratti relativi a prodotti bancari. L'"Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" può essere utilizzata solo per la firma elettronica dei prodotti bancari specificamente scelti e abilitati da CheBanca!.

Per accedere ai servizi dell'ODV il cliente CheBanca! deve prima accedere al sito di *home banking* (www.chebanca.it) mediante una procedura di identificazione ed autenticazione che prevede l'uso delle proprie "Credenziali cliente CheBanca!". Una volta entrato nel sito di *home banking*, per poter utilizzare l'ODV nel ruolo di "Utente FEA" il cliente deve effettuare un secondo livello di autenticazione di tipo forte mediante Codici Dispositivi.

Tali codici sono contenuti nella cosiddetta "Matrice dispositiva", una tessera, in possesso esclusivo del cliente, strutturata per righe e colonne contenente i codici numerici che il cliente deve reperire in corrispondenza dei due incroci lettera/numero richiesti per l'esecuzione dell'operazione di autenticazione.

L'ODV gestisce l'unico ruolo "Utente FEA". L'amministrazione dell'ODV avviene nell'ambiente operativo, nell'ambito della gestione dell'applicazione di *home banking*.

L'ambiente operativo dell'ODV è caratterizzato dai principali elementi riportati in Figura 1.

Il primo elemento è costituito dal "cliente" del servizio di *home banking* che opera da remoto sul proprio conto CheBanca! mediante i propri dispositivi fissi o mobili.

Il secondo elemento è costituito dalla rete Internet a cui il cliente accede col proprio *browser* mediante protocollo sicuro HTTPS.

Il terzo elemento, che costituisce l'ambiente operativo propriamente detto dell'ODV, è costituito dal Data Center di CheBanca! e da un secondo Data Center, operato da Intesi Group S.p.A., all'interno dei quali sono installate le applicazioni di *home banking*, i Servizi di Business, la piattaforma di gestione documentale, e i diversi componenti dell'"Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" (ODV).

Il quarto elemento è costituito da due Data Center certificati ISO 27001, collegati col Data Center CheBanca! mediante VPN IPsec. Il primo ospita la *Certification Authority* che, interfacciandosi con un HSM, si occupa dell'emissione, la conservazione e la revoca dei

certificati digitali utilizzati dall'applicazione di Firma Elettronica Avanzata; il secondo ospita i servizi di Conservatoria Digitale per i contratti firmati dall'"Utente FEA" e dalla Banca.

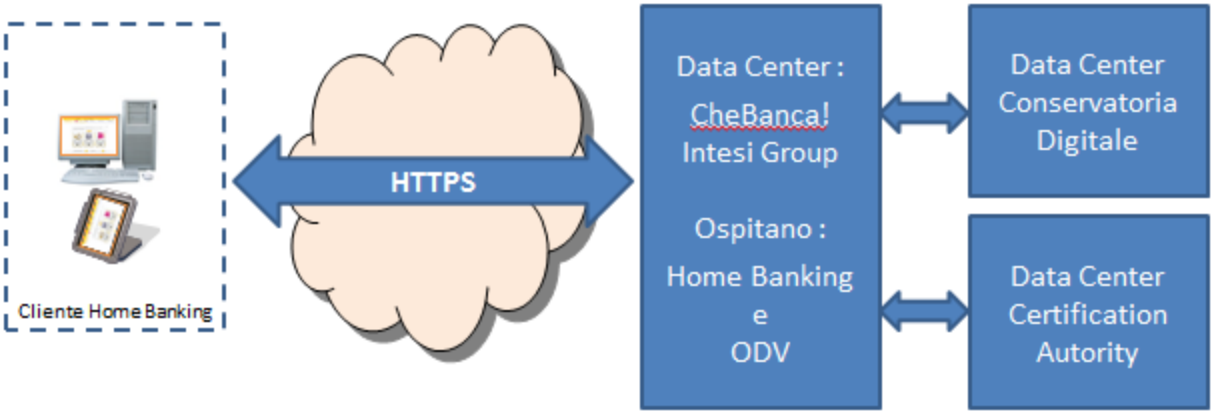

Figura 1 – Ambiente operativo dell'ODV

6.3.1 Architettura dell'ODV

6.3.1.1 Hardware

La descrizione dell'ambito fisico dell'ODV è fornita in [TDS], par. 2.4.1. La descrizione delle caratteristiche hardware e software dei server che ospitano l'ODV è fornita in [TDS], par. 2.6.

Dal punto di vista della sicurezza fisica tutti gli accessi ai Data Center sono protetti da firewall perimetrali e da firewall che isolano i diversi livelli architetturali; inoltre, le applicazioni operano su server ad alta affidabilità e configurati in cluster.

Le chiavi digitali private e pubbliche degli "Utenti FEA" impiegate nel processo di firma sono custodite centralmente in un HSM, in grado di garantire un elevato livello di sicurezza.

6.3.1.2 Software

La descrizione dell'ambito logico dell'ODV è fornita in [TDS], par. 2.4.2.

Le principali componenti dell'"Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" sono:

- **SSE**: gestisce il sistema di autenticazione forte dell'"Utente FEA".
- **PkCA**: funge da interfaccia verso la *Certification Authority* e l'HSM.
- **CaBroker**: è il sistema di attivazione delle componenti dell'ODV e di associazione delle "Credenziali di sicurezza FEA" con le chiavi digitali di firma custodite nell'HSM.
- **PkBox**, **PkBoxRremote**: gestiscono il processo di generazione e apposizione della firma digitale in uno dei formati supportati dalla vigente normativa (CAdES, PAdES e XAdES).

Nell'ambiente operativo si trovano inoltre componenti software specifici per la gestione dei vari servizi di business offerti a tutte le applicazioni CheBanca! (**CheBanca!BSP**) e per la gestione del ciclo di vita documentale di CheBanca!: template contratti, digitalizzazione contratti, modulistica, conservatoria digitale, ecc. (**DocBank**). Inoltre, l'ODV si appoggia per le sue funzionalità ad un server LDAP e a un DBMS Oracle. La *Certification Authority* è sviluppata con tecnologia J2EE (*Java2 Enterprise Edition*).

6.3.2 Caratteristiche di Sicurezza dell'ODV

6.3.2.1 Politiche di sicurezza dell'organizzazione

Le politiche di sicurezza organizzative definite in [TDS], che debbono essere rispettate per avere garanzia del corretto funzionamento dell'ODV, coprono i seguenti aspetti:

- l'utente dell'ODV (Utente FEA) è responsabile della custodia dei propri Codici Dispositivi e delle credenziali cliente CheBanca!;
- l'ODV ed il suo ambiente operativo vengono sottoposti a test di vulnerabilità con cadenza semestrale;
- l'amministrazione dell'ODV è gestita nell'ambito dei servizi già erogati per l'applicazione di *home banking*.

6.3.2.2 Ipotesi

Le ipotesi, le politiche di sicurezza organizzative ed alcuni aspetti delle minacce, così come definite nel Traguardo di Sicurezza [TDS], 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:

- si assume che l'ambiente operativo provveda all'identificazione ed autenticazione di primo livello dei clienti che accedono al sistema di *home banking*;
- si assume che le comunicazioni tra i Data Center CheBanca! e Intesi Group, così come tra "Utenti FEA" e sistema di *home banking* utilizzino protocolli che garantiscano un livello di protezione adeguato dell'integrità e della confidenzialità dei dati/informazioni in transito sulla rete;
- si assume che l'ambiente operativo consenta all'"Utente FEA" di accedere ai contratti da esso sottoscritti, per verifica e stampa;
- si assume che l'ambiente operativo (Data Center) sia certificato secondo la norma ISO 27001. Si assume inoltre che le operazioni di generazione, rinnovo e revoca delle chiavi di firma avvengano in modalità protetta tramite HSM;
- si assume che l'ODV sia installato in un ambiente fisicamente sicuro, il cui accesso sia consentito solo a personale autorizzato.

6.3.2.3 Funzioni di sicurezza

Le principali funzioni di sicurezza dell'ODV sono:

- autenticazione forte dell'"Utente FEA" mediante riconoscimento dei Codici Dispositivi contenuti nella "Matrice dispositiva" in esclusivo possesso del cliente;
- creazione dell'*hash* del documento PDF corrispondente ad un contratto selezionato tra i prodotti sottoscrivibili mediante FEA e dei Codici Dispositivi richiesti in fase di autenticazione;
- cifratura del PIN del Certificato contenuto nelle "Credenziali di sicurezza FEA";
- verifica di esistenza di un "Ticket dispositivo" valido per ogni richiesta di generazione del certificato digitale e per ogni richiesta di sottoscrizione mediante FEA di un contratto.

Le funzioni di sicurezza offerte dall'ambiente operativo sono:

- conservazione del contratto elettronico sottoscritto;
- recupero e verifica del contratto elettronico sottoscritto;
- servizi di comunicazione;
- servizio di generazione della firma elettronica;
- servizio di creazione, utilizzo e revoca del certificato digitale;
- servizi di protezione dati;
- amministrazione del sistema.

Per maggiori dettagli sulle funzioni di sicurezza dell'ODV e del suo ambiente operativo si veda il Traguardo di Sicurezza [TDS], par. 2.8.

6.3.3 Configurazione dell'ODV

L'ODV valutato è identificato in [TDS] nel suo complesso come versione 1.0. Tale versione corrisponde all'ODV in esercizio al momento della chiusura delle attività di valutazione.

6.4 Documentazione

Trattandosi di un applicazione in esercizio, accessibile da parte dell'utente finale esclusivamente da remoto, non sono previste guide per l'installazione e la configurazione dell'ODV. All'utente finale viene resa disponibile esclusivamente la documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto. Questa documentazione 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 raccomandazioni 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 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 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 12 gennaio 2015 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 3 febbraio 2015. 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 – 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.

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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" 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
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

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

Si raccomanda ai potenziali acquirenti e/o utilizzatori del prodotto "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" 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 alle politiche di sicurezza e sotto le ipotesi specificate nei capitoli 4.3 e 4.4 del Traguardo di Sicurezza [TDS]. Si consiglia ai potenziali acquirenti e/o utilizzatori 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, descritta in Appendice B – Configurazione valutata.

Poiché l'ODV è un prodotto in esercizio, si raccomanda ai suoi utilizzatori di seguire scrupolosamente quanto indicato nella Guida Utente FEA [GUI], fornita insieme all'ODV. È responsabilità dell'utente la corretta conservazione e gestione delle proprie credenziali utente e della tessera contenente i Codici Dispositivi necessari per l'accesso ai servizi dell'ODV ("Matrice dispositiva"). Inoltre, si raccomanda agli utilizzatori dell'ODV di prestare particolare attenzione alla sicurezza dei dispositivi personali utilizzati per l'accesso remoto all'ODV.

L'ODV è un'applicazione progettata per realizzare, unitamente al proprio ambiente operativo, 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.

Nel caso di una futura rivalutazione di questo prodotto, non ostante attualmente non vi siano vincoli normativi in tal senso per le soluzioni di FEA, si raccomanda al Fornitore di aggiornare gli algoritmi di *hashing* attualmente in uso (SHA-1, RIPEMD-160) che non sono più raccomandati. In particolare, per quanto riguarda la generazione del *digest* del documento elettronico da firmare, la normativa italiana vigente sulla firma digitale prevede l'uso di algoritmi della famiglia SHA-2.

Si assume che gli operatori di CheBanca! preposti all'amministrazione e manutenzione del servizio di Firma Elettronica Avanzata 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.

Si sottolinea infine che la sicurezza dell'operatività dell'ODV è condizionata alla corretta implementazione e rispetto delle Politiche di sicurezza organizzative e delle ipotesi descritte in [TDS], par. 4.3 e 4.4, in particolare quelle relative al personale ed ai locali all'interno dei quali è installato ed opera l'ODV.

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

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

- Security Target "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", v. 3.4, 16 dicembre 2014 [TDS];
- Guida Utente FEA, v. 1.1 [GUI].

9 Appendice B – Configurazione valutata

L'ODV "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", è un'applicazione software integrata nei servizi di *home banking* offerti attraverso il sito Web www.chebanca.it. Si tratta di un prodotto attualmente in esercizio e disponibile per l'utilizzo ai potenziali utenti.

L'ODV è identificato nel Traguardo di Sicurezza [TDS] con il numero di versione 1.0. Nel seguito sono elencati i singoli componenti software dell'ODV, con le rispettive versioni verificate dai Valutatori all'atto dell'effettuazione dei test e riportate nel Rapporto Finale di Valutazione [RFV]:

- SSE: 3.15
- CABroker: 3.21
- PkBox: 1.3
- PkBox Remote: 1.3
- PkCA: 1.0

Tale lista costituisce la configurazione valutata dell'ODV.

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 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

Poiché l'ODV è un prodotto in esercizio, in accordo con il Committente i test funzionali di sicurezza, le attività di analisi delle vulnerabilità e i test di intrusione sono stati eseguiti direttamente sull'ambiente di produzione dell'Applicazione FEA di CheBanca!. Questo ha comportato la necessità di attivare una speciale procedura preparatoria da parte dell'LVS che ha comportato l'attivazione di due contratti utente *ad hoc* per gli scopi della valutazione presso una filiale CheBanca!. A seguito di tale operazione l'LVS ha ricevuto le credenziali di accesso alle applicazioni di *home banking* e la Matrice dispositiva personale, contenente i Codici Dispositivi che permettono l'autenticazione forte all'applicazione di FEA.

Una parte dei test funzionali, in particolare quelli inerenti le funzioni di autenticazione dell'Utente FEA, è stata quindi effettuata dai Valutatori da remoto, operando presso la sede dell'LVS, accedendo direttamente all'ODV mediante l'interfaccia Web del sito di *home banking* di CheBanca! (www.chebanca.it).

I Valutatori, nella fase di preparazione del piano dei test, hanno esaminato la descrizione dell'ODV riportata nel TDS ed hanno verificato che la configurazione proposta dal Committente per i test fosse coerente con quanto specificato nel Traguardo di Sicurezza [TDS] e nelle specifiche funzionali. Inoltre, prima dell'effettuazione delle singole sessioni di test i Valutatori hanno verificato che l'ODV, nelle sue diverse componenti, fosse installato e configurato come dichiarato dal Committente e riportato in Appendice B – Configurazione valutata.

10.2 Test funzionali ed indipendenti svolti dai Valutatori

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.

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.

In particolare, i test di funzionalità pianificati e svolti dall'LVS hanno coperto i seguenti aspetti di sicurezza.

Test dei servizi crittografici forniti dall'ODV

Mediante opportuni strumenti e procedure sono state verificate, sia direttamente in ambiente di produzione CheBanca!, sia *offline* le seguenti funzionalità crittografiche offerte dall'ODV:

- cifratura AES-192 del PIN di accesso alla chiave privata dell'utente custodita nell'HSM;
- funzionalità di *hashing* (SHA-1) del documento PDF da firmare (DTBS/R);
- funzionalità di *hashing* (RIPEMD-160) delle terne di codici contenute nella Matrice dispositiva.

Test dell'interfaccia utente

È stato verificato il corretto funzionamento delle funzioni dell'ODV di autenticazione e controllo di accesso ai servizi FEA, in particolare per quanto attiene l'uso dei Codici Dispositivi e la verifica di validità della sessione d'utente, mediante:

- esecuzione controllata del processo di registrazione ai servizi FEA;
- esecuzione controllata del processo di sottoscrizione di un documento a seguito della richiesta di attivazione di un servizio.

Test della funzionalità di Firma Elettronica Avanzata

È stato verificato che un documento PDF firmato, emesso al termine del processo di sottoscrizione, fosse conforme agli standard di riferimento. In particolare, i Valutatori hanno verificato il rispetto dei seguenti requisiti:

- il documento deve essere sintatticamente conforme allo standard PDF/A per la conservazione a lungo termine dei documenti;
- i campi relativi alle firme digitali debbono essere correttamente visualizzati;
- la catena di certificazione di ciascuno dei certificati di firma deve essere correttamente pubblicata;
- il documento informatico sottoscritto non può subire modifiche dopo l'apposizione della firma senza che se ne abbia evidenza.

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.

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

10.3 Analisi delle vulnerabilità e test di intrusione

Per la predisposizione delle attività di analisi delle vulnerabilità, il team di valutazione ha effettuato dapprima una ricerca tra le fonti di pubblico dominio per identificare vulnerabilità potenziali che possano essere utilizzate da un attaccante. La ricerca è stata focalizzata sulle potenziali vulnerabilità relative alle Web Application, con particolare riferimento alla sicurezza dei server web e alla corretta gestione delle connessioni cifrate SSL/TLS.

In considerazione del livello di garanzia richiesto per la valutazione e dopo un'attenta analisi dei possibili canali di attacco disponibili ad un ipotetico attaccante, i Valutatori hanno ritenuto sufficiente effettuare scansioni di vulnerabilità direttamente sull'indirizzo IP

pubblico corrispondente all'applicazione di *home banking* di cui l'ODV è parte integrante. Oltre alle scansioni di vulnerabilità, sono stati fatti tentativi di attacchi di tipo XSS (*Cross-site scripting*), di *String overflow* e di produzione di codice JavaScript malevolo.

I risultati delle prove effettuate non hanno evidenziato vulnerabilità potenziali o residue sfruttabili da un attaccante con potenziale di attacco Basic, nell'ambiente operativo dell'ODV.

Successivamente, considerato che l'ODV viene dichiarato dal Committente come applicazione di Firma Elettronica Avanzata (FEA), definita nella normativa italiana nelle "Regole tecniche in materia di firme elettroniche" [DPCM], sono stati individuati i seguenti requisiti di sicurezza specifici della FEA:

- l'identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
- 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;
- la connessione univoca della firma al documento sottoscritto.

Da questi requisiti sono state derivate le seguenti vulnerabilità potenziali per l'applicazione Firma Elettronica Avanzata di CheBanca!:

- l'attaccante firma per un altro soggetto;
- l'attaccante tenta di *bypassare* l'autenticazione forte dell'utente costituita dai Codici Dispositivi;
- l'attaccante modifica il documento informatico già firmato senza che tale modifica possa essere rilevata;
- il firmatario nega di aver avuto la possibilità di controllare quanto sottoscritto;
- il firmatario nega di aver firmato lo specifico documento che risulta sottoscritto;
- l'attaccante inserisce agenti malevoli che possono alterare il documento.

I Valutatori hanno quindi esaminato le vulnerabilità così individuate e 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).

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