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. 4/20

(Certification No.)

Prodotto: *(Product)* **Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0**

Sviluppato da: *(Developed by)* **CheBanca! S.p.A.**

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
Organizzazione:MISE/80230390587
Data:14/07/2020 13:01:09

Roma, 14 luglio 2020

Common Criteria

SOGIS IT SECURITY CERTIFICATE

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

Applicazione Firma Elettronica Avanzata di CheBanca! v2.0

OCSI/CERT/TEC/09/2017/RC

Versione 1.0

14 luglio 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	14/07/2020

2 Indice

3 Elenco degli acronimi

AES Advanced Encryption Standard

API Application Programming Interface

CA Certification Authority

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

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

IPsec Internet Protocol Security

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

OTP One-time Password

PC Personal Computer

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
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSH	Secure SHell
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
UAT	User Acceptance Test
VPN	Virtual Private Network

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “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-2012-09-004, “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

[NIS120] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/20 – Condizioni per l'effettuazione di test da remoto in valutazioni Common Criteria, versione 1.0, 6 aprile 2020

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

4.2 Documenti tecnici

[GUI] "Guida Utente FEA - Applicazione Firma Elettronica Avanzata di CheBanca! Versione 2.0", versione 2.0, CheBanca! S.p.A., dicembre 2017

[RC] "Rapporto di Certificazione Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0", OCSI/CERT/TEC/04/2014/RC, versione 1.0, 5 marzo 2015

[RFV] Rapporto Finale di Valutazione del prodotto "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0", Versione 1.1, Technis Blu S.r.l., 26 maggio 2020

[TDS] Security Target "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0", v. 4.4, CheBanca! S.p.A., 14 aprile 2020

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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0", sviluppata dalla società CheBanca! S.p.A., nel seguito del documento anche indicata come "Applicazione FEA di CheBanca!" o "FEA CheBanca!".

L'ODV opera all'interno di una applicazione di Home Banking ed è supportato da un servizio di Certification Authority. Compito dell'ODV è quello di consentire ad un utente di firmare documenti elettronici e di gestire firma e documenti nel rispetto della vigente normativa sulla FEA ([eIDAS], [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).

Il presente Rapporto di Certificazione è stato emesso a conclusione della ri-certificazione di una precedente versione dello stesso ODV (Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0), già certificato dall'OCSI (Certificato n. 1/15 del 5 marzo 2015 [RC]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore CheBanca! S.p.A. è stato necessario procedere a una ri-certificazione dell'ODV. L'LVS Technis Blu S.r.l. ha potuto riutilizzare parte della documentazione e delle evidenze già fornite nella precedente valutazione.

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.

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente ODV, per facilità di lettura il presente Rapporto di Certificazione è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo ODV "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0".

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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" ai requisiti generali di sicurezza 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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 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	Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0
Traguardo di Sicurezza	Security Target "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0", v. 4.4, 14 aprile 2020
Livello di garanzia	EAL1 con l'aggiunta di ASE_OBJ.2, ASE_REQ.2 e 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. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	19 ottobre 2017
Data di fine della valutazione	26 maggio 2020

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 un'applicazione software denominata "Firma Elettronica Avanzata di CheBanca! v. 2.0", progettata per rispondere, unitamente al proprio ambiente operativo, ai requisiti della Firma Elettronica Avanzata previsti dal DPCM 22 febbraio 2013 [DPCM].

L'ODV può essere utilizzato solo da parte di un "Cliente", "Prospect" o "Lead qualificato" che ha richiesto l'attivazione del servizio FEA CheBanca!, divenendo "Utente FEA". L'ODV può essere utilizzato solo per la firma elettronica dei prodotti bancari specificamente scelti e abilitati da CheBanca!. La soluzione della FEA CheBanca! si basa su un'autenticazione forte mediante l'utilizzo di Codici Dispositivi e di OTP.

I flussi operativi dell'ODV e del suo ambiente sono:

- autenticazione tramite portale Web istituzionale;
- autenticazione tramite Home Banking;
- creazione "Utente FEA";
- firma di un contratto.

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

Le principali componenti dell'Applicazione FEA di CheBanca! v. 2.0 sono:

- sistema di autenticazione forte dell'"Utente FEA";
- interfaccia verso il generatore del certificato digitale (chiavi pubbliche e private) all'interno dei dispositivi HSM;
- sistema di attivazione delle componenti dell'ODV e di associazione delle "Credenziali di sicurezza FEA" con le chiavi digitali di firma generate dall'HSM;
- sistema per l'apposizione della firma digitale in uno dei formati supportati dalla normativa.

Le componenti che realizzano l'architettura complessiva dell'Applicazione FEA di CheBanca! v2.0 sono suddivise tra quelle proprie dell'ODV e quelle dell'ambiente operativo.

La Figura 1 riporta i principali elementi che caratterizzano l'ambiente operativo dell'ODV.

Il primo elemento è costituito dai dispositivi fissi o mobili, purché in grado di ospitare un browser con la gestione di protocollo HTTPS, mediante i quali un "Prospect" o un "Cliente" può operare remotamente con i sistemi CheBanca!.

Il secondo elemento è costituito dalla rete Internet che viene utilizzata mediante protocollo sicuro HTTPS.

Il terzo elemento è costituito dal Data Center di CheBanca! e da un secondo Data Center, chiamato Intesi Group, all'interno dei quali sono operative le applicazioni di Home

Banking, i Servizi di Business e l'ODV. Quest'ultimo viene attivato solo in caso di richiesta di sottoscrizione di un nuovo prodotto bancario sottoscrivibile mediante FEA e previa ulteriore autenticazione forte.

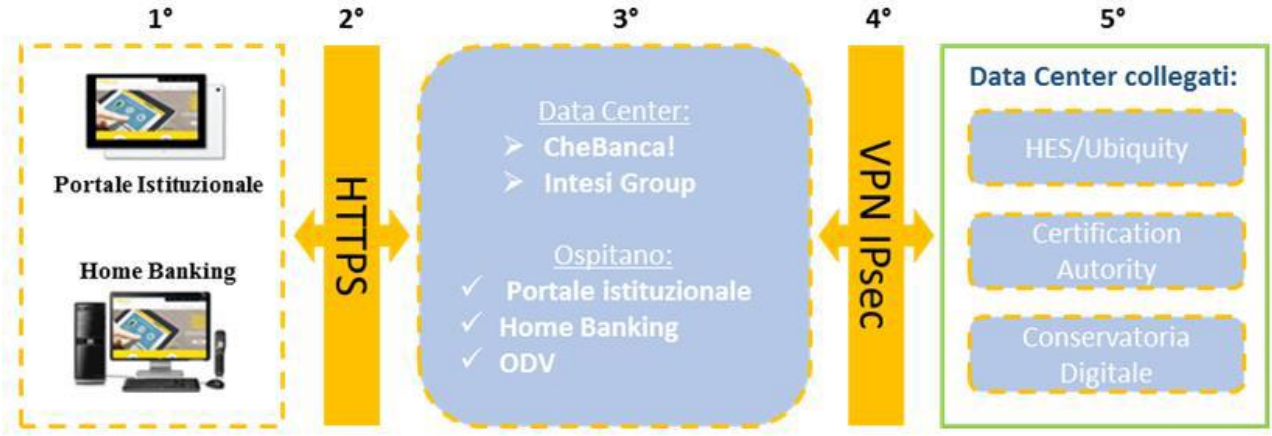

Figura 1 - Ambiente operativo dell'ODV

Mediante il quarto elemento (VPN IPsec) viene collegato il quinto elemento costituito da tre Data Center collegati col Data Center CheBanca!:

- Certification Authority, per l'emissione, la conservazione e la revoca dei certificati digitali utilizzati dall'ODV.
- Conservatoria Digitale, che ospita i contratti firmati dall'"Utente FEA" e dalla Banca.
- HES/Ubiquity, utilizzato per poter inviare il codice di conferma via SMS per le operazioni effettuate dal "Prospect" in fase di acquisizione o l'OTP utilizzato a conferma delle operazioni del "Cliente" o del "Prospect".

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.

7.3.1 Architettura dell'ODV

7.3.1.1 Ambito fisico e hardware dell'ODV

La descrizione dell'ambito fisico dell'ODV è fornita nel Traguardo di Sicurezza [TDS], par. 1.4.1.

La descrizione delle caratteristiche hardware e software dei server che ospitano l'ODV è fornita in [TDS], par. 1.6.

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.

7.3.1.2 Ambito logico dell'ODV

La descrizione dell'ambito logico dell'ODV è fornita nel Traguardo di Sicurezza [TDS], par. 1.4.2.

Le principali componenti dell'"Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" sono:

- **Middletier**: è la componente applicativa software che espone i servizi di sicurezza per la gestione e l'utilizzo delle "Credenziali clienti CheBanca!", a partire dalla generazione fino alla loro dismissione. Inoltre, il componente gestisce la parte di associazione, verifica, blocco e sblocco amministrativo degli OTP. Nel contesto specifico dell'ODV, i servizi utilizzati sono quelli di verifica delle celle dispositive, verifica OTP, creazione e verifica del "Ticket dispositivo"; integra inoltre la componente applicativa software sviluppata appositamente per l'interazione con tutte le componenti applicative dedicate alla gestione dell'ODV dal punto di vista della generazione dei Certificati Digitali, apposizione della firma, verifica delle "Credenziali di sicurezza FEA", gestione del "Ticket dispositivo".

- **PkBoxRemote**: è la componente applicativa software client che calcola l'*hash* del PDF del contratto che l'"Utente FEA" vuole firmare elettronicamente, e successivamente crea il PDF comprensivo dei metadati di firma elettronica ed *hash* del documento.

- **PkBox**: è la componente applicativa che si interfaccia con l'HSM della Certification Authority mediante il quale viene generata la firma elettronica dell'*hash* del documento con la chiave privata dell'"Utente FEA" sottoscrittore conservata nell'HSM stesso.

- **PkCA**: è la componente che fornisce l'accesso alle funzionalità di Certification Authority (gestione dei certificati digitali, rinnovo, revoca e ricerca).

Nell'ambiente operativo si trovano inoltre componenti software specifici per la gestione dei vari servizi di business offerti a tutte le applicazioni CheBanca!, per la gestione del ciclo di vita documentale di CheBanca! e per il supporto alle funzionalità dell'ODV:

- **API Gateway**: l'API Gateway attraverso una connessione sicura HTTPS espone i servizi di business che sono utilizzati mediante il browser del "Cliente" (portale Home Banking).

- **Portale Istituzionale**: è il portale mediante il quale i "Prospect" possono sottoscrivere nuovi prodotti CheBanca! e diventare quindi un "Cliente".

- **CheBanca! BSP**: è la componente software che offre vari servizi di business a tutte le applicazioni CheBanca!. I client, siano essi i front end (portali) o batch, passano da questo strato per chiamare i servizi che implementano le logiche di business distribuite sui diversi sistemi. Per l'ODV i servizi che sono utilizzati consentono al portale di Home Banking di attivare le componenti dell'ODV a fronte della richiesta di sottoscrizione dei servizi FEA e dei prodotti sottoscrivibili mediante la stessa.

- **DocBank**: è la piattaforma che gestisce il ciclo di vita documentale CheBanca! (template contratti, digitalizzazione contratti, modulistica, conservatoria digitale,

ecc..). In particolar modo per l'ODV tra le varie operazioni recupera il "Contratto" e lo passa ai servizi di Sicurezza (Middletier, PkBoxRemote) per l'effettiva apposizione della firma.

- **ORACLE**: è il *repository* all'interno del quale l'ODV esegue le ricerche delle celle dispositive di autenticazione della "Matrice Dispositiva" del "Cliente" e dei "Ticket dispositivi".

- **LDAP**: è il *repository* standard per l'interrogazione, la memorizzazione e la modifica dei servizi di directory implementato da CheBanca! mediante la soluzione CA Directory Server. Gestisce le "Credenziali di sicurezza FEA".

- **CA/HSM**: è la Certification Authority a livello Enterprise sviluppata con l'ausilio della tecnologia J2EE (Java2 Enterprise Edition) che utilizza l'HSM presso la server farm certificata ISO27001 di Intesi Group, acceduta in VPN IPsec con protocollo HTTPS.

- **Time4ID**: è la componente applicativa che fornisce l'accesso alle funzionalità di associazione e verifica dei codici OTP.

- **Provider Invio SMS**: è il fornitore che si occupa di inviare gli SMS ai "Clienti", ai "Lead qualificati" e ai "Prospect".

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. 3 e 4 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consultino il par. 1.8.2 e il cap. 7 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Autenticazione "Utenti FEA"**: autenticazione dell'"Utente FEA" mediante il riconoscimento dei codici dispositivi contenuti nella "Matrice Dispositiva", in esclusivo possesso del "Cliente", e mediante riconoscimento dei codici OTP inviati all'utente;

- **Supporto crittografico (*hash*)**: creazione dell'*hash* del PDF di un "Contratto" tra i prodotti sottoscrivibili mediante FEA (ad es. Conto Corrente, Conto Deposito, Conto Yellow, Conto Tascabile, Conto Titoli), dei codici dispositivi richiesti in fase di autenticazione;

- **Supporto crittografico (cifratura):** cifratura AES-128 del PIN del Certificato e del PIN SOTTOSCRIZIONE contenuti nelle "Credenziali di sicurezza FEA";

- **Controllo Accessi**: verifica di esistenza di un "Ticket dispositivo" valido (chiamata di *callback* dal fornitore) per ogni richiesta di generazione del certificato digitale e per ogni firma elettronica di "Contratto" tra i prodotti sottoscrivibili mediante FEA.

7.4 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 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 Funzionali (SFR) sono stati derivati direttamente dai CC Parte 2 [CC2].

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.

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].

A causa delle restrizioni agli spostamenti imposte dalle misure di contrasto alla pandemia di COVID-19 emanate dal Governo Italiano, le attività di valutazione operative (test funzionali e di intrusione) sono state svolte esclusivamente in modalità remota, in conformità alle indicazioni fornite dall'Organismo di Certificazione nella Nota Informativa dello Schema 1/20 [NIS120].

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 26 maggio 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione l'8 luglio 2020. 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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 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 "Applicazione Firma Elettronica Avanzata di CheBanca! v. 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. 4.2 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.

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.

Nel caso di una futura rivalutazione dell'ODV, si raccomanda al Fornitore di aggiornare gli algoritmi di *hashing* attualmente in uso (SHA-1, RIPEMD-160) che non sono più raccomandati per questo tipo di applicazioni.

Si assume che gli operatori di CheBanca! preposti all'amministrazione e manutenzione del servizio di FEA 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 dell'organizzazione e delle ipotesi per l'ambiente operativo descritte nel Traguardo di Sicurezza [TDS], rispettivamente nei par. 3.3 e 3.4, in particolare quelle relative al personale ed ai locali all'interno dei quali è installato ed opera l'ODV.

9 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 dell'ODV, sono i seguenti:

- Security Target "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0", v. 4.4 [TDS];
- Guida Utente FEA, v. 2.0 [GUI].

Poiché l'ODV è un prodotto in esercizio, si raccomanda ai suoi utilizzatori di seguire scrupolosamente quanto indicato nella Guida Utente FEA.

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.

10 Appendice B – Configurazione valutata

L'ODV è il prodotto software "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0". Si tratta di un prodotto attualmente in esercizio e disponibile per l'utilizzo ai potenziali utenti.

Il nome e il numero di versione identificano univocamente l'unica configurazione prevista dell'ODV a cui si applicano i risultati della valutazione.

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]:

- Middletier: 1.0
- PkBox: 1.3
- PkCA: 1.0
- PkBox Remote: 1.3

Tale lista costituisce la configurazione valutata dell'ODV.

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

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 su un ambiente di collaudo, denominato UAT (*User Acceptance Test*), appositamente predisposto dal Fornitore, che fornisce un'esatta replica dell'ambiente di esercizio.

I Valutatori hanno avuto accesso all'ambiente UAT connettendosi mediante VPN e in SSH utilizzando le credenziali messe a disposizione dal Fornitore. In questo modo hanno potuto raggiungere gli *endpoint*, ossia i portali Web interni che forniscono l'interfaccia utente per le operazioni relative al servizio di FEA, e i server che ospitano l'ODV nell'ambiente UAT.

Nella fase di preparazione del piano dei test, i Valutatori hanno verificato che la configurazione dell'ambiente UAT fosse coerente con quanto specificato nel Traguardo di Sicurezza [TDS] per l'ambiente operativo. Inoltre, prima dell'effettuazione delle singole sessioni di test i Valutatori hanno verificato che l'ODV, nelle sue diverse componenti, fosse installato e configurato nell'ambiente UAT come dichiarato dal Fornitore e riportato in Appendice B – Configurazione valutata.

11.2 Test funzionali ed indipendenti svolti dai Valutatori

Come già indicato in precedenza, le attività di test sono state svolte esclusivamente in modalità remota, in conformità alle indicazioni fornite dall'Organismo di Certificazione nella Nota Informativa dello Schema 1/20 [NIS120].

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 e che gli ambienti UAT e di esercizio fossero tra di loro coerenti.

Nella predisposizione dell'insieme dei test indipendenti da effettuare sull'ODV, i Valutatori hanno tenuto in conto il Traguardo di Sicurezza [TDS], le specifiche funzionali e la Guida Utente FEA [GUI].

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 funzionali progettati e svolti dai Valutatori hanno coperto i seguenti aspetti di sicurezza.

Test delle funzioni di autenticazione

Sono state verificate le seguenti funzionalità dell'ODV, volte a garantire che ogni richiesta di utilizzo della FEA da parte dell'utente venga validata mediante autenticazione forte di secondo livello:

- accesso come "Cliente" tramite l'applicazione di Home Banking e autenticazione di secondo livello mediante matrice dispositiva o OTP;
- accesso come "Prospect" tramite il Portale Istituzionale e autenticazione di secondo livello mediante codice numerico (PIN di Sottoscrizione), confermato mediante doppio inserimento;
- risposta dell'ODV in caso di inserimento errato dei codici della matrice dispositiva o del codice OTP, fino al blocco dell'utenza;
- risposta dell'ODV in caso di inserimento errato del PIN Sottoscrizione e/o del codice di conferma SMS.

Test delle funzioni di controllo di accesso ai servizi FEA

Sono stati verificati i seguenti aspetti dei flussi operativi dell'ODV di creazione "Utente FEA" e firma del contratto:

- esistenza e validità del "Ticket dispositivo" per ogni richiesta di attivazione della FEA per ogni richiesta di sottoscrizione di un contratto;
- validità temporale del certificato digitale per ogni richiesta di sottoscrizione di un contratto;
- corretta apposizione della firma di un contratto, in conformità alla normativa tecnica di riferimento per la firma digitale di documenti PDF.

Test delle funzioni crittografiche

È stata verificate la corretta implementazione delle seguenti funzionalità crittografiche offerte dall'ODV:

- cifratura del PIN del Certificato per le operazioni provenienti da Home Banking (relative agli "Utenti FEA") con algoritmo crittografico AES a 128bit;
- cifratura del PIN Sottoscrizione per le operazioni provenienti dal Portale Istituzionale (relative ai "Lead qualificati") con algoritmo AES a 128bit;
- applicazione della funzione di *hash* delle coppie numeriche presenti nella matrice dispositiva con algoritmo RIPEMD-160;
- firma del PDF del contratto, utilizzando come funzione di *hash* per il calcolo del *digest* l'algoritmo SHA-1.

Tutti i test effettuati dai Valutatori hanno dato esito positivo, dimostrando che l'ODV si comporta come descritto nella documentazione tecnica fornita dal Committente 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 UAT 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 effettuate durante la fase preparatoria dei test funzionali.

In una prima fase, i Valutatori hanno esaminato fonti di informazione pubbliche per la ricerca di potenziali vulnerabilità dell'ODV. In considerazione del livello di garanzia scelto per la valutazione, i Valutatori hanno ritenuto sufficiente effettuare un'analisi mediante strumenti automatici, unitamente ad attacchi di tipo "brute force" sui canali di accesso all'ODV.

La ricerca è stata automatizzata utilizzando i *tool* liberamente disponibili all'interno della distribuzione Kali Linux versione 2020.1b, in esecuzione su un PC virtualizzato in ambiente VMware.

Le scansioni hanno rilevato alcuni potenziali problemi che, dopo ulteriore analisi da parte dei Valutatori, sono stati classificati come falsi positivi, in quanto non sfruttabili nell'ambiente operativo dell'ODV.

Al termine delle sessioni di test di intrusione, i Valutatori hanno potuto verificare 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 residue.