CheBanca!

Security Target

Applicazione Firma Elettronica Avanzata di CheBanca!

Versione 1.0

CheBanca!

REVISIONI DEL DOCUMENTO

Versione	Data	Autore	Descrizione delle modifiche
1.0	30/01/2014	Nicolò Colombo	Prima emissione del documento
2.0	31/03/2014	Nicolò Colombo	Nuova organizzazione del documento conseguente al potenziamento di EAL1 con ASE_OBJ.2 e ASE_REQ.2
3.0	08/05/2014	Nicolò Colombo	Risposta al ROA n.1 e conseguente revisione delle famiglie SPD,OBJ, REQ, TSS e miglioramenti editoriali
3.1	16/07/2014	Nicolò Colombo	Modifiche a seguito dei ROA n. 2 e n. 3
3.2	14/10/2014	Nicolò Colombo	Modifiche a seguito ROA n. 4
3.3	07/11/2014	Nicolò Colombo	Ritocchi editoriali
3.4	16/12/2014	Nicolò Colombo	Modifiche a seguito ROA n. 5 e ritocchi editoriali

Tabella 1 - Revisioni del documento

Sommario

Indice delle figure

Indice delle tabelle

1 PREMESSA

1.1 Struttura del documento

Il Security Target contiene le seguenti sezioni:

- Introduzione al Security Target [Rif. § 2]: questa sezione fornisce una rappresentazione dell'ODV, ne descrive le caratteristiche e ne definisce l'ambito.
- Dichiarazione di conformità [Rif. § 3]: questa sezione presenta le conformità con i CC.
- Definizione del problema di sicurezza [Rif. § 4]: questa sezione riassume i beni da proteggere, le minacce, le ipotesi e le politiche di sicurezza dell'organizzazione.
- Obiettivi di sicurezza [Rif. § 5]: questa sezione descrive in maniera dettagliata gli obiettivi di sicurezza dell'ODV e del suo ambiente operativo.
- Definizione di componenti estese [Rif. § 6]: questa sezione definisce e giustifica l'utilizzo di componenti estese.
- Requisiti di sicurezza [Rif. § 7]: questa sezione definisce i Security Functional Requirements (SFR), i Security Assurance Requirements (SAR) e i razionali dei requisiti di sicurezza.
- Specifiche sommarie dell'ODV [Rif. § 8]: questa sezione descrive come gli SFR trovano riscontro nelle funzioni di sicurezza dell'ODV.
- Appendice [Rif. § 9]: questa sezione contiene la descrizione della gestione dei codici di accesso.

1.2 Acronimi

CC	Common Criteria
ST	Security Target
PP	Protection Profile
EAL	Evaluation Assurance Level
ODV	Oggetto Della Valutazione
HTTPS	HyperText Transfer Protocol over Secure Socket
SAR	Security Assurance Requirement
SF	Security Function
SFR	Security Functional Requirement
SFP	Security Function Policy
TSF	TOE Security Function
TOE	Target Of Evaluation (ODV)
FEA	Firma Elettronica Avanzata
DTBS	Document To Be Signed
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol

IT	Information Technology
PC	Personal Computer
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
CA	Certification Authority
PDF	Portable Document Format
SGSI	Sistema di Gestione della Sicurezza delle Informazioni

Tabella 2 – Acronimi

1.3 Definizioni

Vengono definiti in questa sezione termini specifici utilizzati all'interno del ST con il loro significato nello specifico contesto applicativo. Nel ST quanto i termini qui descritti vengono utilizzati con il significato qui descritto sono evidenziati in "*corsivo"*.

Termine	Definizione
Rapporto	Rappresenta l'accordo scritto intercorso tra un soggetto e CheBanca! mediante il quale il soggetto diviene *"cliente"* CheBanca!. La firma dell'accordo comporta da parte del soggetto l'accettazione delle condizioni e delle modalità di esecuzione ivi contenute.
Contratto/i	Il testo descrittivo del prodotto sottoscrivibile mediante FEA e delle sue condizioni. Il contratto è rappresentato in un file PDF.
Cliente/i	Un soggetto che ha sottoscritto un *"rapporto"* con CheBanca!.
Utente/i FEA	Un *"cliente"* CheBanca! che ha sottoscritto i servizi di utilizzo della "Applicazione Firma Elettronica Avanzata di CheBanca! Versione 1.0".
Credenziali di sicurezza FEA	Sono l'insieme delle quantità di sicurezza univocamente associate ad un *utente* dall'ODV. Sono conservate nel repository LDAP ospitato in ambiente sicuro. Sono costituite da: • l'ID del certificato, contenente il codice fiscale in chiaro del *"cliente"*, che costituisce la chiave unica di accesso per il recupero delle Credenziali di sicurezza FEA di un "*Utente FEA*". • Il PIN associato univocamente al Certificato (nel seguito indicato per brevità come PIN del Certificato), cifrato AES-192, usato per sbloccare la corrispondente chiave privata custodita nell'HSM • La data di scadenza del certificato digitale.
Ticket dispositivo	E' costituito da un codice univoco con validità temporale che viene generato contestualmente ad ogni richiesta di autenticazione forte dell'ODV che ha avuto esito positivo. E' conservato nel repository ORACLE ospitato in ambiente sicuro.

Termine	Definizione
Credenziali cliente CheBanca!	Sono l'insieme delle quantità di sicurezza univocamente associate ad un *"cliente"*. Sono conservate nel repository ORACLE ospitato in ambiente sicuro. Sono costituite da: • l'ID del *"cliente"*; • la data di nascita; • il PIN personale del *"cliente"*.
Matrice dispositiva	E' una tessera strutturata per righe e colonne, contenente i codici dispositivi numerici che il *"cliente"* deve reperire in corrispondenza dei 2 incroci "lettera/numero" richiesti per l'identificazione forte del *"cliente"* (Cosiddetta "Battaglia Navale").

Tabella 3 - Definizioni

1.4 Riferimenti

[RF1] Codice dell'amministrazione digitale (DL 7 marzo 2005 n. 82)

[RF2] Codice dell'amministrazione digitale (DL 30 dicembre 2010)

[RF3] DPCM 22 febbraio 2013 – *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71"*.

[RF4] Contratto di adesione alla Firma Elettronica Avanzata

[RF5] RIPEMD-160 is a 160-bit cryptographic hash function. It is intended to be used as a secure replacement for the 128-bit hash functions MD4, MD5, and RIPEMD. MD4 and MD5 were developed by Ron Rivest for RSA Data Security, while RIPEMD was developed in the framework of the EU project RIPE (RACE Integrity Primitives Evaluation, 1988-1992).

2 INTRODUZIONE AL SECURITY TARGET (ASE_INT)

2.1 Identificazione del security target

Titolo: Security Target v. 3.4 relativo all'ODV "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0"

Data : 16/12/2014

Autore : Nicolò Colombo

2.2 Identificazione dell'ODV

Nome del prodotto: Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0

Sviluppatore: CheBanca! S.p.A.

2.3 Panoramica dell'ODV

La funzionalità della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" ha lo scopo di facilitare l'apertura di nuovi *contratti* da parte di *clienti* che sottoscrivono l'utilizzo dei servizi di Firma Elettronica Avanzata divenendo così *utenti FEA.* In particolare l'*"Utente FEA"* ha la facoltà di firmare elettronicamente un nuovo *contratto*, senza stampare, sottoscrivere e inviare a CheBanca! la modulistica cartacea (Opening Pack), evitando di conseguenza tutti gli oneri di gestione che ne conseguono. Questa modalità elettronica di firma rappresenta l'equivalente digitale di una tradizionale firma autografa e possiede il medesimo valore legale. La soluzione consente l'immediata accettazione del *contratto* con minori tempi di attivazione dello stesso.

La "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" è una applicazione software utilizzata da un *"Utente FEA"* che può firmare elettronicamente nuovi contratti mediante gli strumenti di identificazione ed autenticazione forte in suo possesso.

I canali di utilizzo della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" sono:

- Canale WEB con interfaccia integrata nell'applicazione home banking del portale www.chebanca.it .
- Canale Servizio Clienti esterno all'ODV, in quanto la sua operatività non consente la firma elettronica dei contratti, ma solo la loro selezione (vedi figura seguente).

Figura 1 - Canali di utilizzo della FEA

Per accedere al servizio della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" il *"cliente"*, deve prima accedere al portale home banking mediante la procedura di identificazione ed autenticazione e l'uso delle proprie *"Credenziali cliente CheBanca!"*. Una volta entrato nel portale home banking per utilizzare l'ODV il *"cliente"* deve effettuare un secondo livello di autenticazione di tipo forte (Rif. § "9 - APPENDICE A - GESTIONE CODICI DI ACCESSO").

L'ODV è una applicazione software accessibile da un qualsiasi elaboratore (PC, tablet, telefono, etc.) sul quale sia possibile utilizzare un browser con protocollo sicuro HTTPS per l'uso del portale di Home Banking CheBanca!.

2.3.1 Panoramica dell'ambiente operativo

L'ambiente operativo è caratterizzato dai principali elementi riportati nella figura seguente.

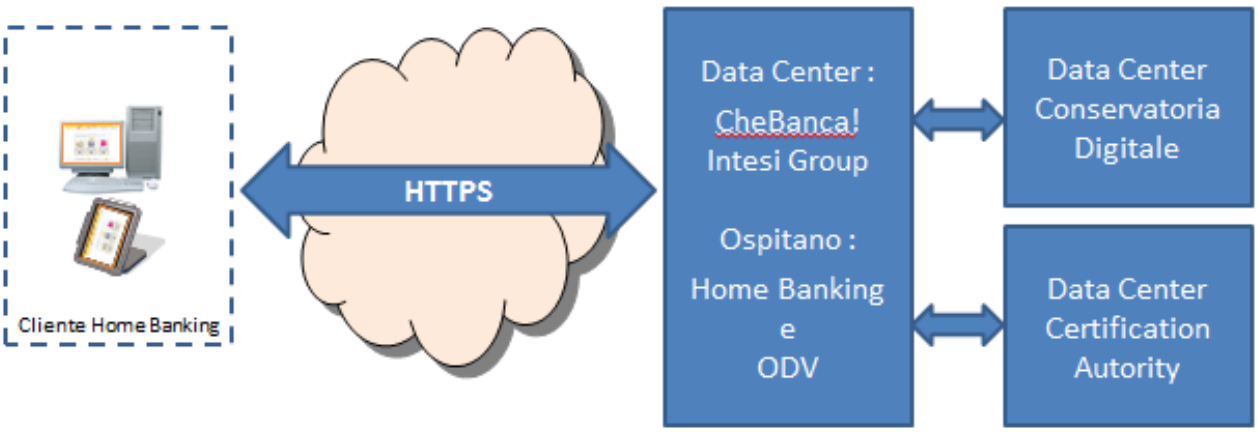

Figura 2 - Ambiente Operativo

Partendo da sinistra vediamo gli elementi che compongono l'ambiente operativo.

Il primo elemento è costituito dal *"cliente"* di Home Banking che, mediante i propri dispositivi fissi o mobili, purché in grado di ospitare un browser con la gestione di protocollo HTTPS, opera remotamente sul proprio conto CheBanca!.

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

Il terzo elemento è in realtà 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 la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0". Quest'ultima viene attivata solo in caso di richiesta di sottoscrizione di un nuovo prodotto bancario sottoscrivibile mediante FEA e previa ulteriore autenticazione forte mediante Codici Dispositivi (Rif. § "9 - APPENDICE A - GESTIONE CODICI DI ACCESSO"). I Data Center di CheBanca! e quello Intesi Group sono certificati ISO27001 e sono soggetti a verifiche semestrali di Vulnerability Assessment e Penetration Test.

Il quarto elemento è costituito da due Data Center certificati ISO27001 collegati col Data Center CheBanca! mediante VPN IPsec:

- quello che ospita la Certification Autority per l'emissione, la conservazione e la revoca dei certificati digitali, utilizzati dall'applicazione di Firma Elettronica Avanzata;
- quello che ospita i servizi di Conservatoria Digitale, fra cui i contratti firmati dall'*Utente FEA"* e dalla Banca.

2.4 Descrizione dell'ODV

L'ODV è una applicazione software, denominata Firma Elettronica Avanzata di CheBanca! v. 1.0, progettata per rispondere, unitamente al proprio ambiente operativo, ai requisiti della Firma Elettronica Avanzata previsti dal DPCM 22 febbraio 2013 **[RF3]**.

2.4.1 Ambito fisico

Lo schema seguente illustra l'architettura nel suo insieme prendendo in considerazione tutte quelle componenti che la costituiscono. All'interno dello schema viene chiaramente identificato l'ODV e le sue componenti applicative. Lo schema mostra quali componenti sono ospitate nel Data Center CheBanca! e quali quelle ospitate nel Data Center Intesi Group. Vengono infine indicati i principali flussi tra le varie componenti.

All'interno del riquadro "Data Center CheBanca!" le componenti applicative sono distinte tra quelle proprie dell'ODV e quelle di ambiente esterne ad esso. La stessa indicazione viene fornita relativamente al riquadro "Data Center Intesi Group". Vengono indicati i protocolli di trasporto ed applicativi sicuri che sono utilizzati tra i due Data Center e tra il *"cliente"* di Home Banking e il Data Center CheBanca!.

Da un punto di vista fisico 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.

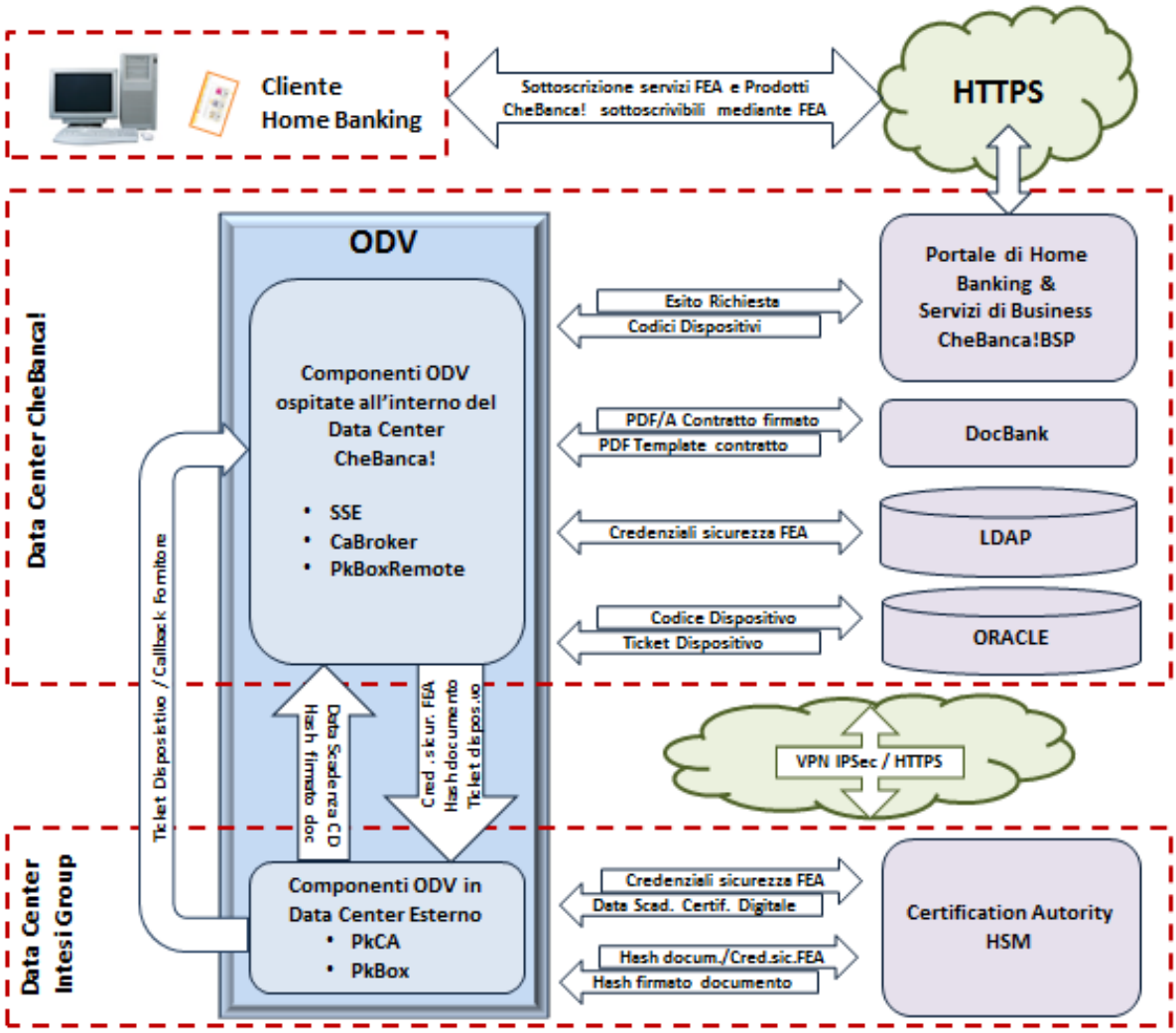

Figura 3 - Architettura generale

Le componenti che realizzano l'architettura complessiva sono suddivise tra quelle proprie dell'ODV e quelle dell'ambiente operativo.

COMPONENTI DELL'ODV

CABroker: è 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"*.

SSE: 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. Nel contesto specifico dell'ODV, i servizi utilizzati sono quelli di verifica delle celle dispositive e creazione e verifica 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).

COMPONENTI DELL'AMBIENTE

CheBanca!BSP: è la componente software che offre vari servizi di business a tutte le applicazioni CheBanca!. I client, siano essi i frontend (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 (CABroker, 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 "Thales nShield

Connect" presso la server farm certificata ISO27001 di Intesi Group, acceduta in VPN IPsec con protocollo HTTPS.

2.4.1.1 Flussi operativi dell'ODV e del suo ambiente

In questo paragrafo vengono descritti i due flussi operativi:

- attivazione dei servizi FEA
- sottoscrizione di *contratti*.

I due flussi operativi vengono scomposti nelle principali fasi costituenti in ordine di sequenza. Vengono identificate all'interno delle varie fasi le componenti applicative interessate, in grassetto quelle dell'ODV.

Flusso operativo di attivazione dei servizi FEA (si effettua solo la prima volta)

Passo 1. Il *"cliente"* per accedere via WEB in HTTPS al portale di home banking deve inserire le *"Credenziali cliente CheBanca!"*, mediante le quali viene effettuato il primo livello di identificazione ed autenticazione. All'interno del portale di home banking se il *"cliente"* decide di sottoscrivere i servizi di FEA vengono mostrate le condizioni contrattuali d'uso della FEA CheBanca!, delle quali il portale di home banking chiede l'accettazione. Se si accettano le condizioni d'uso della FEA, il portale di home banking richiede l'autenticazione forte del *"cliente"* e presenta la maschera d'inserimento di una coppia di terzine della *"Matrice dispositiva"* in esclusivo possesso del *"cliente"*.

Passo 2. "CheBanca!BSP" attiva l'ODV per l'autenticazione forte del *"cliente"* che avviene mediante **"SSE"**, la quale effettua l'hash (RIPEMD-160) delle due terzine e quindi con le *"Credenziali cliente CheBanca!"* accede a "ORACLE" per verificare se l'hash ha una corrispondenza valida. Verificato positivamente la corrispondenza crea il *"Ticket dispositivo"*.

Passo 3. "**CABroker**" viene attivato con la richiesta di creazione di un certificato digitale. "**CABroker**" crea l'*"Utente FEA"* con le *"Credenziali di sicurezza FEA"* (in particolare il PIN del Certificato viene cifrato con algoritmo AES-192) e richiama il Server LDAP per la loro conservazione. La chiave di cifratura è parte integrante del componente **"CABroker"** e non ne è prevista la sostituzione come procedura periodica. "**CABroker"** decifra il PIN del Certificato, richiama "**PkCA**" che per il tramite del *"Ticket dispositivo"* effettua la chiamata di callback dal fornitore (Data Center Intesi Group, vedi fig. 3) e verifica che per la richiesta di creazione del certificato esista effettivamente una transazione attiva da parte del *"cliente"* all'interno dei sistemi CheBanca!.

Passo 4. Superato positivamente il controllo, **"PkCA"** inoltra il PIN del Certificato, decifrato dal **"CABroker"** al passo precedente, per la richiesta di creazione del certificato digitale alla "CA/HSM" ospitata nello HSM "Thales nShield Connect". L'HSM genera la coppia di chiavi associata all'*"Utente FEA"* e restituisce la data di scadenza del certificato digitale creato. La creazione della coppia chiave pubblica (certificato) e

chiave privata è fatta in questo punto ed entrambe risiedono sull'HSM. In questo modo la coppia di chiavi generata rimane sempre custodita all'interno dell'HSM.

Passo 5. **"PkCA"** attiva la **"CABroker"** che accede al Server LDAP per l'aggiornamento dell'istanza del nuovo *"Utente FEA"* con la data di scadenza del certificato digitale e quindi restituisce l'esito a "CheBanca!BSP".

Flusso operativo di sottoscrizione di contratti

Passo 1. Il *"cliente"* per accedere via WEB in HTTPS al portale di home banking deve inserire le proprie *"Credenziali cliente CheBanca!"*, mediante le quali viene effettuato il primo livello di identificazione ed autenticazione. All'interno del portale di home banking se l'*"Utente FEA"* decide di sottoscrivere uno dei prodotti sottoscrivibili mediante FEA, il portale di home banking presenta il *contratto* da "DocBank" e quindi per proseguire chiede una autenticazione forte dell'*"Utente FEA"* mediante la maschera d'inserimento di una coppia di terzine della *"Matrice dispositiva"* in esclusivo possesso dell'*"Utente FEA"*.

Passo 2. "CheBanca!BSP" attiva l'ODV per l'autenticazione forte del *"cliente"* che avviene mediante "**SSE**", la quale effettua l'hash (RIPEMD-160) delle due terzine e quindi con le *"Credenziali cliente CheBanca!"* accede a "ORACLE" per verificare se l'hash ha una corrispondenza valida. Verificata positivamente la corrispondenza crea il *"Ticket dispositivo"*.

Passo 3. **"CABroker"** viene attivato con la richiesta di accesso alle *"Credenziali di sicurezza FEA"*, quindi ricalcola l'ID dell'*"Utente FEA"* (codice fiscale) e con questo accede al Server LDAP". Recuperate le *"Credenziali di sicurezza FEA"* **"CABroker"**, dopo aver decifrato il PIN del Certificato, attiva **"PkBoxRemote"** che elabora il documento, ne calcola l'hash (SHA-1) e quindi attiva **"PkBox"** a cui passa: l'hash del documento, il PIN del Certificato, il *"Ticket dispositivo"*.

Passo 4. **"PkBox"** per il tramite del *"Ticket dispositivo"* effettua la chiamata di callback dal fornitore (Data Center Intesi Group, vedi fig. 3) e verifica che per la richiesta di firma elettronica del *contratto* esista effettivamente una transazione attiva da parte dell'*"Utente FEA"* all'interno dei sistemi CheBanca!.

Passo 5. In caso di esito positivo della verifica **"PkBox"** attiva "CA/HSM" mediante il PIN del Certificato per il calcolo della firma dell'hash del documento. Ottenuta la firma passa l'hash firmato del documento a **"PkBoxRemote"** che crea il PDF/A con il PDF del *contratto* e i metadati di firma e hash del documento.

Passo 6. **"CABroker"** attiva "DocBank" per la conservazione del PDF/A, quindi "CheBanca!BSP" mediante cui comunica l'esito della firma del *contratto* al portale di home banking.

2.4.2 Ambito logico

La soluzione della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" si basa su una autenticazione forte mediante l'utilizzo dei Codici Dispositivi (Rif. § "9 - APPENDICE A -

GESTIONE CODICI DI ACCESSO“) in possesso del *“cliente”*. Non sono necessari quindi PIN aggiuntivi, utilizzo di generatori di token e l’installazione di componenti software specifici.

Le chiavi digitali private e pubbliche degli *“Utenti FEA”* impiegate nel processo di firma sono esclusivamente custodite centralmente nell’ HSM, in grado di garantire un elevato livello di sicurezza.

Le principali componenti della “Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0” sono:

- Sistema di autenticazione forte dell’*“Utente FEA”* (**SSE**)
- Interfaccia verso il generatore del certificato digitale (chiavi pubbliche e private) all'interno dei dispositivi HSM (**PkCA**)
- Sistema di attivazione delle componenti dell’ODV e di associazione delle *“Credenziali di sicurezza FEA”* con le chiavi digitali di firma generate dall’HSM (**CaBroker**)
- Sistema per l’apposizione della firma digitale in uno dei formati supportati dalla normativa (**PkBox, PkBoxRremote**)

Le principali funzionalità di sicurezza offerte dalla “Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0” sono:

- autenticazione dell’*“Utente FEA”* mediante riconoscimento dei codici dispositivi contenuti nella *“Matrice dispositiva”* in esclusivo possesso del *“cliente”*
- 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) 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 (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.

I formati e le modalità di firma sono tutte quelle previste dalla normativa italiana e dalle relative regole tecniche, tra cui CAdES, PAdES e XAdES.

2.5 Confine di utilizzo

La “Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0” può essere utilizzata solo da parte di un *“cliente”* che ne ha richiesto l’attivazione divenendo *“Utente FEA”*. L’essere già *“cliente”* delimita i confini di utilizzo della FEA a persone in possesso delle *credenziali clienti CheBanca!* per l’accesso ai servizi WEB di Home Banking e/o interattivi del Servizio Clienti, ed in possesso dei codici dispositivi personali (Rif. § “9 - APPENDICE A - GESTIONE CODICI DI ACCESSO“).

La “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!.

2.6 Ambiente operativo dell'ODV

Di seguito la configurazione dell'ambiente operativo che ospita e supporta l'ODV.

- Server CABroker:
  - Hardware:
    - CPU: 1 x Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz
    - RAM: 10GB
  - Software:
    - Application server: Jboss EAP 6.1
    - Jdk version: 1.6
    - J2EE version: 6
    - Sistema Operativo: Red Hat Enterprise Linux Server release 6.4
- Server SSE:
  - Hardware:
    - CPU: 2 x Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz
    - RAM: 10GB
  - Software:
    - Application server: Jboss EAP 6.1
    - Jdk version: 1.6
    - J2EE version: 6
    - Red Hat Enterprise Linux Server release 6.4
- Server BSP:
  - Hardware:
    - CPU: 24 x P7
    - RAM: 20GB
  - Software:
    - Application Server: WebSphere AS 8
    - Jdk Version: 1.6
    - J2EE version: 6
    - Sistema Operativo: AIX 1 6 0001E5DBD400
- Server PkBox:
  - Hardware:
    - CPU: 1 x Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
    - RAM: 10GB
  - Software:
    - Application server: Tomcat 4.1.31
    - Jdk version: 1.6
    - Sistema Operativo: Red Hat Enterprise Linux Server release 5.4
- Server PkCA:
  - Hardware:
    - CPU: 1 CPU
    - RAM: 2GB
  - Software:
    - Application server: Tomcat 6.0.24
    - Jdk version: 1.6
    - Sistema Operativo: Red Hat Enterprise Linux Server release 6.4

- Server PkBox Remote:
  - Hardware:
    - CPU: 1 x Intel(R) Xeon(R) CPU X5550 @ 2.67GHz
    - RAM: 10GB
  - Software:
    - Application server: Tomcat 4.1.31
    - Jdk version: 1.6
    - Sistema Operativo: Red Hat Enterprise Linux Server release 5.4
- Oracle Data Base:
  - Sistema Operativo: AIX 6.1.0.0 (64-bit)
  - CPU: 5 x ogni nodo
  - RAM: 30 GB x ogni nodo
  - Version: 11.2.0.3.5 e 11.1.0.7.10
- LDAP:
  - Hardware:
    - CPU: 1 processore Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz con 4 core
    - RAM: 8GB
  - Software:
    - LDAP Server: CA Directory Server r12
    - Sistema Operativo: Red Hat Enterprise Linux Server release 6.3
- HSM:
  - Modello: Thales nShield 500 F3

2.7 Ruoli utente

Il ruolo utente della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" è:

Utente FEA, richiedente ed utilizzatore dell'ODV, è il soggetto fisico che ha aperto un conto CheBanca! e che quindi è in possesso delle *"Credenziali cliente CheBanca!"*. Mediante queste credenziali è in grado di accedere direttamente all'applicazione di home banking dall'interno della quale, per mezzo dei codici della *"Matrice dispositiva"* (richiesti per ogni operazione di tipo dispositivo) e delle *"Credenziali di sicurezza FEA"*, può tra l'altro sottoscrivere nuovi prodotti bancari mediante le funzioni dell'ODV.

2.8 Funzioni di sicurezza

Le funzioni di sicurezza dell'ODV vengono applicate ad un *"Utente FEA"* che utilizza la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" esclusivamente per sottoscrivere il servizio FEA o un *contratto*. L'elenco dei prodotti sottoscrivibili FEA (*contratti*) è pubblicato sul sito www.chebanca.it nella sezione dedicata alla FEA all'interno del portale di home banking.

2.8.1 Funzioni di sicurezza fornite dall'ambiente operativo

Conservazione del contratto elettronico sottoscritto

CheBanca! provvede all'archiviazione digitale dei *contratti* sottoscritti con firma elettronica avanzata per almeno 10 anni in ottemperanza alle indicazioni normative ([**RF1**] e [**RF2**]). A tal fine CheBanca! si avvale del servizio di Conservazione Sostitutiva (come definita dalla deliberazione CNIPA n. 11/2004 ed eventuali modifiche successive) che si occupa della conservazione del contratto elettronico e dell'archiviazione di tutte le evidenze informatiche necessarie a comprovarne l'integrità, la leggibilità, l'assenza di modifiche dopo l'apposizione delle firme e l'autenticità delle firme apposte.

Recupero e verifica del contratto elettronico sottoscritto

Il *"cliente"* può recuperare il *contratto* elettronico sottoscritto attraverso l'apposita funzionalità disponibile in Area Clienti dopo che lo stesso è stato firmato dalla banca.

Il *"cliente"* può verificare l'integrità del documento sottoscritto e la validità della firma attraverso l'apposita funzione disponibile in Area Clienti.

In alternativa il *"cliente"* può procedere in autonomia, seguendo le linee guida pubblicate sul sito, attraverso i passi:

- Salvataggio sul proprio computer del *contratto* elettronico sottoscritto (formato pdf)
- Configurazione del programma "pdf reader" (es: Acrobat Reader) in modo che utilizzi il certificato digitale CheBanca! per la verifica delle firme elettroniche
- Apertura del file con il programma "pdf reader" (es: Acrobat Reader)
- Scaricamento del *certificato* per la verifica

In ogni caso, l'adesione al servizio non esclude la possibilità per il *"cliente"* di richiedere in ogni momento una copia cartacea del contratto sottoscritto.

Servizi di comunicazione

L'ambiente operativo mette a disposizione i seguenti protocolli sicuri di comunicazione:

- protocollo HTTPS per le comunicazioni tra i clienti e CheBanca!
- protocollo HTTPS per le comunicazioni tra CheBanca! e Intesi Group e viceversa
- protocollo VPN IPsec per le comunicazioni fra il Data Center CheBanca! e Intesi Group

Servizio di generazione della firma elettronica

Il sistema di sicurezza realizzato da CheBanca! per la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" prevede che la generazione della Firma Elettronica venga

eseguita dall'ambiente operativo ed in particolare dall'HSM posto nel Data Center Intesi Group.

Servizio di creazione, utilizzo e revoca del certificato digitale

Il sistema di sicurezza realizzato da CheBanca! per la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 1.0" prevede l'utilizzo di un certificato digitale associato univocamente all'*"Utente FEA"* e utilizzato nel processo di firma per contrassegnare il contratto elettronico sottoscritto. CheBanca! implementa tutte le indicazioni normative per l'accesso sicuro al certificato digitale, che può essere sbloccato solo attraverso l'utilizzo dei codici dispositivi in possesso esclusivo del *"cliente"* e delle *"Credenziali di sicurezza FEA"*.

Quando *l'"Utente FEA"* cessa di essere *"cliente"* CheBanca! oppure desidera recedere dal servizio FEA, il certificato associato al medesimo viene revocato.

Servizi di protezione dati

Il certificato digitale e le relative chiavi pubbliche e private dell'*"Utente FEA"* dell'ODV utilizzate nel processo di firma sono custodite esclusivamente centralmente nell' HSM, che garantisce un elevato livello di sicurezza.

I codici dispositivi, le *"Credenziali cliente CheBanca!"* ed i *ticket dispositivi* sono custoditi nel DB Oracle ed usufruiscono delle misure di sicurezza adottate.

Le *"Credenziali di sicurezza FEA"* sono custodite all'interno di un Server LDAP ed usufruiscono delle misure di sicurezza adottate.

Amministrazione del sistema

Non è prevista la figura di amministratore/gestore del sistema FEA, in quanto lo stesso viene amministrato nell'ambito del servizio di home banking.

2.8.2 Rappresentazione ad alto livello delle funzioni di sicurezza dell'ODV

La tabella seguente mostra una sintetica descrizione delle funzioni di sicurezza dell'ODV.

Codice	Funzione di sicurezza	Descrizione
ODV_Aut	Autenticazione *"Utenti FEA"*	Ogni richiesta di utilizzo dell'ODV viene validata tramite una coppia di celle della *"Matrice dispositiva"* in possesso esclusivo dell'*"Utente FEA"*.

Codice	Funzione di sicurezza	Descrizione
ODV_Crypto	Supporti crittografici	L'ODV applica algoritmi di cifratura alle *"Credenziali di sicurezza FEA"* (PIN del certificato). L'ODV applica algoritmi di hashing ai codici dispositivi e al *contratto* da firmare.
ODV_Access	Controllo Accessi	Per ogni richiesta di attivazione dei servizi FEA e per ogni richiesta di sottoscrizione contratti viene verificata la presenza un *"Ticket dispositivo"* valido per autenticare la richiesta di servizio da parte dell'*"Utente FEA"*. Per ogni richiesta di firma di un *contratto* viene verificata la validità della data di scadenza del certificato digitale.

Tabella 4 - Funzioni di sicurezza dell'ODV

3 DICHIARAZIONE DI CONFORMITÀ (ASE_CCL)

Il ST e l'ODV sono conformi alla versione 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.

La dichiarazione di conformità si riferisce a:

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012

Il pacchetto di garanzia dichiarato è EAL1 aumentato di ASE_SPD.1, ASE_OBJ.2 e ASE_REQ.2.

Questo ST non dichiara la conformità ad alcun Protection Profile.

Nel ST non sono previste estensioni.

4 DEFINIZIONE DEL PROBLEMA DI SICUREZZA (ASE_SPD)

Questa famiglia di garanzia serve per dimostrare che il problema di sicurezza indirizzato dall'ODV e dal suo ambiente operativo viene definito in maniera chiara, mediante la descrizione dei beni, delle minacce, delle politiche dell'organizzazione e delle ipotesi per l'ambiente operativo (IT e non IT).

4.1 Beni

Documenti da firmare: Sono i *contratti* che i *clienti* intendono firmare mediante la FEA.

Credenziali: Sono le *"Credenziali di sicurezza FEA"* ed i *ticket dispositivi* che permettono agli *"Utenti FEA"* di accedere ed utilizzare le funzioni dell'ODV.

4.2 Minacce

Di seguito vengono elencate le minacce che sono state considerate per l'ODV.

M.User: impersonificazione dell'*"Utente FEA"*.
Soggetti non autorizzati possono accedere alle funzioni dell'ODV appropriandosi delle credenziali di un *"Utente FEA"* (bene minacciato). L'attaccante può svolgere quindi azioni malevoli e dannose nei confronti dell'*"Utente FEA"*, titolare delle credenziali stesse.

M.Repud: azione di ripudio.
Un *"Utente FEA"* nega di aver firmato un documento da firmare (bene minacciato). In questo caso l'utente può rivalersi sulla banca, creando un contenzioso.

M.Modif: modifica dei documenti.
Un attaccante modifica il documento da firmare (bene minacciato). Così il documento usato dall'ODV non coincide con il documento che l'*"Utente FEA"* intendeva firmare.

4.3 Politiche di sicurezza dell'organizzazione

P.Codici: Il contratto che l'utente deve sottoscrivere per l'adesione alla FEA riporta le politiche stabilite da CheBanca! per l'utilizzo del servizio [RF4] ed in particolare dà al *"cliente"* la responsabilità della custodia dei propri codici dispositivi e delle credenziali *"cliente"* CheBanca!.

P.Test: Al fine di mantenere elevato il grado di sicurezza dell'ODV e del suo ambiente, l'organizzazione di CheBanca! stabilisce che l'ODV ed il suo ambiente operativo devono essere sottoposti a test di vulnerabilità con regolarità almeno ogni sei mesi.

P.Admin: L'organizzazione di CheBanca! ha stabilito che l'amministrazione dell'applicazione FEA venga gestita nell'ambito dei servizi già erogati per l'applicazione di home banking, rispettando le regole di distribuzione delle responsabilità stabilite dalla banca.

4.4 Ipotesi per l'ambiente operativo

Nel seguito sono descritte le ipotesi per l'ambiente operativo.

I.Idau: Si assume che l'ambiente operativo, mediante l'applicazione di home banking, provveda all'identificazione ed autenticazione di primo livello dei *clienti* che in una fase immediatamente successiva chiederanno di aderire alla FEA per la sottoscrizione di un nuovo contratto.

I.Com: Si assume che le comunicazioni tra i Data Center CheBanca! e IntesiGroup, così come tra *"Utenti FEA"* e CheBanca! utilizzino protocolli che garantiscano un livello di protezione adeguato dell'integrità e della confidenzialità dei dati/informazioni in transito sulla rete. In particolare si assume che l'*"Utente FEA"* comunichi con CheBanca! in HTTPS, mentre le comunicazioni tra i Data Center CheBanca! e IntesiGroup avvengano in HTTPS su canale VPN/IPSEC.

I.Control: Si assume che l'ambiente operativo, tramite l'applicazione di home banking, permetta all'*"Utente FEA"* di accedere ai contratti dal medesimo sottoscritti, per verifica e stampa.

I.Prot: Si assume che l'ambiente operativo sia certificato secondo la norma ISO 27001, in modo che, attraverso i controlli previsti dalla citata norma, sia implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), a tutela della Riservatezza, Integrità e Disponibilità delle informazioni gestite. Si assume inoltre che le operazioni di generazione, rinnovo e revoca delle chiavi di firma avvengano in modalità protetta tramite HSM.

I.Amb: Si assume che l'ODV sia installato in un ambiente fisicamente sicuro, il cui accesso sia concesso solo a personale autorizzato.

5 OBIETTIVI DI SICUREZZA (ASE_OBJ)

Questo paragrafo definisce gli obiettivi di sicurezza dell'ODV e del suo ambiente operativo. Gli obiettivi di sicurezza stabiliscono il comportamento atteso nel contrastare le minacce, supportare le ipotesi e le politiche dell'organizzazione.

5.1 Obiettivi di sicurezza per l'ODV

Obiettivo	Descrizione
OO.User	L'ODV, a valle della identificazione e autenticazione del *"cliente"* gestita dall'applicazione di home banking, deve adottare ulteriori procedure di autenticazione, prima di permettere ai *clienti* di accedere ai servizi FEA.
OO.SC	L'ODV deve proteggere il PIN del Certificato mediante cifratura all'atto della creazione, per garantirne la confidenzialità. L'ODV deve applicare algoritmi di hashing ai codici dispositivi e ai *contratti*.
OO.Ticket	L'ODV deve controllare la validità dei *ticket dispositivi* prima di consentire il rilascio di credenziali di firma o la firma dei *contratti*. L'ODV deve controllare la validità della data di scadenza del certificato digitale prima della firma dei *contratti*.

Tabella 5 - Obiettivi di sicurezza per l'ODV

5.2 Obiettivi di sicurezza per l'ambiente operativo

Obiettivo	Descrizione
OE.Idau	Il *"cliente"* prima di accedere all'ODV deve effettuare la procedura di autenticazione all'applicazione di home banking, attraverso l'immissione delle *"Credenziali cliente CheBanca!"* (codice cliente, data di nascita, PIN), in possesso del *"cliente"* stesso.
OE.Network	La rete di comunicazione deve realizzare un elevato livello di protezione al fine di garantire l'integrità e la confidenzialità delle informazioni inerenti l'ODV che viaggiano sulla rete: *"Matrice dispositiva"*, *"Ticket dispositivo"*, credenziali di sicurezza, già riportate nella descrizione dei flussi operativi al par. 2.4.1.1.

Obiettivo	Descrizione
OE.Admin	L'amministrazione dell'applicazione FEA deve essere gestita nell'ambito dei servizi già erogati per l'applicazione di home banking, rispettando le regole di distribuzione delle responsabilità stabilite da CheBanca!. Tutto il personale indirettamente coinvolto nella gestione dell'ODV deve essere scelto tra personale fidato e addestrato alla corretta gestione dell'ODV.
OE.Ver	L'ambiente operativo, attraverso l'applicazione di home banking, deve fornire al *"cliente"* la possibilità di rivedere i propri *contratti* sottoscritti via FEA, di stamparli e di scaricarli sul proprio PC.
OE.Protect	Tutti gli accessi logici ai Data Center devono essere protetti da firewall perimetrali e da firewall che isolano i diversi livelli architetturali, ed inoltre le applicazioni devono operare su server ad alta affidabilità e configurati in cluster. Quanto sopra per garantire la riservatezza, l'integrità, la disponibilità delle informazioni trattate. La generazione, rinnovo e revoca delle chiavi di firma deve avvenire tramite HSM. Le *"Credenziali di sicurezza FEA"*, le *credenziali clienti CheBanca!*, il *"Ticket dispositivo"* ed i documenti firmati dall'*"Utente FEA"* devono essere memorizzati e custoditi in DB Oracle e/o Server LDAP ed usufruire quindi delle misure di sicurezza adottate dagli ambienti ospitanti (certificati ISO 27001).
OE.Ambiente	L'organizzazione deve assicurare che l'ODV sia installato in ambienti sicuri e certificati ISO 27001, al fine di garantire procedure sicure nell'ambito di un SGSI.
OE.Creden	L'organizzazione, mediante la firma del contratto da parte dei *clienti*, deve impegnare i *clienti* stessi a custodire e proteggere i propri codici di identificazione ed i codici dispositivi.
OE.Test	La struttura di management che governa i sistemi IT di CheBanca! deve effettuare vulnerability assessment e penetration test sull'ODV e sul suo ambiente operativo, almeno ogni sei mesi.

Tabella 6 - Obiettivi di sicurezza per l'ambiente operativo

5.3 Razionali degli obiettivi di sicurezza

	ODV			AMBIENTE OPERATIVO							
	OO.User	OO.Ticket	OO.SC	OE.Idau	OE.Network	OE.Admin	OE.Ver	OE.Protect	OE.Ambiente	OE.Creden	OE.Test
M.User	X	X			X						
M.Repud		X	X				X	X			X

	ODV			AMBIENTE OPERATIVO							
	OO.User	OO.Ticket	OO.SC	OE.Idau	OE.Network	OE.Admin	OE.Ver	OE.Protect	OE.Ambiente	OE.Creden	OE.Test
M.Modif			X					X			
I.Idau				X							
I.Com					X						
I.Control							X				
I.Prot								X			
I.Amb									X		
P.Codici										X	
P.Test											X
P.Admin						X					

Tabella 7 - Razionali degli obiettivi di sicurezza

M.User: impersonificazione dell'*"Utente FEA"*.

Soggetti non autorizzati possono accedere alle funzioni dell'ODV appropriandosi delle credenziali di un "Utente FEA" (bene minacciato). L'attaccante può svolgere quindi azioni malevoli e dannose nei confronti dell'"Utente FEA", titolare delle credenziali stesse. La minaccia è contrastata dai seguenti obiettivi di sicurezza per l'ODV:

OO.User: l'ODV, a valle della identificazione e autenticazione del *"cliente"* gestita dall'applicazione di home banking, deve adottare ulteriori procedure di autenticazione, prima di permettere ai *clienti* di accedere ai servizi FEA. Questo avviene tramite l'inserimento della *"Matrice dispositiva"*.

OO.Ticket: L'ODV deve controllare la validità dei ticket dispositivi prima di consentire il rilascio di credenziali di firma e la firma dei contratti. L'operazione avviene dopo l'autenticazione di livello superiore ed ha lo scopo di verificare che l'utente ha effettivamente avviato una procedura di firma elettronica. L'ODV deve controllare la validità della data di scadenza del certificato digitale prima della firma dei contratti.

OE.Network: il contrasto di minacce provenienti dall'esterno deve trovare i primi elementi di attuazione nella sicurezza delle comunicazioni. A tale scopo la rete di comunicazione deve realizzare un elevato livello di protezione per garantire l'integrità e la confidenzialità

delle informazioni inerenti l'ODV che viaggiano sulla rete, riportate nella descrizione dei flussi operativi al par. 2.4.1.1.

M.Repud: azione di ripudio.

Un "Utente FEA" nega di aver firmato un documento da firmare (bene minacciato). In questo caso l'"Utente FEA" può rivalersi sulla banca, creando un contenzioso. La minaccia è contrastata dai seguenti obiettivi di sicurezza per l'ODV:

OO.SC: l'ODV deve proteggere il PIN del Certificato mediante cifratura all'atto della creazione, per garantirne la confidenzialità. L'ODV deve applicare algoritmi di hashing ai codici dispositivi e ai *contratti*.

OO.Ticket: l'ODV deve controllare la validità dei ticket dispositivi prima di consentire il rilascio di credenziali di firma e la firma dei *contratti*. L'operazione avviene dopo l'autenticazione di livello superiore ed ha lo scopo di verificare che l'utente ha effettivamente avviato una procedura di firma elettronica. L'ODV deve controllare la validità della data di scadenza del certificato digitale prima della firma dei *contratti*.

OE.Ver: l'ambiente operativo, attraverso l'applicazione di home banking, deve fornire al *"cliente"* la possibilità di rivedere i propri *contratti* sottoscritti via FEA, di stamparli e di scaricarli sul proprio PC.

OE.Test: obiettivo dell'ambiente operativo è di proteggere i dati custoditi nei propri sistemi IT, ovunque siano fisicamente locati, con tecnologie di sicurezza informatica di alto livello e di monitorare la sicurezza con controlli in tempo reale, anche mediante l'effettuazione di test di vulnerabilità sull'ODV e sul suo ambiente operativo.

OE.Protect: Tutti gli accessi logici ai Data Center devono essere protetti da firewall perimetrali e da firewall che isolano i diversi livelli architetturali, ed inoltre le applicazioni devono operare su server ad alta affidabilità e configurati in cluster. Quanto sopra per garantire la riservatezza, l'integrità, la disponibilità. La generazione, rinnovo e revoca delle chiavi deve avvenire tramite HSM. Le *"Credenziali di sicurezza FEA"*, le *credenziali clienti CheBanca!*, il *"Ticket dispositivo"* ed i documenti firmati dall'*"Utente FEA"* devono essere memorizzati e custoditi in DB Oracle e Server LDAP ed usufruire quindi delle misure di sicurezza proprie dei DB utilizzati.

M.Modif: modifica dei documenti.

Un attaccante modifica il documento da firmare; così il documento usato dall'ODV non coincide con il documento che l'"Utente FEA" intendeva firmare. La minaccia è contrastata dai seguenti obiettivi di sicurezza per l'ODV:

OE.Network: il contrasto di minacce provenienti dall'esterno deve trovare i primi elementi di attuazione nella sicurezza delle comunicazioni. A tale scopo la rete di comunicazione deve assicurare un elevato livello di protezione per garantire l'integrità e la confidenzialità

delle informazioni inerenti l'ODV che viaggiano sulla rete, riportate nella descrizione dei flussi operativi al par. 2.4.1.1.

OE.Protect: Tutti gli accessi logici ai Data Center devono essere protetti da firewall perimetrali e da firewall che isolano i diversi livelli architetturali, ed inoltre le applicazioni devono operare su server ad alta affidabilità e configurati in cluster. Quanto sopra per garantire la riservatezza, l'integrità, la disponibilità. La generazione, rinnovo e revoca delle chiavi deve avvenire tramite HSM. Le *"Credenziali di sicurezza FEA"*, le *credenziali clienti CheBanca!*, il *"Ticket dispositivo"* ed i documenti firmati dall'*"Utente FEA"* devono essere memorizzati e custoditi in DB Oracle e Server LDAP ed usufruire quindi delle misure di sicurezza proprie dei DB utilizzati.

OO.SC: l'ODV deve proteggere il PIN del Certificato mediante cifratura all'atto della creazione, per garantirne la confidenzialità. L'ODV deve applicare algoritmi di hashing ai codici dispositivi e ai *contratti*.

I.Idau

Si assume che l'ambiente operativo, mediante l'applicazione di home banking, provveda all'identificazione ed autenticazione di primo livello dei clienti che in una fase immediatamente successiva chiederanno di aderire alla FEA per la sottoscrizione di un nuovo contratto. L'ipotesi è supportata dal seguente obiettivo:

OE.Idau: l'ipotesi è sostenuta dall'obiettivo dell'ambiente operativo, che gestisce i dati di identificazione del *"cliente"* consistenti in codice cliente, data di nascita e PIN.

I.Com

Si assume che le comunicazioni tra i Data Center CheBanca! e IntesiGroup, così come tra "Utenti FEA" e CheBanca! utilizzino protocolli che garantiscano un livello di protezione adeguato ai dati/informazioni in transito sulla rete. In particolare si assume che l'"Utente FEA" comunichi con CheBanca! in HTTPS, mentre le comunicazioni tra i Data Center CheBanca! e IntesiGroup avvengano in VPN/IPSEC.

L'ipotesi è supportata dal seguente obiettivo:

OE.Network: La rete di comunicazione deve realizzare un elevato livello di protezione al fine di garantire l'integrità e la confidenzialità delle informazioni inerenti l'ODV che viaggiano sulla rete: *"Matrice dispositiva"*, *"Ticket dispositivo"*, credenziali di sicurezza, già riportate nella descrizione dei flussi operativi al par. 2.4.1.1.

I.Control

Si assume che l'ambiente operativo, tramite l'applicazione di home banking, permetta al *"cliente"* di accedere ai contratti dal medesimo sottoscritti, per verifica e stampa. *L'ipotesi è supportata dal seguente obiettivo:*

OE.Ver: l'ambiente operativo, attraverso l'applicazione di home banking, deve fornire al *"cliente"* la possibilità di rivedere i propri *contratti* sottoscritti via FEA, di stamparli e di scaricarli sul proprio PC.

I.Prot

Si assume che l'ambiente operativo sia certificato secondo la norma ISO 27001, in modo che, attraverso i controlli previsti dalla citata norma, sia implementato un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), a tutela della Riservatezza, Integrità e Disponibilità delle informazioni gestite. Si assume inoltre che le operazioni di generazione, rinnovo e revoca delle chiavi crittografiche avvengano in modalità protetta tramite HSM.
L'ipotesi è supportata dal seguente obiettivo:

OE.Protect: obiettivo dell'ambiente operativo è di proteggere i propri sistemi IT, ovunque siano fisicamente locati, con tecnologie di sicurezza informatica di alto livello e con processi normati secondo lo standard ISO 27001, tra cui il monitoraggio della sicurezza con controlli in tempo reale e l'effettuazione periodicamente regolare di vulnerability assessment e penetration test.

I.Amb

Si assume che l'ODV sia installato in un ambiente fisicamente sicuro, accessibile solo da personale autorizzato e che abbia un sistema di gestione sicuro. *L'ipotesi è supportata dal seguente obiettivo:*

OE.Ambiente: obiettivo dell'organizzazione è di installare l'applicazione FEA in ambienti fisicamente protetti, sicuri, controllati, nell'ambito di un SGSI certificato ISO 27001.

P.Codici

Il *"cliente"* è responsabile della custodia del proprio codice dispositivo. *La politica è supportata dal seguente obiettivo*:

OE.Creden: l'adesione di un *"cliente"* al contratto FEA è regolata dalle Condizioni Generali che il *"cliente"* dichiara di accettare. Fra queste c'è l'impegno a custodire i propri codici dispositivi con attenzione.

P.Test

Al fine di mantenere elevato il grado di sicurezza dell'ODV e del suo ambiente, l'organizzazione di CheBanca! stabilisce che l'ODV ed il suo ambiente operativo devono essere sottoposti a test di vulnerabilità con regolarità almeno ogni sei mesi. *La politica è supportata dal seguente obiettivo*:

OE.Test: la struttura di management che governa i sistemi IT di CheBanca! deve effettuare vulnerability assessment e penetration test sull'ODV e sul suo ambiente operativo, almeno ogni sei mesi.

P.Admin

L'organizzazione di CheBanca! ha stabilito che l'amministrazione dell'applicazione FEA venga gestita nell'ambito dei servizi già erogati per l'applicazione di home banking, rispettando le regole di distribuzione delle responsabilità stabilite dalla banca. *La politica* è *supportata dal seguente obiettivo*:

OE.Admin: Poiché non è prevista la figura di amministratore dell'ODV, la gestione/amministrazione dell'applicazione FEA è compresa nelle attività di gestione/manutenzione del sistema di Home Banking. Tutto il personale indirettamente coinvolto nella gestione dell'ODV deve essere scelto tra personale fidato e addestrato alla corretta gestione dell'ODV stesso.

6 DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST non prevede la definizione di alcuna componente estesa.

7 REQUISITI DI SICUREZZA (ASE_REQ)

7.1 Generalità

Questa sezione definisce i requisiti funzionali di sicurezza per l'ODV.

Definisce inoltre i requisiti di garanzia soddisfatti dall'ODV.

Ogni requisito è stato estratto dai Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, Version 3.1 Rev. 4 september 2012 e dai Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 4 september 2012.

7.2 Convenzioni

Assegnazione L'operazione di assegnazione consente di specificare un parametro all'interno di un requisito. Le assegnazioni sono indicate usando un testo in grassetto all'interno di parentesi quadre **[assegnazione]**.

Selezione L'operazione di selezione permette di selezionare uno o più elementi da una lista. Le selezioni sono indicate usando testo in corsivo all'interno di parentesi quadre **[***selezione***]**.

Raffinamento L'operazione di raffinamento consiste nel dare un ulteriore dettaglio a un requisito. Le operazioni di raffinamento sono indicate usando un testo in grassetto per le aggiunte e barrando il testo da cancellare.

Iterazione L'operazione di iterazione permette di utilizzare più di una volta un componente per effettuare operazioni diverse. Una iterazione si effettua ponendo uno slash "/" alla fine del componente seguito da una stringa univoca che identifica l'iterazione.

7.3 SFR

Requisiti Funzionali		
Classi	**Famiglie**	**Descrizione**
FIA: Identification and authentication	FIA_UAU.2	User authentication before any action
	FIA_AFL.1	Authentication failure handling
FCS: Cryptographic support	FCS_COP.1	Cryptographic operation

Requisiti Funzionali		
Classi	**Famiglie**	**Descrizione**
FDP: User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ITC.1	Import of user data without security attributes
	FDP_ETC.2	Export of user data with security attributes
FMT: Security Management	FMT_SMR.1	Security roles

Tabella 8 - ODV Security Function Requirements (SFR)

7.3.1 Autenticazione utenti

FIA_UAU.2 User authentication before any action	
Hierarchical to:	No other components.
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	La procedura per l'utilizzo della FEA prevede che l'*"Utente FEA"* si sia precedentemente identificato ed autenticato all'applicazione di Home Banking, mediante l'immissione di user ID, data di nascita del cliente, PIN del cliente. A seguire, l'*"Utente FEA"* può selezionare il contratto che intende firmare mediante la FEA. Solo dopo aver scelto il contratto l'*"Utente FEA"* deve procedere all'autenticazione alla FEA. In Appendice al par. 9.1 sono descritte le caratteristiche delle credenziali di accesso.

FIA_AFL.1 Authentication failure handling	
Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [**5**] unsuccessful authentication attempts occur related to [a**uthentication based on "Matrice dispositiva"**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**block the authentication**].
Dependencies:	FIA_UID.1 Timing of identification

FIA_AFL.1 Authentication failure handling	
Notes:	Il requisito si riferisce all'autenticazione mediante i codici dispositivi. Per garantire la sicurezza del *"cliente"*, il codice di accesso e la *"Matrice dispositiva"* vengono bloccate automaticamente nel caso di 5 tentativi consecutivi errati di inserimento del *"cliente"* sull'Home Banking. L'applicazione, come ulteriore funzione di sicurezza, non presenta alcun avviso del superamento del numero di tentativi consentiti, ma inibisce le funzioni di autenticazione forte nella sessione in corso. All'atto della apertura di una nuova sessione l'applicazione segnala il blocco dei codici e della *"Matrice dispositiva"*. (v. appendice A)

FMT_SMR.1 Security roles	
Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles: [**Utente FEA**]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	

7.3.2 Cryptographic operations

FCS_COP.1/crypt	
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**192 bit**] that meet the following:[**FIPS PUB 197**].
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
Notes:	L'operazione di cifratura viene eseguita una sola volta all'accettazione dell'accordo per l'utilizzo della FEA. L'ODV cifra il PIN del Certificato e lo memorizza nel Server LDAP. L'operazione di decifratura avviene quando il PIN del Certificato viene prelevato dal server LDAP: per la creazione del certificato digitale (solo prima volta), per il recupero del certificato digitale (per ogni operazione di firma dei contratti).

FCS_COP.1/hash_document	
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**none**] that meet the following:[**FIPS PUB 180-4**].
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
Notes:	

FCS_COP.1/hash_matrix_code	
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**RIPEMD-160**] and cryptographic key sizes [**none**] that meet the following:[**RIPEMD**].
Dependencies:	FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction
Notes:	Per i riferimenti dello standard RIPEMD-160 vedi [RF5]

7.3.3 Attivazione servizi FEA

FDP_ACC.1/attivazione servizi FEA	
Hierarchical to:	No other components
FDP_ACC.1.1	The TSF shall enforce the [**attivazione servizi FEA policy**] on: [**Soggetti:** • **Utente FEA** **Oggetti:** • **Servizi FEA** **Operazioni:** • **Procedura di attivazione**].
Dependencies:	FDP_ACF.1
Notes:	

FDP_ACF.1/attivazione servizi FEA	
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**attivazione servizi FEA policy**] to objects based on the following: **[Attributi Utente FEA: Ticket dispositivo]**.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**L'Utente FEA può effettuare la procedura di Attivazione dei Servizi FEA se esiste ed è valido un Ticket dispositivo associato all'Utente FEA].**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	

FDP_ITC.1/attivazione servizi FEA	
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [**attivazione servizi FEA policy**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.1/attivazione servizi FEA	
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization
Notes:	Questa SFR fa riferimento alla seguente operazione: ricevimento dalla CA/HSM della data di scadenza del certificato digitale associato all'Utente FEA, creato durante la procedura di attivazione dei Servizi FEA.

7.3.4 Sottoscrizione contratti

FDP_ACC.1/sottoscrizione contratti	
Hierarchical to:	No other components
FDP_ACC.1.1	The TSF shall enforce the [**sottoscrizione contratti policy**] on: [**Soggetti:** • **Utente FEA** **Oggetti:** • **Contratti** **Operazioni:** • **Sottoscrizione** **]**
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	

FDP_ACF.1/sottoscrizione contratti	
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**sottoscrizione contratti policy**] to objects based on the following: [**Attributi Utente FEA:** • **Ticket dispositivo** • **Data di scadenza del certificato digitale**].

FDP_ACF.1/sottoscrizione contratti	
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**l'Utente FEA può effettuare l'operazione di sottoscrizione di un Contratto se:** • **esiste ed è valido un Ticket dispositivo associato all'Utente FEA** • **il certificato digitale dell'Utente FEA non è scaduto**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	

FDP_ITC.1/sottoscrizione contratti	
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce the [**sottoscrizione contratti policy**] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization

Notes:	Questa SFR fa riferimento alla seguente operazione: import dell'hash firmato del contratto sottoscritto

FDP_ETC.2/sottoscrizione contratti	
Hierarchical to:	No other components.
FDP_ETC.2.1	The TSF shall enforce the [**sottoscrizione contratti policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [**none**].
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Notes:	Questa SFR fa riferimento all'operazione di invio in conservatoria del PDF/A del contratto sottoscritto dall'Utente FEA.

7.4 SAR

I requisiti di garanzia per l'ODV sono quelli previsti al livello EAL1 con l'aggiunta di ASE_SPD.1, ASE_OBJ.2 e ASE_REQ.2, come specificato nella Parte 3 dei Common Criteria.

Il livello è stato scelto come livello di garanzia in quanto l'ODV opererà in un ambiente protetto, con amministratori competenti e fidati. In questo contesto si assume che eventuali attaccanti avranno un potenziale di attacco limitato, di conseguenza il livello prescelto è appropriato per fornire la garanzia necessaria a contrastare attacchi a limitato potenziale.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Assurance Class	Assurance components
ALC: Life-cycle support	ALC_CMC.1 Labelling of the ODV
	ALC_CMS.1 TOE CM coverage
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Stated security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Tabella 9 - Security Assurance Requirements (SAR)

ADV_FSP.1 Basic functional specification		
Dependencies:	None	
Developer action elements:	ADV_FSP.1.1D	The developer shall provide a functional specification.
	ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
AGD_OPE.1 Operational user guidance		
Dependencies:	ADV_FSP.1 Basic functional specification	
Developer action elements:	AGD_OPE.1.1D	The developer shall provide operational user guidance.
AGD_PRE.1 Preparative procedures		
Dependencies:	None	
Developer action elements:	AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
ALC_CMC.1 Labeling of the TOE		
Dependencies:	ALC_CMS.1 TOE CM coverage	
Developer action elements:	ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMS.1 TOE CM coverage		
Dependencies:	None	
Developer action elements:	ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.

ASE_INT.1 ST introduction	
Dependencies:	None
Developer action elements:	ASE_INT.1.1D The developer shall provide an ST introduction.
ASE_CCL.1 Conformance claims	
Dependencies:	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
Developer action elements	ASE_CCL.1.1D The developer shall provide a conformance claim. ASE_CCL.1.2D The developer shall provide a conformance claim rationale.
ASE_OBJ.2 Security objectives	
Dependencies:	ASE_SPD.1 Security problem definition
Developer action elements	ASE_OBJ.2.1D The developer shall provide a statement of security objectives. ASE_OBJ.2.2D The developer shall provide a security objectives rationale.
ASE_ECD.1 Extended components definition	
Dependencies:	None
Developer action elements	ASE_ECD.1.1D The developer shall provide a statement of security requirements. ASE_ECD.1.2D The developer shall provide an extended components definition.
ASE_REQ.2 Derived security requirements	
Dependencies:	ASE_ECD.1 Extended components definition ASE_OBJ.2 Security objectives
Developer action elements:	ASE_REQ.2.1D The developer shall provide a statement of security requirements. ASE_REQ.2.2D The developer shall provide a security requirements rationale.
ASE_SPD.1 Security Problem Definition	
Dependencies:	None
Developer action elements:	ASE_SPD.1.1D The developer shall provide a security problem definition.

ASE_TSS.1 TOE summary specification	
Dependencies:	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Developer action elements:	ASE_TSS.1.1D The developer shall provide a TOE summary specification.
ATE_IND.1 Independent testing - conformance	
Dependencies:	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements:	ATE_IND.1.1D The developer shall provide the TOE for testing.
AVA_VAN.1 Vulnerability survey	
Dependencies:	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
Developer action elements:	AVA_VAN.1.1D The developer shall provide the TOE for testing.

Tabella 10 - Dettaglio dei singoli componenti di garanzia

7.5 Razionale dei requisiti di sicurezza

La tabella seguente mostra come gli obiettivi di sicurezza dell'ODV sono realizzati dagli SFR.

SFR	OO.User	OO.SC	OO.Ticket
FIA_UAU.2	X		
FMT_SMR.1	X		
FIA_AFL.1	X		
FCS_COP.1/crypt		X	
FCS_COP.1/hash_document		X	
FCS_COP.1/hash_matrix_code		X	
FDP_ACC.1/attivazione servizi FEA			X
FDP_ACF.1/ attivazione servizi FEA			X
FDP_ITC.1/attivazione servizi FEA			X
FDP_ACC.1/sottoscrizione contratti			X
FDP_ACF.1/sottoscrizione contratti			X
FDP_ITC.1/sottoscrizione contratti			X
FDP_ETC.2			X

Tabella 11 - Razionale dei requisiti di sicurezza

OO.User: l'obiettivo dell'ODV è di applicare una autenticazione forte, a valle della identificazione ed autenticazione propri dell'applicazione di home banking, effettuata con l'utilizzo di codici dispositivi associati univocamente al *"cliente"*. L'obiettivo è soddisfatto dal SFR FIA_UAU.2, che completa il percorso di autenticazione. L'utilizzo del SFR FMT_SMR.1 permette l'associazione fra utente e ruolo. L'utilizzo del SFR FIA_AFL.1 controlla l'immissione dei codici dispositivi.

OO.SC: obiettivo dell'ODV è di proteggere il PIN del Certificato mediante cifratura all'atto della creazione, per garantirne la confidenzialità, e di applicare algoritmi di hashing ai codici dispositivi e ai *contratti*. L'obiettivo è soddisfatto dagli SFR FCS_COP.1/crypt, FCS_COP.1/hash_document e FCS_COP.1/hash_ matrix_code.

OO.Ticket: identifica le operazioni ed i controlli da eseguire prima di consentire il rilascio di credenziali di firma e permettere la firma elettronica di un documento. L'obiettivo è soddisfatto dai SFR FDP_ACC.1/attivazione servizi FEA, FDP_ACC.1/ sottoscrizione contratti, FDP_ACF.1/attivazione servizi FEA, FDP_ACF.1/sottoscrizione contratti, FDP_ITC.1/attivazione servizi FEA, FDP_ITC.1/sottoscrizione contratti, FDP_ETC.2.

7.6 Analisi delle dipendenze

La seguente Tabella mostra le dipendenze richieste dai Common Criteria per ogni SFR e SAR al livello di garanzia scelto.

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
SFR		
FIA_UAU.2	FIA_UID.1	**NOTA 1**
FIA_AFL.1	FIA_UID.1	**NOTA 1**
FMT_SMR.1	FIA_UID.1	**NOTA 1**
FCS_COP.1/crypt	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**NOTA 2** **NOTA 3**

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
FCS_COP.1/hash_document	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**NOTA 2** **NOTA 3**
FCS_COP.1/hash_matrix_code	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**NOTA 2** **NOTA 3**
FDP_ACC.1/attivazione servizi FEA	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/attivazione servizi FEA
FDP_ACC.1/sottoscrizione contratti	FDP_ACF.1 Security attribute based access control	FDP_ACF.1/sottoscrizione contratti
FDP_ACF.1/attivazione servizi FEA	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/attivazione servizi FEA **NOTA 4**
FDP_ACF.1/sottoscrizione contratti	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/sottoscrizione contratti **NOTA 4**
FDP_ITC.1/attivazione servizi FEA	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/attivazione servizi FEA **NOTA 4**
FDP_ITC.1/sottoscrizione contratti	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/sottoscrizione contratti **NOTA 4**
FDP_ETC.2	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1/sottoscrizione contratti

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
SAR		
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1 Basic functional specification	ADV_FSP.1
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1 TOE CM coverage	ALC_CMS.1
ALC_CMS.1	None	None
ATE_IND.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1
AVA_VAN.1	ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_FSP.1 AGD_OPE.1 AGD_PRE.1
ASE_INT.1	None	None
ASE_CCL.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ASE_ECD.1 Extended components definition	ASE_INT.1 ASE_REQ.2 There are no extended components
ASE_OBJ.2	ASE_SPD.1 Security problem definition	ASE_SPD.1
ASE_ECD.1	None	None
ASE_REQ.2	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition	ASE_OBJ.2 There are no extended components
ASE_SPD.1	None	None

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
ASE_TSS.1	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ASE_REQ.1 ADV_FSP.1

Tabella 12 - Tabella delle analisi delle dipendenze

Giustificazione per mancate dipendenze

NOTA 1 – La dipendenza FIA_UID.1 non è rispettata in quanto la procedura per l'utilizzo della FEA prevede che l'utente si sia precedentemente identificato ed autenticato all'applicazione di Home Banking, mediante l'immissione di user ID, data di nascita del cliente, PIN del cliente. In Appendice al par. 9.1 sono descritte le caratteristiche delle credenziali di accesso.

NOTA 2 – Per i requisiti funzionali FCS_COP.1/crypt, FCS_COP.1/hash_document e FCS_COP.1/hash_matrix_code le dipendenze con FCS_CKM.1 o FDP/ITC.1 o FDP_ITC.2 non sono rispettate in quanto le chiavi non vengono create dall'ODV essendo a carico dell'ambiente, né vengono importate.

NOTA 3 – Per i requisiti funzionali FCS_COP.1/crypt, FCS_COP.1/hash_document e FCS_COP.1/hash_matrix_code le dipendenze con FCS_CKM.4 non sono rispettate poiché l'ODV non distrugge chiavi in quanto le operazioni relative alle chiavi stesse sono a carico dell'ambiente. La chiave viene configurata all'interno dell'applicazione di Home Banking. La sostituzione della chiave utilizzata non è prevista come procedura periodica.

NOTA 4 – Per i requisiti funzionali FDP_ACF.1 e FDP_ITC.1 e le rispettive iterazioni, la dipendenza con FMT_MSA.3 non è rispettata poiché l'ODV non possiede funzioni di management, in quanto le stesse sono di pertinenza dell'ambiente operativo (vedi P.Admin e OE.Admin).

8 SPECIFICHE SOMMARIE DELL'ODV (ASE_TSS)

Questa sezione fornisce le specifiche sommarie dell'ODV, una definizione ad alto livello delle funzioni di sicurezza soddisfatte dai requisiti funzionali e di garanzia.

8.1 Riepilogo delle funzioni di sicurezza

Le funzioni di sicurezza rappresentate nel Security Target sono le seguenti:

ODV_Aut Autenticazione clienti FEA

ODV_Crypto Supporti crittografici

ODV_Access Controllo accessi

8.1.1 ODV_Aut – Autenticazione clienti FEA

Ogni richiesta di utilizzo della FEA deve essere validata tramite una coppia di codici dispositivi dalla matrice fornita al *"cliente"*. Il *"cliente"*, prima di accedere alla FEA, deve effettuare l'autenticazione forte di secondo livello utilizzando i codici dispositivi messi a sua disposizione.

Operativamente la procedura per l'utilizzo della FEA prevede che l'utente si sia precedentemente identificato ed autenticato all'applicazione di Home Banking (questa operazione è a carico dell'ambiente operativo). A questo punto l'utente deve presentare all'applicazione FEA un secondo livello di autenticazione, ottenibile mediante l'apposizione in appositi campi dei codici dispositivi. L'ODV controlla il numero di tentativi di autenticazione e blocca l'utente in caso di superamento della soglia stabilita. Ogni utente deve autenticarsi prima di eseguire le azioni per la firma elettronica di documenti. Queste operazioni realizzano le SFR **FIA_UAU.2 e FIA_AFL.1**.
Infine viene assicurata l'associazione dell'utente che aderisce alla FEA al ruolo corrispondente, per realizzare la SFR **FMT_SMR.1**.

8.1.2 ODV_Crypto – Supporti crittografici

L'ODV applica algoritmi di cifratura e di hashing ai dati scambiati fra le componenti dell'ODV e con l'ambiente operativo.

La prima implementazione della funzione di hashing viene eseguita sul *contratto* selezionato *dall'"Utente FEA"* per la sua firma. L'hash così ottenuto transita attraverso l'ODV e viene inviato all'esterno dell'ODV e firmato nell'HSM mediante la chiave privata del certificato digitale univocamente associato all'*"Utente FEA"*. Queste funzioni realizzano la SFR

FCS_COP.1/Hash_Document, implementata con algoritmo SHA-1 a 128 bit (trattasi di un troncamento da 160 a 128 bit). Successivamente, la funzione di hashing implementata con algoritmo RIPEMD-160 viene applicata sulle celle della *"Matrice dispositiva"* richieste in fase di autenticazione forte, realizzando così quanto previsto dalla SFR **FCS_COP.1/Hash_Matrix_code**.

Le operazioni di cifratura sono eseguite dalla componente dell'ODV "**CABroker**" che provvede la prima volta a cifrare con algoritmo AES-192 il PIN del Certificato. Successivamente, alla richiesta di sottoscrizioe di un contratto, "**CABroker**" decifra il PIN del Certificato, richiama "**PkCA**" che per il tramite del *"Ticket dispositivo"* effettua la chiamata di callback dal fornitore (Data Center Intesi Group, vedi fig. 3) e verifica che per la richiesta di creazione del certificato esista effettivamente una transazione attiva da parte del *"cliente"* all'interno dei sistemi CheBanca!.

Le operazioni crittografiche che l'ODV esegue sul PIN del Certificato utilizzano l'algoritmo AES (lunghezza della chiave pari a 192 bit). Queste operazioni realizzano la SFR **FCS_COP.1/Crypt.**

8.1.3 ODV_Access – Controllo Accessi

Nel Security Target sono state individuate e descritte due procedure: "attivazione servizi FEA" e "sottoscrizione contratti".

Per la procedura "attivazione servizi FEA", l'ODV attiva il processo di richiesta del certificato digitale a seguito del riconoscimento dei codici dispositivi immessi dall'utente (vedi ODV_Aut). L'ODV effettua le seguenti operazioni:

- crea l'hash dei codici dispositivi e ne verifica la validità
- in caso positivo crea le *"Credenziali di sicurezza FEA"* con la cifratura del PIN e richiama il server LDAP per la conservazione
- provvede alla creazione del *"Ticket dispositivo"* e alla verifica di validità
- in caso positivo invia le credenziali di sicurezza alla CA/HSM richiedendo la generazione del certificato digitale
- importa dalla CA/HSM la data di scadenza del certificato digitale
- aggiorna la data di scadenza delle credenziali di sicurezza sul server LDAP con la data di scadenza del certificato digitale ricevuta dalla CA/HSM.

Mediante quanto descritto, l'ODV realizza le SFR **FDP_ACC.1/attivazione servizi FEA, FDP_ACF.1/attivazione servizi FEA, FDP_ITC.1/attivazione servizi FEA**.

Per la procedura "sottoscrizione contratti" l'ODV attiva la procedura di sottoscrizione di un Contratto da parte dell'Utente FEA a seguito del riconoscimento dei codici dispositivi immessi dall'utente (vedi ODV_Aut) e della selezione del contratto da firmare.

L'ODV effettua le seguenti operazioni:

- calcola l'hash dei codici dispositivi e ne verifica la validità
- in caso positivo calcola l'ID Utente FEA (codice fiscale) e richiama il server LDAP per il recupero delle credenziali di sicurezza utente FEA
- provvede alla creazione del *"Ticket dispositivo"* e alla verifica di validità
- in caso positivo crea l'hash del DTBS
- invia a CA/HSM l'hash del DTBS e il PIN del Certificato per la firma dell'hash del DTBS
- importa l'hash firmato del DTBS
- crea il PDF/A del DTBS firmato e lo invia in Conservatoria.

Mediante quanto descritto, l'ODV realizza le SFR **FDP_ACC.1/sottoscrizione contratti, FDP_ACF.1/sottoscrizione contratti, FDP_ITC.1/sottoscrizione contratti, FDP_ETC.2.**

8.1.4 SFR e funzioni di sicurezza dell'ODV

La tabella seguente fornisce la mappatura dei SFR con le funzioni di sicurezza dell'ODV.

Functional Requirements	ODV_Aut	ODV_Crypto	ODV_Access
FIA_UAU.2	X		
FMT_SMR.1	X		
FIA_AFL.1	X		
FCS_COP.1/crypt		X	
FCS_COP.1/hash_document		X	
FCS_COP.1/hash_matrix_code		X	
FDP_ACC.1/attivazione servizi FEA			X
FDP_ACF.1/attivazione servizi FEA			X
FDP_ITC.1/attivazione servizi FEA			X
FDP_ACC.1/sottoscrizione contratti			X
FDP_ACF.1/sottoscrizione contratti			X
FDP_ITC.1/sottoscrizione contratti			X
FDP_ETC.2			X

Tabella 13 - Mappatura dei SFR con le funzioni dell'ODV

9 APPENDICE A - GESTIONE CODICI DI ACCESSO

9.1 Tipologia dei codici di accesso

L'identificazione del *"cliente"* che utilizza canali remoti, in alternativa al presentarsi di persona in una filiale della banca, avviene secondo un processo di autenticazione che sfrutta:

- lo user ID (UID o Codice Cliente);
- data di nascita del cliente;
- il PIN del cliente.

Lo user ID (UID o Codice Cliente è un codice numerico di 9 cifre univoco e non modificabile, che viene assegnato al *"cliente"* al momento dell'attivazione del primo rapporto con CheBanca!. Nel caso in cui il *"cliente"* abbia diversi rapporti attivi, manterrà come unico UID o Codice Cliente quello assegnatogli inizialmente.

Il PIN del cliente è un codice numerico di 6 cifre che assieme alla UID o Codice Cliente consente l'autenticazione del *"cliente"*. Per questo motivo il *"cliente"* è tenuto a conservare il proprio PIN con riservatezza e a bloccarlo qualora sorga il dubbio che la segretezza di informazione sia stata compromessa. Il PIN viene inviato al *"cliente"* in busta singola dopo l'attivazione del prodotto se il rapporto viene attivato a distanza.

Il PIN può essere variato dal *"cliente"* direttamente dal suo Home Banking dopo il primo accesso o durante la vita del rapporto.

Per operare dai canali remoti il *"cliente"* ha bisogno della *"Matrice dispositiva"* che contiene i codici dispositivi, una tessera strutturata per righe e colonne, contenente i codici numerici che il *"cliente"* deve reperire in corrispondenza dei 2 incroci "lettera/numero" richiesti per l'esecuzione dell'operazione (Cosiddetta "Battaglia Navale").

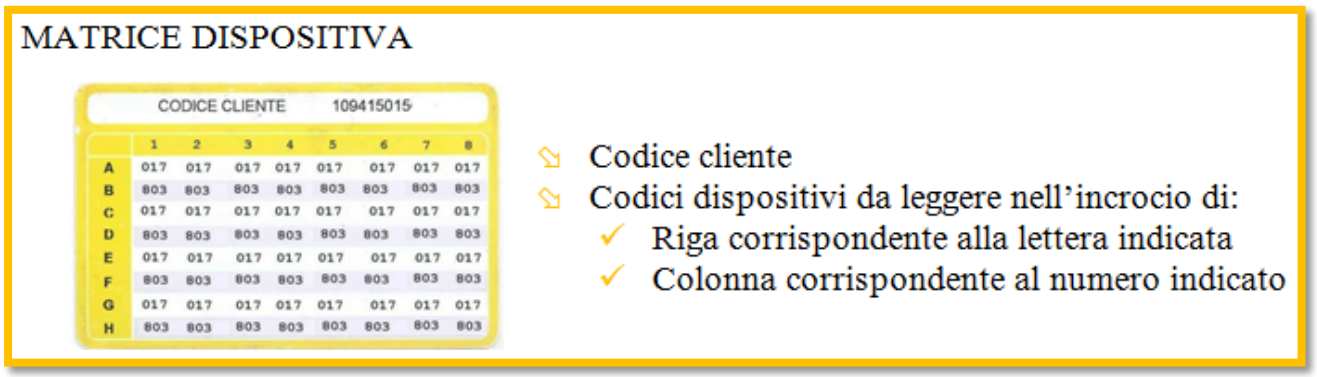

Figura 4 - Matrice dispositiva

9.2 Blocco e riemissione codici

Per garantire la sicurezza del *"cliente"*, il codice di accesso e la *"Matrice dispositiva"* vengono bloccate automaticamente nel caso di 5 tentativi consecutivi errati di inserimento del *"cliente"* sull'Home Banking. L'applicazione, come ulteriore funzione di sicurezza, non presenta alcun avviso del superamento del numero di tentativi consentiti, ma inibisce le funzioni di autenticazione forte nella sessione in corso. All'atto della apertura di una nuova sessione l'applicazione segnala il blocco dei codici e della *"Matrice dispositiva"*.

Il *"cliente"* può richiedere il blocco dei codici in caso di perdita, dimenticanza e sospetto che la sicurezza e la segretezza dei codici sia venuta meno.