CheBanca!

Security Target

Applicazione Firma Elettronica Avanzata di CheBanca!

Versione 4.4

CheBanca!

Sommario

Indice delle figure

Indice delle tabelle

0 PREMESSA

0.1 Struttura del documento

Il Security Target contiene le seguenti sezioni:

- Introduzione al Security Target [Rif. §1]: questa sezione fornisce una rappresentazione dell'ODV, ne descrive le caratteristiche e ne definisce l'ambito.
- Dichiarazione di conformità [Rif. § 2]: questa sezione presenta le conformità con i CC.
- Definizione del problema di sicurezza [Rif. §3]: questa sezione riassume i beni da proteggere, le minacce, le ipotesi e le politiche di sicurezza dell'organizzazione.
- Obiettivi di sicurezza [Rif. § 4]: 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. § 6]: 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. § 7]: questa sezione descrive come gli SFR trovano riscontro nelle funzioni di sicurezza dell'ODV.

0.2 Acronimi

CA	Certification Authority
CC	Common Criteria
DTBS	Document To Be Signed
EAL	Evaluation Assurance Level
FEA	Firma Elettronica Avanzata
HB	Home Banking
HSM	Hardware Security Module
HTTPS	HyperText Transfer Protocol over Secure Socket
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
ODV	Oggetto Della Valutazione
OTP	One-Time Password
PC	Personal Computer
PDF	Portable Document Format
PI	Portale Istituzionale
PP	Protection Profile
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
SAR	Security Assurance Requirement

SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
ST	Security Target
TOE	Target Of Evaluation (ODV)
TSF	TOE Security Function

Tabella 1- Acronimi

0.3 Definizioni

Vengono definiti in questa sezione termini specifici utilizzati all'interno del ST con il loro significato nello specifico contesto applicativo. Nel ST quando 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.
Prospect	Un soggetto che non ha mai sottoscritto un *"Rapporto"* con CheBanca!
Lead Qualificato	Un soggetto che ha iniziato la sottoscrizione di un *"Rapporto"* con CheBanca! e con il quale CheBanca! non ha ancora validato il rapporto.
Cliente/i	Un soggetto che ha sottoscritto un *"Rapporto"* con CheBanca!.
Utente/i FEA	Un soggetto per il quale CheBanca! ha generato un certificato di firma mediante l'HSM ospitato presso la server farm certificata ISO27001 di Intesi Group, acceduta in VPN IPsec con protocollo HTTPS.
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.
Codice di conferma SMS	Codice di conferma generato e inviato via SMS al numero di cellulare del "*Prospect"* da sito Istituzionale (WEB) per la sottoscrizione del servizio di FEA e del contratto.
OTP	One-Time-Password generata tramite utilizzo di App CheBanca! o Token Hardware serve a confermare operazioni dispositive.
APP CheBanca!	APP di banking che permette, tra le varie funzioni, di generare una OTP a conferma di operazioni dispositive.
Token Hardware	Token fisico che genera OTP a conferma di operazioni dispositive.

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", e costituisce la chiave unica di accesso per il recupero delle "Credenziali di sicurezza FEA" di un "Utente FEA"* • Il PIN del Certificato (cifrato AES-128), usato per sbloccare la chiave privata custodita nell'HSM • La data di scadenza del certificato digitale. Il PIN SOTTOSCRIZIONE, costituito da un codice alfanumerico di lunghezza variabile tra 8 e 12 caratteri, che viene scelto dal *"Prospect"* esclusivamente in fase di richiesta della sottoscrizione di un rapporto. Viene cifrato in AES-128 e ha valore relativo all'accettazione del servizio di firma con FEA da parte di un "*Lead Qualificato"*.
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").
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".

Tabella 2 - Definizioni

0.4 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).

1 INTRODUZIONE AL SECURITY TARGET (ASE_INT)

1.1 Identificazione del security target

Titolo: Security Target v. 4.4 relativo all'ODV "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0"

Data: 14/04/2020

Autore: Mauro Martellenghi

1.2 Identificazione dell'ODV

Nome del prodotto: Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0

Sviluppatore: CheBanca! S.p.A.

1.3 Panoramica dell'ODV

La funzionalità della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" ha lo scopo di creare un *"Utente FEA"* e di consentire allo stesso la firma elettronica di un *"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'accettazione del *"Contratto"* da parte di CheBanca! con minori tempi di attivazione dello stesso.

La funzionalità della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" viene richiamata per facilitare l'apertura di nuovi *"Contratti"* sia da parte di *"Clienti"* che da parte dei *"Prospect"*.

La "Applicazione Firma Elettronica Avanzata di CheBanca! v.2.0" è un'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 accesso CheBanca! che utilizzano la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" sono:

- **Istituzionale,** con interfaccia integrata nell'applicazione Wizard per l'acquisizione di nuovi clienti
- **Home Banking,** per i *"Clienti"* con interfaccia integrata nell'applicazione Home Banking del portale CheBanca!

- **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).

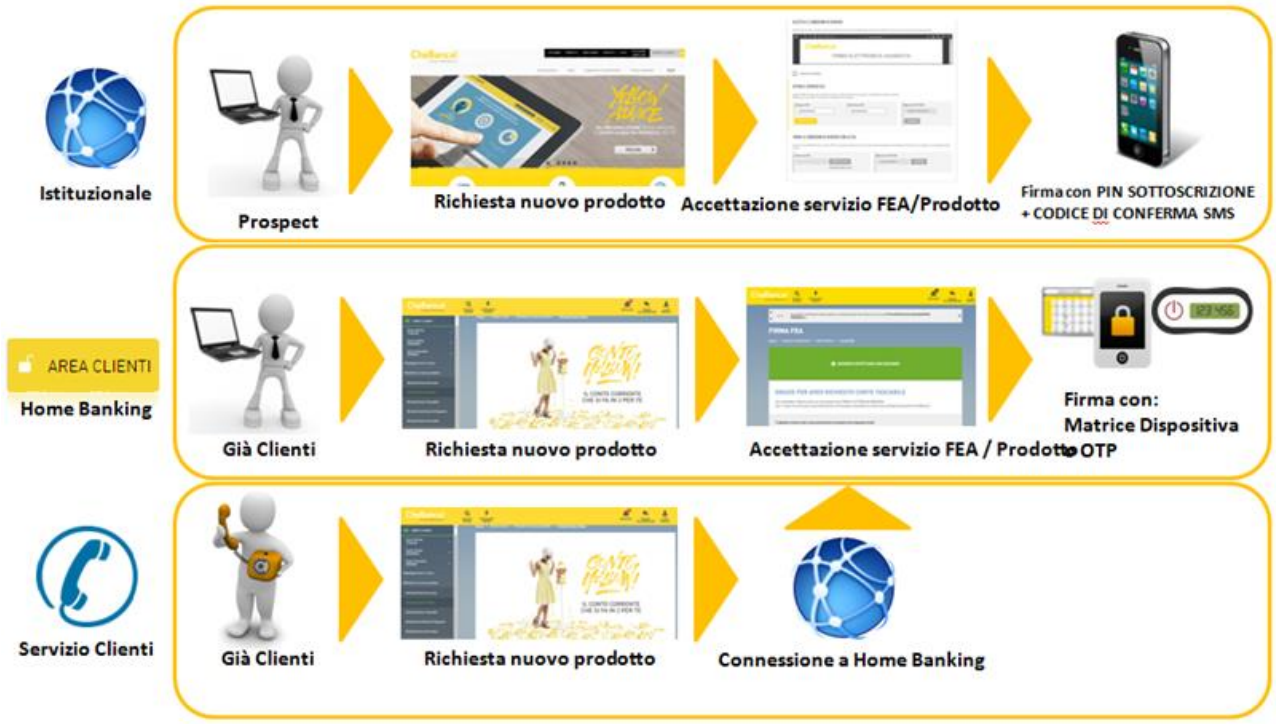

Figura 1 - Canali di utilizzo della FEA

Per divenire un *"Utente FEA"* CheBanca! consente al *"Prospect"* di poter utilizzare il canale Istituzionale; mentre il *"Cliente"* può divenire *"Utente FEA"* mediante il canale Home Banking.

1.3.1 Panoramica dell'ambiente operativo

La figura seguente riporta i principale elementi che caratterizzano l'ambiente operativo.

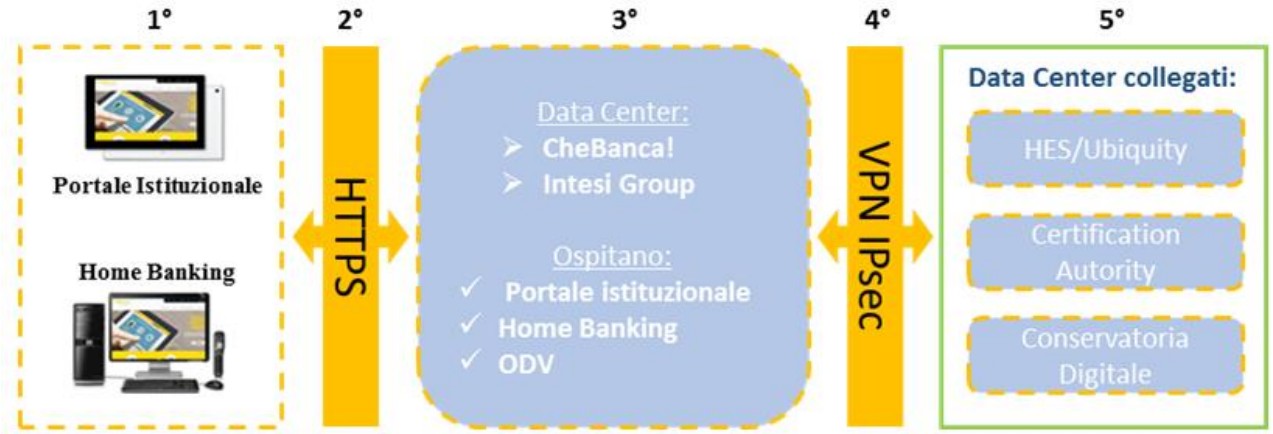

Figura 2 - Ambiente Operativo

Partendo da sinistra ne vediamo i principali elementi.

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 la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0". 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 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"*.

Il Data Center di CheBanca! e quello Intesi Group sono certificati ISO27001 e sono soggetti a verifiche semestrali di Vulnerability Assessment e Penetration Test.

1.4 Descrizione dell'ODV

L'ODV è una 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**[RF3]**.

1.4.1 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 dei riquadri "Data Center CheBanca!" e "Data Center Intesi Group" le componenti applicative sono distinte tra quelle proprie dell'ODV e quelle di ambiente esterne ad esso. Vengono indicati i protocolli di trasporto ed applicativi sicuri che sono utilizzati tra i due Data Center e tra il *"Cliente"* o il *"Prospect"* 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.

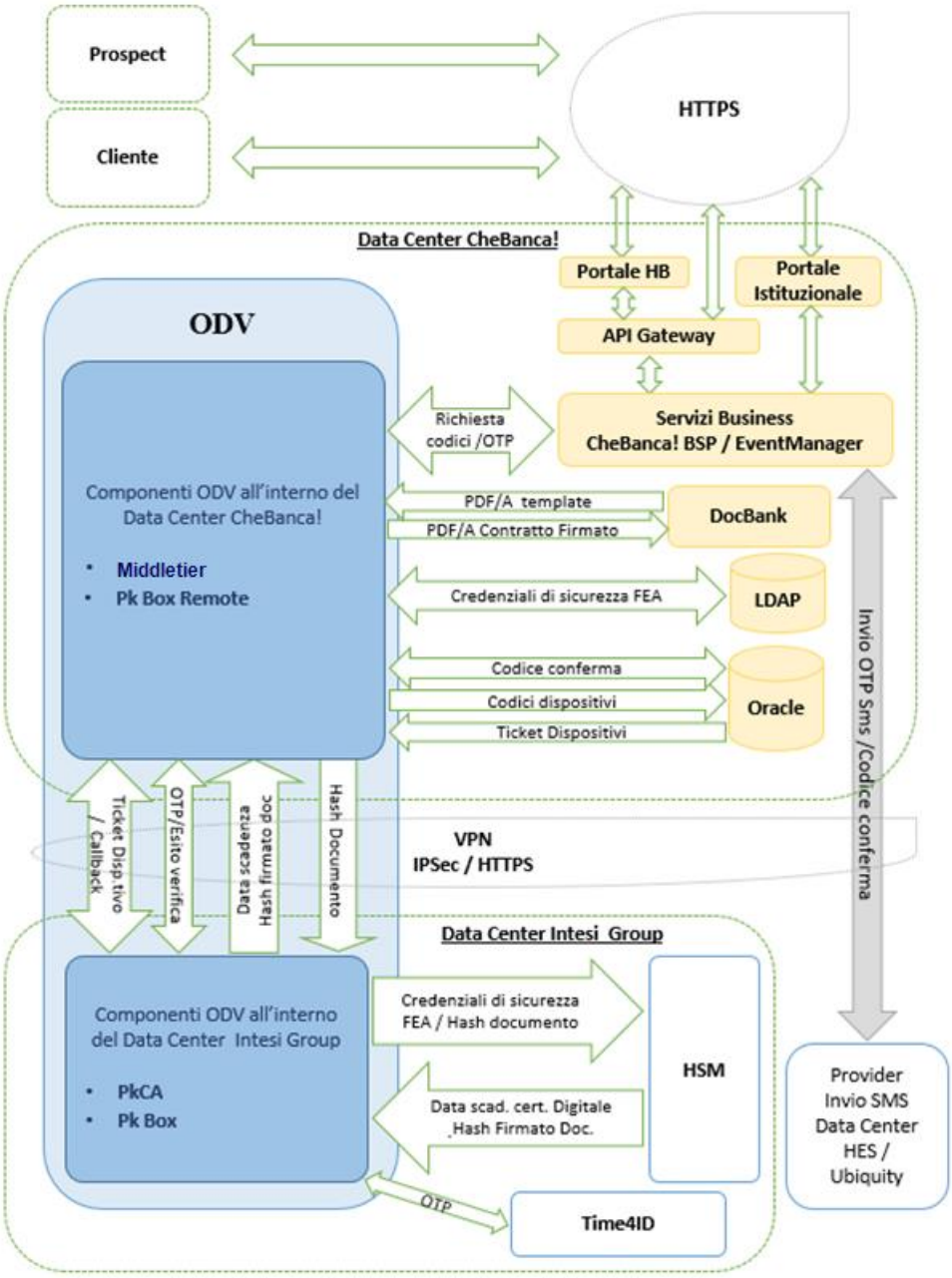

Figura 3 - Architettura generale

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

COMPONENTI DELL'ODV

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).

COMPONENTI DELL'AMBIENTE

API Gateway/:

L'API Gateway, attraverso una connessione sicura HTTPS, espone i servizi di business che sono utilizzati mediante il browser del *"Cliente"* (portale HB).

Portale Istituzionale:

è il portale mediante il quale i "*Prospect"* possono sottoscrivere nuovi prodotti CheBanca! e diventare quindi "*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"* .

1.4.1.1 Flussi operativi dell'ODV e del suo ambiente

In questo paragrafo vengono descritti i quattro flussi operativi:

- autenticazione tramite portale WEB Istituzionale
- autenticazione tramite Home Banking
- creazione *"Utente FEA"*
- firma del contratto.

I 4 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 autenticazione tramite portale Web Istituzionale

Passo 1. Il *"Prospect"* accede via WEB in HTTPS al portale Istituzionale www.chebanca.it. Inizia la sottoscrizione di un prodotto ed arrivato alla fase di riepilogo, cliccando su

conferma, gli vengono generati NDG ed IBAN e diventa un "*Lead Qualificato*". Viene quindi attivato il flusso creazione "Utente FEA".

Passo 2. Per sottoscrivere l'attivazione del servizio di firma con FEA gli viene inizialmente richiesto di visualizzare le condizioni del servizio. Deve quindi attivare il servizio mediante autenticazione, pertanto scegliere un PIN temporaneo (il PIN SOTTOSCRIZIONE) confermato mediante doppio inserimento, ed effettuare la richiesta di invio di un codice di conferma via SMS tramite Provider invio SMS.

Passo 3. CheBanca! BSP in caso di esito positivo dell'autenticazione interroga il Middletier che cifra il PIN SOTTOSCRIZIONE AES-128[(1)] e richiama LDAP per l'aggiornamento delle "*Credenziali di Sicurezza FEA*".

Passo 4. Il *"Lead Qualificato"* per procedere alla conferma della adesione al servizio FEA CheBanca! deve procedere alla identificazione forte tramite le funzioni dell'ODV. Quindi inserisce il PIN SOTTOSCRIZIONE, inserimento che attiva CheBanca! BSP che attiva il Middletier che accede a LDAP per recuperare il PIN SOTTOSCRIZIONE, lo decifra e lo verifica con quello inserito dal "*Lead Qualificato"* inviando l'esito a CheBanca! BSP.

Passo 5. CheBanca! BSP interroga il Middletier, il quale genera il codice che viene inviato tramite Provider "Invio SMS"**.** In caso di esito positivo dell'invio, CheBanca! BSP, sempre tramite Middletier, verifica la corrispondenza del codice inserito dal "*Lead Qualificato"*.

Passo 6. In caso di esito positivo viene quindi attivato il flusso "firma del contratto".

Flusso operativo di autenticazione tramite Home Banking

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.

Passo 2. Una volta autenticato al portale di Home Banking:

a) Il *"Cliente"* decide di sottoscrivere i servizi di FEA e quindi 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.

b) Il "*Cliente*" è già un "*Utente FEA*" e 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.

Passo 3. A seconda della metodologia di autenticazione associata al Cliente, viene presentata la maschera d'inserimento di una coppia di terzine della *"Matrice Dispositiva"* e, successivamente, richiesto l'inserimento OTP in esclusivo possesso del *"Cliente"*.

Passo 4. API Gateway mediante CheBanca! BSP, attiva l'ODV per l'autenticazione forte invocando **Middletier**.

[1]La chiave di cifratura è parte integrante del componente "Middletier" e non ne è prevista la sostituzione come procedura periodica.

- Nel caso in cui il Cliente abbia scelto come modalità di autenticazione la generazione di OTP mediante APP CheBanca! o mediante Token HW verranno richiamati i servizi Time4ID che verificano la bontà dell'OTP che è stato inserito dal Cliente, verificata positivamente la corrispondenza viene creato un "*Ticket dispositivo*".
- Nel caso in cui il Cliente abbia scelto l'utilizzo della matrice, viene effettuato l'hash (RIPEMD-160) delle due terzine e quindi con le *"Credenziali Cliente CheBanca!"* il Cliente accede a ORACLE per verificare se l'hash ha una corrispondenza valida. Verificato positivamente la corrispondenza crea il *"Ticket dispositivo"*.

Passo 5. **Middletier** per il tramite di CheBanca! BSP attiva API Gateway, che a seconda delle scelte effettuate al passo 2 attiva:

- Nel caso 2a la creazione dell'"*Utente FEA*"
- Nel caso 2b la firma contratto per la sottoscrizione di un nuovo prodotto.

Flusso operativo per la Creazione "*Utente FEA*"

Passo 1. **Il Middletier** è attivato da API Gateway mediante CheBanca! BSP con la richiesta di creazione di un certificato digitale. **Il Middletier** crea l'*"Utente FEA"* con le *"Credenziali di sicurezza FEA"*(in particolare il PIN del Certificato viene cifrato con algoritmo AES-128) e richiama LDAP per la loro conservazione. La chiave di cifratura è parte integrante del componente **Middletier** e non ne è prevista la sostituzione come procedura periodica. **Il Middletier** 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 2. Superato positivamente il controllo, **PkCA** inoltra il PIN del Certificato, decifrato dal **Middletier** al passo precedente, per la richiesta di creazione del certificato digitale alla CA/HSM ospitata nello HSM. 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 3. **PkCA** attiva **Middletier** che accede 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 per la firma del contratto

Passo 1. API Gateway mediante CheBanca! BSP attiva **Middletier** con la richiesta di accesso alle *"Credenziali di sicurezza FEA"*, quindi ricalcola accede a LDAP tramite il "Codice Fiscale". Recuperate le *"Credenziali di sicurezza FEA"***Middletier**, dopo aver decifrato il PIN del Certificato, attiva **PkBoxRemote** che elabora il documento di adesione alla FEA, ne calcola l'hash (SHA-1) e quindi attiva **PkBox** a cui passa: l'hash del

documento, il PIN del Certificato, la data di scadenza del certificato, il *"Ticket dispositivo"*.

Passo 2. **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!. In caso di esito positivo verifica che la data del certificato non sia scaduta.

Passo 3. In caso di esito positivo dei controlli al passo precedente **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 4. **Middletier** attiva DocBank per la conservazione del PDF/A, quindi CheBanca! BSP a cui comunica l'esito della firma del *"Contratto"*.

1.4.2 Ambito logico

La soluzione della "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" si basa su una autenticazione forte mediante l'utilizzo dei Codici Dispositivi o utilizzo di OTP.

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. 2.0" sono:

- Sistema di autenticazione forte dell'*"Utente FEA"* (**Middletier**)
- 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 (**Middletier**)
- Sistema per l'apposizione della firma digitale in uno dei formati supportati dalla normativa (**PkBox, PkBoxRemote**).

Le principali funzionalità di sicurezza offerte dalla "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" sono:

- autenticazione dell'*"Utente FEA"* mediante il riconoscimento dei codici dispositivi contenuti nella *"Matrice Dispositiva"* in esclusivo possesso del *"Cliente"* e riconoscimento dei codici di OTP
- 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

- cifratura AES-128 del PIN del Certificato e del PIN SOTTOSCRIZIONE contenuti 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.

1.5 Confine di utilizzo

L'ODV può essere utilizzato solo parte di un *"Cliente" 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!.

1.6 Ambiente operativo dell'ODV

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

- Server Middletier:
  - Hardware:
    - CPU: 4 x Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz
    - RAM: 16GB
  - Software:
    - Application server: Jboss EAP 6.3
    - Jdk version: 1.7
    - J2EE version: 6
    - Red Hat Enterprise Linux Server release 6.9
- Server BSP:
  - Hardware:
    - CPU: 28 x P7
    - RAM: 56GB
  - Software:
    - Application Server: WebSphere AS 8.5
    - Jdk Version: 1.6 -IBM J9 VM
    - J2EE version: 5
    - Sistema Operativo: AIX 7100-04-04-1717
- Server PkBox:
  - Hardware:
    - CPU: 4 x Intel(R) Xeon(R) CPU X5650
    - RAM: 8GB
  - Software:
    - Application server: Tomcat 8.0.30
    - Jdk version: 1.8
    - Sistema Operativo: Red Hat Enterprise Linux Server release 6.6
- Server PkCA:

    - Hardware:
        - CPU: 2 CPU Xeon(R) X5650
        - RAM: 5GB
    - Software:
        - Application server: Tomcat 8.0.32
        - Jdk version: 1.70_111
        - Sistema Operativo: Red Hat Enterprise Linux Server release 7.4
- Server Time4ID:
    - Hardware:
        - CPU: 2 CPU Xeon(R) X5650
        - RAM: 5GB
    - Software:
        - Application server: Tomcat 8.0.32
        - Jdk version: 1.70_111
        - Sistema Operativo: Red Hat Enterprise Linux Server release 7.4
- 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: nCipher mod. nShield Connect 1500 F3

1.7 Ruoli utente

Il ruolo utente della “Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0” è *l’”**Utente FEA”*** che è il richiedente ed utilizzatore dell’ODV ed è identificabile come il soggetto (*"Cliente"* , *"Lead Qualificato")* per il quale è stato generato un certificato digitale.

L' "Utente FEA" per mezzo dei codici dispositivi della *"Matrice Dispositiva"* , OTP e delle *"Credenziali di sicurezza FEA"* può sottoscrivere nuovi prodotti bancari mediante le funzioni dell'ODV.

1.8 Funzioni di sicurezza

Le funzioni di sicurezza dell'ODV vengono applicate ad un *"Utente FEA"* 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.

1.8.1 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 di un programma "PDF Reader" (es: Acrobat Reader) in modo che utilizzi il certificato digitale CheBanca! per la verifica delle firme elettroniche
- Apertura del file con un 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 i Data Center esterni.

Servizio di generazione della firma elettronica

Il sistema di sicurezza realizzato da CheBanca! per la "Applicazione Firma Elettronica Avanzata di CheBanca! v. 2.0" 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. 2.0" 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 o OTP 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 mediante apposito servizio HSM.

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 One Time Password sono verificate mediante una chiamata a servizio JSON-RPC verso fornitore di Intesi (Time4ID).

Le *"Credenziali di sicurezza FEA"* sono custodite all'interno di un Server LDAP e beneficiano 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.

1.8.2 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" e/*o mediante OTP.
ODV_Crypto	Supporti crittografici	L'ODV applica algoritmi di cifratura AES-128 al PIN del certificato ed al PIN SOTTOSCRIZIONE contenuti nelle *"Credenziali di sicurezza FEA"*. L'ODV applica algoritmi di hashing RIPMED-160 ai codici dispositivi, SHA-1 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 3 - Funzioni di sicurezza dell'ODV

2 DICHIARAZIONE DI CONFORMITÀ (ASE_CCL)

Il ST e l'ODV sono conformi alla versione 3.1 Revision 5 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. 5
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 5.

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.

3 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).

3.1 Beni

Documenti da firmare: Sono i "Contratti" che i *"Clienti" o* i *"Lead Qualificati"* 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.

3.2 Minacce

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

M.User: impersonare l'*"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.

M.Disp: compromissione del dispositivo del cliente che riceve l'OTP.
Soggetti non autorizzati possono accedere alle funzioni dell'ODV appropriandosi della APP CheBanca! di un "Utente FEA" (bene minacciato). L'attaccante può svolgere quindi azioni malevoli e dannose nei confronti dell'"Utente FEA", titolare delle credenziali stesse.

3.3 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.

3.4 Ipotesi per l'ambiente operativo

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

I.IdauHB: 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.IdauPI: Si assume che l'ambiente operativo, mediante l'applicazione di portale Istituzionale WEB, provveda all'identificazione ed autenticazione di primo livello dei "*Prospect"* 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 i Data Center esterni, 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"* e il *"Prospect"* e/o *"Lead qualificato"* comunichino con CheBanca! in HTTPS, mentre le comunicazioni tra i Data Center CheBanca! e Data Center esterni 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.

I.OTP: Si assume che l'SDK della Strong Authentication metta a disposizione verifiche, bloccando il segreto condiviso lato server dopo 5 tentativi consecutivi errati della verifica dell'OTP.

4 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.

4.1 Obiettivi di sicurezza per l'ODV

Obiettivo	Descrizione
OO.User	L'ODV, a valle della identificazione e autenticazione del *"Cliente"* e/o del *"Prospect"* gestiti dall'applicazione di Home Banking o dal Portale Istituzionale, deve adottare ulteriori procedure di autenticazione prima di permettere l'accesso ai servizi FEA.
OO.SC	L'ODV deve proteggere il PIN del Certificato e il PIN SOTTOSCRIZIONE 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 4 - Obiettivi di sicurezza per l'ODV

4.2 Obiettivi di sicurezza per l'ambiente operativo

Obiettivo	Descrizione
OE.IdauHB	L'ambiente operativo (Home Banking), prima di permettere l'accesso all'ODV, deve provvedere all'autenticazione del *"Cliente*", effettuata mediante l'immissione delle *"Credenziali Cliente CheBanca!"* (codice Cliente, data di nascita, PIN), in possesso del *"Cliente"* stesso.
OE.IdauPI	L'ambiente operativo (Portale Istituzionale), prima di permettere l'accesso all'ODV, deve provvedere all'autenticazione del *"Prospect*", effettuata mediante l'immissione del PIN SOTTOSCRIZIONE in possesso del *"Prospect"* stesso.

Obiettivo	Descrizione
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 FEA"*.
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"* devono essere memorizzati e custoditi in DB Oracle e/o Server LDAP; documenti firmati dall'*"Utente FEA"* devono essere memorizzati su Documentale 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 deve impegnare i *"Clienti"* a custodire e proteggere i propri dispositivi hardware e software utilizzati, i 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.
OE.OTP	l'SDK della Strong Authentication deve garantire il blocco dell'OTP lato server al superamento di 5 tentativi consecutivi errati.

Tabella 5- Obiettivi di sicurezza per l'ambiente operativo

4.3 Razionali degli obiettivi di sicurezza

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

Tabella 6 - Razionali degli obiettivi di sicurezza

M.User: *impersonare l'"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 delle operazioni di identificazione e autenticazione gestite dalle applicazioni che ne regolano l'accesso, deve adottare ulteriori procedure di autenticazione, prima di permettere ai *"Clienti"* ed ai *"Lead Qualificati*" di accedere ai servizi FEA.

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. 1.4.1.1.

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 FEA*" 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"* devono essere memorizzati e custoditi in DB Oracle e Server LDAP; i documenti firmati dall'*"Utente FEA"* devono essere momorizzati nel Documentale ed usufruire quindi delle misure di sicurezza 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. 1.4.1.1.

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"* devono essere memorizzati e custoditi in DB Oracle e Server LDAP; i documenti firmati dall'*"Utente FEA"* devono essere momorizzati nel Documentale ed usufruire quindi delle misure di sicurezza utilizzati.

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

M.Disp compromissione del dispositivo che riceve l'OTP

Soggetti non autorizzati possono accedere alle funzioni dell'ODV appropriandosi del dispositivo del cliente ("Utente FEA"). L'attaccante può svolgere quindi azioni malevoli e dannose nei confronti dell'"Utente FEA", titolare delle credenziali stesse.

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

dispositivi hardware e software, nonché i codici dispositivi e le proprie credenziali di sicurezza con attenzione e diligenza.

I.IdauHB

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.IdauHB: 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.IdauPI

Si assume che l'ambiente operativo (Portale Istituzionale), prima di permettere l'accesso all'ODV, provveda all'autenticazione dei "Prospect", che in una fase immediatamente successiva, in qualità di "Lead Qualificato" chiederanno di aderire alla FEA per la sottoscrizione di un "Contratto".

L'ipotesi è supportata dal seguente obiettivo:

OE.IdauPI: l'ipotesi è sostenuta dall'obiettivo dell'ambiente operativo, che gestisce i dati di identificazione dei "Prospect".

I.Com

Si assume che le comunicazioni tra i Data Center CheBanca! e Intesi Group, 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 Intesi Group 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. 1.4.1.1.

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 periodica 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.

I.OTP

Si assume che l'ambiente operativo al superamento di cinque tentativi consecutivi errati di inserimento dell'OTP blocchi lo specifico codice OTP.

L'ipotesi è supportata dal seguente obiettivo:

OE.OTP: obiettivo dell'SDK della Strong Authentication è di garantire il blocco dell'OTP lato server al superamento di 5 tentativi consecutivi errati.

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 dispositivi hardware e software, nonché i codici dispositivi e le proprie credenziali di sicurezza con attenzione e diligenza.

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 dei sistemi informativi della Banca. Tutto il personale indirettamente coinvolto nella gestione dell'ODV deve essere scelto tra personale fidato e addestrato alla corretta gestione dell'ODV stesso.

5 DEFINIZIONE DI COMPONENTI ESTESE (ASE_ECD)

Questo ST non prevede la definizione di alcuna componente estesa.

6 REQUISITI DI SICUREZZA (ASE_REQ)

6.1 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. 5 e dai Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 3.1 Rev. 5.

6.2 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]**.

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.

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***]**.

6.3 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
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

Requisiti Funzionali		
Classi	**Famiglie**	**Descrizione**
FMT: Security Management	FMT_SMR.1	Security roles

Tabella 7 - ODV Security Functional Requirements (SFR)

6.3.1 Autenticazione utenti

FIA_UAU.2/HB	
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 due modalità. La prima modalità, dopo aver effettuato l'identificazione e l'autenticazione all'applicazione di Home Banking, prevede che l'autenticazione alla FEA avvenga tramite l'immissione dei codici dispositivi in esclusivo possesso del *"Cliente"*. La seconda modalità, dopo aver effettuato l'identificazione e l'autenticazione all'applicazione di Home Banking, prevede che l'autenticazione alla FEA avvenga tramite l'immissione di un codice OTP ricevuto dal *"Cliente"* via SMS.

FIA_UAU.2/PI	
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 mediante il Portale Istituzionale prevede che il "*Prospect"*, dopo aver effettuato l'identificazione e l'autenticazione all'applicazione del Portale Istituzionale, si autentichi alla FEA tramite l'immissione di un codice numerico di 8-12 cifre, (Pin sottoscrizione) scelto e validato dall'utente stesso.

FIA_AFL.1/HB	
Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [**5**] unsuccessful authentication attempts occur related to [**1. authentication based on "Matrice Dispositiva"** **2. authentication based on OTP**].
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/HB	
Notes:	

FIA_AFL.1/PI	
Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [**5**] unsuccessful authentication attempts occur related to [1. **authentication based on "Pin Sottoscrizione"** 2. **authentication based on "Codice di conferma"**].
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
Notes:	

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:	

6.3.2 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 [**128 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

FCS_COP.1/crypt	
Notes:	La componente "Middletier" provvede alla cifratura del PIN del Certificato per le operazioni provenienti da Home Banking, del PIN Sottoscrizione per le operazioni provenienti dal Portale Istituzionale. Dopo la cifratura i dati vengono memorizzati nel Server LDAP. L'operazione di decifratura avviene quando occorre recuperare il certificato digitale per ogni operazione di firma dei contratti o il Pin Sottoscrizione per l'autenticazione forte del "*Lead Qualificato*".

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:	Lo SHA-1 è usato esclusivamente come meccanismo di hashing del documento da firmare.

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]

6.3.3 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:** • **Lead qualificato** • **Cliente** **Oggetti:** • **Servizi FEA** **Operazioni:** • **Procedura di attivazione**].
Dependencies:	FDP_ACF.1
Notes:	Il prospect non viene elencato tra i soggetti in quanto non interagisce in questo stato con l'ODV ma lo fa quando viene promosso a "Lead Qualificato"

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 dei Soggetti: 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: [**I soggetti possono effettuare la procedura di Attivazione dei Servizi FEA se esiste ed è valido un Ticket dispositivo associato ad essi].**
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/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**].
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.

6.3.4 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:** • **Lead qualificato** • **Cliente** **Oggetti:** • **Contratti** **Operazioni:** • **Sottoscrizione** **]**
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	Il prospect non viene elencato tra i soggetti in quanto non interagisce in questo stato con l'ODV ma lo fa quando viene promosso a "Lead Qualificato"

FDP_ACF.1/sottoscrizione contratti

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 Soggetti:** • **Ticket dispositivo** • **Data di scadenza del certificato digitale**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**I Soggetti possono effettuare l'operazione di sottoscrizione di un Contratto se:** • **esiste ed è valido un Ticket dispositivo associato al Soggetto** • **il certificato digitale del Soggetto 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/sottoscrizione contratti	
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.

6.4 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
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 8 - 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	ALC_CMC.1.1D	The developer shall provide the TOE and a reference

action elements:		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 ASE_CCL.1.2D	The developer shall provide a conformance claim. 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 ASE_OBJ.2.2D	The developer shall provide a statement of security objectives. The developer shall provide a security objectives rationale.
ASE_ECD.1 Extended components definition		
Dependencies:	None	
Developer action elements	ASE_ECD.1.1D ASE_ECD.1.2D	The developer shall provide a statement of security requirements. 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 9 - Dettaglio dei singoli componenti di garanzia

6.5 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/HB	X		
FIA_UAU.2/PI	X		
FMT_SMR.1	X		
FIA_AFL.1/HB	X		
FIA_AFL.1/PI	X		
FCS_COP.1/crypt		X	
FCS_COP.1/hash_document		X	

SFR	OO.User	OO.SC	OO.Ticket
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 10 - Razionale dei requisiti di sicurezza

OO.User: l'obiettivo dell'ODV è di applicare una autenticazione forte, a valle della identificazione ed autenticazione avvenute mediante uno dei portali: Home Banking, Istituzionale. L'obiettivo è soddisfatto dal SFR FIA_UAU.2 con tutte le sue iterazioni, 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 con le sue iterazioni, controlla l'immissione dei codici di autenticazione.

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.

6.6 Analisi delle dipendenze

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

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
SFR		
FIA_UAU.2/HB	FIA_UID.1	**NOTA 1**
FIA_UAU.2/PI	FIA_UID.1	**NOTA 1**
FIA_AFL.1/HB	FIA_UID.1	**NOTA 1**
FIA_AFL.1/PI	FIA_UID.1	**NOTA 1**

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
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**
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.1Security attribute based access control	FDP_ACF.1/attivazione servizi FEA
FDP_ACC.1/sottoscrizione contratti	FDP_ACF.1Security 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**

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
FDP_ITC.1/attivazione servizi FEA	FDP_ACC.1 Subset access control, orFDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/attivazione servizi FEA **NOTA 4**
FDP_ITC.1/sottoscrizione contratti	FDP_ACC.1 Subset access control, orFDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	FDP_ACC.1/sottoscrizione contratti **NOTA 4**
FDP_ETC.2	FDP_ACC.1 Subset access control, orFDP_IFC.1 Subset information flow control	FDP_ACC.1/sottoscrizione contratti
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

Requisiti del ST	Dipendenze richieste dai CC	Dipendenze soddisfatte
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
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 11 - Tabella delle analisi delle dipendenze

6.6.1 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 all'applicazione di Home Banking, oppure al Portale Istituzionale.

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).

7 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.

7.1 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

7.1.1 ODV_Aut – Autenticazione utenti FEA

L'accesso può avere due ambiti:

Accesso da Home Banking

Nel caso di "Cliente", ogni richiesta di utilizzo della FEA deve essere validata tramite una coppia di codici dispositivi (matrice) *e* OTP.

Operativamente la procedura per l'utilizzo della FEA prevede che l'utente si sia precedentemente identificato alle applicazioni bancarie che ne controllano l'accesso (Home Banking). Queste operazioni sono a carico dell'ambiente operativo. A questo punto l'utente deve presentare all'applicazione FEA il secondo livello di autenticazione precedentemente descritto.
Questa operazione è realizzata dal SFR **FIA_UAU.2/HB**.

Accesso da Portale Istituzionale

La procedura per l'utilizzo della FEA, mediante il Portale Istituzionale, prevede che il "Prospect", dopo aver effettuato l'identificazione tramite Portale Istituzionale, diventi "Lead Qualificato" e quindi si autentichi alla FEA tramite l'immissione di un codice numerico di 8-12 cifre, (Pin sottoscrizione) scelto e validato dall'utente stesso.
Dopo tali passaggi, il "Lead Qualificato" risulta abilitato all'utilizzo della FEA, utilizzo che deve essere validato tramite codice OTP ricevuto mediante dispositivo del "Lead Qualificato".
Questa operazione è realizzata dal SFR **FIA_UAU.2/PI.**
L'ODV, in entrambi i casi, controlla il numero di tentativi di autenticazione e blocca l'"Utente Fea" in caso di superamento della soglia stabilita (5 tentativi consecutivi errati). Queste operazioni realizzano le SFR FIA_AFL.1/HB, FIA_AFL.1/PI.

Viene assicurata l'associazione dei soggetti al ruolo corrispondente, per realizzare la SFR **FMT_SMR.1**.

7.1.2 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.

Un'implementazione della funzione di hashing viene eseguita sul *"Contratto"* selezionato *dall'"Utente FEA"* con algoritmo SHA-1 per essere firmato mediante HSM (esterno all'ODV e mediante la chiave privata del certificato digitale univocamente associato all'*"Utente FEA").* Questa funzione di hashing realizza la SFR **FCS_COP.1/Hash_Document**.

Nel caso in cui fosse stata scelta come modalità operativa la *Matrice Dispositiva* la funzione di hashing implementata con algoritmo RIPEMD-160 viene applicata sulle celle richieste in fase di autenticazione forte, realizzando così quanto previsto dalla SFR **FCS_COP.1/Hash_Matrix_code**.

Ulteriori operazioni di cifratura con algoritmo AES-128 sono eseguite dalla componente dell'ODV "**Middletier**" che provvede:

- la prima volta a cifrare il PIN del Certificato per le operazioni provenienti da Home Banking (relative ai "Client")
- alla cifratura del PIN Sottoscrizione per le operazioni provenienti dal Portale Istituzionale (relative ai "Lead qualificati")

Dopo la cifratura i dati vengono memorizzati nel Server LDAP.

Successivamente, alla richiesta di sottoscrizione di un contratto, "**Middletier**" 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!.

L'operazione di decifratura avviene quando occorre recuperare il certificato digitale per ogni operazione di firma dei contratti o il Pin Sottoscrizione per l'autenticazione forte del "Prospect" (che dopo diventa "Lead Qualificato")

Queste operazioni realizzano la SFR **FCS_COP.1/Crypt.**

7.1.3 ODV_Access – Controllo Accessi

Nel Security Target sono state individuate e descritte due flussi: Creazione "Utente FEA" e "Firma del contratto".

Per il flusso Creazione "Utente 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 o richiama il servizio di verifica dell'OTP di Time4ID
- 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 il flusso "Firma del contratto", 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 oppure verifica l'OTP generato dal Cliente e ne verifica la validità. In caso positivo richiama il server LDAP per il recupero delle credenziali di sicurezza Utente FEA attraverso il Codice Fiscale
- 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.**

7.1.4 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/HB	X		
FIA_UAU.2/PI	X		
FMT_SMR.1	X		
FIA_AFL.1/HB	X		
FIA_AFL.1/PI	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 12 - Mappatura dei SFR con le funzioni dell'ODV