Addendum al Manuale Operativo della Firma Qualificata Soluzione per le aziende del Gruppo Crédit Agricole

MANUALE OPERATIVO

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione	29/11/2016

Indice degli argomenti

1 Scopo e campo di applicazione

Il presente documento ha lo scopo di descrivere il contesto operativo, le regole e le procedure operative adottate da TI Trust Technologies per l'emissione dei certificati per chiavi di sottoscrizione con firma qualificata con limiti d'uso in favore di soggetti che si rivolgono alle aziende del Gruppo Crédit Agricole (**il Gruppo**).

Il processo di emissione dei certificati di firma qualificata avviene nell'ambito delle operazioni e delle verifiche che le aziende del **Gruppo** conducono per intrattenere rapporti finanziari per i quali è loro richiesto dalla normativa di settore l'**effettuazione preventiva di un'adeguata verifica dell'identità del cliente**.

Il rilascio dei certificati di firma qualificata, avviene in questo ambito come elemento accessorio del processo di apertura del rapporto fa il titolare e l'azienda del **Gruppo** ed in conformità con la vigente normativa in materia di firma qualificata. Infatti, l'identificazione certa richiesta per il rilascio del certificato è assolta mutuandola dall'adeguata verifica eseguita dal **Gruppo** e non il viceversa.

In particolare riguardo all'adeguata verifica la cui effettuazione è in capo alle aziende del **Gruppo**, si precisa quanto segue.

In base ai commi 3 e 4 della Sezione II del Provvedimento della Banca d'Italia recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231[1], le predette aziende sono tenute "ad acquisire i dati identificativi e a effettuare il riscontro su una copia - acquisita tramite fax, a mezzo posta, in formato elettronico o con modalità analoghe - di un documento di identità non scaduto" e a provvedere ad "un'ulteriore verifica dei dati acquisiti secondo le modalità ritenute più opportune, in relazione al rischio specifico". Lo stesso provvedimento cita, a titolo esemplificativo, le seguenti modalità:

- contatto telefonico su utenza fissa (welcome call);
- invio di comunicazioni a un domicilio fisico con ricevuta di ritorno;
- richiesta di invio di documentazione controfirmata;
- verifica su residenza, domicilio, attività svolta, tramite richieste di informazioni ai competenti uffici ovvero mediante incontri in loco, effettuati avvalendosi di personale proprio o di terzi.

Nell'ambito dei margini di autonomia sopra indicati e nel caso descritto nel presente documento, il **Gruppo** adotta per l'adeguata verifica dell'identità della persona che richiede l'apertura di un rapporto finanziario le seguenti prescrizioni:

1. caricamento di un primo documento di identità fronte/retro;
2. caricamento di un secondo documento di identità fronte/retro;
3. caricamento di un "selfie" (v. par. 2.1, punto 6), con uno dei documenti di identità utilizzati nei precedenti passi 1 e 2
4. caricamento del documento con codice fiscale fronte/retro;
5. verifiche preliminari (descritte al successivo par. 2.3.1, punto 5);
6. welcome call registrata per la verifica dell'aderenza tra le informazioni inserite dal cliente e le sue risposte (descritta al successivo par. 2.3.1, punto 6).

Il servizio descritto nel presente documento è pertanto finalizzato esclusivamente a garantire, tramite la dematerializzazione dei documenti necessari e la celere gestione delle procedure di rilascio, l'erogazione di un certificato di firma digitale che il cliente del **Gruppo** utilizzerà per sottoscrivere i documenti contrattuali previsti nel rapporto esclusivamente tra il cliente ed il Gruppo.

Il presente documento costituisce pertanto addendum al Manuale Operativo della Firma Qualificata di TI Trust Technologies (codice documento CERTQUAL.TT.SOMO16000 Manuale Operativo - Certificati Qualificati di Firma Digitale ai sensi del D. Lgs. 82/2005, Marcatura Temporale, Carta Nazionale dei Servizi), pubblicato all'interno del sito www.trusttechnologies.it e sul sito di AGID, nella pagina in cui è pubblicato l'elenco dei certificatori attivi: http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi. Esso integra il predetto Manuale Operativo della Firma Qualificata in merito alle modalità con cui TI Trust Technologies emette il certificato di firma in questo ambito, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità. Per quanto non espressamente richiamato o derogato dal presente Addendum deve intendersi valido quanto presente nel suddetto Manuale.

La pubblicazione del presente Addendum consente ai soggetti interessati di conoscere le caratteristiche e l'affidabilità della soluzione qui descritta.

[1] Pubblicato nel S. O. n. 35 della G.U.R.I. n. 105 del 7 maggio 2013.

1.1 Identificazione dei certificati di firma

I certificati emessi da TI Trust Technologies nell'ambito delle previsioni del presente Addendum per i Servizi Finanziari sono identificabili dalla presenza al loro interno, nel campo "policyIdentyfier", del seguente identificativo univoco (OID): 1.3.76.33.1.1.28

2 Descrizione della Soluzione Conto Adesso Selfie

2.1 Soggetti coinvolti

Nell'ambito della soluzione Selfie operano i seguenti soggetti:

1. **Gruppo:** il Gruppo Crédit Agricole
2. **Azienda:** banca o Azienda che appartiene al Gruppo Crédit Agricole e che gestisce il servizio finanziario (es: conto corrente e servizi accessori - carte, dossier titoli, ecc., prestito al consumo, ecc.);
3. **Servizio Finanziario**: servizio erogato da Azienda del Gruppo Credit Agricole, che può essere sottoscritto da Portale dell'Azienda e che consente di eseguire le relative operazioni (es: per conto corrente, bonifici, pagamenti, ecc.) tramite il Portale medesimo
4. **Addetto:** addetto dell'Azienda del Gruppo Credit Agricole, dipendente dell'Azienda o di Azienda terza incaricata dal Gruppo, operante nelle strutture di backoffice o di Service Telefonico, addetto alle verifiche previste sull'identità del richiedente e per l'apertura del conto corrente;
5. **Richiedente:** persona fisica o giuridica che intende attivare un Servizio Finanziario utilizzando i servizi offerti dal Portale;
6. **Selfie**: ritratto fotografico che il richiedente esegue da sé stesso, inquadrando il proprio volto e un documento d'identità, nell'ambito del processo di identificazione;
7. **Portale:** sito Internet on-line dell'Azienda del Gruppo;
8. **Dispositivo**: apparato che consente al Richiedente l'accesso via Internet al Portale. Ricadono in questa tipologia i personal computer, i tablet e gli smartphone, non escludendo tuttavia dispositivi diversi (es: smart-TV).
9. **Applicazione:** software sviluppato in modo opportuno, secondo la tipologia del dispositivo, che consente l'esecuzione del selfie e l'upload delle immagini dei documenti d'identità sul portale per la procedura di identificazione.
10. **Soluzione:** soluzione di firma remota che utilizza il riconoscimento del richiedente/titolare per emettere in certificato digitale di firma qualificata
11. **Titolare:** il titolare del certificato di firma qualificata con limiti d'uso (v. più oltre), che corrisponde al richiedente del Servizio Finanziario;
12. **TI Trust Technologies** o **Certificatore** o **CA:** il Certificatore accreditato.

Le Banche del Gruppo, si avvalgono di un proprio portale per acquisire le richieste di apertura di conti correnti senza doversi recare fisicamente in una filiale o sede. Conclusa con successo la fase di apertura del conto corrente, le usuali operazioni bancarie saranno svolte dal richiedente usando i servizi offerti dal Portale.

Mediante l'utilizzo della Soluzione, il richiedente già identificato per l'apertura del rapporto con il Gruppo secondo le modalità richiamate nel cap. 1 e dettagliate nel successivo par. 2.3.1 ed una volta emesso il suo certificato di firma digitale, potrà sottoscrivere in modalità remota la documentazione contrattuale per la richiesta di ulteriori Servizi Finanziari. Per consentire di effettuare l'operazione di adeguata verifica della sua identità, il richiedente invierà all'Azienda, in modalità elettronica, la fotografia di due documenti d'identità e un selfie, tutte eseguite contestualmente all'esecuzione dell'operazione, senza poter richiamare immagini già preventivamente memorizzate sul proprio device. L'Azienda, per mezzo degli addetti del proprio backoffice ed al servizio di Service Telefonico, si accerterà dell'autenticità delle informazioni fornite sia eseguendo una serie di controlli su banche dati proprie e pubbliche (quali SCIPAFI per il controllo del documenti di identità), sia effettuando una chiamata telefonica al richiedente ("welcome call") con la richiesta di una serie di informazioni a conferma di quanto rilevato tramite portale.

Se le verifiche hanno successo, ed esclusivamente dopo che il Servizio Finanziario è stato attivato il certificato digitale è definitivamente abilitato alla piena operatività. In caso di fallimento delle verifiche, tutte le informazioni sono cancellate e il certificato digitale è revocato.

Le operazioni necessarie alla sottoscrizione con firma digitale avvengono con le modalità di autenticazione via cellulare già utilizzate dal Gruppo e descritte nell'addendum al Manuale Operativo dei servizi di firma digitale di TI Trust Technologies richiamato al cap. 1, identificato dal codice CERTQUAL.TT.SOMO14001 - Certificati di

sottoscrizione per le Banche facenti parte del Gruppo Cariparma Crédit Agricole – Manuale Operativo Addendum (cap. 4 – Operatività) e pubblicato sul sito di TI Trust Technologies. Il certificato di firma qualificata necessario per effettuare l'operazione di firma è emesso con limite d'uso (in lingua Italiana ed Inglese) ai rapporti fra il Titolare ed il Gruppo Cariparma CA o qualsiasi ente controllato o altro ente per conto del quale sono erogati prodotti o servizi.

2.2 Descrizione del Contesto

2.2.1 Descrizione dell'applicativo di Acquisizione Selfie

L'acquisizione dei documenti identificativi del cliente (v. par. 2.3.1, punto 3) avviene tramite una APP sullo smartphone del cliente stesso, che consentirà l'acquisizione tramite fotocamera dei vari documenti richiesti.

Tale APP guida il cliente in tutte le fasi del processo di acquisizione delle immagini dei documenti richiesti, impedendo il caricamento di foto o immagini già presenti nel dispositivo, poiché richiede esplicitamente gli scatti fotografici del fronte e del retro dei documenti obbligatori ed effettua in modalità automatica lo scatto quando il documento è correttamente inquadrato, senza richiedere al cliente di effettuare alcuna operazione (scatto, zoom, ecc.) tale da poter alterare il processo di acquisizione.

Anche durante l'acquisizione del Selfie con un documento d'identità, l'APP guida il cliente e scatta automaticamente la foto non appena individua il documento e il viso del cliente correttamente posizionati all'interno dello schermo del dispositivo, in modo tale da impedire il caricamento di foto o immagini già presenti nel dispositivo.

L'APP è composta da moduli software che controllano le immagini e guidano il cliente affinché gli scatti siano chiari e nitidi, riducendo al minimo la possibilità di errori.

I server centrali di gestione del servizio, collocati presso il datacenter della Banca, e la APP stessa sono sottoposti alle verifiche di sicurezza standard della Banca prima della loro pubblicazione, da parte di strumenti e personale incaricato dalla Banca. L'APP, prima della pubblicazione sugli store da cui è scaricabile dagli utenti, è ulteriormente sottoposta ad una verifica da parte di personale dello store stesso per l'assenza di minacce al suo interno.

2.2.2 Rapporto Organizzazione Cliente e Addetti-Dipendenti propri

Il rapporto tra l'Azienda ed i Dipendenti propri addetti alle verifiche, che operano nel backoffice o nel Service Telefonico, è regolato da un contratto di assunzione a tempo indeterminato o a termine.

I Dipendenti vengono previamente identificati e sottoposti ad adeguata verifica, secondo quanto previsto dalla normativa antiriciclaggio vigente, inoltre, devono obbligatoriamente seguire e superare i corsi di formazione predisposti dall'Azienda.

L'Azienda provvede anche al loro aggiornamento con opportuni piani di formazione.

2.2.3 Rapporto Organizzazione Cliente e Addetti-Dipendenti di Terzi

Il rapporto tra l'Azienda e gli addetti dipendenti di terzi è regolato attraverso un contratto di servizi, avente ad oggetto, tra gli altri, i Servizi Finanziari alla cui offerta gli addetti vengono abilitati per conto dell'Azienda.

Per poter erogare i Servizi Finanziari per conto delle Aziende del Gruppo, gli Addetti vengono previamente identificati e sottoposti ad adeguata verifica, secondo quanto previsto dalla normativa antiriciclaggio vigente, inoltre, devono obbligatoriamente seguire e superare un corso di formazione iniziale attestato da apposito certificato, che l'Addetto dovrà stampare e conservare.

L'Azienda provvede anche all'aggiornamento degli stessi corsi di formazione ed alla comunicazione informativa agli Addetti abilitati in concomitanza di variazioni della normativa di riferimento o di variazioni nella proposta commerciale.

2.2.4 Operatività degli Addetti

Gli Addetti possono, in qualunque momento, consultare e scaricare il manuale operativo aggiornato dei Servizi Finanziari da un apposito sito Intranet ad essi dedicato le cui credenziali di accesso sono personali e comunicate direttamente dall'Azienda.

Tutte le operazioni eseguite dagli Addetti sono tracciate su tutti i sistemi interessati e sempre riconducibili all'Addetto che le ha effettuate.

2.3 Descrizione del servizio

Il servizio, dal punto di vista del Titolare, può essere rappresentato nelle seguenti macro-fasi.

2.3.1 Apertura di Conto Adesso tramite Portale

Il Titolare/Richiedente viene identificato ai fini della normativa richiamata nel cap. 1 e riceve un Certificato Digitale Qualificato, con i limiti d'uso specificati in precedenza (v. par. 2.1).

1) *compilazione del form di attivazione del Servizio Finanziario.* Il Titolare/Richiedente accede al Portale e compila il form di apertura conto, inserendo i dati anagrafici, il numero telefonico e mail e gli altri dati richiesti dall'Azienda;
2) *attivazione dell'Applicazione per l'"upload" dei documenti e del Selfie.* Il Portale invia al Dispositivo del Titolare/Richiedente i riferimenti per il download e l'installazione dell'applicazione, con modalità coerenti con il tipo di dispositivo (es: app scaricabile dallo Store Android per smartphone o tablet con quel sistema operativo);
3) *caricamento dei documenti di identità e del Selfie.* Seguendo la procedura interamente guidata dall'APP e descritta al par. 2.2.1, il Titolare/Richiedente acquisisce le immagini dei documenti richiesti (tre documenti in corso di validità: due documenti di identità[2] e il codice fiscale) ed esegue il Selfie con uno dei due documenti d'identità. Al termine l'APP invierà automaticamente le immagini raccolte all'Azienda che effettua le verifiche necessarie.
4) *emissione del certificato digitale e firma della documentazione .* Il Portale richiede al Certificatore di generare un certificato digitale qualificato multifase. Il certificato sarà usato inizialmente solo per la firma della richiesta del Servizio Finanziario, della documentazione del Certificatore per il certificato e per eventuali servizi accessori. Successivamente a questo solo primo utilizzo, **sarà sospeso e non più usabile fino all'attivazione definitiva**. Il Certificato consente di apporre la firma digitale tramite doppia autenticazione mobile (Mobile Strong Authentication via cellulare ed OTP, richiamata al par. 2.1).
5) *Verifiche preliminari.* Tutte le informazioni raccolte dal Portale sono passate al backoffice ed al Service Telefonico, per le successive fasi di lavorazione. Questi eseguono una serie di verifiche preliminari, tra cui:
    - controllo sui dati anagrafici;
    - se il Titolare/Richiedente è già Cliente dell'Azienda, per cui è già stato identificato;
    - verifica di leggibilità delle foto dei documenti d'identità e confronto tra il selfie e la foto sui documenti
    - confronto tra i dati inseriti nel portale e quelli riportati nei documenti d'identità caricati;
    - verifica SCIPAFI;
    - verifica di corretta apposizione di tutte le firme previste sui documenti contrattuali e per l'emissione del certificato
6) *"welcome call" da parte di Service Telefonico.* Il Titolare/Richiedente è chiamato dal Service Telefonico per una verifica incrociata dell'identità: verranno poste al cliente una serie di domande per verificare la corrispondenza tra risposte date e i dati/documenti inseriti nel form.

   Allo scopo di assicurare la conformità del procedimento a quanto disposto dalle normative vigenti che regolano la materia, la chiamata è registrata e conservata dall'Azienda per il periodo previsto (20 anni). I campioni vocali potranno essere impiegati anche per una verifica a posteriori della corretta identificazione del Titolare/Richiedente.
7) *Attivazione definitiva del Certificato Digitale.* A seguito dell'esecuzione con successo di tutte le verifiche, l'Azienda richiede al Certificatore l'attivazione definitiva del certificato digitale, che potrà essere usato dal Titolare/Richiedente per le operazioni eseguite sul Portale.

[2] Come documenti di identità si considerano: Carta d'Identità Cartacea, Carta d'Identità Elettronica, Passaporto, Patente di guida cartacea, Patente di guida formato tessera

8) *Revoca del Certificato Digitale.* In caso di mancato superamento delle verifiche, oppure in caso di cessazione del conto corrente, l'Azienda richiede al Certificatore la revoca del certificato digitale, che non potrà più essere usato dal Titolare/Richiedente in nessuna circostanza.

2.3.2 Rapporto tra l'Azienda e TI Trust Technologies

L'Azienda è stata delegata da TI Trust Technologies ad operare in qualità di proprio Registration Authority Officer (RAO).

L'Azienda conserva per il periodo previsto l'immagine di tutti i documenti d'identità e i dati utilizzati per l'identificazione, compresi i campioni vocali del richiedente ottenuti durante la "welcome call".

In caso di richiesta, l'Azienda fornirà queste informazioni al Certificatore per quanto necessario, in particolare per adempiere gli obblighi di conservazione e di esibizione che ricadono in capo a lui.

3 Regole generali

Le condizioni generali che regolano il servizio di certificazione della firma digitale erogato da TI Trust Technologies nell'ambito dei Servizi Finanziari descritti nel presente Addendum, valgono esclusivamente nell'ambito dei medesimi. Per quanto non diversamente specificato, esse sono analoghe a quelle che regolano il servizio erogato da TI Trust Technologies e descritte nel Manuale Operativo richiamato.

Di seguito si indicano pertanto esclusivamente gli elementi salienti di differenza rispetto ai due schemi di condizioni:

- Il servizio è erogato da TI Trust Technologies per la finalità di firma dei documenti contrattuali relativi all'apertura ed all'operatività dei Servizi Finanziari di Aziende del Gruppo.
- TI Trust Technologies ha l'obbligo specifico di revocare automaticamente un certificato rimasto sospeso per più di 60 giorni, senza che sia pervenuta la richiesta di attivazione da parte dell'Azienda.
- È prevista la possibilità di chiedere la revoca del Certificato da parte del Titolare.
- È causa di revoca su richiesta dell'Azienda il mancato superamento dei controlli effettuati dall'Azienda medesima per la verifica dell'identità del Titolare, secondo le modalità da essa adottate.
- I certificati di firma non saranno pubblicati.
- Con frequenza non superiore all'anno, TI Trust Technologies esegue un controllo di conformità delle modalità descritte in questo Addendum rispetto al proprio processo di erogazione del servizio di certificazione.
- Le informazioni relative al Titolare e all'Azienda di cui TI Trust Technologies viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (chiave pubblica, certificato - se richiesto dal Titolare - date di revoca e di sospensione del certificato).
- Utilizzando una funzione applicativa ed un certificato di firma digitale intestato al referente indicato dall'Azienda, questa sottoscrive ed invia a TI Trust Technologies i dati per la creazione del certificato di firma qualificata (inseriti dal Titolare al momento della richiesta di apertura del conto corrente) e la sua contestuale assunzione di responsabilità per la corretta identificazione. :
- L'incaricato applicativo TI Trust Technologies deve garantire la revoca del Certificato:
    - se è decorso il termine di 60 giorni previsto per il completamento del processo di verifica dell'identità del Titolare;
    - su richiesta dell'Azienda, nel caso in cui non vengano superati i controlli necessari per l'identificazione e/o l'attivazione del Servizio Finanziario.
    - su richiesta dell'Azienda, nel caso in cui il Servizio Finanziario sia chiuso dal Titolare.