Spett Banca d'Italia
Servizio Regolamentazione e Analisi Macroprudenziale,
Divisione Regolamentazione I,
via Milano, 53
00184, Roma

PEC: ram@pec.bancaditalia.it

Roma, 11 giugno 2018

Oggetto: Disposizioni in materia di Adeguata Verifica della Clientela - Risposta di InfoCert SpA alla Pubblica Consultazione

Spettabile Banca d'Italia,

con la presente intendiamo fornire il contributo di InfoCert SpA alla proposta recante le "nuove Disposizioni attuative in materia di adeguata verifica della clientela", che danno attuazione alle previsioni in materia di adeguata verifica contenute nel decreto legislativo 21 novembre 2007, n. 231, come modificato dal decreto legislativo 25 maggio 2017, n. 90, di recepimento della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.

InfoCert è il più grande Qualified Trust Service Provider Europeo eIDAS-compliant per quanto riguarda i certificati qualificati di firma elettronica, di sigillo elettronico, di validazione temporale e certificati di autenticazione a siti web. Inoltre, è Conservatore Accreditato presso AgID, Gestore di Posta Elettronica Certificata e Identity Provider nell'ambito del Sistema Pubblico di Identità Digitale SPID.

Con il presente contributo avanziamo una serie di proposte miranti a aumentare la sicurezza e il trust dei processi di identificazione e adeguata verifica della clientela, mettendo a fattor comune l'esperienza maturata come fornitore delle principali Banche del Paese: InfoCert ha infatti ideato, sviluppato e lanciato sul mercato per prima le soluzioni di video-riconoscimento finalizzato all'identificazione dei cittadini per l'emissione di certificati qualificati e identità digitali SPID, oggi utilizzata da primari Istituti nei propri processi di onboarding della clientela prospect. La soluzione è operativa anche in altri Paesi Europei, pertanto InfoCert è stata consultata da EBA – European Banking Authority nell'ambito degli approfondimenti preventivi all'emanazione della "joint opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector" emanata con ESMA e EIOPA il 20 febbraio 2017.

***

Osservazioni in merito a quanto definito dal documento nella Sezione VII "Disposizioni specifiche in materia di operatività a distanza"

Si valuta positivamente la scelta operata dall'Autorità, in coerenza con quanto già previsto dalle disposizioni vigenti in altri Paesi Europei, di riconoscere ai soggetti destinatari la facoltà di avvalersi di soluzioni di video-identificazione per il riconoscimento da remoto del cliente-persona fisica.

Nei casi in cui i soggetti destinatari intendano esternalizzare tali soluzioni a società terze, si ritiene opportuno suggerire che queste vengano affidate a prestatori di servizi fiduciari qualificati (Qualified Trust Service Provider - QTSP) ricompresi negli elenchi di fiducia di cui all'Art. 22 Regolamento (UE) n. 910/2014 – eIDAS -, a garanzia dei più alti livelli di trust e sicurezza associati all'erogazione di tali servizi sul mercato.

A riguardo si coglie l'occasione per sottolineare come, a livello di sistema Paese, tali procedure siano normate e correntemente utilizzate dai QTSP non solo per l'identificazione finalizzata al rilascio delle credenziali associate all'identità digitale del cittadino nel sistema SPID ma, ormai da diversi anni e prima dell'avvento del Sistema Pubblico per l'Identità Digitale, anche per l'identificazione certa nei servizi di firma elettronica qualificata.

Numerose Banche hanno già introdotto tali soluzioni nell'ambito dei propri processi di apertura conto, sia da desktop che da mobile, al fine di dotare la clientela degli strumenti di firma elettronica necessari alla piena e affidabile dematerializzazione del processo di entrata in relazione, utilizzando la piattaforma TOP – Trusted Onboarding Platform di InfoCert.

Dalle statistiche rilevate e certificate da una società di consulenza internazionale[1], il tasso di richieste apertura conto provenienti da identità potenzialmente fraudolente si attesta a circa lo 0,01%: la riduzione rispetto alle tradizionali modalità di riconoscimento è da imputarsi principalmente ai presidi di sicurezza messi in atto dal QTSP, che sottopone gli operatori addetti al riconoscimento a stringenti procedure di formazione.

Si sottolinea inoltre come l'intera modalità di riconoscimento a mezzo video-identificazione sia soggetta ad audit e approvazione periodica da parte una terza parte indipendente (CAB – Conformity Assessment Body) nell'ambito delle procedure definite dal Regolamento eIDAS per l'ottenimento e il mantenimento della qualifica di Qualified Trust Service Provider.

Il CPS – Certificate Practice Statement InfoCert è il documento ufficiale approvato dal CAB e da AgID nel quale sono descritti i processi di funzionamento del QTSP di firma e le relative modalità di identificazione della clientela utilizzate, inclusa la modalità di riconoscimento video[2].

[1] Si veda il documento "*The Total Economic Impact™ of InfoCert Trusted Onboarding Platform*" di Forrester Consulting, ottobre 2016, che si allega

[2] Si veda il paragrafo 3.2.3.5 dei CPS ICERT-INDI-MO e ICERT-INDI-MO-ENT, che si allegano alla presente e sono anche pubblicati sul sito dell'Agenzia per l'Italia Digitale (https://www.agid.gov.it/sites/default/files/repository_files/manuali_operativi.zip.p7m) che recitano:

3.2.3.5 Riconoscimento effettuato secondo la modalità 5 - VideoID

Nella modalità 5 VideoID è richiesto al Soggetto il possesso di un device in grado di collegarsi a internet (PC, smartphone, tablet, etc.), una webcam e un sistema audio funzionante. L'Incaricato alla Registrazione, adeguatamente formato, verifica l'identità del Soggetto tramite il riscontro con uno o più documenti di riconoscimento in corso di validità, purché muniti di fotografia recente e riconoscibile e ricompresi nella lista dei documenti accettati pubblicata sul sito della CA.

Le RA operanti all'estero, o che comunque identificano Soggetti residenti all'estero, possono essere autorizzati da InfoCert ad accettare documenti di identità emessi da autorità di Paesi appartenenti alla Unione Europea, previa analisi dei documenti e delle loro caratteristiche oggettive di certezza dell'identità e sicurezza nel processo di emissione da parte delle Autorità Emittenti, nonché specifica formazione.

Un ulteriore elemento di valore è la periodicità di questo audit, che deve essere ripetuto con cadenza annuale al fine del mantenimento della qualifica di compliance al Regolamento eIDAS: si ritiene che, se la Vostra Autorità propendesse per l'affidamento in outsourcing della procedura di video-riconoscimento a un QTSP, tale scelta andrebbe nella direzione di garantire al settore bancario il massimo livello di affidabilità e controllo della procedura e della sua esecuzione, senza ingenerare aggravi nei controlli e negli audit, esistendo una infrastruttura di carattere sovranazionale già dedicata allo scopo.

Osservazioni in merito a quanto definito dal documento nell'Allegato 3 "Procedura di video-identificazione"

Si ritiene opportuno segnalare come la definizione di requisiti analitici e dettagliati sulle modalità di adempimento degli obblighi di video-identificazione – in linea peraltro con quanto definito da AgID per SPID – potrebbe portare a difficoltà di pieno assolvimento degli stessi. I requisiti richiesti, confrontati con altre modalità di identificazione in presenza o a distanza, sono infatti tassativi e a un livello di dettaglio molto basso: si suggerisce di rimettere al soggetto vigilato la valutazione e la dimostrazione dell'idoneità degli strumenti e dei processi utilizzati, pur nel rispetto della finalità dell'identificazione.

Tale suggerimento è stato avanzato anche ad AgID immediatamente dopo l'emanazione del Regolamento recante le modalità attuative per la realizzazione dello SPID, cui sembra la Vostra Autorità si sia ispirata nella proposta di adozione del video-riconoscimento. La presenza di una procedura così dettagliata direttamente in un testo avente forza ordinativa, rischia a nostro avviso di precludere l'adozione di modalità di gestione del processo di video-riconoscimento maggiormente sicure e con aggiornati presidi antifrode, comportando quindi la difficoltà del settore a seguire le innovazioni tecnologiche.

In particolare, si ritiene opportuno avanzare alcune considerazioni in merito alle disposizioni riguardanti la verifica dei c.d. "dati di contatto" del cliente-persona fisica.

L'allegato prevede infatti che l'operatore debba verificare il numero di cellulare e l'indirizzo mail del cliente, rispettivamente, attraverso l'invio di un SMS, che il cliente è tenuto a esporre al dispositivo di ripresa, e una mail all'indirizzo di posta elettronica dichiarato da quest'ultimo, con un link ad una URL appositamente predisposta per la verifica.

Si ritiene che tali procedure operative possano comportare un aggravio generale dell'esperienza utente, senza portare un reale valore aggiunto dal punto di vista dei presidi antifrode.

Si considerino, ad esempio, le fisiologiche problematiche legate alla risoluzione e luminosità dello schermo del dispositivo cellulare/smartphone dell'utente, che potrebbero impedire all'operatore di riprendere in maniera chiara il testo dell'SMS di verifica del numero di cellulare.

È facoltà del Richiedente, della RA o dell'Incaricato alla Registrazione escludere l'ammissibilità del documento utilizzato dal Soggetto se ritenuto carente delle caratteristiche elencate. I dati di registrazione, costituiti da file audio-video e metadati strutturati in formato elettronico, sono conservati in forma protetta.

A riguardo si suggerisce la possibilità di prevedere che il cliente debba dettare all'operatore un codice verifica (ad esempio una One Time Password) presente all'interno dell'SMS e quest'ultimo provveda a verificarne la validità la validità real-time durante la sessione, producendo uno specifico report o uno streaming audio-video che tracci l'effettivo buon esito della procedura.

Questa operatività è già in essere in numerosi processi di riconoscimento a mezzo webcam che InfoCert ha sviluppato per conto di Istituti Bancari nell'ambito dell'emissione del certificato qualificato di firma necessario alla sottoscrizione del contratto da parte del prospect. Si è operativamente rilevato che la raccolta dell'evidenza fotografica dello schermo dello smartphone del cliente spesso è particolarmente difficoltosa, un vincolo di questo tipo va quindi ad aumentare considerevolmente il tasso di caduta della procedura, con conseguenti extra costi per la Banca.

Rispetto alla procedura proposta per la verifica dell'indirizzo mail si consideri che, per ottemperare a quanto richiesto, il cliente sarebbe costretto ad abbandonare temporaneamente la sessione aperta con l'operatore per aprire una nuova pagina del browser o la App del proprio mail provider, autenticarsi alla propria casella di posta elettronica per recuperare il messaggio inviatogli da quest'ultimo e, infine, cliccare sul link di verifica in questo contenuto.

Si ritiene che tale operatività, oltre a comportare un allungamento eccessivo dei tempi per il riconoscimento, possa incidere in maniera negativa sui tassi di abbandono volontario o involontario della procedura ed essere soggetta a tentativi di *man-in-the-middle attack*.

Si suggerisce pertanto di riconoscere ai soggetti destinatari la facoltà di definire in autonomia le modalità tecniche e operative di verifica dell'indirizzo mail del cliente, assumendo che questa procedura possa essere gestista anche al di fuori del processo di video-identificazione (ad es. nella più ampia procedura di adesione al prodotto finanziario o bancario proposto), pur nell'ambito della coerenza del processo end-to-end di entrata in relazione.

***

Ringraziando per l'attenzione accordata, rimaniamo a disposizione per ogni eventuale necessità di chiarimento o integrazione.

Si allegano alla presente proposta i seguenti documenti, ivi refenziati:

- "The Total Economic Impact™ of InfoCert Trusted Onboarding Platform" di Forrester Consulting, ottobre 2016
- Certificate Practice Statement ICERT-INDI-MO, v. 3.3 del 07/05/2018
- Certificate Practice Statement ICERT-INDI-MO-ENT, v 3.3 del 07/05/2018

In fede,

Carmine Auletta

Chief Innovation Officer
Firmato digitalmente da:Carmine Auletta
Data:11/06/2018 23:23:37