Dichiarazione sulle prassi del servizio di verifica dell'identità (Identity Proofing Service Practice Statement, «IPSPS»)

per l'apertura di un conto online presso LGT

Versione:	1.1
Data di pubblicazione:	24.08.2023
Approvazione da:	Management Team LGT responsabile della verifica dell'identità

Rapporto

1. Introduzione

1.1. Quadro generale

Il presente documento rappresenta la Dichiarazione sulle prassi del servizio di verifica dell'identità (Identity Proofing Service Practice Statement, «IPSPS») per l'apertura di un conto online presso LGT. Non è una dichiarazione sulle prassi di certificazione (Certification Practice Statement, CPS), in quanto il servizio di verifica dell'identità di LGT copre unicamente gli aspetti relativi alla verifica dell'identità per l'emissione di certificati qualificati e non include servizi di certificazione. I servizi di certificazione e la relativa CPS sono forniti da Swisscom, la CPS è disponibile qui:
https://www.swisscom.ch/it/business/enterprise/offerta/security/digital_certificate_service.html

LGT garantisce che eventuali parti terze fornitrici di tali servizi rispettino le pratiche e le politiche definite nel presente documento.

Al fine di verificare l'identità del/della richiedente, LGT ha sviluppato la LGT Remote Identification. Questa soluzione remota self-service automatizzata consente l'apertura di un conto online che a sua volta consente l'utilizzo dei servizi di Digital Banking disponibili. La LGT Remote Identification verifica l'identità di una persona fisica conformemente ai requisiti normativi del Liechtenstein, della Svizzera, e dell'Austria per il rilascio di una firma elettronica qualificata in conformità alla legge svizzera («FiEle») e alla legge europea («eIDAS») affinché il/la richiedente firmi i documenti contrattuali di LGT. Per i dati rilevanti nelle giurisdizioni summenzionate si applicano periodi di conservazione diversi.

La LGT Remote Identification legge il passaporto biometrico (noto anche come ePassport) di un/una richiedente che utilizza il suo telefono cellulare abilitato NFC. Il servizio garantisce che:

- sia la persona corretta: il volto del/della richiedente corrisponde alla foto del passaporto biometrico;
- sia una persona reale: la tecnologia di analisi del rilevamento della liveness garantisce che si tratti di un essere umano autentico, non di una foto, di una registrazione video, di un deep fake, di un'altra falsificazione;
- l'autenticazione abbia luogo in tempo reale: la sequenza di colori illuminati crea una caratteristica biometrica unica che non può essere riutilizzata o ricreata, e che conferma l'autenticazione in tempo reale.

La figura seguente mostra il workflow della verifica dell'identità:

- ETSI TS 119 461
- ETSI EN 319 401

Il/la richiedente deve essere una persona fisica. Il processo di verifica dell'identità si svolge da remoto e in modo automatizzato.

1.2. Ambito di applicazione

Il presente documento descrive le prassi applicate per fornire la LGT Remote Identification e per rispettare i requisiti normativi vigenti relativi alla verifica dell'identità come definiti nella ETSI TS 119 461, al capitolo 9.2.3.4: «Use case for automated operation» e nella ETSI EN 319 401 per fornire una verifica automatica dell'identità da remoto con operazione automatizzata.

1.3. Processo di verifica dell'identità

La LGT Remote Identification segue la sequenza di verifica dell'identità definita nella ETSI TS 119 461:

La LGT Remote Identification rispetta i requisiti di verifica dell'identità di cui al capitolo 8 della ETSI TS 119 461:

Capitolo	**Sommario**
8.1	Inizio
8.2.1	**Raccolta di attributi e prove** – requisiti generali
8.2.2.1	Raccolta di attributi relativi a una persona fisica
8.2.3	Uso del documento d'identità fisico e digitale come prova
8.3.1	**Convalida di attributi e prove** – requisiti generali
8.3.2	Convalida del documento d'identità digitale
8.4.1	**Legame con il/la richiedente** – requisiti generali
8.4.2	Acquisizione dell'immagine del volto del/della richiedente
8.4.3	Legame con il/la richiedente tramite i dati biometrici facciali automatizzati
8.5.1	Risultato della verifica dell'identità
8.5.2	**Prova del processo di verifica dell'identità**

LGT imponee la condizione che anche i propri fornitori coinvolti o fornitori terzi partecipanti rispettino tali requisiti e adottino opportune precauzioni.

1.4. Termini e abbreviazioni

Termini e abbreviazione	**Descrizione**
Richiedente	Persona fisica la cui identità deve essere verificata
CPS	Dichiarazione sulle prassi di certificazione («Certificate Practice Statement»)
ICAO	Organizzazione dell'aviazione civile internazionale («International Civil Aviation Organization») Gestisce lo standard globale relativo ai documenti di viaggio a lettura ottica (Machine Readable Travel Documents, «MRTD») – documento ICAO 9303
MRTD	Documento di viaggio a lettura ottica («Machine Readable Travel Document»)
MRZ	Zona a lettura ottica («Machine Readable Zone»)
NFC	Comunicazione in prossimità («Near Field Communication»)
TLS	Sicurezza a livello di trasporto («Transport Layer Security»)

2. Amministrazione documenti

Il presente documento viene rivisto e aggiornato regolarmente, in ogni caso almeno una volta per ogni anno civile, in occasione di modifiche di requisiti legali o normativi, direttive LGT, servizi o modifiche nel processo di verifica dell'identità. È necessaria l'autorizzazione del Management Team LGT responsabile della verifica dell'identità.

2.1. Notifica di modifiche

Le/gli utenti saranno informati in merito a modifiche della IPSPS.
Eventuali modifiche della IPSPS dovranno essere approvate dalle/dagli utenti.

2.2. Dati di contatto

gr-a2-liec-clm1@a2.loc

2.3. Termini e condizioni

La presente IPSPS diventa efficace dalla data di pubblicazione sul sito web di LGT.
Eventuali modifiche diventano efficaci al momento della pubblicazione. Il presente documento rimane valido fino alla sua sostituzione con una nuova versione.

3. Copertura dei requisiti della ETSI 119 461

3.1. Inizio

I termini e le condizioni concernenti l'apertura di un conto online presso LGT e i servizi di certificazione di Swisscom sono forniti al/alla
richiedente. Essi includono informazioni riguardo alla giurisdizione in cui i dati sono trattati e archiviati, al periodo di conservazione, alla protezione dei dati,
ad aspetti relativi alla privacy e alle leggi applicabili.
Il/la richiedente deve accettare le Condizioni di utilizzo e l'Avvertenza in materia di protezione dei dati. In Austria e in Liechtenstein il/la richiedente deve inoltre accettare il disclaimer relativo alla Fernabsatzgesetz (legge sui contratti conclusi a distanza).

3.2. Raccolta di attributi e prove

La raccolta di attributi e prove è basata sullo standard previsto dal documento ICAO 9303 per i documenti di viaggio a lettura ottica (MRTD).

La LGT Remote Identification chiede all'utente di scannerizzare la prima pagina del passaporto contenente la zona a lettura ottica (Machine Readable Zone, MRZ) e la zona di ispezione visiva (Visual Inspection Zone, VIZ) - utilizzando la fotocamera del telefono cellulare.
Il nome del/della richiedente indicato nella VIZ è utilizzato per il contratto per motivi legali e normativi.
I dati della MRZ sono utilizzati per creare la password al fine di leggere i dati sul chip del passaporto biometrico tramite NFC.
La LGT Remote Identification raccoglie tutti i dati indicati nella MRZ, nella VIZ e nel chip come specificato nel documento ICAO 9303.
Principali attributi raccolti dal passaporto biometrico:

- Paese emittente
- Data di scadenza
- Numero del documento
- Nome e cognome
- Data di nascita
- Genere
- Foto

Qualora il processo di verifica dell'identità non sia più fornito, LGT conserverà i dati già raccolti conformemente ai requisiti locali locali e informerà opportunamente le parti interessate.

3.3. Convalida di attributi e prove

La convalida di attributi e prove è basata sullo standard previsto dal documento ICAO 9303 per i documenti di viaggio a lettura ottica (MRTD).

L'autenticità del passaporto biometrico è verificata attraverso la convalida delle firme digitali dei dati raccolti dal chip tramite NFC a fronte del certificato di firma del relativo Paese emittente.
La fonte affidabile dei certificati di firma è la Public Key Directory (PKD) della ICAO.
Il contenuto della VIZ, della MRZ e dei dati del chip è sottoposto a controlli incrociati sulla base del documento ICAO 9303.
Valgono le seguenti restrizioni:

- I passaporti provenienti da Paesi sanzionati da LGT non sono accettati
- Il passaporto biometrico deve supportare un meccanismo di rilevamento dei cloni che deve essere accettato, ad esempio, autenticazione attiva o autenticazione del chip
- La Public Key Directory (PKD) della ICAO è la fonte affidabile per la verifica delle informazioni necessarie per l'autenticazione dei documenti di viaggio elettronici a lettura ottica (eMRTD) come ad esempio gli ePassport. Solo i Paesi che pubblicano i loro certificati tramite la PKD della ICAO sono supportati da LGT

La validità del passaporto è verificata controllando la data di scadenza nel chip. La protezione dall'utilizzo malevolo di passaporti rubati è garantita durante il legame con il/la richiedente tramite il confronto facciale. Tutti i dati in transito sono protetti da TLS.

3.4. Legame con il/la richiedente

Durante l'intera sessione di verifica dell'identità, il/la richiedente è registrato/a sulla piattaforma di Smart Banking esistente di LGT e identificato/a in maniera univoca col relativo nome utente. Ciò garantisce l'integrità della sessione, sia sul cellulare del/della cliente che sul back-end.

3.5. Prova del processo di verifica dell'identità

Tutti i dati letti dal passaporto biometrico del/della richiedente nonché il video selfie sono archiviati con un periodo di conservazione di 30 giorni. Tutti i dati sono protetti conformemente alle direttive LGT e ai requisiti legali e normativi applicabili.