Identity Proofing Service Practice Statement (IPSPS)

für die Online-Kontoeröffnung bei der LGT

Version:	1.1
Publikationsdatum:	24.08.2023
Genehmigt durch:	das für Identitätsnachweise zuständige LGT Management Team

Bericht

1. Einleitung

1.1. Übersicht

Bei diesem Dokument handelt es sich um das Identity Proofing Service Practice Statement («IPSPS», die Erklärung zum Identitätsnachweisverfahren) für die Online-Kontoeröffnung bei der LGT. Es stellt kein Certification Practice Statement («CPS», Erklärung zum Zertifizierungsverfahren) dar, weil der Identity Proofing Service von LGT nur die Aspekte der Erbringung von Identitätsnachweisen für die Ausstellung von qualifizierten Zertifikaten abdeckt und keine Zertifizierungsdienstleistungen beinhaltet. Die Zertifizierungsdienstleistungen und das entsprechende CPS werden von Swisscom bereitgestellt. Das CPS ist unter folgendem Link zu finden: https://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html

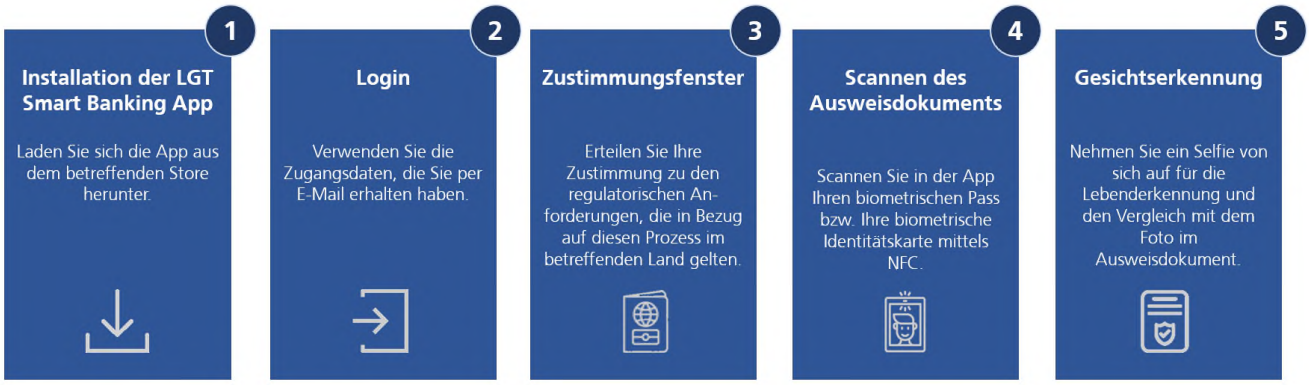
Die LGT stellt sicher, dass Dritte, die solche Dienstleistungen erbringen, die in diesem Dokument definierten Verfahren und Richtlinien einhalten.

Zur Überprüfung der Identität der Antragstellerin oder des Antragstellers hat die LGT die LGT Remote Identification entwickelt. Diese automatisierte Self-Service-Lösung für den Fernzugriff erleichtert die Online-Kontoeröffnung, die Voraussetzung für die Nutzung der verfügbaren Digital-Banking-Dienstleistungen ist. LGT Remote Identification verifiziert die Identität einer natürlichen Person gemäss den regulatorischen Anforderungen Liechtensteins, der Schweiz und Österreichs. Auf dieser Grundlage wird eine qualifizierte elektronische Signatur gemäss Schweizer («ZertES») sowie europäischem («eIDAS») Recht erstellt, welche die Antragstellerin oder der Antragsteller zur Unterzeichnung der Vertragsdokumente der LGT verwenden kann. In den oben genannten Ländern gelten verschiedene Aufbewahrungsfristen für die relevanten Daten.

LGT Remote Identification liest den biometrischen Pass (auch als ePass bekannt) einer Antragstellerin oder eines Antragstellers anhand von deren bzw. dessen NFC-fähigem Mobiltelefon. Durch den Service wird sichergestellt, dass:

- es sich um die richtige Person handelt: Das Gesicht der Antragstellerin oder des Antragstellers stimmt mit dem Foto des biometrischen Passes überein;
- es sich um eine reale Person handelt: Die verwendete Analysetechnologie zur Lebenderkennung garantiert, dass es sich um einen echten Menschen handelt – und nicht um ein Foto, eine Video-Wiedergabe, ein Deepfake oder eine sonstige Fälschung;
- die Authentifizierung in Echtzeit erfolgt: Der Prozess mit seiner Abfolge verschiedenfarbiger Sequenzen auf dem Display erstellt eine biometrische Einmal-Funktion, welche weder wiederverwendet noch nachgebildet werden kann und welche die Echtzeit-Authentifizierung bestätigt.

Die folgende Abbildung veranschaulicht den Ablauf des Identitätsnachweisverfahrens:



- ETSI TS 119 461
- ETSI EN 319 401

Die Antragstellerin oder der Antragsteller muss eine natürliche Person sein. Das Identitätsnachweisverfahren ist automatisiert und wird mittels Fernzugriff durchgeführt.

1.2. Geltungsbereich

Dieses Dokument beschreibt die Verfahren, die angewandt werden, um die Dienstleistung LGT Remote Identification zu erbringen und die geltenden regulatorischen Anforderungen für Identitätsnachweise gemäss Definition in den Normen ETSI TS 119 461, Kapitel 9.2.3.4 «Use case for automated operation», sowie ETSI EN 319 401 für die Durchführung eines unbeaufsichtigten, automatisierten Identitätsnachweisverfahrens mittels Fernzugriff zu erfüllen.

1.3. Identitätsnachweisverfahren

Bei LGT Remote Identification wird der in der Norm ETSI TS 119 461 definierte Ablauf des Identitätsnachweisverfahrens befolgt:

LGT Remote Identification entspricht den Anforderungen für Identitätsnachweise gemäss Kapitel 8 der Norm ETSI TS 119 461:

Kapitel	Inhalt
8.1	Initiation
8.2.1	**Attribute and Evidence Collection** – General Requirements
8.2.2.1	Attribute Collection for Natural Person
8.2.3	Use of physical and digital identity document as evidence
8.3.1	**Attribute and evidence validation** – General Requirements
8.3.2	Validation of digital identity document
8.4.1	**Binding to applicant** – General Requirements
8.4.2	Capture of face image of the applicant
8.4.3	Binding to applicant by automated face biometrics
8.5.1	Result of the identity proofing
8.5.2	**Evidence of the identity proofing process**

Die LGT stellt die Bedingung, dass ihre involvierten oder beteiligten Drittanbieter diese Anforderungen ebenfalls einhalten und entsprechende Vorkehrungen treffen.

1.4. Begriffe und Abkürzungen

Begriffe und Abkürzungen	Erklärung
Antragstellerin oder Antragsteller	Natürliche Person, deren Identität nachgewiesen werden soll
CPS	Certificate Practice Statement (Erklärung zum Zertifizierungsverfahren)
ICAO	International Civil Aviation Organization (Internationale Zivilluftfahrt-Organisation) Die Organisation verwaltet die globale Norm für maschinenlesbare Reisedokumente (ICAO-Dok. 9303).
MRTD	Machine Readable Travel Document (maschinenlesbares Reisedokument)
MRZ	Machine Readable Zone (maschinenlesbarer Bereich)
NFC	Near Field Communication (Nahfeldkommunikation)
TLS	Transport Layer Security (Transportschichtsicherheit)

2. Dokumentverwaltung

Dieses Dokument wird regelmässig, jedoch zumindest einmal pro Kalenderjahr sowie im Bedarfsfall bei Änderungen der gesetzlichen oder regulatorischen Anforderungen, der LGT Richtlinien, der Dienstleistungen oder des Identitätsnachweisverfahrens überprüft und aktualisiert. Die Genehmigung des für die Identitätsnachweise zuständigen Management Teams der LGT ist erforderlich.

2.1. Änderungsbenachrichtigung

Die Benutzerinnen und Benutzer werden über Änderungen der IPSPS benachrichtigt.
Alle Änderungen der IPSPS müssen von den Benutzerinnen und Benutzern genehmigt werden.

2.2. Kontaktangaben

gr-a2-liec-clm1@a2.loc

2.3. Bedingungen

Diese IPSPS tritt am Datum der Veröffentlichung auf der LGT Website in Kraft.
Änderungen treten zum Zeitpunkt der Veröffentlichung in Kraft. Dieses Dokument bleibt so lange gültig, bis es durch eine neue Version ersetzt wird.

3. Abdeckung der Anforderungen der Norm ETSI 119 461

3.1. Anbahnung

Die Bedingungen der Online-Kontoeröffnung bei der LGT und der Zertifizierungsdienstleistungen der Swisscom werden der Antragstellerin bzw. dem Antragsteller vorgelegt.
Darunter fallen Informationen über das Land, in dem die Daten verarbeitet und gespeichert werden, die Aufbewahrungsfrist, die Datenschutz- und Datensicherheitsaspekte sowie die geltenden Gesetze.

Die Antragstellerin oder der Antragsteller muss die Nutzungsbestimmungen und den Datenschutzhinweis akzeptieren. In Österreich und Liechtenstein muss die Antragstellerin bzw. der Antragsteller zudem den Fernabsatzgesetz-Disclaimer akzeptieren.

3.2. Erfassung der Attribute und Nachweise

Die Erfassung der Attribute und Nachweise stützt sich auf die ICAO-Norm Dokument 9303, Machine Readable Travel Documents (MRTD).

Im Rahmen der LGT Remote Identification wird die Benutzerin oder der Benutzer gebeten, mittels der Mobiltelefon-Kamera die erste Passseite zu scannen. Diese enthält den maschinenlesbaren Bereich (MRZ) und den Sichtprüfungsbereich (Visual Inspection Zone, VIZ).
Aus rechtlichen und regulatorischen Gründen wird der Name der Antragstellerin bzw. des Antragstellers aus dem VIZ für den Vertrag verwendet.
Die MRZ-Daten dienen der Erstellung der Passphrase, die erforderlich ist, um die Chipdaten des biometrischen Passes mittels NFC zu lesen.
LGT Remote Identification sammelt alle MRZ-, VIZ- und Chip-Daten gemäss dem ICAO-Dokument 9303.
Es werden folgende Schlüsselattribute des biometrischen Passes erfasst:

- Ausgabeland
- Ablaufdatum
- Dokumentnummer
- Vor- und Nachname
- Geburtsdatum
- Geschlecht
- Foto

Für den Fall, dass das Identitätsnachweisverfahren nicht mehr durchgeführt wird, speichert die LGT die bereits erfassten Daten gemäss den vor Ort geltenden Rechtsvorschriften und kommuniziert dementsprechend mit den betreffenden Parteien.

3.3. Validierung der Attribute und Nachweise

Die Validierung der Attribute und Nachweise stützt sich auf die ICAO-Norm Dokument 9303, Machine Readable Travel Documents (MRTD).

Die Feststellung der Echtheit des biometrischen Passes erfolgt, indem die digitalen Signaturen der mittels NFC erfassten Chip-Daten mit dem Signaturzertifikat des betreffenden Ausgabelands abgeglichen werden.

Als vertrauenswürdige Quelle für die Signaturzertifikate fungiert der ICAO Public Key Directory (PKD).
Die Inhalte der VIZ-, MRZ- und Chip-Daten werden auf Grundlage der ICAO-Norm (Dokument 9303) überprüft und abgeglichen.
Es gelten die folgenden Einschränkungen:

- Pässe von Ländern, die von der LGT mit Sanktionen belegt wurden, werden nicht akzeptiert.
- Damit der biometrische Pass akzeptiert werden kann, muss er einen Klonerkennungsmechanismus wie Active Authentication oder Chip Authentication unterstützen.
- Der ICAO Public Key Directory (PKD) fungiert als vertrauenswürdige Quelle für die Überprüfung der Informationen, die zur Authentifizierung von elektronischen maschinenlesbaren Reisedokumenten (eMRTDs) wie ePässen erforderlich sind. Es werden nur diejenigen Länder durch die LGT unterstützt, die ihre Zertifikate mittels PKD der ICAO publizieren.

Die Gültigkeit des Passes wird durch Überprüfung des Ablaufdatums auf dem Chip festgestellt. Der Schutz vor einer böswilligen Verwendung gestohlener oder verlorener Pässe wird gewährleistet, indem die Verbindung zur Antragstellerin oder zum Antragsteller mittels Gesichtsvergleich hergestellt wird. Bei der Übertragung werden sämtliche Daten durch TLS gesichert.

3.4. Verbindung zur Antragstellerin oder zum Antragsteller

Während der gesamten Identitätsnachweissitzung ist die Antragstellerin oder der Antragsteller in die bestehende Smart-Banking-Plattform der LGT eingeloggt, wo sie/er sich eindeutig mit dem eigenen Benutzernamen identifiziert hat. Dies gewährleistet die Integrität der Sitzung sowohl auf dem Mobiltelefon der Kundin oder des Kunden als auch am Backend.

3.5. Belege aus dem Identitätsnachweisverfahren

Alle aus dem biometrischen Pass der Antragstellerin oder des Antragstellers ausgelesenen Daten und das Video-Selfie werden 30 Tage lang gespeichert. Alle Daten sind im Einklang mit den Richtlinien der LGT und den geltenden rechtlichen und regulatorischen Anforderungen geschützt.