Identity Proofing Service Practice Statement (IPSPS)

for online account opening at LGT

Version:	1.1
Publication Date:	24.08.2023
Approval by :	LGT Management Team responsible for identity proofing

Report

1. Introduction

1.1. Overview

This document represents the Identity Proofing Service Practice Statement ("IPSPS") for online account opening at LGT. It is not a Certification Practice Statement (CPS), as the LGT identity proofing service covers only the aspects of identity proofing for the issuance of qualified certificates and does not include certification services. The certification services and the corresponding CPS are provided by Swisscom. The CPS can be found here:
https://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html

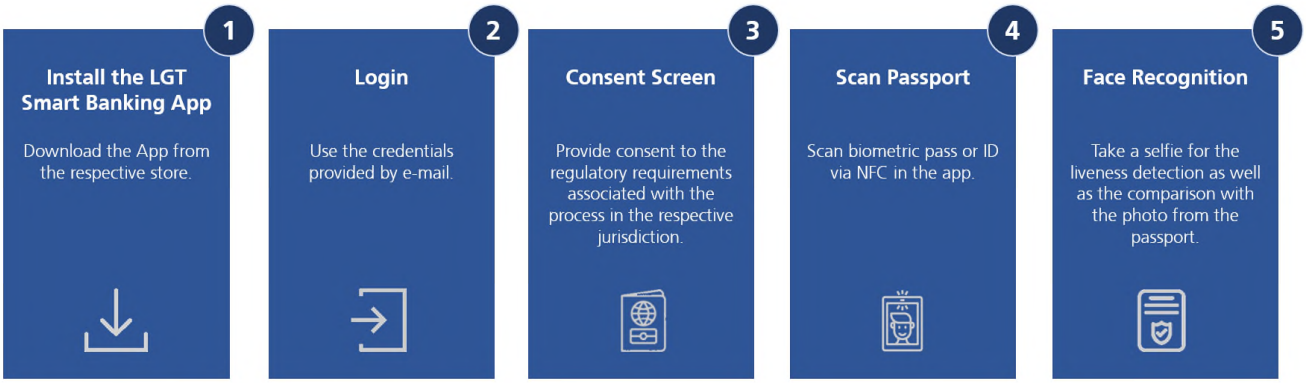
LGT ensures that any third parties providing such services conform to the practices and policies defined in this document.

To verify the applicant's identity, LGT has developed LGT Remote Identification. This automated self-service remote solution facilitates online account opening which in turn enables use of the available digital banking services. LGT Remote Identification verifies the identity of a natural person in accordance with the regulatory requirements in Liechtenstein, Switzerland and Austria in order to issue a qualified electronic signature according to Swiss ("ZertES") as well as European ("eIDAS") law for the applicant to sign the LGT contract documents. Different retention periods for the relevant data are applied for the above-mentioned jurisdictions.

LGT Remote Identification reads the biometric passport (also known as ePassport) of an applicant using their NFC-enabled mobile phone. The service ensures that:

- it is the right person: the applicant's face matches the photo from the biometric passport;
- it is a real person: liveness detection analysis technology guarantees that it is a genuine human, not a photo, a video replay, a deep fake, or other spoof;
- the authentication takes place in real time: the illuminated colour sequence creates a one-time biometric feature that cannot be reused or recreated, and that confirms the real-time authentication.

The following illustration shows the identity proofing workflow:



- ETSI TS 119 461
- ETSI EN 319 401

The applicant must be a natural person. The identity proofing process is remote and automated.

1.2. Scope

This document describes the practices applied to provide LGT Remote Identification and to meet the applicable regulatory requirements for identity proofing as defined in ETSI TS 119 461, chapter 9.2.3.4: "Use case for automated operation" and ETSI EN 319 401 for providing unattended remote identity proofing with automated operation.

1.3. Identity proofing process

LGT Remote Identification follows the identity proofing sequence as defined in ETSI TS 119 461:

LGT Remote Identification conforms to the identity proofing requirements as specified in chapter 8 of ETSI TS 119 461:

Chapter	Content
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**

LGT imposes the condition that its involved or participating third-party providers also comply with these requirements and take appropriate precautions.

1.4. Terms and abbreviations

Terms and abbreviations	Description
Applicant	Natural person, identity to be proven
CPS	Certificate Practice Statement
ICAO	International Civil Aviation Organisation Manages the global standard for Machine Readable Travel Documents (MRTD) – ICAO Doc 9303
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NFC	Near Field Communication
TLS	Transport Layer Security

2. Document administration

This document is reviewed and updated on a regular basis but at least once per calendar year and on the occasion of any changes to legal or regulatory requirements, LGT policies, services or a change in the identity proofing process. Approval is required by the LGT management team responsible for identity proofing.

2.1. Change notification

Users will be notified of changes to the IPSPS.
Any changes to the IPSPS must be approved by the users.

2.2. Contact details

gr-a2-liec-clm1@a2.loc

2.3. Terms and conditions

This IPSPS becomes effective from the date of publication on the LGT website.
Amendments become effective upon publication. This document remains valid until it is replaced by a new version.

3. Coverage of ETSI 119 461 requirements

3.1. Initiation

The terms and conditions of online account opening at LGT and Swisscom certification services are presented to the applicant. This includes information about the jurisdiction where data are processed and stored, the retention period, data protection and privacy aspects and applicable laws.
The applicant must accept the terms of use as well as the data privacy notice. In Austria and Liechtenstein the applicant furthermore must accept the Distance Selling Act (Fernabsatzgesetz) disclaimer.

3.2. Attribute and evidence collection

Attribute and evidence collection is based on the ICAO Doc 9303 standard for Machine Readable Travel Documents (MRTD).

LGT Remote Identification asks the user to scan the first page of the passport that contains the Machine Readable Zone (MRZ) and the Visual Inspection Zone (VIZ) using the camera of the mobile phone.
The applicant's name from the VIZ is used for the contract for legal and regulatory reasons.
The MRZ data is used to create the passphrase to read the data on the chip of the biometric passport via NFC.
LGT Remote Identification collects all the data from MRZ, VIZ and the chip as specified by ICAO Doc 9303.
Key attributes that are collected from the biometric passport:

- Issuing country
- Expiration date
- Document number
- First and last name
- Date of birth
- Gender
- Photo

If the identity proofing process is no longer provided, LGT stores the data already collected in accordance with local legal requirements and communicates accordingly with the relevant parties.

3.3. Attribute and evidence validation

Attribute and evidence validation is based on the ICAO Doc 9303 standard for Machine Readable Travel Documents (MRTD).

The authenticity of the biometric passport is verified by validating the digital signatures of the data collected from the chip via NFC against the signing certificate of the corresponding issuing country.
The trustworthy source for the signing certificates is the ICAO Public Key Directory (PKD).
The content of the VIZ, the MRZ and the chip data is cross-checked based on ICAO Doc 9303.
The following restrictions apply:

- Passports from LGT-sanctioned countries are not accepted
- The biometric passport must support a clone detection mechanism to be accepted, ie Active Authentication or Chip Authentication
- The ICAO Public Key Directory (PKD) is the trusted source for verifying the information required to authenticate electronic Machine Readable Travel Documents (eMRTDs) such as ePassports. Only countries that publish their certificates via ICAO PKD are supported by LGT

The validity of the passport is verified by checking the expiration date from the chip. Protection against malicious usage of stolen or lost passports is ensured during the binding to the applicant through face comparison. All data in transit are protected by TLS.

3.4. Binding to applicant

During the whole identity proofing session, the applicant is logged into LGT's existing SmartBanking platform and uniquely identified with their username. This ensures the integrity of the session, both on the client's mobile phone as well as on the backend.

3.5. Evidence of the identity proofing process

All data read from the biometric passport of the applicant as well as the video selfie are stored with a 30-day retention period. All data are protected according to LGT policies and to the applicable legal and regulatory requirements.