Identity Proofing Service Practice Statement (IPSPS)

pour l'ouverture d'un compte en ligne chez LGT

Version:	1.2
Date de publication:	01.04.2024
Approuvé par:	LGT Management Team responsable du contrôle d'identité

Sommaire

1. Introduction

1.1. Aperçu

Le présent document constitue l'Identity Proofing Service Practice Statement («IPSPS») pour l'ouverture d'un compte en ligne chez LGT. Il ne s'agit pas d'un Certification Practice Statement (CPS), étant donné que le service de contrôle d'identité de LGT ne couvre que les aspects du contrôle d'identité relatifs à la délivrance de certificats qualifiés, sans inclure les services de certification. Les services de certification et le CPS correspondant sont fournis par Swisscom. Le CPS peut être consulté à cette adresse: https://www.swisscom.ch/fr/business/enterprise/offre/security/digital_certificate_service.html

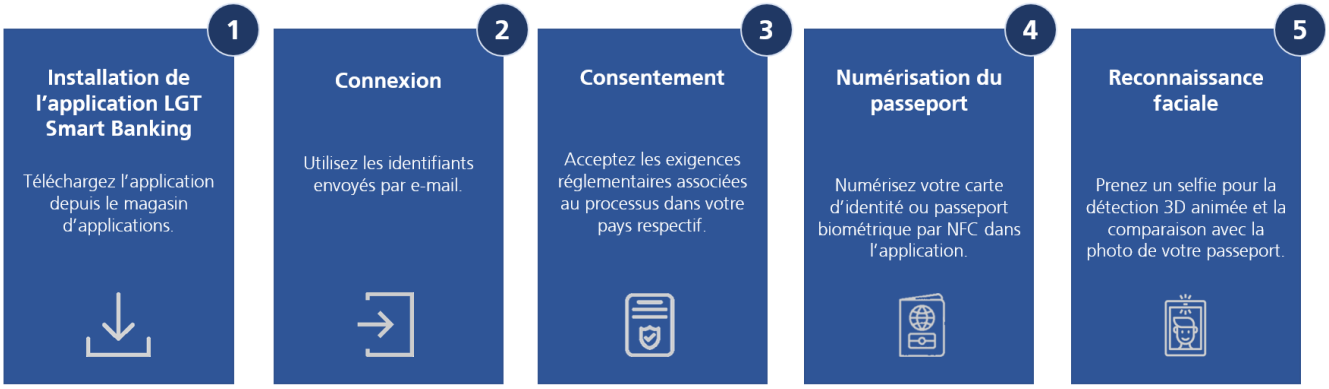
LGT veille à ce que tout tiers fournissant pareils services respecte les pratiques et règles définies dans le présent document.

Pour vérifier l'identité des personnes candidates, LGT a développé la procédure LGT Remote Identification. Cette solution à distance automatisée est en self-service et facilite l'ouverture de compte en ligne en vue de l'utilisation des services de banque en ligne disponibles. La LGT Remote Identification vérifie l'identité d'une personne physique conformément aux exigences réglementaires en vigueur au Liechtenstein, en Suisse et en Autriche, sur la signature électronique qualifiée selon les législations suisses («SCSE») et européennes («eIDAS») qui permet aux personnes candidates de signer les documents contractuels de LGT. Les pays susmentionnés appliquent des périodes de conservation des données variables. Le service d'identification «LGT Remote Identification» proposé doit être à la disposition de toute personne qui peut aussi utiliser celui-ci de façon réglementaire. Le service, expressément non discriminatoire, est également mis à la disposition des personnes en situation de handicap.

La LGT Remote Identification lit le passeport biométrique (également connu sous le nom de passeport électronique) de la personne candidate à partir du téléphone portable NFC de cette dernière. Le service vérifie:

- qu'il s'agit de la bonne personne: le visage de la personne candidate correspond à la photo du passeport biométrique;
- qu'il s'agit d'une personne réelle: la technologie d'analyse de détection 3D animée («liveness») garantit qu'il s'agit d'une vraie personne et non d'une photo, d'un enregistrement vidéo, d'un hypertrucage ou autre contrefaçon;
- que l'authentification se déroule en temps réel: la séquence colorée éclairée crée un attribut biométrique unique qui ne peut pas être réutilisé ou recréé et qui confirme l'authentification en temps réel.

La figure ci-après illustre le déroulement du contrôle d'identité:



- ETSI TS 119 461
- ETSI EN 319 401

La personne candidate doit être une personne physique. Le processus de contrôle d'identité est automatisé et se déroule à distance

1.2. Portée

Le présent document décrit les pratiques mises en place pour fournir le service LGT Remote Identification conformément aux exigences réglementaires en vigueur pour le contrôle d'identité telles que définies par l'ETSI TS 119 461, chapitre 9.2.3.4: «Use case for automated operation» et l'ETSI EN 319 401 pour la fourniture de services de contrôle d'identité à distance sans surveillance avec fonctionnement automatisé.

1.3. Processus de contrôle d'identité

La procédure LGT Remote Identification suit la démarche définie par l'ETSI TS 119 461 pour le contrôle d'identité:

La solution LGT Remote Identification est conforme aux consignes de contrôle d'identité spécifiées au chapitre 8 de l'ETSI TS 119 461:

Chapitre	**Contenu**
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 impose à ses fournisseurs tiers impliqués ou participants de se conformer à ces exigences et de prendre les mesures appropriées.

1.4. Termes et abréviations

Termes et abréviations	**Description**
Personne candidate	Personne physique, identité à prouver
CPS	Certificate Practice Statement
OACI	Organisation de l'aviation civile internationale Gère la norme internationale sur les documents de voyage lisibles à la machine (DVLM) – (ICAO-Doc 9303)
DVLM	Document de voyage lisible à la machine
ZLA	Zone de lecture automatique
NFC	Near Field Communication
TLS	Transport Layer Security

2. Administration des documents

Le présent document est passé en revue et mis à jour régulièrement, dont au moins une fois par année civile, et lors d'évolutions des exigences réglementaires ou juridiques, des règles de LGT, des services ou en cas de changement au sein du processus de contrôle d'identité. L'équipe de gestion de LGT responsable du contrôle d'identité doit donner son approbation.

2.1. Avis de changement

Les utilisatrices et utilisateurs seront informés des changements fondamentaux qui pourraient influencer leur autorisation d'utilisation.
La version actuelle du présent document peut être consultée via le site web de LGT accessible au grand public.

2.2. Coordonnées

lgt.identification@lgt.com

2.3. Conditions

L'IPSPS entre en vigueur à compter de sa date de publication sur le site web de LGT.
Les modifications seront applicables à leur publication. Le présent document restera valable jusqu'à son remplacement par une nouvelle version.

3. Couverture des exigences de l'ETSI 119 461

3.1. Initiation (démarrage)

Les conditions d'ouverture de compte en ligne chez LGT et des services de certification Swisscom sont présentées à la personne candidate.
Y figurent des informations sur les pays où sont traitées et conservées les données, sur leur durée de conservation, sur leur protection, sur leur confidentialité et sur les lois applicables.

La personne candidate doit accepter les conditions ainsi que les informations sur la protection des données. En Autriche et au Liechtenstein, la personne candidate doit également accepter la limitation de responsabilité de la Fernabsatzgesetz.

3.2. Attribute and evidence collection (recueil des attributs et des preuves)

Le recueil des attributs et des preuves s'appuie sur le Doc 9303 OACI relatif aux documents de voyage lisibles à la machine (DVLM) qui sert de norme.

La procédure LGT Remote Identification demande à la personne utilisatrice de numériser la première page de son passeport qui contient la zone de lecture automatique (ZLA) et la zone d'inspection visuelle (ZIV) - en utilisant la caméra de son téléphone portable.
Le nom de la personne candidate qui apparaît dans la ZIV est utilisé pour le contrat pour des raisons juridiques et réglementaires.
Les données ZLA servent à créer la phrase de passe pour lire les données figurant sur la puce du passeport biométrique par NFC.
LGT Remote Identification recueille toutes les données figurant dans la ZLA, dans la ZIV et sur la puce telles que spécifiées dans le Doc 9303 OACI.
Attributs clés recueillis du passeport biométrique:

- pays émetteur
- date d'expiration
- numéro de document
- nom et prénom
- date de naissance
- sexe
- photo

Si le processus de contrôle d'identité prend fin, LGT conservera les données déjà recueillies en accord avec les exigences réglementaires locales et communiquera en conséquence avec les parties concernées.

3.3. Attribute and evidence validation (validation des attributs et des preuves)
La validation des attributs et des preuves s'appuie sur le Doc 9303 OACI relatif aux documents de voyage lisibles à la machine (DVLM) qui sert de norme.

L'authenticité de la pièce d'identité biométrique est vérifiée en validant les signatures numériques des données recueillies à partir de la puce par NFC par rapport au certificat de signature du pays émetteur correspondant.

En guise de source de confiance pour les certificats de signature, il convient d'établir une vérification au regard des données actuelles des pays émetteurs. Pour satisfaire à cette exigence réglementaire, LGT établit une vérification vis-à-vis des listes de certificats publiées officiellement par les États émetteurs. (par exemple en Suisse: https://www.pki.admin.ch/crl/csca-switzerland-2.crl)

Le contenu de la ZIV et de la ZLA ainsi que les données de la puce sont vérifiés par recoupement sur la base du Doc 9303 OACI. Les restrictions ci-après s'appliquent:
- Les pièces d'identité émises par des pays sanctionnés par LGT sont refusées.
- Pour être acceptée, la pièce d'identité biométrique doit supporter un mécanisme de détection de clones, comme l'authentification active ou l'authentification de puce.
- LGT ne soutient que les pays (resp. leurs pièces d'identité) qui publient les certificats correspondants au moyen de l'URL.

La validité de la pièce d'identité est vérifiée en contrôlant la date d'expiration de la puce. Durant la confrontation avec la personne candidate, la comparaison des visages assure la protection contre l'usage malveillant d'une pièce d'identité perdue ou volée. Toutes les données en transit sont protégées par TLS.

3.4. Binding to applicant (confrontation avec la personne candidate)
Durant toute la session de contrôle de l'identité, la personne candidate est connectée à la plateforme de Smart Banking existante de LGT et uniquement identifiée par son nom d'utilisateur. Cette façon de faire garantit l'intégrité de la session, aussi bien sur le téléphone portable de la cliente ou du client qu'à l'arrière-plan.

3.5. Evidence of the identity proofing process (preuve du processus de contrôle d'identité)
Toutes les données lues à partir du passeport biométrique de la personne candidate ainsi que le selfie vidéo sont conservées durant une période de 30 jours. Toutes les données sont protégées conformément aux règles LGT et aux exigences réglementaires et juridiques applicables. Si le régulateur exige que certaines preuves du service d'identification soient conservées ou archivées au-delà de la période de 30 jours indiquée, LGT y veille également.

3.6. Fin de l'affaire bancaire
S'il est mis fin à la relation d'affaires entre l'utilisateur ou l'utilisatrice et LGT, LGT procède à la communication correspondante envers l'utilisatrice ou l'utilisateur et envers Swisscom.