Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1279

(09/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberespace – Gestion des identités

## Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité

Recommandation UIT-T X.1279

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1–X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200–X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300–X.399 |
| SYSTÈMES DE MESSAGERIE | X.400–X.499 |
| ANNUAIRE | X.500–X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600–X.699 |
| GESTION OSI | X.700–X.799 |
| SÉCURITÉ | X.800–X.849 |
| APPLICATIONS OSI | X.850–X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900–X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | |
| Aspects généraux de la sécurité | X.1000–X.1029 |
| Sécurité des réseaux | X.1030–X.1049 |
| Gestion de la sécurité | X.1050–X.1069 |
| Télébiométrie | X.1080–X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (1) | |
| Sécurité en multidiffusion | X.1100–X.1109 |
| Sécurité des réseaux domestiques | X.1110–X.1119 |
| Sécurité des télécommunications mobiles | X.1120–X.1139 |
| Sécurité de la toile | X.1140–X.1149 |
| Protocoles de sécurité (1) | X.1150–X.1159 |
| Sécurité d'homologue à homologue | X.1160–X.1169 |
| Sécurité des identificateurs en réseau | X.1170–X.1179 |
| Sécurité de la télévision par réseau IP | X.1180–X.1199 |
| SÉCURITÉ DU CYBERESPACE | |
| Cybersécurité | X.1200–X.1229 |
| Lutte contre le spam | X.1230–X.1249 |
| **Gestion des identités** | **X.1250–X.1279** |
| APPLICATIONS ET SERVICES SÉCURISÉS (2) | |
| Communications d'urgence | X.1300–X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310–X.1319 |
| Sécurité des réseaux électriques intelligents | X.1330–X.1339 |
| Courrier certifié | X.1340–X.1349 |
| Sécurité de l'Internet des objets (IoT) | X.1360–X.1369 |
| Sécurité des systèmes de transport intelligents | X.1370–X.1389 |
| Sécurité de la technologie des registres distribués | X.1400–X.1449 |
| Protocoles de sécurité (2) | X.1450–X.1459 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Échange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Échange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Échange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Échange garanti | X.1580–X.1589 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| Aperçu de la sécurité de l'informatique en nuage | X.1600–X.1601 |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en œuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |
| COMMUNICATIONS QUANTIQUES | |
| Terminologie | X.1700–X.1701 |
| Générateur quantique de nombres aléatoires | X.1702–X.1709 |
| Cadre de sécurité pour les réseaux QKDN | X.1710–X.1711 |
| Conception de la sécurité pour les réseaux QKDN | X.1712–X.1719 |
| Techniques de sécurité pour les réseaux QKDN | X.1720–X.1729 |
| SÉCURITÉ DES DONNÉES | |
| Sécurité des mégadonnées | X.1750–X.1759 |
| SÉCURITÉ DE LA 5G | X.1800–X.1819 |

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

# Recommandation UIT-T X.1279

## Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité


**Résumé**

La Recommandation UIT-T X.1279 fournit un cadre architectural pour l'authentification renforcée utilisant la télébiométrie et la détection d'usurpation d'identité. Cette Recommandation vise à analyser les menaces concernant les solutions traditionnelles d'authentification télébiométrique et spécifie un cadre architectural de même que les flux de processus d'authentification et les aspects liés à la sécurité de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité.



**Historique**

| Edition | Recommandation | Approbation | Commission d'études | Identifiant unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1279 | 03-09-2020 | 17 | 11.1002/1000/14261 |

**Mots clés**

Détection d'usurpation d'identité, authentification renforcée, télébiométrie.


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T á http://www.itu.int/ITU-T/ipr/.

## TABLE DES MATIÈRES

## Introduction

La technologie d'authentification télébiométrique est fréquemment utilisée dans divers domaines nécessitant un niveau de fiabilité élevé, comme les services bancaires en ligne et les services d'achats. Des efforts doivent être déployés pour élaborer un système de sécurité capable de faire face de manière préventive aux menaces potentielles de sécurité afin d'assurer la sécurité des données télébiométriques.

La présente Recommandation analyse les menaces concernant les solutions traditionnelles d'authentification télébiométrique et propose un cadre pour l'authentification renforcée utilisant la télébiométrie et la détection d'usurpation d'identité (ASD). La détection d'usurpation d'identité vise à déterminer que l'utilisateur qui envoie la demande d'authentification télébiométrique est bien la personne active qui détient les données biométriques. Elle peut être utilisée concomitamment à la vérification télébiométrique pour renforcer le niveau de sécurité et éviter la falsification des données biométriques. La fonction de détection d'usurpation d'identité peut être conçue de manière à renforcer la sécurité et à éviter la fuite de données biométriques.

# Recommandation UIT-T X.1279

## Cadre de l'authentification renforcée utilisant la télébiométrie avec des mécanismes de détection d'usurpation d'identité

### 1 Domaine d'application

La présente Recommandation fournit un cadre architectural pour l'authentification renforcée utilisant la télébiométrie avec des fonctions de détection d'usurpation d'identité. Cette Recommandation vise à analyser les menaces concernant les solutions traditionnelles d'authentification télébiométrique et spécifie un cadre architectural de même que les flux de processus d'authentification et les aspects liés à la sécurité de l'authentification renforcée utilisant la télébiométrie avec des fonctions de détection d'usurpation d'identité.

Le cadre architectural prévu dans cette Recommandation peut servir de guide lors du déploiement de solutions d'authentification télébiométrique renforcée utilisant des fonctionnalités de détection d'usurpation d'identité.

### 2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1086] Recommandation UIT-T X.1086 (2008), *Procédures de protection télébiométriques – Partie 1: Lignes directrices relatives aux mesures techniques et de gestion pour la sécurité des données biométriques*.

[UIT-T X.1087] Recommandation UIT-T X.1087 (2016), *Contremesures techniques et opérationnelles pour les applications de la télébiométrie utilisant des dispositifs mobiles*.

[ISO/CEI 24745] ISO/CEI 24745:2011, *Technologies de l'information – Techniques de sécurité – Protection des informations biométriques*.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 authentification** [b-ISO/CEI 2382-37]: processus permettant de prouver ou de montrer la légitimité d'une demande.

**3.1.2 biométrique** (adjectif) [b-ISO/CEI 2382]: relatif à la biométrie.

**3.1.3 capture biométrique** [b-ISO/CEI 2382-37]: obtention et enregistrement, sous une forme récupérable, d'un ou plusieurs signaux de caractéristiques biométriques directement depuis les individus ou depuis des représentations de caractéristiques biométriques.

**3.1.4 caractéristiques biométriques** [b-ISO/CEI 2382-37]: caractéristiques biologiques et comportementales d'un individu à partir desquelles il est possible d'extraire des éléments biométriques distinctifs et reproductibles à des fins de reconnaissance biométrique.

**3.1.5 données biométriques** [b-ISO/CEI 2382-37]: échantillon biométrique ou agrégation d'échantillons biométriques à n'importe quelle étape de la procédure, par exemple référence biométrique, sonde biométrique, élément biométrique ou propriété biométrique.

**3.1.6 éléments biométriques** [b-ISO/CEI 2382-37]: nombres ou étiquettes extraits des échantillons biométriques et utilisés à des fins de comparaison.

**3.1.7 reconnaissance biométrique/biométrie** [b-ISO/CEI 2382-37]: reconnaissance automatique des individus sur la base de leurs caractéristiques biologiques et comportementales.

**3.1.8 base de données de références biométriques** [b-ISO/CEI 2382-37]: base de données contenant des enregistrements de données de référence biométriques.

**3.1.9 modèle biométrique** [b-ISO/CEI 19784-1]: ensemble d'éléments biométriques stockés directement comparables aux éléments biométriques de reconnaissance.

**3.1.10 vérification biométrique** [b-ISO/CEI 2382-37]: processus qui consiste à confirmer une allégation biométrique par comparaison biométrique.

**3.1.11 comparaison (correspondance)** [b-ISO/CEI 19784-1]: estimation, calcul ou mesure de la similitude ou de la différence entre le ou les échantillons biométriques de reconnaissance/les éléments biométriques/les modèles biométriques et la ou les références biométriques.

**3.1.12 décision de comparaison** [b-ISO/CEI 19784-1]: la question est de savoir si le ou les échantillons biométriques de reconnaissance et la ou les références biométriques ont la même source biométrique, sur la base d'un ou de plusieurs résultats de comparaison, d'une ou de plusieurs politiques de décision incluant un niveau de seuil et d'autres éléments d'information le cas échéant.

**3.1.13 appareil mobile** [b-ISO 18461]: dispositif informatique portable comprenant généralement un écran d'affichage avec entrée tactile, stylet et/ou clavier et connexion Internet.

**3.1.14 utilisateur** [b-ISO/CEI 2382-37]: toute personne ou organisation interagissant de quelque manière que ce soit avec un système biométrique.

**3.1.15 télébiométrie** [b-UIT-T X.1081]: l'application de la télébiométrie aux télécommunications.

## 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 détection d'usurpation d'identité**: processus de détection et de prévention des piratages et des actions illicites à l'intérieur d'un système biométrique.

**3.2.2 obfuscation**: acte délibéré qui consiste à créer un code source ou machine difficilement compréhensible par les humains. Cette technique repose sur un ensemble de transformations qui changent le fonctionnement apparent du logiciel sans changer les résultats. Un programme obfusqué devrait produire exactement les mêmes résultats qu'un programme non obfusqué.

NOTE – L'obfuscation est une technique qui est normalement utilisée pour masquer la signification de certains logiciels en réorganisant les opérations, mais elle peut également être utilisée pour ajouter des filigranes faibles au code. Dans les deux cas, les algorithmes reposent sur un ensemble de transformations qui changent le fonctionnement apparent du logiciel sans changer les résultats. Un programme obfusqué devrait produire exactement les mêmes résultats qu'un programme non obfusqué. [b-Disappearing Cryptography]

**3.2.3 détection de la qualité**: mesure de l'aptitude d'un échantillon biométrique à mettre en œuvre ou à respecter la décision de comparaison biométrique.

**3.2.4 usurpation d'identité**: prétention supposée par une entité d'être une entité différente, en présentant une image enregistrée ou un autre échantillon de données biométriques, ou une caractéristique biométrique artificiellement reproduite, afin d'usurper l'identité d'un individu.

NOTE – Cette définition a été adaptée de [b-UIT M.3016.0].

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

ASD détection d'usurpation d'identité (*anti-spoofing detection*)

PII informations d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique (*public key infrastructure*)

SMS service de messages brefs (*short messaging service*)

SRP mot de passe distant sécurisé (*secure remote password*)

## 5 Conventions

Aucune.

## 6 Menaces de sécurité concernant l'authentification télébiométrique et contremesures

### 6.1 Contexte

Avec l'émergence des services Internet, les mécanismes d'authentification basés sur un mot de passe traditionnel ne peuvent plus satisfaire aux exigences de l'expérience utilisateur et des capacités de sécurité; on utilise aujourd'hui davantage des mécanismes d'authentification télébiométrique pour des raisons de commodité et de sécurité.

Cependant, il existe des obstacles et des risques associés aux mécanismes d'authentification biométrique, par exemple, les auteurs d'attaques peuvent utiliser une photo, une image générée par ordinateur ou un visage à l'écran pour l'authentification par reconnaissance faciale, certains encore peuvent utiliser une copie d'un échantillon télébiométrique (par exemple une empreinte digitale, de l'iris ou vocale) pour l'authentification télébiométrique.

### 6.2 Modes d'authentification de référence

Pour l'authentification télébiométrique sur les appareils mobiles, on distingue deux modes d'authentification de référence de base:

1) mode d'authentification en local: les données biométriques sont stockées sur un appareil mobile et la vérification télébiométrique est réalisée du côté de l'appareil mobile. Le résultat de la vérification télébiométrique est envoyé côté serveur;
2) mode d'authentification à distance: les données biométriques sont stockées sur le serveur et la vérification télébiométrique est réalisée du côté du serveur.

La présente Recommandation porte sur le mode d'authentification à distance.

### 6.3 Menaces de sécurité

#### 6.3.1 Menaces de sécurité côté client

L'authentification télébiométrique fait face, côté client, aux menaces de sécurité suivantes:

– le client est un faux agent ou est modifié avec un code malveillant;
– les auteurs d'attaques tentent de perturber la disponibilité et l'intégrité du client;
– les auteurs d'attaques tentent de voler ou de modifier les données biométriques capturées du client;
– les auteurs d'attaques peuvent utiliser une photo, une image générée par ordinateur ou un visage à l'écran pour l'authentification par reconnaissance faciale;

– les auteurs d'attaques peuvent utiliser une copie des données biométriques (par exemple empreinte digitale, de l'iris ou vocale) pour l'authentification télébiométrique.

### 6.3.2 Menaces de sécurité côté serveur

L'authentification télébiométrique fait face, côté serveur, aux menaces de sécurité suivantes:

– les auteurs d'attaques peuvent faire intrusion sur le serveur pour perturber la base de données du serveur ou l'application du serveur;

– les données biométriques capturées ou données de modèle capturées peuvent être remplacées illégalement ou divulguées, en tant que données modifiées ou volées;

– les données biométriques ou données de modèle capturées peuvent être modifiées illégalement lors du transfert de données;

– un programme de comparaison illégal peut être utilisé.

### 6.3.3 Menaces de sécurité dans le canal de transmission entre le client et le serveur

L'authentification télébiométrique fait face, dans le canal de transmission entre le client et le serveur, aux menaces de sécurité suivantes:

– les auteurs d'attaques peuvent écouter ou modifier les messages entre le client et le serveur;

– les données biométriques peuvent être volées ou modifiées lors de la transmission entre le client et le serveur.

## 6.4 Contremesures

Pour réduire ces menaces qui planent sur l'authentification télébiométrique, la détection d'usurpation d'identité (ASD) est souvent utilisée conjointement avec la vérification télébiométrique pour l'authentification.

La fonction ASD devrait être mise en œuvre dans un cadre d'authentification télébiométrique. Cette fonction peut être utilisée pour déterminer que l'utilisateur qui envoie la demande d'authentification télébiométrique est bien la personne active qui possède les données biométriques. Cela permet d'éviter les situations dans lesquelles un utilisateur illégal utiliserait des données biométriques falsifiées ou copiées pour l'authentification télébiométrique.

La fonction ASD peut être utilisée conjointement avec la vérification télébiométrique, afin de renforcer le niveau de sécurité et d'éviter la falsification des données biométriques. Par exemple, une application mobile peut demander à l'utilisateur de hocher la tête, de secouer la tête, de cligner des yeux, d'ouvrir la bouche, etc., pour valider que l'utilisateur est bien la personne qui a fait la demande d'authentification.

D'autres menaces de sécurité et contremesures sont mentionnées dans les Recommandations [UIT-T X.1086] et [UIT-T X.1087].

# 7 Cadre architectural

## 7.1 Diagramme architectural

Le diagramme architectural de l'authentification renforcée utilisant la télébiométrie avec des mécanismes ASD est illustré à la Figure 1.

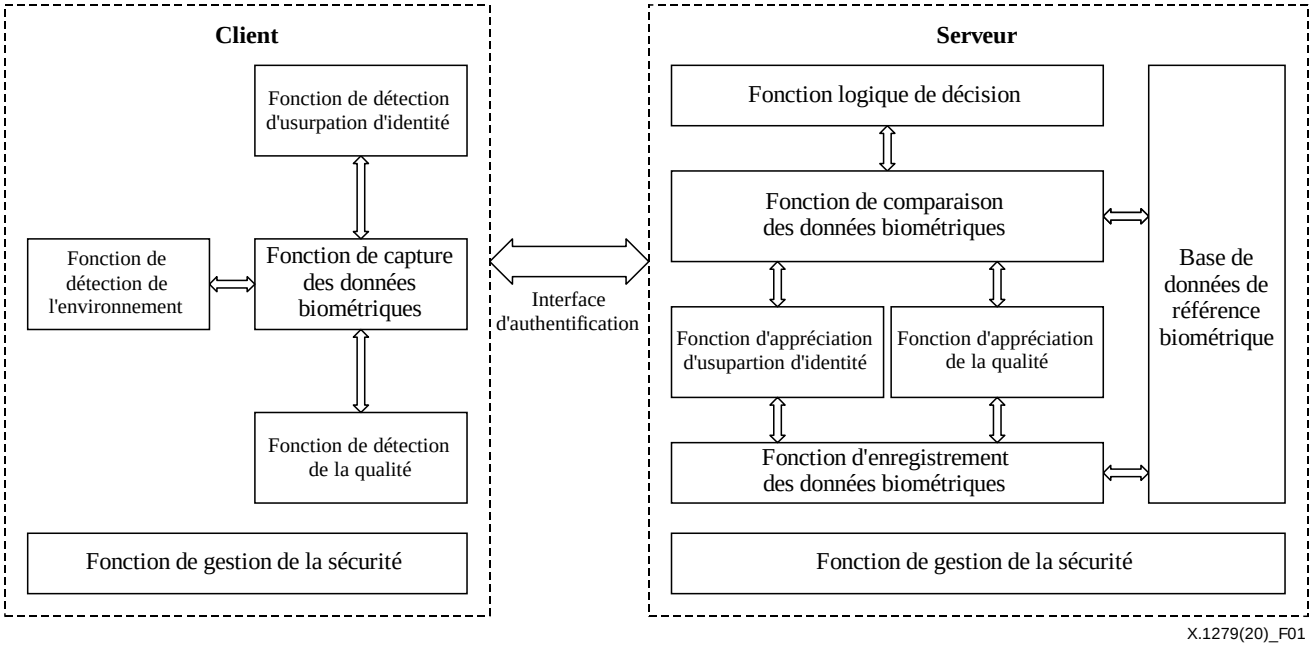


**Figure 1 – Diagramme architectural de l'authentification renforcée utilisant la télébiométrie avec des mécanismes ASD**

La description détaillée des fonctions listées dans ce diagramme architectural est donnée dans les paragraphes 7.2 et 7.3.

## 7.2 Fonctions côté client

### 7.2.1 Fonction de détection de l'environnement

Cette fonction est utilisée pour reconnaître et détecter les caractéristiques biométriques et les conditions environnementales. Par exemple, elle permet d'apprécier si les caractéristiques faciales satisfont ou non aux conditions de collecte et si l'environnement satisfait ou non aux conditions de collecte des données.

### 7.2.2 Fonction de capture des données biométriques

Cette fonction est utilisée pour capturer les données biométriques des utilisateurs finals, envoyer ces données vers une fonction de détection de la qualité en local ainsi que vers une fonction ASD à des fins de traitement et, à l'issue, envoyer les données biométriques sur le serveur au moyen d'une interface d'authentification pour l'authentification à distance.

### 7.2.3 Fonction de détection d'usurpation d'identité

Cette fonction est utilisée pour détecter les mouvements attendus en fonction des stratégies ou politiques du serveur, tels que hocher la tête, secouer la tête, cligner des yeux, ouvrir la bouche, etc.

Il existe plusieurs méthodes applicables à la détection d'usurpation d'identité, mais les techniques de détection du caractère vivant sont beaucoup plus adaptées pour l'authentification télébiométrique sur les appareils mobiles. Le protocole défi-réponse est un outil qui peut être utilisé pour déterminer si un sujet présente les propriétés propres au caractère vivant exposées dans l'acquisition du sous-système de capture des données biométriques. Par exemple, l'iris humain vivant est censé réagir aux variations de la lumière visible (défi) via une modification de la taille de la pupille (réponse attendue sur un sujet vivant).

La détection du caractère vivant peut être effectuée selon les étapes suivantes, lesquelles sont similaires à celles du processus de reconnaissance biométrique:

– capture des données brutes pour la fonction ASD depuis un sujet utilisant le sous-système de capture des données biométriques;
– extraction des éléments depuis les données ASD;
– comparaison entre les éléments ASD et les critères.

### 7.2.4 Fonction de détection de la qualité

Cette fonction est utilisée pour apprécier en amont la qualité des données biométriques selon les stratégies ou politiques du serveur. La fonction de détection de la qualité comprend l'évaluation de la qualité des données biométriques collectées et l'extraction des caractéristiques biométriques. Cette fonction est généralement utilisée conjointement à la fonction ASD et à la fonction de capture des données biométriques afin de produire les meilleures données biométriques aux fins de la modélisation et de l'appréciation des données biométriques.

### 7.2.5 Fonction de gestion de la sécurité

La fonction de gestion de la sécurité côté client inclut la gestion des justificatifs, l'environnement de confiance, etc.

## 7.3 Fonctions côté serveur

### 7.3.1 Fonction d'enregistrement des données biométriques

Cette fonction est utilisée pour traiter l'enregistrement des données biométriques. L'enregistrement des données biométriques peut être collecté auprès d'un client, importé directement par lots ou collecté à partir d'autres canaux tels qu'une base de données d'identité nationale. Ceci peut être réalisé à partir d'un modèle d'enregistrement des données biométriques.

### 7.3.2 Fonction d'appréciation d'usurpation d'identité

Cette fonction permet de repérer les éventuelles falsifications ou copies de données biométriques. Le serveur procédera à une appréciation détaillée anti-usurpation d'identité, sur la base des premiers résultats de détection obtenus côté client ainsi que sur la base des stratégies et politiques du serveur.

Le serveur peut indiquer au client de détecter les mouvements attendus selon les stratégies ou politiques du serveur, tels que hocher la tête, secouer la tête, cligner des yeux, ouvrir la bouche, etc. Le serveur reçoit les données des caractéristiques biométriques extraites du client et utilise sa référence biométrique de même que la stratégie prédéfinie pour déterminer si un sujet présente les propriétés propres au caractère vivant.

### 7.3.3 Fonction d'appréciation de la qualité

Cette fonction vise à apprécier la qualité des données biométriques sur la base des premiers résultats de détection obtenus côté client ainsi que sur la base des stratégies et politiques du serveur. La fonction d'appréciation de la qualité évalue la qualité à l'aune des données biométriques reçues. Si la qualité n'atteint pas le seuil requis, le serveur rejettera les données biométriques reçues et demandera au client de capturer à nouveau les données biométriques. Si la qualité correspond au seuil requis, les données biométriques seront envoyées à la fonction de comparaison des données biométriques.

La capacité de capture des données biométriques peut varier selon les différents types d'appareils et la qualité des données biométriques peut être améliorée si l'on utilise différents types d'appareils. Le serveur peut par conséquent demander à l'utilisateur d'utiliser plusieurs appareils pour capturer les données biométriques afin d'améliorer la qualité. Si la référence biométrique est capturée à partir de différents types d'appareils, le serveur devra stocker et utiliser les différentes références biométriques pour différents types d'appareils.

### 7.3.4 Fonction de comparaison des données biométriques

Cette fonction prend en charge la comparaison et la vérification entre les éléments biométriques extraits d'un client et les références biométriques stockées du côté du serveur. Les références biométriques stockées dans une base de données de référence biométrique sont générées à partir du processus d'enregistrement des données biométriques.

### 7.3.5 Fonction logique de décision

Cette fonction contient des logiques de décision pour exécuter différentes procédures d'authentification et renvoie les instructions associées au client pour la mise en œuvre de ces différentes procédures. La décision est prise sur la base des données de gestion des risques, incluant les informations logicielles et matérielles de l'appareil mobile et le profil de l'utilisateur. Par exemple, si l'analyse des données fait état d'un risque élevé pour l'utilisateur final, une fonction de logique de décision demande au client de mettre en œuvre un mécanisme ASD en plus de la capture et de la comparaison des données biométriques.

### 7.3.6 Base de données de référence biométrique

La base de données de référence biométrique est utilisée pour stocker les données biométriques, les données de gestion des risques, le nom d'utilisateur, l'identité, etc.

### 7.3.7 Fonction de gestion de la sécurité

Cette fonction est utilisée pour garantir l'exécution sécurisée des fonctionnalités du serveur et le stockage sécurisé de la base de données de référence biométrique, pour éviter la falsification ou le vol des données biométriques ou du modèle biométrique.

## 8 Flux de processus d'authentification

### 8.1 Types de message

Dans la pile de protocoles d'authentification télébiométrique sur les appareils mobiles, il existe au moins trois types de messages à différents stades:

– enregistrement: un serveur enregistre les informations d'enregistrement et le type d'authentification d'un utilisateur selon une négociation entre l'utilisateur et le serveur;

– authentification: un serveur compare les données biométriques reçues à une référence biométrique enregistrée;

– désenregistrement: un utilisateur se désenregistre d'un serveur. Le serveur supprime les données d'enregistrement de l'utilisateur.

NOTE – La présente Recommandation porte sur la vérification à distance. Le client enregistre une référence biométrique sur le serveur. Après avoir reçu la demande de vérification, le serveur compare les données biométriques reçues avec la référence biométrique enregistrée.

## 8.2 Flux de processus

### 8.2.1 Flux de processus d'enregistrement

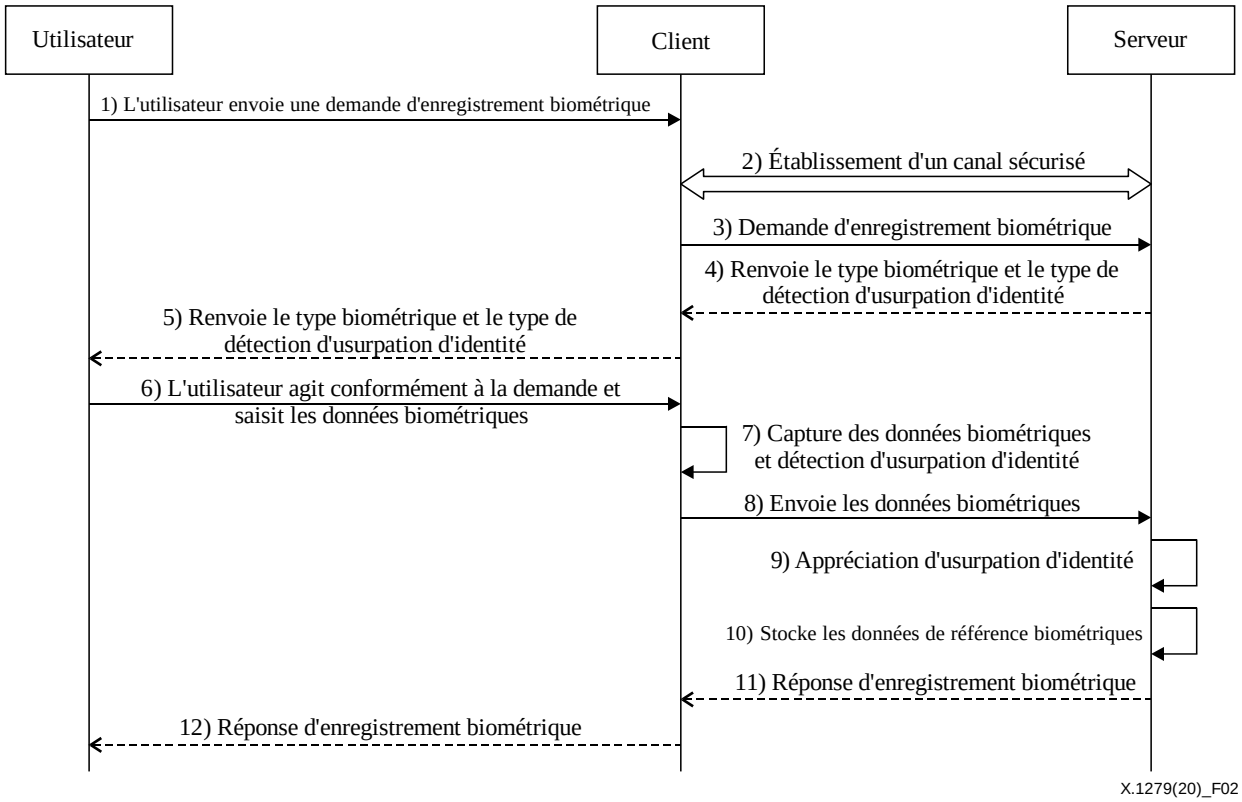


**Figure 2 – Flux de processus d'enregistrement**

La Figure 2 illustre les flux de processus d'enregistrement. Les flux détaillés sont décrits ci-dessous:

Condition préalable: l'utilisateur s'authentifie avec succès auprès du serveur via d'autres mécanismes d'authentification, tels qu'identifiant/mot de passe du compte utilisateur et code de vérification du service de messages brefs (SMS).

1) L'utilisateur utilise un identifiant/mot de passe de compte pour se connecter et envoie une demande d'enregistrement biométrique au client.
2) Le client établit un canal sécurisé avec le serveur pour protéger la session et la transmission des données, par exemple en utilisant le protocole de mot de passe distant sécurité (SRP).
3) Le client envoie au serveur la demande d'enregistrement biométrique avec l'identifiant du compte utilisateur et les données de gestion des risques.
4) La fonction logique de décision sur le serveur renvoie au client le bon type biométrique et le bon type de détection d'usurpation d'identité, sur la base de l'analyse des données de gestion des risques et de la logique commerciale.
5) Le client demande à l'utilisateur d'exécuter les actions spécifiées pour capturer les données biométriques.
6) L'utilisateur agit conformément à la demande et saisit les données biométriques du client.
7) La fonction de capture des données biométriques chez le client capture les données biométriques et la fonction ASD détecte les mouvements attendus de l'utilisateur.
8) Le client extrait les éléments biométriques et envoie ces éléments au serveur comme référence biométrique dans le canal sécurisé établi.

9) Le serveur lie les données biométriques à l'identifiant du compte utilisateur et exécute la fonction ASD.

10) Le serveur stocke la référence biométrique reçue dans la base de données de référence biométrique.

11) Le serveur renvoie la réponse d'enregistrement biométrique au client.

12) Le client informe l'utilisateur de la réponse d'enregistrement biométrique.

### 8.2.2 Flux de processus d'authentification

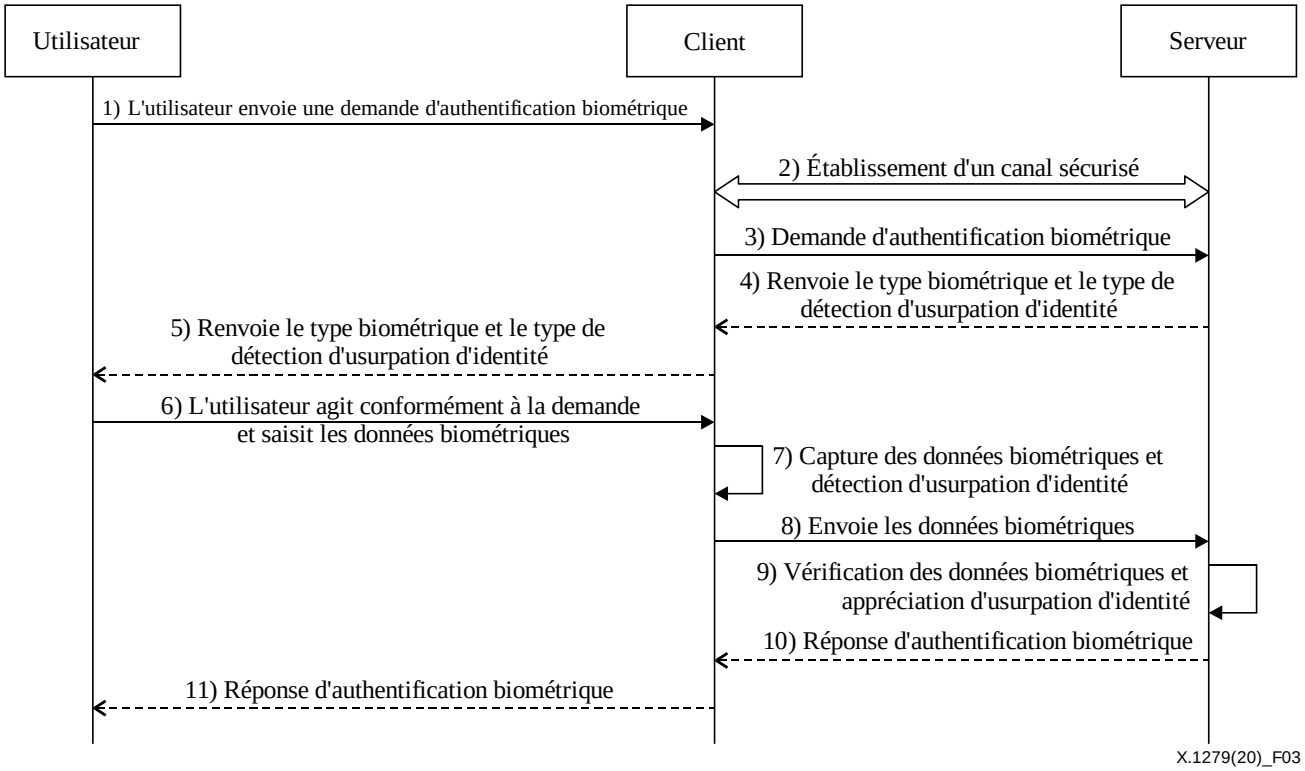


**Figure 3 – Flux de processus d'authentification**

La Figure 3 illustre les flux de processus d'authentification. Les flux détaillés sont décrits ci-dessous:

1) L'utilisateur envoie une demande d'authentification biométrique au client, avec l'identifiant de compte utilisateur.

2) Le client établit un canal sécurisé avec le serveur pour protéger la session et la transmission des données, par exemple en utilisant le protocole de mot de passe distant sécurité (SRP).

3) Le client envoie au serveur la demande d'authentification biométrique avec l'identifiant du compte utilisateur et les données de gestion des risques.

4) La fonction logique de décision sur le serveur renvoie au client le bon type biométrique et le bon type de détection d'usurpation d'identité, sur la base de l'analyse des données de gestion des risques et de la logique commerciale.

5) Le client demande à l'utilisateur d'exécuter les actions spécifiées pour capturer les données biométriques.

6) L'utilisateur agit conformément à la demande et saisit les données biométriques du client.

7) La fonction de capture des données biométriques chez le client capture les données biométriques et la fonction ASD détecte les mouvements attendus de l'utilisateur.

8) Le client envoie au serveur les données de l'élément biométrique extrait dans le canal sécurisé établi.

9) Le serveur procède à une vérification des données biométriques entre l'élément biométrique extrait et la référence biométrique et exécute la fonction ASD.

10) Le serveur renvoie la réponse d'authentification biométrique au client.

11) Le client informe l'utilisateur de la réponse d'authentification biométrique.

### 8.2.3 Flux de processus de désenregistrement

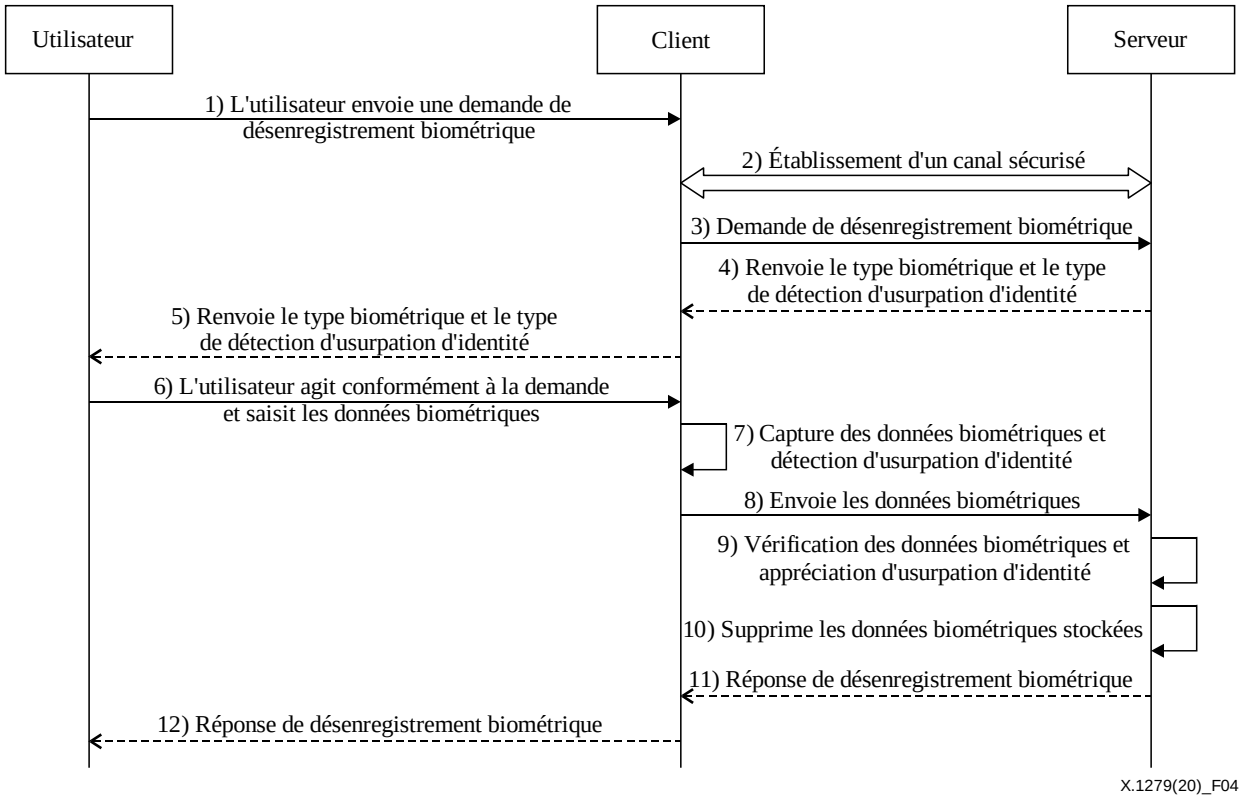


**Figure 4 – Flux de processus de désenregistrement**

La Figure 4 illustre les flux de processus de désenregistrement. Les flux détaillés sont décrits ci-dessous:

Condition préalable: l'utilisateur s'authentifie avec succès auprès du serveur via d'autres mécanismes d'authentification, tels qu'identifiant/mot de passe du compte utilisateur et code de vérification SMS.

1) L'utilisateur utilise un identifiant/mot de passe de compte pour se connecter et envoie une demande de désenregistrement biométrique au client.

2) Le client établit un canal sécurisé avec le serveur pour protéger la session et la transmission des données, par exemple en utilisant le protocole SRP.

3) Le client envoie au serveur la demande d'enregistrement biométrique avec l'identifiant du compte utilisateur et les données de gestion des risques.

4) La fonction logique de décision sur le serveur renvoie au client le bon type biométrique et le bon type de détection d'usurpation d'identité, sur la base de l'analyse des données de gestion des risques et de la logique commerciale.

5) Le client demande à l'utilisateur d'exécuter les actions spécifiées pour capturer les données biométriques.

6) L'utilisateur agit conformément à la demande et saisit les données biométriques du client.

7) La fonction de capture des données biométriques chez le client capture les données biométriques et la fonction ASD détecte les mouvements attendus de l'utilisateur.

8) Le client extrait les éléments biométriques et envoie ces éléments au serveur comme référence biométrique dans le canal sécurisé établi.

9) Le serveur lie les données biométriques à l'identifiant du compte utilisateur et exécute la fonction ASD.

10) Le serveur stocke la référence biométrique reçue dans la base de données de référence biométrique.

11) Le serveur renvoie la réponse d'enregistrement biométrique au client.

12) Le client informe l'utilisateur de la réponse d'enregistrement biométrique.

# 9 Lignes directrices concernant la sécurité

## 9.1 Sécurité du client

Le système d'exploitation de l'appareil mobile devrait être mis à jour avec la dernière version sécurisée disponible.

Le client devrait revêtir une signature qui permettra l'identification de la source du client.

Le client devrait être protégé contre toute modification ou mise à jour non autorisée.

La protection du code et des données devrait être renforcée contre l'ingénierie inverse chez le client, par exemple obfuscation.

L'acquisition des données chez le client devrait être réalisée dans un environnement de confiance, pour assurer la confidentialité et l'intégrité des données collectées.

## 9.2 Sécurité du serveur

Une politique de contrôle d'accès stricte devrait être mise en œuvre sur le serveur; toute opération sur le serveur devrait d'abord être authentifiée et autorisée.

Le serveur devrait avoir la capacité de détecter l'identité du client.

La communication entre le serveur et le client devrait être protégée contre les attaques par répétition, par exemple en utilisant des données dynamiques dans les messages comme "nonce", "challenge" ou "timestamp".

Des journaux devraient être tenus concernant les opérations sur le serveur et l'intégrité des journaux devrait être protégée.

## 9.3 Sécurité du stockage

Les certificats et clés privées UIT-T X.509 devraient être stockés de façon sécurisée et une politique de contrôle d'accès stricte devrait être définie.

Les clés privées devraient être stockées dans un texte chiffré et l'algorithme de chiffrement devrait être protégé par un niveau de sécurité élevé pour éviter le craquage.

Les données biométriques stockées dans le serveur devraient être chiffrées et l'algorithme de chiffrement devrait être protégé par un niveau de sécurité élevé pour éviter le craquage.

Les données biométriques stockées sur le serveur devraient être un élément biométrique extrait et ne pourront pas être restaurées dans les données d'origine.

Toutes les informations relatives à la sécurité du stockage devraient respecter les prescriptions définies dans [ISO/CEI 24745].

## 9.4 Sécurité des communications

Avant toute communication entre le client et le serveur, un canal sécurisé devrait être établi; par exemple, https est approprié pour la sécurité des communications.

Le mécanisme d'échange sécurisé de clés dans l'authentification entre le client et le serveur devrait être fourni; par exemple, le protocole SRP peut être utilisé comme mécanisme d'échange sécurisé de clés.

La clé utilisée pour négocier le canal sécurisé devrait être protégée de toute interception; par exemple, le protocole SRP peut être utilisé pour négocier le canal sécurisé sans transport de clé.

Les informations telles que les données biométriques traitées et le résultat de la composante de décision devraient être codées pour la transmission, et leur intégrité devrait être vérifiée au moyen d'une fonction unidirectionnelle, telle qu'une fonction de hachage ou PKI (infrastructure de clé publique), qui empêcherait toute altération des données pendant la transmission.

Les données biométriques traitées devraient être désensibilisées et chiffrées pour la transmission, et la clé de chiffrement ne devrait pas être la même selon le client. Le serveur déchiffre au moyen de la clé de chiffrement appropriée.

Toutes les informations relatives à la sécurité des communications devraient respecter les prescriptions définies dans [ISO/CEI 24745].

## 9.5 Autres considérations de sécurité

Outre la sécurité du stockage et la sécurité des communications, il existe de nombreux autres aspects de la sécurité qui devraient être pris en compte, tels que la sécurité du traitement, la protection des informations d'identification personnelle (PII), etc. Toutes les informations relatives aux techniques de sécurité et de protection des données devraient respecter les prescriptions définies dans [ISO/CEI 24745].

# Appendice I

## Cas d'utilisation et scénarios

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

### I.1 Étude de cas concernant les services de paiement mobile

Pour ses paiements mobiles, Alice utilise une application de portefeuille mobile. Son utilisation est la suivante:

1) La toute première fois, Alice entre son nom d'utilisateur et son mot de passe pour se connecter à l'application. Comme elle ne souhaite pas avoir à saisir son mot de passe à chaque fois qu'elle effectue un paiement et qu'elle a peur d'oublier son mot de passe, elle clique sur le bouton "Enregistrement pour paiement par reconnaissance faciale" dans l'application du portefeuille mobile.
2) L'application demande à Alice d'activer la caméra et de hocher la tête.
3) Alice reçoit ensuite une notification de l'application: "Vous êtes maintenant enregistré/e".
4) Alice achète un café dans la boutique Starbucks et utilise l'application de portefeuille mobile pour payer. Elle ouvre l'application et s'apprête à payer. L'application lui demande d'activer la caméra et de hocher la tête. L'expérience est concluante.
5) Alice reçoit à l'issue la notification suivante: "Vous avez payé avec succès. Merci!"
6) Après un certain temps, Alice ne souhaite plus utiliser cette fonction pour régler ses achats et clique sur le bouton correspondant pour désactiver l'option.

### I.2 Étude de cas concernant les services de commerce électronique

Bob possède une boutique de vêtements et envisage d'ouvrir une boutique en ligne sur une plate-forme de commerce électronique. La procédure est la suivante:

1) Pour commencer, Bob s'enregistre sur la plate-forme de commerce électronique et demande à ouvrir une nouvelle boutique. Bob saisit son nom d'utilisateur et son mot de passe sur la plate-forme de commerce électronique depuis une application de commerce électronique sur son appareil mobile.
2) L'application mobile demande à Bob d'activer la caméra et d'effectuer plusieurs actions selon une séquence définie, par exemple ouvrir la bouche, secouer la tête, cligner des yeux et hocher la tête devant la caméra.
3) Bob reçoit ensuite une notification de l'application: "Vous êtes maintenant enregistré/e".
4) Bob souhaite ultérieurement publier des vêtements depuis sa boutique. La plate-forme de commerce électronique lui demande d'activer la caméra et d'effectuer plusieurs actions selon une séquence définie, par exemple secouer la tête, cligner des yeux, ouvrir la bouche et hocher la tête devant la caméra.
5) Bob reçoit à l'issue la notification suivante: "Vous vous êtes connecté/e avec succès".
6) Après un certain temps, Bob ne souhaite plus utiliser cette fonction pour s'authentifier et clique sur le bouton correspondant pour désactiver l'option.

# Appendice II

## Mot de passe distant sécurisé (SRP)

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

SRP est un protocole d'authentification d'identité fondé sur un mot de passe avec échange de clés. L'avantage de ce protocole est que le texte en clair de la clé n'est pas soumis à transfert dans le processus d'authentification, les utilisateurs n'ont qu'à conserver le mot de passe. De plus, le serveur ne stocke pas les mots de passe des utilisateurs, mais stocke les informations pertinentes, même si le serveur fait l'objet d'une attaque; un client légitime ne peut pas être falsifié (impossibilité d'obtenir le mot de passe).

De plus amples détails concernant le protocole SRP sont donnés dans le Document [b-RFC 2945].

Le protocole SRP peut être utilisé pour établir des canaux sécurisés entre le client et le serveur lors des processus relatifs à l'enregistrement biométrique, à l'authentification biométrique et au désenregistrement biométrique. Il peut être utilisé pour négocier des connexions sécurisées à l'aide d'un mot de passe fourni par l'utilisateur, tout en éliminant les problèmes de sécurité traditionnellement associés aux mots de passe réutilisables. Le protocole SRP peut également être utilisé pour effectuer un échange de clés sécurisé lors du processus d'authentification, permettant aux couches de sécurité (protection de la vie privée et/ou de l'intégrité) d'être activées pendant la session.

# Appendice III

## Exemples d'utilisation de la fonction ASD dans la reconnaissance faciale

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Liste (non exhaustive) d'exemples d'utilisation de la fonction ASD dans la reconnaissance faciale:

1) Suivant certains conseils ou instructions du serveur, l'utilisateur peut effectuer une action spécifique et le serveur détecte l'action à partir de l'image du visage.
2) Le serveur devrait avoir la capacité de détecter l'angle du visage et de la caméra, et de détecter le corps vivant en modifiant l'angle du visage au cours du processus.
3) Le serveur devrait avoir la capacité de détecter la continuité de l'action du visage, d'empêcher le jeu de glissement et d'empêcher les gens de changer pendant le processus.
4) Le serveur devrait avoir la capacité de détecter la rediffusion de la vidéo d'action du visage.
5) Le serveur devrait avoir la capacité d'empêcher le piratage d'images faciales.
6) Le serveur devrait avoir la capacité de détecter l'utilisation de modèles de visage 3D produits par la technologie graphique informatique.

# Bibliographie


[b-UIT-T M.3016.0] Recommandation UIT-T M.3016.0 (2005), *Sécurité pour le plan de gestion: aperçu général.*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[b-UIT-T X.1081] Recommandation UIT-T X.1081 (2011), *Le modèle télébiométrique multimodal – Cadre général pour la spécification des aspects de sécurité et d'innocuité de la télébiométrie.*

[b-UIT-T X.1085] Recommandation UIT-T X.1085 (2016) | ISO/CEI 17922:2017, *Technologies de l'information – Techniques de sécurité – Cadre d'authentification télébiométrique utilisant un module matériel de sécurité biométrique*.

[b-UIT-T X.1089] Recommandation UIT-T X.1089 (2008), *Infrastructure d'authentification télébiométrique.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification d'entité.*

[b-ISO 18461] ISO 18461:2016, *Statistiques internationales des musées*.

[b- ISO/CEI 19784-1] ISO/CEI 19784-1:2018, *Information technology – Biometric application programming interface – Part 1: BioAPI specification.*

[b-ISO/CEI 19792] ISO/CEI 19792:2009, *Security evaluation of biometrics*.

[b-ISO/CEI 19989] ISO/CEI 19989, *Evaluation of presentation attack detection for biometrics.*

[b-ISO/CEI 2382] ISO/CEI 2382:2015, *Information technology – Vocabulary.*

[b-ISO/CEI 2382-37] ISO/CEI 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics.*

[b-ISO/CEI 24761] ISO/CEI 24761:2009, *Information technology – Security techniques – Authentication context for biometrics*.

[b-ISO/CEI 30107] ISO/CEI 30107:2017, *Information technology – Biometric presentation attack detection.*

[b-ISO/CEI 30125] ISO/IEC 30125:2016, *Biometrics – Biometrics used with mobile devices*.

[b-RFC 2945] RFC 2945, *The SRP Authentication and Key Exchange System.*

[b-Disappearing Cryptography] Disappearing Cryptography (troisième édition), 2009, Pages 355-364

## SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphoniques |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| Série N | Maintenance: circuits internationaux de transmission radiophonique et télévisuelle |
| Série O | Spécifications des appareils de mesure |
| Série P | Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux |
| Série Q | Commutation et signalisation et mesures et tests associés |
| Série R | Transmission télégraphique |
| Série S | Équipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Imprimé en Suisse
Genève, 2021