国 际 电 信 联 盟

ITU-T X.1279

(09/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

云计算安全 – 身份管理

使用具有反欺骗检测机制的远程生物特征识别的增强认证框架

ITU-T X.1279 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1279 建议书

使用具有反欺骗检测机制的远程生物特征识别的增强认证框架

摘要

ITU-T X.1279建议书提供使用具有反欺骗检测机制的远程生物特征识别的增强认证架构框架。本建议书对传统远程生物特征识别认证解决方案面临的威胁做了分析，并针对使用具有反欺骗检测机制的远程生物特征识别的增强认证，规定了架构框架、认证流程和安全考虑。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1279	2020-09-03	17	11.1002/1000/14261

关键词

反欺诈检测、增强认证、远程生物识别。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL：http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

远程生物特征识别认证技术经常用于诸如电子银行和采购业务等需要高可靠性的各种领域。必须努力开发一种能够提前消除潜在安全风险的安全系统，以确保远程生物特征识别数据的安全。

本建议书对传统远程生物特征识别认证解决方案面临的威胁做了分析，并提出了一个有关使用具有反欺骗检测（ASD）机制的远程生物特征识别的增强认证框架。反欺骗检测旨在确定发送远程生物特征识别认证请求的用户是拥有生物特征识别数据的积极分子。反欺骗检测可与远程生物特征识别验证一起使用，以增强安全性并避免伪造的生物特征识别情形。可以设计反欺骗检测功能来增强安全性并避免生物特征识别数据的泄漏。

ITU-T X.1279 建议书

使用具有反欺骗检测机制的远程生物特征识别的增强认证框架

1 范围

本建议书提供一个使用具有反欺骗检测功能的远程生物特征识别的增强认证架构框架。本建议书对传统远程生物特征识别认证解决方案面临的威胁做了分析，并针对使用具有反欺骗检测机制的远程生物特征识别的增强认证，规定了架构框架、认证流程和安全考虑。

在本建议书中规定的架构框架可以用作一个指南，用于帮助部署使用反欺骗检测功能的增强远程生物特征识别认证解决方案。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1086] ITU-T X.1086建议书（2008年），远程生物特征识别保护程序 – 第1部分：生物特征识别数据安全的技术和管理对策的导则。

[ITU-T X.1087] ITU-T X.1087建议书（2016年），使用移动设备的远程生物特征识别应用的技术和操作对策。

[ISO/IEC 24745] ISO/IEC 24745:2011，信息技术 – 安全技术 – 生物特征识别信息保护。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 认证 authentication [b-ISO/IEC 2382-37]：证明或表明无可争议性的行为。

3.1.2 生物特征识别的 biometric（形容词）[b-ISO/IEC 2382]：与生物特征识别技术领域有关。

3.1.3 生物特征识别获取 biometric capture [b-ISO/IEC 2382-37]：以可检索的形式直接从个体或生物特征识别特性陈述中获得并记录生物特征识别特性信号。

3.1.4 生物特征识别特性 biometric characteristic [b-ISO/IEC 2382-37]：个体的生物和行为特性，从中可提取独特的、可重复的生物特征识别特征用于生物特征识别。

3.1.5 生物特征识别数据 biometric data [b-ISO/IEC 2382-37]：在任何处理阶段的生物特征识别样本或生物特征识别样本集，例如，生物特征识别参考、生物特征识别探针、生物特征识别特征或生物特征识别属性。

3.1.6 生物特征识别特征 biometric feature [b-ISO/IEC 2382-37]：从生物特征识别样本中提取并用于比较的数字或标签。

3.1.7 生物特征识别 biometric recognition/biometrics [b-ISO/IEC 2382-37]：基于其生物和行为特性自动识别各个个体。

3.1.8 生物特征识别参考数据库 biometric reference database [b-ISO/IEC 2382-37]：生物特征识别参考数据记录的数据库。

3.1.9 生物特征识别模板 biometric template [b-ISO/IEC 19784-1]：可直接与用于识别生物特征识别样本之生物特征识别特征进行比较的、存储的生物特征识别特征集。

3.1.10 生物特征识别验证 biometric verification [b-ISO/IEC 2382-37]：通过生物特征识别比较来确认生物特征识别声称的过程。

3.1.11 比较（匹配/匹配的） comparison (match/matching) [b-ISO/IEC 19784-1]：估计、计算或测量识别生物特征识别样本/生物特征识别特征/生物特征识别模型与生物特征识别参考之间的相似性或不相似性。

3.1.12 比较决策 comparison decision [b-ISO/IEC 19784-1]：基于比较得分、决策策略（包括一个阈值，可能还包括其他的输入），确定识别生物特征识别样本和生物特征识别参考是否具有相同的生物特征识别来源。

3.1.13 移动设备 mobile device [b-ISO 18461]：便携式计算设备，通常带有触摸屏、输入笔和/或键盘以及互联网连接。

3.1.14 用户 user [b-ISO/IEC 2382-37]：以任何方式与生物特征识别系统进行交互的任何个人或组织。

3.1.15 远程生物特征识别 telebiometrics [b-ITU-T X.1081]：生物特征识别技术在电信中的应用。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 反欺骗检测 anti-spoofing detection：检测和防止通过非法行为欺骗某生物特征识别系统的过程。

3.2.2 混淆处理 obfuscation：故意创建人类难以理解的源代码或机器代码的行为。该技术依赖于一组变换，这些变换可改变软件的外观表现而不会改变结果。混淆程序应产生与非混淆程序完全相同的结果。

注 – 混淆处理是一种技术，通常用于隐藏某些软件的含义，这通过重新安排操作来实现，但它也可以用于在代码中添加弱水印。在这两种情况下，算法均依赖于一组变换，这些变换可改变软件的外观表现而不会改变结果。混淆程序应产生与非混淆程序完全相同的结果。[b-消失密码术]

3.2.3 质量检测 quality detection：测量生物特征识别样本的适合性，以完成或做出生物特征识别比较决策。

3.2.4 欺骗 spoofing：通过展示一幅记录的图像或其他生物特征识别数据样本或者人工衍生的生物特征识别特性，一个实体伪装为一个不同的实体，以便冒充某个个体。

注 – 本定义改编自[b-ITU M.3016.0]。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

ASD 反欺骗检测

PII 个人可识别信息

PKI 公钥基础设施

SMS 短消息业务

SRP 安全远程口令

5 惯例

无。

6 远程生物特征识别认证面临的安全威胁和对策

6.1 背景

随着互联网业务的兴起，基于传统密码的认证机制已不能满足用户体验和安全性能方面的要求。为了方便和安全起见，现在更常用的是远程生物特征识别认证机制。

不过，生物特征识别认证机制存在挑战和风险，例如，攻击者可能使用照片或计算机生成的图片或屏幕上的面部进行面部识别认证，或者用户可能使用远程生物特征识别样本的副本（例如，指纹、虹膜或声纹）来进行远程生物特征识别认证。

6.2 参考认证模式

对于移动设备上的远程生物特征识别认证，有两种基本的参考认证模式：

1) 本地认证模式：生物特征识别数据存储在移动设备上，远程生物特征识别验证在移动设备侧进行。远程生物特征识别验证结果被发送给服务器侧。

2) 远程认证模式：生物特征识别数据存储在服务器上，远程生物特征识别验证在服务器侧进行。

本建议书侧重于远程认证模式。

6.3 安全威胁

6.3.1 客户端侧的安全威胁

远程生物特征识别认证在客户端侧会遇到以下安全威胁：

– 客户端是一个伪造的代理或者被恶意代码做了修改。

– 攻击者试图破坏客户端的可用性和完整性。

– 攻击者试图窃取或修改获取的客户端生物特征识别数据。

– 攻击者可能使用照片或计算机生成的图片或屏幕上的面部来进行面部识别认证。

– 攻击者可能使用生物特征识别数据的一个副本（例如，指纹、虹膜或声纹）来进行远程生物特征识别认证。

6.3.2 服务器侧的安全威胁

远程生物特征识别认证在服务器侧会遇到以下安全威胁：

– 攻击者可能入侵服务器以破坏服务器数据库或服务器应用程序。

– 获取的生物特征识别数据或模板数据可能会被非法替换或泄露，作为更改或被盗的数据。

– 当传输获取的数据时，获取的生物特征识别数据或模板数据可能会被非法更改。

– 可能使用非法的比较程序。

6.3.3 客户端与服务器之间传输信道面临的安全威胁

远程生物特征识别认证对客户端与服务器之间的传输信道有以下安全威胁：

– 攻击可能会窃听或修改客户端与服务器之间的消息。

– 在从客户端到服务器的传输过程中，生物特征识别数据可能被盗或更改。

6.4 对策

为了缓解对远程生物特征识别认证的这些威胁，通常将反欺骗检测（ASD）与远程生物特征识别验证一起用于认证。

ASD应在远程生物特征识别认证框架中予以实施。ASD功能可用于确定发送远程生物特征识别认证请求的用户是拥有生物特征识别数据的积极分子。这可以避免非法用户可能使用伪造或复制的生物特征识别数据进行远程生物特征识别认证的情形。

ASD可以与远程生物特征识别验证一起使用，以增强安全性并避免伪造的生物特征识别的情形。例如，一个移动应用程序可能要求用户点头、摇头、眨眼、张嘴等，以验证用户是否是发出认证请求的实际人员。

[ITU-T X.1086]和[ITU-T X.1087]中提供了额外的安全威胁和对策。

7 架构框架

7.1 架构图

图1所示为使用具有 ASD 机制的远程生物特征识别的增强认证架构图。

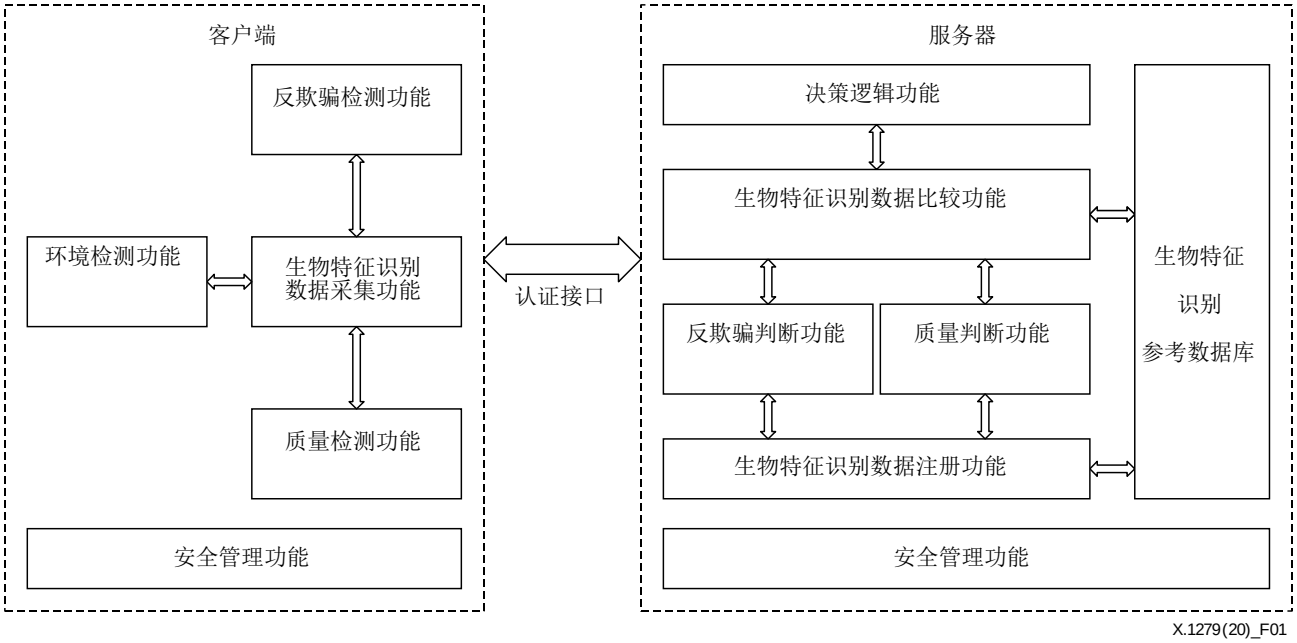

图1 – 使用具有ASD机制的远程生物特征识别的增强认证架构图

对本架构图中各功能的详细描述见第7.2节和第7.3节。

7.2 客户端侧的功能

7.2.1 环境检测功能

本功能负责识别和检测生物特征识别特性和环境条件。例如，它判断面部特性是否满足采集条件、环境是否满足数据采集条件。

7.2.2 生物特征识别数据获取功能

本功能用于获取最终用户的生物特征识别数据，然后将生物特征识别数据发送给本地质量检测功能和ASD功能进行处理，然后再通过认证接口将生物特征识别数据发送给服务器以进行远程认证。

7.2.3 ASD检测功能

根据服务器的策略或政策，本功能用于检测预期的移动，例如，点头、摇头、眨眼、张嘴等。

尽管可以将许多方法用于ASD，但活性检测更适于移动设备上的远程生物特征识别认证。质询响应可以用作一种工具，来确定主体所呈现的行为是否具有生物特征识别数据获取子系统的采集中所显示的活性。例如，预期活人的虹膜会随着瞳孔大小的变化而对可见光照明（质询）的变化做出响应（如果是活着的，则会有预期的响应）。

可以按照类似于生物特征识别过程的以下步骤来执行活性检测：

– 使用生物特征识别数据获取子系统获取某个主体的ASD原始数据；

– 从ASD数据中提取特征；以及

– 将ASD特征与标准进行比较。

7.2.4 质量检测功能

根据服务器的策略或政策，本功能用于预先判断生物特征识别数据的质量。质量检测功能对采集的生物特征识别数据进行质量评估，并提取生物特征识别特性。通常，本功能与ASD功能和生物特征识别数据获取功能一起使用，输出最佳的生物特征识别数据，以便进行生物特征识别数据建模和判断。

7.2.5 安全管理功能

客户端侧的安全管理功能负责证书管理、可信环境等。

7.3 服务器侧的功能

7.3.1 生物特征识别数据注册功能

本功能负责处理生物特征识别数据注册。生物特征识别数据注册可以从客户端采集、直接批处理导入，或者从其他渠道（例如，国家身份数据库）采集。这可以通过生物特征识别数据注册模板来实现。

7.3.2 反欺骗判断功能

本功能用于判断生物特征识别数据是伪造的还是复制的。服务器将根据客户端侧的初步检测结果以及服务器的策略和政策，进行深度的反欺骗判断。

根据服务器的策略或政策，服务器可以指示客户端检测预期的移动（例如，点头、摇头、眨眼、张嘴等）。服务器从客户端接收提取的生物特征识别数据特性，并使用其生物特征识别参考和预先定义的策略来判断主体所呈现的行为是否具有活性。

7.3.3 质量判断功能

根据客户端侧的初步检测结果以及服务器的策略和政策，本功能用于判断生物特征识别数据的质量。质量判断功能对接收到的生物特征识别数据进行质量评估。如果质量未达到要求的阈值，则服务器将拒绝接收到的生物特征识别数据，并要求客户端再次获取生物特征识别数据。如果质量符合要求的阈值，则将生物特征识别数据发送给生物特征识别数据比较功能进行比较。

对于不同的设备类型，生物特征识别数据获取功能可能有所不同。可以基于不同的设备类型来提高生物特征识别数据的质量。服务器可能会要求用户使用多个设备来获取生物特征识别数据以提高质量。如果从不同的设备类型获取生物特征识别参考，则服务器应为不同的设备类型存储和使用不同的生物特征识别参考。

7.3.4 生物特征识别数据比较功能

本功能支持对从客户端提取的生物特征识别特征与存储在服务器侧的生物特征识别参考进行比较和验证。从生物特征识别数据注册过程生成存储于生物特征识别参考数据库的生物特征识别参考。

7.3.5 决策逻辑功能

本功能包含决策逻辑，以运行不同的认证过程，并将相关指令反馈给客户端，以执行不同的认证过程。基于风险管理数据做出决策，包括移动设备的软件和硬件信息以及用户的个人资料。例如，根据数据分析，如果最终用户是高风险用户，则除了进行基本的生物特征识别获取和比较之外，决策逻辑功能还要求客户端执行ASD。

7.3.6 生物特征识别参考数据库

生物特征识别参考数据库用于存储生物特征识别数据、风险管理数据、用户名、身份等。

7.3.7 安全管理功能

本功能用于确保服务器功能的安全执行和生物特征识别参考数据库的安全存储，以避免篡改或盗窃生物特征识别数据或模板。

8 认证流程

8.1 消息类型

在移动设备上的远程生物特征识别认证协议栈中，在不同的阶段中至少有三种类型的消息：

– 注册：根据用户与服务器之间的协商结果，服务器记录用户的注册信息和认证类型；

– 认证：服务器将接收到的生物特征识别数据与注册的生物特征识别参考进行比较；

– 注销：用户从服务器注销。服务器删除用户的注册数据。

注 – 本建议书侧重于远程验证。客户端将生物特征识别参考注册到服务器。在接收到验证请求之后，服务器将接收到的生物特征识别数据与注册的生物特征识别参考进行比较。

8.2 流程

8.2.1 注册流程

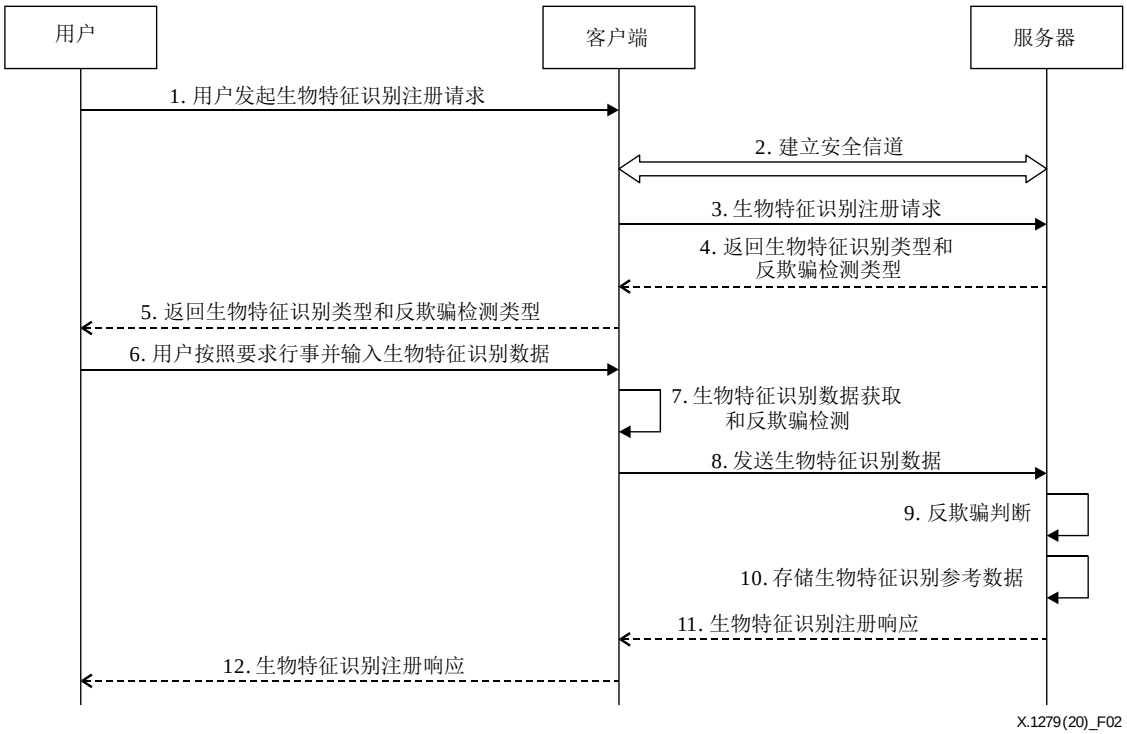

图2 – 注册流程

图2显示了注册流程。详细流程如下所述：

前提条件：用户通过其他认证机制成功与服务器实现认证，例如，用户帐户标识符/密码以及短消息服务（SMS）验证码。

1. 用户使用帐户标识符/密码登录，并向客户端发起生物特征识别注册请求；
2. 客户端与服务器建立安全信道以保护会话和数据传输，例如，通过使用安全远程密码（SRP）协议；
3. 客户端将生物特征识别注册请求以及用户帐户标识符和风险管理数据发送给服务器；
4. 基于对风险管理数据和业务逻辑的分析，服务器中的决策逻辑功能将正确的生物特征识别类型和ASD类型返回给客户端；
5. 客户端要求用户执行指定的操作以获取生物特征识别数据；
6. 用户按照要求行事，并从客户端输入生物特征识别数据；
7. 客户端中的生物特征识别数据获取功能获取生物特征识别数据，ASD功能检测用户的预期移动；
8. 客户端提取生物特征识别特征，并将特征作为已建立的安全信道中的生物特征识别参考发送给服务器；
9. 服务器将生物特征识别数据与用户帐号标识符绑定，并执行ASD；
10. 服务器将接收到的生物特征识别参考存储在生物特征识别参考数据库中；
11. 服务器将生物特征识别注册结果返回给客户端；
12. 客户端将生物特征识别注册结果通知用户。

8.2.2 认证流程

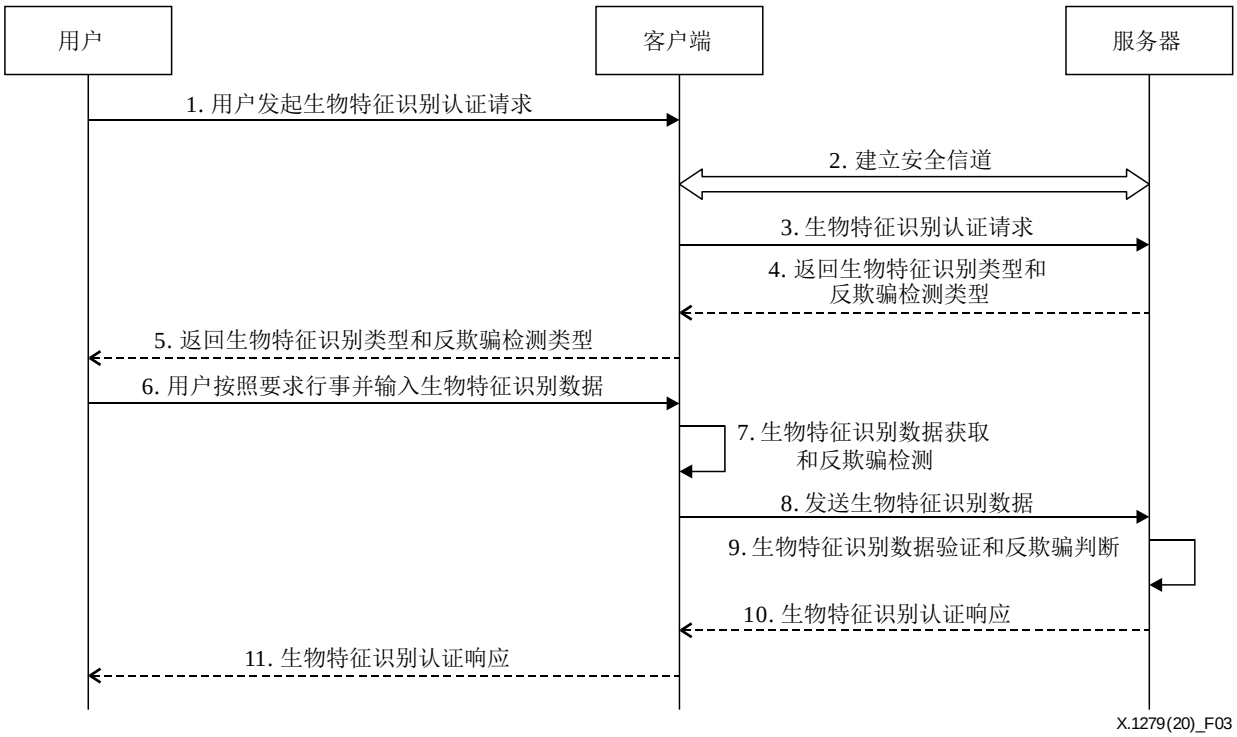

图3 – 认证流程

图3显示了认证流程。详细流程如下所述：

1. 用户使用用户帐户标识符向客户端发起生物特征识别认证请求；
2. 客户端与服务器建立安全信道以保护会话和数据传输，例如，通过使用安全远程密码（SRP）协议；
3. 客户端将生物特征识别认证请求以及用户帐户标识符和风险管理数据发送给服务器；
4. 基于对风险管理数据和业务逻辑的分析，服务器中的决策逻辑功能将正确的生物特征识别类型和ASD类型返回给客户端；
5. 客户端要求用户执行指定的操作以获取生物特征识别数据；
6. 用户按照要求行事，并从客户端输入生物特征识别数据；
7. 客户端中的生物特征识别数据获取功能获取生物特征识别数据，ASD功能检测用户的预期移动；
8. 客户端在已建立的安全信道中将提取的生物特征识别数据发送给服务器；
9. 服务器在提取的生物特征识别特征与生物特征识别参考之间对生物特征识别数据进行验证，并执行ASD；
10. 服务器将生物特征识别认证结果返回给客户端；
11. 客户端将生物特征识别认证结果通知用户。

8.2.3 注销流程

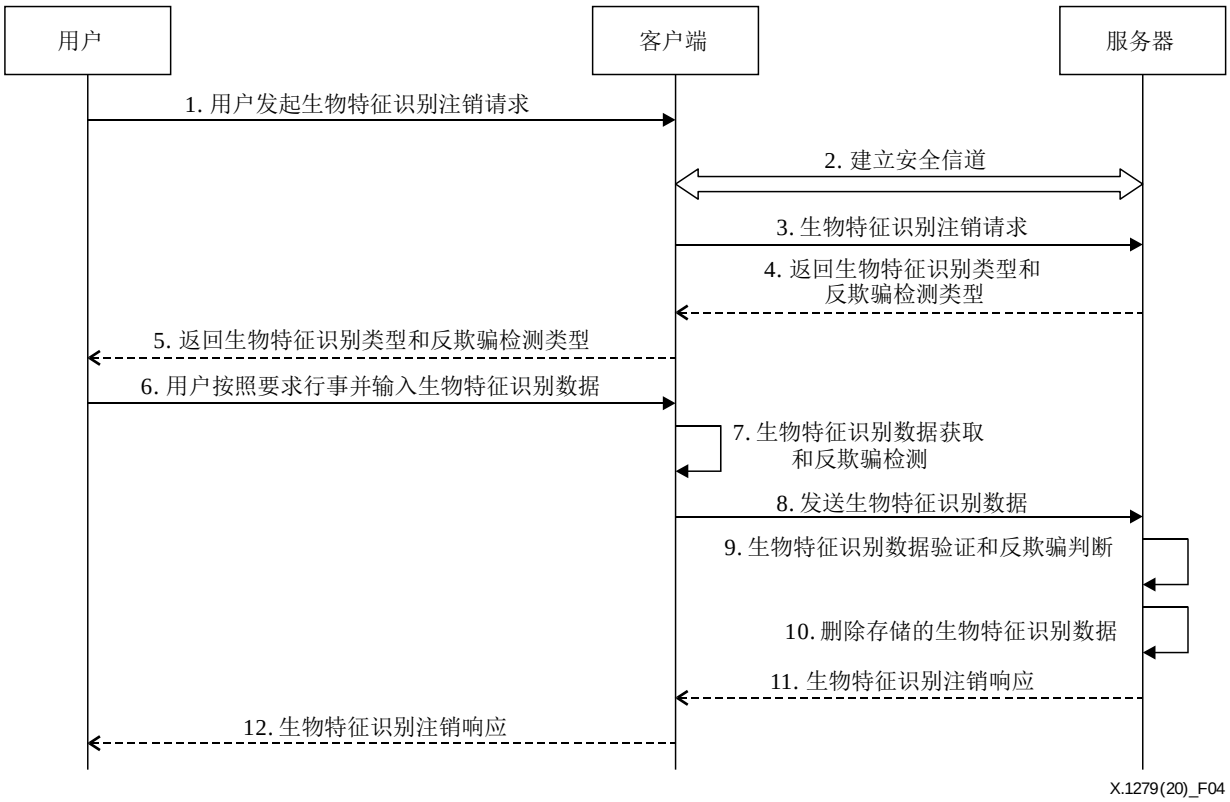

图4 – 注销流程

图4显示了注销流程。详细流程如下所述：

前提条件：用户通过其他认证机制成功与服务器实现认证，例如，用户帐户标识符/密码以及短消息服务（SMS）验证码。

1. 用户使用帐户标识符/密码登录，并向客户端发起生物特征识别注销请求；
2. 客户端与服务器建立安全信道以保护会话和数据传输，例如，通过使用安全远程密码（SRP）协议；
3. 客户端将生物特征识别注销请求以及用户帐户标识符和风险管理数据发送给服务器；
4. 基于对风险管理数据和业务逻辑的分析，服务器中的决策逻辑功能将正确的生物特征识别类型和ASD类型返回给客户端；
5. 客户端要求用户执行指定的操作以获取生物特征识别数据；
6. 用户按照要求行事，并从客户端输入生物特征识别数据；
7. 客户端中的生物特征识别数据获取功能获取生物特征识别数据，ASD功能检测用户的预期移动；
8. 客户端在已建立的安全信道中将提取的生物特征识别数据发送给服务器；
9. 服务器在提取的生物特征识别特征与存储的生物特征识别参考之间对生物特征识别数据进行验证，并执行ASD；
10. 服务器从生物特征识别参考数据库中删除用户的生物特征识别参考；
11. 服务器将生物特征识别注销结果发送给客户端；
12. 客户端将生物特征识别注销结果通知用户。

9 安全导则

9.1 客户端安全

应及时将移动设备操作系统更新为最新的安全版本。

客户端应予签名，以便识别客户端的来源。

客户端应予保护，以便抵御未经授权的修改或更新。

应加强对代码和数据的保护，以防止客户端上的反向工程，例如，混淆。

获取客户端中的数据应在可信环境中实施，以确保所收集数据的机密性和完整性。

9.2 服务器安全

服务器中应实施严格的访问控制策略，对服务器的任何操作均应先经过认证和授权。

服务器应具有识别客户端身份的能力。

服务器与客户端之间的通信应予保护，以便抵御回复攻击，例如，在消息中使用动态数据，例如，随机数、质询或时间戳。

应为服务器上的操作维护日志，并应保护日志的完整性。

9.3 存储安全

ITU-T X.509证书和私钥应予安全存储，并应设置严格的访问控制策略。

私钥应以密文进行存储，并且加密算法应具有较高的安全等级，以防破解。

存储在服务器中的生物特征识别数据应予加密，并且加密算法应具有较高的安全等级，以防破解。

存储在服务器中的生物特征识别数据应是经提取的生物特征识别特征，并且不能还原为原始数据。

有关存储安全的更多详细信息，应符合[ISO/IEC 24745]中的要求。

9.4 通信安全

在客户端与服务器之间进行任何通信之前，应建立安全信道，例如，https适于通信安全之目的。

在客户端与服务器之间应提供用于认证中安全密钥交换的机制，例如，SRP可用作安全密钥交换的机制。

应防止用于协商安全信道的密钥被截获，例如，SRP可用于协商安全信道而无需传输密钥。

诸如经处理的生物特征识别数据和决策结果组件之类的信息应予编码以进行传输，并且其完整性应通过单向函数（例如，哈希函数或公钥基础设施（PKI））进行验证，该函数禁止在传输过程中对数据做任何更改。

经处理的生物特征识别数据应予脱敏并予加密以进行传输，并且加密密钥应与其他客户端的不同，服务器使用匹配的解密密钥进行解密。

有关通信安全的更多详细信息，应符合[ISO/IEC 24745]中的要求。

9.5 其他安全注意事项

除了存储安全和通信安全之外，还需要考虑许多其他方面的安全问题，例如，处理安全、个人可识别信息（PII）保护等。有关生物特征识别信息保护的安全技术的更多详细信息，应符合[ISO/IEC 24745]中的要求。

附录I

用例和场景

（本附录不构成本建议书不可或缺的组成部分）

I.1 移动支付业务的用例研究

爱丽丝（Alice）是一个用户，她使用名为“移动钱包”的应用程序来移动付款。该过程描述如下：

1) 第一次使用时，爱丽丝使用她的用户名和密码登录到移动钱包应用程序。她不想在每次付款时都必须输入密码，而且她也担心忘记密码，因此，她在移动钱包应用程序中点击了“面部验证付款注册”按钮。

2) 移动钱包应用程序要求Alice打开相机，然后冲相机点头。

3) 爱丽丝收到来自移动钱包应用程序的通知：“您已成功注册”。

4) 爱丽丝在星巴克商店里买了一杯咖啡，然后使用移动钱包应用程序付款。爱丽丝打开移动钱包应用程序，并准备付款。移动应用程序要求爱丽丝打开相机并冲相机中点头。爱丽丝非常喜欢这种经历。

5) 爱丽丝收到来自移动钱包应用程序的通知：“您已经成功付款，谢谢！”。

6) 一段时间后，爱丽丝不再想用该功能，则她可通过点击一个按钮以关闭该付款方式选项。

I.2 电子商务业务的用例研究

鲍勃（Bob）拥有一家卖衣服的商店，他想在电子商务平台上开设一个在线商店。该过程描述如下：

1) 第一次使用时，鲍勃在电子商务平台上注册并申请开设一个新商店。鲍勃通过其移动设备上的一个电子商务应用程序来在电子商务平台上设置用户名和密码。

2) 其移动设备上的电子商务应用程序要求鲍勃打开相机并依次执行若干操作，例如，张嘴、摇头、眨眼并冲相机点头。

3) 鲍勃收到来自电子商务移动应用程序的通知：“您已成功注册”。

4) 一段时间后，鲍勃想在他的商店发布一些衣服。电子商务平台要求鲍勃打开相机，并依次执行若干操作，例如，摇头、眨眼、张嘴并冲相机点头。

5) 鲍勃收到来自电子商务平台的通知：“您已成功登录。”

6) 一段时间后，鲍勃不想再用该功能，则他可通过点击一个按钮以关闭该认证选项。

附录II

安全远程密码（SRP）

（本附录不构成本建议书不可或缺的组成部分）

SRP是一种基于密码的身份认证和密钥交换协议。SRP的优点是：密钥明文在认证过程中不会出现传输现象，用户只需持有密码。此外，即使服务器被对手获取，服务器也不会存储用户的密码，但会存储相关的信息；对手无法伪造合法客户端（因为无法获取密码）。

SRP协议的详细信息可在[b-RFC 2945]中找到。

在生物特征识别注册过程、生物特征识别认证过程和生物特征识别注销过程中，SRP协议可用于在客户端与服务器之间建立安全信道。使用用户提供的密码，SRP协议可用来协商安全连接，同时消除传统上与可重用密码相关的安全问题。在认证过程中，SRP协议还可用来执行安全密钥交换，从而允许在会话期间启用安全层（隐私和/或完整性保护）。

附录III

在面部识别中服务器如何执行ASD的示例

（本附录不构成本建议书不可或缺的组成部分）

在面部识别中服务器如何执行ASD的示例包括但不限于：

1) 根据服务器的一些提示或指示，用户可以执行指定的操作，服务器可从面部图像中检测到该操作。
2) 服务器应具有检测面部和摄像机角度的能力，并在此过程中通过改变面部角度来检测活体。
3) 服务器应具有检测面部动作连续性、防止幻灯片播放以及防止人员在此过程中发生变化的能力。
4) 服务器应具有检测面部动作视频重播的能力。
5) 服务器应具有防止面部图像攻击的能力。
6) 服务器应具有检测由计算机图形学技术产生的3D面部模型的能力。

参考书目

[b-ITU-T M.3016.0] ITU-T M.3016.0建议书（2005年），管理平面的安全性：概述。

[b-ITU-T X.509] ITU-T X.509建议书（2019年），信息技术 – 开放系统互连 – 目录：公钥和属性证书框架。

[b-ITU-T X.1081] ITU-T X.1081建议书（2011年），远程生物特征识别多模式模型 – 远程生物特征识别安全方面的规范框架。

[b-ITU-T X.1085] ITU-T X.1085建议书（2016年）| ISO/IEC 17922:2017，信息技术 – 安全技术 – 使用生物特征识别硬件安全模块的远程生物特征识别认证框架。

[b-ITU-T X.1089] ITU-T X.1089建议书（2008年），远程生物特征识别认证基础设施（TAI）。

[b-ITU-T X.1252] ITU-T X.1252建议书（2010年），基线身份管理术语和定义。

[b-ITU-T X.1254] ITU-T X.1254建议书（2012年），实体认证保证框架。

[b-ISO 18461] ISO 18461:2016, *International museum statistics.*

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

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

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

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

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

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

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

[b-ISO/IEC 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 (Third Edition), 2009, Pages 355-364.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦