TC260-PG-2023XX

网络安全标准实践指南

—人脸识别支付场景个人信息保护安全要求

（征求意见稿 v1.0-202305）

全国信息安全标准化技术委员会秘书处

2023 年 05 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国民认证科技（北京）有限公司、蚂蚁科技集团股份有限公司、京东集团、深圳市腾讯计算机系统有限公司、中科院信息工程研究所、小米科技有限责任公司等单位的技术支持。

摘　要

人脸识别支付已成为一种常见的支付手段。然而，人脸识别支付设备的多样化发展以及广泛使用给个人信息保护带来了新的安全挑战。

本实践指南依据政策法规要求，针对室内外各区域中的人脸识别支付场景，向人脸识别支付的服务提供方及相关场所管理方提出个人信息保护要求。

目　录

1 范围

本实践指南针对室内外区域中的人脸识别支付场景，提出个人信息保护要求。

本实践指南不适用于用户在其自有手机或其他自有智能移动终端上进行的人脸识别支付。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 40660　信息安全技术　生物特征识别信息保护基本要求

GB/T 41819　信息安全技术　人脸识别数据安全要求

3 术语和定义

GB/T 40660、GB/T 41819 界定的以及下列术语和定义适用于本文件。

3.1 场所管理方

决定人脸识别支付场景设置情况的组织或个人。

3.2 服务提供方

人脸识别支付服务的提供方。

3.3 用户

进行人脸识别支付的个人用户。

4 基本要求

基本安全要求包括：

a) 人脸识别数据安全应符合 GB/T 41819 的要求。

b) 人脸识别支付过程中，出于维护公共安全、金融安全等目的，按照有关管理部门明确要求处理的数据，应仅用于其所规定的目的，不应自行用于与其无关的活动。

5 服务提供方

安全要求包括：

a) 不应收集人脸识别期间之外的数据：应仅在人工做出点击等明确交互动作后开始收集数据；人脸识别完成后或开始收集数据一分钟后，应停止收集数据。

b) 人脸识别全部过程数据应在本次人脸识别结果产生后全部删除，以下数据除外：

1) 符合 GB/T 40660 要求的人脸识别注册数据；

2) 人脸比对是否成功的结果信息；

3) 人脸支付出现重大故障时的调试数据，但不包含未经授权的个人信息。

c) 人脸识别支付服务获得的人脸相关数据不应用于与本次支付过程无关的目的。

d) 不应支持导出人脸相关数据的功能。

e) 人脸识别支付服务应具备检测运行环境安全状态的能力，发现不安全时，应采取充分的安全保护措施或停止运行。

注：不安全的环境例如已经获取了 root 权限的安卓系统。

6 场所管理方

安全要求包括：

a) 为单一组织内部提供服务的人脸识别支付宜通过在该单位内部搭建局域网、不接入互联网的形式实现。

b) 人脸识别支付所使用的摄像头固定朝向某一区域时：

1) 应通过在该区域入口设置显著标识等方式，使不愿意被收集人脸识别数据的个人可以提前避开；

2) 不应朝向重要敏感区域收集人脸数据，包括政府办公区出入口、军事管理区、人流或车流密集区域等。

附录 A

（资料性附录）

人脸识别支付主要场景及其个人信息安全风险

1 主要场景

常见人脸识别支付场景类型如下：

a) **手机人脸支付**：个人使用其自有手机或其他智能移动终端开展人脸识别支付的场景，主要相关方包括服务提供方及用户。

b) **内部人脸支付**：面向特定组织内部人员开展人脸识别支付的场景，例如食堂人脸识别支付等，主要相关方包括场所管理方、服务提供方、用户。

c) **公用人脸支付**：面向室内或室外不固定人群开展人脸识别支付的场景，例如自动售货机人脸识别支付等，主要相关方包括场所管理方、服务提供方、用户。

2 主要风险

常见人脸识别支付场景下的个人信息保护风险如下：

a) 在手机人脸支付场景下，主要包括人脸识别数据的强采、偷采、滥采、滥用，以及其他未经授权处理人脸相关数据等问题。

注：该部分风险 GB/T 41819 已经较完整覆盖。

b) 在内部人脸支付场景下，人脸识别服务接入互联网时，敏感个人信息泄露风险显著。

c) 在公用人脸支付场景下，主要个人信息保护风险包括：

1) 摄像头在非人脸识别状态下开启，导致超范围、非必要收集个

人信息和相关视频数据；

2) 使用人脸识别支付过程中，除识别对象外，存在额外收集、使用未授权个人信息的风险；

3) 朝向敏感隐私区域收集数据，例如朝向更衣室、洗手间等区域收集数据，侵犯个人隐私的风险；

4) 摄像头朝向重要场所收集数据，例如朝向特定出入口、人流密集区域，导致违法违规处理重要数据或特定身份人员敏感个人信息的风险。