ICS 01.040.35
L 07

团　　体　　标　　准

T/ISC XXXX—XXXX

基于 NFC 的增强身份认证技术要求

Technical requirements of near field communication-based enhanced identity authentication

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

2024-06-28

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国互联网协会归口。

本标准主要起草单位：

本标准主要起草人：

引　言

近些年，随着移动互联网的飞速发展，物理世界正在加速数字化，数字时代已悄然来临。一方面，数字身份作为数字世界的入口，数字身份生命周期贯穿整个数字生态，数字身份安全重要性凸显，解决数字身份及相关数据安全问题成为当务之急；另一方面，在当前数字经济背景下，数字身份成为数字信任的基石，“数字身份+数字信任”正重塑信息时代经济发展模式和治理体系。

传统身份认证往往需要用户提供纸质证件或手动输入身份信息，证件难以辨别真伪的同时用户使用体验也较差。随着NFC技术的不断发展和应用，以NFC硬件为基础的身份管理场景日益增多，结合“NFC硬件载体”的身份认证方式，能够进一步实现身份的数字化并增强数字身份的可靠性；通过NFC直接读取身份凭证能够大大降低用户身份认证操作难度，同时辅以其他模态认证因子的比对，能够确保用户身份信息的准确性，并进一步增强身份认证的安全性，降低用户身份盗用风险，保护用户合法权益。

基于NFC的增强身份认证技术要求

1 范围

本文件给出了基于NFC的增强身份认证角色视图、技术架构、业务流程和技术要求等，从用户端、移动用户端和后台服务端提出相关要求。

本文件适用于面向基于NFC的增强身份认证技术的设计、集成及应用，也适用于基于NFC的增强身份认证系统的验收与评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

ISO/IEC 14443 A/B 超短距离智能卡标准（Cards and security devices for personal identification — Contactless proximity objects）

ISO/IEC 24760-1 信息技术安全和隐私.身份管理框架.第1部分:术语和概念(IT Security and Privacy - A framework for identity management – Part 1: Terminology and concepts)

ITU-T Y.2720 NGN版本1的认证和授权要求(Authentication and authorization requirements for NGN release 1)

GB/T 35273-2020 信息安全技术 个人信息安全规范

YD/T 2592-2013 身份管理(IdM)术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

实体 entity

独立存在并在环境中能被识别的事物。

[来源：YD/T 2592-2013，定义4.59]

3.2

身份 identity

一组与实体所关联的属性集。

[来源：ISO/IEC 24760-1]

3.3

业务身份 business identity

单一机构发行的仅在该机构场景内使用的身份。

3.4

认证 authentication

用来对实体和所呈现身份之间的绑定关系进行充分确认的过程。

[来源：YD/T 2592-2013，定义4.60]

3.5

管理 management

一组用于保证身份信息的功能和能力，保证实体身份，为商业和安全应用提供支持。

[来源：ITU-T Y.2720]

3.6

增强身份认证 enhanced authentication

通过依赖于第三方身份数据库的静态身份数据核验与实时活体采集设备的动态生物特征比对实现的身份认证过程。

3.7

用户 user

使用资源的任何实体，资源包括系统、设备、终端、进程、应用程序或合作网络。

[来源：YD/T 2592-2013，定义 4.85]

3.8

移动用户端 mobile user-side

面向用户的软件程序。

3.9

生物特征采集模块 biometric feature collection module

动态实时采集用户生物特征，完成用户身份识别和活体验证的软硬件模块。

3.10

软件支撑模块 software support module

支撑用户注册及登录、认证接口、授权接口、审计、自助服务等功能的软件模块。

3.11

NFC 识别模块 NFC identification module

具备独立的操作系统和运行空间，可安装软件，并具备NFC读写、定位、接入互联网等功能的硬件模块。

3.12

业务身份认证管理服务 business identity authentication management service

接收并处理用户认证、管理等请求，返回处理结果，并可对接第三方身份认证的服务系统。

3.13

第三方身份服务 third party identity service

满足相关业务需求和政府监管要求，通过对比登记实体的信息，实现信息核验和确认。

3.14

身份凭证 identity credential

描述实体属性的身份证明。

3.15

辅助信息 auxiliary information

用于辅助业务身份认证管理方进行身份认证的个人身份信息。

4 缩略语

下列缩略语适用于本文件。

API:应用接口（Application Interface）

NFC:近场通信(Near Field Communication)

SDK:软件开发工具包（Software Development Kit）
SaaS:软件即服务（Software as a Service）
SSO:单点登录（Single Sign-On）

5 角色视图

5.1 概述

基于NFC的增强身份认证场景下的角色可分为用户、业务身份认证管理方和第三方身份服务提供方，三个角色关系如图1。

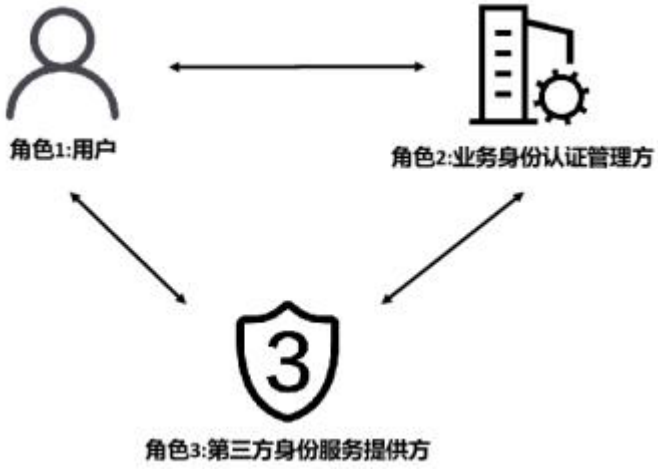

图 1 相关方角色视图

5.2 用户

用户指使用基于NFC增强身份认证服务/应用的实体，包括自然人、法人或机构等。用户角色相关活动包括：

——提供可供 NFC 识别模块读取的实体身份凭证，如身份证件、门禁磁卡、智能卡等；
——提供可供生物特征采集模块读取的生物特征信息，如指纹、人脸、虹膜、静脉掌纹等。

5.3 业务身份认证管理方

业务身份认证管理方指为用户提供身份认证及管理服务的系统平台或机构。业务身份认证管理方接收并处理用户身份认证、身份管理等请求，返回处理结果，实现用户身份的注册、签发、验证与管理，并可对接第三方身份认证服务系统实现增强身份认证。业务身份认证管理方角色相关活动包括：

——提供用户身份验证服务；
——提供用户身份管理服务；
——提供基于 NFC 的增强业务身份认证服务；
——同用户身份凭证交互校验身份凭证真伪；
——提供用户身份数据管理服务。

5.4 第三方身份服务提供方

第三方身份服务提供方指的是根据不同业务需求发行身份凭证、管理身份凭证或提供身份凭证信息读取校验服务的第三方机构。第三方身份服务提供方通过识别、校验已发行、登记的实体身份凭证信息，实现信息读取和身份验证，并向业务身份认证管理方返回结果。第三方身份服务提供方角色相关活动包括：

——同用户身份凭证交互并校验身份凭证真伪；

——根据身份凭证类型提供身份核验服务；

——向业务身份认证管理方提供用于增强用户身份认证的辅助信息。

6 技术架构

6.1 总体概述

基于NFC的增强身份认证技术架构按数据流向可分为两层，分别是移动用户端和服务端，涉及用户、业务身份认证管理方和第三方身份服务提供方，通过静态身份数据核验和动态生物特征比对相结合的方式，实现用户从物理身份到数字身份的可靠映射。基于NFC的增强身份认证技术框架如图2。

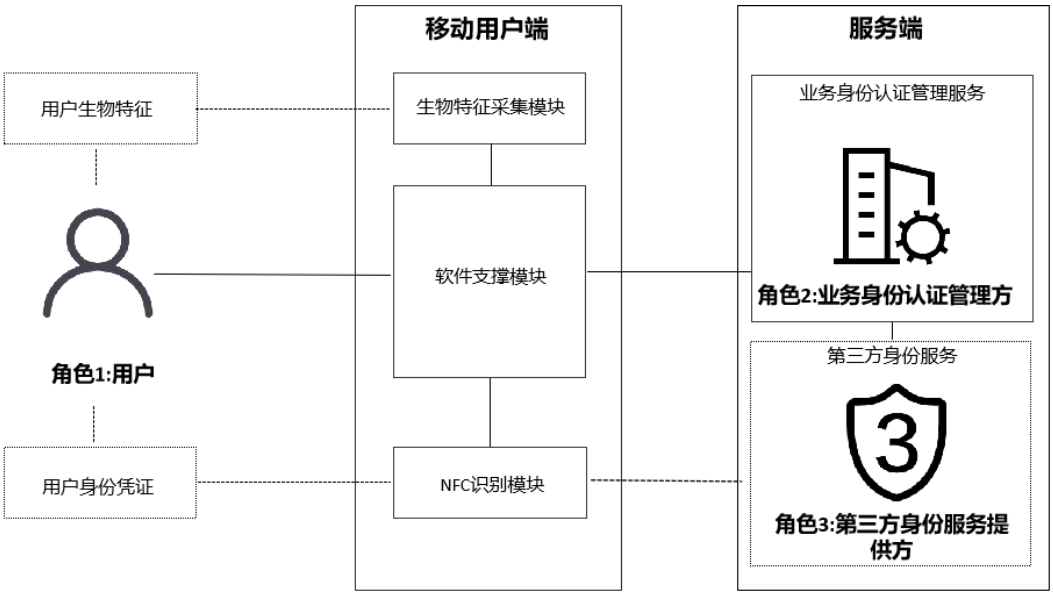

图 2 基于 NFC 的增强身份认证技术框架

6.2 移动用户终端

移动用户端主要包括生物特征采集模块、软件支撑模块和NFC识别模块等。

生物特征采集模块实现用户生物特征信息的安全采集，确保用户生物特征被真实、准确、安全地采集以用于后续用户身份的验证；软件支撑模块与生物特征采集模块、NFC识别模块交互，完成生物特征信息采集、NFC识别，并确保交互过程与相关数据的安全；NFC识别模块与用户身份凭证、第三方身份服务提供方交互，完成身份凭证信息的安全读取并向第三方身份服务提供方或软件支撑模块返回相关信息。

6.3 服务端

服务端为移动用户端提供后台服务，包括业务身份认证管理服务、第三方身份服务等。

业务身份认证管理服务与软件支撑模块、第三方身份服务提供方交互，结合软件支撑模块返回的相关信息或第三方身份服务提供方提供的辅助信息实现对用户身份的认证；第三方身份服务为业务身份认证管理方返回相关信息，用于增强其对用户的身份认证。

7 业务流程

基于NFC的增强身份认证业务流程包括静态身份数据核验和动态生物特征比对流程，相关业务交互如图3。

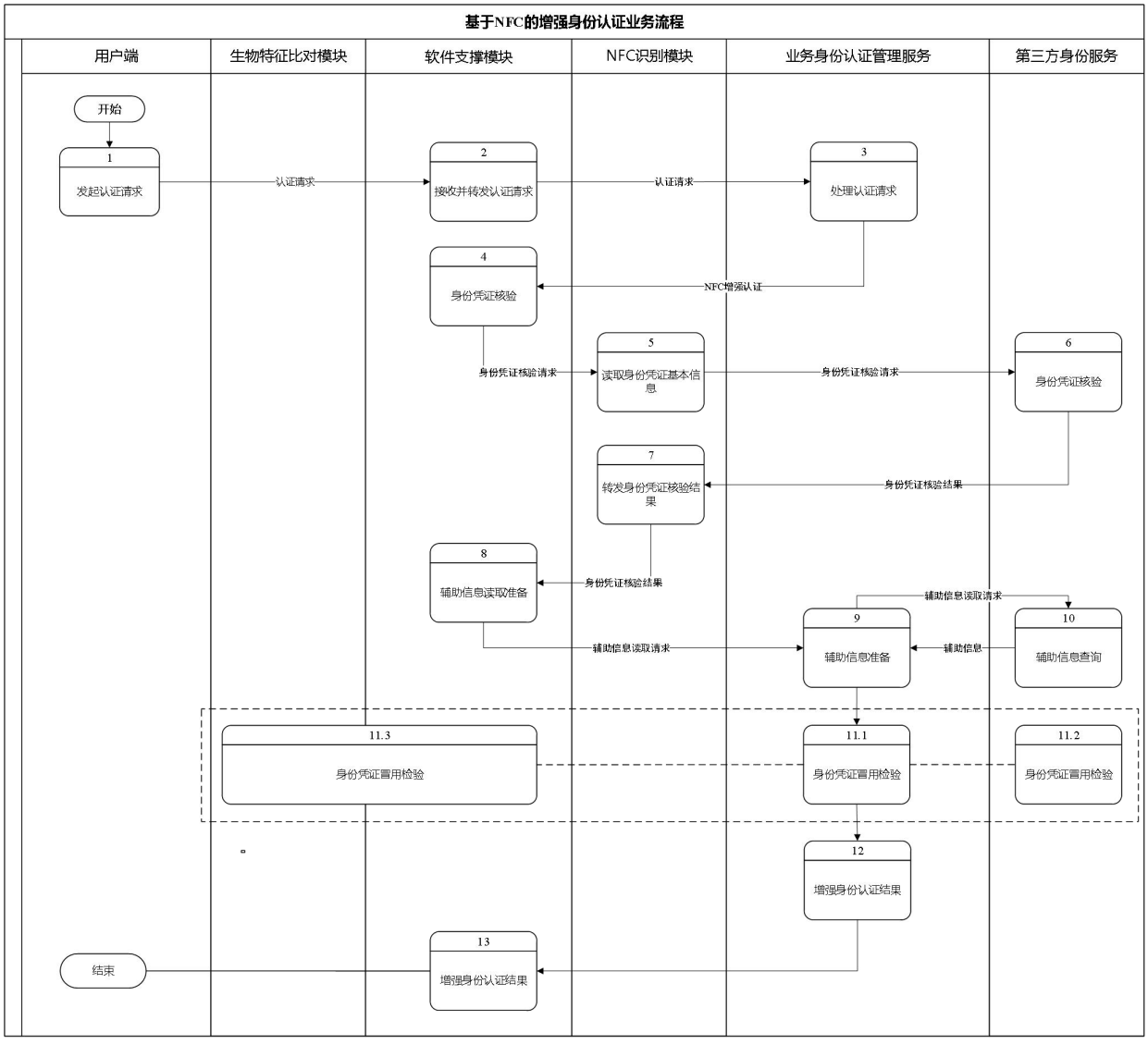

图 3 业务流程图

基于NFC的增强身份认证业务流程包括：

1. 用户：用户发起认证请求；
2. 软件支撑模块：接收并转发认证请求；

3. 业务身份认证管理服务：处理认证请求；
4. 软件支撑模块：发起身份凭证核验请求；
5. NFC 识别模块：读取身份凭证基本信息；
6. 第三方身份服务：进行身份凭证核验并返回身份凭证核验结果；
7. NFC 识别模块：转发身份凭证核验结果；
8. 软件支撑模块：辅助信息读取准备并发起辅助信息读取请求；
9. 业务身份认证管理服务：辅助信息准备；
10. 第三方身份服务：辅助信息查询；
11. 业务身份认证管理服务、第三方身份服务、软件支撑模块或生物特征比对模块：进行身份凭证冒用检验；
12. 业务身份认证管理服务：确认增强身份认证结果；
13. 软件支撑模块：返回增强身份认证结果。

8 技术要求

8.1 移动用户端

8.1.1 基本要求

用户数据包括用户通信信息、使用记录数据、账户信息等个人信息，也包括传感器采集信息、设备信息及文件信息等，相关要求包括：

a) 用户个人信息的保护应满足 GB/T 35273-2020 中的相关要求；
b) 应采取措施确保传感器采集信息的准确性和完整性；
c) 应优先采集和使用设备可变标识符等设备信息并在本地处理；
d) 应采取措施确保文件信息的保密性和完整性。

8.1.2 用户告知

用户告知是指用户使用基于NFC的增强身份认证服务前，提前告知用户认证过程中相关个人信息的收集和使用情况，以及用户需要遵守的规则和要求。除GB/T 35273-2020 中5.4节的相关要求外，用户告知的相关要求包括：

a) 用户个人信息的存储、使用情况，如本地存储或后端服务器存储等；
b) 用户取消、关闭或跳过增强身份认证的方式，以及恢复增强身份认证的方式，避免用户误用和滥用；
c) 用户不慎将 NFC 设备丢失或者被盗后的处置建议，如立即上报相关单位、注销 NFC 认证相关业务功能等；
d) 持续关注 NFC 设备的更新或升级，避免因 NFC 设备漏洞造成损失；
e) 在 NFC 设备出现故障、损坏等情况下的备用身份认证方案。

8.1.3 用户授权同意

用户授权是指用户使用移动用户端服务时，对个人身份及数据的控制与管理，即用户通过授权操作，授予移动用户端与服务端使用个人信息的权利。除GB/T 35273-2020 中5.4节的相关要求外，用户授权同意相关要求包括：

a) 应支持用户身份及相关数据授权管理机制/模型，保证用户对个人信息使用权的控制与管理；

b） 应保证一定时间范围内，系统每次触发用户个人信息使用时，用户拥有完整授权过程，保证用户知情权，避免“一次授权，终生可用”情况；
c） 应避免个人信息授权的默认开启；
d） 用户拒绝授权后，应避免重复多次请求用户授权；
e） 应支持授权行为的留痕与审计，支持用户授权的日志记录、查询等功能，日志宜提供存储归档、持久化存储及防篡改能力；
f） 应支持用户授权变更；
g） 应支持用户授权撤销后的个人信息删除或匿名化；

8.1.4 生物特征采集模块

8.1.4.1 基本要求

生物特征是指人体所固有的生理特征或行为特征，包括人脸识别、指纹识别、掌纹识别、指静脉识别、掌静脉识别、虹膜识别、声纹识别、笔迹识别、步态识别等。生物特征采集模块相关要求包括：

a） 应支持生物特征采集子系统；
b） 应支持生物特征解析子系统；
c） 在满足相关法律法规与政策要求前提下，应支持生物特征缓存子系统；
d） 应支持生物特征比对子系统；
e） 应支持生物特征比对结果决策子系统；
f） 应支持生物特征识别管理子系统，至少提供日志管理、权限管理、用户管理、接口管理功能。

8.1.4.2 生物特征采集

生物特征采集是指通过相关设备采集用户生物特征来进行身份鉴别和辅助证明等。生物特征采集模块相关要求包括：

a） 基本性要求：采集装置固件应由完整性和可用性保护；
b） 合法性要求：在进行生物特征采集时，应明确告知用户采集的目的、范围、方式和使用范围；
c） 必要性要求：生物特征采集应根据实际需求进行，避免过度收集和滥用个人信息；
d） 最小化要求：应尽量减少收集的个人信息数量和种类，只收集与目的相关的最少量信息；
e） 安全性要求：生物特征采集应采取严格的安全措施，确保个人信息的安全存储和传输；
f） 隐私性要求：采集装置在生物特征样本采集结束后应及时清除样本信息，并确保其不可恢复；
g） 透明性要求：应向用户充分披露采集、存储、使用和传输过程中可能涉及的信息风险；
h） 可撤销性要求：用户有权撤销其在生物特征采集中的授权，并要求删除已收集的个人信息；
i） 精细化访问控制要求：采集单元应实施访问控制措施，防止生物特征样本被窃取。

8.1.5 软件支撑模块

8.1.5.1 基本要求

软件支撑模块应实现对NFC识别模块和生物特征采集模块的交互与管理。

8.1.5.2 NFC 读取能力

NFC读取能力是指使用移动用户端NFC识别模块读取用户身份凭证数据，并可与第三方身份服务提供方通信验证用户凭证数据的能力。NFC读取能力相关要求包括：

a） 应保证用户身份认证时的数据传输安全，NFC 模块读取相关证件后开启双向认证加密传输数据；

b） 应保证用户身份认证完成后的数据存储安全，采取密码算法保护 NFC 模块读取的用户个人身份数据；
c） 应保证用户身份认证完成后的数据隐私安全，相关认证过程辅助信息进行统一删除或销毁处理；
d） 应保证 NFC 识别模块的兼容性，保证在不同移动用户端及 NFC 识别模块中的 NFC 读取能力。

8.1.6 NFC 识别模块

NFC识别模块是指具备近距离无线通讯能力的硬件模块。NFC识别模块相关要求包括：
a） 应符合 ISO 14443A/B 中关于 NFC 识别频谱功率和信号接口、初始化和防碰撞算法、传输协议的相关要求；
b） 若移动用户端采用外置 NFC 识别模块，NFC 识别模块应支持指令透传功能。

8.2 服务端

8.2.1 业务身份认证管理服务

8.2.1.1 基本要求

业务身份认证管理服务的基本要求包括：
a） 应具备 7*24 小时的连续服务能力；
b） 应采用分布式高可用架构部署，具备系统负载均衡能力，支持一定数量节点容错能力；
c） 宜支持数据缓存能力；
d） 宜提供支撑系统可靠运行的冗余配置。

8.2.1.2 身份认证

身份认证指对实体和所呈现身份之间的绑定关系进行充分确认的过程。身份认证相关要求包括：
a） 用户身份信息应进行加密处理，确保信息在传输和存储过程中不被窃取或篡改；
b） 用户身份信息的访问权限应进行严格控制，只有授权人员才能访问和使用相关信息；
c） 应使用安全的认证协议，避免篡改、重放、假冒等攻击；
d） 应支持生物特征比对，且当生物特征比对失败时，应提供用户反馈渠道并给出解决办法。

8.2.1.3 身份管理

身份管理指提供身份注册、签发、验证的全生命周期管理的功能。身份管理相关要求包括:
a） 应提供用户身份注册、签发、验证的全生命周期管理能力；
b） 应支持用户身份属性的拓展；
c） 应支持用户通过多种方式找回身份能力；
d） 应支持身份敏感信息加密存储能力；
e） 应支持用户身份与用户属性的一对多映射关系；
f） 宜提供用户身份与法定证件的一对一映射，实现用户身份的信任增强；
g） 宜支持身份更新、冻结、解冻的进阶管理能力；
h） 宜支持对用户行为、设备行为的审计，并对可疑行为进行警告。

8.2.1.4 身份联合

身份联合指允许不同的身份管理系统以安全、快捷、统一方式共享身份认证信息。身份联合相关要求包括：

a) 应支持基于令牌的快捷认证，避免其他域中的重复 NFC 或生物特征认证；
b) 应支持身份联合有效时间管理和接入授权管理；
c) 宜支持标准 SSO 单点登录协议；
d) 宜支持单点登出时的用户会话销毁；
e) 宜支持跨域 SSO 单点登录能力。

8.2.1.5 日志审计

日志审计指对每天所记录的信息进行审计和检查。日志审计相关要求包括：
a) 应支持身份认证、身份管理等关键操作日志审计；
b) 应根据日志信息的隐私分级管理，对隐私信息进行加密、脱敏处理，访问授权以“最小授权”的原则；
c) 关键日志应保存 6 个月以上；
d) 宜支持审计日志权限控制；
e) 宜支持多种事件机制审计，包括主机事件审计、网络事件审计、数据库事件审计和应用系统事件审计。

8.2.1.6 安全保障

安全保障指保障基于NFC增强身份认证服务过程安全性的关键指标。安全保障相关要求包括：
a) 应支持用户身份标识注册、签发、验证与管理过程的安全保障能力；
b) 应支持用户身份标识的安全存储能力；
c) 应支持用户身份标识数据的安全传输能力；
d) 应支持灾备和恢复机制，支持在数据丢失或损坏时进行数据恢复。

8.2.1.7 个人信息保护

个人信息保护指对个人身份信息和隐私进行保护的措施。个人信息保护相关要求包括：
a) 应具备安全防护能力，防止个人信息泄露，包括但不限于采取加密、访问控制等技术手段；
b) 应采取必要的措施，确保移动用户端和服务端存储的个人信息安全，防止个人信息泄露、损毁、丢失等；
c) 第三方身份服务提供方宜采取技术措施防止用户身份信息泄露或重标识；
d) 涉及生物特征识别时，业务身份认证管理方应制定单独协议，对用户进行告知并获得同意；
e) 应对涉及操作、使用和管理身份信息的人员进行权限管控，并对操作行为进行定期审计。

8.2.1.8 口令使用安全

口令使用安全指系统管理、使用口令过程的安全。口令使用安全相关要求包括：
a) 应制定用户口令安全管理方案并严格执行；
b) 应制定用户口令泄漏应急响应方案并严格执行；
c) 应使用安全的密码算法加密存储；
d) 应符合复杂性要求，至少包含大小写字母、数字和特殊字符；
e) 应具备使用一段时间后强制更换密码的功能；
f) 应制定安全管理方案和应急响应方案并严格执行。

8.2.1.9 第三方身份服务接入与管理

第三方服务接入与管理指基于NFC的增强身份认证过程中，接入第三方身份认证产品或服务的能力。第三方服务接入与管理相关要求包括：

a） 宜支持通过第三方开放接口获取用户身份相关数据；
b） 宜定期对接入的第三方身份源有效性进行验证。

8.2.2 第三方身份服务

8.2.2.1 身份凭证解析

身份凭证解析指根据既定规则以身份凭证作为输入，输出相关个人身份信息数据。身份凭证解析相关要求包括：

a） 在解析身份凭证前，应先建立安全通道，实现双向身份认证及加密，需采用国家密码局认可的密码算法；
b） 在解析身份凭证后，辅助身份信息若需缓存，应采用业务管理方的数字证书加密；
c） 业务完成后，辅助身份信息应永久删除。

8.2.2.2 安全保障

安全保障指保障第三方身份认证过程安全性的关键指标，应包括。安全保障相关要求包括：

a） 应指定个人信息安全负责人，并制定相应的管理体系，包括但不限于：个人信息管理制度、教育培训制度、信息安全奖惩管理制度、隐私信息安全管理制度、信息安全管理制度以及应急响应制度；
b） 应通过与业务身份认证管理方签订协议等方式，约定双方在身份认证过程中的权利、责任与义务。

8.3 接口设计

接口指以API、SDK、SaaS等方式为第三方厂商及开发者提供服务，并提供安全防护能力。接口设计相关要求包括：

a） 应确保接口采集数据的准确性和可靠性；
b） 应确保接口传输数据的安全性；
c） 应确保接口设计的灵活性和扩展性；
d） 应满足跨平台兼容性，确保相关接口可在不同的硬件、操作系统上正常使用；
e） 应确保接口的设计和调用过程具备流程控制和权限控制；
f） 应确保数据采集的合法性和规范性，以及对不同国家、地域法律法规的适应性；
g） 应满足接口幂等性原则，保证相同请求数据前提下，一次调用和多次调用接口的结果一致性；
h） 宜提供接口定制化能力，实现接口参数可配置；
i） 宜提供身份全生命周期管理、身份授权管理及身份数据管理功能接口；
j） 宜支持多模态采集接口，如指纹、面部识别、虹膜、声音等多模式特征的组合采集等；
k） 宜提供清晰、详细的接口文档和示例代码。