ICS 35.240.01

CCS M30 49

团　　体　　标　　准

T/FSAS 58—2022

基于互联网的可信数字身份服务技术要求

Technical requirements for internet-based trusted digital identity service

2022-02-10 发布　　2022-02-10 实施

佛　山　市　标　准　化　协　会　发布

目　　次

前　言

本文件按照GB/T 1.1－2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由腾讯科技（深圳）有限公司提出。

本文件由粤港澳大湾区标准创新联盟归口。

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专利的责任。

本文件起草单位：腾讯科技（深圳）有限公司、腾讯科技（北京）有限公司、北京数字认证股份有限公司、中国科学院信息工程研究所、广东省商用密码协会、上海市数字证书认证中心有限公司、广州大学、华南农业大学、华南师范大学、暨南大学、安讯奔（香港）科技有限公司、上海银基信息安全技术股份有限公司、深圳市电子商务安全证书管理有限公司、北京安讯奔科技有限责任公司、澳门智慧城市联盟协会、香港大学、北京京东世纪贸易有限公司。

本文件起草人：蔡冉、周耀辉、于丹、周斌、王永霞、张永强、高能、李敏、彭佳、刘镭、李向锋、刘俊河、曾祥楷、王犇、陈世杰、王旭、陶宇、郑松坚、傅大鹏、张妍、王天华、周权、张猜、龚征、谭武征、李南希、程伟强、吴嘉文、楊毅濤、郭晓锋、郑炎兴、吴俊、王志辉、陈武方、马辉、陈益民、帅涛、贺啸、黄晓林、白亚楠、蒋健敏、吴廷伟、刘晓宇、黄承发、阳光、宓锡梅。

本文件为首次发布。

基于互联网的可信数字身份服务技术要求

1 范围

本文件规定了基于互联网的可信数字身份服务的技术要求，包含了可信数字身份的基础架构和分级分类、功能要求、性能要求、应用集成要求及互操作性要求等内容。

本文件适用于规范互联网环境下，面向自然人、法人、设备等实体的可信数字身份服务的设计、集成和应用。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 35291—2017 信息安全技术 智能密码钥匙应用接口规范

粤港电子签名证书互认证书策略v1.1

粤港澳电子签名证书互认证书策略v1.0

ISO/IEC 9798-2 IT安全技术—实体认证—第2部分：使用认证加密的机制（IT Security techniques — Entity authentication — Part 2: Mechanisms using authenticated encryption）

ISO/IEC 9798-3 IT安全技术—实体认证.第3部分—使用数字签名技术的机制（IT Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques）

ITU-T X.509 信息技术-开放系统互连-目录：公钥和属性证书框架 （Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks）

ITU-T X.1141 安全断言标记语言2.0（Security Assertion Markup Language SAML 2.0）

PKCS#11：加密令牌接口标准 （Cryptographic Token Interface Standard）

RFC 6749 授权框架2.0 （ The OAuth 2.0 Authorization Framework）

RFC 6750 授权框架2.0：承载令牌应用（The OAuth 2.0 Authorization Framework: Bearer Token Usage）

RFC 8628 设备授权授予2.0 （OAuth 2.0 Device Authorization Grant）

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

实体 entity

可对系统或服务发起访问或请求的对象。

注：如自然人、法人、设备等。用户指代自然人、法人。

3.1.2

数字身份 digital identity
实体在互联网中的虚拟身份表示,包括实体的标识和相关属性。

3.1.3

身份服务提供商 identity provider
为实体提供身份信息管理并提供身份鉴别服务的组织。

3.1.4

依赖方 relying party
依赖于身份服务提供商提供的关于访问实体的鉴别结果，对访问实体所使用的资源或系统进行授权的实体。

3.1.5

可信数字身份 trusted digital identity
身份服务提供商以所期望的和所声称的方式，为依赖方提供可信赖的实体数字身份。

3.1.6

身份鉴别 identity authentication
身份服务提供商在指定级别的可信度下确定某实体声称的身份的过程。

3.1.7

身份核验 identity proofing
身份服务提供商对用户、设备等实体进行身份登记、身份真实性核验，并发放身份凭证的过程。

3.1.8

断言 assertion
身份服务提供商生成的对实体身份鉴别结果的声明。
注：可能包含实体属性信息或授权信息等。

3.2 缩略语

下列缩略语适用于本文件。
AD：活动目录(Active Directory)
ABAC：基于属性的访问控制（Attribute Based Access Control）
Basic Auth：基本认证(Basic access authentication)
CAS：集中式认证服务（Central Authentication Service）
CNG：下一代加密技术（Cryptography Next Generation）
DAC：自主访问控制（Discretinoary Access Control）
FIDO：线上快速身份验证（Fast Identity Online）
HTTP：超文本传输协议（HyperText Transfer Protocol）
IdP：身份服务提供商（Identity Provider）
IoT：物联网（Internet of Things）
LDAP：轻型目录访问协议 (Lightweight Directory Access Protocol)
MAC：强制访问控制（Mandatory Access Control）

OAuth：开放授权（Open Authorization）
OIDC：基于OAuth的身份认证（OpenID Connect）
OpenID：去中心化身份认证协议开放标准
RBAC：基于角色的访问控制（Role Based Access Control）
SP：服务提供方（Service Provider）
SaaS：软件即服务（Software as a Service）
SAML：安全断言标记语言（Security Assertion Markup Language）
SCIM：跨域身份管理系统（System for Cross-domain Identity Management）
SDK：软件开发工具包（Software Development Kit）
SSO：单点登录（Single Sign-On）
U2F：通用第二因素（Universal 2nd Factor）
WebAuthN：基于浏览器的认证（Web Authentication）

4 可信数字身份服务基础架构和分级分类

4.1 基础架构

基于互联网的可信数字身份服务基础架构，应包括以下功能，如图1。

a) 可信数字身份服务主要包括可信数字身份的生命周期管理服务、授权服务、数据服务、保障服务、开放服务。
   1） 身份生命周期管理服务包括身份核验、身份鉴别、身份管理、身份映射四部分，提供从最初身份登记和核验，到流转过程中的映射转化，到创建、变更、锁定、解锁、注销、恢复、删除等不同状态管理的能力；身份生命周期管理服务是可信数字身份服务的核心服务，是其他服务的基础；
   2） 身份授权服务是在身份生命周期管理服务基础上提供访问控制能力，包括授权管理、应用管理、单点登录（SSO）；
   3） 身份数据服务提供身份数据模型的管理能力及当身份数据变化时对外同步数据的能力；
   4） 身份保障服务提供流程编排、审计管理、分权管理及隐私管理等保障能力；
   5） 身份开放服务包括自助服务和接口服务，通过自助服务对外提供身份的自管理能力，通过接口服务以标准方式对外提供身份服务能力。
b) 安全可靠运行需要外部支撑系统提供的能力，包括：真实、可靠的身份数据源，可信的证书服务，密码相关服务和安全服务，安全服务提供攻击防护、数据安全保护等安全能力。
c) 第三方应用厂商和第三方开发者提供集成服务，在互联网环境下的各类应用场景中，为用户及设备提供可信数字身份服务。

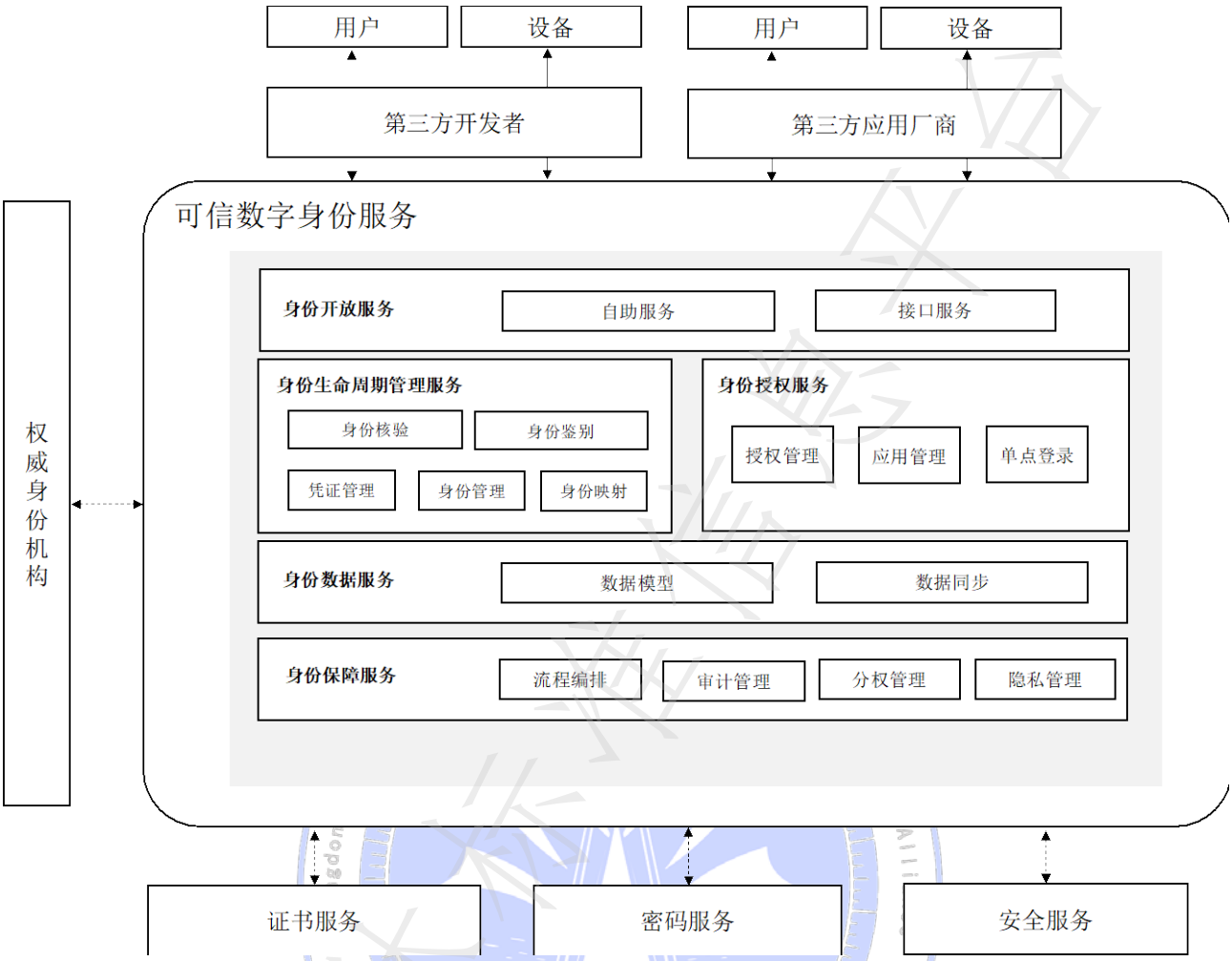

图1　可信数字身份基础架构

4.2　可信数字身份的分类分级

4.2.1　可信数字身份分类

可信数字身份类型包括自然人数字身份、法人数字身份和设备数字身份，具体内容如下：

a）　自然人数字身份是指接入互联网中的各类人群的数字身份；

b）　法人数字身份是指接入互联网中的各类法人的数字身份，包括政府机关、企业、事业单位、社会团体等实体的数字身份；

c）　设备数字身份是指接入互联网中的各类物体的数字身份，包括服务器、个人计算机、移动终端、汽车、IoT 终端设备等实体的数字身份。

4.2.2　可信数字身份的分级

可信数字身份分为低保证、中保证和高保证三个级别：

a）　低保证级别是指对所声称的实体的身份提供有限的信任度，提供有限的数字身份信息。该级别适用于对所声称实体提供有限程度信任的场景，以降低滥用或更改身份的风险；

b）　中保证级别是指对所声称的实体的身份提供充分的信任度，提供重要的数字身份信息。该级别适用于对所声称实体提供较高程度信任的场景，以实质性降低滥用或更改身份的风险；

c） 高保证级别是指对所声称的实体的身份提供更高的信任度，提供充分的数字身份信息。该级别适用于对所声称实体提供更高程度信任的场景，以防止滥用或更改身份的风险。

注：身份服务提供商为实体提供不同保证级别的数字身份服务时，可参考附录A。

5 功能要求

5.1 身份生命周期管理服务

5.1.1 身份核验

5.1.1.1 身份申请

身份申请的要求如下：

a） 支持由实体、身份服务提供商发起身份申请；

b） 实体可通过委托授权，将身份申请和后续行为委托给其它实体，身份服务提供商应核实委托关系真实有效；

c） 当实体为设备时，在申请之前还应包括但不限于为设备粘贴标签或将设备标识符写入到安全存储区域等初始化过程。

5.1.1.2 身份信息和证明文件收集

身份信息和证明文件收集要求如下：

a） 应遵循最小化原则收集满足业务功能需要的身份信息和证明文件；

b） 应包含身份真实性核验所需的必要信息，可依据可信数字身份级别不同而变化；

c） 对用户身份信息和证明文件的收集应满足 GB/T 35273—2020 中规定的个人信息的收集要求。

5.1.1.3 身份核验方式与过程

身份核验方式与过程要求如下：

a） 应至少支持下列身份核验方式之一：

1） 通过交换验证信息的方式，对所声明实体的身份信息进行核验；

示例：验证身份服务商通过邮件或短信发送的验证码。

2） 通过比对有效证件的方式，对所声明实体的身份信息进行核验；

示例：检查物理证件的有效性并将身份证明中的相片/人像与用户比较。

3） 通过与可信第三方核实，对所声明实体的身份信息进行核验；

示例：基于电信运营商或银行提供的信息进行核验。

4） 通过与权威第三方核实，对所声明实体的身份信息进行核验。

示例：基于法定机构提供的渠道或服务进行核验。

b） 应至少支持下列身份核验过程之一：

1） 在线材料证明，包括但不限于通过实体在线提供身份证明材料（如盖章文件等）的方式完成身份验证；

2） 远程身份证明，包括但不限于通过远程方式（如视频、语音）监控实体整个申请身份验证过程完成身份验证；

3） 现场身份证明，即要求实体亲自到现场进行身份验证。

c） 当实体为设备时，应对其关联方的可信数字身份进行核验。

5.1.1.4 身份凭证颁发

身份凭证颁发要求如下：

a) 应在完成身份核验过程，确认身份真实性之后，为实体颁发身份凭证；
b) 应将身份凭证和实体身份进行绑定；
c) 应采用合理的措施确保身份凭证被准确、安全地送达其对应或关联的实体；
d) 如果身份凭证包含了密钥激活材料，应通过独立的安全通道来传递密钥激活材料。

5.1.1.5 身份标识

身份标识要求如下：

a) 应建立统一的控制策略，保证每个实体在数字身份服务提供商处拥有唯一标识；
b) 对于第三方应用，应确保每个实体拥有唯一标识；
c) 可支持在不同的第三方应用为实体分配不同的标识；
d) 应在考虑到个人信息保护因素，及遵循实体要求的基础上，具备向第三方应用或对外提供真名、匿名或假名的能力。

5.1.2 身份鉴别

5.1.2.1 身份鉴别方式

身份鉴别方式如下：

a) 基于静态用户名、口令的鉴别方式：
   1） 可按需设置口令长度、复杂度；
   2） 支持强制要求对口令进行定期修改；
   3） 应支持在设定的时间内超过口令尝试次数后自动锁定用户在 SP 的账号。
b) 基于一次性口令的鉴别方式：
   1） 应采用带外通道传输一次性口令；
   2） 应支持设置一次性口令的有效期；
   3） 可支持基于密码技术的动态口令。
c) 基于数字证书的鉴别方式：
   1） 应对实体数字证书有效性进行验证；
   2） 应支持对实体数字证书的扩展信息项进行校验；
   3） 可支持双向数字证书验证。
d) 基于生物特征的鉴别方式：
   1） 可支持人脸、指纹、虹膜等鉴别方式；
   2） 应满足 5.4.4 规定的隐私管理要求。
e) 基于社交身份提供源的鉴别方式，支持用户使用已持有的社交账号进行验证。
f) 基于推送认证的鉴别方式；
g) 基于 FIDO U2F 和 FIDO2 WebAuthN 的鉴别方式。

5.1.2.2 身份鉴别协议和门户

身份鉴别协议和门户要求如下：

a) 应支持主流协议，包括 OAuth2.0，OIDC，CAS，SAML，HTTP Basic Auth 等协议的一种或多种；
b) 宜支持基于 ISO/IEC 9798-2 或 ISO/IEC 9798-3 的身份鉴别协议；
c) 应根据不同身份保证级别支持多因素鉴别；
d) 宜提供统一的身份鉴别门户并支持分布式部署和配置。

5.1.2.3 配置鉴别策略

配置鉴别策略要求如下：

a) 应支持分布式鉴别服务；
b) 应支持为不同的服务配置差异化鉴别方式；
c) 应支持为不同的可信数字身份级别配置差异化的鉴别方式；
d) 应支持以可视化方式配置鉴别流程；
e) 应支持根据环境、用户、受访资源等因素，执行鉴别保护策略；
f) 应支持基于场景的主动安全防护策略，实现根据用户登录的场景，提供差异化的鉴别保护。

5.1.3 凭证管理

身份鉴别凭证可包括用户名和口令、动态口令、数字证书、硬件令牌、生物特征等。凭证管理应满足以下要求：

a) 应支持身份凭证的全生命周期管理，生命周期环节包括但不限于：创建、颁发、更新、注销、销毁等；
b) 硬件形式的凭证应具有唯一标识；
c) 凭证失效后，应在核验用户身份后支持重置密钥激活材料；
d) 可支持使用托管的密码服务基础设施来存储并管理数字身份凭证。

5.1.4 身份管理

身份管理应满足以下要求：

a) 应支持对实体身份的全生命周期的管理；
b) 应支持对实体身份的层次化、结构化管理；
c) 应支持实体与多个角色的绑定及变更；
d) 应支持实体身份属性的扩展；
e) 可支持对实体按分组、角色等属性批量管理；
f) 宜支持对用户行为、设备行为进行审计，并对可疑行为进行告警；
g) 可支持实体身份与其他数据的关联，并应用于实体身份的鉴别和授权；
g) 应支持来自不同IdP的实体数字身份的聚合，支持统一管理；
i) 可支持用户自主管理数字身份数据的授权，并支持对数据开放范围及授权对象的范围进行管理；
j) 应支持对设备的关联信息进行管理，如生产厂家、使用者等；
k) 应支持对自然人的关联人信息进行管理，如未成年人的监护人；
l) 应支持对法人单位的关联人信息进行管理，如企业的法定代表人的标识。

5.1.5 身份映射

身份映射应满足以下要求：

a) 应支持身份映射过程中，通过多渠道补全所需身份信息；
b) 应支持基于令牌交换进行身份映射；
c) 应支持身份映射扩展；
d) 应支持通过多种渠道获取身份映射信息；

e） 应支持多身份映射并存，并且身份映射之间相互转化；
f） 应支持身份映射最终对应到用户身份属性、角色，以实现在不同应用内的用户权限管控。

5.2 身份授权服务

5.2.1 授权管理

授权管理应满足以下要求：
a） 应至少支持 MAC、DAC、RBAC、ABAC 等访问控制模型中的一种，宜支持多种访问控制模型；
b） 应支持分级授权管理；
c） 应支持自定义权限；
d） 应支持权限申请审批流程，包括用户发起申请流程，用户管理员代表用户发起审批流程；
e） 应支持动态、多节点审批流程，例如根据申请人角色、属性决定审批人及审批节点；
f） 应支持根据可信数字身份保证级别配置授权策略；
g） 应支持批量授权管理；
h） 应支持对授权管理行为的可追溯及可审计要求。

5.2.2 应用管理

应用管理应满足以下要求：
a） 应支持定义应用系统中的业务组织架构、账号数据模型，匹配目标应用的数据模型；
b） 应支持配置与应用系统的单点登录集成；
c） 应支持从外部数据源，例如文件、数据库、LDAP、Rest API、Webservice 等，导入已有账号数据，将账号关联到实体身份；
d） 应支持调用应用提供的接口服务，实现对应用账号的管理；
e） 应支持配置账号风险的分析策略，提供风险账号分析能力；
注：风险账号包括未关联到任何实体的账号、长期不活动账号、有用户记录但目标应用中实际不存在的账号等；
f） 应支持一个应用账号分配给一人或多人使用，支持设置使用期限，支持到期自动收回使用权限；
g） 应支持查看账号与实体的关联关系；
h） 应支持查看账号登录记录，包括登录的实体、登录时间、登录终端、登录来源 IP 等。

5.2.3 单点登录（SSO）

SSO应满足以下要求：
a） 应支持标准 SSO 协议，包括 OIDC、CAS，SAML，OAuth2.0 等；
b） 应支持应用系统私有 SSO 协议；
c） 应支持 SSO 协议动态扩展；
d） 应支持对 SSO 功能扩展；
e） 应支持同域及跨域 SSO；
f） 应支持 SP 或 IdP 发起的 SSO；
g） 应支持单点登出，并销毁用户会话。

5.3 身份数据服务

5.3.1 数据模型

数据模型应满足以下要求：
a） 应支持属性多对多的对应关系；

b） 应支持灵活定义、变更字段属性；
c） 应支持多数据源融合、扩展；
d） 应支持用户数据模型间的关键属性映射；
e） 应支持数据模型动态扩展；
f） 应支持复杂组织结构数据模型；
g） 应支持用户数据快速查找。

5.3.2 数据同步

数据同步应满足以下要求：
a） 应支持分别从第三方系统推送和拉取数据；
注：第三方系统包括第三方应用厂商提供的应用系统、第三方开发者开发的应用系统等。
b） 应支持与标准数据源组件同步数据的能力；
注：如AD、LDAP等标准数据源组件。
c） 应具备支持通过标准协议同步数据的能力；
注：如SCIM协议等。
d） 应具备配置数据同步策略的能力，支持定时同步、增量同步、全量同步等。

5.4 身份保障服务

5.4.1 流程编排

流程编排应满足以下要求：
a） 应支持通过流程编排调整鉴别逻辑和登录逻辑；
b） 应支持通过流程编排配置鉴别级别变化的触发条件及鉴别方式；
c） 应支持通过流程编排配置注册/登录信息填写、鉴别方式、鉴别步骤；
d） 应支持通过流程编排配置身份信息从产生、加工、使用、销毁全生命周期流转过程中每个节点需实现的逻辑。

5.4.2 审计管理

审计管理应满足以下要求：
a） 应支持记录管理员的操作行为，包括不限于添加用户、修改配置、删除配置等，记录内容包括但不限于主体、客体、时间、行为以及结果；
b） 应支持记录用户的业务操作，包括不限于登录、注册、鉴别等，记录内容包括但不限于主体、时间、行为以及结果；
c） 应支持对于所有审计信息的查询，查询条件包括但不限于主体、时间、行为类型以及结果；
d） 应支持审计信息备份及归档，支持配置备份周期和备份策略，包括但不限于全量、增量；
e） 应支持日志防篡改，支持日志篡改发现及告警。

5.4.3 分权管理

分权管理应满足以下要求：
a） 应支持基于 RBAC 的策略，支持为不同角色设置不同权限；
b） 应支持为角色配置操作权限，包括但不限于查询、添加、修改、删除等；
c） 应支持对用户分组，支持为用户组分配角色；
d） 应支持管理员分组，支持为管理员组分配角色；

e） 应支持配置独立的审计管理员角色。

5.4.4 隐私管理

隐私管理实现用户隐私信息的保护，应满足以下要求：

a） 收集用户身份信息，应在服务界面配置用户协议或隐私政策，明确披露收集个人信息的类型和目的，并征得用户的同意；

b） 通过公共网络传输时，应使用加密通道或数据加密的方式进行传输，保障个人敏感信息传输过程的安全；

c） 应采用加密措施确保个人敏感信息存储的保密性；

d） 收集的用户信息若包含生物识别信息，个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息：

1） 仅存储个人生物识别信息的摘要信息；

2） 在采集终端中直接使用个人生物识别信息实现身份识别、鉴别等功能；

3） 在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、鉴别等功能后删除可提取个人生物识别信息的原始图像。

e） 未经用户授权不应将收集的用户身份信息共享、转让至第三方；

注：法律法规另行规定的除外。

f） 应具备隐私信息查询、更正、删除、脱敏的功能；

g） 应具备日志查询脱敏的功能；

h） 当停止服务时，应对其所持有的个人信息进行删除或匿名化处理；

i） 当使用匿名或假名身份凭证时，应具备技术手段可以确定该身份凭证所对应的实体，以满足监管要求。

5.5 身份开放服务

5.5.1 自助服务

自助服务应满足以下要求：

a） 支持用户自助查看用户信息；

b） 支持用户自助修改用户信息，在修改重要信息前应按照用户对应数字身份保证级别要求，重新进行用户身份鉴别、授权；

c） 支持用户重置登录凭证，在重置前应按照用户对应数字身份保证级别要求，重新进行用户身份鉴别、授权；

d） 支持用户自助完成权限申请；

e） 支持用户自助完成账号注销。

5.5.2 接口服务

接口服务以API、SDK、SaaS等方式为第三方应用厂商、第三方开发者提供服务。

接口服务应提供安全防护能力。

接口服务应满足以下要求：

a） 应提供身份生命周期管理功能；

b） 应提供身份授权服务功能；

c） 应提供身份数据服务功能；

6 性能要求

6.1 概述

可信数字服务提供商应在服务等级协议中明确性能要求。性能要求应包括但不限于可用性、可扩展性、部署兼容等方面。

6.2 可用性要求

可用性应满足以下要求：

a) 应具备7*24小时的连续服务能力；

b) 应支持分布式高可用部署模式；

c) 应用层应具备单台服务器可用即可服务的能力；

d) 数据库集群应具备多数服务节点存活即可服务的力；

e) 缓存集群应具备多数服务节点存活即可服务的能力；

f) 可能影响系统可靠性的支撑系统应提供冗余配置；

g) 应在不短于12个月的连续正常负荷运行过程中，不发生系统响应性能下降、响应能力下降、资源占用显著增加等现象。

6.3 可扩展性要求

可扩展性应满足以下要求：

a) 应支持分布式部署架构与分布式数据存储；

b) 应支持性能线性水平扩展，支持的方式包括但不限于增加物理机、虚拟机、容器等；

c) 应支持模块化的部署结构，支持模块的线性水平扩展；

d) 应支持软硬件平台的扩展性、升级及更新能力。

6.4 部署兼容要求

部署兼容能力应满足以下要求：

a) 应支持标准商业应用服务器与开源应用服务器部署；

b) 应支持主流数据库与开源数据库部署；

c) 应支持单机部署、集群部署、分布式部署等多种模式，方便系统后期升级；

d) 集群及分布式模式下应具备系统负载均衡能力，系统故障时能够无缝切换。

7 安全要求

7.1 业务风险与缓解措施

业务风险与缓解措施要求如下：

a) 应针对身份核验中可能的风险提供缓解措施，可采取下列措施：

1） 可通过权威第三方验证身份证明文件中的身份信息，缓解身份信息伪造的风险；

2） 可要求用户在提交的申请材料中签名，缓解用户抵赖的风险；

3） 可使用安全的渠道交付身份凭证并获得用户的确认，缓解凭证或密钥泄露风险。

b） 应针对身份鉴别中可能的风险提供缓解措施，可采取下列措施：

1） 可在鉴别过程中使用动态鉴别因素或进行加密处理，缓解被窃听风险；

2） 可使用强口令或限制身份鉴别的尝试次数的方法，缓解在线猜测风险；

3） 可提供视觉提示或采用专门设计用来检测网络欺诈攻击的手段，缓解钓鱼攻击风险；

4） 可使用双向鉴别机制，确保通信双方能够确认对方身份，或采用加密会话保护通信安全，缓解中间人攻击风险。

7.2 网络与系统安全要求

网络与系统安全要求应遵循本地的网络安全法律法规和安全标准。

网络与系统安全应满足以下要求：

a） 物理安全应符合业务需要的安全防护等级；

b） 网络安全控制

1） 应配备网络防火墙、过滤路由等设备，以阻止非法访问；

2） 网络上传输的敏感信息应进行加密和完整性保护。

c） 计算机安全运行

1） 服务系统应与其它系统进行隔离，只允许已经定义的应用进程对身份服务系统进行访问；

2） 为保护网络免受现有攻击的威胁，未使用的端口和服务应全部关闭。

d） 存储和传输安全

1） 应对用户的核验、授权信息进行安全存储与管理，禁止明文存储，应存储密文或密码杂凑运算结果；

2） 应对存储数据设置访问控制权限；

3） 应采用安全协议等安全措施保证身份核验、鉴别、数据同步等过程中数据传输安全；

e） 安全监控与应急响应：

1） 应结合外部安全监控系统或第三方安全服务等方式，监测服务的运行状态；

2） 应对异常事件进行告警和处置；

3） 应对安全事件及时响应。

8 应用集成要求

8.1 外部支撑系统集成

8.1.1 权威身份源集成

权威身份源集成应满足以下要求：

a） 应支持通过权威身份源开放的接口获取用户身份相关数据；

b） 应定期对集成的权威身份源的有效性进行验证。

8.1.2 证书服务集成

证书服务集成应满足以下要求：

a) 应支持与PKI/CA数字证书服务进行集成；

b) 应定期对集成的证书服务的有效性进行验证。

8.1.3 密码服务集成

密码服务集成应满足以下要求：

a) 应支持与密码服务进行集成；

b) 应定期对集成的密码服务的有效性进行验证；

c) 应采用技术手段保证数字身份凭证的安全创建、初始化、授权、使用、销毁；

d) 应采用技术手段保证在数字身份生命周期管理的各环节中传输的管理指令、密钥激活材料等敏感信息的机密性、完整性和可用性；

8.2 第三方厂商及开发者集成

8.2.1 身份供应集成

身份供应集成应满足以下要求：

a) 应支持对外标准的数据推送和账号管理接口；

b) 应支持使用接入应用提供的账号管理接口实现账号数据推送和账号管理。

8.2.2 鉴别与 SSO 集成

鉴别与SSO集成应满足以下要求：

a) 支持标准协议集成，包括CAS、OAuth2.0、SAML、OIDC等标准SSO协议；

b) 对于不支持标准SSO协议，应用系统需参考服务集成规范进行集成。

9 互操作性要求

9.1 身份标识的互认互通

不同地域及不同的数字身份提供商可能定义不同的数字身份保证级别，应建立对等互认的唯一映射关系以实现互认互通。可采用如下方式：

a) 可在数字身份标识和可验证身份证明中包含可以唯一确定发放机构的机构实体标识；

b) 可采用SAML标准的数字身份进行身份鉴别的断言。

9.2 信任体系的互认互通

信任体系的互认互通可采用如下方式：

a) 采用合适技术路线实现不同的PKI体系的跨域互认，具体的技术路线包括并不限于：统一根CA、分发信任列表、交叉认证、建立桥CA等；

b) 粤港澳不同区域之间的PKI体系的跨域互认，应遵循《粤港澳电子签名证书互认证书策略v1.0》和《粤港电子签名证书互认证书策略v1.1》；

c) 采用ITU-T X.509标准数字证书格式，并针对特定业务场景规定证书信息项的配置要求；

d) 采用本地认可的密码设备接口规范，如SKF（GB/T 35291—2017）、PKCS#11、CryptoAPI、CNG等；

e) 在身份鉴别阶段可采用OpenID、SAML等开放标准协议。

附 录 A
（资料性）
可信数字身份保证级别服务参考

数字身份服务提供商为实体提供不同保证级别的数字身份服务时，可参考表A.1。

表 A.1 可信数字身份保证级别服务参考

数字身份服务		不同保证级别的安全要素		
		低	中	高
身份生命周期管理服务	身份核验	-身份由用户声明，应包括通信属性； -应对通信属性进行验证； -至少支持在线材料证明。	-身份由用户声明，应至少包括通信属性、法定属性； -应对通信属性进行验证； -应收集法定身份证明文件，并对法定属性进行验证； -至少支持远程身份证明。	-身份由用户声明，应至少包括通信属性、法定属性； -应对通信属性进行验证； -应收集法定身份证明文件，并对法定属性进行验证； -通过与权威第三方核实，对所声明实体的身份信息进行核验； -至少支持远程身份证明，宜支持现场身份证明。
	身份鉴别	-可使用单因素鉴别方式对用户进行身份鉴别；	-宜使用多因素鉴别方式对用户进行身份鉴别；	-应使用多因素鉴别方式对用户进行身份鉴别； -宜根据鉴别场景的环境信息、用户行为等信息进行持续鉴别；
	凭证管理	-鉴别通过后，访问令牌的有效时间最长应不超过30天，超过最长时间应强制进行重新鉴别。	-鉴别通过后，访问令牌的有效时间应不超过7天，超过最长时间应强制进行重新鉴别。	-宜采用硬件形式的鉴别凭证； -鉴别通过后，访问令牌的有效时间应不超过1天，超过最长时间应强制进行重新鉴别。
	身份管理	无特殊要求。	无特殊要求。	无特殊要求。
	身份映射	无特殊要求。	无特殊要求。	无特殊要求。
身份授权服务	授权管理	-应对权限变更申请进行审核、审批。	-应对权限变更申请进行多级审核、审批； -应支持对授权管理行为的可追溯及可审计要求。	-应支持动态、多节点审批流程，例如根据申请人角色、属性决定审批人及审批节点； -应支持对授权管理行为的可追溯及可审计要求。
	应用管理	-可支持实体身份与第三方应用的实体账号数据自动进行关联。	-支持实体身份与第三方应用的实体账号数据自动进行关联前，由管理员进行审批。	-支持实体身份与第三方应用的实体账号数据自动进行关联前，应由管理员进行审批并对外部数据来源的真实性进行验证。
	单点登录	无特殊要求。	无特殊要求。	无特殊要求。

表 A.1（续）

数字身份服务		不同保证级别的安全要素		
		低	中	高
身份数据服务	数据模型	无特殊要求。	无特殊要求。	无特殊要求。
	数据同步	无特殊要求。	无特殊要求。	无特殊要求。
身份保障服务	流程编排	无特殊要求。	无特殊要求。	无特殊要求。
	审计管理	-审计日志的备份周期不长于1个月； -审计信息保存时间不少于3个月； -日志审计周期不长于1个月。	-审计日志的备份周期不长于14天； -审计信息保存时间不少于1年； -日志审计周期不长于7天。	-审计日志的备份周期不长于7天； -审计信息保存时间不少于5年； -日志审计周期不长于1天。
	分权管理	无特殊要求。	无特殊要求。	无特殊要求。
	隐私管理	无特殊要求。	无特殊要求。	无特殊要求。
身份开放服务	自助服务	无特殊要求。	无特殊要求。	无特殊要求。
	接口服务	无特殊要求。	无特殊要求。	无特殊要求。

参 考 文 献

[1] ISO/IEC 29100：2011 Information technology Security techniques Privacy framework

[2] NIST SP 800-63-3 Digital Identity Guidelines

[3] ISO/IEC 24760 IT Security and Privacy — A framework for identity management

[4] NIST SP 800-63-3A Digital Identity Guidelines-Enrollment and Identity Proofing

[5] NIST SP 800-63-B Digital Identity Guidelines-Authentication and Lifecycle Management

[6] NIST SP 800-63-3C Digital Identity Guidelines-Federation and Assertions

[7] Personal Data (Privacy) Ordinance （Cap. 486）《个人资料（隐私）条例》（第486章）

[8] Personal Data Protection Act (Act 8/2005) 《个人资料保护法（第 8/2005 号法令）》

[9] European Interoperability Reference Architecture (EIRA) [OL]. [2021-07-02]. https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/eira/

[10] European Commission. eIDAS SAML Attribute Profile Version v1.2 [OL]. [2019-08-31]. https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf

[12] 香港政府资讯科技总监办公室. 粤港两地电子签名证书互认办法. 粤港电子签名证书互认证书策略. [OL]. https://www.ogcio.gov.hk/sc/our_work/business/mainland/cepa/mr_ecert/