ICS 35.240.99
L67

ZWFW

国家政务服务平台标准

C 0131-2018

国家政务服务平台
统一身份认证隐私保护要求

2018-12-28 发布　　2018-12-28 实施

国务院办公厅电子政务办公室 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。

本标准由国务院办公厅电子政务办公室提出并归口。

本标准起草单位：国务院办公厅电子政务办公室、浙江省人民政府办公厅、广东省人民政府办公厅、江西省人民政府办公厅、四川省人民政府办公厅、南京市政务服务管理办公室、中国电子技术标准化研究院。

本标准主要起草人：卢向东、尹智刚、陈治佳、马运领、王齐春、孔令军、徐云、李景曦、王赟萃、李松渊、孙杨、张军、钱学文、李恒训、赵菁华、王立建。

国家政务服务平台统一身份认证隐私保护要求

1 范围

本标准规定了国家政务服务平台统一身份认证隐私数据定级、隐私数据判定、隐私数据使用和隐私数据责任。

本标准适用于国家政务服务平台统一身份认证国家节点、地方和部门节点。

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。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/Z 24294-2009 信息安全技术 基于互联网电子政务信息安全实施指南

GB/T 31072-2014 科技平台 统一身份认证

GB/T 32907-2016 信息安全技术 SM4 分组密码算法

GB/T 32918（所有部分） 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35273-2017 信息安全技术 个人信息安全规范

GM/T 0051-2016 密码设备管理 对称密钥管理技术规范

C 0111-2018 国家政务服务平台统一身份认证系统身份认证技术要求

C 0113-2018 国家政务服务平台统一信任服务平台接口要求

中华人民共和国网络安全法

国办函〔2016〕108 号 国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知

3 术语和定义

GB/T 22239、GB/Z 24294-2009、GB/T 31072-2014、GB/T 32907-2016、GB/T 32918（所有部分）、GB/T 35273-2017、C 0111-2018 界定的以下术语和定义适用于本文件。

3.1

隐私数据 privacy data

统一身份认证系统内自然人个人信息中涉及用户敏感信息的数据。

3.2

用户标识 user id

用户个人信息中的证件号码等唯一识别码形成的散列值。在统一身份认证系统中唯一。

4 隐私数据定级

4.1 一级数据

不能对应到自然人实体身份信息的数据。

4.2 二级数据

可用于标识自然人实体的身份信息，且较公开的数据。如登录账号、姓名、手机号等，统一身份认证隐私数据定级见附录 A。

4.3 三级数据

可用于标识自然人实体的身份信息,且具有较高隐私性的数据。如证件编号、户籍地址、工作单位等，统一身份认证隐私数据定级见附录 A。

5 隐私数据判定

统一身份认证系统内自然人信息中隐私数据定级见附录 A，未满 14 岁的儿童，可提升数据隐私级别，除身份模型所规定的内容，下列信息也属于隐私数据：

a) 生物特征数据
   1) 人脸数据、声纹数据等较为公开的生物特征数据，属于二级数据；
   2) 指纹数据等作为可认定个人信息的生物特征数据，属于三级数据。
b) 访问记录。个人用户在统一身份认证体系中的登录记录、政务门户访问记录等信息，属于二级数据。

6 隐私数据使用

6.1 隐私数据基本原则

各节点应严格执行《中华人民共和国网络安全法》和 GB/T 35273-2017 中所列的基本原则，坚持最小化原则，涉及隐私数据的收集和使用应符合业务需要，明确责权，贯彻知情原则。

6.2 隐私数据收集

国家节点与地方和部门节点应按 C 0111-2018 第 7 章约定的用户信息模型范围收集用户信息。

各节点应对用户提供隐私保障协议，在用户注册时明示数据收集信息，并由用户明确确认。协议见 GB/T 35273-2017 和国办函〔2016〕108 号中所列模板。

地方和部门节点可通过向国家节点进行个人信息查询获得个人信息。地方和部门应优先查询并使用国家节点已经存在的个人信息，禁止重复收集用户个人信息。仅当国家节点无此用户信息时才可进行收集。

地方和部门节点应尽量使用国家政务服务平台统一身份认证系统已有数据。各节点所收集的数据，由各节点自行负责安全。

国家节点可通过以下方式收集个人信息：

a) 用户注册与修改；
b) 地方和部门节点上传。

6.3 隐私数据保存

各级节点必须遵循 GB/T 22239、GB/T 352732017 和以下原则进行隐私数据保存：

a) 一级隐私数据。不作特殊要求，按照通国家有关安全原则及 GB/T 22239、GB/T 35273-2017 执行；
b) 二级隐私数据。应以加密方式存储二级隐私数据；
c) 三级隐私数据。互联网区内三级隐私数据应以不可逆加密方式存储，不得以明文或可逆加密方式进行存储。不可逆加密方法应采用国家节点统一提供的散列函数对明文进行散列运算。三级隐私数据在电子政务外网中应以加密方式存储；
d) 加密密钥。密钥必须存放于符合 GM/T 0051-2016 的系统或设备中。密钥由专人管理。密钥管理人员不得从事数据操作、加工、使用等工作。密钥管理人员应是本节点正式工作人员，不得来自软件开发商、服务商等第三方机构。加密密钥使用 SM2、SM4 算法。

6.4 隐私数据使用

隐私数据在统一身份认证系统中的使用应遵循以下原则：

a) 个人信息显示：
   1) 二级以上隐私数据在以下情况允许全文显示：
      --用户注册时填写的内容，允许全文显示；
      --用户查看和修改个人信息时，应在二次认证后允许全文显示。二次认证级别不低于包括手机短信验证码的双因子认证；修改信息宜使用实名等级四级（实人认证）进行认证。
   2) 除以上情况，系统中默认应脱敏显示二级以上隐私数据。除手机号码外，二级以上隐私数据脱敏范围应不少于 50%，示例如下：
      --姓名脱敏显示：**明。显示姓名的最后 1-2 个汉字；
      --公民身份号码和社保卡号脱敏显示：**********4432。显示最后四位，其他隐藏；
      --手机号码脱敏显示：133****4387。显示前 3 位和后 4 位，其他隐藏；
      --证件有效日期和证件失效日期脱敏显示:****0421。显示后 4 位,其他隐藏；
      --用户邮箱脱敏显示：*********@163.com。显示“@”及之后部分，其他隐藏；
      --用户支付宝号和用户微信号期脱敏显示:****0403。显示后 4 位,其他隐藏；
      --用户户籍地址、用户居住地址、用户工作单位和发卡地脱敏显示：北京市海淀区********。长度大于 12 时,只显示前 6 位，不足 12 位显示不超过 50%，其他隐藏。
b) 以下情况，允许在互联网区临时使用未加密数据：
   1) 互联网区可临时获取用户个人信息用于提交实名核验的未加密数据，禁止使用超过实名核验需要的其他数据，使用后应在系统中销毁。一次实名核验只允许获取一条个人信息，实名核验完成后，应销毁该临时数据；
   2) 用户注册信息上报。允许地方和部门节点将本地注册用户信息临时保存到互联网区，总数不得超过 1000 条，时间不超过 24h。地方和部门节点应在此限定下及时上报到国家节点，上报时以明文数据上报全量数据。上报完成后销毁互联网区明文数据。国家节点收到上报数据后可在互联网区临时保存不超过 8h，完成处理后销毁互联网区明文数据；
   3) 用户信息查询。地方和部门节点可向国家节点通过用户标识查询指定用户所对应的个人信息。查询结果以明文数据下发。查询发起节点应在收到信息 2h

内完成处理，并销毁互联网内的明文数据；查询接口只允许接收和输出一个用户的个人信息，不得存在一次查询多个用户的服务；

4) 通讯安全。所有涉及未加密个人信息数据的传输，按C 0111-2018的8.3、C 0113-2018第7章中安全通讯的规定进行通讯传输。互联网、电子政务外网传输均应按此处理。

c) 用户个人信息除本人或获得用户本人正式授权外，其他人员不得查询和修改。

6.5 数据加工

统一身份认证系统内所有节点禁止以两个或两个以上用户的个人信息进行关联分析，包括以散列值进行分析。除以下情况以外，禁止对用户个人数据中的二级隐私数据和三级隐私数据进行数据加工。

a) 对个人信息通过脱敏、散列化处理等方式进行安全加强；

b) 用户对政务服务门户、政务服务业务系统的访问记录只用于异常登录等安全分析和异常处置，禁止用于其他用途；

c) 允许对个人信息的散列值进行加工。

6.6 隐私数据共享与披露

禁止各级节点对用户数据进行公开披露、转让和共享用户个人数据。

6.7 隐私数据导出与输出

统一身份认证系统各节点应制定数据导出管理制度，明确二级隐私数据和三级隐私数据对少量导出、批量导出、大批量导出的定级定义及相应的管理流程，明确相关责任人，数据导出记录至少保存一年。

数据导出过程应详细进行记录，记录至少包括以下信息：

a) 数据导出用途、时间、操作地点、人员、授权信息等；

d) 导出文件大小、数据数量，所有个人信息的标识（散列值）。

6.8 数据归档与销毁

统一身份认证系统中，数据超出使用时限或完成生命周期后，应归档或销毁。归档后形成离线文档，不可在线查询、获取。

数据销毁应采用不可恢复方式，保证不可从存储介质中恢复。应保证销毁后不存在内存残留、缓存、临时文件、临时库表等剩余信息。

6.9 其他

隐私数据的收集、使用、加工、输出等各个环节均应记录日志。日志保存时间应不少于1年，并在超出时效后及时归档。

7 隐私数据责任

统一身份认证体系各节点应对本系统内收集、存储、使用的用户信息负责。用户数据在系统内被篡改或丢失，由系统所在节点通过权威机构技术鉴定或查实确定责任。

各节点应具备技术保障机制和管理流程，保证用户信息不被泄露。一旦发生泄露，则视

泄露数据的隐私级别进行上报处置。

8 其他

8.1 组织与管理

各级节点按 GB/T 35273—2017 中所列各项要求，建立健全管理组织和相关制度流程，保证数据安全。

8.2 检查检测

国家节点按本要求对各节点组织定期或不定期检查。不符合本要求的节点将暂停接入服务并限期整改。

附 录 A
（规范性附录）
自然人身份信息隐私判定说明

表 A.1 规定了自然人身份信息隐私数据级别定级。

表 A.1 自然人身份信息隐私判定表

信息	隐私级别
自然人姓名	二级数据
自然人登录账号	二级数据
自然人证件类型	一级数据
自然人证件编号	三级数据
证件散列码	一级数据
自然人手机号	二级数据
自然人实名等级	一级数据
证件有效日期	二级数据
证件失效日期	二级数据
自然人实名核验日期	一级数据
社保卡号	三级数据
发卡地	二级数据
用户邮箱	二级数据
注册时间	二级数据
用户生日	二级数据
用户性别	一级数据
用户学历	二级数据
用户支付宝号	二级数据
用户微信号	二级数据
用户户籍地址	三级数据
用户居住地址	三级数据
用户工作单位	二级数据
用户类型	一级数据
用户民族	一级数据
用户国籍	一级数据
用户第二手机号	二级数据
用户第三手机号	二级数据