ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0117—2022

网络身份服务密码应用技术要求

Technical requirements for cryptographic applications of identity service in network

2022-11-20 发布　　2023-06-01 实施

国家密码管理局　　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。

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。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、中国科学院软件研究所、中国科学院信息工程研究所、公安部第一研究所、中国电子技术标准化研究院、支付宝（中国）网络技术有限公司、联想（北京）有限公司、国民认证科技（北京）有限公司、北京中盾安信科技发展有限公司、北京天融信网络安全技术有限公司、兴唐通信科技有限公司、广州大学。

本文件主要起草人：李敏、高能、马存庆、彭佳、屠晨阳、林雪焰、邵淼、傅大鹏、夏鲁宁、刘中、张立武、张严、欧阳晖、郝春亮、落红卫、王昕、柴海新、李俊、王开林、景鸿理、蔡子凡、徐光侠。

网络身份服务密码应用技术要求

1 范围

本文件规定了面向自然人的网络身份服务的密码应用技术要求，给出了网络身份服务模型、网络身份服务安全级别、密码应用需求框架和密码应用安全目标，针对身份核验服务、身份鉴别服务和身份联合服务给出了具体的密码应用技术要求。

本文件适用于面向自然人的网络身份服务中密码应用的规划、设计、开发、部署和应用。

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 15843(所有部分) 信息技术 安全技术 实体鉴别

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37036(所有部分) 信息技术 移动设备生物特征识别

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38556 信息安全技术 动态口令密码应用技术规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 40660 信息安全技术 生物特征识别信息保护基本要求

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

身份服务提供方 identity service provider

在网络中提供身份服务的实体。

3.2

用户 user

使用网络身份服务的自然人。

注：申请方、声称方、订户代表了用户在不同场景下的不同角色。

3.3

依赖方 relying party

依赖身份鉴别结果以确定是否与用户建立信任关系的实体。

3.4

身份核验 identity proofing

收集用户身份信息，并验证用户身份信息的真实性的过程。

3.5

身份鉴别　identity authentication

验证用户所声称身份的过程。

3.6

身份联合　identity federation

依赖不在同一个安全域的身份服务提供方给出用户身份鉴别结果的过程。

3.7

网络身份服务　identity service provider

在网络中为用户提供身份核验、身份鉴别和身份联合服务的活动。

3.8

订户　subscriber

接受身份服务提供方提供的身份服务的合法用户。

3.9

申请方　applicant

请求成为订户的自然人。

3.10

声称方　claimant

宣称自己是订户的自然人。

[来源:GB/T 25069—2022,3.535,有修改]

3.11

用户标识　user identification

用于标识用户的一种字符串或模式。

[来源:GB/T 25069—2022,3.734,有修改]

3.12

远程递交材料身份核验　remote identity proofing

申请方通过在线或离线方式非现场提供身份证明材料进行身份核验的过程。

3.13

本人远程身份核验　in-person over remote channel identity proofing

申请方通过在线方式并亲自操作进行身份核验的过程。

示例:通过视频方式实时验证。

3.14

本人现场身份核验　in-person identity proofing

申请方通过亲自到现场的方式进行身份核验的过程。

3.15

鉴别器　authenticator

用户拥有或掌握的可用于鉴别其身份的功能组件或方法。

注:鉴别器包含实体凭证或凭证生成方法,参与并执行特定的鉴别协议。

3.16

声明　claim

在不给出证据的情况下所做的宣称或说明。

3.17

断言　assertion

身份服务提供方生成的对用户身份鉴别的结果。

注：包括断言主体(被鉴别身份的用户标识符)、断言发放者、断言接收者、签发时间等信息，也可包含用户属性信息等，表明了声称方为订户。

3.18

断言引用　assertion reference

和断言关联的，包含身份服务提供方标识的数据对象。

[来源：GB/T 36633—2018，3.9，有修改]

3.19

持有型断言　bearer assertion

可将断言的持有者看作断言主体的断言类型。

注：不能保证断言的持有者就是断言中的主体。

3.20

密钥拥有型断言　holder-of-key assertion

可通过断言持有者拥有的密钥证明其为断言主体的断言类型。

3.21

网络身份服务系统　identity service system in network

支撑网络身份服务的软硬件集合。

4　缩略语

下列缩略语适用于本文件。

OTP：一次性口令(One Time Password)

5　概述

5.1　网络身份服务模型

网络身份服务模型见图1。本文件定义网络身份服务分为身份核验服务、身份鉴别服务、身份联合服务三类。

a）　身份核验服务，流程如下：

1）　申请方提交身份信息和身份证明文件，进行登记；

2）　身份服务提供方核验身份信息和身份证明文件，核验通过后，向申请方颁发鉴别器，申请方获得身份成为身份服务提供方的订户。

b）　身份鉴别服务，流程如下：

1）　通过鉴别协议，使用鉴别器证明声称方是绑定到特定鉴别器的订户；

2）　对声称方进行身份鉴别，身份鉴别成功后，确认该声称方为订户。

c）　身份联合服务，发生在依赖方与身份服务提供方在不同安全域的情形，身份服务提供方对声称方进行身份鉴别后，将有关身份鉴别结果的断言或断言引用返回给依赖方，流程如下：

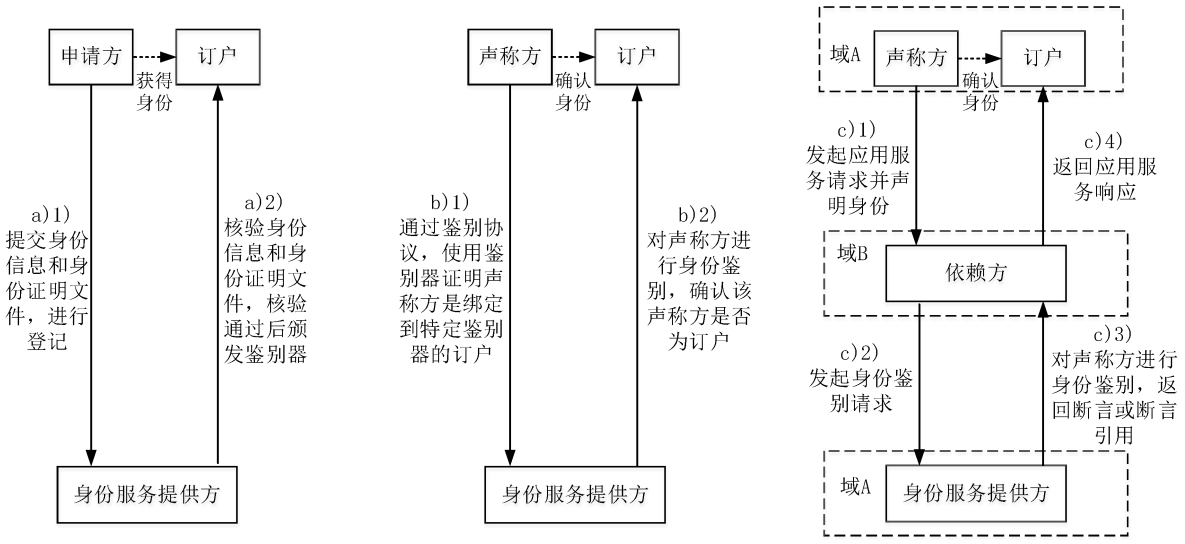
1）　声称方向依赖方发起应用服务请求并声明身份；

2）　依赖方向不同域的身份服务提供方发起身份鉴别请求；

3）　身份服务提供方对声称方进行身份鉴别，向依赖方返回断言或断言引用，声称方身份得到确认；

4）　依赖方向订户返回应用服务响应。

一般情况下，身份服务提供方同时提供身份核验服务和身份鉴别服务，可提供身份联合服务。



a） 身份核验服务　　b） 身份鉴别服务　　c） 身份联合服务

图 1　网络身份服务模型

5.2　网络身份服务安全级别

本文件分别针对身份核验服务、身份鉴别服务、身份联合服务三类网络身份服务规定了四个要求逐级递增的安全级别，高安全级别在低安全级别的基础上进一步提出了更高的安全要求。身份核验服务、身份鉴别服务、身份联合服务中各安全级别要求简要概述如下。

a） 身份核验服务

1） 第一级，阐明了身份核验服务最低级别的安全要求：

- 唯一性：身份在特定语境中是唯一的；
- 收集属性类别：收集的用户属性能够唯一标识用户。

2） 第二级，在第一级的基础上主要增加了收集属性类别、实名核验、远程递交材料身份核验等方面的要求：

- 收集属性类别：收集的用户属性能与现实世界的自然人唯一关联，且拥有联系方式；
- 是否实名：对用户实名核验；
- 核验方法：核验收集的身份属性的真实性，至少采用远程递交材料身份核验等方式进行核验。

3） 第三级，在第二级的基础上主要增加了环境属性等属性收集要求、本人远程身份核验等方面的要求：

- 收集属性类别：在第二级的基础上要求收集用户登录环境信息，根据业务需求收集必要的经济属性、社会属性；
- 核验方法：核验收集的身份属性的真实性，至少采用本人远程身份核验或本人现场身份核验的方式进行核验。

4） 第四级，阐明了身份核验最高级别的安全要求，在第三级的基础上主要增加了收集属性类别、身份证明文件的数量要求、本人现场身份核验等方面的要求：

- 收集属性类别：在第三级的基础上建议收集生物特征属性、行为属性等更多种类的身份属性；
- 核验方法：相较于第三级要求核验更多数量的权威来源身份证明文件，至少采用本人现场身份核验的方式进行核验。

b) 身份鉴别服务

1) 第一级，阐明了身份鉴别服务最低级别的安全要求，支持使用单因素鉴别方式来证明声称方是绑定到特定鉴别器的订户。

2) 第二级，在第一级的基础上要求使用多因素鉴别方式。

3) 第三级，在第二级的基础上增加了对鉴别器中密码技术使用要求、动态鉴别要求。

- 鉴别因素：要求多因素鉴别方式中至少使用密码软件鉴别器或密码设备鉴别器来实现；
- 动态鉴别：具备基于网络环境的风险控制措施。

4) 第四级，阐明了身份鉴别最高级别的安全要求，相较于第三级，要求至少使用密码设备鉴别器，且提高了动态鉴别要求：

- 鉴别因素：要求多因素鉴别方式中至少使用密码设备鉴别器来实现；
- 动态鉴别：具备基于网络环境的风险控制措施，建议具备基于用户行为的风险控制措施。

c) 身份联合服务

1) 第一级，阐明了身份联合服务最低级别的安全要求：

- 断言签名：身份服务提供方到依赖方的断言由身份服务提供方进行签名；
- 断言类型：允许使用持有型断言或密钥拥有型断言。

2) 第二级，在第一级的基础上主要增加了断言加密要求。

3) 第三级，在第二级的基础上主要提高了断言类型要求、断言主体假名化要求：

- 断言类型：要求使用密钥拥有型断言；
- 断言主体假名化：建议断言主体假名化，依赖方和身份服务提供方可协商确定对不同的依赖方是否使用不同的用户假名。

4) 第四级，阐明了身份联合最高级别的安全要求，在第三级的基础上主要提高断言假名化要求，要求断言主体假名化，对不同的依赖方生成不同的用户假名。

5.3 密码应用需求框架

网络身份服务密码应用需求框架如图 2 所示。本文件聚焦身份核验服务、身份鉴别服务、身份联合服务中第一级到第四级的密码应用需求，针对身份核验服务，从通用要求、身份核验、通信保护、记录和存储、风险缓解、系统安全保护等六个方面安全需求展开，对应的具体密码应用技术要求见 7.1、7.2；针对身份鉴别服务，从通用要求、鉴别方式、鉴别协议、鉴别器生命周期管理、会话管理、通信保护等九个方面安全需求展开，对应的具体密码应用技术要求见 7.1、7.3；针对身份联合服务，从通用要求、身份联合互鉴别、断言内容、断言类型、断言签名、断言加密等十一个方面安全需求展开，对应的具体密码应用技术要求见 7.1、7.4。

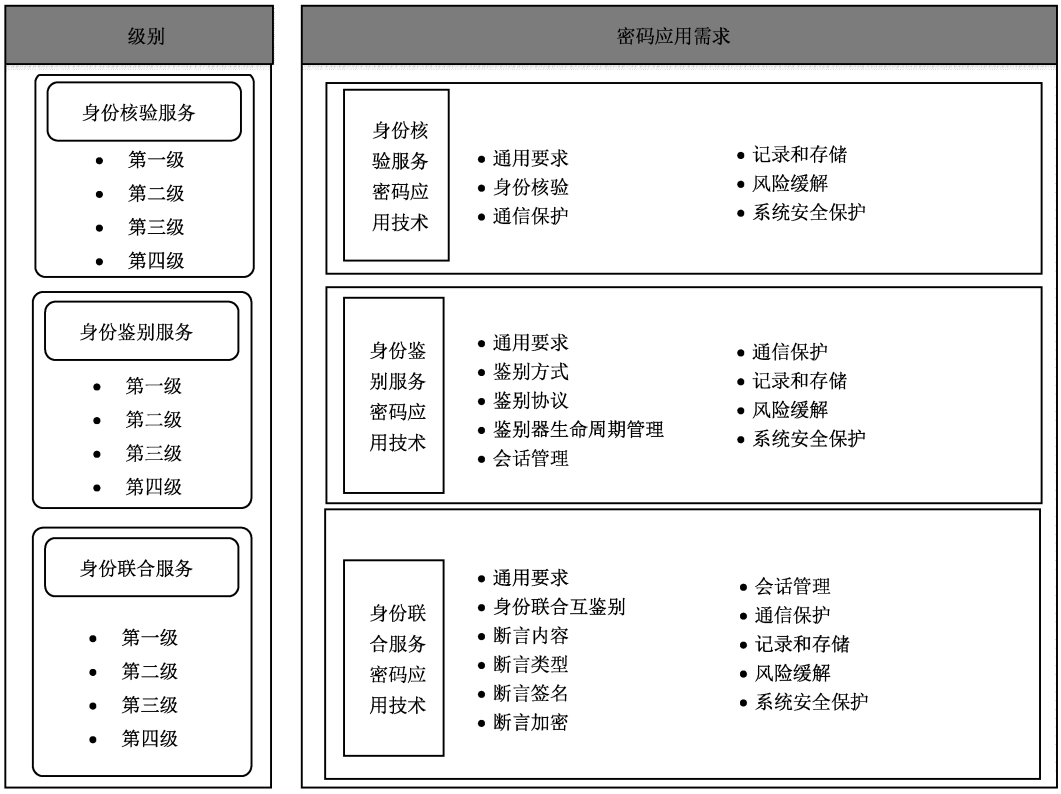


图 2　网络身份服务密码应用需求框架

6　网络身份服务密码应用安全目标

6.1　概述

网络身份服务密码应用安全目标主要是保障身份核验服务、身份鉴别服务、身份联合服务三种网络身份服务中数据的机密性、完整性、真实性以及不可否认性。

6.2　机密性

网络身份服务中的重要的数据(如身份鉴别信息、敏感个人信息、鉴别器的密钥等)在收集、存储、使用、传输等过程中不被非授权实体获取从而被利用或者泄露。使用加密、解密技术等实现机密性。

6.3　完整性

网络身份服务中的重要的数据(如身份鉴别信息、敏感个人信息、鉴别器的密钥等)在收集、存储、使用、传输等过程中不被非授权修改与破坏。使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性。

6.4　真实性

网络身份服务中确认参与实体的身份的真实性,防止身份被占用或假冒。使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制、动态口令机制等密码技术实现真实性。

6.5 不可否认性

网络身份服务中参与方实体不能否认其在网络身份服务中的数据原发行为和数据接收行为。使用基于公钥密码算法的数字签名机制等密码技术实现不可否认性。

7 网络身份服务密码应用技术要求

7.1 通用要求

身份核验服务、身份鉴别服务、身份联合服务中，第一级到第四级应符合以下通用要求：

a) 网络身份服务使用的密码算法、密码技术、密码产品和密码服务应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求；

b) 个人信息的收集、存储、使用、委托处理、共享、转让、公开披露、个人信息安全事件处置应符合GB/T 35273的规定，生物特征识别信息保护要求应符合GB/T 40660的规定。

7.2 身份核验服务要求

7.2.1 第一级

第一级要求如下。

a) 身份核验要求：不要求实名，可使用匿名、假名或实名。

b) 通信保护要求：可采用密码技术保证通信过程数据的完整性，可采用密码技术保证通信过程重要的数据的机密性，可采用密码技术对通信实体进行鉴别。

c) 记录和存储要求：

1) 身份服务提供方应对身份核验服务的必要信息进行记录和存储，包括但不限于：收集的用户身份信息和身份证明文件、身份核验产生的过程信息、核验结果等数据；

2) 可采用密码技术保证重要的数据存储的机密性和完整性。

d) 风险缓解要求：可能面临的风险见附录A中的A.1，可使用密码技术缓解可能存在的风险。

e) 系统安全保护要求：网络身份服务系统应至少符合GB/T 22239规定的第一级安全要求，应至少符合GB/T 39786规定的第一级密码应用技术要求。

7.2.2 第二级

第二级要求如下。

a) 身份核验要求：应采用远程递交材料身份核验、本人远程身份核验、本人现场身份核验中的任一种方式对用户身份进行核验，应进行实名核验。

b) 通信保护要求：可采用密码技术保证通信过程数据的完整性，宜采用密码技术保证通信过程重要的数据（例如公民身份号码、住址、重要证件扫描件等）的机密性，宜采用密码技术对通信实体进行鉴别。

c) 记录和存储要求：

1) 身份服务提供方应对身份核验服务的必要信息进行记录和存储，包括但不限于：收集的用户身份信息和身份证明文件、身份核验产生的过程信息、核验结果等数据；

2) 宜采用密码技术保证重要的数据存储的机密性和完整性。

d) 风险缓解要求：可能面临的风险见A.1，宜使用密码技术缓解可能存在的风险。

e) 系统安全保护要求：网络身份服务系统应至少符合GB/T 22239规定的第一级安全要求，应至少符合GB/T 39786规定的第一级密码应用技术要求。

7.2.3 第三级

第三级要求如下。

a) 身份核验要求：应采用本人远程身份核验或本人现场身份核验对用户身份进行核验，应进行实名核验。

b) 通信保护要求：宜采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要的数据（例如公民身份号码、住址、重要证件扫描件等）的机密性，应采用密码技术对通信实体进行鉴别。

c) 记录和存储要求如下：

1) 身份服务提供方应对身份核验服务的必要信息进行记录和存储，包括但不限于：收集的用户身份信息和身份证明文件、身份核验产生的过程信息、核验结果等数据；

2) 宜采用密码技术保证重要的数据存储的完整性，应采用密码技术保证重要的数据存储的机密性。

d) 风险缓解要求：可能面临的风险见 A.1，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

e) 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第二级安全要求，应至少符合 GB/T 39786 规定的第二级密码应用技术要求。

7.2.4 第四级

第四级要求如下。

a) 身份核验要求：应采用本人现场身份核验方式对用户身份进行核验，应进行实名核验。

b) 通信保护要求：应采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要的数据（例如公民身份号码、住址、重要证件扫描件等）的机密性，应采用密码技术对通信实体进行双向鉴别。

c) 记录和存储要求：

1) 身份服务提供方应对身份核验服务的必要信息进行记录和存储，包括但不限于：收集的用户身份信息和身份证明文件、身份核验产生的过程信息、核验结果等数据；

2) 应采用密码技术保证重要的数据存储的完整性和机密性。

d) 风险缓解要求：可能面临的风险见 A.1，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

e) 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第三级安全要求，应至少符合 GB/T 39786 规定的第三级密码应用技术要求。

7.3 身份鉴别服务要求

7.3.1 第一级

第一级要求如下。

a) 鉴别方式要求：应至少支持单因素鉴别方式，可使用任意一种类型的鉴别器进行身份鉴别（鉴别器类型和鉴别方式见附录 B）。

b) 鉴别协议要求：

1) 应采用动态信息（如随机数、挑战码）、时间戳等方式以防重放攻击；

2) 使用密码技术进行身份鉴别时，应符合 GB/T 15843（所有部分）的规定；

3) 应限制一定时间内身份鉴别的尝试次数，例如，一分钟之内的尝试次数不高于 5 次；

4） 移动设备生物特征识别要求应符合 GB/T 37036(所有部分)的规定；

5） 若鉴别中涉及动态口令，动态口令密码应用技术要求应符合 GB/T 38556 的规定。

c） 鉴别器生命周期管理要求：

1） 鉴别器绑定：可为用户身份绑定两种或两种以上类型的鉴别器(鉴别器类型和鉴别方式见附录 B)；

2） 鉴别器更新要求：应在现有鉴别器到期前一段合适的时间要求用户更新鉴别器；应与初始鉴别器颁发程序保持一致；更新成功后，应撤销被替代的鉴别器；

3） 鉴别器失窃、损坏和复制要求：应采取安全措施防止鉴别器中的秘密信息被提取；应支持鉴别器的挂起和重新激活；应支持对用户身份进行重新核验，并绑定新的鉴别器；

4） 鉴别器到期要求：到期的鉴别器不应再用于身份鉴别；当用户使用到期的鉴别器时，应告知鉴别器已到期；应对到期的鉴别器进行合理处置；

5） 鉴别器撤销要求：定期检查身份是否存在、身份是否满足资格要求、鉴别器风险状态等信息，当身份不存在，或用户提出撤销请求，或确定身份不再满足资格要求时，或鉴别器更新后，应及时撤销与该身份绑定的鉴别器；撤销的鉴别器不应再用于身份鉴别；当鉴别器被撤销时，应对鉴别器进行合理处置，如回收后销毁、彻底清除鉴别器相关数据等。

d） 会话管理要求：身份鉴别成功后身份服务提供方和用户之间可使用密码技术建立安全的会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证对生成的会话相关秘密信息的安全存储和使用。

e） 通信保护要求：可采用密码技术保证通信过程数据的完整性、重要数据的机密性，可采用密码技术对通信实体进行鉴别。

f） 记录和存储要求：

1） 身份服务提供方应对身份鉴别的必要信息进行记录和存储，包括但不限于：使用的身份鉴别协议、身份鉴别方法、鉴别器相关数据及身份鉴别产生的过程信息、鉴别结果等数据；

2） 可采用密码技术保证重要的数据存储的机密性和完整性。

g） 风险缓解要求：可能面临的风险见 A.2，可使用密码技术缓解可能存在的风险。

h） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第一级安全要求，应至少符合 GB/T 39786 规定的第一级密码应用技术要求。

7.3.2 第二级

第二级要求如下。

a） 鉴别方式要求：应使用多因素鉴别方式，不应将生物特征鉴别器作为唯一可选的多因素鉴别方式，以避免强制个人同意收集其生物特征信息(鉴别器类型和鉴别方式见附录 B)。

b） 鉴别协议要求：

1） 应采用动态信息(如随机数、挑战码)、时间戳等方式以防重放攻击；

2） 宜使用密码技术进行身份鉴别，使用密码技术进行身份鉴别时，应符合 GB/T 15843(所有部分)的规定；

3） 应限制一定时间内身份鉴别的尝试次数，例如，一分钟之内的尝试次数不高于 5 次；

4） 若使用生物特征进行鉴别时，移动设备生物特征识别要求应符合 GB/T 37036(所有部分)的规定；

5） 若鉴别中涉及动态口令，动态口令密码应用技术要求应符合 GB/T 38556 的规定。

c） 鉴别器生命周期管理要求：

1） 鉴别器绑定：宜为用户身份绑定两种或两种以上类型的鉴别器(鉴别器类型和鉴别方式见附录 B)；

2） 鉴别器更新要求：应在现有鉴别器到期前一段合适的时间要求用户更新鉴别器；应与初始鉴别器颁发程序保持一致；更新成功后，应撤销被替代的鉴别器；

3） 鉴别器失窃、损坏和复制要求：应采取安全措施防止鉴别器中的秘密信息被提取；应支持鉴别器的挂起和重新激活；应支持对用户身份进行重新核验，并绑定新的鉴别器；

4） 鉴别器到期要求：到期的鉴别器不应再用于身份鉴别；当用户使用到期的鉴别器时，应告知鉴别器已到期；应对到期的鉴别器进行合理处置；

5） 鉴别器撤销要求：定期检查身份是否存在、身份是否满足资格要求、鉴别器风险状态等信息，当身份不存在，或用户提出撤销请求，或确定身份不再满足资格要求时，或鉴别器更新后，应及时撤销与该身份绑定的鉴别器；撤销的鉴别器不应再用于身份鉴别；当鉴别器被撤销时，应对鉴别器进行合理处置，如回收后销毁、彻底清除鉴别器相关数据等。

d） 会话管理要求：身份鉴别成功后身份服务提供方和用户之间可使用密码技术建立安全的会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证对生成的会话相关秘密信息的安全存储和使用。

e） 通信保护要求：可采用密码技术保证通信过程数据的完整性，宜采用密码技术保证通信过程重要数据的机密性，宜采用密码技术对通信实体进行鉴别。

f） 记录和存储要求：

1） 身份服务提供方应对身份鉴别的必要信息进行记录和存储，包括但不限于：使用的身份鉴别协议、身份鉴别方法、鉴别器相关数据及身份鉴别产生的过程信息、鉴别结果等数据；

2） 宜采用密码技术保证重要的数据存储的机密性和完整性。

g） 风险缓解要求：可能面临的风险见 A.2，宜使用密码技术缓解可能存在的风险。

h） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第一级安全要求，应至少符合 GB/T 39786 规定的第一级密码应用技术要求。

7.3.3 第三级

第三级要求如下。

a） 鉴别方式要求：应使用多因素鉴别方式，其中一种鉴别因素至少使用密码软件鉴别器或密码设备鉴别器来实现，且所采用的密码模块应达到 GB/T 37092 二级及以上安全要求。

b） 鉴别协议要求如下：

1） 应采用动态信息（如随机数、挑战码）、时间戳等方式以防重放攻击；

2） 应使用密码技术进行身份鉴别，并符合 GB/T 15843（所有部分）的规定；

3） 应限制一定时间内身份鉴别的尝试次数，例如，一分钟之内的尝试次数不高于 5 次；

4） 若使用生物特征进行鉴别时，移动设备生物特征识别要求应符合 GB/T 37036（所有部分）的规定；

5） 若鉴别中涉及动态口令，动态口令密码应用技术要求应符合 GB/T 38556 的规定。

c） 鉴别器生命周期管理要求：

1） 鉴别器绑定：宜为用户身份绑定两种或两种以上类型的鉴别器（鉴别器类型和鉴别方式见附录 B）；

2） 鉴别器更新要求：应在现有鉴别器到期前一段合适的时间要求用户更新鉴别器；应与初始鉴别器颁发程序保持一致；更新成功后，应撤销被替代的鉴别器；

3） 鉴别器失窃、损坏和复制要求：应采取安全措施防止鉴别器中的秘密信息被提取；应支持鉴别器的挂起和重新激活；应支持对用户身份进行重新核验，并绑定新的鉴别器；

4） 鉴别器到期要求：到期的鉴别器不应再用于身份鉴别；当用户使用到期的鉴别器时，应告知鉴别器已到期；应对到期的鉴别器进行合理处置；

5） 鉴别器撤销要求：定期检查身份是否存在、身份是否满足资格要求、鉴别器风险状态等信息，当身份不存在，或用户提出撤销请求，或确定身份不再满足资格要求时，或鉴别器更新后，应及时撤销与该身份绑定的鉴别器；撤销的鉴别器不应再用于身份鉴别；当鉴别器被撤销时，应对鉴别器进行合理处置，如回收后销毁、彻底清除鉴别器相关数据等。

d） 会话管理要求：身份鉴别成功后身份服务提供方和用户之间可使用密码技术建立安全的会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证对生成的会话相关秘密信息的安全存储和使用。

e） 通信保护要求：宜采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要数据的机密性，应采用密码技术对通信实体进行鉴别。

f） 记录和存储要求如下：

1） 身份服务提供方应对身份鉴别的必要信息进行记录和存储，包括但不限于：使用的身份鉴别协议、身份鉴别方法、鉴别器相关数据及身份鉴别产生的过程信息、鉴别结果等数据；

2） 宜采用密码技术保证重要的数据存储的完整性，应采用密码技术保证重要的数据存储的机密性。

g） 风险缓解要求：可能面临的风险见 A.2，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

h） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第二级安全要求，应至少符合 GB/T 39786 规定的第二级密码应用技术要求。

7.3.4 第四级

第四级要求如下。

a） 鉴别方式要求如下：应使用多因素鉴别方式，其中一种鉴别因素至少使用密码设备鉴别器来实现，且所采用的密码模块应达到 GB/T 37092 三级及以上安全要求，多因素鉴别方式宜包含生物特征鉴别因素，包括但不限于人脸、声纹、指纹、虹膜等。

b） 鉴别协议要求如下：

1） 应采用动态信息（如随机数、挑战码）、时间戳等方式以防重放攻击；

2） 应使用密码技术进行身份鉴别，并符合 GB/T 15843（所有部分）的规定；

3） 应限制一定时间内身份鉴别的尝试次数，例如，一分钟之内的尝试次数不高于 5 次；

4） 若使用生物特征进行鉴别时，移动设备生物特征识别要求应符合 GB/T 37036（所有部分）的规定；

5） 若鉴别中涉及动态口令，动态口令密码应用技术要求应符合 GB/T 38556 的规定。

c） 鉴别器生命周期管理要求：

1） 鉴别器绑定：宜为用户身份绑定两种或两种以上类型的鉴别器（鉴别器类型和鉴别方式见附录 B）；

2） 鉴别器更新要求：应在现有鉴别器到期前一段合适的时间要求用户更新鉴别器；应与初始鉴别器颁发程序保持一致；更新成功后，应撤销被替代的鉴别器；

3） 鉴别器失窃、损坏和复制要求：应采取安全措施防止鉴别器中的秘密信息被提取；应支持鉴别器的挂起和重新激活；应支持对用户身份进行重新核验，并绑定新的鉴别器；

4） 鉴别器到期要求：到期的鉴别器不应再用于身份鉴别；当用户使用到期的鉴别器时，应告知鉴别器已到期；应对到期的鉴别器进行合理处置；

5） 鉴别器撤销要求：定期检查身份是否存在、身份是否满足资格要求、鉴别器风险状态等信息，当身份不存在，或用户提出撤销请求，或确定身份不再满足资格要求时，或鉴别器更新后，应及时撤销与该身份绑定的鉴别器；撤销的鉴别器不应再用于身份鉴别；当鉴别器被

撤销时，应对鉴别器进行合理处置，如回收后销毁、彻底清除鉴别器相关数据等。

d) 会话管理要求：身份鉴别成功后身份服务提供方和用户之间可使用密码技术建立安全的会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证对生成的会话相关秘密信息的安全存储和使用。

e) 通信保护要求：应采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要数据的机密性，应采用密码技术对通信实体进行双向鉴别。

f) 记录和存储要求如下：

1) 身份服务提供方应对身份鉴别的必要信息进行记录和存储，包括但不限于：使用的身份鉴别协议、身份鉴别方法、鉴别器相关数据及身份鉴别产生的过程信息、鉴别结果等数据；

2) 应采用密码技术保证重要的数据存储的机密性和完整性。

g) 风险缓解要求：可能面临的风险见 A.2，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

h) 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第三级安全要求，应至少符合 GB/T 39786 规定的第三级密码应用技术要求。

7.4 身份联合服务要求

7.4.1 第一级

第一级要求如下。

a) 身份联合互鉴别要求：可使用密码技术实现身份服务提供方与依赖方的身份互鉴别，从而防止恶意的服务器伪装成合法的服务器，以及防止恶意的依赖方假冒合法的依赖方获取用户信息。

b) 断言内容要求：

1) 主体[必选]：用户的标识符；

2) 发放者[必选]：发出断言的身份服务提供方的标识符；

3) 接收者[必选]：接收断言的依赖方的标识符；

4) 签发时间[必选]：身份服务提供方发出断言的时间戳；

5) 截止时间[必选]：断言何时失效的时间戳；

6) 标识符[必选]：唯一标识此断言的值；

7) 签名[必选]：身份服务提供方对断言的数字签名或消息鉴别码；

8) 鉴别时间[必选]：身份服务提供方最近一次对用户进行身份鉴别的时间戳；

9) 密钥绑定[可选]：用户拥有的密钥标识符或公钥；

10) 属性和属性引用[可选]：用户属性信息；

11) 属性元数据[可选]：描述用户属性的附加信息。

c) 断言可分为持有型断言和密钥拥有型断言。使用持有型断言时，不需要验证断言的持有者为断言主体。使用密钥拥有型断言时，需要采用密码技术验证断言的持有者为断言主体。断言类型可使用持有型断言或密钥拥有型断言。

d) 应对断言签名，要求如下：

1) 签名内容应覆盖所有重要字段，包括但不限于标识符、发放者、接收者、主体和截止时间；

2) 应由身份服务提供方进行签名，并由依赖方对身份服务提供方的签名进行验证，以保证断言的完整性；

3) 断言签名可通过以下方式实现：

——使用身份服务提供方的签名私钥，生成断言的数字签名；

——使用身份服务提供方和依赖方共享的秘密信息，生成断言的消息鉴别码；

4） 使用数字签名作为断言签名时，依赖方可在运行时以安全的方式获取用于验证数字签名的公钥；

5） 使用消息鉴别码时，身份服务提供方应和不同依赖方共享不同的秘密信息。

e） 断言加密：不作要求。

f） 会话管理要求：身份服务提供方和用户之间、依赖方和用户之间可使用密码技术分别建立安全的会话，并独立管理会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证生成的会话相关秘密信息的安全存储和使用。

g） 通信保护：可采用密码技术保证通信过程数据的完整性、重要数据的机密性，可采用密码技术对通信实体进行鉴别。

h） 记录和存储要求如下：

1） 身份服务提供方应对身份联合的必要信息进行记录和存储，包括但不限于：断言接收者、签发时间、截止时间、断言类型、签名和加密信息及其他身份联合服务产生的相关数据；

2） 可采用密码技术保证重要的数据存储的机密性和完整性。

i） 风险缓解要求：可能面临的风险见 A.3，可使用密码技术缓解可能存在的风险。

j） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第一级等级保护基本要求，应至少符合 GB/T 39786 规定的第一级密码应用技术要求。

7.4.2 第二级

第二级的身份联合服务密码应用技术要求如下。

a） 身份联合互鉴别要求：宜使用密码技术实现身份服务提供方与依赖方的身份互鉴别，从而防止恶意的服务器伪装成合法的服务器，以及防止恶意的依赖方假冒合法的依赖方获取用户信息。

b） 断言内容要求：

1） 主体[必选]：用户的标识符；

2） 发放者[必选]：发出断言的身份服务提供方的标识符；

3） 接收者[必选]：接收断言的依赖方的标识符；

4） 签发时间[必选]：身份服务提供方发出断言的时间戳；

5） 截止时间[必选]：断言何时失效的时间戳；

6） 标识符[必选]：唯一标识此断言的值；

7） 签名[必选]：身份服务提供方对断言的数字签名或消息鉴别码；

8） 鉴别时间[必选]：身份服务提供方最近一次对用户进行身份鉴别的时间戳；

9） 密钥绑定[可选]：用户拥有的密钥标识符或公钥；

10） 属性和属性引用[可选]：用户属性信息；

11） 属性元数据[可选]：描述用户属性的附加信息。

c） 断言可分为持有型断言和密钥拥有型断言，使用持有型断言时，不需要验证断言的持有者为断言主体，使用密钥拥有型断言时，需要采用密码技术验证断言的持有者为断言主体，断言类型宜使用密钥拥有型断言。

d） 应对断言签名，要求如下：

1） 签名内容应覆盖所有重要字段，包括但不限于标识符、发放者、接收者、主体和截止时间；

2） 应由身份服务提供方进行签名，并由依赖方对身份服务提供方的签名进行验证，以保证断言的完整性；

3） 断言签名可通过以下方式实现：

——使用身份服务提供方的签名私钥，生成断言的数字签名，

——使用身份服务提供方和依赖方共享的秘密信息，生成断言的消息鉴别码；

4） 使用数字签名作为断言签名时，依赖方可在运行时以安全的方式获取用于验证数字签名的公钥；

5） 使用消息鉴别码时，身份服务提供方应和不同依赖方共享不同的秘密信息。

e） 断言加密：不作要求。

f） 会话管理要求：身份服务提供方和用户之间、依赖方和用户之间可使用密码技术分别建立安全的会话，并独立管理会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证生成的会话相关秘密信息的安全存储和使用。

g） 通信保护：可采用密码技术保证通信过程数据的完整性，宜采用密码技术保证通信过程重要的数据的机密性，宜采用密码技术对通信实体进行鉴别。

h） 记录和存储要求如下：

1） 身份服务提供方应对身份联合的必要信息进行记录和存储，包括但不限于：断言接收者、签发时间、截止时间、断言类型、签名和加密信息及其他身份联合服务产生的相关数据；

2） 宜采用密码技术保证重要的数据存储的机密性和完整性。

i） 风险缓解要求：可能面临的风险见 A.3，宜使用密码技术缓解可能存在的风险（例如通过非对称密码算法对断言签名以防身份服务提供方抵赖）。

j） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第一级等级保护基本要求，应至少符合 GB/T 39786 规定的第一级密码应用技术要求。

7.4.3 第三级

第三级的身份联合服务密码应用技术要求如下。

a） 身份联合互鉴别要求：应使用密码技术实现身份服务提供方与依赖方的身份互鉴别，从而防止恶意的服务器伪装成合法的服务器，以及防止恶意的依赖方假冒合法的依赖方获取用户信息。

b） 断言内容要求：

1） 主体[必选]：用户的标识符；

2） 发放者[必选]：发出断言的身份服务提供方的标识符；

3） 接收者[必选]：接收断言的依赖方的标识符；

4） 签发时间[必选]：身份服务提供方发出断言的时间戳；

5） 截止时间[必选]：断言何时失效的时间戳；

6） 标识符[必选]：唯一标识此断言的值；

7） 签名[必选]：身份服务提供方对断言的数字签名或消息鉴别码；

8） 鉴别时间[必选]：身份服务提供方最近一次对用户进行身份鉴别的时间戳；

9） 密钥绑定[必选]：用户拥有的密钥标识符或公钥；

10） 属性和属性引用[可选]：用户属性信息；

11） 属性元数据[可选]：描述用户属性的附加信息。

c） 断言可分为持有型断言和密钥拥有型断言，使用持有型断言时，不需要验证断言的持有者为断言主体，使用密钥拥有型断言时，需要采用密码技术验证断言的持有者为断言主体，断言类型应使用密钥拥有型断言。

d） 应对断言签名，要求如下：

1） 签名内容应覆盖所有重要字段，包括但不限于标识符、发放者、接收者、主体和截止时间；

2） 应由身份服务提供方进行签名，并由依赖方对身份服务提供方的签名进行验证，以保证断言的完整性；

3） 断言签名可通过以下方式实现：

——使用身份服务提供方的签名私钥，生成断言的数字签名，

——使用身份服务提供方和依赖方共享的秘密信息，生成断言的消息鉴别码；

4） 使用数字签名作为断言签名时，依赖方可在运行时以安全的方式获取用于验证数字签名的公钥；

5） 使用消息鉴别码时，身份服务提供方应和不同依赖方共享不同的秘密信息。

e） 断言加密：应对断言进行加密，防止非授权用户获取断言信息。

f） 会话管理要求：身份服务提供方和用户之间、依赖方和用户之间可使用密码技术分别建立安全的会话，并独立管理会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证生成的会话相关秘密信息的安全存储和使用。

g） 通信保护：宜采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要的数据的机密性，应采用密码技术对通信实体进行鉴别。

h） 记录和存储要求如下：

1） 身份服务提供方应对身份联合的必要信息进行记录和存储，包括但不限于：断言接收者、签发时间、截止时间、断言类型、签名和加密信息及其他身份联合服务产生的相关数据；

2） 宜采用密码技术保证重要的数据存储的完整性，应采用密码技术保证重要的数据存储的机密性。

i） 风险缓解要求：可能面临的风险见 A.3，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

j） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第二级安全要求，应至少符合 GB/T 39786 规定的第二级密码应用技术要求。

7.4.4 第四级

第四级的身份联合服务密码应用技术要求如下。

a） 身份联合互鉴别要求：应使用密码技术实现身份服务提供方与依赖方的身份互鉴别，从而防止恶意的服务器伪装成合法的服务器，以及防止恶意的依赖方假冒合法的依赖方获取用户信息。

b） 断言内容要求：

1） 主体[必选]：用户的标识符；

2） 发放者[必选]：发出断言的身份服务提供方的标识符；

3） 接收者[必选]：接收断言的依赖方的标识符；

4） 签发时间[必选]：身份服务提供方发出断言的时间戳；

5） 截止时间[必选]：断言何时失效的时间戳；

6） 标识符[必选]：唯一标识此断言的值；

7） 签名[必选]：身份服务提供方对断言的数字签名或消息鉴别码；

8） 鉴别时间[必选]：身份服务提供方最近一次对用户进行身份鉴别的时间戳；

9） 密钥绑定[必选]：用户拥有的密钥标识符或公钥；

10） 属性和属性引用[可选]：用户属性信息；

11） 属性元数据[可选]：描述用户属性的附加信息。

c） 断言可分为持有型断言和密钥拥有型断言，使用持有型断言时，不需要验证断言的持有者为断言主体，使用密钥拥有型断言时，需要采用密码技术验证断言的持有者为断言主体，断言类型应使用密钥拥有型断言。

d） 应对断言签名，要求如下：

1） 签名内容应覆盖所有重要字段，包括但不限于标识符、发放者、接收者、主体和截止时间；

2） 应由身份服务提供方进行签名，并由依赖方对身份服务提供方的签名进行验证，以保证断言的完整性；

3） 断言签名可通过以下方式实现：

——使用身份服务提供方的签名私钥，生成断言的数字签名；

——使用身份服务提供方和依赖方共享的秘密信息，生成断言的消息鉴别码；

4） 使用数字签名作为断言签名时，依赖方可在运行时以安全的方式获取用于验证数字签名的公钥；

5） 使用消息鉴别码时，身份服务提供方应和不同依赖方共享不同的秘密信息。

e） 断言加密：应对断言进行加密，防止非授权用户获取断言信息。

f） 会话管理要求：身份服务提供方和用户之间、依赖方和用户之间可使用密码技术分别建立安全的会话，并独立管理会话，应采取有效的技术手段，保证会话标识符相关信息的随机性，保证生成的会话相关秘密信息的安全存储和使用。

g） 通信保护：应采用密码技术保证通信过程数据的完整性，应采用密码技术保证通信过程重要的数据的机密性，应采用密码技术对通信实体进行双向鉴别。

h） 记录和存储要求如下：

1） 身份服务提供方应对身份联合的必要信息进行记录和存储，包括但不限于：断言接收者、签发时间、截止时间、断言类型、签名和加密信息及其他身份联合服务产生的相关数据；

2） 应采用密码技术保证重要的数据存储的完整性和机密性。

i） 风险缓解要求：可能面临的风险见 A.3，当存在密码技术手段能缓解风险时，应使用密码技术应对风险。

j） 系统安全保护要求：网络身份服务系统应至少符合 GB/T 22239 规定的第三级安全要求，应至少符合 GB/T 39786 规定的第三级密码应用技术要求。

附 录 A
（资料性）
网络身份服务风险缓解

A.1 身份核验服务的风险缓解

身份核验服务中，至少考虑到表 A.1 列出的风险，并采取措施进行缓解。

表 A.1 身份核验服务可能面临的风险和缓解措施

序号	可能的风险	示例	可采取的缓解措施
1	伪造	伪造身份证明文件	1） 核验身份证明文件的物理安全性； 2） 通过比对权威第三方数据核验身份证明文件中的身份信息
2	抵赖	某个申请方在完成登记后，声称其没有登记过	要求申请方提交一份签名表单
3	泄露	口令在传输过程中被攻击者复制	采用安全的渠道交付并确认
4	篡改	口令在传输过程中被攻击者篡改	1） 采用安全的渠道交付并确认； 2） 支持用户对所接收的信息进行完整性校验
5	钓鱼攻击	用户身份信息被冒充的网站所窃取	1） 使用来自正规来源的网站地址； 2） 基于密码技术对网站进行鉴别

A.2 身份鉴别服务的风险缓解

身份鉴别服务中，至少考虑到表 A.2 列出的风险，并采取措施进行缓解。

表 A.2 身份鉴别服务可能面临的风险和缓解措施

序号	可能的风险	示例	可采取的缓解措施
1	鉴别器失窃	鉴别器丢失或被盗取	1） 提供挂失措施； 2） 使用多因素鉴别器
2	鉴别器复制	鉴别器被非法复制	采用防伪造技术（例如密码技术）
3	窃听	通过未加密的网络传输鉴别器的秘密信息，被攻击者截取	1） 鉴别过程使用动态的鉴别参数（例如动态口令）； 2） 秘密信息在传输之前进行加密处理
4	重放攻击	攻击者可重放先前截获的用户与依赖方之间的信息，冒充用户向依赖方鉴别	鉴别协议中使用挑战码、随机数等
5	离线猜测	通过对需要口令激活的多因素密码硬件鉴别器进行字典攻击，识别出正确口令	限制激活鉴别器的尝试次数

表 A.2　身份鉴别服务可能面临的风险和缓解措施（续）

序号	可能的风险	示例	可采取的缓解措施
6	在线猜测	猜测记忆秘密鉴别器或单因素 OTP 设备鉴别器的输出	1）　使用强口令； 2）　限制身份鉴别的尝试次数
7	侧信道攻击	通过对鉴别器进行差分功耗分析或通过分析多次交互的响应时间来提取密钥	使用抗功耗分析的密码技术实现
8	钓鱼攻击	口令被冒充的网站所窃取	1）　禁止来自不可信来源的图像和超文本链接以及在电子邮件客户端中提供视觉提示等方法保护实体免遭网络欺诈攻击； 2）　通信前基于密码技术对通信双方进行鉴别
9	中间人攻击	攻击者将自己置于用户和身份服务提供方之间，截获并修改鉴别协议消息的内容	1）　使用双向鉴别机制，确保通信双方能够确认对方身份； 2）　采用数字签名保护消息的完整性

A.3　身份联合服务的风险缓解

身份联合服务中，至少考虑到表 A.3 列出的风险，并采取措施进行缓解。

表 A.3　身份联合服务可能面临的风险和缓解措施

序号	可能的风险	示例	可采取的缓解措施
1	断言泄露	断言可能包含用户身份鉴别结果、用户身份信息，断言泄露导致用户受到攻击	1）　断言由身份服务提供方为依赖方加密； 2）　使用双向鉴别机制，确保通信双方能够确认对方身份
2	身份服务提供方抵赖	断言签名为消息鉴别码，身份服务提供方否认断言是自己生成的	1）　断言签名使用数字签名； 2）　使用引入可信第三方的消息鉴别码
3	用户抵赖	在前端通道模式下，用户否认向依赖方传递了断言	使用密钥拥有型断言
4	断言重放	攻击者将一个已经被依赖方使用过的断言再次重复使用	1）　断言具有短的有效期； 2）　依赖方对要求在一定时间窗口（可配置）内使用的断言进行跟踪，以确保断言在该时间窗口内不被多次使用

附 录 B
（资料性）
鉴别器类型和鉴别方式

B.1 鉴别器类型

适用于身份鉴别服务的鉴别器包括以下几种类型。

a) 记忆秘密鉴别器：记忆秘密鉴别器是用户选择和可记忆的秘密值（如口令）。

b) 查询秘密鉴别器：查询秘密鉴别器是存储用户和身份服务提供方共享的秘密的物理或电子记录，用户使用该鉴别器查找适当的秘密以回复来自验证者的挑战命令。例如，身份服务提供方可能要求用户从打印在表格中的数字或字符串中提供特定子集。

c) 带外鉴别器：带外鉴别器是唯一可寻址的硬件设备，可通过特殊信道或辅助信道安全地与验证者进行远程交互。设备由用户拥有和控制，支持独立于用户身份鉴别主通道的专有通信信道。例如，用户尝试登录时，需要鉴别用户在手机上接收短信的内容。

d) 生物特征鉴别器：用户的生物特征包括但不限于人脸、声纹、指纹、虹膜等。使用生物特征鉴别器进行鉴别时，生物特征与设备关联，鉴别因素包括关联设备（所拥有的）和生物特征（自身属性）两种因素，属于多因素鉴别。

e) 单因素/多因素 OTP 设备鉴别器：OTP 设备是支持自发生成动态口令的硬件设备，包括硬件设备以及安装在硬件之上的基于软件的动态口令生成器。通过将显示在设备上的动态口令，由用户输入给验证者，从而证明用户对设备的拥有和控制。OTP 设备分为单因素 OTP 和多因素 OTP 设备。单因素 OTP 设备是指使用动态口令作为鉴别因素以完成鉴别的 OTP 设备。多因素 OTP 设备是指使用多种因素协同完成鉴别的 OTP 设备，其中动态口令用来完成身份鉴别，而其他身份鉴别因素（例如记忆秘密或生物特征）用来激活设备中的动态口令生成器。

f) 单因素/多因素密码软件鉴别器：密码软件是存储在磁盘或其他介质中具有密钥存储和密码运算功能的软件，通过证明对密钥的拥有和控制完成鉴别。可分为单因素密码软件和多因素密码软件。单因素密码软件是指使用密钥作为鉴别因素来执行密码运算以完成鉴别的密码软件。多因素密码软件是指使用多种因素协同完成鉴别的密码软件，其中密钥用来执行密码运算以完成身份鉴别，而其他身份鉴别因素（例如记忆秘密或生物特征）用来激活该密钥。

g) 单因素/多因素密码设备鉴别器：密码设备可分为单因素密码设备和多因素密码设备。单因素密码设备是指使用密钥作为鉴别因素来执行密码运算以完成鉴别的密码设备。多因素密码设备是指使用多种因素协同完成鉴别的密码设备，其中密钥用来执行密码运算以完成身份鉴别，而其他身份鉴别因素（例如记忆秘密或生物特征）用来激活该密钥。

B.2 鉴别方式

鉴别方式如下所示。

a) 单因素鉴别实现的方式，包括但不限于使用如下鉴别器：

——记忆秘密鉴别器；

——查询秘密鉴别器；

——带外鉴别器；

——单因素 OTP 设备鉴别器；

——单因素密码软件鉴别器；

——单因素密码设备鉴别器。

b） 多因素鉴别实现的方式，包括但不限于使用如下鉴别器：

——记忆秘密鉴别器和查询秘密鉴别器；

——记忆秘密鉴别器和带外鉴别器；

——记忆秘密鉴别器和单因素 OTP 设备鉴别器；

——记忆秘密鉴别器和单因素密码软件鉴别器；

——记忆秘密鉴别器和单因素密码设备鉴别器；

——生物特征鉴别器；

——多因素 OTP 设备鉴别器；

——多因素密码软件鉴别器；

——多因素密码设备鉴别器。

注：生物特征用于身份鉴别通常分为两种情况：第一种情况，生物特征作为多因素鉴别器的鉴别因素之一，例如，多因素密码设备鉴别器中使用生物特征激活密钥；第二种情况，作为生物特征鉴别器使用，该情况下，生物特征与设备关联，鉴别因素包括生物特征（自身属性）和关联设备（所拥有的）两种因素，属于多因素鉴别。

参 考 文 献

[1] GB/T 36633 信息安全技术 网络用户身份鉴别技术指南
[2] GB/T 40651 信息安全技术 实体鉴别保障框架
[3] ISO/IEC TS 29003 Information technology—Security techniques—Identity proofing
[4] ISO/IEC 29115 Security technique—Entity authentication assurance framework
[5] NIST SP 800-63-3 Digital Identity Guidelines
[6] NIST SP 800-63A Digital Identity Guidelines—Enrollment and Identity Proofing
[7] NIST SP 800-63B Digital Identity Guidelines—Authentication and Lifecycle Management
[8] NIST SP 800-63C Digital Identity Guidelines—Federation and Assertions
[9] GPG No.45 Identity Proofing and Verification of an Individual