国 际 电 信 联 盟

ITU-T X.1254

(09/2020)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 身份管理

实体认证保证框架

ITU-T X.1254 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1360–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1254 建议书

实体认证保证框架

摘要

ITU-T X.1254建议书定义了三个实体认证保证等级（AAL），以及有关这三个等级的标准和威胁。

此外，它：

- 建立了用于管理AAL的框架；
- 基于风险评估，为用于缓解认证威胁的控制技术提供了指南；
- 为将三个AAL映射到其他认证保证方案提供了指南；以及
- 为交换基于三个AAL的认证结果提供了指南。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1254	2012-09-07	17	11.1002/1000/11608
2.0	ITU-T X.1254	2020-09-03	17	11.1002/1000/14260

关键词

AAL、保证、认证、认证保证等级、身份管理、IdM、保证等级、LOA。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库： http://www.itu.int/ITU-T/ipr/。

目录

引言

数字身份是参与在线事务处理之实体的唯一表示。保证（或确信）以之进行交互的数字身份与所声称的身份一致，是在线信任、安全和访问控制的核心。确定了三种类型的保证以帮助建立对数字身份的信任：身份保证、认证保证和联邦保证。

本建议书提供了认证保证的框架。就本建议书而言，认证是为了进行在线事务处理而对所声称的身份进行验证的过程。对于适用回访的业务，成功的认证可提供合理的、基于风险的保证，以确保今天访问该业务的用户与以前访问该业务的用户相同。

本建议书中建立的框架为在线业务提供方（依赖方（RP）和证书业务提供方（CSP））提供了一种系统的方法，以了解其风险并确定控制措施以帮助缓解这些风险。它旨在通过一个由三步组成的过程来促进有条不紊地选择控制措施和风险缓解策略：

1 确定角色和业务，以确定威胁类别；

2 应用有针对性的风险管理过程，以确定所需的控制强度；以及

3 确定采用哪些技术（协议、证书类型等），以进一步完善控制措施。

基于威胁的模型

本建议书旨在促进有条不紊地选择控制措施和风险缓解策略。能够选择适当控制措施和缓解策略的第一步是确定与在线业务提供方的角色和业务相关的风险和威胁类型。参见图0-1。

图0-1 – 业务、风险和控制

该框架是基于风险和威胁类别来组织的，这些类别为在线业务提供方在风险评估过程与控制和风险缓解活动之间提供了一种功能链接。

身份业务提供方可以提供这些数字身份阶段的全部、部分或仅一个功能组件。因此，在数字事务处理生命周期的类似组件化方法中，对风险进行评估并论述控制措施和风险缓解方法是合适的。本建议书论述了有关该生命周期中证书管理和认证阶段的风险和控制问题。其他文件（例如，[b-ISO/IEC TS 29003]）论述登记和身份证明活动的风险和控制问题，以及组织和管理控制问题。可以预期，这些文档和其他文档将调整一致，以代表一组经协调的核心身份管理标准（如图0-2所示），这些标准当组合使用时，将为数字身份事务处理生命周期提供过程、风险和控制措施。

本建议书还提供了特定于其范围（认证和证书管理）的隐私威胁、注意事项和缓解控制措施的目录。本建议书不包括有关身份证明或登记的隐私注意事项。

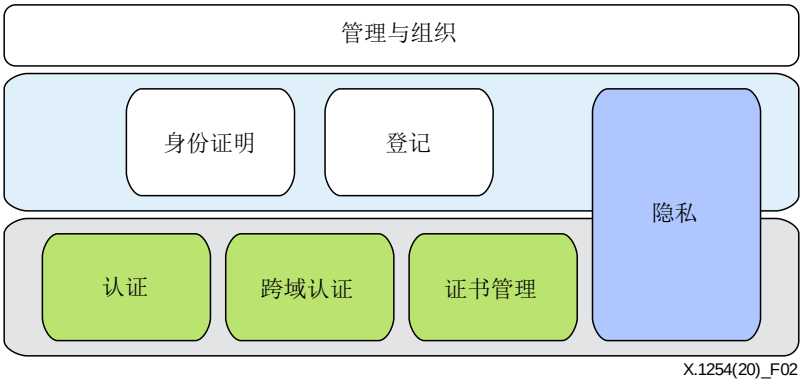


图0-2 – 核心一致的身份管理标准

与本建议书先前版本的关系

本建议书的第1版[b-ITU-T X.1254 (2012)]通过三个阶段介绍了数字身份事务处理的生命周期：登记与身份证明、证书管理和实体认证。自2012年以来，该行业已发生了演进，并出现了新的概念和方法，例如，无密码认证和逐步认证。因此，该行业已从保证等级（LoA）的概念演进为驱动实施方案特定要求的单一序数。取而代之的是，通过将适当的业务和隐私风险管理与任务需求结合在一起，实施方将选择身份保证等级（IAL）、认证保证等级（AAL）和联邦保证等级（FAL）作为不同的选项。本建议书侧重于AAL。IAL和FAL超出了本建议书的讨论范围。

ITU-T X.1254 建议书

实体认证保证框架

1 范围

本建议书规定了特定情境中管理实体认证保证（EAA）的框架。它重点：

– 建立了三个实体认证保证等级（AAL）；
– 为理解这些实体AAL提供了指南；
– 为达成确定的EAA等级规定了标准和指南；
– 为比较和映射不同的认证保证方案提供了指南；
– 为交换基于特定保证等级的认证结果提供了指南；以及
– 基于风险评估，为应用于缓解认证威胁的控制提供了指南。

2 参考文献

无。

3 定义

3.1 在其他地方定义的术语

本建议书使用了以下在其他地方定义的术语：

3.1.1 断言 [b-ITU-T X.1252]：一个实体在无附带其有效性证据的情况下做出的声明。

注 – “声称”和“断言”两词通常被认为具有大体相似的含义，但又有细微差别。就本建议书而言，“断言”被认为是一种比“声称”更强烈的声明。

3.1.2 认证 [b-ISO/IEC 18014-2]：为实体所声称的身份提供的保证。

3.1.3 认证因素 [b-ISO/IEC 19790]：用于认证或验证实体身份的信息片段和/或过程。

注 – 认证因素可分为四类：

– 实体之所有（如设备签名、护照、含有证书的硬件装置、私钥）；
– 实体之所知（如密码、PIN）；
– 实体之所显（如生物特征）；或
– 实体之所为（如行为模式）。

3.1.4 认证协议 [b-ISO/IEC 29115]：在实体与验证方之间确定的消息序列，可供验证方用来认证一个实体。

3.1.5 声称 [b-ITU-T X.1252]：在不能提供证明的情况下声明某事务。

注 – “声称”和“断言”两词通常被认为具有大体相似的含义，但又有细微差别。就本建议书而言，“断言”被认为是一种比“声称”更强烈的声明。

3.1.6 情境 [b-ITU-T X.1252]：一个具有确定边界条件的环境，实体存在和互动于其中。

3.1.7 证书 [b-ITU-T X.1252]：证明声称之身份和/或权利的一组数据。

注 – 有关证书的其他特性，参见附录I。

3.1.8 实体 [b-ITU-T X.1252]：具有独立和独特存在并可在一定情境中识别的事务。

注 – 就本建议书而言，实体也用于有关声称一身份之物的特定情况。

3.1.9 身份；部分身份 [b-ISO/IEC 24760-1]：与一个实体相关的一系列属性。

注 – 在一个具体情境中，一个身份可有使一个实体在该情境中得到唯一识别的一个或多个标识符。

3.1.10 身份信息验证 [b-ISO/IEC 29115]：对比发布方、数据源或其他涉及真实性、有效性、正确性和实体相关性的其他内外部资源，查验身份信息和证书的过程。

3.1.11 身份证明 [b-ISO/IEC 29115]：注册机构（RA）为确定一个实体具有规定或认可的保证等级而捕获和验证足够信息的过程。

3.1.12 中间人攻击 [b-ISO/IEC 29115]：攻击者在双方不知情的情况下能够读取、插入和修改双方消息的攻击

3.1.13 多因素认证 [b-ISO/IEC 29115]：通过至少两个独立认证因素进行的认证。

3.1.14 相互认证 [b-ISO/IEC 29115]:：向两个实体提供对方身份保证的实体身份认证。

3.1.15 不可否认性/不可抵赖性[b-ITU-T X.1252]：防止参与某行动的实体之一否认曾参与全部或部分行动的能力。

3.1.16 网络钓鱼 [b-ISO/IEC 29115]：诱骗电子邮件用户披露个人或机密信息供诈骗者非法使用的一种欺诈行为。

3.1.17 否认/抵赖 [b-ITU-T X.1252]：参与实体之一否认曾参与全部或部分行动。

3.1.18 风险评估 [b-ISO/IEC 27000]：有关风险识别、风险分析和风险评估的整个过程。

3.1.19 共享秘密 [b-ISO/IEC 29115]：认证中使用的、只为实体和验证方所知的秘密。

3.1.20 事务处理 [b-ISO/IEC 29115]：实体与业务提供方之间的一件离散事件，用于支持某项业务或计划的目的。

3.1.21 验证 [b-ISO/IEC 29115]：通过将提供的信息与过去确证的信息进行比较的信息检验过程。

3.1.22 验证方 [b-ISO/IEC 29115]：确证身份信息的参与方。

注 – 验证方可参与实体认证保证框架的多个阶段，并可执行证书验证和/或身份信息验证。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 证书业务提供方（CSP）：发布和/或管理证书的可信参与方。

注 – 本定义基于[b-ISO/IEC 29115]中的定义。

3.2.2 实体认证保证（EAA）：在认证实体身份或预期身份过程中达到的置信度。

注1 – 信任基于实体与所称身份之间绑定中的置信度。

注2 – 本定义基于[b-ITU-T X.1252]中对“认证保证”的定义。

3.2.3 标识符：在特定情境中唯一特征一个实体的一个或多个属性。

注 – 本定义基于[b-ITU-T X.1252]中的定义。

3.2.4 注册机构（RA）：向证书业务提供方（CSP）确认或担保实体身份的一个可信参与方。

注 – 本定义基于[b-ISO/IEC 29115]中的定义。

3.2.5 依赖方（RP）：依赖于身份断言或声称的参与方。

注 – 本定义基于[b-ISO/IEC 29115]中的定义。

4 缩写词和首字母缩略语

本建议书采用了以下缩写词和首字母缩略语：

AAL 认证保证等级
CSP 证书业务提供方
EAA 实体认证保证
FAL 联邦保证等级
FIDO 快速身份在线
HTML 超文本标记语言
HTTP 超文本传输协议
HTTPS 超文本传输协议-安全
IAL 身份保证等级
IdM 身份管理
IDP 身份提供方
LoA 保证等级
MAC 媒质访问控制
MITM 中间人攻击
MITB 人在浏览器中攻击
OAuth 开放认证
OpenID 开放身份
OTP 一次性密码
PIA 隐私影响评估
PII 个人可识别信息
PIN 个人识别码
RA 注册机构
RP 依赖方
SAML 安全断言标记语言
TLS 传输层安全
URL 统一资源定位器

5 惯例

本建议书采用以下语言方式来表达规定：

a) “Shall”（须/宜）表示要求；

b) “Should”（应/应该）表示建议；

c) “May”（可/可以）表示允许；

d) “Can”（能/可能）表示可能性或能力。

6 数字认证流程

6.1 概述

数字身份是参与在线事务处理之实体的唯一表示。数字认证以其最简单的形式，在某个置信度上，参与验证某实体所声称的身份，以便授予其访问在线业务的权限。已注册实体试图通过证明拥有一个认证器（也称为证书，在注册时签发）来对某项在线业务进行认证。然后，在线业务（也称为事务处理中的依赖方（RP））尝试通过身份提供方（IDP）或证书业务提供方（CSP）或验证方来对认证器的有效性进行验证。在 CSP 或验证方对其证书进行验证后，该实体将被授予访问在线业务的权限。

图 6-1 说明了以下数字认证流程：

1 实体访问依赖方（RP）的在线业务；

2 RP将实体重定向到CSP进行认证；

3 CSP验证实体是否拥有注册的认证器；

4 CSP向RP发送认证断言，以断言实体的认证状态；

5 在实体与RP之间建立一个经认证的会话。

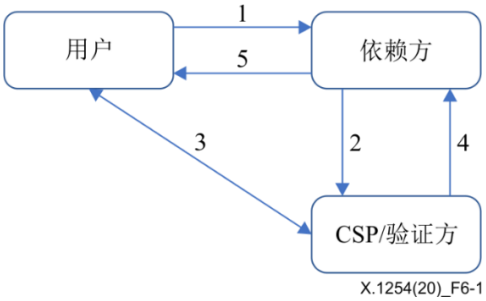


图6-1 – 数字认证流程

以这种方式来说明数字认证流程提供了一种用于理解与数字认证中涉及之各种角色和功能有关的风险的方法。

尽管 RP 可能拥有自己的身份管理（IdM）解决方案并充当自己的 CSP，但本建议书将 RP 和 CSP 呈现为不同的角色。不过，无论哪种情况，每个角色的功能都是相同的。

此外，图 6-1 结合了 CSP 和验证方的角色。即使 CSP 通常执行验证功能，在某些情况下，CSP 仍可使用单独的验证方。

此处描述的数字认证流程假设实体已通过 CSP 进行注册，并拥有一个或多个经注册的认证器。登记和注册过程超出了本建议书的讨论范围。

6.2 数字身份保证

有必要了解涉及数字身份生命周期各个阶段和功能组件的业务是如何相互影响的，以支持在线事务处理中的信任和总的置信度。此类信任通常表示为置信度或保证等级。本建议书为数字身份认证保证阶段以及整个数字身份和认证保证框架的组件功能提供了要求和指南。图 6-2 显示了有关一组核心、一致的 IdM 文档的组件、保证说明和功能活动，以论述此类总体数字身份框架中的保证和控制问题。

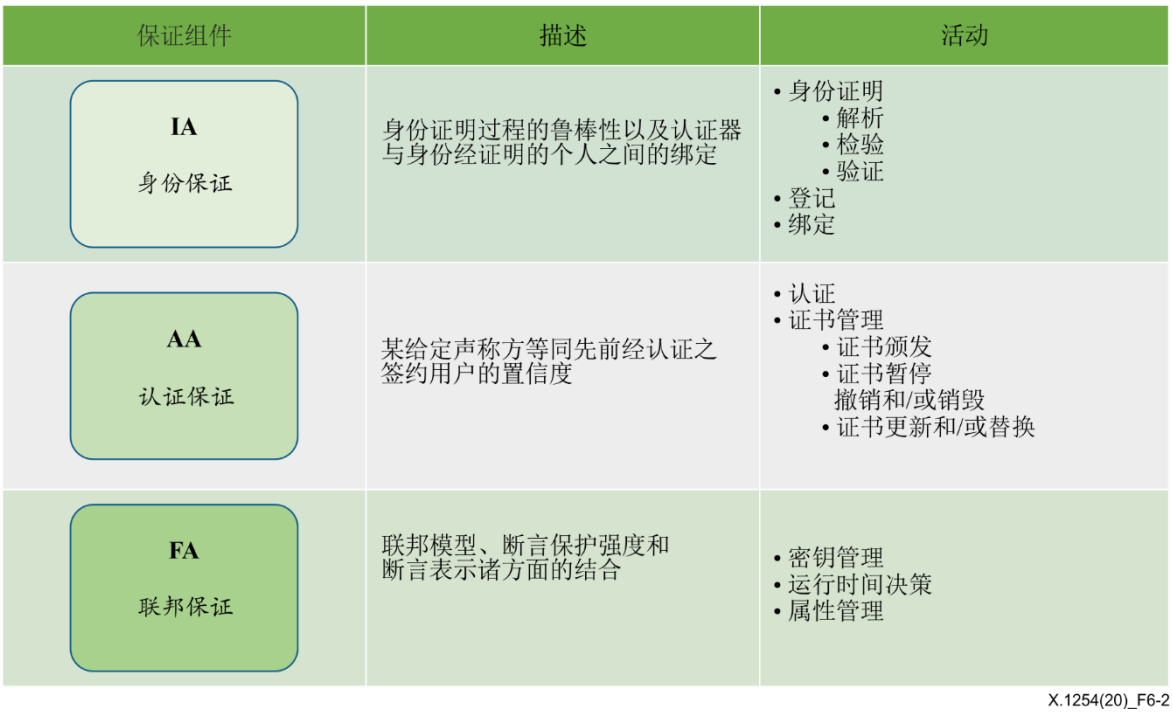


图6-2 – 数字身份保证等级

身份保证：本保证由用于验证主体与其真实身份之间关联性的过程构成。身份保证在[b-ISO/IEC TS 29003]中论述。

认证保证：认证确保尝试访问数字业务的主体可控制用于认证的技术。本保证由用于验证声称之身份等同于参与注册过程且先前已向系统做认证之身份的过程构成。

联邦保证：本保证由用于在不同安全域之间进行通信、保护和验证身份断言的过程构成。身份联邦指的是在两方或多方之间共享在线身份和认证信息。

支持联邦保证的身份保证组件和活动不在本建议书本修订的讨论范围。

6.3 角色

6.3.1 概述

作为以风险为中心的模型，数字认证流程可帮助识别与三个主要角色相关的威胁类别：CSP、RP 和实体。

6.3.2 在线业务提供方

在线业务提供方是提供需要受限访问的在线业务、应用程序和信息的组织，例如，银行业务、医疗保健提供方业务和零售商。根据业务的实现方式，在线业务提供方可以扮演一个或两个以下角色：

- CSP；
- 身份业务提供方；
- 验证方；
- RP。

6.3.3 证书业务提供方（CSP）

CSP 负责验证实体提供的证书（即认证器）。它们执行此操作的过程和严格程度取决于与在线事务处理相关的风险等级以及将要使用身份的环境。CSP 功能既可以由在线业务提供方的内部 IdM 系统来执行，也可以由第三方身份业务来执行。此外，CSP 角色常常负责证书管理活动。

6.3.4 身份业务提供方

身份业务提供方负责对实体所声称身份进行身份证明，并确保该声称身份与该实体使用的证书相关联。它们执行此操作的过程和严格程度取决于与在线事务处理相关的风险等级以及将要使用身份的环境。IDP 还可能负责在特定程序和业务中注册和登记实体。涉及这些 IDP 组件功能的风险和控制措施不在本建议书的讨论范围。

此外，IDP 可能扮演 CSP 的角色。由于此建议书侧重于认证和证书管理，因此在使用术语 CSP 时，它还旨在表示在事务处理中扮演该角色的 IDP。

6.3.5 验证方

验证方负责确认实体的身份，方法是使用认证协议来验证实体对认证器的拥有和控制情况。为此，验证方可能还需要对将认证器链接到实体标识符的证书进行验证，并检查其状态。验证方的角色通常由提供证书业务的 CSP 或 IDP 来扮演。

6.3.6 依赖方

RP 接受（依赖）并利用来自其自身 IdM 业务或外部 CSP 的实体认证状态断言。RP 必须能够信任它们从这些业务中收到的身份信息，以便对是否允许特定实体访问其在线业务和产品做出基于风险的决定。

6.3.7 实体

出于本建议书的目的，实体指的是在线业务提供方提供之业务的用户。

实体负责保护其身份和数字证书免遭欺诈和滥用，并负责以其预期的方式使用其证书。

6.4 认证过程组件

本建议书为业务提供方提供了一种方法，可基于其角色（如第 6.3 节所述）并启用技术来识别与其业务相关的威胁和风险。

为了便于评估与在线业务相关的特定风险和威胁，重要的是确定认证过程中涉及哪些功能和支持技术。

过程组件包括：

- 认证器，例如，存储的秘密（例如密码）、一次性密码（OTP）设备、智能卡、数字证书和生物特征（例如指纹）；
- 客户端和服务器软件；
- 通信和认证协议。例如，超文本标记语言（HTML）、安全断言标记语言（SAML）、传输层安全（TLS），开放认证（OAuth）和开放身份（OpenID）。

认证事务处理易受事务处理损害攻击，攻击的目标是与前一段落所列一个或多个组件相关的漏洞。大多数认证技术，包括硬件、软件和通信协议，都有特定的、相关的威胁和漏洞。作为其风险评估活动的一部分，在线业务提供方须考虑与各个组件相关的漏洞。第 8 节描述了特定的威胁类别、风险和控制。

6.4.1 认证器类型

认证器指的是实体拥有和控制的一些东西，用于认证实体的身份。一个实体可能有多个关联的认证器。认证因素包括你了解的一些东西，例如，一个密码；你拥有的一些东西，如智能卡；以及表明你是谁的一些东西，如某种生物特征。通过使用一个或多个不同的因素，可以提高认证事务处理的强度。

在线业务提供方在选择该业务认证可接受的认证器时须考虑到其业务的风险状况。此外，RP 在接受 CSP 提供的业务之前，须考虑到其业务的保证要求。

认证器的类型包括：

- 存储的秘密；
- 查找的秘密；
- 带外设备；
- 单因素OTP设备；
- 多因素OTP设备；
- 单因素加密软件；
- 单因素密码设备；
- 多因素加密软件；
- 多因素加密设备。

6.4.2 认证器

指的是一个对象或数据结构，它通过一个或多个标识符将一个身份和（可选地）附加属性以授权形式绑定于签约用户拥有和控制的至少一个认证器。虽然常见用法通常假定实体维护认证器，但本建议书也使用该术语来指代由 CSP 维护的电子记录，这些电子记录在签约用户的认证器与身份之间建立某种绑定。认证器最常见的形式是绑定于一个密码或其他认证器的用户名和相关的用户记录。

7 将风险管理应用于认证保证框架

7.1 概述

有效的 IdM 系统取决于了解与组织提供之在线业务类型相关的风险等级。为了理解这些风险，在线业务提供方须考虑其在框架内的特定角色、其用户的性质以及其应用程序处理之数据和事务的类型。

结构化风险管理方法的应用将产生以下结果：识别风险和威胁；有关应如何对待它们的决定；以及选择和实施控制所需的输入。在 IdM 领域，存在一些特定的指南来帮助组织理解这些风险等级是如何等同于保证等级的；即对于在线身份完整性的相对置信度。

在线业务提供方须采用风险管理方法，并制定计划来管理其与数字认证有关的风险。

与数字身份有关的风险评估的范围须至少考虑到与每种已识别风险有关的影响的类型和等级。还可以考虑到每个风险发生的可能性。

7.2 认证风险

在考虑认证风险时，如果认证失败，则基本问题是“要害在哪里？”，也就是说，若将访问权限授予非证书和关联帐号合法所有者的某实体，那会产生什么影响。

在线业务提供方在评估其与认证失败相关的风险时，须考虑以下因素：

- 数据 – 识别在系统边界内处理和保护的数据类型，是确定“要害在哪里”的关键因素。数据类型包括个人可识别信息（PII）、财务信息、专有信息、公开可用的信息和高度敏感的信息。
- 用户 – 识别和了解系统或企业的用户，对于能够识别和分类特定风险而言至关重要。用户类别包括内部用户、外部用户和特权用户。组织还应考虑到其用户是否受任何合同、法律或其他类型协议的约束。
- 攻击动机 – 通过首先定义其用户和数据类型，组织将可以更好地了解攻击动机，例如，如果系统处理并保护银行帐户信息，则可能会促使攻击者欺诈性地访问系统以获取经济利益。

在线业务提供方须基于所评估的风险，选择控制措施和其他威胁缓解选项。

8 威胁类别、风险和控制

本节提供了围绕威胁类别组织的威胁和控制目录。身份业务提供方应根据其与认证有关的角色和业务，确定其要遭受的特定威胁类别。控制按以下威胁类别进行分组：

- 认证器损害；
- 事务处理损害；
- CSP冒充；
- 实体冒充；
- 认证业务损害。

RP 和 CSP 共同承担防范所有认证威胁的职责。认证事务处理中的角色和职责须由各方明确建立并达成共识。

表 8-1 列出了认证威胁类别以及通常指配的、旨在缓解这些威胁的职责。

表8-1 – 角色和威胁类别

角色	威胁类别
RP	• 验证方冒充 • 事务处理损害 • 隐私 • 联邦
CSP	• 验证方冒充 • 事务处理损害 • 签约用户冒充 • 认证器损害 • 认证业务损害 • 隐私 • 联邦

8.1 保证等级

在本建议书，认证是指为了进行在线事务处理而对所声称身份进行认证的过程。在用于验证所声称身份的过程中，越来越严格的要求会带来置信度的提升，即经认证的身份代表该身份的预期主体。认证保证是对置信度的一种度量，系统或方案会建立一系列相对置信度，称为AAL。

本建议书描述了一种认证保证模型，它基于识别和缓解认证事务处理之威胁和风险的概念。在许多情况下，感兴趣的组织、国家机构和社群可以选择建立一个AAL方案，方案将对与其工作环境相关的风险、威胁和控制进行分组。这样做可以带来许多明显的好处，包括在共同定义的等级上确定有关参与事务处理的要求，以及创建满足社群需求之标准产品包的能力。

本建议书撤消了保证等级（LOA）作为驱动实施方案特定要求的单一序数的概念，取而代之的是，通过将适当的业务和隐私风险管理与任务需求结合在一起，实施方将选择IAL、AAL和FAL作为不同的选项。尽管许多系统对IAL、AAL和联邦保证等级（FAL）均具有相同的数值等级，但这不是必需条件，实施者不应假定它们在任何给定的系统中都将相同。

在这些指南中详述的身份保证组件如下所示：

- IAL是指身份证明过程；
- AAL是指认证过程；
- FAL是指联邦化环境中的断言强度，用于将认证和属性信息（如果适用）传递给RP。

分离这些类别为实施者提供了选择身份解决方案的灵活性，并增强了在任何保证等级中将隐私增强技术作为身份系统基本要素的能力。例如，即使使用强大的多因素认证器，该模型也支持允许假名交互的情形。

在当今的环境中，一个组织的身份解决方案不必是由一个系统或供应商来提供所有功能的“庞然大物”。身份业务可以由多个组件组成，从而允许组织和机构根据任务需要采用基于标准的、可插入的身份解决方案。

这三个AAL定义了选项子集，实施者可以根据其风险状况以及因攻击者控制认证器和访问代理机构系统而造成的潜在损害来选择选项。AAL如下所述。

AAL1：AAL1一定程度上保证实体控制绑定于实体帐户上的认证器。AAL1要求使用多种可用的认证技术来进行单因素或多因素认证。成功的认证要求声称方通过安全的认证协议来证明拥有和控制认证器。

AAL2：AAL2高置信度地保证实体控制绑定于实体帐户的认证器。要求通过安全认证协议来证明拥有和控制两个不同的认证因素。AAL2及更高等级要求全球接受的加密技术。

AAL3：AAL3很高置信度地保证实体控制绑定于实体帐户的认证器。AAL3上的认证基于通过密码协议证明拥有一个密钥。AAL3认证须使用基于硬件的密码认证器以及可抵御验证方冒充的认证器；同一设备可以满足这两个要求。为了在AAL3上进行认证，声称方须通过安全认证协议来证明拥有和控制两个不同的认证因素。要求全球接受的加密技术。

本版本建议书未单独提出一套标准化、规范化的保证等级。试图为所有社群创建一个单一的、标准化的保证结构会削弱特定社群管理适于其环境之风险的能力。不过，它确实承认存在这些不同的保证方案，并且身份业务提供方通常必须能够证明遵循一组或多组AAL。

由于AAL方案表示在对声称的身份进行验证中提高可信度，相应地将在认证过程中提高严格程度，因此，本建议书中的控制描述使用相对术语而非谨慎的AAL。对于那些经修改可提供更高置信度的控制，提供最低置信度的条件用“最低AAL”来表示；随后，用“较高AAL”来表示较高置信度；以及，导致最高置信度的条件用“最高AAL”来表示。表8-2提供了有关此约定如何等同于某些更常见认证保证方案的概念性想法。（请注意，表8-2的一致无意在各种方案之间建立直接的等效关系。）

表8-2 – 认证保证等级

AAL	四-AAL方案	三-AAL方案	三-等级方案
最高	AAL 4	AAL 3	高
较高	AAL 3	AAL 2	实质性的
	AAL 2		
最低	AAL 1	AAL 1	低

本节的其余部分提供了规范性控制措施的超集，并根据其缓解的威胁进行了分组。身份业务提供方须根据其角色和业务，确定其所遭受的特定威胁，如本建议书所述。一旦确定了这一点，并且为了能够评估对本建议书的合规性，身份业务提供方须记录本章其余部分中所述的威胁以及相应的控制描述和期望结果。

8.2 认证器损害

8.2.1 认证器损害的风险

认证器损害指的是任何复制、篡改或导致未经授权的证书信息泄露的攻击，这些证书信息可用于成功地进行认证并获得对信息系统的未经授权的访问。在IdM生命周期中的任何时候都可能发生认证器损害。不过，本建议书范围内的威胁和控制措施仅旨在解决认证问题。

证书可遭受多种形式攻击的损害，包括网络钓鱼、盗窃、证书复制、重放攻击以及在线或离线暴力破解攻击。防范证书损害风险并不仅仅属于该威胁类别的控制措施。应该注意的是，任何威胁类别中控制失败的后果都可能导致证书损害。例如，如果认证业务提供方遭受数据泄露，则获得的信息可用于获得对信息系统的未经授权访问。

8.2.2 认证器损害的控制

表 8-3 列出了认证器损害控制措施。

表8-3 – 认证器损害控制

CTRL #	控制描述	预期结果
AC-1	对最高AAL，认证应使用基于硬件的密码认证器和能抵御验证方冒充的认证器 – 同一设备可同时满足这两个要求。	使用适当的认证器来实现预期AAL。
AC-2	对最高AAL，声称方应通过安全认证协议来证明拥有和控制两个不同的认证因素。	遵循适当的认证协议来实现预期AAL。
AC-3	应以经批准的加密模块验证程序要求的程度，对最高AAL所用的多因素认证器进行验证。	以实现预期AAL所需的程度来验证认证器密码术。
AC-4	应对IDP采购的认证器进行验证，以符合经批准的加密模块验证程序所提的要求。	使用经批准的密码术。
AC-5	验证方应实施控制措施，以抵御在线猜测攻击（如果适用于认证器类型的话）。	验证方实施控制以保护认证器免遭在线猜测攻击。
AC-6	除非在给定认证器的描述中另有说明，否则验证方应将对单个帐户的连续失败的认证尝试限制在100次内。	验证方实施控制以保护认证器免遭在线猜测攻击。
AC-7	密码认证器应使用经批准的密码术。	使用经批准的密码术。
AC-8	如果要使用多个认证器进行认证，则至少应有一个能抵御重放攻击。	保护认证器免遭重放攻击。
AC-9	所有密码设备认证器都应能够抵御重放攻击。	采用控制来保护认证器免遭重放攻击。
AC-10	相关的边信道攻击应通过由CSP进行的风险评估来确定。	CSP执行适当的风险评估。

表8-3 – 认证器损害控制

CTRL #	控制描述	预期结果
AC-11	声称方与验证方之间的通信（在带外认证器的情况下，使用主信道）应通过经认证、受保护的信道来进行。	保护声称方与验证方之间的通信。
AC-12	应以经批准的加密模块验证程序要求的程度，对最高AAL所用的单因素密码设备进行验证。	以实现预期AAL所需的程度来验证认证器密码术。
AC-13	在认证过程中使用诸如智能手机之类的设备时，解锁该设备（通常使用个人识别码（PIN）或生物特征）不应被视为认证因素之一。	使用适当的认证器来实现预期AAL。
AC-14	生物特征识别系统应允许不超过10次的连续失败的认证尝试。一旦达到该限制，生物特征识别认证器应： • 在下一次尝试之前施加至少30秒的延迟，并对每次连续尝试成倍增加延迟时间（例如，在下一次失败尝试之前延迟1分钟，在第二次失败尝试之前延迟2分钟）；或者 • 禁用生物特征识别用户认证，并提供另一个因素（例如，如果不是必需的因素，则使用一种不同的生物特征识别形态或PIN/密码）（如果已有这样一种可用的替代方法）。	生物特征识别系统实施控制以保护认证器免遭猜测攻击。

8.3 事务处理损害

8.3.1 事务处理损害的风险

事务处理损害指的是在传输过程中破坏两方间正在交换之数据机密性或可用性的攻击。可能导致事务处理损害的常见攻击是中间人攻击（MItM）、人在浏览器中攻击（MItB），窃听和会话劫持。

8.3.2 事务处理损害的控制

表8-4列出了事务处理损害控制措施。

表8-4 – 事务处理损害控制

CTRL #	控制描述	预期结果
TC-1	在验证方和CSP是单独实体的情况下，验证方与CSP之间的通信应该通过使用经批准的密码术做了相互认证的安全信道（例如，客户端经认证的TLS连接）来进行。	保护验证方与CSP之间的通信。
TC-2	会话秘密应在签约用户的软件与所访问的业务之间共享。	实施和保护会话秘密。
TC-3	统一资源定位符（URL）或HTTP POST [b-IETF RFC 7231]内容应包含一个会话标识符，应通过RP对之进行验证，以确保在会话外采取的行动不会影响所保护的会话。	会话标识符由RP验证。
TC-4	秘密应直接由签约用户的软件来提供，或应使用密码机制来证明拥有秘密。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-5	用于会话绑定的秘密不应用于主机与签约用户端点之间的不安全通信。认证后，经认证的会话不应回退到不安全的传输，如从超文本传输协议-安全（HTTPS）到文本传输协议（HTTP）。	保护会话秘密的传输。
TC-6	在交互过程中（通常在用户认证后立即进行），会话主机应生成用于会话绑定的秘密。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-7	应由经批准的随机位生成器来生成用于会话绑定的秘密，并包含至少64位的熵。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-8	当用户注销时，会话主体应清除用于会话绑定的秘密或使之无效。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-9	应使用经认证的受保护信道来将用于会话绑定的秘密发送到设备或从设备接收。	保护会话秘密的传输。
TC-10	在CSP定义的时间后，用于会话绑定的秘密应超时并且不被接受。	保护会话秘密的传输。
TC-11	在对认证事件的直接响中，会话主机应生成用于会话绑定的秘密。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-12	应将浏览器cookies（写入用户本地终端的数据包）标记为仅在HTTPS会话上可访问。	保护会话秘密的传输。
TC-13	浏览器cookies（写入用户本地终端的数据包）应以最小的实际主机名和路径集来访问。	保护会话秘密的传输。

表8-4 – 事务处理损害控制

CTRL #	控制描述	预期结果
TC-14	经认证会话的连续性应基于认证时对验证方发布之会话秘密的拥有情况，并在会话期间可选择地进行刷新。	会话秘密是随机生成的，适当实施并在使用后予以妥善处理。
TC-15	如果集中进行比较，则所有生物特征的传输都应在经认证的受保护信道上进行。	保护生物特征信息的传输。
TC-16	应该在传感器（或包含一个传感器、抵御传感器替换的端点）与验证方之间建立一条经认证的受保护信道。	保护验证方与端点之间的通信。

8.4 验证方冒充

8.4.1 验证方冒充的风险

验证方冒充指的是实体与假冒的验证方进行交互并被欺骗而泄露证书信息的攻击。攻击者获得的信息将对签约用户冒充或证书损害威胁类别构成重大风险。网络钓鱼是与验证方冒充相关的最常见攻击之一。攻击者能够诱使实体将签约用户证书信息发送给一个不可信的客户端、服务器或业务，并使用获得的证书信息来获得对信息系统的未授权访问。

8.4.2 验证方冒充的控制

表 8-5 列出了验证方冒充控制措施。

表8-5 – 验证方冒充控制

CTRL #	控制描述	预期结果
VI-1	应对验证方进行验证，以满足经批准的密码模块验证程序的要求。	使用经批准的密码术。
VI-2	验证方抵御冒充认证协议应与验证方建立一条经认证的受保护信道。	保护认证器的输出。
VI-3	经认证的受保护信道应牢固且不可逆地将在建立经认证的受保护信道时商定的信道标识符绑定于认证器输出。	保护认证器的输出。
VI-4	验证方应验证签名或用于证明抵御验证方冒充能力的其他信息。	验证方有效执行验证。
VI-5	应在需要的地方，使用经批准的密码算法来建立抵御验证方冒充的能力。	使用经批准的密码术。
VI-6	用于建立抵御验证方冒充之能力的密钥应至少提供适用密码标准中规定的最低安全强度。	验证方未被冒充。

表8-5 – 验证方冒充控制

CTRL #	控制描述	预期结果
VI-7	为被视为具有抵御验证方损害的能力，验证方存储的公钥应与经批准的密码算法的使用相关联，并应至少提供适用密码标准中规定的最低安全强度。	验证方未受损。
VI-8	抵御验证方损害的秘密应使用经批准的哈希算法，并且基础秘密应至少具备适用密码标准中规定的最低安全强度。	验证方未受损。
VI-9	涉及人工登录认证器输出的认证器（例如，带外认证器和OTP认证器）不应被视为具备抵御验证方冒充的能力，因为人工登录不会将认证器输出绑定于要经认证的特定会话。	不使用需要人工登录的认证器来抵御验证方冒充攻击。

8.5 签约用户冒充

8.5.1 签约用户冒充的风险

签约用户冒充指的是涉及伪造合法身份以破坏认证过程并获得对网络或信息系统的未经授权访问的攻击。常见的签约用户冒充攻击包括电子欺骗和会话劫持。电子欺骗攻击的一个例子是，冒充RP的攻击者仿造一个属于经认证设备的媒质访问控制（MAC）地址以获得对网络的未经授权访问。另一个例子是伪装，攻击者通过提供伪造的或盗窃的证据来冒充合法用户并能成功地遵循证书重置协议。

8.5.2 签约用户冒充的控制

表 8-6 列出了签约用户冒充控制措施。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-1	认证过程的结果是一个每次当签约用户向该RP进行认证时都应使用的标识符。	认证c器绑定于适当的签约用户。
SI-2	为了满足给定AAL的要求，应至少以给定的强度等级对声称方进行认证，以便使之能被认可为一个签约用户。	使用适当的认证器，以适当的强度等级，对签约用户进行认证，以实现预期AAL。
SI-3	所有认证和重新认证过程都应展示来自至少一个认证器的认证意图。	展示认证器的意图。
SI-4	CSP应向签约用户提供有关如何适当保护认证器免遭盗窃或丢失的指令。	在不规避预期AAL的情况下，签约用户能够恢复认证器。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-5	最低AAL上的认证应通过使用以下任意一种认证器类型来进行： • 存储的秘密； • 查找的秘密； • 带外设备； • 单因素OTP设备； • 多因素OTP设备； • 单因素密码软件； • 单因素密码设备； • 多因素密码软件； • 多因素密码设备	使用适当的认证器，以适当的强度等级，对签约用户进行认证，以实现预期AAL。
SI-6	较高AAL上的认证应通过使用多因素认证器或者两个单因素认证器的组合来进行。使用多因素认证器时，可以使用以下任意一种认证器类型来进行： • 多因素OTP设备； • 多因素密码软件； • 多因素密码设备	使用适当的认证器，以适当的强度等级，对签约用户进行认证，以实现预期AAL。
SI-7	当使用两个单因素认证器的组合时，它应包括一个存储的秘密认证器和一个来自以下清单的、基于拥有情况的（即“你所拥有的东西”）认证器： • 查找的秘密； • 带外设备； • 单因素OTP设备； • 单因素密码软件； • 单因素密码设备	使用适当的认证器，以适当的强度等级，对签约用户进行认证，以实现预期AAL。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-8	最高AAL上的认证应通过使用认证器的组合之一来进行。可能的组合来自： • 多因素密码设备； • 与存储的秘密结合使用的单因素密码设备； • 与单因素密码设备结合使用的多因素OTP设备（软件或硬件）； • 与单因素密码软件结合使用的多因素OTP设备（仅硬件）； • 与多因素密码软件认证器结合使用的单因素OTP设备（仅硬件）； • 与单因素密码软件认证器和存储的秘密结合使用的单因素OTP设备（仅硬件）	使用适当的认证器，以适当的强度等级，对签约用户进行认证，以实现预期AAL。
SI-9	CSP应提供一种机制，可在收到签约用户通知怀疑认证器丢失或被盗后立即撤销或暂停认证器。	无法使用无效的认证器来成功认证某个个体。
SI-10	为便于安全报告认证器的丢失、被盗或损坏情况，CSP应为签约用户提供一种使用备份或替代认证器向CSP进行认证的方法。该备份认证器应是一个存储的秘密或一个物理的认证器。	在不规避预期AAL的情况下，签约用户能够恢复认证器。
SI-11	如果签约用户使用一个有效的（即未被暂停的）认证器成功向CSP进行认证，并请求重新激活以这种方式被暂停的认证器，则该暂停应是可逆的。	在不规避预期AAL的情况下，签约用户能够恢复认证器。
SI-12	如果认证器过期，则它不能用于认证。	无法使用无效的认证器来成功认证某个个体。
SI-13	在认证器因到期、撤销、终止、更新或CSP定义的其他方式而变得无效后，CSP应要求签约用户尽快放弃或销毁包含CSP签署之属性证书的任何物理认证器。	无法使用无效的认证器来成功认证某个个体。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-14	当在线身份不再存在时、当签约用户提出要求时，或者当CSP确定签约用户不再满足其资格要求时，CSP应立即撤销认证器的绑定。	无法使用无效的认证器来成功认证某个个体。
SI-15	生物特征识别应仅作为利用物理认证器（你拥有的东西）的多因素认证的一部分。	适当地将生物特征识别技术作为认证器。
SI-16	在较高AAL上，除了一个存储的秘密、或者一个或多个生物特征之外，CSP还应将至少一个、或者至少两个物理（你拥有的东西）认证器绑定于签约用户的在线身份。	认证器绑定于适当的签约用户。
SI-17	对较高AAL，如果无法在一次物理的“相遇”或电子的事务处理中完成登记和绑定，则应使用以下方法来确保在整个过程中由同一方作为申请方行事： 对于远程处理的事务： 1. 申请方应通过展示一个临时的秘密来在每次新的事务处理中证明自己的身份，该秘密在先前的事务处理期间建立，或者发送到申请方的电话号码、电子邮件地址或记录的邮政地址上； 2. 长期的认证器秘密应仅在受保护的会话中发放给申请方。 对于亲自处理的事务： 1. 申请方应使用上述远程事务处理（1）中所述的秘密，或者使用先前“相遇”中记录的生物特征来亲自证明自己的身份。 2. 不应重复使用临时的秘密。 3. 如果CSP在一次物理的事务处理期间发放了长期的认证器秘密，则应在本地将其加载到亲自签发给申请方的物理设备上，或者以确认记录地址的方式进行交付。	认证器绑定于适当的签约用户。
SI-18	当将附加的认证器绑定于签约用户的帐户时，CSP应首先要求签约用户至少对将使用新认证器的AAL进行认证。	认证器绑定于适当的签约用户。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-19	对较高AAL，如果签约用户丢失完成多因素认证所需的所有认证器，则该签约用户应重复身份证明过程。	在不规避预期AAL的情况下，签约用户能够恢复认证器。
SI-20	在为较高AAL替换丢失的认证因素时，CSP应要求声称方使用任何剩余因素的认证器进行认证，以确认与现有身份的绑定。	在不规避预期AAL的情况下，签约用户能够恢复认证器。
SI-21	应定期对会话进行重新认证，以确认签约用户继续存在于经认证的会话中。	要求签约用户定期以适当的认证器、以实现预期AAL所需的强度进行重新认证。
SI-22	应定期对签约用户会话进行重新认证。 (a) 在最低AAL上，无论用户活动如何，在扩展的使用会话期间，每30天都应至少对签约用户重复进行一次重新认证。 (b) 在最低AAL上，当达到该时间限制时，应终止（即注销）会话。 (c) 在较高AAL上，无论用户活动如何，在扩展的使用会话期间，每12小时都应至少对签约用户重复进行一次重新认证。 (d) 在较高AAL上，在任何非活动期持续30分钟或更长时间后，都应对签约用户重复进行重新认证。 (e) 在较高AAL上，当达到这些时间限制中的任意一个时，都应终止（即注销）会话。 (f) 在最高AAL上，无论用户活动如何，在扩展的使用会话期间，每12小时都应至少对签约用户重复进行一次认证。 (g) 在最高AAL上，在任何非活动期持续15分钟或更长时间后，都应对签约用户重复进行重新认证。 (h) 在最高AAL上，当达到时间限制(f) 或(g) 中的任意一个时，都应终止（即注销）会话。 (i) 在最高AAL上，应定期使用所有原始认证因素对签约用户会话进行重新认证。	要求签约用户定期以适当的认证器、以实现预期AAL所需的强度进行重新认证。

表8-6 – 签约用户冒充控制

CTRL #	控制描述	预期结果
SI-23	不应仅基于会话秘密的展示来扩展会话。	要求签约用户定期以适当的认证器、以实现预期AAL所需的强度进行重新认证。
SI-24	当会话因超时或其他行动而被终止时，应要求用户通过再次认证来建立新的会话。	要求签约用户定期以适当的认证器、以实现预期AAL所需的强度进行重新认证。
SI-25	会话秘密应是非永久的，也就是说，不应在重新启动关联的应用程序或重新启动主机设备时保留它们。	要求签约用户定期以适当的认证器、以实现预期AAL所需的强度进行重新认证。

8.6 认证业务损害、风险和控制

8.6.1 认证业务损害的风险

认证业务损害指的是对提供身份业务的实体实施的攻击，攻击将使之无效、不准确、不可用或无法按预期运行。实体信息系统控制环境中任何被利用的弱点都有可能损害认证业务。一个例子是，攻击者能够利用未打补丁的软件漏洞，并能够获得对认证业务信息系统的未经授权的特权访问。

8.6.2 认证业务损害的控制

表8-7列出了认证业务损害控制措施。

表8-7 – 认证业务损害控制

CTRL #	控制描述	预期结果
ASC-1	对于[b-ISO/IEC 27002]或等效标准定义的给定安全等级，CSP应采用适当量身定做的安全控制。	保护认证业务的完整性免遭损害。
ASC-2	考虑到整个系统的风险，CSP应确保满足与最低保证有关的控制。	保护认证业务的完整性免遭损害。
ASC-3	如果集中进行比较，则应实施生物特征撤销，在[b-ISO/IEC 24745]中称为生物特征模板保护。	认证业务保护生物特征信息。
ASC-4	认证意图应由认证器自己来建立，尽管多因素密码设备可以通过在认证器使用的端点上重新输入其他认证因素来建立意图。	认证意图仅由认证器建立。

表8-7 – 认证业务损害控制

CTRL #	控制描述	预期结果
ASC-5	在整个数字身份生命周期中，CSP应维护与每个身份关联或已与每个身份关联的所有认证器的记录。	记录和维护认证器信息。
ASC-6	在需要时，CSP或验证方还应维护限制认证尝试所需的信息。	记录和维护认证器信息。
ASC-7	CSP创建的记录应包含认证器绑定于帐户的日期和时间。	记录和维护认证器信息。
ASC-8	认证器应通过以下任一方式绑定于签约用户帐户： • 由CSP发布的内容作为登记的一部分；或者 • 关联CSP可接受的、签约用户提供的认证器。	认证器适当绑定于签约用户帐户。
ASC-9	当任何新的认证器绑定于签约用户帐户时，CSP应确保绑定协议和用于提供关联密钥的协议在与使用认证器的AAL相称的安全等级上完成。	认证器适当绑定于签约用户帐户。
ASC-10	多因素认证器的绑定应要求多因素认证或者与刚刚完成身份证明的会话相关联，以便绑定认证器。	认证器适当绑定于签约用户帐户。

8.7 隐私、风险和控制

8.7.1 隐私的风险

数字认证通过缓解未经授权访问个人信息的风险来支持隐私保护。同时，由于身份证明、认证、授权和联邦涉及对个人信息的处理，故这些功能也会带来隐私风险。因此，这些指南包括隐私要求和注意事项，以帮助缓解潜在的相关隐私风险。

CSP须进行隐私风险评估以保留记录。隐私风险评估的内容可包括以下内容：

1 保留记录可能给签约用户造成问题，例如，侵入或对信息的未授权访问。

2 如果确实发生了这样的问题，则所发生问题造成的影响。

CSP应该能够合理地证明其对已确定之隐私风险所采取的任何应对措施是正当的，包括接受风险、缓解风险和分担风险。使用签约用户同意书是分担风险的一种形式，因此仅在可以合理预期签约用户具有评估和接受所分担风险的能力时才适用。

8.7.2 隐私的控制

表8-8列出了隐私控制措施。

表8-8 – 隐私控制

CTRL #	控制描述	预期结果
P-1	当在线提供自断言的PII或其他个人信息时，IDP至少应选择一个适当的AAL。	CSP强制执行有关认证的隐私策略和隐私控制。
P-2	CSP应根据可能采用的适用的法律、法规和政策，遵循其各自的记录保留政策。如果CSP在没有任何强制性要求的情况下选择保留记录，则CSP应进行风险管理过程，包括评估隐私和安全风险，以确定应保留多长时间的记录，并应将这种保留政策告知签约用户。	CSP根据适用的法律、法规和政策对签约用户进行认证。
P-3	应注意确保PII的使用仅限于其最初的采集目的。	CSP收集最少数量的PII以实现预期AAL。
P-4	如果PII的使用不属于与认证有关的用途，或者不符合法律或法律程序要求，则CSP应予告知并征得签约用户的同意。	CSP根据适用的法律、法规和政策对签约用户进行认证。
P-5	IDP应根据适用的法律和法规进行或发布隐私影响评估结果（PIA），以涵盖对PII和其他个人信息的采集。	CSP进行PIA。
P-6	CSP除进行认证、缓解相关欺诈或者遵循法律或法律程序外，不得出于任何其他目的使用或披露有关签约用户的信息，除非CSP明确告知并征得签约用户的同意以用于其他用途。	CSP根据适用的法律、法规和政策对签约用户进行认证。
P-7	CSP应采用在[ISO/IEC 27002]或等效标准中定义的适当量身定制的隐私控制。	CSP强制执行有关认证的隐私策略和隐私控制。
P-8	CSP不应将同意作为业务的一个条件。	CSP根据适用的法律、法规和政策对签约用户进行认证。
P-9	虽然CSP可以将一个较低的AAL认证器绑定于一个较高的AAL身份，但如果在较低的AAL上对签约用户进行认证，则CSP不应向签约用户披露个人信息，即使它们是自断言的。	CSP收集最少数量的PII或个人信息以实现预期AAL。
P-10	签约用户接受其他用途不应成为提供认证业务的条件。	CSP根据适用的法律、法规和政策对签约用户进行认证。

附录I

使用[b-ITU-T X.1278]的强认证示例

（本附录非本建议书不可或缺的组成部分。）

I.1 引言

通用认证框架[b-ITU-T X.1277]和客户端到认证器协议/通用双重框架[b-ITU-T X.1278]提出了认证和认证保证的方法，这些方法基于开放、可互操作的建议书提供强认证。本附录提供了一个使用[b-ITU-T X.1278]的强认证示例。

I.2 威胁类别

图I.1突出显示了分为两个类别的威胁：

1 可扩展的攻击 – 攻击1 000个还是攻击1 000 000个目标都不会影响攻击成本。

a. 远程攻击服务器并窃取密码。此攻击非常严重，因为用户无法防御它 – RP必须这样做。不过，用户可使情况变得更糟：如果他们在多个RP之间共享密码，则最不安全的RP可能会被黑客入侵，从而影响所有其他用户；

b. 远程攻击大量用户设备。例如，尝试从设备窃取数据来冒充用户；

c. 远程攻击用户设备还可能导致滥用用户设备上的数据来冒充用户。

d. 远程攻击大量用户设备以滥用经强认证的会话。这就是所谓的MITB攻击。

有趣的是可以看到，仅智能卡并不能防止滥用证书，因为智能卡无法知道PIN是由用户输入的还是由以前从用户处网络钓鱼PIN的某些恶意软件注入的。

2 物理攻击 – 需要物理访问设备。物理攻击无法扩展，因为窃取（活动）智能手机每个目标的成本很高。

a. 物理攻击用户设备以窃取数据进行冒充；

b. 物理攻击用户设备以滥用用户设备进行冒充。

I.3 [b-ITU-T X.1278]启用“高保证的强认证”

高保证的强认证意味着：

1 使用两个或更多个因素；

2 至少一个因素利用公钥密码术；

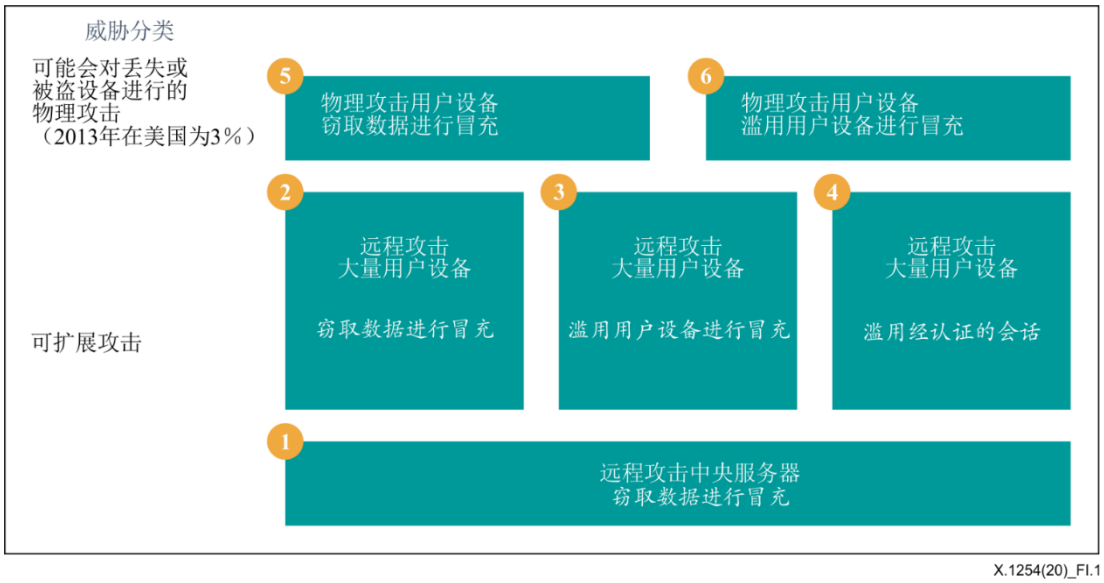
3 不易遭受网络钓鱼、MITM和/或其他针对证书的攻击。

快速身份在线（FIDO）方法的主要区别包括：

- 没有共享秘密 – 使用你拥有的东西（例如，硬件设备）和你的身份/生物特征（例如，指纹）；
- 使用公钥密码术而不是对称的共享秘密；
- 用户通过认证器验证后，而后认证器通过RP进行认证；以及
- 防网络钓鱼的多因素认证。

这些方法支持以下安全和隐私原则：

- 业务或帐户之间没有可链接性；
- 协议中没有第三方；
- 如若用了，则生物特征永远不要离开设备；
- 加密密钥保留在设备上；
- 没有服务器端的共享秘密；以及
- 基于公钥密码术。



图I.1 – 威胁分类

I.4 使用密码的旧的认证过程

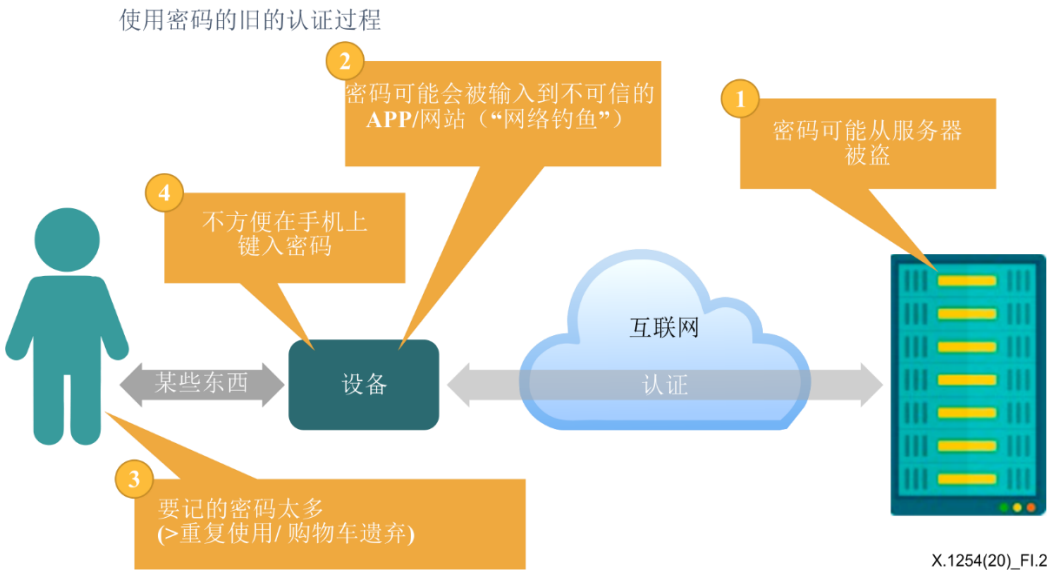
典型的、基于密码的认证过程有若干固有风险，如图I.2所示：

1 密码可从服务器被盗（数据泄露）；

2 密码可能会被输入到不可信的APP或网站中（网络钓鱼）；

3 要记太多密码会导致更大的重复使用（更容易猜测不同站点上的密码）；

4 不方便在手机上键入密码（用户选择更容易猜测的密码）。



图I.2 – 使用密码的旧的认证过程

I.5 使用[b-ITU-T X.127833]的新的认证过程

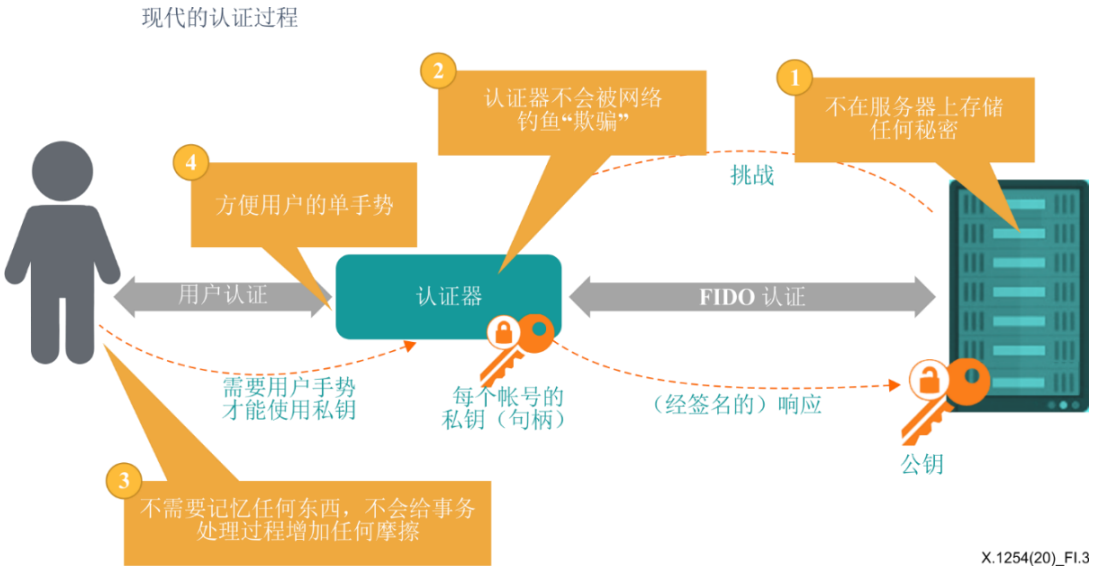
FIDO将认证方面的问题与身份方面的问题分开。图I.3显示了这种方法的好处：

1 不在服务器上存储任何秘密（防止数据泄露）；

2 认证器不会被网络钓鱼欺骗；

3 无需记住密码，也不会增加认证过程的麻烦；不需要记忆任何密码，不会给认证过程增加任何摩擦；

4 方便用户的单手势。



图I.3 – 使用[b-ITU-T X.1278]的新的认证过程

I.6 互操作性和认证

除了创建新的认证方法外，还通过互操作性和认证测试来提高认证解决方案的强度。

- 提高用户或消费者对强认证的接受度；
- 通过更加广泛地部署强认证来降低身份盗用的风险和影响；
- 通过大量认证设备和服务来便利和改善用户体验；
- 降低成本可以增加对强认证的采用。

参考书目

[b-ITU-T X.1252] ITU-T X.1252 (2010)建议书，基线身份管理术语和定义。

[b-ITU-T X.1254 (2012)] ITU-T X.1254 (2012)建议书，实体认证保证框架。

[b-ITU-T X.1277] ITU-T X.1277 (2018)建议书，普遍认证框架。

[b-ITU-T X.1278] ITU-T X.1278 (2018)建议书，客户端到认证器协议/通用双重框架。

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 24745] ISO/IEC 24745:2011, *Information technology — Security techniques — Biometric information protection*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT security and privacy – A framework for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2018), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

[b-ISO/IEC TS 29003] Technical Specification ISO/IEC TS 29003:2018, *Information technology – Security techniques – Identity proofing*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework.*

[b-IETF RFC 7231] IETF RFC 7231 (2014), *Hypertext transfer protocol (HTTP/1.1): Semantics and content*

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦