国际电信联盟
电信标准化部门

建议书

# ITU-T X.1280 (03/2024)

X系列：数据网络、开放系统通信和安全

网络空间安全 – 身份管理（IdM）和认证

# 使用移动设备的带外服务器认证框架

ITU-T X 系列建议书

**数据网络、开放系统通信和安全**

| | |
|---|---|
| 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 | X.1000-X.1099 |
| 安全应用和服务（I） | X.1100-X.1199 |
| 网络空间安全 | X.1200-X.1299 |
| 网络安全 | X.1200-X.1229 |
| 反垃圾信息 | X.1230-X.1249 |
| **身份管理（IdM）和认证** | **X.1250-X.1299** |
| 安全应用和服务（II） | X.1300-X.1499 |
| 网络安全信息交换 | X.1500-X.1599 |
| 云计算安全 | X.1600-X.1699 |
| 量子通信 | X.1700-X.1729 |
| 数据安全 | X.1750-X.1799 |
| 国际移动通信（IMT）安全 | X.1800-X.1839 |
| 元宇宙和数字孪生安全 | X.2000-X.2199 |
| 软件供应链安全 | X.2150-X.2199 |
| 人工智能（AI）/机器学习（ML）安全 | X.2200-X.2249 |

欲了解更详细信息，请查阅 ITU-T 建议书目录。

# ITU-T X.1280 建议书

## 使用移动设备的带外服务器认证框架


### 摘要

在认证技术标准中，防止验证方假冒被认为是一项最高级别认证保证的要求。然而，现有的认证技术集中于用户认证，因此存在不能明确验证服务提供商的限制。

ITU-T X.1280建议书提供了一个使用移动设备进行带外服务器认证的框架，解决了验证方假冒的漏洞以及现有认证器用户终端依赖性的限制。它允许用户在任何用户终端上的用户认证过程中，在明确和独立地验证服务提供商后，提供用户认证信息。



### 历史沿革 *

| 版本 | 建议书 | 批准时间 | 研究组 | 唯一ID |
|---|---|---|---|---|
| 1.0 | ITU-T X.1280 | 2024-03-01 | 17 | 11.1002/1000/15661 |

### 关键词

认证、认证器、信任方、验证、验证方、防止验证方假冒。


* 欲查阅建议书，请在网络浏览器地址域键入URL https://handle.itu.int/，随后输入建议书的唯一识别码.

## 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

# ITU-T X.1280 建议书

# 使用移动设备的带外服务器认证框架

## 1 范围

本建议书提供了一个使用移动设备的带外服务器认证框架，包括以下内容：

- 定义带外服务器认证模式和认证程序；
- 定义使用移动设备生成服务器认证信息的标准和准则；
- 定义带外服务器认证模式中的安全威胁和安全要求；
- 描述带外服务器认证模式的用例；以及
- 描述与其他认证技术的关系。

本建议书不解决与用户认证、监管和隐私方面的考虑相关的问题。

## 2 参考资料

下列ITU-T建议书和其他参引的条款，通过在本文本中的引用而构成当前建议书的条款。所注明版本在出版时有效。所有的建议书和其他参引均会得到修订，鼓励本建议书的所有使用者查证是否有可能使用下列建议书或其他参引的最新版本。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

## 3 定义

### 3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

**3.1.1 认证（authentication）** [b-ISO/IEC 18014-2]：对一个实体声称的身份提供保证。

**3.1.2 证书服务提供商（credential service provider (CSP)）** [b-ITU-T X.1254]：颁发或管理证书的可信参与者。

**3.1.3 信任方（relying party (RP)）** [b-ITU-T X.1254]：信任某一身份断言或声明的参与者。

**3.1.4 验证（verification）** [b-ISO/IEC 29115]：通过将所提供的信息与先前已证实的信息进行比较来对信息进行检查的过程。

**3.1.5 验证方（verifier）** [b-ISO/IEC 29115]：证实身份信息的参与者。

### 3.2 本建议书定义的术语

本建议书定义了下列术语：

**3.2.1 服务器认证（Server authentication）**：通过比较由验证方生成的服务器认证信息和用户的带外服务器认证器来验证服务提供商真实性的过程。

**3.2.2 服务器认证信息（Server authentication information）**：在验证方和用户的带外服务器认证器中使用询问-应答一次性密码（OTP）算法生成的认证码。

**3.2.3 带外用户认证（Out-of-band user authentication）：**使用另一个通信信道验证用户真实性的过程，该信道独立于用于登录或执行交易的通信信道。

**3.2.4 带外服务器认证（Out-of-band server authentication）：**使用另一个通信信道验证服务器真实性的过程，该信道独立于用于登录或执行交易的通信信道。

## 4 缩写词和首字母缩略词

本建议书使用以下缩写词和首字母缩略语：

AI 人工智能

ATM 自动柜员机

CSP 证书服务提供商

CTAP 客户端到认证器协议

DNS 域名系统

FIDO 在线快速身份识别

ID 身份识别

IdP 身份提供商

IP 网际协议

OAuth 开放认证

OTP 一次性密码

PAM 可插拔认证模块

PIN 个人身份识别码

PKI 公钥基础设施

RP 信任方

SAML 安全断言标记语言

SMS 短信服务

SSL 安全套接字层

QR 快速响应码（即二维码）

U2F 通用双因素

## 5 惯例

本建议书采用以下文字形式来表达规定：

a) “须”表示一项要求，

b) “应/应该”表示一项建议，

c) “可/可以”表示一项许可/允许，

d) “可/可能”表示一种可能性或能力。

## 6 引言

在传统的用户认证中，只有服务器对用户进行认证，用户容易受到网络攻击，如网络钓鱼和网址嫁接。

当用户使用带有地址栏的基于浏览器的应用程序时，基于公钥基础设施（PKI）的服务器认证已足够。基于PKI的认证也是独立于用户认证过程执行，这使得用户很容易被忽略。

本建议书为使用移动设备的带外服务器认证提供了一个框架，旨在由用户首先对服务器进行认证，并帮助用户明确地参与与用户认证过程相关的服务器认证。在用户认证中，任何用户认证过程都可以一起应用。

基于浏览器的应用程序以及许多类型的应用程序和操作系统都可以使用带外服务器认证。

由用户验证服务器认证信息，然后由服务器验证用户认证信息，来执行带外服务器认证，从而防止验证方假冒。

借助带外服务器认证，服务提供商和用户可以获得以下益处：

1) 以用户为中心的认证：服务器显示其认证信息，以便用户对服务器进行认证，而不是要求用户记住并输入复杂的用户认证信息。通过将用户的角色从输入用户认证信息变为验证服务器认证信息，用户从用户证书管理负担中解脱出来。图1显示了以用户为中心的认证。


**图1 – 以用户为中心的认证**

2) 相互认证：用户分别使用服务器和带外服务器认证器生成的服务器认证信息来验证服务器的真实性。在用户确认两个服务器认证信息匹配之后，服务器利用发送的用户认证信息来验证用户的真实性。图2显示了相互认证。

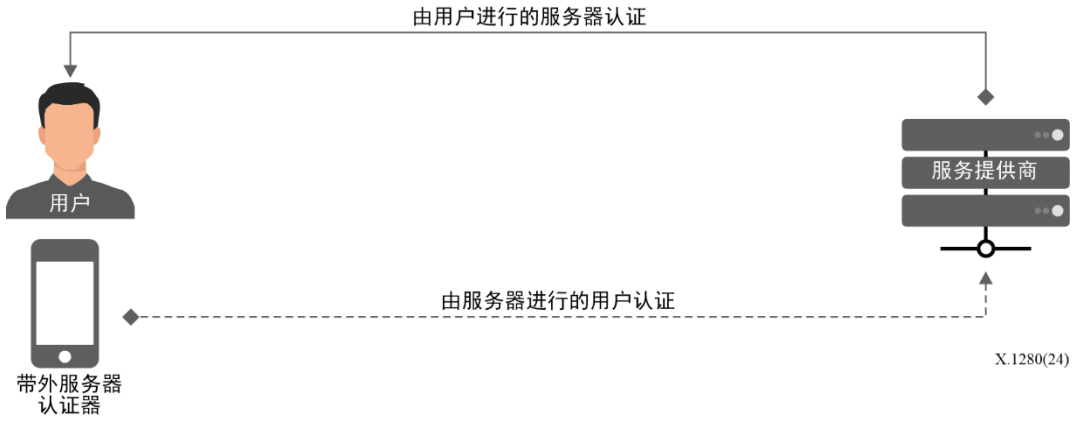



**图2 – 相互认证**

3) 统一认证：即使添加了更多额外的用户终端，如计算机、智能手机、自动柜员机（ATM）和人工智能（AI）扬声器，认证方法也可以统一，因为服务器向用户呈现他们的服务器认证信息，而不是要求用户输入各种认证信息。图3显示了统一认证。

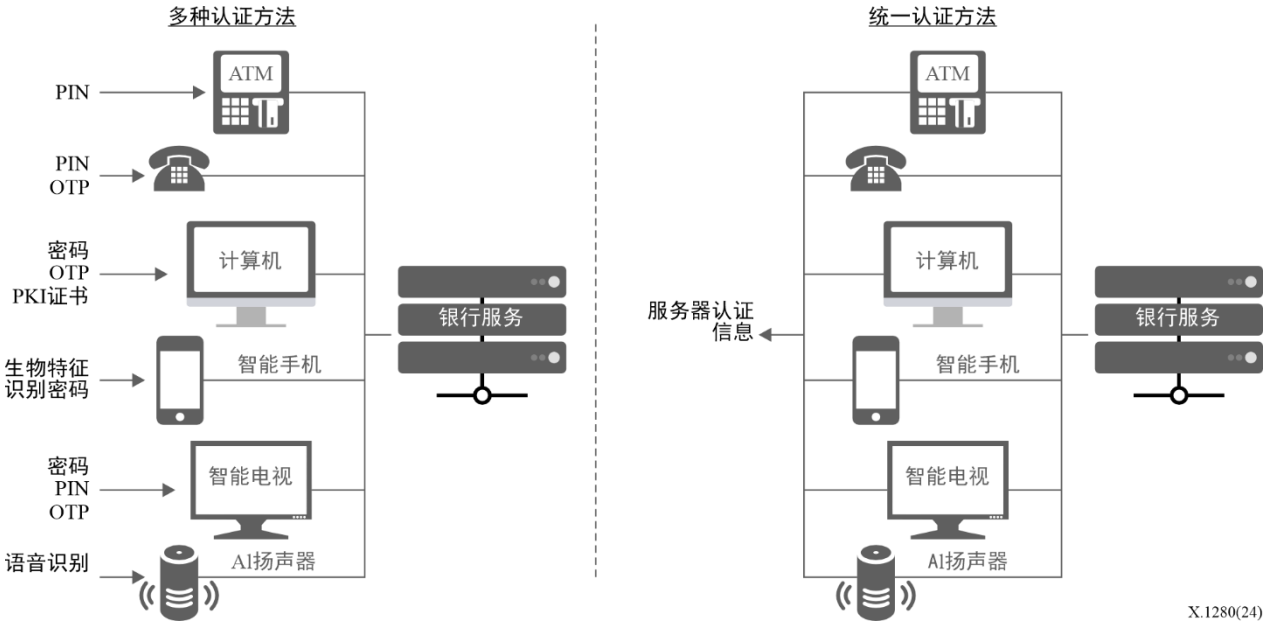



**图3 – 统一认证（如银行服务）**

## 7 带外服务器认证框架

本节定义了带外服务器认证框架认证模式的角色和组件，该框架支持用户与服务器之间的相互认证。核心流程是首先由用户验证服务器认证信息，而后由服务器验证用户认证信息。

### 7.1 角色和组件

表1列出了带外服务器认证框架的角色和组件。

**表1 – 带外服务器认证模式的角色和组件**

| 名称 | 描述 |
|---|---|
| 验证方 | 验证方响应用户的请求，生成服务器认证信息。该信息被发送给信任方，以呈现给用户。它将用于生成服务器认证信息的偏移量发送给带外服务器认证器，以生成呈现给用户的服务器认证信息。 |
| 信任方 | 信任方向用户呈现由验证方生成并发送的服务器认证信息。 |
| 用户 | 用户从信任方和验证方接收服务。 |
| 用户终端 | 用户终端通过应用程序显示服务器认证信息。用户终端的例子有计算机、智能手机、ATM和AI扬声器。 |
| 带外服务器认证器 | 带外服务器认证器使用验证方发送的偏移量生成服务器认证信息。 |

## 7.2 服务器认证信息

服务器认证信息是用户认证服务器时使用的一个多位数字码。一旦用户请求，须使用询问-应答一次性密码（OTP）生成。动态询问值和验证密钥用于计算和生成服务器认证信息。在第8节中定义了动态询问值和验证密钥。

如果服务器生成的服务器认证信息与用户的带外服务器认证器生成的服务器认证信息相匹配，则服务器的真实性得到验证。

## 7.3 认证模式

带外服务器认证的主要流程是用户首先通过比较验证方和带外服务器认证器生成的服务器认证信息来认证服务器。一旦用户对服务器进行了认证，认证器就会生成用户认证信息，并将之发送给验证方。验证方用用户认证信息来对用户进行认证。

图4概述了使用移动设备进行的带外服务器认证。

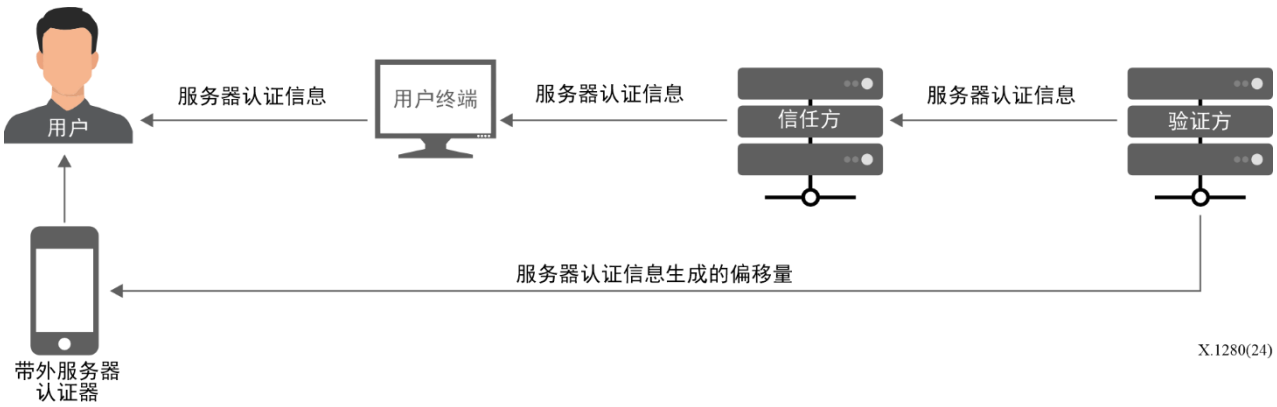



**图4 – 使用移动设备的带外服务器认证概述**

为了使用移动设备启动带外服务器认证，需要用户通过屏幕将用户ID键入用户终端。一旦用户在用户终端上输入ID，信任方须首先在用户终端中向用户呈现由验证方生成的服务器认证信息。而后用户将之与用户的带外服务器认证器生成的服务器认证信息进行比较。

## 8 带外服务器认证的程序

### 8.1 带外服务器认证器的安装和注册

在带外服务器认证器安装和注册步骤中，用户在智能手机上安装认证器应用程序，并在验证方中注册。

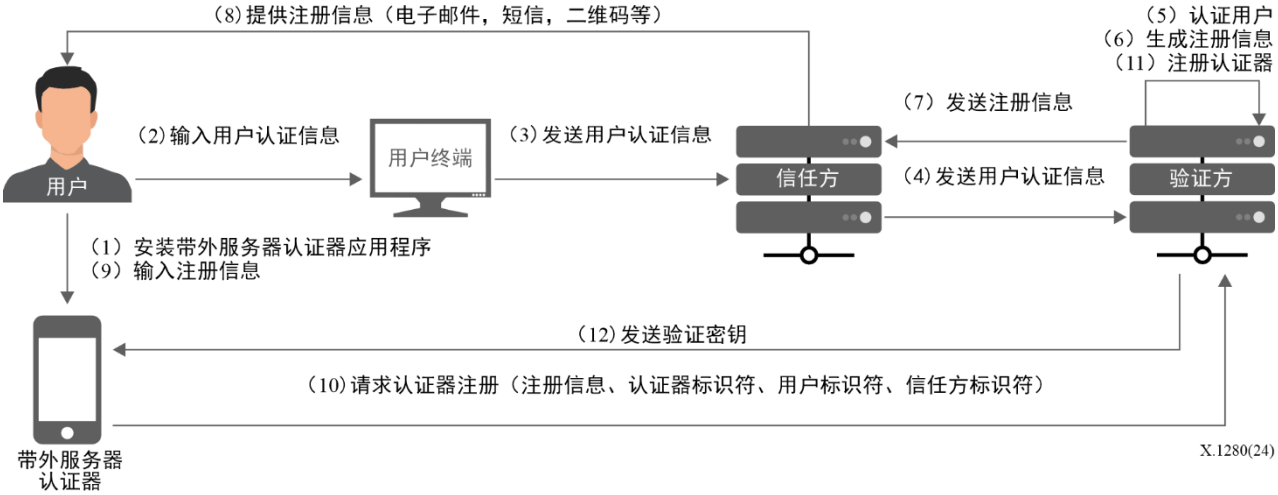



**图5 – 带外服务器认证器安装和注册流程**

图5确定带外服务器认证器安装和注册步骤中所需的数据，并显示流程。对该流程解释如下：

(1) 用户在智能手机上安装带外服务器认证器应用程序。

(2) 根据信任方的策略，用户通过用户终端输入用户认证信息，以通过一种可靠的方法（如登录、电子邮件验证或移动电话识别）来认证为一个合法用户。

(3) 将在用户终端上输入的用户认证信息发送给信任方。

(4) 信任方将用户认证信息发送给验证方。

(5) 验证方验证用户。

(6) 验证方生成对应于所认证用户的注册信息。

(7) 验证方向信任方发送生成的注册信息，包括信任方的用户标识符和信任方标识符。

(8) 信任方使用可信方法向用户提供注册信息，如电子邮件、文本消息、快速响应（QR）码等。

(9) 用户将认证器注册信息输入到安装在智能手机上的认证器中。

(10) 认证器将注册信息、认证器标识符、用户标识符和信任方标识符发送给验证方。

(11) 验证方验证注册信息，并用认证器标识符、用户标识符和信任方标识符注册认证器。

(12) 注册认证器后，验证方将相应的验证密钥发送给认证器。

须通过使用ITU-T X.509证书应用安全套接字层（SSL）协议来提供和执行带外服务器认证器注册流程，以保护认证器与验证方之间的安全通信。

在带外服务器认证器因丢失或损坏而无法使用的情况下，验证方可允许用户注册一个以上的带外服务器认证器作为备用认证器。

## 8.2 服务器认证请求

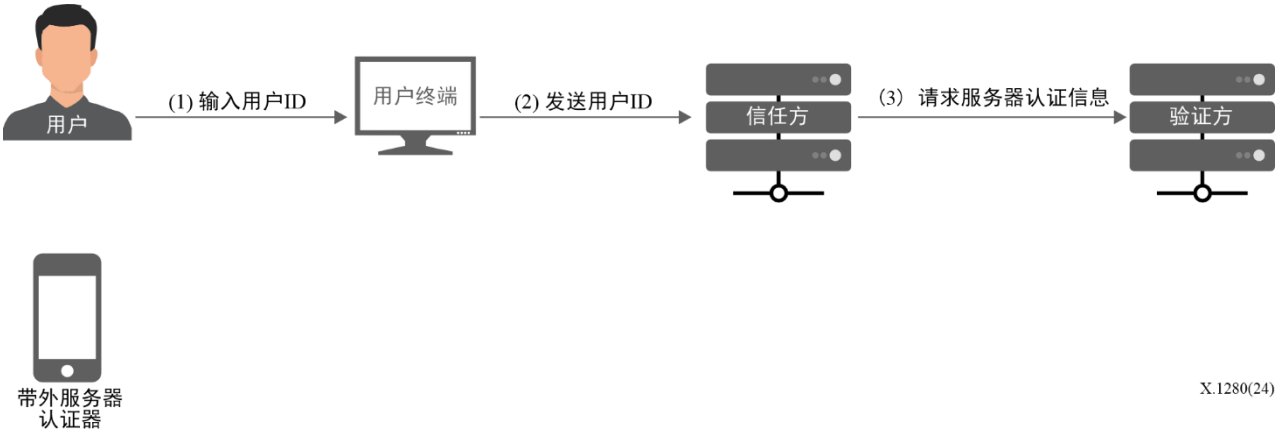



**图6 – 服务器认证请求流程**

图6确定服务器认证请求步骤中所需的数据，并显示流程。对该流程解释如下：

(1) 用户终端中的用户连接到信任方，然后输入其ID。

(2) 将在用户终端中输入的用户ID发送给信任方。

(3) 信任方向验证方请求服务器认证信息。

## 8.3 服务器认证信息的生成和呈现

在服务器认证信息生成和呈现步骤中，一旦接收到来自信任方的服务器认证请求，验证方就生成对应于用户ID的服务器认证信息。然后，验证方将服务器认证信息发送给信任方，以显示在用户终端的屏幕上。验证方还将偏移量发送给用户的带外服务器认证器。认证器使用接收到的偏移量来生成服务器认证信息，并呈现生成的服务器认证信息。

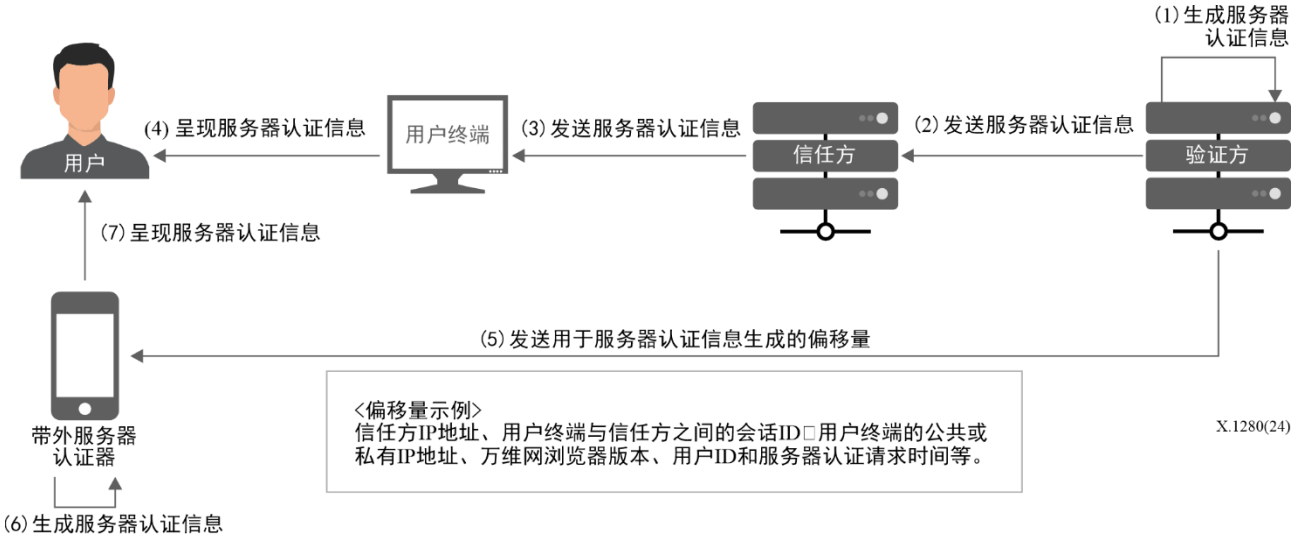



**图7 – 服务器认证信息生成和呈现流程**

图7确定服务器认证信息生成和呈现步骤中所需的数据，并显示流程。对该流程解释如下：

(1) 一旦接收到服务器认证请求，验证方就生成服务器认证信息，包括用户ID和来自信任方的偏移量。验证方利用验证密钥和偏移量计算并生成服务器验证信息，验证方和用户的带外认证器都已在带外服务器验证器安装和注册步骤期间接收并存储验证密钥。

(2) 验证方将生成的服务器认证信息发送给信任方。

(3) 信任方将接收到的服务器认证信息发送给用户终端。

(4) 信任方通过用户终端向用户呈现服务器认证信息。

(5) 验证方还将用于生成服务器认证信息的偏移量发送给用户的带外服务器认证器。

(6) 用户的带外服务器认证器利用验证密钥和偏移量计算并生成服务器认证信息，验证方和用户的带外认证器都已在带外服务器认证器安装和注册步骤期间接收并存储验证密钥。

(7) 带外服务器认证器也将自己生成的服务器认证信息呈现给用户。

偏移量应包括信任方服务器的网际协议（IP）地址、用户终端与信任方服务器之间的会话ID、用户终端的公共IP地址、用户终端的私有IP地址、用户终端的万维网浏览器版本、用户ID和用户的服务器认证请求时间。

应使用验证密钥和偏移量来计算和生成服务器认证信息，然后应将之转换为用户易于阅读的值。该值至少应为6位数字或字符串。该值应显示在用户终端和带外服务器认证器上。此外，根据在线服务的类型，服务器认证信息应具有适当的有效时间，并应在如图8所示的服务器认证信息显示区域内以各种形式直观地显示剩余的有效时间。

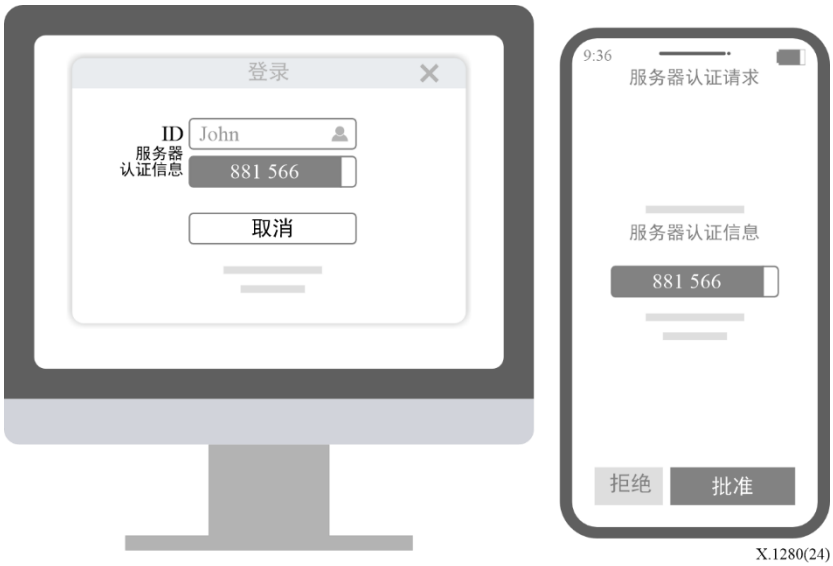



**图8 – 服务器认证信息呈现示例**

替代由用户比较认证信息，信任方可以显示QR码，该QR码包括用于带外服务器认证器读取和验证代码的服务器认证信息。然后，认证器向用户显示可理解的信息，以便他们可以验证服务器是否真实。

## 8.4 服务器认证

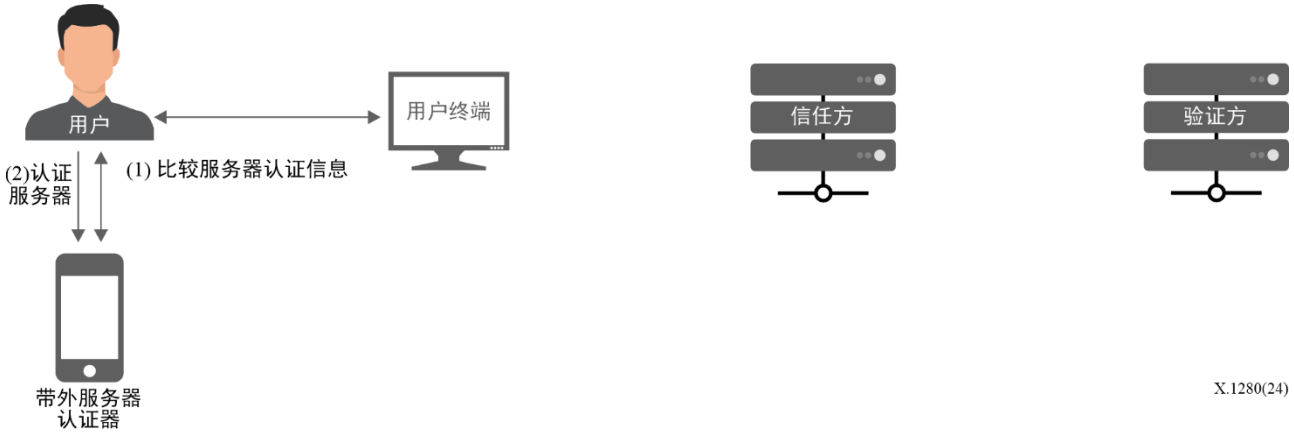



**图9 – 服务器认证流程**

图9确定服务器认证步骤中所需的数据，并显示流程。对该流程解释如下：

(1) 用户可视地比较和验证终端和带外服务器认证器中呈现的服务器认证信息。

(2) 用户通过在用户带外认证器中选择批准来对服务器进行认证。

## 8.5 用户认证和服务提供

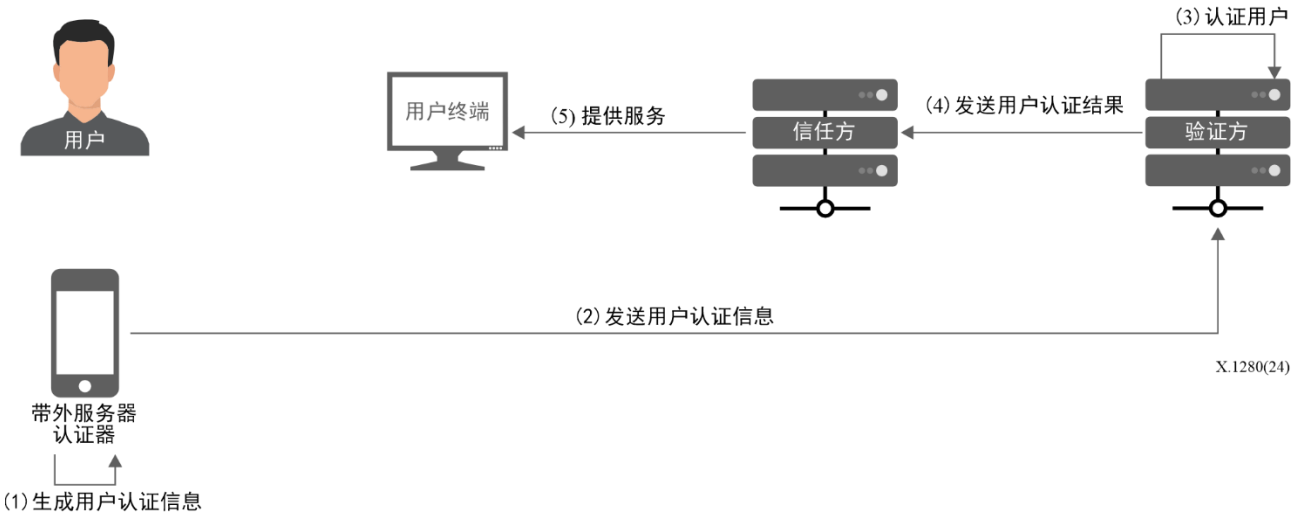



**图10 – 用户认证和服务提供流程**

图10确定用户认证和服务提供步骤中所需的数据，并显示流程。对该流程解释如下：

(1) 当用户在用户的带外服务器认证器中对服务器进行认证时，认证器生成用户的动态用户认证信息，如一次性密码。为了确认合法用户对认证器的使用，可以在智能手机上使用用户的面部和指纹或个人身份识别码（PIN）等生物特征信息来识别用户。

(2) 用户的带外服务器认证器将用户认证信息发送给验证方。

(3) 验证方通过验证接收到的用户认证信息来认证用户。

(4) 验证方将用户认证结果发送给信任方。

(5) 信任方根据从验证方接收的用户认证结果来提供服务。

替代动态用户认证信息，可以使用基于PKI的强用户认证，例如PKI和快速身份在线（FIDO）。基于PKI的用户认证中所需的询问值可以在服务器认证信息生成和呈现步骤中一起接收，或者接收到的偏移量可以用作询问值。

# 9 安全威胁和安全要求

## 9.1 安全威胁

在本节中，确定了带外服务器认证模式可能带来的潜在安全威胁。

### 9.1.1 欺诈性在线服务提供商

攻击者让用户访问欺诈性在线服务提供商，并诱使用户输入其密码以被窃取，而不是使用带外服务器认证器。

### 9.1.2 无法使用带外服务器认证器

如果用户因认证器丢失或损坏而无法使用其带外服务器认证器，则用户可能无法访问在线服务，因为他们可能忘记了当前的用户密码，或者可能无法使用另一种认证方法。

### 9.1.3 未经授权使用带外服务器认证器

攻击者可使用用户的带外服务器认证器，例如，通过窃取的方式。

### 9.1.4 对带外服务器认证器的远程攻击

攻击者可以通过在安装了用户的带外服务器认证器的智能手机上安装恶意软件来远程执行认证。

### 9.1.5 虚假服务器认证请求

当用户使用提供带外服务器认证的在线服务时，当用户通过比较和验证服务器认证信息来尝试服务器认证时，攻击者通过在不同的终端中输入用户ID来向用户的带外认证器发送虚假服务器认证请求，以诱使用户执行错误的认证。

## 9.2 安全要求

在本节中，描述了安全要求，以应对带外服务器认证模式可能带来的潜在安全威胁。附录I中描述了每种安全威胁与安全要求之间的关系。

### 9.2.1 用户密码认证限制

为了防止注册带外服务器认证器的用户窃取或泄露用户密码，可以限制用户密码认证方法，并且仅允许通过带外服务器认证器的用户认证。

### 9.2.2 释放带外服务器认证器和重置用户密码的额外方法

应提供额外的方法来释放注册的带外服务器认证器，并通过单独的用户认证（如身份认证、电子邮件验证和安全问题）来重置用户密码。

### 9.2.3 带外服务器认证器内的其他认证方法

当通过认证器来认证服务器时，可以提供其他的认证方法来验证用户是合法的，例如，通过安装了带外服务器认证器的智能手机的PIN或生物特征认证。

### 9.2.4 同步服务器认证请求控制

在带外服务器认证器显示服务器认证信息后，新的服务器认证请求应被阻止或排队，直至用户完成服务器认证。

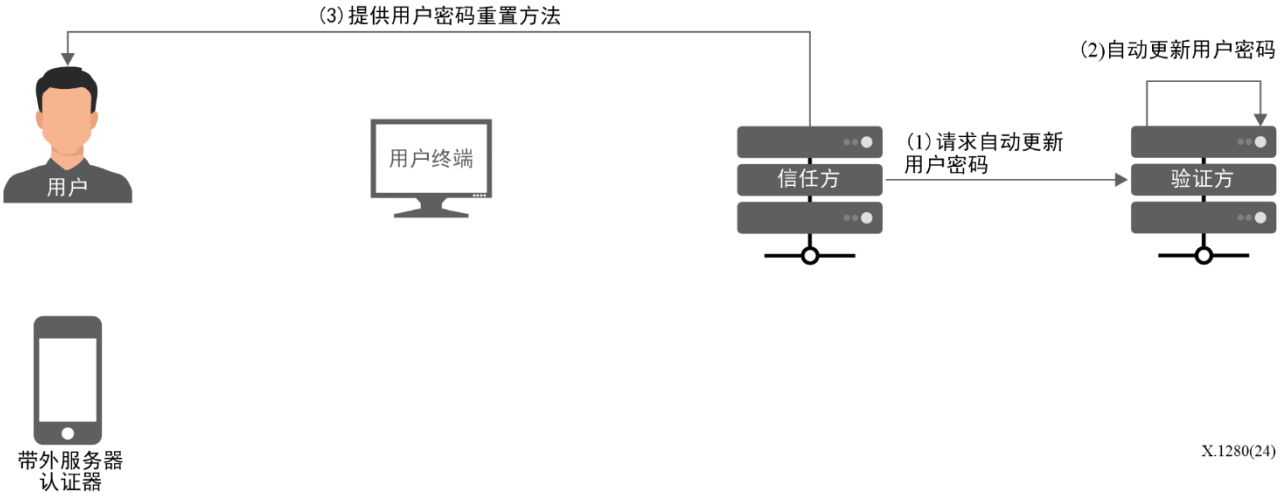
# 附件A

## 带外服务器认证的额外过程

（本附件是本建议书不可分割的组成部分）

### A.1 用户密码自动更新

在用户密码自动更新步骤中，在信任方通过带外服务器认证向用户提供服务之后，在线服务提供商自动更新用户账户的密码。在线服务提供商可以维护用户密码的概念，以最大限度地减少对现有数据结构和功能的更改，同时也加强用户密码的安全性。




**图A.1 – 用户密码自动更新流程**

图A.1确定了用户密码自动更新步骤中所需的数据，并显示了流程。该流程假设验证方执行用户密码自动更新，并且它可以由信任方或验证方来执行。对该流程解释如下：

(1) 带外服务器认证后，在信任方向用户提供服务之后，向验证方发送用户的用户密码更新请求。

(2) 验证方使用一种复杂的规则将用户密码更改为一个随机生成的值。

(3) 在因丢失等原因而无法使用用户注册的带外服务器认证器的情况下，信任方提供一种方法来释放认证器并通过单独的用户认证来重置用户密码，以便用户利用重置的用户密码来使用服务。

用户可以管理其用户密码，而无需自己定期更改密码，并保持安全，防止密码泄露。

# 附录I

## 安全要求与威胁之间的关系

（本附录非本建议书不可分割的组成部分。）

在本附录中，表I.1定义了带外服务器认证模式可能产生的潜在安全威胁与安全要求之间的关系。

**表I.1 – 安全要求与威胁之间的关系**

| 安全要求 | 安全威胁 | | | | |
|---|---|---|---|---|---|
| | 欺诈性在线服务 | 无法使用带外服务器认证器 | 未经授权使用带外服务器认证器 | 对带外服务器认证器的远程攻击 | 虚假服务器认证请求 |
| 用户密码认证限制 | o | - | - | - | - |
| 额外的认证方法 | - | o | - | - | - |
| 其他的用户认证方法 | - | - | o | o | - |
| 同步服务器认证请求控制 | - | - | - | - | o |

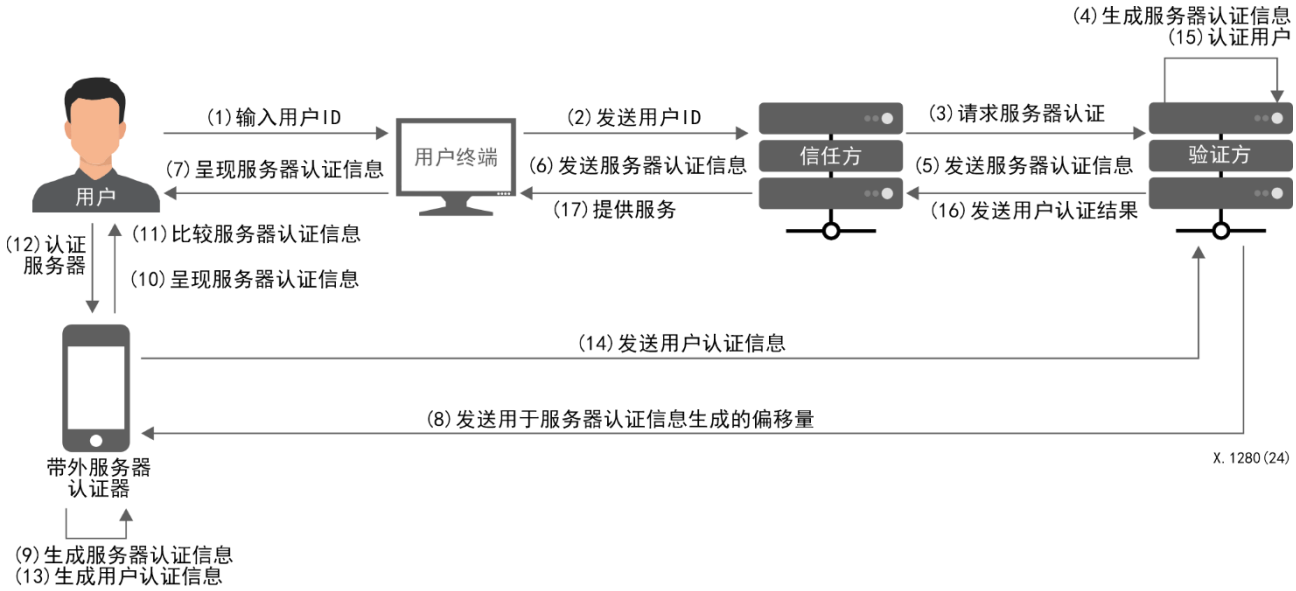
# 附录II

## 带外服务器认证模式的用例

（本附录非本建议书不可分割的组成部分。）

### II.1 网站和应用程序

网站、万维网应用程序以及不使用万维网浏览器的各种应用程序，可以通过应用带外服务器认证模式来解决基于PKI的服务器认证的限制。



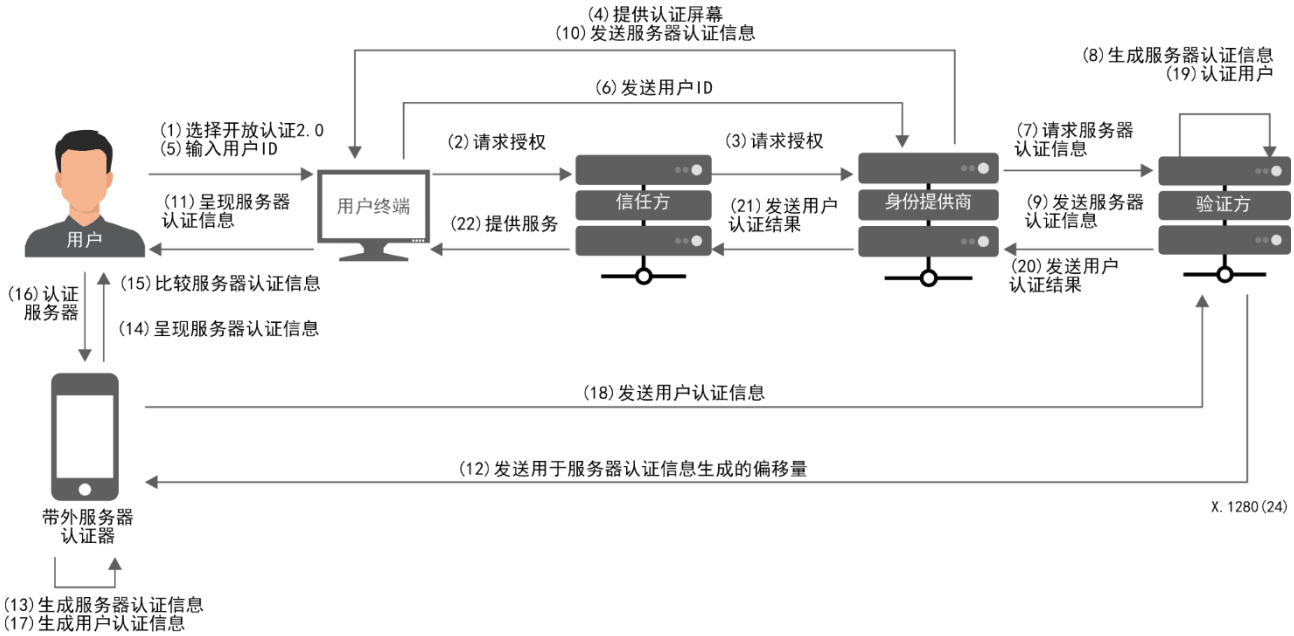

**图II.1 – 网站和应用程序的带外服务器认证流程**

图II.1显示了网站和应用程序的带外服务器认证流程。

即使在使用不能通过认证机构获得PKI证书的私有域名系统（DNS）的公司网站和万维网应用程序、基于IP地址的应用程序以及不使用万维网浏览器的应用程序的情况下，在首先清楚地验证在线服务提供商之后，用户也可以安全地执行认证。

### II.2 身份提供商（IdP）

提供OAuth 2.0和安全断言标记语言（SAML）服务的身份提供商（IdP）可以应用带外服务器认证模式来保护与其连接的所有在线服务的用户账户安全。




**图II.2 – IdP的带外服务器认证流程**

图II.2显示了IdP的带外服务器认证流程。

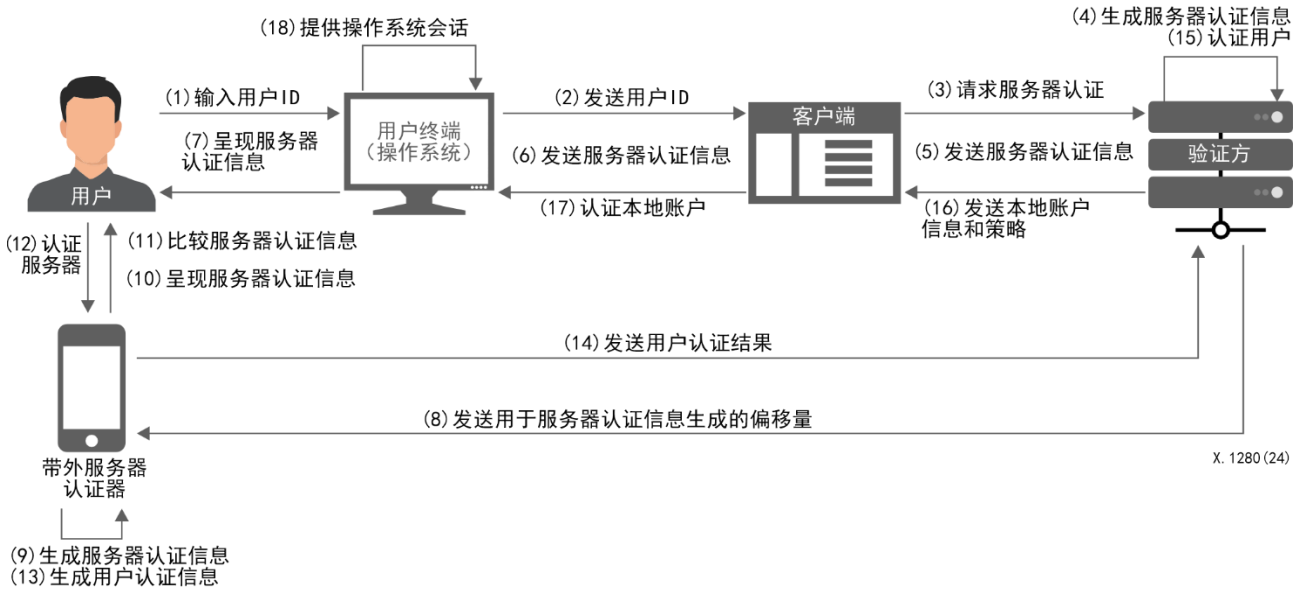
如果ID提供商的用户认证信息因假冒IdP认证屏幕的网络攻击而被泄露，则用户注册的所有服务提供商的用户账户都可能处于危险中。通过添加带外服务器认证，IDP可以免受网络钓鱼和网址嫁接。

## II.3 操作系统

基于Windows和Linux的操作系统可以应用带外服务器认证模式来加强操作系统本地账户的安全性。

为了将认证模式应用于基于Windows的操作系统，有必要安装和配置一个可以控制操作系统证书的第三方证书提供商客户端。

为了将认证模式应用于基于Linux的操作系统，有必要安装和配置可插拔认证模块（PAM）。




**图II.3 – 操作系统的带外服务器认证流程**

图II.3显示了操作系统的带外服务器认证流程。

用户可以清楚地验证其试图访问的操作系统是正确的，并且即使操作系统在云上运行，也有可能防止因在纸上写下访问信息或与其他用户共享访问信息而导致的事故。

此外，如果应用用户密码自动更新（带外服务器认证程序中的一个附加步骤），则可以更轻松、更安全地管理本地账户的密码更改策略。

输入用户ID后，在验证操作系统登录屏幕和带外服务器认证器上显示的服务器认证信息之后，用户可以使用操作系统。用户无需键入用户密码或使用密钥文件来访问操作系统。

此外，如果将用户密码自动更新（带外服务器认证程序中的一个附加步骤）应用于客户端，则可以通过自动更改操作系统本地账户的密码来更轻松、更安全地管理操作系统账户。

# 附录III

## 与其他认证技术的关系

（本附录非本建议书不可分割的组成部分。）

认证技术是在数字时代维护用户和在线服务提供商之间信任的一种基本技术。考虑到认证的安全性、成本效益和便利性，有各种各样的认证技术（如OTP、FIDO和移动推送认证）得到了广泛开发和使用。因此，在[b-ITU-T X.1254]、[b-ISO/IEC 29115]和[b-NIST SP 800-63-3]中为新的认证技术归类了不同的认证保证级别。

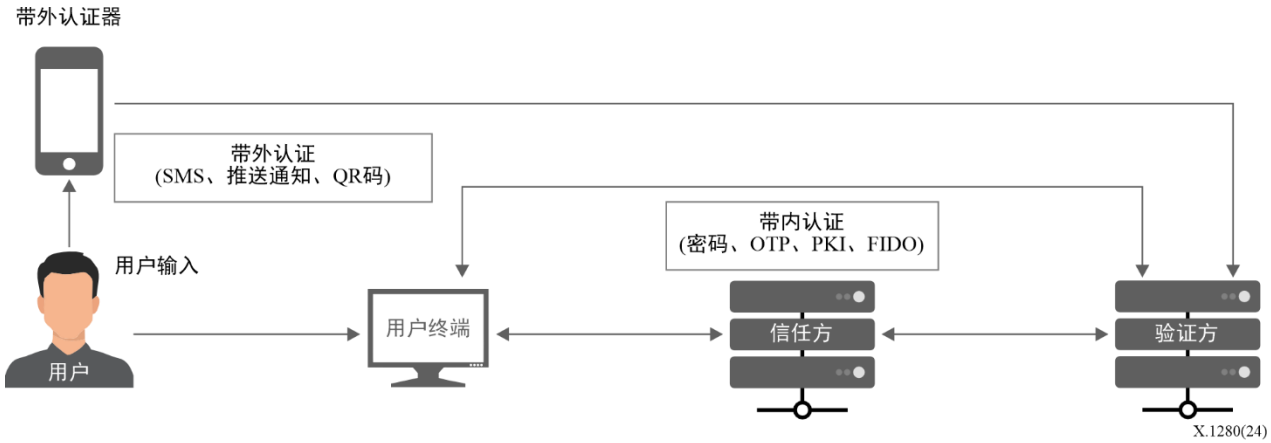
随着认证技术的增强和标准化，非常需要提供防止验证方假冒以及用户真实性。符合要求的认证技术被归类为最高级别。

然而，由于现有的认证技术仅认证用户，因此在仅向服务提供商提供用户认证信息而用户无需对其进行明确验证以防止验证方假冒的情况下，存在局限性。

现有的用户认证技术主要可分为带内认证和带外认证，带内认证通过服务提供商服务器与用户之间的主通信信道提供认证信息，带外认证通过一个单独的通信信道提供认证信息。

带内认证技术是防止验证方假冒的，但不方便且不经济。带外认证技术既方便又经济，但易受验证方假冒。

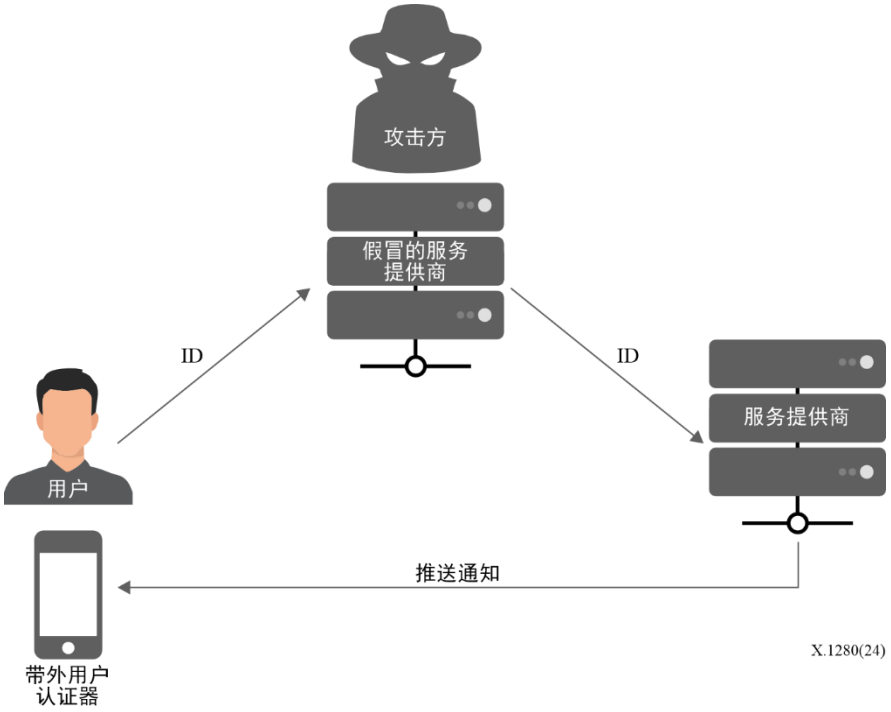
图III.1说明了带内和带外认证的认证信息流。




**图III.1 – 带内和带外认证的认证信息流**

诸如PKI技术之类的带内认证仅隐含地提供防止验证方假冒，因为它没有明确地向用户提供一种用于验证服务提供商的方法。如果服务器或应用程序发生变化，则它需要重新识别用户，并在用户终端上重新颁发证书。特别是，FIDO是一种典型的带内认证技术，因为认证器通过当前连接到信任方的终端来与认证服务器通信，即使通用双因素（U2F）和客户端到认证器协议（CTAP）看起来像是一个独立于终端的外部认证器。因此，如果在家或在工作中使用两个或多个终端，则用户必须在每个终端的FIDO认证器中重新注册服务。此外，即使使用一个CTAP认证器、一个FIDO2外部认证器，也必须注册或重新连接到每个终端。因此，基于PKI的带内认证技术具有终端依赖性，而无需明确地对服务提供商进行验证。

带外认证（如移动推送通知）是一种验证用户是否拥有认证器的认证技术，即使服务器或应用程序发生变化，也无需重新识别用户和重新颁发证书。然而，如果用户已经连接到一个欺诈性服务器，而不知道它们连接到哪里，则用户无法防止验证方假冒，如图III.2所示。




**图III.2 – 带外用户认证对假冒服务提供商的漏洞**

独立于用户认证技术，有一种万维网服务器认证技术，用户可以通过检查浏览器上被称为挂锁符号的ITU-T X.509证书来验证服务提供商，但这与用户认证过程不一致，因此用户可能会发现很难每次都检查证书，并且不熟悉技术的用户甚至可能不会检查证书。此外，这容易受到使用相似域名的社会工程攻击，并且不能使用私有DNS服务器、基于IP地址的在线服务和非基于浏览器的在线服务来验证在线服务。

因此，可能需要一个用于带外服务器认证的框架，该框架克服了在使用带外用户认证技术时可能发生的验证方假冒的漏洞，以及在使用基于PKI的带内用户认证技术时继承的认证器终端依赖性的限制。

# 参考文献


[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework*.

[b-ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework*.

[b-ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework*.

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

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2021, *Information security – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-NIST SP 800-63-3] NIST SP 800-63-3:2017, *Digital Identity Guidelines*.

# ITU-T 建议书系列

| | |
|---|---|
| A 系列 | ITU-T 工作的组织 |
| D 系列 | 资费和结算原则以及国际电信/ICT经济和政策问题 |
| E 系列 | 综合网络运行、电话业务、业务运行和人为因素 |
| F 系列 | 非话电信业务 |
| G 系列 | 传输系统和媒质、数字系统和网络 |
| H 系列 | 视听和多媒体系统 |
| I 系列 | 综合业务数字网 |
| J 系列 | 有线网和电视、声音节目及其他多媒体信号的传输 |
| K 系列 | 干扰的防护 |
| L 系列 | 环境和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 |
| M 系列 | 电信管理，包括电信网管管理和网络维护 |
| N 系列 | 维护：国际声音节目和电视传输电路 |
| O 系列 | 测量设备技术规程 |
| P 系列 | 电话传输质量、电话装置、本地线路网络 |
| Q 系列 | 交换和信令以及相关的测量与测试 |
| R 系列 | 电报传输 |
| S 系列 | 电报业务终端设备 |
| T 系列 | 远程信息处理业务的终端设备 |
| U 系列 | 电报交换 |
| V 系列 | 电话网上的数据通信 |
| **X 系列** | **数据网络、开放系统通信和安全** |
| Y 系列 | 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 |
| Z 系列 | 用于电信系统的语言和一般软件问题 |

瑞士印刷
2024年，日内瓦