FIDO UAF 架构概览 V1.0

FIDO 联盟推荐标准 2014-12-08

当前版本:

https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.html

之前版本:

https://fidoalliance.org/specs/fido-uaf-overview-v1.0-rd-20141008.pdf

编写者:

萨拉特•马可尼（Salah Machani），RSA, EMC 安全部

罗伯•菲尔波特（Rob Philpott），RSA, EMC 安全部

萨姆帕斯•斯里尼瓦（Sampath Srinivas），谷歌（Google, Inc.）

约翰•肯普（John Kemp），FIDO 联盟

杰夫•霍奇斯（Jeff Hodges），贝宝（PayPal, Inc.）

摘要

不管在互联网还是企业内部网络，FIDO UAF 强鉴别框架让在线服务和网站利用用户计算设备自身安全特性来提供强身份鉴别，同时减少了生成与记忆许多在线凭证的相关问题。FIDO UAF 参考框架描述了组件、协议和接口，这些组成了 FIDO UAF 强鉴别生态系统。

文档状态

本章节描述了文档发布时的状态。本文档有可能会被其它文档所取代。当前 FIDO 联盟出版物的列表以及此技术报告的最新修订可在 FIDO 联盟规范索引上找到。网址：https://www.fidoalliance.org/specifications/.

本文档由 FIDO 联盟 作为推荐标准发布。如果您希望就此文档发表评论，请 联系我们 。欢迎所有评论。

本规范中某些元素的实现可能需要获得第三方知识产权的许可，包括（但不限于）专利权。FIDO 联盟及其成员，以及此规范的其他贡献者们不能，也不应该为任何识别或未能识别所有这些第三方知识产权的行为负责。

本 FIDO 联盟规范是“按原样”提供，没有任何类型的担保，包括但不限于，任何明确的或暗示的不侵权、适销性或者适合某一特定用途的担保。

本文档已经由 FIDO 联盟成员评审并签署成为推荐标准。这是一篇稳定的文档，可能会作为参考材料被其它文档引用。FIDO 联盟的作用是引起对规范的注意并促进其广泛的分发。

目录

1. 简介 3
    1.1 背景 4
    1.2 FIDO UAF 文档 5
    1.3 FIDO UAF 目标 6
2. FIDO UAF 高阶架构 8
    2.1 FIDO UAF 客户端 8
    2.2 FIDO UAF 服务器 9
    2.3 FIDO UAF 协议 9
    2.4 FIDO UAF 认证器抽象层 10
    2.5 FIDO UAF 认证器 10
    2.6 FIDO UAF 认证器元数据校验 11
3. FIDO UAF 使用场景和协议消息流 11
    3.1 FIDO UAF 认证器采集和用户注册 11

3.2 认证器注册 11
3.3 鉴别 12
3.4 递进式鉴别 13
3.5 交易确认 14
3.6 认证器注销 15
3.7 新型 FIDO UAF 认证器的使用 15
4. 隐私注意事项 15
5. 与其他技术的关系 16
6. OATH，TCG，PKCS#11 及 ISO 24727 17
7. 图表目录 18

1. 简介

本节是非规范性的。

本文档描述了 FIDO 通用鉴别框架（UAF）参考架构，文档的目标读者是决策者和对 FIDO UAF 强鉴别解决方案和其他相关工业标准有深度理解的技术架构师。

FIDO UAF 规范包括：

- FIDO UAF 协议规范
- FIDO UAF 应用 API 和传输绑定规范
- FIDO UAF 认证器控制命令
- FIDO UAF 认证器特定模块 API
- FIDO UAF 认证器元数据声明
- FIDO UAF 认证器元数据服务
- FIDO 预定义值注册表

下面的 FIDO 文档提供了 UAF 规范相关的重要信息：

- FIDO 应用标识符与类型规范
- FIDO 安全参考
- FIDO 术语表

这些文档都可以在这个网站找到，网址：http://fidoalliance.org/specifications/download/

1.1 背景

本节是非规范性的。

FIDO 联盟的使命是通过以下方式改变在线强鉴别的本质：

- 制定技术规范来定义开放性、可扩展性和交互机制，这些机制将取代口令依赖对在线服务的用户进行安全的身份鉴别。
- 运作工业项目来帮助确保规范成功地在世界范围内被采用。
- 提交成熟的技术规范给被认可的标准研发组织进行正式标准化。

驱动 FIDO 联盟努力的核心思想是 1）易用性，2）私密性和安全性，3）标准化。FIDO 联盟的主要目标是，不管在互联网还是企业内部网络，使在线服务和网站利用用户计算设备自身的安全特性来提供强身份鉴别，同时减少生成与记忆许多在线凭证的相关问题。

FIDO 架构包含两个关键的协议，分别迎合了在使用互联网服务时的两种基本用户体验。两个协议共享许多基础但是分别被调谐到特定预期的用例。

通用鉴别框架（UAF）协议

UAF 协议允许在线服务提供无口令和多因子的安全性。用户通过选择本地鉴别机制，例如滑动手指、看摄像头、对麦克风说话、输入 PIN 码等，将设备注册到在线服务。UAF 协议允许服务选择将哪种鉴别机制呈现给用户。

注册后，当用户需要鉴别服务时只需要简单地重复本地鉴别动作。当从注册的

设备上鉴别时，用户不再需要输入口令。UAF 也支持复合的鉴别机制，例如指纹+PIN 码。

本文档描述了 UAF 参考框架。

通用第二因子(U2F)协议

U2F 协议允许在线服务在用户登录时添加一个强第二因子，从而增强现有口令安全基础设施的安全性。同以前一样，用户使用用户名口令登录，服务可以在任何需要的时候提示用户接入第二因子设备，强第二因子允许服务在不影响安全性的情况下简化口令（例如 4 位 PIN 码）。

在注册和鉴别过程中，用户通过简单地在 USB 设备上按键或通过 NFC 轻敲来提交第二因子。借助于浏览器内部对协议的支持，用户可以在所有的在线服务上使用 FIDO U2F 设备。

参见 FIDO 网站概览和 U2F 协议的相关文档。

1.2 FIDO UAF 文档

本节是非规范性的。

为了理解 FIDO UAF 协议，推荐新读者先阅读这篇架构概览，并且熟悉协议规范中的技术术语（术语表）。之后按照推荐的顺序阅读每一个 UAF 文档。

- **FIDO UAF 架构概览：**即本文档，提供了 FIDO UAF 架构、协议和规范的简介。
- **FIDO 术语表:** 定义了用于 FIDO 联盟规范和文档的技术术语和短语。
- **通用鉴别框架 (UAF)**
    - **UAF 协议规范：**所有 UAF 协议消息的格式和处理规则。
    - **UAF 应用 API 和传输绑定规范：**客户端使用 FIDO UAF 的 API 和交互操作简介。
    - **UAF 认证器控制命令：**为了支持 UAF 协议，UAF 认证器必须实现的底层功能。
    - **UAF 认证器特定模块 API：**认证器特定模块（ASM）提供给

FIDO 客户端的认证器特定模块 API。

- **UAF 认证器元数据声明**：描述了用于交互且制定策略决策的认证器的形态、特点及能力的信息。
- **UAF 认证器元数据服务**：依赖方访问最新的元数据声明的基线方法。
- **UAF 预定义值注册表**：定义 UAF 协议保留的所有字符串和常量。

- **FIDO 应用标识符与类型规范**：用户凭证的范围以及为了解决哪个应用或网页源可以使用哪个密钥的问题，支持应用隔离的可信计算基如何做访问控制决策。
- **FIDO 安全参考**：提供了 FIDO 安全分析，基于 FIDO 协议的目标、假定和内在安全措施相关的安全威胁的详细分析。

概览的剩余部分介绍了 FIDO UAF 设计的关键需求、目标和原则。

围绕着概览，本文档描述了：

- 架构定义的组件、协议和 API 的高阶浏览
- 主要 FIDO UAF 用例和实施所需的协议消息流
- FIDO 协议和相关行业标准的关系

1.3 FIDO UAF 目标

本节是非规范性的。

为了解决现今的强鉴别问题和开发一个能够顺利运作的生态系统，需要一个综合性的、开放的、多供应商的架构解决方案，包括：

- 不论是个人需要、企业需要还是企业级自带设备（BYOD）的用户设备和设备的潜在操作环境，例如家庭、办公室等
- 认证器 [1]
- 依赖方应用程序和应用程序的部署环境
- 满足终端用户和依赖方的需求

- 强烈关注基于浏览器和本地应用的终端用户体验

架构解决方案必须有以下特征：

- FIDO UAF 认证器发现、鉴证和配置
- 利用 FIDO UAF 认证器的跨平台强鉴别协议
- 统一的跨平台认证器 API
- 依赖方集成的简单机制

FIDO 联盟设想了一个开放的、多供应商的、跨平台的参考框架，有如下目标：

- **支持强、多因子鉴别**：通过让终端用户使用两个或两个以上的强鉴别因子（你知道什么，你有什么，你是谁）进行鉴别，从而保护依赖方，防止非授权访问。
- **基于已有的设备能力，但也不是必须的**：通过使用内置的平台认证器或功能（指纹感应器、照相机、麦克风、内嵌的 TPM 硬件）方便用户进行鉴别，但是不排除用户使用额外的独立认证器。
- **允许选择鉴别机制**：方便依赖方和用户从支持的鉴别机制中做选择，以规避特殊用例的风险。
- **简化新身份鉴别功能的集成：**允许组织扩大其使用强鉴别的范围来解决问题，如新的用例、利用新设备的能力，以及使用单一的身份鉴别方法解决新的风险。
- **包含扩展性以适应将来的改进和创新**：设计扩展协议和 API 来支持新型的认证器、鉴别方法和鉴别协议的出现，同时保持合理的向下兼容。
- **利用已有的开放标准，合理的开放创新，向更多方向扩展：一个**开放的、标准化的、免专利的规范会建立生态系统的良性循环，减少风险、复杂性和部署强身份鉴别相关的成本。现存的鸿沟，尤其是统一的认证器配置和鉴证，统一的跨平台认证器 API，一个灵活利用用户认证器的强鉴别挑战-响应协议等将得到解决。
- **补充现有的单点登录、身份联合方案**：业界方案（例如 OpenID、OAuth、SAML 等）通过单点登录或者身份联合技术创建了机制以减少

对口令的依赖，但他们没有直接解决用户和依赖方的初始强鉴别交互需求。

- **保护终端用户隐私**：通过与依赖方共享设备能力信息给用户提供控制权，降低了依赖方之间潜在的合谋可能性。
- **统一终端用户体验**：创建跨所有平台及类似认证器的易用、有趣、统一的最终用户体验。

2. FIDO UAF 高阶架构

本节是非规范性的。

FIDO UAF 架构的设计是满足 FIDO 目标的，也产生了所期望的生态效益。它通过使用标准化的协议和 API 来填补现存的鸿沟以达成目标。

下面的图表总结了参考架构，以及其中的组件是如何与典型用户设备和依赖方相关联的。

参考架构的 FIDO 特定组件如下图所述：

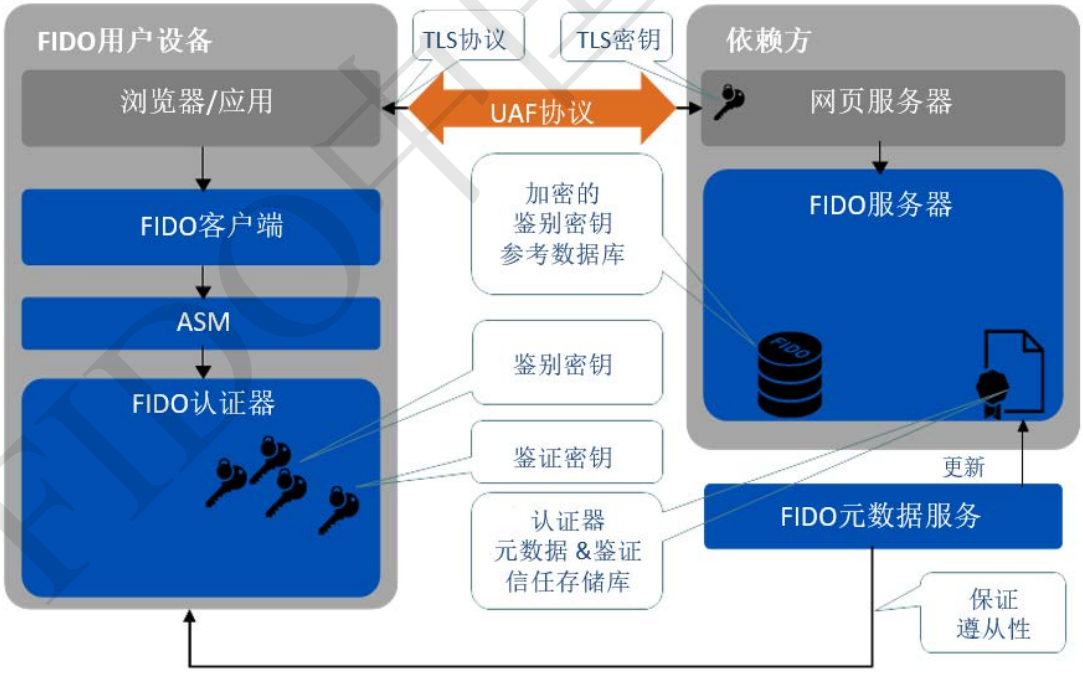

图 1 FIDO UAF 高阶架构

2.1 FIDO UAF 客户端

FIDO UAF 客户端实现 FIDO UAF 协议的客户端部分，负责：

- 通过 FIDO UAF 认证器 API，使用 FIDO UAF 认证器抽象层协议与特定的 FIDO UAF 认证器交互。
- FIDO UAF 客户端与设备上的用户代理（例如一个手机应用、浏览器）进行交互，用户代理通过特定的用户代理接口与 FIDO UAF 服务器进行交流。例如，特定的 FIDO 浏览器插件会使用现有的浏览器插件接口，手机应用可能会使用特定的 FIDO SDK。用户代理随后负责向依赖方的 FIDO UAF 服务器传送 FIDO UAF 消息。

FIDO UAF 架构确保 FIDO 客户端软件能够跨越一系列系统类型、操作系统和网页浏览器而实现的。虽然 FIDO 客户端软件通常是特定于平台的，组件之间的交互应该确保跨平台用户体验的一致性。

2.2 FIDO UAF 服务器

FIDO UAF 服务器实现 FIDO UAF 协议的服务器端部分，负责：

- 与依赖方网页服务器交互，后者通过用户代理将通信的 FIDO UAF 协议消息发送到 FIDO UAF 客户端。
- 对照配置的认证器元数据，校验 FIDO UAF 认证器鉴证，确保只有可信的认证器才能注册使用。
- 管理注册的 FIDO UAF 认证器与依赖方用户账户的关联。
- 评估用户鉴别和交易确认响应来决定他们的有效性。

FIDO UAF 服务器的构想是由依赖方作为本地预置服务器进行部署，或是外包给 FIDO 第三方服务提供者部署。

2.3 FIDO UAF 协议

FIDO UAF 协议承载用户设备和依赖方间的 FIDO UAF 消息。协议消息处理内容：

- 认证器注册：FIDO UAF 注册协议使依赖方能够：
    - 发现用户系统或设备上的可用 FIDO UAF 认证器，发现过程中将传输 FIDO UAF 认证器的属性给依赖方，从而使策略和部署生效。
    - 校验 FIDO UAF 认证器的鉴证断言以确保认证器是真实可信的。校验时使用了通过认证器元数据分发的鉴证公钥证书。
    - 注册认证器并与依赖方的用户账户相关联。认证器一旦被证明有效，依赖方可以提供唯一的特定于依赖方和 FIDO UAF 认证器的安全识别码。识别码可以用于未来在{依赖方，认证器}之间的交互，并且对于任意其它设备是不可知的。
- 用户鉴别：鉴别通常是基于加密的挑战-响应鉴别协议，并可帮助用户在鉴别活动中选择使用哪个 FIDO UAF 认证器。
- 安全交易确认：如果用户认证器有这个能力，依赖方能够向用户显示安全信息进行确认。信息的内容是由依赖方决定并且能够用于不同的场景，例如确认金融交易，用户协议或者发布病人记录。
- 认证器注销：当用户账户从依赖方移除时需要注销认证器。依赖方能够通过请求认证器删除与用户账户相关的 UAF 凭证来触发注销操作。

2.4 FIDO UAF 认证器抽象层

FIDO UAF 认证器抽象层提供统一的 API 给 FIDO 客户端，使支持 FIDO 的操作可以使用基于认证器的加密服务。抽象层提供统一的低层“认证器插件”API，使得多个供应商的 FIDO UAF 认证器和所需驱动的部署更加容易。

2.5 FIDO UAF 认证器

FIDO UAF 认证器是一个安全实体，连接或封装在 FIDO 用户设备中，可以创建与依赖方相关联的密钥材料。密钥可以用来参与 FIDO UAF 强鉴别协议。例如，FIDO UAF 认证器可以使用密钥材料生成加密挑战的响应，这样就可以向依赖方证明自己。

为了满足简化集成可信鉴别能力的目标，FIDO UAF 认证器可以证明它的特定类型（例如生物特征识别）和能力（例如所支持的加密算法）以及原产地。这给依赖方提供了高度的自信：所鉴别的用户的确就是最初在网站注册的用户。

2.6 FIDO UAF 认证器元数据校验

在 FIDO UAF 环境中，鉴证是指认证器在注册时对依赖方进行声明，内容为认证器是如何产生密钥的，以及/或者其所报告的某些措施源自于带有经认证的特征的真正设备。鉴证签名承载于 FIDO UAF 注册协议消息中，由 FIDO UAF 服务器校验。FIDO UAF 认证器在生产时就具有用于签名的鉴证私钥，FIDO UAF 服务器会使用认证器元数据中的认证器鉴证公钥证书来校验签名。包含鉴证证书的元数据是通过带外方式与 FIDO UAF 服务器共享的。

3. FIDO UAF 使用场景和协议消息流

本节是非规范性的。

FIDO UAF 生态系统支持本节简述的用例。

3.1 FIDO UAF 认证器采集和用户注册

用户可以通过不同的方法获取 FIDO UAF 认证器：购买新的附带内嵌 FIDO UAF 认证器能力的系统；购买附带内嵌 FIDO UAF 认证器的设备，或者雇主或其他机构例如银行给予的 FIDO 认证器。

在获取 FIDO UAF 认证器之后，用户必须经过一个特定认证器的注册过程，这个过程是超出 FIDO UAF 协议的。例如，在指纹感应认证器的例子下，用户必须在认证器注册他们的指纹。一旦注册成功，FIDO UAF 认证器就准备好在支持 FIDO UAF 的在线服务和网站进行注册了。

3.2 认证器注册

在 FIDO UAF 架构中，用户通过使用已初始化过的 FIDO UAF 认证器与依赖方

交互，该操作可以很轻易地检测到依赖方。在初始阶段，网站提示用户任何检测到的 FIDO UAF 认证器，并且给用户是否在网站上注册该认证器的选项。

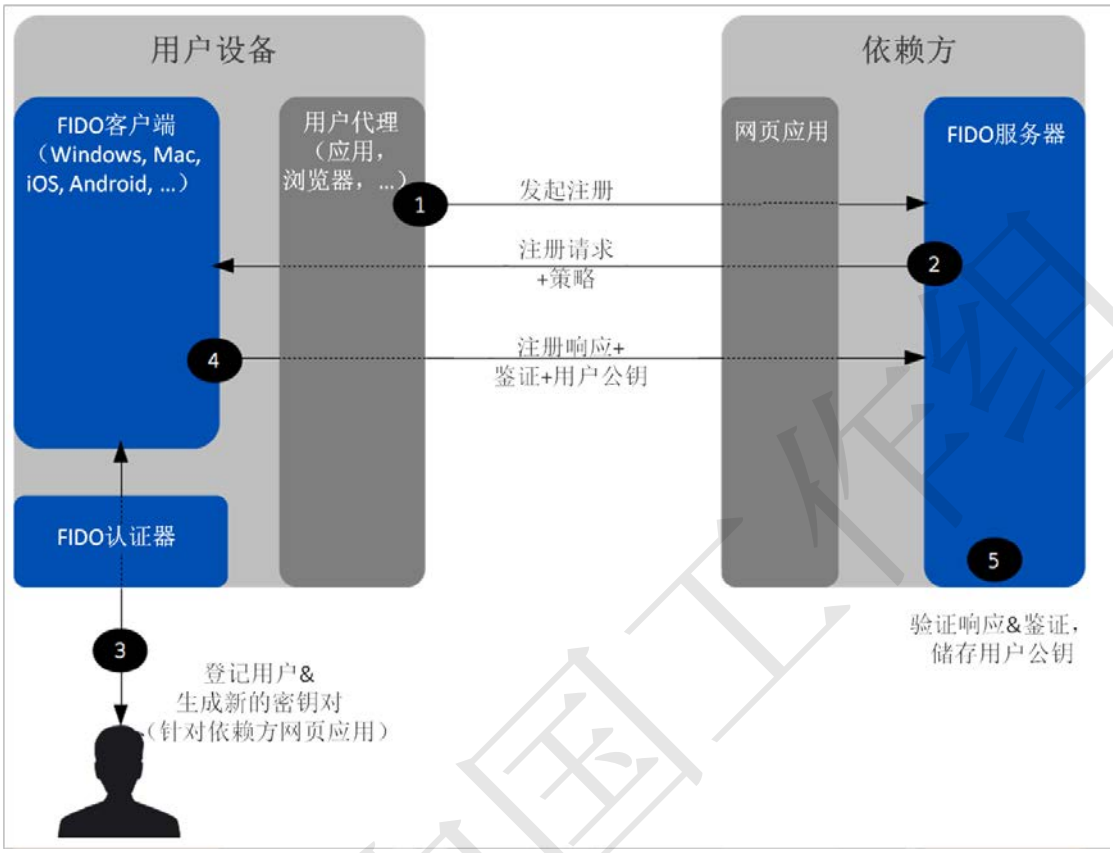

图 2 注册消息流

3.3 鉴别

注册之后，当用户在网站进行身份鉴别时就会使用 FIDO UAF 认证器。当 FIDO 认证器不存在时，网站可以为这些场合提供多种备用策略。这可能包括从允许最小特权的传统登录到不允许登录。

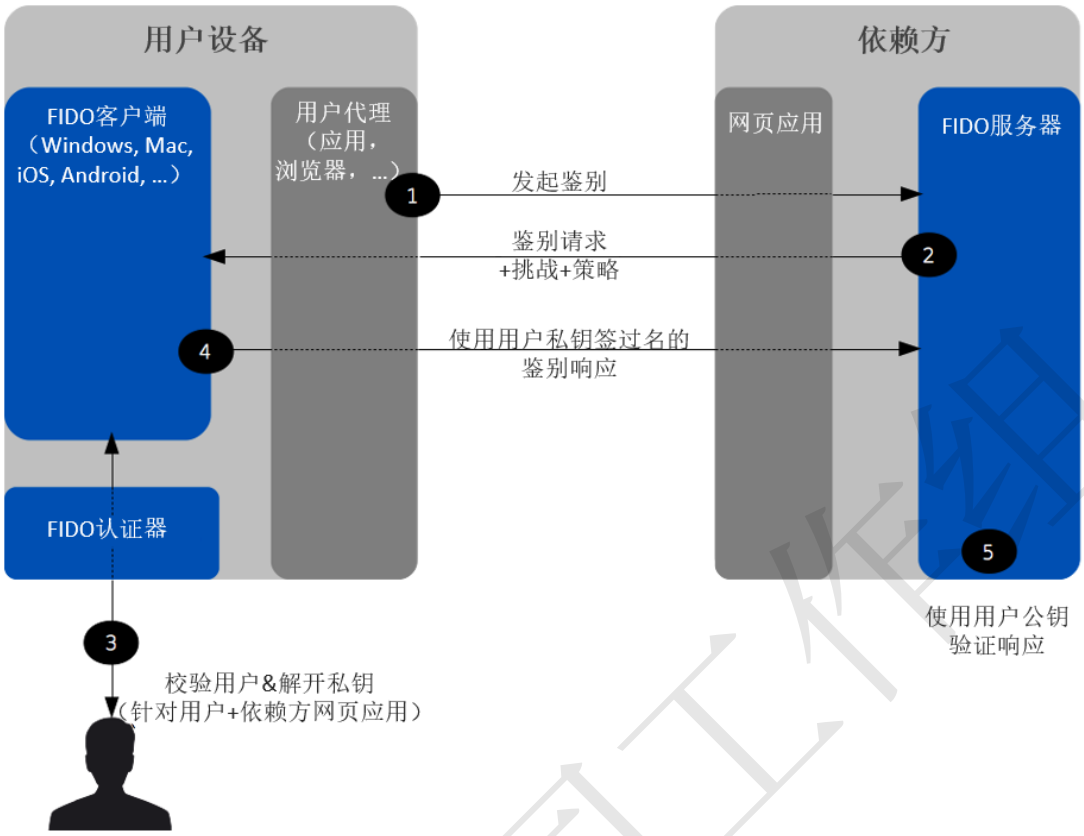

图 3 鉴别消息流

根据使用的 FIDO UAF 认证器的不同，整个场景也会有所不同。一些认证器会对生物特征数据取样，例如面部图形、指纹、声纹。其它认证器则需要 PIN 码或本地认证器特定的口令条目。还有一部分认证器是硬件承载认证器。注意，只要遵守 FIDO 隐私原则，可以允许 FIDO 客户端与外界服务进行交互，此交互作为用户向认证器鉴别的一部分。

3.4 递进式鉴别

递进式鉴别是对基本网站登录用例的升级。通常情况下，在线服务和网站允许未经鉴别的以及/或者名义上鉴别的用户使用，例如信息浏览。但是当用户请求更有价值的交互时，例如进入会员专区，网站就要求进一步的高保障鉴别。如果用户需要购买商品，这个过程会持续几个步骤，交易价值越高，就会有更高的保障措施。

FIDO UAF 会促进这种交互形式，因为网站能发现用户系统中可用的 FIDO UAF 认证器，并可以在任何特定鉴别交互方式中选择合适的认证器组合。因此

在线服务和网站将能够动态调整初始鉴别交互，和递进式鉴别交互一样，考虑到用户所请求的交互，取决于用户能够运用何种认证器以及网站风险分析引擎的所需输入。

3.5 交易确认

更多的创新用例会出现在支持 FIDO UAF 的依赖方和使用 FIDO UAF 认证器的终端用户之间，网站登录和递进式鉴别就是一个简单的例子，安全交易处理就是一个更高级的用例。

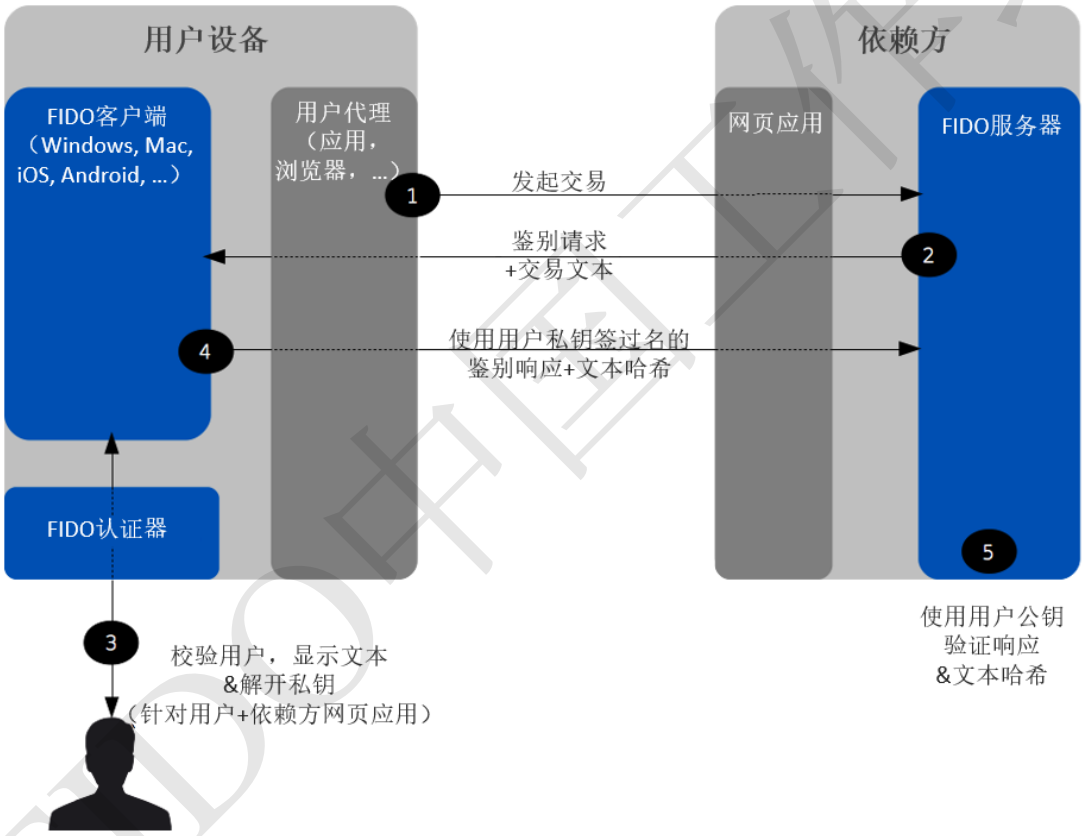

图 4 确认消息流

假设一种情况，依赖方想要终端用户确认一个交易（例如金融活动、特许操作等），从依赖方到用户终端的双向路径上的任何对交易信息的篡改都是可以被监测到的。FIDO 架构的“安全交易”的概念提供了上述功能。总的来说，如果 FIDO UAF 认证器有交易确认显示功能，FIDO UAF 架构确保系统支持“所见即所签” (WYSIWYS)的模式。大量的不同用例可以从这项功能中派生出来，主要涉及交易授权（例如转账、执行特定环境的特权操作、邮箱或地址的确认

等）。

3.6 认证器注销

很多情况下，依赖方需要在认证器上删除与特定用户账户相关的 UAF 凭证。例如，用户账户被注销或删除，用户的 FIDO 认证器丢失或被盗等。在这种情况下，依赖方会要求 FIDO 认证器删除与用户账户绑定的鉴别密钥。

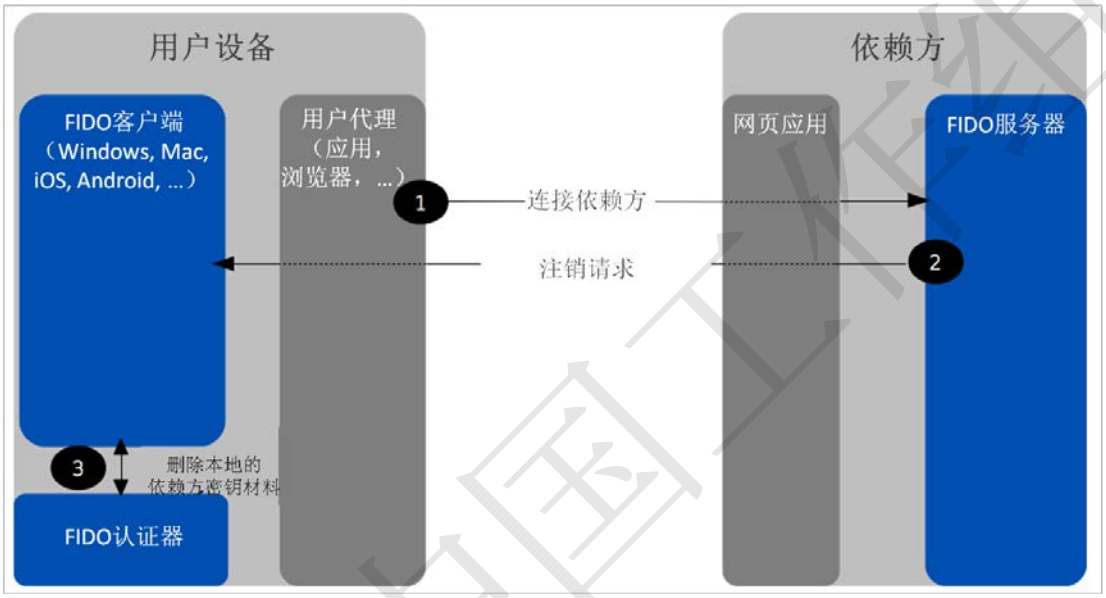

图 5 注销消息流

3.7 新型 FIDO UAF 认证器的使用

认证器将会不断的发展，新的种类也将会出现。FIDO 架构使得用户和依赖方对新认证器的使用变得更加容易。为了支持新的 FIDO UAF 认证器类型，依赖方需要添加描述新认证器配置的条目及其 FIDO 鉴证证书。然后，终端用户就能够在以上依赖方使用新的 FIDO UAF 认证器类型。

4. 隐私注意事项

本节是非规范性的。

用户隐私是 FIDO 的基础并且是被 UAF 设计支持的。一些关键的隐私考虑设计元素总结如下：

- UAF 设备没有一个跨依赖方的可见的全局标识符，对于某个特定的依赖方内部也没有一个全局标识符。例如，如果用户丢失了 UAF 设备，捡到的人不能将其指向某个依赖方，也不能发现原用户是否有账户与此依赖方相关联。同样的，如果两个用户共享一个 UAF 设备并且每个人都在相同的依赖方注册了账户，基于 UAF 协议自身，依赖方是无法辨别两个账户共享一台设备的。
- UAF 协议基于每个设备、每个用户账户、每个依赖方生成唯一的非对称加密密钥对。用于不同依赖方的加密密钥不允许任意方将所有操作链接到同一用户，即 UAF 的非链接性。
- UAF 协议操作只需收集最少的个人数据：充其量只包含用户在依赖方的用户名。个人数据仅用于 FIDO 行为，例如执行用户注册、用户验证或鉴别。个人数据不会离开用户的计算环境，需要时只允许本地使用。
- 在 UAF 中，用户验证是本地执行的，UAF 协议不会将用户生物特征数据发送给依赖方，也不要求在依赖方存储这些数据。
- 用户明确地批准特定的依赖方使用 UAF 设备。只有经过用户同意，注册过程才会产生唯一的加密密钥并绑定到依赖方。
- UAF 认证器仅能在批量生产级别、或制造商和设备型号级别被鉴证证书识别，不能单独被识别。UAF 规范要求制造商以相同鉴证证书和私钥出厂同一批次至少 100,000 个认证器以保证非链接性。

5. 与其他技术的关系

本节是非规范性的。

OpenID，SAML 及 OAuth

FIDO 协议（UAF 和 U2F）是联合身份管理（FIM）框架和网页鉴别协议的补充，联合身份管理框架包括 OpenID 和 SAML，网页鉴别协议包括 OAuth。FIM 依赖方能够在身份提供者（IdP）处利用初始身份鉴别活动。然而，OpenID 和 SAML 没有定义在 IdP 直接进行用户身份鉴别的具体机制。

当 IdP 与 FIDO 认证器服务集成时，可以利用依赖方强鉴别的属性。下图说明了这一关系。基于 FIDO 的鉴别（1）逻辑上首先发生，FIM 协议会利用鉴别活

动完成身份提供者和它的联合依赖方的单点登录活动（2）[2]。

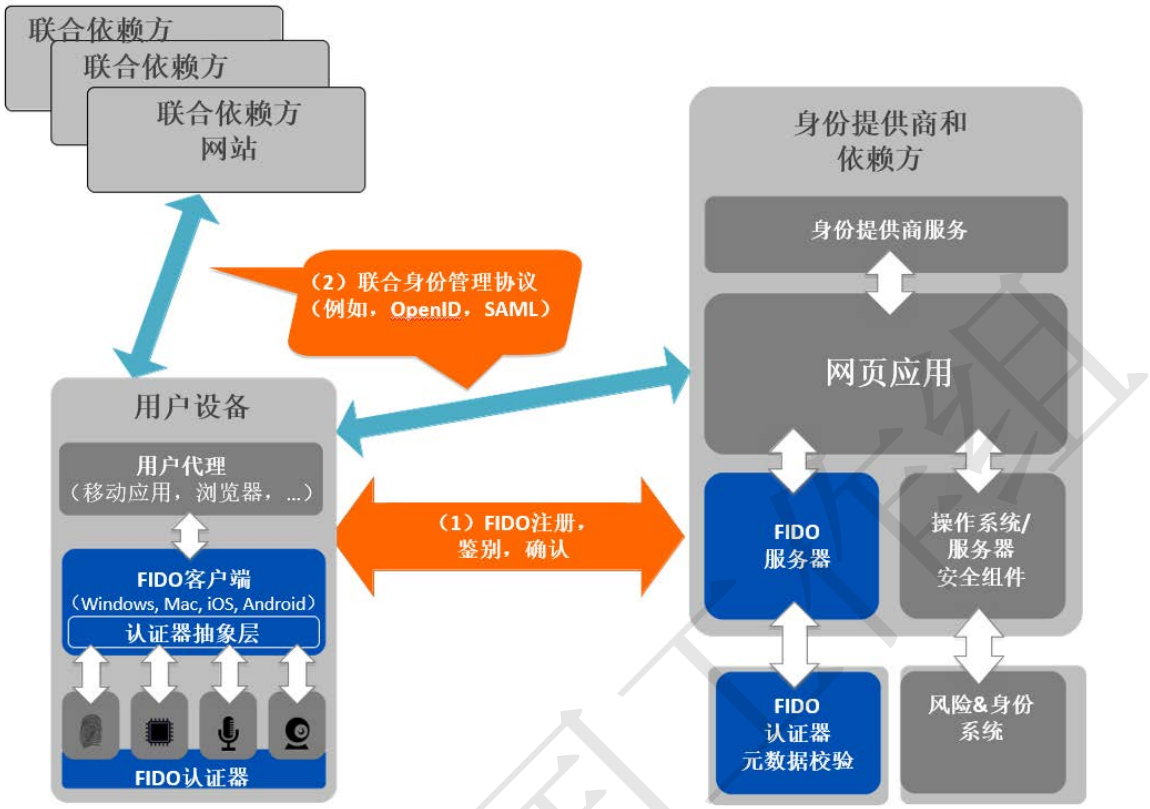

图 6 FIDO UAF 和身份联合框架

6. OATH，TCG，PKCS#11 及 ISO 24727

这些既是方案（OATH，可信计算组（TCG）），也是业界标准（PKCS#11、ISO 24727）。它们都优先关注硬件认证器。

PKCS#11 和 ISO 24727 定义了基于智能卡的认证器抽象概念。

TCG 提供了可信平台模块和网络可信计算的规范。

OATH（开放的鉴别方案），关注于定义对称密钥配置协议和一次性口令（OTP）硬件认证器的鉴别算法。

FIDO 框架分享了上述成果的几个核心概念，例如鉴别抽象接口、认证器鉴证、密钥配置和鉴别算法。FIDO 的工作会利用和扩展部分上述规范。

尤其是，FIDO 会在应对以下方面进行补充：

- 认证器发现
- 用户体验

- 多种认证器类型的结合，例如生物特征、动态口令（OTP）、简单的在场、智能卡、可信平台模块（TPM）等等。

7. 图表目录

图 1 FIDO UAF 高阶架构

图 2 注册消息流

图 3 鉴别消息流

图 4 确认消息流

图 5 注销消息流

图 6 FIDO UAF 和身份联合框架

1、也可被称为鉴别令牌、安全令牌等等。

2、FIM 协议通常通过浏览器 HTTP 重定向和 POSTs 来传输身份提供方和依赖方之间的交互。