FIDO 术语表 V1.0

FIDO 联盟推荐标准 2014-12-8

当前版本:

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

之前版本:

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

编写者:

罗尔夫•林德曼博士（Dr. Rolf Lindemann）, Nok Nok Labs, Inc.

达维特•巴格达萨利安（Davit Baghdasaryan）, Nok Nok Labs, Inc.

布拉德•希尔（Brad Hill）, 贝宝（PayPal, Inc.）

贡献者:

杰夫•霍奇斯（Jeff Hodges）, 贝宝（PayPal, Inc.）

摘要

本文档定义了所有 UAF 协议所用到的字符串和常量。本文档所定义的值被各个 UAF 规范所引用。

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. 注释 2
   1.1 关键字 2
2. 简介 2
3. 定义 3
A 参考文献 14
   A.1 参考规范 14
   A.2 参考资料 14

1. 注释

类型名称、属性名称和元素名称用代码形式书写。

字符串文本包含在双引号“”内，比如“UAF-TLV”。

公式中用 “|” 来表示按字节串联操作。

1.1 关键字

本文档中的关键字：“必须”，“不得”，“要求”，“将”，“将不”，“应该”，“不应该”，“建议”，“可能”，“可选”都会按照[RFC2119]的描述来解释。

2. 简介

本文档是 FIDO 联盟规范性技术术语的词汇表。

本文档并非一份包含所有 FIDO 技术术语的详尽纲要，因为 FIDO 术语是建立在现有术语基础上的，从而许多在上下文普遍用到的术语没有列出来。它们可在参考书目中的术语表/文档/规范中找到。其它术语表/文档/规范没有定义的术语在

这里被定义。

本术语表预计将会和 FIDO 联盟规范和文档一起逐步演变。

3. 定义

AAID

认证器验证标识符（Authenticator Attestation ID）。参见“验证标识符（Attestation ID）”。

Application（应用）

由一个共同的实体（应用程序所有者，也称为依赖方）提供的一组功能，用户可感知为一个合成整体。

Application Facet（应用类型）

一个（应用）类型指的是如何将一个应用程序在不同的平台上实现。例如：应用程序 MyBank 可能有一个安卓应用，一个 IOS 应用，以及一个 WEB 应用。这些就是应用程序 MyBank 的所有类型。

Application Facet ID（应用类型标识符）

指一个应用类型的特定于平台的标识符（URI 统一资源标识符）。

- 对于 WEB 应用程序，其应用类型标识符是 RFC 6454[RFC 6454]所规定的“起源（origin）”。
- 对于安卓应用程序，其应用类型标识符是统一资源标识符（URI）Android：apk-keyhash:<*hash-of-apk-signing-cert*>。
- 对于 iOS 应用程序，其应用类型标识符是统一资源标识符（URI）IOS：bundle-id:<*ios-bundle-id-of-app*>。

AppID（应用标识符）

AppID 是一个依赖方应用程序的一组不同类型的标识符。AppID 是一个统一资源定位符（URL），指向可信的应用程序类型，即与这个应用标识符相关的类型标识符列表。

Attestation（鉴证）

在 FIDO 语境中，“鉴证”是指认证器如何向依赖方申明它们产生的密钥，和（或）它们报告的确定的度量，源自于带有认证的特征的真实设备。

Attestation Certificate（鉴证证书）

与鉴证密钥相关的公钥证书。

Authenticator Attestation ID/AAID（认证器鉴证标识符/AAID）

分配给 FIDO 认证器的一个型号、类别或批次的唯一标识符。这些认证器都拥有相同的特性，并且依赖方可以用 AAID 来查找设备的验证公钥和认证器元数据。

Attestation [Public / Private] Key （鉴证[公/私]钥）

用于 FIDO 认证器鉴证的密钥。

Attestation Root Certification（鉴证根证书）

被 FIDO 联盟明确信任的根证书，链接到鉴证证书。

Authentication（鉴别）

鉴别是指用户使用 FIDO 认证器来证明拥有一个依赖方的注册密钥的过程。

Authentication Algorithm（鉴别算法）

签名和哈希算法的结合，用于认证器到依赖方的鉴别。

Authentication Scheme（鉴别方案）

鉴别算法、消息的语法或构造框架的结合，用于认证器构建响应。

Authenticator, Authnr （认证器）

参见“FIDO 认证器”。

Authenticator , 1stF/First Factor（认证器，第一因子）

FIDO 认证器以事务的方式提供一个用户名和至少两个认证因子：密钥材料（你拥有某种东西）加上用户验证（你知道某种东西/你就是你），所以可以单独用来完成鉴别。

假定这些认证器有一个内部匹配器。这个匹配器能够验证一个已注册的用户。如果有一个以上的用户注册了匹配器，该匹配器也能够识别出正确的用户。

这种认证器的例子是一个生物识别传感器或基于个人识别符（PIN）的验证。那些只检查用户是否在场（例如通过一个物理按钮）或者根本不执行验证的认证器，不能作为第一因子认证器。

Authenticator, 2ndF/ Second Factor（认证器，第二因子）

仅用于第二因子的 FIDO 认证器。第二因子认证器在响应一个 sign 命令前总是需要为其提供一个单独的密钥句柄。它们可能会也可能不会有用户验证手段。假定这些认证器可能会也可能不会有内部匹配器。

Authenticator Attestation（认证器鉴证）

向依赖方传递一个加密声明的过程，即在认证器注册期间提供一个由带有已验证特性的真正的认证器创建并保护的密钥。

Authenticator Metadata（认证器元数据）

关于一个已获得认证的认证器的特点的验证信息，与 AAID 相关并可从 FIDO 联盟获得。FIDO 服务器有望能够获得最新的元数据，以便能够与给定的认证器交互。

Authenticator Policy（认证器策略）

一个 JSON 数据结构，允许依赖方与 FIDO 客户端沟通，在给定的操作中，允许或禁止使用某些能力或特定的认证器。

ASM/Authenticator Specific Module（ASM/认证器特定模块）

与 FIDO 认证器相关的软件，提供了在硬件和 FIDO 客户端软件之间的统一接口。

AV

ASM 版本。

Bound Authenticator（绑定认证器）

一个 FIDO 认证器或认证器与 ASM 的组合，使用访问控制机制将注册密钥的使用限定于可信 FIDO 客户端和/或可信 FIDO 用户设备中。与之相对的是“漫游认证器”。

Certificate（证书）

指在[RFC5280]及后继文档中所指定的配置文件中定义的 X.509v3 证书。

Channel Binding（通道绑定）

参见：[RFC5056]、[RFC5929]以及[ChannelID]。

通道绑定可让应用程序建立两个端点在网络层的安全通道，和在更高层通过绑定鉴别将更高层与更低层的通道绑定起来一样。

Client（客户端）

该术语结合上下文来使用，可以指 FIDO UAF 客户端或其他类型的客户端，例如 TLS 客户端。详情请见“FIDO 客户端”。

Confused Deputy Problem （混淆代理人问题）

混淆代理人是指一个计算机程序无辜受到愚弄，被一些其它方滥用其权限。这是权限提升的一种特定类型。

Correlation Handle（关联句柄）

在 FIDO 协议的上下文中，任何信息都允许隐式或显式的关联，以及用户以为是不同且无关的多次活动的归属，回溯到一个单独的唯一实体。一个在 FIDO 语境之外的关联句柄的例子是用于传统 TLS 双向鉴别的客户端证书：因为它把相同的数据发送到多个依赖方，它们（依赖方）可以共谋来唯一识别和跟踪用户跨越不相关（依赖方）的活动。[Anon Terminology]

Deregistration（注销）

FIDO 协议的一个阶段，依赖方告诉 FIDO 认证器忘记与某个特定的依赖方账号相关联的某个特定的（或所有的）本地管理的密钥，在这种情况下，这些密钥不再被依赖方视为有效。

Discovery（发现）

FIDO 协议的一个阶段，依赖方能够确定客户端设备的 FIDO 功能是否可用，包括可用认证器的元数据。

E（K,D）

表示用密钥 K 对数据 D 加密。

ECDSA

椭圆曲线数字签名算法，由 ANSI X9.62[ECDSA-ANSI]定义。

Enrollment（登记）

使认证器知晓用户的过程。这可能是一个由[NSTCBiometrics]定义的生物识别的登记，或者包含如获得所有权，并为非生物识别的口令存储设备设置 PIN 或口令的过程。登记可能作为 FIDO 协议的一部分发生，或可能发生在 FIDO 语境之外，对于多用途认证器而言。

Facet（类型）

参见“应用程序类型（Application Facet）”。

Facet ID（类型标识符）

参见“应用程序类型标识符（Application Facet ID）”。

FIDO Authenticator（FIDO 认证器）

一个满足 FIDO 联盟的需求并且具有相关元数据的认证实体。

FIDO 认证器负责用户验证并维护依赖方鉴别所需的加密材料。

有一点很重要，值得注意：FIDO 认证器只考虑那些涉及 FIDO 联盟协议的参与方面。因为 FIDO 联盟旨在利用现有的和将来的硬件的多样性，许多 FIDO 使用的设备可能具有其它主要和次要的用途。从这个意义上来说，一个设备被用作非 FIDO 目的，比如本地操作系统登录或者非 FIDO 协议的网络登录，它不会被认为是 FIDO 认证器，并且这些模式的操作是不受 FIDO 联盟的指引或限制的，包括那些与安全和隐私有关的。

FIDO 认证器可以被简称为认证器或缩写成“Authnr”。认证器的能力和用户体验的重要区别可能取决于它是漫游的还是绑定认证器，以及它是“第一因子”还是“第二因子”认证器。

注册声明方案假定认证器对于使用鉴证密钥签名的数据具有独占地位的控制。

某些认证声明方案（例如 TAG_UAFV1_AUTH_ASSERTION）假定认证器对于使用 Uauth Key 签名的数据具有独占地位的控制。

FIDO Client（FIDO 客户端）

在 FIDO 用户设备上处理 UAF 或 U2F 协议消息的软件实体。FIDO 客户端可以采用以下两种形式之一：

- 在用户代理（无论是 web 浏览器还是原生应用程序）中实现的一个软件组件；
- 由若干个用户代理（Web 浏览器或原生应用程序）共享的一个独立的软件。

FIDO Data/FIDO Information（FIDO 数据/FIDO 信息）

作为完成一次 FIDO 交易的一部分而收集或创建的任何信息。包括但不限于生物识别测量或用户和 FIDO 交易记录的参考数据。

FIDO Server（FIDO 服务器）

服务器软件典型地部署在依赖方的基础设施中，符合 UAF 协议服务器需求。

FIDO UAF Client（FIDO UAF 客户端）

参见“FIDO 客户端（FIDO Client）”。

FIDO User Device（FIDO 用户设备）

FIDO 客户端运行其上的计算设备，从这里用户初始化一个使用 FIDO 的动作。

Key Identifier (KeyID)（密钥标识符 KeyID）

对于第一因子认证器来说，KeyID 是一个由认证器注册到一个 FIDO 服务器的密钥的不透明的标识符。它被用于配合 AAID 来标识一个保存了必要的密钥的特定认证器。密钥标识符在一个 AAID 的范围内必须是唯一的。

一个可能的实现是，KeyID 是由 ASM 管理的 KeyHandle 的 SHA256 哈希值。

KeyHandle （密钥句柄）

由 FIDO 认证器创建的一个密钥容器，包含一个私钥和（可选）其它数据（例如用户名）。一个密钥句柄可以被打包（使用一个只有认证器知道的密钥进行加密）或解包。在解包形式中，它被称为原始密钥句柄。第二因子认证器必须从依赖方检索其密钥句柄以便发挥作用，第一因子认证器管理自己的密钥句柄的存储，既可在内部（对于漫游认证器）也可通过相关联的 ASM（对于绑定认证器）。

Key Registration（密钥注册）

在 FIDO 服务器和 FIDO 认证器之间安全地创建一个密钥的过程。

KeyRegistrationData（KRD）（密钥注册数据）

作为认证器的 Register 命令的结果，一个 KeyRegistrationData 对象是由认证器创建和返回的。KRD 对象包含许多项，如认证器的 AAID，新生成的 UAuth.pub key（用户公钥），以及其它认证器特定的信息，如认证器执行加密操作所使用的算法，以及计数器的值等。使用认证器的验证私

钥来对 KRD 对象签名。

KHAccessToken （密钥句柄访问令牌）

为认证器命令充当保卫的秘密值。

KHAccessToken（密钥句柄访问令牌）由 ASM 产生和提供。

Matcher（匹配器）

FIDO 认证器的组件，能够执行（本地）用户验证，例如生物识别对比[ISOBiometrics]、PIN 验证等。

Matcher Protections （匹配器保护）

认证器用于保护匹配器组件的安全机制。

Persona（角色）

存储于认证器里的所有相关数据（如密钥）都与一个单一的“角色”（如“商务”或“私人”角色）有关。有些认证器提供的管理接口（未经过 FIDO 规范化的）允许维护和切换角色。

用户可以切换到“私人”角色并注册新的账户。在切换回“商务”角色后，这些账户将不被认证器认可（直到用户再次切换到“私人”角色）。

PersonaID （角色标识符）

由 ASM 提供的一个标识符，PersonaID 用于关联不同的注册。它可以用于在单个认证器上创建虚拟身份，例如用于区分“私人”和“商务”账户。

PersonaID 可以用于管理认证器的隐私设置。

Reference Data（参考数据）

一个（生物识别）参考数据（也称为样本）是一个从生物体样本提取的特点鲜明的数字化参考。生物识别参考数据在生物识别用户验证过程中[IOSBiometrics]使用。非生物识别参考数据与基于 PIN 码的认证结合使用。

Registration（注册）

FIDO 协议的一个操作。用户生成新的密钥材料，并使之与某个依赖方账户关联起来，该密钥服从于服务器设置的策略以及可接受的鉴证，从而认证器和注册与该策略相匹配。

Registration Scheme（注册方案）

注册方案定义了鉴别密钥是如何在FIDO服务器和FIDO认证器之间被交换的。

Relying Party（依赖方）

使用 FIDO 协议直接鉴别用户（例如进行对等实体鉴别）的 web 站点或其它实体。请注意，如果 FIDO 与联合身份管理协议（例如：SAML，OpenID 连接等）进行组合，身份提供者也将担任 FIDO 依赖方的角色。

Roaming Authenticator（漫游认证器）

一个配置为在不同的 FIDO 客户端和 FIDO 用户设备之间移动的 FIDO 认证器，这样就缺少一个已建立的信任关系：

1. 仅仅使用自己的内部存储用于注册；
2. 允许注册密钥在没有访问控制机制的情况下，在 API 层使用（漫游认证器仍然可以进行用户验证）。

与绑定认证器形成对比。

S（K,D）

使用密钥 K 对数据 D 签名。

Server Challenge（服务器挑战值）

在 UAF 协议的请求（消息）中，由 FIDO 服务器提供的一个随机值。

Sign Counter（签名计数器）

由认证器维护的一个单调递增计数器。每使用一次 Uauth.priv key（用户私钥），它就增加一次。这个值可被 FIDO 服务器用来检测克隆认证器。

SignedData（签名数据）

作为认证器的 Sign 命令的结果，一个 SignedData 对象是由认证器创建并返回的。输入到签名运算的待签名数据将出现在返回的签名数据对象里，表示为原封不动的值或哈希值。该签名数据对象还包括有关认证器及其模式的基本信息，随机数，认证器特定加密算法的信息，以及一个使用计数器。SignedData 对象使用依赖方特定的 UAuth.priv（用户私钥）来签名。

Silent Authenticator（静默（无交互）认证器）

不会提示用户或执行任何用户验证的 FIDO 认证器。

Step-up Authentication （递进式鉴别）

在一个已有鉴别会话之上执行的身份鉴别。

例如：用户最初使用用户名和口令开始鉴别会话，随后 web 站点在此鉴别会话之上请求一次 FIDO 鉴别。

请求递进式鉴别的一个原因可能是对于高价值资源的请求。

FIDO U2F 总是被用于递进式鉴别。FIDO UAF 可用于递进式鉴别，但也可用于初始认证机制。

请注意：一般来说，不存在这样的暗示，即递进式鉴别方法本身“强于”初始鉴别。既然递进式鉴别在一个现有的鉴别之上执行，将导致结合起来的鉴别强度最可能增加，而永远不会减弱。

Template（模板）

参见“参考数据（reference data）”。

TLS

传输层安全。

Token（令牌）

在 FIDO U2F 中，术语“令牌”（Token）常用于表示 UAF 中所谓的认证器的意思。另外，需要注意“令牌”的其他用途，例如：KHAccessToken（密钥句柄访问令牌），用户校验令牌等，都有各自的区别。如果它们没有明确的定义，它们的含义需要根据上下文来确定。

Transaction Confirmation（交易确认）

FIDO 协议的一项操作，允许依赖方要求具有合适能力的 FIDO 客户端和认证器显示一些信息给用户，要求用户在本地进行验证，向 FIDO 认证器确认这些信息，并提供以前注册的密钥材料的拥有证明以及将此确认的验证返回给依赖方。

Transaction Confirmation Display（交易确认显示）

这是 FIDO 认证器的一项特色，能够将一条消息的内容显示给用户，并且保护该消息的完整性。该特色能够通过使用 GlobalPlatform 规定的 TrustedUI（可信用户界面）[TEESecureDisplay]来实现。

TrustedFacets （可信类型）

保存可信类型标识符（FacetID）列表的数据结构。应用标识符（AppID）用于检索该数据结构。

TTEXT

交易文本，例如在“交易确认”的情况下待确认的文本。

Type-length-value/tag-length-value (TLV) （标签-长度-值）

将给定数据以类型、长度和值的形式进行编码的机制。典型地，类型和长度数据字段是固定大小的。这种格式比其它数据编码机制提供了某些优点，这使得其适合于 FIDO UAF 协议。

Universal Second Factor (U2F) （通用第二因子）

FIDO 协议和认证器家族使得云服务能够为其用户提供使用易于使用、基于强安全的开放标准的第二因子设备进行身份鉴别的选择。该协议依赖于在触发身份鉴别之前服务器了解（预期的）用户。

Universal Authentication Framework (UAF) （通用认证框架）

FIDO 协议和认证器家族使得服务能够为其用户提供灵活并且可以互操作的身份鉴别。该协议允许在服务器了解用户之前触发身份鉴别。

UAF Client（UAF 客户端）

参见“FIDO 客户端”。

UAuth.pub/UAuth.priv/UAuth.key （用户公钥/用户私钥/用户密钥）

由 FIDO 认证器生成的用户鉴别密钥。UAuth.pub（用户公钥）是密钥对的公共部分。UAuth.priv 是密钥的私密部分。UAuth.key（用户密钥）是用来指代 UAuth.priv（用户私钥）的更通用的写法。

UINT8

8 位（1 字节）无符号整数。

UINT16

16 位（2 字节）无符号整数。

UINT32

32 位（4 字节）无符号整数。

UINT64

64 位（8 字节）无符号整数。

UPV

UAF 协议版本。

User（用户）

依赖方的用户，FIDO 认证器的拥有者。

User Agent（用户代理）

用户代理是一个客户端应用程序，在客户端-服务器系统中代表一个用户。用户代理的例子包括 web 浏览器和移动应用程序。

User Verification（用户校验）

FIDO 认证器在本地授权使用密钥材料的过程。例如通过触摸、PIN 码、指纹匹配或其他生物识别（完成对用户的校验）。

User Verification Token（用户校验令牌）

用户校验令牌是由认证器产生并在用户校验成功后递交给 ASM 的一个令牌。没有这个令牌，ASM 就不能调用特定的命令如 Register 或 Sign。用户校验令牌的生命周期由认证器管理。产生这种令牌并管理其生命周期的具体技术是供应商特定的和非规范性的。

Username（用户名）

一个具有可读性的字符串，在依赖方标识一个用户账户。

Verification Factor（校验因子）

完成本地用户校验的特定方法。如：指纹，声纹，或 PIN。

这又称为“模态（modality）”。

Web Application, Client-Side（Web 应用程序，客户侧）

建立在“开放 WEB 平台”上的依赖方应用程序的一部分，它在用户代理的上下文中执行。当术语“WEB 应用程序”看上去不合格或在 FIDO 文档中没有特定的语境时，它一般是指一个客户侧的一部分或者是这样的应用程序的客户侧和服务侧的组合。

Web Application, Server-Side（WEB 应用程序，服务侧）

在 web 服务器上运行的依赖方应用程序的一部分，对 HTTP 请求进行响应。当术语“WEB 应用程序”看上去不合格或在 FIDO 文档中没有特定的语境时，它一般是指服务侧的一部分或者这样的应用程序的客户端和服务器端的组合。

A 参考文献

A.1 参考规范

[RFC2119]

S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997. Best Current Practice.

URL: https://tools.ietf.org/html/rfc2119

A.2 参考资料

[AnonTerminology]

"*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology", Version 0.34,*. A. Pfitzmann and M. Hansen, August 2010.

URL: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[ChannelID]

D. Balfanz *Transport Layer Security (TLS) Channel IDs*. (Work In Progress)

URL: http://tools.ietf.org/html/draft-balfanz-tls-channelid

[ECDSA-ANSI]

Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-2005. American National Standards Institute, November 2005,

URL: http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.62%3A2005

[ISOBiometrics]

Project Editor, *Harmonized Biometric Vocabulary*. ISO/IEC JTC 1. 15 November

2007, http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/327973/654118/6687752/N_3004_JTC_1_SC_37_-_Harmonized_Biometric_Vocabular

y_-_for_information.pdf?nodeid=6719683&vernum=0

[NSTCBiometrics]

NSTC Subcommittee on Biometrics, *Biometrics Glossary*. National Science and Technology Council. 14 September 2006,

URL: http://biometrics.gov/Documents/Glossary.pdf

[RFC5056]

N. Williams, *On the Use of Channel Bindings to Secure Channels (RFC 5056)*, IETF, November 2007,

URL: http://www.ietf.org/rfc/rfc5056.txt

[RFC5280]

D. Cooper, S. Santesson, s. Farrell, S.Boeyen, R. Housley, W. Polk; *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, May 2008,

URL: http://www.ietf.org/rfc/rfc5280.txt

[RFC5929]

J. Altman, N. Williams, L. Zhu, *Channel Bindings for TLS (RFC 5929)*, IETF, July 2010,

URL: http://www.ietf.org/rfc/rfc5929.txt

[RFC6454]

A. Barth. *The Web Origin Concept*. December 2011. Proposed Standard.

URL: https://tools.ietf.org/html/rfc6454

[TEESecureDisplay]

GlobalPlatform Trusted User Interface API Specifications GlobalPlatform. Accessed March 2014.

URL: https://www.globalplatform.org/specifications.asp