# FIDO UAF 预定义值的注册表 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-reg-v1.0-ps-20141208.html

### 之前版本:

https://fidoalliance.org/specs/fido-uaf-reg-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.）

### 翻译者:

李俊（Simon Li），联想（Lenovo）

常秉俭（Nick Chang），联想（Lenovo）



---

## 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

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。

本文档中 UAF 的专有术语在 FIDO 术语表[FIDOGlossary]中有定义。

本文档中所有图表、事例、注释均是非规范性的。

## 1.1 关键词

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. 概述

*本节是非规范性的。*

本文档定义了 UAF 特定常量的注册表，被多个 UAF 规范引用。随着时间的推移，预计会有新的常量会添加到这个注册表中。例如，新的鉴别算法和新类型的认证器特性会需要定义新的常量用于规范中。

# 3. 认证器特性

*本节是规范性的。*

## 3.1 用户校验方法

USER_VERIFY 常量是表示为 32 位长整数的位字段中的标志，描述 UAF 认证器用于本地校验用户的方法和能力。这些方法的操作细节对服务器是不透明的。这些常量被用于认证器的官方元数据中，通过 UAF 发现 API 来报告和查询，并用于在 UAF 协议消息中形成认证器策略。

为满足 FIDO 隐私原则，所有用户校验方法必须由认证器在本地实现。

**USER_VERIFY_PRESENCE 0x01**

如果认证器能够以任意方式确认用户在场，就必须设置这个标志。如果对于用户校验来说只设置了此标志而没有设置其它标志，只能保证认证器在没有人为干预的情况下不能操作，不保证用户在场验证提供

任何级别的人的身份鉴别（例如设备需要触摸来激活）。

**USER_VERIFY_FINGERPRINT 0x02**

如果认证器使用任意种类的指纹比对进行用户校验，就必须设置这个标志。

**USER_VERIFY_PASSCODE 0x04**

如果认证器使用本地口令进行用户校验（例如说该口令不为服务器所知晓），就必须设置这个标志。

**USER_VERIFY_VOICEPRINT 0x08**

如果认证器使用声纹来进行用户校验（也称为说话人识别），就必须设置这个标志。

**USER_VERIFY_FACEPRINT 0x10**

如果认证器使用任意方式的面部识别来进行用户校验，就必须设置这个标志。

**USER_VERIFY_LOCATION 0x20**

如果认证器使用任意形式的位置感应器或度量来进行用户校验，就必须设置这个标志。

**USER_VERIFY_EYEPRINT 0x40**

如果认证器使用任意形式的眼部生物识别来进行用户校验，就必须设置这个标志。

**USER_VERIFY_PATTERN 0x80**

如果认证器使用任意形式的绘图模式来进行用户校验，就必须设置这个标志。

**USER_VERIFY_HANDPRINT 0x100**

如果认证器使用任意形式的全手掌来进行用户校验（包括掌纹，手型或者血管形状），就必须设置这个标志。

**USER_VERIFY_NONE 0x200**

如果认证器不需要任何用户交互就可以响应（例如静默认证器），就必须设置这个标志。

**USER_VERIFY_ALL 0x400**

如果认证器对用户校验类型设置了多个标志，那么可能也会设置此标志来表明所有的认证方法都会被强制执行（例如面部识别和声纹识别）。如果设定了多个用户校验方法的标志，但是没有设定此标志，那么只有一个校验方法是必须的（例如指纹识别或者本地口令）。

## 3.2 密钥保护类型

KEY_PROTECTION 常量是表示为 16 位长整数的位字段中的标志，描述认证器用来保护 FIDO 注册的私钥材料的方法。更多关于密钥和密钥保护的细节参见[UAFAuthnrCommands]。这些常量被用于认证器的官方元数据中，通过 UAF 发现 API 来报告和查询，并用于在 UAF 协议消息中形成认证器策略。

当用于描述认证器的元数据时，许多标志是独有的（例如不能组合），经过认证的元数据可能最多有一个互斥的比特位设置为 1。当用于认证器策略时，任意位都可设置为 1，例如表明服务器愿意接受使用了 KEY_PROTECTION_SOFTWARE 或 KEY_PROTECTION_HARDWARE 的认证器。

> 注释
>
> 为了遵循[FIDOSecRef]中的假定，这些标志必须根据密钥的有效安全性进行设置。例如，如果一个密钥保存在安全元件中，但是运行在 FIDO 用户设备上的软件可以调用安全元件中的功能来以明文或者使用任意包裹密钥的形式导出密钥，那么有效安全性就是 KEY_PROTECTION_SOFTWARE 而不是 KEY_PROTECTION_SECURE_ELEMENT。

**KEY_PROTECTION_SOFTWARE 0x01**

如果认证器使用基于软件的密钥管理，就必须设置这个标志。在认证器元数据中与 KEY_PROTECTION_HARDWARE，KEY_PROTECTION_TEE，KEY_PROTECTION_SECURE_ELEMENT

互斥。

**KEY_PROTECTION_HARDWARE 0x02**

如果认证器使用基于硬件的密钥管理，就应该设置这个标志。在认证器元数据中与 KEY_PROTECTION_SOFTWARE 互斥。

**KEY_PROTECTION_TEE 0x04**

如果认证器使用可信执行环境[TEE]进行密钥管理，就应该设置这个标志。在认证器元数据中，此标志应该与 KEY_PROTECTION_HARDWARE 连同设置，在认证器元数据中与 KEY_PROTECTION_SOFTWARE，KEY_PROTECTION_SECURE_ELEMENT 互斥。

**KEY_PROTECTION_SECURE_ELEMENT 0x08**

如果认证器使用安全元件[SecureElement]进行密钥管理，就应该设置这个标志。在认证器元数据中，此标志应该与 KEY_PROTECTION_HARDWARE 连同设置，在认证器元数据中与 KEY_PROTECTION_TEE，KEY_PROTECTION_SOFTWARE 互斥。

**KEY_PROTECTION_REMOTE_HANDLE 0x10**

如果认证器在客户端不存储（被包裹的）UAuth（用户鉴别）密钥，而是依靠服务器提供的密钥句柄，就必须设置这个标志。此标志必须与一个其它的 KEY_PROTECTION 标志连同设置，来表明如何保护本地密钥句柄包裹密钥和操作。如果服务器不准备存储和返回密钥句柄，那么服务器可能在认证器策略中不设置这个标志。例如，如果服务器需要对存在和不存在的 userID 的鉴别尝试进行无差别的响应。详见[UAFProtocol]。

## 3.3 匹配器保护类型

MATCHER_PROTECTION 常量是表示为 16 位长整数的位字段中的标志，描述认证器保护进行用户验证的匹配器的方法。这些常量用于认证器的官方元数据，通过 UAF 发现 API 来报告和查询，并用于在 UAF 协议信息中形成认证器策略。有关匹配器组件的详细信息请参考

[UAFAuthnrCommands]。

> 注释
>
> 为了遵循[FIDOSecRef]中的假定，这些标志必须根据匹配器的*有效*安全性进行设置。例如，如果基于口令的匹配器在安全元件中实现，但是口令预期作为未经鉴别的参数提供，那么有效性安全就是 MATCHER_PROTECTION_SOFTWARE 而不是 MATCHER_PROTECTION_ON_CHIP。

**MATCHER_PROTECTION_SOFTWARE 0x01**

如果认证器的匹配器在软件中执行，就必须设置这个标志。在认证器元数据中与 MATCHER_PROTECTION_TEE，MATCHER_PROTECTION_ON_CHIP 互斥。

**MATCHER_PROTECTION_TEE 0x02**

如果认证器的匹配器在可信执行环境[TEE]中执行，就应该设置这个标志。在认证器元数据中与 MATCHER_PROTECTION_SOFTWARE，MATCHER_PROTECTION_ON_CHIP 互斥。

**MATCHER_PROTECTION_ON_CHIP 0x04**

如果认证器的匹配器在芯片中执行，就应该设置这个标志。在认证器元数据中与 MATCHER_PROTECTION_TEE，MATCHER_PROTECTION_SOFTWARE 互斥。

## 3.4 认证器连接提示

ATTACHMENT_HINT 常量是表示为 32 位长整数的位字段中的标志，描述认证器用来与 FIDO 用户设备通信的方法。这些常量通过 UAF 发现 API 来报告和查询[UAFAppAPIAndTransport]，并被用于在 UAF 协议信息中形成认证器策略。因为连接状态和认证器的拓扑结构可能是暂时的，这些值仅仅是被服务器提供的策略用来指导用户体验的提示。例如宁可选择一个已经连接的并且准备好鉴别或确认小额交易的设备，而不是一个更安全但需要更多用户开销的设备。

> 注释

> 这些标志不是认证器元数据的强制部分，如果存在，只表明在认证器发现过程中时可被报告的可能状态。

**ATTACHMENT_HINT_INTERNAL 0x01**

该标志可能被设置以表明认证器永久地与 FIDO 用户设备连接在一起。

诸如智能手机这样的设备可能有可在本地和远程使用认证器功能。在这种情况下，FIDO 客户端必须在发现过程中和执行策略匹配的时候过滤并互斥地报告仅有的相关位。

这个标志不能与其他任何 ATTACHMENT_HINT 标志连同使用。

**ATTACHMENT_HINT_EXTERNAL 0x02**

该标志可能被设置以表明一个可移除的或远离 FIDO 用户设备的基于硬件的认证器。

诸如智能手机这样的设备可能有可在本地和远程使用认证器功能。在这种情况下，FIDO 客户端必须在发现过程中和执行策略匹配的时候过滤并互斥地报告仅有的相关位。

**ATTACHMENT_HINT_WIRED 0x04**

该标志可能被设置以表明一个当前与 FIDO 用户设备有独有的有线连接的外部认证器，例如通过带有固件程序或更小的 USB 设备。

**ATTACHMENT_HINT_WIRELESS 0x08**

该标志可能被设置以表明一个通过个人区域或者另外的非路由无线协议与 FIDO 用户设备通信的外部认证器，诸如蓝牙或近场通信（NFC）。

**ATTACHMENT_HINT_NFC 0x10**

该标志可能被设置以表明一个能够通过近场通信（NFC）与 FIDO 用户设备通信的外部认证器。作为认证器元数据的一部分或通过发现报告特征时，如果设置了此标志，则标志 ATTACHMENT_HINT_WIRELESS 也应该被设置。

**ATTACHMENT_HINT_BLUETOOTH 0x20**

该标志可能被设置以表明一个能够通过近场通信（NFC）与 FIDO 用

户设备通信的外部认证器。作为认证器元数据的一部分或通过发现（API）报告特征时，如果设置了此标志，则 ATTACHMENT_HINT_WIRELESS 标志也应该被设置。

**ATTACHMENT_HINT_NETWORK 0x40**

该标志可能被设置以表明认证器通过公共网络（例如 TCP/IP 局域网或广域网，与 PAN 个人网络（PAN：Personal Area Network）或点到点连接相对立）与 FIDO 用户设备通信。

**ATTACHMENT_HINT_READY 0x80**

该标志可能被设置以表明外部认证器处于“就绪”状态。此标志由 ASM 自行决定设置。

> 注释
>
> 一般地，此标志应表明设备可用于立即执行用户验证而不需额外动作，诸如连接设备或者创建新的生物识别特征注册，但是其明确含义可能根据设备类型的不同而变化。例如，USB 认证器可能只在被插入时报告它自己处于就绪状态，或者蓝牙认证器只在配对和连接时报告自己处于就绪状态，但是基于 NFC 的认证器可能会总是报告自己处于就绪状态。

**ATTACHMENT_HINT_WIFI_DIRECT 0x100**

该标志可能被设置以表明外部认证器能够用 WiFi 直连与 FIDO 用户设备通信。作为认证器元数据的一部分，当通过发现 API 报告特征时，如果设置了这个标志，则 ATTACHMENT_HINT_WIRELESS 标志也应该被设置。

## 3.5 交易确认显示类型

TRANSACTION_CONFIRMATION_DISPLAY 常量是表示为 16 位长整数的位字段中的标志，描述了交易确认操作所需的交易确认显示能力的可用性和实现。这些常量被用于认证器的官方元数据，通过 UAF 发现 API 来报告和查询，并用于在 UAF 协议信息中形成认证器策略。关于交易确认显示的安全方面的详细情况请参考[UAFAuthnrCommands]。

**TRANSACTION_CONFIRMATION_DISPLAY_ANY 0x01**

该标志必须被设置以表明某种形式的交易确认显示在此认证器上是可用的。

**TRANSACTION_CONFIRMATION_DISPLAY_PRIVILEGED_SOFTWARE 0x02**

该标志必须被设置以表明在享有特权的上下文中基于软件的交易确认显示在此认证器上是可用的。

能够提供此能力的 FIDO 客户端可能为所有支持 ATTACHMENT_HINT_INTERNAL 类型的认证器设置此标志，即使认证器官方元数据没有表明此能力。

> 注释
>
> 基于软件的交易确认显示可能在 ASM 的边界内实现，而不是由认证器自己实现[UAFASM]。

**TRANSACTION_CONFIRMATION_DISPLAY_TEE 0x04**

该标志应该被设置以表明认证器在可信执行环境（[TEE]，[TEESecureDisplay]）中实现了交易确认显示。

**TRANSACTION_CONFIRMATION_DISPLAY_HARDWARE 0x08**

该标志应该被设置以表明在此认证器具有在基于硬件的辅助交易确认显示能力。

**TRANSACTION_CONFIRMATION_DISPLAY_REMOTE 0x10**

该标志应该被设置以表明交易确认显示由一台与 FIDO 用户设备不同的设备提供。

## 3.6 用于加密算法和类型的标签

这些标签表明了特定的认证算法、公钥格式和其它加密相关数据。

### 3.6.1 鉴别算法

UAF_ALG_SIGN 常量是 16 位的长整数，表明特定的签名算法和编码方

式。

> **注释**
>
> FIDO UAF 支持 RAW 和 DER 签名编码以允许低性能认证器实现。

**UAF_ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW 0x01**

在 NIST secp256r1 曲线上的 ECDSA 签名，必须有原始的 R 和 S 缓存，以大端字节顺序编码。

例如[R (32 bytes), S (32 bytes)]

**UAF_ALG_SIGN_SECP256R1_ECDSA_SHA256_DER 0x02**

在 NIST secp256r1 曲线上的 DER[ITU-X690-2008]编码的 ECDSA 签名。

例如 DER 编码的 SEQUENCE { r INTEGER, s INTEGER }

**UAF_ALG_SIGN_RSASSA_PSS_SHA256_RAW 0x03**

RSASSA-PSS [RFC3447]签名必须有原始的 S 缓存，以大端字节顺序编码[RFC4055] [RFC4056]。必须假定[RFC4055]中所规定的默认参数，如：

- 使用 SHA256 的掩码生成算法 MGF1。
- 32 字节的混淆长度，例如 SHA256 哈希值的长度。
- 尾部字段值为 1，以十六进制值 0xBC 表示尾部字段。

例如[ S (256 bytes) ]

**UAF_ALG_SIGN_RSASSA_PSS_SHA256_DER 0x04**

包含 RSASSA-PSS [RFC3447]签名的[RFC4055][RFC4056]DER[ITU-X690-2008]编码的八位字节字符串（不是位字符串！）。必须假定[RFC4055]中所规定的默认参数，如：

- 使用 SHA256 的掩码生成算法 MGF1。
- 32 字节的混淆长度，例如 SHA256 哈希值的长度。
- 尾部字段值为 1，以十六进制值 0xBC 表示尾部字段。

例如 DER 编码的八位字节字符串（OCTET STRING）（包括其标签和长度字节）。

**UAF_ALG_SIGN_SECP256K1_ECDSA_SHA256_RAW 0x05**

在 secp256k1 曲线上的 ECDSA 签名，必须有原始的 R 和 S 缓存，以大端字节顺序编码。

例如[R (32 bytes), S (32 bytes)]

**UAF_ALG_SIGN_SECP256K1_ECDSA_SHA256_DER 0x06**

在 secp256k1 曲线上的 DER [ITU-X690-2008]编码的 ECDSA 签名 [RFC5480]。

例如 DER 编码的 SEQUENCE { r INTEGER, s INTEGER }

### 3.6.2 公钥表示形式

UAF_ALG_KEY 常量是 16 位的长整数，表明特定的签名算法和编码方式。

> **注释**
>
> FIDO UAF 支持 RAW 和 DER 编码用来允许低性能认证器实现。通过定义，认证器必须把公钥作为注册断言的一部分来编码。

**UAF_ALG_KEY_ECC_X962_RAW 0x100**

原始 ANSI X9.62 格式的椭圆曲线公钥[SEC1]。

例如[0x04, X (32 bytes), Y (32 bytes)]。0x04 字节代表未压缩点的压缩方法。

**UAF_ALG_KEY_ECC_X962_DER 0x101**

DER [ITU-X690-2008]编码的 ANSI X.9.62 格式 SubjectPublicKeyInfo [RFC5480] 规定的椭圆曲线公钥。

例如 DER 编码的如[RFC5480]所定义的 SubjectPublicKeyInfo。

认证器的实现必须在包含于 AlgorithmIdentifier 中的 ECParameters 对象中产生 namedCurve。FIDO UAF 服务器必须接受包含于 AlgorithmIdentifier 中的 ECParameters 对象中的 namedCurve。

**UAF_ALG_KEY_RSA_2048_PSS_RAW 0x102**

原始编码的 RSASSA-PSS 公钥 [RFC3447]。

按照[RFC4055]必须假定默认参数，如：

- 使用 SHA256 的掩码生成算法 MGF1。

- 32 字节的混淆长度，例如 SHA256 哈希值的长度。
- 尾部字段值为 1，以十六进制值 0xBC 表示尾部字段。

即[n (256 bytes), e (N-n bytes)]。N 是字段的总长度。这个总长度应该从包含此密钥的对象中获取，如 TLV 编码字段。

**UAF_ALG_KEY_RSA_2048_PSS_DER 0x103**

ASN.1 DER [ITU-X690-2008]编码的 RSASSA-PSS [RFC3447]公钥 [RFC4055]。

按照[RFC4055]必须假定默认参数，如：

- 使用 SHA256 的掩码生成算法 MGF1。
- 32 字节的混淆长度，例如 SHA256 哈希值的长度。
- 尾部字段值为 1，以十六进制值 0xBC 表示尾部字段。

即 DER 编码的 SEQUENCE { n INTEGER, e INTEGER }。

## 3.7 断言方案

断言方案的名字是 8 字符长度的字符串。

**基于 UAF TLV 的断言方案“UAFV1TLV”**

断言方案允许认证器和 FIDO 服务器交换认证器产生的对称鉴别密钥。认证器必须产生一个密钥对（用户公钥/用户私钥），与在鉴别算法（前缀为 UAF_ALG）小节中列出的算法组一起使用。断言方案使用紧凑的标签长度值（TLV）对认证器产生的 KRD 和签名数据消息进行编码。这就是 UAF 协议的默认断言方案。

# 4. 预定义标签

*本节是规范性的。*

UAF 认证器命令的内部结构是一个“标签-长度-值”（TLV）序列。标签是 2 字节的唯一的无符号数，用来描述数据代表的字段的类型；长度是 2 字节的无符号数，指明了该值的字节大小；值是可变大小的连续字节，包含了这个序列中此项的数据。

虽然分配给这个标签 2 字节，只有前 14 位（值一直到 0x3FFF）应被用于适应一些硬件平台的限制。

标签第 14 位（0x2000）的设置表明它很重要，如果接受者不能处理这个标签，就必须放弃处理整个消息。

标签第 13 位（0x1000）的设置表明一个合成的标签，能够被递归下降法解析。

## 4.1 协议中使用的标签

UAF 协议消息中，以下标签被分配给数据类型：

**TAG_UAFV1_REG_ASSERTION 0x3E01**

此标签的内容是认证器对注册（Register）命令的响应。

**TAG_UAFV1_AUTH_ASSERTION 0x3E02**

此标签的内容是认证器对签名（Sign）命令的响应。

**TAG_UAFV1_KRD 0x3E03**

表示密钥注册数据。

**TAG_UAFV1_SIGNED_DATA 0x3E04**

表示认证器用 UAuth.priv 密钥（用户私钥）签名的数据。

**TAG_ATTESTATION_CERT 0x2E05**

表示 DER 编码的鉴证证书。

**TAG_SIGNATURE 0x2E06**

表示签名算法。

**TAG_ATTESTATION_BASIC_FULL 0x3E07**

表示[UAFProtocol]定义的完整基础鉴证。

**TAG_ATTESTATION_BASIC_SURROGATE 0x3E08**

表示[UAFProtocol]定义的替代基础鉴证。

**TAG_KEYID 0x2E09**

代表一个生成的密钥标识符。

**TAG_FINAL_CHALLENGE 0x2E0A**

代表[UAFProtocol]定义的一个生成的最终挑战值。

**TAG_AAID 0x2E0B**

代表[UAFProtocol]定义的一个认证器鉴证标识符。

**TAG_PUB_KEY 0x2E0C**

代表一个生成的公钥。

**TAG_COUNTERS 0x2E0D**

代表认证器的使用次数计数器。

**TAG_ASSERTION_INFO 0x2E0E**

代表消息处理所必须的认证器信息。

**TAG_AUTHENTICATOR_NONCE 0x2E0F**

代表认证器产生的随机数值。

**TAG_TRANSACTION_CONTENT_HASH 0x2E10**

代表发送给认证器的交易内容的哈希。

**TAG_EXTENSION 0x3E11, 0x3E12**

这是一个合成标签，表明内容是一个扩展。

**TAG_EXTENSION_ID 0x2E13**

代表扩展 ID，标签的内容是对 UTF-8 字符串的 UINT8[]编码。

**TAG_EXTENSION_DATA 0x2E14**

代表扩展数据，此标签的内容是一个 UINT8[]字节数组。

# A. 参考文献

## A.1 参考规范


**[FIDOGlossary]**

R. Lindemann, D. Baghdasaryan, B. Hill, J. Hodges, *FIDO Technical Glossary*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-glossary-v1.0-ps-20141208.html

PDF: fido-glossary-v1.0-ps-20141208.pdf

**[ITU-X690-2008]**

X.690: Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), (T-REC-X.690-200811). International Telecommunications Union, November 2008 URL:http://www.itu.int/rec/T-REC-X.690-200811-I/en

**[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

**[RFC3447]**

J. Jonsson; B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. February 2003. Informational. URL: https://tools.ietf.org/html/rfc3447

**[RFC4055]**

J. Schaad; B. Kaliski; R. Housley. Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. June 2005. Proposed Standard. URL:https://tools.ietf.org/html/rfc4055

**[RFC4056]**

J. Schaad. Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS). June 2005. Proposed Standard. URL:https://tools.ietf.org/html/rfc4056

**[RFC5480]**

S. Turner; D. Brown; K. Yiu; R. Housley; T. Polk. Elliptic Curve Cryptography Subject Public Key Information. March 2009. Proposed Standard. URL: https://tools.ietf.org/html/rfc5480

**[SEC1]**

Standards for Efficient Cryptography Group (SECG), SEC1: Elliptic Curve Cryptography, Version 2.0, September 2000.

## A.2 参考资料

**[FIDOSecRef]**

R. Lindemann, D. Baghdasaryan, B. Hill, *FIDO Security Reference*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-security-ref-v1.0-ps-20141208.html

PDF: fido-security-ref-v1.0-ps-20141208.pdf

**[SecureElement]**

GlobalPlatform Card Specifications GlobalPlatform. Accessed March 2014. URL: https://www.globalplatform.org/specifications.asp

**[TEE]**

GlobalPlatform Trusted Execution Environment Specifications GlobalPlatform. Accessed March 2014. URL:https://www.globalplatform.org/specifications.asp

**[TEESecureDisplay]**

GlobalPlatform Trusted User Interface API Specifications GlobalPlatform. Accessed March 2014. URL:https://www.globalplatform.org/specifications.asp

**[UAFASM]**

D. Baghdasaryan, J. Kemp, R. Lindemann, B. Hill, R. Sasson, *FIDO UAF Authenticator-Specific Module API*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-asm-api-v1.0-ps-20141208.html

PDF: fido-uaf-asm-api-v1.0-ps-20141208.pdf

**[UAFAppAPIAndTransport]**

B. Hill, D. Baghdasaryan, B. Blanke, *FIDO UAF Application API and Transport Binding Specification*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-client-api-transport-v1.0-ps-20141208.html

PDF: fido-uaf-client-api-transport-v1.0-ps-20141208.pdf

**[UAFAuthnrCommands]**

D. Baghdasaryan, J. Kemp, R. Lindemann, R. Sasson, B. Hill, *FIDO UAF Authenticator Commands v1.0*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-authnr-cmds-v1.0-ps-20141208.html

PDF: fido-uaf-authnr-cmds-v1.0-ps-20141208.pdf

**[UAFProtocol]**

R. Lindemann, D. Baghdasaryan, E. Tiffany, D. Balfanz, B. Hill, J. Hodges, *FIDO UAF Protocol Specification v1.0*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-protocol-v1.0-ps-20141208.html

PDF: fido-uaf-protocol-v1.0-ps-20141208.pdf