FIDO UAF 认证器元数据声明 v1.0

FIDO 联盟建议标准 2014-12-08

当前版本:

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

之前版本:

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

编写者:

布拉德•希尔（Brad Hill）, 贝宝（PayPal, Inc.）

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

约翰•肯普（John Kemp）， FIDO 联盟

摘要

FIDO 认证器可能会有多种不同形式的因素、特性和能力。本文档定义了一个标准方法来描述一个认证器的相关信息，从而与之互操作，或者在交易涉及到特别的认证器时，做出基于风险的决策。

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 3
    1.1 关键字 4
2. 概览 4
    2.1 范围 4
    2.2 受众 4
    2.3 架构 5
3. 类型 6
    3.1 CodeAccuracyDescriptor 结构 6
        3.1.1 CodeAccuracyDescriptor 结构成员 7
    3.2 BiometricAccuracyDescriptor 结构 7
        3.2.1 BiometricAccuracyDescriptor 结构成员 8
    3.3 PatternAccuracyDescriptor 结构 9
        3.3.1 PatternAccuracyDescriptor 结构成员 9
    3.4 VerificationMethodDescriptor 结构 10
        3.4.1 VerificationMethodDescriptor 结构成员 10
    3.5 verificationMethodANDCombinations 类型定义 11
    3.6 rgbPalletteEntry 结构 11
        3.6.1 rgbPalletteEntry 结构成员 11

3.7 DisplayPNGCharacteristicsDescriptor 结构 12
3.7.1 DisplayPNGCharacteristicsDescriptor 结构成员 12
4. 元数据键 13
4.1 MetadataStatement 结构成员 13
5. 元数据声明格式 17
6. 其他的考虑 20
6.1 字段更新和元数据 20
A. 参考文献 21
A.1 参考规范 21
A.2 参考资料 22

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。

DOM APIs 使用 WebIDL [WebIDL-ED]中的 ECMAScript [ECMA-262]绑定来描述。

根据[WebIDL-ED],结构成员是可选的，除非他们被明确标注为 required。

WebIDL 的结构成员不得为空值。

除非特别声明，如果 WebIDL 的结构成员是 DOMString，则不得为空。

除非特别声明，如果 WebIDL 的结构成员是一个表单，则不得为一个空表单。

本文档中用到的 UAF 专用术语在 FIDO 术语表[FIDOGlossary]中均有定义。

此规范中的所有的图表、示例、注释都是非规范的。

> 注释
>
> 特定的结构成员需要遵从 FIDO 协议的要求。本文档中以 required为标示，标注了这些词汇在 WebIDL 的定义。关键词 required是在开发中版本[WebIDL-ED]提出，如果使用执行 WebIDL 开发程序的解析器[WebIDL]，则可删除在 WebIDL 中的关键词 required并通过其他方式将这些字段填满。

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. 概览

本节是非规范性的。

在竞争激烈的市场中，FIDO协议簇利用各种各样不同的设备使在线认证更简单安全。这背后的大部分复杂性对依赖方的应用程序来说是隐藏的，但是为了达到FIDO的目标，依赖方应该有多种方法来发现并校验认证器的特性。依赖方通过FIDO联盟发布的认证器元数据声明能够获取经核实的认证器信息的子集。访问元数据声明的URL通过元数据服务[UAFMetadataService]提供的元数据TOC（内容列表）文件获取。

相关术语的定义请参考FIDO术语表[FIDOGlossary]。

2.1 范围

本文档描述了*认证器元数据声明*的格式和其中包含的信息。关于不同消息类型的定义列表，可参考预定义值的FIDO注册表[UAFRegistry]。

关于认证器元数据分发过程和方法的描述，以及验证这些元数据的方法在 UAF 元数据服务规范[UAFMetadataService]中描述。

2.2 受众

本文档的目标受众包括：

- 想要为产品生成元数据的FIDO认证器供应商。
- FIDO服务实施者，它需要利用元数据声明来校验认证器的特性和鉴证声明、为协议消息选择合适算法、创建策略声明、或者使其他定制操作适应认证器特性。
- 想要达到下列功能的FIDO依赖方：

- 创建自定义策略声明来表明会接受哪个认证器。
- 基于他们的特性，对核心认证器进行风险评分。
- 校验经鉴证的认证器标识与第三方元数据相互对照。

2.3 架构

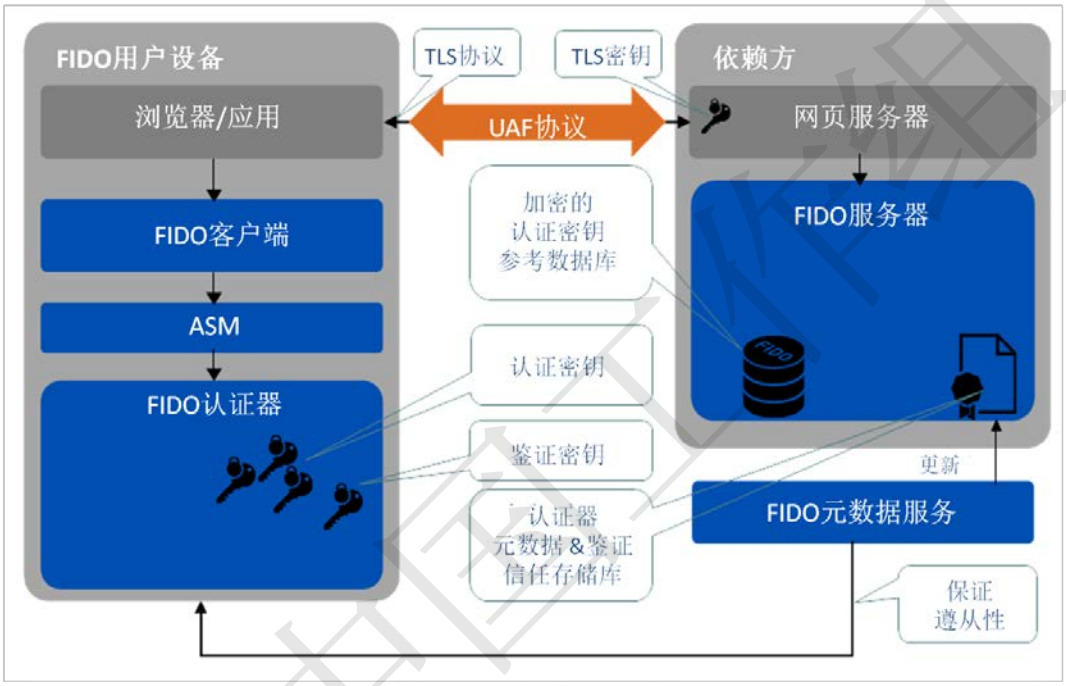

图 1 UAF 架构图

在依赖方的 FIDO 服务器直接使用认证器元数据声明，但是权威的声明中包含的信息会用在一些其他的地方。服务器如何获取元数据声明在[UAFMetadataService]*中做了描述。*

围绕认证器元数据声明的工作流如下：

1. 认证器供应商产生一个元数据声明，描述认证器的特性。
2. 作为 FIDO 认证过程的一部分，将元数据声明提交到 FIDO 联盟。FIDO 联盟按照[UAFMetadataService]中描述的方式，分发该元数据。
3. FIDO 依赖方配置它的注册策略，允许与特定特性匹配的认证器注册。
4. FIDO 服务器发送包含策略声明的注册挑战报文。
5. FIDO UAF 客户端接收到作为挑战报文一部分的策略声明。它根据自身汇报的特性查询可用的认证器，并且（根据用户输入）选择一个与策略相匹配的认证器，来进行注册。

6. 客户端处理并向服务器发送注册响应报文。该报文包含认证器的 AAID，也可以包含签名（可选），使用与认证器鉴证证书中的公钥对应的私钥进行签名。

7. FIDO 服务器使用认证器的 AAID 查询元数据声明。如果元数据声明中列有一个或多个鉴证证书，需要证明已提供鉴证签名，并且该签名是使用下列私钥之一进行签名：（a）对应于元数据声明中的一个证书的私钥，（b）与认证器元数据声明中列出的发行者证书相链接的证书的公钥对应的私钥。

8. FIDO 服务器根据权威元数据声明，验证认证器是否满足提供的原始注册策略。这样能够阻止错误的、被篡改的或者被截获的 FIDO UAF 客户端注册不符合策略的认证器。

9. *可选*，根据依赖方的输入，FIDO 服务器可能会为基于认证器的元数据设定风险或可信分数，包括既定策略中不选择的元素。

10. *可选*，FIDO 服务器可能会为认证器从第三方发布的其他元数据数据库相互对照经鉴证的 AAID。这种第三方元数据可能，例如，会通知 FIDO 服务器，认证器是否已经通过相关的特定市场或垂直行业的认证，或者是否满足应用程序特定的管制要求。

3. 类型

本节是规范性的。

3.1 CodeAccuracyDescriptor 结构

CodeAccuracyDescriptor描述了口令用户验证方式相关的准确性/复杂性。

> 注释
>
> 该方法的一个例子是手机 SIM 卡解锁使用的 4 位 PIN 码。
>
> 由于有足够多的证据[iPhonePasscodes][MoreTopWorstPasscodes]证明用户不会随机均匀分布地选择口令，我们使用数字系统 base（基数）和 minLen，代替可能的数字组合。这样软件可能会考虑不同基数的多种概率分布。这实质

上意味着在实际应用中口令并没有随机选出的那么安全。

```
WebIDL
dictionary CodeAccuracyDescriptor{
    required unsigned short    base;
    required unsigned short    minLength;
    unsigned short             maxRetries;
    unsigned short             blockSlowdown;
};
```

3.1.1 CodeAccuracyDescriptor 结构成员

base类型为 required unsigned short

编码的数字系统基数，例如，十进制数中的 10。

minLength类型为 required unsigned short

该编码的给定基数的最小数字位数，例如，4 代表 4 位数。

maxRetries类型为 unsigned short

认证器阻止该方法前（至少阻止一段时间）的错误尝试的最大次数。0 代表永远不会阻止。

blockSlowdown类型为 unsigned short

强制要求的最短等待时间秒数（例如，由于强制重启或类似操作）。0 代表该用户验证方法将被锁定，可能会永久锁定，也可能锁定该方法直至替代的用户验证方法成功以后。所有替代的用户验证方法必须在元数据的 userVerificationDetails中适当的说明。

3.2 BiometricAccuracyDescriptor 结构

BiometricAccuracyDescriptor描述了生物识别用户验证方式相关的准确性/复杂性。

注释

误识率（FAR）和*误拒率*（FRR）的值通常通过*受试者工作特征*（ROC）曲线相互依赖。

人工制品误识率（FAAR）值反映了检测外观攻击的能力，例如检测橡胶指纹外观。

这里给出的 FAR、FRR 和 FAAR 的值必须反映认证器的真实配置（与理论上的最佳情形的值截然相反）。

FAR、FRR 和 FAAR 必须设置至少一个。如果供应商不想指定这些值，那么 VerficationMethodDescriptor.baDesc必须被省略。

WebIDL

```
dictionary BiometricAccuracyDescriptor {
    double          FAR;
    double          FRR;
    double          EER;
    double          FAAR;
    unsigned short  maxReferenceDataSets;
    unsigned short  maxRetries;
    unsigned short  blockSlowdown;
};
```

3.2.1 BiometricAccuracyDescriptor 结构成员

FAR类型为 double

对于单个参考数据集的误识率[ISO19795-1]，即被接受为有效集的不匹配数据集的百分比。例如 0.1%的 FAR 被编码为 0.001。

注释

当所有参考数据集都被使用时，FAR 结果是 maxReferenceDataSets * FAR。

误识率与安全性相关。误识率越低意味着更高的安全性。

该值只覆盖实时捕获的主体 --- 不是人工制品的外观。

FRR类型为 double

对于单个参考数据集的误拒率，即提供的有效数据集被（错误）拒收的百分比。例如 0.1%的 FRR 被编码为 0.001。

注释

误拒率与便利性相关。误拒率越低意味着更高的便利性。

EER类型为 double

对于单个相关数据集的等错率。

FAAR类型为 double

人工制品误识率[ISO30107-1]，即被系统错误接受的人工制品百分比。例如 0.1%的 FAAR 被编码为 0.001。

> **注释**
>
> 人工制品误识率与系统安全性相关，其越低意味着安全性越高。

maxReferenceDataSets类型为 unsigned short

备选相关数据集的最大数量，例如，如果允许用户在基于指纹的认证器上注册 3 个不同的手指，该值则为 3。

maxRetries类型为 unsigned short

认证器阻止该方法前（至少阻止一段时间）的错误尝试的最大次数。0 代表永远不会阻止。

blockSlowdown类型为 unsigned short

强制要求的最短等待时间秒数（例如，由于强制重启或类似操作）。0 代表该用户验证方法将被锁定，可能会永久锁定，也可能锁定该方法直至替代的用户验证方法成功以后。所有替代的用户验证方法必须在元数据的 userVerificationDetails中适当的说明。

3.3 PatternAccuracyDescriptor 结构

PatternAccuracyDescriptor描述了图案用户验证方式相关的准确性/复杂性。

> **注释**
>
> 这种图案方式的例子，有安卓[AndroidUnlockPattern]屏幕解锁使用的 3x3 的点阵。这种情况下基于用户选择 4 位 PIN （该机制的最低要求），minComplexity是 1624。

WebIDL

```
dictionary PatternAccuracyDescriptor {
    required unsigned long    minComplexity;
    unsigned short            maxRetries;
    unsigned short            blockSlowdown;
};
```

3.3.1 PatternAccuracyDescriptor 结构成员

minComplexity类型为 required unsigned long

可能的图案（有最短长度）的数量，其中恰好有一个是正确的，例如，平均分配时的 1/概率。

maxRetries类型为 unsigned short

认证器阻止该方法前（至少阻止一段时间）的错误尝试的最大次数。0 代表永远不会阻止。

blockSlowdown类型为 unsigned short

强制要求的最短等待时间秒数（例如，由于强制重启或类似操作）。0 代表该用户验证方法将被锁定，可能会永久锁定，也可能锁定该方法直至替代的用户验证方法成功以后。所有替代的用户验证方法必须在元数据的 userVerificationDetails中适当的说明。

3.4 VerificationMethodDescriptor 结构

认证器实现的特定的*基本用户验证方法*的描述符。

基本用户验证方式必须从[UAFRegistry]描述的列表中选择。

> **注释**
>
> 实际上，上述描述的一些方法可能会组合起来。例如，基于指纹的用户验证可能与备选的口令相结合。

相关的 AccuracyDescriptor 的规范是可选的，但推荐使用。

WebIDL

```
dictionary VerificationMethodDescriptor {
    required unsigned long          userVerification;
    CodeAccuracyDescriptor          caDesc;
    BiometricAccuracyDescriptor     baDesc;
    PatternAccuracyDescriptor       paDesc;
};
```

3.4.1 VerificationMethodDescriptor 结构成员

userVerification类型为 required unsigned long

一个单独的 USER_VERIFY常数（参考[UAFRegistry]），不是位标记的组合。该值必须非零。

caDesc类型为 *CodeAccuracyDescriptor*

在 USER_VERIFY_PASSCODE方法的情况下可能会使用。

baDesc类型为 *BiometricAccuracyDescriptor*

在 USER_VERIFY_FINGERPRINT，USER_VERIFY_VOICEPRINT，USER_VERIFY_FACEPRINT，USER_VERIFY_EYEPRINT，或者 USER_VERIFY_HANDPRINT方法的情况下可能会使用。

paDesc类型为 *PatternAccuracyDescriptor*

在 USER_VERIFY_PATTERN方法的情况下可能会使用。

3.5 verificationMethodANDCombinations 类型定义

WebIDL

```
typedef VerificationMethodDescriptor[] VerificationMethodANDCombinations;
```

VerificationMethodANDCombinations必须是非空的。是一个包含作为成功用户验证的一部分而必须通过的基本用户验证方法列表的列表。

如果使用单一的用户验证方法是充足的，则该列表只包含一个条目。

如果该列表包含多个条目，那么所有被列出的用户验证方法都必须作为用户验证过程的一部分被通过。

3.6 rgbPalletteEntry 结构

rgbPalletteEntry是 RGB 三样品元组调色板条目。

WebIDL

```
dictionary rgbPalletteEntry {
    required unsigned short    r;
    required unsigned short    g;
    required unsigned short    b;
};
```

3.6.1 rgbPalletteEntry 结构成员

r类型为 required unsigned short

红色通道取样值。

g类型为 required unsigned short

绿色通道取样值。

b类型为 required unsigned short

蓝色通道取样值。

3.7 DisplayPNGCharacteristicsDescriptor 结构

DisplayPNGCharacteristicsDescriptor 描述了 PNG 图片的特性，如 PNG[PNG]规范中定义的 IHDR(图片头)和 PLTE（调色板表）。

WebIDL

```
dictionary DisplayPNGCharacteristicsDescriptor {
    required unsigned long    width;
    required unsigned long    height;
    required octet            bitDepth;
    required octet            colorType;
    required octet            compression;
    required octet            filter;
    required octet            interlace;
    rgbPalletteEntry[]        plte;
};
```

3.7.1 DisplayPNGCharacteristicsDescriptor 结构成员

width类型为 required unsigned long

图片宽度。

height类型为 required unsigned long

图片高度。

bitDepth类型为 required octet

位深，每个样品或每个调色板索引的位数。

colorType类型为 required octet

颜色类型定义了 PNG 图片的类型。

compression类型为 required octet

用来压缩图片数据的压缩方法。

filter类型为 required octet

过滤方法是压缩之前应用于图片数据的预处理方法。

interlace类型为 required octet

交错方法是图片数据的传输顺序。

plte类型为 *rgbPalletteEntry* 数组

1 到 256 的调色板条目。

4. 元数据键

本节是规范性的。

WebIDL

```
dictionary MetadataStatement {
    required AAID                                   aaid;
    required DOMString                              description;
    required unsigned short                         authenticatorVersion;
    required Version[]                              upv;
    required DOMString                              assertionScheme;
    required unsigned short                         authenticationAlgorithm;
    required unsigned short                         publicKeyAlgAndEncoding;
    required unsigned short[]                       attestationTypes;
    required VerificationMethodANDCombinations[]    userVerificationDetails;
    required unsigned short                         keyProtection;
    required unsigned short                         matherProtection;
    required unsigned long                          attachmentHint;
    required boolean                                isSecondFactoryOnly;
    required unsigned short                         tcDisplay;
    DOMString                                       tcDisplayContentType;
    DiscriptorPNGCharacteristicsDescriptor[]        tcDisplayPNGCharacteristics;
    required DOMString[]                            attestationRootCertificates;
    required DOMString                              icon;
};
```

4.1 MetadataStatement 结构成员

aaid类型为 required AAID

认证器验证标识符。AAID 的结构定义参见[UAFProtocol]。

description类型为 required DOMString

人类可读的对认证器的简短描述。

> **注释**
>
> 该描述应该有助于管理员配置认证器策略。该描述可能与认证器的 ASM 返回的描述有所不同。

authenticationVersion类型为 required unsigned short

最早的（例如，最低的）满足该元数据声明中规定要求的可信 authenticatorVersion。

向元数据 TOC对象[UAFMetadataService]中增加带有状态 UPDATE_AVAILABLE的新 StatusReport条目时，如果这次更新修复了严重的安全问题，必须也修改 authenticatorVersion。例如，之前的 StatusReport条目带有状态码 USER_VERIFICATION_BYPASS，ATTESTATION_KEY_COMPROMISE，USER_KEY_REMOTE_COMPROMISE，USER_KEY_PHYSICAL_COMPROMISE，REVOKED。

如果该版本比认证器显示的固件版本高（新），建议认为风险提高。例如，如果带有状态 USER_VERIFICATION_BYPASS或者 USER_KEY_REMOTE_COMPROMISE的 StatusReport条目高于 UPDATE_AVAILABLE条目，那么任何固件版本低于（旧于）元数据声明中规定的版本，即被认为是易受攻击的。

upv类型为 required Version 数组

该认证器支持的 UAF 协议版本。Version的结构定义参考 [UAFProtocol]。

assertionScheme类型为 required DOMString

认证器支持的断言方案。必须设为 FIDO UAF 注册表[UAFRegistry]中预定义的枚举字符串之一。

authenticationAlgorithm类型为 required unsigned short

认证器支持的认证算法。必须设为 FIDO UAF 注册表[UAFRegistry]中预定义的 UAF_ALG常数之一。

publicKeyAlgAndEncoding类型为 required unsigned short

在注册操作期间，认证器使用的公钥格式。必须设为 FIDO UAF 注册表[UAFRegistry]中预定义的 UAF_ALG_KEY常数之一。因为在与认证器发现或策略相关的 APIs 中不提供该信息，FIDO 服务器必须准备接受和处理任意或所有自身所支持的公钥算法的密钥表示。该值必须不为零。

attestationTypes类型为 required unsigned short 数组

支持的鉴证种类。（例如 TAG_ATTESTATION_BASIC_FULL）参考 UAF

注册表[UAFRegistry]了解更多详情。

userVerificationDetails类型为 required VerificationMethodANDCombinations 数组

一个*备选*的 VerificationMethodADNCombinations 列表。每一个这样的条目都是一个备选的用户验证方法。每一个备选的用户验证方法可能本身是多种形式的“与”组合。

所有有效的备选用户验证方法必须在此正确指定。如果该方法能够被用于以下其中一种情形，则用户验证方法被认为是有效的：

- 向一个用户验证方法注册新的验证参考数据。

  或者

- 成功验证用户以后，直接解锁用户认证密钥。

keyProtection类型为 required unsigned short

16 位的数字，代表 FIDO 注册表预定义值[UAFRegistry]中的 KEY_PROTECTION常数定义的位字段。

该值必须不为 0。

matcherProtection类型为 required unsigned short

16 位的数字，代表 FIDO 注册表预定义值[UAFRegistry]中的 MATCHER_PROTECTION常数定义的位字段。

该值必须不为 0。

> 注释
>
> 如果实现了多个匹配器，那么该值必须反映所有匹配器中*最弱*的实现。

attachmentHint类型为 required unsigned long

32 位的数字，代表 FIDO 注册表预定义值[UAFRegistry]中的 ATTACHMENT_HINT常数定义的位字段。

> 注释
>
> 认证器的连接状态和拓扑结构可能是瞬时的，并且不能作为权威的被依赖方信赖，但是元数据字段应该含有认证器所有可能的拓扑结构的位标记集。例如，一个认证器是一个通过蓝牙通信的单一目的的硬件令牌，应该设为 ATTACHMENT_HINT_EXTERNAL，而不

是 ATTACHMENT_HINT_INTERNAL。

isSecondFactorOnly类型为 required Boolean

指示认证器是否被设计来只能用作是第二因子，例如，需要一些其他的认证方式作为第一因子（比如，用户名+口令）。

tcDisplay类型为 required unsigned short

16 位的数字，代表 FIDO 注册表预定义值[UAFRegistry]中的 TRANSACTION_CONFIRMATION_DISPLAY 常数定义的位字段。

如果认证器不支持交易确认，该值必须设为 0。

tcDisplayContentType类型为 DOMString

交易确认显示支持的 MIME 内容类型[RFC2049]，例如 text/plain 或 image/png。

如果支持交易确认，该值必须出现。例如，tcDisplay不为 0。

tcDisplayPNGCharacteristics类型为 *DisplayPNGCharacteristicsDescriptor* 数组

一个*备选*的 DisplayPNGCharacteristicsDescriptor 列表。每一个条目都是一个备选的支持图片特性，用来显示 PNG 图片。

如果支持交易确认，该列表必须出现，例如，tcDisplay不为 0。

attestationRootCertificates类型为 required DOMString 数组

该数组中的每一个元素都代表一个该 AAID 有效的 PKIX[RFC5280]信任的 X.509 根证书。多个证书可能被相同的 AAID 的不同批次使用。数组并不代表一个证书链，而是仅仅代表这个链的信任锚。

每一个数列元素都是 Base64 编码（[RFC4648]第 4 章）、DER 编码[ITU-X690-2008]的 PKIX 证书值。每一个元素必须是认证器鉴证专用的。

注释

这里列出的证书是信任根。它可能是认证器显示的真实证书，或者它可能是一个从供应商得到的签发机构证书，认证器真正使用的证书与其相链接。

注册断言包括鉴证证书本身和有序的证书链（见[UAFAuthnrCommands]）。

- 制造商鉴证根证书。

  或

- 与特定 AAID 相关的根证书。

都必须在此处规定。

当（a）一个根证书可能覆盖多个认证器类型（例如，多个 AAID）。这种情况下，在鉴证证书的 SubjectDN CommonName (oid 2.5.4.3)项中必须规定 AAID。当（b）根证书仅仅覆盖单一 AAID，鉴证证书的 SubjectDN CommonName 项中不要求包含 AAID。

在备选的基础鉴证（见[UAFProtocol]，“替代的基础鉴证”章节）的情况下，不需要或使用鉴证根证书。因此，在这种情况下该数组必须为空。

icon类型为 required DOMString

认证器的 data:url[RFC2397]编码的 PNG[PNG]图标。

5. 元数据声明格式

本节是非规范性的。

> **规范**
>
> FIDO 认证器元数据声明是一个包含 JSON 编码的 MetadataStatement 结构 文档。

认证器的元数据声明的示例：

- authenticatorVersion（认证器版本）是 2。
- 基于指纹的用户验证，误识率为 0.001。
- 认证器集成在 FIDO 用户设备中。
- 鉴别密钥在可信执行环境中保护。
- (指纹)匹配器在可信执行环境中实现。
- 交易确认显示在可信执行环境中实现。
- 交易确认显示仅支持“image/png”对象的显示。
- 显示宽 320 像素，高 480 像素。每个像素提供 16 位位深的真彩色（=Color Type 2）。Zlib 压缩方式（0）。不支持过滤（例如，filter typeof= 0）并且不支持交错（interlace method = 0）。
- 该认证器可当作是第一因子或者第二因子，例如，isSecondFactorOnly=false。

- 支持“UAFV1TLV”断言方案。
- 使用 UAF_ALG_SIGN_ECDSA_SHA256_RAW鉴别算法。
- 使用UAF_ALG_KEY_ECC_X962_RAW公钥格式（0x100=256十进制）。
- 只实现了 TAG_ATTESTATION_BASIC_FULL方法（0x3E07=15879 十进制）。
- 只实现了 UAF 协议 1.0 版本。

例 1：MetadataStatement


```
{ "aaid": "1234#5678",
   "description": "FIDO Alliance Sample UAF Authenticator",
   "authenticatorVersion": 2,
   "upv": [{ "major": 1, "minor": 0 }],
   "assertionScheme": "UAFV1TLV",
   "authenticationAlgorithm": 1,
   "publicKeyAlgAndEncoding": 256,
   "attestationTypes": [15879],
   "userVerificationDetails": [ [ { "userVerification": 2, "baDesc": { "FAR":
   0.001 } } ] ],
   "keyProtection": 6,
   "matcherProtection": 2,
   "attachmentHint": 1,
   "isSecondFactorOnly": "false",
   "tcDisplay": 4,
   "tcDisplayContentType": ["image/png"],
   "tcDisplayPNGCharacteristics": [{"width": 320, "height": 480, "bitDepth":
   16,
   "colorType": 2, "compression": 0, "filter": 0, "interlace": 0}],
   "attestationRootCertificates": [
"MIICPTCCAeOgAwIBAgIJAOuexvU3Oy2wMAoGCCqGSM49BAMCMHsx
IDAeBgNVBAMMF1NhbXBsZSBBdHRlc3RhdGlvbiBSb290MRYwFAYDV
QQKDA1GSURPIEFsbGlhbmNlMREwDwYDVQQLDAhVQUYgVFdHLDE
SMBAGA1UEBwwJUGFsbyBBbHRvMQswCQYDVQQIDAJDQTELMAkG
A1UEBhMCVVMwHhcNMTQwNjE4MTMzMzMyWhcNNDExMTAzMTMz
MzMyWjB7MSAwHgYDVQQDDBdTYW1wbGUgQXR0ZXN0YXRpb24gU
m9vdDEWMBQGA1UECgwNRklETyBBbGxpYW5jZTERMA8GA1UECwwI
VUFGIFRXRywxEjAQBgNVBAcMCVBhbG8gQWx0bzELMAkGA1UECAw
CQ0ExCzAJBgNVBAYTAlVTMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQ
gAEH8hv2D0HXa59/BmpQ7RZehL/FMGzFd1QBg9vAUpOZ3ajnuQ94PR7a
MzH33nUSBr8fHYDrqOBb58pxGqHJRyX/6NQME4wHQYDVR0OBBYEFP
oHA3CLhxFbC0It7zE4w8hk5EJ/MB8GA1UdIwQYMBaAFPoHA3CLhxFbC0
It7zE4w8hk5EJ/MAwGA1UdEwQFMAMBAf8wCgYIKoZIzj0EAwIDSAAwR
QIhAJ06QSXt9ihIbEKYKIjsPkriVdLIgtfsbDSu7ErJfzr4AiBqoYCZf0+zI55aQe
AHjIzA9Xm63rruAxBZ9ps9z2XNlQ=="],
   "icon": "
iVBORw0KGgoAAAANSUhEUgAAAE8AAAAvCAYAAACiwJfcAAAAAX
NSR0IArs4c6QAAAARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA
```

7DAcdvqGQAAAahSURBVGhD7Zr5bxRlGMf9KzTB8AM/YEhE2W7pQZc
WKKBclSpHATlELARE7kNECCA3FkWK0CKKSCFIsKBcgVCDWGNESdA
YidwgggJBiRiMhFc/4wy8884zu9NdlnGTfZJP2n3nO++88933fveBBx+PqCzJk
TUvBbLmpUDWvBTImpcCSZvXLCdX9R05Sk19bb5atf599fG+/erA541q47aP
1LLVa9SIyVNUi8Ii8d5kGTsi30NFv7ai9n7QZPMwbdys2erU2XMqUdy8+Zca
NmGimE8yXN3RUd3a18nF0fUlovZ+0CTzWpd2Vj+eOm1bEyy6Dx4i5pUMG
Wveo506q227dtuWBIuffr6oWpV0FPNLhow1751Nm21LvPH3rVtWjfz66Lfql
8tX7FRl9YFSXsmSseb9ceOGbYk7MNUcGPg8ZsbMe9rfQUaaV/JMX9sqdzD
CSvp0kZHmTZg9x7bLHcMnThb16eJ+mVfQq8yaUZQNG64iXZ+0/kq6uOZF
O0QtatdWKfXnRQ99Bj91R5OIFnk54jN0mkUiqlO3XDW+Ml+98mKB6tW7r
WpZcPc+0zg4tLrYlUc86E6eGDjIMubVpcusearfgIYGRk6brhZVr/JcHzooL755
0jedLExopWcApi2ZUqhu7JLvrVsQU81zkzOPeemMRYvVuQsX7PbiDQY5Jv
ZonftK+1VY8H9utx530h0ob+jmRYqj6ouaYvEenW/WlYjp8cwbMm682tPwq
W1R4tj/2SH13IRJYl4moZvXpiSqDr7dXtQHxa/PK3/+BWsK1dTgHu6V8tQJ3
bwFkwpFrUOQ50s1r3levm8zZcq17+BBaw7K8lEK5qzkYeark9A8p7P3GzDK
+nd3DQow+6UC8SVN82iuv38im7NtaXtV1CVq6Rgw4pksmbdi3bu2De7YfaB
BxcqfvqPrUjFQNTQ22lfdUVVT68rTJKF5DnSmUjgdqg4mSS9pmsfDJR3G6T
oH0iW9aV7LWLHYXKllTDt0LTAtkYIaamp1QjVv++uyGUxVdJ0DNVXSm
+b1qRxpl84ddfX1Lp1O/d69tsod0vs5hGre9xu8o+fpLR1cGhNTD6Z57C9KM
WXefJdOZ94bb9oqd1ROnS7qITTzHimMqivbO3g0DdVyk3WQBhBztK35YK
NdOnc8O3acS6fDZFgKaXLsEJp5rdrliBqp89cJcs/m7Tvs0rkjGfN4b0kPoZn3U
JuIOrnZ22yP1fmvUx+O5gSqebV1m+zSuYNVhq7TWbDiLVvljplLlop6CLXP
+2qtvGLIL/1vimISdMBgzSoFZyu6Tqd+jzxgsPaV9BCqee/NjYk6v6lK9cwiUc/
STtf1HDpM3b592y7h3Thx5ozK69HLpYWuAwaqS5cv26q7ceb8efVYaReP3iF
U8zj1knSwZXHMmnCjY0Ogalo7UQfSCM3qQQr2H/XFP7ssXx45Yl91ByeCe
p4moZoH+1fG3xD4tT7x8kwyj8nwb9ev26V0B6d+7H4zKvudAH537FjqyzOH
dJnHEuzmXq/WjxObvNMbv7nhywsX2aVsWtC8+48aLeapE7p5wKZi0A2AQ
RV5nvR4E+uJc+b61kApqInxBgmd/4V5QP/mt18HDC7sRHftmeu5lmhV0rn/A
LX232bqd4BFnDx7Vi1cWS2uff0IbB47qexxmUj9QutYjupd3tYD6abWBBMrh
+apNbOKrNF1+ugCa4riXGfwMPPtViavhU3YMOAAnuUb/R07L0yOSeOadE
88ApsXFGff30ynhlJgM51CU6vN9EzgnpvHBFUyiVraePiwJ53DF5ZTZnomE
Ng85kNUd2oJi2Wpr4OmmkfN4x4zHfiVFc8Dv8NzuhNqOidilGvA6DGueZw
O78AAQn6ciEk6+rw5VcvjvqNDYPOoIUwaKShrxAuXLlkH4aYuGfMYDc10
WF5Ta31hPJOfcUhrU/JlINi6c6elRYdBpo6++Yfjx61lGNfRm4MD5rJ1j3FoGH
njDSBNarYUgMLyMszKpb7tXpoHfPs8h3Wp1LzNfNk54XxC1wDGUmYzX
Yefh6z/cKtVm4EBxa9VQGDzYr3LrUMRjHEKkk7zaFKYQA2hGQU1z+85N
FWpXDrkz3vx10GqxQ6BzeNboBk5n8k4nebRh+k1hWfxTF0D1EyWUs5nv+d
gQqKaxzuCdE0isHl02NQ8ah0mXr12La3m0f9wik9+wLNTMY/86MPo8yi31O
fxmT6PWoqG9+DZukYna56mSZt5WWSy5qVA1rwUyJqXAlnzkiai/gHSD7R
kTyihogAAAABJRU5ErkJggg==="
}

示例认证器*用户验证方法*条目含有：

- 基于指纹的用户验证方法，并且：
    - 拥有允许用户最多注册 5 个手指（参考数据集）的能力，并且：
        - 每一个手指的误识率为 1/50000(0.002%)。结果用 FAR 表示是 0.01%（0.0001）。

    - 指纹验证会在 5 次失败后被锁定。
- 最短长度为 4 个十进制数字的 PIN 码必须被设置为备选验证方法。当指纹验证被锁定后，需要输入 PIN 来重新激活基于指纹的验证方式。

例 2：用户验证方式条目

```
[
  [ { "userVerification": 2, "baDesc": { "FAR": 0.00002,
  "maxReferenceDataSets": 5,
  "maxRetries": 5, "blockSlowdown": 0} }],
  [ { "userVerification": 4, "caDesc": { "base": 10, "minLength": 4 } } ]
]
```

6. 其他的考虑

本节是非规范性的。

6.1 字段更新和元数据

元数据声明一旦发布以后应该是稳定的。当认证器的字段中有更新，这样的更新预计将提高认证器安全性（例如，改良误识率或误拒率）。如果有能解决严重的安全问题（例如，之前报告的）固件的更新可用，authenticatorVersion必须更新。

注释

元数据声明假定为与拥有相同 AAID 的所有认证器相关。

注释

如果元数据声明中规定的 authenticatorVersion比认证器中显示的新（高），建议 FIDO 服务器假定风险提高了。

规范

认证器功能的重要变化不在固件更新的范畴中。例如，如果认证供应商想要修改基于 PIN 的认证器来使用“人声识别”作为用户验证方式，那么供应商必须为该认证器分配一个新的 AAID。

规范

一个单一的认证器的实现可以报告它自己是两个使用不同 AAID 的“虚拟”认证器。这样的实现必须妥善保护 UAuth密钥以及其他敏感数据不被其他“虚拟”认证器访问，如同一个普通认证器所做的。

注释

为一个 AAID 注册的鉴别密钥（UAuth.pub）不能被申报了不同 AAID 的认证器使用，即使运行的硬件相同（参考[UAFProtocol]的“FIDO 服务器鉴别响应处理规则”章节）。

A. 参考文献

A.1 参考规范

[ISO19795-1]

ISO/IEC JTC 1/SC 37, *Information Technology - Biometric peformance testing and reporting - Part 1: Principles and framework*, URL:*http://www.iso.org/iso/catalogue_detail.htm?csnumber=41447*

[ISO30107-1]

ISO/IEC JTC 1/SC 37, *Information Technology - Biometrics - Presentation attack detection - Part 1: Framework*, URL:*http://www.iso.org/iso/catalogue_detail.htm?csnumber=53227*

[RFC2049]

N. Freed, N. Borenstein, *Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples (RFC 2049)*, IETF, November 1996, URL: *http://www.ietf.org/rfc/rfc2049.txt*

[RFC2397]

L. Masinter. *The "data" URL scheme.* August 1998. Proposed Standard. URL: *https://tools.ietf.org/html/rfc2397*

[WebIDL-ED]

Cameron McCormack, *Web IDL*, W3C. Editor's Draft 13 November 2014. URL: http://heycam.github.io/webidl/

A.2 参考资料

[AndroidUnlockPattern]

Android Unlock Pattern Security Analysis. Sinustrom.info web site. URL: http://www.sinustrom.info/2012/05/21/android-unlock-pattern-security-analysis/

[ECMA-262]

ECMAScript Language Specification, Edition 5.1. June 2011. URL:http://www.ecma-international.org/publications/standards/Ecma-262.htm

[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

[MoreTopWorstPasswords]

10000 Top Passwords, Mark Burnett (Accessed July 11, 2014) URL:https://xato.net/passwords/more-top-worst-passwords/

[PNG]

Tom Lane. *Portable Network Graphics (PNG) Specification (Second Edition)*. 10 November 2003. W3C Recommendation.

URL:http://www.w3.org/TR/PNG

[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

[RFC4648]

S. Josefsson, *The Base16, Base32, and Base64 Data Encodings (RFC 4648)*, IETF, October 2006, URL:http://www.ietf.org/rfc/rfc4648.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

[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

[UAFMetadataService]

R. Lindemann, B. Hill, D. Baghdasaryan, *FIDO UAF Metadata Service v1.0*. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-metadata-service-v1.0-ps-20141208.html

PDF: fido-uaf-metadata-service-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

[UAFRegistry]

R. Lindemann, D. Baghdasaryan, B. Hill, *FIDO UAF Registry of Predefined Values*. FIDO Alliance Proposed Standard. URLs:

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

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

[WebIDL]

Cameron McCormack. *Web IDL*. 19 April 2012. W3C Candidate Recommendation. URL: http://www.w3.org/TR/WebIDL/

[iPhonePasscodes]

Most Common iPhone Passcodes, Daniel Amitay (Accessed July 11, 2014) URL: http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes