FIDO协议读书笔记

笔记本：	FIDO		
创建时间：	2015/10/16 9:35	**更新时间：**	2015/10/26 9:44
作者：	yangzhou1989@gmail.com		
URL：	file:///E:/workspace/docs/fido/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-...		

蓝色是表疑问

FIDO UAF Protocols
user devices和replying parties之间用FIDO UAF messages通信。这些message处理：
Authenticator Registration

架构：

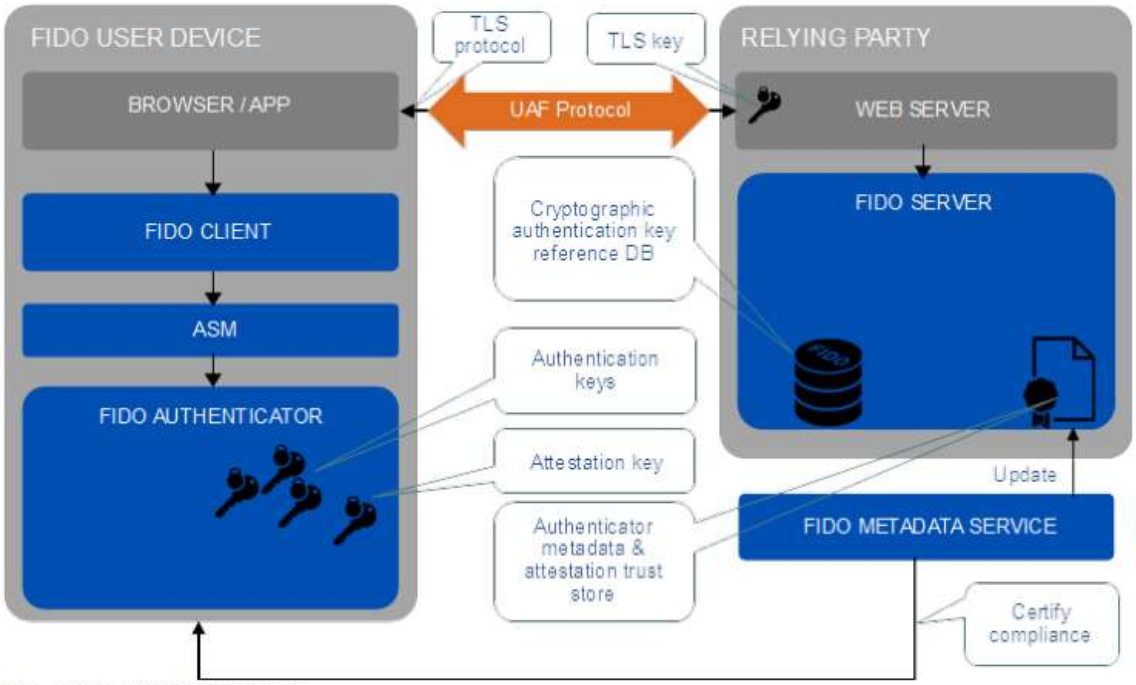
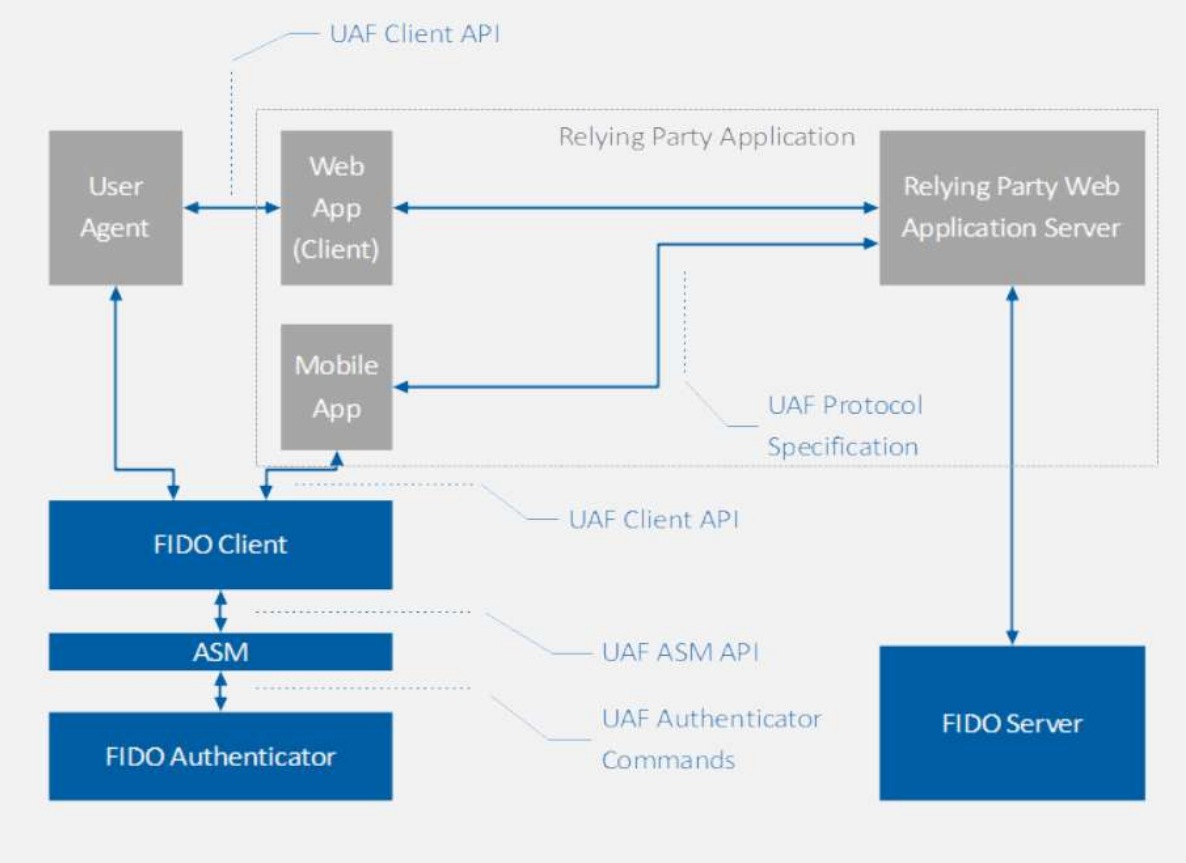


Fig. 1 The UAF Architecture

FIDO METADATA SERVICE：UAF Authenticator Metadata describing all the authenticators it will interact with.
ASM：Autheticator-specific Module
UAF authenticators may be connected to a user device via various physical interfaces (SPI, USB, Bluetooth, etc). The UAF Authenticator-Specific Module (ASM) is a software interface on top of UAF authenticators which gives a standardized way for FIDO UAF Clients to detect and access the functionality of UAF authenticators and hides internal communication complexity from FIDO UAF Client.(ASM Spec)



协议的交互：

Registration

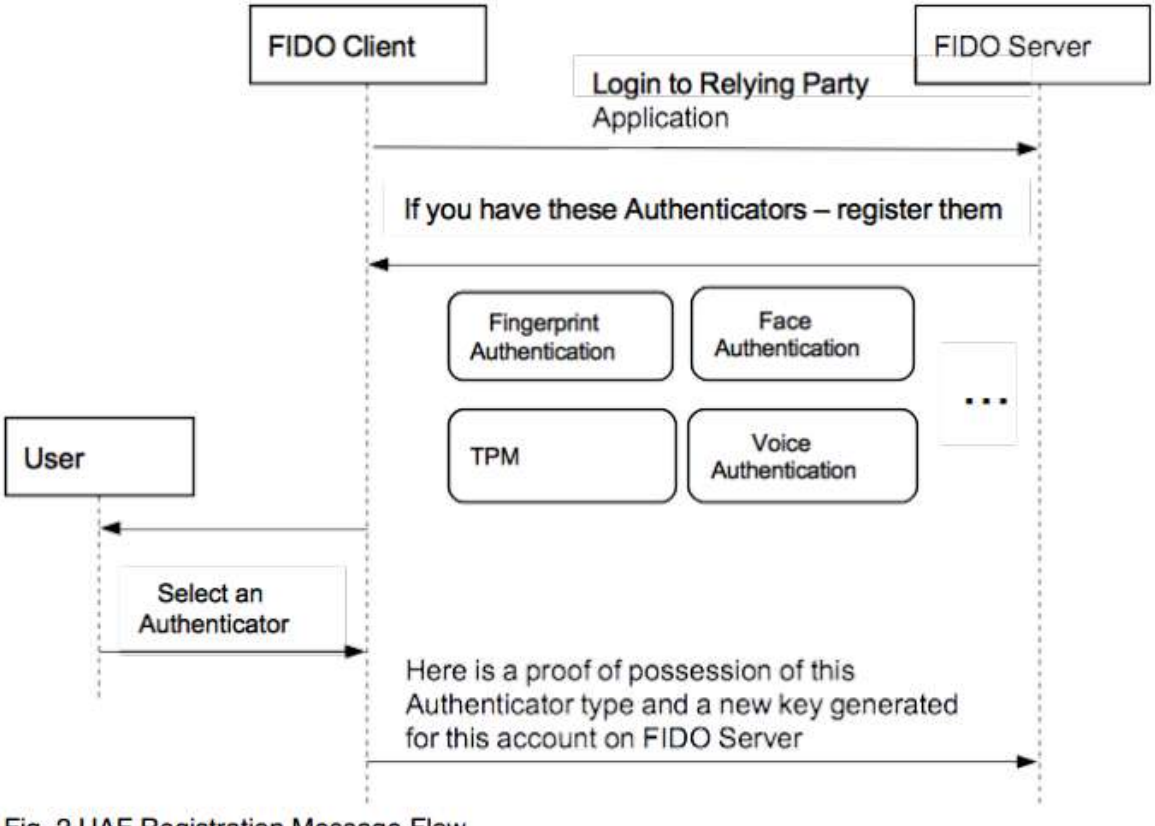


Fig. 2 UAF Registration Message Flow

所以这些认证器(Fingerprint, Face, TPM, Voice)基本都是用户提前就已经做好的（比如拿到手机第一次开机就要求用户输入了指纹，声纹）

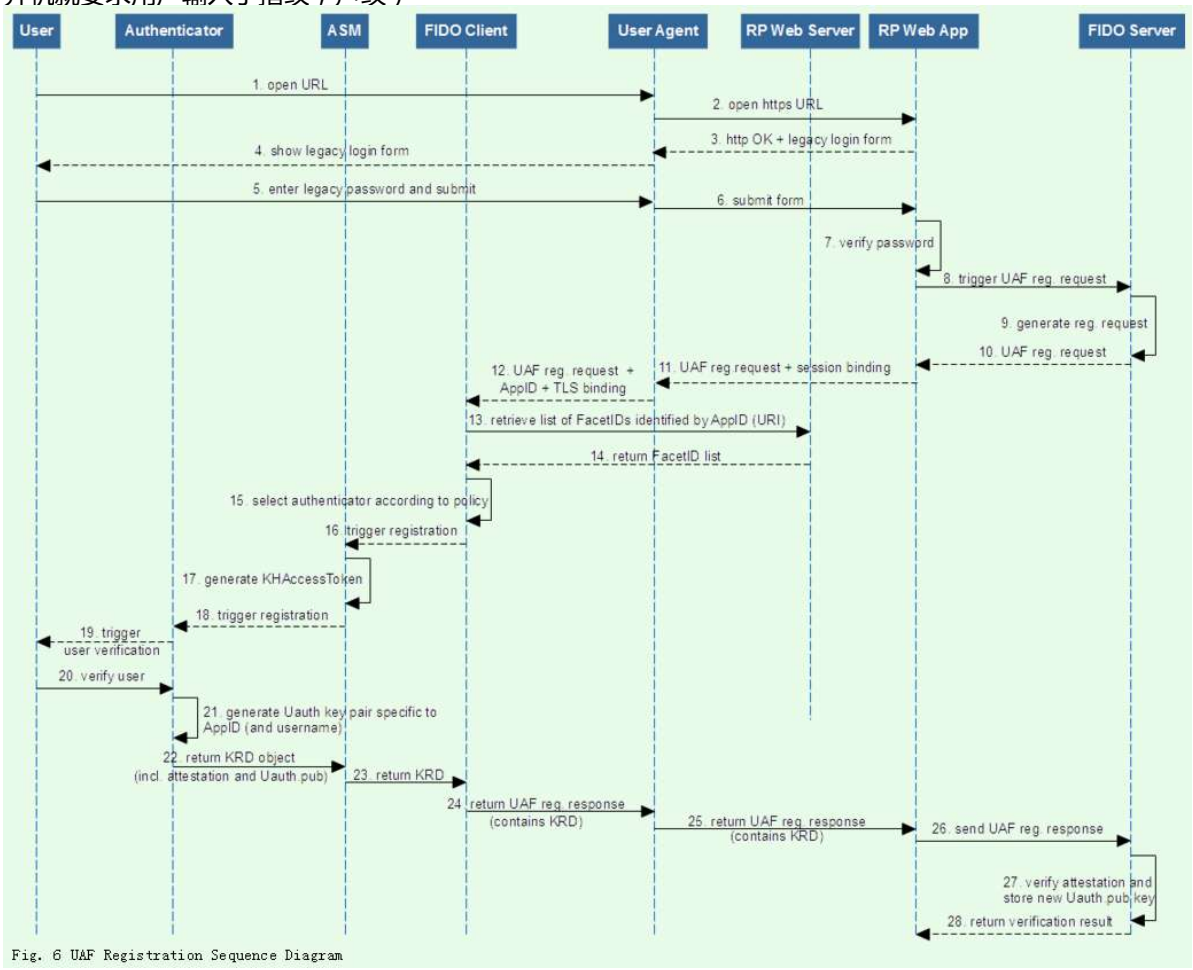
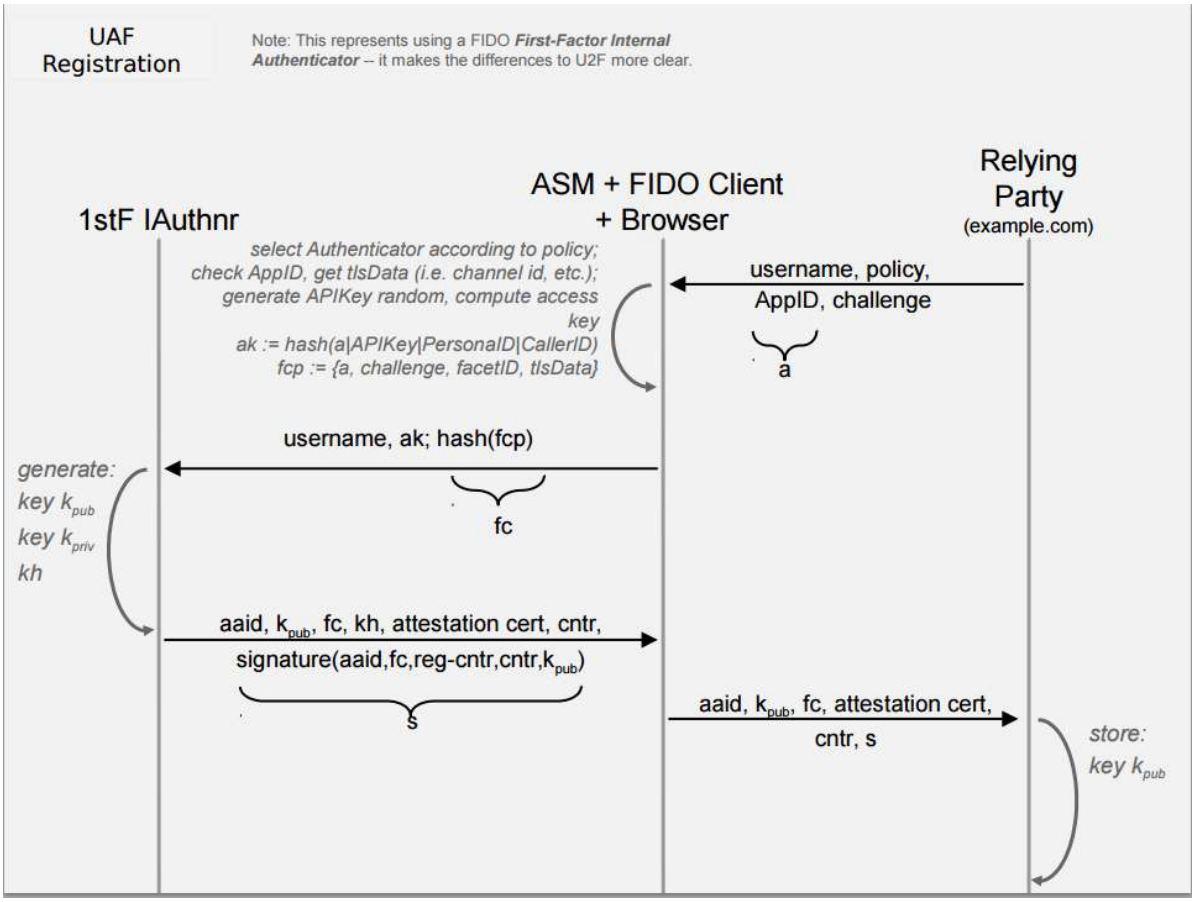


Fig. 6 UAF Registration Sequence Diagram



注意，AppID是Relying Party那边的：The application identifier that the relying party would like to assert.

AppID

The AppID is an identifier for a set of different Facets of a relying party's application. The AppID is a URL pointing to the TrustedApps, i.e. list of FacetIDs related to this AppID.

那么，facetID是什么: 客户端通过AppID去请求一个FacetID List，FacetID List包含一串FacetID，可能分别对应该App的Android端（ the facet id is the URI android:apk-keyhash: <hash-of-apk-signing-cert> ），iOS端(URI ios: bundle-id: <ios-bundle-id-of-app>)，web端(RFC6454 origin)

ak中的PersonalID和CallerID是什么？

aaid又是什么：Authenticator Attestation ID。每一个认证器都要有一个aaid，而厂家生产的特定型号的认证器必须有相同的AAID：

The `AAID` is a string with format "V#M", where

"#" is a separator

"V" indicates the authenticator Vendor Code. This code consists of 4 hexadecimal digits.

"M" indicates the authenticator Model Code. This code consists of 4 hexadecimal digits.

The Augmented BNF [ABNF] for the AAID is:

```
AAID = 4(HEXDIG) "#" 4(HEXDIG)
```

每个AAID都需要对应一个authentication metadata file

KeyID是什么： KeyID is a unique identifier (within the scope of an AAID) used to refer to a specific UAuth.Key. It is generated by the authenticator and registered with a FIDO Server.

所以，KeyID是唯一标识Authentication公私钥对的。一个AAID可以对应多个KeyID，因此在一个AAID范围内，KeyID必须唯一。

The (AAID, KeyID) tuple MUST uniquely identify an authenticator's registration for a relying party. Whenever a FIDO Server wants to provide specific information to a particular authenticator it MUST use the (AAID, KeyID) tuple.

KeyID is the SHA256 hash of the KeyHandle managed by the ASM.

KeyHandle是什么：

A key container created by a FIDO Authenticator, containing a private key and (optionally) other data (such as Username). A key handle may be wrapped (encrypted with a key known only to the authenticator) or unwrapped. In the unwrapped form it is referred to as a Raw Key Handle. 2F Authenticators must retrieve their Key Handles from the Relying Party to function, 1F Authenticators manage the storage of their own Key Handles, either internally (for External Authenticators) or at the ASM layer. (for Internal Authenticators)

string[9]

Each authenticator must have an AAID to identify UAF enabled authenticator models globally. The AAID must uniquely identify a specific authenticator model within the range of all UAF-enabled authenticator models made by all authenticator vendors, where authenticators of a specific model must share identical security characteristics within the model (see Security Considerations).

The AAID is a string with format "V#M", where

"#" is a separator

"V" indicates the authenticator Vendor Code. This code consists of 4 hexadecimal digits.

"M" indicates the authenticator Model Code. This code consists of 4 hexadecimal digits.

The Augmented BNF [ABNF] for the AAID is:

```
AAID = 4(HEXDIG) "#" 4(HEXDIG)
```

Authentication

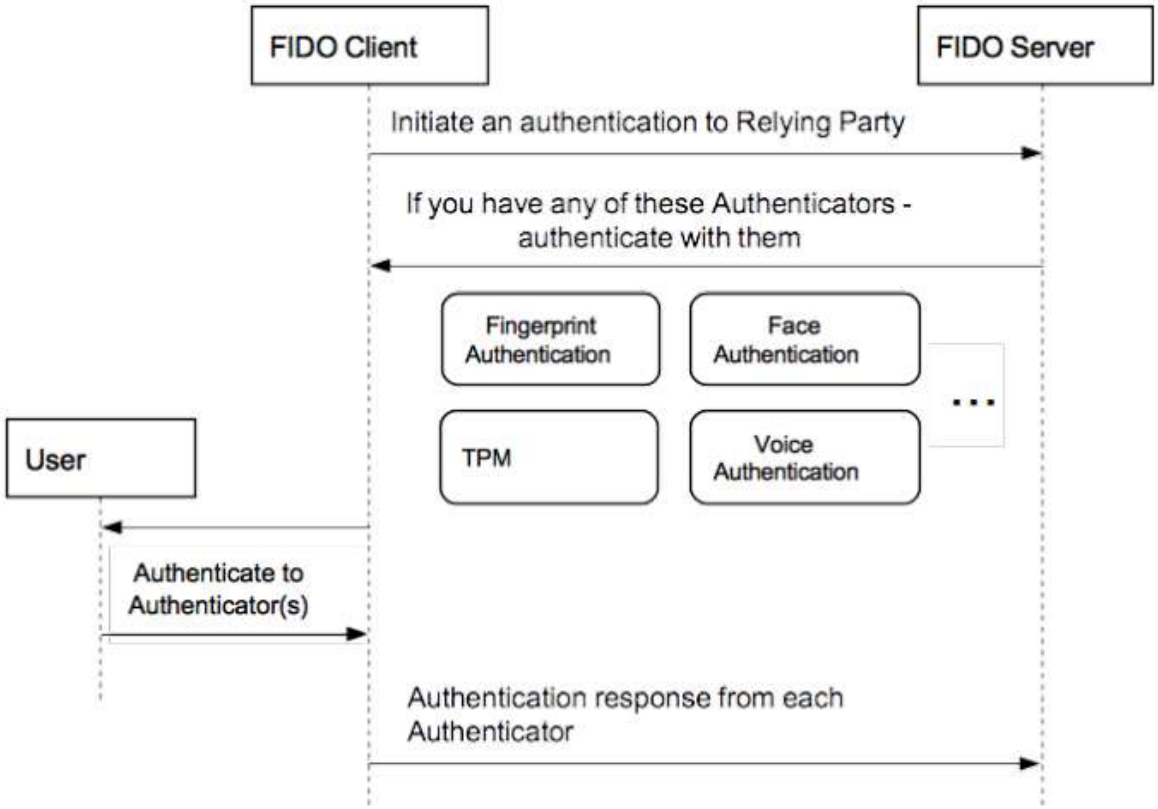
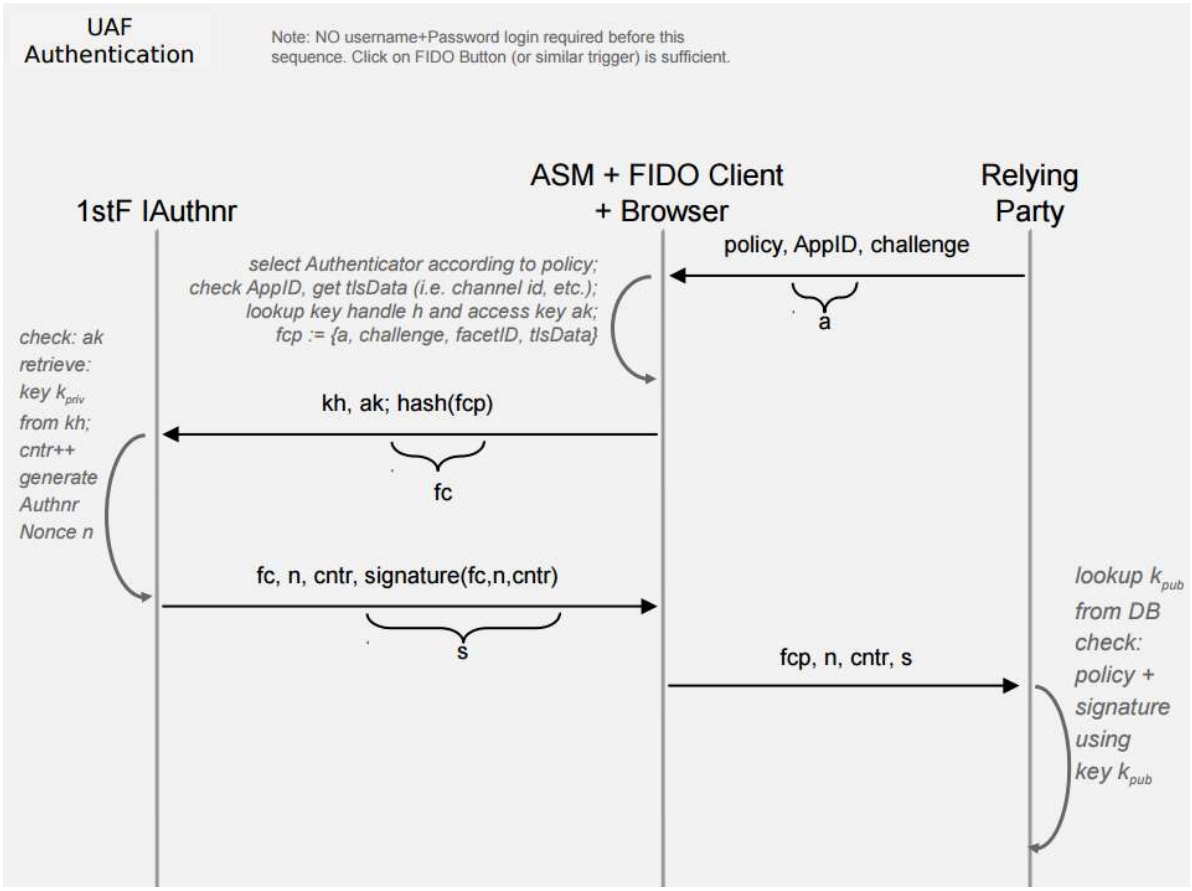


Fig. 3 Authentication Message Flow



Transaction Confirmation

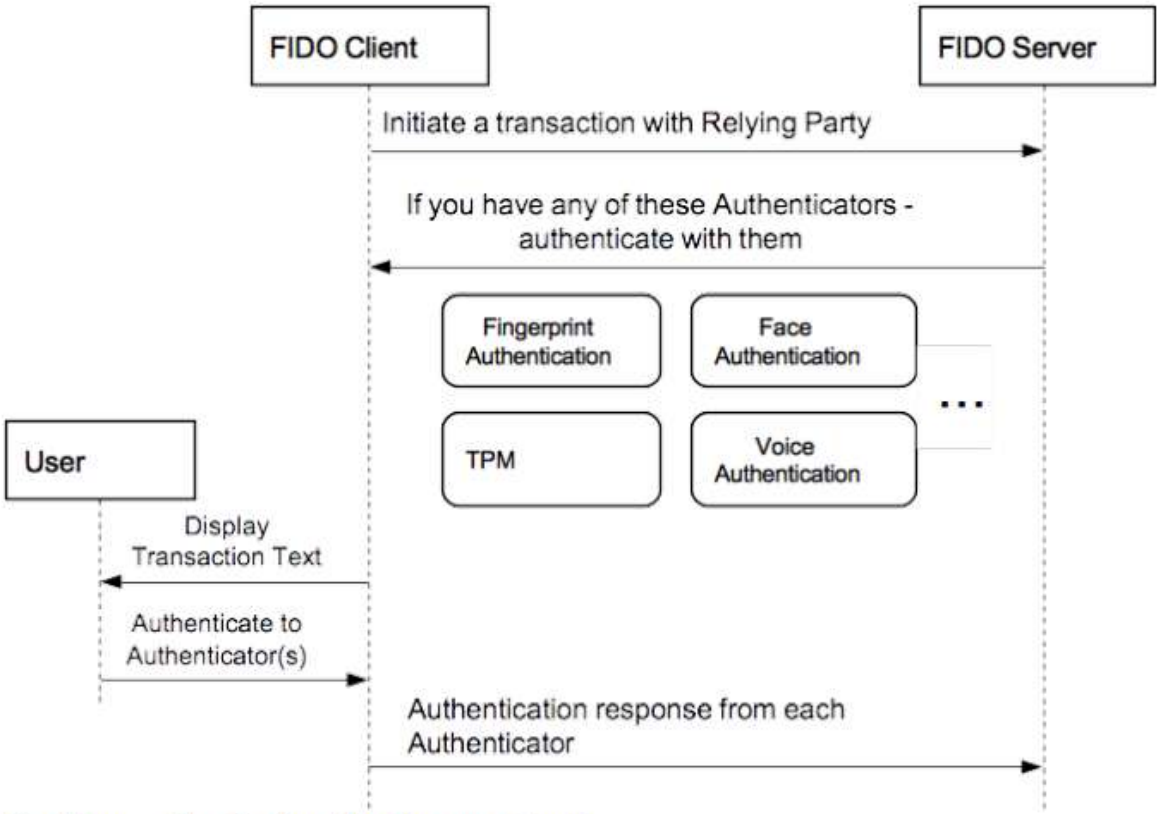


Fig. 4 Transaction Confirmation Message Flow

Deregistration

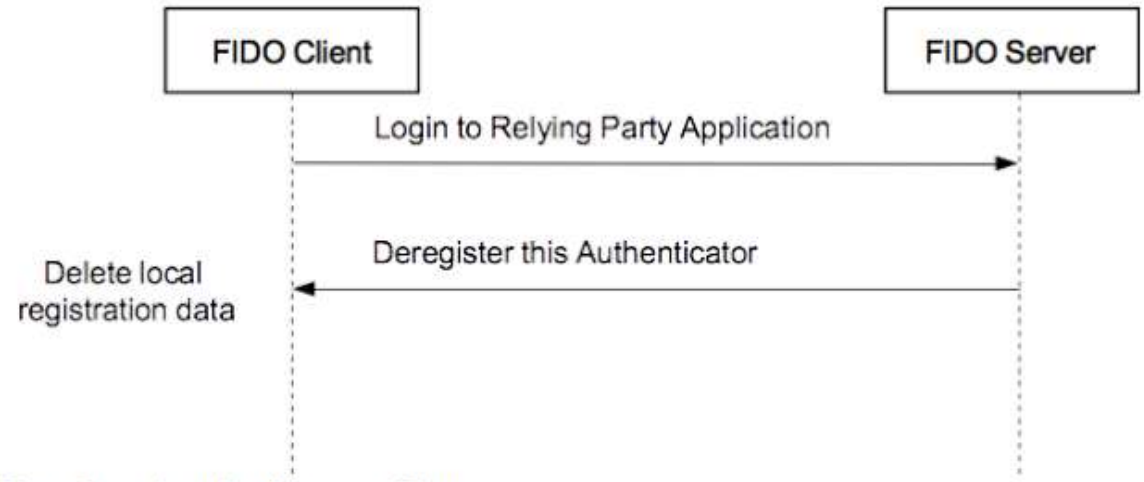
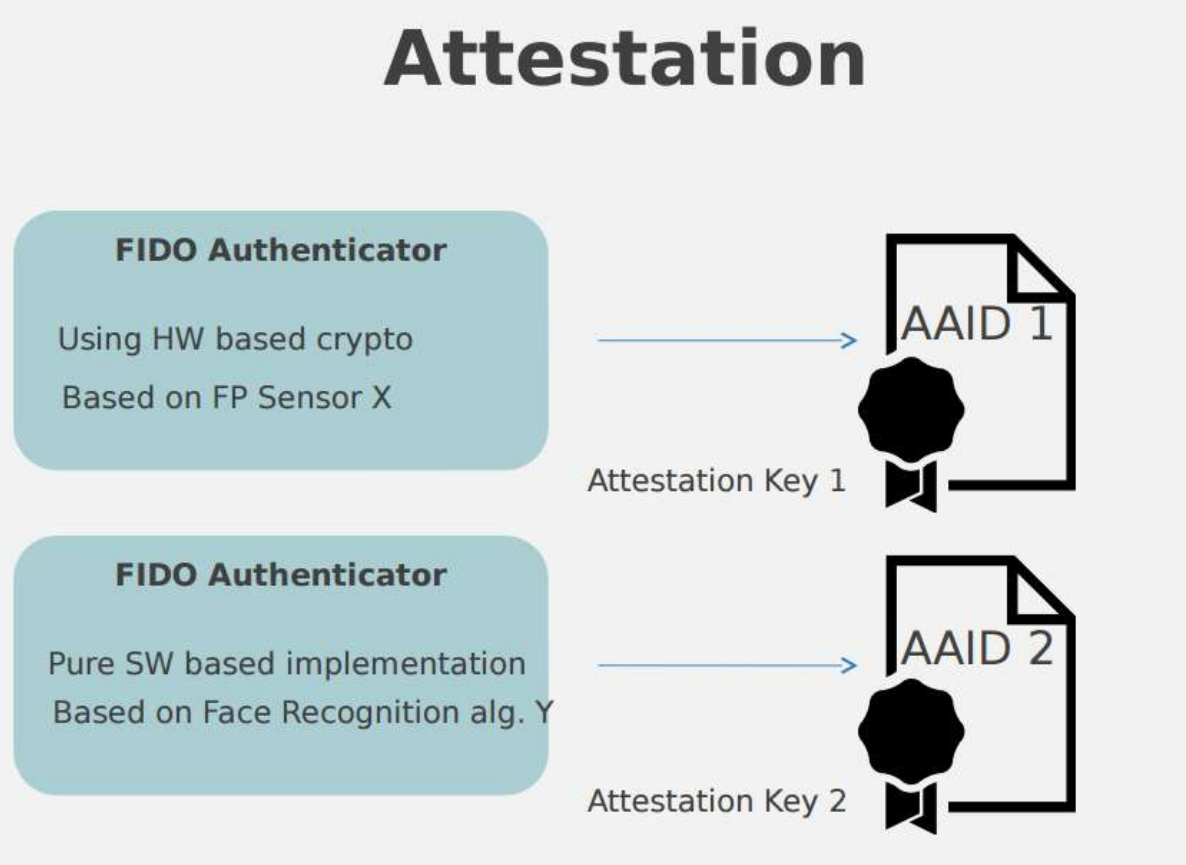


Fig. 5 Deregistration Message Flow

Attestation



Attestation Key是一开始就生成的，嵌入在设备中固定不变的key。而Athentication Key是在注册时运行时生成的

跟AAID的关系？