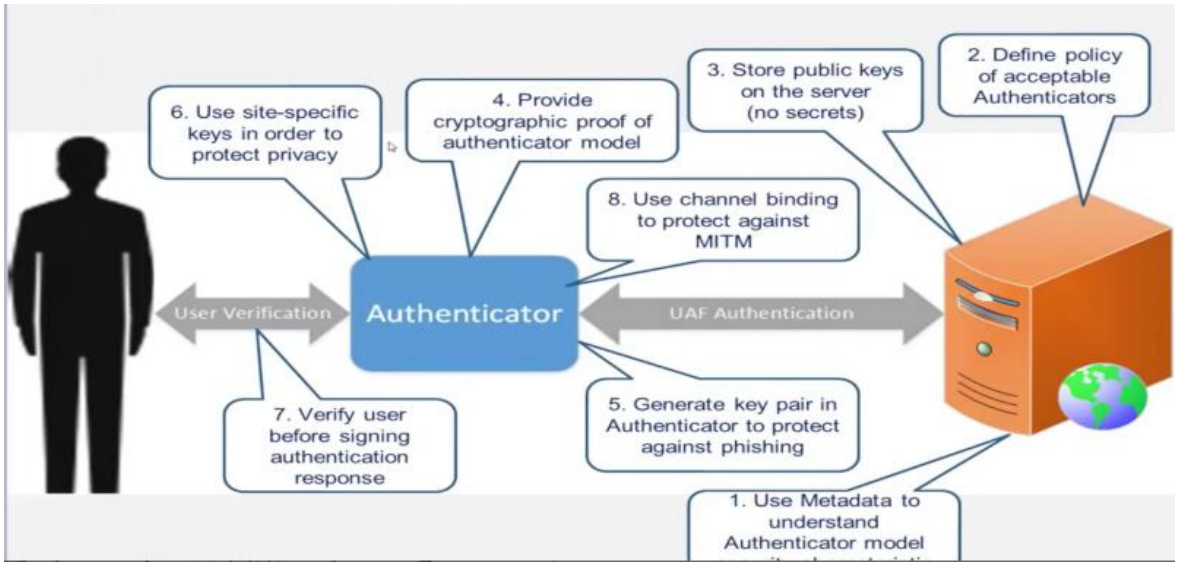
1.FIDO 技术背景

FIDO（Fast Identity Online）联盟成立于 2013 年 2 月，并于 2014 年 12 月公开发布第一版正式文档 FIDO 1.0。其中 UAF :Universal Authentication Framework，提供无密码和多因素认证安全体验，是基于公钥密码体制的一种认证协议，终端设备注册或用户身份认证时通过各种非口令密码机制实现身份认证，如滑动手指，说一句话，或者 pin 码，又或者是多种生物特征结合校验。

UAF 包括本地身份校验和在线公钥身份验证两个步骤，首先由本地认证器设备验证用户身份，之后使得用户有权利调用认证器内的密钥进行在线的公钥身份认证运算。UAF 相对于传统的在线认证有如下的优势：

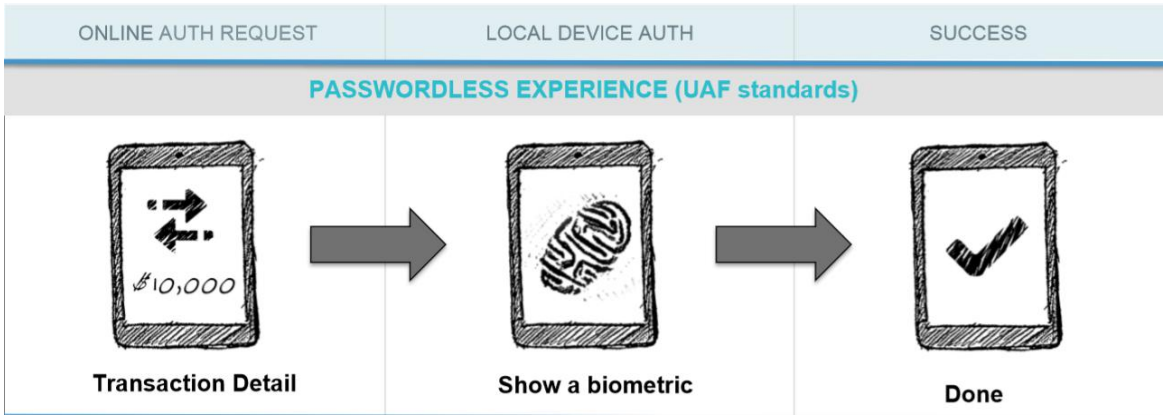
- 隐私和安全

传统的用户名口令方式存在输入困难，不安全，难以记忆等问题。FIDO 的本地认证器负责校验用户信息，服务端只存有一个对应的公钥信息，使得用户隐私得到最大的保护。同时，FIDO 协议在通信层使用 TLS 作为底层通信安全协议，并建议使用 TLS channel ID（Toking Binding）技术防止 TLS 协议的 MITM 攻击。在应用层，本身使用公钥机制实现身份的认证。通信层和应用层的协议规定最大限度的保护了身份认证的安全性。UAF 的工作原理和安全机制如图:



- 便捷友好

无密的认证方式更容易被用户接受，如生物特征，按键等，用户无需对各个网络服务记忆各种口令密码，也无需担心简单的口令会被攻击。用户只要在一个伴身的设备上讲话，按键，指纹按压即可实现多个网络服务的身份认证，更符合用户的场景体验。UAF 应用对用户终端支付过程的一个例子如下：



FIDO 在全球目前已有 200 多个成员，得益于 FIDO 的便捷和安全性，FIDO 在网络支付，登录企业服务，远程医疗产品，云存储服务，企业管理，移动互联网认证等领域有广泛应用。

2.电视购物场景

现有的智能电视仍然缺少较好的人机互动方式，尤其是面向输入文本或数字信息的时候。一些新兴的交互方式如语音，体感等开始普及，但存在识别率不高，偶尔无法正确感知的问题。使用技术对特定场景进行优化，减少用户输入和操作可获得更好的用户体验。

在智能电视购物过程中，简化登录和支付流程，减少密码输入，提供极简和高准确度的用户体验，对于在电视上推广用户购物操作具有非常大的意义。这与 FIDO 推崇的简单，无密认证，基于公钥的强认证技术等理念相吻合。针对智能电视轻交互特点定制 FIDO 方案实现一键用户登录和一键支付，能有效提高用户体验，减少支付流程，增强支付过程安全性。

在电视支付过程实现一键登录和一键支付认证有如下的优势：

1、用户体验

传统的电视支付过程繁琐，如绑定银行卡，短信验证码等。目前的主流解决方案则是扫码支付，通过更容易输入的手机来完成支付，但每次支付需要额外的手机设备，不易培养用户的电视购物习惯。对电视用户来说，只需在伴身的遥控器上一键认证即可完成加入购物

车或者完成支付是极简的方式，有利于培养用户电视支付习惯。直接在遥控器上完成认证过程符合广大的传统电视用户群操作习惯，减少学习成本。

2、用户群扩大

对于购物或支付平台来说，遥控器的一键认证与手机端的指纹支付体验类似，相似的购物体验可以吸引用户在电视端直接完成操作，减少学习成本，从而增加电视业务的价值。与此同时，电视支付可以覆盖传统的电视客户群，新颖的支付方式可增加对传统电视用户的吸引力，增加购物平台/支付平台的用户群数量。

3、较低的成本

认证协议满足 FIDO UAF 1.0，提供定制的终端 SDK 和遥控器产品，采用遵守 FIDO 协议的认证方式，使得与其他环节沟通和研发的成本降低。采用标准化的协议可以减少与购物平台和支付平台的评估时间和沟通时间。

3.电视购物解决方案

FIDO 标准文档只规定了各个节点之间的协议和交互接口 ,没有各个节点的实现方法和形式。 在 FIDO UAF 认证器设计上，为了安全性和便捷性，我们在终端硬件集成了安全 IC 和蓝牙芯片，同时实现了一键认证功能，同时为了以后扩展性的需要，在模块上保留了生物特征识别认证的接口。在认证器模块上，我们利用安全 IC 用于生成，存储认证密钥，并提供密钥的安全和加速计算服务，通过用户的物理接触一键确认实现用户身份的确认，避免软件和一些硬件的攻击。

在方案推广上，我们定制了智能电视的购物方案，认证平台和终端只需要对接 SDK 和含有认证器模块的遥控器即可支持 FIDO 服务，实现一键账户登录和一键支付功能。 终端 SDK 基于蓝牙 smart 4.0 和 android 4.3 以上平台。为了简化购物操作，在注册和注销阶段，智能电视购物方案通过移动端授权/取消授权遥控器使用，授权/取消授权遥控器一键登录和一键支付功能使用；在认证和交易环节，则通过遥控器直接与电视终端交互实现一键登录和一键支付购物。

实现效果截图

4. 电视购物项目优势

1）安全性 ,安全 IC 和遥控器的家庭属性保证终端认证器安全 ,网络层采用基于公钥的 FIDO UAF 协议，确保网络安全。

在超出遥控器使用授权时间范围外，MCU 代码将 lock 相关的 slot 数据，禁止被直接读取到敏感信息；

当遥控器丢失后，用户可使用移动端进行注销，在遥控器授权时间范围内的注销服务端会强制修改登录口令。

安全 IC 负责安全存储密钥 ,lock 掉的 slot 私钥无法直接导出 ,只输出 ECC 运算结果。

用户安全输入对接认证器的安全模块，与蓝牙业务隔离。

一键登录功能与用户手动输入口令安全强度类似，都需要用户参与，但简化了用户操作。

传输和在线认证安全基于 FIDO UAF 1.0，基于 TLS 1.2 以及 channelID 技术，应用层用户认证基于基于挑战的私钥签名。

2）便捷性，支付的便捷性，打造与手机端的指纹支付类似的用户体验。

3）低功耗，采用蓝牙 smart 和低功耗安全 IC，MCU。

4）集成度高，客户业务对接 SDK 和遥控器即可实现一键登录和一键认证支付功能。

5. FIDO 产品定制

我们提供 FIDO 产品定制服务。基于 TrustZone TEE 和 SE 两种平台上 ,我们实现了 FIDO 认证器终端套件。另外 ,我们免费提供与我们 SDK 套件配合的 Android4.3+ FIDO Client。

我们基于 SE 的电视购物遥控器已经通过了 FIDO UAF1.0 的功能性和 L1 安全性认证。使用我们终端 SDK 套件的客户，可委托我们代理向 FIDO 联盟认证客户的 FIDO 产品，获得 FIDO 认证证书。

我们的认证产品请访问：https://fidoalliance.org/product/neldtv-tv-remote/