



# 基于可信平台模块的快速身份认证技术探索

国民技术股份有限公司

可信计算产品业务部执行总监 刘鑫

## 目录

- 1、可信计算和FIDO发展情况、技术介绍
- 2、基于可信计算的认证器FIDO身份认证
- 3、国民技术可信计算产品



## TCG成立的初衷：

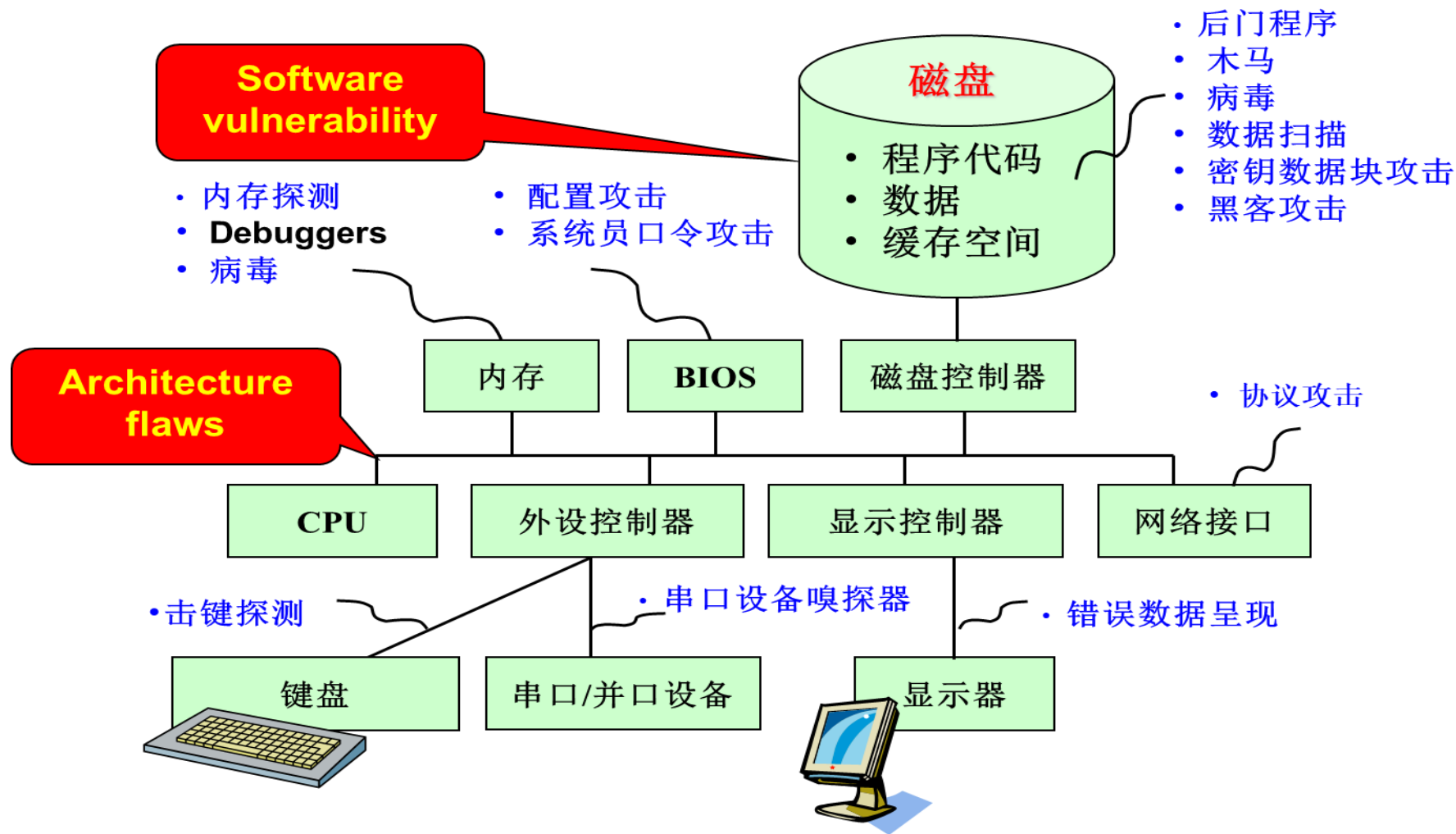
- 制定与推进公开、中立性、适合 产业化、跨平台的可信计算构建模块和软件接口的标准规范。
- 在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性。



200 多位成员

目前已推出1.2、2.0等版本技术规范，并已经成为ISO标准。

传统打补丁式的安全防御机制难以满足安全需求。



FIDO(快速在线身份认证) 是一套身份鉴别框架协议, FIDO联盟于2013年2月正式成立。

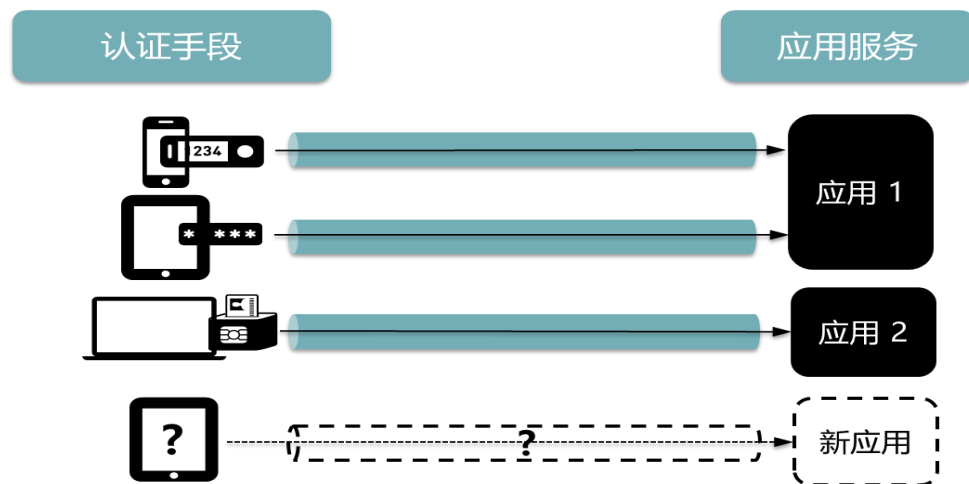
- Fast IDentity Online 是一套身份鉴别框架协议
- FIDO联盟于2013年2月正式成立, 创始人为6家公司



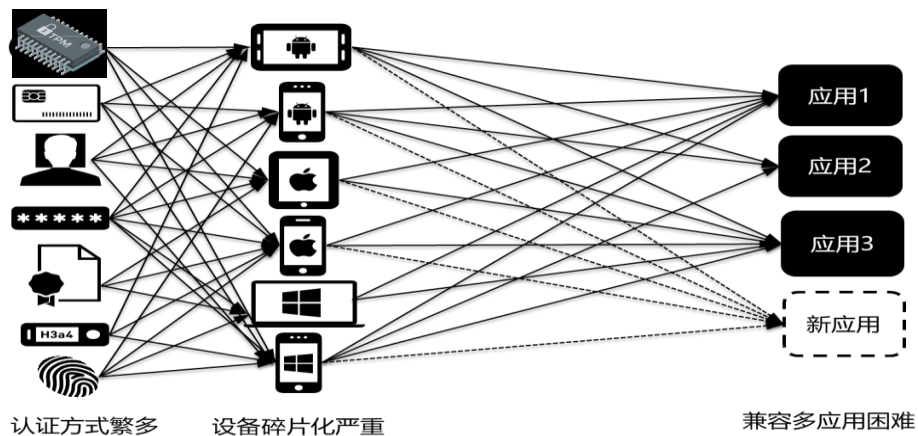
- 至2017年5月联盟成员已达252家, 囊括业界领先厂商



- 目前已推出1.0、1.1、2.0版本技术规范, 包括UAF和U2F、FIDO2。

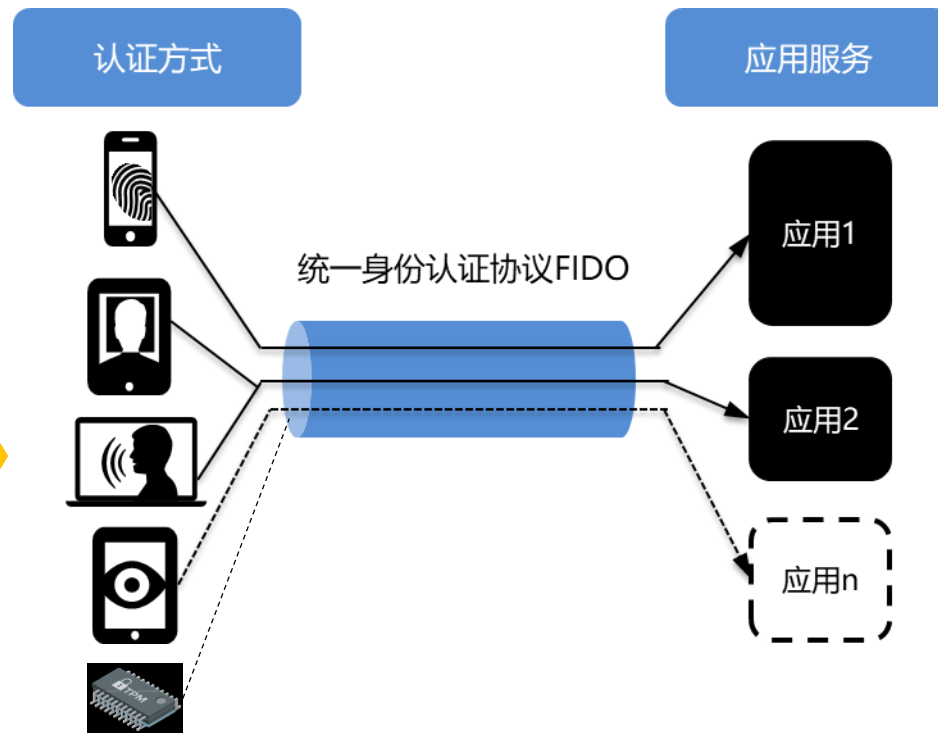


传统身份认证框架导致“孤岛”问题，不同认证方式之间各自为政，无法互操作，从而带来部署复杂、冗余以及高成本的问题



适配标准不统一

兼容多应用困难

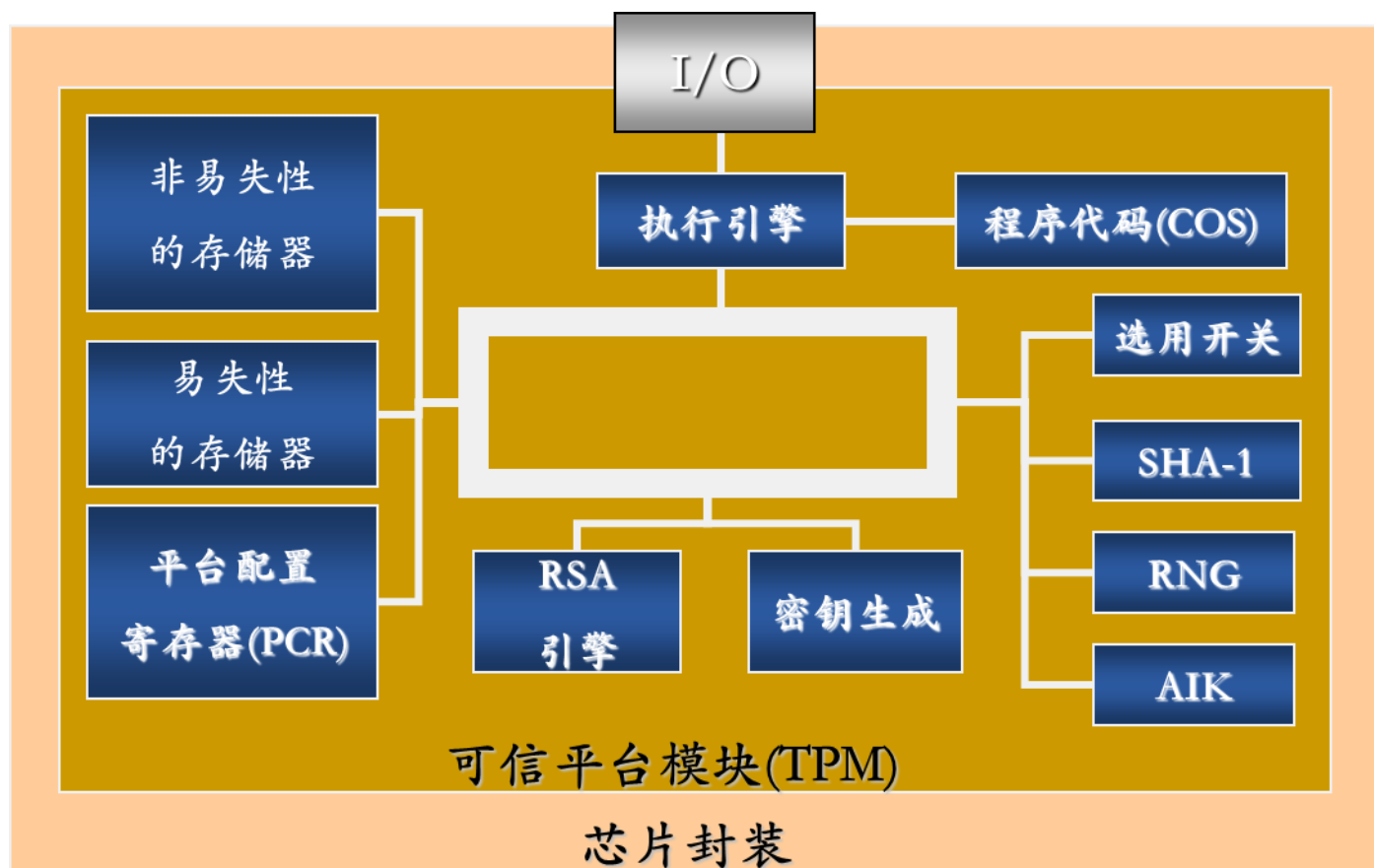


## 思路和目标

- 将认证手段与身份认证协议分离
- 支持尽可能多的认证手段，充分利用现有硬件设备内嵌的安全能力
- 保护用户隐私，使得用户信息不被泄露且无法被非法追踪



安全芯片作为可信计算的根，提供各种密码算法支撑和密钥管理。可以作为设备的“身份证”。



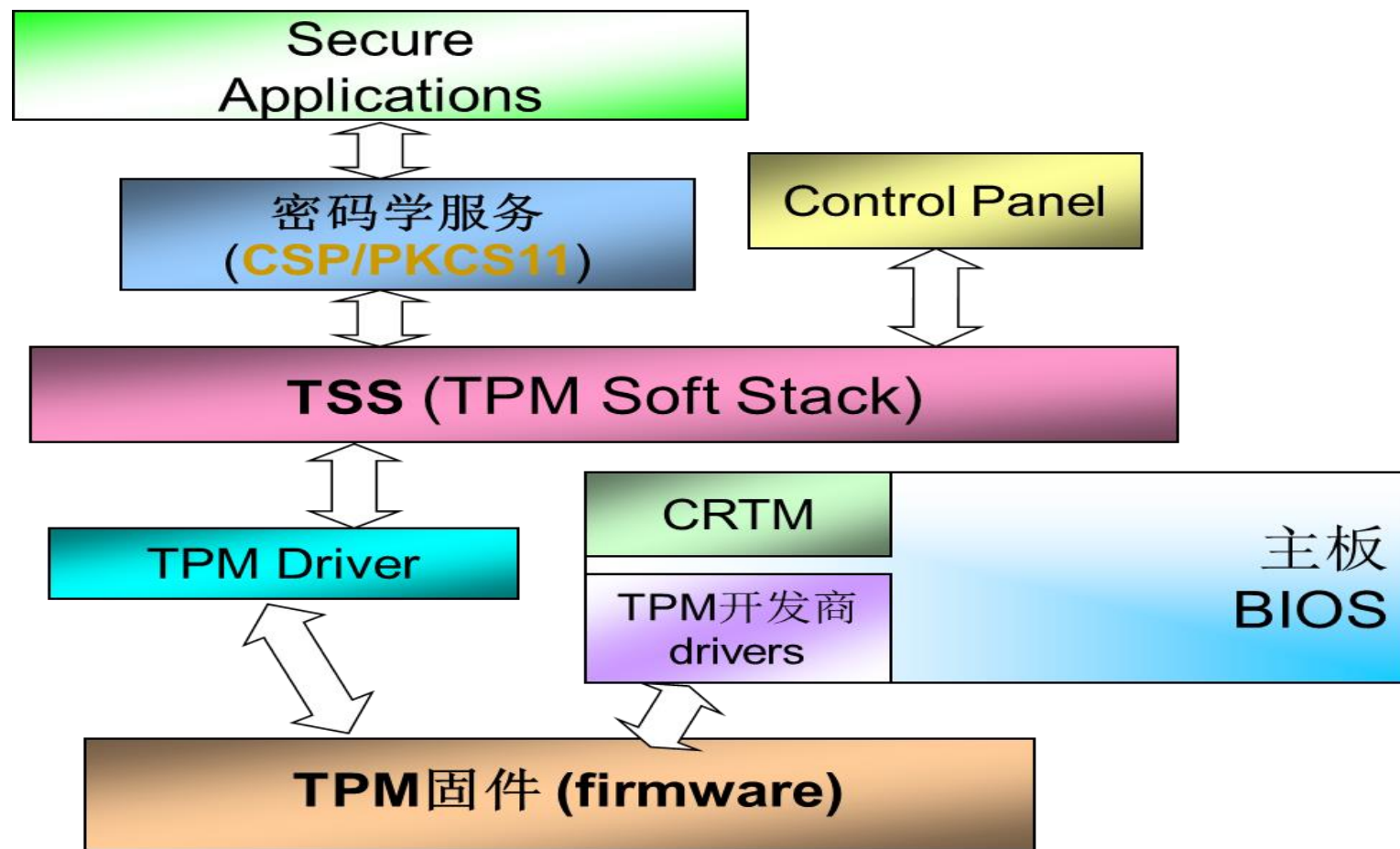
目标：

建立平台安全信任根基

核心功能：

- 1) 度量平台完整性，建立平台免疫力；
- 2) 平台身份唯一性标识；
- 3) 提供硬件级密码学计算与密钥保护。

安全芯片通过相关标准和协议，具备完善的密码服务接口。

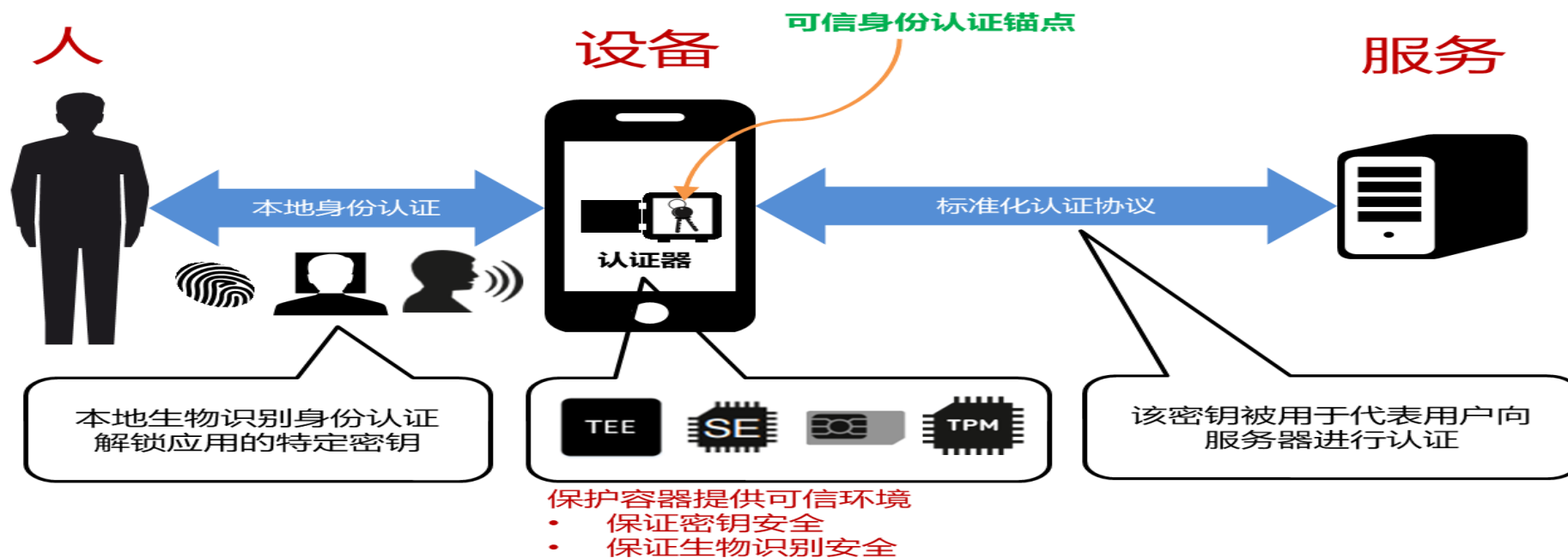




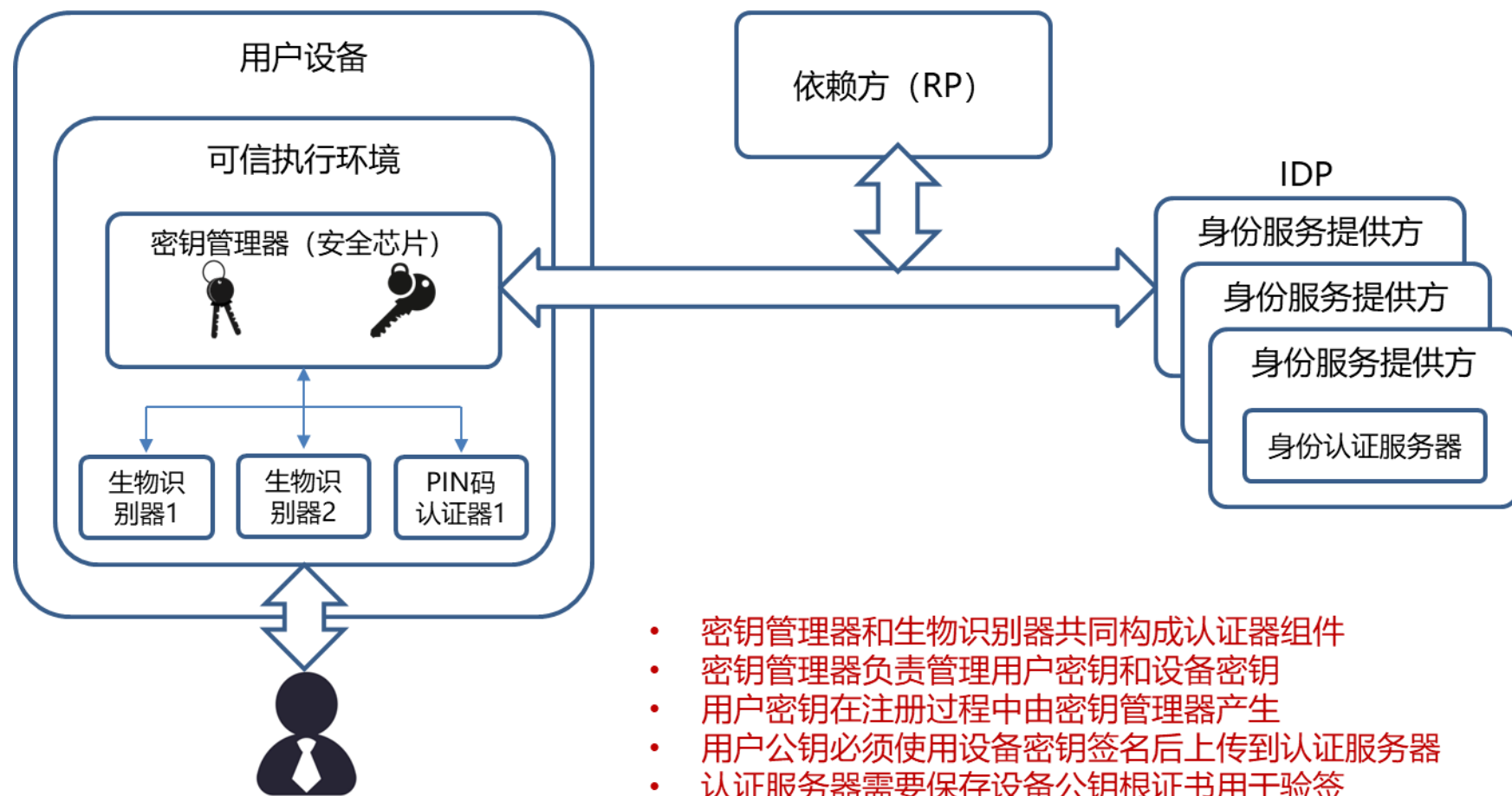
## FIDO与传统认证方式不同，进行两步式认证

- 第一步由设备验证人；
- 第二步由服务验证设备。

以设备的安全载体为基础，利用各种芯片芯片内提供的认证器，进行认证的密钥生产、运算和存储。



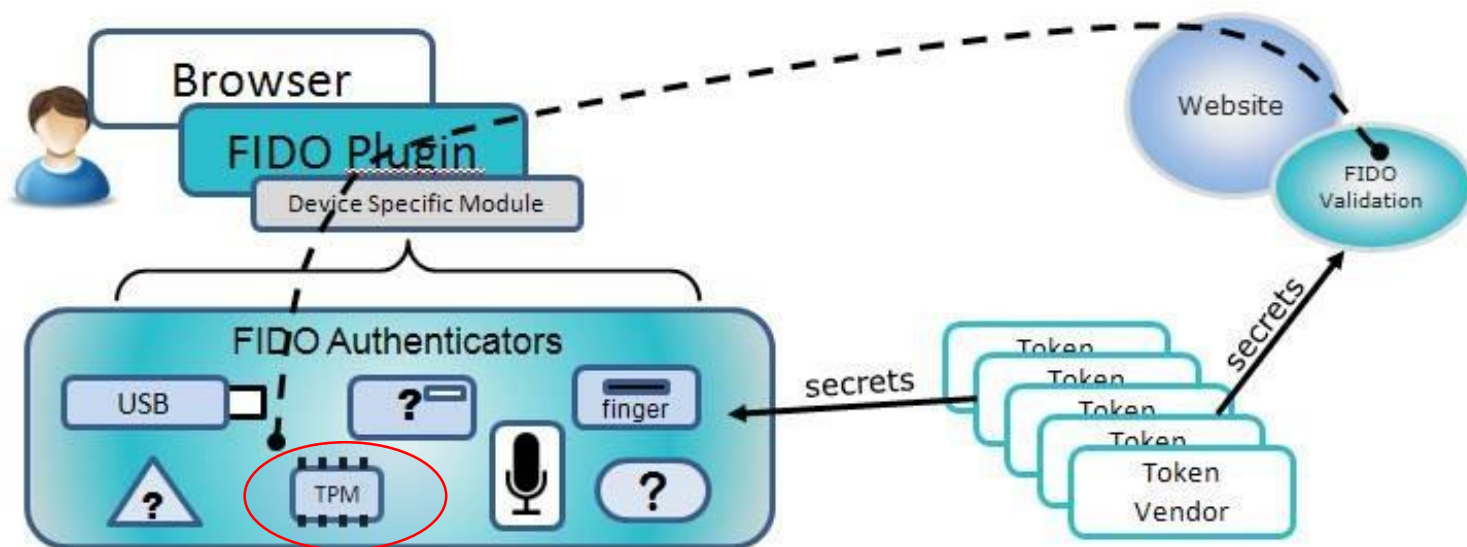
FIDO在设备安全认证器（Authenticator）内管理和保护私钥，在服务端依赖方（RP）或身份服务提供方（IDP）进行公钥验证。



- 密钥管理器和生物识别器共同构成认证器组件
- 密钥管理器负责管理用户密钥和设备密钥
- 用户密钥在注册过程中由密钥管理器产生
- 用户公钥必须使用设备密钥签名后上传到认证服务器
- 认证服务器需要保存设备公钥根证书用于验签
- 密钥管理器与认证服务器之间接口需要标准化

综上所述，可信计算平台模块与FIDO身份认证是紧密结合的两个技术架构和标准体系。

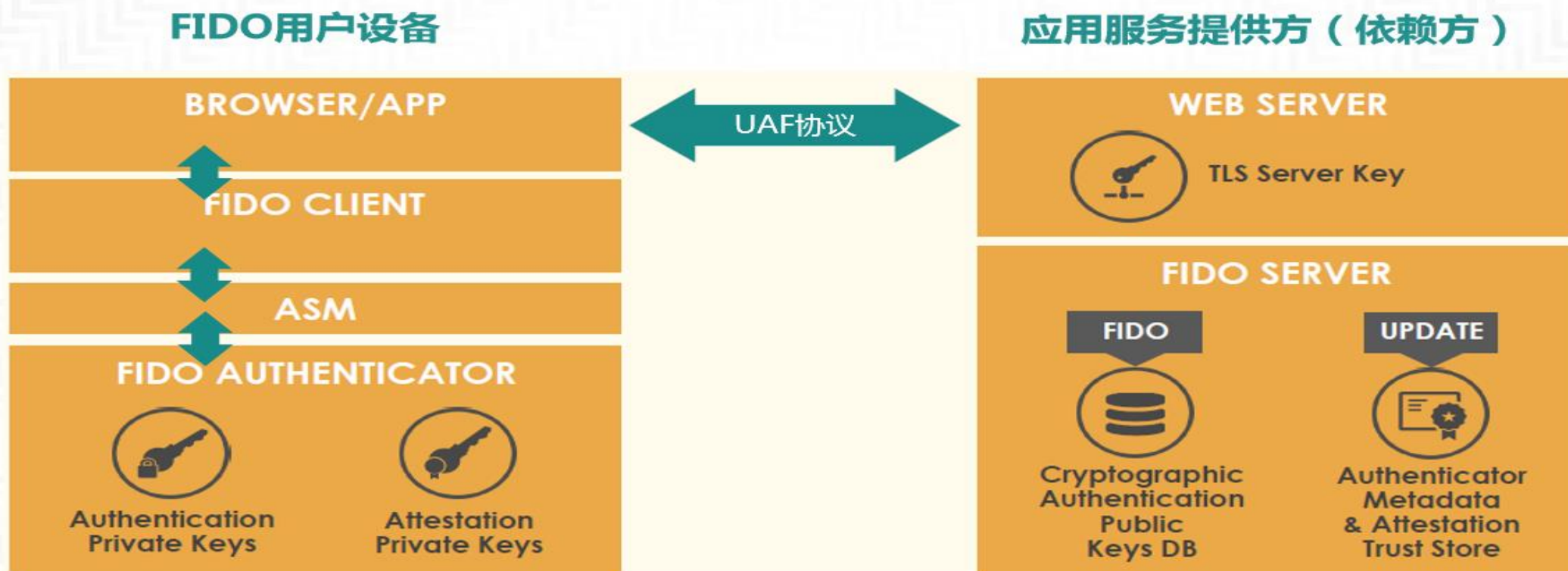
因此，FIDO标准在规范中，明确定义了TPM是标准的认证器之一。并对于接口调用进行详细定义。

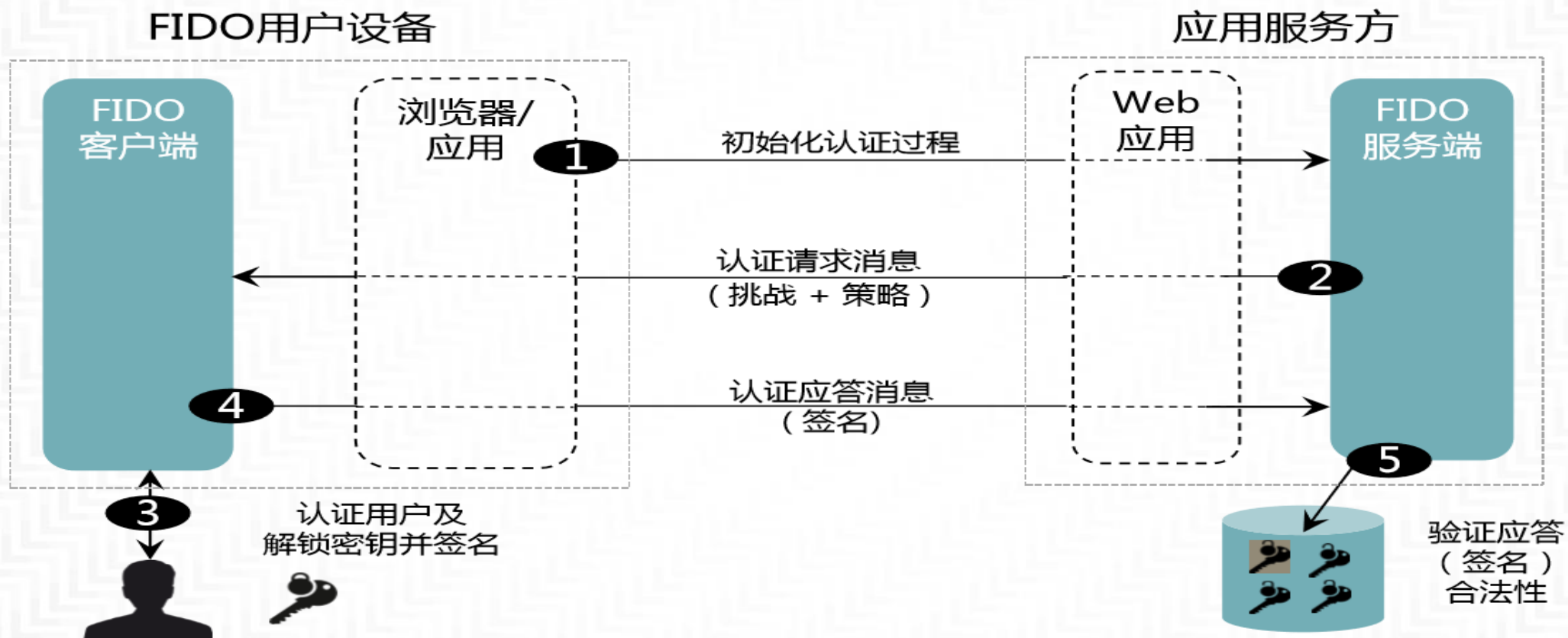




## 目录

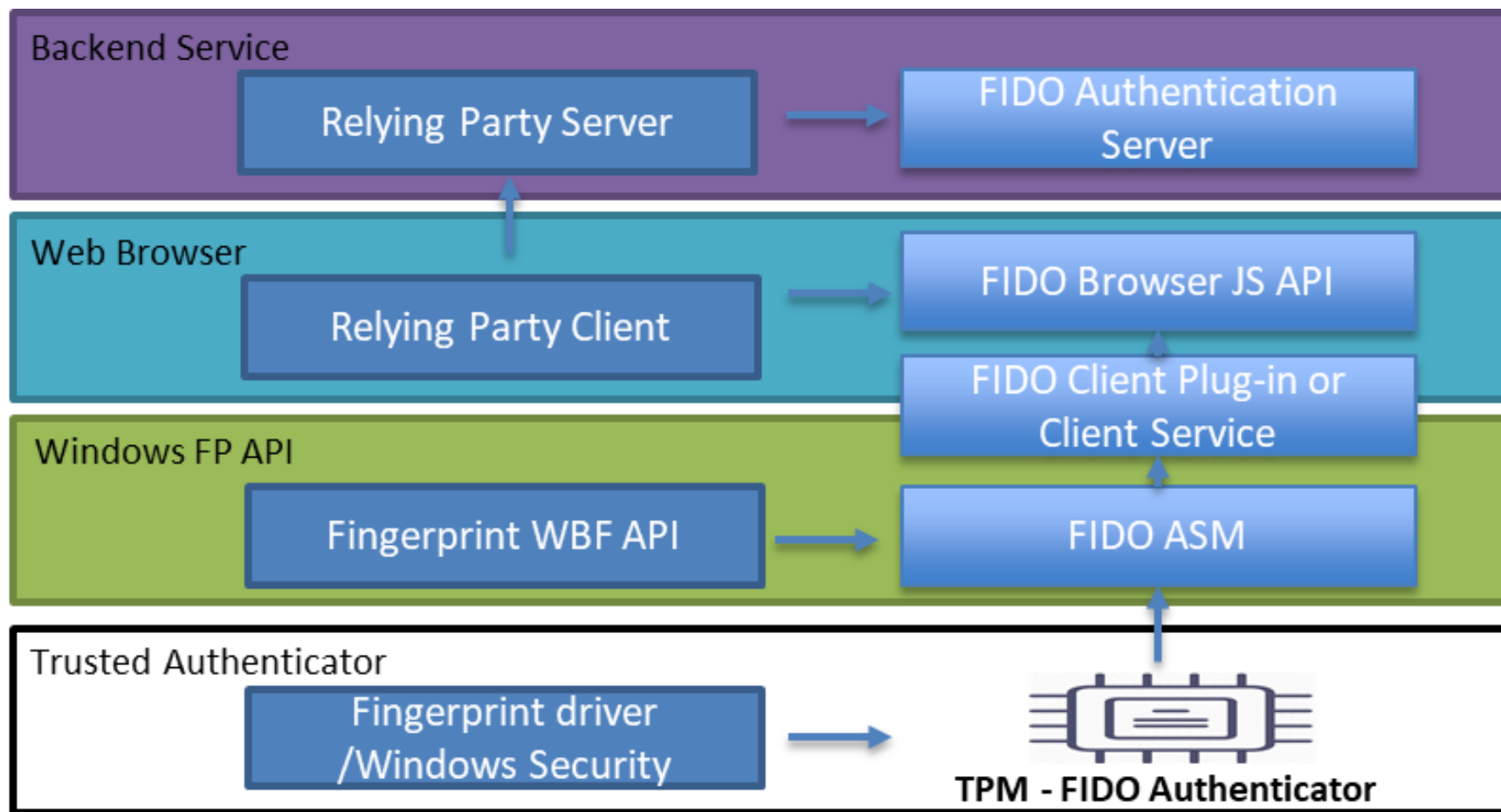
- 1、可信计算和FIDO发展情况、技术介绍
- 2、基于可信计算的认证器FIDO身份认证
- 3、国民技术可信计算产品





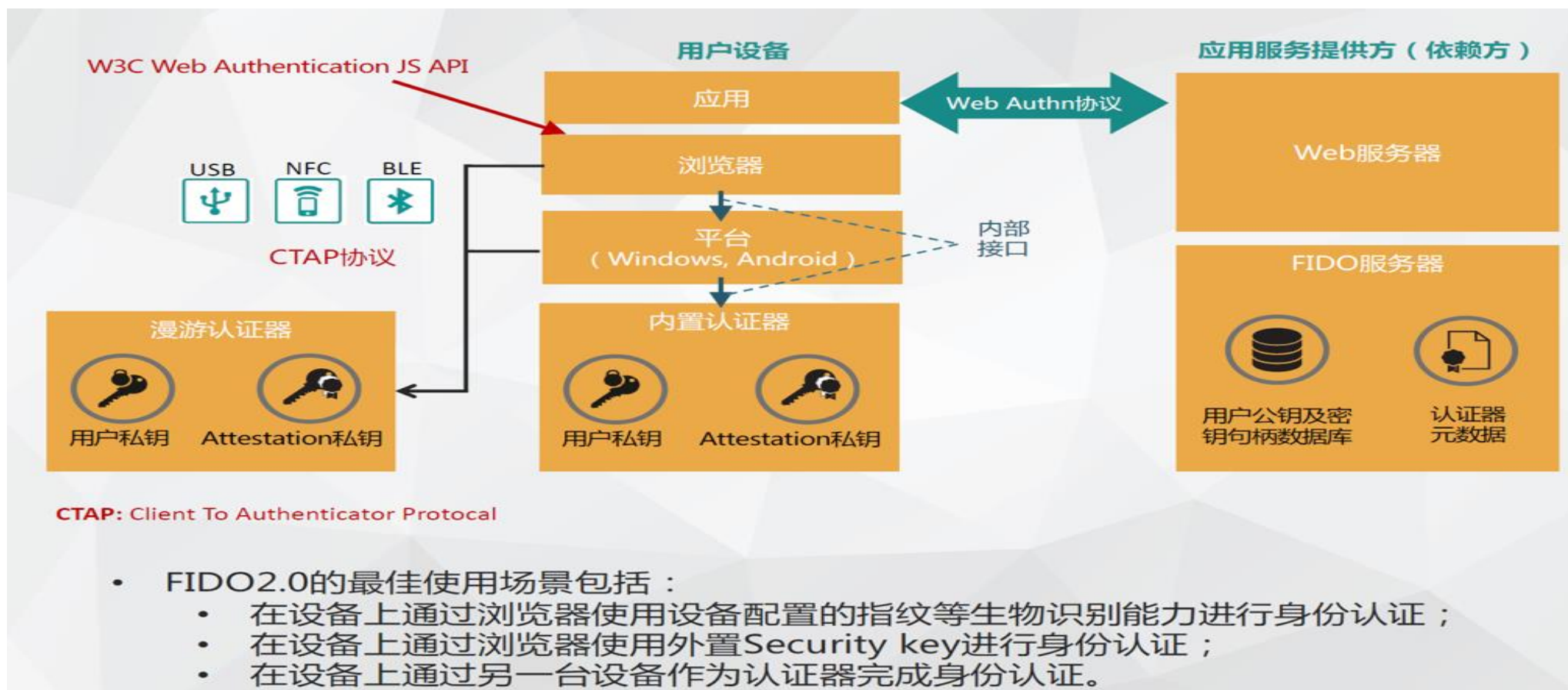


## 采用FIDO UAF的TPM身份认证器技术架构：



- TPM进行密钥管理
  - FIDO的签名密钥都是在TPM创建。
  - FIDO的签名密钥存储在TPM内。
  - FIDO的签名操作在TPM内进行。
- 可以对接指纹、人脸等各种生物认证的验证器：
  - 验证器与认证器在SGX、TEE等安全运行环境中。
  - 验证器与认证器之间密钥加密传输。
- FIDO ASM和Client将TPM认证器进行协议标准化
  - ASM和Client进行协议封装。
  - 浏览器按照W3C标准已经全部支持。

采用FIDO2最新的身份认证框架的TPM身份认证器技术架构：



## FIDO2标准将TPM作为FIDO2认证器可以直接连接浏览器

- 基于CTAP (Client to Authenticator Protocol, 客户端到鉴别器协议) 规范将FIDO规范中的鉴别器 (authenticator) 与WebAuthn API对接, 从而实现了FIDO与WebAuthn的互通。
- 目前, FIDO2已经受到了Windows 10以及Android 7.0以上操作系统的支持。
- 用户通过浏览器访问应用服务器上内嵌WebAuthn API的资源 (页面), 当页面在浏览器加载时, WebAuthn API被调用, 从而启动FIDO协议。
- 鉴别器是FIDO体系中负责生成数字签名的模块。FIDO2项目中的鉴别器可分为以下类型:
  - 内置鉴别器 (On-device authenticator): 内置于客户端主机的模块 (例如Windows 10内置的鉴别器);
  - 外部鉴别器 (External authenticator): 相对独立的模块 (类似智能密码钥匙), 可在不同的客户端主机使用。

### 3.4.2 TPM Attestation

#### 3.4.2.1 Attestation rawData (type="tpm")

The value of `rawData` is the **base64url encoding of a binary object**. This binary object is either a `TPM_CERTIFY_INFO` or a `TPM_CERTIFY_INFO2` structure [TPMv1-2-Part2] sections 11.1 and 11.2, if `attestationStatement.core.version` equals 1. Else, if `attestationStatement.core.version` equals 2, it **must** be the base64url encoding of a `TPMS_ATTEST` structure as defined in [TPMv2-Part2] sections 10.12.9.

The field "extraData" (in the case of `TPMS_ATTEST`) or the field "data" (in the case of `TPM_CERTIFY_INFO` or `TPM_CERTIFY_INFO2`) **must** contain the `clientDataHash` (see [FIDOSignatureFormat]).

#### 3.4.2.2 Signature

If `attestationStatement.core.version` equals 1, (i.e., for TPM 1.2), `RSASSA-PKCS1-v1_5` signature algorithm (section 8.2 of [RFC3447]) can be used by FIDO Authenticators (i.e. `attestationStatement.header.alg="RS256"`).

If `attestationStatement.core.version` equals 2, the following algorithms can be used by FIDO Authenticators:

1. `TPM_ALG_RSASSA` (0x14). This is the same algorithm `RSASSA-PKCS1-v1_5` as for version 1 but for use with TPMv2. `attestationStatement.header.alg="RS256"`.
2. `TPM_ALG_RSAPSS` (0x16); `attestationStatement.header.alg="PS256"`.
3. `TPM_ALG_ECDSA` (0x18); `attestationStatement.header.alg="ES256"`.
4. `TPM_ALG_ECDAA` (0x1A); `attestationStatement.header.alg="ED256"`.



FIDO2 无密码输入认证体验的 web 部分标准，同时也是 W3C 的官方标准。

完整的认证流程采用了一种 挑战-应答（challenge-response）的模式：

- 首先客户端要求用户输入用户名发起挑战请求
- 随后服务器根据用户名对客户端发起挑战
- 随后客户端进行回应，如果此时服务端验证回应是满足的，那么认证成功

WebAuthn 主要分为四个层面：

- 用户层面：包含输入用户名，以及生物认证等操作
- API层面：创建公钥，产生断言验证
- 协议层面：规定挑战-应答流程，对抗钓鱼，对抗重放攻击等实现
- 硬件层面：在硬件上实现公钥的产生和断言验证的产生的协议：CTAP2



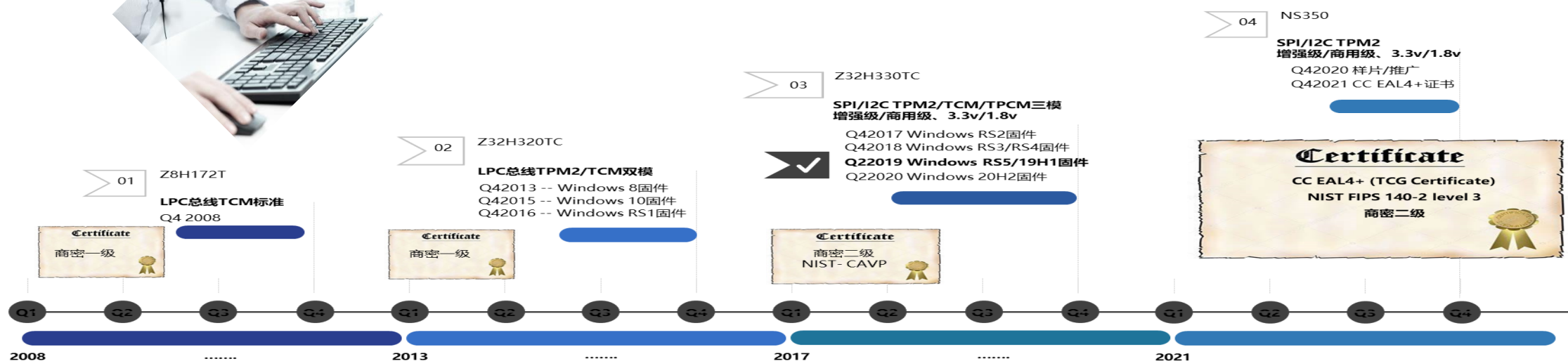
## 目录

- 1、可信计算和FIDO发展情况、技术介绍
- 2、基于可信计算的认证器FIDO身份认证
- 3、国民技术可信计算产品


- 在2006年以前，采用TCG TPM1x规范研制TPM可信计算芯片
  - 联想、兆日等公司采用TPM1.2，并获得国家商用密码管理局型号鉴定证书
- 2006 - 2010, 发展中国自主可信计算标准
  - 2007.12, 国家商用密码管理局颁布了可信计算功能与接口规范 (TCM standard)
  - 2007.12, 国民技术发布了第一款TCM芯片，在联想、同方、方正PC预装
- 2010 至今, 中国国密算法应用
  - 2012.03, 国民技术加入TCG，并在Intel和微软的支持下推动在TPM2.0标准中加入中国商密 SM2/3/4
  - 2015.06 ISO/IEC JTC1 released ISO/IEC 11889:2015 TPM 2.0 标准发布，并支持中国商密算法
    - ballot came from both developed and emerging economies, with approving votes from Australia, Belgium, Canada, **China**, Czech Republic, Denmark, Finland, France, Ghana, Ireland, Italy, Japan, the Republic of Korea, Lebanon, Malaysia, Netherlands, Nigeria, Norway, the Russian Federation, South Africa, the United Arab Emirates, the United Kingdom and the United States.
- 国民技术股份有限公司作为中国可信计算产业的主要创建者和核心推动者，国际可信计算标准参与制定方。
- 国际可信计算产业中，来自中国的领先核心产品
- 支持我国商用密码算法体系的TPM2.0标准正式成为ISO/IEC标准，实现真正意义的商密出口。



支持ISO/IEC国际可信计算TPM 2.0、中国可信密码模块TCM、可信平台控制模块TPCM标准，广泛应用于笔记本、平板电脑、个人电脑、服务器等计算机、嵌入式计算系统和IoT设备等，是微软、英特尔、三星等国际厂商在华可信计算模块供应商。





The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that create a sense of depth and movement, resembling a grid or a series of overlapping planes.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE