TrustZone与TEE的发展历史、技术原理以及产业格局

来源：NFC产业网　作者：佘云峰 2016/11/3 18:18:56

安全是老生常谈的话题，安全技术也在时代的发展下发生了进步和变化，除去硬件级别的安全之外当下最火的要数TEE技术了，那么TEE技术是由何而来呢?TEE又是如何保证移动终端的安全的?目前国内有哪些企业在专注TEE技术方案的开发?本文将从以上几方面简单介绍TEE。

发展历史

关键词1 OMTP(Open Mobile Terminal Platform，开放移动终端平台)

2006年，OMTP工作组智能终端的安全率先提出了一种双系统解决方案：即在同一个智能终端下，除了多媒体操作系统外再提供一个隔离的安全操作系统，这一运行在隔离的硬件之上的隔离安全操作系统用来专门处理敏感信息以保证信息的安全。该方案即TEE的前身。

关键词2 ARM——TrustZone

基于OMTP的方案，ARM公司(嵌入式处理器的全球最大方案供应商，它们架构的处理器约占手机市场95%以上的份额)于2006年提出了一种硬件虚拟化技术TrustZone及其相关硬件实现方案。TrustZone即是支持TEE技术的产品，TrustZone 是所有Cortex-A 类处理器的基本功能，是通过 ARM 架构安全扩展引入的，而ARM也成为了TEE技术的主导者之一。

(Intel公司也提出了类似的基于独立双硬件的技术解决方案，但是在移动芯片领域ARM一直处于领导地位，两者的芯片采用了不同的底层架构，众多开发者总是会优先针对ARM的芯片应用作出优化。)

关键词 3 GlobalPlatform

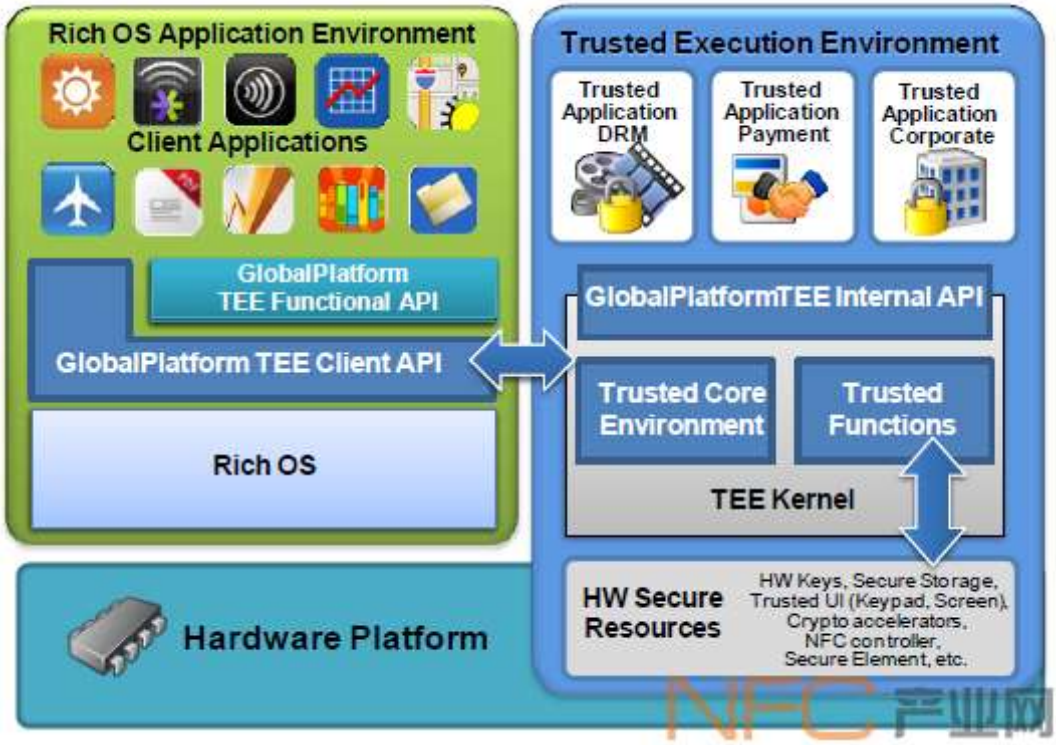
ARM 后将其 TrustZone API 提供给 GlobalPlatform，该 API 已发展为 TEE 客户端 API。

GlobalPlatform(全球最主要的智能卡多应用管理规范的组织，简称为GP)是Visa、MasterCard等国际银行卡组织主导的国际标准化组织，从2011年起开始起草制定相关的TEE规范标准，并联合一些公司(ARM等)共同开发基于GP TEE标准的可信操作系统。因此，如今大多数基于TEE技术的Trust OS都遵循了GP的标准规范。

技术原理

关键词 4 TEE

TEE(Trust Execution Environment)，也叫可信执行环境，是和REE(Rich Execution Environment)相对应的，一般称TEE和REE为Secure World和Normal World。Linux跑在Normal World上，但是有些安全性要求比较高的行为，例如指纹的比对，支付时候用私钥签名的动作等，需要放到Secure World里面去。



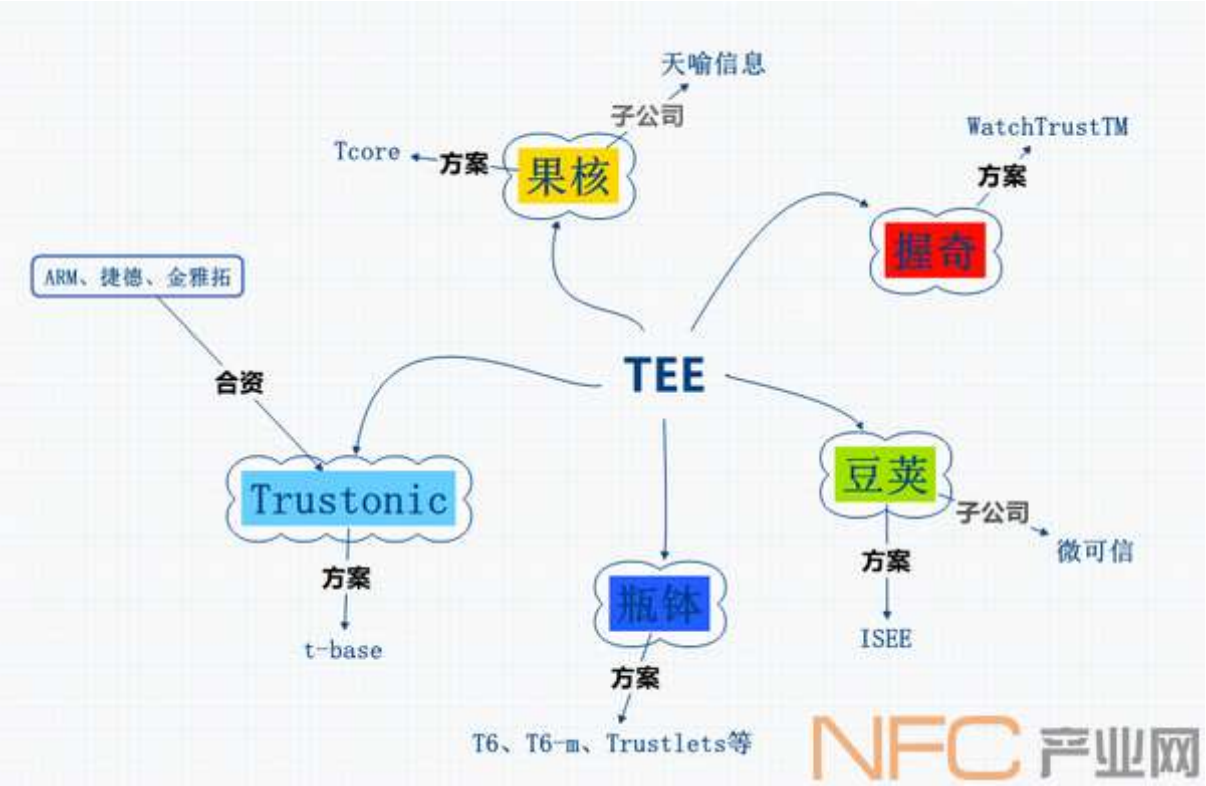
TEE具有其自身的执行空间，也就是说在TEE的环境下也要有一个操作系统。TEE环境比Rich OS(普通操作系统)的安全级别更高，但是比起安全元件(SE，通常是智能卡)的安全性要低一些;另一方面，加入TEE的成本增加比较低，SE的成本则更高。

TEE所能访问的软硬件资源是与Rich OS分离的。TEE提供了授权安全软件(TrustApp可信应用，简称TA)的安全执行环境，同时也保护TA的资源和数据的保密性、完整性和访问权限。为了保证TEE本身的可信根，TEE在安全启动过程中是要通过验证并且与Rich OS隔离的。在TEE中，每个TA是相互独立的，而且不能在未授权的情况下互相访问。

简而言之就是在TEE环境的操作系统上同样有相应的应用程序(TA)， 除了TEE的运行环境与普通操作系统相互独立外，TEE里的每一个TA也是需要授权并相互独立运行的。

产业格局

基于TEE环境的操作系统由不同的企业在推行，例如华为海思有自己的Trustzone的操作系统，高通的QSEE、ARM的Trustonic、还有Linaro开源的OPTEE等。下图为几家主要的TEE解决方案提供商以及相关方案。



关键词 TEE+eSE+TSM、TEE+HCE

据NFC产业网了解，Google也试图将TEE检测内容纳入到CTS认证中，加上指纹识别的普及对安全的要求更加迫切，这成了TEE近来发展迅速的主要原因。

10月中旬，华为海思发布了一款最新的麒麟960芯片，采用了在主芯片上集成安全芯片的inSE方案，并且已经通过了中金国盛和银联的双认证。这一开创性的方案，打破了之前NFC产业链SE的主导权问题，手机厂商将成为移动支付方案的主要控制方，这对于移动支付的宣传和推广相对来说是更加利好的。而值得注意的是，该方案中同样采用了TEE技术，来应对不同应用场景的安全等级。

另外，前不久移动芯片行业巨头高通收购恩智浦尘埃落定，而恩智浦在金融IC卡和城市公交卡领域有着超高的市场份额，据了解目前NXP在国内手机eSE芯片市场占有率超过80%。这样一来，高通和恩智浦的联姻让主控芯片

内置SE的方案有了更加地切实的可能性。而各个手机厂商去推行移动支付应用，尤其是在交通领域，必须自建一套TSM平台用于空中开卡和管理卡片应用，因此未来在主控芯片可能集成SE的基础上，TEE+eSE+TSM 的方案体系将成为趋势。

除此之外，银联系的HCE方案是独立于手机厂商之外的另一个选择，其主导权在各大商业银行手中，尽管目前有Token等相关安全技术的保障，但是HCE模式的安全性众所周知是所有NFC方案中最低的。据了解，早在两年前银联便推广了TEEI的智能终端安全解决方案，而近年来也一直都在研究TEE的相关技术，致力于将TEE规范标准化。未来随着相关技术标准的成熟，结合HCE方案的灵活性特点，TEE+HCE也会成为未来的另一方向。