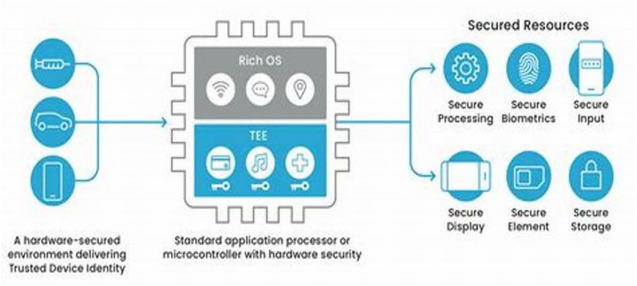
可信执行环境

Trusted Execution Environment

可信执行环境是计算平台上由软硬件方法构建的一个安全区域，可保证在安全区域内部加载的代码和数据在机密性和完整性方面得到保护。其目标是确保一个任务按照预期执行，保证初始状态和运行时状态的机密性、完整性。相较于其他基于密码学的隐私计算技术，TEE 的优势在于性能强大，能够解决复杂场景的业务诉求，同时开发成本低，能够迅速做出满足业务诉求的产品。

不同于联邦学习和多方安全计算的分布式计算范式，可信执行环境是一种集中式的隐私计算技术解决方案，通过硬件隔离的方式实现数据安全和隐私保护，对于通用计算比较友好，复杂算法的实现上也较为灵活。为保证数据流转安全性，可信执行环境常结合密码学算法来实现加密和验证方案，确保在可信执行环境外的数据均为密态。



TEE 一般是直接基于硬件实现的，比如 Intel SGX，AMD SEV，ARM TrustZone 等；基于虚拟化技术也可以构造 TEE，比如微软的 VSM，Intel 的 Trusty for iKGT & ACRN 等。

SGX(软件防护拓展)是 Intel 在 2013 年推出的指令集扩展，旨在以硬件安全为强制性保障，不依赖于固件和软件的安全状态，提供用户空间的可信执行环境。SGX 通过一组新的指令集扩展与访问控制机制，实现不同程序间的隔离运行，保障用户关键代码和数据的机密性与完整性不受恶意软件的破坏。

ARM TrustZone 于 2003 年在伦敦的伦敦塔推出。ARM TrustZone 在处理器层次引入两个不同权限的保护域-安全世界和普通世界，任何时刻处理器仅在其中的一个环境内运行，通过中断路由以及对内存总线和内存管理单元的限制来提供隔离保护。

AMD 在 2017 年提出了 SVE(Secure Encrypted Virtualization)的可信执行环境技术。SEV 为云而设计，为密集计算提供更好的性能，并对运行在支持 SEV 的虚拟机上的软件透明。SEV 使用秘钥加密 VM 达到隔离 VM 的目的，秘钥只能由硬件访问，因此 hypervisor 或者 VM 外其他软件无法干扰加密。SEV 使用了 Secure Memory Encryption(SEM)来加密 VM 内存保护防止物理攻击和特权软件攻击。