FIDO安全评估

FIDO联盟的目标是通过提供基于公共加密密钥的安全、标准化和可互操作的验证生态系统，减少对手机和在线应用程序密码的依赖。FIDO研发了一个认证方案来支持研发和采用新的验证解决方案，使用户能够轻松地识别提供最高质量和信任等级的解决方案。

FIDO认证允许评估身份验证解决方案的安全性和互操作性。不同层次的认证相辅相成，积累了需求。目前，产品可以在前两层进行评估，目前正在研发更多的层，其中将包括更严格的安全要求。
Applus+ Laboratories是FIDO联盟认可的为数不多的对验证系统进行安全评估的实验室之一。

手机支付应用程序

手机服务不断在快速便捷的访问和强健的验证安全之间进行权衡。FIDO旨在扭转这一局面，在提供更强安全性和降低风险的同时，让在线安全成为更简单、更好的用户体验。
银行和支付服务提供商继续将其服务提供的方式逐渐转变为在线和手机服务，但他们不断在快速和便捷的访问和强健的验证安全之间进行权衡。FIDO旨在扭转这一局面，在提供更强安全性和降低风险的同时，让在线安全成为更简单、更好的用户体验。
L2及更高等级的FIDO认证要求您评估FIDO验证器对基本和可扩展攻击的防范。该评估必须由FIDO认可的安全实验室进行。

TEE

除了L3之外，验证器还需要使用某种安全元件来保护资产。
TEE具有针对手机操作系统中生成的软件攻击的防护等级，并帮助控制访问权限。它通过存放敏感的、“可信”应用程序来实现这种防护，这些应用程序需要进行隔离和保护，免

受手机操作系统和可能存在的任何恶意软件的攻击。TEE也非常适合支持生物识别方法（面部识别、指纹传感器和语音授权），这些方法可能比PIN和密码更容易使用，也更难以窃取。
这些特性使得TEE非常适合为FIDO验证器另外增加安全性。L2及更高等级的FIDO认证要求您评估FIDO验证器对基本和可扩展攻击的防范。该评估必须由FIDO认可的安全实验室进行。

生物识别技术

FIDO通常依赖生物特征验证机制来验证用户的身份。在FIDO中，生物识别技术也倾向于作为一种验证机制来访问或使用来自安全元件（如TEE）的数据。
这些生物特征验证机制构成验证器的一部分，因此也包括在评估中。L2及更高等级的FIDO认证要求您评估FIDO验证器对基本和可扩展攻击的防范。该评估必须由FIDO认可的安全实验室进行。

注意：由于Applus+ Laboratories是经过多个评估和认证方案认证的第三方实验室，为了保证其公正性，Applus+工程师从未参与实际的产品研发或解决方案实施。