

通用标准安全评估

确保IT产品的安全水平符合通用标准（ISO15408：2005）



什么是通用标准?

通用标准是评估IT产品安全功能和保证(ISO 15408)的国际公认标准。该标准是基于7个评估保证等级(EAL)的日益严格。供应商选择EAL进行索赔，并将产品提交到由认可的独立实验室进行安全评估。

通用标准认证（从EAL 2到EAL 4）被签署了《通用标准认可协议》(CCRA)的27个国家认可。此外，10个欧洲国家签署了《SOGIS相互承认协定》，就智能卡等特定技术领域的高等级通用标准认证达成一致。

为什么要根据通用标准进行认证?

通用标准证书具有全球性和跨行业的认可度。经通用标准认证的产品在安全性方面具有关键的差异化元素，因为它是由第三方根据强效和定义明确的评估方法进行评估的。

在许多情况下，通用标准是最终用户需求。根据美国（NSTISSP No. 11 - NIAP PCL清单）或欧洲（西班牙ENS、欧洲eIDAS或Tachograph法规）的政府法规要求，公共机构购买的产品必须包括第三方担保证书（这是最常见的通用标准）。

在某些行业中，通用标准可能是市场准入要求（IC或ePassport）或投标中特定的安全保证要求（银行、移动网络运营商）。

Applus+，通用标准评估认可实验室

Applus+是一家经认可的IT安全评估机构(ITSEF)，可进行通用标准和SOG-IS评估。我们对过程进行管理，以取得IT产品的通用标准认证(ISO15408：2005)。

我们的服务包括通用标准评估（认证等级高达EAL 7）。根据评估水平，通用标准要求包括：

- **产品评估:** 关注风险漏洞缓解
- **研发人员设计评估:** 重点关注确保研发过程的可靠性
- **研发现场审计:** 重点确保供应链的完整性和保密性。

通用标准的应用

智能卡和安全元件

智能卡广泛应用于许多行业：电子护照、身份证、交通票务、电子健康。通用标准方法可用于认证智能卡的三层架构：集成电路(IC)、卡操作系统（平台）及其应用程序。

虽然支付等行业有自己的认证方案(EMVCo)，但非最终产品供应商（IC、平台和复合材料）可能需要根据这两种方案进行认证，因为他们的产品可能具有多行业应用特点。在这种情况下，Applus+可以提供组合的安全性评估，以加快上市时间。

电信设备

路由器、交换机、网关和类似产品都是安全关键型产品，最终客户端通常需要安全保证证书（如通用标准）。在某些情况下，例如，政府机构投标，拥有一份通用标准证书可能是准入要求。

手机

随着新的高附加值应用程序向手机（支付、DRM、身份识别、生物识别等）转移，安全问题也随之出现。通用标准是对手机设备或手机应用程序进行评估的完美解决方案。

eIDAS和可信服务

eIDAS法规为数字签名、HSM或时间戳产品提供了欧洲监管环境。欧洲委员会通过规定一组保护框架指定通用标准作为评估这类产品强度的方法。

其他IT产品

对于许多IT产品（如商业软件、软件即服务、云计算平台或硬件安全模块）来说，通用标准是实现安全保证和营销差异的合适选择。

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。