# 如何选择 PKI 密码卡

**1、什么是 PKI？密码卡在 PKI 体系中的作用？**

PKI（Public Key Infrastructure ） 即"公钥基础设施"，是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。 PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。密码卡是高性能基础密码设备，能够适用于各类密码安全应用系统进行高速的、多任务并行处理的密码运算，可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制。因此，密码卡是 PKI 体系中密码算法的提供者，是 PKI 体系中的核心之一。

**2、密码卡怎么用？**

在 PKI 体系中，应用系统或其他安全产品（PKI 密码机等产品）通过调用密码卡提供的标准 API 函数来使用密码服务，API 接口符合国家密码管理局制定的《公钥密码基础设施应用技术体系 密码设备应用接口规范》标准接口规范。

**3、如何选择密码卡？**

首先需要了解应用系统或安全产品的特性，算法需求及性能需求，非对称算法如：RSA、SM2 等密码算法，对称算法如 SM1、SM4 等密码算法，杂凑算法如 SM3 密码算法，选择密码卡时首先看算法需求是否能够全部满足，然后再看性能指标。厂家技术白皮书或销售人员提供的性能指标偏差不会很大，但以在需求平台上的实际测试数据为准。

**4、业界的大体水平**

国内密码卡的性能主要受制于 PCI 传输的性能。目前 SM1 密码算法性能普遍在 400Mbps 左右；1024 位 RSA 密码算法，最大签名性能在 5500 次/秒左右；SM2 密码算法签名性能 6500 次/秒左右。我公司深入研究密码算法且应用高性能密码算法芯片，某些密码算法的性能可达普通水平的数倍。如对密码算法有更高性能的需求，欢迎联系我们。

**5、我们公司的产品及技术力量**

三未信安密码卡已经应用在 PKI 密码机、金融密码机、签名服务器等设备中，稳定性、可靠性得到验证。 满足不同客户需求，我公司推出了性能区分高中低不同档次且密码算法灵活搭配的密码卡产品方便用户选择。

此外,负责密码卡硬件、软件的研发人员均在本行业从业十年以上，有丰富的研发及调试经验，骨干员工及技术支持人员在本行业从业三年以上，售后及技术支持能够得到保障。