Windows的公钥基础结构(PKI)增强功能 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/259/2021_2022_Windows_E7_9A_84_c100_259031.htm Windows 从 Windows 2000 版本起即开始为公钥基础结构 (PKI) 提供强健的、平台范围的支持。该版本包含第一个本机证书颁发机构功能，引入了自动注册，并为智能卡身份验证提供支持。在 Windows XP 和 Windows Server 2003 中，这些功能已得到扩展，可通过版本 2 证书模板提供更灵活的注册选项，并支持自动注册用户证书。在 Windows Vistareg. 2008(以前的代号为“ Longhorn ”)中，Windows&reg. PKI 平台又向前迈了一步，支持高级算法、实时有效性检查，可管理性也更好。本专栏将讨论 Windows Vista 和 Windows Server 2008 中新增的 PKI 功能，以及企业如何利用这些功能来降低成本和增加安全性。 Windows Vista 和 Windows Server 2008 中的 PKI 围绕四个主要核心方面进行了改进：加密、注册、可管理性和吊销。除了这些特定功能的改进外，Windows PKI 平台还受益于其他的操作系统改进(如角色管理器)，这些改进使得创建和部署新的证书颁发机构 (CA) 更加轻松。另外，Windows 的其他许多部分都能够利用 PKI 平台中的改进，如在 Windows Vista 中支持使用智能卡存储加密文件系统 (EFS) 密钥。 加密 对加密服务核心的改进体现在两方面。首先，通过引进下一代加密技术 (CNG)，Windows 现在提供一种可插入的、协议不可知的加密功能，此功能使得以编程方式开发和访问独立算法更加轻松。其次，CNG 还新增了对 Suite B 算法的支持，该算法在 2005 年由 National Security Agency (NSA) 引入。 CNG 是 Microsoft 的

一个新型核心加密界面，也是针对将来基于 Windows 和支持加密的应用程序建议使用的 API。CNG 提供了大量的以开发人员为目标对象的功能，其中包括更方便的算法发现和替换、可替换的随机数生成器和一个内核模式加密 API。提供这些新功能的同时，CNG 还与其处理器 CryptoAPI 1.0 中提供的算法集完全向后兼容。目前，CNG 正在接受通过联邦信息处理标准 (FIPS) 140-2 级别 2 认证以及成为所选平台的通用准则所需的评估。 CNG Suite B 支持包括所需的所有算法：AES(所有密钥大小)、SHA-2 系列(SHA-256、SHA-384 和 SHA-512)哈希算法、椭圆曲线 Diffie-Hellman (ECDH) 以及以美国国家标准与技术研究院 (NIST) 标准原始曲线 P-256、P-384 和 P-521 为标准的椭圆曲线数字签名算法 (ECDSA)。NSA 已表明，经过认证的 Suite B 实现将用于保护以下类别的信息：Top Secret、Secret 以及过去被描述为 Sensitive-But-Unclassified 的隐私信息。所有 Suite B 算法的开发都采取公开形式，其他一些政府也在探索尝试采用 Suite B 算法作为国家标准。 对 Windows PKI 平台的这些低级别改进为开发人员保护数据提供了更安全的方法，同时还创建了易于维护和随时间改进的子系统。由于 CNG 是可插入的体系结构，所以可根据需要添加新算法，CNG 会从应用程序层抽象出这些提供程序。最终结果是，Windows Vista 和 Windows Server 2008 的设计旨在为开发支持 PKI 的应用程序和服务提供高级的可发展平台。 注册 Windows 中的证书注册体验得到了显著改善，提供新的基于向导的注册工具、更佳的证书过期处理、新 API、“ 代表注册 ” 功能以及凭据漫游等功能。这些增强功能通过集中管理的方式更加轻松地在企业范围内部署证书，降低对用户的影

响，从而降低了 PKI 的总体拥有成本。 从注册的角度来看，最显著的变化就是如图 1 和 2 中所示的新证书注册用户界面。此用户界面取代了旧的、受限制的用户界面，旧界面不具备在注册过程中接受来自用户的数据的功能。新界面允许用户在注册过程中输入数据(如果管理员将证书模板配置为要求在注册过程中输入数据)。该界面还针对用户可能无法对特定模板注册的原因进行了清楚的说明。 图 1 选择可用证书 图 2 不可用证书的状态 