PKI 的发展

美国的 PKI 建设过程经历了 1996 年之前的无序、1996—2002 年间以 FBCA 为核心的体系搭建、2003 之后策略管理和体系建设并举的三个阶段。1996 年以前，很多政府部门自建 PKI 系统，例如美国邮政服务部门、社会安全部门、美国国防部、能源部、美国商标与知识产权局等。1996 年美国提出联邦桥接计划，2001 年正式公布，计划最终建立一个覆盖美国 80 个机构、19 个部的 PKI 以保护电子政府的通信安全。

美国联邦 PKI 体系主要由联邦的桥认证机构(Federal Bridge CA，FBCA)、首级认证机构(Principal CA，PCA)和次级认证机构(Subordinate CA，SCA)等组成。联邦 PKI 的体系结构中没有采用根 CA，而采用了首级 CA。

这是因为在美国，信任域的结构是多种多样的，美国联邦 PKI 体系结构可以支持分级(树状)维构、网状结构和信任列表等。联邦的桥 CA 是联邦 PKI 体系中能核心组织，是不同信任域之间能桥梁，主要负责为不同信任域能首级 CA 颁发交叉认证的证书，建立各个信任域的担保等级与联邦 CA 的担保等级之间的映射关系，更新交叉认证证书，发布交叉认证证书注销黑名单。但是联邦的桥 CA 不要求一个机构在与男一个机构发生信任关系时必须述循联邦 PKI 所确定的这种映射关系，而是可以采用它认为合适的映射关系确定彼此之间的信任。

欧洲在 PKI 基础建设方面也成绩显著。已颁布了 93/1999EC 法规，强调技术中立、隐私权保护、国内与国外相互认证以及无歧视等原则。为了解决各国 PKI 之间的协同工作问题，它采取了一系列措施：积极资助相关研究所、大学和企业研究 PKI 相关技术；资助 PKI 互操作性相关技术研究，并建立 CA 网络及其

顶级 CA。并于 2000 年 10 月成立了欧洲桥 CA 指导委员会，于 2001 年 3 月 23 日成立了欧洲桥 CA。

我国的 PKI 技术从 1998 年开始起步，政府和各有关部门对 PKI 产业的发展给予了高度重视。2001 年 PKI 技术被列为“十五”863 计划信息安全主题重大项目，并于同年 10 月成立了国家 863 计划信息安全基础设施研究中心。国家电子政务工程中明确提出了要构建 PKI 体系。我国已全面推动 PKI 技术研究与应用。2004 年 8 月 28 日，十届全国人大常委会第十一次会议 28 日表决通过了电子签名法，规定电子签名与手写签名或者盖章具有同等的法律效力。这部法律的诞生极大地推动了我国的 PKI 建设。

1998 年国内第一家以实体形式运营的上海 CA 中心(SHECA)成立，此后，PKI 技术在我国的商业银行、政府采购以及网上购物中得到了广泛应用。目前，国内的 CA 机构大致可分为区域型、行业型、商业型和企业型四类，并出现了得安科技、创原世纪、国创科技、吉大正元、国瑞数码等一批 PKI 服务提供商