上 海 颖 航 电 子 科 技 有 限 公 司
ShangHai Yinghang Technologies Co.,Ltd.
Tel:021-52063951/52 Fax:021-52063953

将二维条码应用于证卡管理中的解决方案

证卡管理应用

二维条码是一种崭新的数据存储和通讯技术，由于其信息容量大，识读不需要网络及数据库支持，因此使用方便、快捷、成本低。同时二维条码具有可读而不可改写，能够实现一对一验证的可防伪性。因此，可将二维条码技术广泛应用于证卡的管理。将持证人的姓名、单位、证件号码、血型、照片、指纹等重要信息进行编码，并且通过多种加密方式对数据进行加密，有效地解决了证件的自动录入及防伪问题。

基本系统功能

证卡格式制作：完成各种证卡的格式定制。

档案信息建立：在证卡数据输入界面完成信息录入。

证卡印制：采用数据压缩和数据加密技术，将证卡信息数据处理后编译成二维条码，并打印成带二维条码的的证卡。

证卡管理：实现证卡信息的查询统计以及系统维护。

证卡信息自动识别：采用二维条码识读设备和图形图像解压缩技术，实现证卡信息的自动识别和数据采集。

核查比对

证卡相关管理部门根据证卡持有人登记号和密码，打开相应的比对程序界面，通过配备的条码采集器对证卡中的条码进行识别，并与数据库原有信息进行比对，在比对的同时，根据数据库的原有信息数据对核查证卡持证人提供的其他相关材料进行审查。

证卡的户外巡查

证卡巡检系统的重要特征是，相关证卡管理部门人员必须携带移动计算机设备，在户外对各证卡持有单位或个人进行监督管理，该设备上带有被管理对象的资料和管理信息，并能够通过对相关证卡上和提供报表上的条码进行自动识别。

条码信息加密

条码本身具备防伪的特性，在于它的编码原理不被大多数人所了解，因此采用条码本身就具有一定的安全性。但是不能排除造假者具备生成条码的能力，因此还必须通过其他技术来增强条码的防伪性能。

数据加密的基本过程是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的信息，通常称为“密文”。密文只能在输入相应的密钥解密之后才能还原显示出原信息，通过这样的途径来达到保护数据不被非法窃取、造假的目的。该过程的逆过程为解密。

目前，最流行的加密技术有对称式密钥加密体制和非对称式密钥加密体制两种。它们的区别在于加密和解密密钥是否相同。考虑到本方案针对的是一个试点运行项目，为了节省成本简化应用，我们建议采用对称式密钥加密，又称私钥密码体制，即信息的发送方和接受方用同一个密钥去加密和解密数据。它最大的优势是加/解密速度快，适合于对大数据量加密，缺点是密钥管理困难。非对称加密技术比对称加密技术灵活，但加/解密速度相对较慢，尤其是不适合移动设备的使用。

对称加密体制的典型算法有 DES 算法、变形 Triple DES。DES 标准是由美国国家标准局提出的，其密钥长度为 56bit；Triple DES 使用 3 个独立的 56bit 密钥对交换的信息进行 3 次加密，使其有效长度达到 168bit。可见 Triple DES 增强了 DES 算法的可靠性。因此在本方案中，选择 Triple DES（即 3DES）方法，作为加密安全的基本手段。