有法律效力的文件，在解决医患纠纷中有着不可替代的作用。正因如此，在全面无纸化建设的过程中，医院心存诸多顾虑，包括：电子病历中的电子签名是否获得法律认可、电子病历容易复制是否能保证法律依据的唯一性，担心电子形态的病历会成为患者投诉医院的依据。归根结底，就是如何全面解决电子病历与纸质病历具有同等的法律效力的问题。

当前医院中以病人为中心的 EMR 系统（电子病历系统）在应用过程中存在一些不安全因素：登录系统的身份合法性、电子病历的法律有效性、电子病历的正式性、电子病历信息的隐私保护、责任确定、时间取证的公正性、医院之间电子病历共享的安全等问题，这些不安全的因素阻碍着信息化的进一步发展。虽然部分医院的信息化系统建设已经走在前面，但依然保留着传统的病案管理方式，不仅没有解脱传统作业方式，还增加了医生的工作量，从而降低了诊疗效率。

若不解决上述问题，尤其是发生因电子病历引起的医疗纠纷时，无法站在第三方公正机构角度证明电子病历的真实合法性，进而无法起到公正性作用。

这些安全问题愈来愈被卫生管理部门所关注，随着卫生部出台卫生部电子认证相关法规（包括《卫生系统电子认证服务管理办法》、《卫生系统电子认证服务规范》等），以及电子病历相关规范（包括《病历书写基本规范》、《电子病历基本规范》等），营造安全可信的电子医疗卫生环境已成为大势所趋，在电子病历系统中采用数字证书技术进行安全认证能够保证其安全可信。

通过对医院业务特点、IT 现状及安全风险的分析，医院在安全认证方面的安全需求总结如下。

### 1．医院信息系统的用户身份真实性需求

医院信息系统所处环境的封闭性导致其对身份认证强度的弱化。目前，医院医护人员登录信息系统普遍采用“用户名＋口令”的方式，随着医院对信息系统的依赖程度逐步加深，这种弱认证方式的弊端逐渐凸显，它直接导致医生之间冒名顶替、实习医生代替主治医生出具诊断报告等情况，同时这种弱认证方式破解极为简单，很容易导致内部重要医疗数据的外泄，甚至导致医院信息系统遭受破坏性攻击。因此，建设具备高安全性、高可靠性的医院信息系统身份认证机制，保证登录医院信息系统用户身份的真实性，在目前医院信息系统建设过程中显得尤为迫切。

### 2．医疗数据的责任归属问题

随着医院信息系统的各项功能逐步取代医院传统看病诊疗方式的同时，医护人员从对一张纸质诊断书的负责转向对一段数据电文描述内容的认可，数据电文的责任归属是否明确直接关系到信息化流程能否完全取代传统的纸质流程。因此，在用户身份真实可信的前提下，需要结合可靠的电子签名，建立医院信息系统中的责任认定机制，保障医疗数据明确的责任归属，从而消除医疗数据人工打印、手工签字的模式，实现真正意义的无纸化诊疗过程，使信息化的高效率优势充分发挥。

### 3．医疗行为的时间可信需求

医疗管理中电子病历的生成、修改及访问等时间敏感性极高，然而，目前这些事件均由信息系统服务器时间产生，很容易发生在场时间的记录不准确，从而导致医疗行为时间缺乏公信力，因此在保证时间源可信的前提下，需要对所有关键行为操作进行时间戳处理

并记录，确保提供可信的时间服务。

#### 4．数据在网络中完整传输问题

医院信息系统多数运行在医院内的局域网上，局域网上的医院信息系统终端与服务器间的信息传输安全往往被忽视，因此，信息有可能被窃取并篡改，无法保障医务人员在系统终端上输入和浏览的电子病历信息的正确性。

### 21.5.3 应用安全总体架构

电子病历应用安全总体架构主要由3部分组成。

#### 1．卫生部数字证书服务管理系统

根据《卫生系统电子认证服务管理办法（试行）》的规定，卫生部将建设集中的数字证书服务管理系统，用于卫生系统内所有证书用户信息的收集、查询、统计和分析，以及进行用户意见收集、服务质量监督等管理工作。

卫生部通过数字证书服务管理系统对在卫生系统领域开展电子认证服务的CA机构实行接入控制及服务管理。拟为卫生系统领域提供服务的电子认证服务机构，须符合《卫生系统电子认证服务管理办法（试行）》的相关要求，将CA系统接入到卫生部数字证书服务管理系统。

#### 2．CA中心

CA中心为医院电子病历提供电子认证服务，主要包括证书业务服务和技术支持服务。

证书业务服务主要包括证书管理、证书查询和时间戳服务等。证书管理主要包括证书申请、证书发放、证书更新、证书吊销、证书解锁、密钥恢复等业务服务。证书查询主要包括LDAP目录访问服务、OCSP证书在线状态查询服务及CRL证书黑名单列表下载服务。

技术支持服务主要包括使用帮助、应用咨询培训、应急保障和应用集成支持等。

CA中心有将数字证书申请、更新和吊销等相关信息同步到卫生部数字证书服务管理系统的功能。数据同步时，遵循和调用证书服务管理系统的证书信息同步接口。

#### 3．医院安全可信电子病历系统

医院安全可信电子病历系统主要由电子病历系统、安全认证系统、LRA与证书管理员、医护人员和科室机构证书等构成。

证书管理员通过LRA为医护人员、科室机构和内部设备发放数字证书。

安全认证系统主要包括密码模块、设备证书、时间戳、签名/验签、电子签章、签名存储等模块。

网上病历应用安全总体框架如图21-7所示。

### 21.5.4 网络部署结构

部署LRA系统，通过CA中心实现实时互联；为医院证书管理员颁发数字证书，介质为USBKey，进行各种证书业务操作，如证书申请、证书发放、证书更新、证书吊销等。

部署安全认证系统，配置证书注册模块、签名验签模块、签名存储模块、电子签章模块、时间戳模块；部署硬件密码设备，保证密钥存储和密码运算的安全性；在电子病历服务端系统部署并应用集成服务端安全接口模块，在电子病历客户端部署并应用集成客户端安全接口模块。部署数据库系统，用于存储电子签名相关数据。

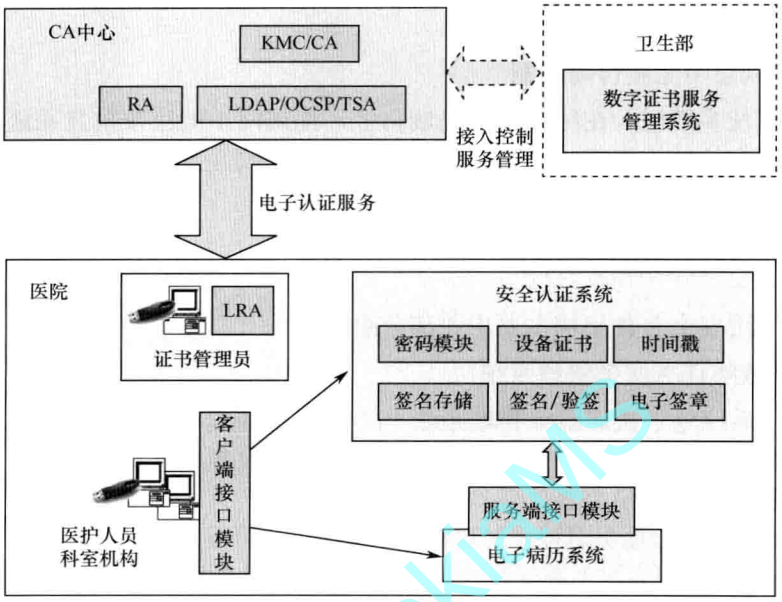


图 21-7　电子病历应用安全总体框架

为医护人员和科室机构签发数字证书，介质为 USBKey；为内部设备签发数字证书，介质为硬件密码设备。

具体部署如图 21-8 所示。

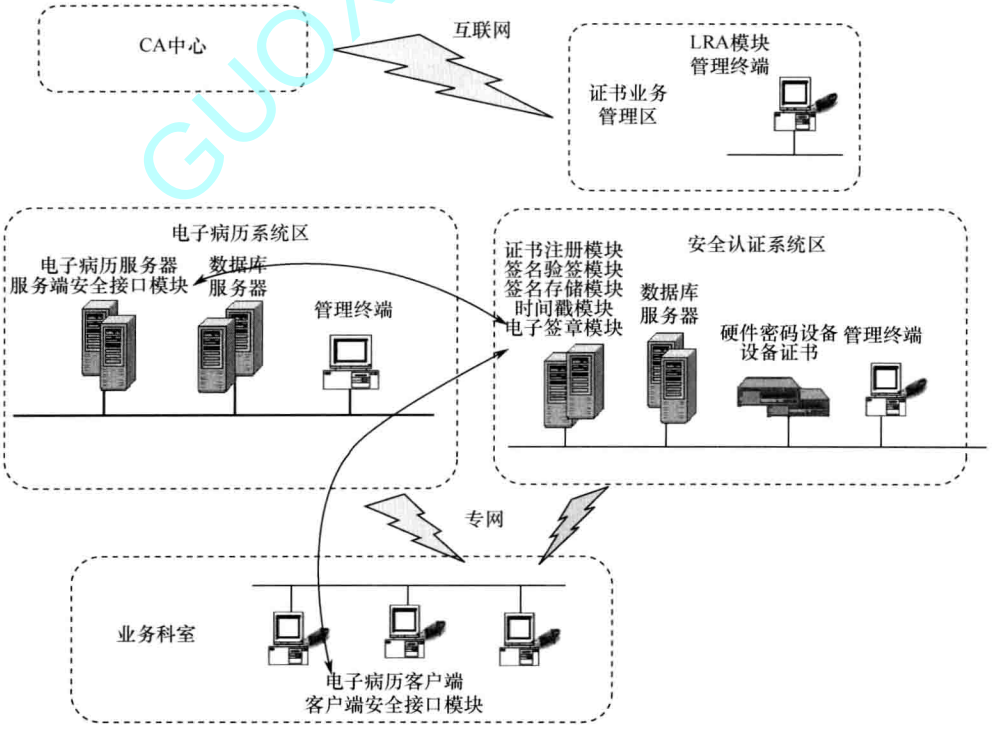


图 21-8　电子病历应用安全网络部署结构

## 21.6 公交IC卡在线充值系统

### 21.6.1 简介

2002年，建设部为了规范全国城市建设事业IC卡应用管理，促进建设事业IC卡市场的健康、有序发展，保障应用系统的安全性和兼容性组织，制定并颁布了《建设事业IC卡应用技术》国家行业标准（编号为CJ/T166-2002），从而使建设事业IC卡应用有章可循。

城市一卡通同样借鉴并发展了金融IC卡的成功技术和经验，并根据公交应用的特殊需求，进行了有针对性的扩展，从而使公交卡更好地满足实际应用的需要，更加方便地为广大市民服务。

城市一卡通在近几年得到了大规模应用。截至2011年，已有90多个城市建立了不同规模和水平的公交IC卡应用系统，累计发卡量2000余万张。经过几年的实践，建设事业IC卡的应用形成了一些特点：一是在公共交通领域实现了“一卡多用”；二是双界面CPU卡已经在建设领域得到了具体应用；三是实现了异地互通；四是实现了跨行业的“一卡多用”。

与PBOC电子钱包/电子存折不同的是，所有IC卡必须含有建设部申请的认证码，才能使用建设事业领域各种应用系统。具体金融IC技术细节请参考《商业银行密码技术应用》“第四章 电子钱包/存折密码应用体系”。

### 21.6.2 应用安全需求

尽管公交IC卡使用非常广泛，但由于公交卡属于匿名购买和无密码消费，为减少公交卡丢失所造成的经济损失，市民一般只在公交卡中存储少量资金，消费完毕后再进行充值，这就导致公交IC卡的频繁充值。但由于当前技术所限，公交卡充值必须要到充值点进行人工充值，给市民带来很多不便。由于受到成本限制，公交卡充值点无法做到随处可见，导致充值点人满为患。

因此通过互联网实现对公交IC卡的在线充值成为未来的发展趋势，不仅可免去持卡人到充值点排队充值的麻烦，同时也降低了公交卡服务机构建立充值点的成本。公交IC卡已采用对称密码体系，只适合在相对封闭的环境下运行。

公交IC卡在线充值应用安全方面的具体需求主要包括：

① 正确鉴别IC卡的身份。保证IC身份的真实性和合法性。

② 保证交易数据的真实性和完整性。防止非法用户对数据进行假冒、篡改和删除，防止数据传送过程中信息的丢失和重复，保证信息传送次序的统一。

③ 保证交易数据的机密性。通过对一些敏感的数据进行加密来保护系统之间的数据交换，防止除接收方之外的第三方截获数据。

④ 不修改IC卡现有的对称密钥体系。

⑤ 审计能力。根据机密性和完整性的要求，对交易结果进行记录。

### 21.6.3 应用安全总体架构

公交 IC 卡在线充值应用安全总体框架如图 21-9 所示。

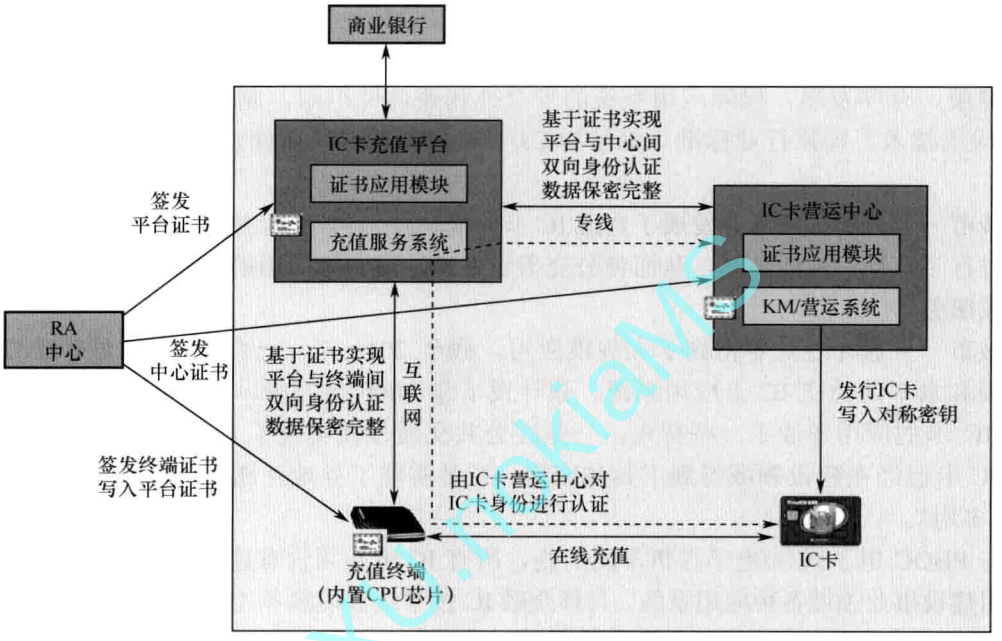


图 21-9 公交 IC 卡在线充值应用安全总体框架

IC 卡充值平台将商业银行和 IC 卡营运中心连接起来，通过互联网为充值终端提供公交卡充值服务。

为保证网络安全性，IC 卡营运中心只允许通过专线与 IC 卡充值平台进行连接。

为保证应用安全性，RA 中心为充值终端、IC 卡充值平台和 IC 卡营运中心签发数字证书，基于数字证书技术实现充值平台与充值终端、充值平台与营运中心之间的双向身份认证、数据保密性和完整性。

公交 IC 卡的所有交易都是基于对称密钥体系的，采用非常严格的密钥管理机制对对称密钥进行全过程管理。为保证对称密钥的安全性，充值终端和充值平台都不能对 IC 卡进行身份认证、充值交易等任何涉及对称密钥的操作，只允许 IC 卡营运中心对 IC 卡进行身份认证、充值交易等涉及对称密钥的操作。充值终端只是充当普通读卡器角色，充值平台只是作为网络传输通道，将 IC 卡与营运中心之间的交互数据进行上传下达而已。

### 21.6.4 充值交易流程

#### 1. 传统充值交易流程

IC 卡传统充值交易流程包括 4 个步骤，如图 21-10 所示。其中，MAC1 由 IC 卡使用基于充值密钥产生过程的密钥生成，营运中心通过验证 MAC1 来确认 IC 卡的合法身份；MAC2 由营运中心使用相同的过程密钥产生，IC 通过验证 MAC2 来确认营运中心的合法