身份，如果 MAC2 验证通过，则 IC 自动更新卡片内金额信息；TAC 由 IC 卡使用 TAC 密钥生成，在 IC 卡中保存一份，同时传送给营运中心。

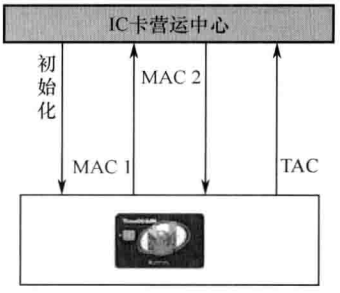

图 21-10　公交 IC 卡传统充值交易流程

2. 在线充值交易流程

为保证充值终端使用认可的数字证书，需要对 IC 卡营运中心加密机进行以下升级改造：

① 支持 RSA 运算。

② 内置 CA 证书。

③ 新增在线充值指令：完成验证终端签名、验证终端证书、验证 MAC1、产生 MAC2 并用终端证书加密。

在线充值交易流程如图 21-11 所示。

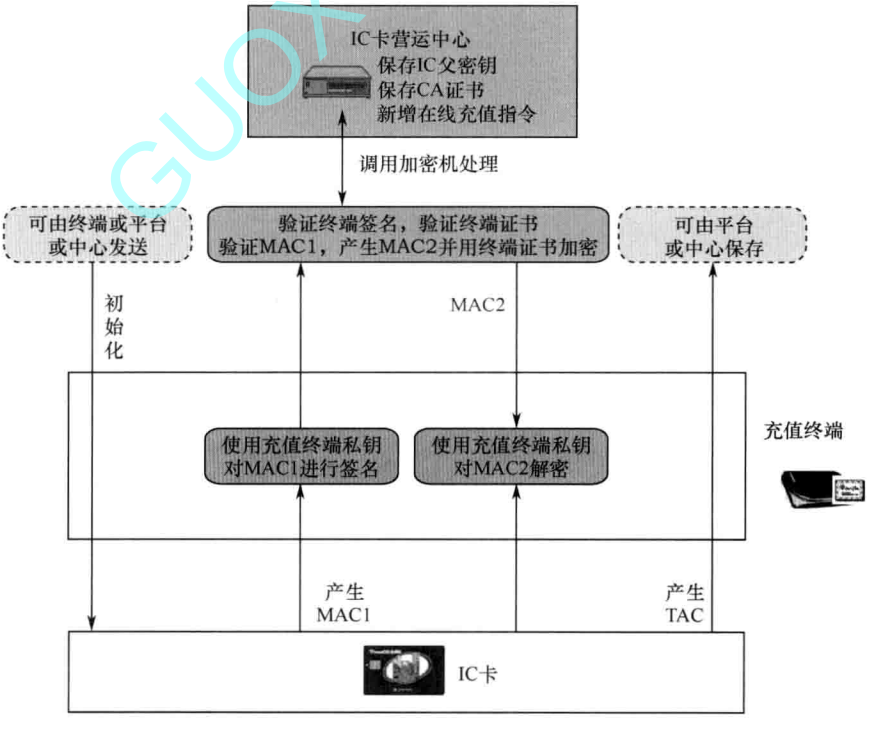

图 21-11　公交 IC 卡在线充值交易流程

① 向 IC 卡发出初始化充值指令：可由充值终端、充值平台或营运中心发起。

② IC 卡产生 MAC1 报文，回送给充值终端。

③ 充值终端使用终端私钥对 MAC1 报文进行签名，连同终端证书一起将签名后的 MAC1 报文发送给营运中心。

④ 营运中心系统调用加密机“在线充值指令”后，产生加密后的 MAC2 报文，发送给充值终端。

⑤ 充值终端接收到加密后的 MAC2 报文并使用私钥进行解密后，将 MAC2 报文发送给 IC 卡。

⑥ IC 卡接收到 MAC2 报文后，进行充值处理，然后产生 TAC 报文。

⑦ TAC 报文可由充值平台或营运中心保存。

第 22 章　实　验　四

22.1　Windows IIS 服务器证书配置

如果没有安装 IIS，需要先安装 IIS 组件。下面以 Windows 7 为例说明 IIS 组件的安装过程。

① 选择“控制面板”→“程序”→“程序和功能”→“打开或关闭 Windows 功能”，如图 22-1 所示。

图 22-1　安装 IIS 组件

② 选择“Internet 信息服务”，对需要的选项进行勾选。一个较小的选项集如图 22-2 所示。

图 22-2　IIS 安装选项

③ 单击“确定”按钮，等待安装完成。

22.1.1 下载并安装服务器证书

在 IIS 中启用 SSL 前，需要安装服务器证书，可以通过 IIS 证书管理功能完成证书申请和导入操作。

① 进入“控制面板”→“系统和安全”→“管理工具”→“Internet 信息服务（IIS）管理器”，出现 IIS 管理界面，如图 22-3 所示。

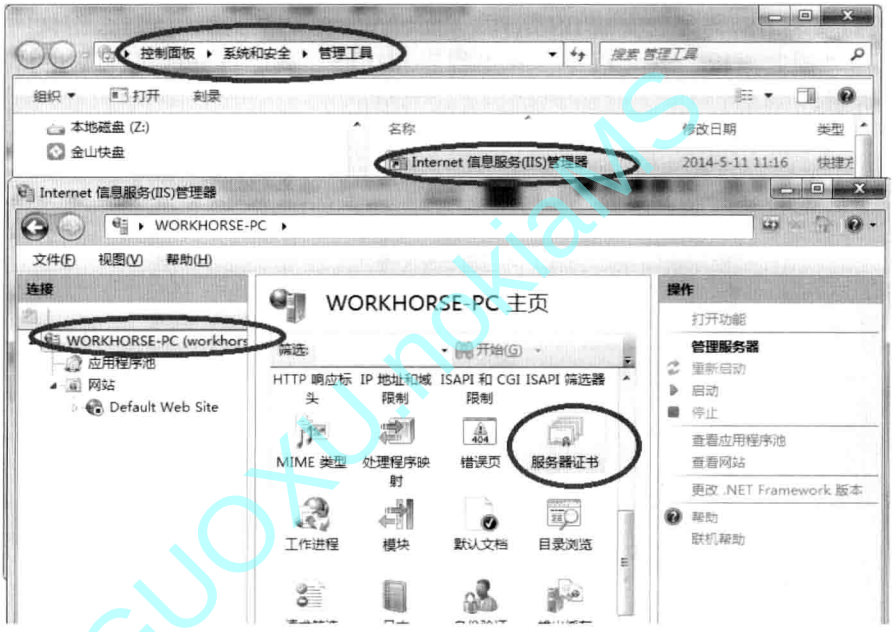

图 22-3 Internet 信息服务（IIS）管理器

② 在 IIS 管理界面单击“服务器证书”，进入服务器证书申请界面，如图 22-4 所示。

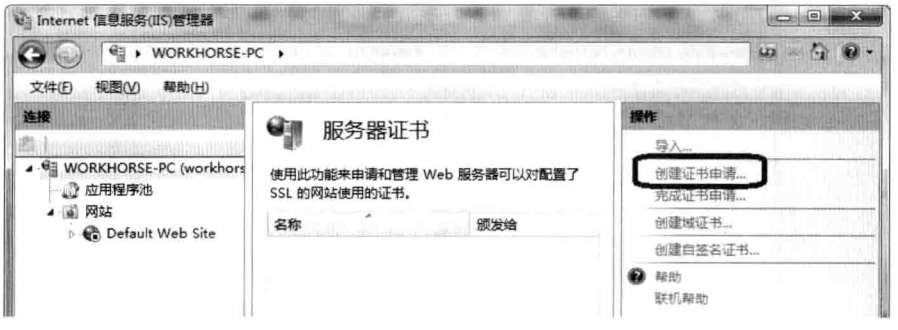

图 22-4 服务器证书管理

③ 单击“创建证书申请”功能链接，进入信息录入界面，如图 22-5 所示。在通用名称栏中输入 localhost（下文将以 localhost 为地址访问 IIS 服务器，应输入域名或 IP 地址），国家/地区中输入 CN（表示中国）。

图 22-5　证书使用者信息录入

④ 单击“下一步”按钮，出现“加密服务提供程序属性”界面，如图 22-6 所示，此处采用默认值。

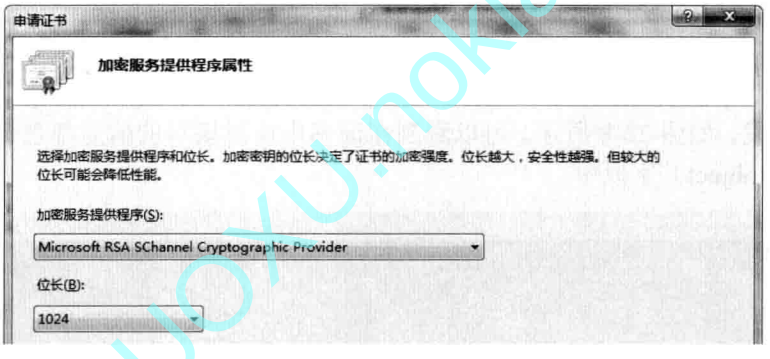

图 22-6　加密服务程序选项

⑤ 单击“下一步”按钮，出现证书请求文件保存路径输入界面，如图 22-7 所示，填入正确的文件路径。

图 22-7　证书请求文件保存路径

⑥ 单击“完成”按钮，生成的证书请求内容如下：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDUTCCAroCAQAwZjELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB2JlaWppbmcxEDAO
BgNVBAcMB2JlaWppbmcxDzANBgNVBAoMBnRlc3RjYTEOMAwGA1UECwwFdGVzdDEx
EjAQBgNVBAMMCWxvY2FsaG9zdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
```