城、异地、本行、跨行的资金转账，辅助功能还包括收款人账户管理、付款用途维护、对外转账限额设置等。延伸功能包括预约转账、批量转账，而预约转账又可分为指定日期转账、预约周期转账、指定条件转账。网上支付即网上即时付款服务。网上支付功能在网银中应用得比较普遍，网上支付是为用户提供在网上购买商品的一种渠道。网上支付有多种方式：从网银链接到网上商城、根据网上支付订单号进行支付、从他行的网站链接到网银的支付平台或在网银外进行网上支付等。自助缴费功能为用户提供向各类银行特约收费单位自行缴纳各类日常费用的服务功能，如公共事业性收费、保险续期缴费等。

（3）投资理财类

投资理财类业务主要包括卡储蓄业务、自助贷款、外汇、黄金、证券、基金、国债、保险、信用卡服务等。卡储蓄业务功能主要体现在个人或家庭可以对所属各类银行卡或存折进行管理、查询和交易，主要指卡内活期转整存整取、零存整取、通知存款、存本取息等。自助贷款业务主要指各种贷款的网上申请、网上放贷、申请展期、贷款试算还贷及额度查询等，可以方便个人或家庭在网上及时办理各类贷款业务，主要包括个人消费贷款、自助质押贷款、住房贷款、汽车贷款等。外汇买卖功能是个人客户委托银行把一种可自由兑换的外币兑换成另一种可自由兑换的外币，并参照国际金融市场行情制定相应汇率。黄金交易分为纸黄金交易和代理实物黄金交易。证券即是早期的网上银行股票买卖交易功能。用户可以在网上银行办理股票委托交易，管理资金账户、查询最新证券信息和股票行情。但由于银监会的监管，目前所有银行已经取消了原来的证券交易功能，只支持银证转账和第三方存管，基本上就是一个银行和证券账户之间的资金互转。基金交易指网上办理与基金相关的各种业务交易，如开户、销户、查询、购买、赎回等。保险主要指网上直接购买保险产品，其有多种方式：直接在网银内选择保险产品并投保、链接到保险公司进行投保或只进行保费的续缴等。国债主要指国债买卖、管理国债账户、查询国债价格和交易明细等。信用卡服务主要指信用卡信息管理、还款设置、网上还款等。

（4）服务管理类

服务管理类主要包括个人设置、网银设置、财务管理等。个人设置包括信息修改、密码设置、通知提醒等。网银设置为个人用户使用网上银行各项业务功能实时提供在线通知提醒或帮助、说明以及各项用户自助服务功能。财务管理主要是指网上银行提供给客户用于各账户情况的财务管理与分析。

21.3.2 应用安全需求

网上银行以 Internet 等开放式网络环境传输交易数据，而且涉及用户资金转移等敏感信息，所以在用户的身份认证、资金的秘密传输以及数据的完整性方面存在许多安全问题。网上银行服务提供者首先需要确定自己的系统不会受到网络黑客的入侵，造成秘密信息泄露，业务损失或服务中断。对用户而言，必须确认在网络上输入的秘密信息不会被盗用，输入的交易资料不会被篡改并且能正确迅速地传送到接收端系统。

网上银行系统应用安全方面的具体需求主要包括以下内容。

（1）正确鉴别用户的个人身份及权限

保证用户身份的真实性和合法性、用户权限的有效性。

（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）抗抵赖

防止发送消息者事后否认其所发送的消息。

（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。

（6）密钥管理

管理用户在网上银行系统中所使用的密钥，保证密钥的真实性、有效性和完整性。

21.3.3 应用安全总体架构

鉴于网上银行采用开放性的 Web 技术和互联网技术，为全面解决网上银行应用安全需求，通常采用 PKI 体系。基于数字证书技术，网上银行能有效解决用户身份认证、敏感数据保密性、交易数据完整性和交易操作不可抵赖性问题，极大地方便了银行企业客户和个人客户。事实上，数字证书（俗称 U 盾）已经成为国内网上银行的标准配置。如果没有数字证书，企业用户将不允许使用网上银行。上亿个人用户已经通过数字证书访问网上银行实现转账或汇款等资金操作。

网上银行应用安全总体框架如图 21-5 所示。

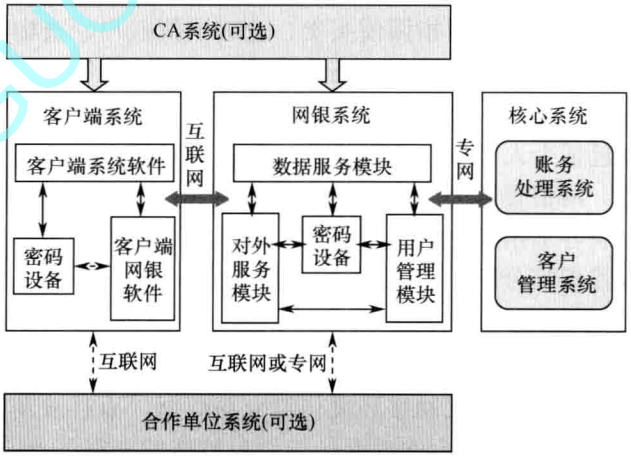

图 21-5 网上银行应用安全总体框架

（1）关联方

网上银行业务涉及的关联方主要包括 4 类：

① 网银用户：即个人或单位，通过网银方式获取各种银行业务服务。

② 商业银行：通过网银方式向个人或单位提供各种银行业务服务。

③ 合作单位：依托网银方式对个人或单位提供网上购物、网上缴费、网上充值等非银

行业务服务。

④ CA 机构：给网银业务涉及的上述 3 个关联方颁发数字证书，提供电子认证服务。当不采用第三方电子认证服务时，CA 机构属于商业银行。

（2）系统构成

网上银行整体系统主要包括 4 部分：

① 客户端系统：指基于互联网技术的各种终端系统，包括计算机、智能终端等。主要由密码设备、客户端系统软件和客户端网银软件组成。网银用户通过客户端系统访问网银系统和合作单位系统（有些网银业务不需要访问合作单位系统）。客户端系统通过互联网与网银系统和合作单位系统互联。

② 网银系统：实现网银业务服务、网银客户管理、网银安全保障等功能。主要由对外服务模块、用户管理模块和数据服务模块组成。网银系统通过专网同银行核心系统互联，通过互联网或专网同合作单位系统互联。

③ 合作单位系统：可选，部分业务不包括此系统。

④ 核心系统：实现银行内核心账务处理和客户信息管理。

⑤ CA 系统：实现数字证书的生命周期管理。

客户端系统主要包括：

① 密码设备：实现用户密钥安全存储和密码安全运算。主要包括：USB-Key、IC 卡、动态令牌等。

② 客户端系统软件：管理本地资源，并保证密码设备与客户端网银软件能通信。主要包括：操作系统、密码设备驱动等。

③ 客户端网银软件：访问密码设备和网银系统。对于 B/S 方式主要包括：浏览器、控件/Applet/插件、客户端软件（可选）等。

网银系统主要包括：

① 对外服务模块：实现网银业务服务；对于 B/S 方式，包括 Web 服务模块和应用服务模块。

② 用户管理模块：实现用户信息管理和身份认证等安全保障功能。

③ 数据服务模块：实现数据存储功能。

④ 密码设备：实现网银系统密钥安全存储和密码安全运算。主要包括：加密机、加密卡、SSL 加速器等。

21.4 网上报税系统

21.4.1 简介

随着 IT 技术的迅速发展及其在税收领域的广泛应用，网上税收已成为不可逆转的发展趋势。目前国内多数的税务机关都面向纳税人开展了网上申报业务，并逐步实现了网上实时缴款，极大方便了纳税人，提高了税收征管的效能。

由于网上纳税申报业务依托互联网开展，而互联网固有的开放性又具有用户真实身份验证困难、信息在网络传输过程中保密性差、容易遭受恶意篡改、用户容易抵赖其网络行为等特点。因此，随着系统不断地推广运行，安全问题逐渐显露。

21.4.2 应用安全需求

解决网上申报业务中的安全和责任问题，使无纸化真正落在实处的核心是：电子申报数据应与上门申报的纸质申报表具有同等的法律效力。

网上申报业务应用安全需求分析如下：

① 确保纳税人登录网上申报系统身份的可靠性。

② 确保纳税人网上申报过程中电子申报数据的保密性和完整性。

③ 采取可靠的技术确保网上申报数据的法律效力，取消纳税人网上申报后递交纸质申报材料。

④ 纳税人自助打印电子缴款凭证。

21.4.3 应用安全总体架构

网上报税应用安全总体架构如图 21-6 所示。

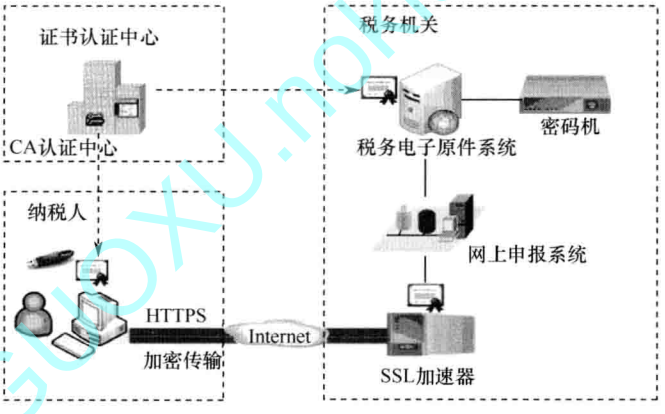

图 21-6 网上报税应用安全总体框架

基于数字证书实现身份认证、利用数字证书实现网上申报数据的可靠电子签名、通过税务电子原件系统对申报电子原件进行可靠管理，使网上申报系统产生的申报电子原件符合电子签名法的相关要求，为税务机关网上申报系统提供具有法律效力的数据电文，为纳税人提供更安全的网上申报服务。

网上报税系统主要包括以下组成部分。

① 数字证书：第三方电子认证服务机构为纳税人和税务机关颁发的电子身份凭证，能可靠标识纳税人的网络身份。

② 税务电子原件系统：根据纳税人的电子申报数据产生可靠的电子签名，向纳税人提供具有税务机关可靠电子签名的申报回执服务和具有可靠电子签名的申报原件查询下载服务，以及电子缴款凭证自助打印服务。

③ SSL 加速器：SSL 加速器是部署在网上申报系统服务器端的硬件，用于提高 SSL 传输处理速度，减轻网上申报系统服务器的负担。

④ 数字证书登录系统是一种优于原有用户名密码登录的安全登录方式。

⑤ 电子申报数据中增加了纳税人的电子签名，使申报原件具有了与纸质申报材料同等的效力。

⑥ 税务机关为纳税人提供了申报电子回执，使电子回执与纸质付款凭证具有了同等的法律效力。

⑦ 税务机关为纳税人提供了基于电子回执的、在线自助打印电子缴款凭证服务，使纳税人无须出门即可获取回执并用作记账凭证。

⑧ 纳税人的申报表及相应的电子签名可直接归档处理，实现了申报原件的在线查询及验证。

电子签名法赋予数字签名法律效力后，数字证书技术就可有效解决网上报税中的应用安全问题，使得企业网上报税成为现实，同时提高了企业和税务部门的工作效率。事实上，国内大部分省份的上千万家企业已经通过数字证书在进行网上报税。

21.5 电子病历系统

21.5.1 简介

病历是病人在医院诊断治疗全过程的原始记录，它包含首页、病程记录、检查检验结果、医嘱、手术记录、护理记录等。电子病历不仅指静态病历信息，还包括提供的相关服务。是以电子化方式管理的有关个人终生健康状态和医疗保健行为的信息，涉及病人信息的采集、存储、传输、处理和利用的所有过程信息。美国国立医学研究所将其定义为：电子病例（EMR）是基于一个特定系统的电子化病人记录，该系统提供用户访问完整准确的数据、警示、提示和临床决策支持系统的能力。

电子病历是随着医院计算机管理网络化、信息存储介质（如光盘和 IC 卡）等的应用及 Internet 的全球化而产生的。电子病历是信息技术和网络技术在医疗领域的必然产物，是医院病历现代化管理的必然趋势，其在临床的初步应用极大地提高了医院的工作效率和医疗质量，但这还仅仅是电子病历应用的起步。

电子病历（EMR，Electronic Medical Record）也叫计算机化的病案系统或称基于计算机的病人记录（CPR，Computer-Based Patient Record）。它是用电子设备（计算机、健康卡等）保存、管理、传输和重现的数字化病人的医疗记录，取代了手写纸张病历。它的内容包括纸张病历的所有信息。

根据国家卫生部颁发的《电子病历基本架构与数据标准电子病历》，电子病历定义为：电子病历是医疗机构对门诊、住院患者（或保健对象）临床诊疗和指导干预的、数字化的医疗服务工作记录。

电子病历是用电子设备（计算机、健康卡等）保存、管理、传输和重现的数字化的病人医疗记录，取代手写纸张病历。电子病历具有主动性、完整和正确、知识关联、及时获取等特征，是医疗机构对门诊、住院患者（或保健对象）临床诊疗和指导干预的、数字化医疗服务工作记录。

21.5.2 应用安全需求

随着电子病历系统在医院的普遍使用，病历无纸化存储再也不是空谈了，消除纸张病历这一信息孤岛的思想已经深入人心。众所周知，病历不仅是病程记录，也是重要的、具