

图 25-13 证书申请类业务流程

25.2.1.1 证书申请

1. 提出申请

用户（证书申请者）如实填写“数字证书申请表”，并认真阅读“数字证书服务协议”，按要求在申请表和服务协议上签名或盖章（个人证书申请应签名，机构证书申请应加盖公章）。个人和机构数字证书申请表样例分别参见表 25-1 和表 25-2。数字证书服务协议样例参见表 25-3。

按要求准备相关资料后，向 CA 中心提交证书申请。

个人证书申请须提交的资料主要包括：个人数字证书申请表、数字证书服务协议、申请人证件复印件及原件、代理人证件复印件及原件等。

机构证书申请须提交的资料主要包括：机构数字证书申请表、数字证书服务协议、机构证件复印件及原件（工商营业执照、组织机构代码证等）、经办人证件复印件及原件等。

表 25-1 个人数字证书申请表样例

证书申请信息					
申请日期		证书数量		证书期限	
证书种类	<input type="checkbox"/> 个人普通证书 <input type="checkbox"/> 个人高级证书 <input type="checkbox"/> 安全邮件证书 <input type="checkbox"/> 其他种类证书，请注明：				
业务类型	<input type="checkbox"/> 新申请 <input type="checkbox"/> 更新 <input type="checkbox"/> 作废				
证书 DN（仅更新或作废时填写）					
申请人信息					
姓名（中文）				姓名（拼音）	
证件类型	<input type="checkbox"/> 身份证 <input type="checkbox"/> 户口簿 <input type="checkbox"/> 护照 <input type="checkbox"/> 军人身份证 <input type="checkbox"/> 武警身份证 <input type="checkbox"/> 港澳通行证 <input type="checkbox"/> 其他，请注明：				
证件号码					
电话		传真		电子邮件	
联系地址				邮政编码	
申请人声明					
本人承诺以上所填写的申请资料真实、有效。本人已认真阅读并同意遵守《数字证书服务协议》、《电子认证业务规则（CPS）》中规定的相关义务。					
申请人签名				日期	
以下信息由 CA 中心填写					

(续表)

证书申请信息					
录入员				录入日期	
审核员		审核意见	<input type="checkbox"/> 审核通过 <input type="checkbox"/> 审核不通过	审核日期	
收费员				收费日期	
制证员				制证日期	
备注				CA 中心盖章	

表 25-2 机构数字证书申请表样例

证书申请信息					
申请日期		证书数量		证书期限	
证书种类	<input type="checkbox"/> 机构普通证书 <input type="checkbox"/> 机构高级证书 <input type="checkbox"/> 服务器证书 <input type="checkbox"/> 设备证书 <input type="checkbox"/> 安全邮件证书 <input type="checkbox"/> 代码签名证书 <input type="checkbox"/> RA 管理员证书 <input type="checkbox"/> 其他种类证书, 请注明:				
业务类型	<input type="checkbox"/> 新申请 <input type="checkbox"/> 更新 <input type="checkbox"/> 作废		证书 DN (仅更新或作废时填写)		
申请机构信息					
机构名称					
英文/拼音简称					
机构证件类型	<input type="checkbox"/> 企业营业执照 <input type="checkbox"/> 组织机构代码证 <input type="checkbox"/> 其他, 请注明:				
机构证件号码					
网站域名或 IP 地址 (仅申请服务器证书时填写)					
机构经办人信息					
经办人姓名					
经办人证件类型	<input type="checkbox"/> 身份证 <input type="checkbox"/> 户口簿 <input type="checkbox"/> 护照 <input type="checkbox"/> 军人身份证 <input type="checkbox"/> 武警身份证 <input type="checkbox"/> 港澳通行证 <input type="checkbox"/> 其他, 请注明:				
经办人证件号码					
电话		传真		电子邮件	
联系地址				邮政编码	
申请机构声明					
本机构承诺以上所填写的申请资料真实、有效。本机构已认真阅读并同意遵守《数字证书服务协议》、《电子认证业务规则 (CPS)》中规定的相关义务。					
申请机构盖章				日期	
以下信息由 CA 中心填写					
录入员				录入日期	
审核员		审核意见	<input type="checkbox"/> 审核通过 <input type="checkbox"/> 审核不通过	审核日期	
收费员				收费日期	
制证员				制证日期	
备注				CA 中心盖章	

表 25-3 数字证书服务协议样例

数字证书是电子认证服务机构签发的包含数字证书使用者身份信息和公开密钥的电子文件。某 CA 中心（以下简称 XYZCA）是工业和信息化部批准的电子认证服务机构和国家密码管理局批准的电子政务电子认证服务机构，遵照《中华人民共和国电子签名法》为用户提供数字证书相关的电子认证服务。

本协议中的用户指数字证书持有人以及申请使用数字证书的实体。

为明确各方权利和义务，XYZCA 和用户就数字证书的申请和使用等事宜达成以下协议，共同遵守执行。

第一条 申请

1. 用户在申请数字证书时，应提供真实、完整和准确的信息及证明材料。如因故意或过失未向 XYZCA 或其设立的注册机构提供真实、完整和准确的信息，导致 XYZCA 签发证书错误，造成相关各方损失的，由用户承担相关责任。

2. XYZCA 设立的注册机构作为证书业务受理单位和服务支持单位，负责用户的信息录入、身份审核和证书制作工作。用户在申请数字证书时应遵照注册机构的规程办理手续。

3. XYZCA 设立的注册机构应完全遵守 XYZCA 安全操作流程进行用户身份审核和证书制作。

4. XYZCA 积极响应各注册机构发出的证书申请请求，及时为通过审核的用户签发证书。如果由于设备或网络故障而导致签发数字证书错误、延迟、中断或者无法签发，XYZCA 不承担任何赔偿责任。

5. 用户在获得数字证书时应及时验证此证书所匹配的信息，如无异议则视为接受证书。

第二条 使用

6. XYZCA 签发的数字证书用于网络上的用户身份标识、数字签名验证及密钥分配，各应用系统可根据需要对其用途进行定义，但不包括涉及违反国家法律、法规或危害国家安全的用途。

7. 用户应确保其应用系统能为数字证书提供安全的应用环境，若因网络、主机、操作系统或其他软硬件环境等存在安全漏洞，由此导致的安全事故及相关后果，XYZCA 不承担责任。

8. 用户应当妥善保管 XYZCA 签发的数字证书、私钥及保护密码，不得泄露或交付他人。如用户保管不善导致数字证书遭盗用、冒用、伪造或者篡改，用户应当自行承担相关责任。

9. 数字证书对应的私钥为用户本身访问和使用，用户对使用数字证书的行为负责。所有使用数字证书在网上交易和网上作业中的活动均视为用户所为，因此而产生的相关后果应当由用户自行承担。

10. 数字证书一律不得转让、转借或转用。因转让、转借或转用而产生的相关后果应当由用户自行承担。

11. XYZCA 承诺，在现有的技术条件下，由 XYZCA 签发的数字证书不会被伪造、篡改。如果发生数字证书被篡改、伪造，经确认确属 XYZCA 责任，XYZCA 承担赔偿责任。赔偿方法参照《XYZCA 电子认证业务规则》。

第三条 更新

12. 数字证书的有效期限自证书受理之日起计算。若在数字证书有效期到期后，用户仍需继续使用数字证书，必须在数字证书到期前一个月内向 XYZCA 设立的注册机构提出数字证书更新请求。否则，证书到期将自动失效，XYZCA 对此不承担责任。

13. 因技术需要，XYZCA 有权要求用户及时更新数字证书。用户在收到更新通知后，应在规定的期限内到 XYZCA 设立的注册机构更新证书。若用户逾期没有更新证书，因此而产生的相关后果应当由用户自行负责。

第四条 作废

14. 如遇数字证书私钥泄露丢失、证书中的信息发生重大变更或用户不希望继续使用数字证书的情况，用户应当立即到 XYZCA 设立的注册机构申请作废证书。作废手续遵循各注册机构的规定。XYZCA 在接到作废申请后，在 24 小时内作废用户的数字证书。用户应当承担在证书作废之前所有因使用数字证书而造成的责任。

15. 如果用户主体资格灭失（如企业注销等），法定责任人应携带相关证明文件及原数字证书，向注册机构请求作废用户证书。相关责任人应当承担其数字证书在作废前所有使用数字证书而造成的相关后果。

16. 对于下列情形之一，XYZCA 有权主动作废所签发的证书：

① 用户申请证书时，提供不真实信息；

- ② 证书对应的私钥泄露或出现其他证书的安全性得不到保证的情况；
- ③ 用户不能履行或违反了相关法律、法规和本协议所规定的责任和义务；
- ④ 法律、法规规定的其他情形。

第五条 其他

17. XYZCA 不对由于意外事件或其他不可抗力事件而导致暂停或终止全部或部分证书服务承担任何责任。

18. 本协议条款可由 XYZCA 随时更新，XYZCA 会通过网站 www.xyzca.com 进行通知和公布，更新后的协议一旦公布即替代原来的协议条款。用户如果不接受修改后的协议，可于通知发布之日起十五日内，向 XYZCA 设立的注册机构提出作废证书的申请。如果逾期没有提出异议，则视为同意接受修订后的协议。

19. 本协议与 XYZCA 网站上公布的《XYZCA 电子认证业务规则》共同构成关于数字证书的完整协议。

20. 本协议的解释适用中华人民共和国法律。若用户与 XYZCA 之间发生任何纠纷或争议，首先应友好协商解决，协商不成的，双方同意将纠纷或争议提交×××法院管辖。

用户确认已经认真阅读并完全理解本协议中的各项规定，用户在申请表上签名盖章即表明接受本协议的约束，本协议即时生效。

2. 受理申请并审核

CA 中心录入员负责内容检查和信息录入。如果检查不合格，则提示申请人补充完善；如果检查合格，则将证书申请信息录入 RA 系统。检查内容主要包括：

- ① 申请书是否填写完整和规范。
- ② 申请书和服务协议是否有个人签名或加盖机构公章。
- ③ 携带资料是否齐全。
- ④ 申请书填写内容是否与资料吻合。

CA 中心审核员负责信息审核。如果审核不合格，则在 RA 系统中标记审核不通过、记录不通过理由，并告知申请人原因、返还申请资料；如果审核合格，则在 RA 系统中标记审核通过。审核内容主要包括：

- ① 申请人是否符合证书发放要求。
- ② 相关证件是否真实有效。
- ③ 申请人的信用情况，是否有不良记录。

CA 中心也可以提供 Web 服务，允许用户通过互联网进行证书申请，录入相关信息后，携带资料到现场进行业务办理。

3. 收费

CA 中心收费员负责费用收取。按计费规定收取费用后，给申请人出具收费票据，并在 RA 系统中记录收费情况。

证书申请费用主要包括证书介质费、证书服务费、增值服务等。选用不同型号的证书介质，则证书介质费不同。不同证书类型、不同的证书有效期，其证书服务费不同。增值服务可包括电子印章、短信提醒等。

CA 中心也可以提供 Web 服务，允许用户通过网上支付方式付费。

4. 制证与领证

CA 中心制证员负责证书的制作和发放。通过 RA 系统完成密钥对生成和证书下载，证书和私钥均存储在证书介质中（如 USB Key、IC 卡等），并打印密码信封（用于访问证书

介质的口令)。

制证完毕后,制证员将证书介质和密码信封交给申请人。

25.2.1.2 证书更新

与证书申请相比,证书更新有以下不同。

1. 用户信息已经审核通过

用户在首次申请证书时,已经提交过纸质资料并审核通过。由于用户信息没有发生变化,因此证书更新时,无需重复提交纸质资料,信息审核环节可以简化(申请人的信用情况可能会发生变化,可能需要再次审核)。

如果 CA 中心提供 Web 服务,则用户就可以通过 Web 服务远程提交证书更新申请,无需到现场进行手工办理。因为可以通过用户已有证书进行身份认证,实现远程确认用户的合法身份。

2. 已经拥有证书介质

通常情况下,证书介质可以复用,即证书到期后,使用原有证书介质可以申请新的证书。

如果 CA 中心提供 Web 服务,则用户可以通过 Web 服务远程更新证书到原来的证书介质中。当然,前提是用户支付证书更新费,并经 CA 中心审核通过。

如果 CA 中心同时提供 Web 服务,允许用户远程提交证书更新申请、网上付款、远程更新证书,则证书更新业务流程就可以完全实现在线办理,从而提高效率。

25.2.1.3 证书变更

由于用户信息已发生变化,因此仍需要严格的信息审核。

证书变更业务流程与证书申请基本相同。

25.2.2 证书作废类

证书作废类的业务流程如图 25-14 所示。

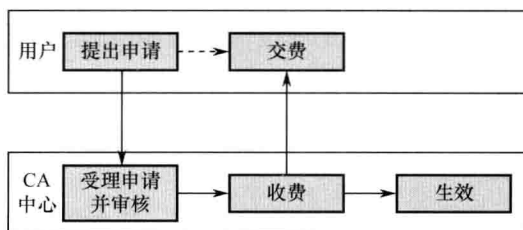


图 25-14 证书作废类业务流程

25.2.2.1 证书作废

当证书仍处于有效期但发生以下原因时,该证书应该作废,不再允许使用:

- ① 证书持有者已改变状态(如信息变更、岗位调整、证件失效等),无权使用证书。
- ② 证书持有者的密钥已遭破坏或证书介质丢失,或者怀疑密钥泄露,为避免遭受损失。
- ③ 证书持有者本人不想再使用该证书。
- ④ 证书签发者 CA 的密钥已被破坏或到期失效。