CFCA 预植数字证书服务协议

（本协议包含 CFCA 的免责条款，请认真阅读，尤其是粗体字内容）

尊敬的网上用户：

中金金融认证中心有限公司(即中国金融认证中心，简称 CFCA)是经国家有关管理机关审批设立的电子认证服务机构，作为金融行业权威的第三方安全认证机构，通过发放数字证书为网上交易提供信息安全保障。**本协议构成预植数字证书持有人（下称订户）与中金金融认证中心有限公司之间的权利义务约定，若同意本协议全部条款，即可申请使用 CFCA 预植数字证书（下称预植证书）。**

预植证书是指该证书由 CFCA 预先在智能存储介质（简称 USBKey）中生成，由订户向发证机构申领，发证机构对订户的身份进行审核并与证书绑定后方生效的数字证书。

一、 CFCA 预植证书提供的服务和 CFCA 的权利、义务

1、 CFCA 确保预植证书私钥是唯一的。

2、 当预植证书与订户身份信息的绑定经发证机构和 CFCA 数字签名确认后，该预植证书即可生效。

3、 CFCA 向相关依赖方提供预植证书绑定信息的查询。

4、 CFCA 依法制定《电子认证业务规则》（简称 CPS）、《预植证书策略》（简称 CP）,并公布于 CFCA 网站（www.cfca.com.cn），明确 CFCA 预植证书的功能、使用证书各方的权利、义务以及 CFCA 的责任范围。

5、 CFCA 为订户提供 7X24 小时热线支持服务（4008809888），5 X 8 小时服务监督电话（010-83519756），CFCA 将在 1 个工作日内对订户的意见和建议做出响应。

6、 在订户通过数字证书对交易信息进行加密和签名的条件下，CFCA 保证交易信息的保密性、完整性、不可抵赖性。如果发生纠纷，CFCA 将依据不同情况承担下述义务：

1） 提供签发数字证书的 CA 证书。

2） 提供数字证书在交易发生时，在或不在 CFCA 发布的数字证书撤销列表内的证明。

3） 提供数字证书在交易发生时，是否与该订户信息绑定的证明。

4） 对数字证书及绑定、数字签名、时间戳的真实性、有效性进行技术确认。

7、 对于下列情况之一，CFCA 有权吊销所签发的数字证书：

1) 订户申领预植证书时，提供的资料不真实；

2) 订户未履行本协议约定的义务；

3) 订户书面申请吊销数字证书；

4) 证书的安全性不能得到保证；

5) 法律、行政法规规定的其他情况。

8、 根据《电子签名法》的规定，订户依据 CFCA 提供的认证服务进行民事活动遭受损失，CFCA 将依据本协议的相关条款给予赔偿，除非 CFCA 能够证明其提供的服务是按照《电子签名法》、《电子认证服务管理办法》、CFCA 向主管部门备案的 CPS 和预植证书 CP 实施的。以下损失不在赔偿之列：

1) 任何直接或间接的利润或收入损失、信誉或商誉损害、任何商机或契机损失、失去项目、或失去或无法使用任何数据、设备或软件；

2) 由上述损失相应生成或附带引起的损失或损害；

9、 CFCA 对预植的企业数字证书订户的赔偿上限为人民币伍拾万元整，即￥500,000.00 元。CFCA 对预植的个人数字证书订户的赔偿上限为人民币贰万元

整，即￥20,000.00 元。

二、 预植证书订户的权利和义务

1、 订户享受 CFCA 作为合法的第三方电子认证服务机构提供的数字证书服务。

2、 订户应遵循诚实、信用原则，申领预植证书时，应当提供真实、完整和准确的信息和资料，并在这些信息、资料发生改变时及时通知发证机构。如因订户故意或过失提供的资料不真实或资料改变后未及时通知，造成的损失由订户自己承担。

3、 订户须使用经合法途径获得的相关软件。

4、 订户应合法使用 CFCA 数字证书，并对使用数字证书的行为负责。

5、 订户应当妥善保管含有预植证书的 USBKey。如因故意或过失导致他人盗用、冒用预植证书时，订户应承担由此产生的责任。

6、 如订户使用的预植证书的 USBKey 丢失或密码泄漏，或者订户不希望继续使用数字证书，或者订户主体不存在，订户或法定权利人应当立即申请吊销该数字证书。

7、 订户应在发证机构或指定网站进行证书更换或展期。

三、 其他

1. 建议订户经常浏览 CFCA 网站，以便及时了解 CFCA 有关证书管理、CPS、预植证书 CP 和本协议变更公示等方面的信息。

2. CFCA 有权对本协议进行修订，修订后的本协议将公布于 CFCA 网站（www.cfca.com.cn）。如订户在公布修订的 1 个月后继续使用 CFCA 提供的数字证书服务，即表明同意接受此等修订的约束。如果订户不予接受本协议中的约束，

订户可以在上述期限内申请停止使用数字证书。

3. 因依据CFCA的电子认证服务而发生的争议,双方先协商解决(必要时CFCA将召集业内专家组成专家小组，详细流程参见CPS的相关条款），双方不能达成一致意见的，将提交北京仲裁委员会申请仲裁。

中金金融认证中心有限公司（中国金融认证中心）

附件 2：

中国金融认证中心数字证书收费标准

根据国家发展和改革委员会价格认证中心（发改价认证【2004】61 号）文件的规定，经过与合作银行的充分协商，CFCA 对合作银行网上银行数字证书的收费标准如下：

计费单位：人民币/年/张

证书名称	证书类型	合作银行收费标准	发改委认证标准
企业证书	企业高级证书	200	300
	企业普通证书	160	260
	企业非支付类证书	140	200
个人证书	个人高级证书	80	100
	个人普通证书	8	10

中金金融认证中心有限公司

预植证书收费标准:

收费标准（以下标准适用于一年内的预植总量）：

- 10000 支以内（包括 10000 支）： 5 元/支
- 10000—150000 支之间（包括 150000 支）： 3 元/支
- 150000—450000 支之间（包括 450000 支）： 1.5 元/支
- 450000 支以上:1 元/支

附件三：

预植证书 DN 标准

（V1.0）

中国金融认证中心

2011 年 11 月

第一条 预植证书是指由 CFCA 事先在 USBKey 等密钥容器中生成，由订户在注册机构处领用，且将其身份信息与证书的相关信息绑定、与应用系统关联后方可有效使用的证书。

第二条 本 DN 标准只适用于 CFCA 预植的证书类型。

第一章 DN 标准

第三条 DN 构成

DN 的具体内容依次由 CN、OU[2]、OU[1]、O、C 五部分组成。其中 CN 用来表示证书 ID，OU[2] 用来表示用户类型，OU[1] 用来表示业务类别，O 用来表示 CA 名称，C 用来表示国家。

第四条 各部分的具体内容按照如下规则进行定义：

（1） CN

CN 部分包括 16 个字符，由数字和字母组成，字母区分大小写：

前 6 位由各注册机构自行定义，可包括数字和字母，但不得重复；

后 9 位的首位用于区分证书类型，若为“9”开头则表示是企业证书，其余数字开头则表示是个人证书，后 8 位表示各注册机

构发放的证书数量，按照各注册机构发放证书的顺序，逐渐累加；

最后 1 位为随机产生的校验码。

示例：企业证书:CN=95561e9000001925

个人证书：CN=1001010000001923

（2） OU[2]

OU[2]部分，用来表示证书类型。详细命名规则如下表：

	个人 普通证书	个人 高级证书	企业 普通证书	企业高级证书
OU=	Customers	Business Customers	Enterprises	Units

注：代表证书类型中的每个英文单词，第一个字母大写，其余小写。

（3） OU[1]

OU[1]部分用来表示此证书为预植证书的类型，具体表示为：

OU[1]＝yuzhi

（4） O

O 部分：用来表示 CA 系统的英文简称，目前已全部为国产 CA 系统发放的证书，表示为：

O=CFCA Operation CA2

（5） C

C 部分用来表示中国的英文简称，全部大写。

C=CN

（6） 示例

一个完整的证书 DN 示例为：

CN=95561e9000001925,

OU[2]＝Enterprises

OU[1]＝yuzhi

O=CFCA Operation CA2

C=CN

第五条 CN 的自定义部分(前 6 位)先由注册机构提交命名申请，标明字符全名称（数字、大小写英文字符串均可，但不能与其它 RA 机构的自定义内容重复），CFCA 批准使用后备案。

第二章 附则

第六条 本办法由业务部解释或修订。

第七条 本办法从颁发之日起施行。

附件四：

中金金融认证中心有限公司

预植证书注册机构运营规范

第一章　　总　　则

第一条　为了加强预植证书注册机构运营的规范化，降低电子认证服务的业务风险，结合注册机构的实际情况，制定本规范。

第二条　预植证书是指由 CFCA 按照一定的规则定义证书 DN 后，预先在安全的存储介质（如 USBKey）中生成私钥并植入的数字证书；订户申领该证书时，注册证机构须对订户的身份进行审核，将证书的 DN 信息与订户的身份信息绑定，并与应用系统进行关联。当预植证书与订户身份信息的绑定信息经注册机构和 CFCA 数字签名确认后，该预植证书方可生效。

第三条　本规定适用于发放预植证书的注册机构，CFCA 依照本规定对注册机构的运营管理进行监督和指导。

第二章　预植前置机系统规范

第四条　系统建设流程管理

在预植证书业务当中，注册机构需要部署预植前置机系统。前置机系统可由 CFCA 部署，也可由其它方进行部署。若前置机系统非由 CFCA 部署,其设计方案须预先提交 CFCA 进行评测,经 CFCA 书面认可后方可实施，建设完成后须由 CFCA 进行测试验收。

第五条 机房建设要求及管理

放置前置机系统的机房应避开易发生火灾的区域，应避开有害气体以及存放腐蚀、易燃、易爆物品的地方，应避开低洼、潮湿、落雷区域和地震频繁的地方，应避开强振动源和强噪音源，做到防水、防静电、防雷击、防电磁辐射。应提供稳定可靠的电源，应设置火灾报警装置，配备灭火器等消防设施。

在条件允许的情况下，注册机构应为放置前置机系统的机房制定人员访问控制的管理规定，并使用专门的门禁系统来实现对人员访问的控制，对进出机房的非工作人员进行登记；机房内应有录像监控系统，实时记录机房内所有人员的工作情况，登记记录和录像应由专人保管，保存期限不少于三个月。

第六条 网络系统建设要求

前置机系统的内部局域网应划分子网，每台主机使用局域网的 IP 地址，不同子网间应使用防火墙隔离并应用访问控制策略；

局域网内应安装有网络入侵检测系统和防病毒软件，对来自外部的恶意攻击能够及时采取措施。

第七条 系统改动要求

如果注册机构根据自身需要，对前置机系统或其他涉及数字证书使用的软件、流程进行改造或变动时，需要提前书面通知CFCA，并在安全方案上经过CFCA的确认。

第八条 系统功能要求

前置机系统应实现证书管理的基本功能,具体包括查询、绑定、解绑定、补发、换发、重发两码、差错同步、制证、证书吊销等功能。

第九条 系统日志管理

前置机系统应当采取标准的日志记录方式,日志应每天备份，每年对日志进行归档保存，归档日志应至少保存五年。

第十条 证书管理

对于在前置机系统中需要用到的证书（如通讯证书或Webserver证书），注册机构应当按照CFCA的要求提供相应的申请材料进行申请，并须对证书进行妥善保管，防止丢失或未授权的使用。

第三章　注册机构业务流程规范

第十一条 注册机构应为每种类型的证书业务申请制订专门的申请表格，表中应包含订户的信息及订户应遵守的规定。订户申请表内至少要记载下述内容作为用户声明：“我方已经认真阅读并同意接受《CFCA 预植数字证书服务协议》、《CFCA 电子认证业务规则（简称 CPS）》、《CFCA 预植证书策略（CP1）》（以上文件公布在 http://www.cfca.com.cn 上），同意这些文件内容构成我方与中金金融认证中心有限公司（简称 CFCA）之间的权利义务约定”，并要求用户签字确认。

第十二条 注册机构除了要求订户填写申请表外，还必须要求订户提供资质证明材料。个人证书申请人须提供能够证明其身份的有效证件，企业证书申请人须提供经办人和机构的有效证件、机构授予经办人的授权书。

第十三条 注册机构对订户提供的申请材料进行查验后，将订户信息录入至数据库中，并将订户信息与预植证书信息进行绑定，与应用系统进行关联后，方可将预植证书发放给订户。

第十四条 注册机构须将绑定和关联后的信息进行数字签名后，通

过与 CFCA 建立的安全通道发送至 CFCA。

第十五条 注册机构应制订合理的业务流程，确保在预植证书发放给订户之前，对预植证书进行妥善保管，并确保在未与订户身份信息进行绑定之前不会被订户使用。

第十六条 注册机构应在合理的时间内完成证书申请处理。在申请者提交资料齐全且符合要求的情况下，处理证书申请的时间不超过 5 个工作日。

第十七条 注册机构须对订户的信息及与认证相关的信息妥善保存，保存期限为数字证书失效后五年。

第十八条 注册机构应使订户明确地知道关于使用预植数字证书的意义、数字证书的功能、使用范围、使用方式、密钥管理以及丢失数字证书的后果和处理措施、法律责任限制。

第四章　注册机构监管规范

第十九条 CFCA 有权对注册机构的业务流程进行不定期抽查，抽查的内容包括 RA 系统的建设是否合规，机房环境是否符合要求，是否制订了相应的业务流程制度及证书保管制度，证书申请材料是否齐全，注册机构工作人员是否严格按照规章制度进行操作等。

第二十条 对于不符合规范的行为，CFCA 将以书面的方式向注册机构提出。注册机构管理人员需及时核实情况，对 CFCA 的意见进行书面确认，并对存在的问题进行限期整改。

第五章 附　　则

第二十一条 本规范如有未尽事宜，由 CFCA 补充或修改。

第二十二条 本规范自发文之日起实行。