证书应用开发指导书

1 文档介绍.....3
1.1 术语与缩写解释.....3
1.1.1 PKI 简介.....3
1.1.2 数字证书.....3
1.1.3 数字证书认证中心（CA： Certificate Authority）.....4
1.1.4 注册机构（RA：Registration Authority）.....4
1.1.5 CRL（Certificate Revocation List，证书撤销列表）.....4
1.1.6 SSL（Secure socket Layer）安全套接层协议.....4
1.1.7 加密.....5
1.1.8 数字签名.....5
1.1.9 常用术语与缩写解释列表.....5
2 常见项目需求.....7
2.1 对身份认证和访问控制的需求.....7
2.2 对数据传输安全性的需求.....8
2.3 对数据完整性的需求.....8
2.4 对交易抗抵赖性的需求.....8
2.5 小结.....8
3 采用数字证书技术的安全解决方案.....9
3.1 证书业务的办理.....9
3.2 身份验证与信息加密传输.....9
3.3 权限控制.....10
3.4 交易的完整性与不可抵赖性.....10
3.5 数据的授权获得.....10
4 证书应用系统开发指南.....11
4.1 了解 CFCA《电子认证业务规则》.....11
4.2 应用系统的身份认证.....11
4.3 应用系统进行电子签名的交易范围.....12
4.4 应用系统中电子签名及验证流程.....12
4.5 应用系统的签名数据保存.....13
4.6 应用系统中进行数据加密的交易范围.....14
4.7 应用系统中数据加解密的流程.....15
参考文档.....17

1. 文档介绍

为了更全面的发挥证书在应用系统的作用，帮助应用系统开发商更严谨的实现证书应用，CFCA 特意编写此文档，供应用系统建设单位参考。

读者对象：应用数字证书技术满足应用系统的应用安全需求的业务及系统设计人员。

1.1 术语与缩写解释

1.1.1 PKI 简介

PKI（Pubic Key Infrastructure）是遵循一系列标准的利用公钥加密技术为基础的一整套安全基础设施的通称。

PKI 必须具有权威认证机构CA 在公钥加密技术基础上对证书的产生、管理、存档、发放以及作废进行管理的功能，包括实现这些功能的全部硬件、软件、人力资源、相关政策和操作程序，以及为 PKI 体系中的各成员提供全部的安全服务。如：实现通信中各实体的身份认证、保证数据的完整、抗否认性和信息保密等。

1.1.2 数字证书

数字证书是各类实体(持卡人/个人、商户/企业、网关/银行等)在网上进行信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方证书的有效性，从而解决相互间的信任问题。简单的说，数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性，证书格式及证书内容遵循 X.509 标准。

从证书的一般用途来看，数字证书可分为签名证书和加密证书。签名证书主要用于对用户信息进行签名，以保证信息的不可否认性；加密证书主要用于对用户传送信息进行加密，以保证信息的真实性和完整性。

1.1.3 数字证书认证中心（CA： Certificate Authority）

数字证书认证中心（Certficate Authority，CA）是整个网上电子交易安全的关键环节。它主要负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认为是安全、权威、足以信赖的机构——根认证中心（根 CA）。

1.1.4 注册机构（RA：Registration Authority）

注册机构是负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和 CA 之间传递证书管理信息。

1.1.5 CRL（Certificate Revocation List，证书撤销列表）

认证机构 CA 签发证书来为用户的身份和公钥进行捆绑，构成了 PKI 证书应用的基础，但在现实物理世界中，因种种原因，还必须存在一种机制来撤销这种捆绑关系，将现行的证书撤销。撤销的原因通常有：用户身份姓名的改变、私钥被窃或泄漏、用户与其所属企业关系变更等，这样就必须存在一种方法警告其他用户不要再使用这个公钥。

证书撤销列表(Certificate Revocation List，简称 CRL)，是一种包含撤销的证书列表的签名数据结构。CRL 是证书撤销状态的公布形式，CRL 就像信用卡的黑名单，它通知大家某些电子证书不再有效。

注意：CA 向目录发布 CRL 是有一定的时间间隔的。通过 RA 撤销的证书，需要隔一段时间才会在目录服务器的 CRL 中发布。具体的发布策略请参看 CFCA 网站上的《电子认证业务规则》。

1.1.6 SSL（Secure socket Layer）安全套接层协议

SSL 安全套接层协议主要是使用公开密钥体制和 X.509 数字证书技术保护信息传输的机密性和完整性，它不能保证信息的不可抵赖性，主要适用于点对点

之间的信息传输，常用 Web Server 方式。

安全套接层协议是网景（Netscape）公司提出的基于 WEB 应用的安全协议，它包括：服务器认证、客户认证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。使用 SSL 可保证信息的真实性、完整性和保密性。但由于 SSL 不对应用层的消息进行数字签名，因此不能提供不可否认性，这是 SSL 的不足。

1.1.7 加密

加密是指使用密码算法对数据作变换，使得只有密钥持有人才能恢复数据面貌，主要目的是防止信息的非授权泄漏。现代密码学的基本原则是：一切密码寓于密钥之中即算法公开，密钥保密。

1.1.8 数字签名

数字签名（亦称电子签名）是指用户用自己的私钥对原始数据的哈希摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，并通过与收到的原始数据产生的哈希摘要对照，便可确信原始信息是否被篡改。这样就保证了数据传输的不可否认性。

1.1.9 常用术语与缩写解释列表

缩写、术语	解 释
数字证书（Certificate）	数字证书也称电子证书（以下简称证书），是一种由特定机构（CA）数字签名的、包含公开密钥以及公开密钥拥有者信息的电子文档。如同现实生活中公安机关颁发的居民身 份证一样，数字证书是网络环境中的一种身份证，用于证明某一实体（如人、服务器等）的身份。
CA 中心（Certificate Authority）	CA 是采用公开密钥基础技术，专门提供网络身份认证服务，负责签发和管理数字证书， 且具有权威性和公正性的第三方信任机构。CA即Certificate Authority，是PKI体系的核心组成部分，业界通称为认证中心。

公钥基础设施 PKI(Pubic Key Infrastructure)	是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。PKI 的核心组成部分 CA(Certification Authority)，即认证中心，它是数字证书的签发机构。数字证书，有时被称为数字身份证，是一个符合一定格式的电子文件，用来识别电子证书持有者的真实身份。
中国金融认证中心 (China Financial Certification Authority)	中国金融认证中心（China Financial Certification Authority，英文简称CFCA）于2000 年 6 月 29 日正式挂牌成立，是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，是重要的国家金融信息安全基础设施之一，CFCA作为权威、公正的第三方安全认证机构，通过发放数字证书为网上银行、电子商务、电子政务提供 安全认证服务：确保网上信息传递双方身份的真实性、信息的保密性和完整性、以及网上交易的不可否认性。
RA (Registration Authority)注册机构	注册机构是负责订户证书的申请受理、审批和管理，直接面向证书订户，并负责在订户和CA之间传递证书管理信息。
公钥和私钥	根据非对称密码学的原理，每个数字证书持有人都持有一对密钥，即公钥（Public Key）和私钥（Private Key）公钥与私钥作数据的互为加解密使用。公钥通常以数字证书的形式公开发布，私钥由证书持有者在本地生成，只能由证书持有者秘密掌握，证书持有者应当妥善保管并注意保密，不能在网上传输。
数字签名	在进行数字签名过程中，发信者使用自己的私钥，通过非对称密码算法，对待发数据的数字摘要（哈希值）进行加密，从而得到一段信息称为数字签名（Sign）这就是签名的过程；
身份认证 (Authentication)	通常用以表示鉴别通讯双方的合法身份。
加密	加密是通过数学变换将明文转变成密文的过程，也就是对明文进行各种伪装从而使其真
(Encryption)	实内容完全隐藏的过程。加密的方法很多，主要是通过数学运算、位移、替换等方法来实现。解密是加密的逆过程，通过数学的方法将密文还原成明文。在加密解密过程中要使用密钥，只有密钥的持有人才能解密，恢复数据的原貌，从而保证了信息传输过程中的保密性。
数字信封	所谓数字信封就是信息发送端用接收端的公钥，将一个对称通信密钥进行加密，形成的 数据称为数字信封。此数字信封传送给接收端，只有指定的接收方才能用自己的私钥打 开数字信封，获取该对称密钥，于是，接收方可以用以解读传送来的密码通信信息。这 就好比在生活中，将一把钥匙装在信封中，邮寄给对方，对方收到信件后，将钥匙取出，用它打开保险箱的道理一样。

时间戳	又称数字时间戳，是由第三方提供的一种对可信时间标记的服务，通过该服务获得的时间戳数据可以用来证明在某一时刻数据已经存在。数字签名配合时间戳服务，能更好地支持数据的抗抵赖。
证书吊销列表(Certificate Revocation List，CRL)	是一种包含吊销的证书列表的签名数据结构。CRL 是证书吊销状态的公布形式，CRL 就像信用卡的黑名单，它通知其他证书订户某些电子证书不再有效。
目录和 LDAP (Lightweight Directory Access Protocol)	目录系统是 CA 的证书发布和查询系统，是一个公共证书库。CA 为用户颁发证书之后， 要将用户证书发布到目录服务器，供其他用户查询和使用。 关于目录服务的国际标准是 X500 协议。但由于这一标准过于庞大，又发明了它的一个子集，即轻量级目录访问协议（Light Directory Access Protocol, LDAP）
唯一甄别名(Distinguished Name, DN)	在数字证书的主体名称域中，用来唯一标识证书用户的名称，体现用户的唯一性。例如可以用户名、证书类型、RA名称、CA名称以及国家名称等的一定规则的组合作为 DN 来标识一位证书用户。
《中华人民共和国电子签名法》	《中华人民共和国电子签名法》于 2004 年 8 月 28 日第十届全国人民代表大会常务委员会第十一次会议审议并通过，自 2005 年 4 月 1 日起施行。共计五章三十六条。该法通过确立电子签名的法律效力、规范电子签名行为、维护有关各方合法权益，在法律制度上保障了电子交易安全。
PKCS#1	PKCS#1 定义了 RSA 公钥函数的基本格式标准，特别是数字签名。它定义了数字签名如何计算，包括待签名数据和签名本身的格式；它也定义了 RSA公/私钥的语法。
PKCS#7	密码消息语法标准。PKCS#7 为使用密码算法的数据规定了通用语法，比如数字签名和数字信封。PKCS#7 提供了许多格式选项，包括未加密或签名的格式化消息、已封装（加密）消息、已签名消息和既经过签名又经过加密的消息。

2 常见项目需求

在对安全性有较高的要求的网上应用系统建设中，不仅使用防火墙、入侵检测软件等方法来保障网络安全，而且对于网上交易过程中的身份认证、交易的私密性、交易数据完整性、交易的抗抵赖性等应用安全方面也提出了安全保障需求。这四项需求可具体描述为：

2.1 对身份认证和访问控制的需求

一般的网络服务器只提供用户匿名访问，但网上应用系统需要确认用户的身

份.因为只有确认了用户的身份才能开放相应的权限和提供针对个人的服务，并能够有效的防止非法用户的侵入。

对于用户身份认证常见的解决方法是采用口令的方式。这种方式简便易行但是存在着诸多的隐患，首先口令容易被黑客以各种方式截获，其次口令也很容易猜测；一旦口令泄密，所有安全机制即失效。

身份认证是访问控制的基础，只有确认了用户的身份，才能为其分配相应的权限。

2.2 对数据传输安全性的需求

网上应用系统用户通过拨号访问应用服务器，双方的数据交互必然发生在 Internet 上，TCP/IP 协议的开放性造成在 Internet 上的信息是处于明文状态的。为了弥补这个安全漏洞有必要对通信通道进行加密保护。

传统的方式是建设一条通信专线在其上运行通信双方约定的加密算法来达到保护通信信道的目的，这种方式存在几方面的缺点：首先需要占用一条专用通信信道，所以费用昂贵；其次配置方式不灵活只能保障固定的几个通信节点的安全；最重要的是不能满足数量众多的网上应用系统用户通过公开网络进行加密通信的要求。

2.3 对数据完整性的需求

网上应用系统交易数据在公网上传输，虽然通过加密能够保证交易数据不被窃取，但还不能有效防止黑客的恶意篡改。为了保证交易的数据的完整性，有必要对用户帐号、交易金额等关键数据进行完整性处理，防止数据被篡改。

2.4 对交易抗抵赖性的需求

不可抵赖性是指指令发出者不能在事后抵赖曾经发出该指令。这对于规范业务，避免法律纠纷起着很大的作用。在网上应用系统中，保证关键交易的不可抵赖性是非常重要的。

2.5 小结

总之，要达到上述应用中的安全性的要求，需要在网上应用系统中采用 PKI 的数字证书技术来实现。作为普适性的安全应用基础设施，PKI 的证书机制提供

了与具体应用结合的接口，方便与各种应用结合。

3 采用数字证书技术的安全解决方案

3.1 证书业务的办理

首先网上应用系统要采用数字证书技术解决应用系统的应用安全需求，必要的条件就是必须为系统的用户或者服务器申领数字证书。数字证书的用户可以通过 CFCA 的注册机构的受理点（或网站）办理证书申请审核手续；注册机构对提交证书申请的用户信息进行审核，对于符合条件的用户，将从 CA 申请的数字证书发放给该用户。

3.2 身份验证与信息加密传输

只有持有合法的有效的数字证书的用户才能登录网上应用系统，没有证书的用户即使知道用户 ID（帐户名）和口令也无法登录系统。同时，在用户使用数字证书进行登录的过程中，系统可以自动获取数字证书中的 DN 信息，此DN 信息与用户在网上应用系统的帐户信息一一对应，这样就可以实现身份验证与用户的 权限控制的双重功能。即对应的用户登录后，就可以进行网上应用系统的操作了。

在此过程中，CFCA 安全代理网关（或其它厂商的 SSL 软硬件设备）会在用户使用数字证书登录网站的过程中，进行双方正式交易以前的证书有效性检查和密钥协商阶段，我们可以把这个过程称为服务器与用户客户端的“握手”过程，在握手的过程中，交易双方都要对对方身份的真实性进行检查。如果用户身份不可信或用户身份有问题（例如证书在 CRL 列表中或证书有效期已过）则不能通过用户身份的校验。只有具有数字证书，并且通过基于数字证书身份校验的用户， 才能进入网上应用系统。

同时在握手的过程中，双方会通过一系列的安全认证的机制和协商加密的算法，建立信息安全传输的加密通道。用户端和系统服务器之间就建立起了一条安全的信息通道。双方可以放心的在这条通道上相互传输交易数据。而不必担心信息被除交易双方的第三方窃取或篡改。用户可以放心的在此系统上进行各类

操作。

3.3 权限控制

首先，网上应用系统应为其合法用户开通帐户并绑定证书 DN（甚至证书序列号），用户只能使用指定帐户配合指定的有效证书进行网上应用系统的登录。应用系统也可以直接将网站的帐户名作为 CFCA 数字证书 DN 的自定义域的内容（有关 DN 的构成见 CFCA DN 标准文档）。这样用户在证书登录电子商务项目应用系统中，服务器可以实现获得 DN 并从中提取出帐户名，显示在登录页面上，以便取消用户输入帐户名的工作。

3.4 交易的完整性与不可抵赖性

当然，在交易中，还有非常重要的一个环节。就是在用户在进行涉及资金转移等重要交易时，需要留下类似于传统交易中纸质签名的交易“痕迹”。即需要有相应的技术手段确认操作确实由发起人完成，交易信息没有被修改，且不可抵赖。在交易中，我们可以采用数字签名的技术来实现网银交易的抗抵赖性。用户在进行操作时对于重要交易的确认信息进行数字签名。服务器端对用户的签名结果进行验证，证明内容有效后，进行后续的操作。签名后的结果被保存下来。在需要的时候，CFCA 作为公信的第三方，可以对数字签名的结果进行验证。任何

对于数字签名原文的微小的篡改都使签名结果完全不同，因此，我们可以很容易通过数字签名的校验，来判断信息的原文是否被篡改，该信息的原文是否由证书持有人签署。

3.5 数据的授权获得

通过证书的加解密应用，使得只有密钥持有人才能恢复数据面貌，主要目的是防止信息的非授权泄漏。即信息发送人使用信息接收人的数字证书（公钥证书）对数据进行加密，获得密文。只要信息接收人确保自己的私钥没有泄漏给其他人，信息发送人将密文以任何渠道发送给信息接收人都不用担心数据的泄漏。因为只有信息接收人的私钥才能从密文中通过解密操作恢复数据原文。其他没有私钥的人即使截获密文数据也无法从中恢复出原文。

4 证书应用系统开发指南

4.1 了解 CFCA《电子认证业务规则》

《电子认证业务规则（CPS，Certification Practice Statement）》是 CFCA 对全部数字证书服务生命周期中（如签发、吊销、更新证书）所应遵循规范的详细描述和声明，是对相关业务、技术和法律责任方面细节的描述。

CFCA 会根据业务的发展情况，对《电子认证业务规则》进行了修订，并向中华人民共和国工业与信息化部进行了备案，并在 CFCA 网站正式发布。

为了更好地了解 CFCA 数字证书生命周期管理地策略，满足应用系统的安全需求，应该阅读并理解 CFCA 的《电子认证业务规则》。

4.2 应用系统的身份认证

证书登录应用系统过程中，应该做如下内容的检查：

1、证书是否在有效期内。

2、证书是否是信任的 CA 签发的证书。

3、证书是否注销。

4、证书是否是应用系统指定账户对应的证书。

检查的方法有如下几种可供选择，可以组合应用：

1、建立 SSL 通道的软硬件通常可以做前三项检查。

对于使用软件或硬件实现的 SSL 双向登录的应用系统，建立 SSL 通道的软硬件通常都会默认包含前两项检查内容。而证书注销与否的检查默认是不启用的， 建议应用系统启用相关功能。检查证书注销与否的功能可能会分成 CRL 检查、OCSP 检查两种。两种的区别在于：

1)、CRL 检查，受制于 CRL 发布的时间间隔，不能在第一时间获得证书已经注销的信息。可以是每次检查连接 CFCA 目录，或者是通过本地 CRL 文件做检查； CFCA 发布的 CRL 文件有三种形式：完整 CRL 和分布点 CRL、分 OU CRL。

我们对检查证书注销的方式进行了归纳和比较：

	完整 CRL	分布点 CRL	分 OUCRL
下载协议	LDAP（不推荐）、HTTP	LDAP（不推荐）	HTTP
发布方式	定时发布	定时发布	定时发布
检查证书是否注销的推荐使用方式	由于完整 CRL 文件较大，建议根据 CFCA 的发布间隔定时下载，本地检查	在线查询	根据 CFCA 的发布间隔定时下载，本地检查

2、应用系统可以通过开发实现全部四项检查内容。

通常的证书应用工具包包含前三项检查的接口，供开发商直接调用。

第三项检查内容即使不通过证书应用工具包实现，配合应用系统本地建立的 RA 系统中记录证书序列号的状态信息，开发商自行开发实现。

第四项的检查内容是开发商自行开发实现的。建立 SSL 通道的软硬件支持将证书信息传送给后台应用系统。这些证书信息可能是证书 DN，或者是完整的数字证书编码，开发商可以通过直接获得证书 DN，或者是通过解析数字证书编码获得证书 DN，从而与后台应用数据库存储的账户信息进行比对，确认身份是否匹配。

4.3 应用系统进行电子签名的交易范围

建议所有涉及资金的流转的操作，或具有风险的操作都进行电子签名，以规避风险。比如：

1、转账交易。

2、报税交易。

3、授权交易。

4、投标操作。

4.4 应用系统中电子签名及验证流程

下面以 B/S 架构的应用系统进行电子签名，以及验证电子签名的流程为例

进行说明，其他应用模式可以参考。

一、客户端的电子签名：

1、客户端进行电子签名的时候建议使用包含签名密钥用法的证书；

2、客户端电子签名的数据格式，通常推荐选择 PKCS#7 标准作为数据格式。采用 PKCS#7 的数据格式，签名结果中包含签名证书，无需在验签的时候单独提供签名证书（公钥证书）。在应用系统对数据量的传输或者保存大小敏感的情况下，可以采用 PKCS#1 标准作为电子签名的格式，以减少电子签名的数据量。

3、客户端电子签名的原文内容。无论原文是否包含在签名数据中，要求签名的原文数据必须包含唯一的交易流水号，防止数据的重放攻击；建议签名原文具有可读性，能够从中清楚的看到谁在什么时间做了什么操作

以及具体的操作内容，防止客户对数据原文的不同理解而引起的异议。

二、服务器端对签名的校验

1、验证电子签名本身。

2、验证签名证书是否在有效期内。

3、验证签名证书是否是信任的 CA 签发的证书。

4、验证签名证书是否注销。

5、验证签名证书是否是应用系统指定账户对应的证书。

上述工作都需要开发商配合使用证书应用工具包自行开发实现。如果对签名时间很敏感的话，建议配合使用时间戳工具包开发实现。

只有服务器端验证电子签名的以上项目均通过后，才进行签名数据的保存，并进行后续的应用操作。如果验证电子签名的过程中发现问题，应该即时中止操作，提示客户端验证电子签名过程中发现的问题，要求客户端重新进行电子签名。

提示：如果电子签名数据中包含时间戳，应进行时间戳的有效性验证。

4.5 应用系统的签名数据保存

验证电子签名通过的签名数据必须妥善保存，以备将来发生纠纷的时候，作为有法律效力的电子证据。保证签名数据存储的完整性，检测到系统管理数据、鉴别信息和印章数据在存储过程中完整性受到破坏，并在检测到完整性错误时采

取必要的恢复措施。采用加密或其他保护措施实现鉴别信息的存储保密性。

关于签名数据的保存，应该注意：

1、保存时间：根据业务的情况确定，至少五年；

2、保存的形式：数据库和文件保存皆可；

3、保存的内容，取决于电子签名的数据格式：

a)PKCS#1 格式的签名，需要保存：PKCS#1 格式的签名数据、签名原文、签名证书。

b)PKCS#7 格式的分离式签名（不含签名的原文），需要保存：PKCS#7 格式的签名数据、签名原文。

c)PKCS#7 格式的非分离式签名（含签名的原文），需要保存：PKCS#7 格式的签名数据。

d)pdf 文件格式需要保存电子签名后的最终版 pdf 签名文件。

注意：保存签名原文的时候，一定不能做任何信息的改动（包括字符集的转码、编码转换等），否则会导致将来无法验证电子签名。

如果应用开发商不确认自己保存的电子签名内容，能否在 CFCA 完成验证工作，可以联系 CFCA 在应用系统上线之前，由 CFCA 根据《CFCA 证书签名验证技术规范》对应用系统中产生的电子签名数据进行验证。并且应用开发商签发证书前必须对订户进行身份鉴别，使用数字证书进行电子文件签署时需保留客户意愿性验证记录。

4.6 应用系统中进行数据加密的交易范围

所有希望他人授权查看的数据都可以进行数据加密，以确保只有指定人员才能查看到原文。比如：

1、标书。

2、对帐单。

3、保密文件。

4.7 应用系统中数据加解密的流程

1、确定哪些人（以下简称“接收方”）可以看到数据原文，则获取接受方的加密证书（公钥证书的密钥用法应该具有数据加密用法）。

2、检查接收方的加密证书的有效性：

a)检查证书的有效期，确保证书在接受方进行数据解密时依然有效。

b)证书是否是信任 CA 签发的。

c)证书注销与否。

d)证书是否属于接收方。

3、使用接收方的加密证书中的公钥对数据进行加密，获得密文；

4、发送密文给接收方；

5、接收方使用自己的私钥对密文进行解密，获得数据原文。

注意：

•考虑到证书是有有效期的，建议发送方不使用即将到期的证书做加密，建议接收方解密后做好原文的保存。

•需要长期保存的密文数据，建议应用系统在接收方使用 CFCA 高级证书用于数据加密。CFCA 高级证书采用双证书机制，其中一张证书是加密证书，根据国家密码管理局的要求，加密证书的私钥托管在 CFCA 的密钥管理中心，即使发生用户加密证书的私钥损坏的情况，用户也能够恢复自己的加密证书的私钥，从而恢复数据。

4.8 数字证书管理需要遵循的原则

如果应用系统中嵌入了证书管理功能，建议遵循如下原则：

1、请开发商阅读 CFCA 的《注册机构运营规范》，作为开发证书管理功能的业务指导文件。

2、严格按照 CFCA 的证书《DN 标准》进行证书的命名。

3、在系统中沿用 CFCA《电子认证业务规则》对证书管理功能的定义，不建议进行概念的转换。比如，证书换发就是颁发相同 DN 的、新截止日期的证书，而非其他概念。

4、如 RA 系统非 CFCA 建设，RA 系统上线前，由 CFCA 根据《注册机构运营规范》对 RA 系统进行验收工作。

5、注册机构的 RA 系统不管是否由 CFCA 建设，在上线运行一年以上，应接受 CFCA 根据《注册机构运营规范》对 RA 系统的运营进行 RA 审计。

注意：CFCA 的《DN 标准》、《注册机构运营规范》可以在与 CFCA 签订《数字证书合作协议》的同时获得。

4.9 证书到期提醒

由于证书是有有效期的，建议应用系统在用户登录成功后根据用户证书的截止日期情况，做到期提醒。通常在到期前的三个月内给用户提醒，告知用户及时进行证书换发，以及证书换发的手续或流程。

以上内容，是需要证书应用开发商注意的一些事项。建议证书应用开发商遵循 CFCA 官网最新版 CPS 开展证书管理服务，参考本文开展证书应用服务。

参考文档

1. 《DN 标准》

2. 《注册机构运营规范》

3. 《电子认证业务规则》

4. 《CFCA 证书签名验证技术规范》

5. 《电子签章产品产品及时要求》

6. 《电子签章应用规范》

7. 《安全电子签章密码技术规范》