云京国密电子印章系统需求文档

|  |  |  |
| --- | --- | --- |
| 编写 | 周鼎翔 | 2018年12月10日 |
| 审核 | 张东礼 | 2018年12月13日 |

|  |  |  |  |
| --- | --- | --- | --- |
| 版本 | 变更人 | 变更日期 | 变更项 |
| V1.0 | 周鼎翔 | 2018-12-10 | 创建 |
| V1.1 | 周鼎翔 | 2018-12-13 | 添加电子签章系统离线导入印章功能（8.2.4-P24）；添加电子签章数据文件属性字段可自定义的需求描述。（6.2.1-P7） |
|  |  |  |  |

目录

[1 背景说明 1](#_Toc532213580)

[2 相关标准 1](#_Toc532213581)

[3 术语和定义 1](#_Toc532213582)

[3.1 电子文件 electronic document 1](#_Toc532213586)

[3.2 电子印章 electronic stamp 1](#_Toc532213587)

[3.3 电子签章 electronic seal 1](#_Toc532213588)

[3.4 电子签章数据 electronic seal data 1](#_Toc532213589)

[3.5 电子印章系统 electronic seal system 1](#_Toc532213590)

[3.6 制章人 electronic stamp maker 1](#_Toc532213591)

[3.7 签章人 electronic seal signer 2](#_Toc532213592)

[3.8 SM2算法 SM2 algorithm 2](#_Toc532213593)

[3.9 SM3算法 SM3 algorithm 2](#_Toc532213594)

[4 系统结构 2](#_Toc532213595)

[5 应用部署 2](#_Toc532213596)

[6 数据格式 3](#_Toc532213597)

[6.1 电子印章 3](#_Toc532213598)

[6.1.1 印章信息 4](#_Toc532213599)

[6.1.2 印章签名信息 5](#_Toc532213600)

[6.2 电子签章 6](#_Toc532213601)

[6.2.1 电子签章数据格式 6](#_Toc532213602)

[7 业务流程 7](#_Toc532213603)

[7.1.1 电子签章生成流程 8](#_Toc532213604)

[7.1.2 电子印章验证流程 9](#_Toc532213605)

[7.1.3 电子签章验证流程 10](#_Toc532213606)

[8 功能模块设置 12](#_Toc532213607)

[8.1. 电子印章管理系统 12](#_Toc532213616)

[8.1.1. 初始化功能 13](#_Toc532213617)

[8.1.2. 登录验证功能 13](#_Toc532213618)

[8.1.3. 用户管理功能 14](#_Toc532213619)

[8.1.4. 印章管理功能 14](#_Toc532213620)

[8.1.4.1. 印章申请功能 14](#_Toc532213621)

[8.1.4.2. 申请审核功能 15](#_Toc532213622)

[8.1.4.3. 印章制作功能 16](#_Toc532213623)

[8.1.4.4. 印章更新功能 17](#_Toc532213624)

[8.1.4.5. 印章验证功能 18](#_Toc532213625)

[8.1.5. 连接配置功能 18](#_Toc532213626)

[8.1.5.1. CRL连接配置 18](#_Toc532213627)

[8.1.5.2. OCSP连接配置 18](#_Toc532213628)

[8.1.5.3. 电子签章服务器连接配置功能 19](#_Toc532213629)

[8.1.6. 证书管理功能 19](#_Toc532213630)

[8.1.6.1. 电子印章管理系统的密钥产生、证书申请 19](#_Toc532213631)

[8.1.6.2. 证书导入和存储 19](#_Toc532213632)

[8.1.6.3. 证书更新 19](#_Toc532213633)

[8.1.6.4. 证书验证 19](#_Toc532213634)

[8.1.7. 备份／恢复 20](#_Toc532213635)

[8.1.8. 访问控制功能 20](#_Toc532213636)

[8.1.9. 日志管理功能 20](#_Toc532213637)

[8.1.10. 系统自检功能 21](#_Toc532213638)

[8.1.11. NTP时间源同步功能 21](#_Toc532213639)

[8.2. 电子签章系统 21](#_Toc532213640)

[8.2.1. 初始化功能 22](#_Toc532213641)

[8.2.2. 登录验证功能 23](#_Toc532213642)

[8.2.3. 用户管理功能 23](#_Toc532213643)

[8.2.4. 印章管理功能 23](#_Toc532213644)

[8.2.4.1. 印章申请功能 24](#_Toc532213645)

[8.2.4.2. 印章更新功能 25](#_Toc532213646)

[8.2.4.3. 印章验证功能 25](#_Toc532213647)

[8.2.5. 连接配置功能 26](#_Toc532213648)

[8.2.5.1. CRL连接配置 26](#_Toc532213649)

[8.2.5.2. OCSP连接配置 26](#_Toc532213650)

[8.2.5.3. 电子印章中心连接配置功能 26](#_Toc532213651)

[8.2.6. 证书管理功能 26](#_Toc532213652)

[8.2.6.1. 电子签章系统的密钥产生、证书申请 26](#_Toc532213653)

[8.2.6.2. 证书导入和存储 27](#_Toc532213654)

[8.2.6.3. 证书更新 27](#_Toc532213655)

[8.2.6.4. 证书验证 27](#_Toc532213656)

[8.2.7. 应用注册功能 27](#_Toc532213657)

[8.2.8. 电子签章功能 28](#_Toc532213658)

[8.2.8.1. 电子签章数据制作 28](#_Toc532213659)

[8.2.8.2. 电子签章数据验证 28](#_Toc532213660)

[8.2.9. 备份／恢复 28](#_Toc532213661)

[8.2.10. 访问控制功能 29](#_Toc532213662)

[8.2.11. 日志管理功能 29](#_Toc532213663)

[8.2.12. 系统自检功能 29](#_Toc532213664)

[8.2.13. NTP时间源同步功能 29](#_Toc532213665)

[9 安全需求 29](#_Toc532213666)

[9.1. 密码设备 29](#_Toc532213668)

[9.2. 系统要求 30](#_Toc532213669)

[9.3. 使用要求 30](#_Toc532213670)

[9.4. 管理要求 30](#_Toc532213671)

[9.4.1. 管理工具 30](#_Toc532213672)

[9.4.2. 管理员管理 30](#_Toc532213673)

[9.4.3. 设备管理 30](#_Toc532213674)

[9.4.3.1. 设备初始化 30](#_Toc532213675)

[9.4.3.2. 设备自检 30](#_Toc532213676)

1. 背景说明

本文档主要用于按照国密相关要求研制电子印章系统对系统的功能需求进行设定，为国密电子印章系统研制开发提供需求标准。

1. 相关标准

本文档所参照的主要标准为：

GM/T0031-2014安全电子签章密码技术规范

GM/T0047-2016安全电子签章密码检测规范

1. 术语和定义

下列术语和定义适用于本文件。

3. 1. 电子文件 electronic document

在数字设备及环境中形成，以数码形式存储于磁带、磁盘、光盘等载体，依赖计算机等数字设备阅读、处理，并可在通信网络上传送的文件。本文中签章原文指电子文件。

* 1. 电子印章 electronic stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

* 1. 电子签章 electronic seal

使用电子印章签署电子文件的过程。

* 1. 电子签章数据 electronic seal data

电子签章过程产生的包含电子印章信息和签名信息的数据。

* 1. 电子印章系统 electronic seal system

包含电子印章管理系统和电子签章软件，其中电子印章管理系统包括印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。电子签章软件是使用电子印章对各类电子文件进行电子签章的软件。

* 1. 制章人 electronic stamp maker

电子印章系统中具有签署和管理电子印章信息权限的管理员。管理员的数字证书可以是单位证书或个人证书，电子印章中的图片和信息必须经制章人的数字证书进行数字签名。

* 1. 签章人 electronic seal signer

电子印章系统中对电子文件进行签章操作的签章持有用户。

* 1. SM2算法 SM2 algorithm

由GBlT 32918《信息安全技术 SM2椭网曲线公钥密码算法》定义的一种算法。

* 1. SM3算法 SM3 algorithm

由GB/T 32905《信息安全技术SM3密码杂凑算法》定义的一种算法。

1. 系统结构

电子印章系统包含电子印章管理系统和电子签章系统，其中电子印章管理系统包括印章管理员管理、电子印章制作与管理、电子印章验证服务以及安全审计等功能。电子签章系统是使用电子印章对各类电子文件进行电子签章的软件。电子印章系统硬件沿用V1.2系统硬件平台。电子印章系统结构如下图所示：



图5-1电子印章系统结构图

1. 应用部署

电子印章系统在实际应用部署时需要同应用系统和数字证书系统配合使用，电子签章系统与应用系统就近部署，用于为应用系统所需各类电子文档提供电子印章签章或验章服务，同时电子签章系统与电子印章管理系统相连为应用提供电子印章的申请、验章和存储服务，电子签章系统与CA中心数字证书系统相连用于获取证书CRL列表和OCSP服务验证制章人证书和签章人证书；电子印章管理系统可独立部署于印章中心，与电子签章系统相连用于响应电子签章系统的印章申请，负责电子印章系统的制章人证书管理和电子印章制作，与CA中心数字证书系统连接用于制章人证书申请和签章人的证书验证；CA中心数字证书系统为电子印章系统提供证书申请、更新、CRL列表下载和OCSP服务。电子印章系统应用部署图如下图所示：

图6-1电子印章系统应用部署图

1. 数据格式

按照国密标准要求电子印章系统主要数据对象包含电子印章数据和电子签章数据格式定义如下。

* 1. 电子印章



图1电子印章数据结构图

|  |  |
| --- | --- |
| 印章信息 | 签名信息 |

图4-1电子印章数据逻辑结构

电子印章数据的ASN.1定义为：

SESeal::=SEQUENCE{

esealInfo SES\_SealInfo，——印章信息

signInfo SES\_SignInfo——制章人对印章签名的信息

}

* + 1. 印章信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 头信息 | 印章标识 | 属性信息 | 印章图片信息 | 自定义数据 |

图4-2印章信息数据逻辑结构

印章信息的ASN.1定义为：

SES\_SealInfo::=SEQUENCE{

Header SES\_Header，——头信息

esID IA5String，——电子印章标识，电子印章数据的唯一标识编码

property SES\_ESPropertyInfo， ——印章属性信息

picture SES\_ESPictrueInfo，——电子印章图片数据

extDatas EXPLICIT ExtensionDatas OPTIONAL——自定义数据

}

其中：

esID:区分电子印章数据的唯一标识编码，用于查找和索引其他信息；

extDatas：用于厂商使用自定义数据。

ExtensionDatas::=SEQUENCE SIZE (O..MAX) OF ExtData

ExtData::=SEQUENCE{

extnID OBJECT IDENTIFIER，——自定义扩展字段标识

critical BOOLEAN DEFAULT FALSE，——自定义扩展字段是否关键

extnValue OCTET STRING——自定义扩展字段数据值

}

1. 印章头信息：

|  |  |  |
| --- | --- | --- |
| 标识 | 版本号 | 厂商ID |

图4-3印章头信息数据逻辑结构

印章头信息的ASN.1定义为：

SES\_Header::=SEQUENCE{

ID IA5 String．——电子印章数据标识

version INTEGER——电子印章数据版本号标识

VidIA5 String——电子印章厂商ID

}

其中：

ID:固定值“ES”；

Version：电子印章数据版本号，如“11”；

Vid:电子印章厂商ID，在互联互通时，用于识别不同的软件厂商实现。

1. 印章属性信息：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 印章类型 | 印章名称 | 签章人证书列表 | 制作日期 | 有效起始日期 | 有效终止日期 |

图4-4印章属性信息数据逻辑结构

印章属性信息的ASN.1定义为：

SES\_ESPropertyInfo::=SEQUENCE{

type INTEGER，——印章类型

name UTF8String，——印章名称

certList SEQUENCE OF cert，——签章人证书列表

createDate UTCTIME，——印章制作日期

validStart UTCTIME，——印章有效起始日期

validEnd UTCTIME——印章有效终止日期

}

certID::=IA5String

其中：

type：代表印章类型，如1为单位印章，2为个人印章；

name:印章的助记名称，如个人章、公章、财务章；

certList：可使用印章进行签章的签章人证书列表；

createDate:印章制作日期；

validStart：印章有效期起始时间；

validEnd:印章有效期终止时间。

1. 印章图片信息

|  |  |  |
| --- | --- | --- |
| 图片类型 | 图片数据 | 图片显示的宽度和高度 |

图4-5印章图片信息数据逻辑结构

印章图片信息的ASN.1定义为：

SES\_ESPictrueInfo::=SEQUENCE{

type IA5String，——图片类型

data OCTET STRING，——图片数据

width INTEGER，——图片显示宽度

height INTEGER——图片显示高度

}

萁中：

type：代表印章图片类型，如GIF、BMP、JPG;

data：印章图片数据；

width：图片显示宽度，单位为毫米(mm)；

height：图片显示高度，单位为毫米(mm)。

* + 1. 印章签名信息

|  |  |  |
| --- | --- | --- |
| 制章人证书 | 签名算法标识 | 签名值 |

图4-6印章签名信息数据逻辑结构

印章签名信息的ASN.1定义为：

SES\_SignInfo::=SEQUENCE{

cert OCTET STRING．——制章人签名证书

signatureAlgorithm OBJECT IDENTIFIER．——签名算法标识

signData BIT STRING——制章人的签名值

}

其中：

cert：代表对电子印章数据进行签名的制章人证书；

signatureAlgorithm：代表签名算法OID标识，遵循GM/T 0006。例如，使用SM2签名的OID为1.2.156.10197.1.501;

signData：代表制章人对电子印章格式中印章信息SES\_SealInfo、制章人证书、签名算法标识按SEQUENCE方式组成的信息内容的数字签名。

如果签名算法使用SM2，则遵循GM/T 0009；如果签名算法使用RSA，则遵循PKCS#1。

* 1. 电子签章

电子签章数据结构如下图所示：

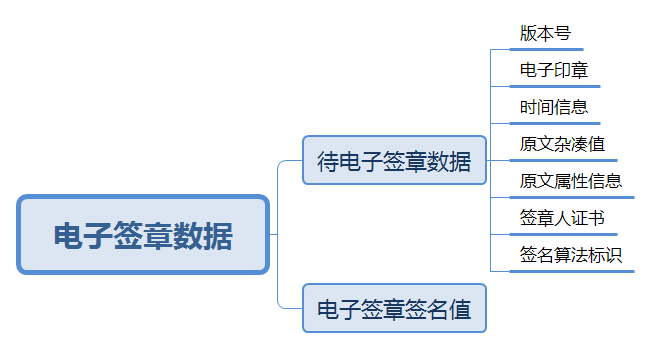


图4-7电子签章数据

* + 1. 电子签章数据格式

电子签章数据由版本号、电子印章、时间信息、原文杂凑值、原文属性信息、证书标识、签名算法标识及签名值等组成。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 版本号 | 电子印章 | 时间信息 | 原文杂凑值 | 原文属性信息 | 签章人数字证书 | 签名算法标识 | 签名值 |

图4-7电子签章数据信息数据逻辑结构

电子签章数据的ASN.1定义为：

SES\_Signature::=SEQUENCE{

toSign TBS\_Sign，——待电子签章数据

signature BIT STRING——电子签章中签名值

}

TBS\_Sign::=SEQUENCE{

version INTEGER，——版本信息

eseal SESeal，——电子印章

timeInfo BIT STRING，——签章时间信息

dataHash BIT STRING，——原文杂凑值

propertyInfo IA5String，——原文数据的属性信息

cert OCTET STRING．——签章人对应的签名证书

signatureAlgorithm OBJECT IDENTIFIER——签名算法标识

}

其中：

version:代表签章数据结构版本号；

eseal:代表生成电子签章使用的电子印章数据；

timeInfo：代表电子签章对应的时间信息，可以是时间戳，也可以是UTCTIME时间；

dataHash:代表待签名原文的杂凑值；

propertyInfo：代表原文数据的属性信息，如文档ID、日期、段落、原文内容的字节数、指示信息、签章保护范围等，此部分受签名保护，propertyInfo的具体含义可自行定义；本项目采用电子文档全签的方式进行操作。propertyInfo数据示例如下：“FILEID:0000000012345678;TIME:2018-12-13-20:00:45; RANGE:ALL;”

cert：代表执行本次签章操作的签章人数字证书；

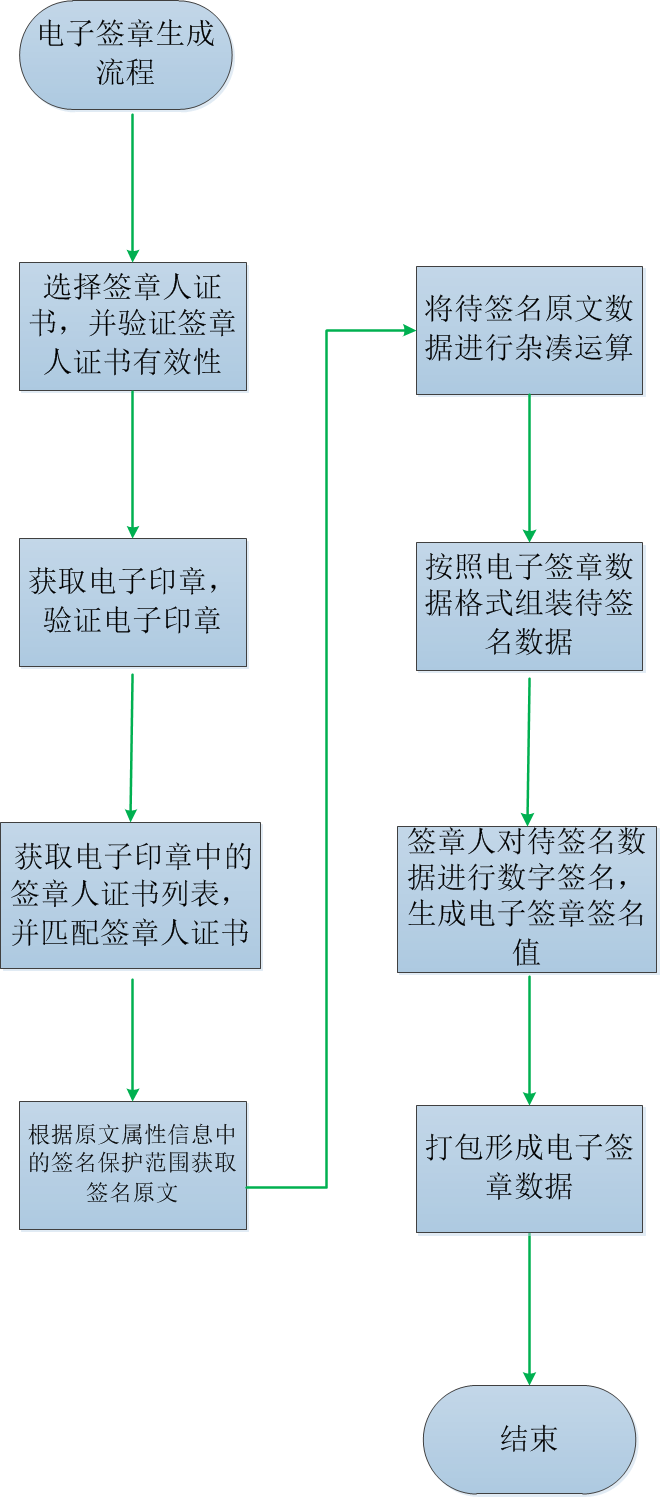
signatureAlgorithm：代表签名算法OID，遵循GM/T 0006。例如，使用SM2签名的OID为1.2.156.10197.1.501;

signature：代表签章人对电子签章数据格式中版本号、电子印章、时间信息，原文杂凑值、原文属性信息、证书、签名算法标识组成的待签章数据TBS\_Sign进行数字签名。

如果签名算法使用SM2，则遵循GMlT 0009；如果签名算法使用RSA，则遵循PKCS#1。

原文杂凑值所采用的杂凑算法应与电子签章签名算法保持一致，如果签名算法是SM2，则杂凑算法应采用SM3算法，遵循GM/T 0003；如果签名算法是RSA，则杂凑算法应采用SHA1或SHA256算法，具体参见相应的国际标准。

1. 业务流程
   * 1. 电子签章生成流程



电子签章生成流程如下：

a) 选择拟进行电子签章的签章人证书，并验证签章人证书有效性：

验证签章人证书有效性，验证项至少包括：证书信任链验证、证书有效期验证、证书是否被吊销、密钥用法是否正确。如果签章人证书验证失败，返回失败原因并退jLH生成流程。

b) 获取电子印章，按照6.1.2验证印章的合规性和有效性。

c) 获取电子印章中的签章人证书列表，使用步骤a）中的签章人证书逐一进行证书数据二进制比对，确认签章人证书是否在签章人证书列表中。

如果比对失败或证书不在列表当中，返回失败原因并退出生成流程。

如果是因为签章人证书执行更新、重签发等操作而导致证书比对失败，此时需要重新制作印章，并重新进行签章生成流程。

d) 按照propertyInfo信息中的签名保护范围获取待签名原文。

e) 将待签名原文数据进行杂凑运算，形成原文杂凑值。

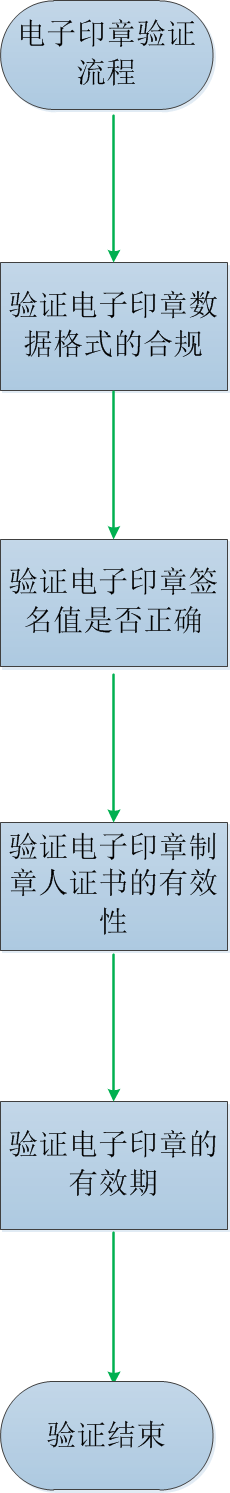
f) 按照电子签章数据格式组装待签名数据：

待签名数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识。

g) 签章人对待签名数据进行数字签名，生成电子签章签名值。

h) 按照电子签章数据格式，把以上数据打包形成电子签章数据。

* + 1. 电子印章验证流程



电子印章验证流程如下：

a) 验证电子印章数据格式的合规性：

按照电子印章格式，解析电子印章，验证是否是符合规范的电子印章格式；

如果电子印章数据格式不合规，则验证失败，返回失败原因并退出验证流程。

b) 验证电子印章签名值是否正确：

根据印章信息数据、制章人证书、签名算法标识验证电子印章签名信息中的签名值是否正确；

如果电子印章签名验证失败，返回失败原因并退出验证流程。

c) 验证电子印章制章人证书的有效性：

验证制章人证书的有效性，验证项至少包括：制章人证书信任链验证、制章人证书有效期验证、

制章人证书是否被吊销、密钥用法是否正确；

知果制章人证书验证失败，返回失败原因并退出验证流程。

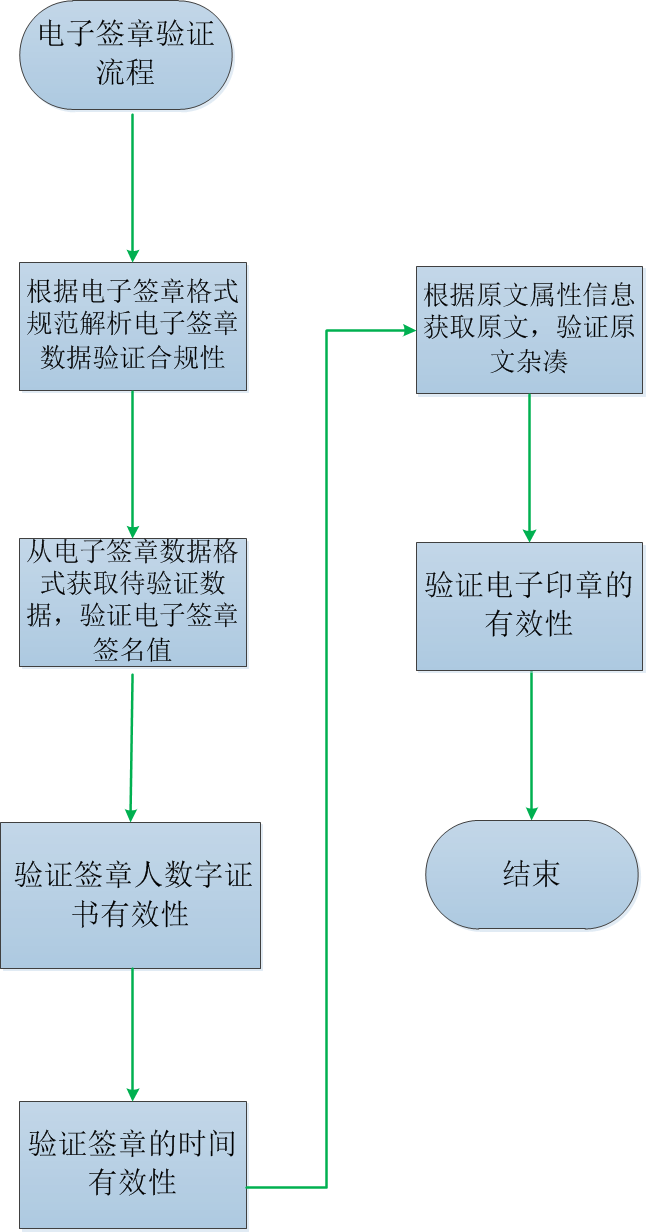
d) 验证电子印章的有效期：

根据印章属性中的印章有效起始日期和有效终止日期，验证电子印章的是否过期；

如果电子印章已过期，则验证失败，返回失败原因并退出验证流程；

e) 如果上述步骤都验证成功，则电子印章验证合规有效，可正常退出验证流程。

* + 1. 电子签章验证流程



电子签章验证流程如下：

a) 验证电子签章数据格式的合规性：

根据电子签章格式规范解析电子签章数据。如果电子签章或电子印章数据格式不合规，则验证失败并退出验证流程。

b) 验证电子签章签名值是否正确：

从电子签章数据格式获取待验证数据，待验证数据包括：版本号、电子印章、时间信息、原文杂凑值、原文属性信息、签章人证书、签名算法标识，验证电子签章签名值的是否正确。

如果签名值验证不正确则验证失败，并将失败原因返回上层应用并退出验证流程。

c) 验证签章人数字证书有效性：

从电子签章数据获得签章人数字证书，验证签章人证书有效性，验证项至少包括：证书信任链验证、证书有效期验证、证书是否被吊销、密钥用法是否正确。

如果是由于证书信任链验证或密钥用法不正确导致的签章人证书有效性验证失败，则返回失败原因并退出验证流程。

如果是由于证书有效期或证书状态已吊销导致的签章人证书有效性验证失败，则还需要进一步结合签章时间进行综合判定。

d) 验证签章的时间有效性：

根据签章人数字证书有效期和电子签章中的时间信息进行比对，判断签章的时间有效性：

1) 如果签章时间处于签章人数字证书有效期内，并且证书有效，则需要继续进一步验证。

2) 如果签章时间不在签章人数字证书有敦期内，则签章无效，验证失败，返回失败原因并退出验证流程。

3) 如果签章时间处于签章人数字证书有效期内，但是证书在签章之前已被吊销，则签章视为无效，验证失败，返回失败原因并退m验证流程。

4)如果签章时间处于签章人数字证书有效期内，但是证书在签章之后被吊销，则需要继续进一步验证。

e)验证原文杂凑：

1) 按照propertyInfo信息中的签名保护范围获取待验证原文；

2) 将待验证原文数据进行杂凑运算，形成待验证原文杂凑值；

3) 获取电子签章数据中的原文杂凑值，与待验证原文杂凑值进行二进制比对，如果比对失败，则电子签章验证失败，返回失败原因并退出验证流程。

f) 验证电子印章的有效性：

首先，获取电子印章，按照6.1.2验证印章的有效性。再根据电子签章中的时间信息验证签章的有效性。

如果签章时间不处于印章有效期内，则签章无效，验证失败，返回失败原因并退出验证流程。

g) 如果上述各步骤验证均有效，那么电子签章验证结果为有效，可正常退出验证流程。

1. 功能模块设置






9. 1. 电子印章管理系统

电子印章管理系统的主要功能模块包含：初始化功能、登录验证功能、用户管理功能、印章管理功能、连接配置功能、证书管理功能、备份恢复功能、访问控制功能、日志管理功能、系统自检功能、时间源同步功能等。



图8-1电子印章管理系统功能结构图

* + 1. 初始化功能

电子印章管理系统初始化功能主要包括系统配置、生成管理员、审计员等，使设备处于正常工作状态。





* + 1. 登录验证功能

电子印章管理系统需提供管理员和审计员的登录验证入口，支持管理员和审计员的系统登录。



* + 1. 用户管理功能

电子印章管理系统需具备用户管理功能，提供对系统管理员用户、审计员用户的账号添加、删除、修改和查找等管理功能。



* + 1. 印章管理功能

电子印章管理系统需具备印章管理功能，提供印章的申请审核、制作、更新、注销、查找和验证功能，支持电子印章的离线制作和签章服务器的电子印章在线申请。



* + - 1. 印章申请功能

电子印章管理系统需具备印章申请的录入功能，支持管理员的印章申请录入操作和电子签章系统的印章申请提交。



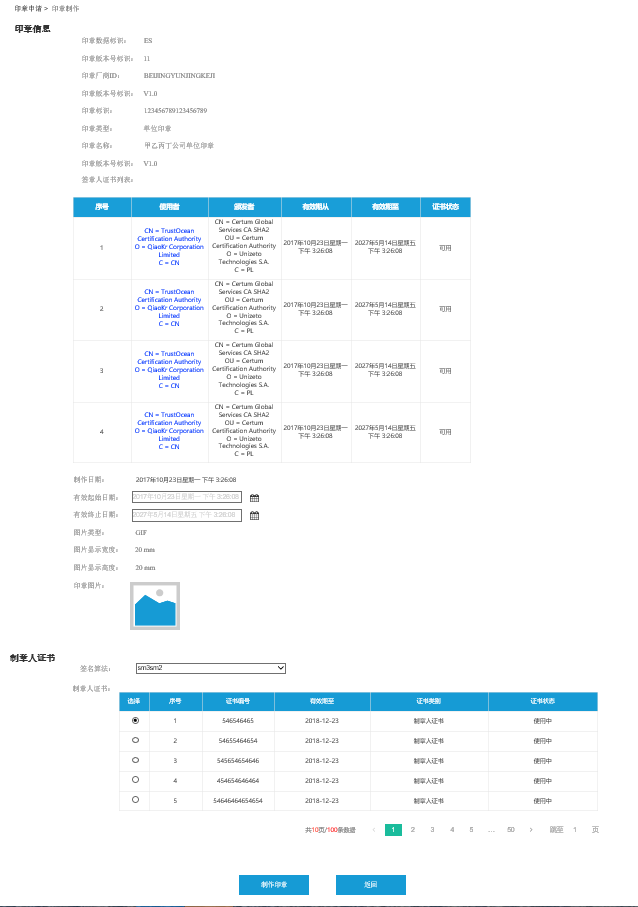
* + - 1. 申请审核功能

电子印章管理系统需具备印章申请的审核功能，所有印章申请必须审核通过才可制作印章，支持印章申请信息的录入、审核和记录存档。



* + - 1. 印章制作功能

电子印章管理系统需对通过审核的印章申请制作符合安全电子印章格式要求的电子印章，电子印章有效期不能超过制章人证书有效期，数据格式符合GM/T0031-2014安全电子签章密码技术规范。



* + - 1. 印章更新功能

电子印章管理系统需对印章有效期到期或印章信息变更的电子印章提供印章更新功能，印章更新需要审核印章信息，审核通过后按照新的有效期或印章信息制作符合安全电子印章格式要求的电子印章，更新后原有印章存档备查，印章数据格式符合GM/T0031-2014安全电子签章密码技术规范。



* + - 1. 印章验证功能

电子印章管理系统需对电子印章提供印章验证功能。验证时需对印章数据格式，印章图片，印章签名，印章证书列表进行验证。

* + 1. 连接配置功能

电子印章管理系统应支持与CA基础设施的连接功能，包括CRL连接配置、OCSP连接配置和电子签章系统连接配置等。



* + - 1. CRL连接配置

电子印章管理系统应支持CRL连接配置功能，通过配置管理界面，提供从CRL发布点获取CRL、导入CRL等功能。

* + - 1. OCSP连接配置

电子印章管理系统可支持OCSP连接配置功能，通过配置管理界面，进行OCSP服务的连接配置管理。OCSP连接配置应遵循GB/T 19713-2005。

* + - 1. 电子签章服务器连接配置功能

电子印章管理系统的签章服务器管理功能主要包括可以连接电子印章管理系统的电子印章签章系统的白名单配置管理，内容包括IP地址，登录TOKEN的管理配置。



* + 1. 证书管理功能

电子印章管理系统的证书包括制章人证书、签章人证书、电子签章系统证书、CA根证书或证书链应具有对证书的导入、存储、验证、使用以及备份和恢复等功能。



* + - 1. 电子印章管理系统的密钥产生、证书申请

电子印章管理系统应具备产生制章人的签名密钥对和证书请求，并支持通过管理界面录入相关证书申请信息。

* + - 1. 证书导入和存储

电子印章管理系统应支持签章人证书、电子签章系统证书、根证书或证书链的导入，导入时应对证书的有效性进行验证。

* + - 1. 证书更新

电子印章管理系统的证书更新时必须保存原来的证书，以防止以前的电子印章不能验证。

* + - 1. 证书验证

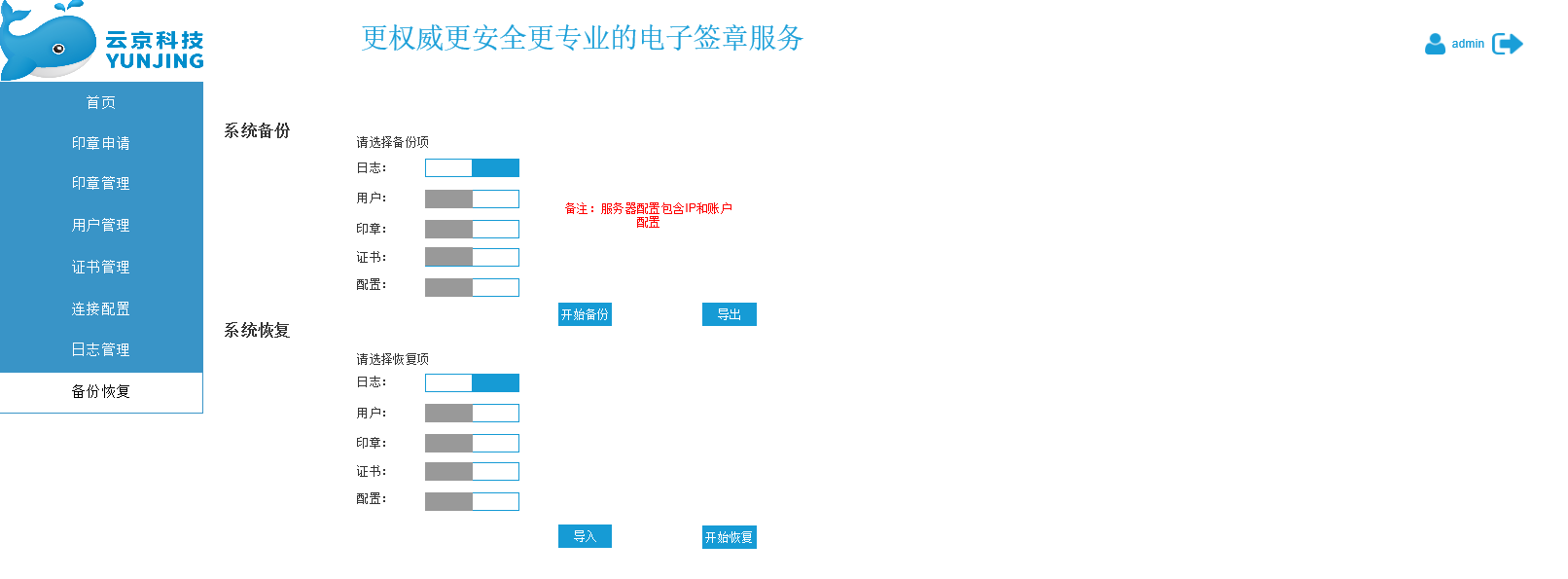
电子印章管理系统应支持对证书的有效性的验证，包括验证证书有效期、验证证书签名有效性、验证是否在CRL中。

* + 1. 备份／恢复

电子印章管理系统应支持备份／恢复功能，包括密钥的备份恢复和证书等数据的备份／恢复。

密钥的备份恢复应通过电子印章管理系统的管理界面实现。

数据的备份／恢复包括证书、配置参数等数据的备份／恢复。备份操作产生的备份文件可存储到电子印章管理系统外的存储介质中，应采取措施保证备份文件的完整性；备份文件可以恢复到电子印章管理系统中。



* + 1. 访问控制功能

电子印章管理系统的管理界面应具备完善的身份鉴别机制，实现管理员身份的鉴别，其中“口令”需要进行时效限制，超过时限，需强制修改密码。管理员登录成功后，通过管理界面进行印章管理、证书管理、系统配置以及日志查询等管理操作。



* + 1. 日志管理功能

电子印章管理系统应提供日志记录、查看、审计和导出功能，具备相应的配置管理和查看界面。日志内容分为系统管理日志、异常事件、系统服务日志等，包括登录认证、系统配置、密钥管理等操作，认证失败、非法访问等异常事件的记录，以及与CA中心连接，对相应操作进行记录，对应用接口的调用进行日志记录。



* + 1. 系统自检功能

电子印章管理系统应具备设备自检功能，包括自身自检和密码设备自检。电子印章管理系统使用的密码设备应具备状态和功能自检功能，能够进行密码算法正确性检查、随机数发生器检查、存储密钥和数据的完整性检查等。电子印章管理系统的自身自检包括密码功能检测、存储信息的完整性检查等。



* + 1. NTP时间源同步功能

电子印章管理系统能够配置时间源服务器，自动同步时间。



* 1. 电子签章系统

电子签章系统的主要功能模块包含：初始化功能、登录验证功能、用户管理功能、印章管理功能、连接配置功能、证书管理功能、应用注册功能、电子签章功能、备份恢复、访问控制功能。日志管理功能、系统自检功能、时间源同步功能等。



图8-2电子签章系统功能结构图

* + 1. 初始化功能

电子签章系统初始化功能主要包括系统配置、生成管理员、审计员等，使设备处于正常工作状态。





* + 1. 登录验证功能

电子签章系统需提供管理员和审计员的登录验证入口，支持管理员和审计员的系统登录。



* + 1. 用户管理功能

电子签章系统需具备用户管理功能，提供对系统管理员用户、审计员用户的账号添加、删除、修改和查找等管理功能。



* + 1. 印章管理功能

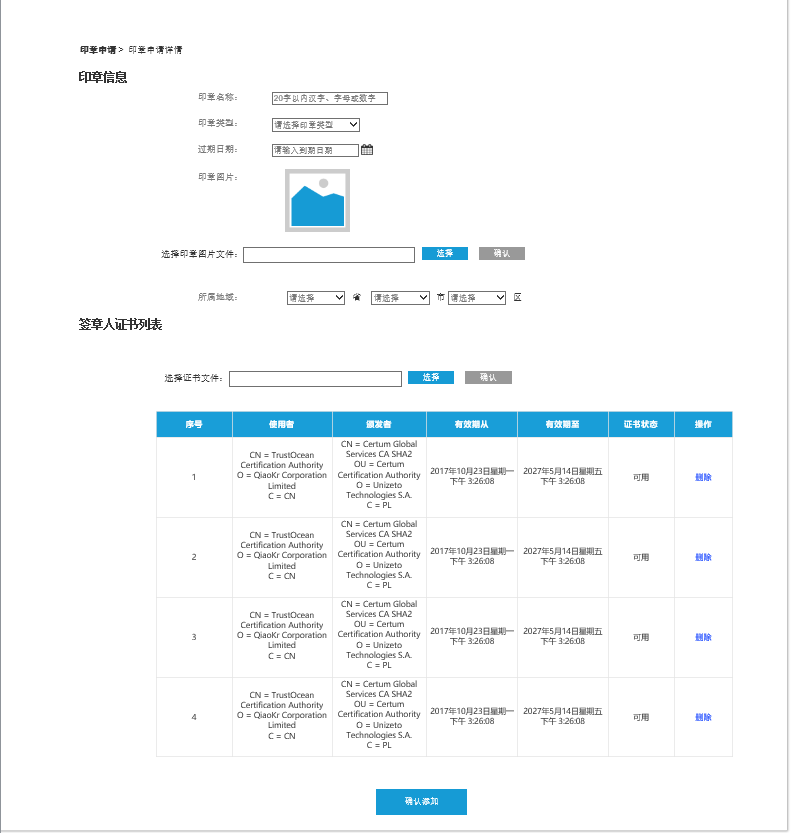
电子签章系统需具备印章管理功能，提供印章的申请、更新、注销、查找和验证功能，支持电子印章的离线申请制作、电子印章在线申请和电子印章导入功能。



* + - 1. 印章申请功能

电子签章系统需具备印章申请信息的录入功能，支持管理员的印章申请录入操作和电子签章系统的印章申请提交。





* + - 1. 印章更新功能

电子签章系统需对印章有效期到期或印章信息变更的电子印章提供印章更新功能，更新后原有印章存档备查。



* + - 1. 印章验证功能

电子签章系统需对电子印章提供印章验证功能。验证时需对印章数据格式，印章图片，印章签名，印章证书列表进行验证。

* + 1. 连接配置功能

电子印章管理系统应支持与CA基础设施的连接功能，包括CRL连接配置、OCSP连接配置和电子印章系统连接配置等。



* + - 1. CRL连接配置

电子签章系统应支持CRL连接配置功能，通过配置管理界面，提供从CRL发布点获取CRL、导入CRL等功能。

* + - 1. OCSP连接配置

电子签章系统可支持OCSP连接配置功能，通过配置管理界面，进行OCSP服务的连接配置管理。OCSP连接配置应遵循GB/T 19713-2005。

* + - 1. 电子印章中心连接配置功能

电子签章系统支持电子印章中心连接配置，包括IP地址配置，登录TOKEN的管理配置。



* + 1. 证书管理功能

电子签章系统的证书包括制签章人证书、电子签章系统证书、CA根证书或证书链应具有证书的导入、存储、验证、使用以及备份和恢复等功能。



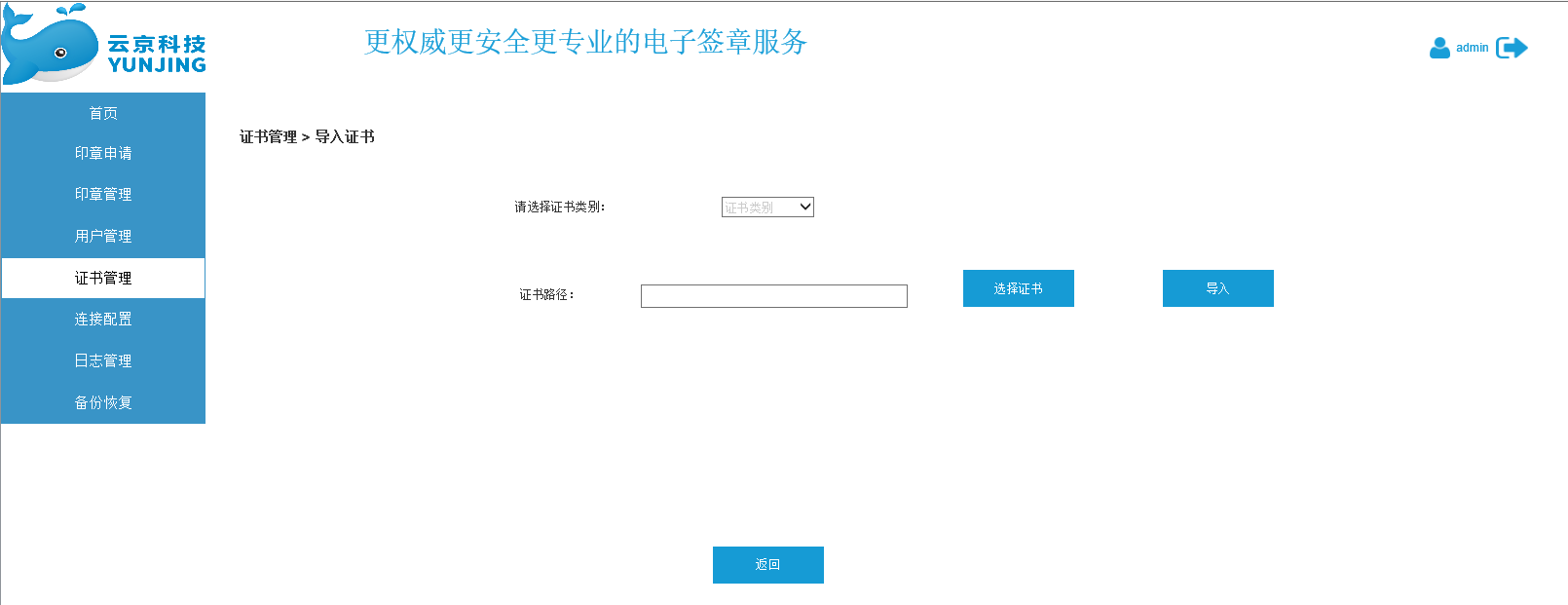
* + - 1. 电子签章系统的密钥产生、证书申请

电子签章系统应具备产生签章人签名密钥对和证书请求功能，并支持通过管理界面录入相关证书申请信息。



* + - 1. 证书导入和存储

电子签章系统应支持签章人证书、电子签章系统证书、根证书或证书链的导入，导入时应对证书的有效性进行验证。



* + - 1. 证书更新

电子签章系统的证书更新时必须保存原来的证书，以防止以前的电子印章不能验证。

* + - 1. 证书验证

电子签章系统应支持对证书的有效性的验证，包括验证证书有效期、验证证书签名有效性、验证是否在CRL中。

* + 1. 应用注册功能

电子签章系统应具有允许连接请求服务的应用白名单设置功能，包括应用实体的注册、设置应用实体名称、配置密钥索引号、配置应用证书、电子印章、导入证书、设置IP地址等。



* + 1. 电子签章功能
       1. 电子签章数据制作

电子签章系统应具备为应用提供电子签章数据制作功能，支持SM2算法的电子签章功能，提供对多种文档格式的PDF转换，签章数据制作及展现。

当签名验签服务器的公钥算法为SM2算法时，数据的结构遵循GM/T 0009、GM/T 0010和GM/T 0031。

* + - 1. 电子签章数据验证

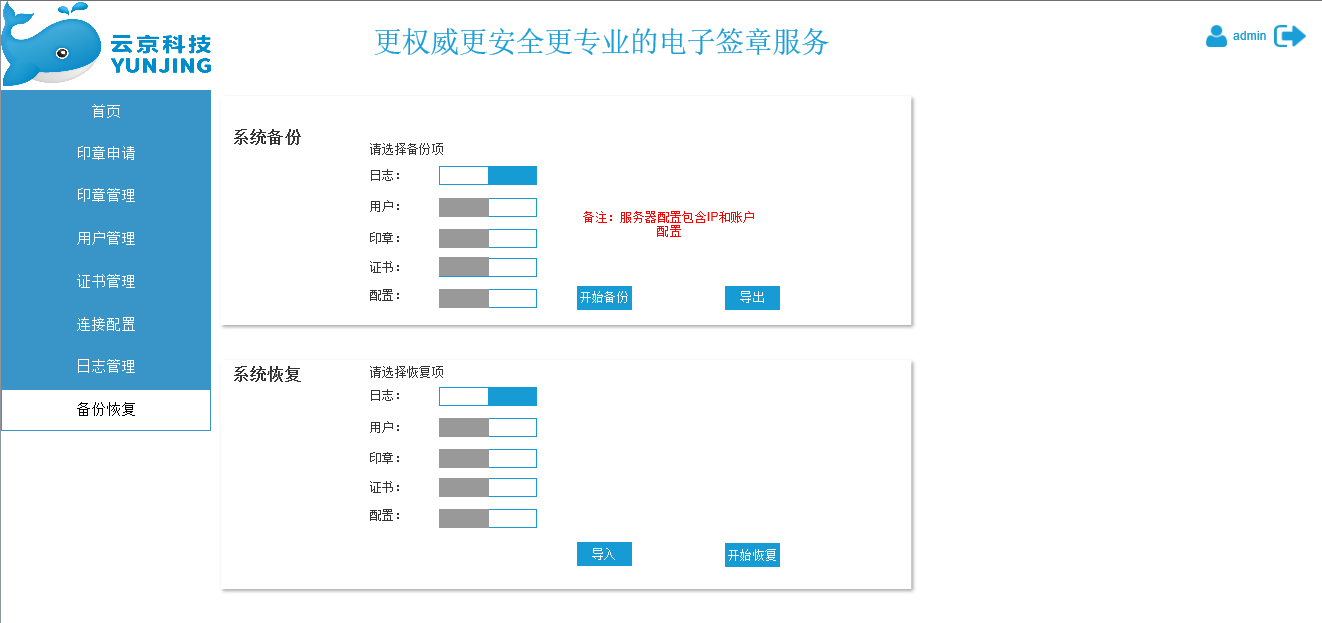
电子签章系统应具备为应用提供电子签章数据验证功能，支持符合国密GM/T 0031使用SM2算法的电子签章数据验证功能，验证电子签章数据时需验证电子印章有效性和签章人证书及签名有效性。

* + 1. 备份／恢复

电子签章系统应支持备份／恢复功能，包括密钥的备份恢复和证书等数据的备份／恢复。

密钥的备份恢复应通过电子签章系统的管理界面实现。

数据的备份／恢复包括证书、配置参数等数据的备份／恢复。备份操作产生的备份文件可存储到电子签章系统外的存储介质中，应采取措施保证备份文件的完整性；备份文件可以恢复到电子签章系统中。



* + 1. 访问控制功能

电子签章系统的管理界面应具备完善的身份鉴别机制，实现管理员身份的鉴别，其中“口令”需要进行时效限制，超过时限，需强制修改密码。管理员登录成功后，通过管理界面进行印章管理、证书管理、系统配置以及日志查询等管理操作。

* + 1. 日志管理功能

电子签章系统应提供日志记录、查看、审计和导出功能，具备相应的配置管理和查看界面。日志内容分为系统管理日志、异常事件、系统服务日志等，包括登录认证、系统配置、密钥管理等操作，认证失败、非法访问等异常事件的记录，以及与CA中心连接，对相应操作进行记录，对应用接口的调用进行日志记录。



* + 1. 系统自检功能

电子签章系统应具备设备自检功能，包括自身自检和密码设备自检。电子印章管理系统使用的密码设备应具备状态和功能自检功能，能够进行密码算法正确性检查、随机数发生器检查、存储密钥和数据的完整性检查等。电子印章管理系统的自身自检包括密码功能检测、存储信息的完整性检查等。



* + 1. NTP时间源同步功能

电子签章系统能够配置时间源服务器，自动同步时间。



1. 安全需求
2. 1. 密码设备

电子印章系统须使用国家密码管理主管部门审批的密码设备。调用密码设备的接口API应遵循GM/T 0018。

* 1. 系统要求

电子印章系统服务器所使用的操作系统应进行安全加固，裁减一切不需要的模块，关闭所有不需要的端口和服务。

* 1. 使用要求

电子印章系统只接受合法的操作指令，电子印章系统软件应采用模块化设计，应通过身份鉴别等技术措施防止用户的非法调用。

* 1. 管理要求
     1. 管理工具

电子印章系统通过管理工具实现对系统的管理功能。

* + 1. 管理员管理

电子印章系统应设置管理员和审计员，管理员和审计员的职责按照国家密码管理机构的要求进行管理。各类管理员通过身份鉴别后执行相关管理操作。

* + 1. 设备管理
       1. 设备初始化

电子印章系统的初始化，除必须由厂商进行的操作外，系统配置、密钥的生成（恢复）与安装、生成管理员和审计员等均应由用户方设备管理人员完成。

* + - 1. 设备自检

电子印章系统的自检包括密码设备的自检和自身的自检，对密码运算功能、随机数发生器和存储的敏感信息进行检查。在检查不通过时应报警并停止工作。