KT系统软件需求说明书

（版本：1.0）

中国金融认证中心

版权声明：本文档的版权属于中国金融认证中心，任何人或组织未经许可，不得擅自修改、拷贝或以其它方式使用本文档中的内容。

**文档修订记录**

*本文档会随时保持更新，请与中国金融认证中心索要最新版本。*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **内容** | **日期** | **编写** | **审核** |
| 1.0 | 新版做成 | 2014/8/28 | 刘芳芳 |  |
| 1.1 | 密钥标识位数改为18位，6位随机数 | 2014/9/1 | 刘芳芳 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1引言 1](#_Toc396981201)

[1.1编写目的 1](#_Toc396981202)

[1.2开发背景 1](#_Toc396981203)

[2软件总体概述 1](#_Toc396981204)

[2.1系统属性和限制 1](#_Toc396981205)

[2.2软件描述 1](#_Toc396981206)

[2.2名词解释 2](#_Toc396981207)

[3功能需求 2](#_Toc396981208)

[3.1产生私钥及P10 2](#_Toc396981209)

[3.2生成pfx证书 3](#_Toc396981211)

[3.3查询pfx证书 5](#_Toc396981213)

[4 风险提示 7](#_Toc396981215)

# 1引言

## 1.1编写目的

该文档是《KT系统》的软件需求说明书，为软件开发和测试各个阶段提供依据。

## 1.2开发背景

提供生成密钥对、生成证书pfx数据流的功能，支持客户实现关键交易的签名验签功能确保交易过程完整性、防篡改和不可否认性。

# 2软件总体概述

## 2.1系统属性和限制

该产品的证书对象为单证 RSA 2048。

该产品对外提供Socket连接方式。

该产品支持Oracle和MySQL两种数据库。

## 2.2软件描述

中文名称：KT系统

版本号码：v3.0.x.x

KTServer-提供Socket服务,实现生成密钥对、生成证书pfx数据等功能。

KTToolkit-外围系统开发工具包（Socket客户端）,以Jar包的方式提供。客户系统利用此工具包连接KTServer的Socket服务。

KTVO-外围系统开发工具包，以Jar包的方式提供。

## 2.2名词解释

密钥标识（KeyIdentifier）：公私钥对的标识，产生一对公私钥的同时生成一个密钥标识。有相同密钥标识的公钥和私钥是相互匹配的，可以完成签名、验签功能。

# 3功能需求

## 3.1产生私钥及P10

产生私钥及P10（含有公钥），私钥信息保存到服务器上并返回P10。

产生并返回密钥标识（年月日时分秒+6位随机数,共18位）。

系统间的调用关系如下：

## 

报文接口定义如下：

|  |  |  |
| --- | --- | --- |
| **请求报文** | | |
| **报文元素** | **约束** | **说明** |
| <Request> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1001 |
| </Head> |  |  |
| <Body/> |  |  |
| </Request> |  |  |
| **返回报文** | | |
| **报文元素** | **约束** | **说明** |
| <Response> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1001 |
| <TxTime> | NOT NULL | 交易时间(2007/08/10 12:40:23) |
| <ResultCode> | NOT NULL | 结果码：成功时该字段为“2000” |
| <ResultMessage> | NOT NULL | 结果描述：成功时该字段为“OK” |
| </Head> |  |  |
| <Body> |  |  |
| <Csr> | NOT NULL | 证书下载请求(P10) |
| <KeyIdentifier> | NOT NULL | 密钥标识（yyMMddHHmmssXXXXXX） |
| </Body> |  |  |
| </Response> |  |  |

## 3.2**生成pfx证书**

根据用户指定的密钥标识，查找对应的私钥，将私钥和公钥证书合成为pfx证书，base64编码后返回。

系统间的调用关系如下：

## 

报文接口定义如下：

|  |  |  |
| --- | --- | --- |
| **请求报文** | | |
| **报文元素** | **约束** | **说明** |
| <Request> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1002 |
| </Head> |  |  |
| <Body> |  |  |
| <KeyIdentifier> | NOT NULL | 密钥标识 |
| <SignatureCert> | NOT NULL | 签名证书 |
| </Body> |  |  |
| </Request> |  |  |
| **返回报文** | | |
| **报文元素** | **约束** | **说明** |
| <Response> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1002 |
| <TxTime> | NOT NULL | 交易时间(2007/08/10 12:40:23) |
| <ResultCode> | NOT NULL | 结果码：成功时该字段为“2000” |
| <ResultMessage> | NOT NULL | 结果描述：成功时该字段为“OK” |
| </Head> |  |  |
| <Body> |  |  |
| <PfxData> | NOT NULL | PFX证书信息 |
| </Body> |  |  |
| </Response> |  |  |

## 3.3查询pfx证书

系统间的调用关系如下：

## 

报文接口定义如下：

|  |  |  |
| --- | --- | --- |
| **请求报文** | | |
| **报文元素** | **约束** | **说明** |
| <Request> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1003 |
| </Head> |  |  |
| <Body> |  |  |
| <KeyIdentifier> | NOT NULL | 密钥标识 |
| </Body> |  |  |
| </Request> |  |  |
| **返回报文** | | |
| **报文元素** | **约束** | **说明** |
| <Response> |  |  |
| <Head> |  |  |
| <TxType> | NOT NULL | 交易类型:1003 |
| <TxTime> | NOT NULL | 交易时间(2007/08/10 12:40:23) |
| <ResultCode> | NOT NULL | 结果码：成功时该字段为“2000” |
| <ResultMessage> | NOT NULL | 结果描述：成功时该字段为“OK” |
| </Head> |  |  |
| <Body> |  |  |
| <PfxData> | NOT NULL | PFX证书信息 |
| </Body> |  |  |
| </Response> |  |  |

# 4 风险提示

客户系统需要维护密钥标识和公私钥的对应关系。

错误场景1：交易1002生成pfx证书

指定的密钥标识和签名证书中公钥的密钥标识不一致时，合成pfx证书失败，报错：私钥与公钥不匹配，请检查输入是否正确。

错误场景2：交易1003查询 pfx证书

指定了错误的密钥标识，得到非本意的其他pfx证书做签名验签。