**密钥管理系统**

**需求规格说明书**

航天二院爱威公司

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **修订人** | **修订日期** | **修订内容** |
| 0.1 | 汤敬浩 | 2016/8/27 | Debug版本 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 文档概述

## 文档约定

文档的描述内容是密钥管理系统的需求规格说明书。

文档采用基于UML建模语言的面向对象建模方式对功能需求进行描述。

主要描述的功能都有对应的用例编号。

针对某一特定角色的功能都由一下三项内容进行需求内容的详细说明：

1. 用例图：一个图可以包含多个基本用例，每个基本用例也可以具有多个扩展和包含类型的子用例。
2. 用例说明：描述基本用例和子用例的详细说明。
3. 系统顺序图：只针对基本用例进行UML图形化描述；基本用例具有扩展和包含用例的，也只需绘制一张系统顺序图，在图上表明角色与子用例的消息交互即可。除此之外，还需明确消息以及消息中包含的参数名称和数据类型（如果，已经编码可参照方法调用的名称以及相应的参数名称）。

文档中所有的UML图形均以visio 2016版本的建模模具进行绘制。

其他需求（例如，性能需求）以文字和列表的形式具体给出。

## 预期的读者和阅读建议

1. 预期的读者和阅读建议

|  |  |  |
| --- | --- | --- |
| 编号 | 预期读者 | 阅读建议 |
| 1 | 客户 | 确认文档中给出的功能需求描述 |
| 2 | 开发方 | 熟悉并掌握项目的各项功能需求 |

## 产品的范围

本文档涉及的项目范围是视频安防监控系统中的密钥管理系统，密钥管理系统包括TCP服务模块、事务处理模块、数据库模块、加密硬件模块。

# 项目背景描述

密码体制是信息安全的基础，密钥管理则负责密码体制中密钥的管理，包括密钥生成、密钥分发、密钥更新、密钥存储、密钥备份、密钥销毁等功能。借助密钥管理服务，用户无需花费大量成本来保护密钥的保密性、完整性和可用性，可以安全、便捷的使用密钥，专注于开发加解密功能场景。

本系统属于视频安防监控系统的子系统，每路视频在传输或保存时都需要使用对称密钥加密。传统的对称密钥管理方法是基于共同保存对称密钥实现的，要保证彼此密钥的交换是安全可靠的，同时还要设定防止密钥泄密和更改密钥的程序。这样，对称密钥的管理和分发工作将变成一件潜在危险的和繁琐的过程。使用公钥加密的数字信封技术是一种解决方案。例如在视频安防监控系统中，摄像头生成一次性对称密钥，用于加密视频流，并用公开密钥对该会话密钥进行加密，加密后与视频流封装在一起，转发给相应的实体，这种模式也有一定隐患，尽管密钥已经被加密，但由于与视频流封装在一起，在非安全的网络中传输或者在非安全的设备中存储（为了方便视频记录与回放，视频信息需要存储很久），仍然有一定风险。因此在这种应用场景下，需要更加安全的密钥管理方法以及系统。

# 系统的需求说明

## 领域建模

### 类图（概念类）：



1. 概念类图

### 活动图

以客户端请求密钥管理创建密钥为例，多泳道活动图如下：

1. 客户端请求密钥管理创建密钥对应的活动图

## 用例建模

### 用例图



1. 用例图

### 角色定义

在视频安防监控系统中，加密客户端指的是摄像头，用于加密摄像头监控的视频流。

在视频安防监控系统中，解密客户端指的是视频监视/回放客户端。

### 用例分析

1. 身份认证用例
2. “身份认证”用例说明

|  |  |  |
| --- | --- | --- |
| 用例编号： | 1 | |
| 用例名称： | 身份认证 | |
| 参与者： | 加密客户端或解密客户端 | |
| 前置条件： | 客户端需要向密钥管理系统申请密钥 | |
| 后置条件： | 客户端和密钥管理系统建立了安全连接 | |
| 成功场景： | 步骤 | 活动 |
| 1 | 客户端向服务器发起TCP连接 |
| 2 | 客户端向服务器发送自己的数字证书和随机产生的随机数rand1 |
| 3 | 服务端向客户端发送自己的数字证书和随机产生的随机数rand2 |
| 4 | 客户端使用自己的私钥加密rand2，并发送给服务端 |
| 5 | 服务端使用自己的私钥加密rand1，并发送给客户端 |
| 6 | 客户端和服务端分别解析对方的证书，查看其有效性 |
| 7 | 客户端使用服务器证书中的公钥解密rand1，解密后与最初自己生成的rand1对比，如果不相同，则断开连接 |
| 8 | 服务端使用客户端证书中的公钥解密rand2，解密后与最初自己生成的rand2对比，如果不相同，则断开连接 |
| 9 | 相互确认身份后建立安全连接，通信内容使用客户端证书中的公钥加密 |

其对应的系统顺序图：



1. “身份认证“对应的系统顺序图

系统顺序图中出现的系统事件对应的操作契约如下：

1. 系统顺序图中的操作“Connect”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | Connect(server\_ip) |
| 交叉引用： | 身份认证 |
| 前置条件： | 客户端需要向密钥管理系统申请密钥 |
| 后置条件： | 一个新的身份认证模块创建 |

1. 系统顺序图中的操作“SendCertAndRand1”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendCertAndRand1() |
| 交叉引用： | 身份认证 |
| 前置条件： | 客户端与密钥管理系统建立了连接 |
| 后置条件： | 密钥管理系统收到了客户端的证书和客户端产生的rand1 |

1. 系统顺序图中的操作“SendCertAndrand2”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendCertAndRand2() |
| 交叉引用： | 身份认证 |
| 前置条件： | 客户端与密钥管理系统建立了连接 |
| 后置条件： | 客户端收到了密钥管理系统的证书和其产生的rand2 |

1. 系统顺序图中的操作“SendRand2WithEncrypted”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendRand2WithEncrypted() |
| 交叉引用： | 身份认证 |
| 前置条件： | 客户端使用自己的私钥加密了rand2 |
| 后置条件： | 服务端收到了客户端发送的加密的rand2，并使用客户端证书中的公钥解密rand2，解密后与最初自己生成的rand2对比是否相同 |

1. 系统顺序图中的操作“SendRand1WithEncrypted”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendRand1WithEncrypted() |
| 交叉引用： | 身份认证 |
| 前置条件： | 服务端使用自己的私钥加密了rand1 |
| 后置条件： | 客户端收到了服务端发送的加密的rand1，并使用服务端证书中的公钥解密rand1，解密后与最初自己生成的rand1对比是否相同 |

1. 请求创建对称密钥用例
2. “请求创建对称密钥”用例说明

|  |  |  |
| --- | --- | --- |
| 用例编号： | 2 | |
| 用例名称： | 请求创建对称密钥 | |
| 参与者： | 加密客户端或解密客户端 | |
| 前置条件： | 加密客户端与密钥管理系统建立了安全连接 | |
| 后置条件： | 密钥管理系统创建了一个新的对称密钥，并将对称密钥通过安全连接发送给加密客户端 | |
| 成功场景： | 步骤 | 活动 |
| 1 | 加密客户端与密钥管理系统建立了安全连接 |
| 2 | 加密客户端向密钥管理系统发送“请求创建对称密钥”请求 |
| 3 | 密钥管理系统随机产生对称密钥和密钥ID，并通过安全连接（使用客户端证书中的公钥加密）发送给加密客户端 |
| 4 | 加密客户端拿到对称密钥后，进行事务操作 |

其对应的系统顺序图：



1. “请求创建对称密钥”对应的系统顺序图

系统顺序图中出现的系统事件对应的操作契约如下：

1. 系统顺序图中的操作“SendRequest”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendRequest(“create\_key”) |
| 交叉引用： | 请求创建对称密钥 |
| 前置条件： | 客户端与密钥管理系统建立了安全连接 |
| 后置条件： | 一个新的事务处理（线程池中的任务）创建  一个新的数据库模块创建  数据库模块与事务处理建立关联  数据库模块状态：开启数据库连接  一个新的安全硬件模块创建  硬件模块与事务处理建立关联  硬件模块状态：打开硬件设备 |

1. 根据密钥ID请求对称密钥用例
2. “根据密钥ID请求对称密钥”用例说明

|  |  |  |
| --- | --- | --- |
| 用例编号： | 3 | |
| 用例名称： | 根据密钥ID请求对称密钥 | |
| 参与者： | 加密客户端和解密客户端 | |
| 前置条件： | 客户端与密钥管理系统建立了安全连接；此对称密钥已经产生；客户端具有该密钥的ID及访问权限 | |
| 后置条件： | 密钥管理系统将此密钥ID对应的对称密钥通过安全连接发送给加密客户端 | |
| 成功场景： | 步骤 | 活动 |
| 1 | 客户端与密钥管理系统建立了安全连接 |
| 2 | 客户端向密钥管理系统发送“根据密钥ID请求对称密钥”请求，并发送密钥ID |
| 3 | 密钥管理系统根据密钥ID查询到对称密钥，并通过安全连接（使用客户端证书中的公钥加密）发送给客户端 |
| 4 | 客户端拿到对称密钥后，进行事务操作 |

其对应的系统顺序图：



1. “根据密钥ID请求对称密钥”对应的系统顺序图

系统顺序图中出现的系统事件对应的操作契约如下：

1. 系统顺序图中的操作“SendRequest”对应的操作契约

|  |  |
| --- | --- |
| 操作（系统事件）： | SendRequest(key\_id) |
| 交叉引用： | 根据密钥ID请求对称密钥 |
| 前置条件： | 客户端与密钥管理系统建立了安全连接；此对称密钥已经产生；客户端具有该密钥的ID及访问权限 |
| 后置条件： | 一个新的事务处理（线程池中的任务）创建  一个新的数据库模块创建  数据库模块与事务处理建立关联  数据库模块状态：开启数据库连接  一个新的安全硬件模块创建  硬件模块与事务处理建立关联  硬件模块状态：打开硬件设备 |

# 其他需求

## 性能需求

要求密钥管理系统可以管理至少200万个对称密钥，并能在1s内响应客户端的请求。

## 密钥有效期

* 定义密钥在生成后2个小时内为“活跃状态”，此时密钥可以用于加密和解密，因此加密客户端和解密客户端均有权限访问。
* 2个小时后，密钥进入“非活跃状态”，此时只有解密客户端具有访问该密钥的权限。
* 在密钥存储6个月后，该密钥自动销毁，此需求可由数据库事务自动（定时）处理。