**需求规格说明书**

**（内部资料，禁止外泄）**

**V1.0**

**2016年11月20日**

**版本修订说明**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 修改内容 | 修改人 | 修改日期 | 审核人 | 发布日期 |
| V1.0 | 创建 |  | 2019-06-20 |  |  |
| V1.1 | 需求更新 |  | 2019-06-22 |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目录

[1.简介 4](#_Toc487035938)

[1.1. 术语和缩写 4](#_Toc487035939)

[1.2. 参考资料 4](#_Toc487035940)

[2.产品描述 4](#_Toc487035941)

[3.用户业务场景分析 4](#_Toc487035942)

[4.与现有产品差异 4](#_Toc487035943)

[5.约束与限制 4](#_Toc487035944)

[6.需求详细描述 5](#_Toc487035945)

[6.1. 产品运行环境 5](#_Toc487035951)

[6.2. 功能需求 5](#_Toc487035952)

[6.3. 接口需求 5](#_Toc487035953)

[6.4. 界面需求 6](#_Toc487035954)

[6.5. 性能需求 7](#_Toc487035955)

[6.6. 可靠性需求 7](#_Toc487035956)

[6.7. 可维护性需求 7](#_Toc487035957)

[6.8. 安全性需求 8](#_Toc487035958)

[6.9. 认证需求 8](#_Toc487035959)

[6.10. 用户文档需求 9](#_Toc487035960)

[6.11. 其他需求 9](#_Toc487035961)

[7.验收标准 10](#_Toc487035962)

# 简介

* 1. 术语和缩写

|  |  |
| --- | --- |
| 术语和缩写 | 解释 |
| PKI | PKI(Public Key Infrastructure) 是公钥基础设施的简称，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。 |
| CA | CA(Certificate Authority)是数字证书认证中心的简称，是PKI系统中通信双方信任的实体，是指发放、管理、废除数字证书的机构，被称为可信第三方。 |
| RSA | RSA加密算法是一个能同时用于加密和数字签名的非对称加密算法 |
| SQL | 一种用于访问查询数据库的语言 |

* 1. 参考资料

1. 《软件工程基础》 赵一丁 北京邮电大学出版社

2. 《软件需求》 劳森 (作者), 刘晓晖 (译者) 电子工业出版社

3. 《软件需求工程：原理和方法》 金芝，刘璘，金英 科学出版社

4. 《实用软件工程》第三版 殷人昆 清华大学出版社

5. 《二维码电子标签的安全技术研究》 廖东方 北京邮电大学

6. 《基于证书的二维码生成和认证系统的研究》 王望羊 电子科技大学

# 产品描述

*包括产品介绍、产品范围、产品遵循的标准等。*

随着二维码使用的普及，二维码扫描也变得越来越实用，扫码登录作为一种新的登录方式，它不仅更为便捷，因无需再次输入用户信息直接扫码登录的方式更意味着减少了账户泄密的风险，相比传统登录方式而言更加安全。基于PKI的二维码安全认证系统在扫码登录的基础上，结合PKI技术进行用户身份认证，进一步提高系统安全性。

在上述设计的基础上，利用存储在手机中的私钥文件在不同用户之间进行电子合同的签名认证服务，同时也提供其他用户对合同签名真伪的验证。

# 用户业务场景分析

*分析用户的真实业务场景，描述用户场景对于产品的需求要点。*

用户已在移动设备端登录之后，需要在电脑上进行登录时，使用基于PKI的二维码扫描技术可以省去输密码的过程，通过手机上扫码验证登录就可完成电脑端用户的登录，从而保证密码的安全性，减少密码泄露的风险。结合实际使用情况需求要点有：操作简单、易用，符合人们日常生活中的使用习惯，避免复杂的操作流程；用户界面简单明了，不需要有太过复杂的功能使用。同时，用户之间在本地拟定合同之后由一方上传文档至Web端，经双方商榷确认之后，共同在Web界面上扫码完成双方签名，最后还能提供合同签名真伪的认证。

# 与现有产品差异

*如果产品是升级产品或从现有产品进行改造，请注明前一产品的规格，并列出与现有产品差异。在备注栏可填写额外的说明信息。*

|  |  |  |
| --- | --- | --- |
| 现有产品功能点 | 新需求差异描述 | 备注 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 约束与限制

*说明在实现时所必须满足的条件和所受的限制，以及相应的原因。如：必须使用或者避免的特定技术、工具、编程语言和数据库、企业策略、政府法规或工业标准**。*

（1）采用符合J2EE技术规范的多层构架，支持管理员操作。

（2）客户端使用浏览器，移动端使用Android手机。

（3）数据库管理系统使用MySQL，应用中间件使用Tomcat。

（4）整个系统运行于应用服务器之上，利用应用中间件支撑系统的运行。

（5）可在手机端和Web端查看登录日志记录。

（6）用户扫码一次只能登录一个Web网页界面，不支持同时登录多界面。

（7）使用长链接的方式，后台维护该随机数与session的对应关系。

（8）手机使用PIN码加密存储私钥文件。

# 需求详细描述

*本文档是从产品整体的角度描述需求，可能会涉及到硬件和软件结合的情况。在产品层次未涉及的硬件详细需求规格，可专门输出《硬件需求规格说明书》。*

首先用户在手机上开始注册，使用Open SSL随机生成RSA密钥对，用户输入PIN码作为口令使用对称加密对手机本地的私钥文件进行加密，向管理员发送公钥和用户信息。

管理员在Web后台系统登录管理员账号，对用户上传的用户名和手机设备号以及公钥生成相应的证书，颁发数字证书，并将用户证书导入数据库。

用户需要登录web时，浏览器使用后台提供的随机数生成二维码，展示二维码，然后后台维护对话，移动APP输入PIN码解密私钥，用私钥完成对二维码随机数的PKI数字签名，并发送到Web后台，后台在接收到客户端发送的签名值后，根据用户名和手机设备号从数据库中取得对应的公钥，对用户签名值的有效性进行验证，确定浏览器是否跳转。

用户可以在登录Web端后，发起一个合同过程，然后在本地编辑好一个合同(.txt .pdf 等文件)，确认无误后上传到服务器，点击确认合同。作为合同的另一方则可以从服务器下载合同，检查或修改合同内容，再次上传合同到更新到服务器，点击确认合同。此时，因为合同可能已被编辑或修改，合同发起人需要再次确认合同内容，下载确认无误之后再次上传重新点击确认。同样的，合同发起人再次上传之后合同另一方需要相同的确认操作，最后直到双方都在没有修改合同的情况下点击了确认，合同内容最终达成一致，变为不可编辑状态。用户可以在浏览器点击给合同签名（签名过程需要手机扫码），当合同双方都对合同签过名之后，成功的生成完整的电子合同。合同双方均可在WEB端一键下载自己签署过的合同，任何用户可以向服务器上传一个完整的电子合同文件来验证合同的有效性。

5. 1. 产品运行环境

* *详细说明各功能模块运行所需的环境（比如运行平台、操作系统、硬件配置、网络环境）。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-E-0001 | 证书颁发模块 | Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |
| PR-E-0002 | 用户注册模块 | Android5.0以上版本  CPU：1G Hz以上 内存：2GB以上 | 高 |
| PR-E-0003 | 用户登录模块 | Android5.0以上版本  CPU：1G Hz以上 内存：2GB以上  Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |
| PR-E-0004 | 扫码签名模块 | Android5.0以上版本  CPU：1G Hz以上 内存：2GB以上 | 高 |
| PR-E-0005 | 用户中心模块 | Android5.0以上版本  CPU：1G Hz以上 内存：2GB以上  Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |
| PR-E-0006 | 二维码登录模块 | Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |
| PR-E-0007 | 合同管理模块 | Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |
| PR-E-0008 | 用户管理模块 | Windows10  CPU：1GHz 以上 内存：2GB以上 | 高 |

*注：*

1. *需求编号采用PR-E-\*\*\*\*的形式，PR代表产品，E代表运行环境，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 功能需求

*产品所实现的功能，即从用户角度要求必须实现的功能点。包括用户陈述的或隐含的需求。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-F-0001 | 用户注册 | 在手机端输入相关信息完成注册，发送至后台生成用户证书 |  |
| PR-F-0002 | 颁发证书 | 管理员对注册用户提供的信息进行审批通过后颁发用户证书 |  |
| PR-F-0003 | 普通登录 | 在已登录设备外的其他设备上登陆时通过扫描新设备的二维码进行登录 |  |
| PR-F-0004 | 扫码登录 | 扫描Web界面提供的二维码进行登录 |  |
| PR-F-0005 | 签署合同 | 双方对已经确认不再修改的合同进行签名 |  |
| PR-F-0006 | 读取合同详情 | 从后台读取与用户有关的所有合同的信息列表 |  |
| PR-F-0007 | 读取登录日志 | 标明每一次的登录情况，区分手机端登录和Web端登录，表明手机设备ID号 |  |
| PR-F-0008 | 合同存储 | 将合同存储在云端 |  |
| PR-F-0009 | 合同分发 | 按需要下载已上传的合同文档 |  |
| PR-F-0010 | 合同验证 | 合同双方签署身份认证 |  |
| PR-F-0011 | 处理新用户注册请求 | 对新用户提交的真实姓名与身份证号进行比对，审批通过后存储用户公钥等相关信息生成用户证书，新户注册成功 |  |
| PR-F-0012 | 处理新设备注册请求 | 新设备点击登录之后会生成随机数二维码，同时Web后台会接收，新设备传送的公钥，已登录设备扫描新设备生成的二维码之后后台录入新设备相关信息，新设备注册完成 |  |
| PR-F-0013 | 处理信息读取请求 | 对读取合同详情、设备详情、登录日志的请求进行处理 |  |
| PR-F-0014 | 验证Web登录 | 对已登录设备的用户及新设备的扫码请求进行登录验证 |  |

1. *需求编号采用PR-F-\*\*\*\*的形式，PR代表产品，F代表功能需求，编号从0001开始依次累加*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 接口需求

*可包括硬件接口、软件接口、通信接口等。*

*硬件接口：要指出每一个接口的逻辑特点、支撑什么样的设备、如何支撑这些设备、有何约定。*

*软件接口：在这里应指定需使用的其他软件产品（例如：数据管理系统、操作系统、或者数学软件包），以及同其他应用系统之间的接口。对于每一个接口，这部分应说明与产品相关的接口软件的目的，并根据信息的内容和格式定义接口，这里不必详细描述任何已有完整文件的接口，只要引用定义该接口的文件即可*

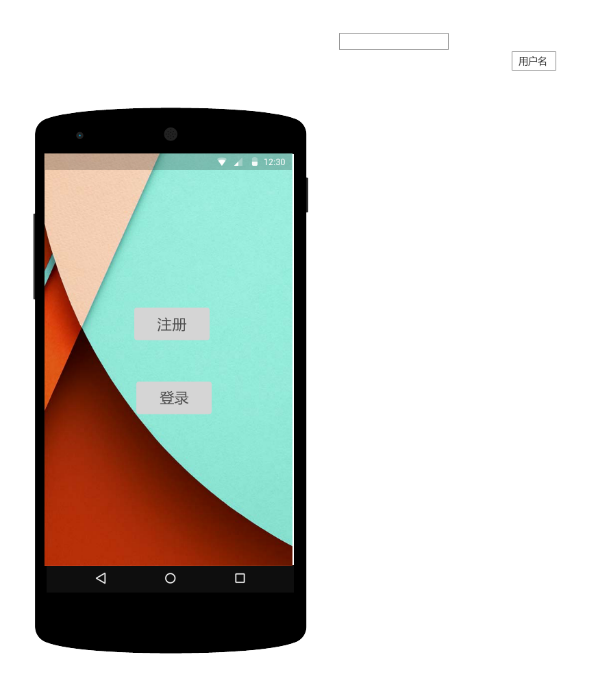
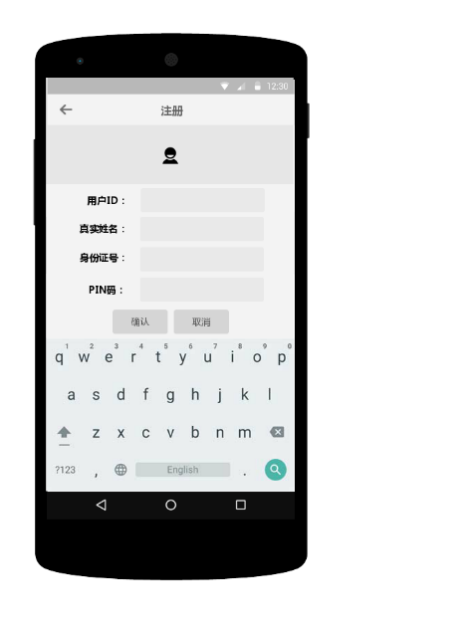
*通信接口：这里指定各个通信接口，例如：局部网络的协议等。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-I-0001 | 合同详情拉取请求接口 | 向后台拉取与用户相关的所有合同的信息列表，合同详情包括合同双方、合同状态、合同生效时间等信息 | 高 |
| PR-I-0002 | 登录日志拉取请求接口 | 向后台拉取登录历史记录信息，日志记录了每一次登录的详细信息，包括登陆时间、登录设备等信息 | 高 |
| PR-I-0003 | 合同创建请求接口 | 由合同一方发起请求创建一份新的合同的请求接口 | 高 |
| PR-I-0004 | 合同删除请求接口 | 对合同不满意需要删除合同，提交删除合同的请求接口 | 高 |
| PR-I-0005 | 合同上传请求接口 | 合同在本地编辑完成后可提交合同更新上传请求 | 高 |
| PR-I-0006 | 合同下载请求接口 | 合同尚未确认签名，可以下载到本地再次修改的请求接口 | 高 |
| PR-I-0007 | 合同签名请求接口 | 合同双方完成对合同确认后提交签名的请求接口 | 高 |
| PR-I-0008 | 合同导出请求接口 | 合同双方确认之后完成签名将签名后的电子合同文档导出的请求接口 | 高 |
| PR-I-0009 | 用户注册信息提交接口 | 用户填写完用户信息之后，向Web后台发送注册信息请求 | 高 |
| PR-I-0010 | 用户登录身份验证接口 | 用户扫描二维码之后向后台发送随机数进行身份验证请求，通过验证之后成功登录 | 高 |
| PR-I-0011 | 合同签名验证接口 | 对已签名的电子合同进行验证，用户向后台发送验证请求，经由后台对合同的签名进行验证 | 高 |
| PR-I-0012 | 审批接口 | 用户提交注册请求，管理员对用户信息进行真实性验证审批，若通过则成功注册 | 高 |

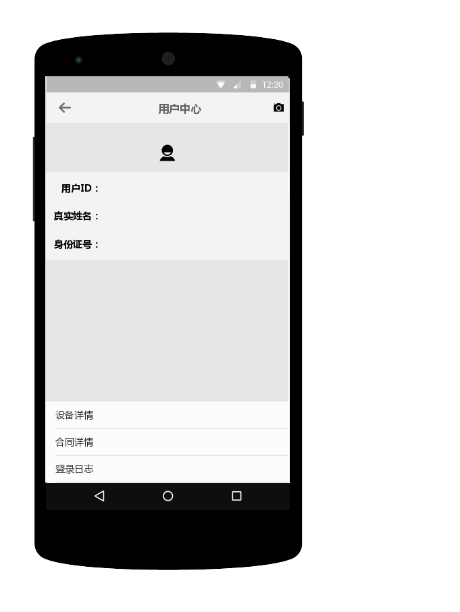
*注：*

1. *需求编号采用PR-I-\*\*\*\*的形式，PR代表产品，I代表接口需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 界面需求

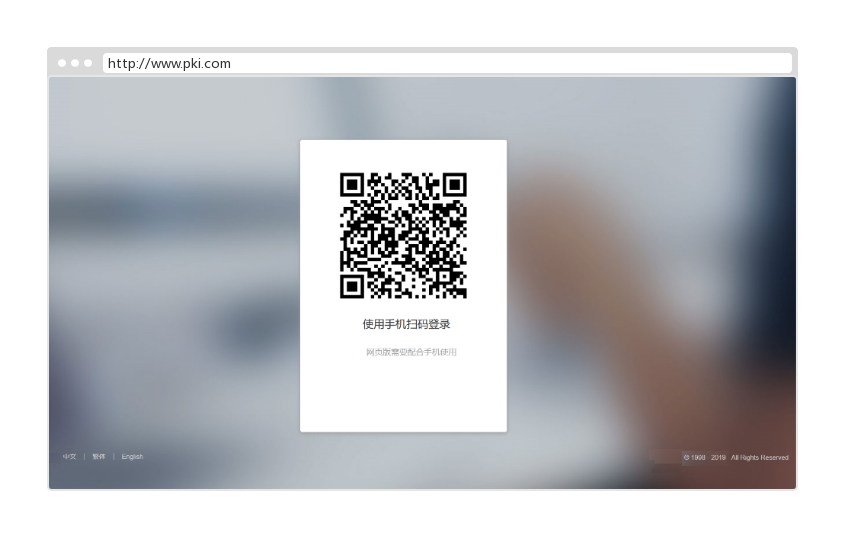
*界面是指产品为使用者提供的交互展示窗体或页面。本章节需要描述产品的界面风格、界面提供的功能，可采用自然语言描述出每个界面需要提供的功能，也可以采用原型图等展示。*

（初始界面） （注册界面）

（新设备登录界面） （登录后用户界面） （扫码界面）



（登录扫码界面）

（登录成功后本操作界面）

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-U-0001 | 初始界面 | 包含登录和注册两个基本功能 | 高 |
| PR-U-0002 | 注册界面 | 用户输入相关信息之后进行注册 | 高 |
| PR-U-0003 | 新设备注册界面 | 显示登录二维码，需要由已登录设备扫码登录 | 高 |
| PR-U-0004 | 登陆后的用户界面 | 包含查看合同详情、登录日志的基础功能 | 高 |
| PR-U-0005 | 扫码界面 | 用户扫描二维码的界面 | 高 |
| PR-U-0006 | Web登录界面 | 显示供用户登录的扫描二维码 | 高 |
| PR-U-0007 | Web用户界面 | 包含查看合同详情、登录日志的基础功能 | 高 |
|  |  |  |  |

*注：*

1. *需求编号采用PR-U-\*\*\*\*的形式，PR代表产品，U代表界面需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 性能需求

*性能通常指产品在功能上满足顾客要求的能力，包括使用性能和外观性能。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-P-0001 | 响应时间 | 扫码之后Web在3秒内响应请求 | 1 |
| PR-P-0002 | 使用外观 | Web网页能够快速显示不出错 | 2 |
| PR-P-0002 | 处理能力 | 允许同时并发用户数达400 | 1 |
|  |  |  |  |

*注：*

1. *需求编号采用PR-P-\*\*\*\*的形式，PR代表产品，P代表性能需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 可靠性需求

*产品在规定的条件下，在规定的时间内，完成规定的功能的能力称为可靠性。对那些发生质量事故会造成巨大损失或危及人身、社会安全的产品，可靠性是使用过程中主要的质量指标。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-R-0001 | 快速扫描 | 扫一扫功能打开之后迅速完成扫码识别，不出现识别不了的情况 |  |
| PR-R-0002 | 极速跳转 | 在扫码成功之后能够快速跳转，不出现bug，或者页面无效等情况 |  |
| PR-R-0003 | 多用户同时登陆 | 在浏览器中可以允许多个用户同时登陆，彼此之间不会相互影响 |  |
|  |  |  |  |

*注：*

1. *需求编号采用PR-R-\*\*\*\*的形式，PR代表产品，R代表可靠性需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 可维护性需求

*所有提高可维护性或可扩展性的需求。如使用行业标准，编码标准，开放式结构，可兼容语言，备份机复原，数据交换，命名约定，类库，维护访问，维护工具等。可以从维护者角度考虑，产品应该提供的错误码反馈、日志记录、自我诊断等功能。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-M-0001 | 源码管理 | 使用Github进行源码管理，便于维护与修复 | 1 |
|  |  |  |  |

*注：*

1. *需求编号采用PR-M-\*\*\*\*的形式，PR代表产品，M代表可维护性需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 安全性需求

*保护产品的要素，以防止各种非法的访问、使用，修改、破坏或者泄密。比如：*

1. *利用可靠的密码技术。*
2. *掌握特定的记录或历史数据集。*
3. *给不同的模块分配不同的功能。*
4. *限定一个程序中某些区域的通信。*
5. *计算临界值的检查和。*

*如果该产品有国家或国际标准、行业标准可循，可以摘录标准中的安全性要求内容，如完全遵守，可以直接写符合《\*\*\*》标准第\*章节安全性要求。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-S-0001 | 数据备份 | 建立合同备份，防止用户丢失数据 | 1 |
| PR-S-0002 | RSA加密 | 通过使用RSA加密技术提高安全性 |  |
| PR-S-0003 | 登陆限制 | 一个用户一次只能扫描一个二维码界面登陆，在其他页面扫描登陆之后当前页面失效 |  |
| PR-S-0004 | 加密传输 | 采用https进行数据传输 |  |

*注：*

1. *需求编号采用PR-S-\*\*\*\*的形式，PR代表产品，S代表安全需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 认证需求

*产品在销售到特定的国家、地区或者行业之前，由第三方机构进行的准入检测，验证产品是否能满足国家、行业等相关技术标准。如：国密局产品型号认证、国际FIPS认证、公安部销售许可证申请、中国CCC认证，欧盟的CE认证等。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-C-0001 | PKCS#1 | 必须符合RSA加密标准，包括待签名数据和签名本身的格式；它也定义了PSA公/私钥的语法。 |  |
|  |  |  |  |

*注：*

1. *需求编号采用PR-C-\*\*\*\*的形式，PR代表产品，C代表认证需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*
   1. 用户文档需求

*用户指南、联机帮助、安装指南、配置文件等。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-D-0001 | 用户指南 | 对二维码扫码功能的使用介绍 |  |
|  |  |  |  |

注：

1. 需求编号采用PR-D-\*\*\*\*的形式，PR代表产品，D代表文档需求，编号从0001开始依次累加。
2. 填写表格时需要按照需求的层次自行增加子章节。
   1. 其他需求

*其他以上未涉及的需求，如使用寿命、可用性、经济性、易用性、效率、可移植性等。如果有明确需要，可在此处添加，否则可裁剪。*

|  |  |  |  |
| --- | --- | --- | --- |
| 需求编号 | 名称 | 需求描述 | 优先级 |
| PR-O-0001 | 使用期 | 只要授权证书不过期可以一直使用 | 1 |
|  |  |  |  |

*注：*

1. *需求编号采用PR-O-\*\*\*\*的形式，PR代表产品，O代表其他需求，编号从0001开始依次累加。*
2. *填写表格时需要按照需求的层次自行增加子章节。*

# 验收标准

*验收标准是从验收的视角出发对需求的定量描述。每条需求都应有明确的指标可以作为验收标准。在验收时主要从两方面考虑需求规格描述是否合格：一是考虑它能否作为测试的数据输入，二是考虑需求的度量方式是否满足产品的目标。*

文档验收标准

文档编写符合国际文档编写规范

·软件需求规格说明书

软件验收标准

　 软件一切功能正常，运行流畅、不卡顿、不闪退，适配大部分的Android手机。

界面验收标准

·注册界面

包含用户信息输入框等内容，下方有”确认”和“取消”按钮

·用户页面

显示登录成功后用户信息，以及相关基本功能

·扫码界面

可以打开二维码扫描功能

·新设备注册界面

可以生成并显示随机数二维码供已登录设备扫描

·Web登录扫码界面

正常显示可供用户登录扫描二维码