URL请求安全方案

修改历史：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 修改日期 | 修改内容 | 修改人 | 备注 | 版本 |
| 1 | 2018-01-08 | 初稿 | 高松 |  | 1.0.0 |
|  |  |  |  |  |  |

### 前言

URL请求是操作租房网后台服务的基本单位，所以对于每个URL请求的检查是对系统安全防范的重要步骤，不仅需要保证URL请求在信息传输过程中的完整性，还需要防止URL请求在信息传输过程中被篡改。

当前，对于URL请求的安全检查分为以下两个部分：

1. URL请求的加密和解密
2. URL签名检查

### 请求加密和解密

#### 实现方式

请求加密和解密方案基于5种基本流程（如下图）。



1. 其中，申请公钥和注册客户端流程是将客户端标识以非对称加密的方式注册到系统中，此过程每个客户端启动时执行一次，保证当前客户端之后可以被系统识别。
2. 客户端标识注册后，所有请求使用客户端标识作为密钥进行对称加密；另外，登录请求是客户端标识请求的一个场景。
3. 登录后的用户，所有请求使用用户标识作为密钥进行对称加密。

#### 作用

URL请求的加密和解密加强了在数据传输过程中对于敏感数据的保护，方式数据篡改，保证完整性。但是，数据加密解密无法对URL本身进行保护。

### URL签名检查

#### 实现方式

所有的URL请求，由前端框架在URL尾部加入token，时间戳，来源后，将URL使用客户单标识进行加密。网关收到URL请求后，使用同样的加密过程生成签名并验证签名。

#### 作用

URL签名检查加强了对URL本身的安全性，防止被URL本身篡改，尤其是token的真实性。和URL请求加密和解密配合使用，可以更好地保证整个请求在传输过程中的安全。