# 网证通手机证书服务器性能测试

# 1 升级原因

网证通手机证书服务器（密钥服务器）V1.1在V1.0的基础上，调整优化了服务器端代码数据结构，使其签名、解密、产生密钥对等功能的性能能够满足1000并发用户的性能指标。

参考资料：

1. 测试申请单：<http://192.168.0.123:8080/browse/RODT-981>；
2. 上个版本测试报告：

<http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA_CRYPTO/current/winX86/设备驱动/手机证书/服务端/测试/网证通手机证书（分割型密钥）服务器V1.0性能测试报告.docx>；

# 2 测试结论

根据测试结果显示，并发用户数为1000的时，内外网条件下，签名平均响应时间均在7s以下，解密平均响应时间均在6.5s以下，详细测试结果见[章节6.](#_6_测试结果)

经项目经理评估，本次测试性能符合需求预期，性能测试评估为**测试通过**。

此次测试分为内网测试和外网测试两部分：

1. **内网测试（服务器IP为192.168.200.58）：**
2. 对接口的获取服务器状态、注册公钥、产生密钥对、签名、解密五个功能进行并发用户为1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | 获取服务器状态 | 注册公钥 | 产生密钥对 | 签名 | 解密 |
| 1000并发 | 响应时间（s） | 3.54 | 6.37 | 7.38 | 6.75 | 6.04 |
| 吞吐量（事务数/sec） | 275.2 | 152.7 | 131.8 | 144.1 | 161.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% |

1. 在服务器含有10w+密钥对的情况下，对接口的签名、解密进行并发用户分别为50,100,300，500,800，1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 并发数 | | 50 | 100 | 300 | 500 | 800 | 1000 |
| 签名 | 响应时间（s） | 0.37 | 0.73 | 2.06 | 3.41 | 5.43 | 6.57 |
| 吞吐量（事务数/sec） | 131.9 | 134.2 | 141.8 | 143.1 | 143.2 | 144.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |
| 解密 | 响应时间（s） | 0.33 | 0.60 | 1.76 | 2.78 | 4.47 | 6.04 |
| 吞吐量（事务数/sec） | 147.5 | 161.5 | 166.7 | 175.8 | 174.3 | 161.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |

1. **外网测试（服务器IP为14.18.158.147）：**
2. 对接口的获取服务器状态、注册公钥、产生密钥对、签名、解密五个功能进行并发用户为1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | 获取服务器状态 | 注册公钥 | 产生密钥对 | 签名 | 解密 |
| 1000并发 | 响应时间（s） | 3.98 | 6.45 | 7.48 | 6.87 | 6.10 |
| 吞吐量（事务数/sec） | 244.8 | 150.9 | 130.1 | 141.7 | 159.6 |
| 成功率 | 99.88% | 100% | 100% | 100% | 100% |

1. 在服务器含有10w+密钥对的情况下，对接口的签名、解密进行并发用户分别为50,100,300，500,800，1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 并发数 | | 50 | 100 | 300 | 500 | 800 | 1000 |
| 签名 | 响应时间（s） | 0.38 | 0.80 | 2.11 | 3.44 | 5.50 | 6.87 |
| 吞吐量（事务数/sec） | 130.2 | 121.9 | 138.8 | 141.8 | 141.8 | 141.7 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |
| 解密 | 响应时间（s） | 0.34 | 0.63 | 1.72 | 3.00 | 4.79 | 6.10 |
| 吞吐量（事务数/sec） | 141.2 | 154.7 | 161.5 | 162.4 | 174.3 | 159.6 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |

# 3 限制条件

1. （新增）测试的时间段不同，网络因素影响有所不同，因此数据可能存在部分差异

# 4 测试策略

1. 并发用户数为1000时，对获取服务器状态、注册公钥、产生密钥对、签名和解密五个功能进行性能测试
2. 服务器含有10w+密钥对的情况下，对签名和解密功能进行并发用户数分别为50， 100，300，500，800，1000的性能测试

# 5 测试要项

### 5.1 测试要项

|  |  |
| --- | --- |
| **产品名称** | 网证通手机证书服务器（密钥服务器）V1.1.0 |
| **最后提测版本** | V1.1.0 |
| **生产单位** | 广东省电子商务认证中心 开发部 |
| **测试单位** | 广东省电子商务认证中心 运维部 |
| **测试类型** | 性能测试 |
| **部署后测试地址** | 内网：<https://192.168.200.58:8443/softCertInterface/allService>；  外网：<https://14.18.158.147:58443/softCertInterface/allService>； |
| **客户端配置** | CPU: Intel(R) Core(TM) i7-6700 CPU @3.40GHz 3.40GHz 8G  网卡：1000M |
| **性能测试负载工具** | Jmeter 5.0 |
| **测试脚本** | http://192.168.0.11:8081/svn/rdrelease/软件发布/NETCA\_CRYPTO/current/winX86/设备驱动/手机证书/服务端/测试/手机软证书服务端\_生产环境\_58.jmx |
| **测试人员** | 廖远贵 |
| **测试日期** | 2018-10-24~2018-10-26 |

### 5.2 服务器配置

|  |  |
| --- | --- |
| **处理器** | Intel Xeon Processor E3-1220V5 4C/4T 3.0GHz 8M |
| **内存** | 8G/DDR4/2133或2400MHz/ECC-Unbuffer/2Ranks(单路专用） |
| **硬盘** | 1T SATA企业级硬盘 |
| **网络带宽** | 100M |
| **操作系统** | CentOS release 6.7 (Final) x64 |
| **JDK** | jdk1.8.0\_40 |
| **WEB服务器** | apache-tomcat-8.0.38 |
| **数据库系统** | MySQL 5.7.19 |
| **时间服务器** | 内网：<https://192.168.200.58:8443/softCertInterface/allService>；  外网：  <https://14.18.158.147:58443/softCertInterface/allService> |
| **安全中间件** | Java - Linux64位，V5.6.2 |

# 6 测试结果

所有性能测试，均在30s内从0用户上升到目标并发用户数，在达到目标并发用户数后，稳定运行10分钟

## 内网：

1. 对接口的获取服务器状态、注册公钥、产生密钥对、签名、解密五个功能进行并发用户为1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | 获取服务器状态 | 注册公钥 | 产生密钥对 | 签名 | 解密 |
| 1000并发 | 响应时间（s） | 3.54 | 6.37 | 7.38 | 6.75 | 6.04 |
| 吞吐量（事务数/sec） | 275.2 | 152.7 | 131.8 | 144.1 | 161.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% |

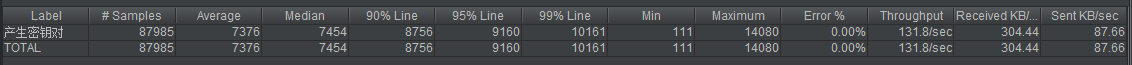
1. 获取服务器状态：



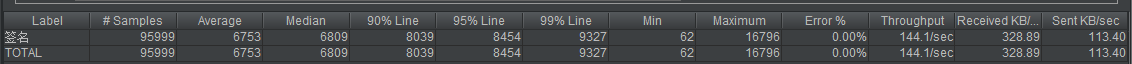
1. 注册公钥：



1. 产生密钥对：



1. 签名：1000并发



1. 解密



1. 在服务器含有10w+密钥对的情况下，对接口的签名、解密进行并发用户分别为50，100，300，500，800，1000的性能测试，测试结果如下表：

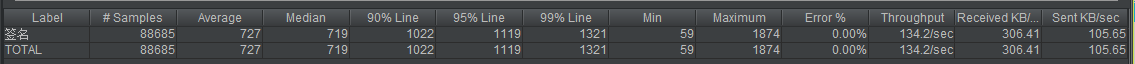
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 并发数 | | 50 | 100 | 300 | 500 | 800 | 1000 |
| 签名 | 响应时间（s） | 0.37 | 0.73 | 2.06 | 3.41 | 5.43 | 6.57 |
| 吞吐量（事务数/sec） | 131.9 | 134.2 | 141.8 | 143.1 | 143.2 | 144.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |
| 解密 | 响应时间（s） | 0.33 | 0.60 | 1.76 | 2.78 | 4.47 | 6.04 |
| 吞吐量（事务数/sec） | 147.5 | 161.5 | 166.7 | 175.8 | 174.3 | 161.1 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |

**签名**：

50并发：



100并发：



300并发：



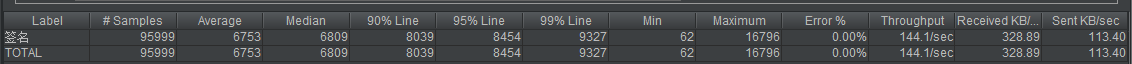
500并发：



800并发：



1000并发：



**解密**：

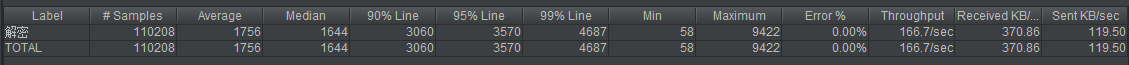
50并发：



100并发：



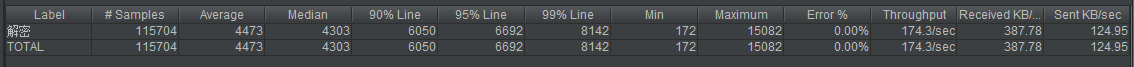
300并发：



500并发：



800并发：



1000并发：



### 外网：

1. 对接口的获取服务器状态、注册公钥、产生密钥对、签名、解密五个功能进行并发用户为1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | 获取服务器状态 | 注册公钥 | 产生密钥对 | 签名 | 解密 |
| 1000并发 | 响应时间（s） | 3.98 | 6.45 | 7.48 | 6.87 | 6.10 |
| 吞吐量（事务数/sec） | 244.8 | 150.9 | 130.1 | 141.7 | 159.6 |
| 成功率 | 99.88% | 100% | 100% | 100% | 100% |

1. 获取服务器状态：



1. 注册公钥：



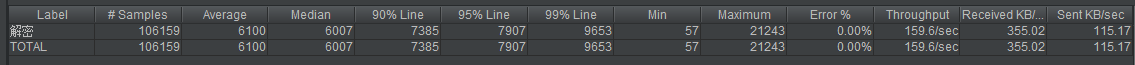
1. 产生密钥对：



1. 签名：1000并发



1. 解密



1. 在服务器含有10w+密钥对的情况下，对接口的签名、解密进行并发用户分别为50，100，300，500，800，1000的性能测试，测试结果如下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 并发数 | | 50 | 100 | 300 | 500 | 800 | 1000 |
| 签名 | 响应时间（s） | 0.38 | 0.80 | 2.11 | 3.44 | 5.50 | 6.87 |
| 吞吐量（事务数/sec） | 130.2 | 121.9 | 138.8 | 141.8 | 141.8 | 141.7 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |
| 解密 | 响应时间（s） | 0.34 | 0.63 | 1.72 | 3.00 | 4.79 | 6.10 |
| 吞吐量（事务数/sec） | 141.2 | 154.7 | 161.5 | 162.4 | 174.3 | 159.6 |
| 成功率 | 100% | 100% | 100% | 100% | 100% | 100% |

**签名**：

50并发：



100并发：



300并发：



500并发：



800并发：

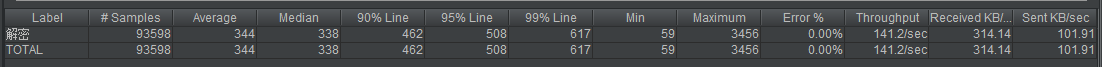


1000并发：



**解密**：

50并发：



100并发：



300并发：



500并发：



800并发：



1000并发：

