**时间戳服务器**

**Java语言接口使用规范**

北京神州安付科技股份有限公司

2023-03-16

目录

[1. 设备连接与关闭 3](#_Toc13333)

[1.1. 获取设备 3](#_Toc15139)

[1.2. 关闭设备 3](#_Toc15737)

[2. 设备接口描述 4](#_Toc553)

[2.1. 时间戳请求 4](#_Toc23152)

[2.2. 时间戳响应 4](#_Toc587)

[2.3. 时间戳请求并响应 4](#_Toc19864)

[2.4. 时间戳验证 4](#_Toc25669)

[2.5. 获取时间戳信息 5](#_Toc13040)

[2.6. 获取时间戳详细信息 5](#_Toc22919)

[3. 附录 5](#_Toc3565)

[3.1. TSMInfoFlag 获取时间戳详细信息 信息标识 5](#_Toc6251)

1. **设备连接与关闭**
   1. **获取设备**

|  |  |  |
| --- | --- | --- |
| 方法 | AFTSDevice device = new AFTSDevice.Builder("192.168.10.40", 8008, "abcd1234") // 服务器IP、端口、设备密钥为必须参数  //以下为可选参数 根据实际情况设置  .connectTimeOut(10000) // 连接超时时间，默认5秒  .responseTimeOut(100000) // 响应超时时间，默认10秒  .retryCount(3) // 重试次数，默认3次  .retryInterval(1000) // 重试间隔，默认1秒  .bufferSize(1024 \* 1024) // 缓冲区大小，默认1M  .channelCount(10) // 通道数，默认10个  .build(); | |
| 作用 | 获取设备 | |
| 参数 | connectTimeOut | 连接超时时间，默认5秒 |
| responseTimeOut | 响应超时时间，默认10秒 |
| retryCount | 重试次数，默认3次 |
| retryInterval | 重试间隔，默认1秒 |
| bufferSize | 缓冲区大小，默认1M |
| channelCount | 通道数，默认10个 |
| 返回值 | AFTSDevice | 时间戳服务器设备 |

* 1. **关闭设备**

|  |  |  |
| --- | --- | --- |
| 方法 | default void close(NettyClient client) | |
| 作用 | 与设备断开连接,释放连接资源 | |
| 参数 | client | 设备的连接客户端 |
| 调用 | device.close(AFTSDevice.getClient()); | device :时间戳服务器设备 |

1. **设备接口描述**
   1. **时间戳请求**

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] tsRequest(byte[] data, int reqType) throws AFCryptoException; | |
| 作用 | 获取时间戳请求 | |
| 参数 | data | 预加盖时间戳的用户信息 |
| reqType | 间戳服务类型 0代表响应包含TSA证书 1代表响应不包含TSA证书 |
| 返回值 | 时间戳请求信息数据（DER 编码） | |

* 1. **时间戳响应**

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] tsResponse(byte[] asn1Request) throws AFCryptoException; | |
| 作用 | 时间戳响应 | |
| 参数 | asn1Request | 时间戳请求信息数据（DER 编码） |
| 返回值 | 时间戳响应数据（DER 编码） | |

* 1. **时间戳请求并响应**

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] tsRequestAndResponse(byte[] data, int reqType) throws AFCryptoException; | |
| 作用 | 获取时间戳请求并响应 | |
| 参数 | data | 预加盖时间戳的用户信息 |
| reqType | 间戳服务类型 0代表响应包含TSA证书 1代表响应不包含TSA证书 |
| 返回值 | DER编码的时间戳 | |

* 1. **时间戳验证**

|  |  |  |
| --- | --- | --- |
| 方法 | public boolean tsVerify(byte[] tsValue, int signAlg, byte[] signCert) throws AFCryptoException; | |
| 作用 | 时间戳信息验证 | |
| 参数 | tsValue | 时间戳响应信息 |
| signAlg | 签名算法标识（SGD\_SM2|SGD\_SM2\_1|SGD\_SM2\_2|SGD\_SM2\_3） |
| signCert | TSA证书 |
| 返回值 | 验证结果 | |

* 1. **获取时间戳信息**

|  |  |  |
| --- | --- | --- |
| 方法 | public String getTsInfo(byte[] tsValue) throws AFCryptoException; | |
| 作用 | 获取时间戳信息 | |
| 参数 | tsValue | 时间戳响应信息 |
| 返回值 | 时间戳信息 | 格式: TSA通用名|签发时间 |

* 1. **获取时间戳详细信息**

|  |  |  |
| --- | --- | --- |
| 方法 | public byte[] getTsDetailInfo(byte[] tsValue, TSMInfoFlag infoFlag) throws AFCryptoException; | |
| 作用 | 获取时间戳信息 | |
| 参数 | tsValue | 时间戳响应信息 |
| infoFlag | 信息标识 定义在com.af.constant.TSMInfoFlag中 附录3.1 |
| 返回值 | 时间戳信息 | 格式: TSA通用名|签发时间 |

1. **附录**
   1. **TSMInfoFlag 获取时间戳详细信息 信息标识**
      1. STF\_TIME\_OF\_STAMP("签发时间", 0x00000001),
      2. STF\_CN\_OF\_TSSIGNER("签发者的通用名", 0x00000002),
      3. STF\_ORINGINAL\_DATA("时间戳请求的原始信息", 0x00000003),
      4. STF\_CERT\_OF\_TSSERVER("时间戳服务器的证书", 0x00000004),
      5. STF\_CERTCHAIN\_OF\_TSSERVER("时间戳服务器的证书链", 0x00000005),
      6. STF\_SOURCE\_OF\_TIME("时间源的来源", 0x00000006),
      7. STF\_TIME\_PRECISION("时间精度", 0x00000007),
      8. STF\_RESPONSE\_TYPE("响应方式", 0x00000008),
      9. STF\_SUBJECT\_COUNTRY\_OF\_TSSIGNER("签发者国家", 0x00000009),
      10. STF\_SUBJECT\_ORGNIZATION\_OF\_TSSIGNER("签发者组织", 0x0000000A),
      11. STF\_SUBJECT\_CITY\_OF\_TSSIGNER("签发者城市", 0x0000000B),
      12. STF\_SUBJECT\_EMAIL\_OF\_TSSIGNER("签发者联系电子邮箱", 0x0000000C);