

中安云科时间戳问题

1、颁发者证书

在获取时间戳应答的时候报错

```
2024-06-07 23:48:40.620 [http-nio-8090-exec-1] - 525 : Initializing Servlet 'dispatcherServlet'
2024-06-07 23:48:40.621 [http-nio-8090-exec-1] - 547 : Completed initialization in 1 ms
进入了时间戳测试函数
初始化服务连接: 0
STF_CreateTSResponse_Ex=MMCAQEWITA7BgUrbqMCGqUABBSpSo/1zLGbphxMCHP7kemHmC+70wIIaasled792fUBAf8=
STF_CreateTSResponse_ExLen=53
=====>STF_CreateTSResponse_Ex OK
创建请求成功
pucTSRequest: [48, 51, 2, 1, 1, 48, 33, 48, 9, 6, 5, 43, 14, 3, 2, 26, 5, 0, 4, 20, -87, 74, -113, -27, -52, -79, -101, -90, 28, 76, 8, 115, -45, -111, -23, -121, -104, 47, -69, -45, 2, 8, 105, -92, -91, 121, -34, -3, -39, -11, 1, 1, -1]
----->TSA_CreateTSResponse Err = 67149831
获取应答出错
pucTSResponse: null
开始验证有效性
时间戳无效
valid: 67149834
获取时间为空
date: null
获取通用名为空
about: null
TimeStampInfo(valid=false, about='null', time=null, timeStamp='null')
^C2024-06-07 23:49:11.283 [SpringContextShutdownHook] - 218 : Shutting down ExecutorService 'taskScheduler'
2024-06-07 23:49:11.284 [SpringContextShutdownHook] - 218 : Shutting down ExecutorService 'applicationTaskExecutor'
```

在文档中查了错误码（67149831），说是没有颁发者证书

| | | |
|-----------------------------|------------|------------|
| GM_ERR_NO_ISSUER_CERT | 0x0400A004 | 没找到颁发者证书 |
| GM_ERR_NO_SIGNER_ID | 0x0400A005 | 没有对应的证书 ID |
| GM_ERR_NO_SIGNER_PUBLIC_KEY | 0x0400A006 | 没有颁发者公钥 |
| GM_ERR_NO_SIGNER_SIGN_CERT | 0x0400A007 | 没有颁发者证书 |
| GM_ERR_SIGN_METHOD | 0x0400A008 | 签名算法错误 |
| GM_ERR_DIGEST_METHOD | 0x0400A009 | 摘要算法错误 |

我获取应答的函数如下

```
1 usage
private static byte[] getTSResponse(TSHandle handle, byte[] pucTSRequest){
    byte[] pucTSResponse = ZaTSAApi.STF_CreateTSResponse(handle, pucTSRequest, signAlg);
    if (Objects.isNull(pucTSResponse)) {
        assert handle != null;
        System.out.println("----->TSA_CreateTSResponse Err = " + handle.getErrCode());
    } else {
        System.out.println("TSA_CreateTSResponse=" + new String(Base64.encode(pucTSResponse)));
        System.out.println("TSA_CreateTSResponseLen=" + pucTSResponse.length);
        System.out.println("=====>STF_CreateTSResponse OK");
    }
    return pucTSResponse;
}
```

文档中的描述是这样的

2.4 生成应答数据

| | | |
|------|--|------|
| 功能描述 | 对明文数据进行摘要运算 | |
| 函数原型 | public static byte[] STF_CreateTSResponse(TSHandle handle, byte[] pucTSRequest, int signAlgID) | |
| 参数 | TSHandle handle | 句柄对象 |

| | | |
|-----|-------------------------------------|--------------|
| | byte[] pucTSRequest | 请求数据 |
| | int signAlgID | 签名算法，见附录 3.5 |
| 返回值 | !null - 执行成功 数据为应答数据 null - 执行错误 | |

并没有传入证书的参数，我不清楚这个颁发者证书是指什么

2、验证时间戳有效性证书

这是验证时间戳有效性的函数，需要传入参数cert证书

```
1 usage
private static int verifyValidity(TSHandle handle, byte[] pucTSResponse, byte[] cert){
    System.out.println("开始验证有效性");
    return ZaTSAApi.STF_VerifyTSValidity(handle, pucTSResponse, hashAlg, signAlg, cert);
}
```

文档描述如下

2.5 验证应答数据有效性

| | | |
|------|--|----------------|
| 功能描述 | 验证应答数据有效性 | |
| 函数原型 | public static int STF_VerifyTSValidity(TSHandle handle, byte[] pucTSResponse, int uiHashAlgID, int uiSignatureAlgID, byte[] pucTSCert) | |
| 参数 | TSHandle handle | 句柄对象 |
| | byte[] pucTSResponse | 应答数据 |
| | int uiHashAlgID | 摘要算法，见附录 3.4 |
| | int uiSignatureAlgID | 签名算法，见附录 3.5 |
| | byte[] pucTSCert | 证书数据，null 为不验证 |
| 返回值 | 0 -- 执行成功，验证通过 !=0 -- 验证失败，详见附录 | |

这个证书我没有，如果后续要测试的话，可能需要你提供