原文保全 API 对接指南

杭州天谷信息科技有限公司

2017 年 5 月 17

目 录

保密声明
本文档包含杭州天谷信息科技有限公司的专用商业信息和保密信息。本文档保密时间为 20 年。 接受方同意维护本文档所提供信息的保密性，承诺不对其进行复制，或向其他公司或个人公开此信息。对于以下三种信息，接受方可不向天谷公司承担保密责任： ● 可以通过其他渠道公开获得的信息； ● 天谷科技承诺可公开的信息； ● 已超过保密时间要求的信息。

文档修改记录			
序号	修改人	修改日期	修改内容
1	天云	2017-5-13	创建文档
2			
3			

原文保全 API 接口使用说明

1 重要提示

- 若未遇特别说明，所有接口调用时请采用 UTF-8 编码方式；
- 请求报文体采用 JSON 数据格式；
- 存证记录编号（eId）只有在成功上传文档后才生效，若获取到文档保全上传 Url 后 1 小时内未成功上传文档，则该存证记录编号（eId）失效需重新获取；
- 文档保全上传 Url 有效期为 1 小时，有效期内文档上传失败无需重新获取 Url，可再次上传；
- 存证记录编号（eId）和文档保全上传 Url 为一一对应关系且每次仅能上传一个文档；

2 获取原文保全 Url

简要描述：获取文档保全上传 Url 和存证记录编号（eId）

2.1 请求地址

测试环境地址：

http://smlcunzheng.tsign.cn:8083/evi-service/evidence/v1/preservation/original/url

正式环境地址：

http://evislb.tsign.cn:8080/evi-service/evidence/v1/preservation/original/url

2.2 请求方式

POST

2.3 Http 请求报文格式

参数名	必选	说明
X-timevale-project-id	是	项目名称
X-timevale-signature	是	请求签名信息<*点击查看获取方法*>
X-timevale-signature-algorithm	是	请求签名算法
X-timevale-mode	是	请求签名方式，仅支持 package
Content-Type	是	请求报文数据格式，仅支持 application/json

示例：

X-timevale-mode:package

X-timevale-project-id:1111563517

X-timevale-signature:515d0527c8d704536dde42df321fbb3e9f3a7fec35b0edf6d8f185c300dfbf48

X-timevale-signature-algorithm:hmac-sha256

Content-Type:application/json

2.4 请求参数

参数类型：JSON

参数名	必选	类型	说明
eviName	是	string	保全记录名称
content	是	Object	待保全内容对象
contentDescription	是	string	内容描述，如文件名等
contentLength	是	string	内容数据长度，如文件大小 单位：字节
contentBase64Md5	是	string	内容字节流MD5的Base64编码值，即文件MD5的Base64编码
eSignIds	是	List	电子签名证据ID列表，至少包含1个值： 0代表e签宝电子签名签署成功时返回的signServiceId签署记录ID 1代表e签宝时间戳服务成功时返回的timestampId时间戳数据记录ID
bizIds	否	List	e签宝业务ID列表： 0代表e签宝实名认证服务成功时返回的serviceId 实名认证请求ID

示例：

```
{
    "eviName":"我的原文保全",
    "content":{
        "contentDescription":"我的保全.pdf",
        "contentLength":245000,
        "contentBase64Md5":"XFW1JOIAF23AF13=="
    },
    "eSignIds":[{
            "type":0,
            "value":"862958877468037120"
      },{
            "type":1,
            "value":"456987-12f11230123-12ojawfowjfoj-afweafawfe"
      }],
    "bizIds":[{
            "type":0,
            "value":"3684eb08-f089-49f9-b5e3-bfa251669fe6",
      }]
}
```

2.5 返回参数

参数类型：JSON

参数名	类型	说明
url	String	文档保全上传 Url
eid	String	存证记录编号

示例：

{
"evid": "857628677268103170",
"url": "http://esignoss.oss-cn-hangzhou.aliyuncs.com/1111563789/e79ad7f6-4644-43f1-82a7-fdd6e38cb844/test.txt?Expires=1493313168&OSSAccessKeyId=STS.KDwv834X48FhHkN6ZYRoeoKWg&Signature=KyeFyCCPpYniS%2BJFmzNqA8aP1AQ%3D&callback-var=eyJ4OmZpbGVfa2V5IjoiJDM4ZTdhMjFkLTVlMDAtNDVlYy05OWJhLWZiYTQ5ZGQ4YWMzYiQ3Mzc4MDE1NzQifQ%3D%3D&callback=eyJjYWxsYmFja1VybCI6Imh0dHA6Ly8xMjEuNDAuNzkuMTAwOjgwODIvZmlsZS1zeXN0ZW0vY2FsbGJhY2svYWxpb3NzIiwiY2FsbGJhY2tCb2R5IjogIntcIm1pbWVUeXBlXCI6JHttaW1lVHlwZX0sXCJzaXplXCI6ICR7c2l6ZX0sXCJidWNrZXRcIjogJHtidWNrZXR9LFwib2JqZWN0XCI6ICR7b2JqZWN0fSxcImV0YWdcIjogJHtldGFnfX0iLCJjYWxsYmFja0JvZHlUeXBlIjogImFwcGxpY2F0aW9uL2pzb24ifQ%3D%3D&security-token=CAIS%2BAF1q6Ft5B2yfSjIqofCPYKH2YcVj4SDSk3/0loMXuBJgI78hTz2IHtKdXRvBu8Xs/4wnmxX7f4YlqB6T55OSAmcNZEoEDelGtDiMeT7oMWQweEurv/MQBqyaXPS2MvVfJ%2BOLrf0ceusbFbpjzJ6xaCAGxypQ12iN%2B/m6/Ngdc9FHHPPD1x8CcxROxFppeIDKHLVLozNCBPxhXfKB0ca0WgVy0EHsPnvm5DNs0uH1AKjkbRM9r6ceMb0M5NeW75kSMqw0eBMca7M7TVd8RAi9t0t1/IVpGiY4YDAWQYLv0rda7DOltFiMkpla7MmXqlft%2BhzcgeQY0pc/RqAAV9iORBvO5/IZQP0hOVfFbJmjX0lcMEZLqYOUG9GSImNNwOYty3xKdX92Xfh9oIGU91/DIOC1p1GINbbkXxfj7YxWPDjSOnCvNuLPlP9NrWSg8r0S3PT2DsW4FX4HvKX3fSdovVBuvt65Tv4wcgV1imCetrPo%2B1L0sJudjGYfY0b",
"errCode": 0,
"msg": "成功",
"success": true
}

3 文档保全上传

简要描述：将需要保全的文档通过 Url 上传

3.1 请求地址

既 2 获取原文保全 Url 请求返回的文档保全上传 Url

3.2 请求方式

PUT

3.3 Http 请求报文格式

参数名	必选	说明
Content-MD5	是	内容字节流 MD5 的 Base64 编码值，既文件 MD5 的 Base64 编码
Content-Type	是	请求报文数据格式，application/octet-stream

示例：

Content-MD5:XFW1JOIAF23AF13==
Content-Type:application/octet-stream

3.4 请求参数

参数类型：JSON

示例：文件的流数组

3.5 响应参数

HTTP 状态码 200 OK 表示文件上传成功。

4 请求签名信息获取方法

- 加密算法：HmacSHA256
- 参考网址：http://tool.oschina.net/encrypt?type=2
- 示例：

- 加密方法：

1. 准备 JSON 数据格式的请求参数；如：

```
{
    "eviName":"我的原文保全",
    "content":{
        "contentDescription":"我的保全.pdf",
        "contentLength":245000,
        "contentBase64Md5":"XFW1JOIAF23AF13=="
    },
    "eSignIds":[{
            "type":0,
            "value":"862958877468037120"
     },{
            "type":1,
            "value":"456987-12f11230123-12ojawfowjfoj-afweafawfe"
     }],
    "bizIds":[{
            "type":0,
            "value":"3684eb08-f089-49f9-b5e3-bfa251669fe6",
     }]
}
```

将请求参数作为明文，projectSecret 作为密钥，使用 HmacSHA256 进行加密即可获取到 X-timevale-signature 签名信息；

5 异常信息

- 获取 Url 失败，文件系统异常；
- 签名验签失败；
- 参数必填；
- 账户套餐余额不足，请先购买容量套餐；
- Url 需要在 1 小时内完成上传；
- 最大上传 50M 的内容
- 每类 ID 最多 10 个