

深圳前海微众银行股份有限公司

批量文件交互指南

文件修订历史

2017-10-20 V1.1	新建	沈立	
2018-07-16 V1.2		旷波	
2018-09-19 v1.3		旷波	
2018-12-13 v1.4	修改 CAP 配置申请方式	江鹤	
2019-04-22 v1.5	推送目录调整	旷波	
2019-07-05 v1.6	更正和删除部分描述	梁子敬	
2019-09-08 v2.0	影像文件打包给合作方	旷波	
2020-04-09 v2.1	影像文件目录与示例调整	旷波	

目 录

1 接入方式简介.....	3
2 文件接入流程.....	3
2.1 推送文件到合作方 sftp 模式接入流程.....	3
2.2 合作方从微众 sftp 拉取模式接入流程.....	4
2.3 合作方上传数据到微众 sftp 模式接入流程.....	4
2.4 微众从合作方 sftp 定时拉取模式接入流程.....	4
3 微众数据文件格式.....	4
3.1 结构化数据文件格式	4
3.2 媒体类数据文件格式	5
3.2.1 压缩包命名规范.....	5
3.2.2 包格式说明.....	6
4 合作方数据解析流程.....	7
5 结构化文件打包指引.....	7
6 媒体文件打包指引	8
7 媒体文件缺失重推指引.....	11
7.1 数据包及文件格式说明.....	11
7.2 数据包内容规范说明.....	12
8 sftp 公钥生成指引.....	13
附录:	14
签名验证示例.....	14

1 接入方式简介

微众与合作方的文件交互统一使用 sftp 协议，文件交互一共支持四种模式。

从数据的流向，文件交互方式可分为两大类：

1. 微众生产数据提供给合作方消费

按 sftp 服务器所在的不同，可细分为：

A) 推送文件到合作方 sftp

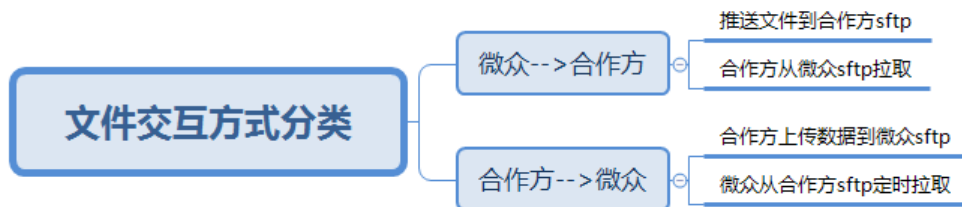
B) 合作方从微众 sftp 拉取

2. 合作方生产数据提供给微众消费

按 sftp 服务器所在的不同，可细分为：

A) 合作方上传数据到微众 sftp

B) 微众从合作方 sftp 定时拉取



特别说明：尽管支持四种推送拉取方案，但目前实现方式均采用 B 方案（文件放置产生方 SFTP），对于需要使用 A 方案的情况，需进行特殊说明。

微众产品方：需提前商定合作方渠道标识与产品编码，并提供给运维人员与文件开发人员。

注意下方的目录：渠道标识_业务标识，无特殊说明均为大写。

2 文件接入流程

2.1 推送文件到合作方 sftp 模式接入流程

1. 合作方建立 sftp 服务器，新建 sftp 帐号，在根目录下新建目录 webank_push。帐号需要对 webank_push 目录上传文件，创建目录，移动文件的权限。
2. 微众方运维团队与合作方运维团开通网络策略，双方进行环境联通性测试。
3. 微众方回复邮件，提供文件格式，文件内容说明。
4. 合作方参照合作方数据解析流程，解析文件数据并测试。
5. 于上线时间 T-2 日，配置生产环境，做生产环境联通性测试。

2.2 合作方从微众 sftp 拉取模式接入流程

1. 微众根据合作方简称提供 SFTP 帐号,并根据帐号生成 sftp 公钥。详见 sftp 公钥生产指南。
2. 微众方运维团队与合作方运维团开通网络策略,双方进行环境联通性测试。
3. 微众方回复邮件,提供文件格式,文件内容说明。微众生产的文件格式有两类,一日单批数据文件格式与一日多批数据文件格式。详见一日单批数据文件格式,一日多批数据文件格式。
4. 合作方参照合作方数据解析流程,解析文件数据并测试。
5. 于上线时间 T-2 日,配置生产环境,做生产环境联通性测试。

2.3 合作方上传数据到微众 sftp 模式接入流程

1. 微众根据合作方简称提供 SFTP 帐号,并根据帐号生成 sftp 公钥。详见 sftp 公钥生产指南。
2. 微众方运维团队与合作方运维团开通网络策略,双方进行环境联通性测试。
3. 合作方先上传文件到相应的上传目录,上传完成后,上传同名.check 文件,check 文件为文本格式,内容为文件的 MD5 值。比如上传 test.txt 到/webank/XX_REPORT/{yyyyMMdd}目录完成后,再上传 test.txt.check 到/webank/XX_REPORT/{yyyyMMdd}目录,test.txt.check 的文件内容为 test.txt 的 MD5 值。
4. 于上线时间 T-2 日,做生产环境联通性测试。

2.4 微众从合作方 sftp 定时拉取模式接入流程

1. 合作方建立 sftp 服务器,新建 sftp 帐号,在根目录下新建目录 webank。帐号需要对 webank 目录及所有子目录有下载权限。
2. 每一种类型的文件需要放在单独的文件夹,以当天时间 yyyyMMdd 为时间子目录,目录结构为/webank/渠道标识_业务标识/{yyyyMMdd}。比如提供媒体文件给微众,需要先创建/webank/XX_MEDIAFILE 父目录,每天创建子目录/webank/XX_MEDIAFILE/{yyyyMMdd}。2017 年 11 月 11 号的文件放在/webank/XX_MEDIAFILE/20171111 目录。2017 年 12 月 12 号的文件放在/webank/XX_MEDIAFILE/20171212 目录。
3. 参照媒体文件打包指引或结构化文件打包指引生成文件。详见结构化文件打包指引及媒体文件打包指引。
4. 上传文件到指定目录,与微众方联调。
5. 于上线时间 T-2 日,做生产环境联通性测试。

3 微众数据文件格式

以下为微众数据文件推送至合作方。

3.1 结构化数据文件格式

微众外送数据格式分为标准文件格式和非标准文件格式。其中标准文件格式是指 HIVE 出库

文件，非标准文件格式需与开发人员另行协定，其中标准文件格式可参考下图表述。

数据包及文件格式

概述：数据包目录结构及文件格式

.../表名_合作方简写_日期批次号.tar.gz^①
.../表名_合作方简写_日期批次号.tar.gz.check^②

解压目录结构：


```
.../表名_合作方简写_日期批次号  
|--表名③  
    md5sum.txt.asc④  
    signature.txt⑦  
    |--XXXXXX_X.gz⑤  
    |--XXXXXX_X.gz⑥  
    |--....
```

文件格式：

类型	编码	说明
gz编码	Utf-8	数据文件为gz压缩的utf-8编码的文本文件
字段分隔符	\001	数据文件中各字段分隔符，CTRL+A，ascii码1
行分隔符	\n	数据文件中换行符，ascii码10
md5sum.txt.asc	Utf-8	校验文件中每行字段以\t作为分隔符，格式：文件md5码+\t+压缩包全名，以\n作为换行符
signature.txt	Utf-8	Md5sum.txt.asc文件私钥签名

备注：

①：如tm_test_XXX_20010101.tar.gz
②：后缀为check的文件表示该数据包准备就绪
为了保证数据安全使用，里面存放md5值
WEBANK可对数据包以合作机构为单位进行对称加密；加密密码与合作方线下商定(建议采用8位以上数字字母组合)，也可以选择加密。
解密方法：ddif=\$(压缩包名) |openssl des3-d -k \$[密码] |tar xvfz -
③：贴源表名，如tm_test
④：合作机构简写，如上海合作方：SHB
⑤：同③
⑥：用于校验数据完整性的校验文件
⑦：签名文件，对md5sum.txt.asc签名，数据防篡改
⑧：数据文件的数量不固定，可能存在N个数据包。请先读取md5sum.txt.asc文件，根据文件中包括的文件名遍历读取文件并处理。



无论标准文件还是非标准文件，微众侧推送至合作方，有标准文件目录格式：

/webank_push/渠道标识_业务标识/{yyyyMMdd}。

- 1、文件放置微众服务器需严格按照上面目录标准。
- 2、文件放置合作方服务器可与开发协商确定文件目录和文件名形式。

入库说明：

check文件中包括了tar.gz数据包的MD5值，拉取数据后必须计算数据包的MD5值并与.check文件中的MD5对比，来校验文件的完整性，如MD5校验未通过，不能作入库处理。

3.2 媒体类数据文件格式

微众侧送给合作方文件，可进行签名与分包。由微众侧文件开发人员与合作方侧开发人员进行沟通商定，默认不分包不签名。

目录格式:/webank_push/渠道标识_业务标识/{yyyyMMdd}。目前由双发协商存放当前时间目录，还是业务时间目录。

3.2.1 压缩包命名规范

A. ZIP包命名：

文件头_业务标识_渠道标识_描述_分包标识_切包编号(是否签名).zip

文件名长度小于 512

字段说明：

- 文件头：数据时间-唯一标识 不定长
 - 数据时间：yyyyMMdd 8 位
 - 唯一标识：流水 ID（不定长，不固定）
- 业务标识：表示文件所属业务的缩写

- 渠道标识：表示文件所属渠道的缩写
- 描述：简要描述文件的用途等
- 分包标识：表示是否对文件根据指定字段进行分开打包。不分包-all；分包-分包字段内容（如用户的 id_no）
- 切包编号：确保包文件不超过 1G ， 001、002
- 是否签名：是针对原 zip 包签名，如签名则生成一个新 zip 包。签名-sign；不签名-无
- 分隔符使用双下划线，后缀统一使用 zip

示例：压缩包名字：20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001__sign.zip

B. ZIP 包对应 check 文件命名：

文件头__业务标识__渠道标识__描述__分包标识__切包编号(__是否签名).zip.check

说明：字段信息含义同包名，文件中内容为 zip 包 md5 值

示例：check 文件名字：20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001__sign.zip.check

3.2.2 包格式说明

A. 总包

所有文件打在一个 zip 包中，文件可以依据不同特性（如：客户编号、文件类型）归于到 zip 包中不同的文件夹。

示例：媒体文件包(总包)：

```
20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001.zip
20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001
|-- /{id_no-1}
|-- |-- /{file_type-1}
|-- |-- |-- /{file-1.jpg}
|-- |-- |-- /{file-2.pdf}
|-- |-- |-- /{file-3.txt}
|-- |-- /*
|-- /*
|-- |-- /*
```

示例：文件包签名：

```
20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001__sign.zip
|-- 20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__all__001.zip
|-- md5sum.txt.asc
|-- signature.txt
```

B. 分包

文件可以按商量的维度进行打包，如客户编号、文件类型等。

示例：媒体文件包(分包)：

```
20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__[order_no]__001.zip
|-- /{file_type-1}
|-- |-- /{file-1.jpg}
|-- |-- /{file-2.pdf}
|-- |-- /{file-3.txt}
|-- /*
|-- |-- /*
```

示例：媒体文件包(分包)签名：

```
20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__[order_no]__001__sign.zip
p
|--20181010-11015__ClaimConfirm__XB__ClaimConfirmFile__[order_no]__001.zip
|-- md5sum.txt.asc
|-- signature.txt
```

4 合作方数据解析流程

- 1.连接微众的 sftp 服务器，根据要获取的数据类型，cd 到相应的文件路径。见文件存放路径。
- 2.根据文件命名规范，在文件夹中遍历所有文件并下载符合文件命名的文件及相应.check 文件。
- 3.检查文件的 md5 值与.check 文件的 md5 值是否匹配。如不匹配，说明文件下载不完整，重新拉取。
- 4.解压 zip 文件。
- 5.运行以下命令做数字签名校验

```
openssl dgst -sha1 -keyform PEM -verify pubkey.pem -signature signature.txt md5sum.txt.asc
```

- 6.数字签名校验不通过，说明文件不合法，不处理。重新拉取文件。
- 7.按行读取 md5sum.txt.asc，每一行为 文件 MD5 文件名，用两个空格分隔，获取压缩包中含有的文件，根据文件名依次读取文件并处理。（注意压缩包中可能有多个文件，且文件名没有规律，所以一定要先读取 md5sum.txt.asc，根据信息摘要中描述的文件来处理）

5 结构化文件打包指引

以下为合作方结构化数据文件推送至微众。

结构化文件及 check 文件命名规范

结构化文件使用 zip 或者 tar.gz 包。 Check 文件存放压缩包的 MD5 值。**(MD5 值采用小写形式)**

媒体文件包名：TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip

Check 文件名：TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip.check

示例中，业务标识为 INSUREPOLICYINFO，渠道标识为[CHANNEL]；(此处的渠道标识与业务标识协商给出)

例如：TABLE_INSUREPOLICYINFO_[CHANNEL]_20170622_001.zip

TABLE_INSUREPOLICYINFO_[CHANNEL]_20170622_001.zip.check

结构化文件存放路径

微众拉取文件 sftp 目录结构：/webank/[CHANNEL]_[BUSSINESS]/[结构化文件批次号(YYYYMMDD)]/

比如 /webank/[CHANNEL]_INSUREPOLICYINFO/20170622

在批次目录下存放文件包及 check 文件，check 文件必须要有。

整体目录结构如下：

/webank/[渠道标识]_[业务标识]/[批次日期]/TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip

/webank/[渠道标识]_[业务标识]/[批次日期]/TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip.check

比例：

/webank

/[CHANNEL]_INSUREPOLICYINFO

/20170622

/TABLE_INSUREPOLICYINFO_[CHANNEL]_20170622_001.zip

/TABLE_INSUREPOLICYINFO_[CHANNEL]_20170622_001.zip.check

结构化文件内容规范

TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip 解压缩后的目录及文件如下：

/TABLE_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号]

/[表名].txt

文件格式：

类型	编码	说明
数据文件编码	Utf-8	数据文件为utf-8编码的文本文件
字段分隔符	\001	数据文件中各字段分隔符，CTRL+A， ascii码1
行分隔符	\n	数据文件中换行符， ascii码10

[表名].txt 为文件描述文件，要求**保证每个表只存在一个文件**，**文件名即约定表名**。如：

InsurePolicyInfo.txt

注意点

1. 必须要有 check 文件，并且 check 中存放 zip 包的 md5 值。
2. 文件及文件夹的命名必须严格按照此文档的规范，否则无法处理。
3. [表名].txt 的行分隔符为\n 列分隔符为\001。使用空格、Tab、|等其它分隔符无效。
4. [表名].txt 为文件描述文件，要求**保证每个表只存在一个文件**，**文件名即约定表名**。
5. 单个文件大小不要超过 1G，大文件请切分多个包传送。

6 媒体文件打包指引

以下为合作方媒体类数据文件推送至微众。

媒体文件及 check 文件命名规范

媒体文件使用 zip 或者 tar.gz 包。 Check 文件存放 zip 包 MD5 值。

媒体文件包名：MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip

Check 文件名：MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip.check

示例中 业务标识为 MEDIAFILE 渠道标识为 XX (此处的渠道标识协商给出, 业务标识固定为 MEDIAFILE)

例如：MEDIA_MEDIAFILE_XX_20170622_001.zip

MEDIA_MEDIAFILE_XX_20170622_001.zip.check

媒体文件存放路径

微众拉取媒体文件 sftp 目录结构：/webank/[CHANNEL]_[BUSSINESS]/[媒体文件批次号(YYYYMMDD)]/

比如 /webank/XX_MEDIAFILE/20170622

在批次目录下存放媒体文件包及 check 文件，check 文件必须要有。

整体目录结构如下：

/webank/[渠道标识]_[业务标识]/[批次日期]/MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip

/webank/[渠道标识]_[业务标识]/[批次日期]/MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip.check

比例：

/webank

/XX_MEDIAFILE

/20170622

/MEDIA_MEDIAFILE_XX_20170622_001.zip

/MEDIA_MEDIAFILE_XX_20170622_001.zip.check

媒体文件内容规范

MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号].zip 解压缩后的目录及文件如下：

/MEDIA_[业务标识]_[渠道标识]_[批次日期]_[3 位分包编号]

/MEDIA_RELATION.txt

/[业务主键]_[文件类型编号]_[3 位分页编号].jpg

MEDIA_RELATION.txt 为文件描述文件，必须要有。

里面的 MEDIA_RELATION.txt 结构如下：

第 1 列：（长度不超过 32）业务主键 - 根据 excel 中影像字典给出（app_no 或者 nbs_order_no）

第 2 列：（长度不超过 1）1:合作机构主键 0:WEBANK 业务主键 - 0 （使用 0）

第 3 列：（长度不超过 64）文件名称 - 格式为[影像字典给出：app_no 或者 nbs_order_no]_[文件类型编号]_[分页编号].[后缀]，例如 0000000000000001_002_001.jpg

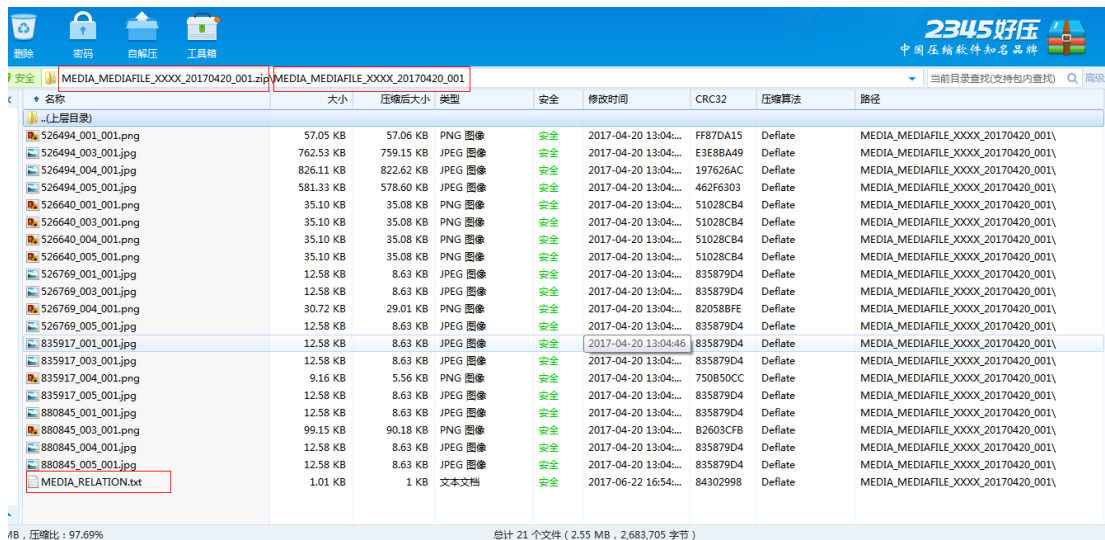
第 4 列：（长度不超过 12）业务标识 - MEDIAFILE

第 5 列：（长度不超过 16）渠道标识 - XX

第 6 列：（长度不超过 6）文件类型编号 - 002 （在接口文档中有具体的字典表,主要用于区分文件类型）

第 7 列：（长度不超过 10）3 位文件分页编号 - 001 （比例有一个合同共 5 页，将有 5 个 jpg 文件，文件名前面相同，分页编号_001,_002 等来区分不同页）

第 8 列：（长度不超过 32）备注 - NULL（暂未使用此字段，可留空）



注意点:

1. 必须要有 **check** 文件, 并且 **check** 中存放 **zip** 包的 **md5** 值。
2. 文件及文件夹的命名必须严格按照此文档的规范, 否则无法处理。
3. 必须要有 **MEDIA_RELATION.txt** 文件 (名称也必须一样, 比如改为 **media_relation.txt** 也无效)
4. **MEDIA_RELATION.txt** 的行分隔符为 **\n** 列分隔符为 **\001**。使用空格、Tab、|等其它分隔符无效。
6. **MEDIA_RELATION.txt** 中写入的文件名必须与文件内文件一一匹配。

微众压缩媒体包后先读取 **MEDIA_RELATION.txt**, 遍历每一行, 读取文件名及其它信息, 依次处理, 如果 **MEDIA_RELATION.txt** 中写入的文件在压缩包中不存在会报错。如果文件在压缩包

存在的文件没有在 MEDIA_RELATION.txt 中写入，同样会报错。

7. 单个 zip 压缩包大小不要超过 1G，日传输大小不要超过 10G（如果超过 10G，请提前告知我行进行评估）。

常见问题：

1. zip 包的 md5 值与 check 中的内容不匹配，check 文件为空或者内容不符。
2. sftp 服务器目录下只有 zip 包，未找到对应的 check 文件。
3. zip 包中的文件与 MEDIA_RELATION.txt 所描述不一致，如 txt 文件中有文件描述，zip 包没有对应的文件。
4. zip 包下应该有一层与包名同名的文件夹。

请合作方做好校验，避免出现上述问题。

媒体文件样本

此样本包含了

sftp 路径的样例 /webank/[CHANNEL]_MEDIAFILE/20170420/

媒体压缩包及 check 文件样例

MEDIA_MEDIAFILE_XXXX_20170420_001.zip

MEDIA_MEDIAFILE_XXXX_20170420_001.zip.check



webank.zip

7 媒体文件缺失重推指引

合作方根据约定传输用户相应的影像文件，我行会根据订单对用户进行影像件是否缺失的校验。将缺失文件列表打包存放在我行的 sftp 服务器目录下，需要合作方自行拉取，解析出订单的缺失数据择机进行补传。

7.1 数据包及文件格式说明

数据包及文件格式规范根据业务（BUSINESS）的不同，规范有所不同。
银团业务数据包及文件格式如下：

数据包及文件格式

概述：数据包目录结构及文件格式

.../表名_合作方简写_日期批次号.tar.gz^①
.../表名_合作方简写_日期批次号.tar.gz.check^②

解压目录结构：

.../表名^③
|--表名^④
 md5sum.txt.asc^⑤
 signature.txt^⑥
 |--XXXXXX_X.gz^⑦
 |--XXXXXX_X.gz^⑦
 |--....

文件格式：

类型	编码	说明
gz 编码	Utf-8	数据文件为gz压缩的utf-8编码的文本文件
字段分隔符	\001	数据文件中各字段分隔符, CTRL+A, ascii码1
行分隔符	\n	数据文件中换行符, ascii码10
md5sum.txt.asc	Utf-8	校验文件中每行字段以\t作为分隔符, 格式: 文件md5码+\t+压缩包全名, 以\n作为换行符
signature.txt	Utf-8	Md5sum.txt.asc文件私钥签名

备注：

①：如tm_test_XXX_20010101.tar.gz

②：后缀为check的文件表示该数据包准备就绪

为了保证数据安全使用, 里面存放md5值

WEBANK可对数据包以合作机构为单位进行对称加密; 加密密码与合作方线下商定(建议采用8位以上数字字母组合), 也可以选择加密。

解密方法: dd if=\${压缩包名} | openssl des3 -d -k \${密码} | tar xvfz -

③：贴源表名, 如tm_test

④：合作机构简写, 如上海合作方: SHB

⑤：同③

⑥：用于校验数据完整性的校验文件

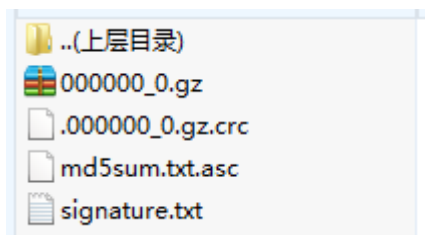
⑦：签名文件, 对md5sum.txt.asc签名, 数据防篡改

⑧：数据文件的数量不固定, 可能存在N个数据包。请先读取

md5sum.txt.asc文件, 根据文件中包括的文件名遍历读取文件并处理。

WeBank

表名_合作方简写(渠道标识)_日期批次号.tar.gz 解压缩后目录及文件如下：



7.2 数据包内容规范说明

7.2.1 check 文件内容规范

表名合作方简写日期批次号.tar.gz.check 内容：

表名合作方简写日期批次号.tar.gz 对应的 MD5 值 表名合作方简写日期批次号.tar.gz

如：文件 tm_media_type_missing_list_XXXX_20290925.tar.gz.check 里对应的内容：

44e6ec9837ef8dc2057a6ab2ef6ceca2 tm_media_type_missing_list_XXXX_20290925.tar.gz

7.2.2 txt 文件内容规范

xxxxxx_x.gz 解压后为 xxxxxx_x.txt 文件, 主要描述缺失文件信息。

第1列：id_no 身份证号

第2列：app_no 申请号

第3列：mer_loan_nbr 平台申请号

第4列：mer_order_no 平台订单号

第5列：nbs_order_no 订单号

第6列：miss_types 缺失类型列表, 以 '|' 为分割符, 将缺失的文件类型编号连接成字符串格式,

如：101|102|002 (缺失文件类型为 101,102,002。可参考产品编号对应文件类型编号,文件类型 101 是

融资租赁合同，102 是车辆抵押合同，002 是承租人身份证）。

注意点：

xxxxxx_x 行分隔符为\n 列分隔符为\001。 使用空格、Tab、|等其它分隔符无效。

媒体文件样本

此样本包含了

sftp 路径的样例 /webank_push/[CHANNEL]_[BUSINESS]/20290925/

媒体压缩包及 check 文件样例

tm_media_type_missing_list_XXXX_20290925.tar.gz

tm_media_type_missing_list_XXXX_20290925.tar.gz.check



tm_media_type_missing_list_XXXX_20290925.tar.gz.check



tm_media_type_missing_list_XXXX_20290925.tar.gz

合作方收到媒体文件缺失列表后，根据文件中所描述的内容，将对应用户订单的影像文件在新的一个日期批次补传给我行，传输协议依据第 7 章节。

8 sftp 公钥生成指引

要求合作放的 ssh 是 6.0 以上版本，生成公钥的方法如下：

1. 合作方切换到要访问我们 sftp 目录的用户下面；如用 test 账号登录我行 sftp 服务器，先切换到 test 用户下

```
su test
```

2. 运行 ssh-keygen -t rsa -b 1024

生成公钥过程中不要输入密码

```
ssh-keygen -e -f $HOME/.ssh/id_rsa.pub > test
```

把生成用户名这个文件发给我们

私钥请妥善保管，切勿丢失！

待网络防火墙开通后，使用我行提供的 NAT IP 登录服务器

方式一：

```
sftp -oport=57000 test@NAT_IP
```

方式二：

指定私钥路径登录

```
sftp -oIdentityFile=/test/.ssh/id_rsa -oport=57000 test@NAT_IP
```

附录：

签名验证示例

验证签名 java：使用 SHA256WithRSA

```
public static RSAPublicKey getPublicKey(String keyStr) throws InvalidKeyException, NoSuchAlgorithmException {
    byte[] buffer = Base64.decodeBase64(keyStr);
    X509EncodedKeySpec keySpec = new X509EncodedKeySpec(buffer);
    KeyFactory keyFactory = KeyFactory.getInstance("RSA");
    return (RSAPublicKey) keyFactory.generatePublic(keySpec);
}

public static boolean verify(RSAPublicKey key, byte[] content, byte[] signedContent) throws SignatureException, NoSuchAlgorithmException, InvalidKeyException {
    Signature verify=Signature.getInstance("SHA256WithRSA");
    verify.initVerify(key);
    verify.update(content);
    return verify.verify(signedContent);
}
```

公钥：

请咨询平台开发。