**区块链授权存证**

**系统方案说明书**

# 版本

|  |  |  |
| --- | --- | --- |
| **日期** | **修订人** | **修订内容** |
| 2018-01-02 | 缪君 | 初稿 |
| 2018-02-06 | 缪君 | 补充APP SDK说明，完善用户直接授权流程 |

# 目标简述

在当前的互联网金融领域中，用户数据使用授权，一直是监管部门、金融机构、数据源等各方关注和头疼的问题，接入方式不统一、用户体验一般、过程难以监管和溯源都是当前已有数据授权方案存在的弊端。

享宇金服推出的基于区块链超级账本技术的授权存证系统（以下简称存证系统），正是针对这一系列问题而专门设计和研发的，目标是构建一个包括监管部门、金融机构、数据源、数据加工方的机构联盟，要求联盟内各机构自律且互信，共享合作关系下的用户数据使用授权，统一技术接口和业务流程，并对授权和鉴权行为进行不可篡改的存证，确保行为记录可监管、可溯源。

机构联盟基于自律互信和用户直接授权原则，要求用户在金融机构办理业务时，通过区块链SDK和系统接口，直接将个人数据使用授权写入区块链系统；区块链系统记录授权后通过SDK返回消息通知金融机构，金融机构在获取授权成功通知后，即可向数据源、数据加工方申请获取该用户的数据，其他两方将对区块链系统中记录的授权信息进行确认，确认通过则以双方确认安全的方式发送数据。监管机构对以上所有流程具备完全监管权限，确保各方行为合规有效。

# 存证方式

基于采用用户的直接授权模式的原因，存证系统要求金融机构使用的授权方式和采集的授权数据，必须满足以下要求，达到1次授权，在有效期和限定范围内可以重复使用，不需要再次授权的目标：

1. 信息电子化– 授权信息必须电子化，以确保授权信息可以完整被记录和上链
2. 用户身份标识 – 授权信息必须包含能够确确认用户唯一身份的标识信息，以确保授权信息的准确、真实和完整

根据以上要求，存证系统对记录的授权信息内容框架进行统一，确认授权信息和鉴权信息必须包含以下内容：

**授权信息**

1. 授权金融机构信息
2. 授权用户信息
3. 授权时间

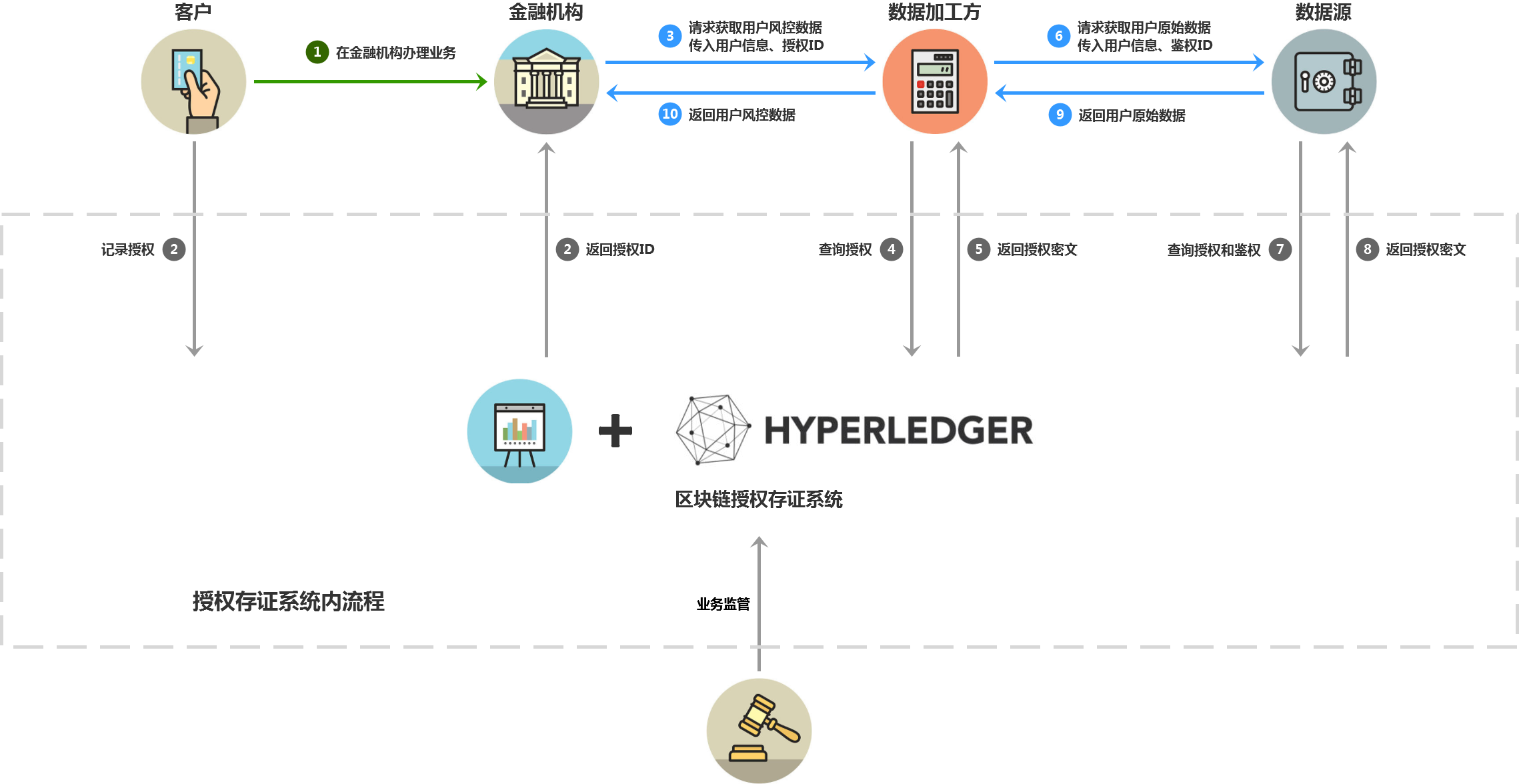
**鉴权信息**

1. 鉴权机构信息
2. 被鉴权机构信息
3. 被鉴权的记录流水号
4. 被鉴权的记录类型
5. 鉴权时间

因授权信息中包含了用户的个人信息，因此存证系统将采用行为记录的逻辑进行授权和鉴权存证，即存证系统仅对授权和鉴权行为进行存证，授权内容的真实有效，由机构自行判断，从而减少用户信息外流的可能性

# 业务流程

存证系统业务流程图如下：



如图所示：

1. 客户在金融机构办理业务时，使用金融机构APP进操作；
2. 因业务需要，用户在APP中填写个人信息
3. 用户填写信息完成后，APP可先进行信息验真，再调用SDK，确保上链数据真实有效
4. APP调用SDK，传入用户个人信息和选择的加密方式，SDK完成信息加密，将加密信息写入区块链；区块链系统写入完成后，将授权记录流水号（以下称为授权ID）返回给SDK，SDK返回给APP
5. 获取授权ID后，在需要使用客户数据时，金融机构与数据加工方之间，按双方约定的方式，进行数据请求，金融机构在请求时将授权ID传给数据加工方
   1. 由于双方有数据合作关系，所以数据加工方可获取被请求用户的个人信息，可自行将个人信息按相同方式加密得到密文
6. 数据加工方获取授权ID后，通过存证系统API查询授权记录，记录存在则存证系统以API返回的方式向数据加工方回传授权信息的密文数据、数据类型和加密方式
   1. 除密文数据外，存证系统也会返回本次授权记录查询行为在区块链系统中生成的鉴权记录的流水号（鉴权ID）
7. 数据加工方获取授权密文数据和加密方式后，先使用线下获取的用户信息进行加密，生成比对密文，然后将授权密文与自己生成的比对密文进行比对，如果一致则表示授权有效，可向金融机构返回该用户数据
8. 同理，数据加工方（或金融机构）向数据源请求获取用户数据时，也是按双方约定的方式进行，只是数据加工方（或金融机构）会向数据源提供鉴权ID（金融机构提供授权ID）；而数据源通过存证系统API，对记录进行查询，获取密文数据后进行校验比对，成功则向数据加工方（或金融机构）返回用户数据
9. 监管机构在存证系统中，可查看所有记录的流水号，并获取对应的密文数据，但出于对用户数据保密的要求，监管机构获取密文数据后，需要向用户请求获取其个人数据，用于自行比对授权数据是否正确有效。

# 监管机制

监管机制是基于存证系统和机构联盟处于监管机构监管的前提，设定的一套基于系统功能和联盟工作流程的规则办法，用于规范联盟机构行为，从监管的满足解决存证系统的合规需求。

## 机构准入

任何机构加入存证联盟，必须向监管机构提交加入申请，并签订联盟合作协议，同意遵守机构联盟的共识规则，接受监管机构的授权业务监管。

机构确认接受后，监管机构为机构分配存证系统使用账号，并根据机构角色，赋予账号相应的角色和权限，并监督机构进行系统接入和流程改造。

机构获取使用账号、接入文档和SDK资源后，按存证系统要求进行SDK接入，接入完成后，向监管机构提交系统接入完成说明，确认合规。

监管机构确认后，向机构联盟公布该机构接入存证系统。

## 系统监管

在存证系统运行过程中，监管机构可随时对系统业务数据进行监察，监管机构通过存证系统管理后台，可查看授权信息完整的记录链，从授权开始，到授权查验，再到鉴权查验，对授权流转、操作机构和记录数据进行一一查验。

同时，出于监管需要，监管机构可要求金融机构配合，进行授权用户信息的查验，即金融机构与存证系统进行对接，监管机构在管理后台抽查某一授权记录的用户信息，存证系统从金融机构请求获取该用户的真实信息，然后存证系统模拟查验过程，比对真实信息加密所得密文，与授权记录的密文是否一致，一致表示查验通过。

## 机构禁用

在监管过程中，如监管机构发现某一机构存证违规行为，则可第一时间在存证系统管理后台禁用该机构的系统账号；

禁用后该机构将无法参与存证系统操作，即不会出现更多的违规记录；

然后监管机构可发起对该机构的违规调查，通过对已有记录进行查验，确认该机构的违规事实，给出相应处罚。

# 上链数据

## 授权上链数据

授权上链数据是指金融机构将用户对其数据使用授权写入区块链的记录

|  |  |
| --- | --- |
| 上链数据 | 说明 |
| 记录流水号 | 记录的流水号 |
| 授权时间 | 授权的日期时间，采用系统记录时间，格式为yyyy-mm-dd hh:mm:ss |
| 授权有效时间 | 授权的到期时间，根据金融机构调用SDK时传入有效期进行换算，格式为yyyy-mm-dd hh:mm:ss |
| 授权机构编号 | 授权（写入）机构在区块链系统中的编号，以SDK配置为准 |
| 数据加密方式 | 用户个人信息加密的方式，SDK支持多种符合国家法规要求的加密标准，以供金融机构选择 |
| 用户密文数据 | 用户个人信息加密后数据 |

## 鉴权上链数据

鉴权上链数据是指数据源、数据加工方对用户授权校验查询的行为记录

|  |  |
| --- | --- |
| 上链数据 | 说明 |
| 记录流水号 | 记录的流水号 |
| 鉴权时间 | 查验的日期时间，采用系统记录时间，格式为yyyy-mm-dd hh:mm:ss |
| 鉴权机构编号 | 查验机构在区块链系统中的编号 |
| 授权流水号 | 被查验的授权记录流水号 |
| 鉴权流水号 | 被查验的鉴权记录流水号 |

# SDK说明

## SDK功能

存证系统SDK，用于嵌入金融机构APP进行用户授权操作。

SDK功能如下：

|  |  |
| --- | --- |
| SDK功能 | 说明 |
| 流水凭证接口 | 用于前端调用，生成流水凭证接口 |
| 用户授权接口 | 用于前端调用，写入用户授权信息 |
| 数据加密模块 | 用于对用户数据进行不可逆加密，得到用户信息密文 |
| 授权写入模块 | 用于将用户信息密文及相关授权信息写入存证系统区块链 |

### 流水凭证接口

流水凭证接口是金融机构APP/H5前端嵌入SDK后，可调用的接口，用于产生授权流水凭证号。

请求参数：无

返回参数：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| 流水凭证号 | encryptContent | String | SDK按算法产生的授权流水凭证号，全局唯一 |

### 用户授权接口

用户授权接口是金融机构APP/H5前端嵌入SDK后，可调用的接口，用于直接向区块链系统写入用户授权。

请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 机构token | token | String | Y | 系统分配的机构唯一token，用于标记校验机构权限 |
| 流水凭证号 | encryptContent | String | Y | SDK按算法产生的授权流水凭证号，全局唯一 |
| 用户姓名 | name | String | Y | 用户的姓名 |
| 用户身份证 | idcard | String | Y | 用户的身份证号码 |
| 用户手机 | mblno | String | Y | 用户的手机号码 |
| 用户银行卡 | bankcard | String | Y | 用户的银行卡号 |
| 机构签名私钥 | signPrivateKey | String | Y |  |
| 联盟签名公钥 | signPublicKey | String | Y |  |
| 加密方式 | encryption | String | Y | 选择的加密方式  包括SHA和SM3 |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| body(json域) | recordNo | String | 记录流水号 |
| 错误消息 | errMsg | String | 错误消息描述 |
| 错误码 | errorCode | Int | 0为通过，其他值为错误 |
| 业务消息 | message | String | 保留字段 |

### 用户数据加密

用户数据加密为SDK内部功能，即用户授权接口接到用户数据后，必须先使用用户数据加密功能，将收到的用户信息进行加密处理，然后再写入区块链

功能入参

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 用户姓名 | name | String | Y | 用户的姓名 |
| 用户身份证 | idcard | String | Y | 用户的身份证号码 |
| 用户手机 | mblno | String | Y | 用户的手机号码 |
| 用户银行卡 | bankcard | String | Y | 用户的银行卡号 |
| 加密方式 | encryption | String | Y | 选择的加密方式  包括SHA和SM3 |

功能返回

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| 密文 | encryptContent | String | 用户信息加密内容 |

用户信息加密排序必须为姓名、手机、身份证、银行卡

按以下JSON格式进行组装：

{"realName":"肖宇舟",

"mobile":"13912341234",

"idCard":"5101230000000000",

"bankCard":""

},将组装后的JSON字符串在进行加密处理。

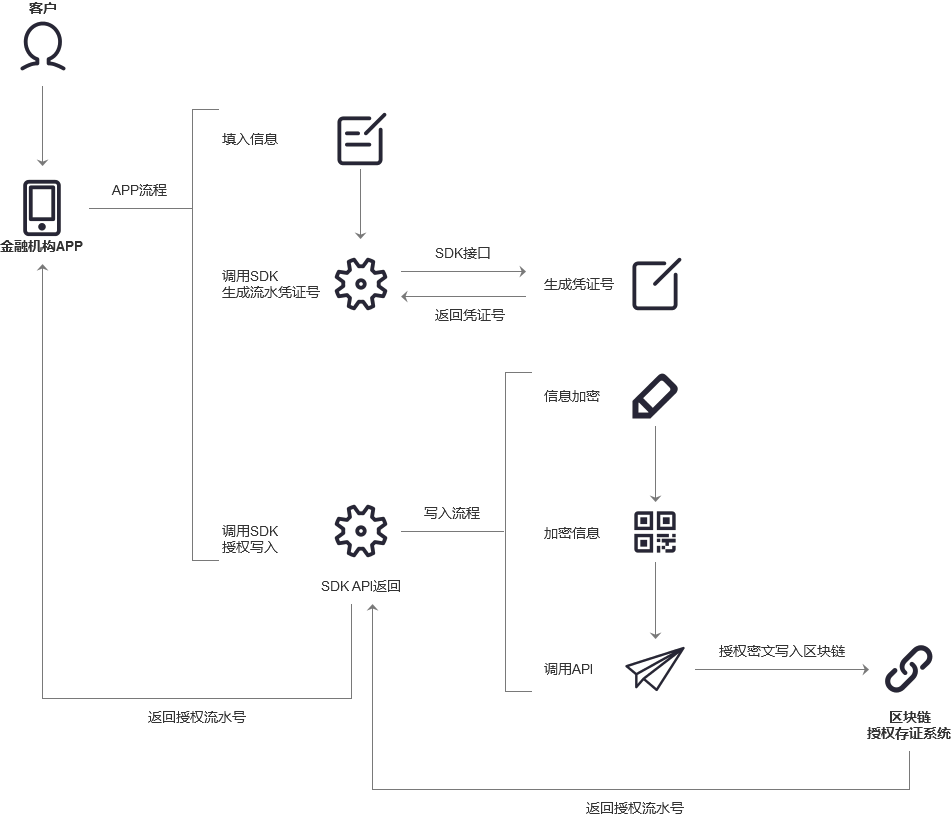
若value等于null,需要设置成""(空字符串)

### 授权写入模块

授权写入模块为SDK内部功能，即调用区块链授权存证系统的授权存证接口，进行授权写入。

## SDK授权流程

SDK工作流程图如下：



如图所示：

1. 用户在金融机构APP中填写完个人信息后，APP调用SDK
2. APP先调用SDK接口，生成本次授权流水的凭证号
   1. 凭证号用于标记本次授权记录，以便金融机构在因网络异常未收到授权流水号时，通过后端接口进行查询
3. 生成授权流水凭证号之后，APP调用SDK接口，向SDK传入用户的个人信息，指定加密方式
4. SDK根据传入的信息和加密方式，对用户个人信息进行加密
5. 加密完成后，SDK调用存证系统API，将授权信息写入区块链
6. 区块链写入完成后，存证系统将授权流水号返回给SDK，SDK再将授权流水号返回给金融机构APP

# 接口说明

## 授权流水查询接口

说明：需要进行查询SDK写入授权的流水是否成功时，调用该接口

接口地址：https://blockchain.xyebank.com/api/v1/authentication/authorizeSNCheck/

请求方式：POST

请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 机构token | token | String | Y | 系统分配的机构唯一token，用于标记校验机构权限 |
| 授权流水凭证号 | auzCertificateNo | String | Y | SDK按算法产生的授权流水凭证号，全局唯一 |
| 签名 | signature | String | Y |  |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| body(json域) | authorizeNo | String | 授权流水对应的授权存证记录的流水号 |
| 错误消息 | errMsg | String |  |
| 错误码 | errorCode | Int | 0为通过，其他值为错误 |
| 业务消息 | message | String | 备用字段 |
| 签名 | signature | String |  |

## 授权存证接口

说明：SDK调用该接口写入授权，该接口仅限SDK调用

接口地址：https://blockchain.xyebank.com/api/v1/authorize/

请求方式：POST

请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 机构token | token | String | Y | 系统分配的机构唯一token，用于标记校验机构权限 |
| 密文 | encryptContent | String | Y | 加密内容 |
| 加密方式 | encryption | String | Y | 加密方式  暂时支持：  SM3 |
| 授权流水凭证号 | auzCertificateNo | String | Y | SDK按算法产生的授权流水凭证号，全局唯一 |
| 有效时间 | activeTime | String | Y | 授权的到期时间  格式yyyy-MM-dd HH:mm:ss |
| 签名 | signature | String | Y |  |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| body(json域) | recordNo | String | 记录的流水号 |
| 错误消息 | errMsg | String |  |
| 错误码 | errorCode | Int | 0为通过，其他值为错误 |
| 业务消息 | message | String | 备用字段 |
| 签名 | signature | String |  |

## 授权查验接口（鉴权）

说明：需要进行授权记录查验（鉴权）时，调用该接口

接口地址：https://blockchain.xyebank.com/api/v1/authentication/auzCheck/

请求方式：POST

请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 机构token | token | String | Y | 系统分配的机构唯一token，用于标记校验机构权限 |
| 授权ID | authorizeNo | String | Y | 要查验的授权记录流水号 |
| 签名 | signature | String | Y |  |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| body(json域) | recordNo | String | 记录流水号 |
| encryptContent | String | 用户信息加密文本 |
| encryption | String | 加密方式 |
| authorizeOrgNo | String | 授权机构编号 |
| authorizeTime | String | 授权时间 |
| isVaild | Boolean | 授权是否有效 |
| 错误消息 | errMsg | String | 错误消息描述 |
| 错误码 | errorCode | Int | 0为通过，其他值为错误 |
| 业务消息 | Message | String | 保留字段 |
| 签名 | signature | String |  |

## 鉴权查验接口

说明：需要进行鉴权记录查验时，调用该接口

https://blockchain.xyebank.com/api/v1/authentication/aucCheck/

请求方式：POST

请求参数：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 必填 | 备注 |
| 机构token | token | String | Y | 系统分配的机构唯一token，用于标记校验机构权限 |
| 鉴权ID | authorizeNo | String | Y | 要查验的授权查验记录流水号（鉴权ID） |
| 签名 | signature | String | Y |  |

返回参数

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 参数名称 | 类型 | 备注 |
| body(json域) | recordNo | String | 记录流水号 |
| encryptContent | String | 用户信息加密文本 |
| encryption | String | 加密方式 |
| authorizeOrgNo | String | 授权机构编号 |
| authorizeTime | String | 授权时间 |
| isVaild | Boolean | 授权是否有效 |
| authenticateOrgNo | String | 鉴权机构编号 |
| authenticateTime | String | 鉴权时间 |
| 错误消息 | errMsg | String | 错误消息描述 |
| 错误码 | errorCode | Int | 0为通过，其他值为错误 |
| 业务消息 | message | String | 保留字段 |
| 签名 | signature | String |  |

## 签名机制

### 概述

为保证数据传输过程中的真实性，完整性和不可抵赖，双方需要对数据进行数字签名，机构在接收签名数据之后必须进行签名校验。

首先，对报文中出现签名域之外的所有数据元采用**key=value** 的形式按照key升序排序，然后以&作为连接符拼接成待签名串(value 为空的域，不参与待签名串，签名之前的value不要做URL编码操作,signature不参与签名)。使用机构 RSA 私钥证书对待签名串做签名操作。

最后，将签名后的签名串放在签名表单域里和其他表单域一起通过Https Post 的方式传输给授权存证系统平台。

### 加签说明

请求前：

token=xxxx&encryptContent=xxxx&encryption=1&authorizeTime=xxxx&activeTime=xxxx&auzCertificate=xxxx&versionNo=1.0.0

排序后：

activeTime=xxxx&authorizeTime=xxxx&auzCertificate=xxxx&encryptContent=xxxx&encryption=1&token=xxxx&versionNo=1.0.0

将排序后的值，使用自己RSA私钥进行签名(与提交给授权存证系统的公钥必须为一对)，得到签名字符串signature，将signature追加到表单域中提交给授权存证系统。

### 验签说明

首先判断返回内容中，errorCode是否为0(成功)，非0不做验签处理。

业务系统取出body中的元素，将参数排序后(signature不参与),使用授权存证系统公钥验证排序后的签名是否与signature一致。

## 错误码

|  |  |
| --- | --- |
| 错误码 | 错误描述 |
| 0 | 业务发起成功 |
| -1 | 系统异常 |
| 900001 | 读写集不合法，读写集为空或者count为0！ |
| 900002 | 返回值中ChaincodeID为空！ |
| 900003 | 至少有1节点背书失败 |
| 900007 | 区块链查询失败 |
| 900013 | 鉴权记录不存在！ |
| 900014 | 鉴权记录对应的授权记录不存在！ |
| 900015 | 授权关系不存在！ |
| 900019 | 授权ID不能为空 |
| 900020 | 授权ID/鉴权ID不能都为空 |
| 900021 | 授权ID/鉴权ID不能同时传入 |
| 900022 | 身份不合法，鉴权失败！ |
| 900101 | 身份不合法，写入授权失败！ |
| 900102 | 授权时间必须传递，格式为: yyyy-MM-dd HH:mm:ss |
| 900103 | 授权时间不合法，请检查！ |
| 900104 | 授权有效时间必须传递，格式为: yyyy-MM-dd HH:mm:ss |
| 900105 | 授权有效时间不合法，请检查！ |

## 机构编码（测试阶段）

|  |  |  |
| --- | --- | --- |
| 编码 | 机构名称 | 类型 |
| XYZFFCMX | 享宇金服蜂巢模型 | 数据加工方 |
| YDSJD | 移动手机贷 | 金融机构 |
| SCYD | 四川移动 | 数据源 |