UniTrust 数字身份卡包

SaaS 服务规范

上海市数字证书认证中心有限公司
2024 年 4 月

文档修订历史

序号	版本	修订章节	修订说明	修订日期	修订人
1	V1.0	全文	第一版，编制卡包 DID SaaS 服务规范	2024-04-09	高泽晨 王天华

1. 文档说明

1.1. 文档目的

本文档适用于客户端应用对接 UniTrust 数字身份卡包（下称：身份卡包）的可控匿名的分布式数字身份 SaaS 服务（下称：SaaS 服务）。

1.2. 文档范围

本文档规定了身份卡包对外提供的 SaaS 服务能力以及接入规范。

1.3. 阅读对象

本文档面向想要对接或了解身份卡包 SaaS 服务的产品经理、项目经理、设计人员、开发人员、测试人员等。

1.4. 术语和定义

下列术语和定义适用于本文档。

术语	定义
数字证书	也称公钥证书，由证书认证机构(CA)签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。
私钥	非对称密码算法中只能由拥有者使用的不公开密钥
DID	DID 是全球唯一的标识符，不需要集中的注册机构。DID 通用格式由方案标识符 did、did 方法标识符和 did 方法定义的唯一、方法特定的标识符组成（如 "did:example:123456789abcdefghi"）。DID 用于唯一标识任何实体对象，包括人、机、物。

DID 文档	DID 文档是描述 DID 主体的一组数据，包括公钥加密、与 DID 主体交互相关的服务等机制。DID 主体或 DID 委托可以使用这些机制来证明自己与 DID 的关联。
VC	可验证凭证 VC 是可以通过密码学验证的防篡改的身份凭证。可验证凭证可以代表物理凭证所代表的所有相同信息。依靠数字签名等技术，可验证凭证比相应物理凭证更防篡改、更值得信赖。
VP	可验证表达 VP 由 VC 持有者基于 VC 派生，向验证者表达自己 VC 的部分身份属性。VP 是可以通过密码学验证的防篡改的身份表达，具有选择性披露和隐私保护的特点。
数字身份卡包	面向个人和法人用户提供的移动端数字身份管理软件，围绕合规合法的可信数字身份构建用户自我主权身份，帮助用户基于真实身份生成并管理可控匿名的分布式数字身份，承载并管理用户身份证明、数字资产等信息，提供安全、可靠、便捷的各类数字身份使用能力。

2. SaaS 服务介绍

2.1. SaaS 服务形态

身份卡包 SaaS 服务提供一组 H5 页面和 REST Web API 接口，应用开发者可以通过访问 H5 页面和调用 API 接口来使用可控匿名的分布式数字身份服务。

2.2. SaaS 服务特点

- 可控匿名

在个人信息保护的前提下，实现身份信息的用户自主可控、跨平台互认、凭证可溯源，并为机构提供更便捷、高效、安全的用户身份接入和认证方式。

- 多维认证

面向法人和自然人分别提供多维度的认证方式，针对不同应用场景提供各种安全可靠的用户身份信息真实性核验服务。

- 权威可信

服务对接的数据源均采用国家和行业的权威数据源，核验结果真实可靠。

- 服务灵活

可根据不同业务场景动态配置 SaaS 服务能力，应用一旦接入，无需二次开发。

- 部署方便

支持公有云和混合云部署模式，可根据行业特性和业务要求使用不同的部署模式。

- 安全可靠

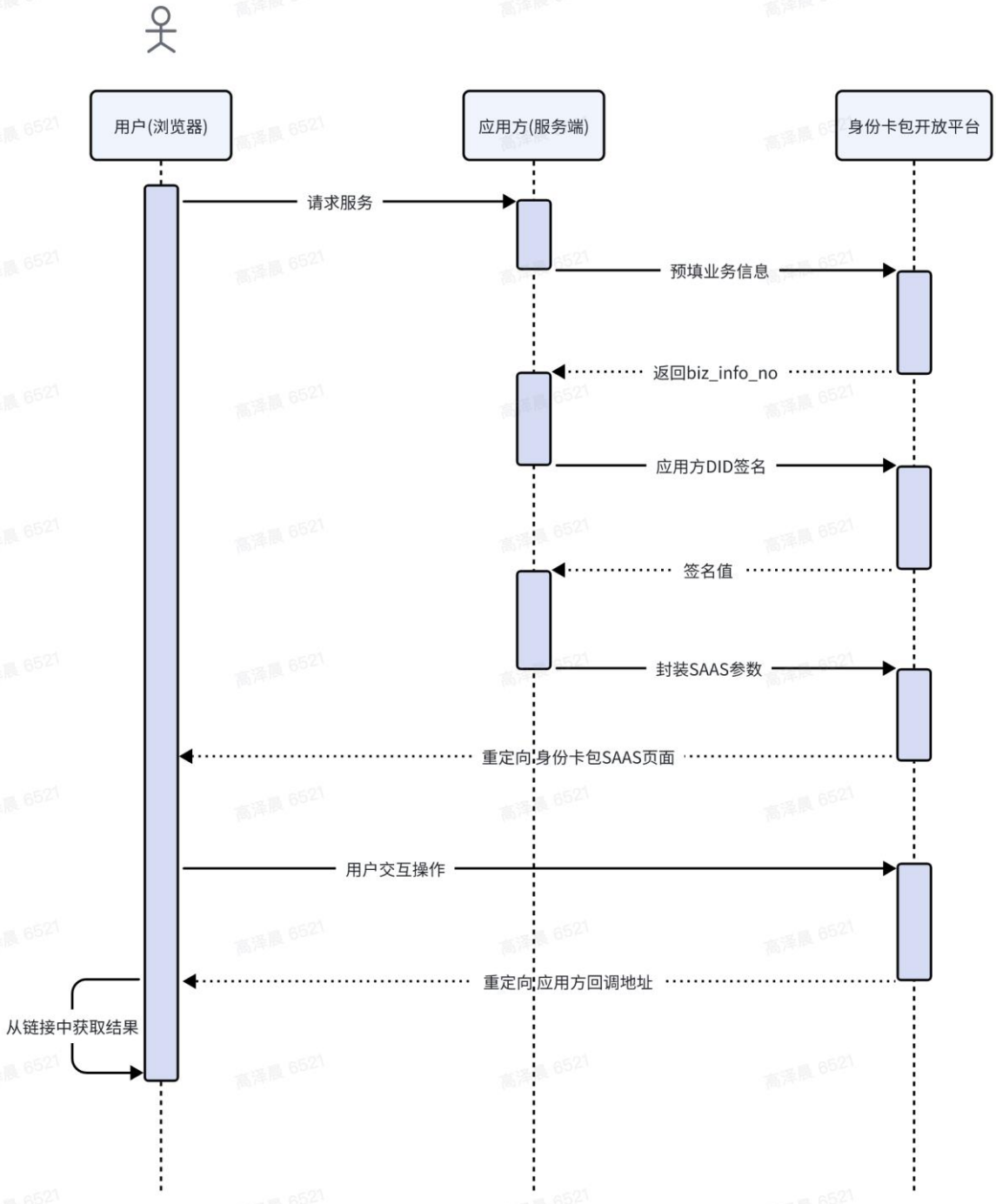
从网络传输、数据管理等各个环节保障数据安全，并使用数字签名和数据加密技术，访问过程安全可靠。

- 集成简单

分布式数字身份服务页面由身份卡包统一提供，大大减少接入应用的开发和测试工作量。

2.3. SaaS 服务调用过程

身份卡包 SaaS 服务总体调用过程如下图所示。



1. 接入方从身份卡包运营方获取访问 SaaS 服务所需的应用唯一标识（client_id）、应用密钥（client_secret）和访问地址（baseUrl）。
2. 接入方按照以下格式拼接 URL 访问，进入数字身份卡包 SAAS 服务页面：

```
https://{baseUrl}/did/person/create?client_id={your_client_id}&redirect_uri={your_redirect_uri}&timestamp=1712557113282&app_biz_no={your_bussinessNo}&biz_info_no=123456&signature=xxxxxxxxx
```

redirect_uri: 接入方给定的回调地址，必须提供 https 域名。

biz_info_no：访问 API 接口中“预填业务信息”相关接口获得。

signature ： 使用 did 私钥签名，可访问 API 接口中的“接入方 DID 签名”获得。

3. 用户在身份卡包页面进行操作（如进行身份核验、设置身份口令等），操作成功后，身份卡包会重定向至接入方给定的回调地址（redirect_uri），并返回相应的业务响应参数。
4. 接入方获取业务响应参数，进行后续业务操作。

3. H5 服务接口规范

3.1. 自然人注册 DID

- 服务描述

接入方需要为自然人用户注册 DID 时，重定向到该 H5 服务页面。该服务进行自然人用户实名认证，申领数字证书，生成用户实名 DID 和可控匿名的应用级 DID，创建自然人区块链可信账户，并注册到身份链上。

- 服务地址

https://{baseUrl}/id_wallet/did/person/create

- 请求方式

GET

- 请求参数

参数名称	类型	必选	参数说明
client_id	String	是	应用唯一标识符
redirect_uri	String	是	应用回调地址
timestamp	String	是	13 位系统时间戳（链接存在时效性，时间戳必须和北京时间一致保证每次时间戳都是最新的，时间上下容错 5 分钟否则链接失效）
app_biz_no	String	是	应用业务流水号，由接入方生成。 一般用于双方业务对账或问题诊断。

biz_info_no	String	否	用户信息流水号。 调用“预填业务信息-自然人注册 DID”接口获得。 系统判断该参数以决定是否进行隐式认证： 1.当传入此参数时，进行隐式认证。 2.未传入此参数时，用户需要进行“手机号实名+人脸识别”实人认证。
signature	String	是	签名值：对 client_id + client_secret +timestamp 进行拼接后，使用 did 私钥签名。 该参数调用“接入方 DID 签名”接口获得。

- 请求示例

```
https://{baseUrl}/id_wallet/did/person/create?client_id={your_client_id}&redirect_uri={your_redirect_uri}&timestamp=1712557113282&app_biz_no={your_bussinessNo}&biz_info_no=123456&signature=xxxxxxxxx
```

- 响应参数

用户操作成功后，身份卡包会重定向至接入方给定的回调地址 redirect_uri，并在链接后拼接上以下参数：

参数名称	**类型**	**必选**	**参数说明**
did	string	是	自然人 DID
app_biz_no	string	是	接入方业务流水号

- 响应示例

```
https://{redirect_uri}?did=12345678&app_biz_no=12345678
```

3.2.法人注册 DID

- 服务描述

接入方需要为法人用户注册 DID 时，重定向到该 H5 服务页面。该服务在法人用户使用法人一证通登录后，生成法人用户实名 DID 和可控匿名的应用级 DID，创建法人区块链可信账户，并注册到身份链上。

- 服务地址

https://{baseUrl}/id_wallet/did/corporation/create

- 请求方式

GET

- 请求参数

参数名称	类型	必选	参数说明
client_id	String	是	应用唯一标识符
redirect_uri	String	是	应用回调地址
timestamp	String	是	13 位系统时间戳（链接存在时效性，时间戳必须和北京时间一致保证每次时间戳都是最新的，时间上下容错 5 分钟否则链接失效）
app_biz_no	String	是	应用业务流水号，由接入方生成。 一般用于双方业务对账或问题诊断。
biz_info_no	String	是	业务信息流水号。 调用“预填业务信息-法人注册 DID”接口获得。
signature	String	是	签名值：对 client_id + client_secret +timestamp 进行拼接后，使用 did 私钥签名。 该参数调用“接入方 DID 签名”接口获得。

- 请求示例

```
https://{baseUrl}/id_wallet/did/corporation/create?client_id={your_client_id}&redirect_uri={your_redirect_uri}&timestamp=1712557113282&app_biz_no={your_bussinessNo}&biz_info_no=123456&signature=xxxxxxxxx
```

- 响应参数

用户操作成功后，身份卡包会重定向至接入方给定的回调地址 redirect_uri，并在链接后拼接上以下参数：

参数名称	类型	必选	参数说明
did	string	是	自然人 DID
app_biz_no	string	是	接入方业务流水号

- 响应示例

```
https://{redirect_uri}?did=12345678&app_biz_no=12345678
```

3.3.自然人 DID 签名

- 服务描述

接入方需要自然人用户进行 DID 签名时，重定向到该 H5 服务页面。该服务显示待签名信息，用户确认并输入身份保护口令后，解锁 DID 私钥进行数据签名。

- 服务地址

https://{baseUrl}/id_wallet/did/person/sign

- 请求方式

GET

- 请求参数

参数名称	类型	必选	参数说明
client_id	String	是	应用唯一标识符
redirect_uri	String	是	应用回调地址
timestamp	String	是	13 位系统时间戳（链接存在时效性，时间戳必须和北京时间一致保证每次时间戳都是最新的，时间上下容错 5 分钟否则链接失效）
app_biz_no	String	是	应用业务流水号，由接入方生成。 一般用于双方业务对账或问题诊断。
biz_info_no	String	是	业务信息流水号。 调用“预填业务信息-DID 签名”接口获得。
signature	String	是	签名值：对 client_id + client_secret +timestamp 进行拼接后，使用 did 私钥签名。 该参数调用“接入方 DID 签名”接口获得。

- 请求示例

```
https://{baseUrl}/id_wallet/did/corporation/create?client_id={your_client_id}&redirect_uri={your_redirect_uri}&timestamp=1712557113282&app_biz_no={your_bussinessNo}&biz_info_no=123456&signature=xxxxxxxxx
```

- 响应参数

用户操作成功后，身份卡包会重定向至接入方给定的回调地址 redirect_uri，并在链接后拼接上以下参数：

参数名称	类型	必选	参数说明
signature	string	是	使用 DID 私钥签名待签名数据的签名值
app_biz_no	string	是	接入方业务流水号

- 响应示例

```
https://{redirect_uri}?signature=xxxxxxxxxxxxxxxxxxxxxxx&app_biz_no=12345678
```

4. API 接口规范

4.1. 接口公共说明

所有接口未经特殊说明情况下，应以 REST 接口形式提供，所有涉及编码处理的都应采用 UTF-8 编码。所有接口请求调用时需使用 HTTPS 协议（TLS1.2 及以上），以保证数据传输过程中的机密性和完整性。

4.2. 接口鉴权

为保证 API 调用过程的安全可靠，API 除了统一采用 HTTPS 传输协议外，还需要进行安全接入鉴权认证。平台提供“OAuth2.0 鉴权”这种安全接入鉴权认证方式。

4.2.1 OAuth2.0 鉴权说明

OAuth2.0 鉴权方式采用标准的 OAuth2.0 Client Credentials 方式进行认证鉴权，用来授权第三方应用，获取接口调用权限。

接入方必须预先登记，以便于获取由平台分配的两个应用身份识别码：应用唯一标识（client_id）和应用密钥（client_secret）。应用登记由平台管理员进行登记，并将创建成功的 client_id 和 client_secret 发送至应用联系人邮箱。

接入方调用平台业务 API 之前，需要先调用【申请接口访问令牌】接口，根据 client_id 和 client_secret 申请一个短期的接口访问令牌。接入方成功获取接口访问令牌后，可以访问平台的业务 API，但需要在 HTTP 请求头中携带平台自定义参数

“access_token”，以传入接口访问令牌。其请求头格式如下：

参数名称	类型	必选	参数说明
client_id	String	是	应用唯一标识，由平台分配
access_token	String	是	接口访问令牌
Content-Type	String	是	application/json; charset=UTF-8

4.2.2 申请接口访问令牌

- 接口描述

根据 client_id 和 client_secret 申请接口访问令牌（token）。后续在 token 有效期内接入方可以通过 token 获取业务接口调用权限。token 有效时长为 7200 秒。当 token 即将到期时需要调用接口重新获取 token。

平台服务端允许接入方多次获取 token，但只有最新获取的 token 有效。之前的 token 会失效，无权调用业务 API 接口。如果接入方同时有多台服务器调用 API 接口，建议统一处理 token 以确保其唯一性。

- 接口地址

/auth/token

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
client_id	string	是	应用 id，由平台分配
client_secret	string	是	应用密钥，由平台分配，不可泄露

- 请求示例

```
{
  "client_id": "b09db3feb12924be37",
  "client_secret": "8613*E1574A651CFEE"
```

```
}
```

- 响应参数

用户操作成功后，身份卡包会重定向至接入方给定的回调地址 redirect_uri，并在链接后拼接上以下参数：

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息
result	object	是	返回结果集，json 格式，详见明细
┝access_token	String	是	应用访问令牌
┝expires_in	String	否	令牌有效时间（秒）

- 响应示例

```
{
   "code": 0,
   "msg": "success",
   "result": {
      "access_token": "07268da35051a0e29b595a1b0e1486e4",
      "expires_in": "7200"
   }
}
```

4.3. 通用返回结果

每个 API 接口的返回结果均为 JSON 字符串，示例如下：

{"code":int,"msg":String,"result":String}

字段定义如下：

参数名称	类型	必选	参数说明

code	int	是	返回码，0 表示成功。
msg	String	是	返回消息。多用于描述请求失败时的错误信息。
result	String	否	返回结果集。多用于描述请求成功时返回的业务数据。 若无返回数据，该字段的值为空。

4.4. API 接口说明

4.4.1 接入方 DID 签名

- 接口描述

使用接入方 DID 私钥对数据进行签名。

- 接口地址

https://{baseUrl}/id_wallet/api/did/client/escrow/sign

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
client_did	String	是	接入方 DID
plain_text	String	是	待签名原文

- 请求示例

```
{
  "client_did": "07268da35051a0e29b595a1b0e1486e4",
  "plain_text": "待签名原文"
}
```

- 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息

result	object	是	返回结果集，json 格式，详见明细
├ signature	String	是	签名值

- 响应示例

```
{
   "code": 0,
   "msg": "success",
   "result": {
      "signature": "07268da35051a0e29b595a1b0e1486e4"
   }
}
```

4.4.2 预填业务信息-自然人注册 DID

- 接口描述

自然人用户已实名认证时，接入方可以通过后端安全信道调用该接口，预先注册自然人实名身份信息进行隐式实名认证，以跳过身份卡包后续实人认证环节，减少用户交互。

- 接口地址

https://{baseUrl}/id_wallet/api/did/person/create/info

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
name	String	是	用户姓名
id_type	String	是	证件类型，默认值：1-身份证
id_no	String	是	证件号码
mobile	String	是	手机号码

- 请求示例

```
{
   "name": "user name" ,
   "id_type": "1" ,
   "id_no": "123456789012345678",
   "mobile": "13312341234"
}
```

- 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息
result	object	是	返回结果集，json 格式，详见明细
├ biz_info_no	String	是	用户信息流水号

- 响应示例

```
{
   "code": 0,
   "msg": "success",
   "result": {
      "biz_info_no": "1234567890"
   }
}
```

4.4.3 预填业务信息-法人注册 DID

- 接口描述

接入方可以通过后端安全信道调用该接口，预先注册法人数字证书信息，以减少前端交互信息量。

- 接口地址

https://{baseUrl}/id_wallet/api/did/corporation/create/info

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
cert	String	是	法人数字证书，base64 编码格式

- 请求示例

```
{
   "cert": "法人数字证书 Base64 编码"
}
```

- 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息
result	object	是	返回结果集，json 格式，详见明细
├ biz_info_no	String	是	预填业务信息流水号

- 响应示例

```
{
   "code": 0,
   "msg": "success",
   "result": {
      "biz_info_no": "1234567890"
   }
}
```

4.4.4 预填业务信息-自然人 DID 签名

- 接口描述

接入方可以通过后端安全信道调用该接口，预先注册待签名信息，以避免敏感信息通过不安全的前端信道传递时泄露。

- 接口地址

https://{baseUrl}/id_wallet/api/did/person/sign/info

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
person_did	String	是	自然人 DID
plain_text	String	是	待签名原文

- 请求示例

```
{
  "person_did": "07268da35051a0e29b595a1b0e1486e4",
  "plain_text": "待签名原文"
}
```

- 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息
result	object	是	返回结果集，json 格式，详见明细
├ biz_info_no	String	是	预填业务信息流水号

- 响应示例

```
{
```

```
  "code": 0,
  "msg": "success",
  "result": {
     "biz_info_no": "1234567890"
  }
}
```


4.4.5 自然人注册子 DID

- 接口描述

接入方可以通过后端安全信道调用该接口，在某个父场景（如碳普惠）DID 名下注册子场景（如公交出行）DID，以按需建立层级可控匿名身份。

- 接口地址

https://{baseUrl}/id_wallet/api/did/person/create/child

- 请求方式

POST

- 请求参数

参数名称	类型	必选	参数说明
parent_did	String	是	父场景下自然人 DID
parent_client_did	String	是	父场景接入方 DID，如碳普惠管理平台
child_client_did	String	是	子场景接入方 DID，如上海公交、申通地铁、美团单车等
app_biz_no	String	是	应用业务流水号，由接入方生成。 一般用于双方业务对账或问题诊断。
signature	String	是	签名值：对 person_did + parent_client_did + child_client_did + app_biz_no 进行拼接后，使用父场景 client_did 私钥签名。

			该参数调用“接入方 DID 签名”接口获得。

- 请求示例

```
{
   "parent_did": "11148da35051a0e29b595a1b0e1486e4",
   "parent_client_did": "06068da35051a0e29b595a1b0e1486e4",
   "child_client_did": "07268da35051a0e29b595a1b0e14793",
   “app_biz_no“:“your_bussinessNo“，
    "signature": "07268da35051a0e29b595a1b0e1486e4"
}
```

- 响应参数

参数名称	类型	必选	参数说明
code	int	是	返回码，0 表示成功
msg	String	是	返回消息，多用于描述请求失败时的错误信息
result	object	是	返回结果集，json 格式，详见明细
⊦ child_did	string	是	子场景自然人 DID
⊦ app_biz_no	string	是	接入方业务流水号

- 响应示例

```
{
   "code": 0,
   "msg": "success",
   "result": {
      "child_did": "83648da35051a0e29b595a1b0e140726",
      "app_biz_no": "1234567890"
   }
}
```