

矩阵元 MPC Demo 用户手册

矩阵元技术（深圳）有限公司

文档控制

更改记录

日期	版本	更改人	审批人	更改条款及内容
2017-09-12	V1.0	毕淦欣	姜珍	新建

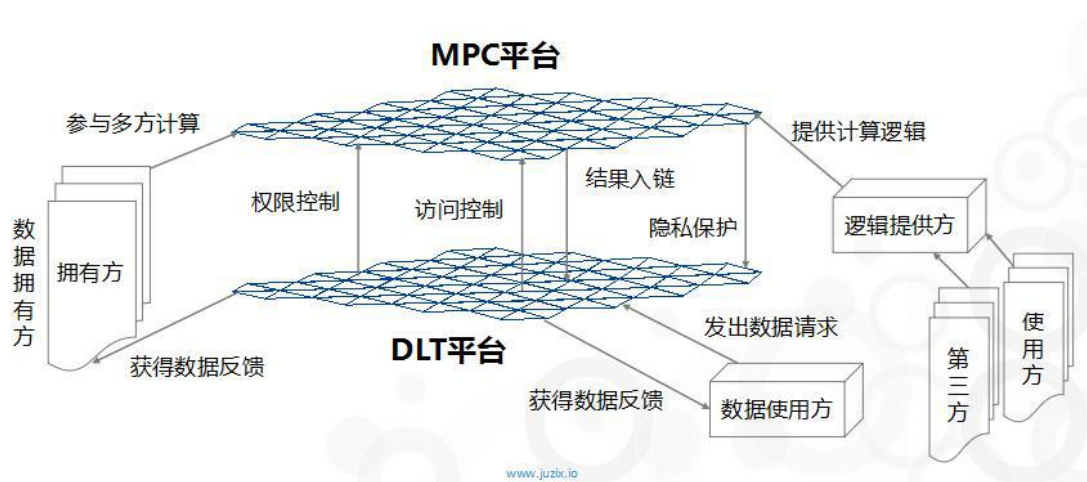
目录

第 1 章 产品简介	3
第 2 章 产品主要功能说明	4
2.1 注册用户	4
2.2 恢复私钥	4
第 3 章 产品详细操作说明	5
3.1 注册用户	5
3.2 删除私钥	9
3.3 恢复私钥	11

第 1 章 产品简介

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC 是在该价值理念下的解决方案与工程实现。借助矩阵元的 MPC 框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

矩阵元将 MPC 与区块链两种数据治理方案进行结合，让区块链基于隐私保护、权限控制、不可伪造篡改等特性为 MPC 提供可信的数据计算参与方；MPC 平台基于 OT 协议完成可信的数据计算并将结果入链作为存证。



本 Demo 基于 MPC（多方安全计算）实现了一个区块链私钥的安全备份方案

1. 通过人脸识别等生物特性实现对账户私钥的加密存储与备份
2. 通过人脸识别等生物特性实现对账户私钥的快速恢复

第 2 章 产品主要功能说明

2.1 注册用户

用户注册时在本地生成账户私钥，并进行人脸识别，将自己的生物特征（人脸特征）作为 MPC 输入与业务系统进行 MPC 计算，对私钥进行加密，私钥加密结果保存在安全的业务系统中。

2.2 恢复私钥

用户在私钥丢失或者不小心删除之后，可通过人脸识别，将自己的生物特征（人脸特征）作为 MPC 输入与业务系统进行 MPC 计算，对私钥进行解密，解密成功，客户端即可获取丢失的私钥

第 3 章 产品详细操作说明

3.1 注册用户

用户下载并安装完 App 后，启动 App 进入 MPC 应用首页，点击【注册用户】，进入注册流程。

基于MPC的私钥恢复

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC是在该价值理念下的解决方案与工程实现。借助矩阵元的MPC框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

本应用展示了基于矩阵元MPC框架应用于私钥恢复的方案

您可以通过以下流程体验该方案：



第1步：注册用户

注册时，用户私钥除了本地保存，还将通过您的人脸识别生物特征进行MPC加密安全保存在远程。注册后，您可以登录使用系统。



第2步：删除私钥

为了体验MPC私钥恢复，您可以手动删除本地用户私钥，然后再恢复私钥。删除后，您将无法登录使用系统。



第3步：恢复私钥

当本地私钥遗失或者被手动删除后，您可以通过提交您的人脸识别生物特征从远程将私钥进行MPC恢复到本地，从而正常使用系统。

[登录](#)

点击【注册用户】，进入注册流程

注册流程：

- 1、输入账户信息：姓名、身份证号、手机号、登录密码
- 2、人脸识别：按照操作引导，进行人脸识别

矩阵元技术（深圳）有限公司

5

3、完成注册

下午3:41

< 返回 用户注册

1 账户信息 2 人脸识别 3 完成注册

姓名 请输入姓名

身份证 请输入身份证号码

手机号 请输入手机号

密码 请输入密码(8-20位, 英文和数字组合)

确认密码 确认密码

下一步

输入账户信息：姓名、身份证号、手机号、登录密码

下午3:43

< 返回 用户注册

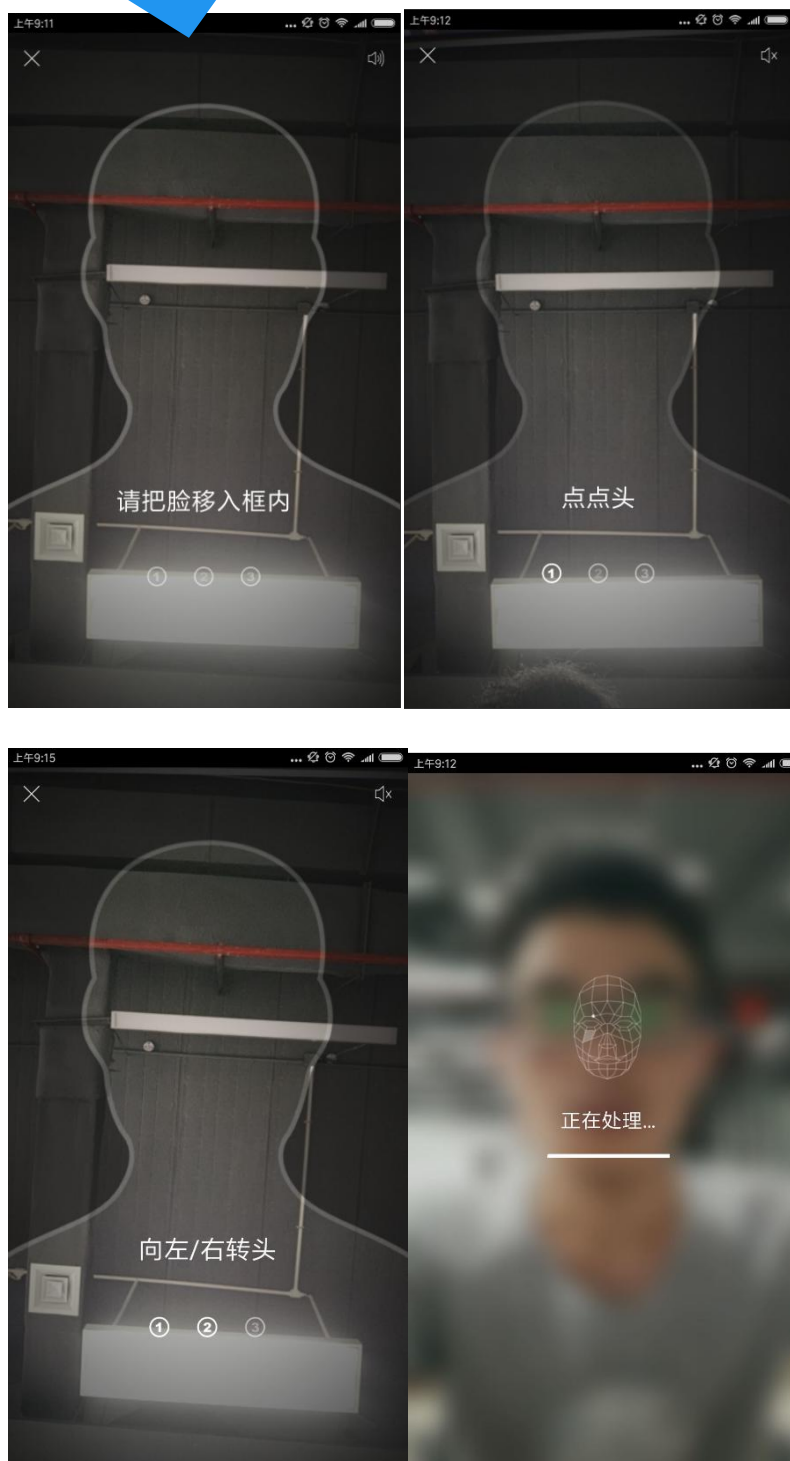
1 账户信息 2 人脸识别 3 完成注册

请将脸置于提示框内，并按提示做相应动作！

开始识别

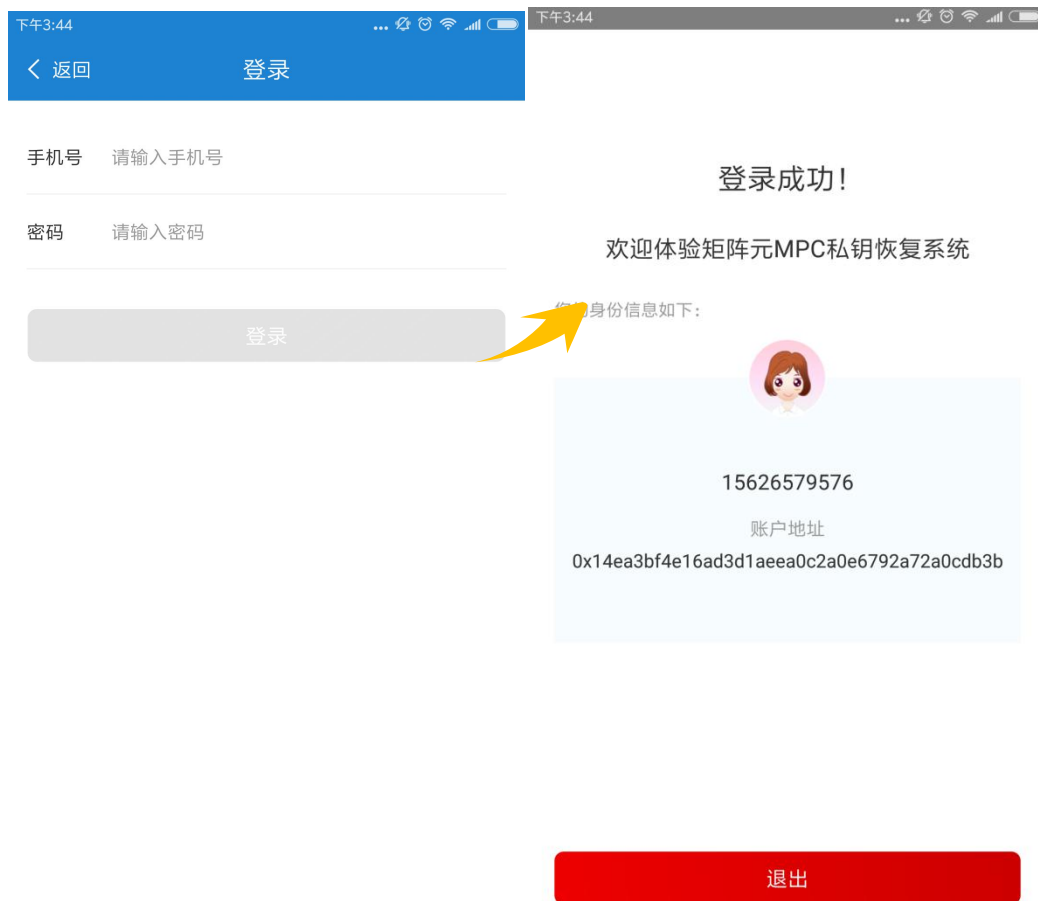
点击【开始识别】按钮
进入人脸识别流程

按照操作引导，完成人
脸识别





注册完成可进行登录验证，点击【去登录】进入登录页面，输入刚注册的手机号、登录密码，点击【登录】，如果成功进入“登录成功欢迎页面”，则表示注册成功！



3.2 删除私钥

为体验 MPC 私钥恢复，在当前注册手机上，点击【删除私钥】，在弹出的确认提示框中，点击【确认】，即可删除本地手机所有私钥文件；

PS：如果有两部手机，可以直接在另一部手机上进行【恢复私钥】操作

基于MPC的私钥恢复

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC是在该价值理念下的解决方案与工程实现。借助矩阵元的MPC框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

本应用展示了基于矩阵元MPC框架应用于私钥恢复的方案

您可以通过以下流程体验该方案：



第1步：注册用户

注册时，用户私钥除了本地保存，还将通过您的人脸识别生物特征进行MPC加密安全保存在远程。注册后，您可以登录使用系统。



第2步：删除私钥

为了体验MPC私钥恢复，您可以手动删除本地用户私钥，然后再恢复私钥。删除后，您将无法登录使用系统。



第3步：恢复私钥

当本地私钥遗失或者被手动删除后，您可以通过提交您的人脸识别生物特征从远程将私钥进行MPC恢复到本地，从而正常使用系统。

登录

点击【删除私钥】，弹出确认框

基于MPC的私钥恢复

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC是在该价值理念下的解决方案与工程实现。借助矩阵元的MPC框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

本应用展示了基于矩阵元MPC框架应用于私钥恢复的方案

您可以

私钥删除确认？

私钥是您登录系统和资产所有权的唯一凭证。
确定删除吗？

取消

确认



第2步：删除私钥

为了体验MPC私钥恢复，您可以手动删除本地用户私钥，然后再恢复私钥。删除后，您将无法登录使用系统。



第3步：恢复私钥

当本地私钥遗失或者被手动删除后，您可以通过提交您的人脸识别生物特征从远程将私钥进行MPC恢复到本地，从而正常使用系统。

登录

点击【确认】，即可删除本地私钥

删除完成，可点击【登录】进入登录页面，输入手机号、密码，点击【登录】可以验证当前私钥文件已不存在，无法登录！

基于MPC的私钥恢复

可信的数据交换、有价值的数据传递是矩阵元在数据安全领域秉持的价值理念，MPC是在该价值理念下的解决方案与工程实现。借助矩阵元的MPC框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

本应用展示了基于矩阵元MPC框架应用于私钥恢复的方案

您可以通过以下流程体验该方案：

**第1步：注册用户**

注册时，用户私钥除了本地保存，还将通过您的人脸识别生物特征进行MPC加密安全保存在远程。注册后，您可以登录使用系统。

**第2步：删除私钥**

为了体验MPC私钥恢复，您可以手动删除本地用户私钥，然后再恢复私钥。删除后，您将无法登录使用系统。

**第3步：恢复私钥**

当本地私钥遗失或者被手动删除后，您可以通过提交您的人脸识别生物特征从远程将私钥进行MPC恢复到本地，从而正常使用系统。

登录

下午3:44

[< 返回](#)[登录](#)

手机号 请输入手机号

密码 请输入密码

登录

3.3 恢复私钥

在删除私钥或者更换新手机之后，点击【恢复私钥】，在弹出的确认提示框中，点击【确认】，进入私钥恢复流程：

基于MPC的私钥恢复

可信的数据交换、有价值的信息传递是矩阵元在数据安全领域秉持的价值理念，MPC是在该价值理念下的解决方案与工程实现。借助矩阵元的MPC框架，能够保证在多方价值主体之间完成数据运算，但是又不丧失数据的所有权。在当下大数据、云计算、人工智能等以数据为基石的应用领域，为数据的有价值流动提供了可靠的解决方案和应用场景。

本应用展示了基于矩阵元MPC框架应用于私钥恢复的方案

您可以通过以下流程体验该方案：



第1步：注册用户

注册时，用户私钥除了本地保存，还将通过您的人脸识别生物特征进行MPC加密安全保存在远程。注册后，您可以登录使用系统。



第2步：删除私钥

为了体验MPC私钥恢复，您可以手动删除本地用户私钥，然后再恢复私钥。删除后，您将无法登录使用系统。



第3步：恢复私钥

当本地私钥遗失或者被手动删除后，您可以通过提交您的人脸识别生物特征从远程将私钥进行MPC恢复到本地，从而正常使用系统。

登录

点击【恢复私钥】，弹出确认框



点击【确认】，进入恢复私钥流程

私钥恢复流程：

- 1、输入用户信息：姓名、身份证号、手机号
- 2、人脸识别：按照操作引导，进行人脸识别
- 3、设置新密码
- 4、完成私钥恢复

下午3:46

< 返回 密钥恢复

1 2 3 4

用户信息 人脸识别 设置新密码 完成

姓名 请输入姓名

身份证 请输入身份证号码

手机号 请输入手机号

下一步

输入用户信息：姓名、
身份证号、手机号



点击【开始识别】, 进入人脸识别流程



人脸识别成功后, 设置新的登录密码



恭喜您，您的私钥恢复成功！

去登录

私钥恢复成功！点击
【去登录】进行验证

恢复成功可进行登录验证，点击【去登录】进入登录页面，输入手机号、新的登录密码，点击【登录】，如果成功进入“登录成功欢迎页面”，则表示恢复成功！



手机号 请输入手机号

密码 请输入密码

登录

登录成功！

欢迎体验矩阵元MPC私钥恢复系统

您的账户信息如下：



15626579576

账户地址

0x5e023109612884f7be6b8ed14b9238009dfdd91d

退出