

零售App用户认证授权方案讨论会议纪要

会议时间： 2026年8月31日 16:59-17:37

会议主题： Retail Solution 用户认证与授权方案讨论

讨论范围： Retail App 外部零售商用户与马牌内部用户的账号来源、用户身份分发、登录认证、访问授权及 SSO 方案

一、会议结论摘要

本次会议主要对 Retail Solution 中两类用户的账号与认证授权方案进行了澄清：

1. **零售商外部用户：店主 / 店员**
2. **马牌内部用户：Retail App 管理后台使用人员**

两类用户采用不同的用户来源和认证方式。

1. 零售商外部用户

零售商用户继续沿用现有的 **马上下单 + 门店店员信息分发机制**。

整体原则：

马上下单承担零售商门店及店员身份信息的主数据管理，门店店员信息分发机制负责将用户 Identity 及系统 Access 信息分发给 Retail App、O2O、ROOS 等下游系统。

Retail App 接收到用户信息后，自行负责：

- 用户登录认证
- Session / Token 管理
- App 内部权限
- 黑名单
- 风控状态
- 应用侧账号状态

门店店员身份信息的新增、修改、删除最终仍需要进入马上下单侧统一维护。

2. 马牌内部用户

Retail App 管理后台的内部用户原则上通过 **Global AD / SSO** 完成登录认证。

基本逻辑：

Global AD

- 完成员工身份认证
- Retail App 判断该用户是否属于允许访问后台的人员
- Retail App 决定是否放行及赋予相应权限

对于“哪些内部员工允许访问 Retail App”，会议讨论了：

- 通过 ContID / 组织信息向 Retail App 提供人员范围；
- 在 SMT / AD 中维护 Retail App 专用用户 Group。

内部用户最终采用哪一种访问名单管理方式，本次会议未最终确定。

二、零售商用户主数据来源

2.1 门店与初始管理员

当前门店首先在 **马上下单** 中建立。

门店建立时，会同步产生门店初始管理员 / 店铺联系人信息，包括：

- 姓名
- 手机号
- 所属门店
- 相关系统 Access 信息

相关数据进入现有的 **门店店员信息分发机制**，并实时向下游系统分发。

Retail App 上线后，也将作为新的下游系统接收相关用户信息。

因此本次会议确认：

| **马上下单继续作为零售商门店及店员身份信息的 Source of Truth。**

三、Retail App 用户数据同步机制

3.1 首次接入

Retail App 第一次接入现有用户体系时，需要进行一次：

全量用户数据同步

即：

马上下单 / 门店店员信息

→ 门店店员信息分发

→ Retail App 用户库

3.2 后续同步

首次全量同步完成后，后续采用：

实时增量分发

当发生以下变化时，触发对应用户信息更新：

- 新增店员
- 修改店员
- 删除 / 失效店员
- 用户 Access 信息发生变化

会议明确：

当前门店店员信息分发为实时触发机制，不采用定时批处理作为主要同步方式。

四、Retail App 店员管理方式

未来 Retail App 可以提供店主 / 店铺管理员维护店员的前端入口。

例如：

- 新增店员
- 修改店员
- 删除店员

但相关操作仍需进入马上下单现有账户体系。

建议的数据流为：

店主 / 店铺管理员

↓

Retail App 店员管理页面

↓

调用马上下单账户管理接口

↓

马上下单完成店员 Identity 新增 / 修改 / 删除

↓

触发门店店员信息分发

↓

同步至 Retail App、O2O、ROOS 及其他下游系统

因此 Retail App 不单独形成第二套零售商用户主数据。

会议确认的原则为：

Retail App 可以提供用户操作入口，实际的零售商用户 Identity 仍由马上下单统一管理。

五、用户身份分发

现有门店店员信息体系的主要职责是：

维护并分发零售商用户的 Identity，以及用户可以访问哪些系统的基础 Access 信息。

当前可同步的信息包括：

- 姓名
- 手机号
- 所属门店
- 用户身份信息
- 可以访问的系统 / Access 信息

例如：

- Retail App
- O2O

- ROOS
- 延保相关系统
- 其他零售业务系统

门店店员信息分发体系主要回答：

| 这个人是谁，以及这个人是否具备进入某个系统的基础资格。

六、Authentication 登录认证

会议进一步澄清了用户 Identity 分发与登录认证的边界。

用户身份数据被提前分发到 Retail App 后：

Retail App 自行负责实际登录认证。

例如未来可以采用：

- 手机号 + 验证码
- 手机号 + 密码
- 微信登录
- 其他 Retail App 支持的认证方式

用户登录 Retail App 时，原则上无需每一次都实时请求马上下单进行用户认证。

典型逻辑：

用户输入登录信息

↓

Retail App 完成手机号 / 其他方式认证

↓

查询 Retail App 本地用户数据

↓

判断该用户是否存在，以及是否具备 Retail App Access

↓

允许 / 拒绝登录

因此：

马上下单及门店店员信息分发体系提供用户身份基础数据，Retail App 负责自身 Authentication。

七、Authorization 访问授权

Authorization 建议分为两个层级理解。

7.1 系统访问资格

由上游 Identity / Access 信息提供。

例如：

某用户是否具备：

- Retail App Access
- O2O Access
- ROOS Access
- 其他系统 Access

这一层解决的是：

这个用户是否应该进入某个系统。

7.2 应用内部权限

用户进入 Retail App 后，更细粒度的权限和状态由 Retail App 自己管理。

例如：

- 店主 / 店员权限
- 页面权限
- 功能权限
- 业务操作权限
- 黑名单
- 风控状态
- 用户冻结
- 应用内部角色

这一层解决的是：

| **用户进入 Retail App 后可以做什么。**

因此本次会议形成的责任划分为：

上游身份体系

→ Identity + Application Access

Retail App

→ Authentication + Application Authorization + Risk Control

八、零售商账号的管理责任

会议确认：

零售商自己的员工账号原则上仍由 **零售商自己维护**。

当前马上下单已经提供零售商维护门店员工的能力。

马牌后台管理人员通常不会直接修改零售商的：

- 姓名
- 手机号
- 店员基础身份信息

系统侧可以针对某个业务系统进行：

- 拉黑
- 禁用
- 风控限制

但这些属于具体系统的应用级管理，并不会改变零售商用户的基础 Identity。

因此：

| **零售商负责管理自己的店主 / 店员身份，业务系统负责管理自身的访问和业务状态。**

九、微信 OpenID / UnionID

会议讨论了 Retail App 未来接入微信登录的可能性。

现阶段 Retail App 暂未将微信登录作为必要方案。

未来如果增加微信登录，可以考虑将 Retail App 接入马牌现有的微信开放平台。

如果相关应用属于同一个微信开放平台，可以通过 **UnionID** 对同一个微信用户进行关联。

当前零售商用户体系中仍以：

| 手机号作为主要的用户识别信息。

因此 UnionID 主要可以用于：

- 微信快捷登录
- 减少重复输入手机号
- 多个微信应用之间进行用户识别
- 提升用户登录体验

不会替代马上下单中的零售商用户主数据。

会议同时确认：

| 微信支付与微信登录属于不同机制，Retail App 使用微信支付并不意味着必须采用微信登录。

十、Compliance / 隐私政策

会议提出，马上下单采集的零售商姓名、手机号等个人信息，未来如果继续分发并用于 Retail App，需要确认现有隐私政策是否覆盖新的使用场景。

现有处理原则为：

| 每增加新的个人信息使用系统或场景，相应更新隐私政策中的使用范围说明。

因此 Retail App 接入后，需要进一步确认：

零售商用户

- 马上下单现有隐私政策是否覆盖 Retail App
- 是否需要增加 Retail App 数据使用说明
- 用户手机号、姓名等信息向 Retail App 分发的合规说明

内部员工

内部员工信息目前已有 HR、ContiID、SAT 等相关管理体系。

Retail App 使用内部员工 Identity 时，是否需要增加额外的隐私 / Compliance 说明，由相关责任团队进一步确认。

十一、内部员工用户方案

Retail App 的 Web 管理后台预计会有马牌内部员工使用。

内部用户登录原则上可以采用：

Global AD SSO

典型流程：

员工进入 Retail App Web

↓

跳转 Global AD

↓

完成员工身份认证

↓

返回邮箱 / User Identity

↓

Retail App 判断该员工是否具备 Retail App Access

↓

允许登录

↓

Retail App 根据自身权限体系进行授权

11.1 AD 与 Retail App Access 的关系

Global AD 可以确认：

■ 该用户是否属于马牌内部员工。

但单纯通过 AD 无法判断：

■ 该员工是否应该访问 Retail App。

因此还需要维护 Retail App 的内部用户访问范围。

11.2 方案一：ContiID / 组织信息同步

ContiID 可以基于：

- 邮箱
- Department
- Organization
- Employee Identity

向 Retail App 提供指定组织范围的内部员工信息。

Retail App 完成 SSO 后，根据邮箱等字段与本地内部用户信息进行匹配。

符合 Retail App 用户范围则允许访问。

11.3 方案二：SMT / AD Group

会议中提出另一种方式：

建立 Retail App 专用内部用户 Group。

例如：

Retail App Backend Users

由马牌内部管理员维护该 Group 的人员。

Retail App 完成 AD SSO 后，通过 Group 信息判断该员工是否具备访问 Retail App 的资格。

该方式可以减少 Retail App 与 ContiID 用户同步之间的依赖。

11.4 当前结论

两种方式目前均具备可行性。

内部用户最终采用：

- ContiID / Organization 同步；
- SMT / AD Group；

仍需进一步确认。

十二、术语统一

本次会议认为，在零售商用户场景中继续使用 **ContiID** 容易产生理解混淆。

当前实际语境中，ContiID 更多用于描述：

马牌内部员工 Identity / Internal User 体系

而零售商店主 / 店员属于另一套用户管理和身份分发机制。

因此后续方案建议统一术语。

内部员工

使用：

ContiID / Internal User Identity

零售商用户

使用：

Retailer User Identity

或：

门店店员信息

避免将以下几个概念混在一起：

- Internal User Identity
- Retailer User Identity
- Authentication
- Authorization
- SSO
- User Distribution

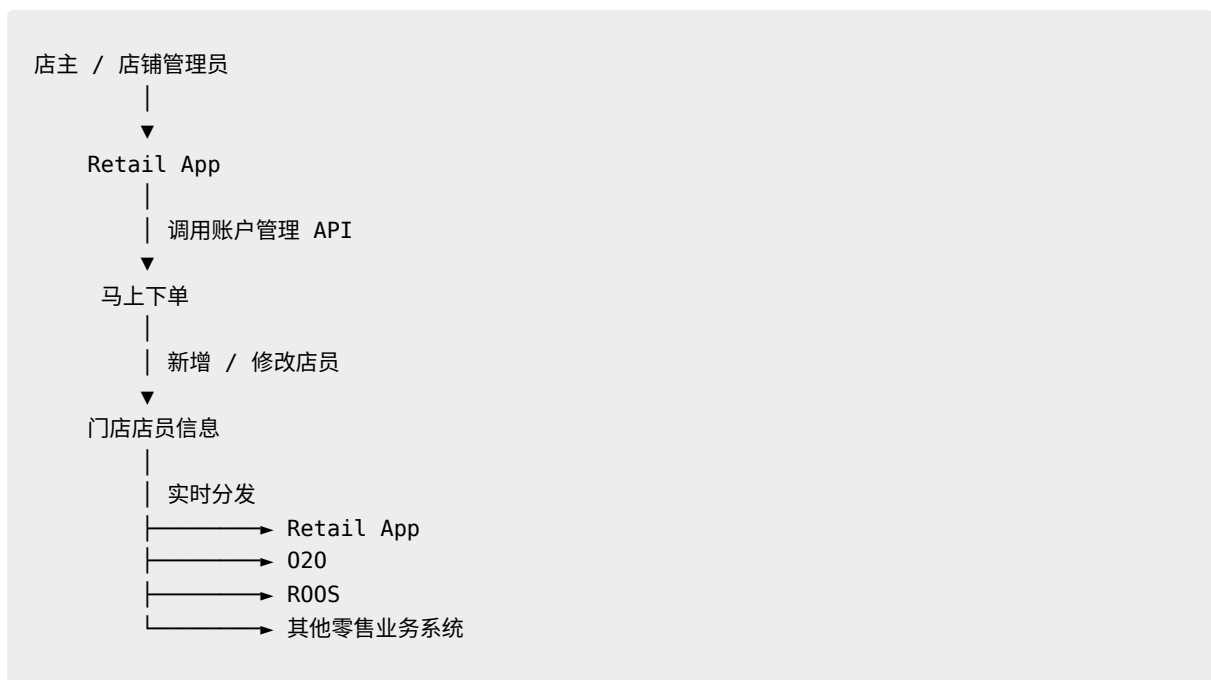
十三、整体数据流

13.1 零售商用户初始创建

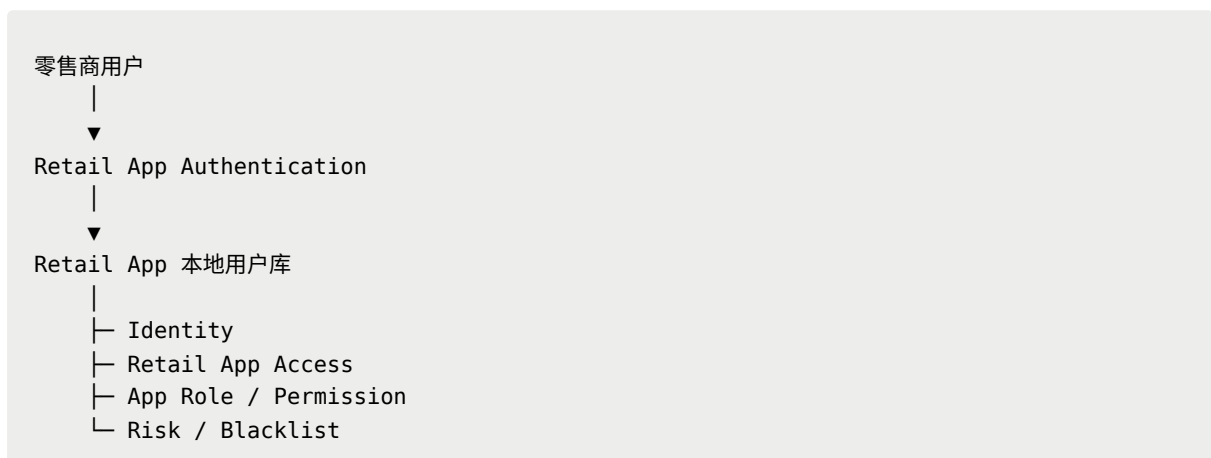
马上下单
|
| 创建门店



13.2 Retail App 新增 / 修改店员

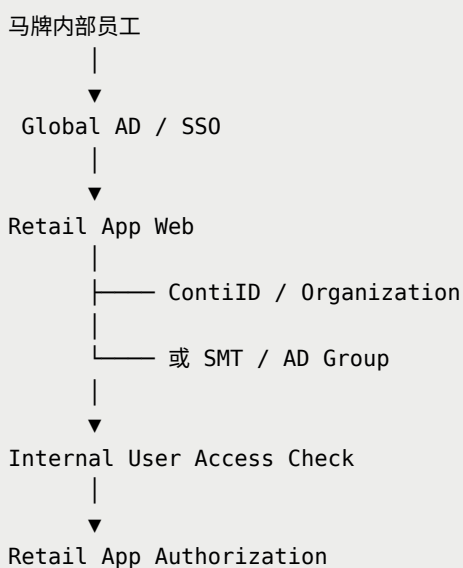


13.3 Retail App 登录



↓
允许 / 拒绝访问

13.4 内部员工



十四、已确认事项

#	事项	会议结论
1	门店主数据来源	马上下单
2	门店初始管理员	随门店建立产生并向下游分发
3	零售商店员 Identity	马上下单作为 Source of Truth
4	Retail App 首次接入	进行一次全量用户数据同步
5	后续用户同步	实时增量分发
6	Retail App 新增店员	调用马上下单账户管理接口
7	Retail App 修改店员	调用马上下单账户管理接口
8	用户 Identity 分发	由现有门店店员信息分发机制负责
9	Retail App Authentication	Retail App 自行实现
10	Retail App 应用内部权限	Retail App 自行管理
11	黑名单 / 风控	各应用自行管理

#	事项	会议结论
12	O2O / ROOS 等下游用户	继续通过现有身份分发机制获取
13	微信支付	与微信登录无直接依赖
14	内部员工认证	原则上使用 Global AD SSO
15	Retailer 用户命名	后续避免直接使用 ContilD

十五、待确认事项 / Action Items

#	Action Item	责任方	状态
1	提供现有门店店员信息分发流程图	JUETECH	待提供
2	提供目前向下游同步的用户字段清单	JUETECH	待提供
4	明确 Retail App 调用的店员新增 / 修改 / 删除接口	Retail App + JUETECH	待确认
5	明确 Retail App 外部用户具体 Authentication 方式	Retail App / T-Systems	待设计
6	确认内部后台用户采用 ContilD / Organization 还是 SMT / AD Group	相关 IT 团队 / Retail App	待确认
7	确认 Retail App 使用零售商个人信息所需的隐私政策更新	相关业务 / Compliance 团队	待确认
8	后续如规划微信登录，确认 Retail App 与现有微信开放平台的关系	Retail App / 相关平台团队	后续规划