

# 助力零信任安全架构的下一代IAM

中通快递 信息安全负责人 | 伏明明

01 业务背景

02 面临的安全风险

03 下一代IAM

04 实践总结

05 未来展望

国内业务量最大

业务规模世界第一

连续两年稳居行业第一

2017年业务量达到62.2亿件



中通人  
30万+



网络合作伙伴  
9400+



服务网点  
29500+



覆盖区县  
98%+



覆盖乡镇  
85.24%+

# 生态中通

——中通集团的  
多元化经营战略



中通快运



中通云仓



中通国际 (跨境)



中通商业 (电商)



中通金融

01 业务背景

02 面临的安全风险

03 下一代IAM

04 实践总结

05 未来展望

业务系统众多和异构

组织人员和设备变动

敏感数据参与业务

开放平台API管理

01 业务背景

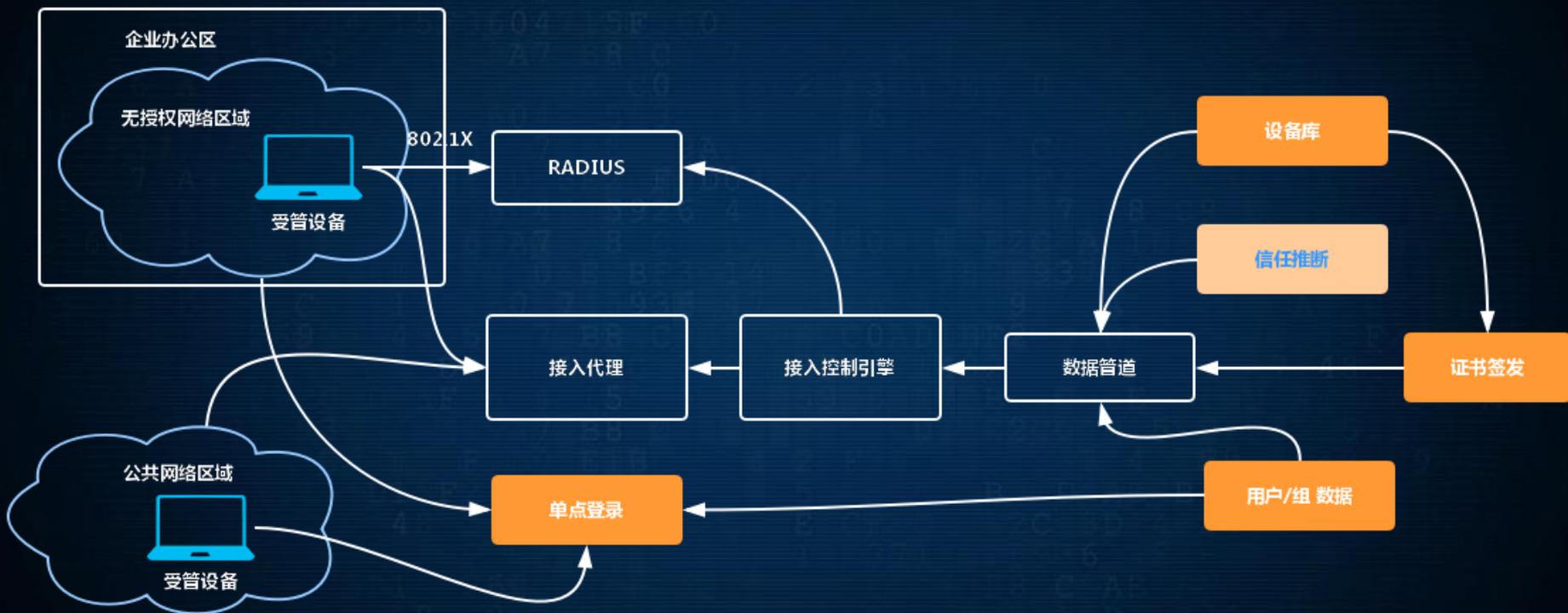
02 面临的安全风险

03 下一代IAM

04 实践总结

05 未来展望

# 下一代IAM——零信任安全架构（Google BeyondCorp）及其中的IAM组件





### 全面身份化支持

1. 使用通用安全身份框架 SPIFFE，实现支持万物互联的身份认证技术
2. 将客观世界的对象抽象成逻辑上具备不同属性的身份，如人员、设备、应用、API等



### 云原生支持

1. 真正打通本地/云/办公等网络边界，全面从网络层访问控制升级为应用层动态智能深度检测和控制
2. 使用容器、微服务、服务网格、编排等技术实现灵活的水平扩展、异构系统互操作支持和端到端的安全加密



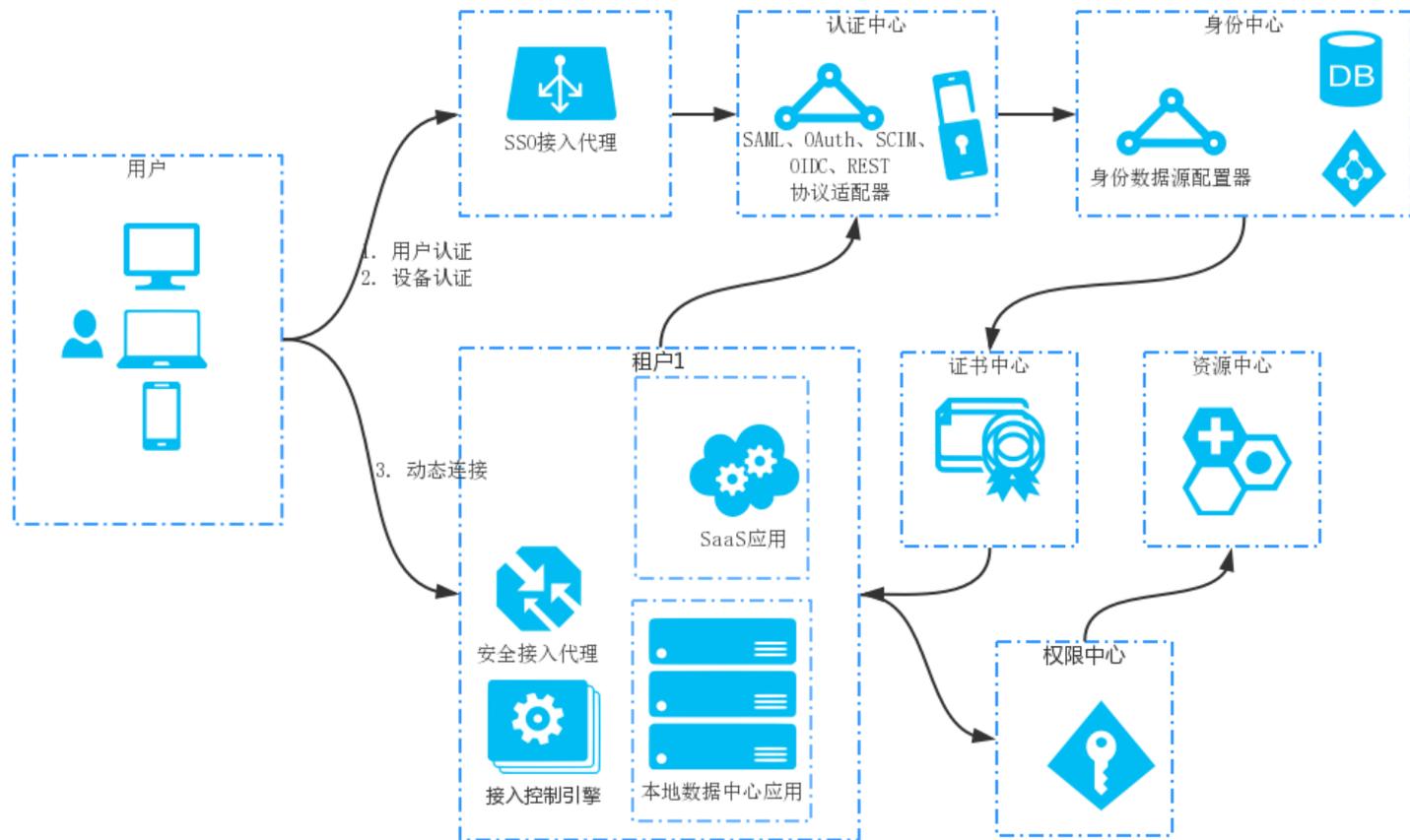
### 复杂组织的支持

1. 跨租户、跨帐号体系、跨端、跨用户渠道、跨应用、跨生态的支持
2. 应用和身份数据分离的联邦和多协议的支持
3. 在资源层面对所有操作进行分类分级及自动化审计

# 下一代IAM——功能全景视图



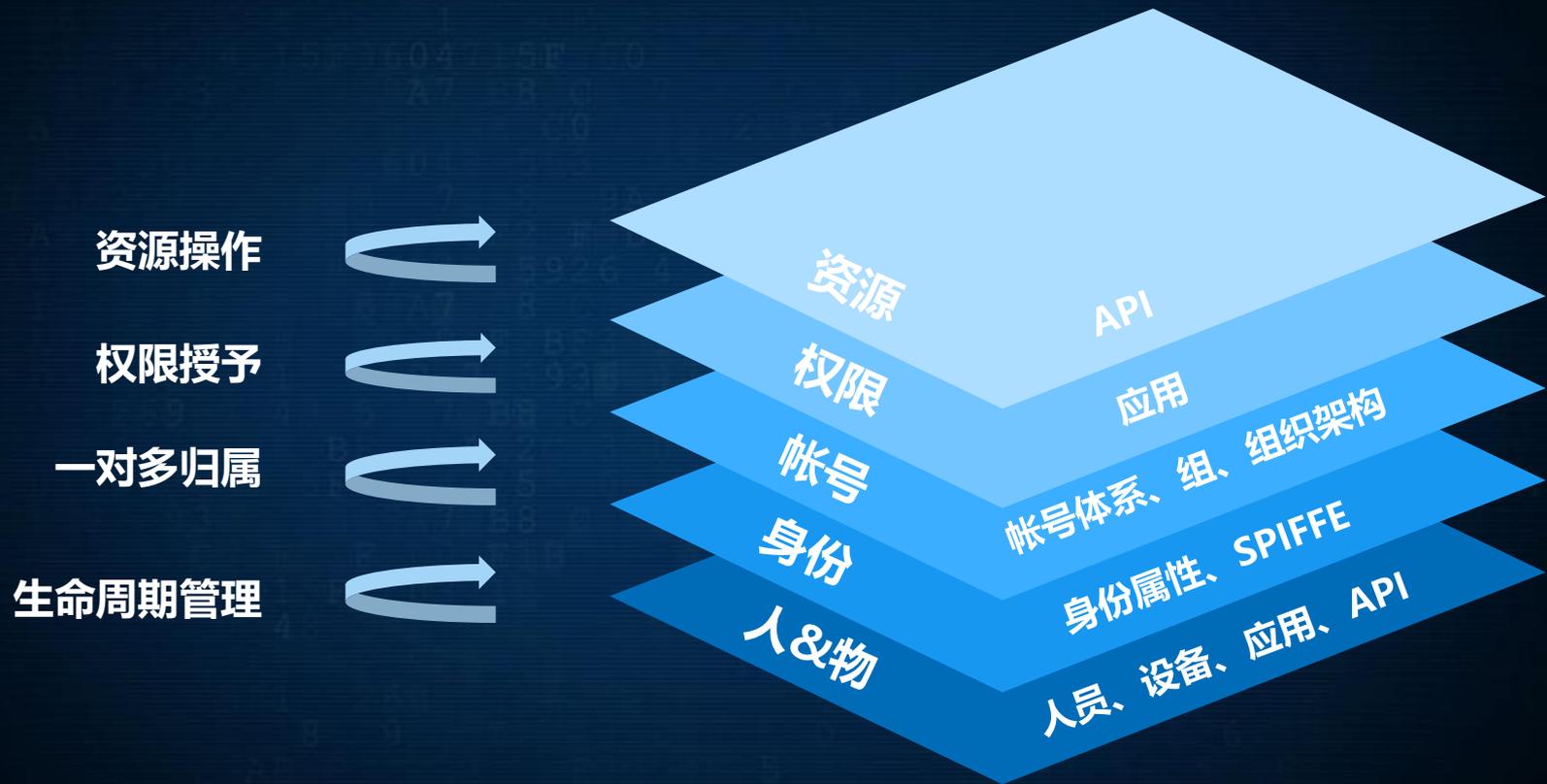
# 下一代IAM——总体工作流程



# 下一代IAM——本质上是对资源操作更灵活及更细粒度的管控



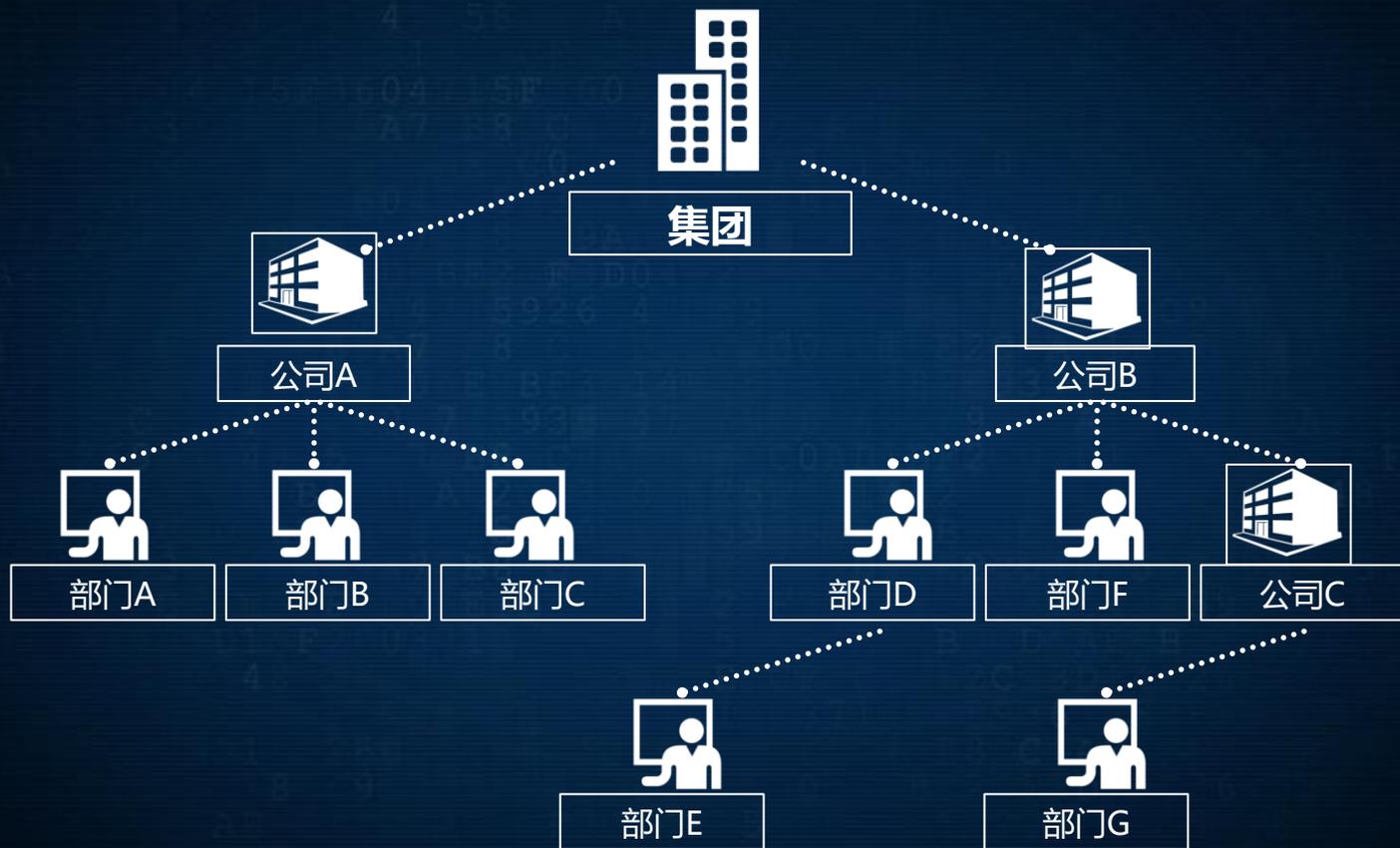
# 下一代IAM——身份空间



## 下一代IAM——帐号、帐号组、帐号体系



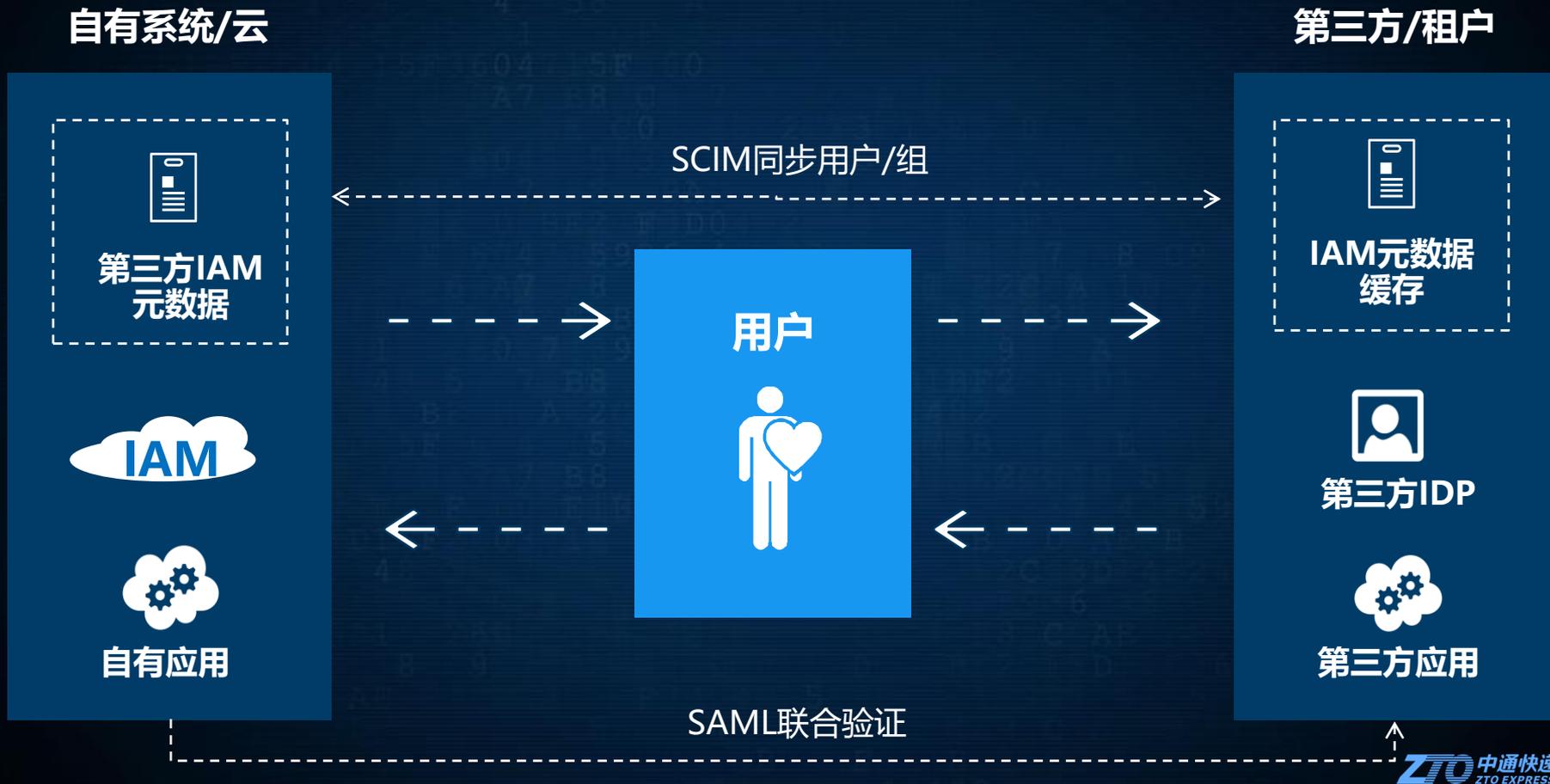
# 下一代IAM——组织架构



# 下一代IAM——组织架构群组



# 下一代IAM——系统集成



## 权限模型

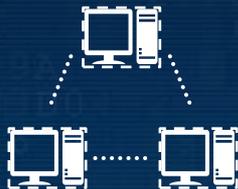


ACL

RBAC

ABAC

## 授权方式



基于身份的

基于资源的

访问控制策略

添加权限边界

## 授权过程



定义 Resource

定义每个Resource 上的Action

定义 Identity实体

定义 Policy 语法/权限/角色

解析 Policy 给出裁决结果



## 授权本质

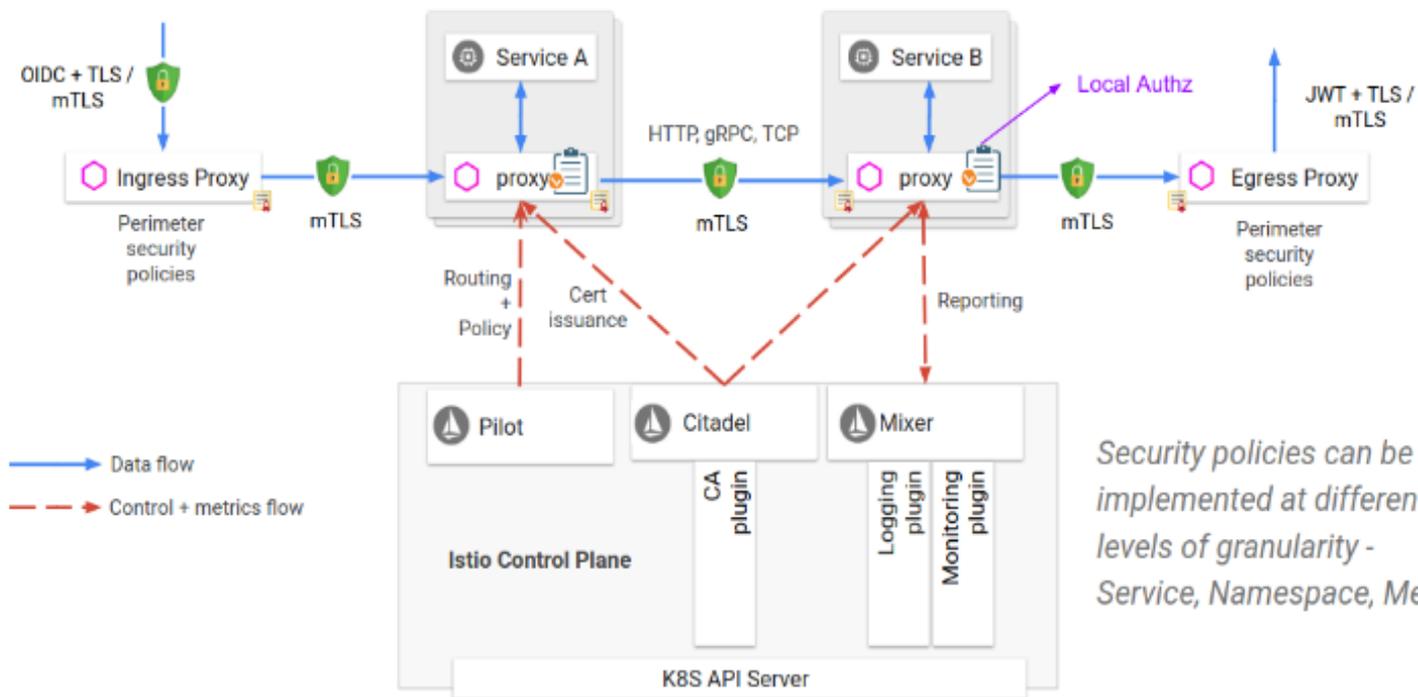
谁  
能不能  
在什么样的上下文  
对什么样的资源  
做什么样的操作



## DSL语法

```
{  
  "appid": "eihxiidhh23s", "user": "jack", "action": "getArticleID", "resource": "resources:articles:zto", "context": {"remoteIP": "192.168.0.5", "trustScore": "90"}  
}  
  
{  
  "allowed": true //裁决结果  
  "options": {"id": 11} //数据权限  
}
```

# 下一代IAM——微服务安全架构（双向认证、加密、隔离）



Security policies can be implemented at different levels of granularity - Service, Namespace, Mesh.

Istio Security Architecture

# 下一代IAM——证书签发、轮换和吊销机制



## 安全审计概念



- 跟踪记录谁在什么时间什么地点以什么样的方式做了什么
- 聚焦在及时发现异常和处理上

## 自动化



- 对所有资源进行分类
- 对所有资源和操作对分级
- 根据分类分级和权限过滤异常
- 与其它系统集成自动过滤异常

## 交付物



- 主动及时汇报和确认异常以推动策略实施及问题解决
- 确保审计对象得到合理准确的处理和合规
- 对企业内审计对象进行关联性分析并得到综合性的报告

## 安全模块

风控解锁

移动SSO

扫码

动态码

推送

安全评估

## 吉信模块

单聊

群聊

好友

通讯录

文件

公告

## 应用模块

应用Portal

事件流推送

帐号申请审批

权限申请

## 工具模块

个人资料维护

中通邮箱激活

实人认证

系统设置

01 业务背景

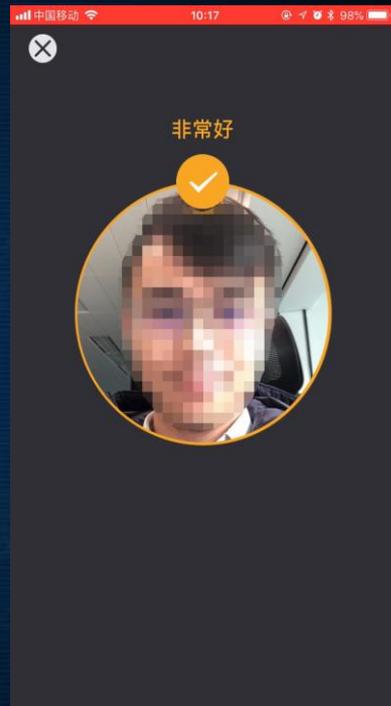
02 面临的安全风险

03 下一代IAM

04 实践总结

05 未来展望

# 实践总结——SSO支持多种认证方式（密码/短信/TOTP/推送/扫码/刷脸/会话代理等）



# 实践总结——身份管理支持实人认证（人、证、帐号、设备合一）



# 实践总结——敏感操作审计（刷脸认证日志）



周 [姓名] 信息中心

实人认证 v3

真实姓名 [姓名]

移动电话 186899 [号码]

注册时间 2016-05-16

上次登录 2017-03-25

## 人脸登录日志

2017-03-25 20:12 人脸登录



无动作



眨眼

2017-03-25 08:49 人脸登录



无动作



眨眼



无动作



眨眼

2017-03-24 22:12 注册人脸



无动作



眨眼



张嘴



抬头

2017-03-24 21:45 公安网比对



人像-提取自身份证

## 电脑登录



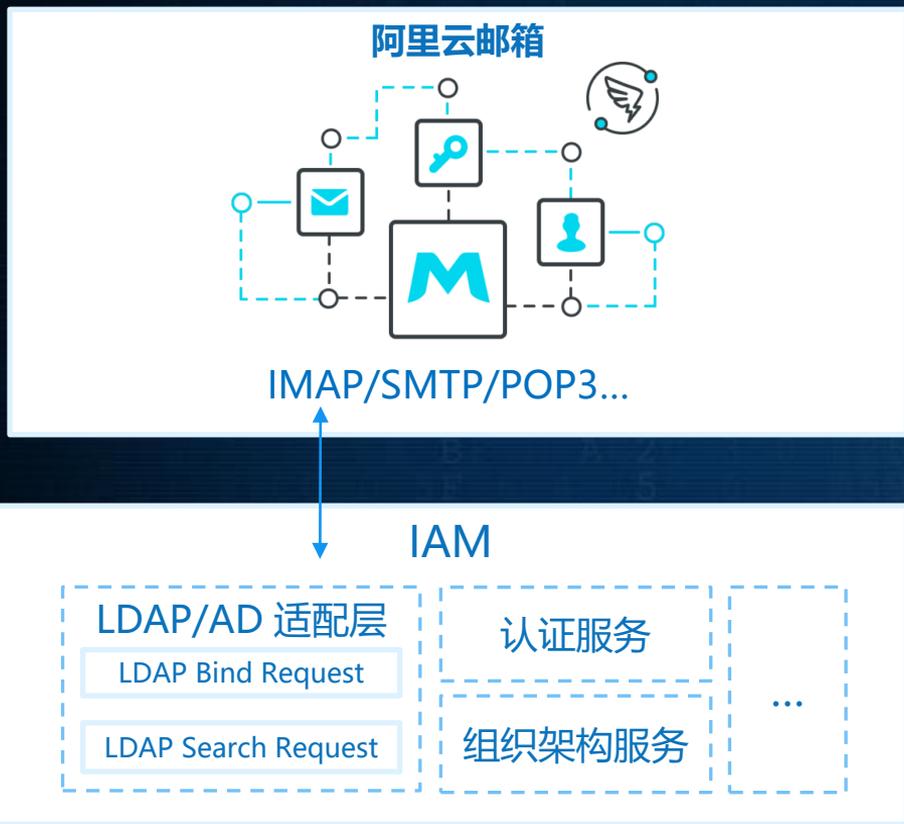
## 手机确认



## 进入办公区自动连 Wi-Fi



# 实践总结——IAM支持联邦认证与阿里云邮箱集成



# 实践总结——IAM支持认证互操作/移动端APP（与钉钉和菜鸟应用集成）



# 实践总结——IAM支持跨应用的集中权限管理



应用与权限管理系统

用户管理

权限管理

应用管理

我的工单

使用手册



数据



数据分析系统

服务保障数据分析

新数据驾驶舱

数据驾驶舱

数据开放平台

管控数据

数据罗盘

> 添加角色

▼ 单独添加权限 人数多或固定岗位用户需求权限的, 请联系开发者新增角色, 不要单独赋予权限!

允许访问省市区 (不允许)	选择
允许访问省市区全国范围 (不允许)	选择
业务系统访问许可 (允许)	选择
区域完成情况分析 (不允许)	选择
区域时效 (不允许)	选择
组织列表 (不允许)	选择
收件路由中心 (允许)	选择
中心一二派分析 (不允许)	选择
中心操作量分析 (不允许)	选择
日期业务量统计分析 (不允许)	选择
用户信息删除 (不允许)	选择
派件重量段分析 (不允许)	选择
派件路由 (不允许)	选择
派件路由中心 (不允许)	选择

已选择的权限字段

- 允许访问省市区
- 允许访问省市区全国范围
- 业务系统访问许可

# 实践总结——IAM支持权限矩阵实现SOD

> 互斥配置 <	巴枪功能开关...	机房告警管理...	机房信息管理	机房性能监控...	机房综合监控...
巴枪功能开关...					
机房告警管理...					
机房信息管理					
机房性能监控...				> 别点我 <	
机房综合监控...					> 别点我 <
告警策略管理...					
告警记录查询...					
设备管理-维...					
基础信息管理...					

机房性能监控管理 <-> 机房告警管理菜单权限  
添加互斥

# 实践总结——IAM支持双向权限审计

The screenshot displays a comprehensive IAM system interface with several key components:

- 账号与权限管理系统 (Account and Permission Management System):** Features a grid of permissions such as "可以添加永久白名单" (Can add permanent whitelist), "可以审核工单" (Can audit tickets), "可以审核实名认证" (Can audit real-name authentication), "可以变更申请账号的主管" (Can change the supervisor of the application account), "特殊管理权限" (Special management permissions), "可以注销账号" (Can cancel account), "可以管理黑名单" (Can manage blacklist), "可以管理全局角色" (Can manage global roles), "可以操作用户的全局角色" (Can operate user's global roles), "可以管理白名单" (Can manage whitelist), "可以管理渠道" (Can manage channels), "可以审查操作记录" (Can review operation records), "可以使用管理中心" (Can use management center), and "网点管理权限" (Branch management permissions).
- 安全风控系统 (Security Risk Control System):** Includes "业务系统访问许可" (Business system access permission), "问题件信息查询限制" (Problem piece information query limit), "收件人信息查询限制" (Recipient information query limit), and "可以查询收件人信息" (Can query recipient information).
- 查询系统 (Query System):** Offers "业务系统访问许可" (Business system access permission), "地区实名寄递监管" (Regional real-name express supervision), "菜单访问量统计" (Menu access volume statistics), "查询记录查询" (Query record query), "查询记录查询" (Query record query), "数据对比" (Data comparison), "统计" (Statistics), "到件" (Arrival), "到派对比" (Arrival and delivery comparison), "到发件率统计" (Arrival and delivery rate statistics), "发件" (Mailing), "发签对比" (Mailing signature comparison), "月到件" (Monthly arrival), "月派件" (Monthly delivery), "月收件" (Monthly receipt), "月发件" (Monthly mailing), "目的网点月统计" (Destination branch monthly statistics), "目的网点月统计(对账)" (Destination branch monthly statistics (reconciliation)), "快件运单状态查询" (Express waybill status query), "派件" (Delivery), "派签对比" (Delivery signature comparison), "实名登记明细查询" (Real-name registration details query), and "实名制统计" (Real-name statistics).
- 客服客户关系管理系统 (Customer Relationship Management System):** Contains "网投新建工单" (New online ticket), "业务系统访问许可" (Business system access permission), "网点提交申诉" (Branch complaint submission), "AddBusinessConsultationIndex", "AddBusinessConsultationIndex", "业务咨询添加试图" (Business consultation addition attempt), "通讯录" (Address book), "通讯录" (Address book), "网点电话咨询" (Branch phone consultation), "快件跟踪API" (Express tracking API), "呼叫系统" (Call system), "网点云呼未接来电" (Branch cloud call missed call), "投诉报表(网点)" (Complaint report (branch)), "超时未处理超时报表" (Overdue unprocessed overdue report), and "客户开通功能" (Customer activation function).
- 角色反查 (Role Backcheck):** A table listing roles and their associated permissions. The table has columns for "用户编码" (User code), "姓名" (Name), "网点" (Branch), "网点编号" (Branch number), "部门" (Department), and "操作" (Action). The "权限反查" (Permission backcheck) tab is active, showing a search for "机刷" (Machine刷) and a list of permissions: "机刷管理菜单权限" (Machine刷 management menu permissions), "机刷信息管理" (Machine刷 information management), "机刷性能监控管理" (Machine刷 performance monitoring management), "机刷综合监控菜单管理" (Machine刷 comprehensive monitoring menu management), and "机刷综合监控菜单管理" (Machine刷 comprehensive monitoring menu management).



安全文件存储

基本信息

业务域名

回调通知

权限配置

权限互斥配置

角色管理

文件存储

菜单配置

展示渠道

变更日志



### 安全文件存储

all

提供各种应用的文件上传、下载、存储、加密存储、删除、水印、缩略图等功能

App ID: [zt9NasLMmJWie\\_o4pjpYyzjA](#)

App Secret: [查看](#)

How To Use: [SSO和权限接入文档](#)

Max QPS: 0

Enable Permission:

ZTO 中通快递  
ZTO EXPRESS

# 实践总结——应用中心支持应用集中统一权限配置



## 行为权限管理 ① 接入文档

自动分组:

我们推荐使用 "\_" 下划线命名 key\_name, 之后将基于

[+ 新增](#) [📄 保存](#) [🔗 生成导出链接](#)

业务系统访问许可	是否允许用户访问此业务系统, 默认仅允许用户访问所在网点下的资源。	bool	access_granted
可以添加应用		bool	can_add_app
可以添加永久白名单		bool	can_add_permanent_whitelist
可以审核外发管理工单		bool	can_audit_forward_getway_issue
可以审核工单		bool	can_audit_issues
可以审核实名认证		bool	can_audit_usercert
可以变更申请账号的主管		bool	can_change_applicationaccount_manager
特殊管理权限		bool	can_execute_special_action
可以管理全局角色		bool	can_manage_global_role
可以操作用户的全局角色		bool	can_manage_global_role

### 基本信息

业务域名

回调通知

### 权限配置

权限互斥配置

角色管理

文件存储

菜单配置

展示渠道

变更日志

# 实践总结——应用中心支持应用集中统一菜单配置及自动关联权限

添加菜单 [全部展开/折叠](#)

注: 删除时会更新子级至顶级菜单.

默认 (default)

名称	链接	访问权限
<input type="checkbox"/> 基础信息管理		
查询	<a href="/plusSite/siteSearch">/plusSite/siteSearch</a>	(查询)
基础配置	<a href="/plusSite/checkBalance">/plusSite/checkBalance</a>	限查看【网点基础信息配置】菜单项
网点设置	<a href="/SiteService">/SiteService</a>	设置
配置	<a href="/plusSite/belongToArea">/plusSite/belongToArea</a>	置
中心管理	<a href="/plusSite/transferCenter">/plusSite/transferCenter</a>	管理
设置	<a href="/plusSite/oneStageCode">/plusSite/oneStageCode</a>	置 (查询)
设置	<a href="/plusSite/twoStageCode">/plusSite/twoStageCode</a>	置 (查询)
设置	<a href="/plusSite/threeStageCode">/plusSite/threeStageCode</a>	置 (查询)
管理	<a href="/site/ContractManager">/site/ContractManager</a>	(查询)
物料	<a href="/plusSite/forwarderIndex">/plusSite/forwarderIndex</a>	
<input type="checkbox"/> 配置		
计费公式设置	<a href="/system/formulaSet">/system/formulaSet</a>	费公式设置

01 业务背景

02 面临的安全风险

03 下一代IAM

04 实践总结

05 未来展望

## 未来展望——在IAM基础上集成更多的安全组件



端到端加密组件



零信任安全组件



SDL工具/组件

## 未来展望——积极拥抱开源技术和开源文化

### 积极采用开源技术



已采用或即将采用的开源技术: tango、gokit、docker、k8s、istio、hydra、CDH、spark、redis、kafka、es、pg、tidb、openresty、kong、pika、fastdfs、grafana等

### 定期与同行技术分享



中通安全应急响应中心 ( <https://sec.zto.com> ) 微信公众号 ZTO\_SRC 每月推送两到三篇技术分享文章以及参加相关会议

### 制定分步开源计划



计划将IAM平台及其它安全系统组件化后, 2019年起逐步开源, 希望能帮助到有需要的朋友

# 未来展望——持续吸纳专业的安全人才



2016

5



2017

10



2018

20+



相互交流或投递简历

# 问题讨论

---

# Q&A