人像登录问题分析

**一、问题描述和处置：**

12月7日上午9：14，太平资管交易员tpzc02通过业务场务报机构用户权限设置页面能够查询并设置其他机构用户信息，下午反馈仅通过人像登录出现越权情况，Ukey登录正常。经调查，人像登录提供的登录方式字段枚举值与Ukey登录方式枚举值不同导致该越权问题。当日晚上通过紧急变更修复。

**二、问题原因调查简述**

1、**UUAS的代码遗留问题**

“登录方式”元数据枚举定义为1非代理、2场务代理。UUAS Ukey登录老代码中，枚举定义为0非代理、1场务代理。为与元数据保持一致，IMIX转mateobject做了枚举值映射转换。

UUAS人像登录于UUASv2.8.8上线,新代码中登录方式枚举遵循元数据定义发送，但老UUAS的IMIX转换逻辑还在。因此在人像场景下，UUAS发送枚举值变为1（非代理），TBS实际接收枚举值变为2（场务代理）（相关代码上线后至今未做过改动。）。

2、**V142以前新本币未受影响**

V142以前，TBS用户权限设置功能，通过tbs-dp-dqs进程配置的过滤器（ts-auth-filter）解析token获取该用户机构六位码，根据六位码过滤用户列表范围，完成数据权限控制；如六位码为空，则为场务用户查所有。**该过滤器未采用登录方式字段进行判断。**

因此，随人像上线后,Ukey登录、人像登录“登录方式”枚举值差异这颗雷生产环境一直存在，但未对用户权限功能造成影响。

**3、V142版本的问题引入**

V142版本集成初期（2020年4月10日），为解决获取做事价差接口401错误问题（缺陷编号：RMB1800124290）。开发人员雷阳错分析为过滤器不匹配导致，并更新tbs-dp-dqs进程过滤器为ses-auth-filter。但导致接口401真正的原因是进程父工程版本太低。4月15日更新父工程后上述缺陷解决。

ses-auth-filter过滤器开发于2018年10月，用于同一进程同时支持场务端、客户端接口调用场景（成交共享进程，全局搜索进程均使用该过滤器），**实现逻辑中会根据“登录方式”判断用户类型**。又因为人像登录一直提供的是错误登录方式枚举，导致会员用户错判为场务用户产生越权。

1. **责任分析**

问题产生根源为UUAS，人像登录这颗雷早在新本币接手UUAS之前已经上线，但由于UUAS非前置团队，因此对UUAS的问题责任，此报告不予追究。

**1、142版本集成阶段（技术负责员：沈一筹，主责。技术守门员：张洋弘，次责）**

142版本集成初期，集成问题的分析解决依靠单个开发问题分析，应该针对没有十足把握的解决方案，多人二次确认。另外，真正问题修改后，也未意识到之前过滤器更新是不必要修改而进行回退。集成阶段，虽集成初期所有代码提交并不经过守门员审核。但5月15日1406版本合并142时已在过滤器上产生冲突，守门员也未评估出142的修改其实没必要。将该不必要修改再次漏出。

**1、142版本集中测试（需求守门员：徐慧鹏，技术守门员：申冬东，主责）**

UUAS改造一期内容属于142版本范围，虽然改动不涉及UUAS线上进程，需求守门员、技术守门员提供测试范围应包含人像识别登录以及权限检查场景，但：一是需求守门员交底的集中测试场景仅包括人像登录测试，未进行人像登录后系统的各个操作和查询等主流程验证，只验证了登录是否成功；二是技术守门员对UUAS改造范围评估不够准确，未能涉及权限检查。

**2、UUAS HW改造（负责人：赵攀，次责）**

UUAS V3.4.0.12版本为UUAS高危漏洞修复版本，6月10-14日在UAT4验证人像功能，**包括人像登录后本币简单功能冒烟（**包括用户新建、赋权），由于UAT4当时新本币版本为140，因此未在验收阶段发现该问题。但当UUAS版本进模拟后与142版本在6月16-17日有两天重合期，原本计划进行人像登录验证，即可发现问题，但因环境不通且验收环境测试通过而取消，错过本有可能发现问题的机会。

* 客观因素：人像测试环境

目前UAT1-UAT4无一套可用的人像登录环境。只有模拟具备测试条件。