Ksuser 安全认证中心

V1.0

设计文档

目录

1.系统概述

1.1 项目背景

随着目前越来越多的业务从早期单一的网站、APP 形态逐渐扩展到现在的多终端协同，原先只用简单用户名+密码登录的模式受到了诸多挑战：第一，认证入口分散。网页、桌面与移动端各自开发登录逻辑，造成体验割裂，也会直接导致维护成本上升；第二，安全风险提升。传统“密码+会话”难以覆盖跨设备登录、敏感操作确认与异常行为识别，简单密码易存在“撞库”风险；第三，接入场景复杂，既要支持站内账号体系，也要兼容 OAuth/OIDC 等标准化联合身份能力。因此本项目致力于尝试解决这些问题，打造统一安全认证中心，通过 SpringBoot 提供稳定的认证与授权能力，通过 Vue3 承载统一认证门户和授权页面，通过 Flutter 与 Kotlin/Swift 将认证能力延伸到原生终端，形成一套跨端一致、可扩展、可审计的身份平台。

该项目的认证方式包括但不限于传统的密码登录、邮箱验证码登录、也存在新颖的通行密钥 Passkey 无密码认证、TOTP 一次性验证码、会话刷新与撤销、敏感操作二次校验、第三方开放应用的登录/绑定、内部 SSO 与 OIDC Discovery 等；结合限流、风险评分、敏感日志与多设备会话管理，实现“可用性”与“安全性”的平衡。

同时项目按按照不同终端分模块管理，并配套独立 CI 工作流，支持分端迭代与并行交付，将认证从“功能点”升级为“平台能力”，为其余业务系统的展开提供统一可信的身份底座，降低重复建设成本，提升跨端登录体验与安全基线。

1.2 系统介绍

该系统采用“统一账号中心+多终端协同”的方式，为用户提供统一账号系统的无缝流转。无论是在浏览器、电脑客户端还是手机上，用户都可以使用同一套账号体系完成注册、登录和身份验证，并在不同设备间保持顺畅切换。系统支持多种认证方式，兼顾便捷与安全。针对改密码、改邮箱等高风险操作，风控部

分也会自动触发二次校验，降低账号被他人非法使用。用户还可以查看和管理已登录设备，及时撤销异常会话。同时该系统具有开放能力，可以让第三方应用快速便捷地接入该套账号体系并作为第三方登录的手段之一，满足了不同场景下的接入需求。

2.总体设计

2.1 开发环境

系统采用多技术栈协同开发：后端使用 Java21，Spring Boot 框架构建统一认证服务；Web 端采用了国内十分流行的 Vue3+Vite+TypeScript 实现认证门户与授权交互，确保能在大部分主流浏览器中顺利运行；桌面端基于 Flutter 跨平台框架构建的客户端，能让 Windows 与 Mac 等设备的体验几乎相同；移动端则采用 Kotlin 与 Swift 分别来实现 Android/IOS 的 APP 开发，使用官方推荐语言能更好地发挥系统的底层原生能力，确保系统的通行密钥等新颖验证方法能获得支持。该架构兼顾了多终端一致性、开发效率与可维护性，能够支撑密码登录、验证码登录、Passkey、MFA、会话管理及 OAuth/OIDC 等认证能力。系统的开发环境如表 1 所示。

名称	参数/版本
处理器	Apple M4
操作系统	MacOS Tahoe
开发平台	Visual Studio Code, IntelliJ Idea, Android Studio, Xcode，DataGrip
后端开发语言	Java21
后端框架	SpringBoot 4.0.2
Web 开发语言	TypeScript 5.9.3
Web 框架	Vue 3.5.26
Web 构建工具	Vite 7.3.1

Node.js	22.12.0
桌面端框架	Flutter Stable（Dart SDK 3.11.4）
移动端语言	Kotlin Swift
Android 构建插件	Android Gradle Plugin 9.1.0
移动端 UI	Jetpack Compose BOM 2026.02.01
移动端网络库	Retrofit 2.11.0
缓存组件	Redis
数据库	MySQL

表 1 系统开发环境

2.2 架构设计

本节将会对前端设计、后端设计以及数据库设计这三个部分的业务逻辑使用流程图来表达。通过流程图的方式，展示本节行文思路和整个系统的逻辑结构。图 1 是设计流程图。

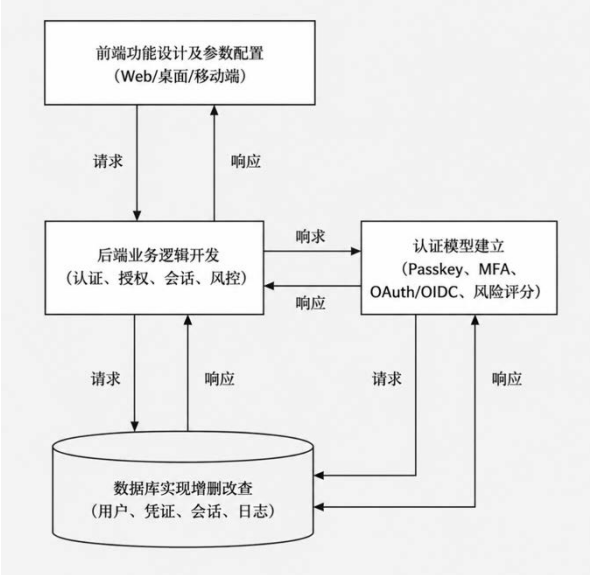


图 1 整体架构图

本项目采用前后端分离的认证架构，通过后端 NGINX 反代提供的专用 api 接口完成多端交互。系统前端负责登录、验证、授权等页面展示与用户操作，向认证服务发起请求；后端接收请求后完成参数校验、身份核验、业务处理与结果返回，确保前端只负责展

示，后端只负责处理数据，保障了整体安全性。图 2、3 为前后端交互流程示意。后端基于 Java21 的 Web 框架实现统一账号能力，能在高并发环境下稳定支撑密码登录、验证码登录、Passkey 通行密钥、MFA 双重验证、会话管理等核心流程。前端主要使用 JavaScript、HTML、CSS（Vue 渐进式 js 框架）等技术实现页面渲染和交互逻辑。借助这些框架化能力将路由、控制器、服务与数据访问进行分层设计，能让认证流程更加清晰明了、后期维护也会更加高效。系统在业务执行时会从数据库读取用户与会话信息（具体数据库结构可见 3.3 数据库设计），经过后端充分的规则校验和安全处理后才会返回前端展示，从而实现“统一登录入口、跨端一致体验、全过程可追踪”的目标。

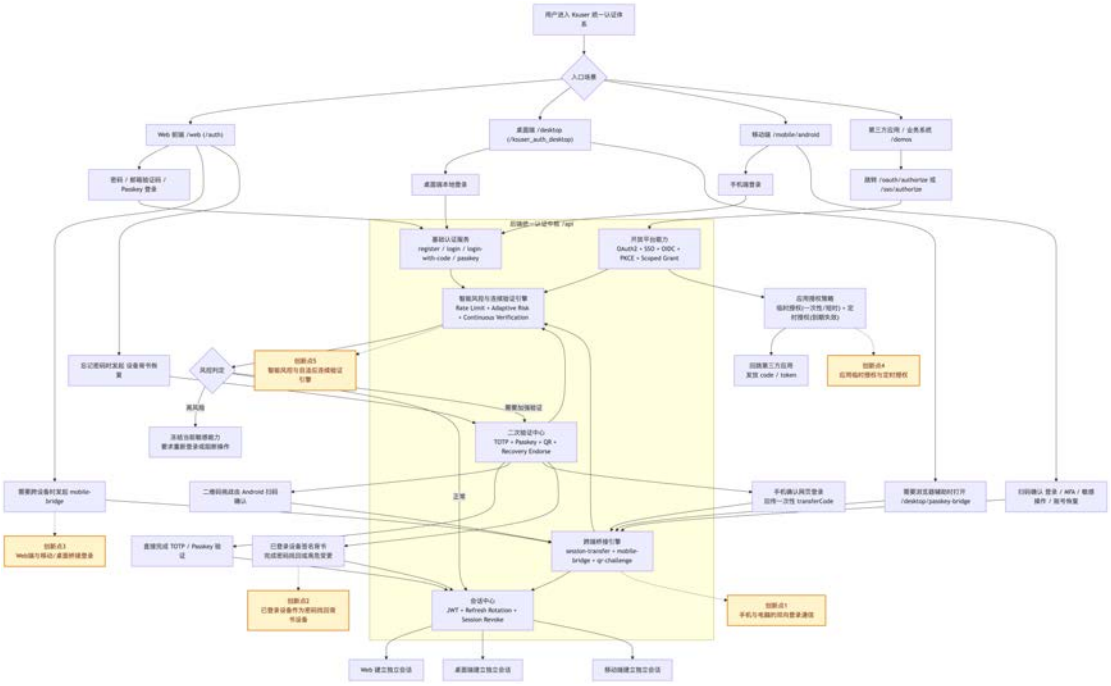


图 2 前后端交互图

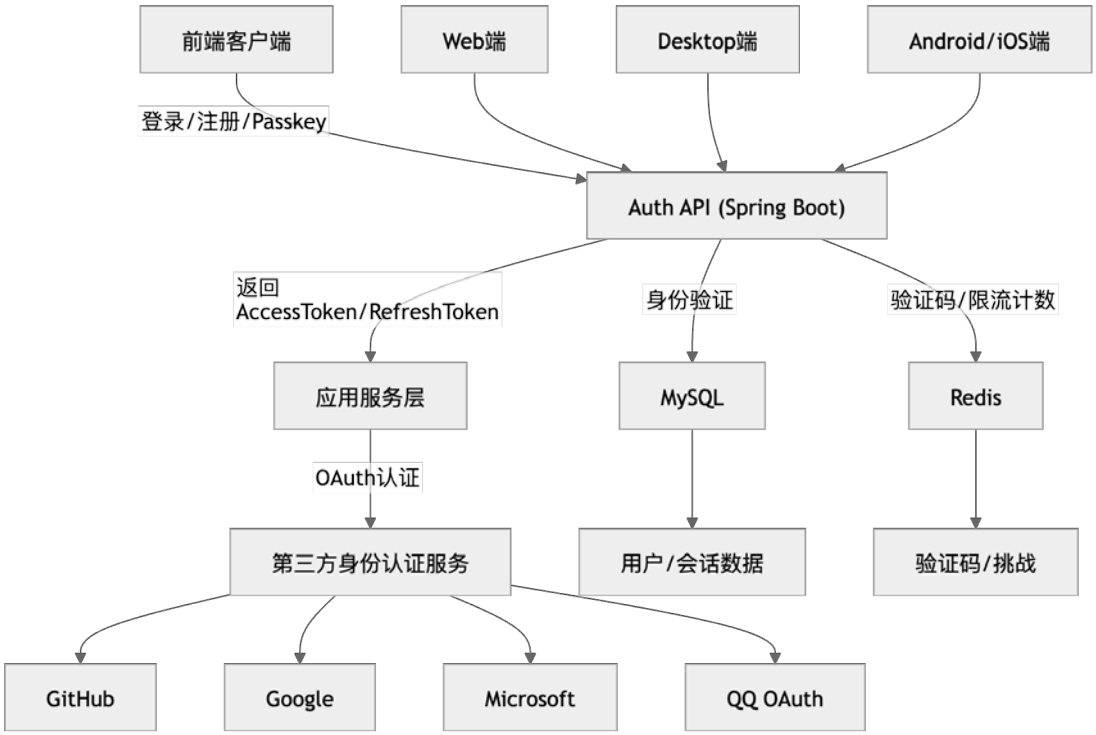


图 3 前后端交互图（简略）

2.3 功能模块设计

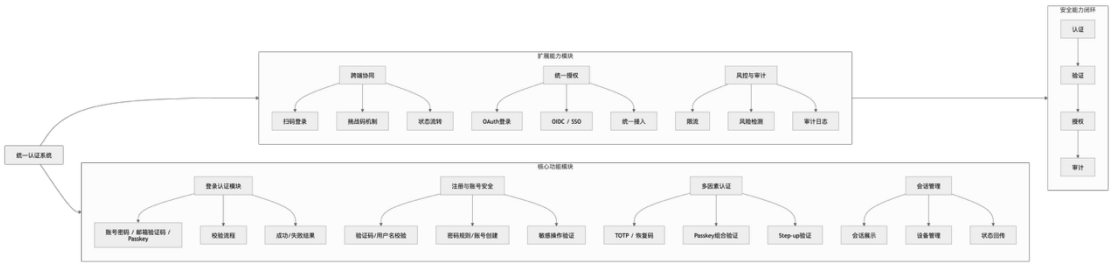


图 4 功能设计思维导图

图 4 的思维导图可以清楚看到本认证系统的整体模块实现。

系统在登录认证模块中，采用账号密码、邮箱验证码与 Passkey 三种入口，页面通过按钮、输入框和 form 表单组织交互；后端接收表单参数后进行账号校验、验证码校验与凭证校验，并结合数据库中的用户与凭证信息返回登录结果，成功后创建会话并跳转主页，失败则返回对应提示。

在注册与账号安全模块中，系统通过校验用户用户名可用性、邮箱验证码正确性、密码规则动态校验等一系列流程后才会批准账号的创建。

在多因素认证模块中，系统提供 TOTP 一次性验证码与对应恢复码、Passkey 通行密钥进行组合式验证，后端会根据风控状态和验证结果决定是否放行或触发

step-up 验证。

在会话管理模块中，前端以表格方式展示当前设备与所有登录设备记录，支持制定设备会话的撤销和全设备下线；后端负责执行查询、刷新、撤销等操作并实时回传状态。

在跨端协同模块中，支持手机对网页或桌面端登录请求进行扫码确认，后端通过一次性随机密钥（challenge）码与状态机控制确认、取消、过期等分支流程。

在统一授权模块中，系统支持标准 OAuth2.0 与 OIDC 协议，便于第三方业务系统统一接入。

最后在风控与审计模块中，系统会对账号的登录频率、异常行为和敏感操作进行限流、风险评分与日志记录，形成“认证-验证-授权-审计”闭环，保障多端登录体验与账号安全。

3.详细设计

3.1 总览

系统采用统一认证内核，面向 Web/Desktop/Mobile 三端提供一致能力，核心由五层组成：接入层、认证编排层、授权协议层、风控决策层、数据与审计层。

接入层负责端侧请求标准化；认证编排层负责密码、验证码、Passkey、MFA 的流程调度；授权协议层负责 OAuth/OIDC/SSO 协议处理；风控决策层负责限流与风险分决策；数据与审计层负责会话持久化、挑战态缓存和敏感日志。

鉴权方式则采用传统的 JWT Token+RefreshToken 刷新轮换制，对 JWT Token 进行严格的定期刷新机制，确保不会被长时间盗用。

3.2 核心功能设计

3.2.1 手机与电脑的双向通信登录

传统扫码登录往往只解决“在电脑上登录一个已在手机上存在的账号”这一单向问题，且底层机制更偏向于简单的登录结果转移。本项目在这一场景上的推进重点，是将手机从“扫码工具”提升为“可信确认终端”，并围绕一次性二维码挑战、设备信息预览、服务端会话重签发和目标端类型约束，构建双向登录通信机制。当前实现中，电脑端或其他终端先发起登录挑战并生成二维码，手机端扫码后能够查看客户端名称、浏览器、系统、IP 地址与归属地等上下文信息，在用户确认后，由服务端为目标端重新签发一套新的独立会话，而不是直接复制已有 token。

这一方案的理论意义在于，它将跨端登录行为重构为“挑战发起—可信确认—目标端建会话”的完整身份确认链条，使手机承担了主动确认与风险感知的角色；其工程价值则在于，后端已将目标端抽象为 Web、移动端、桌面端三类，因此同一套会话迁移机制不仅可用于手机辅助电脑登录，也可用于电脑辅助手机登录或其他设备间的会话导入，能够较好体现该项目与其他产品在多端身份交互上的差异化设计。

图 5 手机端扫码后对目标终端登录请求进行上下文预览与确认

3.2.2 已登录设备作为密码找回背书设备

在账号恢复问题上，传统密码找回方案通常高度依赖邮箱或手机号等单一通道。该类方案虽然操作简便，但无法进一步证明用户是否仍然控制某一台可信终端，因而在邮箱泄露、短信劫持或旧设备残留会话等场景下仍存在明显风险。针对这一问题，该项目已完成“已登录设备背书式账号恢复”核心原型。当前流程要求用户先在已登录设备上完成一次敏感验证，随后系统才允许签发一次性的恢复码或恢复二维码；该恢复授权同时绑定发起背书的会话标识、设备来源与上下文信息，并设置短时有效期，从而保证恢复行为建立在“仍控制可信终端”的更强前提之上。

新设备进入找回密码流程后，可以通过扫码或手动输入恢复码的方式读取恢复上下文；在正式确定修改新密码时，系统会再次校验背书设备对应会话是否仍然活跃。若原背书设备已经退出登录，则恢复授权自动失效；若恢复完成成功，系统将同步更新密码、清空敏感验证状态、撤销旧会话，并为当前设备签发新会话。这一设计将恢复流程由“单点通道验证”升级为“可信设备控制权验证+恢复授权一次性消费+旧会话风险收口”的闭环过程，具备更强的安全性。

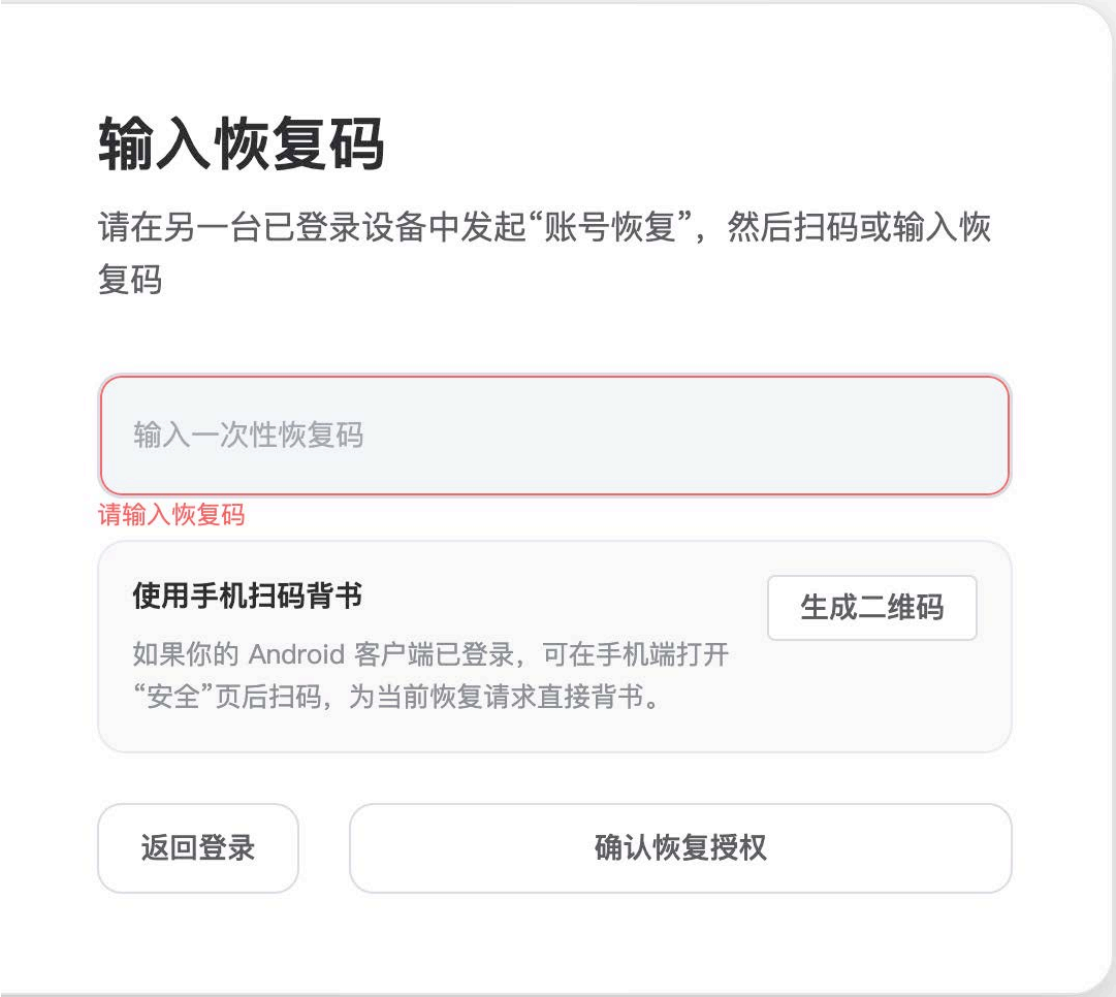


图 6 忘记密码页中引入已登录设备扫码背书与一次性恢复码机制

3.2.3 Web 端与移动/桌面桥接登录

在多端一体化身份体验方面，该项目已完成两类具有代表性的桥接方案。其一是 Web 端与 App 的身份桥接（这里以 Android 客户端为例）：浏览器侧先创建 bridge 挑战，再通过 AppLink 拉起已登录移动端，由 App 完成确认，最后浏览器仅凭一次性 transferCode 向服务端换取自己的网页登录态。在这一过程中，浏览器不会直接读取 App 本地 Token，App 也不会直接给浏览器写入 Cookie，真正的会话仍由后端基于挑战结果重新签发，因此既保留了“App 已登录，浏览器可快速继续”的体验优势，也守住了最小共享原则与会话边界。

其二是Web端与桌面端之间的桥接。考虑到当前桌面原型阶段在原生Passkey调用上受平台签名与系统条件限制，项目采用了“浏览器执行 WebAuthn，桌面

端通过本地回调接收结果”的过渡型桥接方案。这样做虽然在形式上会拉起浏览器，但能够在不改动后端认证协议的前提下，完成桌面端登录、MFA、敏感验证和 Passkey 注册等操作验证。把“终端身份孤岛”问题转化为可治理的桥接问题，并通过一次性挑战、白名单 returnUrl、短时票据与服务端重签发机制维持安全边界。

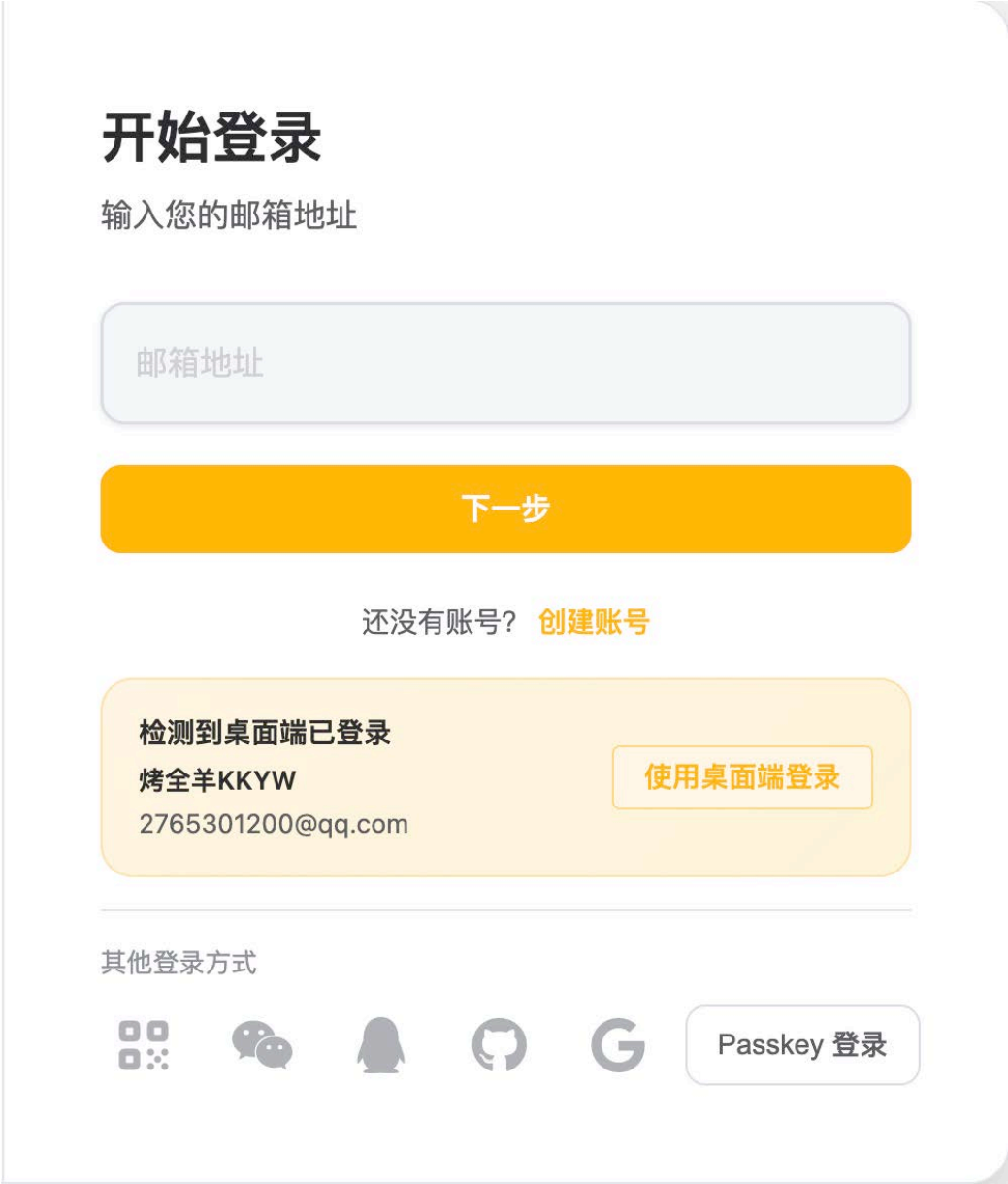


图 7 Web 登录页检测到桌面端已登录并支持桥接复用身份

3.2.4 应用临时授权与定时授权

围绕应用接入治理，项目已将 OAuth/OIDC 授权从传统的“同意/拒绝”二元开关扩展为可配置的授权生命周期控制模型。当前授权页已支持长期授权、一次性授权与限时授权三种模式，后端策略模块负责对授权模式进行标准化、对有效时长进行合法性校验，并据此计算到期时间与授权复用条件。其中，长期授权适合需要频繁访问的长期合作应用；一次性授权适合临时导出、单次操作等高敏感场景；限时授权则面向短期协作、临时办公等真实业务需求，在可用性与最小授权原则之间提供折中。

该项工作的重要意义在于，不再把授权看作静态、一次性的用户确认动作，而是将其进一步上升为身份平台的治理对象。在当前实现中，前端授权页、已授权应用管理页以及后端授权记录结构之间已经形成联动，能够展示授权方式、最近授权时间和授权有效期等信息，初步具备了授权生命周期可视化与可撤销管理能力。这一能力对于高校数字身份在临时接入、轻量集成和数据共享等场景中的精细化治理具有现实意义。

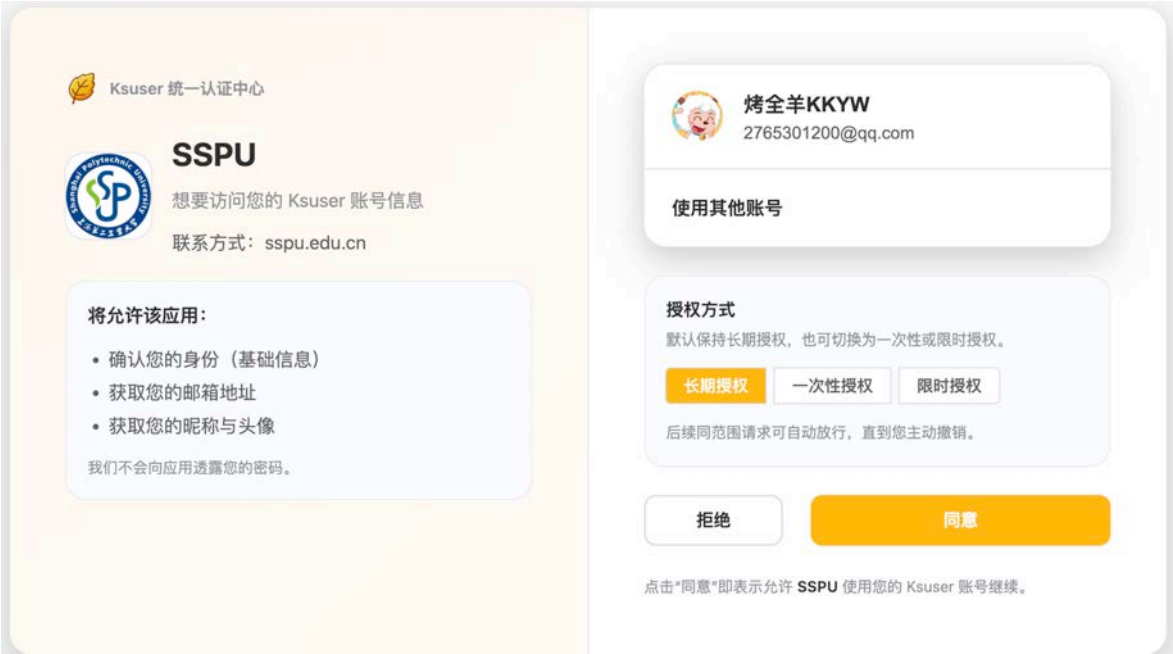


图 8 授权页已支持长期授权、一次性授权与限时授权三种模式

3.2.5 智能风控与自适应连续认证引擎

除认证前的身份校验外，当前还在着重推进了“登录之后如何持续判断会话可信度”的问题。为此，后端已实现基于多因素信号的风险评估与策略编排机制，可综合当前 IP 与建会话 IP 是否一致、地理位置是否变化、会话持续时间、空闲时长、近期失败认证事件、最近一次风险事件评分、最近一次 MFA 或敏感验证时间等因素，对当前会话进行低、中、高三级风险划分，并生成对应的推荐动作。对于中等风险场景，系统会触发 step-up 验证；对于高风险场景，则可进一步冻结当前会话并要求重新登录。

与此同时，风控逻辑并未仅仅停留在基础的单次打分层面，而是继续引入了风险决策日志、去重缓存、主动告警与效果指标统计等机制。Web 端、移动端和桌面端当前均已具备风险状态展示面板，能够查看风控值、等级、当前会话环境、误报率与平均验证时延等指标，这为后续实现更精细的策略联动、异常行为拦截和统一安全账本奠定了基础。

图 9 自适应连续认证引擎的当前会话风险状态与指标面板

3.3 数据库设计

3.3.1 数据模型

为了方便项目的查询与管理，将所有的数据存入数据库，包括了 user 基本信息表，user_settings 用户偏好设置表，user_sessions 用户会话表，user_sensitive_logs 用户敏感操作信息表，user_passkeys 用户通行密钥表等，数据表之间的关系如图 12 所示。

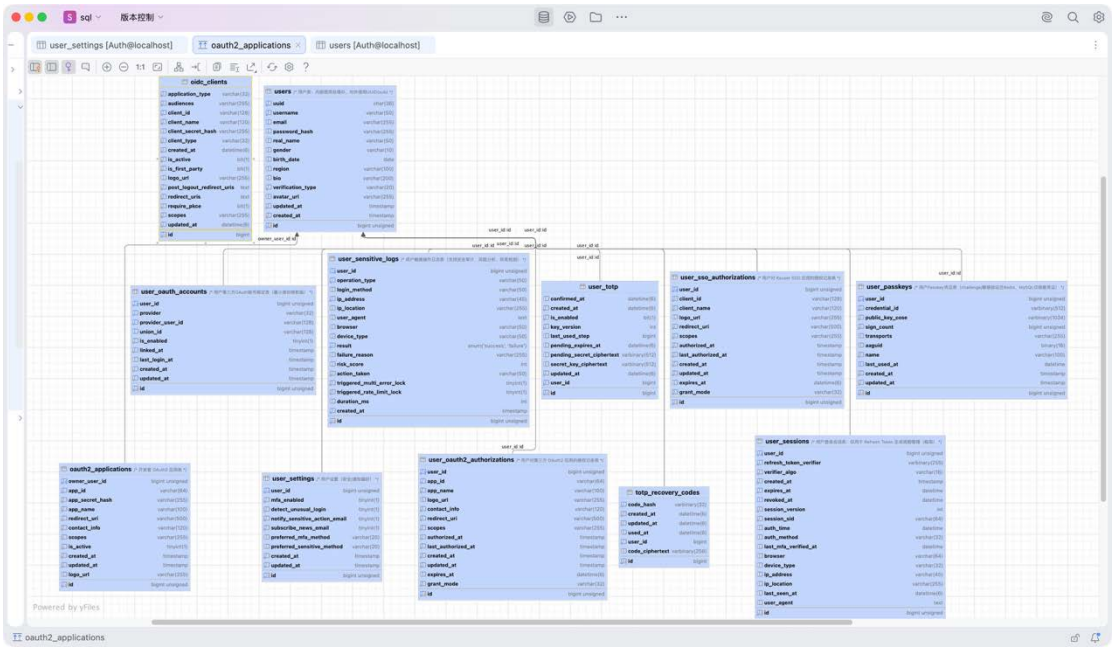
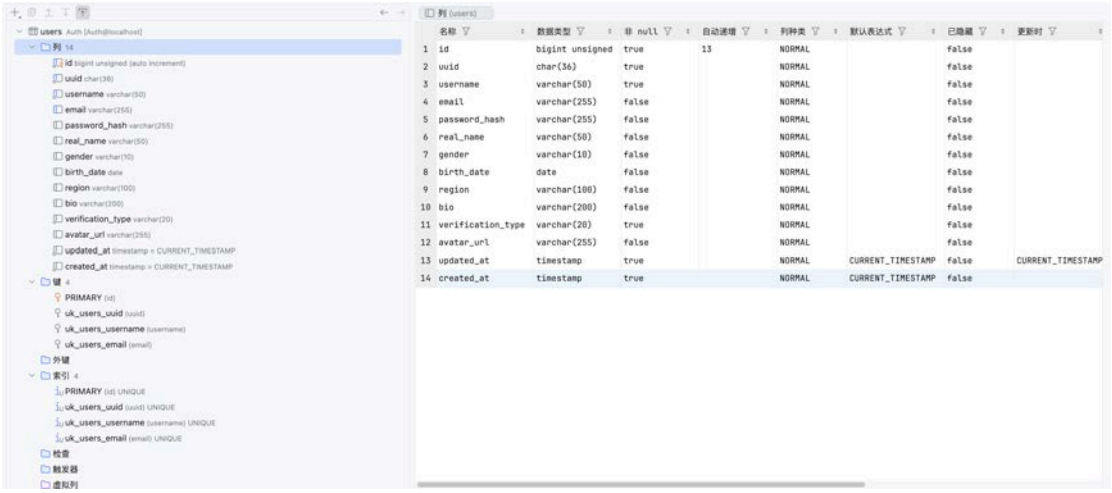


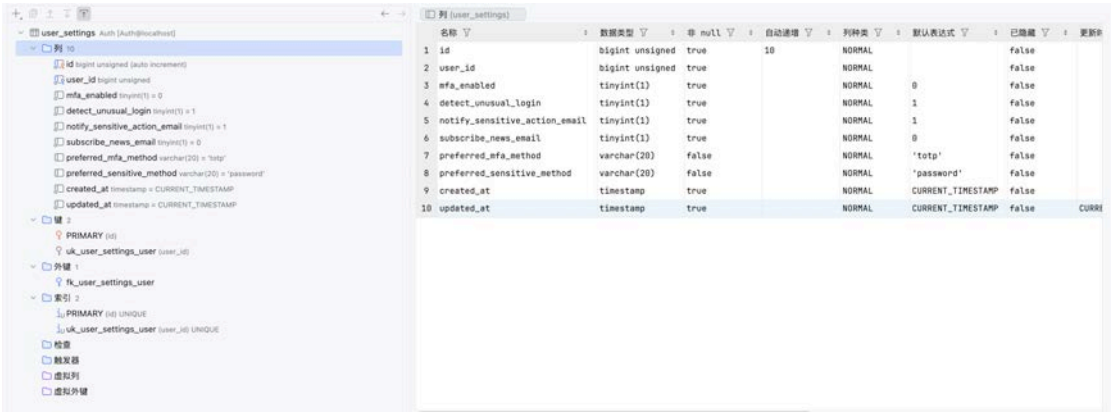
图 10 数据模型图

3.3.2 数据字典



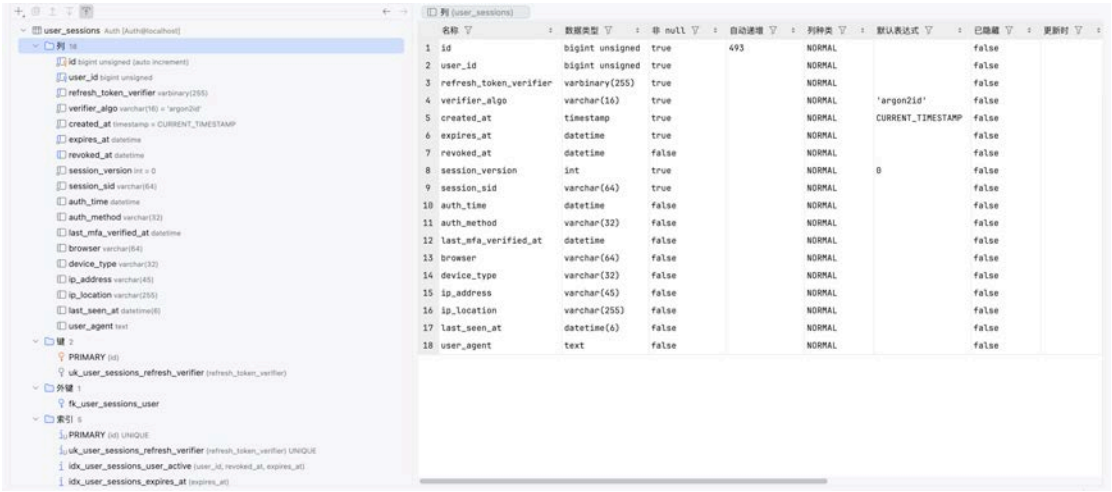
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	13	NORMAL		false	
2	uuid	char(36)	true		NORMAL		false	
3	username	varchar(50)	true		NORMAL		false	
4	email	varchar(255)	false		NORMAL		false	
5	password_hash	varchar(255)	false		NORMAL		false	
6	real_name	varchar(50)	false		NORMAL		false	
7	gender	varchar(10)	false		NORMAL		false	
8	birth_date	date	false		NORMAL		false	
9	region	varchar(100)	false		NORMAL		false	
10	bio	varchar(200)	false		NORMAL		false	
11	verification_type	varchar(20)	true		NORMAL		false	
12	avatar_url	varchar(255)	false		NORMAL		false	
13	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAMP
14	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	

图 11 user 数据字典表



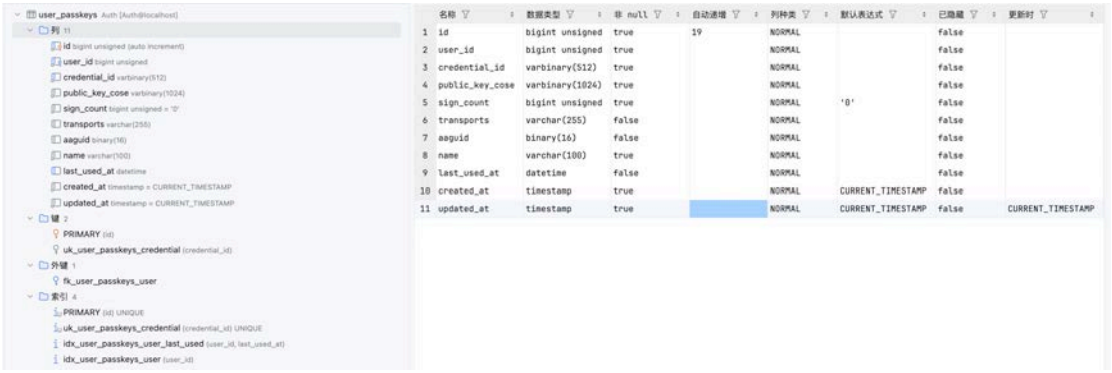
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新
1	id	bigint unsigned	true	10	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	mfa_enabled	tinyint(1)	true		NORMAL	0	false	
4	detect_unusual_login	tinyint(1)	true		NORMAL	1	false	
5	notify_sensitive_action_email	tinyint(1)	true		NORMAL	1	false	
6	subscribe_news_email	tinyint(1)	true		NORMAL	0	false	
7	preferred_mfa_method	varchar(20)	false		NORMAL	'totp'	false	
8	preferred_sensitive_method	varchar(20)	false		NORMAL	'password'	false	
9	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
10	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRE

图 12 user_settings 数据字典表



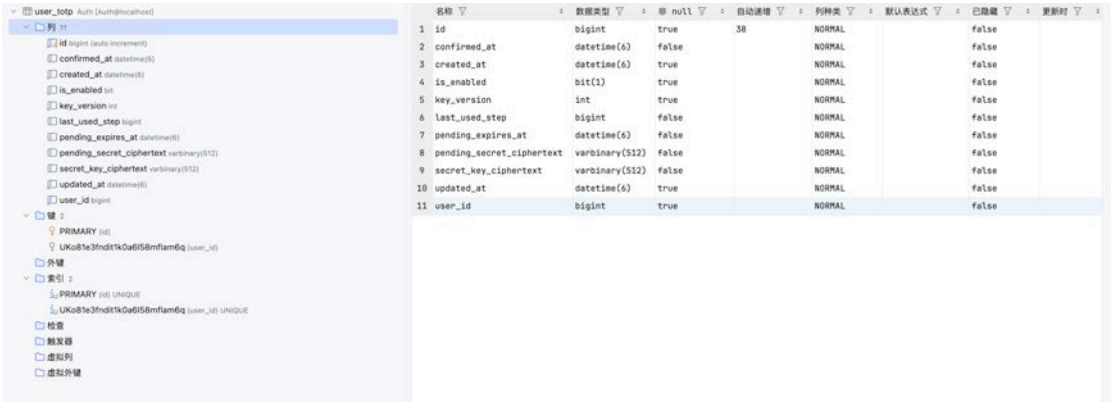
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	493	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	refresh_token_verifier	varbinary(255)	true		NORMAL		false	
4	verifier_algo	varchar(16)	true		NORMAL	'argon2id'	false	
5	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
6	expires_at	datetime	true		NORMAL		false	
7	revoked_at	datetime	false		NORMAL		false	
8	session_version	int	true		NORMAL	0	false	
9	session_sid	varchar(64)	true		NORMAL		false	
10	auth_time	datetime	false		NORMAL		false	
11	auth_method	varchar(32)	false		NORMAL		false	
12	last_mfa_verified_at	datetime	false		NORMAL		false	
13	browser	varchar(64)	false		NORMAL		false	
14	device_type	varchar(32)	false		NORMAL		false	
15	ip_address	varchar(45)	false		NORMAL		false	
16	ip_location	varchar(255)	false		NORMAL		false	
17	last_seen_at	datetime(6)	false		NORMAL		false	
18	user_agent	text	false		NORMAL		false	

图 13 user_sessions 数据字典表



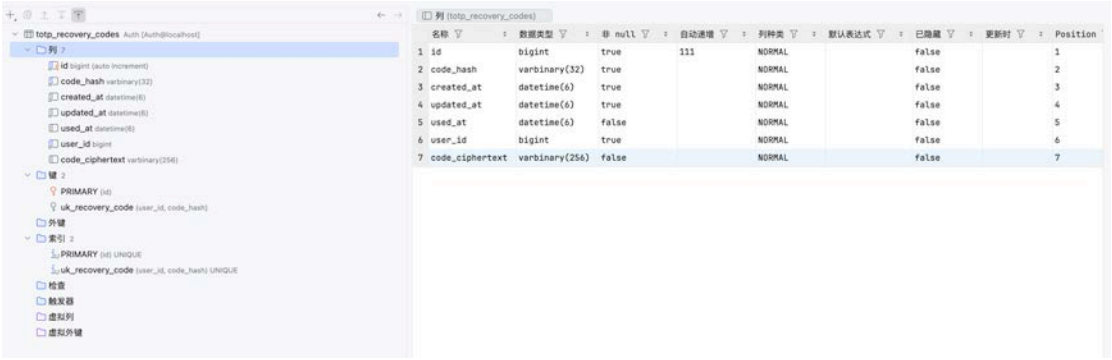
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	19	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	credential_id	varbinary(512)	true		NORMAL		false	
4	public_key_cose	varbinary(1024)	true		NORMAL		false	
5	sign_count	bigint unsigned	true		NORMAL	'0'	false	
6	transports	varchar(255)	false		NORMAL		false	
7	aaguid	binary(16)	false		NORMAL		false	
8	name	varchar(100)	true		NORMAL		false	
9	last_used_at	datetime	false		NORMAL		false	
10	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
11	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAMP

图 14 user_passkeys 数据字典表



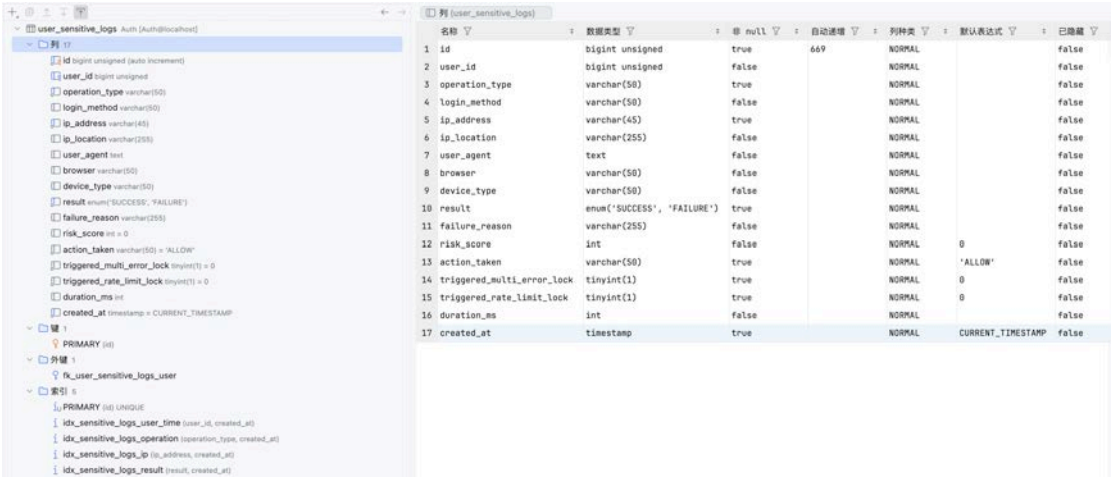
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint	true	38	NORMAL		false	
2	confirmed_at	datetime(6)	false		NORMAL		false	
3	created_at	datetime(6)	true		NORMAL		false	
4	is_enabled	bit(1)	true		NORMAL		false	
5	key_version	int	true		NORMAL		false	
6	last_used_step	bigint	false		NORMAL		false	
7	pending_expires_at	datetime(6)	false		NORMAL		false	
8	pending_secret_ciphertext	varbinary(512)	false		NORMAL		false	
9	secret_key_ciphertext	varbinary(512)	false		NORMAL		false	
10	updated_at	datetime(6)	true		NORMAL		false	
11	user_id	bigint	true		NORMAL		false	

图 15 user_totp 数据字典表



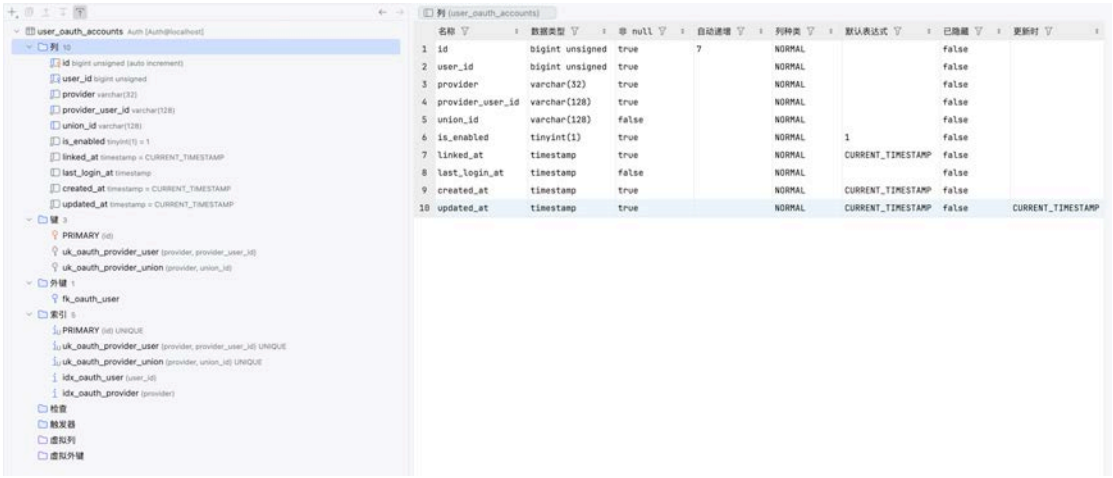
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时	Position
1	id	bigint	true	111	NORMAL		false		1
2	code_hash	varbinary(32)	true		NORMAL		false		2
3	created_at	datetime(6)	true		NORMAL		false		3
4	updated_at	datetime(6)	true		NORMAL		false		4
5	used_at	datetime(6)	false		NORMAL		false		5
6	user_id	bigint	true		NORMAL		false		6
7	code_ciphertext	varbinary(256)	false		NORMAL		false		7

图 16 totp_recovery_codes 数据字典表



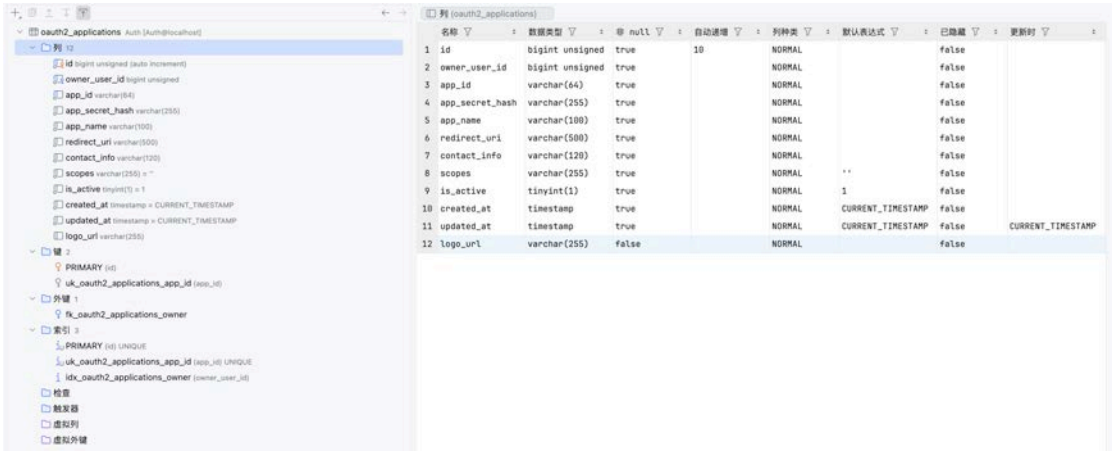
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏
1	id	bigint unsigned	true	669	NORMAL		false
2	user_id	bigint unsigned	false		NORMAL		false
3	operation_type	varchar(50)	true		NORMAL		false
4	login_method	varchar(50)	false		NORMAL		false
5	ip_address	varchar(45)	true		NORMAL		false
6	ip_location	varchar(255)	false		NORMAL		false
7	user_agent	text	false		NORMAL		false
8	browser	varchar(50)	false		NORMAL		false
9	device_type	varchar(50)	false		NORMAL		false
10	result	enum('SUCCESS', 'FAILURE')	true		NORMAL		false
11	failure_reason	varchar(255)	false		NORMAL		false
12	risk_score	int	false		NORMAL	0	false
13	action_taken	varchar(50)	true		NORMAL	'ALLOW'	false
14	triggered_multi_error_lock	tinyint(1)	true		NORMAL	0	false
15	triggered_rate_limit_lock	tinyint(1)	true		NORMAL	0	false
16	duration_ms	int	false		NORMAL		false
17	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false

图 17 user_sensitive_logs 数据字典表



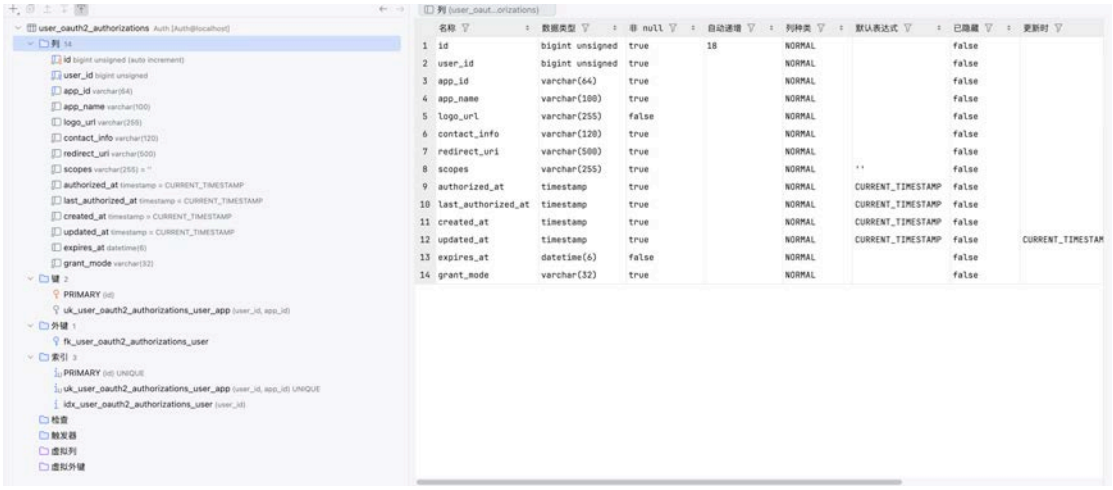
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	7	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	provider	varchar(32)	true		NORMAL		false	
4	provider_user_id	varchar(128)	true		NORMAL		false	
5	union_id	varchar(128)	false		NORMAL		false	
6	is_enabled	tinyint(1)	true		NORMAL	1	false	
7	linked_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
8	last_login_at	timestamp	false		NORMAL		false	
9	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
10	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAMP

图 18 user_oauth_accounts 数据字典表



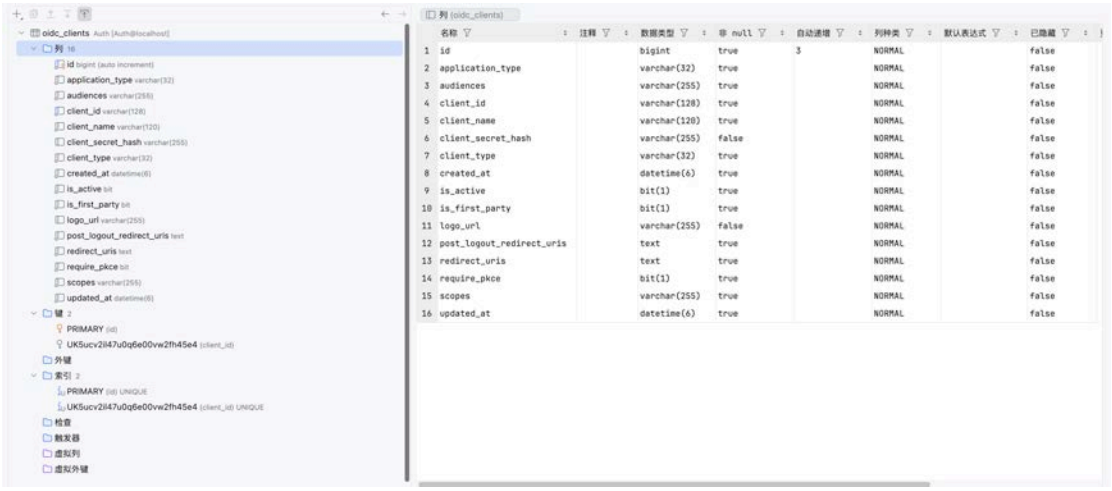
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	10	NORMAL		false	
2	owner_user_id	bigint unsigned	true		NORMAL		false	
3	app_id	varchar(64)	true		NORMAL		false	
4	app_secret_hash	varchar(255)	true		NORMAL		false	
5	app_name	varchar(100)	true		NORMAL		false	
6	redirect_uri	varchar(500)	true		NORMAL		false	
7	contact_info	varchar(120)	true		NORMAL		false	
8	scopes	varchar(255)	true		NORMAL	''	false	
9	is_active	tinyint(1)	true		NORMAL	1	false	
10	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
11	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAMP
12	logo_url	varchar(255)	false		NORMAL		false	

图 19 oauth2_applications 数据字典表



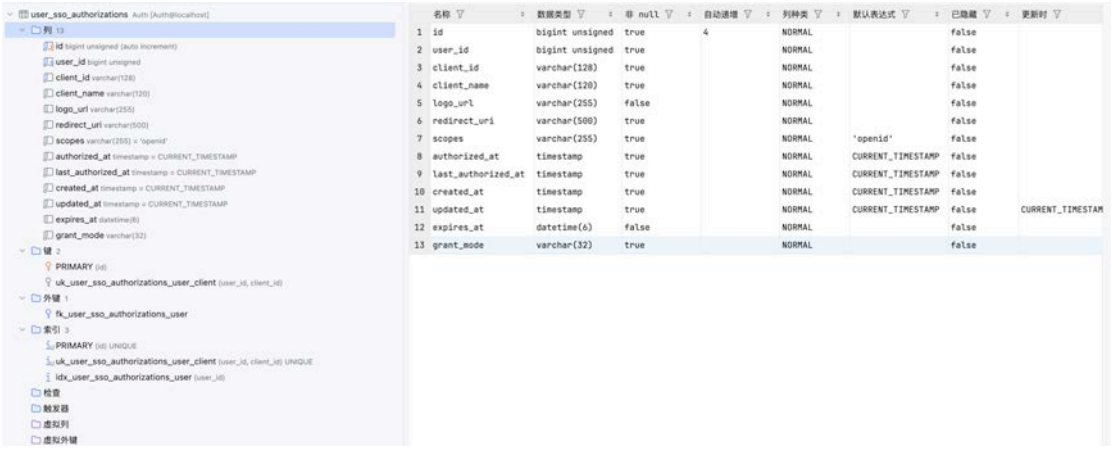
	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	18	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	app_id	varchar(64)	true		NORMAL		false	
4	app_name	varchar(100)	true		NORMAL		false	
5	logo_url	varchar(255)	false		NORMAL		false	
6	contact_info	varchar(120)	true		NORMAL		false	
7	redirect_uri	varchar(500)	true		NORMAL		false	
8	scopes	varchar(255)	true		NORMAL	''	false	
9	authorized_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
10	last_authorized_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
11	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
12	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAM
13	expires_at	datetime(6)	false		NORMAL		false	
14	grant_mode	varchar(32)	true		NORMAL		false	

图 20 user_oauth2_authorizations 数据字典表



	名称	注释	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏
1	id		bigint	true	3	NORMAL		false
2	application_type		varchar(32)	true		NORMAL		false
3	audiences		varchar(255)	true		NORMAL		false
4	client_id		varchar(128)	true		NORMAL		false
5	client_name		varchar(120)	true		NORMAL		false
6	client_secret_hash		varchar(255)	false		NORMAL		false
7	client_type		varchar(32)	true		NORMAL		false
8	created_at		datetime(6)	true		NORMAL		false
9	is_active		bit(1)	true		NORMAL		false
10	is_first_party		bit(1)	true		NORMAL		false
11	logo_url		varchar(255)	false		NORMAL		false
12	post_logout_redirect_uris		text	true		NORMAL		false
13	redirect_uris		text	true		NORMAL		false
14	require_pkce		bit(1)	true		NORMAL		false
15	scopes		varchar(255)	true		NORMAL		false
16	updated_at		datetime(6)	true		NORMAL		false

图 21 oidc_clients 数据字典表



	名称	数据类型	非 null	自动递增	列种类	默认表达式	已隐藏	更新时
1	id	bigint unsigned	true	4	NORMAL		false	
2	user_id	bigint unsigned	true		NORMAL		false	
3	client_id	varchar(128)	true		NORMAL		false	
4	client_name	varchar(120)	true		NORMAL		false	
5	logo_url	varchar(255)	false		NORMAL		false	
6	redirect_uri	varchar(500)	true		NORMAL		false	
7	scopes	varchar(255)	true		NORMAL	'openid'	false	
8	authorized_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
9	last_authorized_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
10	created_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	
11	updated_at	timestamp	true		NORMAL	CURRENT_TIMESTAMP	false	CURRENT_TIMESTAM
12	expires_at	datetime(6)	false		NORMAL		false	
13	grant_mode	varchar(32)	true		NORMAL		false	

图 22 user_sso_authorizations 数据字典表

3.4 功能模块设计

3.4.1 登录模块

登录模块（这里以 Web 为例），该系统提供用户多种登录方式：

一、 以邮箱为载体

用户输入邮箱后，会让用户选择具体登录方式（邮箱+密码/邮箱+验证码），用户在输入正确的密码/验证码后即可登录（频繁错误则会触发风控甚至锁定，详见风控模块）

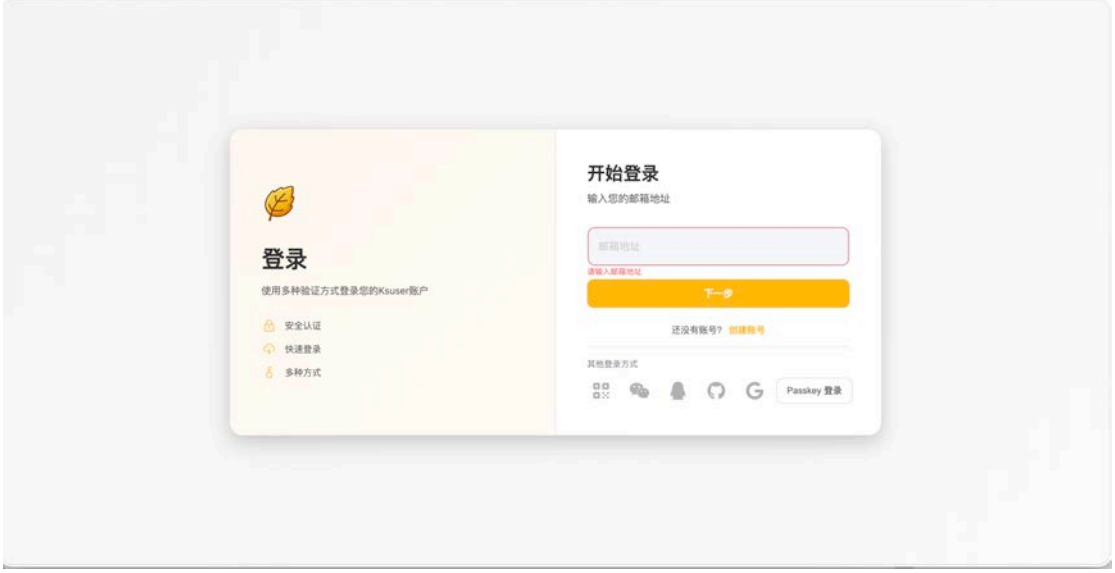


图 23 web 登录页面(1)

图 24 web 登录页面(2)

二、 以第三方为载体

用户可以选择微信、QQ、微软账号等方式进行第三方登录（需提前在账号中心绑定）

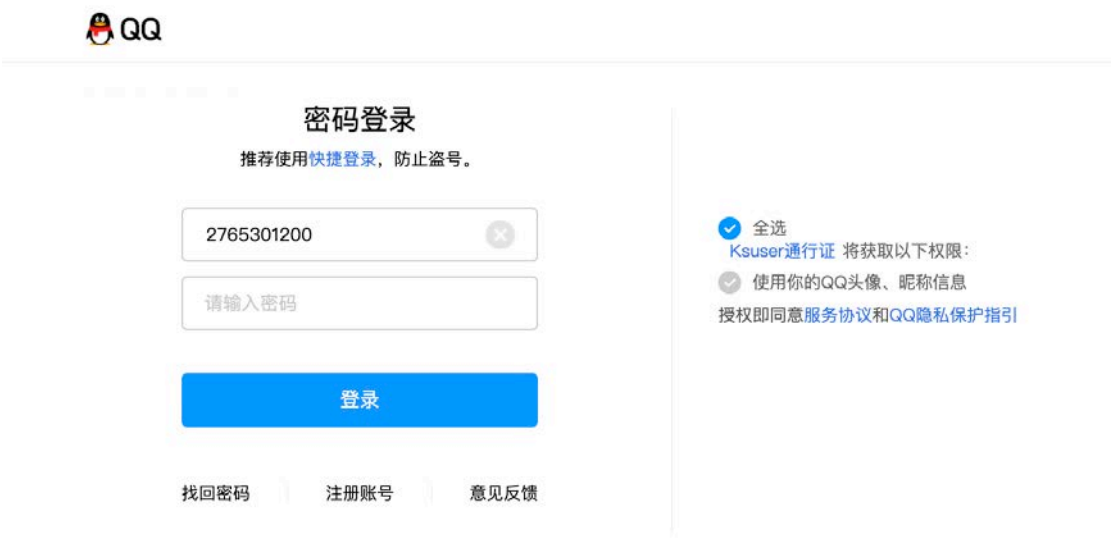


图 25 web 第三方登录页面

三、 以通行密钥为载体

用户可以使用实体密钥（例如 YubiKey）或者虚拟通行密钥（例如 1Password、Apple KeyClain）进行无密码身份认证，这种方法相较于传统密码更加安全，且不需要记忆密码，不用担心密码丢失或泄露的问题。

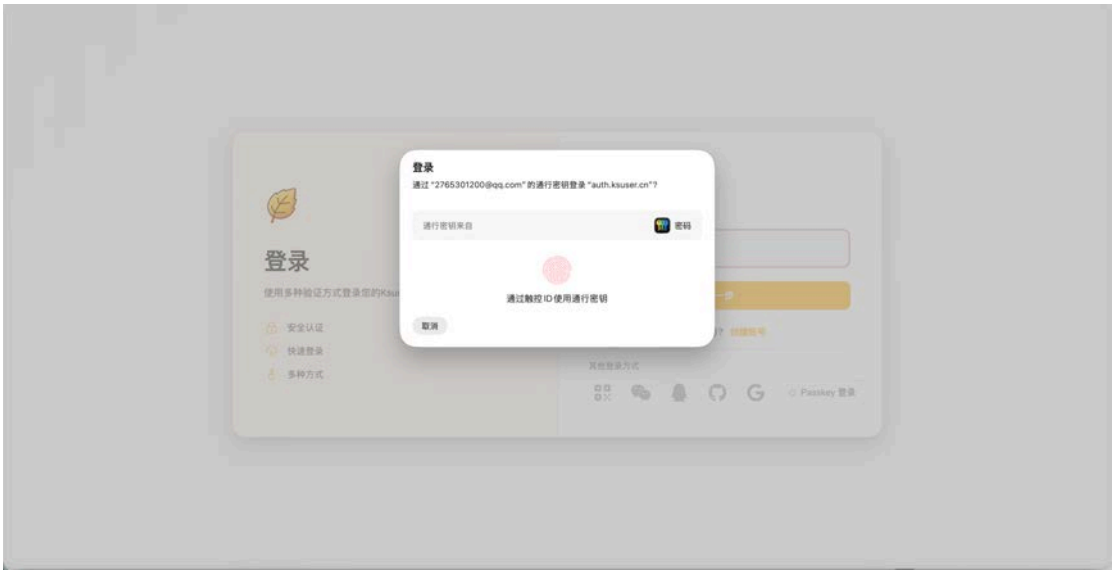


图 26 web 虚拟 Passkey（通行密钥）登录页面

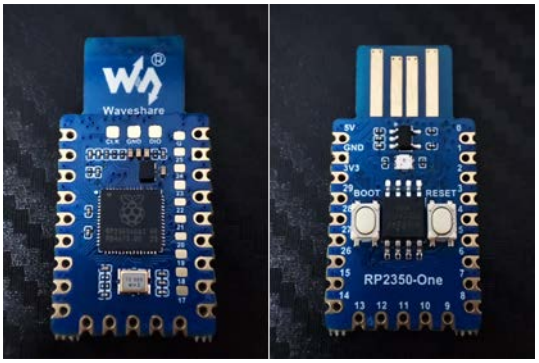


图 27 实体硬件密钥（WaveShare RP2350 - PicoKey）（左）

图 28 web 实体 Passkey（通行密钥）登录页面（右）

四、 以信任移动端设备为载体

用户还可以选择使用已登录且**风险评分低于 60 分**的移动端 APP 进行扫码登录

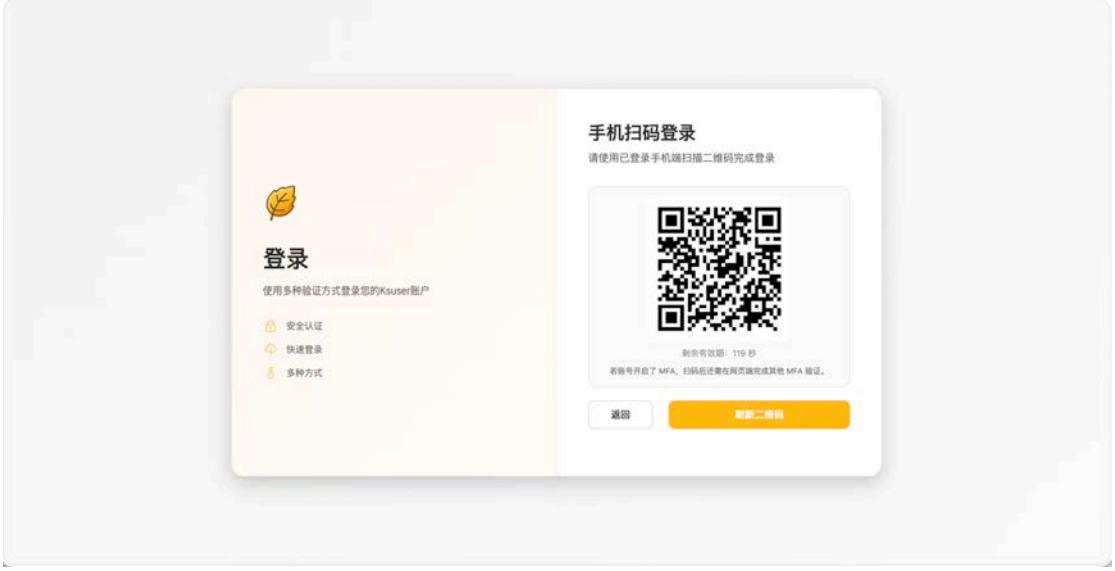


图 29 web 手机扫码登录页面

如果账号开启了 MFA（多因素身份验证），则还需要进行二次验证，二次验证支持 Passkey（通行密钥）与 TOTP（一次性验证码）。用户需要提前绑定以上其一才能开启 MFA。除此之外，当用户使用 Passkey 登录且开启 MFA 时，则须使用 TOTP 或另一个 Passkey 进行二次验证。

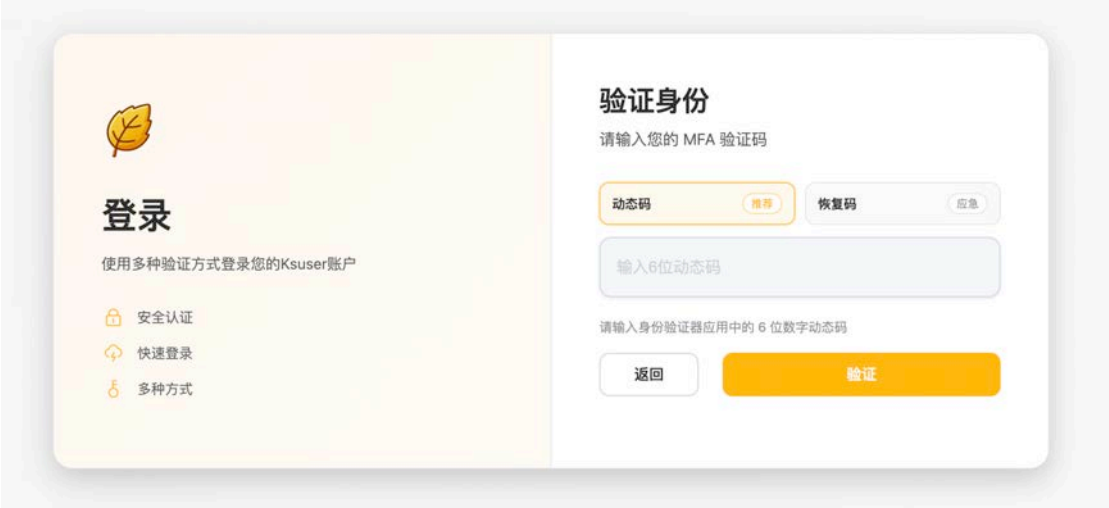


图 30 web MFA 多因素验证登录页面

上述登录功能全取自网页端，特此同时附上桌面端与移动端的登录页面截图

图 31 桌面端登录页面

图 32 移动端登录页面

3.3.2 Web 端模块

进入主页后，可以在左侧导航栏中进行响应数据内容的查看与操作

一、 账号总览页

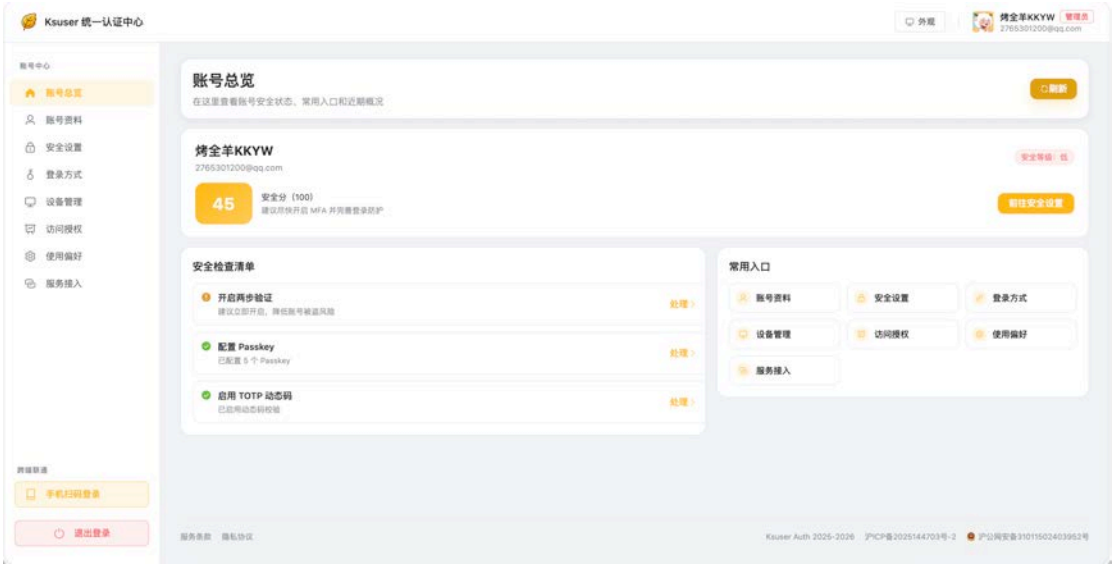


图 33 web 主页页面

二、 账号资料页

用户可以在这里更改自己的基础信息

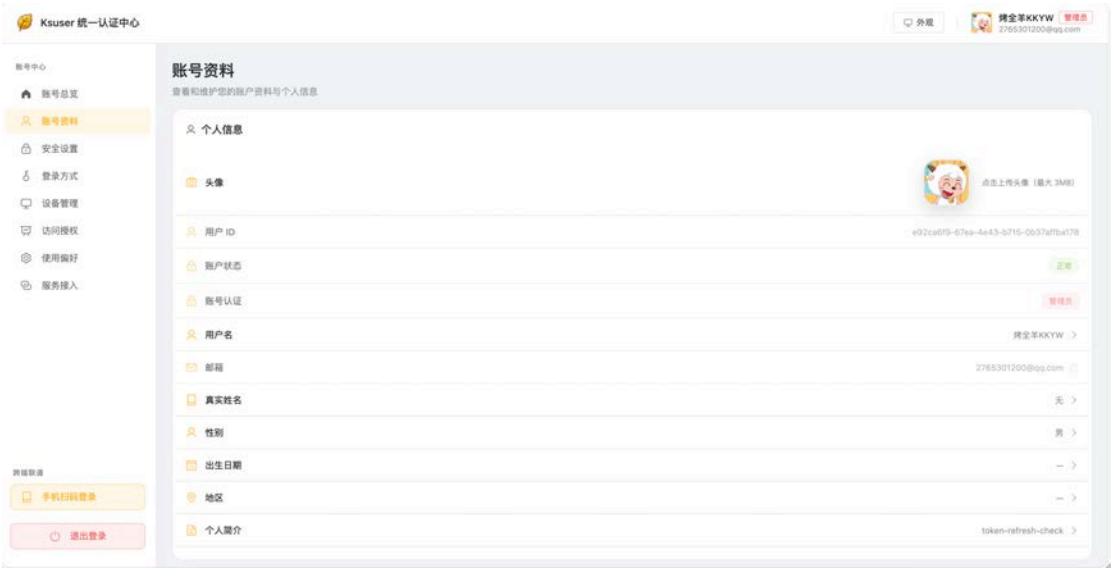


图 34 web 账号资料页面

三、 安全设置页

用户可以在这里管理账号安全，配置 MFA 等安全设置；并查看该账号近期执行过的敏感操作

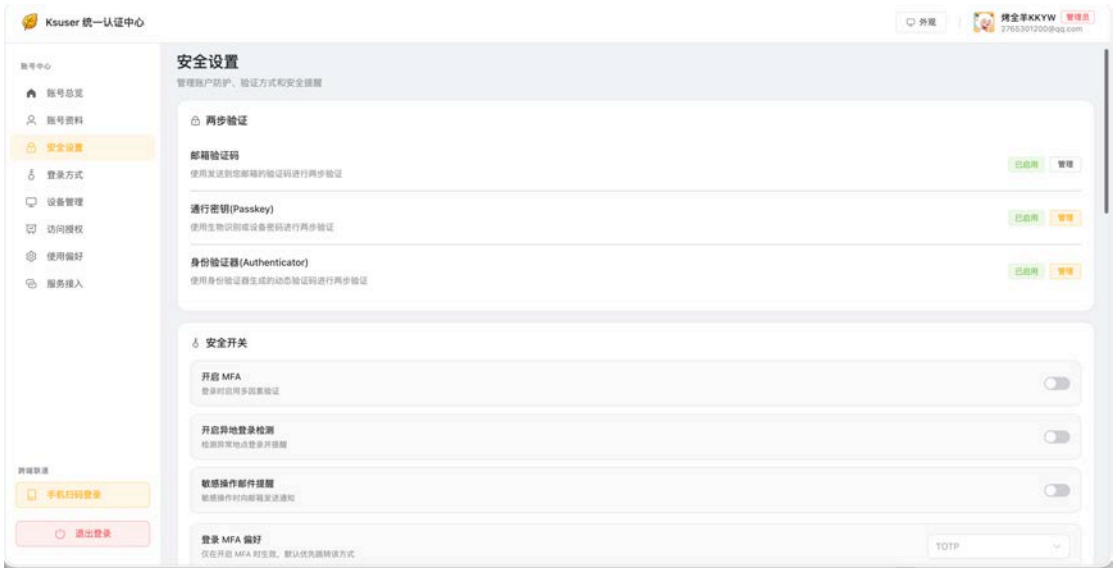


图 35 web 安全设置页面（1）

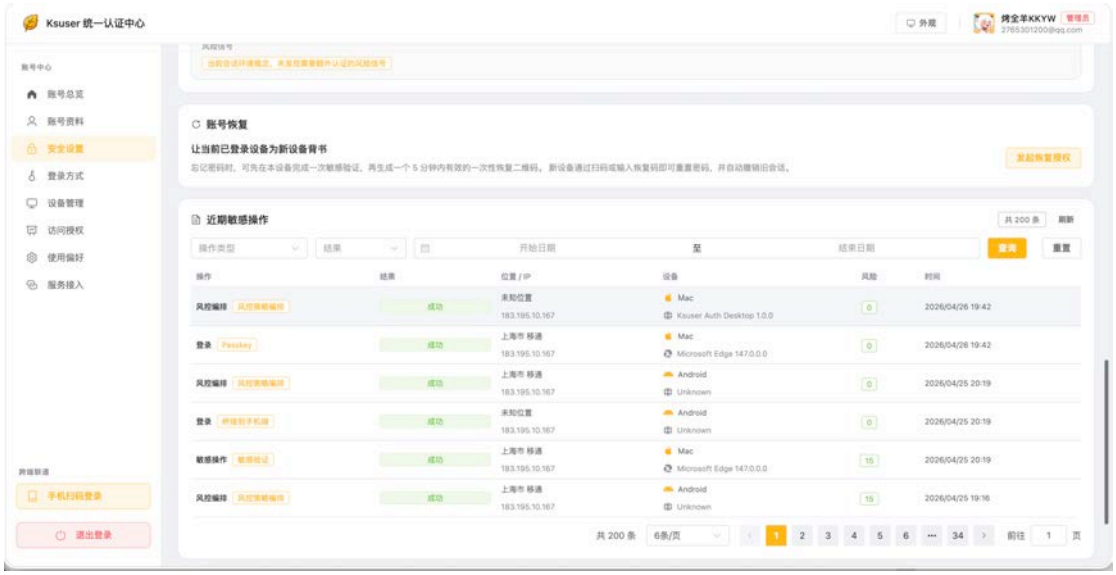


图 36 web 安全设置页面（2）

四、 登录方式页

用户可以在这里修改自己的登录方式，包括修改绑定邮箱、密码、第三方登录信息、Passkey 通行密钥、TOTP 一次性密码

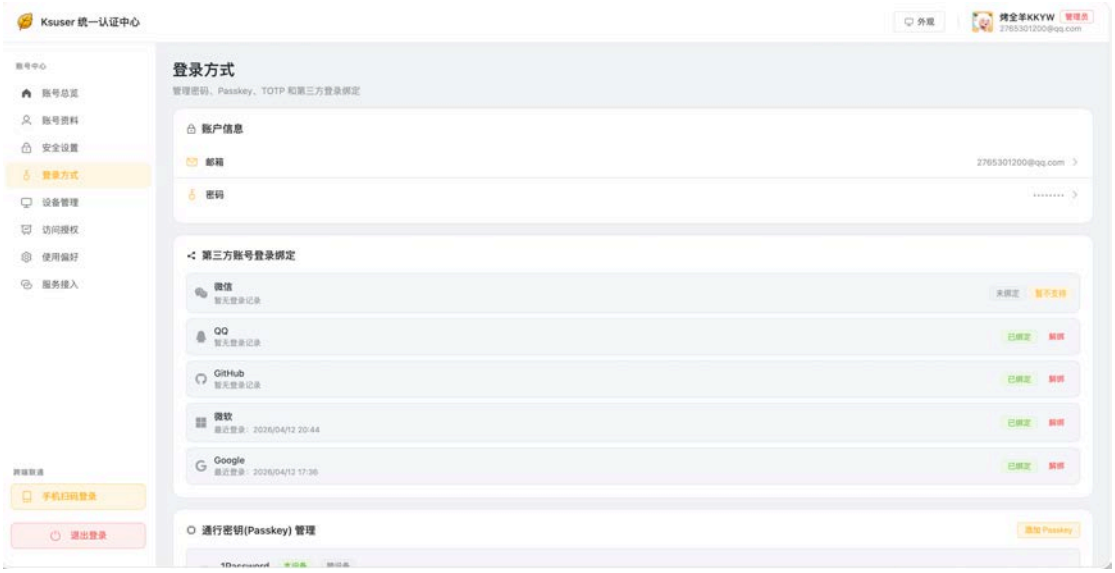


图 37 web 登录方式页面（1）

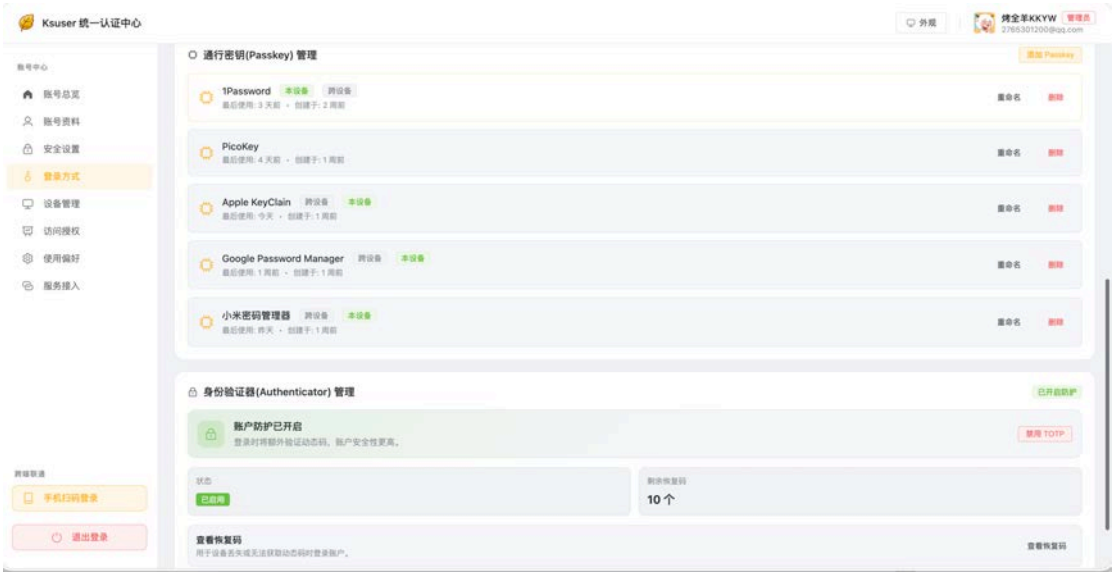


图 38 web 登录方式页面（2）

五、 设备管理页

用户可以在这里查看已经登录的设备，并可随时退出任一会话

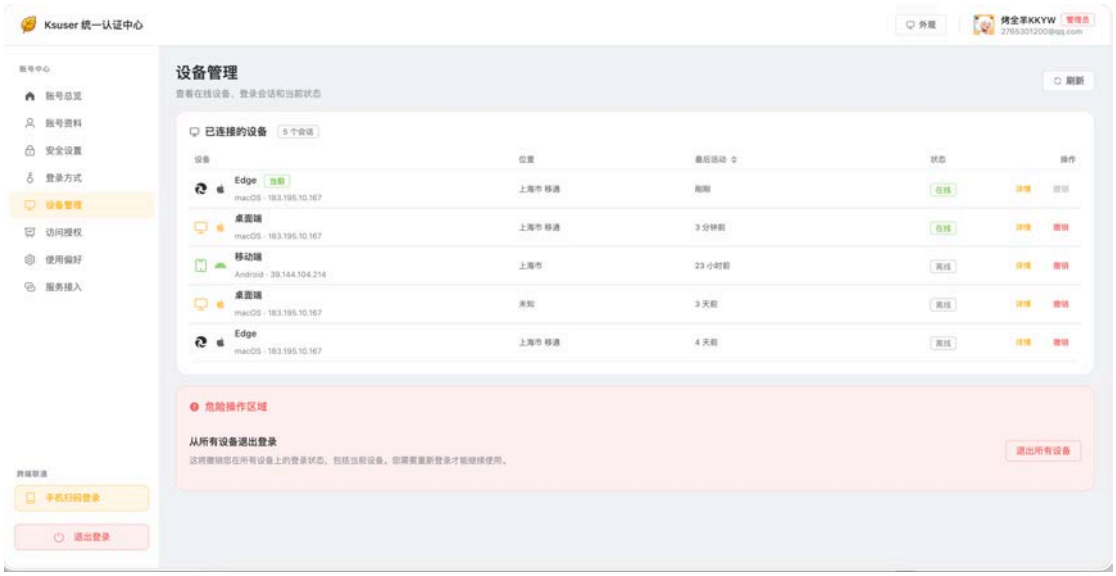


图 39 web 设备管理页面

六、 访问授权页

用户可以在这里查看自己已经授权过的应用，并可随时取消授权；还可以一键下载自己的账号信息数据到本地，确保用户的信息始终都在用户自己的手上

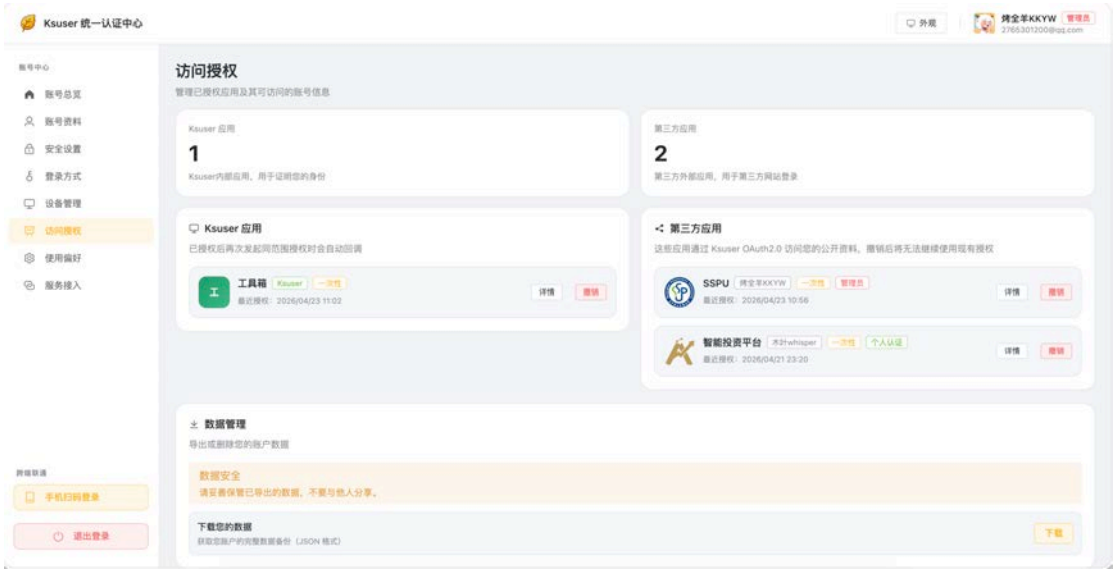


图 40 web 访问授权页面

七、 使用偏好页

用户可以在这里选择推送偏好与页面色彩主题

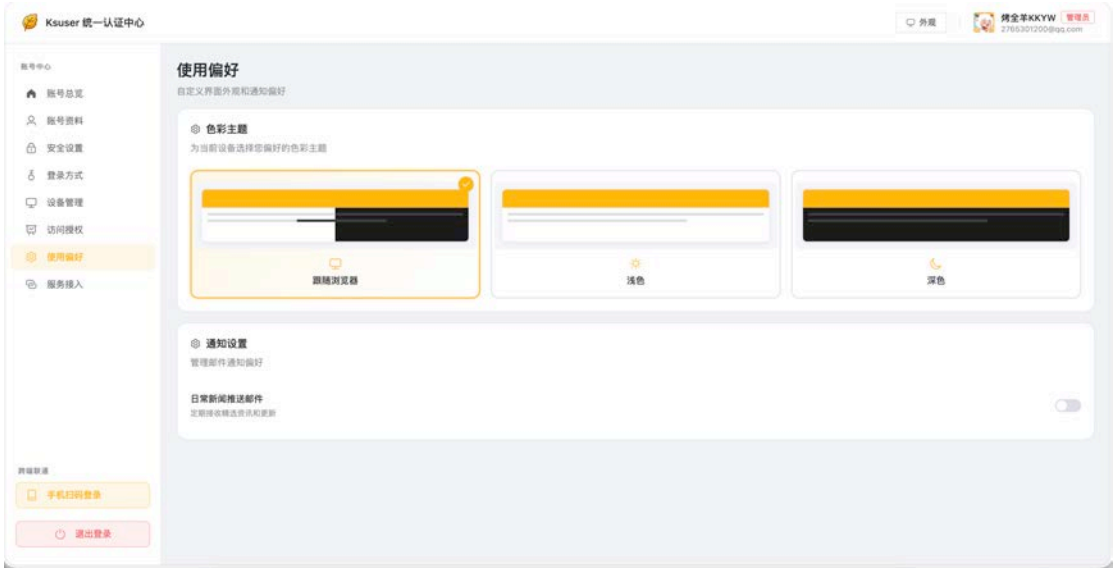


图 41 web 使用偏好页面

八、 服务接入页

经认证的用户可以在这里创建 OAuth 应用与 SSO 内部应用（**仅管理员**）

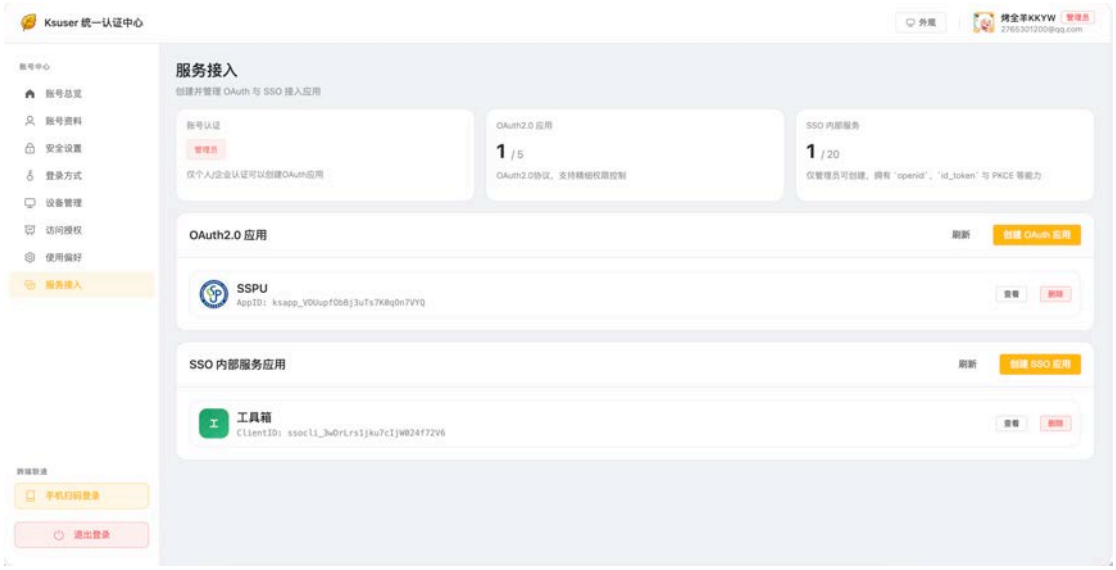


图 42 web 服务接入页面

3.3.3 移动端模块

图 43 移动端概览页面（左）

图 44 移动端资料页面（右）

图 45 移动端安全页面（左）

图 46 移动端会话页面（中）

图 47 移动端日志页面（右）

3.3.4 桌面端模块

一、 账号总览

图 48 桌面端账号总览页面

二、 账号资料

图 49 桌面端账号资料页面

三、 安全设置

图 50 桌面端安全设置页面（1）

图 51 桌面端安全设置页面（2）

四、 设备管理

图 52 桌面端设备管理页面

五、 操作日志

图 53 桌面端操作日志页面

3.3.5 隐秘无感认证模块（桌面端）

在桌面端的右上角有一个图标（如图），在 Windows 系统中点击后自动到系统托盘，MacOS 则会隐藏到菜单栏（图中左二），但仍持续保存用户当前会话状态。在这种情况下 OAuth 与 SSO 应用可以无感识别桌面端登录状态，实现静默鉴权，极大优化用户体验。

图 54 桌面端（MacOS）最小化菜单栏（1）

图 55 桌面端（MacOS）最小化菜单栏（2）

图 56 web 端 OAuth 应用检测桌面端登录状态页面

3.3.5 请求频率限制模块

为了防止自动化程序造成的用户账号安全性降低的问题，该系统采用较为严格的频率限制措施,阈值总览如图 45

图 57 后端各项操作频率限制示意图

1. 登录尝试限流

主要作用于密码登录接口： /auth/login，先检查邮箱与 IP 是否超限，再记录次数，然后才做账号密码校验。判断逻辑： Redis 计数小于阈值才放行；窗口分别是 1 分钟和 1 小时。同时第三方 OAuth 回调登录也复用了 TYPE_LOGIN 的 IP 限流，防止回调端点被刷。

2. 验证码发送限流

主要作用于验证码发送接口：/auth/send-code 在发邮件前先做两层 IP、邮箱两层限流，若命中分钟阈值返回“发送过于频繁，请 1 分钟后再试”；命中小时阈值返回“每小时最多发送 14 次”。限流通过后才生成并发送验证码，发送成功后再写入 Redis 计数（分钟键+小时键）。

3. 注册尝试限流

对 register 类型还叠加“注册成功次数锁定”（当天同 IP/UA 达到 2/3/4 次则分别锁定 10 分钟/1 小时/1 天）。

4. 错误次数限流

针对所有错误请求的计数（包括但不限于 Passkey 验证失败、totp 一次性验证码验证失败等，验证码若未发送不计入错误次数），错误计数达到 5 次即锁邮箱 1 小时；锁定期间无法继续发送或验证该邮箱验证码。当验证成功后会清除该邮箱错误计数，避免历史错误长期累积。

4 总结

通过开发，我更加明确地认识到，数字身份认证平台的难点并不只是把“登录”做出来，而是如何在安全边界、用户体验与多端协同之间取得平衡。例如，在跨端登录与桥接登录场景中，如果直接共享既有 Token，虽然实现简单，但会破坏不同终端之间的会话边界；而采用一次性挑战、服务端重新签发会话的方式，虽然实现复杂度更高，却能更好体现统一认证平台对身份可信链条的控制能力。

同时，我也体会到了在真实环境的中，兼容性尝尝会直接影响方案选择。桌面端原生 Passkey 在当前开发条件下存在平台限制，因此项目采用了浏览器桥接方案作为过渡。这让我认识到：研究与实现不能脱离实际环境，方案设计既要坚持安全原则，也要具备工程上的实际可落地性。

此外，多端接口联调、统一数据结构设计与日志审计等的闭环建设，也培养了我的系统化思维，而不像以前一样仅关注单个页面或单个接口。

图 58 全认证系统分解缩略图