



运营商发展统一账号认证业务技术方案

郭茂文, 张荣, 卢燕青, 黎艳

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 针对当前互联网应用的痛点, 在分析了运营商发展统一账号认证业务应考虑的关键因素的基础上, 提出了以手机号为核心的统一账号认证业务的技术实现方案, 包括系统总体架构、应用接口场景以及差异化认证能力的实现, 然后分析运营商统一账号认证业务互联互通的相关思路, 最后对运营商发展统一账号认证业务的前景进行展望。

关键词: 统一账号; 移动网关认证; 用户卡认证; 互联互通

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018026

Technical scheme of the unified account authentication service for operators

GUO Maowen, ZHANG Rong, LU Yanqing, LI Yan

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: Aiming at the pain point of current internet applications, on the basis of analyzing the key factors that should be considered in the development of unified account authentication service, a technical scheme of unified account authentication service based on mobile phone number was put forward, including the overall architecture of the system, the application interface scene, and the implementation of differentiated authentication. Then, the related ideas about the operators' unified account authentication service interconnection were analyzed. Finally, the prospect of the operators to develop unified account authentication service was also discussed.

Key words: unified account, mobile gateway authentication, user card authentication, interconnection and inter-operation

1 引言

随着互联网和智能移动终端的高速发展, 基于智能移动终端的应用出现了爆发式增长, 这些丰富的应用给人们的工作和生活提供了极大的便利, 但也带来了新的问题。绝大部分应用需要用户进行注册, 有可能注册时需要输入用户的隐私

信息, 如身份证号码、出生日期、联系方式等, 注册过程中用户还需要设置复杂的账号/密码用于后续的应用登录。另外, 由于同一个用户需要使用的应用数量众多, 因此, 用户需要记忆大量的应用账号和密码信息。

这种传统的账号/密码方式的应用在用户体验和安全性方面存在多处痛点, 如密码复杂繁琐、记

忆困难;账号/密码信息容易被不良木马盗窃;用户身份核实困难,只能依赖手机号和身份证信息^[1]。

针对以上这些应用痛点,近两年,国内各电信运营商纷纷利用自身的移动网络 and 用户卡资源优势,大力发展统一账号增值服务业务,如中国移动的和通行证^[2]、中国联通的沃通行证^[3]以及中国电信的天翼账号等。

2 影响发展统一账号认证业务的关键因素

(1) 多网络多终端支持

目前,互联网及智能终端已经非常普遍,用户可以方便地通过各个运营商的3G/4G移动网络或者Wi-Fi网络来使用互联网业务,同一个互联网应用会在智能移动终端、平板电脑或者PC之间频繁使用。因此,运营商的统一账号认证服务必须满足用户在不同类型网络、不同类型终端环境下的正常使用。

(2) 运营商间的互联互通

运营商用户与互联网应用用户具有天然的差异性,互联网应用用户具有跨运营商特性。因此,运营商在发展统一账号认证服务时,必须考虑与其他运营商的互联互通,否则,无法做到互联网应用用户的全覆盖。

(3) 多种认证方式的协同

除了传统的账号/密码和短信验证码认证方式外,运营商还可以提供独有的移动网关认证和用户卡认证。但是,移动网关认证需要用户的移动终端开启移动数据网络功能;用户卡认证需要用户卡下载安装运营商提供的卡应用。因此,统一账号认证服务要求运营商能够准确判断认证过程中用户移动终端和用户卡环境,如果不具备这两种认证能力,必须能够自动切换到传统的账号/密码或短信验证码认证方式。

3 统一账号认证业务的技术实现

3.1 统一账号认证系统总体架构

运营商统一账号认证业务是指以手机号作为

账号体系^[4],以手机为认证载体,以运营商独有的差异化的移动网络 and 用户卡认证能力为核心功能,整合运营商相关资源,向运营商自有应用 and 第三方合作应用提供多等级多因子的安全认证服务,同时输出基础电信能力服务。

基于互联网及智能移动终端技术现状,运营商的统一账号认证业务应能够支持Android和iOS移动应用以及平板电脑/PC的Web应用。为充分利用运营商的网关认证 and 用户卡认证能力,Web应用的登录认证方式可采用移动应用扫描Web登录页面的二维码认证方式实现。在这种应用需求下,运营商的统一账号认证系统架构如图1所示。

统一账号认证系统分为网络侧 and 终端侧两部分,具体介绍如下。

网络侧主要完成应用认证能力开放、认证策略管理、认证能力集成等功能,具体可以分为统一账号认证业务能力开放平台、统一账号认证能力管理平台以及各认证能力子系统。其中,认证能力子系统主要有网关认证系统、卡应用认证系统、账号/密码认证系统和短信验证码认证系统。

终端侧的组成部分主要是统一账号认证业务在终端上的必要能力封装。对于应用,由统一账号提供登录框给应用合作方,在应用合作方Web页面通过iframe的方式嵌入统一账号登录框。登录方式可以包括二维码扫码登录、账号/密码登录、短信验证码登录以及其他的第三方应用账号授权登录等,应用合作方可以根据自身需要选择优先的登录方式。对于移动端应用,由统一账号提供SDK给应用合作方,SDK主要实现对终端认证能力信息的收集,并与统一账号认证能力开放平台配合实现认证功能。另外,对于用户卡认证方式,移动终端需要在用户卡中预置卡应用Applet。

3.2 统一账号认证系统特点

基于上述的统一账号认证系统总体架构可以看出,统一账号认证业务的特点主要如下。

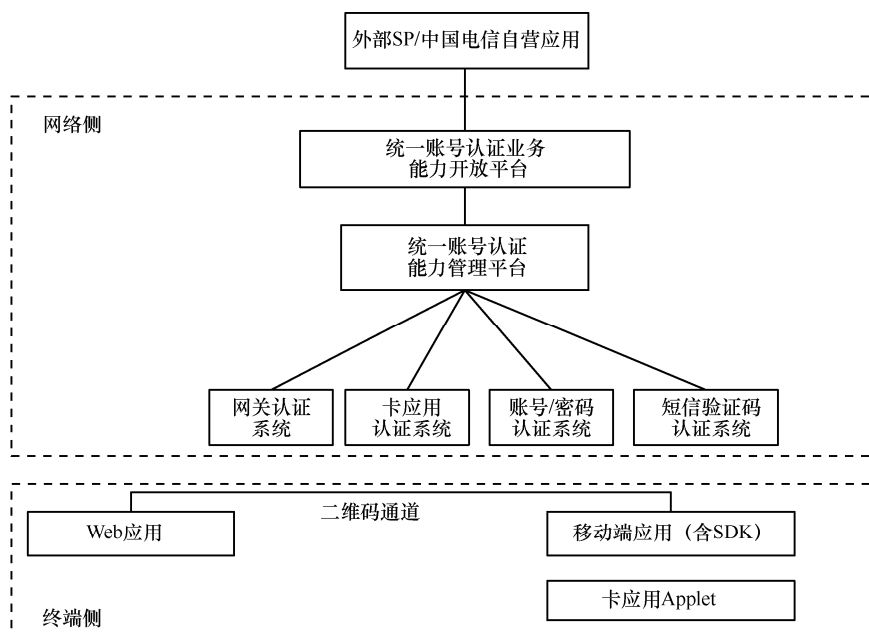


图1 统一账号认证系统总体架构

（1）一号通行

一套以手机号为核心的账号系统可以通行运营商的多个业务和应用，如中国移动的飞信、139邮箱、和彩云以及和通讯录等；中国电信的天翼云、翼健康和号簿助手等。

（2）差异化认证方式

在传统的账号/密码、短信验证码认证方式基础上，运营商还可以利用移动数据网络 and 用户卡资源优势，采用移动通信网关取号以及用户卡识别等技术，提供更安全、更方便快捷的网关认证和用户卡认证能力。

（3）可扩展的“认证+”业务生态能力

统一账号认证服务除了提供基本的登录认证功能外，运营商还可以通过统一账号认证能力开放平台与其他的运营商能力系统对接实现向第三方合作应用开放其核心能力，如“账号+二次放号识别”“账号+支付”“账号+云存储”等^[5]，第三方合作应用不需要多头对接就可以方便快捷地获得这些核心能力。

3.3 关键应用接口场景

运营商统一账号认证系统与第三方合作应用

对接时的接口应用场景主要有两种：一种是移动端应用接口场景；另一种是PC端的Web应用接口场景。

对于移动端应用接口场景，运营商统一账号认证系统可以通过移动端SDK与第三方合作应用对接。移动端应用使用统一账号SDK获得AccessToken，然后通过获取用户信息API利用AccessToken换取手机号码及其他用户信息等。在移动端应用发起登录请求时，由SDK检测移动终端环境，选择最优的认证方式并携带认证方式标志向统一账号业务能力开放平台发起身份认证请求。主要流程实现方案如图2所示。

对于PC端Web应用接口场景，运营商统一账号认证系统可以提供登录框给应用合作方，在应用合作方Web页面通过iframe的方式嵌入统一账号登录框。主要流程实现方案如图3所示。

3.4 差异化认证能力实现方案

运营商差异化的认证能力主要体现在移动网关认证和用户卡认证，其方案实现思路如下。

- 对于移动网关认证来说，需要移动终端开启移动数据网络功能。移动终端上的应用

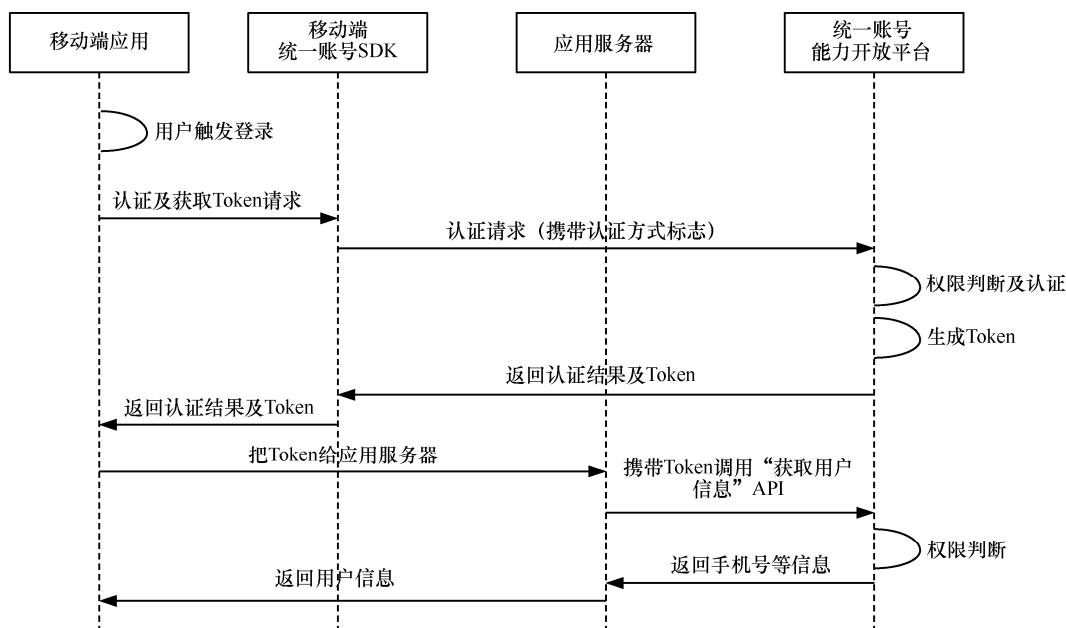


图2 移动端应用接口场景实现流程

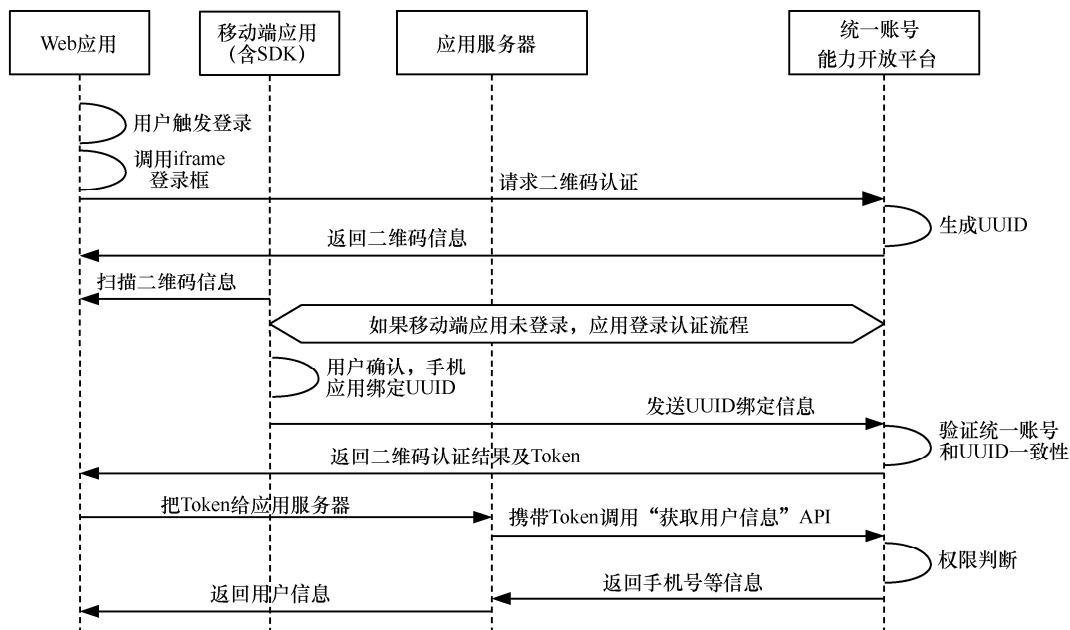


图3 PC端Web应用接口场景实现流程

SDK 通过移动数据网络发送登录请求消息的过程中，在请求消息经过移动网关（PGW）时，移动网关在用户的 HTTP 请求分组头加入加密的用户信息（手机号码 MDN、IMSI、手机 IP 地址、PGW IP 地址等）后传递给网关认证系统，网关认证系统对用户信息进行解密后识别用户手机号

码，确认用户身份，用户即可登录认证成功。实现方案如图 4 所示。

- 对于用户卡认证来说，需要在用户卡中预置卡应用 Applet^[6]。卡应用 Applet 初始化时会通过 OTA 数据短信方式与卡认证系统进行卡认证配置数据的同步，卡认证系统确认该用户支持卡认证。用户登录时，移

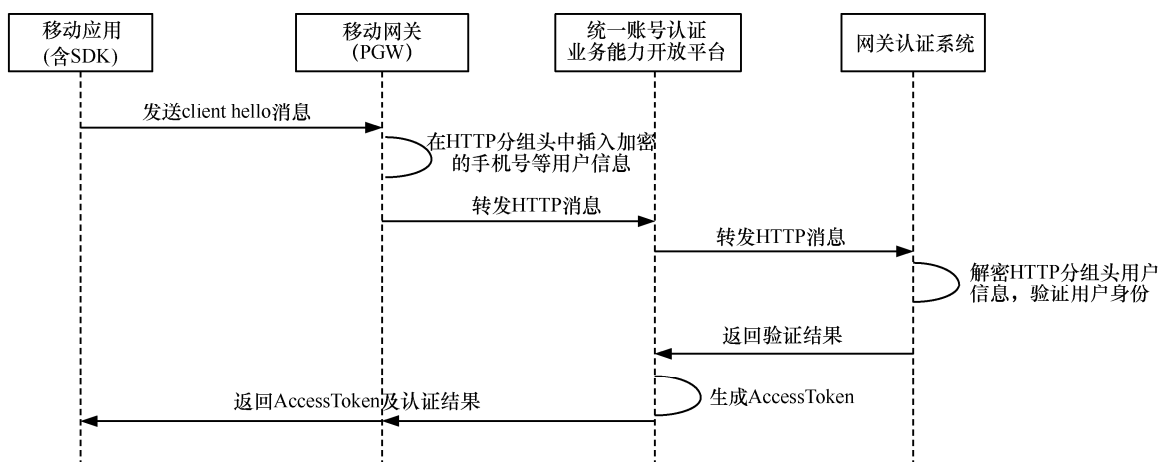


图4 移动网关认证实现方案

动终端上的应用 SDK 发送登录请求消息给统一账号业务能力开放平台，该请求消息通过统一账号认证能力管理平台传递给用户卡认证系统。用户卡认证系统通过短信网关下发 OTA 数据短信到用户卡，用户卡根据短信信息在手机上弹出用户登录确认的 UTK 提示框，用户确认（输入 PIN 码或点击 OK）后，用户卡发送登录确认短信给用户卡认证系统，用户即可登录认证成功。实现方案如图 5 所示。

无论是移动网关认证还是用户卡认证方式，对用户移动终端环境都有一定的要求。移动网关认证方式需要移动终端能够用户在手机设置中开

启移动数据网络开关，而用户卡认证方式需要用户卡预置有卡应用 Applet，并进行初始化同步。因此，对于某个用户来说，每次登录时选择何种认证方式需要通过应用 SDK 与统一账号认证能力开放平台的配合和信息交互来确定。运营商也可以通过认证策略配置来实现认证方式的最优选择，如当用户手机的移动数据网络功能开启时，可让用户每次登录时优先选择移动网关认证方式；当用户登录后的网络行为需要进行二次身份认证时，可选择安全性更高的用户卡认证方式，以替代传统的短信验证码认证方式，当然，其前提是现网用户的用户卡预置卡应用 Applet 比较普及。当用户移动终端环境无法支持移动网关认证

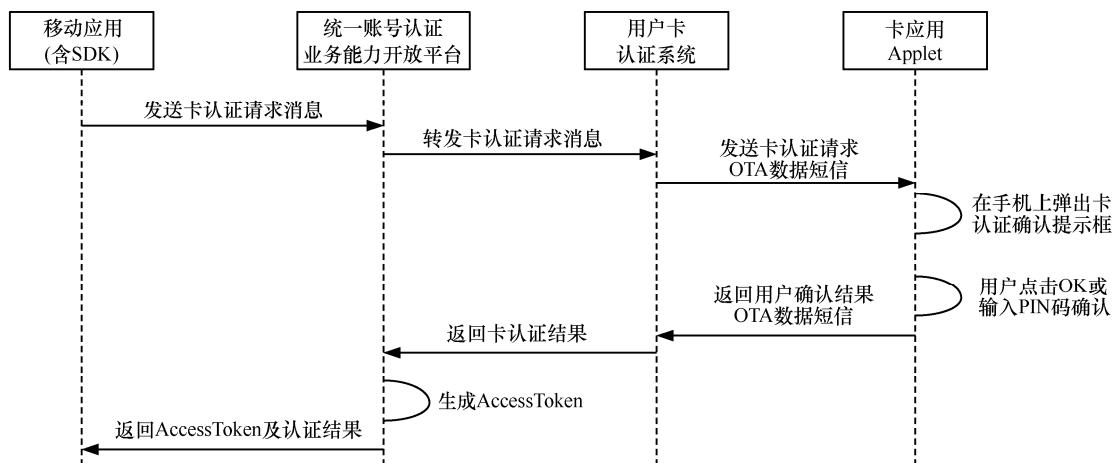


图5 用户卡认证实现方案

和用户卡认证这两种方式时,统一账号认证系统能够根据用户或第三方合作应用的选择回退到账号/密码或短信验证码的认证方式。

4 统一账号认证业务的互联互通

运营商发展统一账号认证业务的优势在于差异化的移动网关认证和用户卡认证技术,但是,由于单个运营商所拥有的用户无法覆盖单个互联网应用所拥有的用户,因此,统一账号认证业务必须要做到运营商之间的互联互通^[7]。这样,SP(服务提供商)应用只需要与单个运营商对接,其所有用户均可以使用统一账号认证业务。

运营商统一账号认证业务互联互通的关键是认证系统能够对以手机号为核心的统一账号进行识别,并基于手机号的归属实现路由转发。根据前面所述的应用接口场景,这里提出一种基于代理转发机制的运营商对等自治互联互通模型来进行分析,如图6所示。

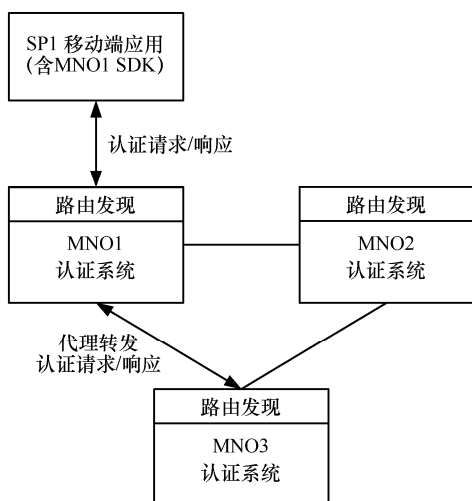


图6 运营商对等自治互联互通模型

如图6所示,SP1的移动端应用包含有MNO1运营商的SDK,即SP1的移动端应用在登录认证时只向MNO1运营商的认证系统发送认证请求。各运营商的认证系统均具有相对独立的号码识别和路由发现功能,并且各自互信对接。这里以MNO3运营商用户使用与MNO1运营商认证系统

对接的SP1移动端应用为例来分析不同认证方式的互联互通方案。

传统的账号/密码认证方式不需要互联互通,只需要MNO3运营商用户使用与MNO1运营商认证系统对接的SP1移动端应用时,以其手机号(归属MNO3运营商)在MNO1运营商认证系统注册成统一账号即可,MNO1运营商认证系统就可以在本地完成对异网手机号的统一账号用户完成账号/密码方式的认证。

对于短信验证码方式,只需要运营商各自的短信网关系统能够互通即可。MNO3运营商用户的短信验证码通过MNO1运营商认证系统产生,MNO1运营商的短信网关将该短信验证码转发给MNO3运营商的短信网关,MNO3运营商的短信网关再将短信验证码直接发送到其用户手机上。

对于移动网关认证方式,其互联互通的实现思路可以如下:

(1) MNO3运营商用户在移动端发起SP1应用(与MNO1运营商的认证系统对接)的登录操作;

(2) SP1应用SDK通过MNO3运营商的移动数据网络发送client hello消息;

(3) MNO3运营商的移动网关插入用户手机号等用户信息;

(4) MNO1运营商的认证系统接收到SP1应用SDK的HTTP消息,并解析;

(5) MNO1运营商的认证系统将SP1应用SDK的HTTP消息转发给MNO3运营商的认证系统;

(6) MNO3运营商的认证系统验证用户手机号的合法性,验证通过后,产生AccessToken,并与验证结果一起发送给MNO1运营商的认证系统;

(7) MNO1运营商的认证系统转发AccessToken和验证结果给SP1应用SDK;

(8) SP1应用将AccessToken发送给SP1应用服务器;

(9) SP1应用服务器携带AccessToken向MNO1运营商的认证系统调用“获取用户信息”API;



(10) MNO1 运营商的认证系统通过 MNO3 运营商的认证系统获得用户信息, 并返回给 SP1 应用服务器。

这种移动网关认证方式互联互通的关键是每个运营商的移动网关必须采用一致的 HTTP 头增强功能, 以及 AccessToken 与用户信息在运营商认证系统之间的安全传输。

对于用户卡认证方式的互联互通, 其实现方案比较简单, SP1 应用 SDK 发送卡认证请求(携带手机号信息, 如首次认证时用户手工输入其手机号)给 MNO1 运营商的认证系统后, MNO1 运营商的认证系统根据手机号判断其归属运营商, 并将认证请求转发给归属运营商的认证系统。归属运营商的认证系统完成卡认证后, 直接将认证结果和 AccessToken 返回给 MNO1 运营商的认证系统。在卡认证方式情况下, SP1 应用服务器获取用户信息的方法与移动网关认证方式情况是类似的。

5 结束语

总的来说, 随着互联网应用和智能移动终端的大规模普及, 运营商发展统一账号认证业务可以实现电信与互联网的跨体系融合发展。这样既可以作为密码认证的替代品, 减少多重身份校验带来的麻烦, 提升用户账户的安全性, 又可以实现整合运营商自身的基础电信能力输出, 增强用户黏性, 提升运营商在互联网时代的价值。但是, 由于现网移动终端环境千差万别, 运营商必须完善独有的差异化移动网关认证和用户卡认证技术, 并实现运营商相互之间的互联互通, 优化和提升用户业务体验, 运营商的统一账号认证业务才会具有良好的应用前景。

参考文献:

- [1] 孙韩林, 刘建华. 公众网络统一身份认证服务及标准研究[J]. 电信科学, 2013, 29(2): 84-88.
SUN H L, LIU J H. Study on unified identifier authentication service and standards on public network[J]. Telecommunications Science, 2013, 29(2): 84-88.
- [2] 中国移动集团公司. 中国移动能力开放白皮书[R]. 2016.
China Mobile Communications Corporation. The white paper of China Mobile's ability[R]. 2016.
- [3] 刘镝, 张云勇, 张尼, 等. “沃互联”统一认证技术研究[J]. 电信科学, 2015, 31(6): 6-11.
LIU D, ZHANG Y Y, ZHANG N, et al. Research on “Wo Connect” uniform authentication technology[J]. Telecommunications Science, 2015, 31(6): 6-11.
- [4] CCTIME 飞象网. 运营商统一帐号体系背后的战略思考[Z]. 2016.
Dumbo CCTIME. Strategic thinking behind the unified account number system of the operators[Z]. 2016.
- [5] 中国电信集团公司. 中国电信统一账号业务规范[S]. 2017.
China Telecom Co. Business specification of China Telecom [S]. 2017.
- [6] 董双赫, 严斌峰, 胡博, 等. 基于 SIM 卡的金融应用移动数字签名业务研究[J]. 电信科学, 2015, 31(6): 12-17.
DONG S H, YAN B F, HU B, et al. Research on SIM card-based mobile digital signature and authentication for financial services[J]. Telecommunications Science, 2015, 31(6): 12-17.
- [7] 张荣, 黎艳, 郭建昌. 基于用户卡的移动认证技术方案与应用[J]. 移动通信, 2015(5): 31-35.
ZHANG R, LI Y, GUO J C. Technical solution and application of mobile authentication based on sim-applet[J]. Mobile Communications, 2015(5): 31-35.

[作者简介]



郭茂文(1973—), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为移动互联网技术与业务、互联网应用安全等。

张荣(1973—), 女, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为移动互联网新技术与业务、智能管道等。

卢燕青(1973—), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为互联网网络技术和应用、移动互联网核心业务等。

黎艳(1981—), 女, 中国电信股份有限公司广州研究院工程师, 主要研究方向为移动互联网安全、智慧家庭等。