



中国电信用户数据库-总体规范

V 1.0

中国电信集团公司

2009 年 8 月

前 言

用户数据库（**UDB**）是实现中国电信应用层统一认证的基础网元设备，也是有效支撑中国电信帐号经营的基础平台。通过 **UDB** 将中国电信各个独立应用系统整合成以统一帐号为中心的一个大的服务平台，提升客户感知和服务体验。

本规范为中国电信统一用户数据库总体规范，共含三个分册，分别为：流程与接口规范、设备与功能规范、测试规范。

本规范由中国电信集团公司组织制定和颁布，是中国电信用户数据库的系列规范之一。中国电信集团公司具有对本规范的解释和修订权，如与此前颁布相关规范或规定有冲突，以本规范为准。

本规范起草单位：中国电信股份有限公司北京研究院

中国电信股份有限公司四川设计院

中国电信股份有限公司四川分公司

本规范起草人：何潇 熊小明 潘卫 杨鑫 蓝青 黄鹏 李根军 韩苏川 解冲锋 瞿晓波等

目 录

1	适用范围	4
2	引用标准	5
3	缩略语	6
4	规范体系	7
5	术语定义	8
6	中国电信认证体系架构	9
7	UDB 在网络中位置	10
8	UDB 功能描述	11
9	UDB 接口描述	13
9.1	UDB 接口描述	13
9.2	UDB 对于周边系统的要求	15
10	主要数据编码	16
10.1	用户类型编号	16
10.2	通用密码格式编码	16
10.3	用户状态编号	16
10.4	省别编号及简写	17
10.5	应用系统类型编号	18
11	主要应用场景	20
11.1	帐号申请示例流程	20
11.2	统一密码修改示例流程	22
11.3	帐号升级示例流程	22
11.4	用户登录认证场景	23
11.4.1	后台认证	23
11.4.2	重定向认证	24
11.5	宽带接入场景	25
11.6	单点登录场景	26
11.6.1	省内应用系统之间的单点登录	26
11.6.2	省内应用系统与全国应用系统之间的单点登录	27
11.6.3	宽带接入系统与应用系统之间的单点登录	29
11.6.4	网上营业厅与应用系统之间的单点登录	32
11.7	自服务门户应用场景	33
11.8	第三方应用系统合作场景	34

1 适用范围

本规范适用于中国电信 UDB 系统的建设与部署，是中国电信 UDB 招标采购、工程设计、网络运营、维护管理等方面的技术依据，并可作为设备提供商和集成商 UDB 系统设计、设备开发的技术依据。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

- (1) 《中国电信 CDMA 手机用户短信获取密码使用无线宽带 (WiFi) 业务规范 V1.0》
- (2) 《中国电信股份有限公司企业标准 SMGP 协议 V3.0.0》
- (3) 《中国电信股份有限公司企业标准 SMGP 协议 V3.0.3》
- (4) 《中国电信宽带业务管理平台 ISMP 规范总册 (RC1.0) 》
- (5) 《中国电信互联星空技术规范—流程与接口分册 v3.1》
- (6) 《中国电信统一帐号业务规范 (暂定稿)》
- (7) 《中国电信用户数据库—总体规范 V1.0 》
- (8) 《中国电信用户数据库—功能与设备规范 V1.0》
- (9) 《中国电信 C+W PC 版产品—技术规范》
- (10) RFC 2865, Remote Authentication Dial In User
- (11) RFC 2866, RADIUS Accounting
- (12) RFC 2868, RADIUS Attributes for Tunnel Protocol Support
- (13) ITU-T D 83 – E, Report of the meeting of the Service and Network Operations Group (SNO)
- (14) 3GPP TR32.808, Study of Common Profile Storage (CPS)
Framework of User Data for network services and management
- (15) 3GPP TS23.008, Organization of subscriber data
- (16) 3GPP TS23.240, 3GPP Generic User Profile (GUP); Architecture

3 缩略语

缩略语	英文全称	中文描述
UDB	User Database	用户数据库
AAA	Authentication, Authorization, Accounting	认证、授权、计费
ADSL	Asymmetric Digital Subscriber Line	非对称数字用户线路
BOSS	Business & Operation Support System	业务运营支撑系统
CRM	Customer Relation Management	客户关系管理
CT Passport	China Telecom Passport	中国电信通行证
HTTP	Hypertext Transfer Protocol	超文本传输协议
LDAP	Lightweight Directory Access Protocol	轻量目录访问协议
ISAG	Integrated Service Access Gateway	综合业务接入网关
ISAP	Integrated Service Access Protocol	统一业务接入协议
ISMP	Integrated Service Management Platform	综合业务管理平台
OCS	Online Charging System	在线计费系统
OTP	One Time Password	一次性密码
Radius	Remote Authentication Dial In User Service	远程认证拨号接入服务
SOAP	Simple Object Access Protocol/SOAP	简单对象访问协议
SP	Service Provider	服务提供商
SS	Service System	应用系统
SSO	SingleSign-On	单点登录
UAM	MBOSS Unified Authentication	MBOSS域统一认证
UIM	User Identity Model	用户识别模块
WLAN	Wireless LAN	无线局域网
XML	eXtensible Markup Language	可扩展标记语言

4 规范体系

1. 中国电信用户数据库—总体规范
2. 中国电信用户数据库—接口与流程规范
3. 中国电信用户数据库—功能与设备规范
4. 中国电信用户数据库—测试规范
5. 集成方案
 - A. 中国电信UDB与ISMP-B集成方案（待补充）

5 术语定义

下述术语定义适用于中国电信用户数据库规范体系所有涉及的文档。

用户数据库：是实现中国电信应用层统一认证的基础网元，主要完成统一帐号、密码、状态等的集中维护和管理功能。

统一帐号：用户使用电信业务的通用帐号，也称为通行证。通过一个统一帐号即可使用中国电信宽带接入、189 邮箱、互联星空、爱音乐等应用，及中国电信互信的第三方应用。

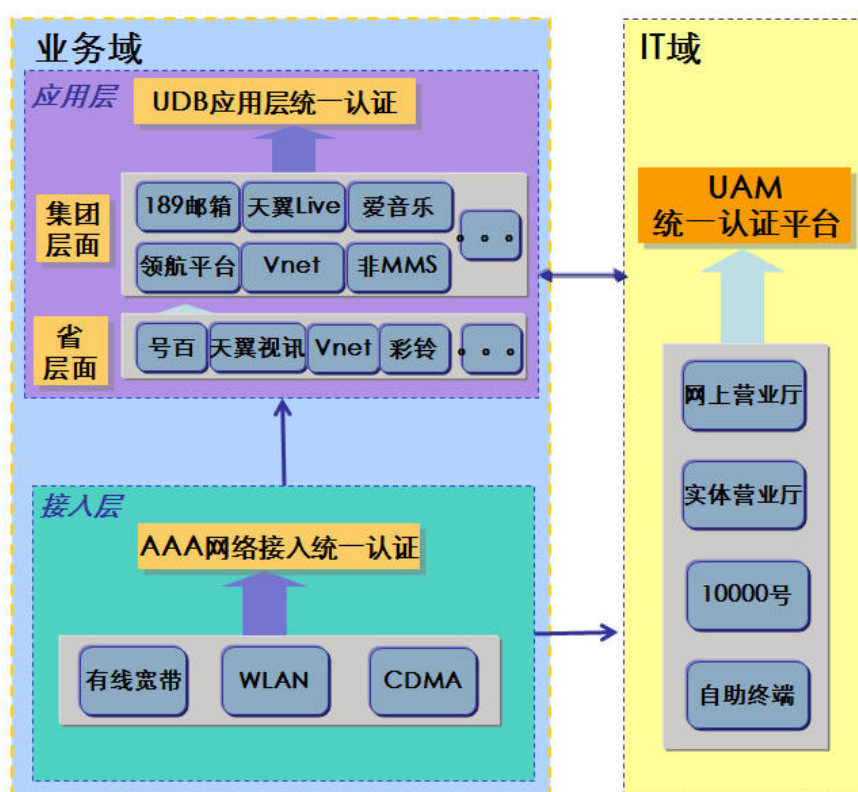
通用密码：通用密码是用户通过使用宽带接入、产品应用的统一密码，实现“一个帐号，一个密码”。通用密码可支持静态密码或短信密码。

业务密码：业务密码是统一帐号用户登录某项应用系统的专用（私有）密码。业务密码只针对该应用系统有效，必要时需要用户进行二次认证。

应用系统：为实现某个业务功能而搭建的业务平台和应用平台，等同于“业务平台”、“业务系统”、“业务能力”等描述。

6 中国电信认证体系架构

中国电信认证体系架构由应用层统一认证（UDB）、接入层认证（AAA）、IT 域认证（UAM）共同构成，如下图所示：



应用层统一认证（UDB）按集团、省两级架构建设，分别负责集团和省层面的应用系统的集中认证。全国UDB主要负责全国性应用系统的统一认证服务，并作为各省漫游认证请求的路由枢纽；省UDB主要负责基于统一账号的省内应用系统和固网/无线宽带接入系统的认证服务。

IT域统一认证（UAM）按照集团、省两级架构建设，分别负责集团和省层面IT系统集中认证。IT域认证通过UAM独立实现，UDB承接网上营业厅的单点登录通道建设。接入域统一认证（AAA）原则上以省为单位集中建设，负责宽带接入鉴权和计费功能。

用户数据库完成应用层和接入层的用户认证（Authentication）功能，业务的鉴权（Authorization）、计费（Accounting）由应用系统实现。对于订购关系、SP管理等功能应由SMP实现，不可以纳入UDB管理。

7 UDB 在网络中位置

UDB 作为中国电信应用层统一认证的基础网元，主要完成统一帐号、密码、状态等的集中维护和管理功能。UDB 在网络中的位置如下图：

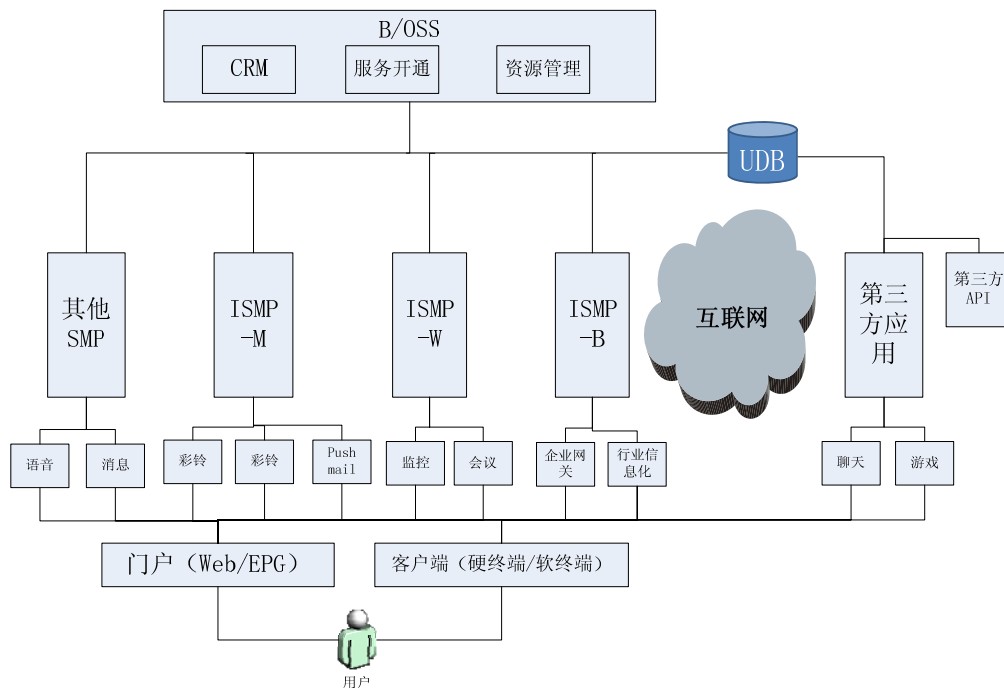


图 7-1. UDB 在网络中的位置

作为应用层统一认证的网元，UDB 与现网中的认证系统，采用“有则互通、无则共享”的原则（新建平台直接采用 UDB 的认证模块，旧有平台采用互通方式实现）：

- 用户使用原有帐号登录电信自营应用时，原认证体系保持不变；使用统一帐号进行登陆，全部转 UDB 进行认证。
- 用户使用原有宽带帐户进行网络接入时，宽带认证流程不变；使用统一帐号进行宽带接入登陆，转 UDB 进行用户认证。
- 新建的应用系统原则上不新建认证模块，全部转 UDB 进行统一认证。

8 UDB 功能描述

UDB 作为应用层用户数据库，以统一账号为核心，集中管理账号、密码、状态等信息，实现认证服务、协议适配、单点登录、用户自服务等功能。UDB 通过公共接口与相关应用系统相连，为相关的应用提供集中认证服务，用户可以方便的实现 189 邮箱、互联星空、天翼 Live、爱音乐、宽带接入、彩信等应用。

UDB 系统设计应遵循 SOA 的思想，即以功能相对独立的模块为服务，以服务可扩展为核心设计 UDB 的框架。其系统架构参考图 8-1 所示：

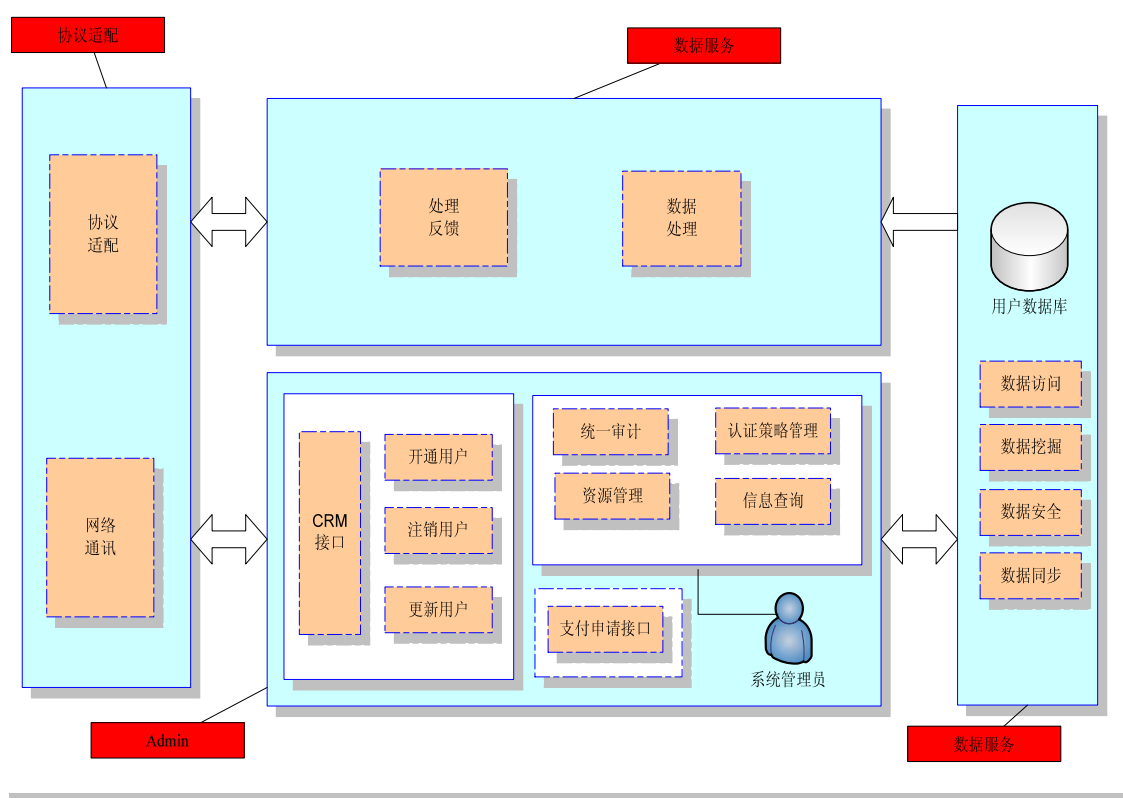


图 8-1 UDB 系统架构参考图

- 采用代理服务（AgentService）模块来封装所有协议适配功能，并兼顾未来协议的扩展。
- 采用认证服务（AuthServices）模块来封装各种具体服务，服务之间保持松耦合的原则，使未来扩展服务的影响最小化。

- 采用账户管理（AcctManager）模块来封装账户变更绑定等服务，同时提供账户信息增加修改查询外部接口，供外部模块使用。
- 采用 LDAP 数据库做为信息存储的载体，用前置代理服务来分担协议适配和服务指派的任务，同时缓存参数配置数据，充分保证信息查询的速度。

9 UDB 接口描述

9.1 UDB 接口描述

UDB 和周边系统接口表述见图 9-1：

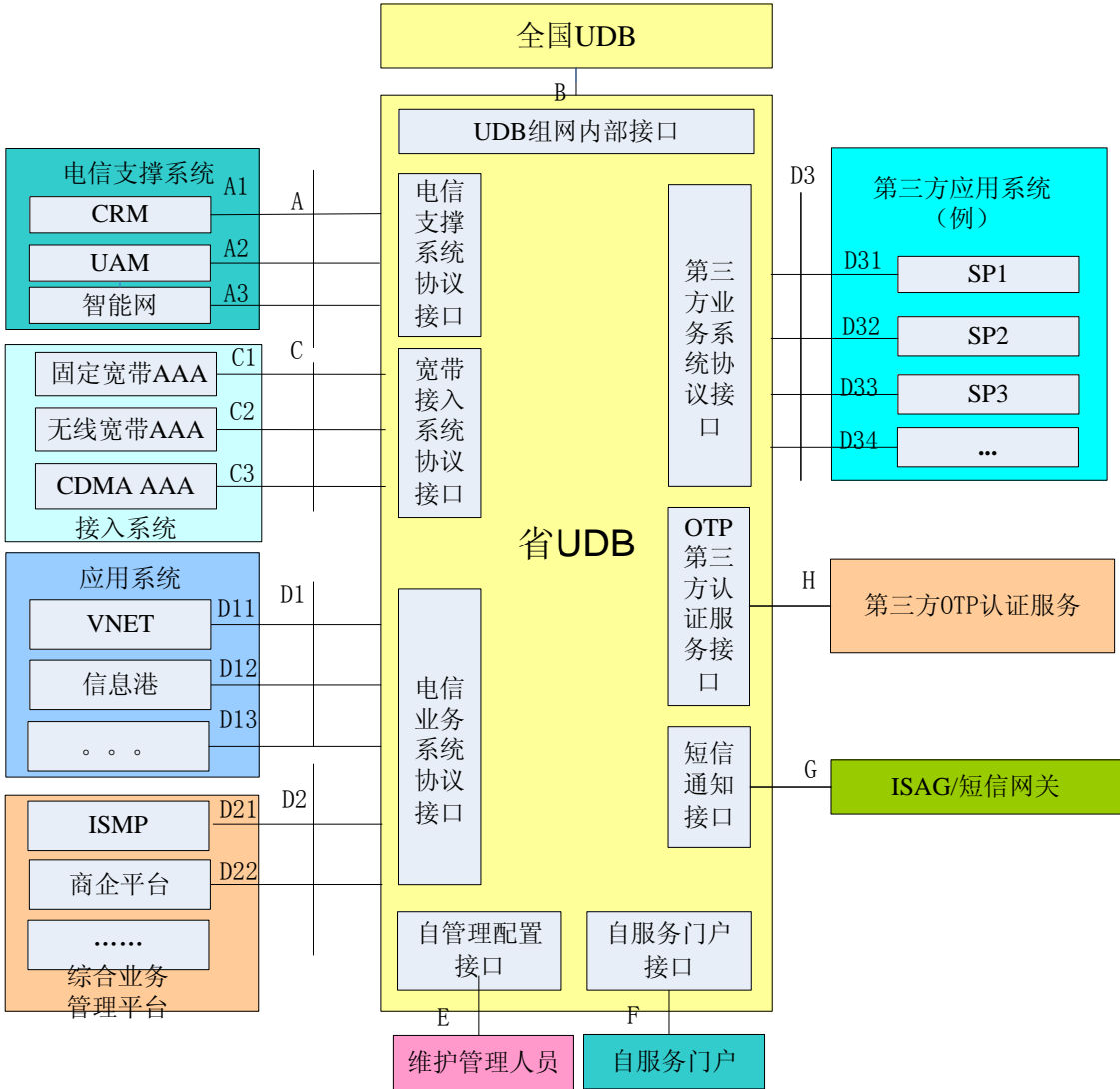


图 9-1. 中国电信用户数据库 UDB 结构

1. 参考点 A(省 UDB 与电信支撑系统 BOSS 之间的接口)：

- 1) A1：省 UDB 与归属地 CRM 之间的接口：涉及业务受理时的帐号开通，用户帐号信息更新的通知等。

- 2) A2: UDB 与 UAM 的接口：网厅到应用系统单点登录。
- 3) A3: UDB 与智能网的接口：预付费帐号欠费状态查询接口；
2. 参考点 B(省 UDB 与全国 UDB 中心之间的接口)：包括全国 UDB 到省 UDB 的帐号信息查询、相互维护的帐号信息更新等；全国 UDB 平台做漫游认证的转发等服务。
3. 参考点 C(UDB 与宽带接入系统 AAA Radius 服务器之间的接口)：
 - 1) C1: UDB 与固网 AAA 之间的接口；
 - 2) C2: UDB 与 WLAN AAA 之间的接口；
 - 3) C3: UDB 与 CDMA AAA 之间的接口；
4. 参考点 D(UDB 与应用系统之间的接口)：
 - 1) D1: UDB 与电信自营应用系统之间的接口，主要是帐号认证、用户业务注册和上线状态通知、业务密码设置、短信密码获取请求等消息交互。
 - D11: UDB 与 SP1 平台之间的认证接口：涉及 UDB 与省 VNET；
 - D12: UDB 与 SP2 之间的接口（彩铃门户如果割接到 ISMP，此接口取消）；
 - D13: UDB 与 SP3 应用系统之间的接口。
 - 2) D2: UDB 与综合业务管理系统平台之间的接口。
 - D21: UDB 与 ISMP 之间的接口，可以采取用户数据 push 给 ISMP 和认证请求 pull 给 UDB 两种模式；
 - D22: UDB 与其他业务管理平台系统的接口（如商企等）
 - 3) D3: UDB 与第三方 CP/SP 应用系统之间的接口，主要是帐号绑定及认证服务消息交互。
5. 参考点 E(UDB 自身管理配置的接口)：主要传递系统管理操作员的登录认证以及对 UDB 的配置、统计、管理维护操作信息交互。

6. **参考点 F**(UDB 与用户自服务门户之间的接口): UDB 与用户服务门户(单独提供统一帐号管理或者纳入网上营业厅)之间有关帐号信息查询、设置及更新的接口操作。
7. **参考点 G**(UDB 与短信网关/ISAG 之间的接口): 短信通知下发接口。
8. **参考点 H**(UDB 与第三方身份认证服务的接口): 对于涉及支付等高安全性的认证可以采取动态密码/一次性密码等认证方案, UDB 需要与第三方(如 verisign 等)的 OTP 认证服务等进行二次认证交互。

9.2 UDB 对于周边系统的要求

1. **接入平台:** 视省内情况, 若本省 WLAN AAA 与 DSL AAA 统建, 则需要划分出一套新 AAA 作为 189 账号登陆使用。若本省 WLAN AAA 与 DSL AAA 采用分离建设, 则对于 ADSL AAA 需要分别进行新 AAA 改造, WLAN AAA 的改造重点除 UIM 认证外 (C+W 工程实现), 主要实现不需要 UIM 硬件认证的场景下, 采用统一账号登陆无线宽带的场景。
2. **第三方应用系统:** 若本省接入第三方应用系统, 则认证功能只允许采用 (重定向/界面内嵌) 接口。详见接口规范 7.5.3 章节相关描述。对于第三方发起的账号绑定工作, 请明确**第三方作为绑定关系的维护单位**, UDB 负责提供统一账号的登陆信息检验, 并反馈给第三方检验结果。
3. **自营应用系统:** 自营应用系统的认证分为两类: 完全自营的通信类应用 (彩铃门户、智能短信平台 MSP 等) 和第三方承建的互联网应用系统。对于通信类应用系统, 可选择 ISAP 接口和 Web Service 接口; 对于第三方承建平台, 只可以采用 (重定向/界面内嵌) 接口。
4. **客户端及门户:** UDB 集成的客户端和门户 (E 家终端、ECP、WLAN PORTAL 等) 需要进行 IE 功能集成改造, 部分改造已在其他文件中进行要求。要求客户端和终端能够识别并建立 Token 令牌, 并能够识别 IE 同一进程的不同应用系统。

10 主要数据编码

10.1 用户类型编号

2 字节字符串（全国和省 UDB 通用，其他类型待扩展）

取值	描述	备注
09	MSISDN	手机号码
05	PHS	小灵通号码
04	固话	固定电话号码
02	宽带	宽带接入帐号

由于各省 CRM 对用户类型的编码不统一，为确保各省及全国 UDB 用户数据一致，各省与 CRM 对接时需要维护编码中间表进行转换。

10.2 通用密码格式编码

该字段由各省公司帐号经营的市场策略来制定，并由省 UDB 系统管理员配置后，通过省 UDB 向全国 UDB 进行同步：

编码值	描述	备注
1	6 位数字	通用密码，与客服密码保持一致性，只能是数字号码
2	16 位字符串	通用密码，可设置为字符格式，与客服密码分开，独立设置

10.3 用户状态编号

定义各省及全国 UDB 统一的帐号状态属性。

取值	描述	对应各省 CRM 的用户状态
01	预开户	预开户
02	正常状态	开户、复机、取消停机保号、解挂、在用
03	欠费单停	欠停(单向)

04	欠费双停	欠停(双向)
05	停机保号	用户报停
06	其他停机	挂失、违章停机、加锁停机等
07	拆机状态	拆机、预拆机、违章拆机、欠费拆机
08	暂停服务	障碍、施工未完、资源封锁等

各省分公司 CRM 用户状态要与全国统一状态建立中间表转换表: 以下是某省公司 CRM 的实际状态属性标识, 需要归并同类状态属性。

编码	描述
01	在用
02	用户报停
03	用户拆机
04	预先
05	欠停(双向)
06	欠停(单向)
07	违章停机
08	挂失
09	欠费拆机
10	违章拆机
11	施工未完
12	障碍
13	预拆机
14	资源封锁
15	加锁停机
16	预开户待激活

10.4 省别编号及简写

省别 ID	省份名称	省别简写	省别 ID	省份名称	省别简写
01	北京	bj	19	湖南	hn
02	上海	sh	20	广东	gd
03	天津	tj	21	广西	gx
04	重庆	cq	22	海南	hi
05	河北	he	23	四川	sc
06	山西	sx	24	贵州	gz

07	内蒙古	nm	25	云南	yn
08	辽宁	ln	26	西藏	xz
09	吉林	jl	27	陕西	sx
10	黑龙江	hlj	28	甘肃	gs
11	江苏	js	29	青海	qh
12	浙江	zj	30	宁夏	nx
13	安徽	ah	31	新疆	xj
14	福建	fj	32	台湾	tw
15	江西	jx	33	香港	hk
16	山东	sd	34	澳门	ma
17	河南	ha	35	全国中心	zx
18	湖北	hb	36	海外	os

10.5 应用系统类型编号

应用系统类型	归属域	编号
UDB	UDB	0000
UDB Portal（自服务）		0001
CRM	IT 支撑系统	1000
网上营业厅		1001
服务开通系统		1002
OCS		1003
智能网		1004
UAM		1005
...		1006-1099
ISMP（ISMP-M）	业务管理系统	2000
VNET（ISMP-W）		2001
商企平台（ISMP-B）		2002
...		2003-2099
WLAN AAA	接入系统	3000
固网 AAA		3001
CDMA AAA		3002
...		3003-3099
保留	应用系统/系统	4000
189 邮箱		4001
天翼 Live 客户端		4002
爱音乐		4003
非 MMS 系统		4004

...		4005-4050
IPTV		4051
全球眼		4052
信息港		4053
超级信使		4054
.....		4055-4099
ISAG	业务网元	5000
SMS GW		5001
SMSC		5002
MMSC		5003
.....		5004

11 主要应用场景

用户登录认证场景：后台（Web Services）、重定向两个方式

宽带接入场景：WLAN 和 AD

单点登录：四类场景

自服务

第三方合作

11.1 帐号申请示例流程

在 UDB 中需要维护 189 账户和其他应用系统账户的关联关系,以 189 帐号作为主 ID 帐号,其他应用系统帐号和这个主 ID 进行关联。对于新开通 189 帐号的用户,可能还没有或者部分拥有其他服务帐号开通,可以在开通 189 业务的时候,一起开通其他应用系统帐号,所以在新开 189 账户的时候可以能与如下两种情况:

➤ 用户已经有其他应用系统帐号

在开通 189 帐号的时候,用户提供其他应用系统的帐号和密码。为了防止虚假信息,在绑定应用系统的帐号的时候,需要将用户提供的应用系统的帐号和密码交给各个应用系统进行验证,只有验证通过了才可以实施绑定。

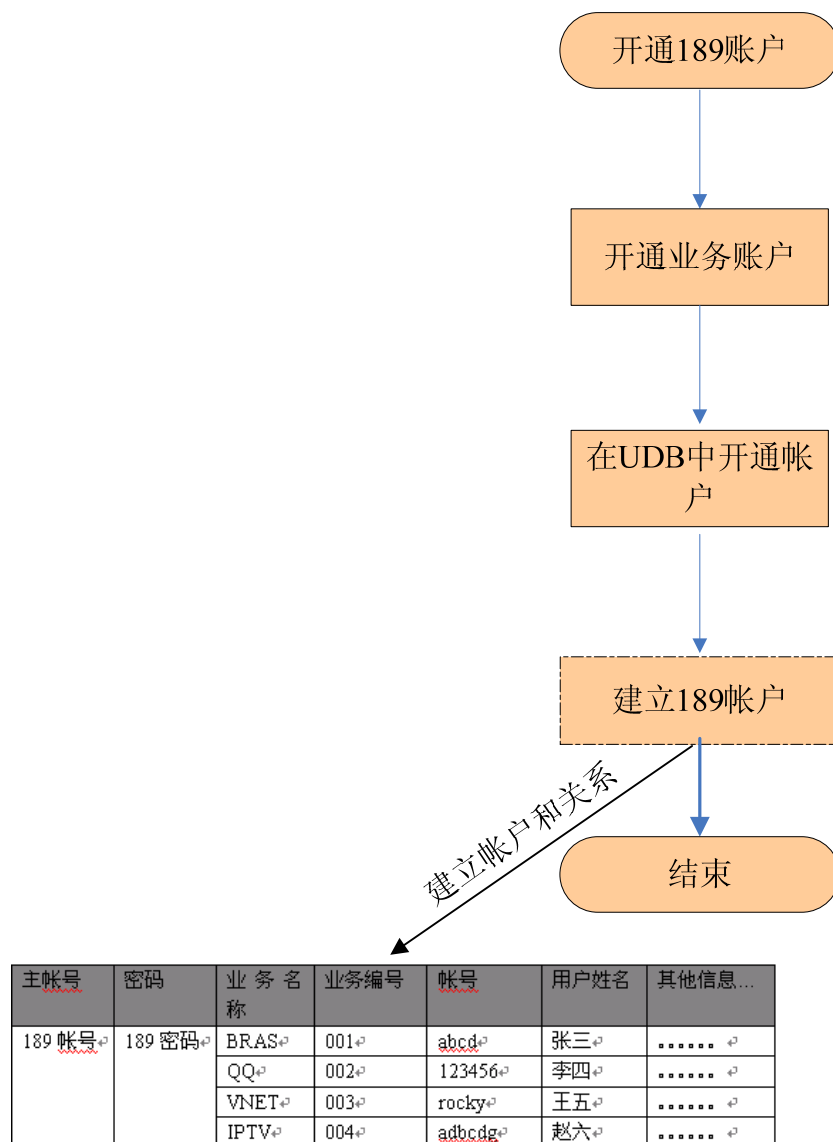
一旦创建成功后,UDB 系统将 189 帐号和其他应用系统的帐号的关系保存到数据库中,形成了如下的映射关系:

表 11-1.账户对应表示例

主帐号	密码	业务名称	业务编号	帐号	其他信息...
189 帐号	189 密码	AAA	001	abcd	XXX
		QQ	002	123456	XXX
		ISMP	003	rocky	XXX
		IPTV	004	adbcdg	XXX

➤ 用户没有或者是拥有部分其他用户应用系统帐号

如果开通 189 账户的时候，用户没有开通其他应用系统账户，可以在开通 189 账户的同时选择为用户开通其他应用系统帐号。最终也会形成如上表一样的映射关系。综合来看，整体流程如下：



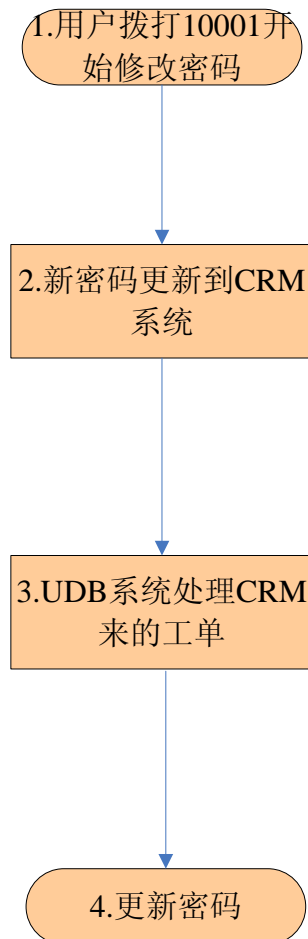
申请过程说明如下：

- 1) 用户使用在开通 189 帐户
- 2) 用户选择是否创建新的关联的应用系统帐户
- 3) UDB 创建 189 帐户，并且创建应用系统关联关联帐户

11.2 统一密码修改示例流程

用户可以修改 189 帐户的密码。

修改密码流程如下所示：



登录过程说明如下：

- 1) 用户拨打 10001 号码修改密码
- 2) 新密码更新到 CRM 系统中，并且触发工单
- 3) UDB 系统接收 CRM 来的工单，进行密码的修改
- 4) 完成密码修改

11.3 帐号升级示例流程

189 账户是可以作为通讯号码和服务号码的。UDB 需要维护 189 的这种状

态。当一个 189 用户从服务号码升级成通讯号码的时候，UDB 需要更新此状态信息。维护此状态的好处是：通过该识别，UDB 可以判断是否可以将信息发送到用户的手机上。帐号升级的过程很简单，只是将更新 189 用户在 UDB 数据库中的一个状态字段即可。

在一下描述的几个场景都是设计到用户服务的，所以我们在描述这几个场景之前做一个说明：

➤ 服务限制

为了保证帐号和密码的安全性，我们在服务方法上做了一个约定：

外网服务的必须通过 OTP(one time password)进行服务，如果是内网服务可以通过 OTP,用户的固定密码，手机短消息发送动态密码的方式进行服务。

➤ 服务接口

外部系统来 UDB 来服务需要遵循 UDB 的服务协议，提供必要的信息，如下表示：

基础账户	账户级别	网络类别	平台名称	内部密码	OTP 密码	短信密码
189/133/153/PHS	服务账户 / 通信账户	外网/内网	BRAS/QQ/盛大	用户记忆	密令卡密码	一次性短信密码

具体的接口方面的细节将在服务接口部分描述。

11.4 用户登录认证场景

11.4.1 后台认证

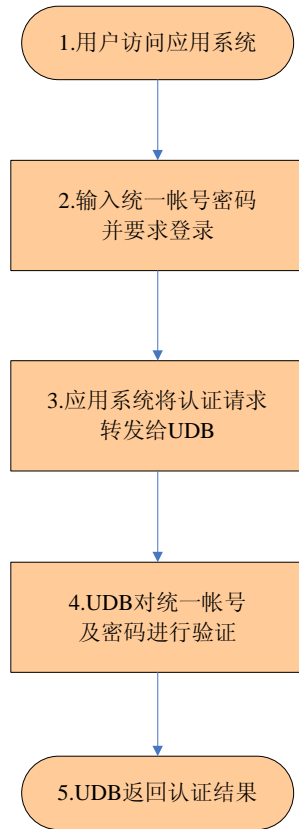
用户访问应用系统，在应用系统登录页面输入统一帐号及密码，并且要求登录。应用系统将用户的登录请求通过后台认证接口发送给 UDB。UDB 对统一帐号及密码进行验证。

若认证通过，UDB 将认证成功的结果以及统一帐号相关信息返回给应用系统，应用系统接受用户的登录请求。

若认证未通过，UDB 将认证失败的结果返回给应用系统，应用系统拒绝用

户的登录请求。

该场景流程如下图所示：



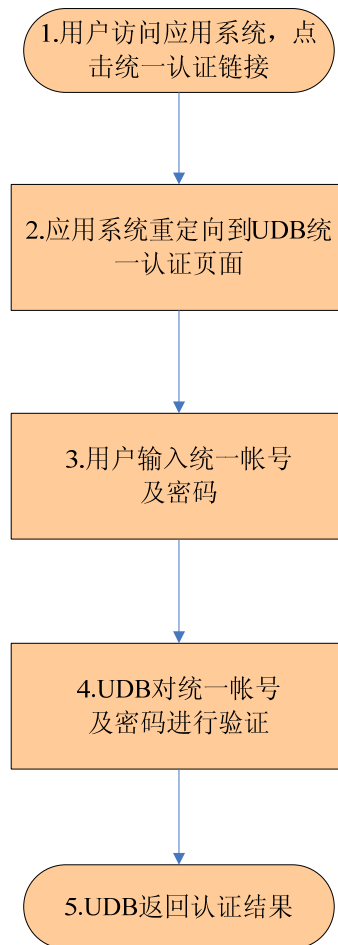
11.4.2 重定向认证

用户访问应用系统，并在应用系统门户页面上点击中国电信统一帐号登录的链接。应用系统重定向到中国电信统一认证的登录页面。用户在该统一认证页面上输入统一帐号和密码。UDB 对输入的统一帐号和密码进行验证。

若认证通过，UDB 将认证成功的结果以及统一帐号相关信息通过重定向的方式返回给应用系统，应用系统接受用户的登录请求。

若认证未通过，UDB 将认证失败的结果通过重定向的方式返回给应用系统，应用系统拒绝用户的登录请求。

该场景流程如下图所示：



11.5 宽带接入场景

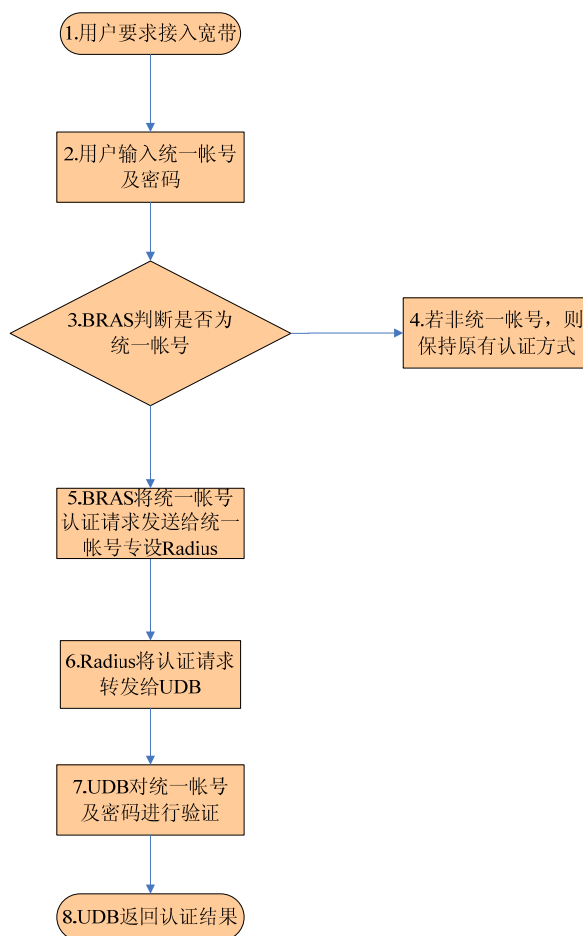
用户通过中国电信专用客户端软件（如天翼Live PC版）或第三方拨号软件，输入统一帐号及密码，进行固网宽带拨号。或者用户通过中国电信WLAN Portal页面，输入统一帐号及密码，进行无线宽带登录。

BRAS将相应的统一帐号认证请求发送给为统一帐号认证专设的Radius服务器。该Radius服务器再将认证请求转发给UDB。UDB对统一帐号及密码进行验证。

若认证通过，UDB把收到的认证请求返回给Radius服务器。Radius服务器判断最大连接数和绑定信息，通过后再将认证结果返回给BRAS。BRAS通知用户登陆成功，用户宽带接入成功；

若认证失败，UDB直接返回拒绝接入的认证结果，用户宽带接入失败。

该场景流程如下图所示：



11.6 单点登录场景

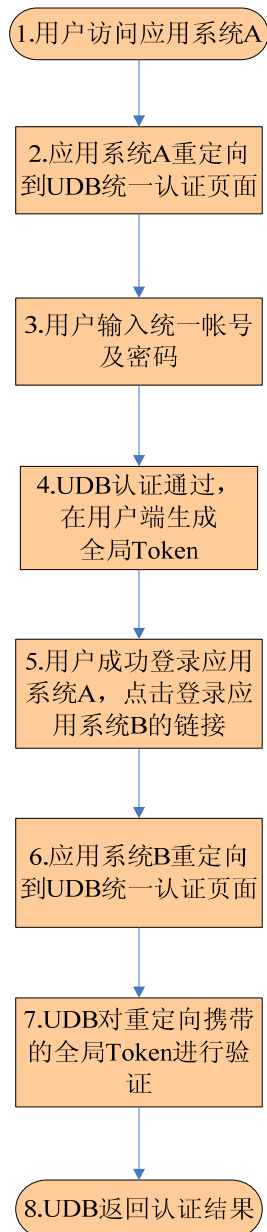
11.6.1 省内应用系统之间的单点登录

用户访问省内应用系统 A，并在应用系统 A 门户页面上点击中国电信统一帐号登录的链接。应用系统 A 重定向到中国电信统一认证的登录页面。用户在该统一认证页面上输入统一帐号和密码。UDB 对输入的统一帐号和密码进行验证。若认证通过，UDB 在用户端生成全局 Token。UDB 将认证成功的结果以及统一帐号相关信息通过重定向的方式返回给应用系统 A，应用系统 A 接受用户的登录请求。

用户成功登录省内应用系统 A 后，点击登录省内应用系统 B 的链接。应用系统 B 携带用户全局 Token 信息重定向到中国电信统一认证的登录页面，UDB 对全局 Token 进行验证。若验证通过，UDB 直接向应用系统 B 返回用户帐号信

息。应用系统 B 接收用户的登录请求。

该场景流程如下图所示：



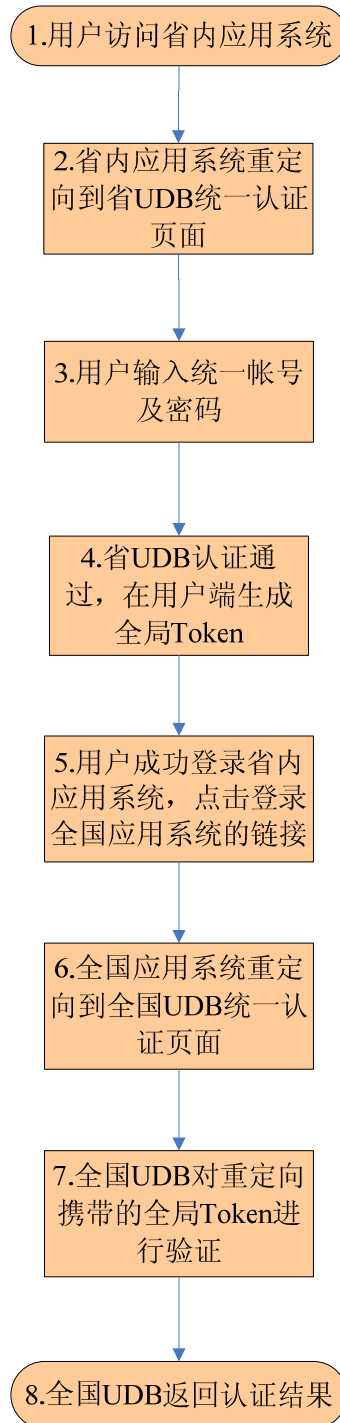
11.6.2 省内应用系统与全国应用系统之间的单点登录

用户访问省内应用系统，并在省内应用系统门户页面上点击中国电信统一帐号登录的链接。省内应用系统重定向到中国电信统一认证的登录页面。用户在该统一认证页面上输入统一帐号和密码。省 UDB 对输入的统一帐号和密码进行验证。若认证通过，省 UDB 在用户端生成全局 Token。省 UDB 将认证成功的结果以及统一帐号相关信息通过重定向的方式返回给省内应用系统，省内应

用系统接受用户的登录请求。

用户成功登录省内应用系统后，点击登录全国应用系统的链接。全国应用系统携带用户全局 Token 信息重定向到中国电信统一认证的登录页面。由于省 UDB 与全国 UDB 属于同一个域，所以全国 UDB 能够对由省 UDB 生成的全局 Token 进行验证。若验证通过，全国 UDB 直接向全国应用系统返回用户帐号信息。全国应用系统接收用户的登录请求。

该场景流程如下图所示：



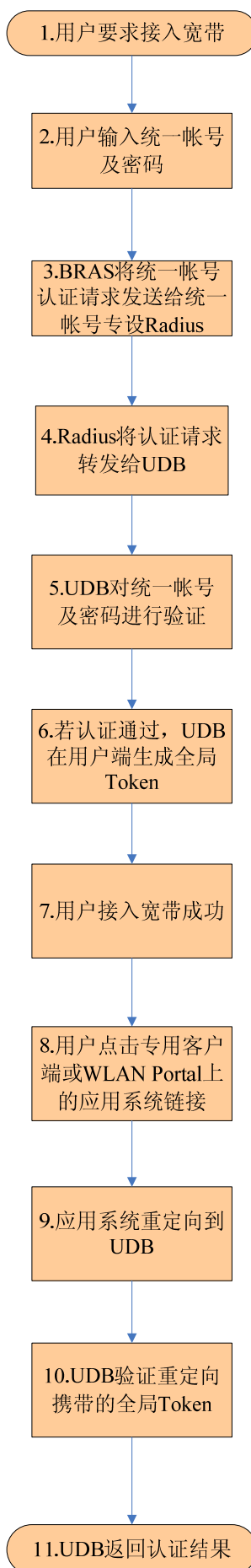
11.6.3 宽带接入系统与应用系统之间的单点登录

用户通过中国电信专用客户端软件（如天翼 Live PC 版），输入统一帐号及密码，进行固网宽带拨号。或者用户通过中国电信 WLAN Portal 页面，输入统一帐号及密码，进行无线宽带登录。

宽带接入认证流程请参照 11.2 中的描述。

当用户接入宽带成功后，**UDB** 会在用户端生成全局 **Token**。当用户在专用客户端或 **WLAN Portal** 页面上点击登录应用系统的链接。应用系统携带用户全局 **Token** 信息重定向到中国电信统一认证的登录页面，**UDB** 对全局 **Token** 进行验证。若验证通过，**UDB** 直接向应用系统返回用户帐号信息。应用系统接收用户的登录请求。

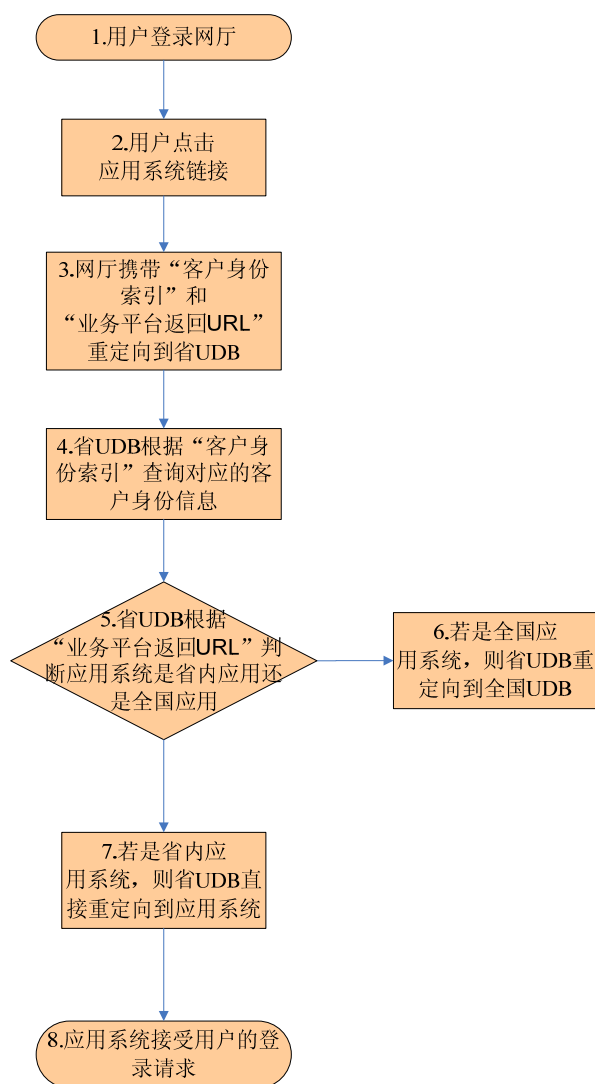
该场景流程如下图所示：



11.6.4 网上营业厅与应用系统之间的单点登录

用户成功登录网上营业厅后，点击登录应用系统的链接。网厅内部系统携带“客户身份索引”和“业务平台返回 URL”重定向到省 UDB。省 UDB 根据“客户身份索引”查询对应的客户身份信息。省 UDB 根据“业务平台返回 URL”判断应用系统是省内应用还是全国应用。若是省内应用系统，省 UDB 直接重定向到应用系统，应用系统接受用户的登录请求；若是全国应用系统，省 UDB 先重定向到全国 UDB，再由全国 UDB 重定向到应用系统，应用系统接受用户的登录请求。

该场景流程如下图所示：



11.7 自服务门户应用场景

用户访问自服务门户，在登录页面输入统一帐号及密码，并要求登录。自服务门户将用户的登录请求发送给 UDB。UDB 对统一帐号及密码进行验证。

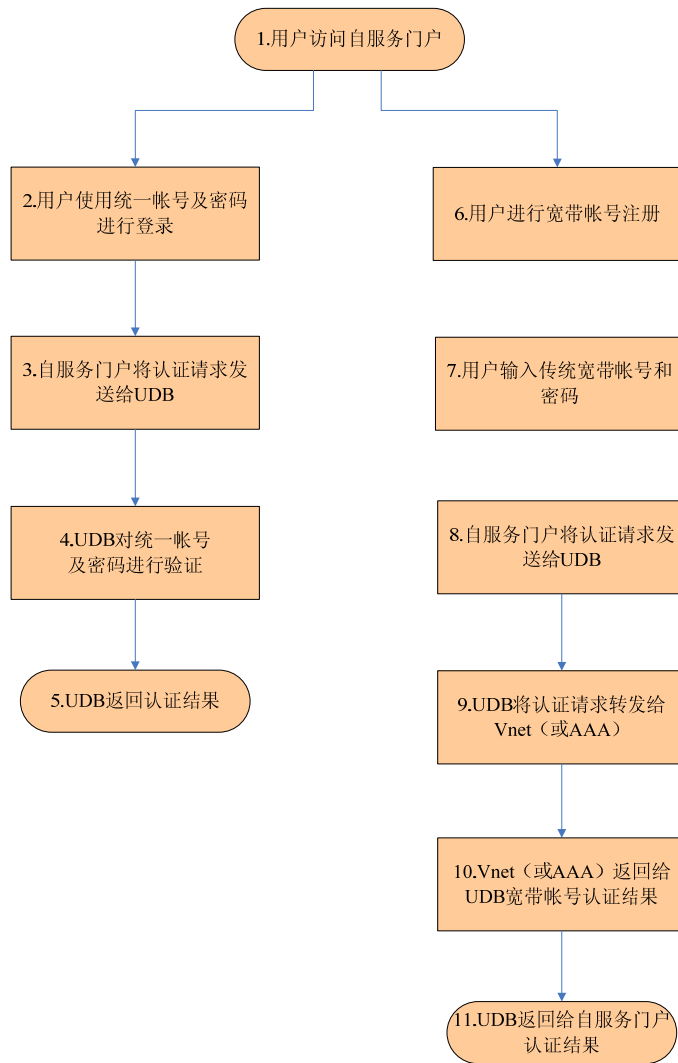
若认证通过，UDB 将认证成功的结果返回给自服务门户。自服务门户向 UDB 请求获取用户统一帐号对应的信息后，自服务门户接收用户的登录请求，并在页面上显示统一帐号的相关信息。

若认证未通过，UDB 将认证失败的结果返回给应用系统，应用系统拒绝用户的登录请求。

用户使用统一帐号成功登录自服务门户之后，能够通过自服务门户来修改别名、通用密码、密码策略等信息。

用户还能通过自服务门户进行传统宽带用户的注册。用户在未登录自服务门户时，选择宽带用户注册，在注册页面上输入传统宽带帐号及密码进行认证，自服务门户将认证请求发送给 UDB，UDB 再向 Vnet（或 AAA 服务器）转发认证请求。Vnet（或 AAA 服务器）对传统宽带帐号及密码进行验证。若验证通过，UDB 向自服务门户返回用户传统宽带帐号对应的统一帐号，并且自服务门户会提示用户设置统一帐号对应的密码。整个注册流程结束后，用户便可以通过统一帐号及密码来进行宽带接入。

该场景流程如下图所示：



11.8 第三方应用系统合作场景

用户访问电信自营应用系统，输入统一帐号及密码进行登录。电信自营应用系统将认证请求发送给 UDB。UDB 对统一帐号和密码进行验证。若认证通过，UDB 将认证成功的结果和统一帐号相应信息返回给电信自营应用系统。电信自营应用系统接受用户的登录请求。

用户成功登录电信自营应用系统后，点击登录第三方合作应用系统的链接。电信自营应用系统携带第三方合作应用系统地址等信息重定向到 UDB，UDB 判断该重定向信息来自于电信自营应用系统，则携带用户统一帐号信息直接重定向到第三方合作应用系统。第三方合作应用系统接受用户的登录请求。

该场景流程如下图所示：

