



---

---

# **中国电信用户数据库—接口与流程规范**

## **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集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。

本规范规定了中国电信 **UDB** 的接口与流程：包括 **UDB** 与 **IT** 支撑系统、宽带接入认证系统、电信自营应用系统、第三方合作应用系统、综合业务管理平台、自服务门户，以及全国 **UDB** 和省 **UDB** 之间通信接口。

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：熊小明 杨鑫 何潇 潘卫 黄鹏 蓝青 李根军 韩苏川 解冲锋 瞿晓波

## 目 录

1	适用范围 .....	7
2	引用标准 .....	8
3	缩略语 .....	9
4	术语定义 .....	10
5	UDB 组网及接口概述.....	11
5.1	UDB 组网方案.....	11
5.2	省 UDB 接口概述.....	12
5.3	全国 UDB 接口概述.....	14
5.4	UDB 接口安全策略.....	15
6	UDB 公共接口.....	16
6.1	公共接口概述 .....	16
6.2	重定向接口 .....	16
6.2.1	接口概述.....	16
6.2.2	重定向认证请求接口.....	17
6.2.3	重定向单点登录接口.....	19
6.3	WEB SERVICES 接口 .....	20
6.3.1	接口概述.....	20
6.3.2	业务认证请求接口.....	22
6.3.3	短信密码获取请求.....	25
6.3.4	业务密码设置接口.....	28
6.3.5	帐号信息查询接口.....	29
6.3.6	帐号信息更新接口.....	32
6.3.7	外部帐号绑定接口.....	35
6.3.8	业务注册状态通知.....	37
6.3.9	业务在线状态通知.....	38
6.3.10	帐号验证及短信申请.....	39
6.3.11	安全密钥通知接口.....	40
6.3.12	用户身份信息查询接口.....	41
6.4	ISAP 接口 .....	44
6.4.1	接口概述.....	44
6.4.2	编码定义.....	45
6.4.3	基本数据类型.....	46
6.4.4	PDU 概述.....	47
6.4.5	PDU 定义.....	48
7	省 UDB 接口.....	68
7.1	电信支撑系统接口 .....	68
7.1.1	接口概述.....	68
7.1.2	接口流程.....	68

7.1.3	接口内容.....	70
7.1.4	对支撑系统的要求.....	74
7.2	宽带接入系统接口 .....	74
7.2.1	宽带接入的 UDB 集成方案.....	74
7.2.2	接口流程.....	79
7.2.3	接口内容.....	84
7.3	电信自营应用系统接口 .....	88
7.3.1	接口概述.....	88
7.3.2	接口流程.....	88
7.3.3	接口内容.....	96
7.3.4	对应用系统的相关建议.....	96
7.4	综合业务管理平台接口 .....	97
7.4.1	ISMP- M 的接口.....	97
7.4.2	ISMP- B 的接口.....	100
7.5	第三方合作应用系统接口 .....	101
7.5.1	接口方案建议.....	101
7.5.2	帐号关联的建立.....	103
7.5.3	重定向认证接口.....	104
7.5.4	单点登录互信接口.....	105
7.5.5	独立密码认证接口.....	107
8	全国 UDB 的接口.....	109
8.1	电信自营应用系统接口 .....	109
8.1.1	全国 UDB 提供给 189 邮箱接口.....	109
8.1.2	189 邮箱提供给全国 UDB 接口.....	110
8.1.3	全国 UDB 提供给天翼 Live 客户端接口.....	114
8.2	第三方合作应用系统接口 .....	120
9	省 UDB 与全国 UDB 接口 .....	121
9.1	接口概述 .....	121
9.2	接口流程 .....	121
9.2.1	帐号查询流程.....	121
9.2.2	别名设置流程.....	125
9.2.3	通用密码设置.....	127
9.2.4	其他信息更新.....	129
9.2.5	设置/取消活跃标记.....	130
9.2.6	漫游认证转发流程.....	131
9.2.7	安全密钥管理流程.....	133
9.2.8	通用密码格式通知.....	133
9.2.9	个人通讯录信息.....	134
9.3	接口内容 .....	134
9.3.1	设置/取消全国活跃标记.....	135
9.3.2	通用密码格式更新接口.....	136
10	单点登录功能接口 .....	137

10.1	接口概述 .....	137
10.2	接口流程 .....	137
10.2.1	全国性平台（或省级平台）内部的 SSO .....	137
10.2.2	全国性—省级平台之间的 SSO .....	139
10.2.3	宽带接入—应用系统的 SSO .....	141
10.2.4	网上营业厅—应用系统的 SSO .....	145
10.3	接口消息 .....	147
10.3.1	UDBToken 格式及读取 .....	147
10.3.2	UDB 提供的客户端单点认证接口 .....	149
10.3.3	UDB 提供的 UAM 单点登录接口 .....	151
11	自服务门户接口 .....	153
11.1	自服务概述 .....	153
11.2	接口流程 .....	153
11.2.1	自服务门户登录 .....	153
11.2.2	用户帐号别名设置 .....	154
11.2.3	通用密码修改设置 .....	155
11.2.4	业务(私有)密码设置 .....	156
11.2.5	传统宽带用户注册 .....	157
11.3	接口内容 .....	159
11.3.1	宽带帐号的验证请求 .....	159
12	OTP 认证服务接口 .....	161
12.1	接口概述 .....	161
12.2	接口流程 .....	161
12.2.1	OTP 令牌激活流程 .....	161
12.2.2	OTP 认证请求流程 .....	162
12.3	接口内容 .....	163
12.3.1	OTP 令牌激活/取消 .....	163
12.3.2	OTP 认证请求接口 .....	164
13	其他接口类型 .....	165
13.1	短信网关接口 .....	165
13.2	互联星空的宽带认证接口 .....	165
13.3	UAM 的客户信息查询接口 .....	166
13.4	电信自营应用的 SSO 接口 .....	168
13.5	第三方应用的 SSO 接口 .....	169
14	UDB 数据编码规范 .....	171
14.1	用户类型编号（USERIDTYPE） .....	171
14.2	用户状态编号（USERIDSTATUS） .....	171
14.3	通用密码格式编码 .....	172
14.4	用户唯一标识（PUSERID） .....	172
14.5	用户证件类型（CERTIFICATE TYPE） .....	173
14.6	省别编号（PROVINCE NO）及简写 .....	174

14.7	地市编号 (CITYNo) 及区号 (AREACODE) .....	174
14.8	应用系统类型编号 (SSTYPE) .....	179
14.9	应用系统设备标识 (DEVICENO) .....	180
14.10	业务套餐类型编号 (SERSETTYPE) .....	180
14.11	用户身份索引 (UDBTICKET) .....	181
14.12	接口返回码 (RESULTCODE) .....	181
<b>15</b>	<b>附录 .....</b>	<b>183</b>
15.1	统一认证 WEB 页面参考 .....	183
15.1.1	重定向登录 .....	183
15.1.2	自服务界面 .....	184
15.1.3	设置用户别名 .....	184
15.1.4	修改密码界面 .....	185
15.2	WEB SERVICES 接口概述文件 .....	185
15.2.1	UDB 公共接口 (UDBCommon.wsdl) .....	185
15.2.2	UDB 与 CRM 接口 (CRMInterface.wsdl) .....	185
15.2.3	UDB 与应用系统接口 (SSInterface.wsdl) .....	185
15.2.4	UDB 与 ISMP 接口 (ISMPInterface.wsdl) .....	185
15.2.5	UDB 与自服务接口 (PortalInterface.wsdl) .....	185

# 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 术语定义

**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。

## 5 UDB 组网及接口概述

### 5.1 UDB 组网方案

UDB 采用全国一省二级架构进行部署。全国 UDB 主要负责全国性应用系统（如 189 邮箱、彩铃全国中心等）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 主要负责省内应用系统和固网/无线宽带接入系统的统一认证服务。

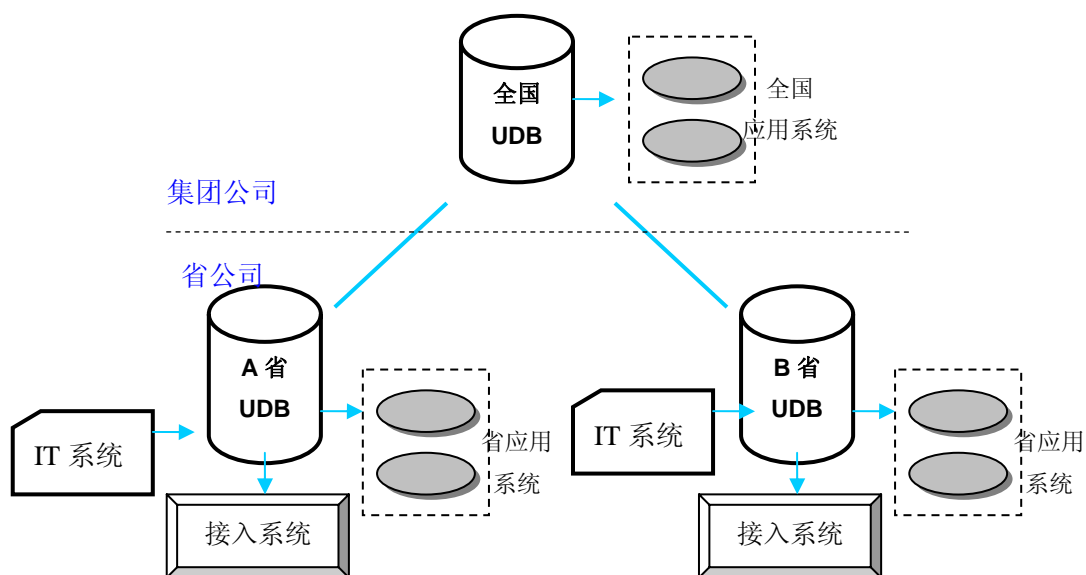


图 5.1-1 全国和省 UDB 的二级组网架构

全国和省 UDB 系统通过 CN2 网络进行承载，两点之间配置双链路备份机制。省 UDB 系统和周边系统之间可采用 CN2、DCN、Internet 等不同承载网络进行互通：

- 1、CN2 和 DCN 网络：主要承载 UDB 与中国电信自营应用系统、支撑系统、宽带认证系统之间的接口，如 CRM、UAM、ISMP、AAA，互联星空等；
- 2、Internet 网络：主要承载 UDB 与中国电信自营或第三方 Web 应用系统。

## 5.2 省 UDB 接口概述

省 UDB 和周边系统接口总体框架如图 5.2-1 所示：

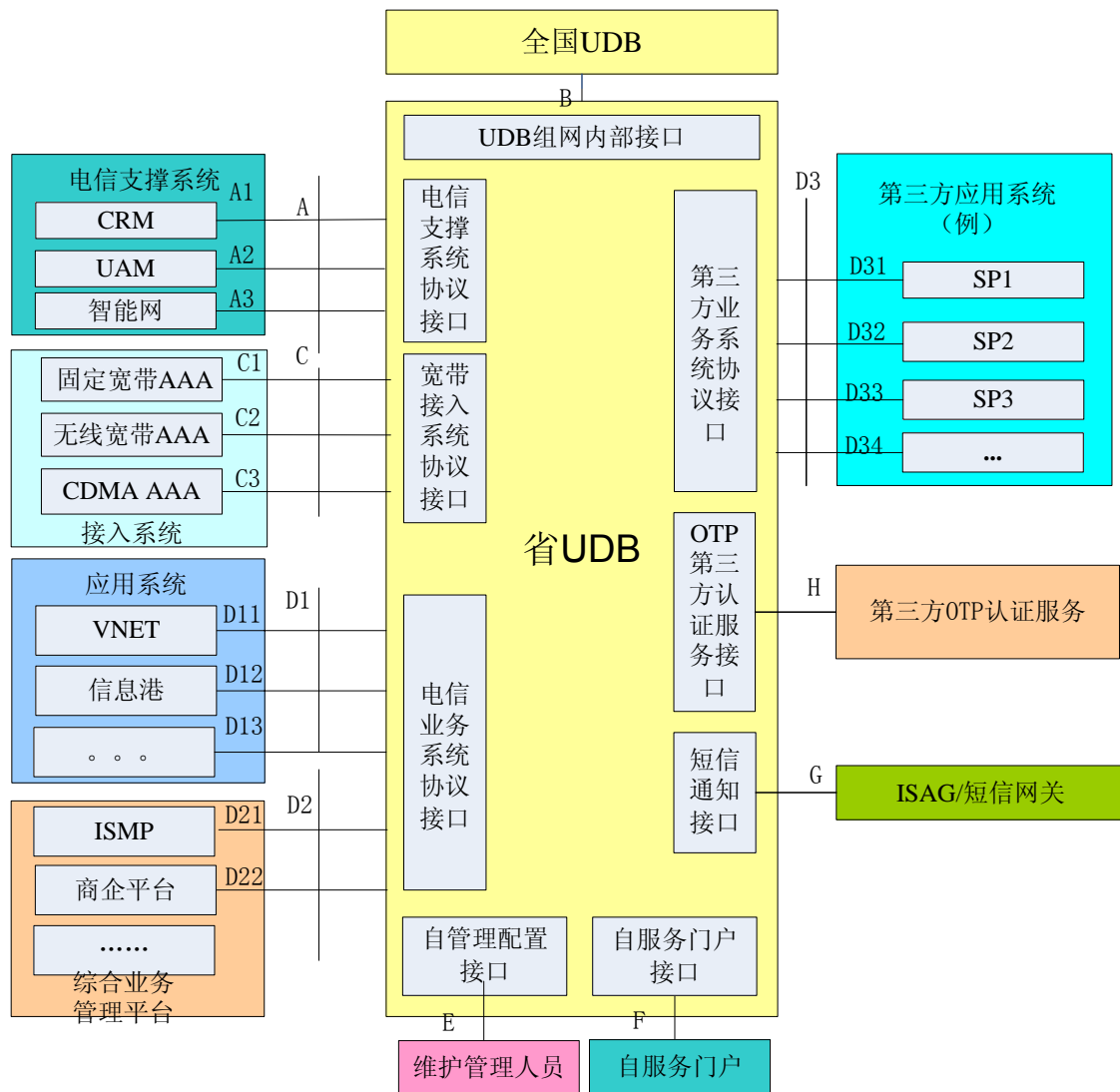


图 5.2-1：.省 UDB 接口参考模型

1. 参考点 A(省 UDB 与电信支撑系统 BOSS 之间的接口):
  - 1) A1: UDB 与 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：客户信息查询及单点登录接口。
  - 3) A3: UDB 与智能网的接口（预留）：预付费帐号欠费状态查询接口。
2. 参考点 B(省 UDB 与全国 UDB 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 与宽带接入认证系统 AAA 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，主要是用户认证、用户注册和上线状态通知、短信密码获取请求等消息交互。
  - D11: UDB 与 VNET 省平台之间的认证接口；
  - D12: UDB 与信息港等业务平台之间的接口；
  - D13: UDB 与省内其他应用系统（如超级信使等）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，可采取重定向认证请求或 SOAP 对接等模式；
  - D22: UDB 与商企平台系统的接口；
  - D23: UDB 与其他业务管理平台系统的接口（如 ISMP-M 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/关联及认证重定向服务交互。

5. 参考点 E(省 UDB 管理配置的接口): 主要传递系统管理员的登录认证以及对 UDB 的配置、统计、管理维护操作的信息交互。

6. 参考点 F(省 UDB 与自服务门户之间的接口): UDB 与自服务门户之间有关帐号信息查询、用户信息维护管理等接口操作。

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与第三方合作的动态密码或一次性密码认证方案。

## 5.3 全国 UDB 接口概述

全国 UDB 主要负责全国性应用系统的认证服务，并从省 UDB 获取用户基本帐号信息，承接全国漫游认证的转发服务。

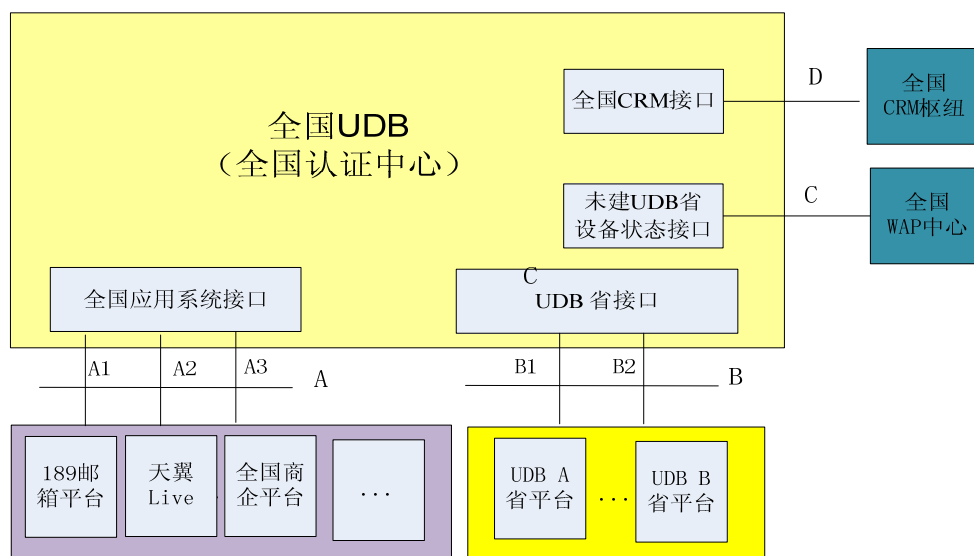


图 5.3-1: 全国 UDB 接口参考模型

- 参考点 A** 全国 UDB 与全国应用系统接口，典型应用系统如下：
  - 1) A1: 189 邮箱平台;
  - 2) A2: 天翼 Live 平台;
  - 3) A3: 全国商企平台;
- 参考点 B** 全国 UDB 与省 UDB 平台的接口，连接各省 UDB，进行用户帐号查询及信息更新、全国认证漫游枢纽等工作。
- 参考点 C** 未建设部署省 UDB 的省份，其设备开停机操作通过全国 WAP 中心进行部分数据同步。
- 参考点 D** 全国 CRM 枢纽接口：全国 UDB 与全国 CRM 枢纽/中心的接口，UDB 获取全国性用户的帐号数据同步。

## 5.4 UDB 接口安全策略

为确保 UDB 设备的网络接口安全,实施和部署时应从传输层和应用层进行以下保护措施,保障应用层统一认证平台的全网可靠性和安全性:

1. 网络传输层,可使用如下的一种或者多种方法的组合:
  - (1) 第三方 SP 应用系统可通过专线连接与电信 UDB 连接;
  - (2) UDB 位于受防火墙保护的 DMZ 区域,在防火墙本身设置策略,允许指定的应用系统服务器的 IP 和端口与 UDB 连接。
2. 应用层方面,可以使用如下的一种或者多种方法的组合:
  - (1) UDB 系统和第三方外围系统的数据交互可采用 SSL 协议进行;
  - (2) 第三方 SP 应用系统连接 UDB 的时候可采用双向数字证书服务。

## 6 UDB 公共接口

### 6.1 公共接口概述

公共接口是指 UDB 设备与周边系统之间进行网络对接的通用接口。任何周边系统可根据对接功能要求选择以下公共接口与 UDB 进行通信。

UDB 提供统一的业务认证请求接口、业务密码设置接口、业务注册状态通知、业务在线状态通知、短信密码获取接口，以及用户帐号信息查询、帐号信息更新等通用接口。针对各应用系统存在的不同协议适配，允许各应用系统与 UDB 协商遵循不同的协议格式。在进行新的协议扩展的时候，UDB 只需要增加相应的协议解析模块即可。

UDB 主要提供以下三类公共接口：

- 面向应用层，主要是第三方 SP 应用系统的重定向认证接口；
- 面向应用层，主要是电信内部应用系统或客户端软件的 Web Services 接口；
- 面向需要大容量并发处理的电信应用系统/业务管理平台的自定义 ISAP 协议接口(解决 Web Services 性能问题)。

### 6.2 重定向接口

#### 6.2.1 接口概述

重定向（Redirect）是指允许旧 URL 被重新指向到新 URL，实现完全的跳转，浏览器将会得到跳转 URL 地址，并重新发送请求链接。

所有涉及第三方 SP 的应用均要求采用重定向到 UDB 进行集中认证。

全国 UDB 及省 UDB 的重定向域名与省自服务门户域名相同，由中国电信集团公司进行统一规划和申请。



## 6.2.2 重定向认证请求接口

(1) 接口信息:

接口名称	PassportLogin
接口描述	提供给使用统一帐号的业务应用系统的用户重定向认证接口； UDB 提供统一的重定向认证接口及认证页面。
请求消息名	http://省别简写.Passport.189.cn/ PassportLogin
应答消息名	ReturnURL
接口协议	重定向
提供者	UDB 系统
主要使用者	电信自营应用，或第三方应用系统

(2) 参数说明:

1) 请求消息

http://省别简写.Passport.189.cn/PassportLogin?PassPortLoginRequest =  
PassPortLoginRequestValue

Passport.189.cn 是中国电信应用层统一认证的暂定域名，其中省别简写，参考第 14 章数据编码规范的省别信息。

PassPortLoginRequestValue 为接口参数值，包含如下信息:

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发起端的应用系统设备标识
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss， 其中 HH 取值为 00-23，时区为东八区
ReturnURL	String		1	UDB 系统返回认证结果时需要调用的 URL

PassPortLoginRequestValue 的生成算法如下:

$\text{Digest} = \text{Base64}(\text{Hash}(\text{SrcSsDeviceNo} + \text{TimeStamp} + \text{ReturnURL}))$

其中，Hash 算法采用 SHA-1。

$\text{PassPortLoginRequestValue} = \text{URLEncoding}(\text{SrcSsDeviceNo} + \$ + \text{Base64}(\text{Encrypt}(\text{TimeStamp} + \$ + \text{ReturnURL} + \$ + \text{Digest})))$

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，SysKey 是 UDB 系统

发给该应用系统的密钥。

UDB 在接收到重定向认证请求后，需要再做一次哈希转换：

$Digest = Base64(Hash(SrcSsDeviceNo + TimeStamp + ReturnURL))$

将 Digest 与接收到 Digest 进行比较，若两者相同，则传送消息没有被篡改。

本规范中所有涉及到的 3DES 算法，均默认使用 CBC 模式；填充方式均默认使用 PKCS7Padding。

## 2) 应答消息

接口方法为：

`http://ReturnURL?PassPortLoginResponse= PassPortLoginResponseValue`

其中，ReturnURL 从 PassPortLoginRequest 中获得。

PassPortLoginResponseValue 为接口参数值，包含如下信息：

参数名称	数据类型	长度 (字节)	出现频次	说明
Result	Int	2	1	0: 成功 其他: 失败
DesSsDeviceNo	String	16	1	返回方应用系统设备标识
UDBTicket	String	64	0-1	返回给应用系统的 Ticket 信息； 若认证失败，则不返回 Ticket。
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss， 其中 HH 取值为 00-23,时区为东八区

PassPortLoginResponseValue 的生成算法如下：

$Digest = Base64(Hash(Result + DesSsDeviceNo + UDBTicket + Timestamp))$

其中，Hash 算法采用 SHA-1。

$PassPortLoginResponseValue = URLEncoding(DesSsDeviceNo + "$" + Base64(Encrypt ( Result + "$" + UDBTicket + "$" + TimeStamp + "$" + Digest)))$

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，Syskey 是 UDB 系统颁发给该系统的密钥。

调用方系统在接收到 UDB 的返回结果后，需要对重定向返回所携带的消息再做一次哈希转换：

Digest ' = Base64(Hash(Result + DesSsDeviceNo + UDBTicket + TimeStamp))

将 Digest '与接收到的 Digest 进行比较，若两者相同，则说明传送消息没有被篡改。

### 6.2.3 重定向单点登录接口

(1) 接口信息：

接口名称	PassportSSO
接口描述	提供给 UDB 的互信方的专用单点登录接口，无须二次认证用户便可直接使用目标应用
请求消息名	http://省别简写.Passport.189.cn/PassportSSO
应答消息名	无应答
接口协议	重定向
提供者	UDB 系统
主要使用者	UAM、电信自营应用系统、第三方应用系统

(2) 参数说明：

1) 请求消息

http://省别简写.Passport.189.cn/PassportSSO? PassportSSORequest =  
PassportSSORequestValue

Passport.189.cn 是中国电信应用层统一认证的暂定域名，其中省别简写，参考第 14 章数据编码规范的省别信息。

PassportSSORequestValue 为接口参数值，包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发起端的电信应用系统设备标识 【UDB 需要为 UAM，及第三方应用分配统一的设备标识】
UserID	String	40	0-1	用户统一帐号 【该字段针对电信自营应用系统，要访问第三方应用】
PUserID	String	11	0-1	用户唯一标识：2 位省 ID+9 位用户标识 ID 【该字段仅针对第三方应用，要 SSO

				到电信自营应用】
UAMTicket	String	64	0-1	UAM 的客户随机标识 【该字段仅针对 UAM 的 SSO 到电信应用】
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区
SSOURL	String		1	重定向到目标应用系统的 URL

PassportSSORequestValue 的生成算法如下：

$$\text{Digest} = \text{Base64}(\text{Hash}(\text{SrcSsDeviceNo} + \text{UserID} + \text{PUserID} + \text{UAMTicket} + \text{TimeStamp} + \text{SSOURL}))$$

其中，Hash 算法采用 SHA-1。

$$\text{PassportSSORequestValue} = \text{URLEncoding}(\text{SrcSsDeviceNo} + \$ + \text{Base64}(\text{Encrypt}(\text{UserID} + \$ + \text{PUserID} + \$ + \text{UAMTicket} + \$ + \text{TimeStamp} + \$ + \text{SSOURL} + \$ + \text{Digest})))$$

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，SysKey 是 UDB 系统发给该应用系统的密钥。

UDB 在接收到重定向认证请求后，需要再做一次哈希转换：

$$\text{Digest}' = \text{Base64}(\text{Hash}(\text{SrcSsDeviceNo} + \text{UserID} + \text{PUserID} + \text{Ticket} + \text{TimeStamp} + \text{SSOURL}))$$

将 Digest' 与接收到 Digest 进行比较，若两者相同，则传送消息没有被篡改。

## 2) 应答消息

无应答。

## 6.3 Web Services 接口

### 6.3.1 接口概述

对 Web Service 的调用采用 SOAP 协议，SOAP 接口若无特殊说明，均承载在 HTTP 协议上。承载 SOAP 调用的 HTTP 请求头中使用 POST 命令。接口具体的 XML 格式定义参考相应的 WSDL(见附件)。

## SOAP:

SOAP (Simple Object Access Protocol, 简单对象访问协议) 是一种使用 XML 为数据编码格式的在松散的、分布的环境中交换包括结构化、类型化数据等信息的轻量级协议。SOAP 传送信息的基本承载单元是基于 XML 的 SOAP 消息, SOAP 可以广泛的作为各种应用的信息传递协议。

SOAP 消息结构如图 6.3-1 所示, SOAP 信封(SOAP Envelope)是表示 SOAP 消息的 XML 文档的根元素, SOAP 头部(SOAP Header)是一个可选元素, 包含一些与安全性、路由信息以及消息处理模型相关的一些重要信息。SOAP 主体(SOAP Body)是必需的元素, 包含需要传输的实际信息。SOAP 消息传递的具体实现可以使用通过特定绑定协议的特性来优化, 例如, HTTP 可以使 SOAP 应答消息以 HTTP 应答的方式传输, 并使用同一个连接返回请求。

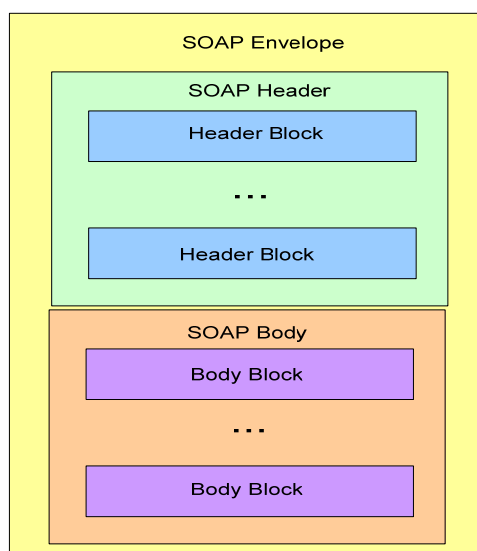


图 6.3-1: SOAP 消息结构

关于 SOAP 需注意的两个问题:

- RPC(Remote Process Call, 远程过程调用)和文档(Document)风格的 SOAP 消息绑定 (在 WSDL soap:binding 元素的 style 属性制定): SOAP 交互本身是基于消息的, 但是也包含了过程或者方法调用的支持。RPC 风格指出 SOAP 消息主体中包含了某个 RPC 调用或者响应的 XML 表示, 而文档风格指出 SOAP 消息主体包含的只是一个 XML 文档, 发送方和接收方需要遵循该文档的格式。

- 使用文字(Literal)和使用编码(Encoded)的 SOAP 消息绑定用法(WSDL soap:body 元素的 use 属性制定): 消息绑定用法指的是用于确定数据序列映射到普通的 XML 格式的序列化机制。使用文字用法, 将由 XSD(XML Schema Definition, XML 模式定义)确定 SOAP 主体的 XML 格式, 不具有二义性, 而使用编码用法, SOAP 处理器必须在运行时遍历各种 SOAP 编码规则以确定 SOAP 主体正确的序列化, 这将易于导致错误和互操作性方面的问题。SOAP 编码的用法是 XSD 没有完善之前提出的一种 SOAP 消息绑定用法, 对它的支持已经成为可选甚至被要求不再支持。

在本规范中 Web Services 接口中默认采用 Document 风格绑定以及 Literal 的消息绑定用法。并且 Web Services 接口传送的密文默认使用十六进制字符串形式。

为增强安全性, UDB 需对调用 Web Services 接口的各应用系统 IP 地址进行验证, 只允许响应符合预先设置的 IP 地址发送的请求。

### 6.3.2 业务认证请求接口

#### (1) 接口信息:

接口名称	AccountLogin
接口概述	UDB 通过此接口, 为电信内部应用系统, 提供统一帐号(或别名)+通用/业务密码等的认证请求服务; UDB 将认证结果, 及该用户状态属性等信息反馈给应用系统。 该接口主要由电信内部应用系统或 UDB 设备之间进行调用。
请求消息名	AccountLoginRequest
应答消息名	AccountLoginResponse

#### (2) 参数说明

##### 1) 请求消息

AccountLoginRequest 包含如下参数:

参数名称	数据类型	长度(字节)	出现频次	说明
Authenticator	String	256	1	认证码, 用于鉴别发送者。 取值 = base64(3DES(SHA1(SrcSsDeviceNo+AuthSsDeviceNo+UserID+Alias+TimeStamp))), 3DES 采用

				UDB颁发给调用系统的Key 为密钥
SrcSsDeviceNo	String	16	1	消息发送端的应用系统设备 标识： 源端若为非 UDB 设备，则为 直接认证请求； 源端若为 UDB 设备，则为漫 游认证转发请求；
AuthSsDeviceNo	String	16	1	目标认证的应用系统设备标 识： 【适用于ISMP平台为多个 业务/SP分别提供请求】
UserID	String	40	0-1	用户统一帐号 手机号码、区号+固话号码 等
Alias	String	40	0-1	用户别名
AuthUserType	Integer	2	1	认证用户帐号格式 0: 统一帐号【默认】 1: 用户别名认证
AuthPWDDType	Integer	2	1	密码鉴权类型： 0: 通用/业务密码认证； 1: 动态短信密码认证； 2: OTP 密码认证(默认的首 选 OTP 厂商)； 【保留类型，待后续认证功 能扩展使用】 3: 扩展密码认证； 4: 通用+扩展密码认证； 5: 通用或者扩展密码认证； 99: 其他；
NormalPasswordEncryType	Integer	2	1	认证密码加密方法： 0: MD5 加密【默认】 1: 3DES 9: 明文传送
NormalPassword	String	64	1	认证密码传送值
ExtPasswordType	Integer	2	0-1	扩展密码类型： 0: 手机短信密码； 1-99: OTP 厂商代码； 100-: 其他；
ExtPasswordEncr	Integer	2	0-1	扩展密码加密方法：

yType				0: MD5 加密【默认】 1: 3DES 9: 明文传送
ExtPassword	String	64	0-1	扩展密码传送值:
TimeStamp	String	19	1	时间戳: 时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区 用于统计以及动态密码的实效性判断等
ReturnSslInfo	Integer	1	0-1	返回其他应用系统的状态数组信息 0: 不返回【默认】 1: 返回

UDB 接收到该请求后, 应该按照 Authenticator 参数的原始签名加密的处理方式, 对接收到的相应参数再做一次相同的签名加密处理, 得到一个 Authenticator'。若两者结果一致, 则表示传送消息没有被篡改, 进行正常响应。

## 2) 响应消息

AccountLoginResponse 包含如下参数:

名称	数据类型	长度 (字节)	出现频次	说明
ResultCode	Integer	2	1	认证结果码, 统一定义 如果结果码不成功, 自第三个参数以后可都不传送
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识位
Alias	String	40	0-1	别名
BindingAccessNo	String	40	0-1	绑定的宽带接入 ID 【该项只对注册成统一帐号的宽带用户, 且登录电信自营应用才有效】
ThirdSsUserID	String	40	0-1	绑定的第三方应用系统的原用户帐号 ID 【该项只对第三方应用才有效】
UserIDStatus	String	2	0-1	统一帐号状态
UserIDSsStatus	String	2	0-1	用户在该应用系统注册状态: 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停



				4: 业务停用/业务注销 5: 其他 【应用系统可根据实际需要，选择是否使用该参数】
UserPayType	String	2	0-1	用户付费类型： 1: 后付费用户 2: 预付费用户
PrePaySystemNo	String	14	0-1	预付费用户，需提供此字段，表明在哪个预付费系统扣费
ReturnSsInfoList	ReturnSsInfo	—	0-1	应用系统相关信息
Description	String	128	0-1	对认证请求结果的详细描述信息

ReturnSsInfo定义如下：

参数名称	数据类型	长度（字节）	出现频次	说明
SsType	String	4	0-n	应用系统类型
UserIDSsStatus	String	2	0-n	统一帐号对该业务的注册状态 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务注销/停用 5: 其他
UserIDSsLoginStatus	String	2	0-n	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他

### 6.3.3 短信密码获取请求

本接口参考《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》，增加请求短信密码获取请求的业务类型字段和获取密码类型的字段，作为实现多种业务短信获取密码的公共接口。

(1) 接口信息：

接口名称	StdGetPasswordService
接口概述	<b>适用范围：</b> 只有与 UDB 之间通过 SOAP/ISAP 协议认证请求的电信自营应用系统，才在其应用系统界面提供手机短信密码获取功能；对采用重定向

	认证的应用系统，仅在 UDB 统一提供的登录界面提供短信密码获取功能。 根据应用系统/Portal 的手机短信密码请求（UDB 生成随机密码，或查询通用密码（业务密码）），并通过短信网关发送至用户手机，并向应用系统/Portal 返回开通结果。
请求消息名	StdGetPasswordServiceRequest
应答消息名	StdGetPasswordServiceResponse

## （2） 参数说明

### 1) 请求消息

StdGetPasswordServiceRequest 包含如下参数：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	源发送的应用系统号码
ReqSsDeviceNo	String	16	1	短信请求的应用系统号码
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识位 【第三方合作应用时，可通过该标识明确具体用户】
PWDType	Integer	2	1	获取密码类型： 0：随机密码【默认】 1：通用/业务密码：【该功能主要实现密码查询服务。对应用系统获取密码，则将其密码策略所对应的密码发送】。 2：其他
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

- 请求对象中的 UserID 字段目前要求为统一帐号（今后可根据具体省份的要求进行扩展）；经过统一帐号有效性校验后，无论是否首次使用，系统均生成新的密码并发送密码短信；
- 请求对象中的 TimeStamp 字段为时间戳字段，用于报文有效性校验，如果时间戳与系统当前时间差距大于一定时间段，则不进行操作，并返回-5 错误；

为了防止重复提交，可以扩充时间戳字段的用途，在一定时间内的反复提交，认为是无效操作，自动进行过滤，此外要求应用系统/Portal 系统实现防止重复提交的功能，避免在很短的时间内多次向 UDB 发送请求。

为使用时间戳，应用系统/Portal 与 UDB 需与标准时间同步。

### 2) 响应消息

StdGetPasswordServiceResponse 包含如下参数：

名称	数据类	长度（字节）	出现频次	说明
----	-----	--------	------	----

	型			
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识位 【第三方合作应用时，可通过该标识明确具体用户】
ResultCode	Integer	2	1	0: 开通成功 1: 用户未开通（或号码不存在） 2: 用户停机 3: 用户欠费 5: 请求数据异常（时间同步差异大等） 6: 失败（其他原因）
PwdLiveTime	Integer	4	0-1	密码有效期： （以秒为单位），与时间戳共同确定失效时间，本域值为 0 表示密码有效期由接收的应用系统维护。
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区
Description	String	128	0-1	对操作结果的详细描述信息

- 返回对象中的 **ResultCode** 为操作结果，根据操作结果返回，**Description** 字段返回可补充描述操作原因。成功时，**Description** 可返回具体业务提示信息，失败时，**Description** 可返回具体失败原因；
- 应用系统/Portal 根据返回对象的 **ResultCode** 信息通过页面或弹出窗口提示用户(各应用系统自定义)，如 C+W 业务具体如下：

结果代码	说明	应用系统/Portal提示用户开通结果信息
0	开通成功	尊敬的CDMA用户，密码已通过短信发送到您的手机中，如1分钟内未收到短信，请刷新页面并操作重新获取密码
1	用户未开通（或号码不存在）	尊敬的用户：该号码是空号，请检查号码是否存在或开户地输入错误，详情咨询开户地客服热线10000
2	用户停机	尊敬的用户：您的手机已停机，不能开通此项业务，请咨询开户地客服热线10000
3	用户欠费	尊敬的用户：您的手机欠费，不能开通此项业务，请咨询开户地客服热线10000
5	请求数据异常	尊敬的用户：业务开通失败，详细原因请咨询开户地客服热线10000
6	开通失败（其他原因）	尊敬的用户：业务开通失败，详细原因请咨询开户地客服热线10000

### (3) 其他说明

- 如果调用该接口的应用系统/Portal 在设定的时间内(如 10 秒等, 各应用系统/Portal 自定义)没有收到归属地 UDB 短信开通返回的响应, 则提示用户开通失败。

### 6.3.4 业务密码设置接口

#### (1) 接口信息:

接口名称	AccountSsPWRefresh
接口概述	<p>此接口是为实现业务密码（私有密码）策略功能而设, 由 UDB 提供, 供应用系统直接调用。</p> <p><b>适用范围:</b> 只有与 UDB 之间通过 SOAP/ISAP 协议认证请求的电信自营应用系统, 才需要考虑调用该接口; 对采用重定向认证的应用系统, 不提供该功能接口。</p> <p>当用户在具体应用系统修改业务密码后, 调用此接口将密码同步到 UDB, 同时此帐户对应业务密码认证策略改为业务密码登录策略, UDB 保存此业务密码。</p> <p>用户设置了应用系统的业务密码, 则通用密码将无法再登录该应用系统, 用户只能通过重置密码策略才能可复原。</p>
请求消息名	AccountSsPWRefreshRequest
应答消息名	AccountSsPWRefreshResponse

#### (2) 参数说明

##### 1) 请求消息

AccountSsPWRefreshRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现频次	说明
Authenticator	String	256	1	认证码, 用于鉴别发送者。取值 = base64(3DES(SHA1(SrcSsDeviceNo+UpdateSsDeviceNo+UserID+PUserID+ThirdSsUserID))), 3DES 采用 UDB 颁发给调用系统的 Key 为密钥
SrcSsDeviceNo	String	16	1	消息发送端应用系统设备标识
UpdateSsDeviceNo	String	16	1	更新密码的目标应用系统设备标识
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识
ThirdSsUserID	String	40	0-1	用户在第三方系统帐号

				【只针对采用帐号绑定的第三方合作平台，否则返回空】
SsPWStatus	String	2	1	应用系统的密码策略 0: 重置为通用密码【默认】 1: 设为业务密码登录
SsPWEncryType	Integer	2	0-1	密码加密方式:【通过明文或可解加密】 1: 3DES 9: 明文传送
SsPassword	String	64	0-1	业务密码的传送值
OldSsPassword	String	64	0-1	原业务密码的传送值 【针对需要进行修改密码，需进行原密码核对场景；若无须验证，则该值可不传送，UDB 不做处理】

UDB 接收到该请求后，应该按照 Authenticator 参数的原始签名加密的处理方式，对接收到的相应参数再做一次相同的签名加密处理，得到一个 Authenticator'。若两者结果一致，则表示传送消息没有被篡改，进行正常响应。

## 2) 响应消息

AccountSsPWRefreshResponse 包含如下参数：

名称	数据类型	长度（字节）	出现频次	说明
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识
ResultCode	Integer	2	1	结果码，统一定义
Description	String	128	0-1	对业务密码更新操作的描述信息

## 6.3.5 帐号信息查询接口

### (1) 接口信息：

接口名称	AccountInfoQuery
接口描述	支持多种帐号格式（如统一帐号、用户别名、宽带帐号）的查询请求，也可选择不同查询方式，如查询全部信息，或部分信息等；

	全国 UDB 向省 UDB 发起请求，或自服务门户向 UDB 发起请求，查询统一帐号的用户详细信息。被查询 UDB 对象应将该用户的所有相关详细信息传送给查询方。 应用系统注册统一帐号用户时，UDB 可为部分应用系统提供统一帐号的合法性及当前状态属性查询，以协助应用系统判断是否给该用户成功注册。
请求消息名	AccountInfoQueryRequest
应答消息名	AccountInfoQueryResponse

## (2) 参数说明

### 1) 请求参数

AccountInfoQueryRequest 包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	14	1	发送端应用系统设备标识：全国 UDB，或自服务门户、应用系统等发起请求
QuerySsDeviceNo	String	14	1	查询帐号信息的应用系统设备标识：【适用于 ISMP 可为多个业务/SP 分别提供帐号查询请求】【若非 ISMP，则该参数与 SrcSsDeviceNo 一致】
UserID	String	40	0-1	统一帐号
Alias	String	40	0-1	用户别名
AccessNo	String	40	0-1	宽带帐号
QueryUserType	Integer	1	1	查询帐号的类型 0：统一帐号 1：用户别名 2：宽带帐号
QueryInfoType	Integer	2	1	查询类型： 0：该帐号全部信息 1：该帐号状态查询

### 2) 响应消息

AccountInfoQueryResponse 包含如下信息：

参数名称	数据类型	度（字节）	出现频次	说明
UserID	String	40	1	用户统一帐号
userIDType	String	2	0-1	用户帐号类型
PUserID	String	11	0-1	用户唯一标识
ResultCode	Integer	2	1	结果码，统一定义

Alias	String	40	0-1	用户别名
ProvinceNo	String	2	0-1	归属省
CityNo	String	3	0-1	归属地市
AreaCode	String	4	0-1	地市区号
CustomerID	String	20	0-1	客户 ID（CRM 系统标识）
UserName	String	40	0-1	用户姓名
CertificateType	Integer	2	0-1	用户证件类型
CertificateNo	String	40	0-1	用户证件号
UserPayType	String	2	0-1	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystemNo	String	14	0-1	预付费用户，需提供此字段，表明在哪个预付费系统扣费。
SerSetType	String	2	0-1	套餐属性 【待定，暂不考虑】
AccessNo	String	40	0-1	【只针对宽带帐号类型用户】绑定的宽带帐号
UserIDStatus	String	2	0-1	用户帐号状态属性
NormalPasswordEncryType	Integer	2	0-1	通用密码加密方法：【必须明文或可解加密方式传送】 1：3DES 9：明文传送
NormalPassword	String	64	0-1	通用密码传送值
SsStatusList	SsStatusInfo	—	0-1	相关应用系统信息
Description	String	128	0-1	对查询结果的详细描述信息

#### SsStatusInfo

名称	数据类型	长度（字节）	出现频次	说明
SsType	String	4	0-n	应用系统类型
ThirdSsUserID	String	40	0-n	第三方应用系统的绑定帐号 【对电信内部应用系统认证，该值为空】
UserIDSsStatus	String	2	0-n	统一帐号对该业务的使用状态 1：业务未开通/业务未注册 2：业务开通/业务注册 3：业务暂停 4：业务停用/业务注销 5：其他

UserIDSsLoginStatus	String	2	0-n	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他
SsPWStatus	String	2	0-n	应用系统的密码策略 0: 重置为通用密码【默认】 1: 设为业务密码登录
SsPWEncryType	Integer	2	0-n	业务密码加密方式:【必须明文或可解加密方式传送】 1: 3DES 9: 明文传送
SsPassword	String	64	0-n	业务密码的传送值

### 6.3.6 帐号信息更新接口

#### (1) 接口信息:

接口名称	AccountInfoRefresh
接口描述	全国 UDB 和省 UDB 之间, 或自服务门户与 UDB 之间, 当用户主动进行信息变更时 (如通用密码、密码策略、业务密码、别名设置等), 需相互通知最新更新, 以确保多个系统保存的信息一致性。 当帐号信息在省 UDB 发生变化并且帐号已经做了标记, 省 UDB 向全国 UDB 发起帐号信息更新请求, 全国 UDB 进行更新并返回更新结果; 当帐号信息在全国 UDB 发生变化, 全国 UDB 向省 UDB 发起帐号信息更新请求, 省 UDB 进行更新并返回更新结果; 当用户在自服务门户进行了帐号信息设置, 也同步更新给 UDB。
请求消息名	AccountInfoRefreshRequest
应答消息名	AccountInfoRefreshResponse

#### (2) 参数说明

##### 1) 请求参数

AccountInfoRefreshRequest 包含如下信息:

参数名称	数据类型	长度 (字节)	出现频次	说明
SrcSsDeviceNo	String	16	1	发送端应用系统设备标识, 全国 UDB、省 UDB 或自服务门户系统
UserID	String	40	1	用户统一帐号
UserIDType	String	2	0-1	帐号类型



UpdateFlag	String	2	1	更新标识： 0：全部更新 1：别名更新（仅更新别名） 2：通用密码更新 3：用户状态更新 4：付费属性更新（付费类型+付费系统号） 5：套餐属性更新（待定） 6：身份更新（姓名、证件类型及证件号码等） 7：业务信息更新（包括业务密码策略、业务密码设置等） 8：别名更新+全部信息上传
Alias	String	40	0-1	别名
UserName	String	40	0-1	用户姓名
CertificateType	Integer	2	0-1	用户证件类型
CertificateNo	String	40	0-1	用户证件号
UserPayType	String	2	0-1	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystemNo	String	14	0-1	预付费用户，需提供此字段，表明在哪个预付费系统扣费。
SerSetType	String	2	0-1	套餐属性 【待定】
BindingAccessNo	String	40	0-1	统一帐号绑定的宽带帐号
UserIDStatus	String	2	0-1	用户帐号状态属性
NormalPasswordEncryType	Integer	2	0-1	密码加密方法【必须明文或可解加密传送】 1：3DES 9：明文传送
NormalPassword	String	64	0-1	通用密码传送值
OldNormalPassword	String	64	0-1	原通用密码传送值： 【仅针对用户在自服务门户修改通用密码，且需要验证原密码情况；若无须验证原密码需要，则该值可不传送，UDB 不做处理】
SsStatusList	SsStatusInfo	—	0-1	相关应用系统的信息

#### SsStatusInfo

名称	数据类型	长度（字	出现频次	说明
----	------	------	------	----

		节)		
SsType	String	4	0-n	应用系统类型
ThirdSsUserl D	String	40	0-n	绑定的第三方应用系统帐号： 【对电信内部应用系统认证，该 值为空】
UserIDSsStat us	String	2	0-n	统一帐号对该业务的使用状态 1：业务未开通/业务未注册 2：业务开通/业务注册 3：业务暂停 4：业务停用/业务注销 5：其他
UserIDSsLogi nStatus	String	2	0-n	统一帐号对该业务的在线状态 1：用户上线 2：用户下线 3：其他
SsPWStatus	String	2	0-n	应用系统的密码策略 0：重置为通用密码【默认】 1：设为业务密码登录
SsPWEncryTy pe	Integer	2	0-n	业务密码加密方式：【业务密码必 须明文或可解加密通知】 1：3DES 9：明文传送
SsPassword	String	64	0-n	业务密码传送值
OldSsPasswo rd	String	64	0-n	原业务密码传送值 【仅针对用户在自服务门户修改 业务密码，且需要验证原业务密 码情况；若无须验证原密码需要， 则该值可不传送, UDB 不做处理】

## 2) 响应消息

AccountInfoRefreshResponse 包含如下信息：

参数名称	数据类型	长度（字节）	出现 频次	说明
UserID	String	40	1	用户统一帐号
ResultCode	Integer	2	1	结果码，统一定义
Description	String	128	0-1	帐号更新结果的描述信息

### 6.3.7 外部帐号绑定接口

对中国电信内部应用系统的原有用户 ID，主要通过统一帐号替换原用户 ID 方式，逐步实现中国电信的帐号统一，原在应用系统的认证流程全部转到 UDB 进行统一认证。对第三方 SP 的应用系统，中国电信可选择提供外部帐号绑定服务，即建立中国电信统一帐号与原用户帐号 ID 的绑定关系，一般要求第三方合作伙伴提供用户帐号绑定服务流程和界面，UDB 提供外部帐号绑定接口，将绑定关系相关的用户信息在中国电信 UDB 设备进行集中管理。

外部帐号绑定，是中国电信与第三方 SP 进行合作的一种选择模式。绑定关系也可维护在第三方，中国电信只负责统一帐号的认证服务。

#### (1) 接口信息：

接口名称	AccountBind
接口概述	此接口提供第三方应用系统原有帐号与统一帐号进行绑定的功能。绑定成功后，第三方应用系统通过 UDB 的统一帐号及密码进行认证，认证成功后，UDB 返回绑定的原用户帐号给第三方应用系统进行。注意：对于与第三方进行重定向认证合作的 SP，则绑定后重定向返回的用户信息是原帐号（而非统一帐号）
请求消息名	AccountBindRequest
应答消息名	AccountBindResponse

#### (2) 参数说明

##### 1) 请求消息

AccountBindRequest 包含如下参数：

参数名称	数据类型	长度（字节）	出现频次	说明
Authenticator	String	256	1	认证码，用于鉴别发送者。取值=base64 (3DES(SHA1 (SrcSsDeviceNo+BindSsDeviceNo+UserID+PUserID+TimeStamp))), 3DES采用UDB颁发给调用系统的Key为密钥
SrcSsDeviceNo	String	16	1	发送端应用系统设备标识
BindSsDeviceNo	String	16	1	被绑定帐号的原应用系统设备标识
UserID	String	40	0-1	用户统一帐号（与 PUserID 两者必须出现其一）
PUserID	String	11	0-1	用户唯一标识位
ThridSsUserID	String	40	1	绑定第三方应用系统的原用户帐号 ID

SsPWEncryType	Integer	2	0-1	第三方业务密码加密方式：【必须通过明文或可解加密方式通知】 1: 3DES 9: 明文传送 【若为第三方采用 OTP 等密码方式，则绑定可不传业务密码】
SsPassword	String	64	0-1	第三方业务密码的（加密）传送值
BindType	String	2	1	绑定类型： 0:绑定 1:解绑
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区
BindEffectMode	Integer	1	0-1	绑定生效模式： 0: 默认实时绑定 1: 下月 1 号绑定(根据时间戳判断) 2: 次日绑定(根据时间戳判断) 3: 指定时间绑定(指定 EffectTimeStamp 作为绑定生效时间) 4: 其他
EffectTimeStamp	String	19	0-1	帐号绑定生效时间：时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区，RefreshEffectMode=3 时有效，注册状态生效模式为其他值时无效，可为空

UDB 接收到该请求后，应该按照 Authenticator 参数的原始签名加密的处理方式，对接收到的相应参数再做一次相同的签名加密处理，得到一个 Authenticator'。若两者结果一致，则表示传送消息没有被篡改，进行正常响应。

## 2) 响应消息

AccountBindResponse 包含如下参数：

名称	数据类型	长度（字节）	出现频次	说明
ResultCode	Integer	2	1	结果码，统一定义
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识位
Description	String	128	1	对绑定操作结果的详细描述信息

### 6.3.8 业务注册状态通知

#### (1) 接口信息：

接口名称	AccountSsStatusRefresh
接口概述	应用系统对统一帐号用户的注册状态更新通知：当用户在应用系统发生了业务注册/开通、业务注销、业务暂停等状态变更时，应用系统需实时向 UDB 发送变更的注册状态，UDB 进行保存。 一般 UDB 需要判断发送端应用系统类型与需要更新业务注册状态的应用系统类型是否一致，是否合法。
请求消息名	AccountSsStatusRefreshRequest
应答消息名	AccountSsStatusRefreshResponse

#### (2) 参数说明

##### 1) 请求消息

AccountSsStatusRefreshRequest 包含如下参数：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	消息发送端应用系统设备标识
UpdateSsDeviceNo	String	16	1	需更新注册的应用系统设备标识
UserID	String	40	0-1	用户统一帐号：
PUserID	String	11	0-1	用户唯一标识
UserIDSsStatus	String	2	1	统一帐号对该业务的使用状态 1：业务未开通/业务未注册【此项不主动通知】 2：业务开通/业务注册 3：业务暂停 4：业务注销/停用 5：其他
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23，时区为东八区，用于标明发送端发起的状态更新时间
RefreshEffectMode	Integer	1	0-1	注册/注销状态生效模式： 0：实时更新【默认】 1：下月 1 号更新(根据时间戳判断) 2：次日更新(根据时间戳判断) 3：指定时间更新(指定 EffectTimeStamp 作为更新生效时间)

				4: 其他
EffectTimeStamp	String	19	0-1	状态更新生效时间: yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区, <b>RefreshEffectMode=3</b> 时有效, 注册状态生效模式为其他值时无效, 可为空

## 2) 响应消息

AccountSsStatusRefreshResponse 包含如下参数:

名称	数据类型	长度 (字节)	出现频次	说明
UserID	String	40	0-1	用户统一帐号:
PUserID	String	11	0-1	用户唯一标识
ResultCode	Integer	2	1	结果码, 统一定义
Description	String	128	0-1	对状态更新结果的详细描述信息

## 6.3.9 业务在线状态通知

### (1) 接口信息:

接口名称	AccountSsLoginStatusRefresh
接口概述	应用系统对统一帐号用户的在线状态更新通知: 当用户在应用系统进行登录和退出, 应用系统需实时向 UDB 发送在线状态的通知, 由 UDB 进行保存和维护, 以供扩展单点登录、用户呈现等服务使用。 一般 UDB 需要判断发送端应用系统类型与需要更新业务在线状态的应用系统类型是否一致, 是否合法。
请求消息名	AccountSsLoginStatusRefreshRequest
应答消息名	AccountSsLoginStatusRefreshResponse

### (2) 参数说明

#### 1) 请求消息

AccountSsLoginStatusRefreshRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现频次	说明
SrcSsDeviceNo	String	16	1	消息发送端应用系统设备标识
UpdateSsDeviceNo	String	16	1	需更新业务在线状态的应用系统设备标识
UserID	String	40	0-1	用户统一帐号:
PUserID	String	11	0-1	用户唯一标识
UserIDSsLoginStatus	String	2	1	统一帐号对该业务的在线状态 1: 用户上线

				2: 用户下线 3: 其他
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区,

## 2) 响应消息

AccountSsLoginStatusRefreshResponse 包含如下参数:

名称	数据类型	长度 (字节)	出现频次	说明
UserID	String	40	0-1	用户统一帐号:
PUserID	String	11	0-1	用户唯一标识
ResultCode	Integer	2	1	结果码, 统一定义
Description	String	128	0-1	对状态更新结果的详细描述信息

## 6.3.10 帐号验证及短信申请

## (1) 接口信息:

接口名称	AccountInfoConfirm
接口概述	用户申请开通某项业务(如使用 CDMA 号码发送短信开通 189 邮箱), 应用系统向 UDB 申请验证用户的状态属性(是否正常、欠费, 或停机); UDB 在用户身份正常的情况下, 通过短信告知用户: “您已开通 XXX 业务, 登录密码为 XXX”; 应用系统根据返回验证信息, 正常的话则开通/注册用户。
请求消息名	AccountInfoConfirmRequest
应答消息名	AccountInfoConfirmResponse

## (2) 参数说明

## 1) 请求消息

AccountInfoConfirmRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现频次	说明
SrcSsDeviceNo	String	16	1	消息发送端应用系统设备标识
UserID	String	40	1	用户统一帐号
SmsPwdFlag	Integer	1	1	是否通过短信下发通用密码 【UDB 只允许对指定业务平台 (如 189 邮箱或天翼客户端) 提供该接口功能】 0: 不发送【默认值】 1: 发送通用密码
TimeStamp	String	19	1	时间戳: yyyy-MM-dd

				HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区 用于标明应用系统发送请求的时间
--	--	--	--	------------------------------------------------------

## 2) 响应消息

AccountInfoConfirmResponse 包含如下参数:

名称	数据类型	长度(字节)	出现频次	说明
UserID	String	40	1	用户统一帐号
ResultCode	Integer	2	1	结果码, 统一定义
UserIDStatus	String	2	0-1	统一帐号状态
Description	String	128	0-1	对注册鉴权判断的详细描述信息

### 6.3.11 安全密钥通知接口

安全密钥的更新分为正常更新和紧急更新两种。

正常更新是指全国 UDB-省 UDB 之间, 或 UDB-应用系统之间定期(不定期)主动更新密钥, 以避免出现密钥泄漏的情况。在正常更新情况下, UDB 生成新的密钥, 应用系统接到密钥更新通知后, 必须在本地保留密钥的所有相关信息。原密钥加密的信息在规定的有效时间内仍然有效, 超过有效时间后应拒绝服务请求, 并作相应的处理。

紧急更新是指全国 UDB-省 UDB 之间, 或 UDB-应用系统之间的密钥出现泄漏时, 需要紧急替换该密钥。原密钥加密的信息应即时失效, 例如用原密钥加密的用户 Token 信息应即时失效, 用户需要再次登录方可继续使用。

密钥更新过程中涉及相关方采用数字证书验证身份, 采用 WebService 方式, 密钥的实时传输采用 SSL 以保证安全。特殊情况下, 安全密钥可通过人工方式进行相互通知。

## (1) 接口信息:

接口名称	SecurityKeyRefresh
接口描述	安全密钥由全国 UDB 进行统一维护, 然后调用省 UDB 接口更新到各省 UDB。
请求消息名	SecurityKeyRefreshRequest
应答消息名	SecurityKeyRefreshResponse



## (2) 参数说明

## 1) 请求参数

SecurityKeyRefreshRequest 包含如下信息:

参数名称	数据类型	长度 (字节)	出现频次	说明
SrcDeviceNo	String	16	1	发送端应用系统设备标识, 全国 UDB, 或省 UDB
UpdateDeviceNo	String	16	1	需要更新密钥的应用系统设备标识, 省 UDB, 或应用系统
EncryType	Integer	2	0-1	加密方法: 【密钥必须通过明文或可解加密方式通知 UDB】 1: 3DES 9: 明文传送
UpadateKeyValue	String	256	1	密钥传送值
UpdateMode	Integer	1	1	密钥更新类型: 0: 正常更新 【默认】 1: 紧急更新
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区 用于标明发送端发起的状态更新时间

## 2) 响应消息

SecurityKeyRefreshResponse 包含如下信息:

名称	数据类型	长度 (字节)	出现频次	说明
ResultCode	integer	2	1	结果码, 统一定义
Description	String	128	0-1	对操作结果的详细描述信息

## 6.3.12 用户身份信息查询接口

## (1) 接口信息:

接口名称	AccountInfoCheck
接口概述	UDB 提供的接口, 为电信内部的应用系统, 或全国和省 UDB 之间调用;

	提供基于用户身份临时标识的真实信息查询功能。
请求消息名	AccountInfoCheckRequest
应答消息名	AccountInfoCheckResponse

## (2) 参数说明

## 1) 请求消息

AccountInfoCheckRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现频次	说明
Authenticator	String	256	1	认证码, 用于鉴别发送者。 取值 = base64 (3DES(SHA1 (SrcSsDeviceNo + AuthSsDeviceNo + UDBTicket + TimeStamp))), 3DES 采用 UDB 颁发给调用系统的 Key 为密钥
SrcSsDeviceNo	String	16	1	消息发送端的应用系统设备 标识:
AuthSsDeviceNo	String	16	1	目标查询的应用系统设备标 识: 【适用于 ISMP 平台为多个 业务/SP 分别提供请求】
UDBTicket	String	64	1	UDB 通过重定向方式返回给 应用系统的 UDBTicket
TimeStamp	String	19	1	时间戳: 时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区
ReturnSsInfo	Integer	1	0-1	返回其他应用系统的状态数 组信息 0: 不返回【默认】 1: 返回

UDB 接收到该请求后, 应该按照 Authenticator 参数的原始签名加密的处  
理方式, 对接收到的相应参数再做一次相同的签名加密处理, 得到一个  
Authenticator'。若两者结果一致, 则表示传送消息没有被篡改, 进行正常响应。

## 2) 响应消息

AccountInfoCheckResponse 包含如下参数:

名称	数据类型	长度 (字 节)	出现频次	说明
----	------	-------------	------	----

Result	Integer	2	1	0—成功 其他—失败
UserType	Integer	2	1	用户数据的类型 0: 统一帐号 【当 UserType=0 时, 无须传送 ReturnUserGroupList 数组信息; 当查询对象是全国 UDB, 只需要传送 UserID, 当查询对象是电信应用系统, 则可携带用户状态等信息】 1: 用户数组 【UAM 提供的包含客户、产品帐号的数组, 当 UserType=1 时, 只需要传送 ReturnUserGroupList 数组信息, 其他不传】
ReturnUserGroupList	ReturnUserGroup	—	0-1	用户数组信息
UserID	String	40	0-1	用户统一帐号
PUserID	String	11	0-1	用户唯一标识位
Alias	String	40	0-1	别名
BindingAccessNo	String	40	0-1	绑定的宽带接入 ID 【该项只对注册成统一帐号的宽带用户, 且登录电信自营应用才有效】
ThirdSsUserID	String	40	0-1	绑定的第三方应用系统的原用户帐号 ID 【该项只对第三方应用才有效】
UserIDStatus	String	2	0-1	统一帐号状态
UserIDSsStatus	String	2	0-1	用户在该应用系统注册状态: 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务停用/业务注销 5: 其他 【应用系统可根据实际需要, 选择是否使用该参数】
UserPayType	String	2	0-1	用户付费类型: 1: 后付费用户

				2: 预付费用户
PrePaySystemNo	String	14	0-1	预付费用户，需提供此字段，表明在哪个预付费系统扣费
ReturnSslInfoList	ReturnSslInfo	—	0-1	应用系统相关信息
Description	String	128	0-1	对认证请求结果的详细描述信息

ReturnUserGroup 定义如下：

参数名称	数据类型	长度（字节）	出现频次	说明
UserIDType	String	2	0-n	用户帐号的类型
UserID	String	40	0-n	用户帐号

ReturnSslInfo定义如下：

参数名称	数据类型	长度（字节）	出现频次	说明
SsType	String	4	0-n	应用系统类型
UserIDSsStatus	String	2	0-n	统一帐号对该业务的注册状态 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务注销/停用 5: 其他
UserIDSsLoginStatus	String	2	0-n	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他

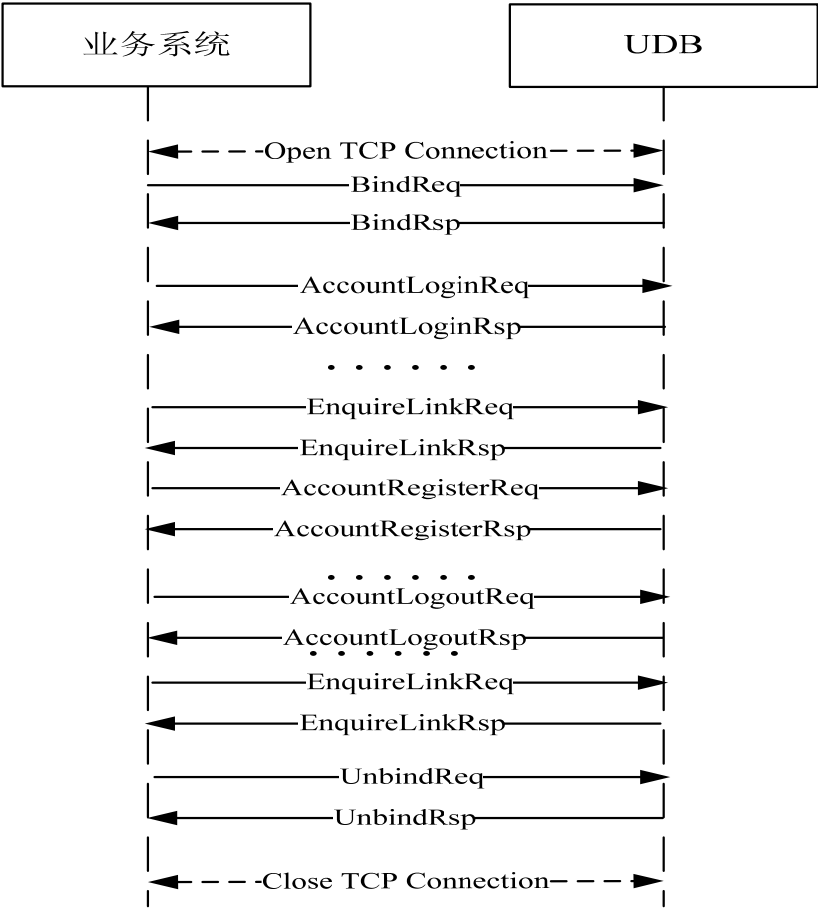
## 6.4 ISAP 接口

### 6.4.1 接口概述

ISAP（Integrated Service Access Protocol）是 UDB 和各业务平台之间，建立在 TCP 连接上，基于协议数据单元（PDUs）交换认证的接口。交互流程如下：

各应用系统作为客户端应先建立与 UDB 的 TCP 连接，然后 ISAP 协议的双方在会话期间开始交换 PDUs。当 TCP 连接上没有信息交换的时候，双方应该

每 C 分钟相互发送 EnquireLinkReq PDUs，以保持连接。如果在 T 秒之后，仍然没有响应信息回复，发送方应该再一次发送 EnquireLinkReq PDUs。如果在发送方发送 N-1 条 EnquireLinkReq PDUs 到另一方之后，仍然没有响应信息回复，发送方应该关闭连接。在提供的系统中应该可以设定 C，T，N 的值。建议 C 的典型值为 60 秒，T 为 60 秒，N 为 3 次。



6.4.2 编码定义

Command ID 定义:

命令字	值	描述
BindReq	0x11000001	连接，用于建立从应用系统到 UDB 的加密连接
BindRsp	0x81000001	响应消息
UnbindReq	0x11000002	去连接，一个安全的断链消息以清除连接资源资源
UnbindRsp	0x81000002	响应消息
EnquireLinkReq	0x11000003	用于维持UDB和应用系统之

		间的TCP连接
EnquireLinkRsp	0x81000003	响应消息
AccountLoginReq	0x11000031	登录认证请求
AccountLoginRsp	0x81000031	响应消息
AccountBindReq	0x11000034	帐号绑定
AccountBindRsp	0x81000034	响应消息
AccountSsStatusRefreshReq	0x11000035	业务注册状态通知请求
AccountSsStatusRefreshRsp	0x81000035	响应消息
StdGetPasswordReq	0x11000036	短信密码获取请求
StdGetPasswordRsp	0x81000036	响应消息
AccountSsPWRefreshReq	0x11000037	业务密码设置请求
AccountSsPWRefreshRsp	0x81000037	响应消息
AccountInfoQueryReq	0x11000038	帐号信息查询请求
AccountInfoQueryRsp	0x81000038	响应消息
AccountInfoRefreshReq	0x11000039	帐号信息更新请求
AccountInfoRefreshRsp	0x81000039	响应消息
AccountInfoConfirmReq	0x11000040	帐号验证及短信通知请求
AccountInfoConfirmRsp	0x81000040	响应消息
AccountSsLoginStatusRefreshReq	0x11000041	业务在线状态通知请求
AccountSsLoginStatusRefreshRsp	0x81000041	响应消息
AccountInfoCheckReq	0x11000042	身份信息查询请求
AccountInfoCheckRsp	0x81000042	响应消息

### 6.4.3 基本数据类型

名称	描述
Unsigned Integer	无符号整数。
Integer4	4字节整数。
Integer2	2字节整数。
Integer1	单字节整数。
Octet String	固定长度串，不足长度则右补二进制0，此类型字符串定义的最大长度不包括结束符'\0'的长度。
C-Octet String	以'\0'结束的C类型字符串。

TLV String	TLV方式定义的字符串类型，此类型不需要带结束符“\0”，长度以TLV中的Length的值为准。对于所有TLV String的字段，在ISAP协议接口传输时不能省略是必填必传参数，即使为空也要传递一个空值参数。
------------	-----------------------------------------------------------------------------------------------------------

#### 6.4.4 PDU概述

所有 PDUs 包括一个消息头和一个消息体。

PDU的组成	描述
Message Header	消息头。
Message Body	消息体。

消息头定义：

名称	类型	字节大小	描述
TotalLength	Unsigned Integer	4	一个PDU的总字节数包括这一字段的4个字节。
CommandId	Unsigned Integer	4	命令标识符。
SequenceId	Unsigned Integer	4	用于请求和响应间保持联系的序号。

可选或者变长参数：

TLV 参数可用于表示 ISAP 消息中的非必须携带的参数以及可变长度的参数。全部 TLV 参数必须出现在 PDU 的尾部。

TLV 字段的定义：

名称	类型	字节大小	描述
Tag	Integer	2	字段的标签
Length	Integer	2	字段的长度
Value	Octet String	可变长度	字段内容

TLV 参数都有一个 Tag 编码， ISAP 协议 TLV 参数定义如下：

TLV 参数	Tag	Length	Value	描述
ReturnSsInfoList	0x0001	8*n	认证接口返回的应用系统信息数组	8 为应用系统信息的字节长度： (ssType+UserIDSsStatus+UserIDSsLoginStatus)， n 为应用系统个数

NormalPassword	0x0002	≤64	新通用密码值	64 为 Value 字段的最大长度
OldNormalPassw ord	0x0003	≤64	原通用密码值	64 为 Value 字段的最大长度
ExtPassword	0x0004	≤64	扩充密码值	64 为 Value 字段的最大长度
SsPassword	0x0005	≤64	新业务密码值	64 为 Value 字段的最大长度
OldSsPassword	0x0006	≤64	原业务密码值	64 为 Value 字段的最大长度
SsStatusList	0x0007	≤ 116*n	应用系统信息 数组	116 为每个应用系统信息的最大长度： ( SsType+ ThirdSsUserID+ UserIDSsStatus+ UserIDSsLoginStatus+ SsPWStatus+ SsPWEncryType+ SsPassword) n 为应用系统个数
Description	0x1000	≤128	详细描述内容	详细描述信息, 128 为 Value 字段的最大长度

## 6.4.5 PDU定义

### 6.4.5.1 连接请求

连接请求 (BindReq)

方向：应用系统→ UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发端应用系统类型
SrcSsDeviceNo	Octet String	16	发端应用系统设备标识
DestSsType	Octet String	4	目标端应用系统类型
DestSsDeviceNo	Octet String	16	目标端应用系统设备标识
AuthenticatorSo	Octet String	16	该域用来对发端进行鉴权。



urce			它生成的 MD5 加密算法如下： 发端认证号码=发端应用系统设备标识+共享密钥+时间戳 共享密钥由 UDB 分配，时间戳由发端设备生成，格式是： YYYYMMDDHH24MISS，年月日时分秒。
TimeStamp	Octet String	19	时间戳：时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23，时区为东八区
Version	Integer4	4	协议版本。

**连接应答（BindRsp）：**

方向：UDB-&gt;应用系统

参数：见表

名称	类型	字节大小	描述
ResultCode	Integer2	2	结果码，统一定义

**6.4.5.2 链路查询****链路查询请求（EnquireLinkReq）**

方向：应用系统 &lt;-&gt; UDB

参数：无

**链路查询应答（EnquireLinkRsp）**

方向：应用系统 &lt;-&gt; UDB

参数：无

**6.4.5.3 去连接请求****去连接请求（UnbindReq）**

方向：应用系统-&gt; UDB

参数：无

**去连接应答（UnbindRsp）**

方向：UDB-&gt; 应用系统

参数：见表

名称	类型	字节大小	描述
----	----	------	----

ResultCode	Integer2	2	结果码，统一定义
------------	----------	---	----------

#### 6.4.5.4 业务认证请求接口

认证请求(AccountLoginReq)

方向：应用系统→ UDB

参数：见表

名称	类型	字节大小	描述
Authenticator	Octet String	256	认证码，用于鉴别发送者。取值 = base64 (3DES(SHA1 (SrcSsDeviceNo+AuthSsDeviceNo +UserID+Alias+TimeStamp))), 3DES采用UDB颁发给调用系统的Key为密钥
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
AuthSsType	Octet String	4	需要认证的应用系统类型
AuthSsDeviceNo	Octet String	16	需要认证的应用系统设备标识
UserID	Octet String	40	用户统一帐号
Alias	Octet String	40	别名
AuthUserType	Integer2	2	认证用户帐号格式 0：统一帐号【默认】 1：别名认证
AuthPWDDType	Integer2	2	密码鉴权类型： 0：通用/业务密码认证； 1：动态短信密码认证； 2：OTP 密码认证(默认的首选OTP厂商)； 【保留类型，待后续认证功能扩展使用】 3：扩展密码认证； 4：通用+扩展密码认证； 5：通用或者扩展密码认证； 99：其他；
NormalPasswordEncryType	Integer2	2	认证密码加密方法： 0：MD5 加密【默认】

			1: 3DES 9: 明文传送
NormalPassword	TLV String		发送过来的认证密码值
ExtPasswordType	Integer2	2	扩展密码类型: 0: 短信动态密码(UDB 自生成); 1-99: OTP 厂商代码; 100-: 其他
ExtPasswordEncryType	Integer2	2	扩展密码加密方法: 0: MD5 加密【默认】 1: 3DES 9: 明文传送
ExtPassword	TLV String		用户在UDB的扩展密码
TimeStamp	Octet String	19	时间戳: 时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区 用于统计以及动态密码的实效性判断等
ReturnSsInfo	Integer1	1	返回其他应用系统的状态数组信息 0: 不返回【默认】 1: 返回

UDB 接收到该请求后, 应该按照 **Authenticator** 参数的原始签名加密的处理方式, 对接收到的相应参数再做一次相同的签名加密处理, 得到一个 **Authenticator'**。若两者结果一致, 则表示传送消息没有被篡改, 进行正常响应。

认证应答 (AccoutLoginRsp)

方向: UDB→应用系统

参数: 见表

名称	类型	字节大小	描述
ResultCode	Integer2	2	结果码
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
Alias	Octet String	40	别名
BindingAccessNo	Octet String	40	绑定的宽带接入 ID
ThirdSsUserID	Octet String	40	绑定的第三方应用系统帐号: 【对电信内部应用系统认证, 该值可返回空】
UserIDStatus	Octet String	2	用户统一帐号状态

UserIDSsStatus	Octet String	2	用户在该应用系统注册状态： 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务停用/业务注销 5: 其他 【应用系统可根据实际需要，选择是否使用该参数】
UserPayType	Octet String	2	用户付费类型： 1: 后付费用户 2: 预付费用户
PrePaySystemNo	Octet String	2	预付费用户，需提供此字段，表明在哪个预付费系统扣费
ReturnSsInfoList	TLV String		应用系统相关信息
Description	TLV String		可选参数，对操作结果的详细描述信息

ReturnSsInfoList定义如下：

名称	类型	字节大小	描述
SsType	Octet String	4	应用系统类型 与请求消息的 returnSsType对应，与 ThirdSsUserID、UserIDSsStatus三者匹配出现
UserIDSsStatus	Octet String	2	统一帐号对该业务的注册状态 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务注销/停用 5: 其他
UserIDSsLoginStatus	Octet String	2	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他

#### 6.4.5.5 短信密码获取请求

获取密码请求 StdGetPasswordReq

方向：应用系统—> UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
ReqSsType	Octet String	4	申请短信密码的系统类型
ReqSsDeviceNo	Octet String	16	申请短信密码的系统设备标识
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
PWDType	Integer2	2	密码类型： 0：随机密码【默认】 1：通用/业务密码：【该功能主要实现密码查询服务。对应用系统获取密码，则将其密码策略所对应的密码发送】。 2：其他
TimeStamp	Octet String	19	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

## 获取密码响应 StdGetPasswordRsp

方向：UDB→应用系统

参数：见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
ResultCode	Integer2	2	0：开通成功 1：用户未开通（或号码不存在） 2：用户停机 3：用户欠费 5：请求数据异常（时间同步差异大等） 6：失败（其他原因）
PwdLiveTime	Integer4	4	密码有效期： （以秒为单位），与时间戳共同确定失效时间，本域值为 0 表示密码有效期由接收的应用系统维护。
TimeStamp	Octet String	19	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

Description	TLV String		对操作结果的详细描述信息
-------------	------------	--	--------------

#### 6.4.5.6 业务密码设置接口

业务密码设置请求 AccountSsPWRefreshReq

方向：应用系统—> UDB

参数：见表

名称	类型	字节大小	描述
Authenticator	Octet String	256	认证码，用于鉴别发送者。取值 = base64 (3DES(SHA1 (SrcSsDeviceNo+UpdateSsDeviceNo +UserID+PUserID+ThirdSsUserID))), 3DES 采用 UDB颁发给调用系统的Key为密钥
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	更新密码的目标应用系统类型
DestSsDeviceNo	Octet String	16	更新密码的目标应用系统设备标识
UpdateSsType	Octet String	4	需要更新业务密码的系统类型
UpdateSsDeviceNo	Octet String	16	需要更新业务密码的系统设备标识
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
ThirdSsUserID	Octet String	40	用户在第三方系统帐号 【只针对采用帐号绑定的第三方合作平台，否则返回空】
SsPWStatus	Octet String	2	应用系统的密码认证策略 0: 重置通用密码策略 1: 业务密码登录策略
SsPWEncryType	Integer2	2	密码加密方式：【通过明文或可解加密】 1: 3DES 9: 明文传送
SsPassword	TLV String		业务密码的传送值
OldSsPassword	TLV String		原业务密码的传送值

UDB 接收到该请求后，应该按照 Authenticator 参数的原始签名加密的处理方式，对接收到的相应参数再做一次相同的签名加密处理，得到一个

Authenticator’。若两者结果一致，则表示传送消息没有被篡改，进行正常响应。

#### 业务密码设置响应 AccountSsPWRefreshRsp

方向：UDB—>应用系统

参数：见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
ResultCode	Integer2	2	结果码
Description	TLV String		可选参数，对操作结果的描述信息

#### 6.4.5.7 帐号信息查询接口

##### 帐号信息查询请求(AccountInfoQueryReq)

方向：全国 UDB—> 省 UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
QuerySsType	Octet String	4	需要查询帐号信息的系统类型
QuerySsDeviceNo	Octet String	16	需要查询帐号信息的系统设备标识
UserID	Octet String	40	用户统一帐号
Alias	Octet String	40	用户别名
AccessNo	Octet String	40	宽带帐号
QueryUserType	Integer1	1	查询帐号的类型 0：统一帐号 1：用户别名 2：宽带帐号
QueryInfoType	Integer2	2	查询类型： 0：该帐号全部信息 1：该帐号状态查询

##### 帐号信息查询应答 (AccountInfoQueryRsp)

方向：省 UDB—>全国 UDB

参数：见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
UserIDType	Octet String	2	帐号类型，见总体规范
PUserID	Octet String	11	用户唯一标识
ResultCode	Integer2	2	结果码
Alias	Octet String	40	用户别名
ProvinceNo	Octet String	2	归属省
CityNo	Octet String	3	归属地市
AreaCode	Octet String	4	地市区号
CustomerID	Octet String	20	客户 ID（CRM 系统标识）
UserName	Octet String	40	用户姓名
CertificateType	Integer2	2	用户证件类型，见总体规范
CertificateNo	Octet String	40	用户证件号
UserPayType	Octet String	2	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystemNo	Octet String	14	预付费的系统平台号
SerSetType	Octet String	2	套餐属性 【待后续扩展使用】
BindingAccessNo	Octet String	40	【只针对宽带帐号类型用户】绑定的宽带帐号
UserIDStatus	Octet String	2	用户统一帐号状态
NormalPasswordEncryType	Integer2	2	通用密码加密方法：【必须明文或可解加密方式传送】 1：3DES 9：明文传送
NormalPassword	TLV String		通用密码传送值
SsStatusList	TLV String		相关应用系统信息
Description	TLV String		对查询结果的详细描述信息

SsStatusList定义如下：

名称	类型	字节大小	描述
SsType	Octet String	4	应用系统类型
ThirdSsUserID	Octet String	40	绑定的第三方应用系统帐号： 【对电信内部应用系统认证，该值为空】
UserIDSsStatus	Octet String	2	统一帐号对该业务的使用状态 1：业务未开通/业务未注册



			2: 业务开通/业务注册 3: 业务暂停 4: 业务停用/业务注销 5: 其他
UserIDSsLoginStatus	Octet String	2	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他
SsPWStatus	Octet String	2	应用系统的密码认证策略 0: 通用密码（默认值） 1: 业务密码
SsPWEncryType	Integer2	2	业务密码加密方式:【必须明文或可解加密方式传送】 1: 3DES 9: 明文传送
SsPassword	TLV String		可选参数，加密后的密码传送值

#### 6.4.5.8 帐号信息更新接口

帐号信息更新请求 AccountInfoRefreshReq

方向：全国 UDB、门户→ 省 UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
UserID	Octet String	40	用户统一帐号
UserIDType	Octet String	2	帐号类型，见总体规范
UpdateFlag	Octet String	2	更新标识： 0: 全部更新 1: 别名更新（仅更新别名） 2: 通用密码更新 3: 用户状态更新 4: 付费属性更新（付费类型+付费系统号） 5: 套餐属性更新 6: 身份更新（姓名、证件及号码等） 7: 业务信息更新（包括业务密码策略、业务密码设置等）

			8: 别名更新+全部信息上传
Alias	Octet String	40	用户别名
UserName	Octet String	40	用户姓名
CertificateType	Integer2	2	用户证件类型
CertificateNo	Octet String	40	用户证件号
UserPayType	Octet String	2	用户付费类型: 1: 后付费用户 2: 预付费用户
PrePaySystemNo	Octet String	14	预付费的系统平台号
SerSetType	Octet String	2	套餐属性 【待定】
BindingAccessNo	Octet String	40	统一帐号绑定的宽带帐号
UserIDStatus	Octet String	2	用户统一帐号状态
NormalPasswordEncryType	Integer2	2	密码加密方法:【通用密码必须明文或可解加密传送】 1: 3DES 9: 明文传送
NormalPassword	TLV String		新通用密码传送值
OldNormalPassword	TLV String		原通用密码传送值
SsStatusList	TLV String		相关应用系统的信息

SsStatusList定义如下:

名称	类型	字节大小	描述
SsType	Octet String	4	应用系统类型
ThirdSsUserID	Octet String	40	绑定的第三方应用系统帐号: 【对电信内部应用系统认证, 该值为空】
UserIDSsStatus	Octet String	2	统一帐号对该业务的使用状态 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务停用/业务注销 5: 其他
UserIDSsLoginStatus	Octet String	2	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他
SsPWStatus	Octet String	2	应用系统的密码认证策略 0: 通用密码 (默认值)

			1: 业务密码
SsPasswordEncryType	Integer2	2	业务密码加密方式:【业务密码必须明文或可解加密通知】 1: 3DES 9: 明文传送
SsPassword	TLV String		加密后的密码传送值
OldPassword	TLV String		加密后的原密码传送值

#### 帐号信息更新响应 AccountInfoRefreshRsp

方向: 省 UDB—>全国 UDB、门户

参数: 见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
ResultCode	Integer2	2	结果码
Description	TLV String		对更新结果的详细描述信息

### 6.4.5.9 外部帐号绑定接口

#### 绑定请求 BindAccountReq

方向: 应用系统—> UDB

参数: 见表

名称	类型	字节大小	描述
Authenticator	Octet String	256	认证码, 用于鉴别发送者。取值 = base64 (3DES(SHA1 (SrcSsDeviceNo+BindSsDeviceNo +UserID+PUserID+TimeStamp))), 3DES采用UDB颁发给调用系统的Key为密钥
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
BindSsType	Octet String	4	需要帐号绑定的应用系统类型
BindSsDeviceNo	Octet String	16	需要帐号绑定的应用系统设备标识
UserID	Octet String	40	用户在UDB的统一帐号
PUserID	Octet String	11	用户唯一标识位
ThirdSsUserID	Octet String	40	绑定的第三方应用系统的原用

			户帐号 ID
SsPWEncryType	Integer2	2	业务密码加密方式：【必须通过明文或可解加密方式通知】 1: 3DES 9: 明文传送 【若为第三方采用 OTP 等密码方式，则绑定可不传业务密码】
SsPassword	TLV String		业务密码的（加密）传送值
BindType	Integer1	1	操作类型： 0: 解绑； 1: 绑定
TimeStamp	Octet String	19	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区
BindEffectMode	Integer1	1	绑定生效模式： 0: 默认实时绑定 1: 下月 1 号绑定(根据时间戳判断) 2: 次日绑定(根据时间戳判断) 3: 指定时间绑定(指定 EffectTimeStamp 作为绑定生效时间) 4: 其他
EffectTimeStamp	Octet String	19	帐号绑定生效时间：时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区，RefreshEffectMode=3 时有效，注册状态生效模式为其他值时无效，可为空

UDB 接收到该请求后，应该按照 Authenticator 参数的原始签名加密的处理方式，对接收到的相应参数再做一次相同的签名加密处理，得到一个 Authenticator'。若两者结果一致，则表示传送消息没有被篡改，进行正常响应。

#### 绑定响应 BindAccountRsp

方向：UDB→应用系统

参数：见表

名称	类型	字节大小	描述
ResultCode	Integer2	2	结果码
UserID	Octet String	40	用户统一帐号

PUserID	Octet String	11	用户唯一标识位
Description	TLV String		对绑定结果的详细描述信息

#### 6.4.5.10 业务注册状态通知

业务注册状态通知请求(AccountSsStatusRefreshReq)

方向：应用系统→ UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
UpdateSsType	Octet String	4	需要更新业务注册的应用系统类型
UpdateSsDeviceNo	Octet String	16	需要更新业务注册的应用系统设备标识
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识
UserIDSsStatus	Octet String	2	统一帐号对该业务的使用状态 1: 业务未开通/业务未注册【此项不主动通知】 2: 业务开通/业务注册 3: 业务暂停 4: 业务注销/停用 5: 其他
TimeStamp	Octet String	19	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区, 用于标明发送端发起的状态更新时间
RefreshEffectMode	Integer1	1	注册/注销状态生效模式: 0: 实时更新【默认】 1: 下月 1 号更新(根据时间戳判断) 2: 次日更新(根据时间戳判断) 3: 指定时间更新(指定 EffectTimeStamp 作为更新生效时间) 4: 其他

EffectTimeStamp	Octet String	19	状态更新生效时间： yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八 区， <b>RefreshEffectMode=3</b> 时 有效，注册状态生效模式为其他 值时无效，可为空
-----------------	--------------	----	----------------------------------------------------------------------------------------------------------------------------

#### 业务注册状态通知响应(AccountSsStatusRefreshRsp)

方向：UDB—>应用系统

参数：见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识
ResultCode	Integer2	2	结果码
Description	TLV String		对绑定结果的详细描述信息

#### 6.4.5.11 业务在线状态通知

##### 业务在线状态通知请求(AccountSsLoginStatusRefreshReq)

方向：应用系统—> UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
UpdateSsType	Octet String	4	需要更新业务在线状态的应用 系统类型
UpdateSsDeviceNo	Octet String	16	需要更新业务在线状态的应用 系统设备标识
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识
UserIDSsLoginStatus	Octet String	2	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他
TimeStamp	Octet String	19	时间戳yyyy-MM-dd HH:mm:ss, 其中HH取值为00-23,时区为东 八区，用于标明发送端发起的状

			态更新时间
--	--	--	-------

**业务在线状态通知响应(AccountSsLoginStatusRefreshRsp)**

方向：UDB→应用系统

参数：见表

名称	类型	字节大小	描述
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识
ResultCode	Integer2	2	结果码，统一定义
Description	TLV String		对通知结果的详细描述信息

**6.4.5.12 帐号验证及短信申请****帐号验证及短信通知请求(AccountInfoConfirmReq)**

方向：应用系统→UDB

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
UserID	Octet String	40	用户统一帐号
SmsPwdFlag	Integer1	1	是否通过短信下发通用密码 【UDB 只允许对指定业务平台 (如 189 邮箱或天翼客户端) 提供该接口功能】 0: 不发送【默认值】 1: 发送通用密码
TimeStamp	Octet String	19	时间戳: yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23, 时区为东八区 用于标明应用系统发送请求的时间

**帐号验证及短信通知响应(AccountInfoConfirmRsp)**

方向：UDB→应用系统

参数：见表

名称	类型	字节大小	描述
----	----	------	----

UserID	Octet String	40	用户统一帐号
ResultCode	Integer2	2	结果码
UserIDStatus	Octet String	2	统一帐号状态
Description	TLV String		对注册鉴权判断的详细描述信息

#### 6.4.5.13 安全密钥通知接口

##### 安全密钥更新请求(SecurityKeyRefreshReq)

方向：全国 UDB—>省 UDB 或 省 UDB—>业务系统

参数：见表

名称	类型	字节大小	描述
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
EncryType	Integer2	2	加密方法：【密钥必须通过明文或可解加密方式通知 UDB】 1：3DES 9：明文传送
UpdateKeyValue	Octet String	256	密钥传送值
UpdateMode	Integer1	1	密钥更新类型： 0：正常更新【默认】 1：紧急更新
TimeStamp	Octet String	19	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区 用于标明发送端发起的状态更新时间

##### 安全密钥更新响应(SecurityKeyRefreshRsp)

方向：省 UDB—>全国 UDB 或 业务系统—>省 UDB

参数：见表

名称	类型	字节大小	描述
ResultCode	Integer2	2	结果码
Description	TLV String		对安全密钥更新结果的详细描述信息



#### 6.4.5.14 用户身份信息查询接口

##### 用户身份信息查询请求(AccountInfoCheckReq)

方向：应用系统—> UDB

参数：见表

名称	类型	字节大小	描述
Authenticator	Octet String	256	认证码，用于鉴别发送者。取值 = base64 (3DES(SHA1 (SrcSsDeviceNo + AuthSsDeviceNo + UDBTicket + TimeStamp)))，3DES 采用 UDB 颁发给调用系统的 Key 为密钥
SrcSsType	Octet String	4	发送端应用系统类型
SrcSsDeviceNo	Octet String	16	发送端应用系统设备标识
DestSsType	Octet String	4	目标应用系统类型
DestSsDeviceNo	Octet String	16	目标应用系统设备标识
AuthSsType	Octet String	4	需要认证的应用系统类型
AuthSsDeviceNo	Octet String	16	需要认证的应用系统设备标识
UDBTicket	Octet String	64	UDB 通过重定向方式返回给应用系统/全国 UDB 的 Ticket 信息
TimeStamp	Octet String	19	时间戳：时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23，时区为东八区
ReturnSsInfo	Integer1	1	返回其他应用系统的状态数组信息 0：不返回【默认】 1：返回

UDB 接收到该请求后，应该按照 Authenticator 参数的原始签名加密的处理方式，对接收到的相应参数再做一次相同的签名加密处理，得到一个 Authenticator'。若两者结果一致，则表示传送消息没有被篡改，进行正常响应。

##### 认证应答 (AccoutInfoCheckRsp)

方向：UDB—>应用系统

参数：见表

名称	类型	字节大小	描述
ResultCode	Integer2	2	结果码
UserType	Integer2	2	用户数据的类型 0：统一帐号 <b>【当 UserType=0 时，无须传送 ReturnUserGroupList 数组信息；当查询对象是全国 UDB，只需要传送 UserID，当查询对象是电信应用系统，则可携带用户状态等信息】</b> 1：用户数组 <b>【UAM提供的包含客户、产品帐号的数组，当UserType=1时，只需要传送 ReturnUserGroupList数组信息，其他不传】</b>
ReturnUserGroupList	TLV String		用户数组组的相关信息
UserID	Octet String	40	用户统一帐号
PUserID	Octet String	11	用户唯一标识位
Alias	Octet String	40	别名
BindingAccessNo	Octet String	40	绑定的宽带接入 ID
ThirdSsUserID	Octet String	40	绑定的第三方应用系统帐号： <b>【对电信内部应用系统认证，该值可返回空】</b>
UserIDStatus	Octet String	2	用户统一帐号状态
UserIDSsStatus	Octet String	2	用户在该应用系统注册状态： 1：业务未开通/业务未注册 2：业务开通/业务注册 3：业务暂停 4：业务停用/业务注销 5：其他 <b>【应用系统可根据实际需要，选择是否使用该参数】</b>
UserPayType	Octet String	2	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystemNo	Octet String	2	预付费用户，需提供此字段，表明在哪个预付费系统扣费

ReturnSsInfoList	TLV String		应用系统相关信息
Description	TLV String		可选参数，对操作结果的详细描述信息

RetrunUserGroup定义如下：

名称	类型	字节大小	描述
UserIDType	Octet String	2	用户帐号的类型
UserID	Octet String	40	用户帐号

ReturnSsInfoList定义如下：

名称	类型	字节大小	描述
SsType	Octet String	4	应用系统类型 与请求消息的 returnSsType对应，与 ThirdSsUserID、UserIDSsStatus三者匹配出现
UserIDSsStatus	Octet String	2	统一帐号对该业务的注册状态 1: 业务未开通/业务未注册 2: 业务开通/业务注册 3: 业务暂停 4: 业务注销/停用 5: 其他
UserIDSsLoginStatus	Octet String	2	统一帐号对该业务的在线状态 1: 用户上线 2: 用户下线 3: 其他

## 7 省 UDB 接口

### 7.1 电信支撑系统接口

#### 7.1.1 接口概述

电信支撑系统是 UDB 的用户数据的基础来源。

UDB 与电信支撑系统(包括 CRM、OCS 等)之间需要进行用户帐号信息的建立、变更、删除等同步传送，实现功能范围包括用户的开通通知（用户类型包括手机用户、固话用户、PHS 用户、宽带用户，及商企用户等），及用户相关的身份信息、状态属性、密码信息、付费属性等的变更通知等。

#### 7.1.2 接口流程

电信运营支撑系统（也即是 IT 系统）包括 CRM、业务开通系统、OCS、10001 服务平台等，而 CRM 不但包括其业务受理和营销功能，也涵盖逐渐加入的多种服务渠道，包括网上营业厅、10000 号客服、自助终端、短信营业厅、WAP 自服务等相关渠道能力。各省分公司对应本章的接口要求，视情况选择相应用户数据源平台进行对接。

##### 7.1.2.1 用户帐号开通流程

**触发条件：**用户在电信营业厅等渠道开通移动手机、固定电话、宽带业务等，省电信支撑系统将用户帐号信息从 CRM 通知给 UDB，生成新用户帐号记录。

**注：**对商企客户的帐号信息，有待集团相关帐号规范定义后再实施。

**交互流程：**

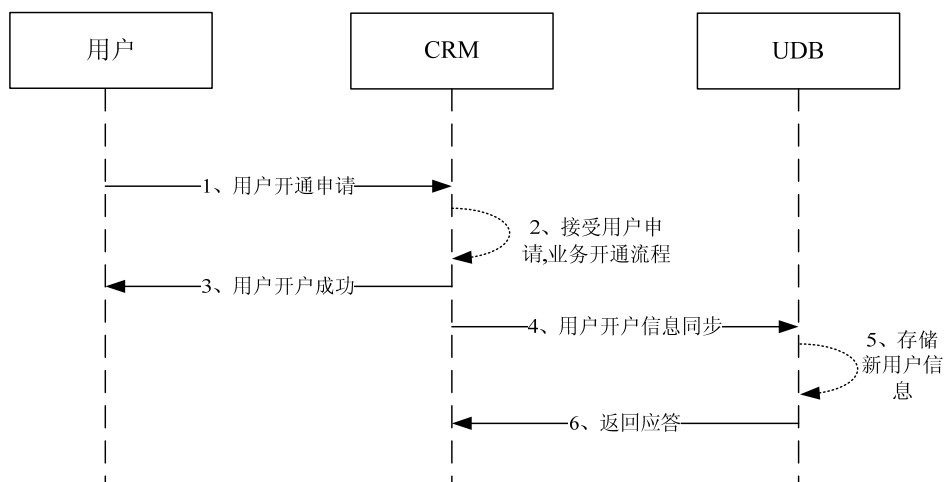


图 7.1-1 用户开户通知流程

**流程描述：**

1. 用户通过中国电信各种销售渠道提交开户申请；
2. CRM 接受用户申请请求，并提交开通流程，记录用户信息；
3. 营业厅等渠道向用户反馈开通结果信息；
4. CRM将新开户信息通知给UDB，调用用户帐号信息同步接口 (CheckFlag=1)；
5. UDB存储新用户信息记录；
6. UDB向CRM系统返回应答消息（如果采用中间表方式该步骤可省略）

**7.1.2.2 帐号信息变更通知**

**触发条件：**移动手机用户、固定电话用户、宽带用户等中国电信基础用户，当其用户状态、服务密码、付费类型、套餐属性、绑定电话号码（针对宽带用户）、证件信息等任何属性信息发生变化时，CRM需要将相关变化信息及时通知UDB。

**交互流程：**

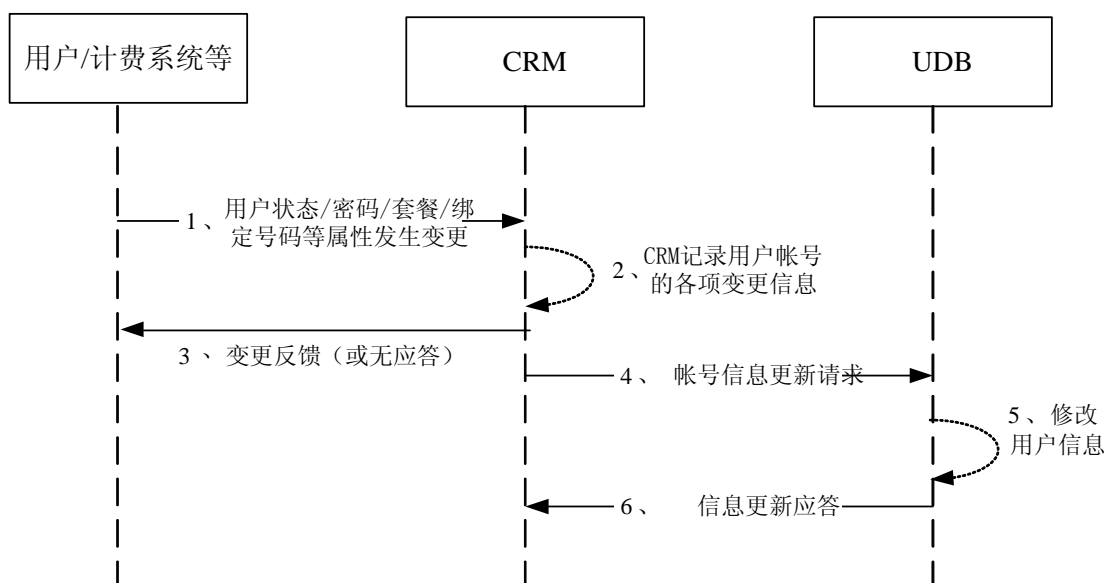


图 7.1-2 用户帐号信息的通知流程

#### 流程描述:

1. 用户主动发起（如挂失/主动停机），或被动触发（如欠费停机），或通过其他渠道，引起了帐号信息的变更；
2. CRM进行用户信息变更记录；
3. 营业厅等渠道向用户反馈变更应答，或无该流程；
4. CRM将新开户信息通知给UDB，调用用户帐号信息同步接口。
5. UDB存储新用户信息记录；
6. UDB向CRM系统返回应答消息（如果采用中间表方式该步骤可省略）

### 7.1.3 接口内容

UDB 与电信支撑系统（CRM 系统）之间接口可采用两种形式：中间接口表方式、实时同步方式（采用 Web Services 协议）。各省可根据支撑系统的实际情况进行接口方式选择：

#### 7.1.3.1 “中间表”同步接口—表格内容

CRM 平台与 UDB 之间可以采用共写“中间表”方式进行帐号信息交互，可基本实现准实时信息同步，减少 UDB 系统对 CRM 系统的实时资源消耗：即

CRM 动态实时把用户帐号信息（包括帐号开通及密码等属性全部更新）写到 CRM 的指定接口中间表，UDB 定期（如每分钟）对该中间表进行查询，并将最新记录信息更新到 UDB 数据库。对于已读取的记录（无论是信息准确或错误），UDB 都应将 CheckFlag 置为“已读取”状态，CRM 定期对“已读取”状态记录进行清除。

对用户帐号信息开通、帐号信息属性更新等可采用同一中间接口表 UserInfoSync，如下所示：

参数名称	数据类型	长度（字节）	出现频次	说明
SerialNumber	Number	20	1	订单流水号 (SerialNumber 字段表示每条记录的插入顺序，自增的 ID 号。表明了每条记录插入的先后顺序)
Coid	String	20	1	订单号，CRM 系统提供的订单标识
CheckFlag	Integer	2	1	<b>读取标识：</b> 0：已读取； 1：新用户/新开户 【所有字段必需传送】； 2：更新全部信息； 3：用户状态变化； 4：服务密码变化； 5：付费类型变化； 6：套餐属性变化； 7：绑定号码编号；（只针对宽带用户） 8：证件信息变化；
TimeStamp	Date		1	时间戳
SrcDeviceNo	String	16	1	CRM 平台号
UserID	String	40	1	用户帐号
UserIDType	String	2	1	帐号类型
ProvinceNo	String	2	0-1	归属省
CityNo	String	3	0-1	归属地市
AreaCode	String	4	0-1	地市区号
CustomerID	String	20	0-1	CRM 的客户 ID 标识
UserName	String	40	0-1	用户姓名
CertificateType	Integer	2	0-1	用户证件类型
CertificateNo	String	40	0-1	用户证件号

UserPayType	String	2	0-1	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystem No	String	14	0-1	预付费用户，需提供此字段， 表明在哪个预付费系统扣费。
SerSetType	String	2	0-1	套餐属性【该字段待定】
BindingTeleNo	String	40	0-1	【只针对宽带帐号类型用户】 绑定的固定电话号码 【含首位为 0 的区号】
UserIDStatus	String	2	0-1	用户帐号状态属性
Password	String	64	0-1	通用服务密码（建议采用明文， 或协商加密算法） 【对宽带帐号，该密码可不传 送，或为空】

由于各省 CRM 系统对帐号类型、地市编码、证件类型、套餐类型、状态属性等均编码格式差异较大，为确保全国 UDB 的用户数据标识统一，各省 UDB 从归属省 CRM 获取用户基础数据时需要进行编码格式转换，请参见第 14 章“UDB 数据编码规范”。

省 UDB 从 CRM 所获得的同步用户信息，如果构建 UDB 自身内部用户数据库，对不同帐号之间关联关系的处理原则及记录信息的合并方法，详细请参考《中国电信用户数据库-功能和设备规范》的相关内容。

### 7.1.3.2 实时同步接口—用户帐号信息同步

(1) 接口信息：

接口协议	Web Service
接口名称	UserInfoSync
接口概述	用户帐号信息同步接口，CRM 调用此接口在 UDB 建立或更新用户帐号信息。
请求消息名	UserInfoSyncRequest
应答消息名	UserInfoSyncResponse

(2) 参数说明

1) 请求消息

UserInfoSyncRequest 包含如下参数：



参数名称	数据类型	长度（字节）	出现频次	说明
SrcDeviceNo	String	16	1	CRM 的平台号
TimeStamp	Date		1	时间戳
CheckFlag	Integer	1	1	<b>读取标识：</b> 1：新用户/新开户； 2：更新全部信息； 3：用户状态变化； 4：服务密码变化； 5：付费类型变化； 6：套餐属性变化； 7：绑定号码变更；（只针对宽带用户） 8：证件信息变化；
UserID	String	40	1	用户帐号
UserIDType	String	2	1	帐号类型
ProvinceNo	String	2	0-1	归属省
CityNo	String	3	0-1	归属地市
AreaCode	String	4	0-1	地市区号
CustomerID	String	20	0-1	客户 CRM 的标识 ID
UserName	String	40	0-1	用户姓名
CertificateType	Integer	2	0-1	用户证件类型
CertificateNo	String	40	0-1	用户证件号
UserPayType	String	2	0-1	用户付费类型： 1：后付费用户 2：预付费用户
PrePaySystemNo	String	14	0-1	预付费用户，需提供此字段，表明在哪个预付费系统扣费。
SerSetType	String	2	0-1	套餐属性【该字段功能待定】
BindingTeleNo	String	40	0-1	【只针对宽带帐号类型用户】 绑定的电话号码 【含首位为 0 的区号】
UserIDStatus	String	2	0-1	用户帐号状态属性
PWEncryType	Integer	2	0-1	密码加密方式：【过明文，或对称加密算法】 1：3DES 9：明文传送
Password	String	64	0-1	密码传送值

## 2) 响应消息

UserInfoSyncResponse 包含如下参数：

名称	数据类型	长度（字节）	出现频次	说明
UserID	String	40	1	用户帐号
UserIDType	String	2	1	帐号类型
ResultCode	Integer	2	1	结果码，统一定义
Description	String	128	0-1	对帐号信息同步结果的描述信息

### 7.1.4 对支撑系统的要求

UDB 上线初期，要求省公司电信支撑系统应一次性将本省用户数据信息按标准格式导入到省 UDB。后续除了新开用户通知外，电信支撑系统要求做到实时/准实时将用户相关属性变更通知给归属省 UDB。

支撑系统与 UDB 之间接口不能堵单，并支持批量停开机。

为了支持省公司客服密码、应用密码和接入密码的统一，省公司可考虑 CRM（或 UAM）适当开放密码修改同步的接口供 UDB 调用，或通过中间表方式通知 CRM 更改客服密码。

## 7.2 宽带接入系统接口

UDB 可为省固网宽带接入系统（ADSL 和 LAN），和无线宽带接入系统（WLAN）提供基于统一帐号及通用密码登录的用户集中认证服务。

### 7.2.1 宽带接入的UDB集成方案

#### 7.2.1.1 固网 AAA—UDB 的集成方案

为实现采用统一帐号的固网宽带接入认证与原宽带帐号的固网宽带接入认证的区分，并减少对现有 AAA 改造的影响，建议对统一帐号的固网宽带接入 AAA 单独设置 Radius 服务器（本规范暂命名为新 AAAfor189），并且 UDB 只与该台 Radius 服务器进行对接，采用 Radius 协议进行消息交互。

UDB 支持 Radius 协议，直接参与固网接入系统 AAA 流程的 Authentication 工作，记录宽带用户上下线状态，并实现宽带接入—应用系统的单点登录功能。

考虑到现有固网宽带接入系统支持预付费的情况各省不统一，统一帐号的固网宽带接入是否支持预付费形式，由各省的现有固网宽带接入系统能力来决定（如 AAA 系统是否实现了与 OCS 的查询功能接口等）：如果现有固网宽带接入支持预付费形式的话，则省内也可支持预付费手机号码的宽带登录服务。

对省内宽带接入系统的配合调整，可根据省内特点自行选择以下方案：

#### 方案一：基于统一后缀(@189.cn)的统一帐号接入方案

BRAS 根据认证请求的帐号后缀，对所有后缀为@189.cn 域名的帐号请求全部转发给新 AAAfor189，其他的帐号请求仍转发给原 AAA 系统。该方案的特点是对现有 AAA 基本不做改动，完全由 BRAS 来识别和转发统一帐号的请求。

UDB 负责统一帐号及密码的认证功能。新 AAAfor189 主要负责统一帐号的宽带接入鉴权、计费等工作，与 UDB 一起完成完整的 AAA 服务功能。

E家客户端

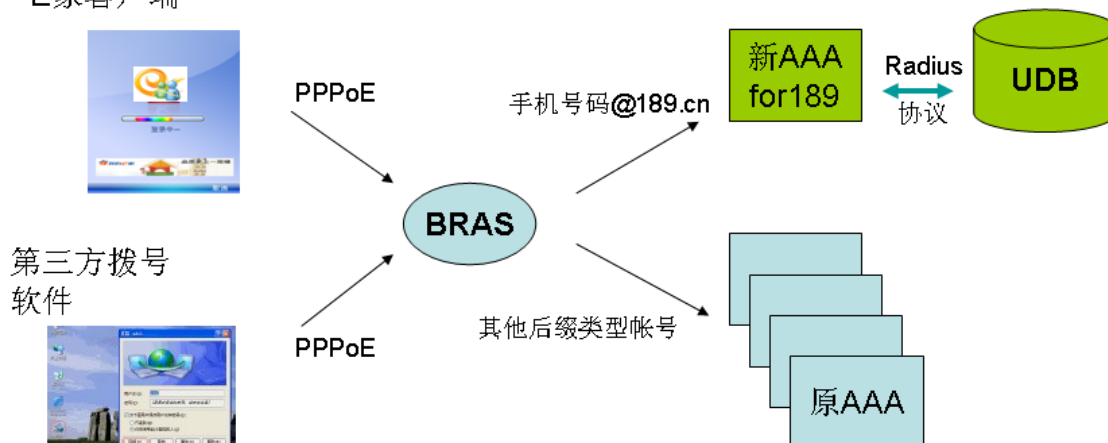


图 7.2-1 固网宽带接入登录的认证方案（方案一）

#### 对用户拨号客户端的相关要求

客户端软件应对用户输入的统一帐号格式进行@189.cn后缀添加，以确保BRAS能正确路由转发：

- 目前E家客户端（天翼Live客户端）的用户登录帐号都统一为“统一帐号@189.cn”格式，但用户只需输入统一帐号（手机号码），客户端通过PPPoE向BRAS发送“统一帐号@189.cn”格式的认证请求；
- 对用户使用的第三方拨号软件，需要用户在拨号时输入的统一帐号格式为“统一帐号@189.cn”。

## 方案二：基于统一帐号的宽带接入方案

无论是 E 家客户端，还是用户使用的第三方拨号软件，用户只输入中国电信统一帐号（如 CDMA 手机号码、区号+固定电话号码等），现有 AAA 能有效识别统一帐号的认证请求，并全部转发给新 AAAfor189 进行认证，而对其他帐号认证请求则由现有 AAA 自行处理。该方案特点是对客户端/市场宣传比较简单，且省内现有 AAA 具备识别统一帐号及认证转发的能力。

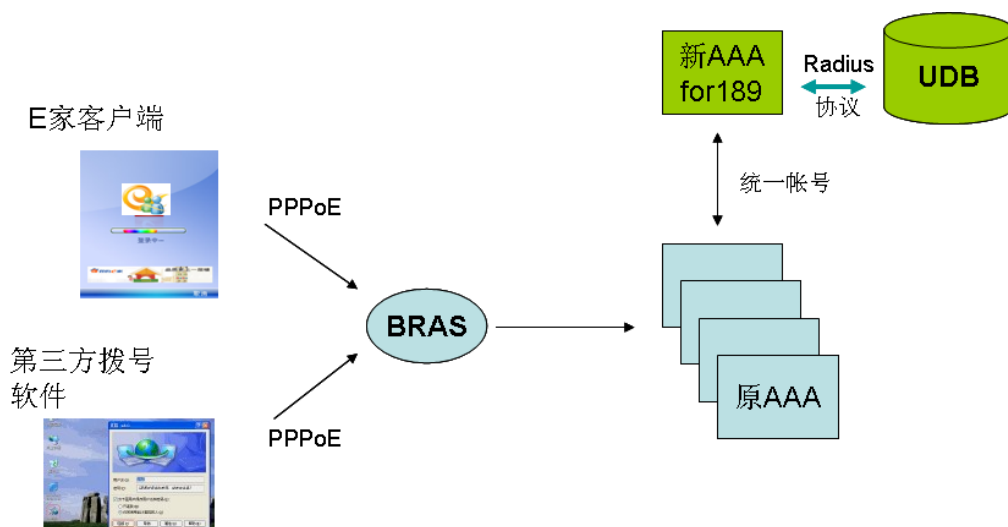


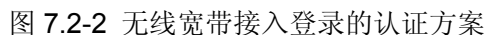
图 7.2-2 固网宽带接入登录的认证方案（方案二）

### 7.2.1.2 WLAN AAA—UDB 的集成方案

对于现有WLAN Portal门户的无线宽带接入，可根据省内实际部署需要，基于UDB支持统一帐号及通用密码认证，以及动态短信密码生成等工作。

对于基于UIM卡认证（如EVDO卡）的无线宽带接入认证，不在本规范定义。

参照中国电信《CDMA用户短信获取密码使用 WiFi参考技术方案》中对WLAN Portal页面要求，所有CDMA手机号码登录WLAN Portal，Portal系统向BRAS认证请求时先自动填加“@CW.省别.chntel.com”域名后缀，如四川省用户则为CDMA号@CW.sc.chntel.com。以下以四川CDMA用户的无线宽带接入为例，简要描述其实现方案：



对于四川省CDMA用户在外省漫游登录场景，用户认证请求将通过WLAN全国漫游中心转发到四川WLAN AAA。WLAN AAA根据域名后缀，将所有CDMA号码@CW.sc.chntel.com帐号认证转发给省内新AAAfor189服务器，其他域名后缀帐号认证在WLAN AAA进行终结认证。

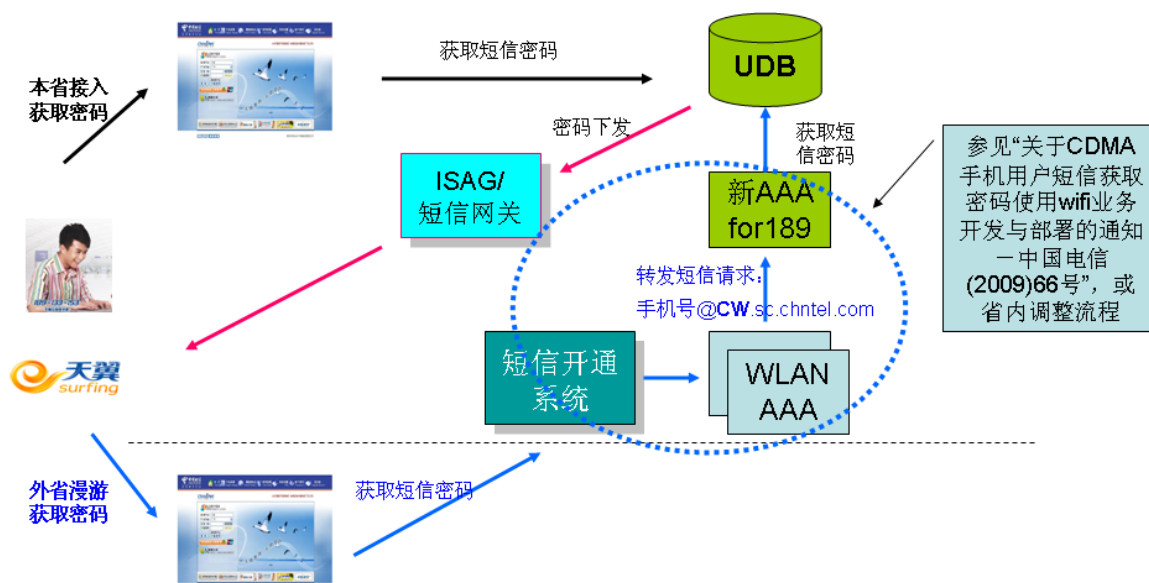


图 7.2-2 无线宽带接入获取短信密码的方案

用户在本省WLAN Portal点击获取密码，则直接Portal向UDB申请动态短信密码；对于用户在外省市漫游，在接入地点点击获取密码，则接入地Portal向归属省短信开通系统申请密码，短信开通系统再向省内WLAN AAA，参见《CDMA用户短信获取密码使用 WiFi参考技术方案》，可再通过新AAAfor189服务器向UDB请求短信密码。各省也可根据实际情况适当精简省内流程和环节，直接由短信开通系统向UDB申请动态密码。

### 1、对 WLAN AAA 的转发要求

对本省用户在全国漫游的情况，省内 WLAN AAA 从全国漫游转发中心获取用户认证请求。WLAN AAA 将原手机号码@CWLAN.省名.tel.com 域名后缀号码的认证，由原来 WLAN AAA 自己认证终结，配置成全部转发给新 AAAfor189 的 Radius 服务器进行认证。同时，WLAN AAA 仍保留其他号码@CWLAN.省名.tel.com 域名后缀号码的终结认证。

### 2、对短信开通系统的改造建议

部分省公司已按集团《关于 CDMA 手机用户短信获取密码使用 wifi 业务开发与部署的通知—中国电信（2009）66 号》文件要求进行了省内短信开通系统平台的建设。为了实现密码的集中分发和集中认证，可对现有短信开通系统改

造，直接与 UDB 通过 Web Services 短信密码获取接口进行对接，不再通过 WLAN AAA 和新 AAAfor189 服务器进行转发。

### 7.2.1.3 对新 AAAfor189 服务器的要求

无论是固网新 AAAfor189 的 Radius 服务器，还是 WLAN 新 AAAfor189 的 Radius 服务器，主要实现两方面功能：

—认证漫游转发功能，将统一帐号（重点是手机号码）的认证请求转发给 UDB，由 UDB 进行身份验证和密码检验，即 Authentication。

—认证终结功能，对 UDB 身份验证之后，由新 AAAfor189 的 Radius 服务器进行 Authorization 鉴权决定用户是否能真正上网，同时也要完成计费操作。

省公司应将所有 CDMA 手机号码开通的固网宽带、无线宽带的帐号信息集中存储新 AAAfor189 的 Radius 服务器。如果省内已开通“区号+固话号码”的宽带接入帐号，也可将所有这些数据集中存储在新 AAAfor189 的服务器。

各省也可根据实际需要，对新 AAAfor189 服务器考虑分别建设漫游转发、认证终结两台 Radius 服务器。即接口关系由“新 AAA（即做转发也做认证终结—UDB”变成“漫游转发 AAA—UDB—认证终结 AAA”。

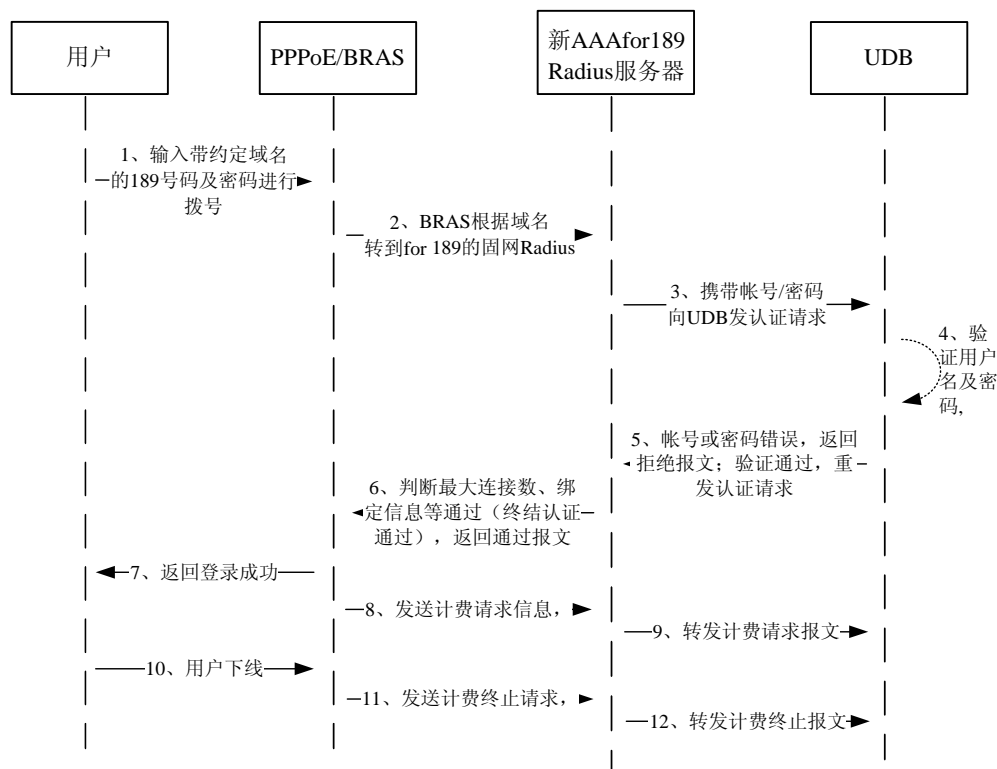
新 AAAfor189 服务器，既可新建，也可利旧现网设备进行改造。

## 7.2.2 接口流程

### 7.2.2.1 统一帐号的固网宽带登录

**触发条件：**用户已开通统一帐号的固网宽带接入业务之后，通过统一帐号进行宽带拨号接入。以下以189用户的拨号（方案一）为例，说明流程：

**交互流程：**



### 流程描述:

1. 用户通过中国电信专用客户端软件（如天翼Live PC版）输入手机号码，或第三方拨号软件输入“手机号码@189.cn”，通用密码，进行拨号；
2. BRAS通过PPPoE客户端传送的帐号后缀域名来判定往哪个固网Radius服务器转发认证请求和计费请求：@189.cn后缀域名的认证请求全转发给新AAAfor189的固网Radius 服务器。
3. 新AAA将认证请求报文转发给UDB，携带手机号码及密码等信息；
4. UDB根据新AAA转发过来的认证请求，完成用户帐号及密码的有效性判断；
5. 如果帐号或密码错误，则直接返回认证拒绝报文；如果验证通过，则把收到的请求报文直接认证转发给新AAA Radius服务器。
6. 新AAA Radius服务器认证根据UDB转发过来的认证请求、判断最大连接数和绑定信息，通过后再将认证结果返回给回给BRAS；
7. BRAS通知用户登陆成功，用户接入网络；
8. BRAS向新AAA Radius服务器发送计费请求报文（新AAA Radius服务器生成话单给营帐计费）；
9. 新AAA同时也向UDB转发一份计费请求报文，不用等待回复；UDB记录该用



户的固网宽带上线状态。

10. 当用户下线时，BRAS中断线路；

11. BRAS向终结Radius服务器发送计费请求报文（中止状态）；

12. 新AAA同时也向UDB转发一份计费请求报文（中止状态），不用等待回复；  
UDB同步记录该用户下线状态。

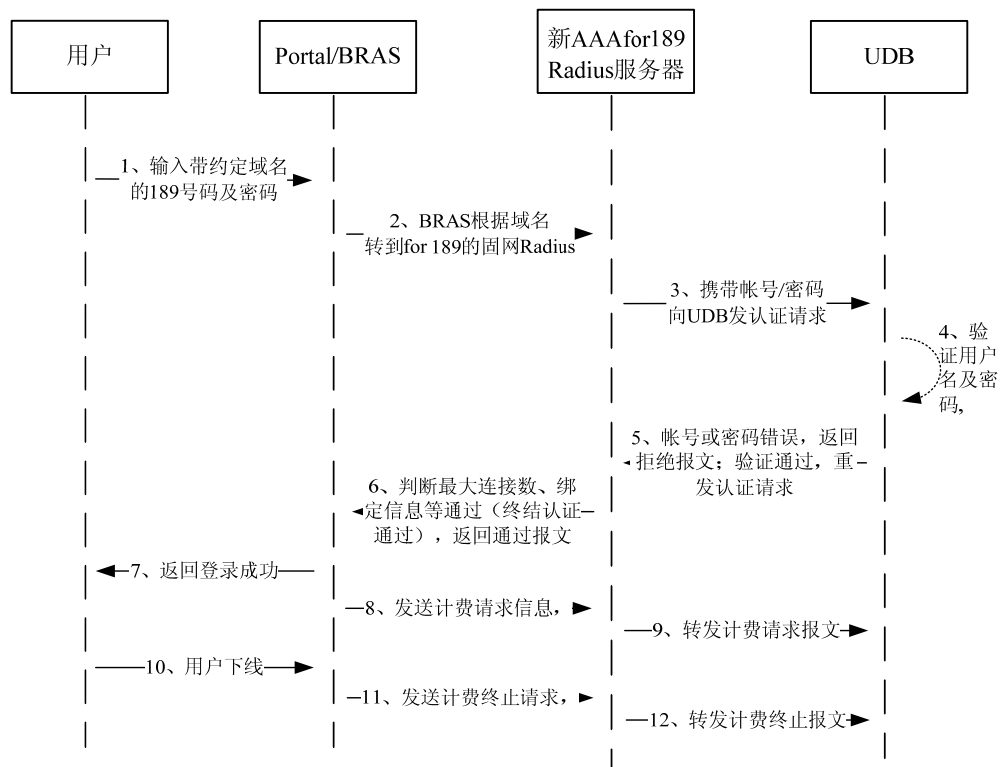
注：UDB 在维护用户在线状态的策略，要与省内 AAA 系统策略保持一致，如多长时间没响应可置位用户下线等。

### 7.2.2.2 统一帐号的无线宽带登录

**触发条件：**用户开通统一帐号的无线宽带接入业务之后，或办理了相应套餐，在本省WLAN Portal页面手机号码和密码进行无线宽带接入。

对于全国漫游的无线宽带接入，则需要通过WLAN全国漫游流程，认证请求会转发到省内WLAN AAA，由WLAN AAA将手机帐号的认证请求转发给新WLAN AAAfor189服务器，新AAAfor189—UDB之间处理流程基本一致，不再描述。

**交互流程：**



**流程描述：**

1. 用户通过中国电信WLAN Portal页面，输入手机号码及密码，进行登录；
2. BRAS通过Portal传送的后缀域名来判定往哪个WLAN Radius服务器转发认证请求和计费请求：“@cw.省别.chntel.com” 后缀域名的认证请求全转发给新WLAN AAAfor189的Radius服务器。
3. 新AAA将认证请求转发给UDB，携带手机号码及密码等信息；
4. UDB根据新AAA转发过来的认证请求报文，完成用户帐号及密码的有效性判断；
5. 如果帐号或密码错误，则直接返回认证拒绝报文；如果验证通过，则把收到的请求报文直接认证转发给新WLAN AAA Radius服务器。
6. 新AAA Radius服务器认证根据UDB转发过来的认证请求、判断最大连接数和绑定信息，通过后再将认证结果返回给回给BRAS；
7. BRAS通知用户登陆成功，用户接入网络；
8. BRAS向新AAA Radius服务器发送计费报文（新WLAN AAA Radius服务器生成话单给营帐计费）；
9. 新WLAN AAA同时也向UDB转发一份计费请求报文，不用等待回复；UDB记录该用户的固网宽带上线状态。
10. 当用户下线时，用户接入链路中断；
11. BRAS向终结Radius服务器发送计费中止报文；
12. 新AAA同时也向UDB转发一份计费请求报文（中止），不用等待回复；UDB同步记录该用户下线状态。

注：UDB 在维护用户在线状态的策略，要与省内 AAA 系统策略保持一致，如多长时间没响应可置位用户下线等。

### 7.2.2.3 无线宽带用户获取短信密码

**触发条件：**用户在 WLAN Portal 页面输入手机号码，并点击获取短信密码；

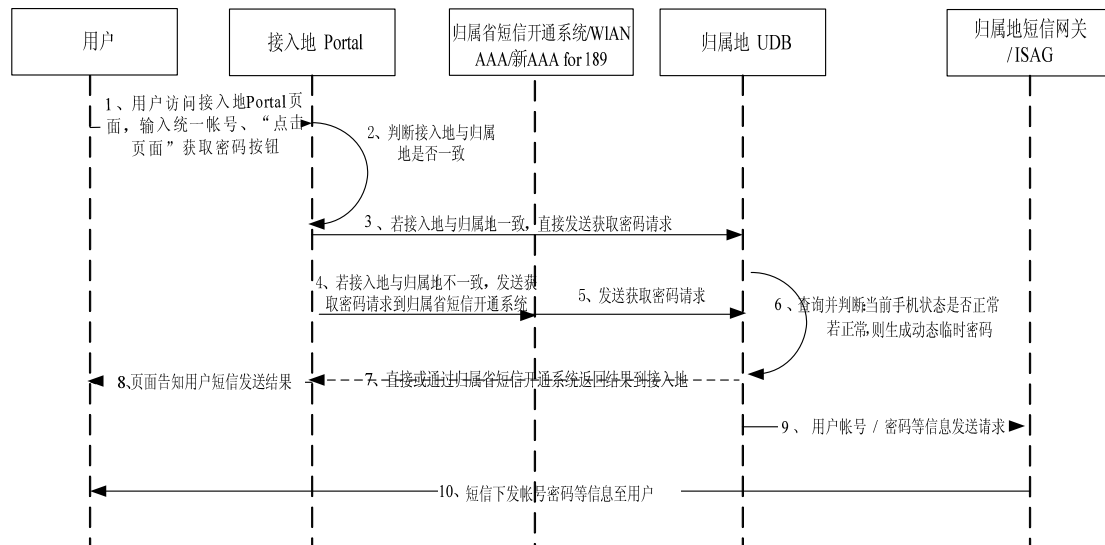
对于 CDMA 用户在本省 Portal 的请求，WLAN Portal 向 UDB 请求生成动态密码，UDB 通过短信网关下发给用户手机。

对于 CDMA 用户在外省接入地 Portal 的请求，则通过接入地 Portal 直接向归属省短信开通系统发送密码获取请求，归属地短信开通系统或直接，或通过新 AAAfor189 向 UDB 请求密码。请参见《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》。

注：若用户在没开通无线宽带接入业务或相关套餐的前提下，则用户使用获取的短信密码登录时，由 WLAN AAA 鉴权不通过时，提示用户进行注册。

流程交互：



流程描述：

1. 用户在接入地Portal帐号区域输入作为统一帐号的CDMA手机号码，选择开户地（如手机号码归属地），输入验证码后点击“获取密码”。
2. 接入地Portal判断接入地与号码归属地是否一致。
3. 如果接入地与归属地一致（属于同一个省），接入地Portal将获取密码的请求通过短信密码获取请求接口直接发往归属地UDB。
4. 如果接入地与归属地不一致，接入地Portal将获取密码的请求发往归属地的短信开通系统。
5. 归属地的短信开通系统根据情况将短信获取密码请求直接发往归属地UDB或通过WLAN AAA与新AAA for 189的服务器转发给归属地UDB（各省根据情况可选择不同途径）。
6. 归属地UDB判断该用户手机号码状态是否正常。若正常，则生成动态临时密码。
7. 归属地UDB将验证结果信息返回给接入地Portal系统（直接返回或通过新AAA for 189、WLAN AAA、归属地的短信开通系统返回）。

8. 接入地Portal通过页面提示用户发送短信密码结果信息。

9. UDB向短信网关/ISAG提交短信发送请求。

短信网关/ISAG 向用户手机发送密码及提示短信。

### 7.2.3 接口内容

短信密码获取请求接口消息，参见公共 Web Service 接口 6.3.3 节。本节重点就新 AAAfor189 服务器—UDB 之间的 Radius 接口协议进行定义。

#### 7.2.3.1 Radius 接口内容描述

新 AAA 服务器和 UDB 之间采用标准的 Radius 协议进行互通。UDB 应该遵循[RFC 2865]、[RFC 2866]、[RFC 2868]、[RFC 2869]和[RFC 3162]定义的规范。BRAS 向 AAA 发送的常用参数如下：

属性名称	类型	描述
User-Name	1	用户统一账号
User-Password	2	用户密码
CHAP-Password	3	CHAP方式用户密码
NAS-IP-Address	4	BRAS的地址
NAS-Port	5	BRAS的端口
Service-Type	6	服务类别
Framed-Protocol	7	
Framed-IP-Address	8	用户IP地址
Framed-IP-Netmask	9	
Framed-Routing	10	
Filter-Id	11	
Framed-MTU	12	
Framed-Compression	13	
Login-IP-Host	14	
Login-Service	15	
Login-TCP-Port	16	
Reply-Message	18	radius返回的消息
Callback-Number	19	
Callback-Id	20	
Framed-Route	22	
Framed-IPX-Network	23	
State	24	

Class	25	
Vendor-Specific	26	用户自定义属性，如集团自定义属性 <b>10000</b>
Session-Timeout	27	可用时长（秒）
Idle-Timeout	28	空闲时长
Termination-Action	29	
Called-Station-Id	30	
Calling-Station-Id	31	
NAS-Identifier	32	BRAS的标识
Proxy-State	33	
Acct-Status-Type	40	
Acct-Delay-Time	41	
Acct-Input-Octets	42	
Acct-Output-Octets	43	
Acct-Session-Id	44	话单唯一性标识
Acct-Authentic	45	
Acct-Session-Time	46	
Acct-Input-Packets	47	
Acct-Output-Packets	48	
Acct-Terminate-Cause	49	
Acct-Multi-Session-Id	50	
Acct-Link-Count	51	
Acct-Input-Gigawords	52	
Acct-Output-Gigawords	53	
Event-Timestamp	55	
CHAP-Challenge	60	CHAP值
NAS-Port-Type	61	用户上网类型
Port-Limit	62	
Login-LAT-Port	63	
NAS-Port-Id	87	线路的端口编码

注：以上为BRAS发来的常见属性，并非全部属性

AAA 服务器和 UDB 服务器应该支持简单 IP RADIUS 属性描述表和计费要求一节定义的属性，属性描述表如下：

属性表	类型	接入—请求	接入—接受	接入—拒绝	接口
User-Name	1	M	M		AAA←→UDB
User-Password	2	O注1			AAA→UDB
CHAP-Password	3	O注2			AAA→UDB
NAS-IP-Address	4	O注3			AAA→UDB
NAS-IPv6-Address	95	O注3			AAA→UDB

s					
CHAP-Challenge	60	O			AAA→UDB
Correlation ID	26/44	M	O		AAA←→UDB
Calling-Station-ID	31	M			AAA→UDB
Always On	26/78		O		AAA←UDB
NAS-Port-Type	61	O注4			AAA→UDB
Carrier-ID	26/142	M			AAA→UDB
NAS-ID	32	O注5			AAA→UDB
Session-Timeout	26		O		AAA←UDB
Reply-Message	18			O	AAA←UDB

(M) 表示必选属性

(O) 表示可选属性

注 1：如果采用 PAP，User-Password 是必选的。

注 2：如果采用 CHAP，CHAP-Password 是必选的。

注 3：至少包括 NAS-IP-Address 或 NAS-IPv6-Address 之一。

注 4：建议包含 NAS-Port-Type，用于多网络接入技术的区分

注 5：在认证和计费请求消息中至少有其一包含 NAS-ID

如果使用 CHAP 或 PAP,AAA 给归属 UDB 发送一个带有 CHAP 或 PAP 认证信息的 RADIUS 接入请求消息 RADIUS Access-Request，这与[RFC 2865]一致。当收到 RADIUS Access-Request 消息时，归属 UDB 应该发送 RADIUS Access-Accept 或者 RADIUS Access-Reject 消息给 AAA 服务器。

对 WLAN 话单格式应符合《中国电信 EV-DO Rev.A 移动通信网设备技术规范—AAA 设备分册》的相关要求。

### 7.2.3.2 Radius 认证请求报文（新 AAA→UDB）

新AAA Radius服务器 -> UDB的请求报文，标准Radius协议报文。

关注的主要协议接口参数有：（PAP与CHAP互斥出现）

属性名称	类型	描述
User-Name	1	用户统一账号
User-Password	2	用户密码（PAP）
CHAP-Password	3	CHAP密码（CHAP）
CHAP-Challenge	60	CHAP挑战值（CHAP）

### 7.2.3.3 Radius 认证拒绝报文（UDB→新 AAA）

UDB认证失败（密码错误或账户状态无效），则返回拒绝报文。

关注的主要协议接口参数有：

属性名称	类型	描述
Reply-Message	18	失败描述

### 7.2.3.4 Radius 认证转发报文（UDB→新 AAA）

UDB认证通过后，将收到的漫游转发Radius服务器请求报文返回给新AAA Radius服务器。

关注的主要协议接口参数有：

属性名称	类型	描述
User-Name	1	用户统一账号
User-Password	2	认证通过后的，新AAA默认该密码为通过。（省内自定义）
User-Status		用户的状态标识（该字段为新扩展字段）

### 7.2.3.5 Radius 计费请求报文（新 AAA→UDB）

BRAS 向新 AAA Radius 服务器发送计费请求报文，同时新 AAA 也向 UDB 转发以下该报文，以便 UDB 记录上线状态。

属性名称	类型	描述
User-Name	1	用户统一账号
Acct-Status-Type	40	1 Start: 上线 2 Stop: 下线 3 Interim-Update: 在线更新 7 Accounting-On: 计费开始 8 Accounting-Off: 计费结束

## 7.3 电信自营应用系统接口

电信自营应用系统，是指中国电信自运营自建设的应用系统。省 UDB 可为省内应用系统提供统一帐号登录的认证服务，如省内互联星空、超级信使、信息港、商企平台、号百平台、IPTV 等。

本节重点就省 UDB 与省内应用系统对接的通用流程和接口进行规范，对有特殊功能要求的应用系统可基于以下流程及接口进行扩展。

### 7.3.1 接口概述

UDB 为应用系统主要提供统一帐号用户登录的认证服务，并将认证结果及用户状态等信息反馈给应用系统，由应用系统根据认证结果及状态策略进行业务鉴权，以决定是否允许用户登录。应用系统需将用户注册状态、在线状态，及业务密码设置等通知 UDB。

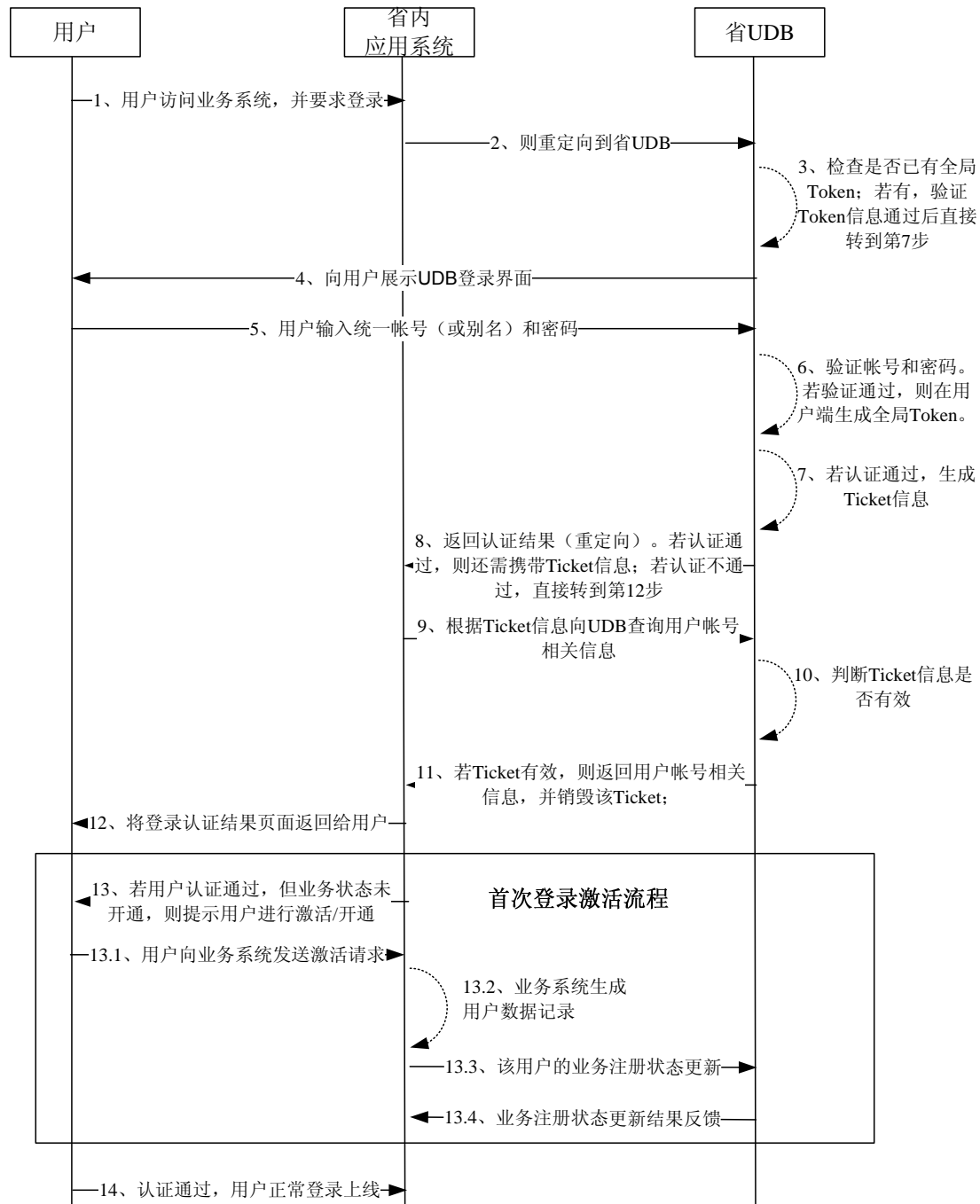
### 7.3.2 接口流程

#### 7.3.2.1 用户登录应用系统

##### 1、重定向认证流程

**触发条件：**用户访问应用系统，并点击其门户网站的“登录”或“通行证登录”，应用系统将重定向到UDB的统一认证界面。





### 流程描述：

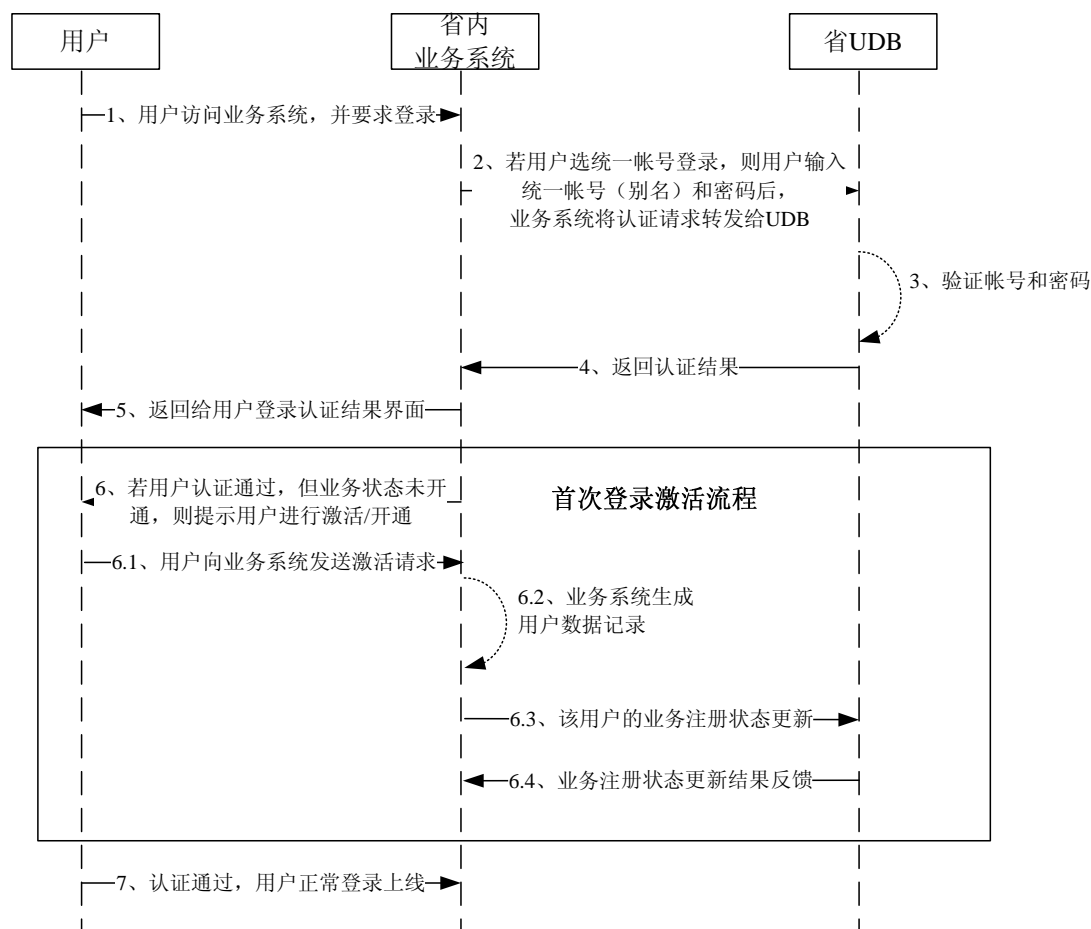
1. 用户访问应用系统；
2. 若用户选择登录或通行证登录，应用系统登录将重定向到UDB；
3. UDB检查重定向是否有携带用户全局Token信息；若已存在全局Token，则对Token信息进行验证，验证通过后直接转到第7步；
4. UDB向用户展示UDB的统一认证登录界面；
5. 用户输入统一帐号（或别名）和密码，并点击登录；

6. UDB验证用户帐号和密码信息；若验证通过，则生成全局Token，在用户端写内存Cookie，具体流程参见10.2.1；
7. 若认证通过，UDB生成Ticket信息；
8. UDB重定向并返回认证结果信息到应用系统；若认证通过，则重定向消息中还需携带Ticket消息；若认证未通过，则直接转到第12步；
9. 应用系统根据Ticket信息向UDB查询用户帐号相关信息；
10. UDB判断应用系统传过来的Ticket是否有效；
11. 若Ticket有效，UDB向应用系统返回用户帐号相关信息；同时UDB销毁该Ticket；
12. 应用系统向用户展示登录认证结果页面；
13. 如果用户认证通过,但该用户尚未注册,则需要用户注册/激活,可参照7.3.2.4相关流程，成功后允许用户登录；
14. 认证通过，则允许用户正常登录。

## 2、SOAP认证流程

**触发条件：**用户访问应用系统，并在其门户网站的登录框直接输入统一帐号和密码，应用系统通过后台SOAP方式向UDB进行认证请求。

**交互流程：**



### 流程描述：

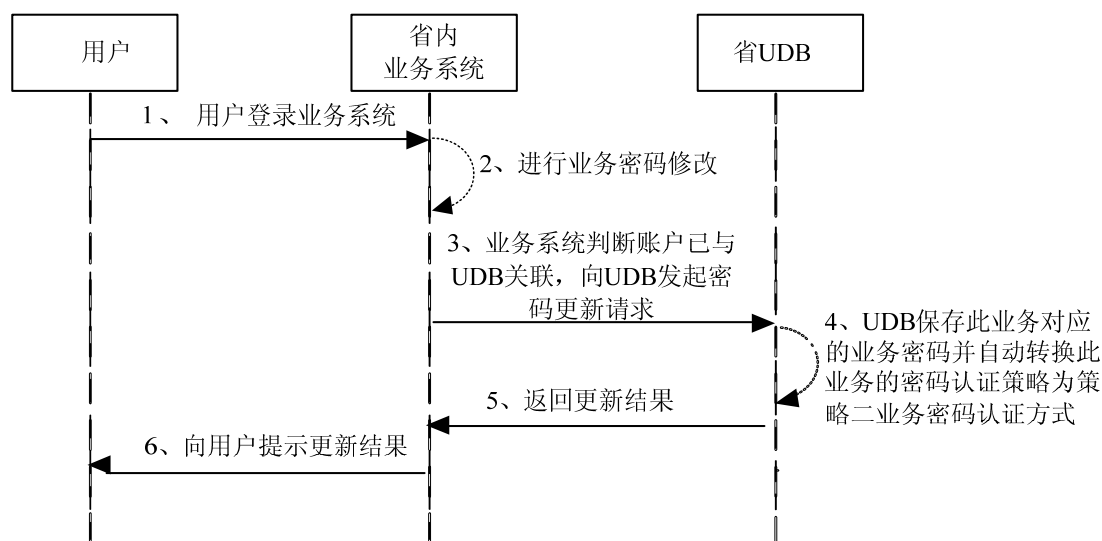
1. 用户访问应用系统，并要求登录；
2. 若用户选择统一帐号登录，则用户输入统一帐号（或别名）和密码后，应用系统将这个认证请求转发给UDB；
3. UDB验证用户帐号和密码信息；
4. UDB返回认证结果信息到应用系统；
5. 应用系统向用户展示登录认证结果界面；
6. 如果用户认证通过，但该用户尚未注册，则需要用户注册/激活，可参照7.3.2.4相关流程，成功后允许用户登录；
7. 认证通过，则允许用户正常登录。

### 7.3.2.2 业务密码设置流程

**触发条件：**

用户正常登录应用系统之后，通过应用系统提供的业务密码修改功能进行业务密码设置，和登录密码策略设置，并通知 UDB 进行记录。

**适用范围：**只有与 UDB 之间通过 SOAP/ISAP 协议认证请求的电信自营应用系统，才需要考虑设置业务密码的场景；对采用重定向认证的应用系统，可不提供该流程和接口。

**交互流程：****流程描述：**

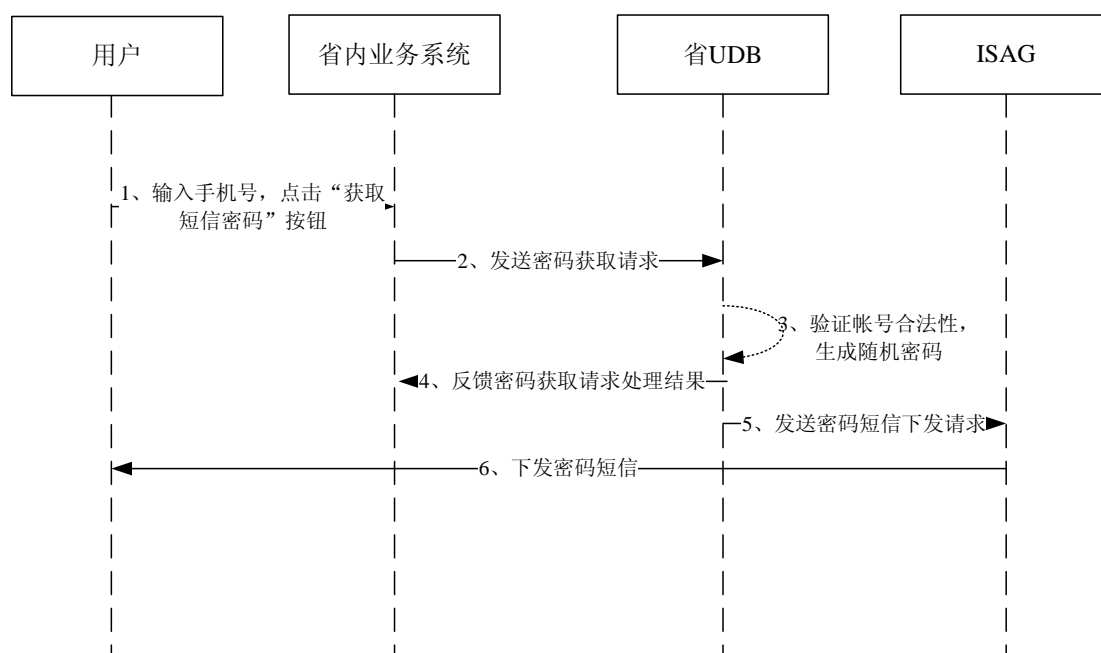
- 1) 用户经过帐户认证后登录应用系统；
- 2) 用户在应用系统进行业务密码修改（初次设置，可直接输入新密码；修改密码，需要输入新、原密码；重置为通用密码登录，则只传送密码策略）
- 3) 应用系统进行判断此用户是否是通过省UDB进行统一认证的用户，如果是，应用系统向UDB发起业务密码设置请求，将更新后的业务密码信息同步到省UDB；
- 4) 省UDB保留设置的登录密码策略；如果是设置或修改业务密码，则进行原密码比对和新密码保存。
- 5) 省UDB向应用系统返回更新结果；
- 6) 应用系统提示用户更新的结果。

**7.3.2.3 短信密码获取流程**

**触发条件:**

用户在应用系统的登录界面，点击“点击获取短信密码”按钮，或点击“忘记密码”。

**适用范围:** 只有与 UDB 之间通过 SOAP/ISAP 协议认证请求的电信自营应用系统，UDB 才提供手机短信密码获取功能；对采用重定向认证的应用系统，应用系统的 Portal 不提供该功能。

**交互流程:****流程描述:**

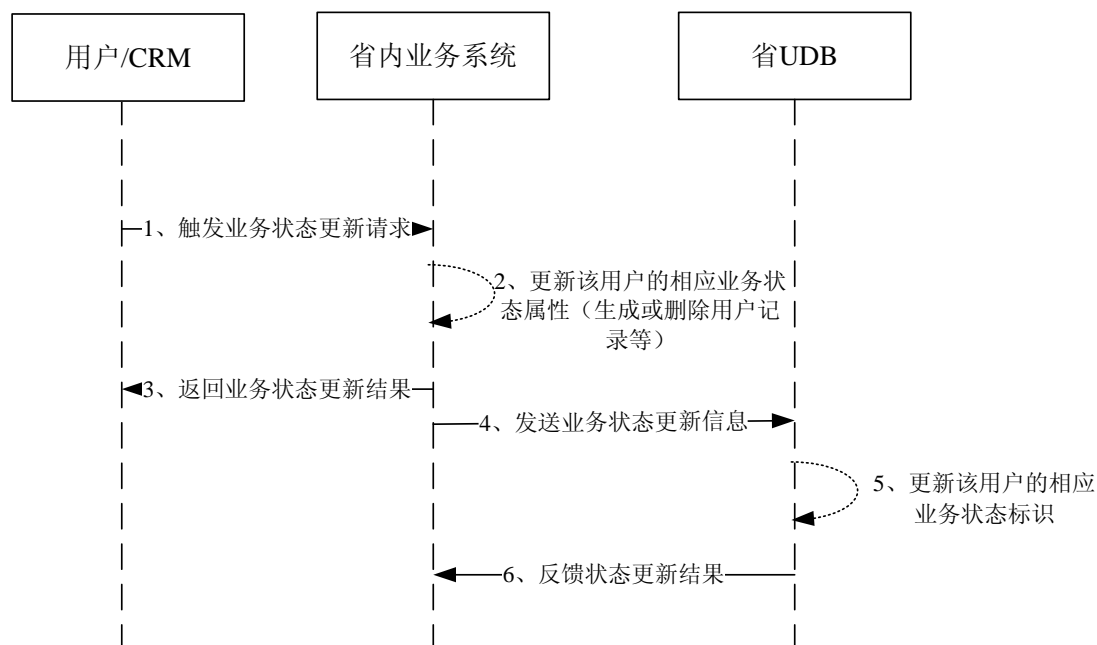
1. 用户在应用系统的服务界面，输入手机号码，点击“获取短信号码”按钮；
2. 应用系统通过短信密码获取接口，向省UDB发送请求；
3. 省UDB验证了帐号的合法性后，生成随机数字密码；
4. 省UDB向应用系统反馈处理结果；
5. 省UDB向ISAG发起请求，下发手机短信密码；
6. ISAG向用户下发密码短信。

**7.3.2.4 注册状态变更通知**

**触发条件:** 用户通过电信服务渠道（如电信营业厅、网上营业厅、10000/10001号、掌上营业厅、短信服务平台等）或直接登录应用系统开通业务订购；用户

通过电信渠道（如营业厅、网厅或短信服务等）或应用系统平台自身，对已注册/订购的该业务进行主动注销，不再使用；及其他业务状态更新操作（如用户暂停业务使用等）。

**交互流程：**



**流程描述：**

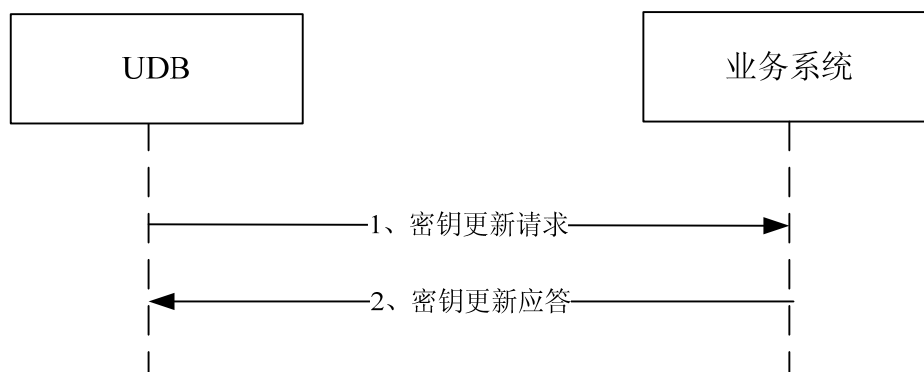
1. 用户/CRM将业务状态更新请求发送给应用系统；
2. 应用系统更新相应业务状态；
3. 应用系统返回业务状态更新结果；
4. 应用系统将业务状态更新信息，通过业务注册状态通知接口发送给省UDB；
5. 省UDB更新相应业务状态标识；
6. 省UDB返回业务状态更新的记录结果。

### 7.3.2.5 安全密钥更新流程

密钥更新是指对 UDB 和应用系统之间的共享密钥更新管理。对所有需要与 UDB 之间进行安全数据传送的应用系统都需要配置安全密钥。

密钥更新过程中涉及相关方采用数字证书验证身份，采用 WebService 方式，密钥的实时传输采用 SSL 以保证安全。

密钥更新流程如下：



流程描述：

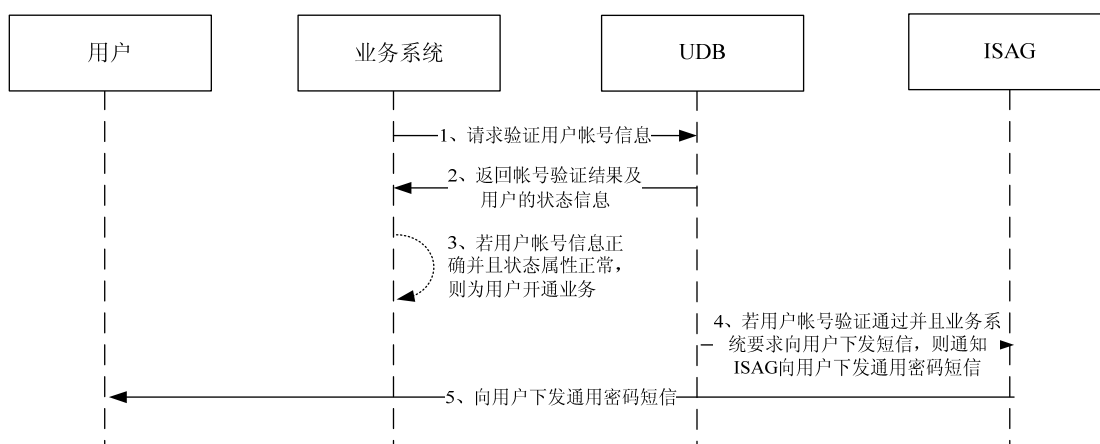
1. UDB定期，或不定期生成新安全密钥，向应用系统发送更新请求；
2. 应用系统更新密钥，并返回给UDB密钥更新应答。

### 7.3.2.6 帐号验证及短信通知流程

触发条件：

用户申请开通某项业务（如使用 CDMA 号码发送短信开通 189 邮箱），应用系统向 UDB 申请验证用户的状态属性（是否正常、欠费，或停机）；UDB 在用户身份正常的情况下，通过短信告知用户：“您已开通 XXX 业务，登录密码为 XXX”；应用系统根据返回验证信息，正常的话则开通/注册用户。

交互流程：



流程描述：

1. 应用系统向UDB请求验证用户统一帐号相关信息，调用“帐号验证及短信申

请”接口进行请求；

2. UDB向应用系统返回帐号验证结果以及用户的状态属性；
3. 若用户帐号信息正确并且状态属性正常，应用系统则为用户开通业务；
4. 若用户帐号验证通过并且应用系统要求向用户下发密码短信，那么UDB通知ISAG向用户下发通用密码短信；
5. ISAG向用户下发通用密码短信。

### 7.3.3 接口内容

业务认证请求接口（包括重定向接口及 **Web Services** 接口）、业务密码设置接口、短信密码获取接口、帐号信息查询接口、业务在线状态通知、业务注册状态通知，安全密钥更新接口以及用户身份信息查询接口等，参见第六章公共接口部分的具体接口内容信息。

### 7.3.4 对应用系统的相关建议

UDB 为应用系统提供统一认证功能，同时可为应用系统提供用户状态等信息以提升差异化服务能力。

#### 7.3.4.1 应用系统界面的改造

对于采用重定向认证方式，并且需维持原有应用系统的门户页面不做大改造的情况，需要在其 **Portal** 提供中国电信统一帐号（通行证）登录的链接。一旦用户选择“登录”或“通行证登录”时，应用系统将重定向到中国电信统一认证的登录页面。对于帐号类型比较多样的应用系统，要有明确的“通行证登录”提示。另外，应用系统应提供通行证自服务的链接。

对于采用后台认证（**SOAP** 或 **ISAP** 协议）应用系统，建议业务界面要分别提供支持统一帐号（通行证帐号）、通用密码、动态密码的输入框，如果要支持别名登录，则应用系统还必需提供单独帐户录入框。

#### 7.3.4.2 用户状态属性的利用



应用系统在 UDB 认证反馈消息，可获得该用户状态信息（正常、单停、双停、停机、拆机、暂停等）。应用系统可根据用户状态进行鉴权判断：是否继续为其提供服务，或执行计费管理等。

对应用户(手机/固话)不同状态，对统一帐号所能使用的业务权限，建议如下规则，供各应用系统使用参考：

表 7.3-1 用户状态与业务权限的关系

手机状态	统一帐号的业务/应用权限
正常	各项业务或应用均正常使用
欠费单停	免费业务可继续使用，收费应用停用（已缴包月费业务允许使用到月底）
欠费双停	停止所有应用使用（已缴包月费业务允许使用到月底）
停机保号	一有余额（预付费）及信用允许（后付费）：不影响应用层用户体验，所有业务正常使用。 一无余额（预付费）及信用不足（后付费）：停止所有应用使用（已缴包月费业务允许使用到月底）。
拆机、其他停机、暂停服务	停止所有业务使用（包括网厅）

## 7.4 综合业务管理平台接口

综合业务管理平台 ISMP 提取业务网络的公共功能，提供面向基于不同电信承载网络的增值业务运营的统一管理、统一鉴权和统一计费功能。

基于业务网络目标架构的演进，未来中国电信综合业务管理平台系列 ISMP-B、ISMP-M、ISMP-W 的认证功能将全部由 UDB 统一提供

### 7.4.1 ISMP- M的接口

#### 7.4.1.1 接口概述

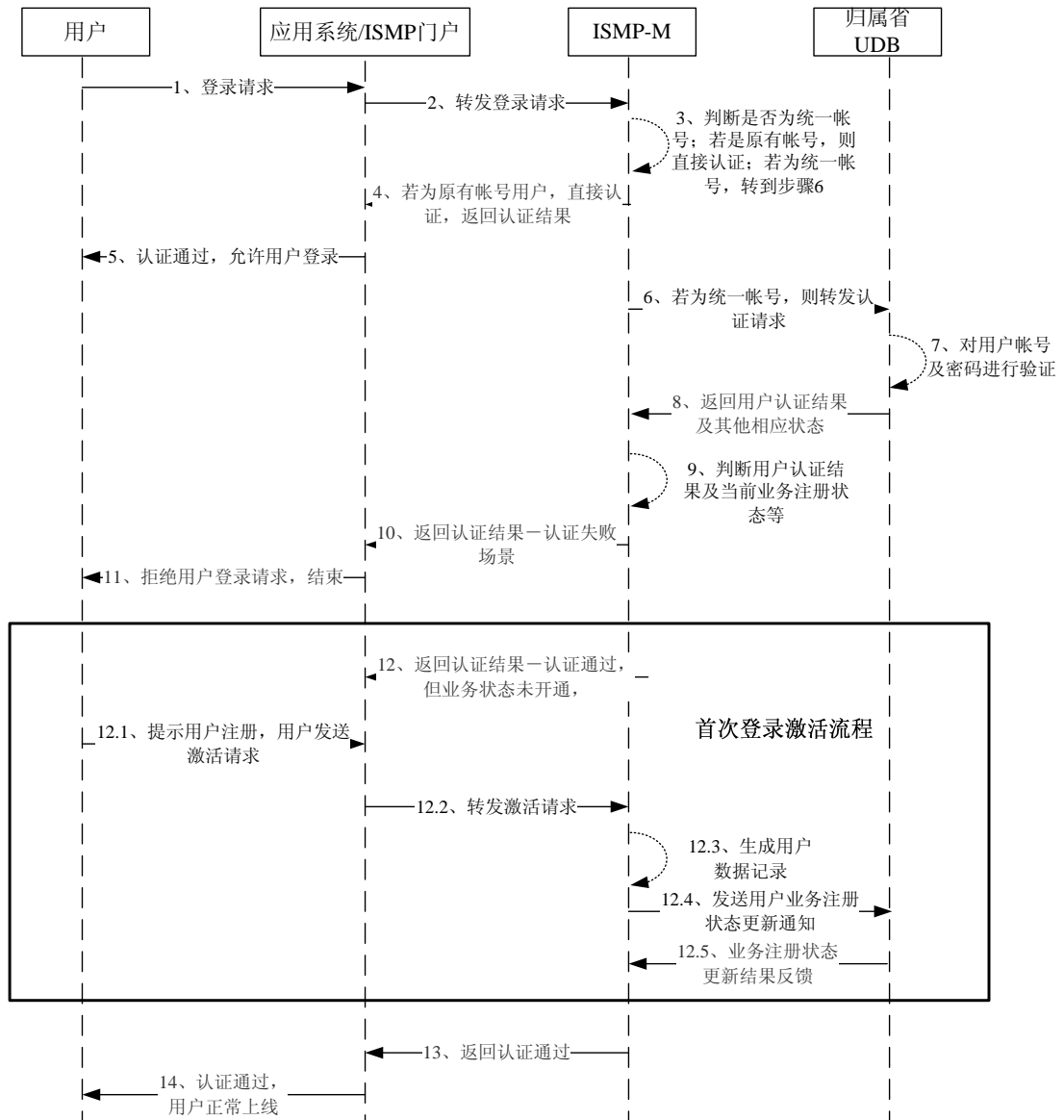
ISMP-M 平台主要管理短信、彩铃、彩信、WAP、定位等基于移动通信的增值业务。ISMP-M 的统一认证功能将逐步剥离，UDB 主要完成 ISMP-M 相关应用门户的登陆验证、号码状态等信息提供等。

用户登录中国电信 ISMP-M 的应用门户（如彩铃门户），用户身份由原 ISMP-M 集中验证，转由 ISMP-M 通过专用接口转发 UDB 进行集中认证。具体的接口类型包括如下几种场景：

- 在用户登录 ISMP-M 的应用门户时，ISMP-M 需调用 UDB 提供的业务认证请求接口。
- 用户在彩铃门户/ISMP-M 进行业务/应用注册时，ISMP-M 维护其订购关系，并同时调用 UDB 的业务注册状态通知接口。
- 当用户需要获取短信动态密码时，ISMP-M 需调用 UDB 提供的短信密码获取接口，由 UDB 生成和下发短信密码。

#### **7.4.1.2 接口流程**

适用于受 ISMP-M 负责管理的应用系统，如彩铃门户、彩信门户等。



### 流程描述：

1. 用户登录ISMP-M门户或者ISMP-M所管辖应用系统；
2. ISMP-M门户或者应用系统向ISMP-M发送认证请求；
3. ISMP-M判断是否为已经注册为统一帐号；若是原有帐号，则直接认证；若是统一帐号，转步骤6；
4. 若为原帐号用户，ISMP-M系统将对用户进行本地认证，返回认证结果；
5. 原有帐号认证通过，应用系统/ISMP-M门户允许用户登录；
6. 若为统一帐号，ISMP-M调用业务认证请求接口，向UDB转发认证请求；
7. UDB对用户的统一帐号及密码进行验证；
8. UDB向ISMP-M返回用户认证结果及相关的用户状态信息；

9. ISMP-M判断用户认证结果以及当前业务注册状态;
10. 若是UDB认证失败, 则ISMP-M向应用系统/ISMP-M门户返回认证失败;
11. 应用系统/ISMP-M门户拒绝该用户的登录请求;
12. 若是UDB认证通过, 但用户注册状态尚未开通, 则提示用户进行业务激活/开通, 进入用户首次登陆的激活流程;
  - 12.1) 用户向应用系统/ISMP-M门户发送激活请求;
  - 12.2) 应用系统/ISMP-M门户向ISMP-M转发激活请求;
  - 12.3) ISMP-M生成用户数据记录信息;
  - 12.4) ISMP-M向UDB发送用户业务注册状态通知;
  - 12.5) UDB向ISMP-M返回业务注册状态更新反馈结果。
13. 若是UDB认证通过, 且用户已成功注册, 则返回用户正常登录;
14. 应用系统/ISMP-M门户允许用户登录。

用户在 ISMP-M 应用门户点击“获取短信密码”, 其流程基本与 7.3.2.3 一致, ISMP-M 调用获取短信密码接口, 不再重复描述。

#### 7.4.1.3 接口内容

综合业务管理平台 ISMP-M 与 UDB 之间接口, 建议采用 ISAP 协议, 业务认证请求接口、业务注册状态通知、获取短信密码接口均为公共接口。

#### 7.4.1.4 对 ISMP-M 的改造要求

如 ISMP-M 需要为更多第三方 SP 提供认证功能, 可由 ISMP 统一提供重定向登录页面 (参见 UDB 重定向页面), ISMP-M 与 UDB 之间仍通过 ISAP 接口进行对接, 这样可确保 ISMP-M 能及时了解用户认证结果, 进而做业务鉴权和计费等操作。

### 7.4.2 ISMP- B的接口

#### 7.4.2.1 接口概述

面向商企客户的领航平台 BNET (综合业务管理平台 ISMP-B), 也不再新

建用户认证模块，全部由 UDB 提供统一认证服务。省 UDB 和全国 UDB，分别负责省 ISMP-B 和全国 ISMP-B 平台的认证：

- 领航平台将 UDB 通行证作为用户认证的一种方式。
- UDB 支持商航领航用户绑定手机、固话号码、邮箱账号等统一账号作为登陆账号。
- UDB 支持商务领航用户采用邮箱账号作为统一账号。
- 领航平台通过 UDB 实现网厅至领航平台的单点认证。

#### 7.4.2.2 接口流程

本期需分别规定领航帐号的创建流程、领航帐号的绑定流程、领航帐号的认证流程、网厅—BNET 单点登录流程等四个典型场景。

#### 7.4.2.3 接口内容

根据领航平台的特点，对接口内容定义如下接口：领航用户数据同步接口、领航帐号的绑定接口、领航用户的认证接口（支持多种登录帐号），以及领航平台的单点登录接口等。

#### 7.4.2.4 对 ISMP-B 的改造要求

### 7.5 第三方合作应用系统接口

中国电信与第三方 SP 合作，建立互信机制，用户通过中国电信统一帐号便可使用第三方业务，提升用户的服务感知，扩大中国电信帐号资源的利用。

#### 7.5.1 接口方案建议

中国电信与第三方合作应用系统之间的对接，可选择如下方案：

### 7.5.1.1 方案一：重定向集中认证方式

用户登录第三方应用系统时，通过重定向方式到中国电信的统一认证界面进行登录和认证，认证通过后返回第三方应用系统的登录后界面。

该方案实现较为简单，同时有利于保护中国电信的帐号体系和密码的安全（如只需要返回 PUserID 即可，而无须返回用户的真正手机号码）；对第三方 SP 业务来说需要适当改变用户的登录习惯。

该方案比较适合于影响力和规模较小的 SP，中国电信处于帐号主导地位，对方可直接识别和使用中国电信的统一帐号。

### 7.5.1.2 方案二：单点登录互信合作

中国电信在统一应用门户，或部分电信自营业务平台（如互联星空等），维护有第三方 SP 应用的 SSO 链接。当中国电信对用户身份验证通过之后，无须进行二次认证便可直接使用第三方应用服务；也可根据双方合作需要，中国电信信任用户在第三方的认证结果，用户成功登录第三方后无须二次认证就直接使用中国电信提供的应用服务。

此方案要求电信和合作第三方都保留自身的认证功能和用户数据，并且建立互信机制，并且彼此之间帐号密码体系相互独立（通过中国电信内部 PUserID 标识，双方之间建立用户关联关系），实施安全性和使用方便都比较好。

该方案比较适合于具有较大行业影响力和规模的 SP，中国电信与其合作保持比较对等的关系，实现真正的互赢合作。

### 7.5.1.3 方案三：独立登录密码方案

在第三方应用登录时，中国电信为用户提供一个静态私有密码（只针对该应用系统有效，而需二次认证），或发放令牌卡方式生成随机动态密码，或每次登录通过手机终端获取动态密码，动态密码也是一次有效。

此方案需要用户记住通用密码之外的私有密码，或每次登录都要生成随机密码（对 USB KEY/令牌卡等方式还会增加用户成本），造成用户的一些不便。

该方案适合于需要高安全保障的 SP 和业务场景，如支付合作应用。

## 7.5.2 帐号关联的建立

建立中国电信和第三方之间的帐号关联，是实现重定向认证、单点登录互信的基础，以便双方都能准确定位服务对象。这种帐号关联有相互保密或者相互公开的两种方式，根据实际合作方的特点进行选择。

如果合作双方采用相互公开（信任）的帐号管理，则可通过中国电信 UserID 或绑定第三方帐号 ID 来相互定位用户。

### 7.5.2.1 相互保密的帐号关联建立

如果中国电信的统一帐号用户想使用第三方 SP 应用，则中国电信根据统一帐号（UserID）所对应的客户标识（PUserID），与第三方 SP 提出帐号关联请求，由对方为该 PUserID 分配其自有帐号 ID（该 ID 不用通知中国电信）。这样，便建立了合作双方的相互保密用户数据关联关系：

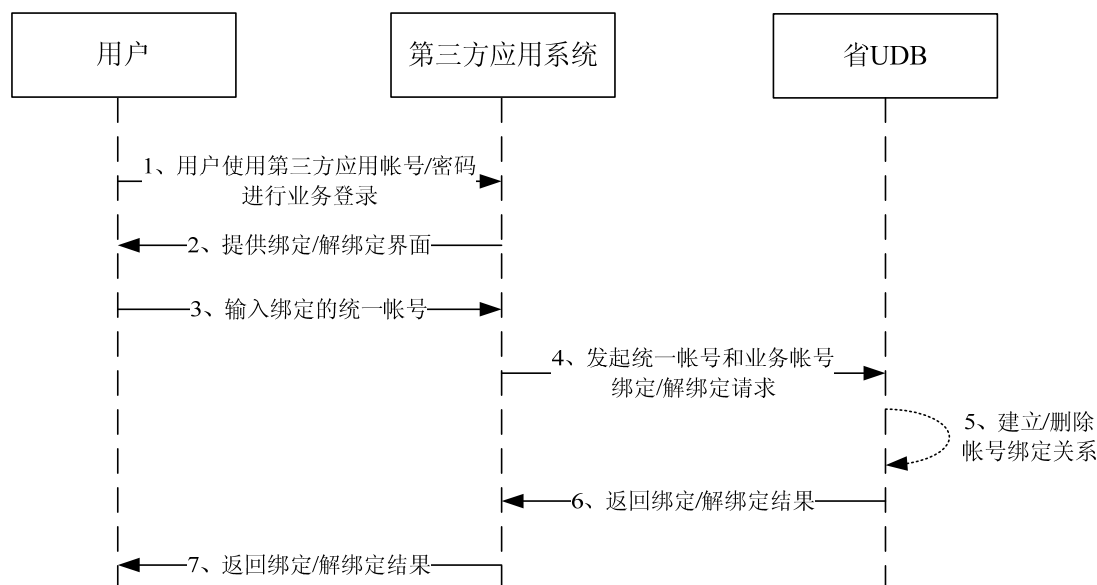
**UserID**（只中国电信知晓）—**PUserID**（双方知晓，标识键）—第三方应用帐号 ID（只第三方 SP 知晓）。

如果合作双方采用相互保密的帐号关联，则任何一方认证通过后，通过 PUserID 标识告知对方该用户的登录请求。

### 7.5.2.2 相互公开的帐号绑定流程

对第三方合作的应用系统，中国电信提供外部帐号的绑定服务，即建立中国电信统一帐号与原用户帐号ID的绑定关系，一般要求第三方合作伙伴提供用户帐号绑定服务流程和界面，**UDB**提供外部帐号绑定接口，将绑定关系相关的用户信息在中国电信**UDB**设备进行集中管理。

用户第三方系统帐号ID与中国电信统一帐号之间的关联绑定关系，也可选择由第三方应用系统自己维护，那么用户在第三方做帐号绑定后，并不需要调用该接口通知**UDB**；用户登录**UDB**验证通过后，**UDB**返回用户的统一帐号ID。不建议采用该方式。



#### 流程描述:

1. 用户使用第三方应用系统的帐号/密码进行业务登录;
2. 第三方应用系统向用户提供帐号绑定或是解绑定的界面;
3. 用户在绑定/解绑定界面上输入将绑定的统一帐号;
4. 第三方应用系统向省UDB发起帐号绑定/解绑定请求;
5. 省UDB建立/删除帐号绑定关系;
6. 省UDB向第三方应用系统返回帐号绑定/解绑定结果;
7. 第三方应用系统向用户返回帐号绑定/解绑定结果。

### 7.5.3 重定向认证接口

采用重定向认证请求接口，也是目前中国电信互联星空等普遍采用的合作模式。

#### 7.5.3.1 接口流程及接口内容

重定向认证的流程和接口，可参照 7.3.2.1 节不再重复描述。

基于重定向认证接口技术，可有效实现单点登录功能，即电信自营系统—第三方应用的 SSO 功能，其流程和接口可参照 10.2.1 或 10.2.2 节，



### 7.5.3.2 第三方应用的改造要求

第三方 SP 应用系统的界面，应提供中国电信统一帐号（通行证）用户的专用登录的链接或控件，一旦用户选择统一帐号用户登录时，自动重定向到中国电信的统一认证页面。

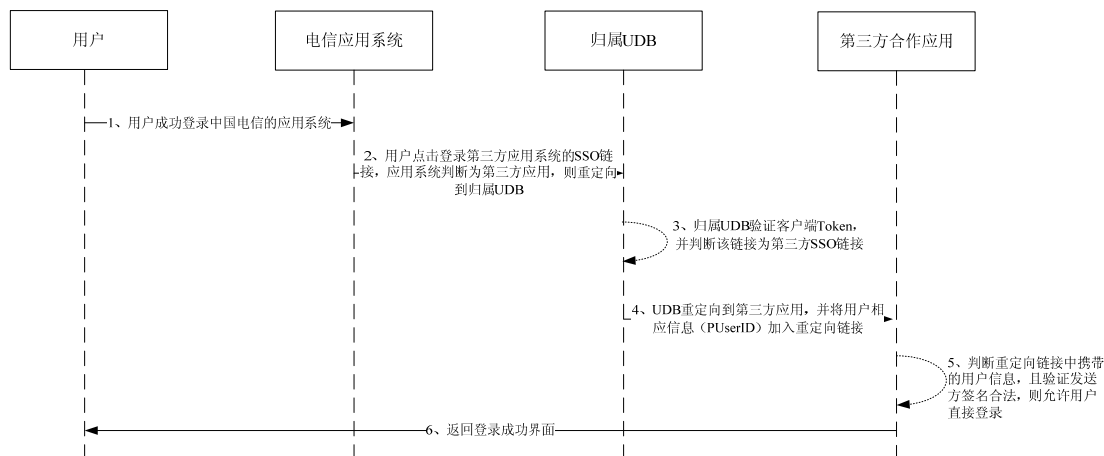
## 7.5.4 单点登录互信接口

中国电信与第三方 SP 应用系统之间，相互保留各自的认证功能，并且相互信任对方已经认证的结果。

### 7.5.4.1 接口流程及接口内容

#### 1、接口流程：

##### 场景1：电信应用—第三方应用的单点登录



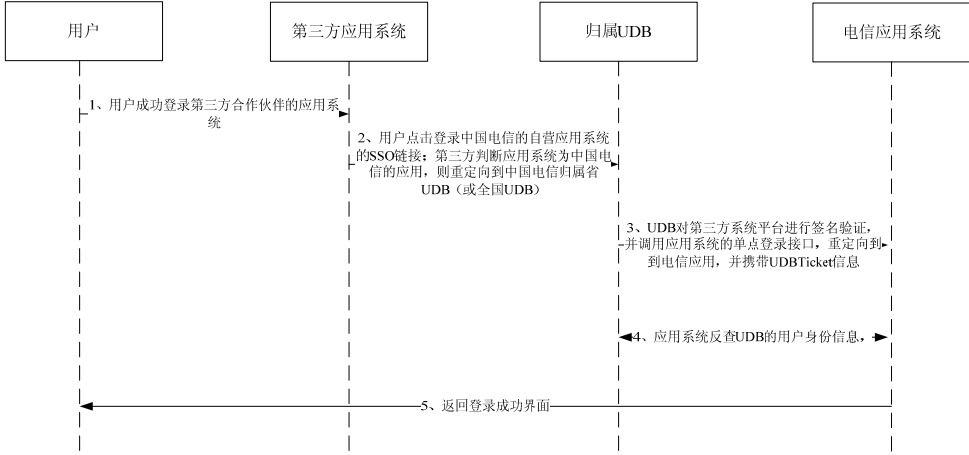
#### 流程描述：

- 1) 用户通过统一帐户认证后成功登录电信的应用系统；
- 2) 用户点击第三方合作应用的SSO链接，电信应用系统判断为第三方应用，则调用UDB的重定向单点登录接口，发起单点登录请求；
- 3) UDB验证客户端的Token信息合法（判断用户是否已通过认证），并根据重定向链接地址判断为第三方合作应用；
- 4) UDB将访问重定向到第三方的应用系统（调用第三方应用系统提供的重定向单点登录接口），并携带PUserID用户标识信息；
- 5) 第三方应用系统判断重定向链接中的用户信息，且验证发送方UDB的签名是

否合法？

6) 验证通过，则直接向用户展现登录成功界面；否则，需要用户重新登录。

场景2：第三方应用—电信应用的单点登录



流程描述：

- 1) 用户正常登录了中国电信合作的第三方应用系统；
- 2) 用户点击第三方应用的中国电信自营应用SSO链接，第三方应用则直接调用UDB的重定向单点登录接口，携带目标访问URL；
- 3) UDB验证重定向携带信息的合法性，如通过，则向目标访问URL的应用系统重定向，调用应用系统的单点登录接口，携带UDB临时生成的Ticket信息；
- 4) 电信应用系统接收到Ticket信息，通过调用UDB的用户身份验证接口，获取用户的统一帐号信息；
- 5) 电信应用系统根据获取的用户身份信息，直接向用户展现登录成功界面。

2、接口内容：

UDB提供的重定向单点登录接口，参见6.2.3节。对于电信自营应用系统、第三方合作应用系统的重定向单点登录接口，参见13.4、13.5节。

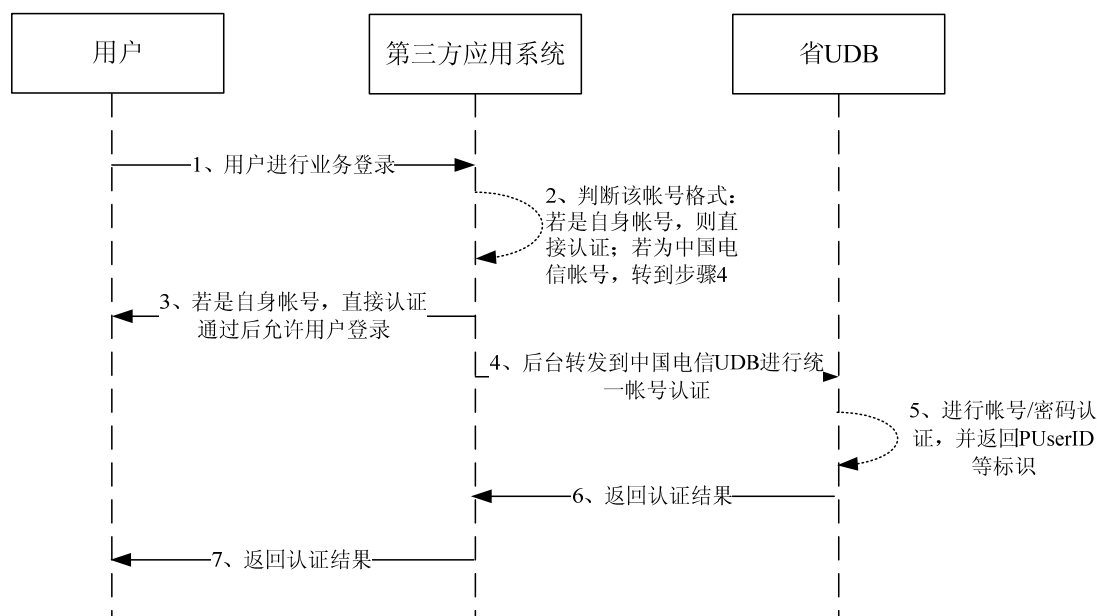
7.5.4.2 第三方应用的改造要求

参与双方合作的第三方SP应用系统，需要提供特定的重定向单点登录接口，供中国电信UDB调用。第三方SP应提供统一的针对中国电信的SSO链接，同时能有效识别中国电信的自营合作应用，将其SSO链接重定向到UDB。

## 7.5.5 独立密码认证接口

为第三方SP提供私有密码，或动态密码登录验证，而且该密码权限只限于用户访问该应用系统，或一次性使用。

### 7.5.5.1 接口流程及接口内容



#### 流程描述：

1. 用户在第三方应用系统进行登录；
2. 第三方应用系统判断登录该帐号格式：若是应用系统自身帐号，则直接认证；若为中国电信的统一帐号，转到步骤4；
3. 若是应用系统自身帐号，第三方应用系统直接认证通过后允许用户登录；
4. 第三方应用系统向中国电信UDB转发统一帐号的业务认证请求，调用UDB的业务认证请求接口；
5. 省UDB进行帐号/密码认证；
6. 省UDB向第三方应用系统返回帐号认证结果；
7. 第三方应用系统向用户返回帐号认证结果。（若用户尚未在第三方应用系统注册过业务帐号，首次登录就使用统一帐号时，那第三方系统会根据实际情况自动为用户注册或提示激活）

用户认证请求接口，请参见公共 Web Service 接口具体信息。

#### **7.5.5.2 第三方应用的改造要求**

第三方 **SP** 的应用系统页面，应专门提供中国电信统一帐号（通行证）用户的帐号及私有密码的专用登录框，如果需要二次认证（如 **OTP** 密码）则要在提供二次密码录入框。如果帐号格式类型特点可明显区分，则第三方应用系统也可维持统一登录框，但必需对用户录入帐号格式进行筛选，所有统一帐号格式的登录由中国电信 **UDB** 进行统一认证。

## 8 全国 UDB 的接口

### 8.1 电信自营应用系统接口

电信自营应用系统，是指中国电信自运营自建设的应用系统。

全国 UDB 为全国应用系统平台提供统一帐号登录的认证服务，如 189 邮箱、天翼 Live 平台、全国互联星空、全国爱音乐平台、全国商企业平台等。

全国 UDB 与全国应用系统的通用接口参见第 6 章内容，以下重点就全国 UDB 与 189 邮箱、天翼 Live 客户端的接口进行描述。

#### 8.1.1 全国UDB提供给189邮箱接口

全国 UDB 为全国应用系统提供统一帐号用户登录的认证服务，并将认证结果及用户状态等相关信息反馈给全国应用系统。

##### 8.1.1.1 邮箱认证接口

(1) 接口信息：

接口名称	EmailLogin
接口概述	提供给邮箱系统的用户重定向认证接口，在邮箱系统登录，邮箱系统首先重定向到全国 UDB 系统，如果已有 PassPort 身份则直接通过，如果没有 PassPort 身份则直接返回到邮箱系统指定页面，提示用户输入用户名和密码，然后再次认证。外网访问。
请求消息名	http://Passport/ EmailLogin
应答消息名	ReturnURL
接口协议	重定向
提供者	全国 UDB 系统
主要使用者	邮箱系统

(2) 参数说明

1) 请求消息

<http://Passport.189.cn/EmailLogin?EmailLoginRequest=EmailLoginRequestValue>

EmailLoginRequestValue 为接口参数值，包含如下信息：

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起方系统 ID
Alias	String	40	1	别名
Password	String	64	1	密码

TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区
ReturnURL	String		1	通行证系统返回认证结果时需要调用的 URL

EmailLoginRequestValue 的生成算法如下:

Digest = Base64(Hash(SrcDeviceNo+ Email+ Password+ TimeStamp+ ReturnURL))

其中, Hash 算法采用 SHA-1。

EmailLoginRequest= URLEncoding(SrcDeviceNo + "\$"+ Base64(Encrypt(Email + "\$"+ Password "\$"TimeStamp + "\$"+ReturnURL + "\$"+ Digest)))

其中, 加密算法采用 3DES, Key=SysKey, SysKey 是通行证系统发给该系统的密钥。

## 2) 响应消息

接口方法为:

http://ReturnURL?EmailLoginResponse= EmailLoginResponseValue

其中, ReturnURL 从 EmailLoginRequest 中获得。

EmailLoginResponseValue 为接口参数值, 包含如下信息:

参数名称	数据类型	长度 (字节)	出现 频次	说明
Result	Int		1	0: 成功
DestDeviceNo	String	16	1	返回方系统 ID
ProvinceNo	String	2	1	统一帐号用户所在省
PUserID	String	11	1	用户唯一标识
UserID	String	40	1	PassPort
Alias	String	40	1	邮箱别名
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区

EmailLoginResponseValue 的生成算法如下:

Digest = Base64(Hash(Result + DestDeviceNo + ProvinceNo + PUserID + UserID + Alias + TimeStamp))

其中, Hash 算法采用 SHA-1。

EmailLoginResponseValue= URLEncoding(DestDeviceNo + "\$"+ Base64(Encrypt (Result + "\$"+ ProvinceNo + "\$"+ PUserID + "\$"+ UserID + "\$"+ Alias + "\$"+ TimeStamp + "\$"+ Digest)))

其中, 加密算法采用 3DES, Key=SysKey, Syskey 是通行证系统颁发给该系统的密钥。

## 8.1.2 189邮箱提供给全国UDB接口

### 8.1.2.1 用户状态变更通知接口

(1) 接口信息:

接口名称	PUserStatusNotify
接口概述	用户在全国 UDB 修改状态信息后, 同步到邮箱系统
请求消息名	PUserStatusNotifyRequest

应答消息名	PUserStatusNotifyResponse
接口协议	SOAP
提供者	189 邮箱系统
主要使用者	全国 UDB 系统

(2) 参数说明

1) 请求消息

PUserStatusNotifyRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起系统 ID
ProvinceNo	String	2	1	用户所在省【不能根据此字段匹配更新】
PUserID	String	11	1	用户唯一标识(以 PUserID 作为更新依据)
UserID	String	40	1	PassPort (邮箱名)
UserIDStatus	String	2	1	见附件
Extension	String		0-1	Xml 格式的扩展字段(可空)

2) 响应消息

PUserStatusNotifyResponse 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
Result	Int	4	1	0: 成功
DestDeviceNo	String	16	1	返回系统 ID
PUserID	String	11	1	用户唯一标识
Extension	String		0-1	Xml 格式的扩展字段(可空)
ErrorDescription	String	≤256	0-1	错误描述 (Result 为 0 时可空)

### 8.1.2.2 用户密码变更通知接口

(1) 接口信息:

接口名称	PUserPasswordNotify
接口概述	用户在 UDB 系统修改密码信息后, 同步到邮箱系统
请求消息名	PUserPasswordNotifyRequest
应答消息名	PUserPasswordNotifyResponse
接口协议	SOAP
提供者	邮箱系统
主要使用者	全国 UDB 系统

(2) 参数说明

1) 请求消息

PUserPasswordNotifyRequest 包含如下参数:

参数名称	数据类型	长度	出现	说明
------	------	----	----	----

		(字节)	频次	
SrcDeviceNo	String	16	1	发起系统 ID
ProvinceNo	String	2	1	用户所在省【不能根据此字段匹配密码更新】
PUserID	String	11	1	用户唯一标识（以 PUserID 作为更新依据）
UserId	String	40	1	PassPort （邮箱名）
Password	String	64	1	用户密码 明文传递
Extension	String		0-1	Xml 格式的扩展字段(可空)

## 2) 响应消息

PUserPasswordNotifyResponse 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
Result	Int	4	1	0: 成功
DestDeviceNo	String	16	1	返回系统 ID
PUserID	String	11	1	用户唯一标识
Extension	String		0-1	Xml 格式的扩展字段(可空)
ErrorDescription	String	≤256	0-1	错误描述 (Result 为 0 时可空)

## 8.1.2.3 邮箱别名通知接口

## (1) 接口信息:

接口名称	AliasNotify
接口概述	用户在 UDB 系统设置或修改了 PassPort 别名时通知邮箱系统。内网访问。
请求消息名	AliasNotifyRequest
应答消息名	AliasNotifyResponse
接口协议	SOAP
提供者	邮箱系统
主要使用者	全国 UDB 系统

## (2) 参数说明

## 1) 请求消息

AliasNotifyRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起方系统 ID
ProvinceNo	String	11	1	用户所在省【不能根据此字段匹配别名更新】
PUserID	String	11	1	用户唯一标识（以 PUserID 作为更新依据）
UserID	String	40	1	PassPort (189 邮箱)
Alias	String	40	1	189 邮箱别名
Extension	String		0-1	扩展信息 xml(可空)



## 2) 响应消息

AliasNotifyResponse 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
Result	Int	4	1	0: 成功
DestDeviceNo	String	16	1	返回方系统 ID
PUserID	String	11	1	用户唯一标识
Extension	String		0-1	扩展信息 xml(可空)
ErrorDescription	String	≤256	0-1	错误描述 (Result 为 0 可空)

## 8.1.2.4 邮箱服务通知接口

## (1) 接口信息:

接口名称	ProductOrderNotify
接口概述	用户订购收费邮箱并注册成为 PassPort 后, VNet 将付费邮箱通知全国 UDB 系统, 全国 UDB 系统同步到邮箱系统, 此消息作为收费邮箱服务授权依据。如用户订购多个服务, 不发邮箱变更, 根据授权情况决定用户是否可以使用邮箱。内网访问。
请求消息名	ProductOrderNotifyRequest
应答消息名	ProductOrderNotifyResponse
接口协议	SOAP
提供者	邮箱系统
主要使用者	全国 UDB 系统

## (2) 参数说明

## 1) 请求消息

ProductOrderNotifyRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起方系统 ID
ProvinceNo	String	2	1	用户所在省 (用户所在省关联或者绑定宽带会发生变化)
PUserID	String	11	1	用户唯一标识 (以 PUserID 作为更新依据)
Email	String	50	1	邮箱名
OPType	String	1	1	操作类型 1 订购 2 取消订购[保留]
ServiceID	String	16	1	服务 ID, 唯一确定一个服务
StartTime	String	16	1	服务开始时间
EndTime	String	16	1	服务结束时间
Extension	String		0-1	Xml 格式的扩展字段(可空)

## 2) 响应消息

ProductOrderNotifyResponse 包含如下参数：

参数名称	数据类型	长度 (字节)	出现 频次	说明
Result	Int		1	0 成功
SrcDeviceNo	String	16	1	发起方系统 ID
PUserID	String	11	1	用户唯一标识
Extension	String		0-1	Xml 格式的扩展字段(可空)
ErrorDescription	String	256	0-1	错误描述 (Result 为 0 时可空)

### 8.1.3 全国UDB提供给天翼Live客户端接口

#### 8.1.3.1 E 家通行证认证接口

参见公共 Web Service 接口相关的业务认证请求接口。

#### 8.1.3.2 E 家通行证注册接口

参见公共 Web Service 接口的接口“帐号验证及短信申请”接口内容。

#### 8.1.3.3 帐号属性查询接口

(1) 接口信息：

接口名称	e 家通行证 EHomeRegister
接口概述	天翼 Live 需要根据用户宽带状态及宽带类型判断用户对 e 家电话的使用权限。因此需要通过全国 UDB 查询宽带帐号属性。
请求消息名	e 家通行证 EHomeRegisterRequest
应答消息名	e 家通行证 EHomeRegisterResponse
接口协议	SOAP
提供者	全国 UDB 系统
主要使用者	天翼 Live 后台

(2) 参数说明

1) 请求消息

EHomeRegisterRequest 包含如下参数：

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起方系统 ID, 6: 新 E 家
AccountType	String	2	1	帐号类型: 00: 互联星空帐号 01: 窄带帐号; 02: 宽带帐号; 03: 宽窄带统一帐号;

				04: 固话号码 05: 小灵通号码 06: 用户 ID, 即 UserID 07: VNetID
Account	String	57	1	帐号

## 2) 响应消息

EHomeRegisterResponse 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
DestDeviceNo	String	16	1	应答方系统 ID
UserID	String	40	0-1	用户 ID (Passport)
UserIDStatus	String	2	1	支付帐号的状态: 01: 正常态; 02: 正常暂停态; 03: 欠费暂停态; 04: 黑户暂停态; 05: 注销态; 06: 过户; 07: 移机改号; 08: 其它不正常状态
CreditValue	Long	8	0-1	信用额度, 以分为单位 (未建省可为空)
Balance	Long	8	0-1	帐户余额, 以分为单位(未建省可为空)
PaymentAccount Type	String	2	1	支付帐号类型: 01: 窄带帐号; 02: 宽带帐号; 03: 宽窄带统一帐号; 04: 固话号码 05: 小灵通号码 06: 卡账号 08: 银行转账账号 09: 3G 帐号 (手机帐号) 10: 网吧帐号 11: 公免帐号, 此类型的帐号做不做公免由各个省自己决定 12: 联名卡帐号 13: 体验卡帐号 14: 现金帐号 99: 其它
PaymentAccount	String	40	1	支付帐号
PersonalID	String	20	0-1	身份证号码 (可为空)
Name	String	20	0-1	真实姓名 (可为空)
AreaCode	String	3 或 4	0-1	用户所在地区电话区号 (可为空)
PhoneNum	String	15	0-1	宽窄带注册电话号码 (可为空)
PortStatus	String	2	0-1	端口状态 (可为空): 00: 接入端口未绑定 01: 接入端口模糊绑定

				02: 接入端口精确绑定
RoamStatus	String	2	0-1	账号漫游状态（可为空）： 00: 用户在注册端口上网 01: 用户未在注册端口上网，即宽带接入账号漫游
PortID	String	≤20	0-1	用户上网物理端口 ID（可为空）
SVCIDs	SVCID[]		1	支付帐户上开通的业务类型
ErrorDescription	String	≤256	0-1	对错误/异常的详细描述信息
CityCode	String	3 或 4	1	用户所属地区区号
PaymentType	String	2	1	付费类型 01: 预付费 02: 后付费
Email	String	40	0-1	支付账户关联的 email 地址（可为空）

响应消息中，SVCIDs 包括以下信息

参数名称	数据类型	长度 (字节)	出现 频次	说明
SVCID	Element		N	支付帐户上开通的业务类型，可出现多次

SVCIDs 中，SVCID 包括以下信息：

参数名称	数据类型	长度 (字节)	出现 频次	说明
ID	String	20	1	业务类型说明，如： e8-1，表示我的 E 家的 e8-1 业务类型，（支持 2 台电脑终端）； e8-2，表示我的 E 家的 e8-2 业务类型，（支持 4 台电脑终端）； E6
RecordExtendField	String	≤256	0-1	扩展字段 xml 格式，留空

响应消息中，ExtendField 包括以下信息

参数名称	数据类型	长度 (字节)	出现 频次	说明
HighRisk	String	2	1	高风险帐号类型标识，此类账号类型用户每次消费都需要支付密码 00: 非高风险帐号类型标识 01: 高风险帐号类型标识

#### 8.1.3.4 宽带帐号认证接口

(1) 接口信息：

接口名称	宽带帐号认证接口 RoamAuth
------	-------------------

接口概述	天翼 Live 支持老 e 家客户端的宽带直接登录方式（不需要输入通行证帐号密码登录），天翼 Live 后台向全国 UDB 系统请求认证宽带用户身份。认证通过后可访问天翼 Live 的普通频道，不能登录 MSN 和使用 e 家电话。
请求消息名	RoamAuthRequest
应答消息名	RoamAuthResponse
接口协议	SOAP
提供者	全国 UDB 系统
主要使用者	天翼 Live 后台

## （2） 参数说明

### 1) 请求消息

RoamAuthRequest 包含如下参数：

参数名称	数据类型	长度 (字节)	出现 频次	说明
ProvinceNo	String	2	1	用户所属省的省份代码
AccountType	String	2	1	帐号类型： 02: 宽带帐号；（必须实现）
UserAccount	String	57	1	帐号, 格式"XXXX@省份 code(大写).chinavnet.com"
Password	String	64	1	密码
IPAddress	String	15	1	用户当前的 IP 地址
TimeStamp	String	≤18	1	时间戳, 从 1970 年 1 月 1 日 0 时开始的毫秒数, 时区为东八区

### 2) 响应消息

RoamAuthResponse 包含如下参数：

参数名称	数据类型	长度 (字节)	出现 频次	说明
ProvinceNo	String	2	1	应答方的省份码
UserID	String	40	1	用户的唯一标识 当 Result=2 时可为空
NickName	String	40	1	昵称 当 Result=2 时可为空
Result	Int	4	1	0: 用户认证通过（宽带认证通过，且互联星空用户已注册） 2: 宽带认证通过，但该宽带帐号未注册互联星空用户
ErrorDescription	String	≤256	0-1	对错误/异常的详细描述信息
UserProfile	String	≤3000	1	用户的授权信息，此字段固定为空。用户使用普通服务时由 SP 授权，使用产品时调用省或中心提供的产品授权接口
TimeStamp	Int	≤18	1	时间戳
UserProvince			0-1	用户归属省 id 当 Result=2 时可为空

UserArea			0-1	用户归属地市 id 当 Result=2 时可为空 以 UserInfoQuery 接口返回的 AreaCode 为准
PhoneNum	String	15	0-1	宽窄带注册电话号码（可为空）
ExpireTime	String	≤18	1	失效时间，从 1970 年 1 月 1 日 0 时开始的毫秒数
ADSLStatus	String	2	1	直接返回省里应答代码，中心不做转换 支付帐号的状态： 01：正常态； 02：正常暂停态； 03：欠费暂停态； 04：黑户暂停态； 05：注销态； 06：过户； 07：移机改号； 08：其它不正常状态 按照 UserInfoQuery 应答参数定义
ADSLType	String	2	1	绑定的宽带账号类型，取值如下： e6 e8 e8-1 e8-2 当 ADSLAccount 为空的时候该值为空,当 ADSLAccount 不为空的时候该值为空表明为普通宽带。
UserToken	String	<1024	1	Vnet 生成的 UserToken 取值，该 UserToken 由 EHome 客户端写入启动的浏览器中
PassPortToken	String		1	UDB 生成的 PassPortToken 取值，该 PassPortToken 由 EHome 客户端写入启动的浏览器中
HomeEmail	String	50	0-1	家庭邮箱地址暂时返回空

### 8.1.3.5 IP 反查接口

#### (1) 接口信息：

接口名称	IP 反查接口 QueryAdslInfoFromIp
接口概述	天翼 Live 支持老 e 家客户端的宽带直接登录方式（不需要输入通行证帐号密码登录），通过客户端 IP 获取用户的部分基本属性，包括客户宽带帐号，帐号所属套餐，帐号所属省份，然后对该宽带用户进行认证，认证通过后可访问天翼 Live 的普通频道，不能登录 MSN 和使用 e 家电话。
请求消息名	QueryAdslInfoFromIpRequest
应答消息名	QueryAdslInfoFromIpResponse
接口协议	SOAP
提供者	全国 UDB 系统
主要使用者	天翼 Live 后台

(2) 参数说明

1) 请求消息

QueryAdslInfoFromIpRequest 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
SrcDeviceNo	String	16	1	发起方系统 ID, 6: 新 E 家
IPAddress	String	15	1	客户端的 IP 地址
TimeStamp	Int	≤18	1	时间戳, 从 1970 年 1 月 1 日 0 时开始的毫秒数, 时区为东八区

2) 响应消息

QueryAdslInfoFromIpResponse 包含如下参数:

参数名称	数据类型	长度 (字节)	出现 频次	说明
TimeStamp	Int	≤18	1	时间戳, 从 1970 年 1 月 1 日 0 时开始的毫秒数, 时区为东八区
ADSLAccount	String	30	1	ADSL 帐号
ADSLProvince	String	2	0-1	宽带账号所属省 当 ADSLAccount 为空的时候该值为空
ADSLType	String	2	1	绑定的宽带账号类型, 取值如下: e6 e8 e8-1 e8-2 当 ADSLAccount 为空的时候该值为空, 当 ADSLAccount 不为空的时候该值为空表明为普通宽带。
Result	Int	4	1	0: 成功
ErrorDescription	String	≤256	0-1	对错误/异常的详细描述信息
CityCode			1	以 UserInfoQuery 接口返回为准
ExpireTime	String	≤18	1	失效时间, 从 1970 年 1 月 1 日 0 时开始的毫秒数
ADSLStatus	String	2	1	支付帐号的状态: 01: 正常态; 02: 正常暂停态; 03: 欠费暂停态; 04: 黑户暂停态; 05: 注销态; 06: 过户; 07: 移机改号; 08: 其它不正常状态 以 UserInfoQuery 接口返回的为准, 中心不做转换
UserToken	String	<1024	1	Vnet 生成的 UserToken 取值, 该 UserToken 由 EHome 客户端写入启动的浏览器中
PassPortToken	String		1	UDB 生成的 PassPortToken 取值,

				该 PassPortToken 由 EHome 客户端写入启动的浏览器中
HomeEmail	String	50	0-1	家庭邮箱地址

## 8.2 第三方合作应用系统接口

参考 7.5 节相关方案建议，流程及接口描述。



## 9 省 UDB 与全国 UDB 接口

### 9.1 接口概述

按全国 UDB 二级组网架构功能定位，全国 UDB 平台负责全国性应用系统的认证服务，省 UDB 平台负责省内应用系统、宽带接入系统的认证服务，同时全国 UDB 还负责全国漫游认证的转发功能。

全国 UDB 从各省 UDB 获取用户帐号信息，而且为保障全国 UDB 的运行效率，全国 UDB 只保留全国业务平台注册及活跃用户的信息。全国 UDB 从全国 CRM 获取部分全国商企客户的帐号信息。

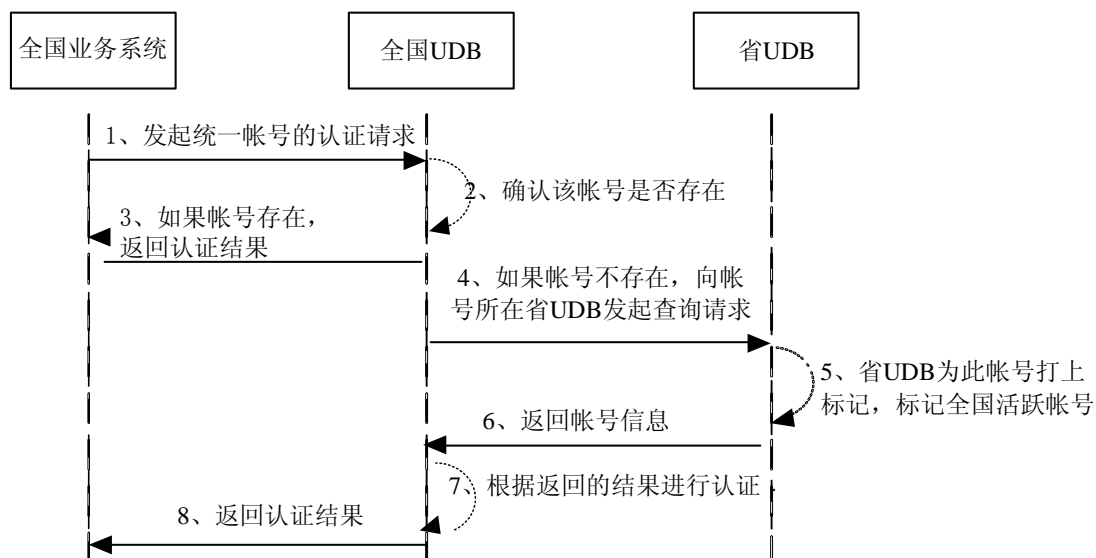
### 9.2 接口流程

#### 9.2.1 帐号查询流程

##### 9.2.1.1 全国一>省（统一帐号查询）

**触发条件：**用户首次登录全国性的应用系统，全国应用系统向全国 UDB 进行认证请求，而全国 UDB 无该用户帐号的记录，则通过统一帐号向省 UDB 发起帐号信息查询操作。

**交互流程：**



#### 流程描述：

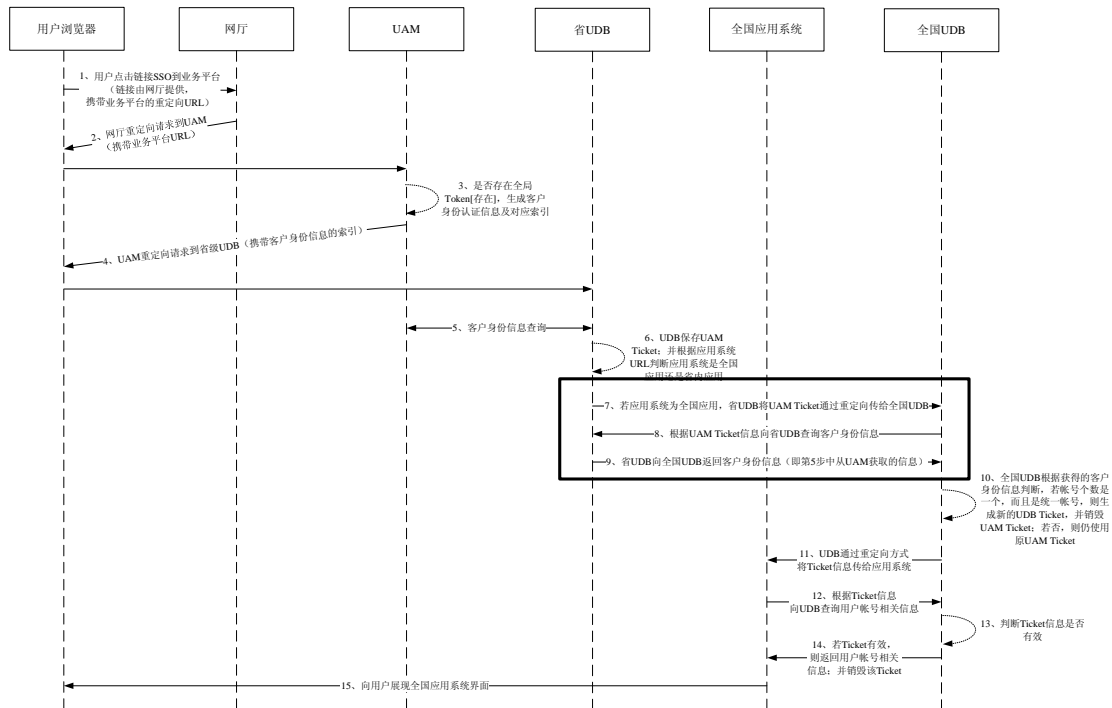
- 1) 全国性应用系统(如189邮箱)，或全国自服务门户，向全国UDB发起统一帐号的认证请求；
- 2) 全国UDB判断该帐号信息在全国UDB是否存在；
- 3) 如果全国UDB存有该帐号，进行认证后向返回认证结果；
- 4) 如果全国UDB不存在此帐号，则根据帐号归属特性向帐号所在省UDB设备发起帐号查询请求（如果帐号格式不符合，则返回帐号错误）；
- 5) 如果省UDB存在此帐号，则为此帐号打上标记，标记为全国活跃帐号（对于打上标记的帐号，当帐号信息变化时，需实时向全国UDB同步更新）；
- 6) 省UDB向全国UDB返回该帐号全部信息；
- 7) 全国UDB根据返回的帐号信息进行认证；
- 8) 全国UDB向应用系统返回认证的结果。

#### 9.2.1.2 全国一>省（宽带帐号查询）

**触发条件：**用户登录全国门户系统，输入老的宽带 ID 查询统一帐号的信息，全国 UDB 无该帐号的记录，则向省 UDB 发起用户帐号信息查询接口。

**交互流程：**





### 流程描述:

1. 用户点击网厅上的链接单点登录到全国应用系统, 单点登录的链接由网厅提供, 携带全国应用系统的重定向URL;
2. 网厅携带“应用系统返回URL”重定向到省UAM;
3. 省UAM根据全局Token, 生成当前客户的身份以及对应的索引UAM Ticket;
4. 省UAM携带“客户身份索引”, 通过省UDB提供的单点登录重定向接口, 重定向请求到省UDB;
5. 省UDB根据“客户身份索引”查询对应的客户身份信息;
6. 省UDB保存UAM生成的UAM Ticket信息, 并根据“应用系统返回URL”判断当前应用系统是全国应用系统还是省级应用系统;
7. 若应用系统为全国应用, 省UDB通过重定向的方式将UAM Ticket传给全国UDB, 调用全国的重定向单点登录接口;
8. 全国UDB根据UAM Ticket信息, 调用用户身份信息查询接口, 向省UDB查询客户身份信息;
9. 省UDB向全国UDB返回客户身份信息 (即第5步中从UAM获得的信息)
10. 全国UDB根据获得的客户身份信息进行判断: 若身份信息中帐号个数是一

个，而且该帐号是统一帐号，则全国UDB生成新的UDB Ticket，销毁原UAM Ticket；若否，则仍使用原UAM Ticket；

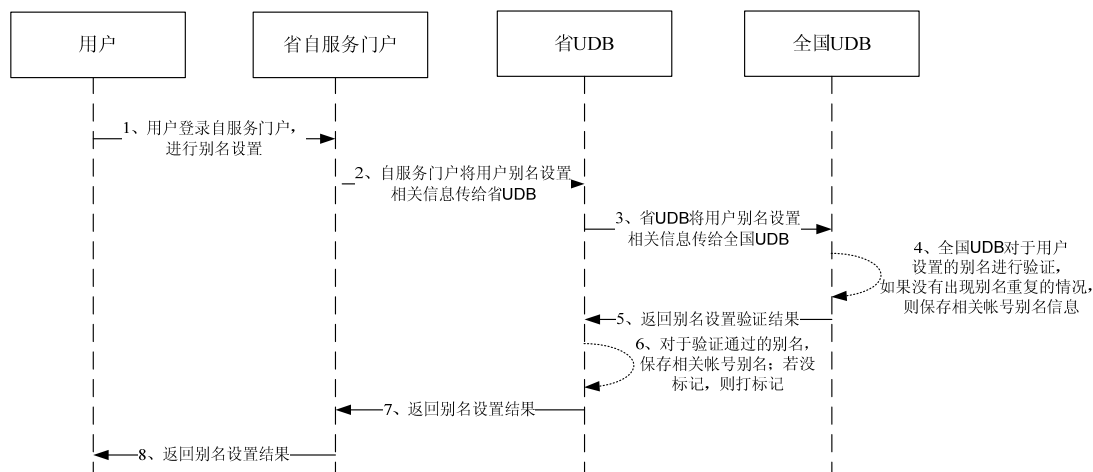
11. 全国UDB通过重定向方式将Ticket信息传给全国应用系统；
12. 全国应用系统根据Ticket信息向全国UDB查询用户帐号信息；
13. 全国UDB判断该Ticket信息是否有效；
14. 若Ticket有效，全国UDB向全国应用系统返回用户帐号相关信息；同时全国UDB销毁该Ticket；
15. 向用户展现全国应用系统界面。

## 9.2.2 别名设置流程

### 9.2.2.1 省→全国

**触发条件：**用户登录省自服务门户，点击“设置别名”，输入别名之后，点击“确认”，省UDB向全国UDB发起别名设置（修改）操作流程。

**交互流程：**



**流程描述：**

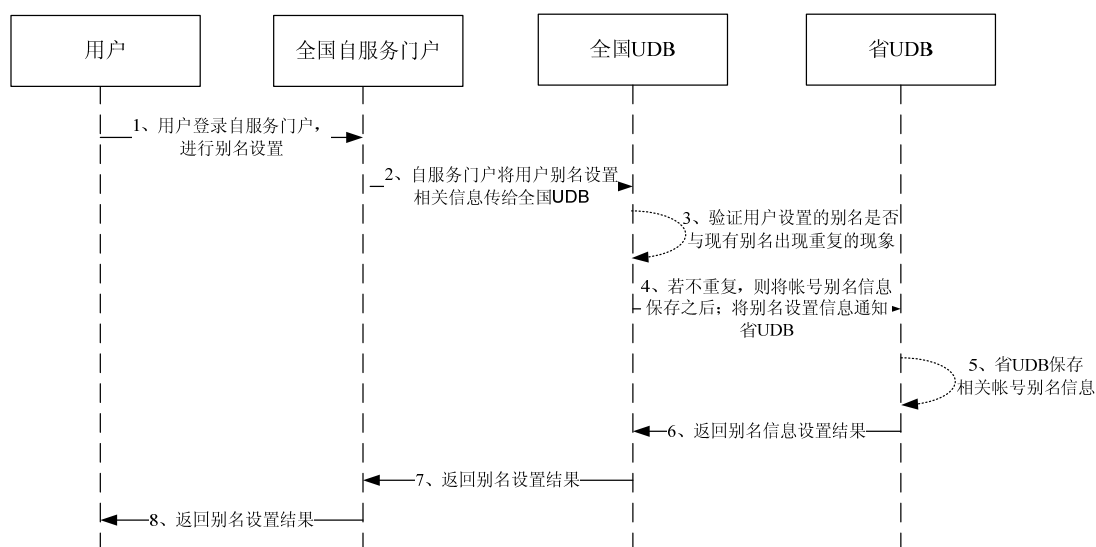
1. 用户登录省自服务门户，进行别名设置：输入别名，并点击“确认”；
2. 省自服务门户将用户别名设置相关信息传给省UDB；
3. 省UDB将用户别名及帐号的全部信息传给全国UDB；（帐号信息更新接口，更新标识位为8，全国UDB即要保存用户帐号，也要做别名验证）

4. 全国UDB对于用户设置的别名进行唯一性验证，如果没有出现别名重复的情况，则保存记录相关帐号所有信息；如果重复，则返回失败结果；
5. 全国UDB向省UDB返回别名设置验证的结果；
6. 省UDB对于验证通过的别名，保存相关帐号别名信息，如果该帐号尚未标识为“全国活跃用户”，则打标记；对于失败，则不作记录；
7. 省UDB向省自服务门户返回别名设置结果消息；
8. 省自服务门户向用户返回别名设置结果。

### 9.2.2.2 全国一>省

**触发条件：**用户登录全国自服务门户后，点击“设置别名”。

**交互流程：**



**流程描述：**

1. 用户登录全国自服务门户，进行别名设置；
2. 全国自服务门户将用户别名设置相关信息传给全国UDB；
3. 全国UDB对于用户设置的别名进行验证，是否出现别名重复的情况
4. 若不重复，全国UDB保存相关帐号别名信息，并将用户别名设置相关信息通知给省UDB（帐号信息更新接口）；
5. 省UDB保存相关帐号别名信息；
6. 省UDB向全国UDB返回别名设置结果；

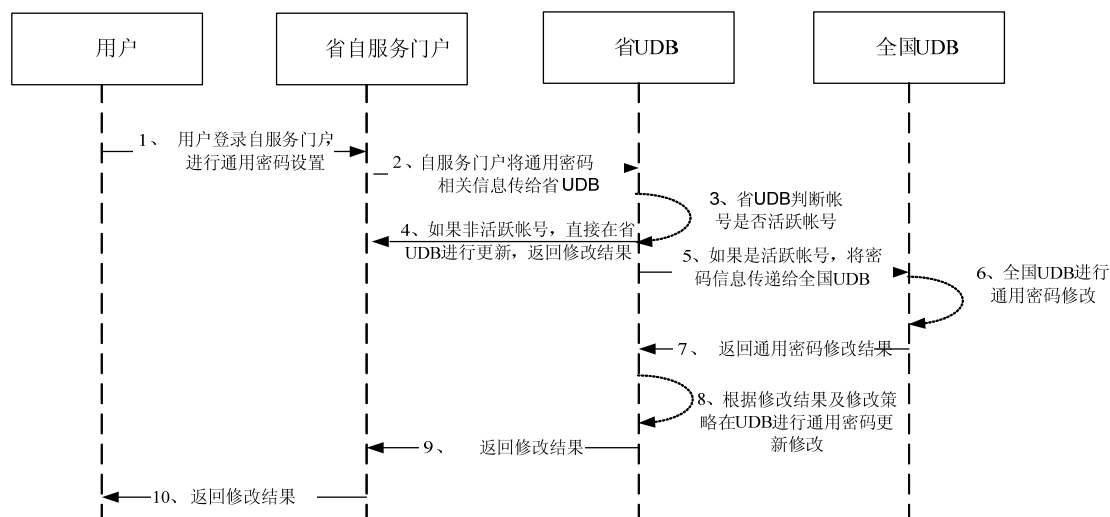
7. 全国UDB向全国自服务门户返回别名设置结果；
8. 全国自服务门户向用户返回别名设置结果。

## 9.2.3 通用密码设置

### 9.2.3.1 省→全国

**触发条件：**用户登录省自服务门户后，点击“设置通用密码”，输入密码之后，点击“确认”。

**交互流程：**



**流程描述：**

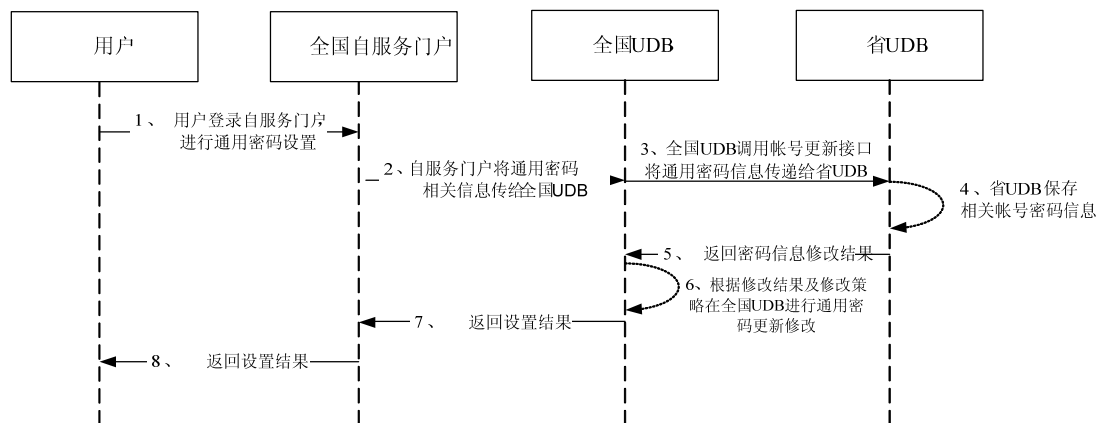
1. 用户登录省自服务门户，进行通用密码设置：输入密码，点击“确认”；
2. 省自服务门户将通用密码设置相关信息传给省UDB；
3. 省UDB判断帐号是否“全国平台活跃”帐号；
4. 如果帐号非全国活跃帐号，则根据“通用密码格式”进行密码有效性验证，若通过则直接在省UDB进行密码更新，然后向省自服务门户返回更新结果；
5. 如果帐号是全国活跃帐号，省UDB通过帐号信息更新接口（通用密码更新）将密码信息传递给全国UDB；
6. 全国UDB进行通用密码更新操作：根据“通用密码格式”进行密码有效性验证，若通过则直接在全国保存；
7. 全国UDB向省UDB返回更新结果；

8. 省UDB根据更新结果及更新策略进行更新（如果全国UDB更新成功，直接进行省UDB的密码更新；如果全国UDB更新失败，省UDB根据更新策略的配置决定是否允许继续更新）；
9. 省UDB向省自服务门户返回更新结果；
10. 省自服务门户向用户返回更新结果。

### 9.2.3.2 全国一>省

**触发条件：**用户登录全国自服务门户后，点击“设置通用密码”，输入密码之后，点击“确认”。

**交互流程：**



**流程描述：**

1. 用户登录全国自服务门户，进行通用密码设置：输入密码，点击“确认”；
2. 全国自服务门户将通用密码设置相关信息传给全国UDB；
3. 全国UDB通过帐号信息更新接口（通用密码更新）将密码传递给省UDB；
4. 省UDB进行通用密码更新操作：根据“通用密码格式”进行密码有效性验证，若通过则直接保存；
5. 省UDB向全国UDB返回更新结果；
6. 全国UDB根据更新结果及更新策略进行更新（如果省UDB更新成功，直接进行全国UDB的密码更新；如果省UDB更新失败，全国UDB根据更新策略的配置决定是否允许继续更新）；
7. 全国UDB向全国自服务门户返回更新结果；



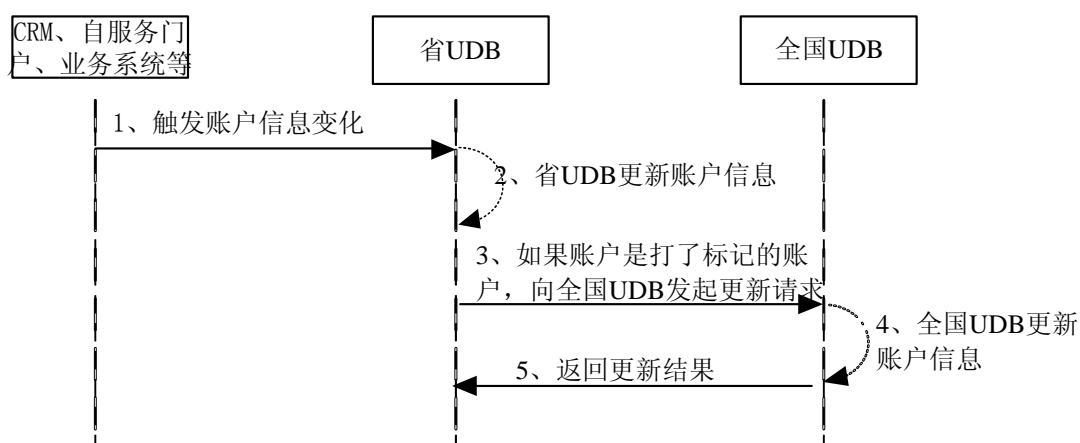
8. 全国自服务门户向用户返回更新结果。

## 9.2.4 其他信息更新

### 9.2.4.1 省→全国

**触发条件：**用户帐号信息发生变更（如用户状态、付费类型/套餐属性等），则省 UDB 记录后，若该用户为全国活跃标记用户，则向全国 UDB 发起用户帐号信息更新请求。

**交互流程：**



**流程描述：**

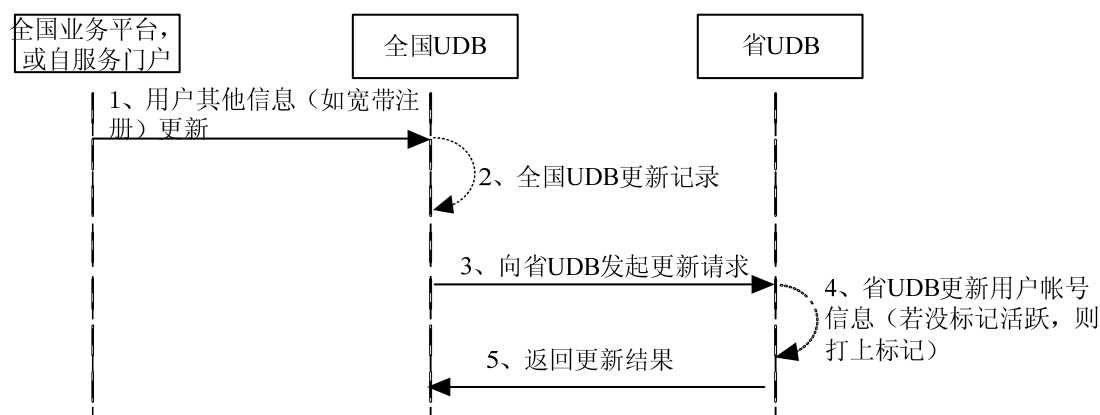
- 1) 省CRM、自服务门户、应用系统等触发了用户帐号信息的变更；
- 2) 省UDB更新帐号信息，并保存；
- 3) 省UDB判断统一帐号的状态，如果打了全国活跃用户标记，则向全国UDB发起帐号更新请求；
- 4) 全国UDB更新帐号信息；（如果帐号不存在则创建）
- 5) 向省UDB返回更新结果。（若反馈结果更新失败，省UDB可根据策略决定是否重发，或定时重发更新）

### 9.2.4.2 全国→省

**触发条件：**用户在全国业务平台，或全国自服务门户发起了用户帐号信息的变更（如宽带用户注册等），则全国 UDB 记录信息：若该帐号信息源自省内 UDB，

则向省 UDB 发起帐号信息更新请求。

**交互流程：**



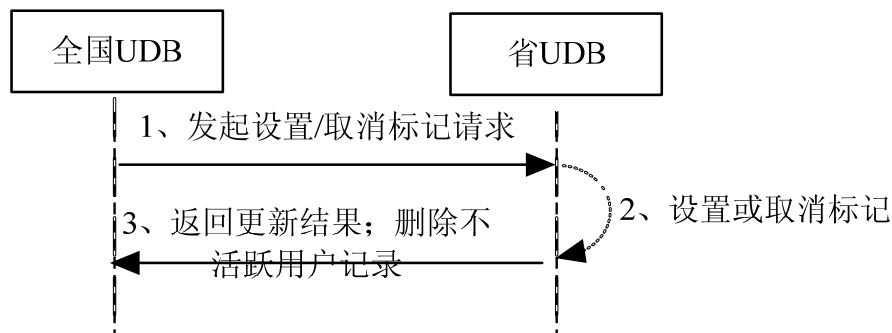
**流程描述：**

- 1) 在全国业务平台，或全国自服务门户触发了帐号信息变更（如宽带用户注册）的请求；
- 2) 全国UDB更新统一帐号用户的相关信息；
- 3) 全国UDB根据号码向归属省UDB发起更新请求：若该帐号信息源自省内UDB，则向省UDB发起用户帐号信息更新请求；
- 4) 省UDB进行帐号信息更新。若没标记，则标记此帐号为全国活跃帐号；
- 5) 省UDB向全国UDB返回更新结果。（若反馈结果更新失败，省UDB可根据策略决定是否重发，或定时重发更新）

### 9.2.5 设置/取消活跃标记

**触发条件：**全国 UDB 定期对其所保存的帐号进行检查：对一段时限内不活跃的用户帐号进行批量清理（对于带别名的帐号不能进行清除），并向省 UDB 发起取消标记的请求；对重要的帐号，要求省内进行全国活跃用户的标记，以便及时更新状态。

**交互流程：**

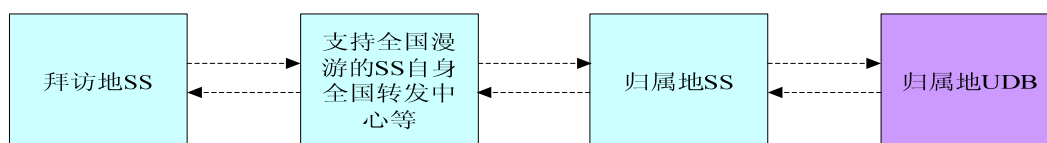


#### 流程描述：

- 1) 全国UDB对帐号进行定期检查，对重要帐号及不活跃帐号向省UDB发起设置/取消标记的请求；
- 2) 省UDB对统一帐号进行标记设置或取消；
- 3) 向全国UDB返回更新结果；全国UDB进行不活跃用户的清理。

### 9.2.6 漫游认证转发流程

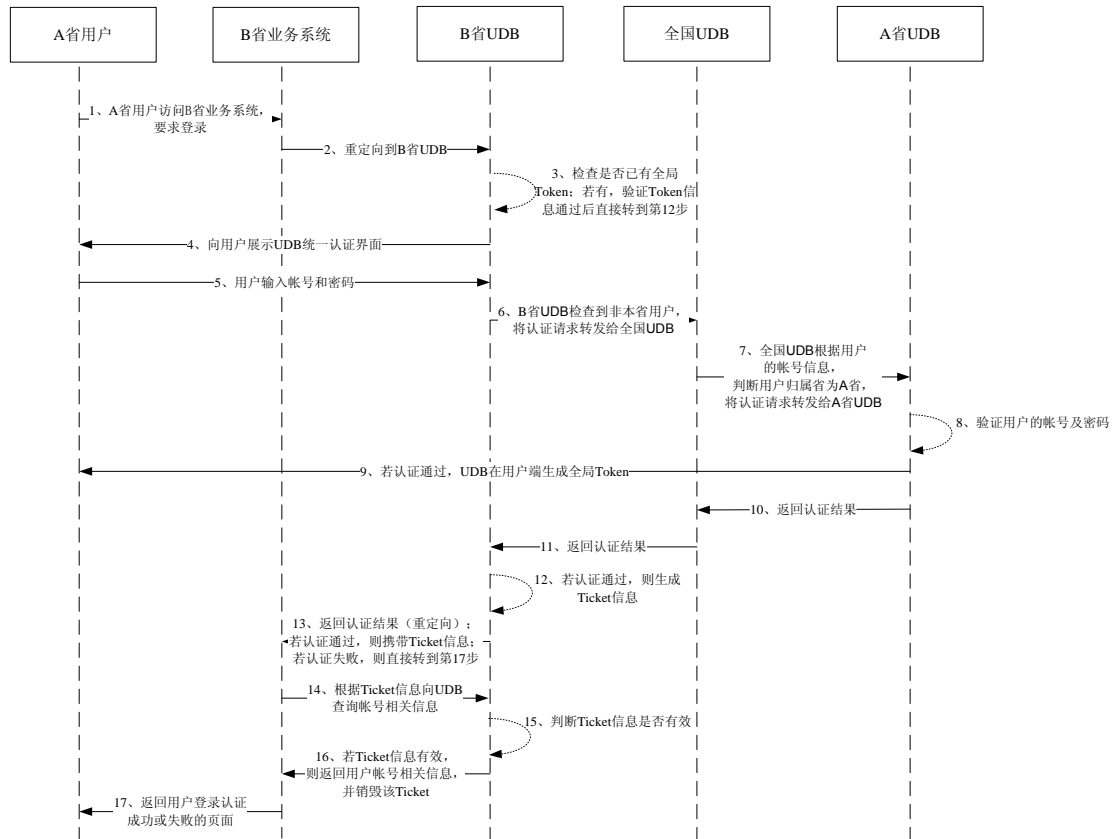
对于中国电信应用系统本身已支持全国统一帐号漫游机制的话，原则上仍通过原有应用系统的漫游机制回到归属地应用系统，然后再与归属地 UDB 进行认证交互，流程关系如下图所示：



对于按省接入的应用系统，若原有应用系统不支持全国漫游或外省市用户的登录，那么部署 UDB 后也没必要进行漫游认证转发。本处重点对那些需要 UDB 进行漫游认证转发的应用系统提供服务。

**触发条件：** A 省用户访问 B 省应用系统，发送登录认证请求。

**交互流程：**



### 流程描述：

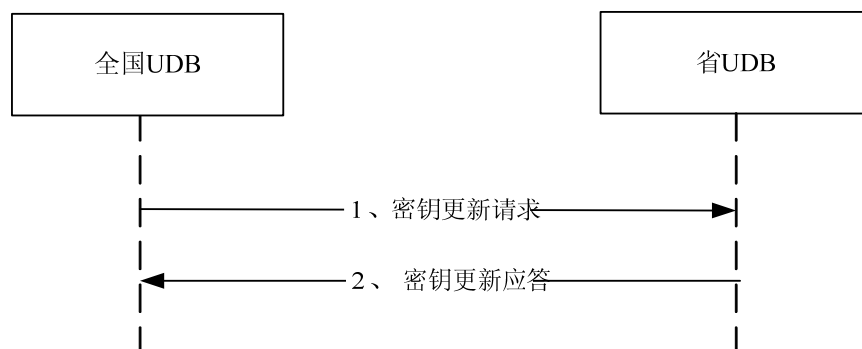
1. A省用户登录B省应用系统，发送登录认证请求；
2. B省应用系统调用重定向认证请求接口发送给B省UDB；
3. B省UDB检查重定向是否有携带用户全局Token信息；若已存在全局Token，则对Token信息进行验证，验证通过后直接转到第12步；
4. B省UDB向用户展示UDB统一认证登录界面；
5. 用户输入统一帐号和密码；
6. B省UDB检查到非本省用户，将认证请求转发给全国UDB，调用业务认证请求接口（使用SOAP协议）；
7. 全国UDB根据用户的帐号信息，判断用户的归属省为A省，将认证请求转发给A省UDB，调用业务认证请求接口（使用SOAP协议）；
8. A省UDB验证用户的帐号及密码；
9. 若验证通过，A省UDB在用户端生成全局Token，写内存Cookie；
10. A省UDB向全国UDB返回认证结果；
11. 全国UDB向B省UDB返回认证结果；

12. 若认证通过，B省UDB生成Ticket信息；
13. B省UDB重定向并返回认证结果信息到B省应用系统；若认证通过，则重定向消息中还需携带Ticket消息；若认证未通过，则直接转到第17步；
14. B省应用系统根据Ticket信息向B省UDB查询用户帐号相关信息，调用用户身份信息查询接口；
15. B省UDB判断Ticket信息是否有效；
16. 若Ticket信息有效，则B省UDB向B省应用系统返回用户帐号相关信息，并销毁该Ticket；
17. B省应用系统返回给用户登录成功或失败的界面（若为首次登录，则是否需注册等由应用系统决定）。

### 9.2.7 安全密钥管理流程

**触发条件：**全国 UDB 向各省 UDB 定期（不定期）主动更新密钥，以避免出现密钥泄露的情况。

**交互流程：**



**流程描述：**

1. 全国UDB更新密钥后，定时或紧急通知省UDB进行密钥更新；
2. 省UDB收到密钥更新请求，进行密钥更新，反馈更新结果；

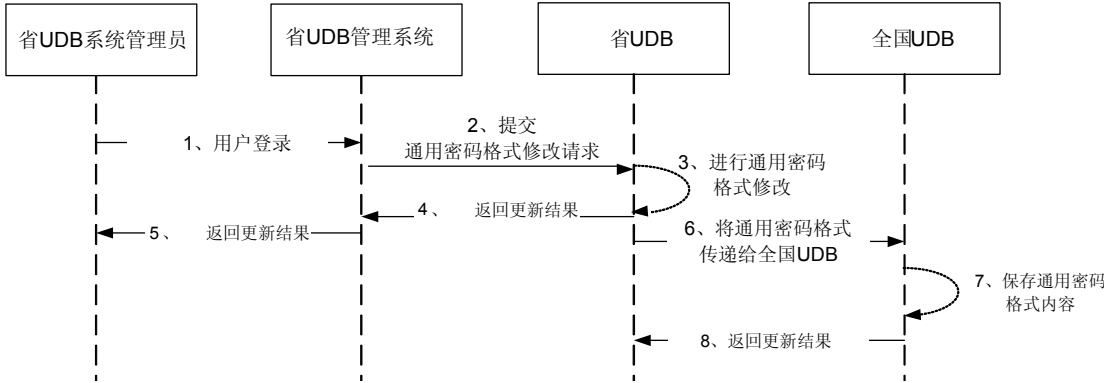
### 9.2.8 通用密码格式通知

通用密码的具体格式，可根据各省公司帐号经营的市场策略来订，由省UDB 系统管理员配置管理，然后通知全国 UDB，以确保同一省的用户在使用

省内和全国业务平台的服务体验及感知一致性。

**触发条件：**省 UDB 系统管理员进行通用密码格式设置，并通知全国 UDB。

**交互流程：**



**流程描述：**

1. 省UDB系统管理员登录省UDB的管理系统；
2. 进行通用密码格式设置或修改，并提交给省UDB；
3. 省UDB进行通用密码格式修改保存；
4. 省UDB向省UDB管理系统返回更新结果；
5. 省UDB管理系统通知省UDB系统管理员更新结果；
6. 省UDB定时将通用密码更新结果通知全国UDB；
7. 全国UDB进行通用密码格式的规则更新；
8. 全国UDB向省UDB返回更新结果。

### 9.2.9 个人通讯录信息

参见“中国电信通行证系统统一通讯录”的相关规范。

## 9.3 接口内容

全国 UDB 和省 UDB 之间的帐号信息查询接口、帐号信息更新接口、认证转发接口（认证请求接口）、安全密钥更新接口等，参见公共 Web Service 接口部分。

### 9.3.1 设置/取消全国活跃标记

全国 UDB 定期对其所保存的帐号进行检查：对一段时限内不活跃用户，并且没有设置别名的用户帐号，进行批量清理，并向省 UDB 发起取消标记的请求。

全国 UDB 也可根据业务开展需要，对部分帐号，要求省内进行“全国活跃用户”的批量设置标记，以便省内及时将更新状态向全国同步。

#### (1) 接口信息：

接口名称	AccountMarkRefresh
接口描述	全国 UDB 向省 UDB 发起请求，对省 UDB 中的帐号进行全国活跃用户标记设置或取消标记
请求消息名	AccountMarkRefreshRequest
应答消息名	AccountMarkRefreshResponse

#### (2) 参数说明

##### 1) 请求参数

AccountMarkRefreshRequest 包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发送端应用系统设备标识，标明由全国 UDB 发起请求
UserIDList	UserIDInfo	—	1	进行标记设置或取消的帐号数组
OpeType	Integer	1	1	操作类型： 0:取消标记 1:设置标记

UserIDInfo 定义如下：

参数名称	数据类型	长度（字节）	出现频次	说明
UserID	String	40	1-n	统一帐号

##### 2) 响应消息

AccountMarkRefreshResponse 包含如下信息：

名称	数据类型	长度（字节）	出现频次	说明
ResultCode	Integer	2	1	结果码，统一定义
Description	String	128	1	对操作结果的详细描述信息

### 9.3.2 通用密码格式更新接口

(1) 接口信息：

接口名称	NormalPWDStyleRefresh
接口描述	通用密码的格式根据各省公司帐号经营的市场策略来订，由省 UDB 系统管理员配置管理保存在省 UDB，然后通知全国 UDB。
请求消息名	NormalPWDStyleRefreshRequest
应答消息名	NormalPWDStyleRefreshResponse

(2) 参数说明

1) 请求参数

NormalPWDStyleRefreshRequest 包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发送端应用系统设备标识，即省 UDB
NormalPWDStyle	String	2	1	通用密码格式
TimeStamp	String	19	1	时间戳时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

2) 响应消息

NormalPWDStyleRefreshResponse 包含如下信息：

名称	数据类型	长度（字节）	出现频次	说明
ResultCode	Integer	2	1	结果码，统一定义
Description	String	128	0-1	对操作结果的详细描述信息



## 10 单点登录功能接口

### 10.1 接口概述

单点登录功能，是指用户在成功登录中国电信的宽带接入、网厅或业务平台之后，已经获得用户身份合法性验证，再访问中国电信其他应用及服务时，或者是中国电信信任的第三方应用，无须二次认证即可直接登录。

注：对于用户设置了私有密码的应用系统，该应用系统不允许单点登录功能，链接其他应用系统必需进行二次认证；只有必过通用密码验证成功之后才具有生成全局 UDBToken 能力，才能单点登录。

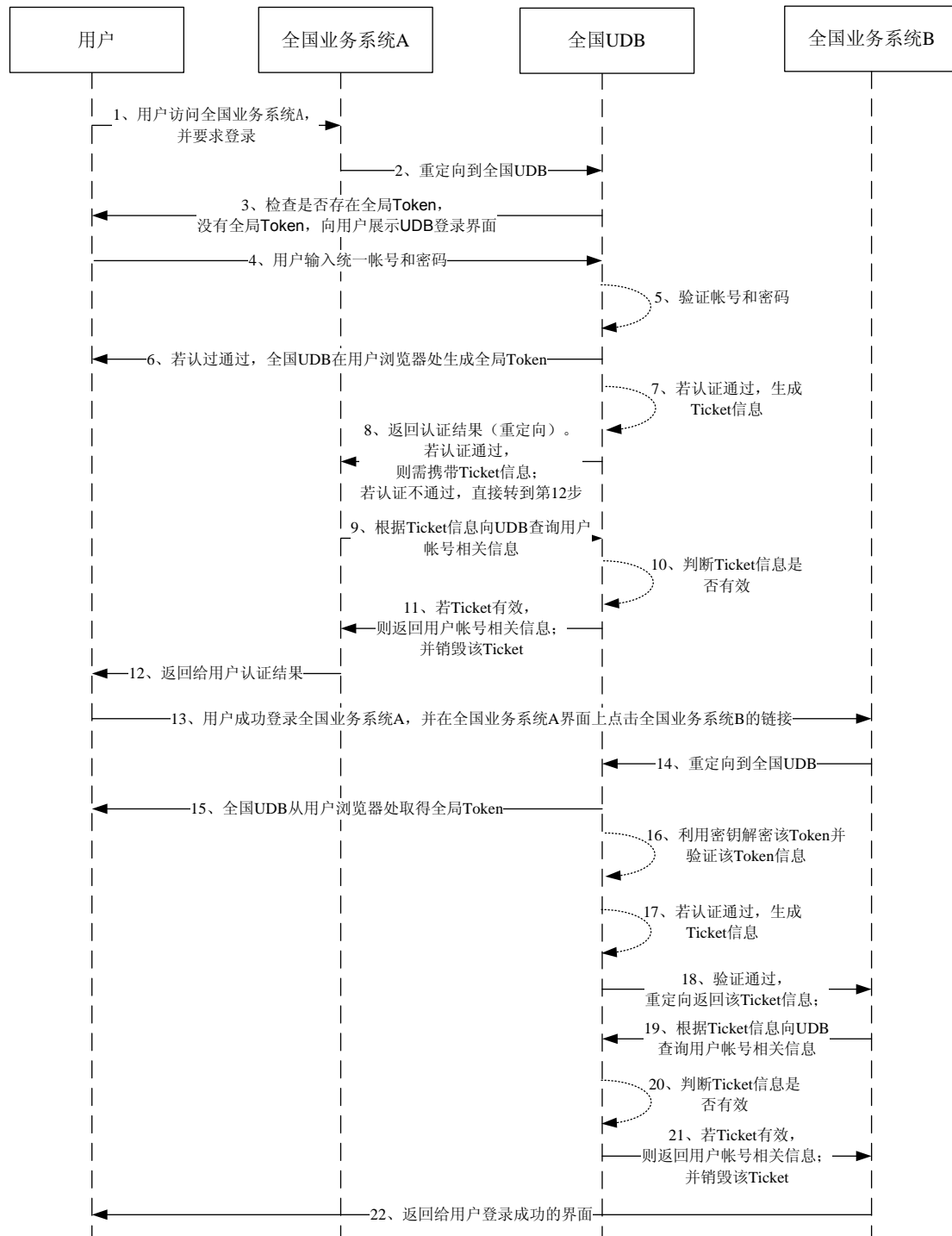
### 10.2 接口流程

#### 10.2.1 全国性平台（或省级平台）内部的SSO

**触发条件：**用户成功登陆全国应用系统 A，在全国应用系统 A 中点击登录全国应用系统 B 的链接。

注：需要实现 SSO 的应用系统必须调用重定向接口，不能调用 SOAP 接口。

**交互流程：**



#### 流程描述：

1. 用户访问全国应用系统A，并要求登录；
2. 全国应用系统A调用重定向认证请求接口发送给全国UDB；
3. 全国UDB检查是否存在用户全局Token。没有全局Token，向用户展示UDB登录界面；
4. 用户输入统一帐号和密码，并提交；

5. 全国UDB对帐号和密码进行验证；
6. 若认证通过，全国UDB在用户浏览器处生成全局Token，写内存Cookie；
7. 若认证通过，全国UDB生成Ticket消息；
8. 全国UDB通过重定向的方式向全国应用系统A返回认证结果；若认证通过，则重定向消息中还需要携带Ticket消息；若认证不通过，则直接转到第12步；
9. 全国应用系统A根据Ticket信息向全国UDB查询用户帐号信息，调用用户身份信息查询接口；
10. 全国UDB判断Ticket信息是否有效；
11. 若Ticket有效，全国UDB向全国应用系统A返回用户帐号相关信息；同时UDB销毁该Ticket；
12. 全国应用系统A将认证结果返回给用户；
13. 用户成功登录全国应用系统A后，在全国应用系统A的界面上点击全国应用系统B的链接；
14. 全国应用系统B调用重定向认证请求接口发送给全国UDB；
15. 全国UDB从用户浏览器处取得全局Token；
16. 全国UDB利用密钥解密全局Token信息，并对Token进行验证；
17. 若Token认证通过，全国UDB生成Ticket消息；
18. 若认证通过，全国UDB通过重定向的方式向全国应用系统B返回认证结果以及Ticket信息；若Token验证未通过，则全国UDB通过重定向的方式向全国应用系统B返回认证失败的结果；
19. 全国应用系统B根据Ticket信息向全国UDB查询用户帐号信息，调用用户身份信息查询接口；
20. 全国UDB判断Ticket信息是否有效；
21. 若Ticket有效，全国UDB向全国应用系统B返回用户帐号相关信息；同时全国UDB销毁该Ticket；
22. 全国应用系统B向用户返回登录成功的界面。

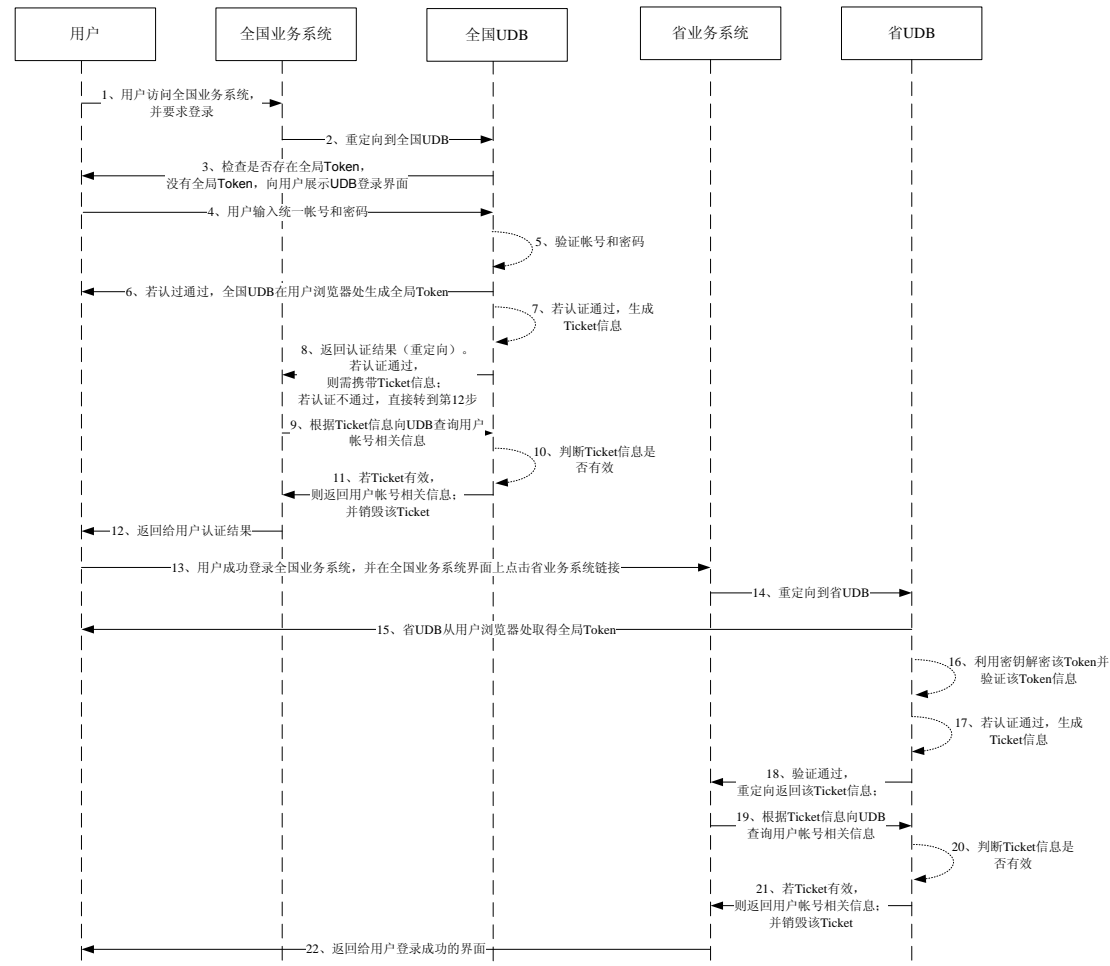
### 10.2.2 全国性—省级平台之间的SSO

用户先访问省内平台再访问全国平台，与先访问全国平台再访问省内平台，

其流程基本相似；以下主要描述以下先访问全国应用再到省内应用的流程。

**触发条件：**用户成功登陆全国应用系统，在全国应用系统中点击登录省应用系统的链接。

**交互流程：**



**流程描述：**

1. 用户访问全国应用系统，并要求登录；
2. 全国应用系统调用重定向认证请求接口发送给全国UDB；
3. 全国UDB检查是否存在用户全局Token。没有全局Token，向用户展示UDB登录界面；
4. 用户输入统一帐号和密码，并提交；
5. 全国UDB对帐号和密码进行验证；
6. 若认证通过，全国UDB在用户浏览器处生成全局Token，写内存Cookie；
7. 若认证通过，全国UDB生成Ticket消息；
8. 全国UDB通过重定向的方式向全国应用系统返回认证结果；若认证通

过，则重定向消息中还需要携带Ticket消息；若认证不通过，则直接转到第12步；

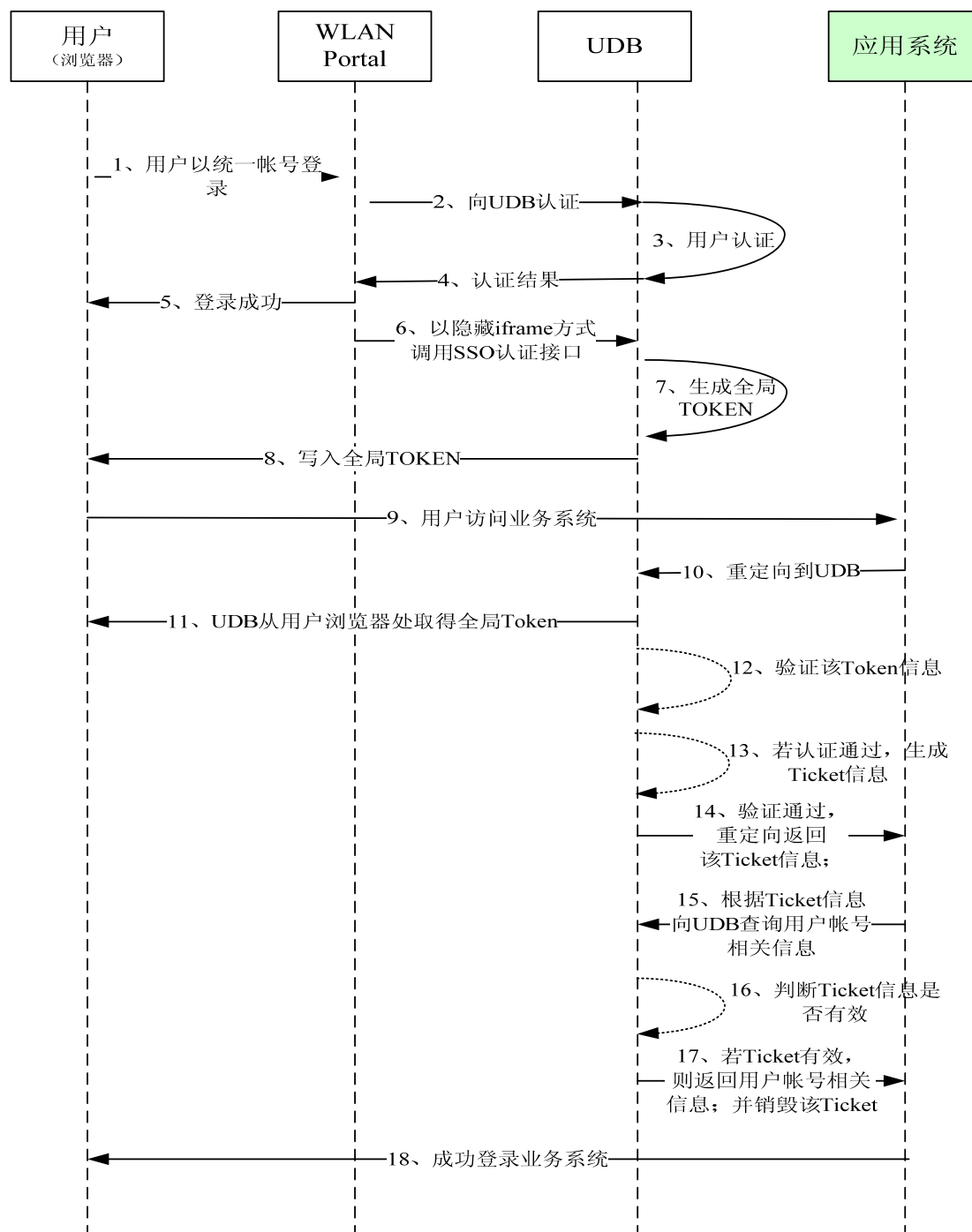
9. 全国应用系统根据Ticket信息向全国UDB查询用户帐号信息，，调用用户身份信息查询接口；
10. 全国UDB判断Ticket信息是否有效；
11. 若Ticket有效，全国UDB向全国应用系统返回用户帐号相关信息；同时全国UDB销毁该Ticket；
12. 全国应用系统将认证结果返回给用户；
13. 用户成功登录全国应用系统后，在全国应用系统的界面上点击省应用系统的链接；
14. 省应用系统调用重定向认证请求接口发送给省UDB；
15. 省UDB从用户浏览器处取得全局Token；
16. 省UDB利用密钥解密全局Token信息，并对Token进行验证；
17. 若Token认证通过，省UDB生成Ticket消息；
18. 若认证通过，省UDB通过重定向的方式向省应用系统返回认证结果以及Ticket信息；若Token验证未通过，则省UDB通过重定向的方式向省应用系统返回认证失败的结果；
19. 省应用系统根据Ticket信息向省UDB查询用户帐号信息，调用用户身份信息查询接口；
20. 省UDB判断Ticket信息是否有效；
21. 若Ticket有效，省UDB向省应用系统返回用户帐号相关信息；同时省UDB销毁该Ticket；
22. 省应用系统向用户返回登录成功的界面。

### 10.2.3 宽带接入—应用系统的SSO

**触发条件：**用户通过统一帐号成功登录宽带之后，点击访问（或同一窗口输入网址浏览）中国电信其他应用系统时，无须二次认证便可直接使用。

**交互流程：**

通过WLAN Portal进行宽带接入的流程

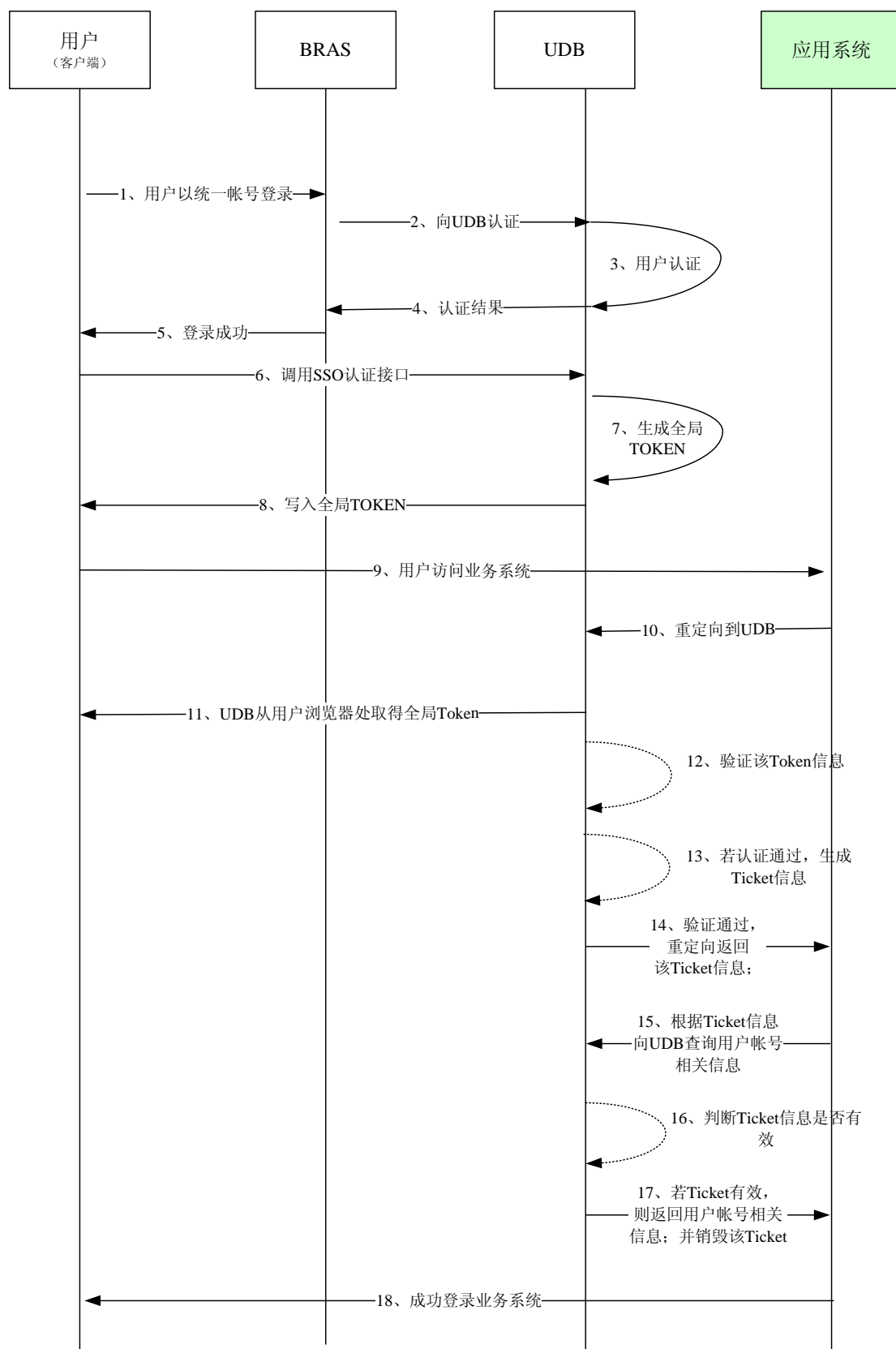


#### 流程描述：

1. 用户在WLAN Portal输入统一认证帐号和密码，输入统一帐号及通用密码，；
2. WLAN Portal识别输入的帐号后缀域名（@189.cn），将统一帐号的宽带接入认证请求报文转发UDB；
3. UDB检验用户帐号及密码验证的有效性
4. UDB将认证结果返回（认证拒绝报文，或认证转发报文）；

5. 通知用户登陆成功;
6. 登录成功后, WLAN Portal通过隐藏iframe的方式调用UDB提供的客户端单点登录接口(含用户名和用户密码)。
7. UDB再次检查用户密码, 并生成全局Token;
8. UDB在客户端浏览器内存写全局Token信息, 生成Cookie;
9. 用户发起访问应用系统的请求;
10. 应用系统调用重定向认证请求接口发送给UDB;
11. UDB从用户处获取全局Token;
12. UDB验证该Token信息;
13. 若Token验证通过, UDB生成Ticket消息;
14. 若认证通过, UDB通过重定向的方式向应用系统返回认证结果以及该Ticket消息; 若Token验证未通过, 则UDB通过重定向的方式向应用系统返回认证失败的结果;
15. 应用系统根据Ticket信息向UDB查询用户帐号信息, 调用用户身份信息查询接口;
16. UDB判断Ticket信息是否有效;
17. 若Ticket有效, UDB向应用系统返回用户帐号相关信息; 同时UDB销毁该Ticket;
18. 用户成功单点登录应用系统。

通过专用客户端进行宽带接入的流程



### 流程描述:

1. 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

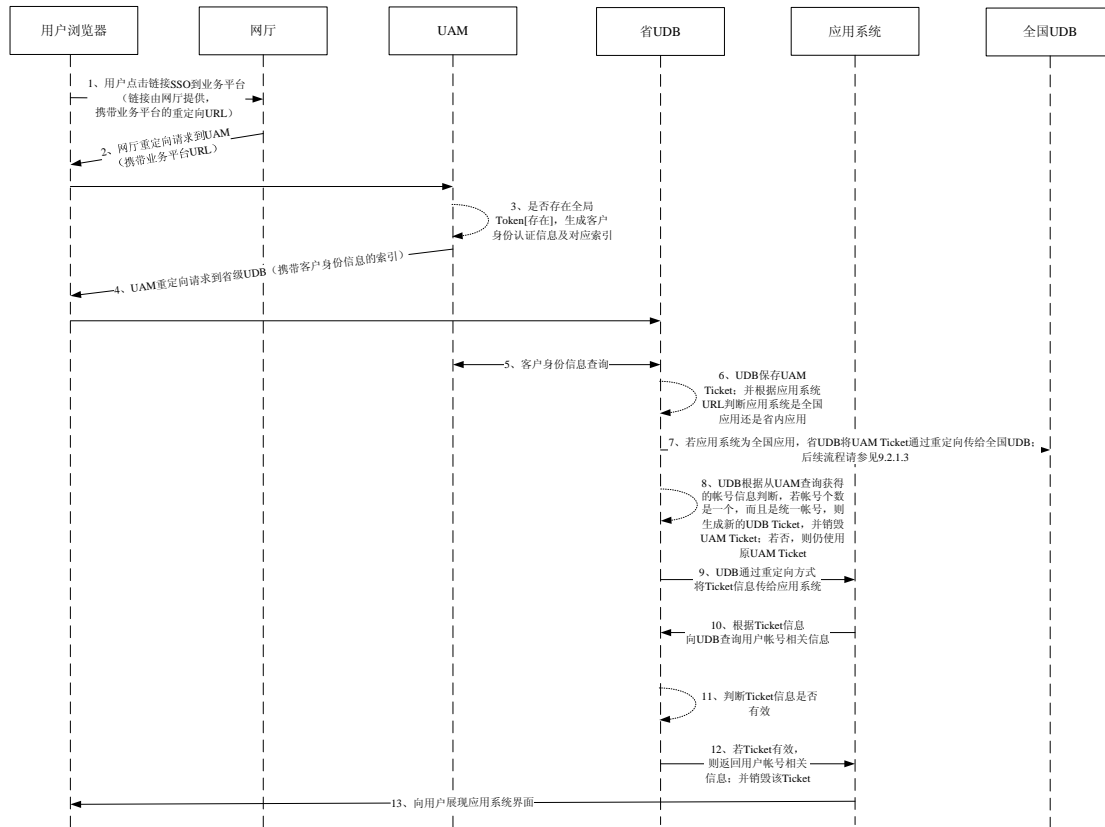


通用密码，进行宽带拨号；

2. BRAS通过PPPoE客户端输入的帐号后缀域名（@189.cn），将统一帐号的拨号登录认证请求转发给向UDB转发认证请求；
3. UDB检验用户帐号及密码验证的有效性
4. UDB将认证结果返回；
5. 通知用户登陆成功；
6. 登录成功后，客户端调用UDB提供的客户端单点登录认证接口（含用户名和用户密码）；
7. UDB再次检查用户密码，并生成全局Token
8. UDB在客户端软件的内嵌浏览器写入Token信息；
9. 用户发起访问应用系统的请求；
10. 应用系统调用重定向认证请求接口发送给UDB；
11. UDB从用户处获取全局Token；
12. UDB验证该Token信息；
13. 若Token验证通过，UDB生成Ticket消息；
14. 若认证通过，UDB通过重定向的方式向应用系统返回认证结果以及该Ticket消息；若Token验证未通过，则UDB通过重定向的方式向应用系统返回认证失败的结果；
15. 应用系统根据Ticket信息向UDB查询用户帐号信息，调用用户身份信息查询接口；
16. UDB判断Ticket信息是否有效；
17. 若Ticket有效，UDB向应用系统返回用户帐号相关信息；同时UDB销毁该Ticket；
18. 用户成功单点登录应用系统。

#### 10.2.4 网上营业厅—应用系统的SSO

用户登录网厅后，单点登录到与 UDB 对接的应用系统时流程如下：



1. 用户点击网厅上的链接单点登录到应用系统，单点登录的链接由网厅提供，携带应用系统的重定向URL；
2. 网厅携带“应用系统返回URL”重定向到省UAM；
3. 省UAM根据全局Token，生成当前客户的身份以及对应的索引Ticket；
4. 省UAM携带“客户身份索引”，通过UDB提供的重定向单点登录接口，重定向请求到省级UDB；
5. 省UDB根据“客户身份索引”查询对应的客户身份信息；
6. 省UDB保存UAM生成的UAM Ticket信息，并根据“应用系统返回URL”判断当前应用系统是全国应用系统还是省级应用系统；
7. 若应用系统为全国应用，省UDB调用全国UDB提供的重定向单点登录接口将UAM Ticket传给全国UDB；与全国UDB相关的后续流程请参见9.2.1.3的描述。
8. 若应用系统为省内应用，省UDB根据获得的客户身份信息进行判断：若身份信息中帐号个数是一个，而且该帐号是统一帐号，则省UDB生成新的UDB Ticket，销毁原UAM Ticket；若否，则仍使用原UAM Ticket；

9. 省UDB调用电信自营应用的SSO接口将Ticket信息传给省内应用系统；
10. 省内应用系统根据Ticket信息向省UDB查询用户帐号信息，调用用户身份信息查询接口；
11. 省UDB判断该Ticket信息是否有效；
12. 若Ticket有效，省UDB向省内应用系统返回用户帐号相关信息；同时省UDB销毁该Ticket；
13. 向用户展现全国应用系统界面。

注 1：无论用户单点登录的应用系统是全国平台还是省级平台，省 UAM 重定向到对应省的省级 UDB，由省 UDB 负责区分。

注 2：如果 UAM 给 UDB 的用户信息带有多个产品帐号，则应用系统不允许用户直接登录，必须选择一个帐号并进行正常登录验证过程。

## 10.3 接口消息

### 10.3.1 UDBToken格式及读取

UDBToken（令牌）是临时颁发的代表用户有效身份的凭证，例如在用户登录应用后由 UDB 发给用户的唯一标识字符串。Cookie 是保存在用户端的一小段文本信息，伴随着用户请求及页面在 Web 服务器和用户端浏览器之间传递。出于信息安全的考虑，服务器只能访问它所属 DNS 域的 Cookie。

UDBToken 采用内存 cookie 的形式保存在用户的浏览器端，其 domain 属性设置为 UDB 域名（待定），该 cookie 必须设置属性 httponly。

全局 UDBToken 是由 UDB 在用户端浏览器生成的，可实现用户在不同应用系统之间、宽带接入系统与应用系统之间、网厅与应用系统之间等进行单点登录的功能。由于全国 UDB 和省级 UDB 属于相同的 DNS 域，所以全国 UDB 能够访问省级 UDB 生成的全局 Token；省级 UDB 也能够访问全国 UDB 生成的全局 Token。

属性名	描述
SysDeviceNo	生成 UDBToken 的系统
ProvinceNo	用户所在省
PUserID	用户唯一标识
UserID	统一帐号
Alias	别名
ExpireTime	过期时间 标准时间格式 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区 目前对 UDBToken 设置为 2 小时过期
AuthType	登录认证的类型， 目前定义的类型为： 00：通用密码认证【默认】 01：短信/动态密码 02：OTP 认证 03：数字证书 08：新 E 家宽带认证或 IP 反查产生的 Passport 认证 09：新 E 家根据 PUserID 获取 Passport 信息

**UDBToken = SysDeviceNo + "\$" + UDBToken**

其中，SysDeviceNo 是生成 UDBToken 的系统 ID，加密算法采用 3DES，加密过程如下：

a. 生成摘要信息

Digest=Base64(SHA1(ProvinceNo+PUserID+UserID+Alias+ExpireTime + AuthType))

其中, Hash 算法采用 SHA-1, PUserID 为用户唯一标识。

b. 采用 3DES 算法对原始数据以及摘要信息进行加密, 如下所示

$$\text{UDBToken} = \text{Base64} \left( \text{3DES} \left( \text{OriginalUDBToken} + "\$"+\text{Digest} \right) \right)$$

其中，3DES 算法 Key=SysKey，SysKey 是中心用于加密 cookie 的统一密钥。

OriginalUDBToken 的格式:

OriginalUDBToken="ProvinceNo="+value+"\$"+PUserID="+value+"\$"

```
+"UserID="+value+"$"+"Alias="+value+"$"
```

+"ExpireTime="+value+"\$"+AuthType="+value

属性名大小写敏感，多个属性之间以“\$”分隔，在属性名与“=”之间不允许有空格，在属性值与“=”之间不允许有空格。

#### UDBToken 读取要求：

随着业务发展，在未来版本中 UDBToken 可以按照上述格式添加字段属性，对于新字段属性的增加，UDBToken 的读取和解释程序必须保证不受到影响。

建议 UDBToken 按顺序读取分隔的字段，得到相应的值。

### 10.3.2 UDB提供的客户端单点认证接口

#### 10.3.2.1 接口内容

(1) 接口信息：

接口名称	PassportSSOforClient
接口描述	提供给 WLAN Portal、IM 客户端等中国电信有特殊需求的系统单点认证接口，生成和分发全局 Token 信息。 UDB 系统可配置允许调用该接口的系统，只允许白名单中的系统调用。
请求消息名	http://省别简写.Passport.189.cn/ PassportSSOforClient
应答消息名	ReturnURL
接口协议	重定向
提供者	UDB 系统
主要使用者	WLAN Portal、IM 客户端等中国电信有特殊需求的系统

(2) 参数说明：

1) 请求消息

http:// 省 别 简 写 .Passport.189.cn/ PassportSSOforClient?  
PassportSSOforClientRequest =  
PassportSSOforClientRequestValue

注 1：对 E 家天翼客户端，SSO 接口的请求对象是全国 UDB；对 WLAN Portal，SSO 接口的请求对象是省 UDB。相应域名不同。

PassportSSOforClientRequestValue 为接口参数值，包含如下信息：

名称	数据类型	长度(字节)	说明
SrcSsDeviceNo	String	16	发起端的应用系统设备标识
TimeStamp	String	19	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区
UserID	String	40	用户统一帐号 手机号码、区号+固话号码等
Password	String	16	统一密码(加密)
ReturnURL	String		UDB 系统返回结果时需要调用的 URL

PassportSSOforClientRequestValue 的生成算法如下:

Digest = Base64(Hash(SrcSsDeviceNo + TimeStamp+ UserID + Password + ReturnURL))

其中, Hash 算法采用 SHA-1。

PassportSSOforClientRequest=URLEncoding(SrcSsDeviceNo+"\$"+Base64(Encrypt(TimeStamp+"\$"+UserID+"\$"+Password+"\$"+ReturnURL+"\$"+Digest)))

其中, 加密算法 Encrypt 采用 3DES, Key=SysKey, SysKey 是 UDB 系统发给该应用系统的密钥。

## 2) 应答消息

接口方法为:

http://ReturnURL?PassportSSOforClientResponse=

PassportSSOforClientResponseValue

其中, ReturnURL 从 PassportSSOforClientRequest 中获得。

PassportSSOforClientResponseValue 为接口参数值, 包含如下信息:

名称	数据类型	长度(字节)	说明
Result	Int	2	0: 成功 其他: 失败
DesSsDeviceNo	String	16	返回方应用系统设备标识
ProvinceID	String	2	统一帐号用户所在省
PUserID	String	11	用户唯一标识 2 位省 ID+9 位用户标识 ID
UserID	String	40	用户统一帐号
Alias	String	40	用户别名
TimeStamp	String	19	时间戳 yyyy-MM-dd HH:mm:ss, 其中 HH 取值为 00-23,时区为东八区

PassportSSOforClientResponseValue 的生成算法如下：

$$\text{Digest} = \text{Base64}(\text{Hash}(\text{Result} + \text{DesSsDeviceNo} + \text{ProvinceID} + \text{PUserID} + \text{UserID} + \text{Alias} + \text{TimeStamp}))$$

其中，Hash 算法采用 SHA-1。

$$\begin{aligned} \text{PassportSSOforClientResponseValue} = & \text{URLEncoding}(\text{DesSsDeviceNo} + \\ & \$ + \text{Base64}(\text{Encrypt}(\text{Result} + \$ + \text{ProvinceID} + \$ + \text{PUserID} + \$ + \text{UserID} \\ & + \$ + \text{Alias} + \$ + \text{TimeStamp} + \$ + \text{Digest}))) \end{aligned}$$

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，Syskey 是 UDB 系统颁发给该系统的密钥。

#### 10.3.2.2 对客户端的改造要求

天翼 E 家客户端的改造已完成，具备向全国 UDB 申请全局 Token 的单点登录功能。WLAN Portal 则需要各省公司独立改造。

### 10.3.3 UDB提供的UAM单点登录接口

#### 10.3.3.1 接口内容

参见 6.2.3 节，重定向单点登录接口。

#### 10.3.3.2 对应用系统的改造要求

对于一个客户帐号下只有一个产品帐号的情况，则应用系统允许用户直接成功登录，而不作任何选择和二次认证。

对于一个客户帐号下存在多个产品帐号标识的情况，该场景不再实现用户单点登录功能，必须要求用户选择其中的一个产品帐号。对于该场景，UDB 会将客户及产品帐号全部信息同步给应用系统，由应用系统通过界面控制用户选择其中一个产品帐号（对于在该应用系统不存在的产品帐号可剔除），并让用户

根据选择的产品帐号，输入相应密码进行二次认证。



## 11 自服务门户接口

### 11.1 自服务概述

用户自服务门户，主要是面向中国电信统一帐号用户提供的自助式管理的客户服务网站。自服务门户与 UDB 统一认证界面集成在一起。

除了包括用户信息维护、通用密码修改、业务（私有）密码设置、别名设置、宽带用户注册、记录查询等，今后个人通信录、群组管理、应用展示等功能可纳入自服务范畴，将围绕以用户数据库为核心的应用领域而不断扩展。

自服务门户网站分为全国和省分公司两级架构：全国中心主要提供全国通用管理能力，面向全国应用系统的相关展示服务，并提供到各省公司门户的链接服务；省分公司可在集团统一服务功能要求的基础上，也进一步根据省内统一帐号用户的特殊需求开发具本地特色的服务功能。各省公司运行初期也可直接借用全国自服务门户能力，而不单独建设。

全国自服务门户和省分公司自服务门户采用统一域名，初步定为“passport.189.cn”和“省别简称.passport.189.cn”的域名。

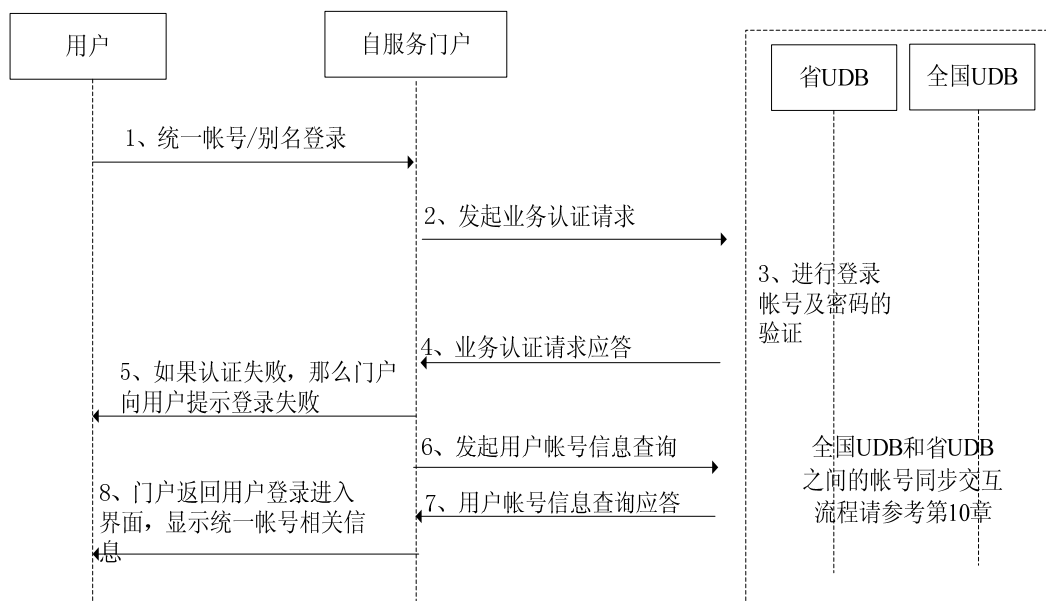
以下章节的流程和接口对全国自服务门户和省自服务门户均适用，流程可根据省内自服务门户的功能而调整。

### 11.2 接口流程

自服务门户只与归属地 UDB 交互（全国门户只与全国 UDB 交互）。本节重点在描述门户与 UDB 之间交互流程，由于自服务门户的信息查询、修改和设置所引起的全国 UDB 和省 UDB 之间信息交互流程具体参见第 9 章，本处以全国 UDB 和省 UDB 简化其流程，避免重复描述。

#### 11.2.1 自服务门户登录

**触发条件：**用户通过自服务门户网站输入统一帐号（或别名）和通用密码进行登录，由归属地 UDB 提供验证服务，如果正确将返回用户所有相关信息。

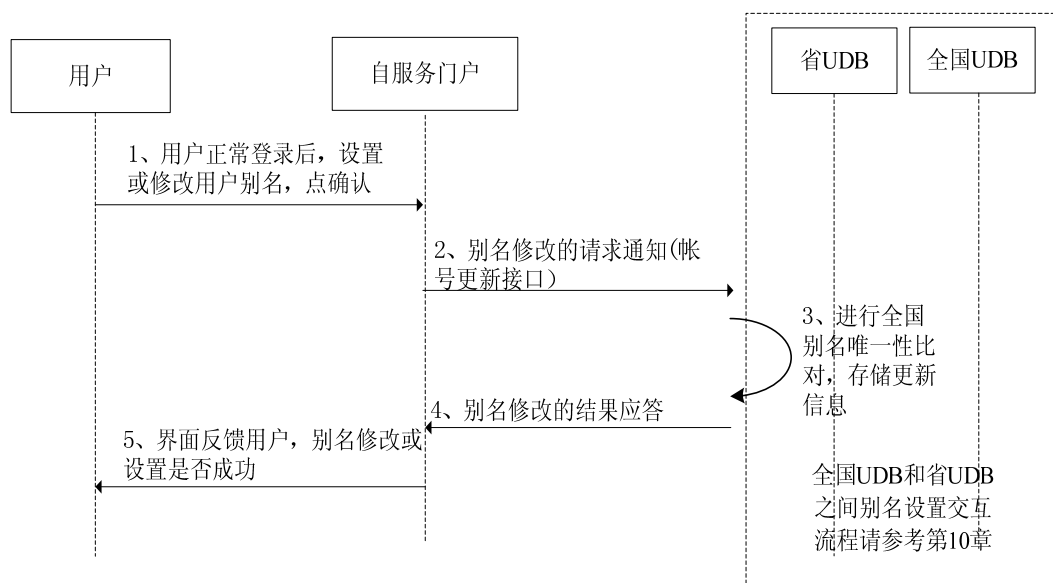
**交互流程：****流程描述：**

- 1) 用户使用统一帐号+通用密码登录自服务门户；
- 2) 用户自服务门户向UDB进行用户的认证请求；
- 3) UDB执行自服务门户的认证请求；
- 4) UDB将认证结果返回给用户自服务门户；
- 5) 如果认证失败，则自服务门户提示用户认证失败和失败的原因；
- 6) 如果认证成功，自服务门户继续向UDB查询该用户的帐号信息；
- 7) UDB返回用户帐号信息的查询结果；
- 8) 自服务门户显示统一帐号的用户基本信息、注册状态、密码策略等信息。

**11.2.2 用户帐号别名设置**

**触发条件：**用户通过自服务门户进行别名设置或修改操作。

**交互流程：**



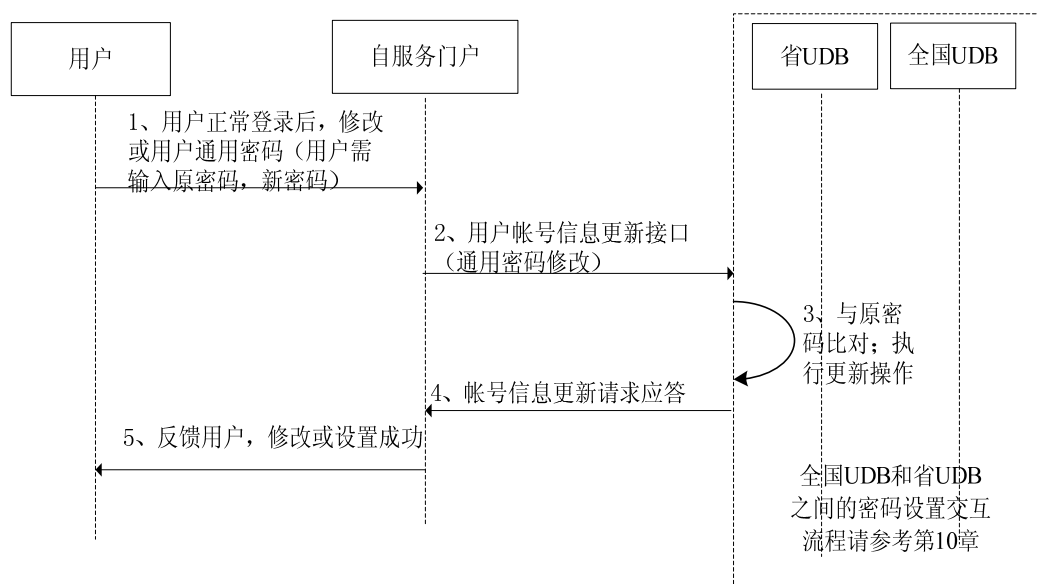
#### 流程描述：

- 1) 用户登录自服务门户成功后，对帐号别名进行设置或修改，并点击确认；
- 2) 用户自服务门户向UDB发起用户帐号别名的修改请求消息；
- 3) UDB执行全国别名的唯一性检验，如合法则存储别名，修改成功；
- 4) UDB将修改结果返回给用户自服务门户；
- 5) 自服务门户反馈给用户，别名修改或设置成功与否。

### 11.2.3 通用密码修改设置

**触发条件：**用户通过自服务门户进行统一帐号的通用密码的修改。

**交互流程：**



#### 流程描述：

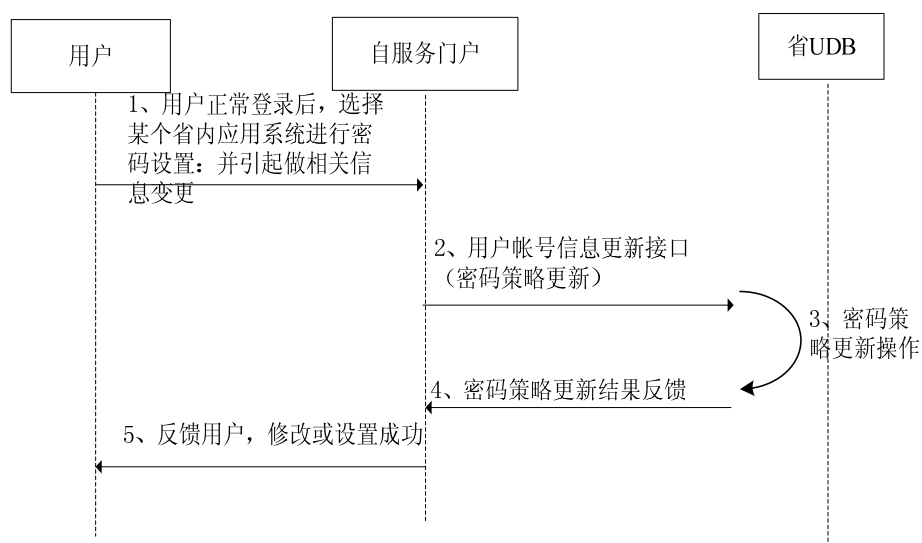
- 1) 用户登录自服务门户成功后，对通用密码进行修改：用户需输入原密码，新密码（二次）；
- 2) 用户自服务门户向UDB发起用户帐号信息更新请求；
- 3) UDB执行自服务门户的帐号更新请求，若原密码正确，则保存新密码；
- 4) UDB将更新请求结果返回给用户自服务门户；
- 5) 反馈给用户，用户通用密码修改成功与否。

### 11.2.4 业务(私有)密码设置

**触发条件：**这主要针对省公司在自服务门户为用户提供灵活的密码策略场景，即满足用户在某些具体应用系统设置单独业务/私有密码。

用户通过自服务门户进行应用系统的密码设置：对省内应用系统，可直接提供密码策略选择，及业务密码修改界面；对全国性应用系统，则直接单独转到全国性应用系统进行相关服务。以下主要以省内平台的密码设置流程描述。

#### 交互流程：



#### 流程描述：

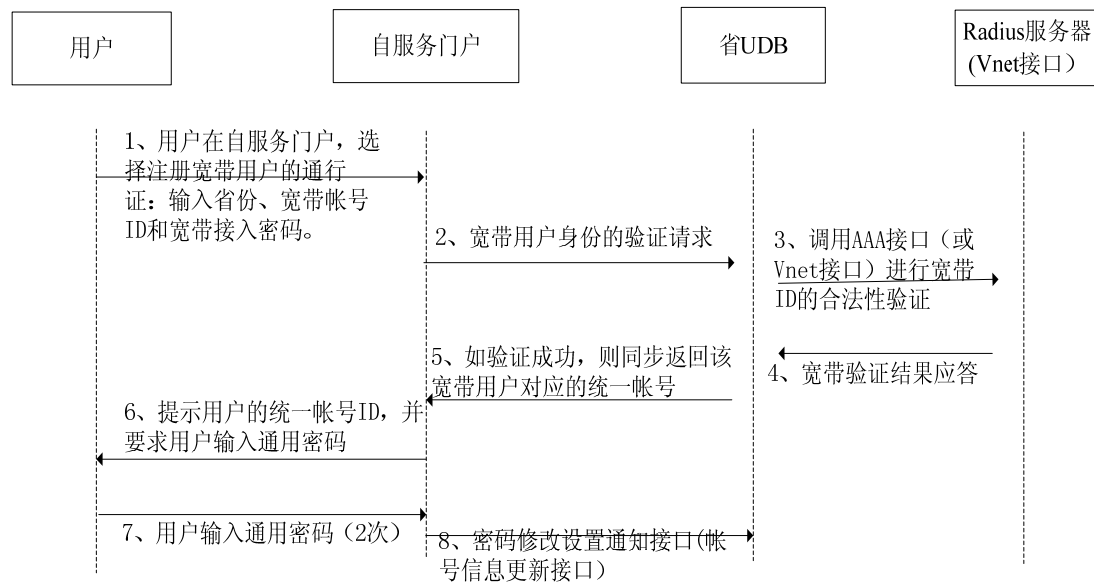
- 1) 用户登录自服务门户成功后，选择对已注册的某省内应用系统的密码进行设置：如设置私有密码、修改私有密码、启用通用密码等操作。
- 2) 用户自服务门户向UDB发起密码更新的请求：设置密码策略，和输入新原密码进行修改；对设置密码策略，及修改业务密码。调用用户帐号信息更新接口。
- 3) UDB执行应用系统的密码策略更新，或保存业务/私有密码；
- 4) UDB将密码策略设置结果返回给用户自服务门户；
- 5) 自服务界面反馈用户，用户密码策略设置成功与否。

### 11.2.5 传统宽带用户注册

针对中国电信，采用非手机、非固话（含 PHS）号码的宽带接入用户，自服务门户提供统一帐号（通行证）的用户自主注册功能。重点是为用户提供激活帐号（需验证身份合法性）、输入通用密码、反馈用户帐号等界面。

**触发条件：**用户通过自服务门户进行别名设置或修改操作。

**交互流程：**



#### 流程描述：

- 1) 用户登录自服务门户，选择进行宽带用户的统一帐号（通行证）注册，并输入省份、宽带帐号、接入密码进行身份验证。如果是全国平台，还需要输入用户的归属省别。
- 2) 用户自服务门户向归属省UDB发起宽带用户的身份验证请求；
- 3) 归属省UDB通过与省内互联星空的宽带帐号认证接口，或省内Radius服务器的宽带帐号查询接口，进行身份请求验证。（UDB调用的查询接口，参考“中国电信互联技术规范—流程与接口分册v3.1，宽带帐号认证接口”，或省内Radius的查询接口规范；具体见13.2节。）
- 4) Radius服务器将宽带用户身份的合法性验证结果返回UDB；
- 5) UDB向自服务门户反馈验证结果，如果验证成功，同步返回该宽带用户所对应的统一帐号ID；
- 6) 自服务门户向用户提示：您申请的统一帐号（通行证）号码为XXXXXX，并要求用户输入该统一帐号对应的通用密码；
- 7) 用户该提示要求输入密码（2次）；
- 8) 自服务门户向归属省UDB进行密码设置的更新通知；UDB记录该用户通用密码，并且将该用户的统一帐号状态从“未激活”变成“激活”。

## 11.3 接口内容

UDB 与自服务门户之间的接口,包括用户登录自服务门户登录的认证请求、用户帐号信息查询、用户帐号信息更新(包括别名、通用密码、密码策略等),参考第 6 章的 Web Service 公共接口部分。其他消息接口如下:

### 11.3.1 宽带帐号的验证请求

(1) 接口信息:

接口名称	BandWidthAccountAuthen
接口描述	宽带用户在自服务门户进行通行证注册,并输入其宽带接入帐号及接入密码,请 UDB 进行身份合法性验证。
请求消息名	BandWidthAccountAuthenRequest
应答消息名	BandWidthAccountAuthenResponse

(2) 参数说明

1) 请求参数

BandWidthAccountAuthenRequest 包含如下信息:

参数名称	数据类型	长度(字节)	出现频次	说明
SrcSsDeviceNo	String	16	1	发送端应用系统设备标识: 自服务门户发起请求
ProvinceNo	String	2	0-1	归属省
BandWidthAccount	String	40	1	用户的宽带帐号 ID
PasswordValue	String	20	1	宽带接入密码传送值
IPAddress	String	15	0-1	用户当前的 IP 地址

2) 响应消息

BandWidthAccountAuthenRequest 包含如下信息:

参数名称	数据类型	长度(字节)	出现频次	说明
ResultCode	Integer	2	1	结果码 0: 验证成功 1: 验证失败
BandWidthAccount	String	40	1	用户宽带帐号 ID

UserID	String	40	0-1	用户统一帐号
Description	String	128	0-1	对查询结果的详细描述信息



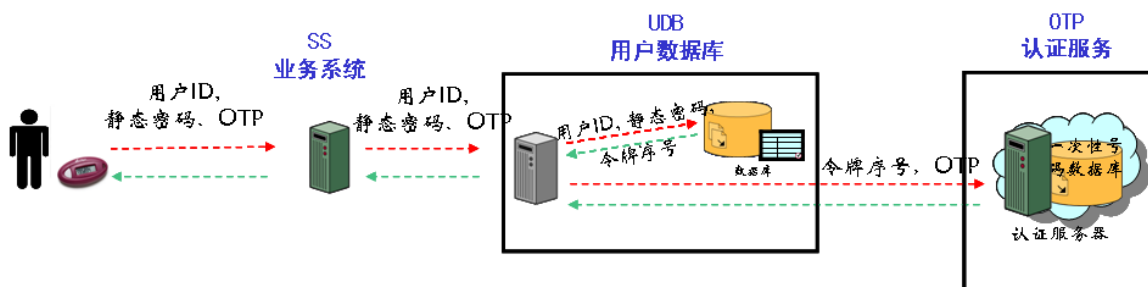
## 12 OTP 认证服务接口

一次性密码 OTP（One Time Password）又称动态密码，主要是为了解决一般身份认证“用户名+口令（或帐号+密码）”单因子方式容易遭到强力攻击破解的情况，有效保障网上银行、电子政务、第三方支付等应用系统的交易和会话安全性。

OTP 认证服务，可基于全国 UDB 平台对接进行全国集中部署，或基于各省 UDB 平台对接进行省分公司独立部署，提供本地化强身份认证服务。

### 12.1 接口概述

一次性密码利用密码产生器（OTP 令牌）产生一次性密码，一般可分为计次使用以及计时使用两种。OTP 的典型使用网络架构示意图如下：用户登录应用系统而判断用户 ID 为非本地帐号时，应用系统转发用户信息“统一帐号+通用密码+OTP”给 UDB 网元设备进行认证，其中“统一帐号+通用密码”由 UDB 的本身数据库进行匹配认证，而对 OTP 则可通过自建 OTP 认证引擎或第三方专用认证服务提供商的网络进行验证。

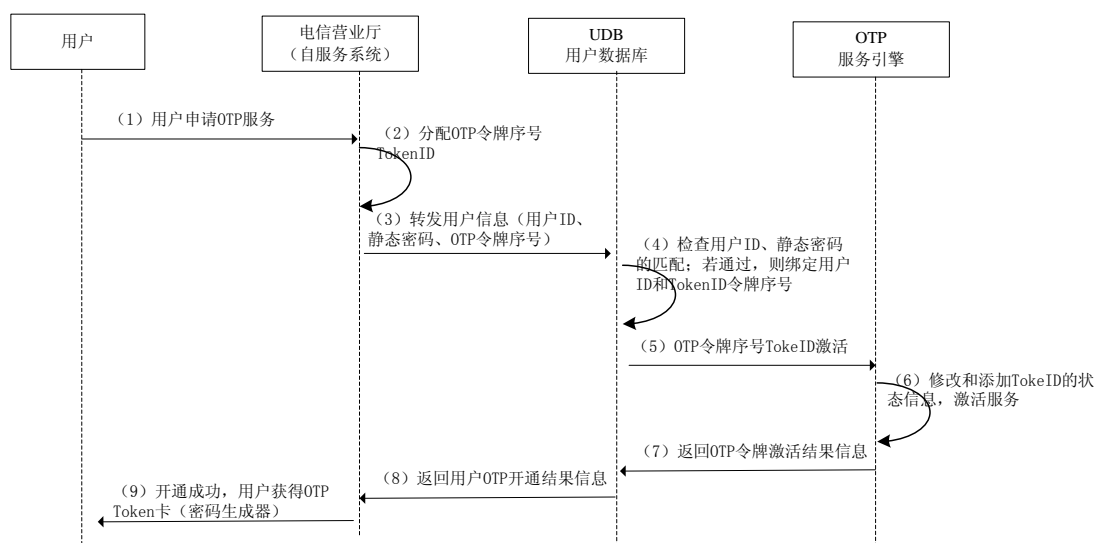


UDB 和 OTP 认证服务器交互基于 Web Service，采用 SOAP 协议，核心是实现 OTP 密码的认证查询功能，以及 OTP 令牌 TokenID 的激活和取消。

### 12.2 接口流程

#### 12.2.1 OTP 令牌激活流程

**触发条件：**用户通过电信营业厅，或自服务门户渠道进行 OTP 服务申请。

**交互流程：**

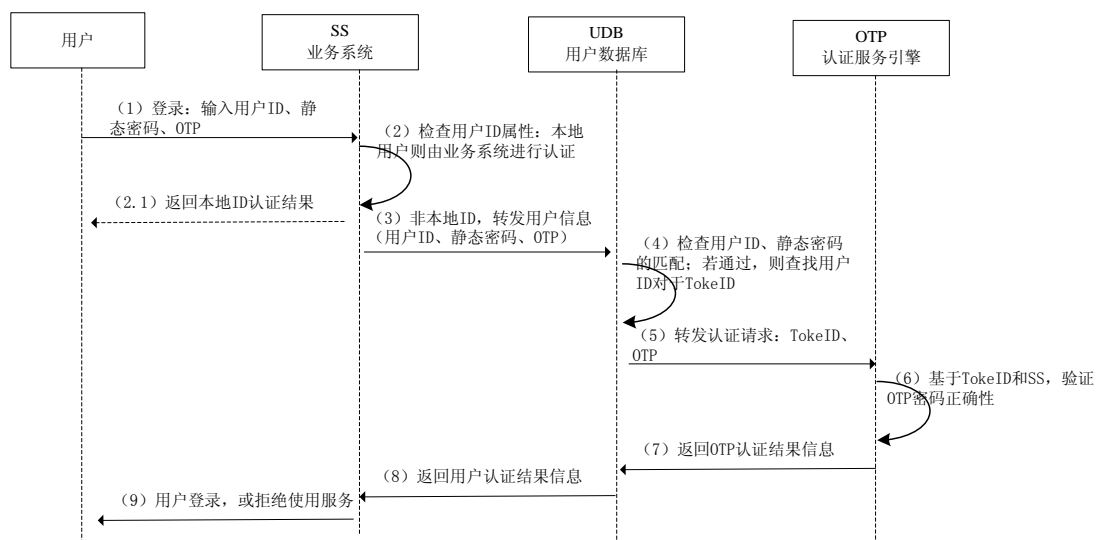
图中各步骤说明如下：

- 1) 用户在电信营业厅（或自服务系统）申请 UDB 帐户的 OTP 服务功能
- 2) 电信营业厅预先分配一个 OTP TokenID
- 3) 电信营业厅通过 UDB 管理系统服务功能，在 OTP 开通界面输入用户信息和令牌序号
- 4) UDB 检验用户基本信息，并修改数据库，建立 UDB 帐号与 OTP 令牌序号的映射关联
- 5) UDB 平台向 OTP 服务引擎，发送 TokenID 的激活请求
- 6) OTP 服务引擎基于 OTP TokenID，激活服务并保存状况
- 7) OTP 服务引擎将 TokenID 的激活结果信息返回给 UDB
- 8) UDB 平台将用户 OTP 开通结果返回给电信营业厅（或自服务界面）
- 9) 如一切正常开通，则电信营业厅为用户分发一个 OTP 令牌卡（密码生成器）

### 12.2.2 OTP认证请求流程

**触发条件：**用户在应用系统登录界面，输入 OTP 密码进行登录认证。

**交互流程：**OTP 认证查询的典型应用范例流程：



图中各步骤说明如下:

- 1) 用户在应用系统登录界面输入统一帐号, 通用密码和一个 OTP 值 (从 OTP 令牌上获得数值)
- 2) 应用系统应用程序判断用户帐号的属性, 如属本地帐号则自行认证
- 3) 如用户帐号属 UDB 统一帐号, 则 SS 将用户信息转发给 UDB 进行认证 (统一帐号, 通用密码, OTP)
- 4) UDB 服务器在用户目录 (数据库) 中定位统一帐号并对通用密码比对; 如果 UserID 和通用密码匹配, 查找得到用户关联的令牌序号 TokenID
- 5) UDB 将 TokenID, OTP 转发给 OTP 认证服务引擎
- 6) OTP 认证服务引擎基于令牌的 SS 和当前计数 count 计算期望的 OTP 值, 并与收到 OTP 进行比较, 验证是否一致
- 7) OTP 服务引擎将 TokenID 的认证结果返回给 UDB
- 8) UDB 服务器将用户的认证结果返回给应用系统应用程序
- 9) 应用系统应用程序根据认证结果, 允许用户登录/继续操作 (认证通过), 或拒绝用户使用该项服务 (认证不通过)

## 12.3 接口内容

### 12.3.1 OTP令牌激活/取消

接口概述: UDB 平台请求 OTP 认证引擎激活/取消 OTP 令牌

应答方: OTP 认证引擎

请求方：UDB 平台

接口类型：Web Services/SOAP

接口方法：OTPTokenEnable

名称	中文注释	数据类型	长度	可空否	说明
请求（request）					
TokenID	令牌序号	整数	10	不能	TokenID和UDB帐户是绑定对应关系
Enable/Disable	激活/取消	整数	1	不能	0（激活请求）， 1（取消请求）
Summary	备注	字符串	可变	可以	
应答（response）					
Result	结果	整数	2	不能	0（激活成功），1（激活失败），2（取消成功），3（取消失败），9（其他错误）
Err_msg	结果信息	字符串	可变	可以	其他错误的具体原因描述

### 12.3.2 OTP认证请求接口

接口概述：UDB 平台请求 OTP 认证引擎进行 TokenID 认证服务

应答方：OTP 认证引擎

请求方：UDB 平台

接口类型：Web Services/SOAP

接口方法：OTPAuthentica

名称	中文注释	数据类型	长度	可空否	说明
请求（request）					
TokenID	令牌序号	整数	10	不能	TokenID和UDB帐户是绑定对应关系
OTP	一次性密码	字符串	可变	不能	
Summary	备注	字符串	可变	可以	
应答（response）					
Result	结果	整数	2	不能	0（认证成功），1（密码错误），2（无此帐号），9（其他错误）
Err_msg	结果信息	字符串	可变	可以	认证失败的具体原因描述

## 13 其他接口类型

本章重点描述 UDB 与周边系统对接时，需要调用其他系统的接口情况。

本规范定义的接口，各周边系统可根据实际需要采用，或在此基础上双方协商而定，以保证双方可正常对接。

### 13.1 短信网关接口

全国或省 UDB，可通过 ISAG/短信网关向用户直接发送手机短信动态密码、统一帐号密码更新、统一帐号停用等短信通知。

UDB 短信接口支持中国电信短信网关协议规范，如《中国电信股份有限公司企业标准 SMGP 协议 V3.0.0》或《中国电信股份有限公司企业标准 SMGP 协议 V3.0.3》，以及中国电信 ISAG 短信协议接口。

### 13.2 互联星空的宽带认证接口

省 UDB 通过与本省互联星空或省内 Radius（AAA）系统，对省内的宽带帐号进行查询和验证服务。具体接口，参考“中国电信互联星空技术规范一流程与接口分册 v3.1，宽带帐号认证接口”，或省内 Radius 的开放接口规范。

以下为省互联星空的宽带帐号认证接口，UDB 可进行调用：如互联星空技术规范升级，请以最新版本为准。

#### （1）接口信息：

接口名称	AccountAuthenAAA
接口描述	提供方：省互联星空，或宽带接入Radius服务器 使用方：省UDB 宽带用户归属省UDB会调用省内互联星空或省内Radius服务器的宽带帐号验证接口，来查询该宽带用户帐号的合法性。
请求消息名	AccountAuthenAAARequest
应答消息名	AccountAuthenAAAResponse

#### （2）参数说明

##### 1) 请求参数

AccountAuthenAARequest 包含如下信息:

参数名称	数据类型	长度(字节)	出现频次	说明
ProvinceNo	String	2	1	用户归属省的省别简写
AccountType	String	2	1	帐号类型: 02: 宽带帐号
BandWidthAccount	String	57	1	用户的宽带帐号 ID
PasswordValue	String	20	1	宽带接入密码传送值
IPAddress	String	15	1	用户当前的 IP 地址
TimeStamp	String	19	1	时间戳, 从 1970 年 1 月 1 日 0 时开始的毫秒数,时区为东八区

2) 响应消息

AccountAuthenAAResponse 包含如下信息:

参数名称	数据类型	长度(字节)	出现频次	说明
ProvinceNo	String	2	1	应答方的省别简写
PUserID	String	11	0-1	用户唯一标识 当 ResultCode=2 时可为空
BandWidthAccount	String	57	1	用户的宽带帐号 ID
ResultCode	Integer	4	1	结果码 0: 用户认证通过 (宽带认证通过, 且互联星空用户已注册) 2: 宽带认证通过, 但该宽带帐号未注册互联星空用户 其他: 失败
ErrorDescription	String	256	0-1	对错误/异常的详细描述信息
UserProfile	String	3000	0-1	UserProfile, 用户的授权信息 当 ResultCode=2 时可为空
TimeStamp	String	19	1	时间戳, 从 1970 年 1 月 1 日 0 时开始的毫秒数,时区为东八区

### 13.3 UAM 的客户信息查询接口

UDB 接收 UAM 的重定向单点登录请求后, 获得了 UAMTicket 参数。UDB 根据 UAMTicket 参数内容再调用 UAM 客户身份信息查询接口, 获取具体的客

户身份信息。接口名称：<http://xxx/SSOFromUAM?UATicket=请求参数>

### 1) 接口消息

接口名称	客户身份信息查询接口
接口描述	UDB 调用 UAM 提供的接口，告知 UDB 当前访问的客户身份信息，以及客户要重定向的应用系统 URL
接口方式	Web Service
接口提供者	省 UAM
接口使用者	省 UDB

### 2) 参数说明

#### (1)、请求

元素名称	约束	类型	长度	描述	取值说明
UAMTicket	1	String	V64	客户身份索引	UAM 统一生成的随机唯一标识

#### (2)、应答

元素名称	约束	类型	长度	描述	取值说明
AccountType	1	String	F7	帐号类型	用户在 UAM 认证的帐号类型
AccountID	1	String	V30	帐号标识	用户在 UAM 认证的帐号标识
TrustedAccList	0-n	--	--	帐号列表	
ReturnURL	1	String	V512	应用系统重定向 URL	

其中，TrustedAccList 数组信息包括：

AccountNo	1-n	String	F3	帐号序号	对于客户下存在 n 个帐号的情况，标识当前帐号在帐号列表中的序号
AccountType	1-n	String	F7	帐号类型	
AccountID	1-n	String	V30	帐号标识	

UDB 和 UAM 之间通过内网调用“客户身份信息查询接口”，传递信息必须进行签名，签名具体要求如下：

- 签名：要求对完整协议包进行摘要。
- 签名加密算法：sha1-DSA，DSA 密钥位数 1024
- 证书保存格式：X.509

- 签名后以 16 进制方式（字符串为大写）保存

## 13.4 电信自营应用的 SSO 接口

满足从电信自营应用—电信自营应用、网厅—电信自营应用、第三方应用—电信自营应用的单点登录 SSO 需求，电信自营应用系统需提供专门 SSO 接口，仅供 UDB 直接调用。

（1）接口信息：

接口名称	应用系统的 SSO 接口
接口描述	提供给 UDB 的互信方的专用单点登录接口，无须二次认证用户便可直接使用目标应用
请求消息名	<u>http://XXX/SSOFromUDB</u>
应答消息名	无应答
接口协议	重定向
提供者	电信自营应用系统
主要使用者	UDB 系统

（2）参数说明：

1) 请求消息

http://XXX/SSOFromUDB? SSOFromUDBRequest = SSOFromUDBValue

http://XXX/为电信自营应用系统的 URL；

SSOFromUDBValue 为接口参数值，包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发起端的电信应用系统设备标识（UDB 设备标识）
UDBTicket	String	40	1	用户临时身份标识
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

SSOFromUDBValue 的生成算法如下：

Digest = Base64(Hash(SrcSsDeviceNo + UDBTicket + TimeStamp))

其中，Hash 算法采用 SHA-1。

SSOFromUDBValue = URLEncoding(SrcSsDeviceNo + "\$" +



**Base64(Encrypt(UDBTicket + “\$” + TimeStamp+ “\$”+ Digest)))**

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，SysKey 是 UDB 系统发给该应用系统的密钥。

电信自营应用系统在接收到重定向认证请求后，需要再做一次哈希转换：

**Digest ‘= Base64(Hash(SrcSsDeviceNo + UDBTicket + TimeStamp))**

将 Digest ‘与接收到 Digest 进行比较，若两者相同，则传送消息没有被篡改。

## 2) 应答消息

无应答。

## 13.5 第三方应用的 SSO 接口

中国电信与第三方 SP 应用系统，采用“单点登录互信合作”模式。对中国电信已完成认证的统一帐号用户访问其第三方应用时，则需通过 UDB 重定向到第三方应用系统（携带用户信息 PUserID 等），UDB 调用第三方 SP 应用系统提供的互信 SSO 接口。传递的信息必须进行签名已确保安全性。

### (1) 接口信息：

接口名称	第三方应用系统的 SSO 接口
接口描述	提供给 UDB 的互信方的专用单点登录接口，无须二次认证用户便可直接使用第三方目标应用
请求消息名	<u><a href="http://XXX/SSOFromUDB">http://XXX/SSOFromUDB</a></u>
应答消息名	无应答
接口协议	重定向
提供者	第三方应用系统
主要使用者	UDB 系统

### (2) 参数说明：

#### 1) 请求消息

<http://XXX/SSOFromUDB?SSOFromUDBRequest> = SSOFromUDBValue

<http://XXX/>为第三方应用系统的 URL；

SSOFromUDBValue 为接口参数值，包含如下信息：

参数名称	数据类型	长度（字节）	出现频次	说明
SrcSsDeviceNo	String	16	1	发起端的电信应用系统设备标识（UDB 设备标识）
PUserID	String	40	1	用户统一帐号
ThirdSsUserID	String	40	0-1	绑定的第三方应用系统的原用户帐号 ID 【该项只对第三方应用才有效】
TimeStamp	String	19	1	时间戳 yyyy-MM-dd HH:mm:ss，其中 HH 取值为 00-23,时区为东八区

SSOFromUDBValue 的生成算法如下：

$$\text{Digest} = \text{Base64}(\text{Hash}(\text{SrcSsDeviceNo} + \text{PUserID} + \text{ThirdSsUserID} + \text{TimeStamp}))$$

其中，Hash 算法采用 SHA-1。

$$\text{SSOFromUDBValue} = \text{URLEncoding}(\text{SrcSsDeviceNo} + \$ + \text{Base64}(\text{Encrypt}(\text{PUserID} + \$ + \text{ThirdSsUserID} + \$ + \text{TimeStamp} + \$ + \text{Digest})))$$

其中，加密算法 Encrypt 采用 3DES，Key=SysKey，SysKey 是 UDB 系统发给该应用系统的密钥。

第三方应用系统在接收到重定向认证请求后，需要再做一次哈希转换：

$$\text{Digest}' = \text{Base64}(\text{Hash}(\text{SrcSsDeviceNo} + \text{PUserID} + \text{ThirdSsUserID} + \text{TimeStamp}))$$

将 Digest' 与接收到 Digest 进行比较，若两者相同，则传送消息没有被篡改。

## 2) 应答消息

无应答。

## 14 UDB 数据编码规范

### 14.1 用户类型编号（UserIDType）

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。

### 14.2 用户状态编号（UserIDStatus）

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

### 14.3 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

### 14.4 用户唯一标识（PUserID）

PUserID 是用户全国唯一标识的序列号，主要是在为第三方 SP 服务时只根据该标识进行用户识别，而不必要将用户的真实帐号信息暴露给第三方。

PUserID 的编码格式如下： 省别码 + 序列号

其中，省别码（见 14.5）代表用户所属的省份，省份码为 2 位数字；序列

号是 9 位的数字序列，由省 UDB 随机生成或顺序生成，需要保证同一省份内所有用户的序列标识号码不同。

## 14.5 用户证件类型（CertificateType）

编码	描述
1	身份证
2	军人证
3	税务证
4	工商注册号
5	电信识别号
6	驾驶证
7	教师证
8	学生证
9	护照
10	社保卡
11	组织机构代码
12	客户卡
13	客户标识码
20	营业执照
22	记者证
23	企业代码证
24	暂住证
25	华侨证
26	其它
30	集团客户编码
31	省级客户编码
32	客户关联关系类型
33	本地客户编码
88	公章
99	其他

各省 CRM 记录的用户证件类型若与 UDB 设备规范的约定不尽相同，数据

同步时需要做中间转换表。

## 14.6 省别编号（ProvinceNo）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

## 14.7 地市编号（CityNo）及区号（AreaCode）

省份	省别码	地市码	区号	地址	省份	省别码	地市码	区号	地址
北京	01	010	010	北京	湖北	18	027	027	武汉
上海	02	021	021	上海		18	710	0710	襄樊
天津	03	022	022	天津		18	711	0711	鄂州
重庆	04	235	023	渝北局		18	712	0712	孝感
	04	236	023	璧山局		18	713	0713	黄冈
	04	237	023	江津局		18	714	0714	黄石
	04	238	023	合川局		18	715	0715	咸宁
	04	239	023	北碚局		18	716	0716	荆州
	04	240	023	巴南局		18	717	0717	宜昌
	04	241	023	永川局		18	718	0718	恩施
	04	242	023	万州局		18	719	0719	十堰
	04	243	023	开县局		18	720	0728	潜江
	04	244	023	涪陵局		18	721	0728	仙桃

	04	245	023	石柱局		18	722	0722	随州
	04	246	023	长寿局		18	723	0719	林区
	04	247	023	大足局		18	724	0724	荆门
	04	248	023	双桥局		18	728	0728	天门
	04	249	023	潼南局	湖南	19	730	0730	岳阳
	04	250	023	荣昌局		19	731	0731	长沙
	04	251	023	巫溪局		19	732	0731	湘潭
	04	252	023	忠县局		19	733	0731	株洲
	04	253	023	云阳局		19	734	0734	衡阳
	04	254	023	奉节局		19	735	0735	郴州
	04	255	023	城口局		19	736	0736	常德
	04	256	023	丰都局		19	737	0737	益阳
	04	257	023	南川局		19	738	0738	娄底
	04	258	023	酉阳局		19	739	0739	邵阳
	04	259	023	秀山局		19	743	0743	吉首
	04	260	023	彭水局		19	743	0743	自治州
	04	261	023	綦江局		19	744	0744	张家界
	04	262	023	万盛局		19	745	0745	怀化
	04	263	023	铜梁局		19	746	0746	永州
	04	264	023	梁平局	广东	20	020	020	广州
	04	265	023	武隆局		20	660	0660	汕尾
	04	266	023	垫江局		20	662	0662	阳江
	04	267	023	黔江局		20	663	0663	揭阳
	04	268	023	南坪局		20	668	0668	茂名
	04	269	023	上清寺局		20	750	0750	江门
	04	270	023	观音桥局		20	751	0751	韶关
	04	271	023	沙坪坝局		20	752	0752	惠州
	04	272	023	杨家坪局		20	753	0753	梅州
	04	273	023	数据局		20	754	0754	汕头
	04	274	023	北部新区局		20	755	0755	深圳
	04	275	023	巫山局		20	756	0756	珠海
河北	05	310	0310	邯郸		20	757	0757	佛山
	05	311	0311	石家庄		20	758	0758	肇庆
	05	312	0312	保定		20	759	0759	湛江
	05	313	0313	张家口		20	760	0760	中山
	05	314	0314	承德		20	762	0762	河源
	05	315	0315	唐山		20	763	0763	清远
	05	316	0316	廊坊		20	766	0766	云浮
	05	317	0317	沧州		20	768	0768	潮州
	05	318	0318	衡水		20	769	0769	东莞
	05	319	0319	邢台	广西	21	770	0770	防城港
	05	335	0335	秦皇岛		21	771	0771	崇左
山西	06	349	0349	朔州		21	771	0771	南宁
	06	350	0350	忻州		21	772	0772	来宾
	06	351	0351	太原		21	772	0772	柳州
	06	352	0352	大同		21	773	0773	桂林

	06	353	0353	阳泉		21	774	0774	贺州
	06	354	0354	晋中		21	774	0774	梧州
	06	355	0355	长治		21	775	0775	贵港
	06	356	0356	晋城		21	775	0775	玉林
	06	357	0357	临汾		21	776	0776	百色
	06	358	0358	吕梁		21	777	0777	钦州
	06	359	0359	运城		21	778	0778	河池
内蒙古	07	470	0470	呼伦贝尔	海南	21	779	0779	北海
	07	471	0471	呼和浩特		22	200	0898	海口
	07	472	0472	包头		22	212	0898	海口
	07	473	0473	乌海		22	213	0898	文昌
	07	474	0474	乌兰察布		22	214	0898	定安
	07	475	0475	通辽		22	215	0898	琼海
	07	476	0476	赤峰		22	216	0898	万宁
	07	477	0477	鄂尔多斯		22	217	0898	陵水
	07	478	0478	巴彦淖尔		22	218	0898	三亚
	07	479	0479	锡林郭勒		22	219	0898	澄迈
	07	482	0482	兴安盟		22	220	0898	屯昌
	07	483	0483	阿盟		22	221	0898	琼中
辽宁	08	024	024	沈阳		22	222	0898	五指山
	08	410	0410	铁岭		22	223	0898	保亭
	08	411	0411	大连		22	224	0898	临高
	08	412	0412	鞍山		22	225	0898	儋州
	08	413	0413	抚顺		22	226	0898	白沙
	08	414	0414	本溪		22	227	0898	昌江
	08	415	0415	丹东		22	228	0898	东方
	08	416	0416	锦州		22	229	0898	乐东
	08	417	0417	营口		22	230	0898	海口
	08	418	0418	阜新		22	231	0898	海口
	08	419	0419	辽阳		22	232	0898	海口
	08	421	0421	朝阳		22	233	0898	海口
	08	427	0427	盘锦		22	898	0898	海口
	08	429	0429	葫芦岛	四川	23	028	028	成都
吉林	09	431	0431	长春		23	812	0812	攀枝花
	09	432	0432	吉林		23	813	0813	自贡
	09	433	0433	延边		23	816	0816	绵阳
	09	434	0434	四平		23	817	0817	南充
	09	435	0435	通化		23	818	0818	达州
	09	436	0436	白城		23	825	0825	遂宁
	09	437	0437	辽源		23	826	0826	广安
	09	438	0438	松原		23	827	0827	巴中
	09	439	0439	白山		23	830	0830	泸州
黑龙江	10	451	0451	哈尔滨		23	831	0831	宜宾
	10	452	0452	齐齐哈尔		23	832	0832	内江
	10	453	0453	牡丹江		23	824	0832	资阳
	10	454	0454	佳木斯		23	833	0833	乐山
	10	455	0455	绥化		23	823	0833	眉山



	10	456	0456	黑河		23	834	0834	西昌
	10	457	0457	大兴安岭		23	835	0835	雅安
	10	458	0458	伊春		23	836	0836	甘孜
	10	459	0459	大庆		23	837	0837	阿坝
	10	464	0464	七台河		23	838	0838	德阳
	10	467	0467	鸡西		23	839	0839	广元
	10	468	0468	鹤岗		24	851	0851	贵阳
	10	469	0469	双鸭山		24	852	0852	遵义
江苏	11	25	025	南京	贵州	24	853	0853	安顺
	11	510	0510	无锡		24	854	0854	黔南
	11	511	0511	镇江		24	855	0855	黔东南
	11	512	0512	苏州		24	856	0856	铜仁
	11	513	0513	南通		24	857	0857	毕节
	11	514	0514	扬州		24	858	0858	六盘水
	11	515	0515	盐城		24	859	0859	黔西南
	11	516	0516	徐州	云南	25	691	0691	版纳
	11	517	0517	淮安		25	692	0692	德宏
	11	518	0518	连云港		25	870	0870	昭通
	11	519	0519	常州		25	871	0871	昆明
	11	523	0523	泰州		25	872	0872	大理
	11	527	0527	宿迁		25	873	0873	红河
浙江	12	570	0570	衢州		25	874	0874	曲靖
	12	571	0571	杭州		25	875	0875	保山
	12	572	0572	湖州		25	876	0876	文山
	12	573	0573	嘉兴		25	877	0877	玉溪
	12	574	0574	宁波		25	878	0878	楚雄
	12	575	0575	绍兴		25	879	0879	普洱
	12	576	0576	台州		25	883	0883	临沧
	12	577	0577	温州		25	886	0886	怒江
	12	578	0578	丽水		25	887	0887	迪庆
	12	579	0579	金华		25	888	0888	丽江
	12	580	0580	舟山	西藏	26	891	0891	拉萨
	13	550	0550	滁州		26	892	0892	日喀则
	13	551	0551	合肥		26	893	0893	山南
	13	552	0552	蚌埠		26	894	0894	林芝
	13	553	0553	芜湖		26	895	0895	昌都
	13	554	0554	淮南		26	896	0896	那曲
	13	555	0555	马鞍山		26	897	0897	阿里
	13	556	0556	安庆	陕西	27	291	029	西安
	13	557	0557	宿州		27	292	029	咸阳
	13	560	0558	亳州		27	293	029	杨凌
	13	558	0558	阜阳		27	911	0911	延安
	13	559	0559	黄山		27	912	0912	榆林
	13	561	0561	淮北		27	913	0913	渭南
	13	562	0562	铜陵		27	914	0914	商洛
	13	563	0563	宣城		27	915	0915	安康

	13	564	0564	六安		27	916	0916	汉中
	13	565	0565	巢湖		27	917	0917	宝鸡
	13	566	0566	池州		27	919	0919	铜川
福建	14	591	0591	福州	甘肃	28	930	0930	临夏
	14	592	0592	厦门		28	931	0931	兰州
	14	593	0593	宁德		28	932	0932	定西
	14	594	0594	莆田		28	933	0933	平凉
	14	595	0595	泉州		28	934	0934	庆阳
	14	596	0596	漳州		28	945	0935	金昌
	14	597	0597	龙岩		28	935	0935	武威
	14	598	0598	三明		28	936	0936	张掖
	14	599	0599	南平		28	947	0937	嘉峪关
江西	15	701	0701	鹰潭	青海	28	937	0937	酒泉
	15	790	0790	新余		28	938	0938	天水
	15	791	0791	南昌		28	939	0939	陇南
	15	792	0792	九江		28	941	0941	甘南
	15	793	0793	上饶		28	943	0943	白银
	15	794	0794	抚州		29	970	0970	海北
	15	795	0795	宜春		29	971	0971	西宁
	15	796	0796	吉安		29	972	0972	海东
	15	797	0797	赣州		29	973	0973	黄南
	15	798	0798	景德镇		29	974	0974	海南
山东	15	799	0799	萍乡		29	975	0975	果洛
	16	530	0530	菏泽	宁夏	29	976	0976	玉树
	16	531	0531	济南		29	977	0977	海西
	16	532	0532	青岛		29	979	0979	格尔木
	16	533	0533	淄博		30	951	0951	银川
	16	534	0534	德州		30	952	0952	石嘴山
	16	535	0535	烟台		30	953	0953	吴忠
	16	536	0536	潍坊		30	954	0954	固原
	16	537	0537	济宁		30	955	0955	中卫
	16	538	0538	泰安	新疆	31	901	0901	塔城
	16	539	0539	临沂		31	902	0902	哈密
	16	543	0543	滨州		31	903	0903	和田
	16	546	0546	东营		31	906	0906	阿勒泰
	16	631	0631	威海		31	908	0908	克州
	16	632	0632	枣庄		31	909	0909	博乐
	16	633	0633	日照		31	990	0990	克拉玛依
	16	634	0634	莱芜		31	991	0991	乌鲁木齐
	16	635	0635	聊城		31	992	0992	奎屯
河南	17	370	0370	商丘		31	993	0993	石河子
	17	371	0371	郑州		31	994	0994	昌吉
	17	372	0372	安阳		31	995	0995	吐鲁番
	17	373	0373	新乡		31	996	0996	巴州
	17	374	0374	许昌		31	997	0997	阿克苏

17	375	0375	平顶山		31	998	0998	喀什
17	376	0376	信阳		31	999	0999	伊犁
17	377	0377	南阳					
17	378	0378	开封					
17	379	0379	洛阳					
17	391	0391	焦作					
17	392	0392	鹤壁					
17	393	0393	濮阳					
17	394	0394	周口					
17	395	0395	漯河					
17	396	0396	驻马店					
17	398	0398	三门峡					

## 14.8 应用系统类型编号（SsType）

编号规则如下：

N1 N2 N3 N4

电信内部编号如下：

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	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
.....		5004-5099
	第三方应用	6000-6099

## 14.9 应用系统设备标识(DeviceNo)

应用系统设备标识编码规则：

**【省份 2 位 + SP 编号 8 位 + 应用系统类型 4 位 + 设备号 2 位】：**

省份标识：参见 13.3 省别编号

应用系统类型编号：参见 13.5 系统类型编号

设备编号：顺序编号，从 01 开始，用于识别多台同类设备

SP 编号：

1) 对于中国电信互联星空、ISMP 等管理的 CP/SP 编号，与互联星空、ISMP 管理平台的 CP/SP 编码格式保持一致；若编码字节有差异，则前面自动填零（如某个 SP 为 12345，则 UDB 记录为 00012345）

2) 对电信内部系统，取值为 8 个零（八个零代表电信内部平台）

## 14.10 业务套餐类型编号（SerSetType）

待定。

## 14.11 用户身份索引（UDBTicket）

由 UDB 生成的一串随机数，与 UDB 的统一帐号对应。

UDB 维护 UDBTicket 状态，一旦 Ticket 被应用系统查询过则由 UDB 进行销毁；或在一定时间内（如 2 秒）未被查询也自动失效。

## 14.12 接口返回码（ResultCode）

在 Web Services 和 ISAP 协议中除标准短信密码获取请求的返回码(为兼容集团现有短信业务开通系统定义的接口协议)之外的其他接口返回码 ResultCode 的统一定义：

编码	描述
0	<b>成功：</b> 认证通过、更新成功、绑定成功、查询成功等
1	帐号不存在/错误
2	帐号非法/暂停服务
3	帐号类型非法
4	
5	时间错误
6-9	保留
10	认证密码错误
11	短信密码错误
12	OTP 密码错误
13	扩展密码错误
14	加密方式错误（加密算法超过规定范围）
15	密码策略错误（密码策略超过约定范围）
16-19	保留
20	发端应用系统类型非法
21	发端应用系统设备 ID 非法
22	目标应用系统类型非法
23	目标应用系统设备 ID 非法
24	需要认证的应用系统类型非法
25	需要认证的应用系统设备 ID 非法
26	需要查询的应用系统类型非法
27	需要查询的应用系统设备 ID 非法
28	需要更新（密码设置、注册及上线状态）的系统类型非法

29	需要更新（密码设置、注册及上线状态）的系统设备 ID 非法
30	需要绑定的应用系统类型非法
31	需要绑定更新的应用系统设备 ID 非法
32-39	保留
40	缺少发端应用系统设备鉴权
41	发端应用系统设备鉴权未通过
42-49	保留
50	信息错误
51	
52-59	保留
60	查询错误
61-69	保留
70	激活错误
71-99	保留
100	重复的连接请求
101	没有连接
102-998	保留
999	其他错误
其他	保留

# 15 附录

## 15.1 统一认证 Web 页面参考

### 15.1.1 重定向登录



## 15.1.2 自服务界面



## 15.1.3 设置用户别名





## 15.1.4 修改密码界面



## 15.2 Web Services 接口概述文件

### 15.2.1 UDB公共接口（UDBCommon.wsdl）

### 15.2.2 UDB与CRM接口（CRMInterface.wsdl）

### 15.2.3 UDB与应用系统接口（SSInterface.wsdl）

### 15.2.4 UDB与ISMP接口（ISMPInterface.wsdl）

### 15.2.5 UDB与自服务接口（PortalInterface.wsdl）