中国电信用户数据库－功能与设备规范

V1.0

中国电信集团公司

2009 年 8 月

前　　言

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

本规范规定了用户数据库的功能要求、接口与协议要求、数据要求和性能要求等内容，以指导用户数据库的设备开发及网络部署。

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

目　　录

1 适用范围

本规范规定了中国电信用户数据库（UDB）的功能要求、接口与协议要求、数据要求和性能要求等内容。

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 系统设计与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 术语和缩略语

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

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。

4 UDB 在网络中的位置

中国电信认证服务体系主要有三个层面：应用层统一认证（UDB）、接入层统一认证（AAA）、IT 域统一认证（UAM）共同构成统一认证体系，如下图所示：

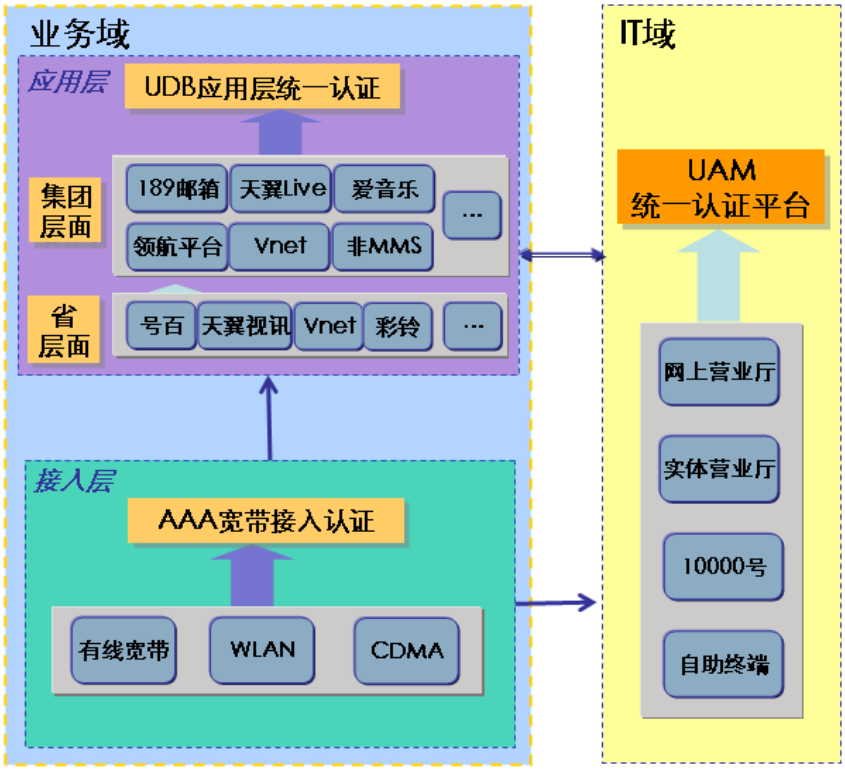

图 4-1 认证服务体系参考图

其中服务层面 IT 域统一认证（UAM）主要为 IT 域各渠道系统提供认证服务，包括网上营业厅、10000 号、自助终端、营业厅、WAP 营业厅、短信营业厅等。接入层 AAA 主要实现宽带接入认证、鉴权和计费。应用层 UDB 主要为各应用系统和互联网应用提供统一认证服务。

应用层用户数据库（UDB）定位为业务网络的统一用户数据库，通过公共接口与相关应用系统相连，为相关的业务提供集中认证服务，实现统一账户管理和统一账户服务。

UDB 应采用全国－－省两级应用系统认证体系，形成两级架构的应用层统

一帐号服务平台，提供统一的用户账号管理和统一的认证服务，实现一次登录、全网通行。如下图所示：

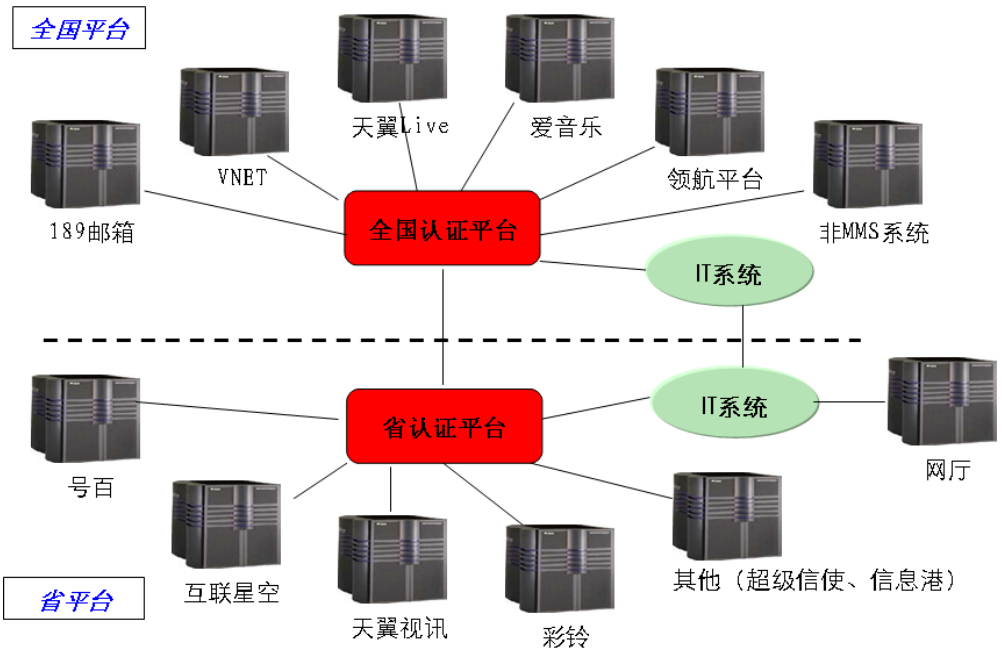

图 4-2 UDB 认证体系结构图

其中，全国认证平台（以下简称全国 UDB）可采用中国电信全国 Passport 平台，实现全国应用系统的统一认证服务，并承接全国漫游认证的转发服务。省级认证平台（以下简称省 UDB）可采用 UDB 系统，实现省应用系统及宽带接入系统的统一认证服务。两者互为补充，形成统一账号下的统一认证体系。

全国 UDB 和省 UDB 通过 CN2 网络进行承载，两点之间配置双链路备份机制。省 UDB 和周边系统可采用 CN2/DCN 或 Internet 不同承载网络进行互通。

5 系统架构

UDB 系统架构参考下图所示：

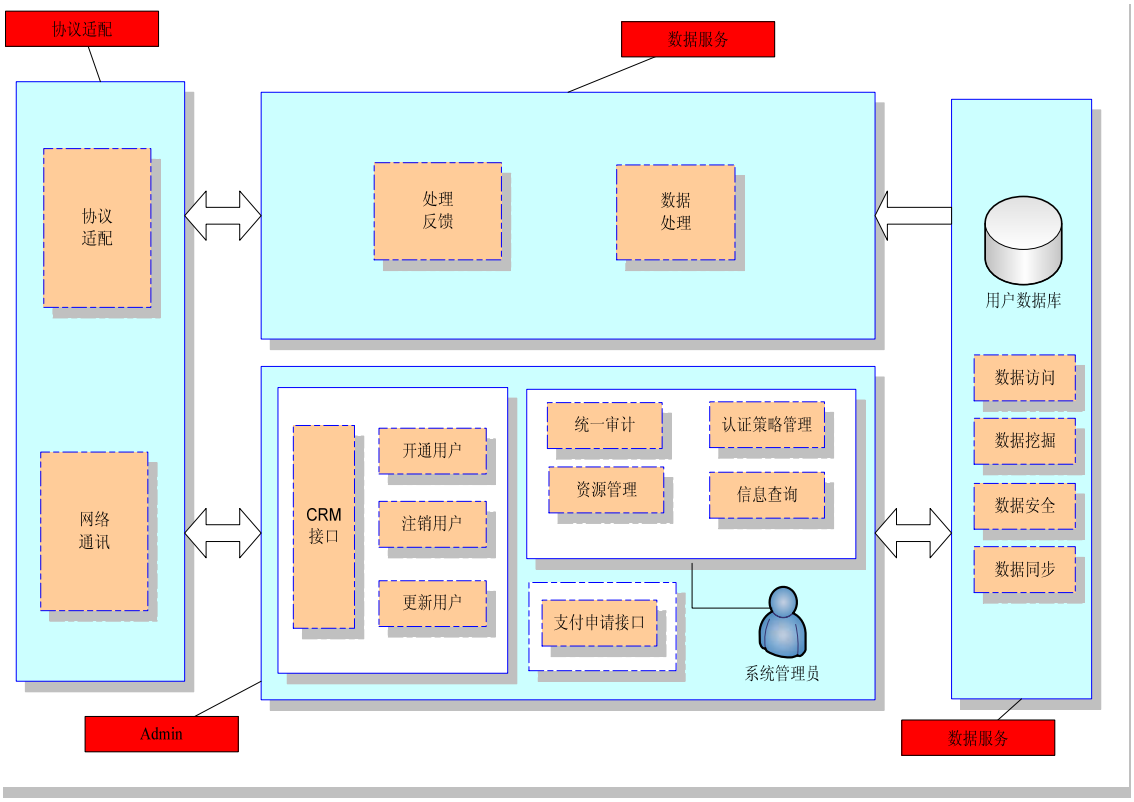

图 5-1 UDB 系统架构参考图

UDB 系统设计应遵循 SOA 的思想，即以功能相对独立的模块为服务，以服务可扩展为核心设计 UDB 的框架。

1) 采用代理服务（AgentService）模块来封装所有协议适配功能，并兼顾未来协议的扩展。
2) 采用认证服务（AuthServices）模块来封装各种具体服务，服务之间保持松耦合的原则，使未来扩展服务的影响最小化。
3) 采用账户管理（AcctManager）模块来封装账户变更绑定等服务，同时提供账户信息增加修改查询外部接口，供外部模块使用。
4) 可采用 LDAP 数据库做为信息存储的载体，用前置代理服务来分担协议适配和服务指派的任务，同时缓存参数配置数据，充分保证信息查询的速度。

近期 UDB 主要为了支撑中国电信“账号经营”的总体思路，通过统一帐号（如 189/133/153 手机号码或固定号码），将固定、宽带、移动等业务融合绑定，为各种应用提供统一账户和密码认证，用户可以方便的实现 189 邮箱、互联星空、天翼 Live、爱音乐、宽带接入、彩信等应用。

6 功能要求

6.1 账号数据存储与管理

UDB 应支持用户统一账号数据、密码、状态信息等用户信息的存储与管理。

UDB 存储的统一账号用户信息包括：

- 客户信息
- 用户付费类型
- 统一账号用户编号类型（UserIDType）
- 统一账号（UserID）
- 别名
- 用户唯一标识（PUserID）
- 通用密码
- 各个应用系统的类型编号（SsType）
- 各个应用系统的设备标识（DeviceNo）
- 统一账号对各应用系统的密码认证策略
- 统一账号对各个应用系统的业务密码
- 支付密码
- 短信动态密码
- 短信动态密码属性
- 各密码有效期
- 认证密码加密方式
- 共享密钥
- 统一账号的用户状态信息（UserIDStatus）
- 统一账号对各个业务的使用状态信息
- 统一账号的在线状态信息
- 统一账号对各个应用系统的业务在线状态信息
- 管理员设置的统一账号激活状态信息
- 管理员设置的统一账号对各个业务的服务状态信息

- 全国 UDB 活跃用户标记（仅对于省 UDB 有效）
- 下传省 UDB 设备标识列表（仅对于全国 UDB 有效）
- 统一账号绑定的宽带接入账号
- 单点登录 SSO 策略标记
- 接口返回码（ResultCode）等

具体要求为：

1）客户信息

主要为客户的姓名、性别、联系电话、证件类型、证件号等。

2）用户付费类型

用户付费类型主要有：后付费用户、预付费用户。

3）统一账号用户编号类型

统一账号用户编号类型主要有：个人账号、企业账号。其中个人账号主要有中国电信移动电话、固定电话及宽带接入账号等产品号码。

该信息应可扩展，初期用户编号类型默认为个人账号。

4）统一账号

统一账号应支持 1－40 位（数字或字母）不等长编号。

对于个人账号，账号命名规则为：

- 对于中国电信手机用户，帐号名为手机号码（189/133/153/…）。
- 对于中国电信固定电话用户，使用“区号+固话号码”作为帐号名。
- 对于中国电信的宽带用户：
    - 可使用其宽带绑定的固定电话号码作为帐号名，即“区号+固话号码”（含绑定的虚拟电话号码）。如该账号在 UDB 不存在，则直接作为统 UDB 的一账号；如该账号在 UDB 中已经存在，则将该宽带账号的全部信息数据保存在 UDB 已存在的统一账号绑定的宽带接入账号用户信息数据中。

- 对于没有绑定固定电话号码的宽带账号，使用“区号+0+7位数字”作为UDB的统一帐号。7位数字由UDB随机生成，该账号需用户通过UDB自服务界面激活后才能使用，其初始密码也由用户通过UDB自服务界面进行设置。在激活时，用户需在自服务界面输入宽带账号与密码，UDB向相应的Radius服务器进行宽带账号与密码的反查，验证通过后向用户提示“区号+0+7位数字”的统一帐号并激活。

UDB应能够根据帐号信息，判断账号的省份属性。

对于企业账号为企业用户在领航平台上注册的用户帐号，应从领航平台导入并生成用户信息数据。用户账号格式为：xxx@客户账号，xxx 由字母和数字组成，由企业管理员在领航平台上设置；客户帐号是在客户第一次在营业厅订购商航产品时由CRM系统分配，由字母和数字组成。如客户账号为abc时，企业管理员添加的用户账号为a@abc，该账号为该企业用户在UDB的统一账号。

UDB 应支持商航领航用户绑定手机、固话号码、邮箱账号等号码或账号作为领航平台登陆账号，绑定关系由领航平台设置实现并同步给UDB。

5）别名

由用户自行设置，一个统一账号只能对应一个别名。别名应为长度为5到15个符号，并以英文字母开头，中间可使用英文字母、数字、减号、下划线、小数点。别名使用的英文字母不区分大小写。

UDB应支持别名＋密码的认证方式。

用户通过UDB自服务门户设置别名，设置成功后，UDB需将该信息发送给各个应用系统。

为避免出现别名重复的现象，由全国UDB来维护所有的别名信息，并保证可基于别名进行全国漫游路由，如用户通过省UDB自服务门户设置别名，省UDB需同步给全国UDB，如该用户的“全国UDB活跃用

户标记”未标记，数据更新后省 UDB 将该标记置为标记状态。如用户通过全国 UDB 自服务门户设置别名，全国 UDB 需同步给相应的省 UDB。

6）用户唯一标识

用户唯一标识是用户全国唯一标识的序列号，主要用于第三方 SP 服务时只根据该标识进行用户识别，无需将用户的真实帐号信息暴露给第三方。

用户唯一标识为 11 位数字编号，包括 2 位省别码和 9 位数字序列。

用户唯一标识由省 UDB 维护，省 UDB 从 CRM 导入并生成用户信息数据时随机生成用户唯一标识，并同步给全国 UDB。

7）通用密码

通用密码是统一账号对应的静态密码，是用户登录各个应用系统的统一密码。一个统一账号只能设置一个通用密码。

通用密码应支持 6 位数字编号，并能够平滑升级支持 16 位。

通用密码可采用加密存储的方式（加密算法待定）。

初始通用密码可从 CRM 获得，后续通过 UDB 自服务门户实现通用密码的修改或重置，该信息需全国 UDB 与省 UDB 之间同步。

UDB 系统管理员应能够配置 UDB 系统的通用密码编码格式（采用 6 位数字的方式或 16 位字符的方式），省 UDB 通用密码格式变更后，需省 UDB 通过通用密码格式更新接口通知全国 UDB。

8）各个应用系统的类型编号

应用系统类型编号用于 UDB 识别请求认证的发送端应用系统类型，采用 4 位编码。

对于 IT 支撑系统包括 CRM、网厅、服务开通系统等，对于业务管理平台包括 ISMP、VNET 等，对于各应用系统包括 189 邮箱、互联星空、天翼 Live、爱音乐、领航平台、非 MMS 系统、彩铃门户、彩信门户、

超级信使等应用系统，此外还包括 UDB 自服务门户、ISAG、SMSC、SMS GW 等设备。具体参见接口与流程规范第 14 章。

该信息应可扩展。

9）各个应用系统的设备标识

应用系统设备标识用于 UDB 识别请求认证的发送端应用系统设备，具体参见接口与流程规范第 14 章。

该信息应可扩展。

10）统一账号对各应用系统的密码认证策略

统一账号对各应用系统的密码认证策略用于标识某应用系统是采用通用密码认证方式（含短信动态密码）还是采用业务密码认证方式。

如用户为某项应用系统设置了业务密码，则只能采用所设置的业务密码登录该应用系统，采用通用密码登录应返回失败。

对于某项采用业务密码认证方式的业务，用户可通过自服务界面将密码认证策略更换为通用密码认证方式，对于全国应用系统的密码认证策略更改（用户通过在省内的 UDB 自服务界面设置），需省 UDB 同步给全国 UDB。

该信息应可扩展。

初期全国 UDB 可暂不实现对各个全国应用系统的业务密码认证功能。

11）统一账号对各个应用系统的业务密码

业务密码是用户登录某个应用系统的专用（私有）密码，主要针对用户需要为某些应用系统设置区别于通用密码的单独密码场景。

业务密码在自服务界面上设置（对于全国应用系统的业务密码设置，初期可由自服务门户单点登录到全国应用系统的服务页面，由全国应用系统完成该系统业务密码的设置与保存）。业务密码格式由各个应用系统定义。

该信息需全国 UDB 通过账号信息更新接口同步给省 UDB（全国应用系

统设置业务密码），省 UDB 无需同步给全国 UDB（省内应用系统设置业务密码）。

业务密码可采用加密存储的方式（加密算法待定）。

12）支付密码

支付密码主要用于用户的网上付费等支付场景，及登录电子政务等高安全性要求的场景。

具体要求待定。

13）短信动态密码

短信动态密码为用户通过短信方式获取的动态密码，为一定时间期限内有效或一次性有效的统一账号通用密码。短信动态密码由 UDB 生成，其格式同通用密码。

用户可以通过 UDB 自服务界面或各个应用系统的门户或服务界面点击短信动态密码获取，并通过短信密码获取请求由 UDB 生成短信动态密码。

该信息需全国 UDB 同步给省 UDB（用户通过全国应用系统或全国 UDB 自服务界面获取短信动态密码），或省 UDB 同步给全国 UDB（用户通过省内应用系统或省 UDB 自服务界面获取短信动态密码）。

14）短信动态密码属性信息

短信动态密码属性主要有：有效期方式/一次性认证方式。

有效期方式为该短信动态密码在一定时间期限内有效，一次性认证方式为该短信动态密码 UDB 仅提供一次认证服务。

该信息需全国 UDB 同步给省 UDB（通过全国 UDB 设置），或省 UDB 同步给全国 UDB（通过省 UDB 设置）。

该信息应可扩展。

15）各密码有效期

即通用密码、各应用系统的业务密码、短信动态密码的有效期设置。

该信息需全国 UDB 同步给省 UDB（通过全国 UDB 设置），或省 UDB 同步给全国 UDB（通过省 UDB 设置）。

16）认证密码加密方式

即应用系统认证请求时发送过来的认证密码（包括通用密码、业务密码或短信动态密码）采用的加密算法，包括：MD5 加密、SHA 加密、不加密等。

该信息应可扩展。

17）共享密钥

如应用系统认证请求的通用密码采用 MD5 等加密算法，共享密钥应由 UDB 生成，并发送给相应的应用系统。

18）统一账号的用户状态信息

统一账号的用户状态信息即该账号用户状态，主要有：预先、正常、欠费单停、欠费双停、停机保号、其他停机、拆机和暂停服务等八种状态。

该信息由省 UDB 从 CRM 定期获取。

用户状态信息与认证结果需返回给请求认证的应用系统，由应用系统根据认证结果与用户状态判断是否对用户进行授权操作（允许、禁止、受限等处理）。

该信息需省 UDB 同步给全国 UDB。

该信息应可扩展。

19）统一账号对各个业务的使用状态信息

统一账号对各个业务的使用状态信息即用户对某个业务的状态信息，包括：业务开通、业务注销、业务暂停。

业务的使用状态信息由相应应用系统发送给 UDB，UDB 在认证时不判断该状态信息。

该信息需全国 UDB 同步给省 UDB（信息来源为全国应用系统），或省 UDB 同步给全国 UDB（信息来源为省应用系统）。

该信息应可扩展。

20）统一账号的在线状态信息

统一账号的在线状态信息主要有：在线/离线。

对于采用通用密码认证方式（包括短信动态密码）的应用系统，只要 1 个或多个在线状态信息为在线状态，则统一账号的在线状态信息应置为在线状态；当所有采用通用密码认证方式（包括短信动态密码）的应用系统，其在线状态信息均为离线状态，则统一账号的在线状态信息应置为离线状态。

对于采用业务密码认证策略的应用系统，其业务在线状态信息的改变不影响统一账号的在线状态信息。

该信息需全国 UDB 同步给省 UDB（用户登录全国应用系统），或省 UDB 同步给全国 UDB（用户登录省应用系统）。

21）统一账号对各个应用系统的在线状态信息

统一账号下各个应用系统的在线状态信息主要有：在线/离线。

用户通过统一账号登录或退出应用系统后，应用系统通过业务在线状态通知接口将在线或离线状态通知 UDB，UDB 根据业务在线状态通知更新相应应用系统的在线状态信息。

该信息全国 UDB 与省 UDB 之间不进行同步。

22）管理员设置的统一账号激活状态信息

即由 UDB 管理员对该账号设置是否提供认证服务的标识，主要有：激活/去激活。默认为激活。

该信息由 UDB 管理员进行设置，与 CRM 定义的用户状态无直接关系。如设置为去激活，则 UDB 停止对该账号的所有认证服务，并向请求认证的应用系统返回认证失败结果及原因值。

该信息需全国 UDB 同步给省 UDB（通过全国 UDB 设置），或省 UDB 同步给全国 UDB（通过省 UDB 设置）。

23）管理员设置的统一账号对各个业务的服务状态信息

即由 UDB 管理员对该账号下的各个业务设置是否提供认证服务的标识，主要有：暂停服务/提供服务。默认为提供服务。

该信息由 UDB 管理员进行设置，与 CRM 定义的用户状态无直接关系。

如某个业务设置为暂停服务，则 UDB 停止该账号对相应应用系统的认证服务，对该应用系统的认证请求返回认证失败结果及原因值。

该信息需全国 UDB 同步给省 UDB（通过全国 UDB 设置省内业务），或省 UDB 同步给全国 UDB（通过省 UDB 设置全国业务）。

24）全国 UDB 活跃用户标记

该标记仅对于省级 UDB 有效，主要有标记/未标记。默认为未标记。

如省 UDB 将该统一账号用户信息上传至全国 UDB 后，将该标记置为“标记”状态。全国 UDB 的用户数据只增不减。

25）下传省 UDB 设备标识列表

该参数仅对于全国 UDB 有效，主要保存全国 UDB 将该统一账号用户信息下传的省 UDB 设备标识。

该参数仅适用于企业用户账号的用户信息数据。

如全国 UDB 将该企业账号用户信息下传某省 UDB 后，将保存该省 UDB 的设备标识，如全国 UDB 中该企业账号的通用密码进行更新，则全国 UDB 向列表中的省 UDB 发起用户信息更新请求。

26）统一账号绑定的宽带接入账号用户信息数据

即用户统一账号所绑定的宽带接入账号的全部用户信息数据。当用户在 CRM 系统上开通了宽带业务后，向 UDB 发送的数据中如果绑定的电话号码为 UDB 已经存在的统一账号，UDB 应将该宽带账号的全部信息

数据保存在 UDB 已存在的统一账号绑定的宽带接入账号用户信息数据中。当用户通过统一账号认证之后，UDB 可以向应用系统返回绑定的宽带账号。

27）单点登录 SSO 策略标记

该标记为由 UDB 管理员对该账号设置是否提供单点登录（SSO）服务的标识，主要有：允许 SSO/禁止 SSO。默认为允许 SSO。

该信息由 UDB 管理员进行设置，如设置为禁止 SSO，则 UDB 不生成 Token，不支持用户单点登录到其他应用系统。

该信息需全国 UDB 同步给省 UDB（全国 UDB 设置），或省 UDB 同步给全国 UDB（省 UDB 设置）。

28）接口返回码

即 UDB 统一定义的 resultCode，具体参见接口与流程规范第 14 章。

该信息应可扩展。

UDB 应能够根据实际情况平滑扩展统一账号下的用户信息或某用户信息的参数与属性。

用户开户后，省 UDB 定期（可配置，默认 5 分钟）从 CRM 导入并生成用户信息数据，并默认开通统一账户对应的各应用系统使用权限。对于初始通用密码可采用 UIM 卡初始 6 位数字（新开 cdma 用户）、网厅服务密码（已有 cdma 用户）或通过电信营业厅/10000 人工服务设置（固定电话用户）。

用户登录全国应用系统并到全国 UDB 进行统一账号认证，如全国 UDB 没有该用户信息的统一账号数据，则通过与相应省 UDB 的账号查询接口，实时向省 UDB 发起请求，省 UDB 响应请求，将该统一账号用户信息上传全国 UDB，并将该用户的全国 UDB 活跃用户标记置为标记状态，全国 UDB 导入用户数据后，提供该统一账号的认证服务。

对于省 UDB 中全国 UDB 活跃用户标记为标记状态的统一账号，如该账号的用户状态、别名、通用密码、全国应用系统的业务密码、统一账号的登录状

态信息、统一账号的用户状态信息、各个业务的业务状态信息、各应用系统认证策略等数据变更，省 UDB 需实时向全国 UDB 发起账号数据更新。

如用户在全国应用系统设置了某全国应用系统的业务密码，全国应用系统需实时向全国 UDB 更新相应应用系统的业务密码和认证策略，全国 UDB 再实时向相应的省 UDB 发起账号数据更新。

如用户在全国 UDB 中设置的统一账号有效活动期内，没有登录全国应用系统的操作，则全国 UDB 应向相应的省 UDB 发送去除“全国 UDB 活跃用户标记”账号数据更新请求，省 UDB 响应请求并将该标记置为未标记状态，全国 UDB 收到响应后删除该统一账号的所有用户信息数据。（可选）

UDB 应支持对用户信息的增加、删除、修改和查询等功能。

如用户忘记通用密码，可以在自服务界面上通过手机短信获取随机验证码，实现通用密码重置；也可以通过 189 邮箱实现通用密码重置通用，或通过 10000 号客服申请密码重置。

对于一个用户具有两个或多个 cdma 号码或固话的情况，在 UDB 中等同于两个或多个用户。

6.2 认证服务

认证服务是 UDB 提供的主要服务内容，通过 UDB 提供的业务认证请求接口，在 UDB 系统已经注册的各应用系统，可以使用统一账号与密码到 UDB 进行认证。其中全国 UDB 负责全国应用系统（包括 189 邮箱、互联星空、天翼 Live 平台、全国爱音乐平台、领航平台和非 MMS 系统等）的统一认证服务，省 UDB 负责省内应用系统的统一认证服务。

UDB 认证服务的实现流程主要为：

1) 用户登录应用系统并输入账号与密码；
2) 应用系统判断输入账号是否为应用系统自有账号的认证；
   - 如果是自有帐号，应用系统将按照已有的认证模式进行认证，并返回认证结果；
   - 如果不是自有帐号，则应用系统通过业务认证请求接口到相

应的 UDB 进行认证；

3) UDB 判断账号是否存在；

- 如不存在：
  - ✓ 对于全国UDB，则通过与省UDB的账号信息查询接口，实时向账号归属的省 UDB 发起请求，省 UDB 响应请求，如省 UDB 存储有该账号的用户信息，通过账号信息更新接口将该统一账号的用户信息上传全国 UDB，并将“全国 UDB 活跃用户标记”置为“标记”状态，并转第 4 步；如省 UDB 无该账号的用户信息，则向全国 UDB 响应账号未开通，全国 UDB 向应用系统返回认证失败结果及原因值。
  - ✓ 对于省 UDB，则先判断该账号的账号用户编号类型，如为个人客户，则直接返回认证失败结果及原因值。如为企业客户，则通过与全国 UDB 的账号信息查询接口，实时向全国 UDB 发起请求，全国 UDB 响应请求，如全国 UDB 存储有该账号的用户信息，通过账号信息更新接口将该统一账号的下传到发起请求的省 UDB，并将该省 UDB 的设备标识保存在“下传省 UDB 设备标识列表”中，并转第 4 步；如全国 UDB 无该账号的用户信息，则向发起请求的省 UDB 响应账号未开通，省 UDB 向应用系统返回认证失败结果及原因值。
- 如果存在，则到第 4 步。

4) UDB 判断管理员设置的统一账号激活状态信息；

- 如统一账号激活状态为激活状态，则到第 5 步；
- 如统一账号激活状态为去激活状态，则 UDB 返回认证失败结果及原因值。

5) UDB 判断统一账号的用户状态信息；

- 如统一账号的用户状态为正常、欠费单停、欠费双停、停机保号或其他停机状态，则到第 6 步；

- 如统一账号的用户状态为预先、拆机或暂停服务状态，则UDB返回认证失败结果及原因值。

6) UDB 根据需要认证的应用系统设备标识，判断该应用系统的管理员设置的服务状态信息；

- 如该业务的服务状态为提供服务，则到第 7 步；
- 如该业务的服务状态为暂停服务，则 UDB 返回认证失败结果及原因值。

7) UDB 根据发送端业务认证请求的鉴权类型，判断是采用通用密码/业务密码认证方式或采用短信动态密码认证方式；

- 如为采用通用密码/业务密码认证方式，则到第 8 步；
- 如为采用短信动态密码认证方式，则选择短信动态密码为认证密码，并到第 9 步。

8) UDB 根据需要认证的应用系统设备标识，判断该应用系统的密码认证策略；

- 如为采用通用密码认证方式，则选择通用密码为认证密码，并到第 9 步；
- 如为采用业务密码认证方式，则选择相应的业务密码为认证密码，并到第 9 步。

9) UDB 判断认证密码的有效期是否超时；

- 如超过有效期，则返回认证失败结果及原因值，应用系统返回失败认证结果给用户，并提示用户更新密码；
- 如在有效期内，则到第 10 步。

如采用短信动态密码认证方式，且短信动态密码属性设置为一次性认证方式，则 UDB 需保存并判断该认证密码的认证次数；

- 如为首次认证，则到第 10 步；
- 如为二次认证，则返回认证失败结果及原因值，应用系统返回失败认证结果给用户，并提示用户短信动态密码实效。

10) UDB 根据发送端业务认证请求的加密算法，判断认证密码的加密方式，选择相应的加密算法（或不加密）；

11)UDB 进行认证服务，将认证结果及返回码通知给请求认证的应用系统；

12)应用系统返回认证结果给用户。

应用系统向 UDB 请求认证时，应能够标明是采用统一账号＋密码认证或是采用别名＋密码认证。UDB 根据认证请求消息中的认证用户账号格式，判断该认证请求是采用统一账号认证还是别名认证。

对于别名＋密码的认证方式，认证流程同统一账号＋密码的认证方式。对于全国应用系统到全国 UDB 的认证，如全国 UDB 判断别名不存在，则全国 UDB 向应用系统返回认证失败结果及原因值。对于省应用系统到省 UDB 的认证，如省 UDB 判断别名不存在，则通过与全国 UDB 的漫游认证转发接口，将该认证请求转发至全国 UDB，如全国 UDB 判断别名不存在，则全国 UDB 通过相应的省 UDB 向应用系统返回认证失败结果及原因值，如存在则按照流程提供认证服务，并通过相应的省 UDB 向应用系统返回认证结果。

UDB 应支持漫游认证转发功能，对于漫游的统一账户用户认证，漫游省 UDB 根据认证请求的账号信息，判断为漫游用户，并将认证请求通过漫游认证转发接口转发到全国 UDB，全国 UDB 根据账号信息再将认证请求转发到归属省 UDB，归属省 UDB 进行认证服务，并将认证结果返回到全国 UDB，全国 UDB 返回到漫游省 UDB，漫游省应用系统根据漫游省 UDB 返回的认证结果，返回给用户登录成功或失败界面。对于漫游的别名用户认证，漫游省 UDB 判断别名不存在，通过漫游认证转发接口转发到全国 UDB，由全国 UDB 进行认证服务，并返回漫游省 UDB。

各应用系统应配合 UDB 认证修改各自的登录认证流程，增加对统一账号用户的支持。

已有的应用系统可保留对自有账号的认证，无需到 UDB 进行认证。

对于统一账号的宽带接入认证，参见 6.8 节。

所有涉及外部 SP 业务的认证应重定向到 UDB 进行集中认证。

6.3 协议适配

UDB 应支持与相关系统的协议交互，提供针对各个具体应用的认证接口。认证完成后，通过相应协议接口返回认证结果。

UDB 应提供统一的业务认证请求接口，针对各应用系统存在的不同协议进行适配，UDB 接收消息后，统一转换成 UDB 可以识别的格式，认证服务完成后，将数据封装成特定的协议，返回给相应的应用系统。UDB 应支持通过增加相应的协议解析模块，支持新的协议扩展。

近期 UDB 主要提供以下三类接口：

- 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；
- 面向宽带接入认证服务器的 Radius 协议接口（仅对于省 UDB 有效）。

6.4 单点登录

单点登录功能主要实现网厅到应用系统的单点登录、应用系统到应用系统的单点登录以及宽带接入到应用系统的单点登录，即用户在成功登录中国电信的宽带接入、网厅或应用系统之后，再进入其他应用系统时，无须进行二次认证，即可进入服务界面。

1、网厅到应用系统的单点登录

对于网厅到应用系统的单点登录，即用户使用统一账号登录网厅后，通过点击网厅上应用系统链接访问该应用系统时，不再二次输入账号与密码，直接进入登录后服务界面。

功能实现要求如下：

1）用户通过统一账号成功登录网厅，并点击网上营业厅上的某个应用系统

链接，网厅将请求重定向到省 UAM，并携带目标应用系统的 URL。省 UAM 根据 UAM 的全局 Token，生成当前用户的身份信息及对应的用户身份索引（Ticket）。

2）省 UAM 携带 Ticket 及应用系统重定向 URL，通过 UDB 提供的单点登录重定向接口，重定向请求到省 UDB。

3）省 UDB 保存重定向请求中的 Ticket，并根据 Ticket 通过客户身份信息查询接口向省 UAM 查询用户身份信息，且根据 URL 判断是全国应用系统还是省级应用系统：

a) 如是全国应用系统，由省 UDB 负责重定向到全国 UDB，并携带保存的 UAM Ticket 及应用系统重定向 URL，全国 UDB 保存重定向请求中的 Ticket，并根据 Ticket 通过与省 UDB 的用户身份查询接口，向相应的省 UDB 查询用户身份信息。

b) 如是省级应用系统，则进行下一步。

4）省 UDB/全国 UDB 对用户身份信息中的账号列表进行查询和判断：

a) 账号列表如为空（即账号不存在）：

i. 则 UDB 将请求重定向到被链接的应用系统的登录认证界面。

ii. UDB 销毁保存的 UAM Ticket。

b) 账号列表存在多个账号：

i. UDB 重定向到应用系统 URL，并携带保存 UAM Ticket；

ii. 应用系统根据 Ticket 向 UDB 查询用户帐号信息，UDB 响应后销毁保存的 UAM Ticket；

iii. 应用系统根据账号列表中携带的多个账号，在登录认证界面上提示用户选择用于登录的账号（列表方式）；

iv. 用户选择登录账号后，应再输入登录密码，应用系统向 UDB 发起认证请求。具体认证要求同 6.2 节。

c) 账号列表为一个账号，省 UDB/全国 UDB 进一步判断是否为 UDB 中存储的统一账号：

i. 如非 UDB 统一账号：

- ✓ 对于全国 UDB，需通过与相应省 UDB 的账号信息查询接口，实时向账号归属的省 UDB 发起请求，省 UDB 响应请求，如省 UDB 存储有该账号的用户信息，通过账号信息更新接口将该统一账号的用户信息上传全国 UDB，并将“全国 UDB 活跃用户标记”置为“标记”状态，并进行下一步操作；如省 UDB 无该账号的用户信息，则向全国 UDB 响应账号未开通，或者全国 UDB 无法根据账号发起到省 UDB 的查询，则全国 UDB 重定向到应用系统 URL，并携带保存的 UAM Ticket；应用系统根据 Ticket 向全国 UDB 查询用户帐号信息，全国 UDB 响应后销毁保存的 UAM Ticket；应用系统根据账号列表中携带的账号，向用户返回登录成功的界面（该账号为应用系统自有账号）或登录认证界面（该账号非应用系统自有账号）；
- ✓ 对于省 UDB，则省 UDB 重定向到应用系统 URL，并携带保存的 UAM Ticket；应用系统根据 Ticket 向省 UDB 查询用户帐号信息，省 UDB 响应后销毁保存的 UAM Ticket；应用系统根据账号列表中携带的账号，向用户返回登录成功的界面（该账号为应用系统自有账号）或登录认证界面（该账号非应用系统自有账号）；

ii. 如为 UDB 统一账号，则进行下一步操作。

5）省 UDB/全国 UDB 判断用户账号的状态，如用户状态为预先、拆机或暂停服务，则将用户重定向到被链接业务的拒绝登录界面，并销毁 Ticket。如果用户状态为正常、欠费单停、欠费双停、停机保号或其他停机状态，则进行下一步处理；

6）省 UDB/全国 UDB 生成 UDB Ticket 及用户身份信息，并将用户重定向到应用系统 URL，并携带认证通过结果和生成的 UDB Ticket。

7）应用系统根据 UDB Ticket 通过用户身份信息查询接口向省 UDB/全国 UDB 查询用户帐号信息。

8）省 UDB/全国 UDB 判断该 UDB Ticket 信息是否有效：

a) 如 UDB Ticket 有效，省 UDB/全国 UDB 向应用系统返回用户帐号信息和用户状态信息等，同时 UDB 销毁该 UDB Ticket，应用系统向用户返回登录成功的界面。

b) 如无此 Ticket，省 UDB/全国 UDB 向应用系统返回失败结果，应用系统向用户返回登录认证界面。

对于网厅到应用系统的单点登录，UDB 不进行管理员设置的统一账号激活状态信息、应用系统的管理员设置的服务状态信息和密码认证策略等用户信息参数的判断。

网厅到 UDB 重定向传递的信息应封装成 XML 协议包，并采用数字签名＋对称算法加密的方式。

2、应用系统的单点登录

对于应用系统到应用系统的单点登录，即当用户用统一账号登录应用系统 A 之后，再进入应用系统 B 时无须二次认证。应用系统的单点登录包括省级应用平台到省级应用平台、全国应用平台到全国应用平台、以及省级应用平台与全国应用平台之间的单点登录。

功能实现要求如下：

1）用户访问应用系统 A，应用系统 A 通过重定向认证请求接口将认证请求重定向到 UDB。

2）UDB 检查是否存在用户的全局 Token。如没有全局 Token，则向用户提供登录认证界面；

3）用户输入统一账号和通用密码，并点击登录应用系统；

4）UDB 对用户进行认证，如果认证通过，则生成全局 Token，并向用户浏览器传递 Token（向浏览器写 Cookie），且 UDB 生成 UDB Ticket 及用户身份信息，进行下一步操作；如用户输入是统一账号＋业务密码或认证未通过，则不生成全局 Token，并向应用系统 A 返回认证结果；

5）UDB 将认证结果重定向返回应用系统 A。认证结果中包含：

a) 认证结果：成功、失败。在如下条件下返回认证失败：

1. 用户的统一账号不存在
2. 用户的密码不正确
3. 用户状态为预先、拆机或暂停状态

b) 返回方应用系统的设备标识

c) UDB Ticket

d) 时间戳等

6）应用系统 A 根据 Ticket，通过用户身份信息查询接口向 UDB 查询用户帐号信息。

7）UDB 判断该 UDB Ticket 信息是否有效：

a) 如 UDB Ticket 有效，UDB 向应用系统 A 返回用户帐号信息和用户状态信息等，同时 UDB 销毁该 UDB Ticket，应用系统 A 向用户返回登录成功的界面。

b) 如无此 Ticket，UDB 向应用系统 A 返回失败结果，应用系统 A 向用户返回登录认证界面。

8）用户成功登录应用系统 A 后，在应用系统 A 的服务界面上点击应用系统 B 的链接。

9）应用系统 B 将认证请求重定向到 UDB。

10）UDB 从用户浏览器得到全局 Token，并对 Token 进行验证：

a) 如 Token 认证通过，则 UDB 生成 UDB Ticket 及用户身份信息， UDB 通过重定向的方式向应用系统 B 返回认证结果及 Ticket，并进行下一步操作；

b) 如 Token 认证未通过，则 UDB 通过重定向的方式向应用系统 B 返回认证失败的结果，应用系统 B 向用户返回登录认证界面。

11）应用系统 B 根据 Ticket，通过用户身份信息查询接口向 UDB 查询用户帐号信息。

12）UDB 判断该 UDB Ticket 信息是否有效：

a) 如 UDB Ticket 有效，UDB 向应用系统 B 返回用户帐号信息和

用户状态信息等，同时 UDB 销毁该 UDB Ticket，应用系统 B 向用户返回登录成功的界面。

b) 如无此 Ticket，UDB 向应用系统 B 返回失败结果，应用系统 B 向用户返回登录认证界面。

3、宽带接入到应用系统的单点登录

对于宽带接入与应用系统之间的单点登录，指用户用统一账号进行宽带拨号成功后，再访问或同一窗口输入应用系统网址后，无须进行二次认证便可直接使用。

功能实现要求如下：

1）用户通过中国电信专用客户端软件（如天翼 Live PC 版）或 WLAN 的 portal，输入统一账号和通用密码，进行宽带拨号。

2）当宽带登录成功后，客户端调用 UDB 提供的客户端单点登录认证接口，或 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。

3）UDB 生成全局 Token，并向用户浏览器传递 Token（向用户浏览器或客户端内嵌浏览器写入 Cookie）。

4）用户发起应用系统的访问请求，其实现同应用系统单点登录的流程。

为实现应用系统的单点登录功能，UDB 应具备如下功能：

1）UDB 应能提供用户登录认证界面，并提示用户输入帐号类型、帐号标识、密码类型、密码、归属省等信息。UDB 登录认证界面应支持嵌入式登录页面。

2）UDB 应能为用户生成全局 Token（采用通用密码认证方式并验证成功后）。对于省内采用业务密码认证方式的应用系统，应不支持单点登录到其他应用系统，UDB 不生成 Token。如某统一账号的单点登录 SSO 策略标记设置为禁止 SSO，对该用户 UDB 不生成 Token，也不支持该用户单点登录到其他应用系统的操作。

- 全局 Token 中应包含：生成全局 Token 系统的设备 ID、用户所在的省、用户唯一标识(PUserID)、用户的统一账号(UserID)、用户别名(Alias)、Token 的过期时间、登录认证的类型等。具体参见接口与流程规范第 10.3 节。
- Token 中的各个属性之间用$进行连接，比如：

"ProvinceID="+value+"$"+"PUserID="+value+"$" +"PUserName="+value+"$"+"Alias="+value+"$"
+"ExpireTime="+value+"$"+"AuthType="+value

- UDB 应能支持扩展性：随着应用系统的发展，UDB 应能按照上述格式扩展新属性。属性的变化不应影响现有业务。
- UDB 应支持由 3DES 等加密算法对 Token 的所有属性进行加密。

3）UDB 应能向用户浏览器传递全局 Token，Token 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，该 cookie 必须设置属性 httponly。

4）UDB 应能接收客户端或 Portal 的 Token 请求，并返回全局 Token。

5）UDB 应能根据用户的全局 Token 得到用户的统一账号等数据。

6）UDB 应能生成 UDB Ticket 及用户身份信息，并能够把 Ticket 重定向到应用系统，应用系统通过该 Ticket 从 UDB 获取用户身份等信息，Ticket 为由 UDB 随机生成的唯一序列号。

7）UDB 应能接收应用系统的重定向认证请求，并能从重定向认证请求中得到发起端应用系统设备标识、UDB 返回结果时需要调用的 URL 和时间戳等信息。

8）UDB 应能根据认证结果向应用系统重定向返回认证结果。

9）为保证全国 UDB 和省 UDB 能得到唯一的全局 Token，省 UDB 和全国 UDB 应在同一个域内。

10）UDB 管理员应能够配置 Token、Ticket 有效期等参数。Token 默认有效期为 2 小时，有效期过后应失效，Ticket 默认有效期为 2 秒，有效期过后应销毁。

11）UDB 应能支持 Passport 系统现有的重定向机制。并能够扩展支持标准

的 SAML 机制。

6.5 用户状态变更

省 UDB 存储的统一账号用户状态主要来自于 CRM 系统，省 UDB 定义的用户状态主要有：

1) 预先
2) 正常
3) 欠费单停
4) 欠费双停
5) 停机保号
6) 其他停机
7) 拆机
8) 暂停服务

各省在 UDB 建设与实施中，需根据 CRM 定义的用户状态，确定与省 UDB 定义的用户状态的对应关系。

1） 预先：对于省 UDB，该状态为用户已申请账号，但 UDB 对该账号的用户信息数据的生成未完结（生成完结后，省 UDB 将用户状态更改为正常）；对于全国 UDB，该状态为已发起对该账号到相应省 UDB 的账号查询请求，但省 UDB 还未响应（省 UDB 将该账号的用户信息数据上传全国 UDB 后，且全国 UDB 生成完结后，全国 UDB 将用户状态更改为正常）。该状态下 UDB 应停止对该账号的认证服务，并向请求认证的应用系统返回认证失败结果及相应原因值。省 UDB 的预先状态可对应于 CRM 的预开户、预先等状态。

2） 正常：该状态下 UDB 应提供对该账号的认证服务，并返回认证成功结果及相应用户状态信息。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的正常状态可对应于 CRM 的开户、复机、取消停机保号、解挂、在用等状态。

3） 欠费单停：该状态下 UDB 应提供对该账号的认证服务，并返回认证成功结果及相应用户状态信息，请求认证的应用系统根据 UDB 返回的认证结果和用户状态信息判断是否为该账号提供服务。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的欠费单停状态可对应于 CRM 的欠费单停状态。

4） 欠费双停：该状态下 UDB 应提供对该账号的认证服务，并返回认证成功结果及相应用户状态信息，请求认证的应用系统根据 UDB 返回的认证结果和用户状态信息判断是否为该账号提供服务。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的欠费双停状态可对应于 CRM 的欠费双停状态。

5） 停机保号：该状态下 UDB 应提供对该账号的认证服务，并返回认证成功结果及相应用户状态信息，请求认证的应用系统根据 UDB 返回的认证结果和用户状态信息判断是否为该账号提供服务。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的停机保号状态可对应于 CRM 的用户报停状态。

6） 其他停机：该状态下 UDB 应提供对该账号的认证服务，并返回认证成功结果及相应用户状态信息，请求认证的应用系统根据 UDB 返回的认证结果和用户状态信息判断是否为该账号提供服务。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的其他停机状态可对应于 CRM 的用户挂失停机、违章停机、加锁停机等状态。

7） 拆机：该状态下 UDB 应注销该账号，并停止对该账号的认证服务，向请求认证的应用系统返回认证失败结果及相应原因值。该状态信息需省 UDB 同步给全国 UDB。省 UDB 的拆机状态可对应于 CRM 的用户拆机、预拆机、违章拆机、欠费拆机等状态。拆机用户的账号数据 UDB 应能够保留一段时间（默认为三个月，可配置），保留期过后 UDB 应能自动删除该统一账号的所有用户信息数据。

8） 暂停服务：该状态下 UDB 应停止该账号的认证服务，并向请求认证的应用系统返回认证失败结果及相应原因值（该原因值不同于 UDB 管理员将该账号设置为去激活状态下，认证失败的原因值）。

该状态信息需省 UDB 同步给全国 UDB。省 UDB 的暂停服务状态可对应于 CRM 的障碍、施工未完、资源封锁等状态。如用户有换号需求，UDB 管理员可为用户更新新的统一账号并保留已有的用户信息数据，在 UDB 对用户信息数据更新未完结期间，对该账号的用户状态可设定为暂定服务，更新完结后，省 UDB 将用户状态更改为正常。

6.6 短信动态密码生成

短信动态密码可由用户在 UDB 自服务界面、各个应用系统的门户或服务界面上点击“短信获取动态密码”进行触发，并由 UDB 生成短信动态密码，通过 ISAG/短信网关/短信中心下发给用户手机。

如申请账号未开通、号码不存在、号码错误、或用户停机、拆机等，UDB 应向短信密码获取请求的发送端回复失败及原因值。

短信动态密码等同于通用密码，属于只在一定时间期限内有效或一次性登录认证的统一账号通用密码。对于每个统一账号，UDB 可以设置短信密码采用有效期方式还是一次性密码认证方式。

如采用短信动态密码认证，应用系统在认证时应提供不同的密码输入窗口，并在向 UDB 进行业务认证请求时设置相应的鉴权类型（通用密码认证/短信动态密码认证等），供 UDB 进行判断。

6.7 用户自服务

UDB 应提供自服务界面实现用户自助式管理的功能，用户在自服务门户通过输入统一帐号（或别名）和通用密码进行登录后，可以实现：

1）客户信息维护，如用户姓名、联系电话、联系邮箱等信息的查询与修改。

2）别名设置。设置统一账号对应的别名。

3）通用密码更改。用户可以在自服务门户上修改通用密码。修改时需输入“原密码”、“新密码”和“确认密码”。“确认密码”应与“新密码”一致。输入的密码以圆点显示，密码设置成功后提示“新密码设置成功”。

4）通用密码重置。如用户忘记通用密码，可点击进入通用密码重置界面，并通过短信或邮箱实现通用密码的重置。

5）短信动态密码获取。用户在登录时可在自服务界面上提供短信动态密码获取功能框和短信动态密码输入窗口。

6）宽带用户“区号+0+7 位数字”UDB 虚拟账号激活。对于没有绑定固定电话号码的宽带用户，用户通过自服务界面输入该宽带账号后，由 UDB 对该宽带账号生成“区号+0+7 位数字”的 UDB 虚拟账号，用户可通过自服务界面激活该 UDB 虚拟账号后，UDB 可对该账号提供认证服务。

7）省内各应用系统的认证密码策略设置与省内应用系统业务密码设置。通过自服务界面能够向用户呈现该账号所提供认证服务的应用类型，如用户将已设置为业务密码认证方式的某应用更改为通用密码认证方式，可通过自服务界面进行设置，设置时采用列表选择的方式设置。如用户将已设置为通用密码认证方式的某业务更改为业务密码认证方式，可通过自服务界面进行设置，并进一步在自服务界面上设置相应的业务密码。对于全国业务的业务密码设置，则直接单点登录到该全国应用系统的服务页面，由全国应用系统完成设置与业务密码的保存，在认证时全国应用系统判断用户是否设置了业务密码，如设置，则根据场景让用户输入该业务密码进行二次认证。

首次设置业务密码需输入“新密码”和“确认密码”，“确认密码”应与“新密码”一致，输入的密码以圆点显示，密码设置成功后提示“新密码设置成功”。在自服务门户上修改业务密码需输入“原密码”、“新密码”和“确认密码”，“确认密码”应与“新密码”一致，输入的密码以圆点显示，密码设置成功后提示“新密码设置成功”。

8）历史记录查询。用户可查询登录相关的历史记录信息，如登录认证总次数、登录各应用系统认证次数及时间等。

9）后续可扩展通信录、积分管理、群组管理等功能或其他应用服务，用户可以在自服务界面中查询通信录、积分、群组等数据，也可在自服务界面中修改通信录、设置群组。

自服务门户分为全国和省两级架构：全国门户主要提供通用管理能力，面

向全国应用系统的相关展示服务，并提供到各省门户的链接服务；省级门户可在全国统一服务功能要求的基础上，进一步根据省内统一帐号用户的需求开发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，不单独建设。

全国自服务门户和省自服务门户采用统一域名，暂定为“passport.189.cn”的二级域名，各省采用三级域名，域名规划由集团统一安排。

UDB 用户登录界面与自服务门户应为同一域名，参考页面参见接口与流程规范 15.1 节。

6.8 统一账号宽带接入认证

用户应能够利用统一账号（cdma 号码或区号＋固定电话），实现宽带接入认证服务，该功能仅对于省 UDB 有效。

UDB 应能够对统一帐号及密码的验证（密码错误、账户无效）、以及 Radius 服务器返回的 Radius 报文（计费请求、计费终止），同步 UDB 中该账号数据中的宽带接入在线状态。

宽带接入认证服务的实现流程主要为：

1）用户通过统一账号进行宽带接入拨号，拨号账号后缀域名应采用专用域名（如 189xxxxxxxx@189.cn）；

2）BRAS 判断账号后缀域名，并根据既定策略将认证请求转发到相应的 Radius 服务器，Radius 服务器判断账号后缀域名，将该认证请求转发到 UDB；

3）UDB 收到宽带接入认证请求，完成密码验证及账户状态有效性判断（参见 6.2 节）。如果密码错误或者账户状态无效，则直接返回拒绝报文；如果验证通过，则把收到的请求报文直接转发给 Radius 服务器，该请求报文的密码由 UDB 重置为固定密码（固定密码各省自行规定，Radius 服务器默认该密码为认证通过），并包含用户状态信息；

4）Radius 服务器根据 UDB 转发过来的认证请求、判断最大连接数和绑定信息，通过后再将认证报文返回给 BRAS，并通知用户登陆成功；

5）BRAS 向 Radius 服务器发送计费报文，由 Radius 服务器生成话单给营

帐计费；

6）Radius 服务器向 UDB 发送计费请求报文，UDB 将该统一账号的宽带接入置为在线状态。如用户下线，Radius 服务器向 UDB 发送计费终止报文，UDB 将该统一账号的宽带接入置为离线状态。

6.9 系统管理

为保证 UDB 系统正常运行，应提供系统管理功能。

6.9.1 运行监控

UDB 应支持对系统设备的 CPU、内存、硬盘等系统资源的监视功能，并支持对这些参数设置阈值，当实际参数值高于或低于阈值时，能够产生系统告警。

应监视的系统资源包括：

- 系统认证运行情况
- 硬盘占用率
- 内存占用率
- CPU 资源等

6.9.2 数据管理

UDB 应具有数据库备份、恢复等功能。

UDB 通过自身界面可将指定的数据备份到指定的外围存储器中，外围存储器可以包括磁盘、磁带、数据库等。也可将指定外围存储器中的内容恢复到系统中。

UDB 提供数据导出功能，包括如下数据：

- 设备资源及配置数据
- 用户数据
- 日志数据：操作日志，接口日志等
- 告警数据

- 性能数据等

6.9.3 统计分析

UDB 应支持对系统运行情况等进行检查，采集关键的系统及业务性能指标，并在此基础上提供统计分析工具，供管理员进行故障排查和性能分析使用。包括各应用系统认证统计、用户登录行为记录与分析、用户自服务统计、系统性能数据等。

UDB 应支持对统一账号及管理业务信息进行统计分析，包括基于用户对其绑定的所有业务类型的统计分析和已绑定了某种业务类型的所有用户的统计分析等。

全国 UDB 应支持统一账号使用全国业务的统计分析，并支持查询账号登录全国应用系统的日志。

省 UDB 应能支持统一账号使用省内业务的统计分析，并支持统一账号使用所有业务的统计分析。

6.9.4 日志管理

UDB 应支持系统日志、接口日志、错误日志、操作日志、数据库和目录服务器运行及出错日志。

日志以文本或数据库的方式进行存储，可以灵活定义其日志级别，同时也可结合统计分析工具对这些日志进行查询、分析、统计以及报表打印等服务。

UDB 应支持根据给定条件对日志进行查询，并可对查询到的日志进行排序，查询条件包括给定时间或时间段进行查询、给定用户进行查询和给定的日志类型等。

6.9.5 管理员门户

UDB 应提供面向管理员的管理界面，系统管理员通过该门户登录系统后进行系统的监控和维护，包括对用户信息的增加、删除、修改和查询等管理功能，管理员信息的查询、增删改等功能，管理员权限的分配管理等，管理员可以查

询系统的日志，使用系统提供报表功能，并可以管理系统的配置信息等。

6.9.6 账号审计功能

UDB 应支持账号审计功能，如果一个账号的密码输入错误超过 N 次（可配置），UDB 应延时响应，如果一个账号的密码输入超过 M 次之后，UDB 应能够锁定这个账号，并发送告警。

6.10 其他功能

UDB 后续可根据需要进一步提供支付认证功能、共享数据的管理功能。

6.10.1 支付认证功能

UDB 应支持向支付系统提供支付认证请求接口，支付系统可以用统一账号、支付密码和支付业务的标识向 UDB 请求支付认证。

UDB 应能判断支付业务是否合法，如果合法，UDB 应能根据统一账号、支付密码和支付业务进行支付认证。

6.10.2 共享数据的管理

UDB 应支持通信录功能、积分、群组数据等共享数据的管理功能。

UDB 应支持应用系统使用用户的业务账号或统一账号查询和修改用户的共享数据（如积分、通信录等）。

UDB 应能判断应用系统是否具有修改特定数据的能力，如通信录只能通过自服务门户和邮箱系统修改。

UDB 应支持应用系统通过群组标识等业务数据的标识查询和修改业务共享数据。

7 接口与协议要求

UDB 作为应用层用户数据库，需与 IT 支撑系统、各个应用系统、ISMP、Radius 服务器等实现接口互通。各系统接口协议主要有 ISAP、SOAP 和 Radius，后续根据业务需求在进行新的协议扩展的时候，UDB 应只需增加相应的协议解析模块。

接口与协议要求具体参见《中国电信用户数据库接口与流程规范》。

8 数据要求

8.1 数据库模型要求

UDB 数据库模块示例如下图所示：

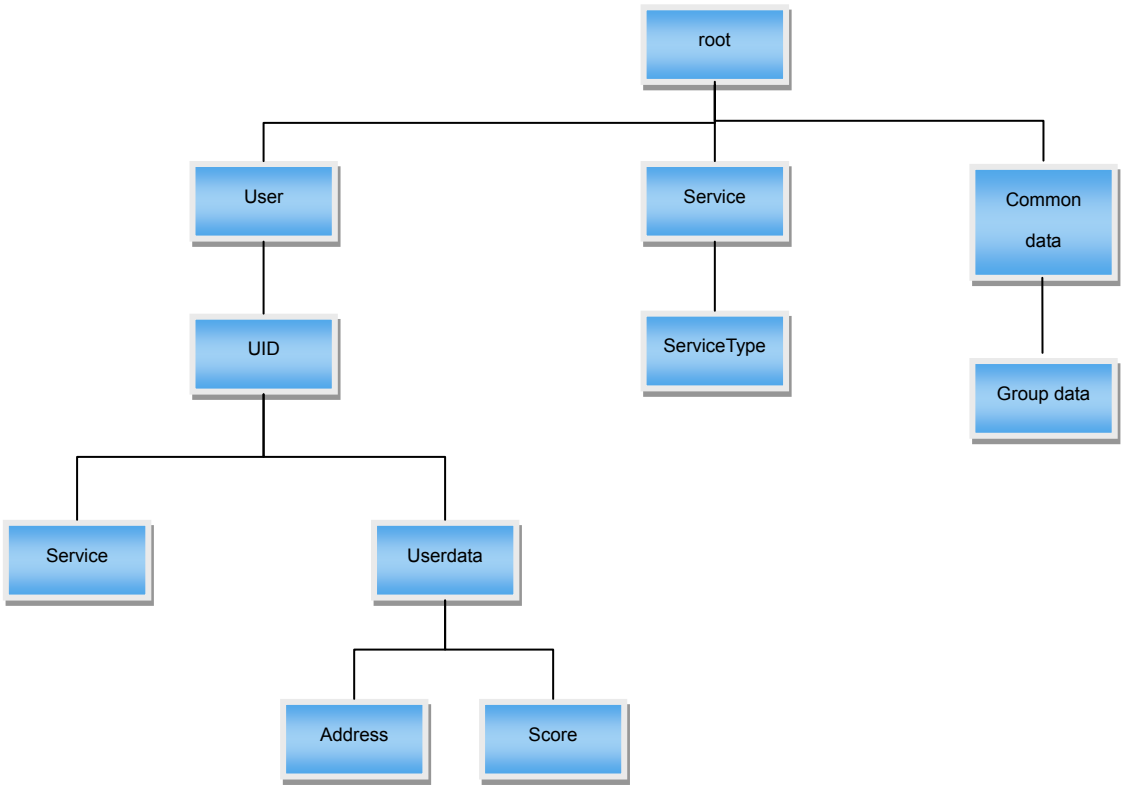

图 8-1 UDB 数据库模块示意图（示例）

UDB 的数据库模型应能够管理三类数据：

User 用于管理 UDB 中用户数据信息，每个统一账号生成一个 UID 目录，包含：UID 用户统一账号节点，管理统一账号，客户信息，密码，用户状态等统一账号的用户信息。

Service 是统一账号绑定的业务数据，包含有业务类型，业务账号和业务密码等业务的信息。

Userdata 主要用于管理用户的共享数据，如通信录、积分等。

Service 目录用于管理所有需要和统一账号绑定的应用系统的数据，每类业

务一个 ServiceType 节点，ServiceType 节点是描述业务的数据，包含有业务类型，业务名称等业务描述信息。

Comm data 目录用于管理所有业务共享的全局数据，如群组数据等。

UDB 数据库的数据模型应能够支持模型的在线升级，升级包含目录结构的变化和节点数据类型的变化。对于目录结构的升级，可以在一类目录下增加新节点类型和子目录类型，也可以删除一类目录下的一个子目录类型或节点类型。对于节点数据类型的变化，可以向一类节点中增加或删除属性。

8.2 数据字段定义

数据字段的示例说明如下面表格所示。

表名：USERID（用户统一账号表）（示例）

字段名称	数据类型	长度（字节）	说明
USER_ID	String	40	统一帐号
PASSWD	String	64	统一帐号密码
EXT_PASSWD	String	64	扩展密码
TMP_PASSWD	String	64	动态临时密码
TMP_CREATE_TIME	uint4	4	动态密码生成时间
TMP_EXIRATION_TIME	Uint4	4	动态密码的超时时间
OTP_TOKENID	int4	4	OTP 的 TOKENID
USERID_STATUS	String	2	统一帐号状态
USERID_TYPE	String	2	统一帐号类型
SEX	int1	1	性别 （0：缺省 1：男 2：女）
EMAIL	String	64	电子邮件地址
CREATE_TIME	uint4	4	记录创建时间
LAST_MODIFY_TIME	uint4	4	最近修改时间

PROVINCE_NO	String	2	归属省份
CITY_NO	String	4	归属地市（区号）
CERTIFICATE_TYPE	String	2	用户证件类型
CERTIFICATE_NO	String	40	用户证件号
PAY_TYPE	String	2	用户付费类型
PRE_PAY_SYSTEM_NO	String	14	预付费系统设备号
PAY_EFFECT_MODE	int1	1	付费类型更新生效模式
PAY_EFFECT_TIME	uint4	4	付费类型状态更新生效时间
SRC_DEVICE_NO	String	14	发起最后修改操作 CRM 平台号
ACTIVE_STATUS	int1	1	激活状态（0 去活 1 激活）
UPDATE_FLAGE	Int1	1	上传全国 UDB 的标志

表名：SERVICE（和统一账绑定的应用系统的数据）（示例）

字段名称	数据类型	长度（字节）	说明
SS_ID	String	40	应用系统设备标识
SS_STATUS	String	2	应用系统状态
SS_TYPE	String	4	应用系统类型
SS_PASSWORD	String	64	统一账号的业务密码
SS_DEVICE_NO	String	14	发起最后修改操作应用系统设备标识
CREATE_TIME	uint4	4	创建时间
LAST_MODIFY_TIME	uint4	4	最近修改时间
AUTH_SRC	String	16	高安全认证
REG_EFFECT_MODE	int1	1	注册状态生效模式
REG_EEFFECT_TIME	uint4	4	注册状态更新生效时间
BIND_TYPE	int1	2	绑定类型

BIND_EFFECT_MODE	int1	1	绑定生效模式
BIND_EFFECT_TIME	uint4	4	帐号绑定生效时间

表名：ServiceType（示例）

字段名称	数据类型	长度（字节）	说明
ServiceType	String	4	应用系统的类型
ServiceName	String	80	业务名称

8.3 数据关联关系要求

对于 UDB 数据关联关系，UID 目录下 Service 节点中的 SS_TYPE 和 ServieType 中节点中的 ServiceType 节点实现关联，SS_TYPE 可引用 ServiceType，如下图所示。

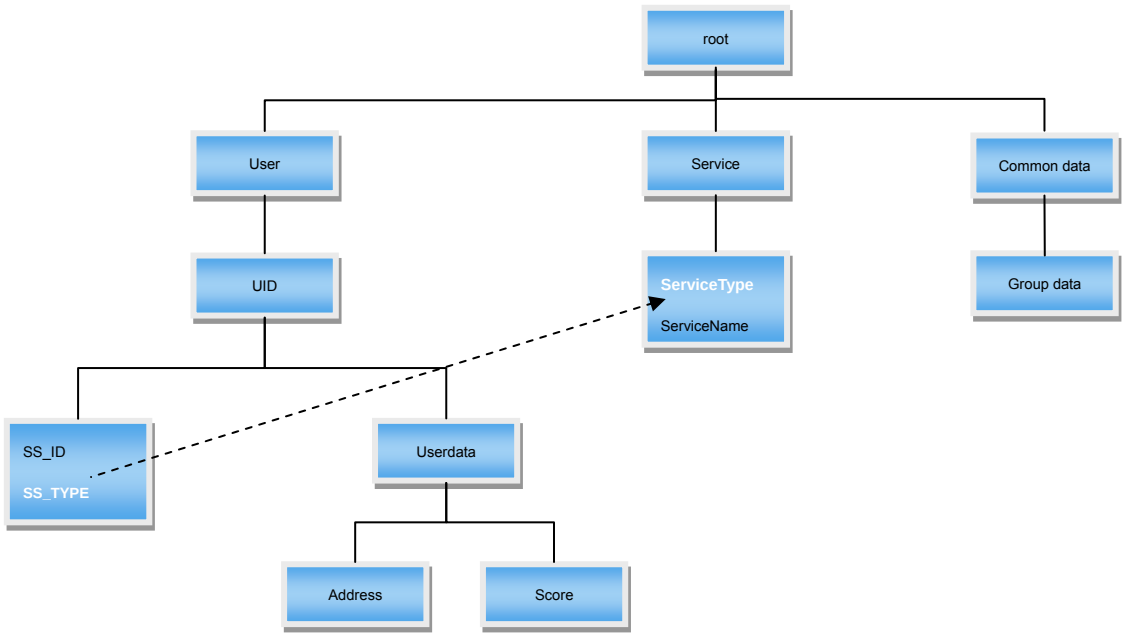

图 8-2 UDB 数据关联关系示意图（示例）

9 网管要求

UDB 网管系统主要实现系统本地的配置管理、故障管理、安全管理和性能管理。

UDB 网管系统应具备以下特性：

（1）实时性：系统在完成各类实时功能时应保证系统反应的实时性，包括实时故障监视、实时性能分析和操作维护等。

（2）安全性：系统应有多级安全管理机制。

（3）可靠性：避免由于单点故障影响整个系统的正常稳定运行，避免关键管理信息的丢失。

（4）可维护性：系统应具有完善的自身监视和管理功能。

（5）可操作性：提供友好的中文图形化操作界面和在线帮助。

（6）开放性：充分考虑与其他的系统（如其他网管系统等）的接口。

（7）可扩充性：系统的软件设计采用模块化的体系结构，新功能的引入不影响原有的功能模块，具有良好的可扩展性。同时，系统的容量可随硬件的扩容和软件的升级达到更高的要求。

9.1 配置管理

配置管理提供树状配置结构图和网络拓扑图，支持基于 Web Browser 实现的图形配置管理模式，完成对设备的配置、查询和操作功能。

9.2 故障管理

故障管理主要包括对设备的故障分级，故障分类，故障提示，故障实时监控，故障诊断及定位分析。硬件故障应具有障碍定位的功能，以便维护人员及时准确的处理障碍。在发生硬件故障时，应能隔离有故障的硬件或自动倒换至无故障的备用硬件，保证系统继续正常运行。发生软件故障时，系统应具有一定的自纠能力和自动恢复功能，包括再启动和再装入等功能。

故障告警建议分为三个级别，即紧急告警、重要告警、普通告警。告警级

别应能够支持自定义。

9.3 安全管理

UDB 应提供统一的安全策略控制，包括：

- 登录策略管理，系统应提供设置非法登录系统的次数及锁定时间，提供设置系统管理用户的账号有效期，提供设置登录超时退出时间等。
- 应提供系统管理用户密码重置的功能，重置密码不得为空。
- 系统管理用户密码设置策略，应提供限制系统管理用户设置的密码长度、密码组成等功能。
- 应支持系统管理用户登录的 IP 管理策略，将登录的系统管理用户与 IP 地址绑定，保证访问的安全。

（1）用户权限管理

系统应能够提供基于用户组的访问控制功能，并通过对用户组的授权来实现，在系统中应能设置如下的功能执行权限：

－ 数据管理的权限：数据查询、数据增加、数据修改、数据删除的权限。

－ 用户资料管理的权限：用户查询、增加用户、修改用户资料、删除用户资料的权限。

－ 系统功能模块的使用权限。

－ 对网管系统配置参数修改的权限（可选）。

－ 系统使用时间的选择权限。

－ 系统用户可以远端访问网管系统的权限。

（2）数据安全管理

网管系统对系统中告警、配置、性能、用户资料等数据的安全性提供保障措施，防止数据受到破坏或丢失。网管系统具有数据备份和数据恢复的功能，以保证数据的完备、可靠和安全。在对数据的管理和使用上，根据用户的权限及职能划分对该用户能够管理和使用的数据进行限制，包括：

－ 根据用户的功能执行权限，对数据的种类，如告警、配置、性能、用户

资料等，加以限制。

－ 根据用户的职能划分，对数据的管理范围，如所属管理部门等加以限制。

－ 用户只能对自己权限和职能范围内的数据进行使用和管理，权限和职能范围以外的数据对用户不可见。

－ 对于数据进行修改和删除的权限需要在功能执行权限和职能划分权限的基础上进一步加以限制，以保证网管系统数据的安全使用。

（3）安全检测功能

当用户操作出现以下情况时，网管系统应能及时产生警告信息，并禁止当前用户的进一步操作。

－ 试图多次用无效帐号登录

－ 密码的多次尝试

－ 用户多次试图操作自身权限范围之外的操作功能

－ 其它非法操作

网管系统应提供权限策略定义功能，以定义合法的权限定义与访问操作，提供安全检测标准。需定义的权限信息包括：

－ 权限有效时效

－ 密码有效长度

－ 密码有效尝试次数

－ 其他必须的权限定义策略

（4）分权分域管理

分权分域管理将角色管理和设备的分组管理形成二维的组合管理，这些资源与操作权限的组合，形成二维的分权分域模型和新的权限集合，以便分配给系统管理用户，达到控制系统管理用户权限的目的。

系统应支持创建管理域（组的概念）和用户帐号的功能：

1、系统应具有创建、删除管理域的功能；每个管理域代表可管理的设备范围；

2、系统应具有为管理域分配不同的角色的功能；每个角色至少包括对系统各模块的查看、更改、删除等权限；每个角色内的权限避免冲突；

3、系统应具有将用户帐号归属到不同的管理域的功能；

4、系统至少支持 3 级以上的分权分域管理，包括省、市、区等。

9.4 性能管理

网管系统应提供性能统计功能。

10 性能要求

10.1 性能指标

UDB 应采用模块化方式，其存储容量、处理能力应能够根据业务的要求平滑扩展。

省 UDB 可支持的最大用户数据容量不低于 2 千万用户，并可按需扩展。全国 UDB 可支持的最大用户数据容量不低于 5 千万用户，并可按需扩展。

UDB 支持的并发连接数为 5000 个连接以上。

UDB 支持的账户认证处理能力为 5000 次/秒以上。

省 UDB 数据查询处理时间平均小于 3 ms，最大小于 20 ms；数据更新处理时间平均小于 10 ms，最大小于 30 ms。全国 UDB 数据查询处理时间平均小于 5ms，最大小于 50ms。

从收到各应用系统认证请求到返回应答期间，由于系统原因造成的消息丢失率 $P \leq 10^{-7}$。

UDB 硬件设备的 CPU 忙时利用率平均不超过 70%，内存忙时利用率平均不超过 70%。

UDB 应支持负载均衡，系统在切换过程中应保证已经处理过的业务正常运行。

UDB 应支持数据的分布式存储和访问。

UDB 对于 Radius 协议的支持，要求 Radius 支持的最大用户数不低于 100 万，Radius 同时处理的认证数不小于 400 次/秒，Radius 处理认证的时间应小于 50ms。

10.2 可靠性要求

UDB 应具有安全防御能力，防止非法入侵，对系统如硬件、操作系统、网

络、数据库应设计详尽的故障处理方案，保证系统的快速恢复性，并采用冗余技术（冗余设备、冗余通信链路、RAID 技术）保证数据可靠存储、网络系统可靠运行。对系统运行状况采用自动检测、告警、监控等方式实现实时观测。

系统可靠性要求：

（1）排除人为误操作因素，由于系统自身原因导致的系统崩溃故障，平均无故障时间（MTBF）应不小于 26280 小时（3 年），系统平均无故障率不低于 99.999%。

（2）系统应具备电信级可靠性、多种冗余、备份和集群处理的机制和功能，重要部件、数据库等采用双备份配置，具备冗余和负载分担机制，保证系统无单一故障点。主要模块冗余度为 1+1，易于扩容和维护。

（3）系统处理能力应采用相应的流量控制措施，满足对处理时延、CPU 使用率的要求，保证系统的稳定运行。

10.3 可扩展性

UDB 系统设计应充分考虑可扩展性，能够以多种方式支持系统的扩展，包括业务功能的增加，接口模块的增加、系统升级以及系统扩容等。

10.4 可维护性

系统应具有完善的自身监视和管理功能，并具有故障诊断和故障定位功能。

10.5 备份、倒换和故障恢复要求

- 系统应采用多级负荷控制机制，实现负荷分担和节点级备份。
- 系统应有良好的备份和恢复的日常工作计划，系统数据和业务数据可联机备份、联机恢复，恢复的数据应保持其完整性和一致性。
- 系统出现故障后，应能够快速切换（包括人工或自动切换），保证系统连续工作。
- 系统应具备自动或手动恢复措施，在系统使用过程中，由于硬件出现故障或其它原因造成系统暂时性的中断后系统重新启动时，能够保证系统

将原有的数据快速恢复。

- 系统应支持异地备份，当工作设备所在地区发生各种灾害而导致系统瘫痪时，应能启动另一地区的备份设备继续提供服务。
- 系统发生故障时，应该能够尽快维护和恢复。系统恢复时间应小于 30 分钟。

11 安全要求

11.1 认证安全

- 为了保障信息的安全，UDB与各应用系统之间的信息通讯应进行加密/解密。应用系统与UDB所使用的共享密钥应定期更新管理，避免出现密钥泄漏的情况。在正常更新情况下，由UDB生成新的密钥，应用系统收到密钥更新通知后，应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，如在处理请求时，删除过期的原密钥所加密的用户Token信息。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。
- UDB应提供基于SSL的HTTPS加密传输，在用户输入账号和密码提交UDB进行认证的关键页面应强制采用HTTPS传输，不允许采用HTTP方式，以保证用户密码在传输过程中的安全。
- UDB提供的登录认证页面应采用动态验证码方式，以防止攻击。
- UDB应以密文方式存储密码。

11.2 网络安全

网络安全主要通过网络设备的设置和传输的加密，保证数据在网络传输中的安全。

- 应通过防火墙等措施对进入内部网络的数据包进行扫描过滤，能够根据用户、IP地址、访问类型等方式进行访问规则限制，并能够对常见的入侵行为进行检测并阻止。
- 防火墙要求如下：
  - 并发会话≥128,000。
  - 时间表≥256。
  - 支持NAT(所有端口)。

- ◆ 支持PAT(端口地址转换)。
- ◆ 每个端口的用户数，信任端没有限制。
- ◆ 信任端支持内部DHCP服务器。
- ◆ 支持DHCP Relay。
- ◆ 支持检测死ping(Ping of death)、检测IP欺骗(IP spoofing)、检测端口扫描(Port scan)、检测陆地攻击(Land attack)、检测撕毁攻击(Tear drop attack)、过滤IP源路由选项(Filter IP source route option)、检测IP地址扫描攻击(IP address sweep attack)、检测WinNuke attack攻击等。
- ◆ 专用隧道≥1,000。
- ◆ 支持远程接入VPN(Remote access VPN)。
- ◆ 支持Versign、Entrust、Microsoft、RSA Keon、IPlanet(Netscape)、等认证。
- ◆ 支持ARP、TCP/IP、UDP、ICMP、HTTP、RADIUS、IPSec(IPESP)、MD5、SHB-1、 DES、3DES、SNMP、DHCP、PPPoE等标准。
- ◆ 支持VPN通道监视程序(VPN tunnel monitor)。
- ◆ 支持网址浏览器配置管理（WebUI:HTTP and HTTPS）。
- ◆ 必须支持动态和静态的内部网与外部网之间的地址转换、映射。
- ◆ 应该支持路由、透明、混合工作模式。
- ◆ 必须能对所有端口的访问权限进行有效控制和管理。
- ◆ 必须能有效地实现内部网到外部网的单向访问控制，可以禁止外部网对内部网的访问。
- ◆ 必须能侦测、过滤或跟踪非法访问企图，能自动实时告警，并生成相应日志记录。
- ◆ 必须能对经过防火墙的网络流量进行统计和管理，并定期生成相应报告文件。
- ◆ 必须支持SNMP和SNMPv2协议。
- ◆ 应该能够防范DoS、DDoS等攻击。

➢ 厂商应提供防火墙各项指标，包括但不限于以下内容：明文吞吐量、密

文吞吐量、并发连接数、丢包率、延时、是否支持均衡负载、是否支持策略路由、是否支持 radius、支持的防火墙策略、是否支持802.1q及VPN，是否支持IPsec的NAT穿越等。

- 各子网间或远程用户传输中的数据应进行安全保护，利用加密等方式保证数据不被非法截获，并提供用户身份认证、授权等功能。
- 系统对内对外有多种方式的联接，在各种途径的数据交换中都可能含有病毒感染的隐患。对于这些存在的安全问题，应提供有效的手段，对在网络中传输的数据进行实时的监视，对各种类型的文件都能够进行病毒的查杀工作，并能够自动进行病毒代码库的更新。

11.3 系统安全

系统应能够防止未授权用户的非法访问。具体要求如下：

- 应能够限制用户访问主机资源，不同部门或类型的用户只能访问相应的文件或应用，并能够采取授权方式限定用户对主机的访问范围。
- 对于需要登录系统访问的用户，应能够提供安全策略强制实现用户口令的安全，如限制口令长度、限定口令修改时间间隔等，保证其身份的合法性。
- 应提供完善的漏洞扫描手段，及时发现系统的安全隐患，并据此提供必要的解决方案。
- 对主机等设备的安全事件应该进行详细的记录，并根据需要随时进行查阅。

12 软硬件要求

12.1 软件要求

12.1.1 总体要求

- 系统应支持 IPv4 协议，建议支持 IPv6 协议。

- 系统应遵循开放性、安全可靠性、先进性、高效性、易用性、可维护性和可扩展性等原则。
- 系统建设应基于业界开放式标准，包括各种网络协议、硬件接口、数据库接口等，具有良好的互操作能力。
- 系统应遵循简洁、易用、统一风格的中文客户界面，提供维护管理和实时监控功能，简化系统的使用和维护。

12.1.2 操作系统要求

操作系统要求如下：

- 关键主机（如应用服务器、数据库服务器）应采用 Linux/UNIX 操作系统；
- 操作系统应支持虚拟内存管理，支持多用户、多任务、多进程和多线程。
- 操作系统应达到 C2 级以上的安全标准，并通过对操作系统进行设置、加固达到 C2 级的安全标准。
- 支持完全对称多处理器（SMP）；
- 操作系统应遵循 X/open XPG4，POSIX 1003.1 等国际或工业标准。
- 操作系统应提供图形化的系统管理工具。
- 应支持在线诊断和软硬件的自动错误记录，在电源故障或其他紧急情况可提供自保护和自恢复功能。
- 应支持中文大字符集等相关国家标准。

12.1.3 数据库要求

数据库系统应满足以下要求：

- 应支持 ANSI/ISO SQL-89、ANSI/ISO SQL-92 标准。
- 应支持中文汉字内码，符合双字节编码。
- 应支持主流厂商的硬件平台及操作系统平台。
- 数据库系统应该具有良好的伸缩性。
- 应支持主流的网络协议（如：TCP/IP、IPX/SPX、NETBIOS 及混合

协议）。

- 应具有良好的开放性，支持异种数据库的互访；
- 应支持分布式事务及两阶段提交功能。
- 应具有并行处理能力（如：多服务器协同技术、事务处理的完整性控制技术等）。
- 应支持联机事务处理（OLTP）；要求能够实现数据的快速装载、高效的并发处理和交互式查询。
- 应支持 C2 或以上级安全标准、多级安全控制。
- 应支持数据库存储加密及相应冗余控制。
- 应提供 Web 服务接口模块，对客户端输出协议支持 HTTP2.0、SSL 等。
- 应支持联机存储和备份功能（如：磁带方式、光盘方式）。
- 应具有强的容错能力、错误恢复能力、错误记录及预警能力。
- 应支持对多媒体数据及大数据量处理的技术需求。
- 应提供易使用、开发效率高、维护方便的维护管理工具。
- 应支持分区技术。
- 应避免数据库死锁的出现，一旦死锁能够自动解锁。

12.1.4 应用软件要求

应用软件应满足的基本要求：

- 实时性：系统在完成各类实时功能时应保证系统反应的实时性，包括实时的故障监视、实时的性能分析和操作维护等。
- 安全性：系统应有多级安全管理机制。
- 可靠性：应支持集群（cluster）避免由于单点故障影响整个系统的正常稳定运行，避免关键管理信息的丢失，应具备相应系统容错能力。整个应用软件系统应能够连续 7×24 小时不间断工作，应用软件中的任一模块更新、加载时，在不更新与上下模块的接口的前提下，不影响业务运转和服务。
- 可维护性：系统应具有完善的自身监视和管理功能，要求具有故障诊

断和故障定位功能。

- 可操作性：提供友好的中文的图形化操作界面和在线帮助。应具有完整的操作权限管理功能和完善的系统安全机制，能够对每个操作员的每次操作有详细的记录，对每次非法操作产生告警；应用软件应具有较高的自动化程度，如：自动任务调度、自动故障告警、自动任务恢复等。
- 开放性：充分考虑与其他的系统的接口。
- 可扩充性：系统的软件设计采用模块化的体系结构，新功能的引入不影响原有的功能模块，具有良好的可扩展性。
- 规范性：遵循中国电信的相关规范。

12.2 硬件要求

12.2.1 总体要求

硬件总体要求：

- 硬件体系需要高速计算能力、高度的系统可靠性、海量数据存储处理能力。
- 系统采用的计算机系统，主要是高性能服务器，要求在性能、可靠性、可管理性和易用性、可扩展性、服务与支持等方面能够达到电信级服务器的水准，重点满足数据库的操作和数据计算功能。
- 各类计算机系统的处理能力配置可根据系统忙时数据处理量及系统联机存储容量等参数进行综合计算，要求按照忙时数据处理量来进行配置，并提供较大的余量。
- 应能够保证系统方便的扩容和升级。系统联机存储容量按照保存两年的要求来进行配置，并提供方便的脱机存储和恢复工具。提供大容量光盘（DVD）刻录方式保存历史数据。
- 计算机设备应具有较强的扩充能力，包括系统处理能力的扩充、存储容量的扩充及 I/O 能力的扩充等；支持 CPU 升级。
- 应能够提供高级别 RAID，大容量磁盘阵列系统。

- 网络连接设备，主要包括路由器、网络交换机、I/O 设备等，需 7*24 小时连续运行。

12.2.2 主机设备要求

对于处理系统关键业务逻辑的主机设备要求如下：

- 应采用主流小型机平台的主流机型，或者 ATCA 服务器，支持多处理器，采用 64 位处理器。
- 应组成双机或多机高可用群集系统。当其中任意一台主机（包括运行在该主机上的数据库实例或应用）发生故障时，可将其上的应用自动地切换到其他正常主机上，待故障主机修复后再切换回来。集群系统中某一台计算机出现故障时，应该不影响系统的使用。
- 多机群集系统中的每台主机都应同时处于工作状态，并根据配置的情况运行相同或者不同的应用（或应用模块），以保证主机资源的充分利用。
- 主机的处理能力应该能够满足所有业务应用和一定用户规模的需求，而且需考虑全部系统的开销及应用切换时性能余量。系统设计时应考虑 30%的性能冗余。
- 内存容量的配置应考虑到主机正常运行状态下的内存利用率不应大于 70%，保证系统在业务高峰时仍具有较强的抗冲击能力。
- 主机应支持 1000Mb/s 等高速连接接入系统核心局域网。
- 主机的硬盘、高速 PCI 插槽、网络接口、网络连接及电源等均应考虑足够的冗余。
- 应支持电源、I/O 设备、存储设备的热插拔。
- 主机设备应具有适当的扩充能力，包括 CPU 的扩充、内存容量的扩充及 I/O 能力的扩充等；并可支持 CPU 模块的升级和群集内节点数的平滑扩充；应至少保证还有 30%以上的扩展能力。

12.2.3 存储设备要求

存储设备主要指磁盘阵列等，实现对系统数据的联机存储，存储设备的要求

如下：

- 磁盘阵列设备应能和主流厂家的主机系统相连。
- 磁盘阵列应满足多机高可用群集系统的需要。
- 磁盘阵列应采用ULTRA SCSI 接口或FC-AL 接口，建议使用FC-AL 接口，必须支持RAID1+0，RAID5，可以支持RAID0、RAID1、RAID0+1、RAID3 等。应提供多通道、双电源及冗余风扇。
- 磁盘阵列应支持电源、磁盘等的热拔插要求。
- 磁盘阵列磁盘的转速应大于10000RPM。
- 磁盘阵列设备应具有较强的平滑扩充能力，包括系统存储容量的扩充及I/O 能力的扩充等。
- 磁盘阵列应支持存储区域网（SAN）等存储、备份方式。
- 磁盘阵列应具备完善的存储系统管理软件，同时该软件应能与主流的通用网管软件进行集成。

12.2.4 备份设备要求

备份设备一般指大容量的磁带库或光盘库等，主要用于系统数据的脱机备份，也可以使用磁盘阵列作为数据备份的介质进行数据归档。

- 为了进行历史数据的保存与归档，必须从业务及维护上定义备份的策略，以减少历史数据堆积对系统性能的影响。
- 备份系统应该能在6~10 个小时内完成系统的全备份工作，避免备份工作对实际生产的影响。在业务运行高峰期运行的备份工作所耗费的数据库服务器主机系统资源应小于5%。
- 备份设备容量应满足系统两次完整备份的空间及备份周期内日常增量备份及数据库归档备份需求。
- 使用磁带库作为备份设备时，设备应有良好的安全可靠性安全要求。
- 磁带库要求支持ULTRA SCSI 或SCSI-2 或FWD SCSI 或FC-AL 接口。大型的磁带库设备要求提供冗余的数据接口和机械手设备；
- 备份设备应具有较强的平滑扩充能力，包括系统设备容量的扩充及I/O 能力的扩充。

13 运行环境要求

13.1 机房环境条件

机房建设应采用节能环保材料，机房的墙壁应具有良好隔热能力，外门窗采用节能门窗等。无人值守机房应用隔热材料封堵所有玻璃窗户。根据设备和业务需求合理控制层高，在电器上采用节能型设备，如采用节能灯具，空调、电梯等电器采用节能型设备等。

- 机房环境条件必须达到如下条件：机房附近不应有易燃易爆品、污染气体、强电磁场、强震动源、强噪声源及所有危害系统正常操作或运行的因素。
- 门窗：机房所有门窗应该密封，以减少尘埃及噪音等外来干扰，门户及走道之大小应足够让设备在安装时运输之用。
- 地板：机房必须采用防静电活动地板，机房内电力电缆（包括地线）和通信电缆应该采用上走线方式。装修后机房净高应该大于3500mm。
- 照明：参考《电子计算机机房设计规范》（GB50174-93）要求，主机房照度应300 Lx，控制室照度应300 Lx；同时应设机房疏散照明、安全出口标志灯，其照度应0.5Lx。
- 安全消防应该达到如下要求：
  - 采用七氟丙烷气体等消防措施。
  - 机房内材料、设施使用防火耐用材料。
  - 机房内吊顶上下应设置探测器。
  - 机房内配备手动或自动灭火设备，手动灭火器应放置在机房的显眼处，且方便存取。
  - 机房安全出口不少于两个，且要保持畅通，不可放置杂物。
  - 机房应有紧急照明设备。
  - 可以采用防火隔离措施。
  - 符合建筑物消防设备规定，如《建筑设计防火规范》等。
- 天花板有如下要求：
  - 不能用易燃及易脱落尘埃或脱落微粒的物质做吊顶。

- 吊顶应该选用不起尘的吸声材料。

➢ 墙壁有如下要求：

- 机房墙壁应该采用防尘材料。
- 隔墙可以采用玻璃隔断。

➢ 机房环境要求应该达到如下要求：

机房内常年设置恒温恒湿机房专用空调机。设备开机时主机房的环境要求如下：

- 温度：夏季、23±2℃，冬季、20±2℃。
- 相对湿度：45%～65%。
- 温度变化率：5℃/h，不结露。
- 防尘：静态条件下测试，空气中0.5m的尘粒数，应少18000粒/升。

➢ 机房承重：机房楼板的荷重必须达到或超过600Kg/m2 (不包括电源部分)。

➢ 场地监控及门禁：机房内应该设置场地监控系统，对设备提供24小时全天候监控，并根据需要设置门禁系统。

➢ 其他要求：机器设备的四周必须留有足够的散热空间，避免阳光直射。

13.2 接地要求

➢ 机房要求有良好的接地系统，必须达到如下标准：

- 交流工作接地：接地电阻不大于2欧姆。
- 安全保护接地：接地电阻不大于2欧姆。
- 直流工作接地：接地电阻按计算机系统具体要求进行。
- 防雷接地：按现行国家标准《建筑防雷设计规范》执行。

13.3 空调及电源

➢ 空调

机房空调系统必须具有供风、加热、加湿、冷却、去湿和空气除尘能力，以满足以上的机房环境要求。

机房中的空调系统应合理的组织室内空气的流动使机房内的温度、湿度和洁净度能够更好的满足要求。提倡采用节能型空调，采用合理的实施方案提高空调

的制冷效率。

- 电源
  - 目标系统的每个节点都需要可靠的电源，可以采用直流电源，也可采用220V或380V交流电源，要求必须从UPS引接；每台设备的多路电源必须要求有不同的输入。
  - 目标系统应该配备至少两台UPS，互为热备份。在无外电供应的情况下能为设备供电不少于30分钟。
  - UPS电源必须符合GB7620-87的标准。
  - 应采用绿色节能型电源系统，采用合理的技术(如谐波整理等)提高目前电源系统中的电能转换效率。

其他应按照国家标准《电子计算机机房设计规范》（GB50174-93）或专门的机房设计执行。