**《XXXX代码设计文档》**

版本：

组长：

组员：

修改人：

创建日期：

完成日期：

版本修订记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **版本号** | **修订时间** | **修订内容** | **修订人员** |
| 1 | V1.0 | 2022/\*\*/\*\* |  |  |
| 2 | V2.0 |  |  |  |
| 3 | V3.0 |  |  |  |
| ... |  |  |  |  |

目录

[一、引言 7](#_Toc103763502)

[1.1 编写目的 7](#_Toc103763503)

[1.2 项目背景 7](#_Toc103763504)

[1.3 定义 8](#_Toc103763505)

[1.4 参考资料 8](#_Toc103763506)

[二、 总体设计 9](#_Toc103763507)

[2.1 系统总览 9](#_Toc103763508)

[2.1.1 网页端总览 9](#_Toc103763509)

[2.1.1.1 需求概述 9](#_Toc103763510)

[2.1.1.1.1 功能要求 9](#_Toc103763511)

[2.1.1.1.2 性能要求 9](#_Toc103763512)

[2.1.1.1.3 输入输出要求 9](#_Toc103763513)

[2.1.1.2 硬件结构 9](#_Toc103763514)

[2.1.1.3 软件结构 9](#_Toc103763515)

[2.1.1.3.1 总览组前端整体框架 9](#_Toc103763516)

[2.1.1.3.2 总览组前端模块 10](#_Toc103763517)

[2.2 设备认证 10](#_Toc103763518)

[2.2.1 设备认证组前端 10](#_Toc103763519)

[2.2.1.1 需求概述 11](#_Toc103763520)

[2.2.1.1.1 功能要求 11](#_Toc103763521)

[2.2.1.1.2 性能要求 11](#_Toc103763522)

[2.2.1.1.3 输入输出要求 11](#_Toc103763523)

[2.2.1.2 硬件结构 11](#_Toc103763524)

[2.2.1.3 软件结构 12](#_Toc103763525)

[2.2.1.3.1 设备认证组前端整体框架 12](#_Toc103763526)

[2.2.1.3.2 设备认证组前端模块 12](#_Toc103763527)

[2.2.2 设备认证组安卓端 13](#_Toc103763528)

[2.2.2.1 需求概述 13](#_Toc103763529)

[2.2.2.1.1 功能要求 13](#_Toc103763530)

[2.2.2.1.2 性能要求 13](#_Toc103763531)

[2.2.2.1.3 输入输出要求 13](#_Toc103763532)

[2.2.2.2 硬件结构 13](#_Toc103763533)

[2.2.3 设备认证组后端 13](#_Toc103763534)

[2.2.3.1 需求概述 14](#_Toc103763535)

[2.2.3.1.1 功能要求 14](#_Toc103763536)

[2.2.3.1.2 性能要求 14](#_Toc103763537)

[2.2.3.1.3 输入输出要求 14](#_Toc103763538)

[2.2.3.2 硬件结构 14](#_Toc103763539)

[2.2.3.3 软件结构 14](#_Toc103763540)

[2.2.3.3.1 设备认证组后端整体框架 14](#_Toc103763541)

[2.2.3.3.2 设备认证组后端模块 14](#_Toc103763542)

[2.3 用户认证 14](#_Toc103763543)

[2.3.1 用户认证组安卓端 14](#_Toc103763544)

[2.3.1.1 需求概述 15](#_Toc103763545)

[2.3.1.1.1 功能要求 15](#_Toc103763546)

[2.3.1.1.2 性能要求 15](#_Toc103763547)

[2.3.1.1.3 输入输出要求 15](#_Toc103763548)

[2.3.1.2 硬件结构 15](#_Toc103763549)

[2.3.1.3 软件结构 16](#_Toc103763550)

[2.3.1.3.1 设备认证组安卓端整体框架 16](#_Toc103763551)

[2.3.2 用户认证组后端 16](#_Toc103763552)

[2.3.2.1 需求概述 16](#_Toc103763553)

[2.3.2.1.1 功能要求 16](#_Toc103763554)

[2.3.2.1.2 性能要求 16](#_Toc103763555)

[2.3.2.1.3 输入输出要求 17](#_Toc103763556)

[2.3.2.2 硬件结构 17](#_Toc103763557)

[2.3.2.3 软件结构 17](#_Toc103763558)

[2.3.2.3.1 用户认证组后端整体框架 17](#_Toc103763559)

[2.3.2.3.2 用户认证组后端模块 18](#_Toc103763560)

[2.4 生物认证 19](#_Toc103763561)

[2.4.1 生物认证组安卓端 19](#_Toc103763562)

[2.4.1.1 需求概述 19](#_Toc103763563)

[2.4.1.1.1 功能要求 19](#_Toc103763564)

[2.4.1.1.2 性能要求 19](#_Toc103763565)

[2.4.1.1.3 输入输出要求 19](#_Toc103763566)

[2.4.1.2 硬件结构 20](#_Toc103763567)

[2.4.1.3 软件结构 20](#_Toc103763568)

[2.4.1.3.1 生物认证组安卓端整体框架 20](#_Toc103763569)

[2.4.2 生物认证组后端 20](#_Toc103763570)

[2.4.2.1 需求概述 20](#_Toc103763571)

[2.4.2.1.1 功能要求 20](#_Toc103763572)

[2.4.2.1.2 性能要求 20](#_Toc103763573)

[2.4.2.1.3 输入输出要求 21](#_Toc103763574)

[2.4.2.2 硬件结构 21](#_Toc103763575)

[2.4.2.3 软件结构 21](#_Toc103763576)

[2.4.2.3.1 生物认证组后端整体框架 21](#_Toc103763577)

[2.4.2.3.2 （软）生物认证模块 21](#_Toc103763578)

[三、模块核心数据结构说明 23](#_Toc103763579)

[3.1 数据结构设计 23](#_Toc103763580)

[3.2 数据格式设计 23](#_Toc103763581)

[3.3通用数据结构及变量 23](#_Toc103763582)

[3.3.1 宏定义 23](#_Toc103763583)

[3.3.2 变量 23](#_Toc103763584)

[3.3.3 结构体 24](#_Toc103763585)

# 一、引言

## 1.1 编写目的

本文档内容为云雾混构系统总览模块、设备认证模块、用户认证模块以及生物认证模块代码设计的书面文件，其预期读者为云雾混构系统总览模块、设备认证模块、用户认证模块以及生物认证模块代码设计的编码人员及负责人，用于指导编码人员进行开发。

## 1.2 项目背景

随着移动通信技术的持续发展，未来无线网络将呈现终端多元化、网络节点高密度海量、通信技术多样共存等特点。而未来移动互联网将由第五代移动通信（5G）主要载体，融入更多的应用场景，形成云雾混构计算框架，为用户提供高通信质量及多样化的服务。目前，大量的智能设备与感知节点都在陆续地接入至移动互联网中。信息技术分析机构Gartner公布的最新报告显示，预计至2020年将有超过200亿个连接入网络的传感器和端点，而其中物联网设备在2019年达到142亿，到2021年将增长到250亿，以海量智能设备为基础，为用户提供具有适应性的数字服务，形成智能计算网格，构成移动互联网空间。移动互联网用户将通过数千亿台设备连接到网络并享受服务，但不同类型的设备和应用场景具有不同的网络要求，网络实体节点的身份管理及认证方案性能将直接影响系统安全及服务质量。

为解决上述问题，首先，需要对海量差异化网络节点进行标识，形成移动互联网统一身份管理体系，并建立标识解析架构，支撑跨域管理、服务/数据共享及设备智能协同。移动互联网中的实体因认证方式或服务权限的差异，有多样化身份的需求，传统的身份标识体系并未考虑多元身份关联问题，同一实体的多项身份在系统中孤立存在，导致身份管理效率及安全性降低。因此，需要研究移动互联网中多元关联的统一身份标识与安全解析架构，支撑网络中大规模实体的身份管理及可信认证。

其次，在 5G 移动互联网中，确保安全有效的认证机制至关重要。5G移动互联网中存在多种不同的异构网络，而设备接入不同的网络需要不同的接入认证机制，这无疑会增加整个系统的复杂性。将各种类型的无线网络融合起来，在一个通用的网络平台上统一提供服务至关重要。此外，当前已经存在的接入认证方案不能同时满足相互认证，密钥协商，隐私保护，前向、后向安全等属性，且耗费较多的通信时延和计算开销。因此，针对 5G 异构互联网络中的设备研究一种统一、安全、有效的自适应接入认证机制至关重要。

再次，相较于传统互联网络，5G 移动互联网络中连接设备数量巨大且设备具有严格的时延和性能要求，大规模设备的安全和高效访问认证的设计是保证未来第五代（5G）系统下的应用安全性的关键点。若每个终端都与接入网络执行一次完全接入认证过程，可能会造成信令拥塞，从而对网络中关键节点的性能造成重大的影响。此外，这些海量连接的设备，例如医疗监控终端、体感传感器、安防监控终端等等，通常计算能力较低且能耗有限，无法支持当前通用的密码学算法。因此，针对海量设备提出轻量级群组认证机制是一个关键问题。

最后，生物特征作为一种快捷有效的生物标识，已逐渐被安全认证系统所认可和采用。当前普遍采用的生物特征包括指纹、人脸、虹膜、声纹和步态等，这些特征对于用户来说通常都是独一无二的，可以唯一确认用户的身份。与传统的认证方法相比，生物认证具有多种优势。它们被认为更安全、更可靠，因为生物特征很难复制、共享/分发，并且需要用户在认证时在场（活体检测）。在 5G网络中，海量设备的参与和海量应用的发布将对用户身份的认证提出更强的要求，充分利用生物特征认证的特点和优势，研究适合于5G网络的生物特征识别技术，对于提高用户体验并保护用户安全将起到至关重要的作用。

## 1.3 定义

clion：代码编写环境

API：应用编程接口

## 1.4 参考资料

[1]《云雾混构开发与维护文档》

[2]《云雾混构测试计划文档》

# 总体设计

## 2.1 系统总览

### 2.1.1 网页端总览

#### 2.1.1.1 需求概述

##### 2.1.1.1.1 功能要求

网页端总览的功能要求与项目功能要求无关，其具体功能包括：

（1）项目信息展示；

（2）设备认证、用户认证和生物认证信息展示；

（3）设备认证、用户认证和生物认证的运行状态和参数控制；

（4）网页端项目管理后台用户鉴权。

##### 2.1.1.1.2 性能要求

无

##### 2.1.1.1.3 输入输出要求

本部分主要进行内部数据交互，不与其他模块存在数据交互。

#### 2.1.1.2 硬件结构

无

#### 2.1.1.3 软件结构

##### 2.1.1.3.1 总览组前端整体框架

如图2-1所示，总览组前端整体实现使用的是B/S框架，其中B端即为总览组前端，S端为SpringBoot后台。S端从数据库中获取数据，为B端提供数据展示和权限控制的功能；与容器操作模块进行socket通信来获取或控制认证服务的运行状态。



图2-1 总览组前端整体框架

##### 2.1.1.3.2 总览组前端模块

在上述框架的基础上，主要分为四个模块来实现网络端总览的功能，分别为（1）项目信息展示模块；（2）认证信息展示模块；（3）认证服务操作模块；（4）权限控制模块。其中各个模块支持的操作和实现的功能如下：

（1）项目信息展示模块：静态信息，展示项目的基本情况；

（2）认证信息展示模块：从数据库中获取数据，聚合数据并按需展示各个认证服务的认证结果数据；

（3）认证服务操作模块：该部分可以探测当前各个认证服务的运行状态，支持开启和关闭指定认证服务的操作；

（4）权限控制模块：支持用户权限展示、更改，以及修改不同权限对应的可操作范围。

## 2.2 设备认证

### 2.2.1 设备认证组前端

#### 2.2.1.1 需求概述

##### 2.2.1.1.1 功能要求

前端仿真系统依据3GPP标准、行业现状、国密算法标准为基础，实现了基于LTE、5G网络、自适应网络三个安全仿真平台，具体功能包括：

（1）4G、5G、自适应单独认证流程：包括UE开机、驻留基站、附着、移动、切换等步骤的动态链接过程以及关键信息的展示。

（2）4G群组、5G群组的认证流程：包括群主标识、群组中的UE开机、接入认证、移动、切换等步骤的动态链接过程以及关键信息的展示。

##### 2.2.1.1.2 性能要求

无

##### 2.2.1.1.3 输入输出要求

此模块的数据流动形式为设备认证组后端-设备认证前端-网页展示。

单个认证：开机、驻留基站、附着、切换数据包必须包含“userID”；移动UE数据包必须包含“NewBaseStation”；

群组认证:群主标识数据包必须包含“group”；开机、驻留基站、附着、切换数据包必须包含“userID”；移动UE数据包必须包含“NewBaseStation”。

#### 2.2.1.2 硬件结构

无

#### 2.2.1.3 软件结构

##### 2.2.1.3.1 设备认证组前端整体框架

移动互联网中存在多种不同的异构网络，而设备接入不同的网络需要不同的接入认证机制，这无疑会增加整个系统的复杂性，将各种类型的无线网络融合起来，在一个通用的网络平台上统一提供服务至关重要。针对此问题，设备认证组前端主要分为三个子模块进行设计，分别是4G接入认证、5G接入认证、自适应接入认证。在4/5G接入认证模块中又分为单个UE认证和群组认证过程。

##### 2.2.1.3.2 设备认证组前端模块

这部分内容主要说明设备认证前端数据模型模块的设计。

4G接入认证、5G接入认证、自适应接入认证三个子模块的设计要满足以下2个目标。

（1）单个UE认证需在地图上动态展示相关步骤的链接情况：如开机、驻留基站、附着等操作，点击信息栏可以展示关键信息。

（2）群组接入认证需在地图上动态展示相关步骤的链接情况：如群主的出现、群组中的UE开机、接入认证等操作，点击信息栏可以展示关键信息。

基于上述目标，在4/5G子模块中设计了以下模块：单个UE接入认证、与群组接入认证。如下图所示：



图2-2设备认证前端模块架构

### 2.2.2 设备认证组安卓端

#### 2.2.2.1 需求概述

##### 2.2.2.1.1 功能要求

设备认证组安卓端依据3GPP标准、行业现状、国密算法标准为基础，实现了基于LTE、5G网络、自适应网络的设备认证方式，具体功能包括：

（1）EPS-AKA；

（2）5G-AKA；

（3）EAP-AKA’；

（4）自适应认证。

##### 2.2.2.1.2 性能要求

无

##### 2.2.2.1.3 输入输出要求

此模块的数据输入形式为手机终端输入。

设备认证时，有四种方式可以选择，用户随便选择一种设备认证方式进行设备认证。

此模块的数据输出形式为手机终端输出。

认证成功手机会有相应的界面跳转与弹框提醒。

#### 2.2.2.2 硬件结构

无

### 2.2.3 设备认证组后端

#### 2.2.3.1 需求概述

##### 2.2.3.1.1 功能要求

设备认证组后端依据3GPP标准、行业现状、国密算法标准为基础，以及当前针对密钥生成、密钥交换、安全接入认证、安全切换、安全漫游、群组接入等相关领域的最新研究进展为基础，重点实现以下具体功能包括：

（1）UE驻留基站；

（2）UE附着-包括EPS-AKA，5G-AKA，EAP-AKA’，群组接入认证与自适应接入认证；

（3）UE切换测量；

（4）UE切换认证-包括X2切换，S1切换，N2切换，Xn切换与群组切换认证。

#### 2.2.3.3 软件结构

依赖于redis6.1.5、openssl 1.1.1与自研密码库。

##### 2.2.3.3.1 设备认证组后端整体框架

这部分内容主要说明设备认证组的后端整体软件框架，分别从整体和各个模块的角度进行描述。

设备认证后端主要分为5个部分

（1）基站功能模块

（2）移动性管理功能模块

（3）认证管理功能模块

（4）统一认证数据管理模块

（5）前端统一控制接口

其中，（1）-（4）之间都采用采用socket的通信形式，协议为UDP协议，端口号均可通过修改配置文件进行自动更新；（5）通过守护进程的方式，可以实现对四个功能模块的启动与管理，并且开放端口65531与基站进行TCP通信。

整体软件框架图如下图2-3所示：



图2-3 设备认证后端框架图

##### 2.2.3.3.2 设备认证组后端模块

（1）工具类tools

|  |  |
| --- | --- |
| **文件名** | **功能** |
| XD\_TDYTH\_UNIFIED\_config.h | 存放配置文件 |
| XD\_TDYTH\_UNIFIED\_crypto.c/h | 存放协议中用到的加密算法 |
| XD\_TDYTH\_UNIFIED\_log.c/h | 格式化输出模块，print使用该头文件中定义的 |
| XD\_TDYTH\_UNIFIED\_tools.c/h | 协议流程中使用的工具：随机数，时间戳等 |
| XD\_TDYTH\_UNIFIED\_udp.c/h udp | 通信相关函数 |
| XD\_TDYTH\_UNIFIED\_BROADCAST.h | 存放关于基站广播与群组广播的常用函数 |
| XD\_TDYTH\_UNIFIED\_cJson.h JSON | 存放关于json操作相关函数 |
| XD\_TDYTH\_UNIFIED\_redis\_util.c | 存放关于redis操作的常用函数 |

（2）结构体structs

|  |  |
| --- | --- |
| 文件名 | 备注 |
| XD\_TDYTH\_UNIFED\_common.h | 存放长度等宏定义声明和常用头文件引用，包括45G通用 |
| XD\_TDYTH\_UNIFED\_4G\_common.h | 存放长度等宏定义声明和常用头文件引用，仅包括4G特有 |
| XD\_TDYTH\_UNIFED\_5G\_common.h | 存放长度等宏定义声明和常用头文件引用，仅包括5G特有 |
| XD\_TDYTH\_UNIFED\_4G\_structs.h | 存放4G所有协议步骤的结构体 |
| XD\_TDYTH\_UNIFED\_5G\_structs.h | 存放5G认证协议步骤的结构体 |
| XD\_TDYTH\_UNIFED\_5G\_EAP\_structs.h | 存放5G-EAP认证协议步骤的结构体 |
| XD\_TDYTH\_UNIFED\_5G\_GROUP\_structs.h | 存放5G群组协议步骤的结构体 |
| XD\_TDYTH\_UNIFED\_5G\_SWITCH\_structs.h | 存放5G切换协议步骤的结构体 |

（3）功能定义类

（每个角色单独使用一个.c文件编写，文件中包含main函数，在cmake中定义要求每个角色的源文件生成一个可执行程序。）

|  |  |
| --- | --- |
| **文件名** | **备注** |
| XD\_TDYTH\_UNIFIEDPLATFORM\_UE.c/h | 用户/群成员 |
| XD\_TDYTH\_UNIFIEDPLATFORM\_NB.c/h | 基站，包括4G eNB与5G gNB |
| XD\_TDYTH\_UNIFIEDPLATFORM\_AMFF.c/h | AMF，包括4G的MME功能与5G的AMF功能 |
| XD\_TDYTH\_UNIFIEDPLATFORM\_AUSF.c/h | AUSF，包括4G的AUC功能与5G的AUSF功能 |
| XD\_TDYTH\_UNIFIEDPLATFORM\_UDM.c/h | UDM ，包括4G的HSS功能与5G的UDM功能 |
| XD\_TDYTH\_UNIFIEDPLATFORM\_GROUP\_UEL.c/h | 群主 |

实体功能详细描述

* UE

1）UE 向基站发送自己加密后的用户的身份信息 SUCI或者已有5G-GUTI，请求接入网络。

2）UE 收到SEAF发送的认证请求后，通过提取和计算AUTN中的MAC，计算XMAC，比较 XMAC 和MAC是否相等，同时检验序列号SQN是否在正常的范围内、检查AMF格式是否正确、并且检查ngKSI是否使用过。如果认证通过，则计算RES与KSEAF，并将 RES传输给SEAF。在EAP下还可以根据附件A.3推导出CK’和IK’。



图2-4 UE侧认证向量计算过程

3）每隔一段时间上传测量报告。成群阶段只需要发送自己的GUTI给群主即可。

4）根据NCC以及本地存储先和来判断并计算新的会话密钥。成群阶段则根据随机数计算新的会话密钥。

* 群主

1）认证开始时，群主向群成员广播群组接入认证通知。

2）群主设置定时器，将一定时间内收到的所有群成员认证请求聚合，计算聚合消息认证码并发送给基站。

3）向群成员广播来自基站的群组认证响应。

4）群主收到群成员认证确认信息后计算，并且将RESG发送给基站。

* NB

1）转发来自群主的群组接入认证请求和接入认证确认。

2）转发来自SEAF的群组认证响应。

3）基站广播功能

* AMF/MME

1）提供SNID用以标识附着请求消息。

2）接收或，计算，提供安全上下文相关的ngKSI，并转发部分消息。

3）对认证成功消息RES\*做验证，生成密钥和，分配新的5G-GUTI给终端。

1）接收切换消息，更新NCC的值，并计算相关切换中间密钥。

2）若是N2或者群组切换，则要根据源基站发送的信息确定目标基站，并生成中间密钥。

* AUSF/AUC

1）转发认证请求。

2）存储以及认证响应，如果是5G-AKA或者群组认证则要计算新的认证向量，EAP框架下只需要转发消息即可。

3）验证终端发送的认证响应消息RES。

* UDM

以5G-AKA认证为例进行详述：

UDM收到消息后，首先验证SNID的合法性。然后UDM计算，利用IK验证SUCI中mac的有效性，利用EK解密获得SUPI，根据SUPI选择接入认证方式。若为5G-AKA的方法，UDM在其数据库中搜索与SUPI对应的主密钥K，然后按照如下操作生成5GHE AV。最后，UDM将5G HE AV 以及SUPI发送给AUSF；



图2-5 认证中心认证向量生成过程

具体包含以下流程：

①UDM生成一个新的SQN和一个不可挑战的随机数RAND（利用f0算法生成随机数RAND）（SQN参考3GPP 33.102 Annex C3.1执行）

②计算消息认证码；5G中AMF的separation bit必须设置为1

③计算期望响应

④计算加密密钥

⑤计算完整性密钥

⑥计算匿名密钥

⑦生成认证令牌；

⑧计算

⑨计算，取低位128位作为

⑩认证向量AV 的生成：计算。

（4）配置类

|  |  |
| --- | --- |
| **文件名** | **功能** |
| CMakeLists.txt | 定义了多个实体的可执行程序编译规则 |
| test.sh | 用于一次性打开协议所有实体可执行程序（终端平铺形式） |
| config.json | 以json格式保存的系统配置文件 |

##### 2.2.3.3.2 通用协议流程处理函数设计

（1）命名格式：协议流程处理函数命名由协议步骤开头，后使用下划线分割写清楚协议类型(全大写)，子类型(全大写 AUTH/REAUTH/SWITCH)，备注。

（2）参数：函数的参数列表固定为4个参数，依次为待处理数据、待处理数据长度、保存发送数据的缓冲区、生成的发送数据长度。 默认接收数据只为上一步的数据包体，包头已被去掉(用于判断数据包类别)。发送数据为完整的发送数据包(包含包头包尾)。

（3）返回值函数返回值为0时该步骤执行成功，为负值时该步骤执行失败（返回的负数需要有相应的错误原因宏定义）

示例：

int step5\_5G\_AUTH\_UDM(unsigned char \*recvBuf, unsigned int recvLen, unsigned char \*sendBuf, unsigned int \*sendLen);

int step11\_5G\_GROUP\_AUTH\_UE(unsigned char \*recvBuf, unsigned int recvLen, unsigned char \*sendBuf, unsigned int \*sendLen);

##### 2.2.3.3.2 通用协议流数据包接收与发送流程设计

（1）数据包识别：用于判断数据包是否属于某种协议

（2）数据包子类别分类：用于判断数据包用途（认证/切换）

（3）数据包步骤分类：用于判断数据包步骤

（4）调用具体的步骤处理函数

（5）根据函数返回值(步骤运行结果)发送给相应的实体

## 2.3 用户认证

### 2.3.1 用户认证组安卓端

#### 2.3.1.1 需求概述

##### 2.3.1.1.1 功能要求

具体功能包括：

（1）用户注册；

（2）密码认证；

（3）验证码认证；

（4）totp认证；

（5）密码与验证码认证；

（6）密码与totp认证；

（7）验证码与totp认证。

##### 2.3.1.1.2 性能要求

无

##### 2.3.1.1.3 输入输出要求

此模块的数据输入形式为手机终端输入。

用户认证时，有6种方式可以选择，用户随便选择一种用户认证方式进行认证。填写相关的认证信息，如密码登录填写用户名与密码。

此模块的数据输出形式为手机终端输出。

认证成功手机会有相应的界面跳转与弹框提醒。

#### 2.3.1.2 硬件结构

无

#### 2.3.1.3 软件结构

##### 2.3.1.3.1 设备认证组安卓端整体框架

用户认证组分为两个子模块进行设计：用户注册与用户认证。

注册需要填写用户名、手机号、密码与邮箱。然后将数据封装为json格式发往<https://cloud.gorio.top:16443/registering/IndividualRegistration>。然后根据接收到的json来判断是否注册成功。

用户认证又分为密码认证、验证码认证、totp认证、密码与验证码认证、totp与密码认证、totp与验证码认证。

### 2.3.2 用户认证组后端

#### 2.3.2.1 需求概述

##### 2.3.2.1.1 功能要求

用户认证模块负责完成用户身份注册以及和服务器端的双向身份认证和密钥协商功能，主要分为中间件、调度、认证服务器三个子模块，基于TCP套接字接口和国密算法实现了用户登录信息的安全传递和密码、验证码和TOTP等认证因子按需组合的实体身份认证。

中间件模块是负责客户端侧身份认证和安全传输等功能的TCP套接字程序。

调度模块是负责中间件到服务器传输功能的TCP套接字程序。

认证服务器模块负责实体身份认证、密钥协商以及数据库信息查询和更新功能的TCP套接字程序。

##### 2.3.2.1.2 性能要求

用户认证模块的具体性能指标包括：

（1）5G云雾混构环境下海量实体认证系统支持10万用户并发下认证响应≤1s；

（2）高速实体认证系统认证处理时间≤500ms。

##### 2.3.2.1.3 输入输出要求

此模块的输入输出数据均为TCP套接字数据流，其格式要求和具体内容见第三节。

#### 2.3.2.2 硬件结构

要求CPU I78代以上，内存都为32GB，Ubuntu 18.04.5 LTS。

#### 2.3.2.3 软件结构

##### 2.3.2.3.1 用户认证组后端整体框架

这部分内容主要说明用户认证组的整体软件框架，分别从整体和各个模块的角度进行描述。

用户认证组主要分为3个部分

（1）中间件子模块

（2）调度子模块

（3）认证服务器子模块

其中，中间件、调度和认证服务器之间都采用采用socket的通信形式，协议为TCP/IP协议，端口号分别为：中间件对客户端开放TCP 26020:2204端口，调度对中间件开放TCP 26019:3309端口，调度对认证服务器开放TCP 8888端口。

整体软件框架图如下2-6所示：



图2-6 整体软件框架图

其后的各小节将分别对此三个子模块进行较详细的描述。

##### 2.3.2.3.2 用户认证组后端模块

1、用户认证组中间件模块

这部分内容主要说明用户认证组中间件模块数据模型模块的设计。

用户认证组中间件模块设计要满足以下几个目标。

（1）监听客户端发来的认证和业务请求，从与客户端的连接获取数据，进行数据的解析与封装，数据的解析与封装包括加解密、签名验签等。

（2）主动与认证服务器侧建立连接，向认证服务器请求用户的token等信息，与调度建立连接进行数据传输。

（3）接收来自调度的认证响应，获取数据，并进行数据的解析与封装。

基于上述目标，设计了以下子模块：事件循环模块（Epoll）、IO模块、逻辑控制模块、业务逻辑模块与缓存模块。如图2-7所示：



图2-7 用户认证中间件模块架构

2、用户认证组调度模块

这部分内容主要说明用户认证组调度模块数据模型模块的设计。

用户认证组调度模块设计要满足以下几个目标。

（1）监听中间件发来的认证和业务请求，从连接获取数据，进行数据的解析与封装，与认证服务器建立连接进行数据传输。

（2）监听认证服务器发来的认证和业务请求，从连接获取数据，进行数据的解析与封装，与中间件建立连接进行数据传输。

基于上述目标，子模块设计参照中间件模块。

3、用户认证组认证服务器模块

这部分内容主要说明用户认证组认证服务器数据模型模块的设计。

用户认证组认证服务器模块设计要满足以下几个目标。

（1）监听调度发来的认证和业务请求，获取数据，进行数据的解析与封装。

（2）数据的解析与封装包括加解密、签名验签等。

（3）与调度建立连接进行数据传输。

基于上述目标，子模块设计参照中间件模块。

## 2.4 生物认证

### 2.4.1 生物认证组安卓端

#### 2.4.1.1 需求概述

##### 2.4.1.1.1 功能要求

具体功能如下：

（1）生物注册，包括身高体重、人脸、声纹；

（2）未加密的声纹认证；

（3）软生物加密声纹认证；

（4）未加密的人脸认证；

（5）软生物加密人脸认证。

##### 2.4.1.1.2 性能要求

无

##### 2.4.1.1.3 输入输出要求

此模块的数据输入形式为手机终端输入。

生物认证时，有2种方式可以选择，用户随便选择一种生物认证方式进行认证。填写相关的认证信息，如未加密人脸登录需要拍照然后点击登录按钮。

此模块的数据输出形式为手机终端输出。

认证成功手机会有相应的界面跳转与弹框提醒。

#### 2.4.1.2 硬件结构

无

#### 2.4.1.3 软件结构

##### 2.4.1.3.1 生物认证组安卓端整体框架

生物认证组分为两个子模块进行设计：软生物信息注册、生物认证。

注册需要填写用户名、身高体重、声纹与人脸照片，然后将数据封装为json格式发往<https://cloud.gorio.top:16443/fog/bioRegister>。并根据接收到的json格式判断注册是否成功。

生物认证又分为未加密声纹认证、未加密人脸认证、软生物加密声纹认证、软生物加密人脸认证。

### 2.4.2 生物认证组后端

#### 2.4.2.1 需求概述

##### 2.4.2.1.1 功能要求

功能要求为基于软生物特征的支持2种以上生物特征的身份鉴别及认证方法，支持活体检测技术。具体功能包括：

（1）用户信息注册；

（2）软生物特征（不）加密的人脸识别；

（3）软生物特征（不）加密的声纹识别；

（4）人脸活体检测。

##### 2.4.2.1.2 性能要求

无

##### 2.4.2.1.3 输入输出要求

（软）生物认证模块的数据流动形式为json形式。

#### 2.4.2.2 硬件结构

无

#### 2.4.2.3 软件结构

##### 2.4.2.3.1 生物认证组后端整体框架

这部分内容主要说明的整体软件框架，分别从整体和各个模块的角度进行描述。

（1）软件架构采用c/s架构；

（2）FCC、Cloud、AUC、LDM均为服务器端，有自己的ThreadingTCPServer类，是socketserver框架中的多线程TCP服务器类；

（3）UE为客户端，发起注册或认证请求。

##### 2.4.2.3.2 （软）生物认证模块

这部分内容主要说明（软）生物认证数据模型模块的设计。

（软）生物认证模块的设计要满足以下几个目标：

（1）5G云雾混构环境下个体生物特征的隐私保护和快速鉴权；

（2）确保生物特征模板数据存储与外包安全；

（3）支持人脸生物特征活体检测技术。

基于上述目标，在（软）生物认证模块中设计了以下子模块：用户终端子模块、雾计算节点子模块、统一认证云子模块、认证中心子模块及活体检测子模块。如下图所示：



图2-8（软）生物认证模块架构

# 三、模块核心数据结构说明

描述模块使用的核心数据结构设计说明。

## 3.1 数据结构设计

用户认证模块核心数据结构为结构体，数据交互使用json数据格式。

（软）生物认证模块核心数据结构为字典，数据交互使用json数据格式，在python中由字典转为json。字典以键值对组成，在字典中填入待传输的数据。如：data\_obj = {'to': 'user', 'msg': '20','step':'step-x','from':account,'code':203, ……}

## 3.2 数据格式设计

1、设备认证数据报文格式定义

1）数据域首部格式



2）数据报文格式



## 3.3通用数据结构及变量

### 3.3.1 宏定义

1、设备认证模块宏定义

|  |  |  |
| --- | --- | --- |
| **宏定义名** | **宏定义值** | **备注** |
| D\_XD\_TDYTH\_UNIFIED\_REGISTER | 0x01 | 注册流程 |
| D\_XD\_TDYTH\_UNIFIED\_CELLSELECTION | 0x02 | 小区选择流程 |
| D\_XD\_TDYTH\_UNIFIED\_AUTH | 0x03 | 认证流程 |
| D\_XD\_TDYTH\_UNIFIED\_GROUP | 0x04 | 群组流程 |
| D\_XD\_TDYTH\_UNIFIED\_TAU | 0x05 | TAU流程 |
| D\_XD\_TDYTH\_UNIFIED\_SWITCH | 0x06 | 切换流程 |
| D\_XD\_TDYTH\_UNIFIED\_IMS | 0x07 | IMS流程 |
| D\_XD\_TDYTH\_UNIFIED\_WXZW | 0x08 | 卫星组网流程 |
| D\_XD\_TDYTH\_UNIFIED\_5G\_REAUTH | 0x09 | 再次认证流程 |

2、用户认证模块宏定义

|  |  |  |
| --- | --- | --- |
| **宏定义名** | **宏定义值** | **备注** |
| ID\_LEN | 16 | 发送方和接收方ID长度 |
| SERVER\_ID\_LEN | 20 | 认证服务器ID |
| RANDOM\_NUMBER\_LEN | 16 | 随机数长度 |
| AUTHENTICATION\_CIPHER\_LEN | 32 | 认证加密长度 |
| TIME\_KEY\_LEN | 8 | TOTP长度 |
| MAC\_LEN | 32 | MAC长度 |

### 3.3.2 结构体

1、设备认证模块

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyFirstUEToGNB** | |
| **描述：** | **5G接入认证第1步UE到GNB数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucAUTHTAG | 用户标识符 |
|  | aucAUTHPKX | 用户公钥X |
|  | aucAUTHMSGC | 用户密文C |
|  | aucAUTHMac | 用户消息认证码 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodySecondGNBToAMF** | |
| **描述：** | **5G接入认证第2步GNB到SEAF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucAUTHTAG | 用户标识符 |
|  | aucAUTHPKX | 用户公钥X |
|  | aucAUTHMSGC | 用户密文C |
|  | aucAUTHMac | 用户消息认证码 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyThirdAMFToAUSF** | |
| **描述：** | **5G接入认证第3步SEAF到AUSF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucAuthID | 用户标识符 |
|  | aucAuthPkeyX | 用户公钥X |
|  | aucAuthMsgC | 用户密文C |
|  | aucAUTHMac | 用户消息认证码 |
|  | aucSNID | SN |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyFourthAUSFToUDM** | |
| **描述：** | **5G接入认证第4步AUSF到UDM数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucAUTHTAG | 用户标识符 |
|  | aucAUTHPKX | 用户公钥X |
|  | aucSNID | SN |
|  | aucAUTHMSGC | 用户密文C |
|  | aucAUTHMac | 用户消息认证码 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyFifthUDMToAUSF** | |
| **描述：** | **5G接入认证第5步UDM到AUSF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucHEAV | UDM生成HE |
|  | aucSUPI | 用户身份请求标识 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodySixthAUSFToSEAF** | |
| **描述：** | **5G接入认证第6步AUSF到SEAF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucAV | 5G认证向量 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodySeventhAMFToGNB** | |
| **描述：** | **5G接入认证第7步SEAF到GNB数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucRAND | 随机数 |
|  | aucAUTN | 认证数据 |
|  | aucNGKSI | 密钥集标识符 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyEighthGNBToUE** | |
| **描述：** | **5G接入认证第8步GNB到UE数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucRAND | 随机数 |
|  | aucAUTN | 认证数据 |
|  | aucNGKSI | 密钥集标识符 |
|  | aucTerminalId | 终端ID |

|  |  |  |  |
| --- | --- | --- | --- |
| **原型：** | | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyNinthUEToGNB** | |
| **描述：** | | **5G接入认证第9步UE到GNB数据包** | |
|  | aucTimeStamp | | 时戳 |
|  | ucIdNumber | | 标识位 |
|  | aucDstId | | 目的ID |
|  | aucSrcId | | 源ID |
|  | iDataLen | | 数据长度 |
|  | aucRES | | 认证响应RES\* |
|  | aucTerminalId | | 终端ID |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyNinthUEToGNBMACErr** | | | |
| **描述：** | **5G接入认证第9步UE到GNB到SEAF** | | **MAC验证失败数据包** | |
|  | | aucTimeStamp | 时戳 |  |
|  | | ucIdNumber | 标识位 |  |
|  | | aucDstId | 目的ID |  |
|  | | aucSrcId | 源ID |  |
|  | | iDataLen | 数据长度 |  |
|  | | ucCause | MAC验证失败cause值 | MAC failure |
|  | | aucTerminalId | 终端ID |  |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyNinthUEToGNBSQNErr** | |
| **描述：** | **5G接入认证第9步UE到GNB到SEAF** | **SQN验证失败数据包** |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | ucCause | SQN验证失败cause值 |
|  | ucAUTS | AUTS=SQNMS⊕AK||MAC-S |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5G\_AuBodyNinthUEToGNBAMFErr** | |
| **描述：** | **5G接入认证第9步UE到GNB到SEAF** | **AMF验证失败数据包** |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | ucCause | AMF验证失败cause值 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5G\_AuBodyNinthUEToGNBNGKSIErr** | |
| **描述：** | **5G接入认证第9步UE到GNB到SEAF** | **ngKSI使用过失败数据包** |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | ucCause | ngKSI使用过的失败cause值 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyTenthGNBToAMF** | |
| **描述：** | **5G接入认证第10步GNB到SEAF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucRES | 认证响应RES\* |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyEleventhAMFToAUSF** | |
| **描述：** | **5G接入认证第11步SEAF到AUSF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucRES | 认证响应RES\* |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyEleventhAMFToUEErr** | |
| **描述：** | **5G接入认证第11步SEAF认证失败到UE的数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | ucCause | 认证拒绝消息 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyTwelfthAUSFToAMF** | |
| **描述：** | **5G接入认证第12步AUSF到SEAF数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucSUPI | 用户身份请求标识 |
|  | aucTerminalId | 终端ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyTwelfthAUSFToAMFErr** | |
| **描述：** | **5G接入认证第12步AUSF到SEAF认证失败数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | ucCause | 认证拒绝消息 |
|  | aucTerminalId | 终端ID |

|  |  |  |  |
| --- | --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyThirteenthAMFToGNB** | | |
| **描述：** | **5G接入认证第13步SEAF到GNB数据包** | | |
|  | aucTimeStamp | | 时戳 |
|  | ucIdNumber | | 标识位 |
|  | aucDstId | | 目的ID |
|  | aucSrcId | | 源ID |
|  | iDataLen | | 数据长度 |
|  | aucGUTI | | 5G-GUTI |
|  | aucKENBI | | 基础密钥KeNB-i |
|  | aucTerminalId | 终端ID | |

|  |  |  |
| --- | --- | --- |
| **原型：** | **St\_XD\_TDYTH\_UNIFIED\_5GAKA\_AuBodyFourteenthGNBToUE** | |
| **描述：** | **5G接入认证第14步GNB到UE数据包** | |
|  | aucTimeStamp | 时戳 |
|  | ucIdNumber | 标识位 |
|  | aucDstId | 目的ID |
|  | aucSrcId | 源ID |
|  | iDataLen | 数据长度 |
|  | aucGUTI | 5G-GUTI |
|  | aucTerminalId | 终端ID |

2、用户认证模块

|  |  |  |
| --- | --- | --- |
| **原型：** | **HeaderControllerToServer/HeaderServerToController** | |
| **描述：** | **调度服务器到后台服务器数据包头部** | |
| 参数： | acceptId | 连接ID |
|  | record | 线程池结构体指针 |
|  | version | 协议版本号 |
|  | secureMode | 安全码 |
|  | reservedField | 保留字段 |
|  | pktSerialNum | 报文序号 |
|  | pktLen | 报文长度 |
|  | modulerCode | 模块码 |
|  | subType | 子类码,协议类型 |
|  | step | 步骤码 |
|  | senderId | 发送方ID |
|  | receiverId | 接收方ID |
|  | globalId | 全局ID |
|  | recId |  |
|  | parentReId | 父ID |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAuBodySecondMidToSer** | |
| **描述：** | **密码认证第二步中间件到服务器body数据包** | |
| 参数： | userIdType | 账号类型 |
|  | userIdLen | 账号长度 |
|  | userId | 账号 |
|  | timeStamp | 时间戳 |
|  | encryMethodCode | 加密算法编码 |
|  | encryptRandom | 加密随机数1 |
|  | hashMethodCode | HASH函数编码 |
|  | userAuth | 用户认证信息 |
|  | tosend | 发送cjson格式 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAuBodyThirdSerToMid** | |
| **描述：** | **密码认证第三步服务器到中间件body数据包** | |
| 参数： | userIdType | 账号类型 |
|  | userIdLen | 账号长度 |
|  | userId | 账号 |
|  | authResult | 认证结果 |
|  | authServerId | 认证服务器ID |
|  | encryMethodCode | 加密算法编码 |
|  | encryptRandom2 | 加密随机数2 |
|  | hashMethodCode | HASH算法编码 |
|  | serverAuth | 服务器认证信息 |
|  | tosend | 发送cjson格式 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAuBodyThirdSerToMid** | |
| **描述：** | **密码认证第四步中间件到服务器body数据包** | |
| 参数： | userIdType | 账号类型 |
|  | userIdLen | 账号长度 |
|  | userId | 账号 |
|  | ack | 认证确认消息 |
|  | code | MAC函数编码 |
|  | mac | MAC |
|  | tosend | 发送cjson格式 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAuBodyFifthSerToMid** | |
| **描述：** | **密码认证第五步服务器到中间件body数据包** | |
| 参数： | userIdType | 账号类型 |
|  | userIdLen | 账号长度 |
|  | userId | 账号 |
|  | idNum | 用户身份唯一识别符 |
|  | encryMethodCode | 加密模块代码 |
|  | encryMsgLen | 加密信息长度 |
|  | encryMsg | 加密信息 |
|  | ucUserNameLen | 用户名认证长度 |
|  | ucUserName | 用户名 |
|  | code | MAC函数编码 |
|  | mac | MAC |
|  | tosend | 发送cjson格式 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **TkAuBodySecondMidToSer** | |
| **描述：** | **TOTP认证第二步中间件到服务器body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | ullTimeStamp1 | 时间戳1 |
|  | uiHashId | HASH算法编码 |
|  | uiSymEncryptId | 加密算法编码 |
|  | aucEncryptRandom1 | 加密随机数1 |
|  | aucUserAuth | 用户认证信息 |
|  | aucTimeKey | TOTP |

|  |  |  |
| --- | --- | --- |
| **原型：** | **TkAuBodyThirdSerToMid** | |
| **描述：** | **TOTP认证第三步服务器到中间件body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | pucServerId | 服务器账号 |
|  | ullTimeStamp2 | 时间戳2 |
|  | uiHashId | HASH算法编码 |
|  | uiSymEncryptId | 加密算法编码 |
|  | aucEncryptR2R3 | 加密随机数2||3 |
|  | aucServerAuth | 服务器认证信息 |
|  | ucAuthResult | 认证结果 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **TkAuBodyForthMidToSer** | |
| **描述：** | **TOTP认证第四步中间件到服务器body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | pucServerId | 服务器账号 |
|  | ullTimeStamp4 | 时间戳4 |
|  | uiHashId | HASH算法编码 |
|  | uiSymEncryptId | 加密算法编码 |
|  | aucEncryptTimeStamp4 | 加密时间戳4 |
|  | uiMacType | MAC类型 |
|  | aucMAC | MAC |

|  |  |  |
| --- | --- | --- |
| **原型：** | **TkAuBodyFifthSerToMid** | |
| **描述：** | **TOTP认证第五步服务器到中间件body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | pucServerId | 服务器账号 |
|  | ullTimeStamp5 | 时间戳5 |
|  | ucAuthResult | 认证结果 |
|  | auctoken | token |
|  | uiMacType | MAC类型 |
|  | idNum | 用户身份唯一识别符 |
|  | encryMethodCode | 加密模块代码 |
|  | encryMsgLen | 加密信息长度 |
|  | encryMsg | 加密信息 |
|  | ucUserNameLen | 用户名认证长度 |
|  | ucUserName | 用户名 |
|  | aucMAC | MAC |
|  | tosend | 发送cjson格式 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAndMsAuBodySecondMidToSer** | |
| **描述：** | **密码与验证码结合第二步中间件到服务器body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | ullTimeStamp1 | 时间戳1 |
|  | M3 | 加密信息 |

|  |  |  |
| --- | --- | --- |
| **原型：** | **PwAndMsAuBodyThirdSerToMid** | |
| **描述：** | **密码与验证码结合第三步到服务器中间件body数据包** | |
| 参数： | ucUserIdType | 账号类型 |
|  | ucUserIdLen | 账号长度 |
|  | pucUserId | 账号 |
|  | ullTimeStamp2 | 时间戳2 |
|  | aucToken | token |
|  | aucTokenLen | token长度 |
|  | M4 | 加密信息 |
|  | tosend | 发送cjson格式 |
|  | ucAuthResult | 认证结果 |