ICS 33.030
CCS L70

T/CAICI

中 国 通 信 企 业 协 会 团 体 标 准

T/CAICI XXXX—XXXX

5G 消息业务增强能力规范—统一认证能力要求

5G Messaging Services Enhancement Capability Specification – Unified Authentication Capability Requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国通信企业协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信企业协会团体标准管理委员会提出并归口。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：中国移动通信集团有限公司、中国信息通信研究院、中国通信企业协会增值服务专业委员会、中国电信集团有限公司、中国联合网络通信集团有限公司

本文件主要起草人：

本文件为中国通信企业协会首次发布。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到……[条]……与……[内容] ……相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利持有人姓名：……

地址：……

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

5G 消息业务增强能力规范—统一认证能力要求

1 范围

本标准规定了5G消息业务增强能力中的统一认证能力要求，包括统一认证能力的功能要求、系统架构、技术流程等。供运营商、网络设备商、终端厂商使用，为其在中国境内建设、使用5G消息统一认证能力时提供技术依据。

基于GBA鉴权机制的5G消息统一认证能力，未来可进一步演进形成通用服务和标准，应用于除5G消息业务外的其它业务服务流程。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 3989-2021 5G 消息总体技术要求

3 术语和定义

下列术语、定义和缩略语适用于本标准：

3.1 术语、定义

词语	解释
5G消息	短信业务的升级，面向用户提供增强的消息服务，能够为用户提供文本、图片、音频、视频、位置、联系人（vCard）等媒体内容的发送和接收。
Chatbot（聊天机器人）	通过会话交互形式为个人用户提供服务的应用形态。
第三方应用系统（Chatbot）	以Chatbot形态向个人用户提供服务的客户，包括行业客户、梦网客户、公共应急通知服务等。
点与应用间消息	5G消息业务中个人用户与Chatbot应用之间的交互消息，包括A2P（Application to Person）消息和P2A（Person to Application）消息。

3.2 缩略语

缩略语	英文全称	中文含义
GBA	Generic Bootstrapping Architecture	通用引导架构
USIM	Universal Subscriber Identity Module	用户全球识别卡
BSF	Bootstrapping Server Function	引导服务功能
BIR	Bootstrapping-Info Request	自举信息请求
BIA	Bootstrapping-Info Answer	自举信息应答消息

4 统一认证能力概述

4.1 统一认证能力开放需求

YD/T 3989-2021《5G消息 总体技术要求》中已经规定了HTTP类业务采用GBA对终端用户进行认证，但只有5G消息系统功能（如5G消息终端获取配置、chatbot搜索、文件上传下载等）能够使用GBA认证能力。为了向Chatbot应用提供统一的用户身份认证能力，本标准将制定统一认证能力开放技术要求，将GBA认证能力进行封装，并开放给Chatbot使用。Chatbot使用该能力后，用户点击该Chatbot发送的5G消息中包含该Chatbot自有系统的链接时，从5G消息界面跳转到该Chatbot的网页，跳转后，用户无需输入其在该Chatbot系统上的用户名和密码，即可快捷登录到该Chatbot的网页上。

4.2 统一认证能力开放实现方案

4.2.1 概述

统一认证能力开放需要终端侧设置GBA认证模块，网络侧设置GBA认证能力开放平台,终端与平台相互配合，完成对用户身份进行认证后登录第三方应用网页。

在第三方应用获取用户身份信息（本标准中主要指手机号码，也可根据业务需要扩展支持其他的用户信息）前，用户需要授权该第三方应用获得其身份信息，授权只对当次请求有效。终端侧实现该授权及认证流程有2种不同的实现方式：

方案一：GBA认证能力开放平台提供网页版授权页面，下文中简称为“内置浏览器方案”。

方案二：终端GBA认证模块提供native版授权页面，下文中简称为“终端Native方案”。

4.2.2 方案一：内置浏览器方案

当用户点击5G消息中包含第三方应用外链的按钮或内容时，终端应调起5G消息应用中的内置浏览器，内置浏览器与网络侧GBA认证能力开放平台交互，获取授权页面，用户确认向该Chatbot授权获取其身份信息后,内置浏览器应与终端GBA认证模块交互,终端GBA认证模块再与GBA认证能力开放平台交互，对第三方应用和用户的身份进行认证鉴权，用户无需输入其在该Chatbot系统上的用户名和密码，即可快捷登录到第三方应用网页。

4.2.3 方案二：终端 Native 方案

当用户点击5G消息中包含第三方应用外链的按钮或内容时，终端应调用GBA认证模块获取native版授权页面，用户确认向该Chatbot授权获取其身份信息后，终端GBA认证模块与GBA认证能力开放平台交互，对第三方应用和用户的身份进行认证鉴权，用户无需输入用户名和密码，即可快捷登录到第三方应用网页。

5 统一认证能力功能要求

5.1 终端获取统一认证能力服务器地址

5G消息的配置数据应扩展一个统一认证能力服务器地址的配置参数，终端应通过配置流程获取统一认证能力服务器的地址。

统一认证能力服务器地址的配置参数应设置在MESSAGING参数下，参数名称为“Single sign-on”，配置数据形如：

```
<characteristic type="MESSAGING">
    ……
    <characteristic type="Single sign-on">
       <parm name="SSOURI" value="https://xxx.com/ssoserver"/>
    </characteristic>
    ……
</characteristic>
```

5.2 第三方应用申请开通统一认证能力

第三方应用要获得统一认证能力，应在统一认证能力的归属运营商进行开通。运营商应支持在线开通方式。如果第三方应用的主体为企业，在线提交的企业信息应至少包括企业名称、企业法人信息、企业营业执照信息、企业联系人信息（包括手机号码）、申请使用认证能力的Chatbot名称。如果第三方应用的主体为个人，在线提交的个人信息应至少包括姓名、个人身份证信息、个人手机号信息、个人证件照信息、申请使用认证能力的Chatbot名称。

开通成功后，第三方应用可选择资费模式（包括免费模式和收费模式）和套餐包，支付后，即可接入GBA认证能力开放平台，使用GBA认证能力开放平台提供的统一认证能力。

运营商可结合业务需求，简化统一认证能力的开通流程。如在商户申请开通Chatbot流程中，增加同时开通统一认证能力的可选项。如果Chatbot选择了同时开通统一认证能力，可继续添加具体使用统一认证能力的外部链接，具体功能可由运营商自行设计。

5.3 用户免密登录第三方应用网页

用户通过5G消息界面打开Chatbot提供的非5G消息系统内的链接（下文中可简称为外部链接、或者外链）时，如果该Chatbot开通了统一认证能力，Chatbot在获得用户身份之前，应向用户展示授权询问页面，用户点击“确认”或“同意”后，该Chatbot方可获得用户的身份信息，并应依据用户的身份信息为该用户展示登录后的页面。

5.4 第三方应用提供的链接格式

第三方应用可在文本消息、卡片消息中携带链接，用户点击链接后可免密登录到第三方应用的网页。链接格式可采用如下2种方式：

1) 通过 GBA 开放平台跳转到第三方应用网页，链接中应携带 GBA 开放平台地址、第三方应用的 appid、网页链接、运营商标识，链接格式形如：
https://www.cmccgba.com?appid=xx&url=xxx&operator=xxx;

2) 直接跳转到第三方应用网页，链接中应携带第三方应用的网页链接、appid、运营商标识、GBA 认证标识，链接格式形如：https://www.abc.com?appid=xx&operator=xxx&gba=0。

注：上述 2 种格式的链接既适用于终端内置浏览器方案，又适用于终端 Native 方案。

对第一种链接中各项要素的说明如表 1 所示。对第二种链接中各项要素的说明如表 2 所示。

表 1 链接方式 1 参数说明

参数名	必选	描述	示例
GBA 开放平台地址	是	GBA 开放平台提供的 web url，终端通过该地址获取授权确认页面，由提供 GBA 能力开放的运营商提供	www.cmccgba.com
appid	是	第三方应用的唯一凭证，由 GBA 开放平台分配，为一个字符串	——
第三方应用的网页链接	是	第三方应用提供的 web url，终端通过该地址访问第三方应用的页面，由第三方应用提供，主域名应在其开通 Chatbot 时在运营商登记过。	www.abc.com
operator	是	运营商标识，采用一位数字表示：	——

		中国移动：1 中国电信：2 中国联通：3 中国广电：4	

表 2　链接方式 2 参数说明

参数名	必选	描述	示例
第三方应用的网页链接	是	第三方应用提供的 web url，终端通过该地址访问第三方应用的页面，由第三方应用提供，主域名应在其开通 Chatbot 时在运营商登记过。	www.abc.com
operator	是	运营商标识，采用一位数字表示： 中国移动：1 中国电信：2 中国联通：3 中国广电：4	——
appid	是	第三方应用的唯一凭证，由 GBA 开放平台分配，为一个字符串	——
gba	是	GBA 认证标识，采用一位数字表示： 需要 GBA 认证：0 不需要 GBA 认证：1 默认值为 1	——

6　统一认证能力系统架构

6.1　系统逻辑架构图

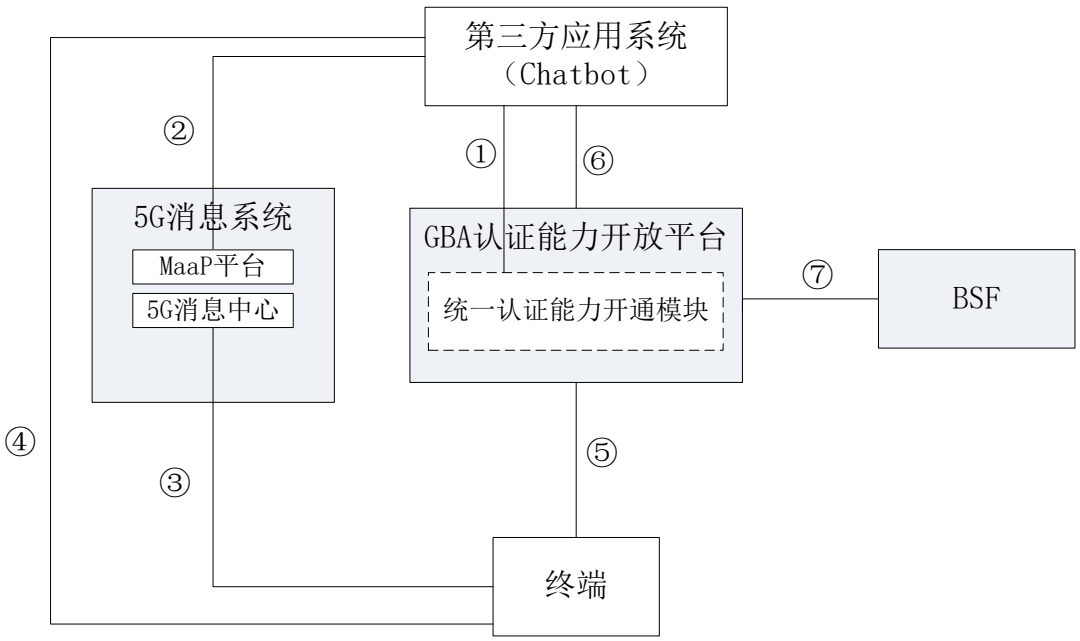

图1　统一认证系统架构及接口

如图1所示，统一认证能力开通模块，可在GBA认证能力开放平台内部实现，也可以作为独立子模块，在5G消息系统中集成，以进一步满足业务的定制化需求。

在5G消息系统中集成时，5G消息系统需要代Chatbot去GBA认证能力开放平台去开通认证能力，再把开通结果转给Chatbot。本标准中按GBA认证能力开放平台实现开通进行规定，5G消息系统集成开通的方式由运营商根据运营需求自行实现，不在本标准规定范围内。

6.2　网元功能

统一认证涉及到的网元及网元功能如下。

5G消息系统：包含MaaP平台、5G消息中心、统一认证能力开通逻辑模块（可选），接收第三方应用系统向用户发送的Chatbot消息，并转发给终端；负责为第三方应用系统开通统一认证能力（可选）。

GBA认证能力开放平台：负责为第三方应用系统开通统一认证能力，通过GBA认证流程获取终端用户的身份信息，开放给第三方应用系统。

BSF：与GBA认证能力开放平台交互，向其提供终端用户身份信息。

第三方应用系统：通过5G消息系统向终端用户下发Chatbot消息；通过调用GBA认证能力，向用户提供登录后的网页内容。

6.3　接口描述

统一认证能力涉及到的接口如图 1 中接口①~⑧所示。

接口①：第三方应用系统与统一认证能力开通逻辑模块间的接口，完成统一认证能力开通相关的 Chatbot 信息提交以及开通结果通知等。

接口②：第三方应用系统与 5G 消息系统中 MaaP 平台间的接口，完成 Chatbot 消息交互，采用 HTTP/HTTPS 协议通信。

接口③：5G 消息系统中 5G 消息中心与终端间的接口，完成 Chatbot 消息交互，采用 SIP 协议通信。

接口④：第三方应用系统与终端间的接口，采用 HTTP/HTTPS 协议，用于终端访问第三方应用系统的网页。

接口⑤：GBA 认证能力平台与终端间的接口，用于终端用户向 Chatbot 授权其获取用户身份信息，终端 GBA 模块获取用户身份信息等。

接口⑥：GBA 认证能力开放平台与第三方应用系统间的接口，用于第三方应用系统获取用户授权询问页面、用凭证换取用户信息等。

接口⑦：GBA 认证能力开放平台与 BSF 间的接口，用于 GBA 认证能力开放平台从 BSF 获取用户身份信息。

7　统一认证技术流程

7.1　第三方应用开通统一认证能力流程

第三方应用到GBA认证能力开放平台申请开通统一认证能力，流程如图2所示。

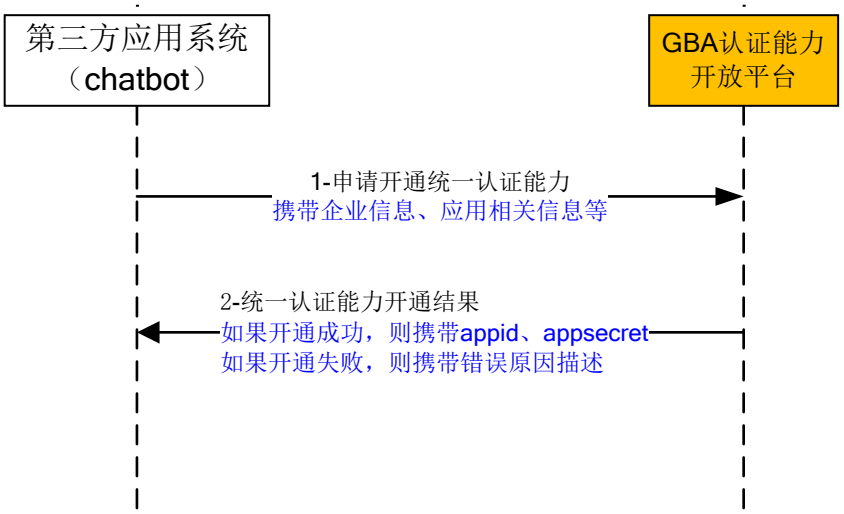

图2　应用开通统一认证能力流程

流程介绍如下：

1、第三方应用系统申请开通统一认证能力，携带第三方应用的企业名称、管理者身份、Chatbot 名称等信息。

2、GBA 认证能力开放平台为第三方应用系统开通统一认证能力，并向其返回开通结果，如果开通成功，则携带 appid、appsecret；如果开通失败，则携带开通失败的错误原因描述。运营商可根据 5G 消息业务运营需求，appid 和 appsecret 复用 Chatbot 注册时为其分配的账号及校验参数信息。

7.2　用户授权确认流程

7.2.1　内置浏览器方案下的用户授权确认流程

用户通过5G消息应用中的链接访问第三方应用提供的网页时，第三方应用如果要获得用户身份信息，需要取得用户授权，用户确认授权后，5G消息终端与GBA认证能力开放平台、第三方服务平台交互，获得登录后的第三方应用网页。用户获取授权页面流程如图3所示，用户确认授权流程如图4所示。

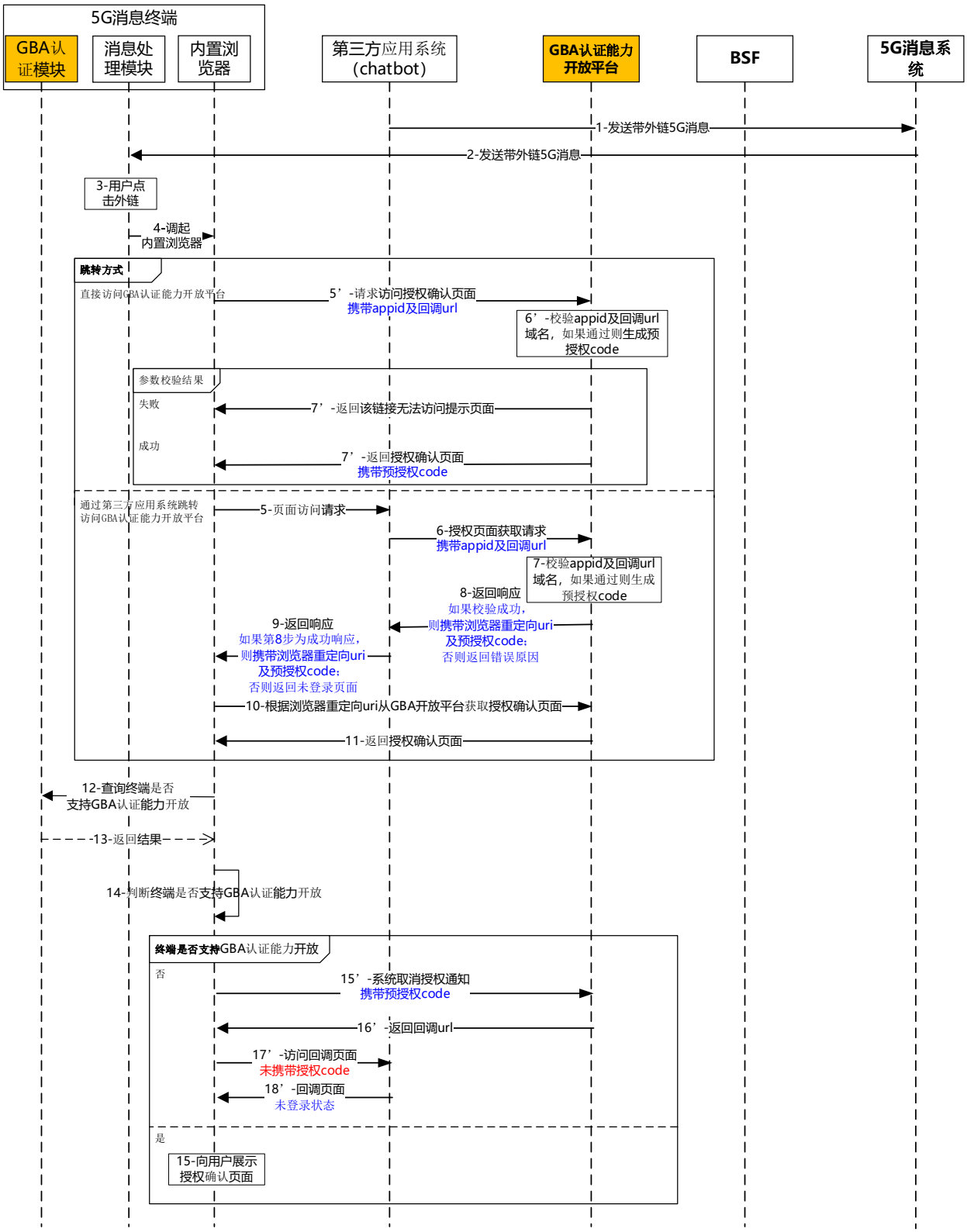

图3　用户获取授权页面流程

流程介绍如下：

1~4、用户点击 5G 消息中的外链，调起 5G 消息终端内置浏览器访问外链。

用户授权确认页面的触发方式可以通过 2 种机制实现，可由运营商根据应用类型、业务策略等灵活选择采用何种机制。

——机制 1：直接访问 GBA 认证能力开放平台。5’~7’：外链直接指向 GBA 认证能力开放平台，外链中携带预先由 GBA 认证能力开放平台为 Chatbot 分配的 appid 和 Chatbot 的回调 URL 参数。GBA 认证能力开放平台对 appid 和回调 URL 进行校验，如果校验通过，则返回授权确认页面，携带预授权 code；如果校验不通过，则返回校验不通过的结果及不通过的原因提示页面。

——机制 2：通过第三方应用系统跳转访问 GBA 认证能力开放平台。5~9：第三方应用系统向 GBA 认证能力开放平台请求获得授权询问页面，请求中携带预先由 GBA 认证能力开放平台为其分配的 appid 和第三方应用平台的回调 URL。GBA 认证能力开放平台对 appid 和回调 URL 进行校验，如果校验通过，则返回授权确认页面 URL 和预授权 code，第三方应用系统将其转发至 5G 消息终端内置浏览器；如果校验不通过，则返回校验不通过的结果及不通过的原因，第三方应用系统按照其自有逻辑处理后续流程。

10~11、终端内置浏览器根据授权确认页面 URL 访问 GBA 认证能力开放平台，GBA 认证能力开放平台返回授权确认页面。

12~13、页面调用 GBA 认证模块查询终端是否支持 GBA 认证能力开放。

14、页面对查询结果进行判断，如果调用查询报错或者返回错误码则认定不支持，code 为 0 则认定支持，具体调用方式参见第 9.1 节。

15’~18’、对于不支持 GBA 认证能力开放的终端，页面向 GBA 认证能力开放平台通知用户取消授权的结果，，具体调用方式参见第 9.2 节。GBA 认证能力开放平台记录该事件，向终端返回第三方应用系统的回调 URL。页面自动跳转，继续访问未经认证的第三方应用页面。

15、如果终端支持 GBA 认证能力开放，终端内置浏览器展示授权确认页面，询问用户是否同意该 chatbot 获取用户身份信息（手机号码）。

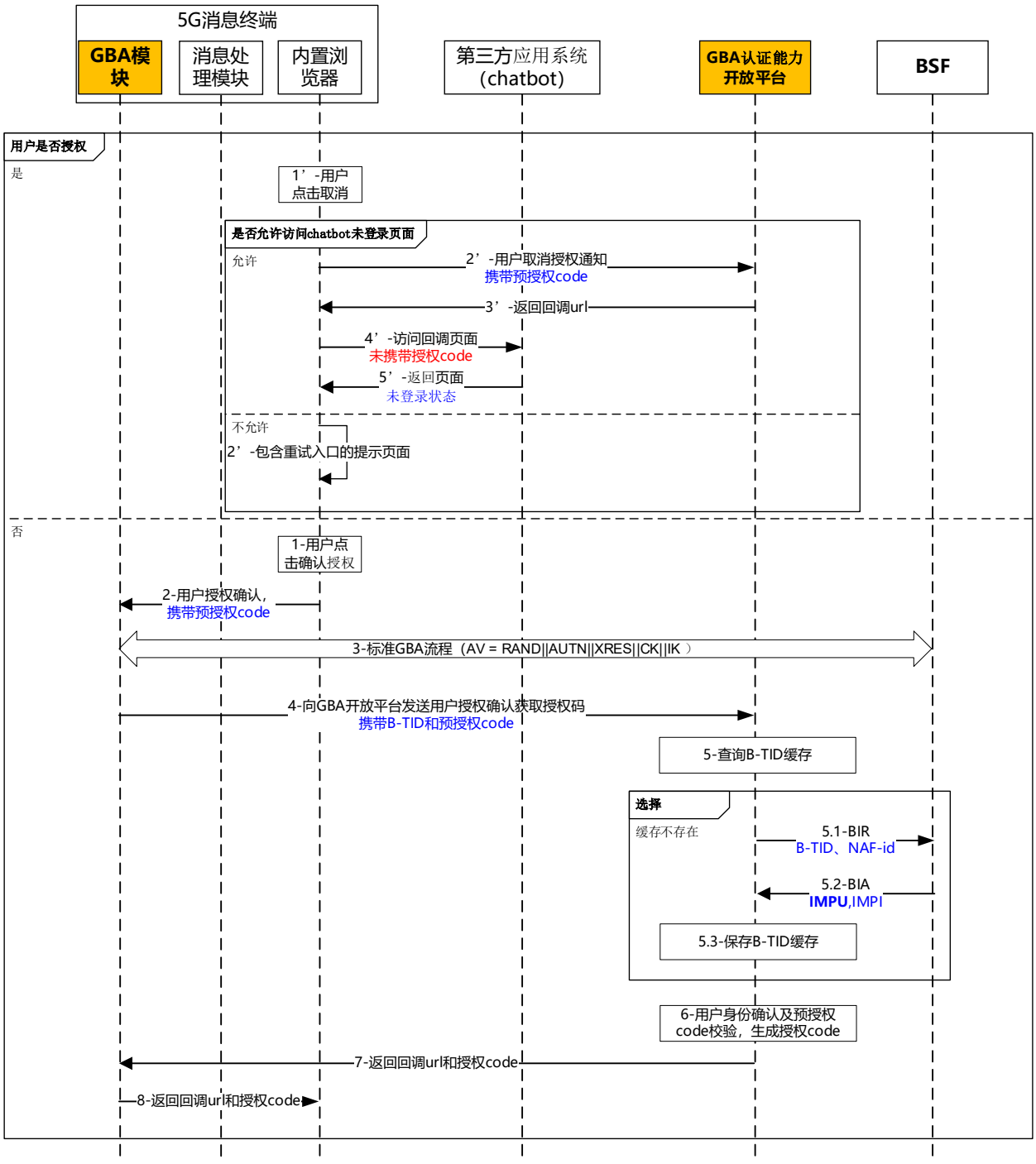

图4　用户授权确认流程

流程介绍如下：

1’~5’、用户点击取消授权。如果 Chatbot 设置为允许访问 Chatbot 未登录页面，GBA 认证能力开放平台获得用户取消授权的结果后，记录该事件，并向用户返回第三方应用系统的回调 URL，用户继续访问未经认证的第三方应用页面；如果 Chatbot 设置为不允许访问 Chatbot 未登录页面，则跳转到一个提示页面，页面中包含重试入口，用户可点击后再次选择是否确认授权。

1~3、用户点击授权确认。 内置浏览器向终端 GBA 认证模块通知用户授权确认的结果，携带预授权

code，具体调用方式参见第 9.1 节。如果 GBA 认证模块没有有效的 B-TID，则向 BSF 发起标准 GBA 认证流程；如果 GBA 认证模块有有效的 B-TID，则使用该有效的 B-TID 继续执行第 4 步。

4~6、终端 GBA 认证模块向 GBA 认证能力开放平台发送用户授权确认，携带 B-TID 和预授权 code。GBA 认证能力开放平台如果没有 B-TID 的缓存信息或缓存有效期已过期，则 GBA 认证能力开放平台与 BSF 执行 GBA 认证的后续流程，获得用户的 IMPU 和 IMPI，并保存缓存信息；GBA 认证能力开放平台如果有 B-TID 的缓存信息且在有效期范围内，则使用缓存信息。GBA 认证能力开放平台确认用户身份并校验预授权 code，校验通过后生成授权 code。

7~8、GBA 认证能力开放平台向终端 GBA 认证模块返回第三方应用的回调 URL 和授权 code，具体调用方式参见第 9.2 节。GBA 认证模块向内置浏览器返回第三方应用的回调 URL 和授权 code。

7.2.2 终端 Native 方案下的用户授权确认流程

用户通过5G消息应用中的链接访问第三方应用提供的网页时，第三方应用如果要获得用户身份信息，需要取得用户授权，用户确认授权后，5G消息终端与GBA认证能力开放平台交互，获得登录后的第三方应用网页。native终端用户授权确认如图5所示。

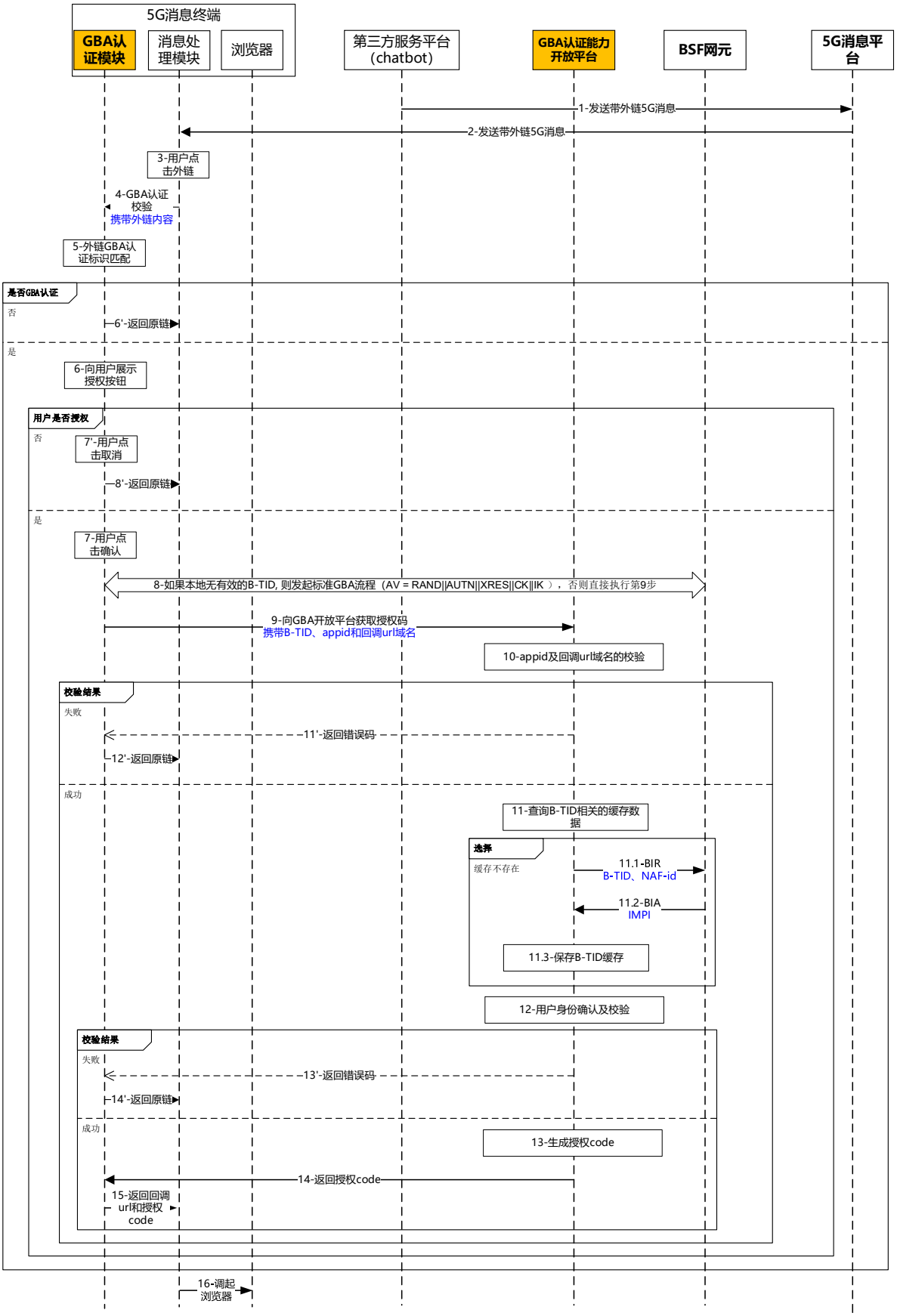
5G消息终端
GBA认证模块
消息处理模块
浏览器
第三方服务平台(chatbot)
GBA认证能力开放平台
BSF网元
5G消息平台
1-发送带外链5G消息
2-发送带外链5G消息
3-用户点击外链
4-GBA认证校验
携带外链内容
5-外链GBA认证标识匹配
是否GBA认证
否
6'-返回原链
是
6-向用户展示授权按钮
用户是否授权
否
7'-用户点击取消
8'-返回原链
是
7-用户点击确认
8-如果本地无有效的B-TID, 则发起标准GBA流程（AV = RAND||AUTN||XRES||CK||IK），否则直接执行第9步
9-向GBA开放平台获取授权码
携带B-TID、appid和回调url域名
10-appid及回调url域名的校验
校验结果
失败
11'-返回错误码
12'-返回原链
成功
11-查询B-TID相关的缓存数据
选择
缓存不存在
11.1-BIR
B-TID、NAF-id
11.2-BIA
IMPI
11.3-保存B-TID缓存
12-用户身份确认及校验
校验结果
失败
13'-返回错误码
14'-返回原链
成功
13-生成授权code
14-返回授权code
15-返回回调url和授权code
16-调起浏览器

图5 native终端用户授权确认流程

流程介绍如下：

1~4、Chatbot 向用户发送携带外链的 5G 消息，用户点击 5G 消息中的外链，终端侧的消息处理模块调起 GBA 认证模块，GBA 认证模块执行是否需要进行 GBA 认证的校验。

5、终端GBA认证模块根据外链的格式及参数进行校验，判断该外链是否需要进行GBA认证。如果需要，则提取出appid、回调url、回调url域名、权限范围（可选，如果链接中携带，则提取该参数值）。

6’、对于不需要进行GBA认证的链接，终端GBA认证模块直接返回原链给终端消息处理模块。

6、对于需要进行GBA认证校验的链接，GBA认证模块弹出授权页面。

7’~8’、用户点击取消授权。终端GBA认证模块直接返回原链给终端消息护理模块。

7~8、用户点击授权确认，如果GBA认证模块没有有效的B-TID，则向BSF发起标准GBA认证流程；如果GBA认证模块有有效的B-TID，则使用该有效的B-TID继续执行第9步。

9、终端 GBA 认证模块向 GBA 认证能力开放平台发送用户授权确认，携带 B-TID、appid 和回调 URL 域名。

10、GBA 认证能力开放平台对 appid 有效性进行校验，同时校验 appid 在 GBA 开放平台配置的域名跟回调 url 的域名是否一致。

11’~12’、对于 appid 无效或者域名配置不匹配的情况，GBA 认证能力开放平台返回错误码，终端 GBA 认证模块直接返回原链给终端消息处理模块。

11、对于 appid 有效且域名配置匹配的，GBA 认证能力开放平台检查本地缓存是否有该 B-TID 对应的用户信息，如果没有 B-TID 的缓存信息或缓存有效期已过期，则 GBA 认证能力开放平台与 BSF 执行 GBA 认证的后续流程，获得用户的 IMPU 和 IMPI，并保存缓存信息；GBA 认证能力开放平台如果有该 B-TID 对应的缓存用户信息且在有效期范围内，则使用该缓存的用户信息。

12、GBA 认证能力开放平台根据 BSF 返回的 BIA 消息中的用户信息来确认用户身份并进行标准 GBA 校验（根据用户的 USS 信息，验证 UE 传送过来的身份信息 IMPU 是否一致；利用 B-TID（用户名）和 Ks_NAF（口令）进行 HTTP Digest 计算 response，并与请求消息头域 Authorization 中的 response 值比对是否一致）。

13’~14’、对于身份信息不符或者 response 不匹配，GBA 认证能力开放平台返回错误码，终端 GBA 认证模块直接返回原链给终端消息处理模块。

13~15、对于身份信息符合且 response 匹配的，GBA 认证能力开放平台生成授权 code 并返回给终端 GBA 认证模块，GBA 认证模块返回回调 url 和授权 code 给终端消息处理模块。

16、消息处理模块调起 5G 消息终端浏览器访问 GBA 认证模块返回的链接（链接中携带授权 code）。

7.3 用户授权后免密登录第三方应用网页流程

用户通过 5G 消息中的链接访问第三方应用提供的网页时，需要在授权询问页面进行用户授权。用户确认授权后，终端侧 GBA 认证模块与网络侧 GBA 认证能力开放平台交互，获取授权 code，并将授权 code 和第三方应用系统的回调 URL 返回给内置浏览器（流程参见第 7.2 节）。使用该授权 code，即可免密登录到第三方应用的网页。免密登录第三方应用网页的流程如图 5 所示。

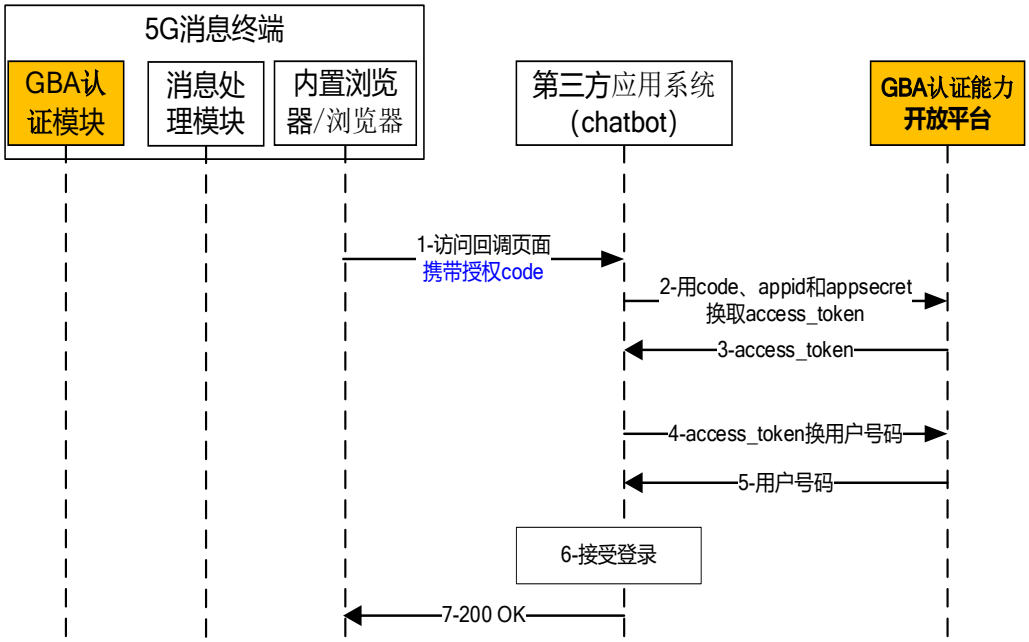

图5　免密登录第三方应用网页的流程

流程介绍如下：

1、内置浏览器携带授权 code 访问第三方应用系统。

2~3、第三方应用系统通过授权 code 和其之前申请的 appid、appsecret 去 GBA 认证能力开放平台获取 access_token.

4~5、第三方应用系统通过 access_token 去 GBA 认证能力开放平台换取用户号码。

6~7、第三方应用系统为用户登录后向用户返回登录后的网页内容。

8　统一认证相关平台侧接口

8.1　第三方应用系统与统一认证能力开通模块间的接口（接口 1）

本接口完成统一认证能力开通相关的Chatbot信息提交以及开通结果通知等。具体实现方法遵循归属运营商的相关规范。

8.2　第三方应用系统与 MaaP 平台间的接口（接口 2）

本接口完成Chatbot消息交互，采用HTTP/HTTPS协议通信。具体实现方法遵循归属运营商的相关规范。

8.3　5G 消息中心与终端间的接口（接口 3）

本接口完成Chatbot消息交互，采用SIP协议通信。具体实现方法遵循归属运营商的相关规范。

8.4　第三方应用系统与终端间的接口（接口 4）

终端访问第三方应用系统的接口链接，遵循标准的HTTP协议。

8.5　GBA 认证能力开放平台与终端间的接口（接口 5：内置浏览器方案）

8.5.1　鉴权消息接口

8.5.1.1　接口说明

终端向 GBA 认证能力开放平台发起 HTTP 请求，终端应使用 GBA 方式（3GPP TS 33.220）进行鉴权，应按照 3GPP TS 24.109 规定在 HTTP POST 头中添加 User-Agent 参数。

请求方法：GET

请求地址：/gbaop/v1/auth/code

8.5.1.2 HTTP 请求头信息

参数名	必填	描述	示例
User-Agent	Y	终端类型	NAF1 Application Agent Release-6 3gpp-gba
X-3GPP-Intended-Identity	Y	请求账号	sip:+8613911111111@operator.com

8.5.1.3 HTTP 请求参数

http 请求 params 的参数：

无

http 请求 body 的参数：

无

8.5.1.4 HTTP 响应参数

http 响应头的参数：

参数名	必填	可选值	示例
WWW-Authenticate	Y	认证参数	Digest realm="3GPP-bootstrapping@ftcontentserver.rcs.mnc00.mcc460.pub.3gppnetwork.org ", nonce="6629fae49393a05397450978507c4ef1", algorithm=AKA_v1_SHA256, qop="auth,auth-int", opaque="5ccc069c403ebaf9f0171e9517f30e41"

http 响应 body 参数：

无

8.5.1.5 http 响应码

返回码	说明
401	未认证

8.5.1.6 接口示例

```
GET /gbaop/v1/auth/code HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
X-3GPP-Intended-Identity: sip:+8613911111111@operator.com
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 401 Unauthorized
```

Server: Apache/1.3.22 (Unix) mod_perl/1.27
Date: Thu, 24 July 2019 10:50:35 GMT
WWW-Authenticate: Digest realm="3GPP-bootstrapping@ ftcontentserver.rcs.mnc00.mcc460.pub.3gppnetwork.org ", nonce="6629fae49393a05397450978507c4ef1", algorithm=AKA_v1_SHA256, qop="auth,auth-int", opaque="5ccc069c403ebaf9f0171e9517f30e41"

8.5.2 授权 code 获取接口

8.5.2.1 接口说明

5G 消息终端 GBA 模块通过本接口向 GBA 认证能力开放平台申请授权 code，采用 HTTPS 协议。

请求方法：GET

请求地址：/gbaop/v1/auth/code

8.5.2.2 请求头信息

参数名	必填	描述	示例
Authorization	Y	鉴权头参数 GBA 方式鉴权：Digest realm="...", nonce="...", ...	Digest username="(B-TID)", realm="3GPP-bootstrapping@naf.home1.net", nonce="a6332ffd2d234==", uri="/", qop=auth-int, nc=00000001, cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=SHA-256
X-3GPP-Intended-Identity	Y	用户地址	+8613844445678

8.5.2.3 请求参数

http 请求 params 的参数：

序号	字段	数据类型	可选属性	描述
1	pre_auth_code	varchar(64)	M	预授权 code，且必须与 8.7.1 步骤中的该参数值保持一致。

http 请求 body 的参数：无

8.5.2.4 响应参数

http 响应头的参数：

参数名	必填	描述	示例
content-type	Y	请求内容类型，此处必填 application/json	application/json

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data：

序号	字段	数据类型	可选属性	描述
1	redirect_uri	varchar(64)	M	重定向地址，包含 auth_code 和 state 参数。 auth_code：授权 code，必选项。该码的有效期应该很短，通常设为 10 分钟，终端只能使用该码一次，否则应被 GBA 开放平台拒绝。该码与终端手机号码和重定向 URI，是一一对应关系。 state： 如果 8.7.1 中终端的请求中包含该参数，GBA 认证能力开放平台的回应也应包含该参数，例如： https://client.example.com/cb?code=SplxlOBeZQQYbYS6WxSbIA&state=xyz

8.5.2.5 http 响应码

返回码	说明
302	认证成功，重定向
404	认证不存在
410	认证过期

8.5.2.6 接口示例

```
GET /gbaop/v1/auth/code?pre_auth_code=kdflsflsdkf HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
X-3GPP-Intended-Identity: +8613844445678
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@naf.home1.net", nonce="a6332ffd2d234==",
uri="/", qop=auth-int, nc=00000001, cnonce="6629fae49393a05397450978507c4ef1",
response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=SHA-256
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 200 OK
```

```
Access-Control-Allow-Origin: *
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 02:03:33 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "data": {
        "redirect_uri": "  https://client.example.com/cb?auth_code=SplxlOBeZQQYbYS6WxSbIA&state=xyz "
    },
    "message": "OK"
}
```

8.5.3 取消授权接口

8.5.3.1 接口说明

终端(5G 消息内置浏览器)通过本接口向 GBA 认证能力开放平台申请取消授权，包括用户取消授权（即用户不同意授权该 Chatbot 查看其身份信息）和由于终端不支持 GBA 认证能力开放而导致的系统取消授权 2 个场景。

调用方式：H5 ->GBA 认证能力开放平台

请求方法：GET

请求地址：/gbaop/v1/auth/cancel

8.5.3.2 请求头信息

参数名	必填	描述	示例
User-Agent	Y	终端类型,内置浏览器特殊约定的类型	XXXX

8.5.3.3 请求参数

http 请求 params 的参数：

序号	字段	数据类型	可选属性	描述
1	pre_auth_code	varchar(64)	M	预授权 code，且应与 8.7.1 节中的该参数值保持一致。

http 请求 body 的参数：

无

8.5.3.4 响应参数

http 响应头的参数：

参数名	必填	描述	示例
Location	Y	重定向地址，回调 url 加 state 参数，不包含 auth_code ，只包含了 state 参数. 回调 url：8.7.1 节中终端的请求参数 state： 如果 8.7.1 节终端的请求中包含这个参数，GBA 认证能力开放平台的应答也应包含这个参数。	https://client.example.com/cb?state=xyz

http 响应 body 参数：

无

8.5.3.5 http 响应码

返回码	说明
302	认证成功，重定向
404	认证不存在
410	认证过期

8.5.3.6 接口示例

```
POST /gbaop/v1/auth/cancel?pre_auth_code=kdflsflsdkf HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 302 Found
Location: https://client.example.com/cb?state=xyz
```

8.6 GBA 认证能力开放平台与终端间的接口（接口 5：终端 Native 方案）

8.6.1 接口说明

5G 消息 Native 终端 GBA 模块通过本接口向 GBA 认证能力开放平台申请授权 code，采用 HTTPS 协议。

请求方法：GET

请求地址：/gbaop/v1/auth/code

8.6.2 请求头信息

参数名	必填	描述	示例
Authorization	Y	鉴权头参数	Digest username="(B-TID)", realm="3GPP-bootstrapping@naf.home1.net", nonce="a6332ffd2d234==", uri="/",

参数名	必填	描述	示例
		GBA 方式鉴权：Digest realm="...", nonce="...", ...	qop=auth-int, nc=00000001, cnonce="6629fae49393a05397450978507c4ef1", response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=SHA-256
X-3GPP-Intended-Identity	Y	用户地址	+8613844445678

8.6.3 请求参数

http 请求 params 的参数：

序号	字段	数据类型	可选属性	描述
1	appid	varchar(64)	M	应用的 ID，第三方服务平台的唯一标识
2	domain	varchar(64)	M	回调 url 域名
3	scope	varchar(64)	O	权限范围

http 请求 body 的参数：无

8.6.4 响应参数

http 响应头的参数：

参数名	必填	描述	示例
content-type	Y	请求内容类型，此处必填 application/json	application/json

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data：

序号	字段	数据类型	可选属性	描述
1	auth_code	varchar(64)	M	授权码。该码的有效期应该很短，通常设为 10 分钟，客户端只能使用该码一次，否则会被授权服务器拒绝。

8.6.5 http 响应码

返回码	说明
302	认证成功，重定向
404	认证不存在
410	认证过期

8.6.6 接口示例

```
GET /gbaop/v1/auth/code?appid=XX&domain=XX&scope=XX HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
X-3GPP-Intended-Identity: +8613844445678
Authorization: Digest username="(B-TID)", realm="3GPP-bootstrapping@naf.home1.net", nonce="a6332ffd2d234==",
uri="/", qop=auth-int, nc=00000001, cnonce="6629fae49393a05397450978507c4ef1",
response="6629fae49393a05397450978507c4ef1", opaque="5ccc069c403ebaf9f0171e9517f30e41", algorithm=SHA-256
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 02:03:33 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "data": {
        "auth_code": "XXXX"
    },
    "message": "OK"
}
```

8.7 第三方应用系统与 GBA 认证能力开放平台间的接口（接口 6）

8.7.1 授权确认页面获取接口（内置浏览器方案）

8.7.1.1 接口说明

终端(系统内置浏览器内)通过本接口向 GBA 认证能力开放平台申请授权确认页面 URL。

请求方法：GET

请求地址：/gbaop/v1/auth/authorizepage

8.7.1.2 请求头信息

参数名	必填	描述	示例
User-Agent	Y	终端类型,内置浏览器特殊约定的类型	XXXX

8.7.1.3 请求参数

http 请求 params 的参数：

序号	字段	数据类型	可选属性	描述
1	response_type	varchar(64)	M	授权类型，此处的值固定为"code"
2	appid	varchar(64)	M	应用的 ID，是该应用的唯一标识
3	redirect_uri	varchar(64)	M	重定向 URI
4	scope	varchar(64)	O	权限范围，默认取值为：telnum 运营商可根据实际情况扩展其他值，用于开放更多的权限类型，如用户位置等
5	state	varchar(256)	O	终端的当前状态，可以指定任意值，GBA 认证能力开放平台应原样返回这个值
6	cancel_redirect	bool	O	如果用户取消授权是否跳转 redirect_uri，取值可为： true:跳转； false：不跳转，转到包含重试的取消提示页面，默认为 false

http 请求 body 的参数：

无

8.7.1.4 响应参数

http 响应头的参数：

参数名	必填	描述	示例
content-type	Y	请求内容类型，此处必填 application/json	application/json

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码，具体请见 8 章节的全局响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data:

序号	字段	数据类型	可选属性	描述
1	auth_url	varchar(255)	M	授权确认页面 url，包含如下参数： pre_auth_code:预授权 code，用于获取授权 code 时使用 app_name:应用名称 cancel_redirect: 取消授权是否跳转 例如： https://client.example.com/gbaopv/index.html?pre_auth_code=SplxlOBeZQQYbYS6WxSbI&app_name=应用名称 &cancel_redirect=false

8.7.1.5 响应码

返回码	说明
0	获取成功
40002	参数不合法

8.7.1.6 接口示例

```
GET /gbaop/v1/authorizepage?response_type=code&appid=s6BhdRkqt3&state=xyz&redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
X-3GPP-Intended-Identity: sip:+8613911111111@operator.com
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 02:03:33 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "data": {
        "auth_url": "
https://client.example.com/gbaopv/index.html?pre_auth_code=SplxlOBeZQQYbYS6WxSbI&app_name%E8%B6%85%E7%BA%A7%E5%BA%94%E7%94%A8&cancel_redirect=false "
    },
    "message": "OK"
}
```

8.7.2 申请令牌接口

8.7.2.1 接口说明

第三方应用系统通过本接口向 GBA 认证能力开放平台申请令牌，采用 HTTPS 请求和应答的方式。申请到的令牌用于后续换取用户身份信息。

请求方法：POST

请求地址：/gbaop/v1/auth/token

8.7.2.2 请求头信息

参数名	必填	描述	示例
content-type	Y	请求内容类型，此处必填 application/json	application/json

8.7.2.3 请求参数

http 请求 params 的参数：

无

http 请求 body 的参数：

序号	字段	数据类型	可选属性	描述
1	grant_type	varchar(64)	M	授权模式，此处的值固定为"authorization_code"
2	auth_code	varchar(64)	M	授权 code ,即 8.5.2 节中获得的授权 code
3	appid	varchar(64)	M	应用的 ID，为应用的唯一标识
4	appsecret	varchar(64)	M	应用的 secret

8.7.2.4 响应参数

http 响应头的参数：

无

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码，具体请见 8 章节的全局响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data:

序号	字段	数据类型	可选属性	描述
1	access_token	varchar(64)	M	访问令牌,认证 token
2	token_type	varchar(64)	M	令牌类型，该值大小写不敏感，默认取值为：bearer
3	expires_in	int	M	过期时间，单位为秒。如果省略该参数，应以其他方式设置过期时间
4	refresh_token	varchar(64)	O	更新令牌，用于获取下一次的访问令牌
5	scope	varchar(256)	O	权限范围，如果与终端申请的范围一致，此项可省略

8.7.2.5 http 响应码

返回码	说明
200	响应OK

8.7.2.6 接口示例

```
POST /gbaop/v1/auth/token HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
Content-Type: application/json
Connection: Keep-Alive
Content-Length: 45

{
    "grant_type":"authorization_code",
    "auth_code":"dfdfsdf",
     "redirect_uri ":"https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb",
    "appid":"fhfghgfhgfh",
    "appsecret":"dfdfsdf"
}

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 02:03:33 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "data": {
        "access_token": "d2bbd4f22a0f9050e2fb17f2bdaa0bef",
        "token_type":"bearer",
        "expires_in":3600,
        "refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA",
```

```
                "scope":"telnum"
            },
            "message": "OK"
        }
```

8.7.3 刷新令牌接口

8.7.3.1 接口说明

第三方应用系统通过本接口向 GBA 认证能力开放平台刷新令牌，如果之前的 access_token 已经过期，更新为新的，如果没过期，仅仅更新有效期，采用 HTTPS 请求和应答的方式。申请到的令牌用于后续换取用户身份信息。

请求方法：POST

请求地址：/gbaop/v1/auth/refreshtoken

8.7.3.2 请求头信息

参数名	必填	描述	示例
content-type	Y	请求内容类型，此处必填 application/json	application/json

8.7.3.3 请求参数

http 请求 params 的参数：

无

http 请求 body 的参数：

序号	字段	数据类型	可选属性	描述
1	refresh_token	varchar(64)	M	更新令牌，用来获取下一次的访问令牌

8.7.3.4 响应参数

http 响应头的参数：

无

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码，具体请见 8 章节的全局响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data:

序号	字段	数据类型	可选属性	描述
1	access_token	varchar(64)	M	访问令牌,认证 token
2	token_type	varchar(64)	M	令牌类型，该值大小写不敏感，必选项，可以是 bearer 类型或 mac 类型
3	expires_in	int	M	过期时间，单位为秒。如果省略该参数，应以其他方式设置过期时间
4	refresh_token	varchar(64)	O	更新令牌，用来获取下一次的访问令牌
5	scope	varchar(256)	O	权限范围，如果与终端申请的范围一致，此项可省略

8.7.3.5 http 响应码

返回码	说明
200	响应OK

8.7.3.6 接口示例

```
POST /gbaop/v1/auth/refreshtoken HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
Content-Type: application/json
Connection: Keep-Alive
Content-Length: 45

{
    "refresh_token": "d2bbd4f22a0f9050e2fb17f2bdaa0bef"
}

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 02:03:33 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "data": {
        "access_token": "d2bbd4f22a0f9050e2fb17f2bdaa0bef",
        "token_type":"bearer",
        "expires_in":3600,
        "refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA",
       "scope":"telnum"
```

```
        },
        "message": "OK"
    }
```

8.7.4 查询用户身份信息接口

8.7.4.1 接口说明

第三方应用系统通过本接口向 GBA 认证能力开放平台查询用户的身份信息(手机号码),采用 HTTPS 协议。

调用方式：第三方应用系统->GBA 认证能力开放平台

请求方法：GET

请求地址： /gbaop/v1/auth/phonenum

8.7.4.2 请求头信息

参数名	描述	必填	可选值
content-type	请求内容类型	Y	application/json

8.7.4.3 请求参数

http 请求 params 的参数：

序号	字段	数据类型	可选属性	描述
1	access_token	varchar(64)	M	认证 token

http 请求 body 的参数：

无

8.7.4.4 响应参数

http 响应头的参数：

无

http 响应 body 参数：

序号	字段	数据类型	可选属性	描述
1	code	varchar(64)	M	响应码，具体请见 8 章节的全局响应码
2	message	varchar(64)	M	响应码说明
3	request_id	varchar(64)	C	请求 id
4	data	Object	O	响应数据

data:

序号	字段	数据类型	可选属性	描述
1	tel_number	varchar(64)	M	手机号码，经过 AES 加密 其加密过程为 AES(mobile,md516(appsecret))

8.7.4.5 http 响应码

返回码	说明
200	响应OK

8.7.4.6 接口示例

```
GET  /gbaop/v1/auth/phonenum?access_token=ACCESS_TOKEN HTTP/1.1

User-Agent: NAF1 Application Agent Release-6 3gpp-gba
Date: Thu, 08 Jan 2019 10:50:35 GMT
X-3GPP-Intended-Identity: sip:+8613911111111@operator.com
Connection: Keep-Alive
Content-Length: 0

HTTP/1.1 200 OK
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun, 08-Nov-2020 13:46:12 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Date: Mon, 09 Nov 2020 13:46:12 GMT
Keep-Alive: timeout=60
Connection: keep-alive

{
    "code": "0",
    "message": "成功",
    "requestId": null,
    "data": {
        "tel_number ":"Ag0s+dnXycKAAV44sTqj4w=="
    },
}
```

8.8 GBA 认证能力开放平台与 BSF 间的接口（接口 7）

GBA 认证能力开放平台通过本接口从 BSF 获取用户身份信息，具体接口遵循运营商关于 GBA 认证相关的规范。

8.9 全局响应码

本章各个接口中共享使用的全局响应码如表X所示。

表X

返回码	说明
-1	系统忙

0	受理成功
40001	授权失败
40002	凭证不合法
40003	该链接无法访问
40061	不合法的参数

9 统一认证相关终端侧接口

9.1 查询终端是否支持 GBA 认证能力开放

网页代码通过本接口中的调用函数查询终端是否支持 GBA 认证能力开放，终端通过结果回调函数向页面返回查询结果。

调用函数：

```
window.android.checkGbaAuthorization(
      version   // 选填，版本
);
```

结果回调函数：

```
function setCheckGbaAuthResult(code,des) {
// 查询终端是否支持 GBA 认证能力开放后会执行此函数，如支持，code 为 0 标识；其他则为失败，同时通过 des 查看错误描述。这里可以执行响应的逻辑。
}
```

9.2 获取授权码

网页代码通过本接口中的调用函数向 GBA 认证能力开放平台获取授权 code，GBA 认证能力开放平台通过结果回调函数向页面返回携带授权 code 的回调 url。

调用函数：

```
window.android.startGbaAuthorization (
      pre_auth_code    // 必填，预授权码
);
```

结果回调函数：

```
function setGbaAuthResult(code,des,url) {
// 获取授权码后会执行此函数，如成功，code 为 0 标识，同时通过 url 获取携带授权 code 的回调 url；其他则为失败，同时通过 des 查看错误描述。这里可以执行响应的逻辑。
}
```

10 统一认证相关接口安全要求

GBA 认证能力开放平台应支持采用数据加密与签名机制来保障其与第三方应用平台间交互数据的安全性。GBA 认证能力开放平台应支持第三方应用设置对称密钥和非对称密钥，第三方应用可先加密请求数据，再对加密后的密文进行签名，确保内容不被篡改。

GBA 认证能力开放平台应支持第三方应用设置 IP 白名单，启用后，只有通过白名单中的 IP 才能访问 GBA 认证能力开放平台。

在第三方应用平台向 GBA 认证能力开放平台申请令牌、刷新令牌、查询用户身份信息时，应支持第三方应用选择其采用的安全级别，包括是否启用对称加密、是否启用非对称加密、是否启用 IP 白名单等。