国际电信联盟
电信标准化部门

建议书

ITU-T X.1817 (09/2023)

X系列：数据网、开放系统通信和安全性

IMT-2020安全性

5G消息业务的安全要求

ITU-T X系列建议书

数据网、开放系统通信和安全性

公众数据网络	X.1-X.199
开放系统互连	X.200-X.299
网络间的互通	X.300-X.399
消息处理系统	X.400-X.499
目录	X.500-X.599
OSI组网和系统概貌	X.600-X.699
OSI管理	X.700-X.799
安全	X.800-X.849
OSI应用	X.850-X.899
开放式分布式处理	X.900-X.999
信息和网络安全	X.1000-X.1099
安全应用和服务 （1）	X.1100-X.1199
网络空间安全	X.1200-X.1299
安全的应用程序和服务 （2）	X.1300-X.1499
网络安全信息交换	X.1500-X.1599
云计算安全	X.1600-X.1699
量子通信	X.1700-X.1729
数据安全	X.1750-X.1799
IMT-2020安全性	**X.1800-X.1819**

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1817建议书

5G消息业务的安全要求

摘要

ITU-T X.1817建议书提出了5G消息业务的安全要求，其中包括5G消息业务的访问安全要求、管理安全要求和控制安全要求。

历史沿革*

版本	建议书	批准时间	研究组	唯一ID
1.0	ITU-T X.1817	2023-09-08	17	11.1002/1000/15524

关键词

5G消息业务、安全框架、安全要求。

* 欲查阅建议书，请在网络浏览器地址域键入URL https://handle.itu.int/，随后输入建议书的唯一识别码。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

页码

1 范围 1
2 参引 1
3 定义 1
3.1 他处定义的术语 1
3.2 本建议书定义的术语 1
4 缩略语和首字母缩写词 2
5 惯例 2
6 概述 3
6.1 5G消息业务 3
6.2 5G消息业务的安全要求架构 3
6.2 5G消息业务与4G/3G/5G/WLAN的安全要求之间的功能差异 4
7 5G消息业务接入的安全要求 4
7.1 用户卡补卡或换卡的安全要求 4
7.2 用户认证 4
7.3 消息接收安全 8
7.4 消息发送安全 8
7.5 消息访问安全 8
8 5G消息业务管理的安全要求 8
8.1 用户管理安全 8
8.2 密钥和证书管理 8
8.3 安全审计 9
8.4 软件管理安全 10
9 5G消息业务控制的安全要求 10
9.1 业务能力限制 10
9.2 主叫黑名单 10
9.3 被叫黑名单 10
参考文献 11

ITU-T X.1817建议书

5G消息业务的安全要求

1 范围

5G消息业务是短消息业务（SMS）的升级。它是基本电信业务之一，其中包括3GPP定义的短消息业务（SMS）和GSMA定义的富媒体通信业务（RCS）。需特别指出，它支持个人与个人之间或应用与个人之间的消息，其消息亦支持各种媒体（例如，长文本、图片、视频、音频、文件和位置等）。本建议书描述了可减轻5G消息业务的安全威胁和挑战的安全要求，并提供了5G消息业务的安全要求，其中包括5G消息业务的访问安全要求、管理安全要求和控制安全要求。本建议书还描述了5G消息业务和4G/3G/5G/WLAN等的安全要求之间的功能差异。

2 参引

下列ITU-T建议书和其他参引的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有建议书和其他参引均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参引的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ETSI TS 123 040] ETSI TS 123 040 v17.2.0（2022年），数字蜂窝电信系统（阶段2+）；通用移动通信系统（UMTS）；LTE；5G；短消息业务（SMS）的技术实现

[ETSI TS 124 229] ETSI TS 124 229（2017年），数字蜂窝电信系统（阶段2+）（GSM）；通用移动通信系统（UMTS）；LTE；基于会话发起协议（SIP）和会话描述协议（SDP）的IP多媒体呼叫控制协议；阶段3

[ETSI TS 129 109] ETSI TS 129 109（2018年），数字蜂窝电信系统（阶段2+）；通用移动通信系统（UMTS）；LTE；通用认证架构（GAA）；基于直径协议的Zh和Zn接口；阶段3

[ISO/IEC 11770-1] ISO/IEC 11770-1：2010年，信息技术 – 安全技术 – 密钥管理 – 第1部分：框架。

3 定义

3.1 他处定义的术语

本建议书使用了他处定义的以下术语：

3.1.1 聊天机器人（chatbot）[b-GSMA RCC.71]：一种提供给用户的、基于富媒体通信业务（RCS）的自动化业务，其输出以对话形式呈现。

3.2 本建议书定义的术语

本建议书定义了以下术语：

3.2.1 5G消息中心（5G message centre）：提供5G消息业务的服务器。

3.2.2 消息平台（message platform）：第三方应用连接5G消息中心的平台。

3.2.3 5G消息用户设备（5G message user equipment（UE））：其消息应用同时支持短消息业务（SMS）和富媒体通信业务（RCS）的5G用户设备（UE）。

3.2.4 5G消息业务（5G messaging service）：5G消息业务，其中包括短消息业务（SMS）和富媒体通信业务（RCS）。5G消息业务支持个人与个人之间或应用与个人之间的消息，其消息亦支持各种媒体（例如，长文本、图片、视频、音频、文件和位置等）。

4 缩略语和首字母缩写词

本建议书采用以下缩写词和首字母缩写词：

3GPP 第三代合作伙伴项目

A2P 应用对个人

AKA 认证和密钥协议

GBA 通用自举架构

GSMA 全球移动通信系统协会

HSS 家庭用户业务

HTTPS 超文本传输安全协议

IMS IP多媒体子系统

MO 移动发起

MT 移动终接

OTP 一次性密码

P2P 个人对个人

RCS 富媒体通信业务

SIM 用户识别模块

SIP 会话发起协议

SMS 短消息业务

UE 用户设备

UDM 统一数据管理

VoLTE 长期演进技术语音通话

WLAN 无线局域网

5 惯例

本建议书使用下列惯例：

关键词“须”表示一项必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“建议”表示一项建议的、并非需要绝对遵守的要求，因此，声称遵守本建议书并不需要存在本要求。

6 概述

6.1 5G消息业务

5G消息业务遵守GSMA富媒体通信业务（RCS）通用配置文件的要求，允许多媒体消息、群组聊天和消息平台等高级业务。5G消息业务基于终端的本地短消息业务（SMS）门户，允许用户发送和接收文本、图片、音频、视频、位置数据、联系人信息和其他媒体内容，其中包括以下业务功能：

- 个人对个人（P2P）消息

P2P消息是指个人用户之间发送的消息，支持以下媒体内容：文本（包括表情符号）、图片、音频、视频、位置、联系人（vCard）和文档。

- 群发消息

群发消息是指单个用户同时向多个其他个人用户发送的消息。用户可一次输入多个联系号码，或从地址簿中选择多个消息接收方，以便向多个消息接收方群发消息。每个消息接收方都会收到一条包含相同内容的消息，消息发送方的号码是其真实手机号，消息接收方可直接以P2P消息的形式回复消息给消息发送方。

- 群聊消息

群聊消息是加入群组的所有个人用户之间的消息交互。

- 应用对个人（A2P）信息：

在应用的帮助下产生、并打算发送给个人持有的移动设备的任何消息都被称为A2P消息。A2P消息使公司品牌能够通过聊天机器人与用户交流。用户可向Chatbot发送RCS消息，其中包括文本（含表情符号）、图片、音频、视频、位置、联系人（vCard）和文档。聊天机器人可通过一对一或一对多的方式向用户发送消息，并发送富媒体消息，其中包括文本（含表情符号）、图片、音频、视频、位置、联系人（vCard）和文档。聊天机器人亦可发送“富媒体卡”，并提供由“建议的答复和操作”组成的“选项列表”（suggested chip list）。

6.2 5G消息业务的安全要求架构

图1显示了5G消息业务的安全要求架构，其中包括5G消息业务的用户平面安全要求、管理平面安全要求和控制平面安全要求。

5G消息业务的用户平面安全要求包括用户卡的安全要求，用于补卡或换卡、用户认证、消息接收安全、消息发送安全和消息访问安全。

5G消息业务的管理平面安全要求包括用户管理安全、密钥和证书管理、安全审计和软件管理安全。

5G消息业务的控制平面安全要求包括业务能力限制、主叫黑名单控制和被叫黑名单控制。

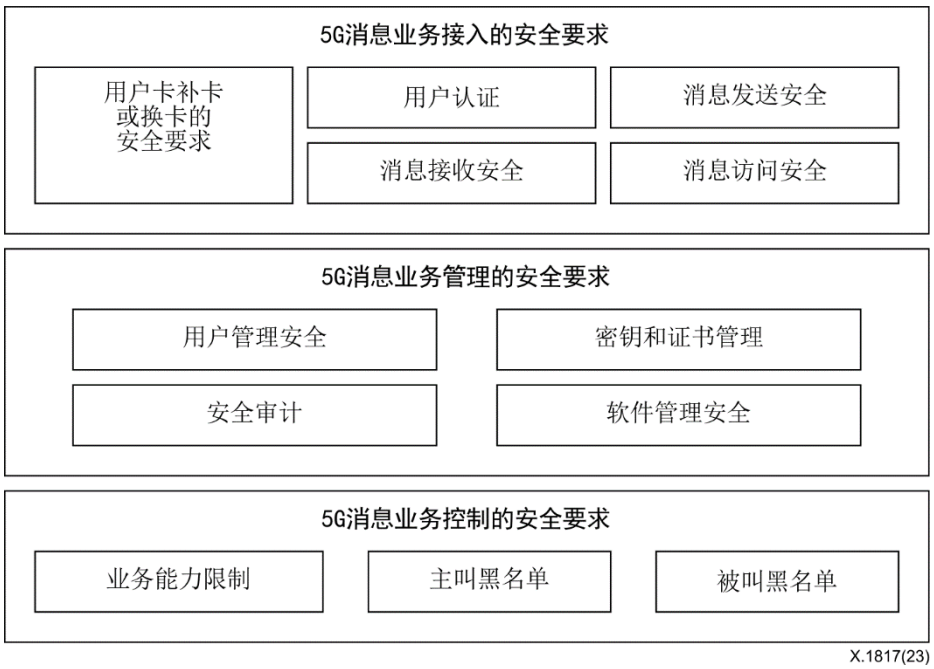

图1 – 5G消息业务的安全要求架构

6.2 5G消息业务与4G/3G/5G/WLAN的安全要求之间的功能差异

5G消息业务和传统短消息的区别在于，传统短消息只能发送文本，而5G消息可以发送多种媒体类型，其中包括文本（含表情符号）、缩略图、图片、音频、视频、位置、联系人和文档。

当使用5G消息业务时，终端可以通过3G、4G、5G或无线局域网（WLAN）访问功能模块。终端完成网络接入后，首先从配置服务器获取业务参数，然后向接入点发起会话发起协议（SIP）注册过程。注册成功后，终端便可收发5G消息，其中包括个人消息和行业消息。

第6.2节中描述的5G消息安全要求架构提供了5G消息安全保护架构。无论通过何种网络模式访问终端，5G消息业务都将受到保护。

7 5G消息业务接入的安全要求

7.1 用户卡补卡或换卡的安全要求

对于长期演进技术语音通话（VoLTE）和5G消息业务的用户而言，如果其因SIM卡丢失/被盗而造成SIM卡不可挽回的丢失，用户便需更换其用户识别模块（SIM）卡，建议5G消息中心更新/刷新相关信息，以便用户在更换SIM卡后可以顺利使用5G消息业务。

7.2 用户认证

用户认证要求消息发送方和接收方均须满足认证要求，业务平台只对认证用户开放5G消息业务。

7.2.1 个人用户认证

5G消息涉及多种业务实现方式，并对应多种用户认证机制。5G消息业务类型和相关的安全认证要求如表1所示。

表1 – 5G消息业务安全认证要求

5G消息业务	安全认证要求
5G消息（各种即时消息交互，其中包括P2P消息、群聊、聊天机器人消息和其他相关信令和媒体）	USIM IMS AKA （SIP注册支持AKA认证）
5G消息（消息存储，其中包括消息中多媒体内容的上传和下载）	USIM GBA_ME
聊天机器人发现	
聊天机器人信息查询	
终端配置管理	首次使用手机号插入认证（蜂窝网）或短消息一次性密码（OTP）（非蜂窝网），在后续获取配置的过程中，终端配置管理可根据需要选择通用自举架构（GBA）进行认证，亦可选择协作签名机制进行认证。建议SMS OTP遵循[ETSI TS 123 040 v17.2.0]。

认证方法描述如下：

a) USIM IMS AKA：对5G消息用户而言，在向5G消息中心注册IP多媒体子系统（IMS）的过程中，5G消息中心通过Zh接口从用户自有的HSS/UDM获取用户的认证和密钥协议（AKA）认证向量，并基于该认证向量完成用户的IMS AKA认证。建议AKA认证符合[ETSI TS 124 229]。

b) USIM GBA_ME：支持5G消息的终端须支持GBA接口。5G消息系统中的非SIP应用服务器须支持GBA Zn接口。建议GBA认证符合[ETSI TS 124 229]。

c) 终端配置管理：首次使用手机号插入认证（蜂窝网）或短消息OTP（非蜂窝网），在后续过程中获取配置。为了防止密钥泄漏，可使用协作签名机制。

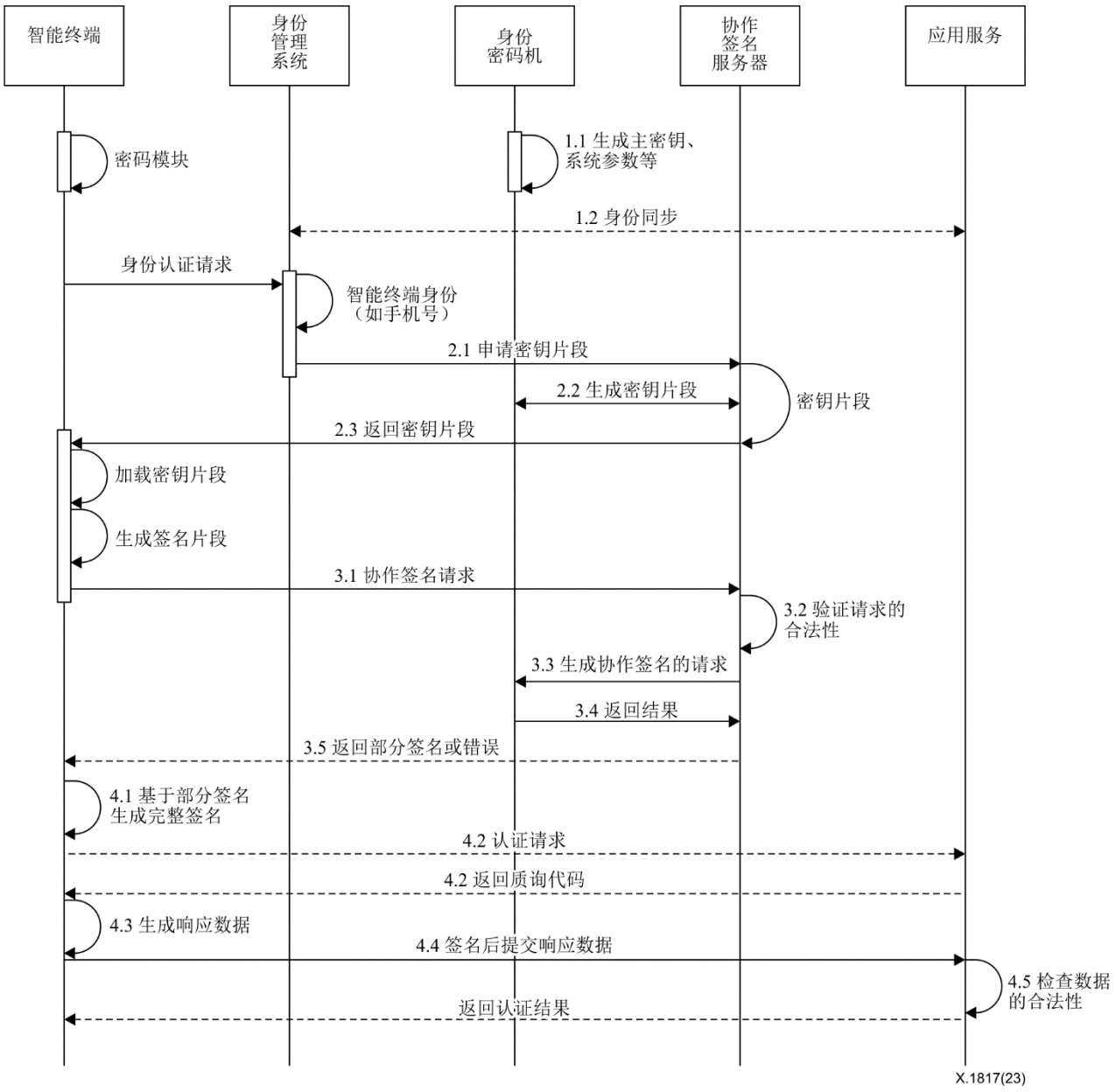

图2 – 5G消息业务的协作签名机制

图2所示的协作签名机制用于5G消息中的身份认证。主要流程如下：

1) 身份密码机生成主密钥、系统参数和身份密钥组件。身份管理系统和应用服务之间的身份同步可根据主密钥、系统参数和身份密钥组件基于预设算法进行。预设算法包括密钥生成算法、签名算法和验证算法中的至少一种。这些步骤描述如下：

   - 步骤1.1：身份密码机生成主密钥、系统参数和身份密钥组件。
   - 步骤1.2：身份管理系统和应用服务之间的身份同步可根据主密钥、系统参数和身份密钥组件基于预设算法进行。

2) 在身份管理系统和应用服务之间的身份同步之后，智能终端身份用于与协作签名服务器的协作签名身份认证。智能终端将智能终端身份（如手机号）发送给身份管理系统。身份管理系统基于智能终端身份向协作签名服务器发送密钥请求。协作签名服务器根据密钥请求将密钥片段反馈给智能终端。这些步骤描述如下：

- 步骤2.1：智能终端发起身份认证请求，并向协作签名服务器申请密钥片段。
- 步骤2.2：协作签名服务器生成密钥片段。
- 步骤2.3：协作签名服务器根据密钥请求向智能终端反馈密钥片段。

3) 智能终端加载密钥片段并生成相应的签名片段。智能终端基于签名片段向协作签名服务器发送协作签名请求。协作签名服务器验证协作签名请求的合法性。当协作签名身份认证通过时，协作签名服务器将协作签名请求转发给身份密码机。身份密码机根据协作签名请求生成部分签名，协作签名服务器将部分签名反馈给智能终端。这些步骤描述如下：

- 步骤3.1：智能终端根据签名片段向协作签名服务器发送协作签名请求。
- 步骤3.2：协作签名服务器验证协作签名请求的合法性。
- 步骤3.3：当协作签名身份认证通过时，协作签名服务器将协作签名请求转发给身份密码机。
- 步骤3.4：身份密码机根据协作签名请求生成部分签名，并将部分签名反馈给协作签名服务器。
- 步骤3.5：协作签名服务器向智能终端反馈部分签名。

4) 智能终端基于部分签名生成完整签名。基于完整签名的应用服务联合签名身份认证过程如下。智能终端基于完整签名向应用服务发送认证请求。应用服务基于认证请求向智能终端反馈质询代码。智能终端根据本地密钥片段和质询代码生成响应数据，并将响应数据发送给应用服务。接收到响应数据后，应用服务验证响应数据的合法性，并基于完整签名验证智能终端的身份。联合签名身份认证完成，应用服务将认证结果反馈给智能终端。这些步骤描述如下：

- 步骤4.1：智能终端从部分签名生成完整签名。
- 步骤4.2：智能终端基于完整签名向应用服务发送认证请求，应用服务向智能终端发送质询代码。
- 步骤4.3：智能终端根据本地密钥片段和质询代码生成响应数据。本地密钥片段是由协作签名服务器反馈的密钥片段。
- 步骤4.4：智能终端向应用服务发送响应数据。
- 步骤4.5：应用服务验证响应数据的合法性。联合签名身份认证完成，应用服务将认证结果反馈给智能终端。

7.2.2 聊天机器人服务器认证

在连接到消息平台之前，聊天机器人需要进行认证。认证采用平台认证和应用层认证相结合的方式。平台认证可使用基于超文本传输安全协议（HTTPS）的数字证书认证，应用层认证可使用基于用户名和密码的认证。

聊天机器人服务器须通过合法的认证机构（CA）申请服务器证书，并在用户注册过程中向消息平台提供CA根证书、聊天机器人服务器的合法域名或IP地址以供注册审核。注册完成后，消息平台在聊天机器人访问过程中对聊天机器人服务器进行身份认证。认证包括聊天机器人服务器证书的验证、聊天机器人身份的认证等。

7.3 消息接收安全

5G消息应用可与终端系统合作，以实现只有5G消息应用可接收5G消息，以确保其不会被恶意使用，且用户消息私人数据不会被泄露。

7.4 消息发送安全

5G消息应用可与终端系统合作，以实现只有5G消息应用可发送5G消息，且发送消息的权限不能被授权给任何其他应用，以确保其不会被恶意使用。

7.5 消息访问安全

5G消息应用可与终端系统合作，以限制5G消息的授权访问能力。终端侧的消息文件须只能由5G消息应用读取或执行其他管理操作（如删除和备份）。建议平台侧的消息为消息所有者提供查询和阅读（包括日志相关数据）功能，其他用户（包括管理员）则一般禁止访问。

8 5G消息业务管理的安全要求

8.1 用户管理安全

8.1.1 角色和权限的划分

用户管理安全根据业务模块分区和权限功能将业务平台划分为层和区域。建议根据不同的权限设置管理员帐户，其中包括超级管理员、业务管理员和审计员：

a) 超级管理员：对业务功能平台拥有高级管理权限，且可以管理业务管理员和审计员。

b) 业务管理员：拥有业务管理和操作的部分或全部权限，但不能拥有审计权限，亦不能管理其他业务管理员。

c) 审计员：拥有记录审计和操作审计的权限，但没有业务处理权限。

8.1.2 异常行为监控

监控和审计一些异常行为，如异常登录、多个位置同时登录、发送超过阈值速率的消息（将该行为归类为垃圾信息）。对于此类异常行为，需要采取相应的措施（例如，添加到黑名单和冻结账户）来限制此类异常用户。

8.2 密钥和证书管理

8.2.1 密钥管理

密钥管理是5G消息终端和业务平台管理其敏感数据加密密钥的管理机制。当平台侧或终端侧对敏感数据进行加密存储时，建议为不同类型的敏感数据设置不同的加密密钥。建议密钥管理要求符合[ISO/IEC 11770-1]。

5G消息系统可设计相应的密钥来保护不同的对象，且至少包括表2中所示的以下密钥类型：

表2 – 5G消息系统密钥类型和描述

类型	描述
数据安全存储密钥	保护存储的重要数据和敏感信息。
安全通信密钥	GBA密钥是在终端和多平台的登录认证过程中通过GBA进程生成的（建议有关具体生成方法的要求符合[ETSI TS 129 109]中的GBA认证）。
用户识别信息加密密钥	保护用户身份信息
密钥数据加密密钥	保护密钥相关数据
数据安全传输密钥	保护传输中的重要数据和敏感信息

8.2.2 证书管理

要实现HTTPS安全连接，web服务器需要配置一个数字证书来证明服务器的使用类型。对于需要配置数字证书的服务器，如果有多个域名，则需要为每个域名申请一个服务器证书。当服务器使用IP提供业务时，如果有多个IP，则需要为每个IP申请一个服务器证书，这些证书类型如表3所示。

表3 – 5G消息系统服务器证书配置描述

服务器名称	访问方式	证书类型
5GMC	域名	普通SSL证书（终端须预置CA根证书）
消息平台	域名	普通SSL证书（终端须预置CA根证书）
消息平台管理模块	域名	普通SSL证书
聊天机器人	域名	普通SSL证书

8.3 安全审计

日志记录重要的用户行为、系统资源的异常使用以及平台中重要平台命令的使用。记录可包括日期和时间、类型、主题标识、对象标识和事件结果。业务安全日志中可记录的内容包括但不限于用户操作日志、管理员操作日志和业务日志。

a) 用户操作日志：记录帐户操作和结果、业务操作和结果等。用户操作日志可包括用户信息、用户操作、操作对象、操作时间、操作结果、异常结果等。

b) 管理员操作日志：记录帐户操作和结果、业务操作和结果等。管理员操作日志包括管理员信息、管理员操作、操作对象、操作时间、操作结果、异常结果等。

c) 业务日志：建议系统记录其业务日志。该平台可存储指定时间内的各种日志，以便根据需要进行在线查询；对于超过在线存储时间要求的日志，可指定离线存储时间。在线日志存储在数据库或系统指定的方法中。业务平台管理访问权限，只能由指定的管理员（审计员）查看、导出或审计；对于离线日志，可导入系统或使用特殊工具进行查询、审计等操作。包含敏感数据的离线日志在导出后可存储在加密文件中。

8.4 软件管理安全

8.4.1 面向5G消息的软件开发管理安全

5G消息业务系统的安全编码原则须包括：

a) 检查用户输入数据的有效性，并过滤敏感符号。

b) 加密存储敏感数据，如密码。

c) 通过HTTPS传输敏感数据，如用户名和密码。

d) 不要直接访问系统资源，如文件。

e) 不要在与Web相关的代码中使用外壳（shell）。

f) 使用安全功能进行编程。

8.4.2 5G消息系统的运营管理安全

5G消息系统可监控重要流程和业务处理逻辑，并在发现故障时发出警报。

9 5G消息业务控制的安全要求

9.1 业务能力限制

业务能力限制包括群人数限制、群功能差异化控制和群聊限制。

a) 群人数限制：群发5G消息操作需要设置群发人数的上限，从而将潜在的不利影响限制在有限的范围内。

b) 群功能差异化控制：业务平台可支持群业务被叫用户数量的差异化控制。

c) 群聊限制：业务平台可支持群聊的用户规模限制，用户的群数量参数可以配置，业务平台亦可支持群名长度限制。

9.2 主叫黑名单

对于5G移动发起（MO）消息，需要增加主叫黑名单列表认证控制功能，以防止5G消息轰炸的风险。可为群聊监控机制建立一个控制系统，火焰控制系统可以为群聊建立监控机制，分析恶意群发消息的行为，此类消息将通过自动添加、人工审查和其他方式被添加到主叫黑名单控制中。然后，主叫黑名单控制便可拦截和控制恶意群发消息的行为。

9.3 被叫黑名单

对于5G移动终接（MT）消息，需要添加被叫黑名单控制，以降低终端用户投诉的可能性。个人用户可通过拨打客服电话、登录自助服务界面、前往营业厅等方式进行投诉或设置被叫黑名单。火焰控制系统可以建立被呼叫黑名单控制系统或相关业务系统，此系统可根据特定的用户或业务类型拦截用户发出的消息。

参考文献

[b-GSMA RCC.71] GSM Association (2019), *RCS Universal Profile Service Definition Document*.

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2024年，日内瓦