ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1817 (09/2023)

SERIES X: Data networks, open system communications and security

IMT-2020 Security

Security requirements for 5G messaging service

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	**X.1800-X.1819**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1817

Security requirements for 5G messaging service

Summary

Recommendation ITU-T X.1817 provides the security requirements for 5G message service, including access security requirements, management security requirements and control security requirements for 5G message service.

History[*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1817	2023-09-08	17	11.1002/1000/15524

Keywords

5G message service, security framework, security requirement.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T X.1817

Security requirements for 5G messaging service

1 Scope

The 5G messaging service is an upgrade of the short message service (SMS). It is one of the basic telecommunication business services and includes the short message service (SMS) defined in 3GPP and the rich communication service (RCS) defined in GSMA. Especially, it supports messages between persons or between applications and persons, and it also supports various media (e.g., long text, picture, video, audio, file and position) in the message. This Recommendation describes security requirements that could mitigate the security threats and challenges of the 5G messaging service. This Recommendation provides the security requirements for the 5G messaging service, including access security requirements, management security requirements and control security requirements for 5G messaging service. This Recommendation also describes the functional differences between the security requirements for 5G messaging service those of 4G/3G/5G/WLAN.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ETSI TS 123 040] ETSI TS 123 040 v17.2.0 (2022), *Digital cellular telecommunications system (Phase 2+) GSM; Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of the Short Message Service (SMS).*

[ETSI TS 124 229] ETSI TS 124 229 (2017), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.

[ETSI TS 129 109] ETSI TS 129 109 (2018), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*.

[ISO/IEC 11770-1] ISO/IEC 11770-1:2010, *Information technology – Security techniques – Key management – Part 1: Framework*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 chatbot [b-GSMA RCC.71]: A rich communication service (RCS)-based (automated service provided to users whose output is presented in a conversational form.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 5G message centre: Server providing the 5G messaging service.

3.2.2 message platform: A platform for third-party application to connect with the 5G message centre.

3.2.3 5G message user equipment (UE): A 5G user equipment (UE) whose message app supports both short message service (SMS) and rich communication service (RCS).

3.2.4 5G messaging service: A 5G messaging service including short message service (SMS) and rich communication service (RCS). 5G messaging service supports messages between persons or between applications and persons, and it also supports various media (e.g., long text, picture, video, audio, file and position) in the message.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3GPP	3rd Generation Partnership Project
A2P	Application to Person
AKA	Authentication and Key Agreement
GBA	Generic Bootstrapping Architecture
GSMA	Global System for Mobile Communications Association
HSS	Home Subscriber Service
HTTPS	Hypertext Transfer Protocol Secure
IMS	IP Multimedia Subsystem
MO	Mobile Originate
MT	Mobile Terminate
OTP	One-Time Password
P2P	Person to Person
RCS	Rich Communication Service
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
UE	User Equipment
UDM	Unified Data Management
VoLTE	Voice over Long-Term Evolution
WLAN	Wireless Local Area Network

5 Conventions

This Recommendation uses the following conventions:

The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview

6.1 5G messaging service

The 5G messaging service, following the GSMA rich communication service (RCS) universal profile, allows advanced services such as multimedia messaging, group chat, and message platform. The 5G messaging service is based on the terminal's native short message service (SMS) portal, allowing users to send and receive text, pictures, audio, video, location data, contacts information and other media content, including the following service functions:

- Person to person (P2P) messages

P2P messages refer to messages sent between individual users and support the following media content: text (including emoticons), pictures, audio, video, location, contacts (vCard), and documents.

- Group messages

A group message refers to a message sent by an individual user to multiple other individual users at the same time. The user can enter multiple contact numbers at a time or select multiple recipients from the address book to send a group message to multiple recipients. Each receiver will receive a message containing the same content, the sender's number is his real mobile phone number, and the receiver can directly reply to the message to the sender in a P2P message.

- Group chat messages

A group chat message is a message interaction between all individual users who join the group.

- Application to person (A2P) messages

Any message originated with the help of an application and intended for mobile equipment held by a person is called A2P messaging. A2P messaging enables company brands to communicate with users through Chatbot. Users can send RCS messages to Chatbot including text (including emoticons), pictures, audio, video, location, contacts (vCard), and documents. Chatbots could message users via one-to-one or one-to-many and send rich messages including text (including emoticons), pictures, audio, video, location, contacts (vCard), and documents. Chatbot could send 'rich cards' that provide a 'suggested chip list' consisting of 'suggested replies and actions'.

6.2 Security requirements architecture for 5G messaging service

Figure 1 shows the security requirements architecture for 5G messaging service, which consists of the user plane security requirements, the management plane security requirements and the control plane security requirements for 5G messaging service.

The user plane security requirements for 5G messaging service include the security requirement of a user card for make-up or change, user authentication, message receive security, message send security and message access security.

The management plane security requirements for 5G messaging service include user management security, key and certificate management, security audit and software management security.

The control plane security requirements for 5G messaging service include service ability restriction, calling blacklist control and called blacklist control.

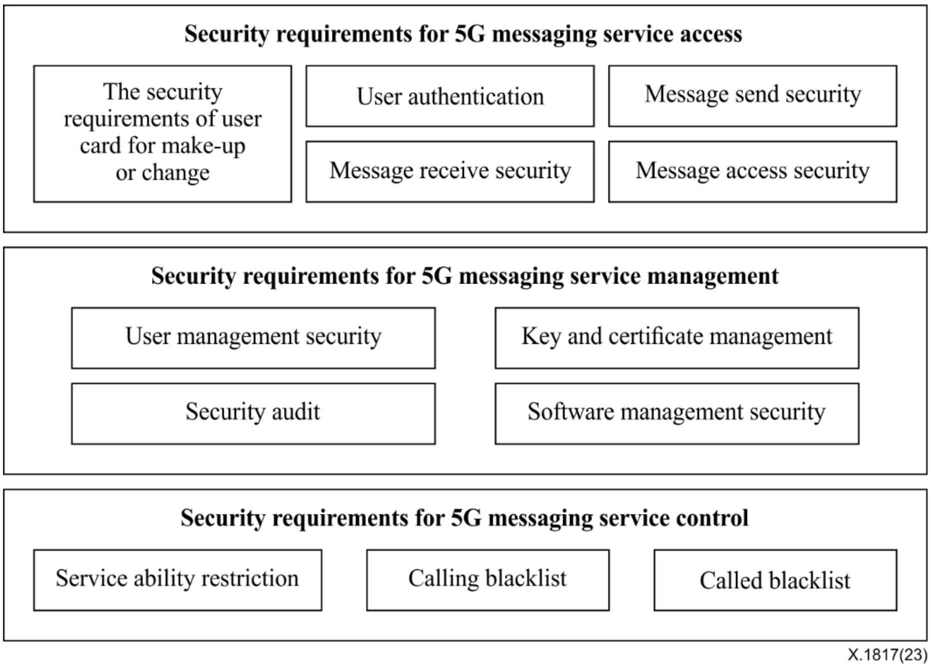
Security requirements for 5G messaging service access
The security requirements of user card for make-up or change
User authentication
Message send security
Message receive security
Message access security
Security requirements for 5G messaging service management
User management security
Key and certificate management
Security audit
Software management security
Security requirements for 5G messaging service control
Service ability restriction
Calling blacklist
Called blacklist
X.1817(23)

Figure 1 – Security requirements architecture for 5G messaging service

6.2 The functional difference between the security requirements for 5G messaging service with 4G/3G/5G/WLAN

The difference between the 5G messaging service and the traditional SMS message is that while the traditional SMS can only send text, 5G message can send a variety of media types, including text (including emoticons), thumbnails, pictures, audio, video, location, contacts, and documents.

When using 5G messaging services, terminals can access function modules through 3G, 4G, 5G, or wireless local area network (WLAN). After completing network access, terminals first obtain service parameters from the configuration server, and then initiate a session initiation protocol (SIP) registration process to the access point. After successful registration, they can send and receive 5G messages, including personal messages and industry messages.

The 5G message security requirements architecture described in clause 6.2 provides the 5G message security protection architecture. 5G messaging services will be protected regardless of the network mode through which terminals are accessed.

7 Security requirements for 5G messaging service access

7.1 Security requirements of user card for make-up or change

For users of voice over long-term evolution (VoLTE) and 5G messaging service who are required to change their subscriber identity module (SIM) card due to the lost/stolen SIM card being irretrievably lost, it is recommended that the 5G message centre need to update/refresh related information so that users can use 5G messaging service smoothly after changing SIM cards.

7.2 User authentication

It is required that user authentication between the message sender and receiver meets the authentication requirements, and that the service platform opens the 5G messaging service only to authenticated users.

7.2.1 Personal user authentication

5G messages involve a variety of service implementation methods, corresponding to a variety of user authentication mechanisms. The 5G messaging service types and related security authentication requirements are shown in Table 1.

Table 1 – 5G messaging service security authentication requirements

5G messaging service	Security authentication requirements
5G messaging (various instant messaging interactions, including P2P messaging, group chat, Chatbot messaging and other related signalling and media)	USIM IMS AKA (SIP registration supports AKA authentication)
5G messaging (message storage, including upload and download of multimedia content in messages)	USIM GBA_ME
Chatbot discovering	
Chatbot information querying	
Terminal configuration management	For the first time, use the mobile phone number insertion authentication (cellular network) or SMS one-time password (OTP) (non-cellular network), in the subsequent process of obtaining the configuration, terminal configuration management can choose generic bootstrapping architecture (GBA) authentication as needed. It can also select the collaborative signature mechanism for authentication. It is recommended that the SMS OTP comply with [ETSI TS 123 040 v17.2.0].

The authentication methods are described as follows:

a) USIM IMS AKA: For a 5G message user, during IP multimedia subsystem (IMS) registration with the 5G message centre, the 5G message centre obtains the authentication and key agreement (AKA) authentication vector of the user from the user's owned HSS/UDM through the Zh interface and completes IMS AKA authentication of the user based on the authentication vector. It is recommended that the AKA certification comply with [ETSI TS 124 229].

b) USIM GBA_ME: It is required that terminals of support 5G messages support GBA interfaces. It is required that Non-SIP application servers in the 5G messaging system support GBA Zn interfaces. It is recommended that the GBA certification comply with [ETSI TS 124 229].

c) Terminal configuration management: For the first time, uses the mobile phone number insertion authentication (cellular network) or SMS OTP (non-cellular network), in the subsequent process of obtaining the configuration. To protect keys from key leakage, it can use the collaborative signature mechanism.

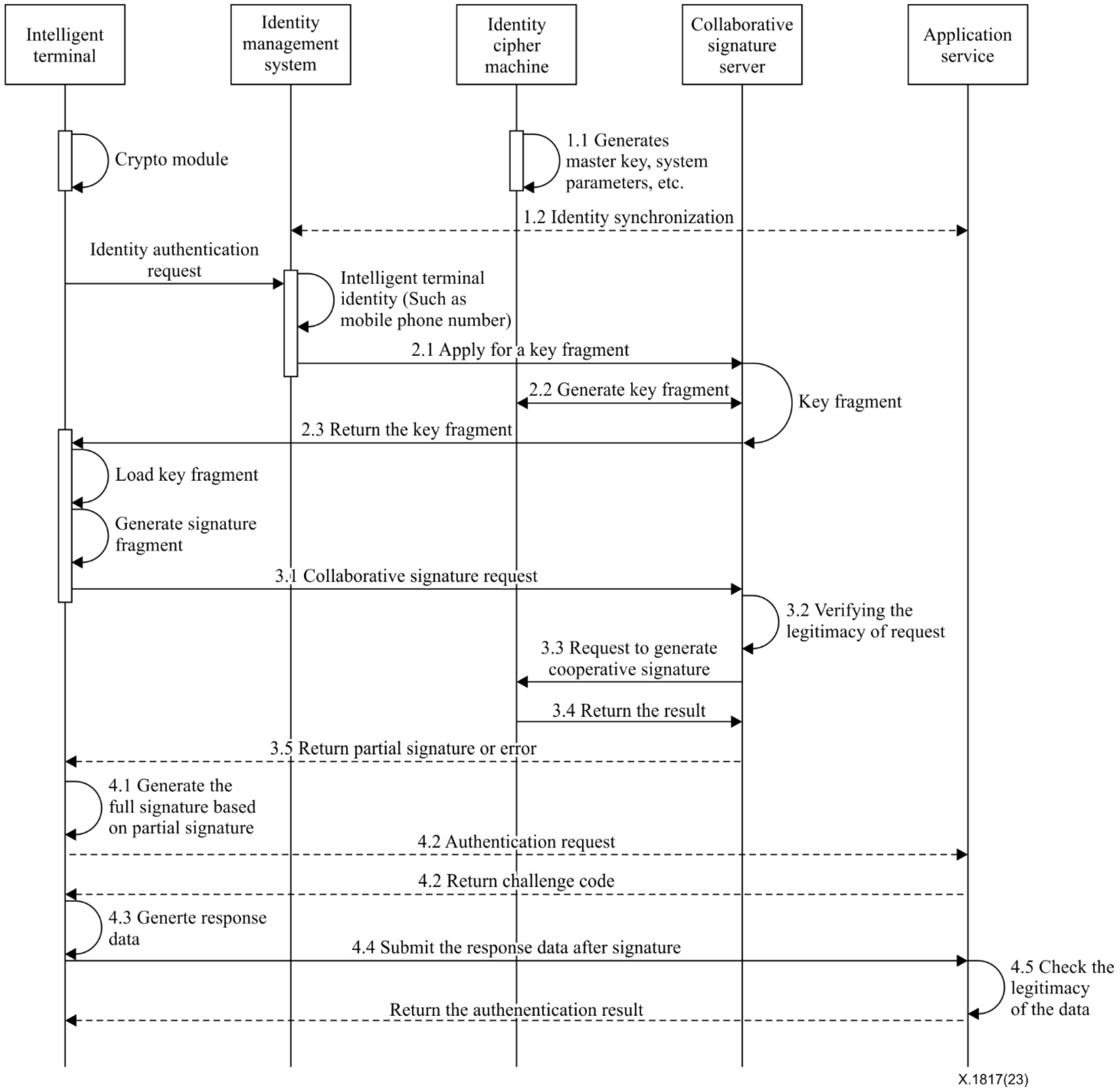
Intelligent terminal
Identity management system
Identity cipher machine
Collaborative signature server
Application service
Crypto module
1.1 Generates master key, system parameters, etc.
1.2 Identity synchronization
Identity authentication request
Intelligent terminal identity (Such as mobile phone number)
2.1 Apply for a key fragment
2.2 Generate key fragment
Key fragment
2.3 Return the key fragment
Load key fragment
Generate signature fragment
3.1 Collaborative signature request
3.2 Verifying the legitimacy of request
3.3 Request to generate cooperative signature
3.4 Return the result
3.5 Return partial signature or error
4.1 Generate the full signature based on partial signature
4.2 Authentication request
4.2 Return challenge code
4.3 Generte response data
4.4 Submit the response data after signature
4.5 Check the legitimacy of the data
Return the authenentication result
X.1817(23)

Figure 2 – Collaborative signature mechanism for 5G messaging service

The collaborative signature mechanism shown in Figure 2 is used for identity authentication in 5G messages. The main process is as follows:

1) The identity cipher machine generates the master key, the system parameters and the identity key component. The identity synchronization between the identity management system and the application service can be carried out based on the preset algorithm according to the master key, system parameters and the identity key component. The preset algorithm includes at least one of the key generation algorithm, signature algorithm and verification algorithm. The steps are described below:
   - Step 1.1: The identity cipher machine generates the master key, the system parameters and the identity key component.
   - Step 1.2: The identity synchronization between the identity management system and the application service can be carried out based on the preset algorithm according to the master key, system parameters and the identity key component.

2) After identity synchronization between the identity management system and the application service, the intelligent terminal identity is used for collaborative signature identity authentication with the collaborative signature server. The intelligent terminal sends the intelligent terminal identity (such as the mobile phone number) to the identity management system. The identity management system sends the key request to the collaborative signature server based on the intelligent terminal identity. The collaborative signature server feeds back the key fragment to intelligent terminal based on the key request. The steps are described below:

- Step 2.1: The intelligent terminal initiates an identity authentication request and applies for a key fragment from the collaborative signature server.
- Step 2.2: The collaborative signature server generate key fragment.
- Step 2.3: The collaborative signature server feeds back the key fragment to the intelligent terminal based on the key request.

3) The intelligent terminal loads the key fragment and generates the corresponding signature fragment. The intelligent terminal sends a collaborative signature request to the collaborative signature server based on the signature fragment. The collaborative signature server verifies the legitimacy of the collaborative signature request. When the collaborative signature identity authentication passes, the collaborative signature server forwards the collaborative signature request to the identity cipher machine. The identity cipher machine generates partial signature according to the collaborative signature request, and the collaborative signature server feeds back the partial signature to the intelligent terminal. The steps are described below:

- Step 3.1: The intelligent terminal sends a collaborative signature request to the collaborative signature server based on the signature fragment.
- Step 3.2: The collaborative signature server verifies the legitimacy of the collaborative signature request.
- Step 3.3: When the collaborative signature identity authentication passes, the collaborative signature server forwards the collaborative signature request to the identity cipher machine.
- Step 3.4: The identity cipher machine generates partial signature according to the collaborative signature request, and feeds back the partial signature to the collaborative signature server.
- Step 3.5: The collaborative signature server feeds back the partial signature to the intelligent terminal.

4) The intelligent terminal generates a full signature based on the partial signature. The process of joint signature identity authentication with application service based on the full signature is as follows. The intelligent terminal sends an authentication request to the application service based on the full signature. The application service feeds back a challenge code to the intelligent terminal based on the authentication request. The intelligent terminal generates a response data according to the local key fragment and challenge code, and sends the response data to the application service. After receiving the response data, the application service verifies the legitimacy of the response data and verifies the identity of the intelligent terminal based on the full signature. The joint signature identity authentication is completed, and the application service feeds back the authentication result to the intelligent terminal. The steps are described below:

- Step 4.1: The intelligent terminal generates the full signature from the partial signature.
- Step 4.2: The intelligent terminal sends an authentication request to the application service based on the full signature, and the application service sends a challenge code to the intelligent terminal.

- Step 4.3: The intelligent terminal generates response data according to the local key fragment and the challenge code. The local key fragment is the key fragment that is fed back by the collaborative signature server.
- Step 4.4: The intelligent terminal sends the response data to the application service.
- Step 4.5: The application service verifies the legitimacy of the response data. The joint signature identity authentication is completed, and the application service feeds back the authentication result to the intelligent terminal.

7.2.2 Chatbot server authentication

Before Chatbot is connected to the message platform, Chatbot needs to be authenticated. The authentication adopts a combination of platform authentication and application layer authentication. Platform authentication can use digital certificate authentication based on hypertext transfer protocol secure (HTTPS) protocol, and application layer authentication can use authentication which is based on a username and password.

It is required that the Chatbot server apply for a server certificate through a legal Certification Authority (CA), and provide the CA root certificate, the legal domain name or IP address of the Chatbot server to the message platform for registration review during the user registration process. After the registration is completed, the message platform performs identity authentication on the Chatbot server during the Chatbot access process. The authentication includes the verification of the Chatbot server certificate, the authentication of the Chatbot identity.

7.3 Message receive security

5G messaging applications could cooperate with the terminal system to realize that only 5G messaging applications can receive 5G messages to ensure that they will not be maliciously used, and that user message private data will not be leaked.

7.4 Message send security

5G messaging applications could cooperate with the terminal system to realize that only 5G messaging applications can send 5G messages, and the permission to send messages cannot be authorized to any other applications to ensure that they will not be maliciously used.

7.5 Message access security

5G messaging applications could cooperate with terminal systems to restrict the authorized access capabilities of 5G messages. It is required that the message file on the terminal side only be read by the 5G messaging application or perform other management operations (such as deletion and backup). It is recommended that the message on the platform side provide query and read (including log-related data) for the message owner, and that other users (including administrators) generally be prohibited access.

8 Security requirements for 5G messaging service management

8.1 User management security

8.1.1 Division of roles and permissions

User management security divides the service platform into layers and areas according to service module zoning and privilege functions. It is recommended that an administrator account is set according to different privileges which include super administrator, service administrator and auditor:

a) Super administrators: they have advanced management authority for the service function platform which means they could manage service administrators and auditors.

b) Service administrators: they have part or full authority for service management and operation. However, service administrators cannot have audit authority or manage other service administrators.

c) Auditors: they have the authority for logging audits and operating audits, but they cannot have the authority for service processing.

8.1.2 Abnormal behaviour monitor

Monitoring and auditing some abnormal behaviours such as abnormal login, multiple places login at the same time, sending messages beyond a threshold rate (to categorize the action as spam). For these abnormal behaviours, there is a corresponding need to take actions (e.g., add to blacklist and frozen account) to restrict these abnormal users.

8.2 Key and certificate management

8.2.1 Key management

Key management is the management mechanism through which the 5G message terminal and service platform manage their sensitive data encryption keys. It is recommended that there is a set of different encryption keys for different types of sensitive data which could be used when the platform side or terminal side do the encrypted storage of sensitive data. It is recommended that key management requirements comply with [ISO/IEC 11770-1].

The 5G messaging system could design corresponding keys to protect different objects, including at least the following key types shown in Table 2:

Table 2 – 5G message system key types and descriptions

Types	Descriptions
Data security storage key	Protect stored important data and sensitive information.
Secure communication key	The GBA key is generated during the login authentication process of the terminal and multiple platforms through the GBA process (the specific generation method and it is recommended that requirements comply with GBA authentication in [ETSI TS 129 109].
User identification information encryption key	Protect user identification information.
Key data encryption key	Protect key-related data.
Data security transfer key	Protect important data and sensitive information in transit.

8.2.2 Certificate management

To implement HTTPS secure connections, the web server needs to be configured with a digital certificate that certifies the type of server usage. For servers that need to be configured with digital certificates, if there are multiple domain names, there is a need to apply for a server certificate for each domain name. When a server uses IP to provide services, if there are multiple IPs, there is a need to apply for a server certificate for each IP and these certificate types are shown in Table 3.

Table 3 – 5G message system server certificate configuration description

Server name	Access method	Certificate type
5GMC	Domain name	Ordinary SSL certificate (Requires the terminal to preset the CA root certificate)
Message platform	Domain name	Ordinary SSL certificate (Requires the terminal to preset the CA root certificate)

Table 3 – 5G message system server certificate configuration description

Server name	Access method	Certificate type
Message platform management module	Domain name	Ordinary SSL certificate
Chatbot	Domain name	Ordinary SSL certificate

8.3 Security audit

Logs are records of important user behaviours, abnormal use of system resources, and the use of important platform commands in the platform. The records could include date and time, type, subject identification, object identification, and event results. The contents that could be recorded in the service security log include, but are not limited to, user operation logs, administrator operation logs, and service logs.

a) User operation logs: they record account operations and results, service operations and results and so on. The user operation logs could include user information, user operations, operation objects, operation time, operation results, abnormal results and so on.

b) Administrator operation logs: they record account operations and results, service operations and results and so on. The administrator operation logs could include administrator information, administrator operations, operation objects, operation time, operation results, abnormal results and so on.

c) Service logs: It is recommended that systems could record their service logs. The platform could store all kinds of logs within a specified time for online query according to demand; for logs that exceed the online storage time requirements, the offline storage time could be specified. Online logs are stored in a database or a system-designated method. The service platform manages access rights, and can only be viewed, exported or audited by a designated administrator (auditor); for offline logs, they could be imported into the system or use special tools for query, audit and other operations. Offline logs containing sensitive data could be stored in encrypted files after being exported.

8.4 Software management security

8.4.1 Software development management security for 5G messaging

It is required that the secure coding principles of the 5G messaging service system include:

a) Checking the effectiveness of user input data, filtering sensitive symbols.

b) Encrypting storage sensitive data, such as passwords.

c) Transmitting sensitive data by HTTPS, such as usernames and passwords.

d) Do not access system resources directly, such as files.

e) Do not use shells in the codes associated with Web.

f) Using a safety function to programme.

8.4.2 Operation management security for 5G message system

The 5G message system could monitor the important processes and the logic of service processing, and will emit an alarm when faults are discovered.

9 Security requirements for 5G messaging service control

9.1 Service ability restrictions

Service ability restrictions include restrictions of the number of people in a group, the differentiated control of group functions and the restrictions of group chats.

a) The restriction of the number of people in a group: the group sending 5G message operations needs to set the upper limit of the number of group sending, so as to limit the potential adverse effects to a limited range.

b) The differentiated control of group functions: service platforms could support the differentiated control of the number of called users of a group service.

c) The restrictions of group chats: service platforms could support the user scale restriction of group chats, the parameters of the group number of users can be configured, service platforms could support the restriction of group name length.

9.2 Calling blacklist

For 5G mobile originate (MO) messages, there is a need to add calling backlist authentication control function to prevent the risks of 5G message bombing. A flame control system could establish a monitoring mechanism for group chats which could analyse the actions of malicious mass messages which will be added into a calling blacklist control by automatically added, manual reviews and in other ways The calling blacklist control could then intercept and control the actions of malicious group messages.

9.3 Called blacklist

For 5G mobile terminate (MT) messages, there is a need to add called blacklist control to decrease the possibility of terminal user complaints. Personal users could complain or set a called blacklist by calling customer service, logging onto a self-service interface, going to a service hall and in other ways. A flame control system or related service systems could establish a called blacklist control which could intercept the messages by users according to a given user or service type.

Bibliography

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023