ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1817 (09/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

Безопасность сетей IMT-2020

Требования безопасности для услуги обмена сообщениями 5G

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

Сети передачи данных, взаимосвязь открытых систем и безопасность

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	X.1000–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200–X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300–X.1499
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600–X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750–X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	**X.1800–X.1819**

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1817

Требования безопасности для услуги обмена сообщениями 5G

Резюме

В Рекомендации МСЭ-Т X.1817 представлены требования безопасности для услуги обмена сообщениями 5G, включая требования безопасности использования, требования безопасности управления и требования безопасности контроля в отношении услуги обмена сообщениями 5G.

Хронологическая справка[*]

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1817	08.09.2023 г.	17-я	11.1002/1000/15524

Ключевые слова

Услуга обмена сообщениями 5G, система безопасности, требования безопасности.

[*] Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами/авторскими правами на программное обеспечение, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1817

Требования безопасности для услуги обмена сообщениями 5G

1 Сфера применения

Услуга обмена сообщениями 5G представляет собой усовершенствованную услугу передачи коротких сообщений (SMS). Это одна из основных бизнес-услуг электросвязи, которая включает услугу передачи коротких сообщений (SMS), определенную в стандарте 3GPP, и услугу связи с расширенными возможностями (rich communication service (RCS)), определенную в стандарте GSMA. В частности, она поддерживает сообщения между физическими лицами или между приложениями и физическими лицами, а также различные мультимедийные средства (длинный текст, изображения, видео, аудио, файлы и данные о местоположении) в составе сообщений. В настоящей Рекомендации описаны требования безопасности, помогающие смягчить угрозы и проблемы безопасности, связанные с услугой обмена сообщениями 5G. В этой Рекомендации представлены требования безопасности для услуги обмена сообщениями 5G, включая требования безопасности доступа, требования безопасности управления и требования безопасности контроля услуги обмена сообщениями 5G. В этой Рекомендации также описываются функциональные различия между требованиями безопасности для услуги обмена сообщениями 5G и для услуг обмена сообщениями 4G/3G/5G/WLAN.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[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 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в других документах:

3.1.1 чат-бот (chatbot) [b-GSMA RCC.71]: Автоматизированная услуга обмена сообщениями на основе услуги связи с расширенными возможностями (RCS), предоставляемая пользователям, поддерживающим разговор в диалоговой форме.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 центр обмена сообщениями 5G (5G message centre): Сервер, предоставляющий услугу обмена сообщениями 5G.

3.2.2 платформа обмена сообщениями (message platform): Платформа для подключения сторонних приложений к центру обмена сообщениями 5G.

3.2.3 пользовательское оборудование обмена сообщениями 5G (5G message user equipment (UE)): Пользовательское оборудование (UE) 5G, на котором установлено приложение для обмена сообщениями, поддерживающее как услугу передачи коротких сообщений (SMS), так и услугу связи с расширенными возможностями (RCS).

3.2.4 услуга обмена сообщениями 5G (5G messaging service): Услуга обмена сообщениями 5G, включающая услугу передачи коротких сообщений (SMS) и услугу связи с расширенными возможностями (RCS). Услуга обмена сообщениями 5G поддерживает сообщения между физическими лицами или между приложениями и физическими лицами, а также различные мультимедийные средства (длинный текст, изображения, видео, аудио, файлы и данные о местоположении) в составе сообщений.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

3GPP	3rd Generation Partnership Project	Проект партнерства третьего поколения
A2P	Application to person	Между приложением и физическим лицом
AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключах
GBA	Generic Bootstrapping Architecture	Общая архитектура начальной загрузки
GSMA	Global System for Mobile communications Association	Ассоциация глобальной системы подвижной связи
HSS	Home Subscriber Service	Услуга для абонента в сети регистрации абонента
HTTPS	Hypertext Transfer Protocol Secure	Защищенный протокол передачи гипертекста
IMS	IP Multimedia Subsystem	Мультимедийная IP-подсистема
MO	Mobile Originate	Мобильное устройство – источник сообщений
MT	Mobile Terminate	Мобильное устройство – приемник сообщений
OTP	One-Time Password	Одноразовый пароль
P2P	Person to person	Между физическими лицами
RCS	Rich Communication Service	Услуга связи с расширенными возможностями
SIM	Subscriber Identity Module	Модуль идентификации абонента
SIP	Session Initiation Protocol	Протокол инициации сеанса
SMS	Short Message Service	Услуга передачи коротких сообщений
UE	User Equipment	Пользовательское оборудование
UDM	Unified Data Management	Единое управление данными
VoLTE	Voice over Long-Term Evolution	Передача голоса по сети LTE
WLAN	Wireless Local Area Network	Беспроводная локальная сеть

5 Соглашения

В настоящей Рекомендации используются следующие условные обозначения.

Ключевые слова "**требуется**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации.

Ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии это требование не является обязательным.

6 Обзор

6.1 Услуга обмена сообщениями 5G

Услуга обмена сообщениями 5G, следуя универсальному профилю услуги связи с расширенными возможностями (RCS) GSMA, обеспечивает усовершенствованные услуги, такие как обмен мультимедийными сообщениями, групповой чат и платформа для обмена сообщениями. Услуга обмена сообщениями 5G основана на собственном портале услуги коротких сообщений (SMS) терминала и позволяет пользователям передавать и получать текст, изображения, аудио, видео, данные о местоположении, контактную информацию и другой мультимедийный контент, включая перечисленные ниже служебные функции.

- Обмен между физическими лицами (P2P)

Сообщения P2P – это сообщения, которые передаются между отдельными пользователями и могут содержать следующий мультимедийный контент: текст (включая значки настроения), изображения, аудио, видео, информацию о местоположении, контактную информацию (vCard) и документы.

- Групповые сообщения

Групповое сообщение – это сообщение, которое отдельный пользователь отправляет нескольким другим пользователям одновременно. Чтобы отправить групповое сообщение нескольким получателям, пользователь может указать сразу несколько контактных номеров или выбрать нескольких получателей из адресной книги. Каждый получатель получит сообщение с одним и тем же содержанием, номером отправителя служит его реальный номер мобильного телефона, и получатель может напрямую ответить на это сообщение отправителю сообщением P2P.

- Групповые сообщения в чате

Групповые сообщения в чате – это способ обмена сообщениями между всеми пользователями, присоединившимися к группе.

- Сообщения приложение – физическое лицо (A2P)

Обменом сообщениями A2P называется любой обмен сообщениями, созданными с помощью приложения и предназначенными для персонального мобильного устройства. Обмен сообщениями A2P позволяет компаниям общаться с пользователями через чат-бот. Пользователи могут отправлять в чат-бот сообщения RCS, включая текст (в том числе значки настроения), изображения, аудио, видео, информацию о местоположении, контактную информацию (vCard) и документы. Чат-боты могут отправлять пользователям персональные или групповые сообщения, а также расширенные сообщения, содержащие текст (включая значки настроения), изображения, аудио, видео, информацию о местоположении, контактную информацию (vCard) и документы. Чат-бот может отправлять "расширенные карточки", содержащие "предлагаемый чиплист", состоящий из "предлагаемых ответов и действий".

6.2 Архитектура требований безопасности для услуги обмена сообщениями 5G

На рисунке 1 показана архитектура требований безопасности для услуги обмена сообщениями 5G, состоящая из требований безопасности плоскости пользователя, требований безопасности плоскости управления и требований безопасности плоскости контроля услуги обмена сообщениями 5G.

К требованиям безопасности плоскости пользователя для услуги обмена сообщениями 5G относятся требования обеспечения безопасности карты пользователя при ее создании или изменении, требования аутентификации пользователя, безопасности получения сообщений, безопасности передачи сообщений и безопасности доступа к сообщениям.

К требованиям безопасности плоскости управления для услуги обмена сообщениями 5G относятся безопасность управления пользователями, управление ключами и сертификатами, проверка безопасности и безопасность управления программным обеспечением.

К требованиям безопасности плоскости контроля для услуги обмена сообщениями 5G относятся ограничение условий предоставления услуги, управление черным списком входящих сообщений и управление черным списком исходящих сообщений.

Рисунок 1 – Архитектура требований безопасности для услуги обмена сообщениями 5G

6.3 Функциональные различия между требованиями безопасности для услуги обмена сообщениями 5G и для услуг обмена сообщениями 4G/3G/5G/WLAN

Разница между услугой обмена сообщениями 5G и традиционными услугами обмена сообщениями SMS заключается в том, что если традиционные SMS позволяют передавать только текст, то сообщение 5G может содержать различные типы мультимедиа, включая текст (в том числе значки настроения), эскизы, изображения, аудио, видео, информацию о местоположении, контактную информацию и документы.

При использовании услуги обмена сообщениями 5G терминалы могут получать доступ к функциональным модулям через сети 3G, 4G, 5G или беспроводную локальную сеть (WLAN). Получив доступ к сети, терминалы сначала получают параметры услуги от сервера конфигурации, а затем инициируют процесс регистрации протокола инициации сеанса (SIP) в точке доступа. После успешной регистрации они могут отправлять и получать сообщения 5G, включая личные и деловые сообщения.

Архитектура требований безопасности сообщений 5G, описанная в пункте 6.2, обеспечивает архитектуру защиты сообщений 5G. Услуги обмена сообщениями 5G должны быть защищены независимо от режима работы сети, через которую осуществляется доступ к терминалам.

7 Требования безопасности для доступа к услуге обмена сообщениями 5G

7.1 Требования безопасности при создании и изменении карт пользователей

Если пользователям услуг передачи голоса по сети LTE (VoLTE) и услуг обмена сообщениями 5G понадобится заменить карту модуля идентификации абонента (SIM-карту) вследствие ее утери/кражи, необходимо, чтобы центр обмена сообщениями 5G произвел обновление соответствующей информации, с тем чтобы пользователи могли беспрепятственно пользоваться услугой обмена сообщениями 5G после замены SIM-карты.

7.2 Аутентификация пользователей

Необходимо, чтобы аутентификация пользователей на линии отправитель–получатель сообщения соответствовала требованиям аутентификации и чтобы платформа услуг предоставляла услуги обмена сообщениями 5G только аутентифицированным пользователям.

7.2.1 Персональная аутентификация пользователей

Для обмена сообщениями 5G используются разные методы предоставления услуг, соответствующие различным механизмам аутентификации пользователей. В таблице 1 приведены типы услуг обмена сообщениями 5G и связанные с ними требования к безопасности процедур аутентификации.

Таблица 1 – Требования к безопасности процедур аутентификации для услуги обмена сообщениями 5G

Услуга обмена сообщениями 5G	Требования к безопасности процедур аутентификации
Обмен сообщениями 5G (различные способы обмена мгновенными сообщениями, включая обмен сообщениями P2P, групповой обмен сообщениями в чате, обмен сообщениями с чат-ботами и другие соответствующие способы сигнализации и передачи информации)	USIM IMS AKA (регистрация SIP поддерживает аутентификацию AKA)
Обмен сообщениями 5G (хранение сообщений, включая загрузку и передачу мультимедийного контента в сообщениях)	USIM GBA_ME
Обнаружение чат-ботов	
Запрос информации о чат-боте	
Управление конфигурацией терминала	В первый раз следует проводить аутентификацию с вводом номера мобильного телефона (в сотовой сети) или использованием одноразового пароля в SMS (OTP) (вне сотовой сети), впоследствии в процессе получения конфигурации система управления конфигурацией терминала может по мере необходимости выбрать аутентификацию на основе общей архитектуры начальной загрузки (GBA). Она также может выбрать для аутентификации механизм совместной подписи. Рекомендуется, чтобы одноразовый пароль в SMS соответствовал требованиям [ETSI TS 123 040 v17.2.0].

Методы аутентификации описываются следующим образом.

a) USIM IMS AKA. Для пользователя сообщений 5G во время регистрации подсистемы IP-мультимедиа (IMS) в центре обмена сообщениями 5G этот центр получает вектор аутентификации пользователя в соответствии с соглашением об аутентификации и ключах пользователя (AKA) от принадлежащего пользователю HSS/UDM через интерфейс Zh и с помощью этого вектора аутентификации выполняет аутентификацию пользователя IMS AKA. Рекомендуется, чтобы сертификация AKA соответствовала [ETSI TS 124 229].

b) USIM GBA_ME. Требуется, чтобы терминалы поддержки сообщений 5G поддерживали интерфейсы GBA. Требуется, чтобы серверы приложений, не поддерживающие SIP, в системе обмена сообщениями 5G поддерживали интерфейсы Zn GBA. Рекомендуется, чтобы сертификация GBA соответствовала [ETSI TS 124 229].

c) Управление конфигурацией терминала. В первый раз используется аутентификация путем ввода номера мобильного телефона (в сотовой сети) или OTP SMS (вне сотовой сети) – в последующем процессе получения конфигурации. Для защиты ключей от утечки может использоваться механизм совместной подписи.

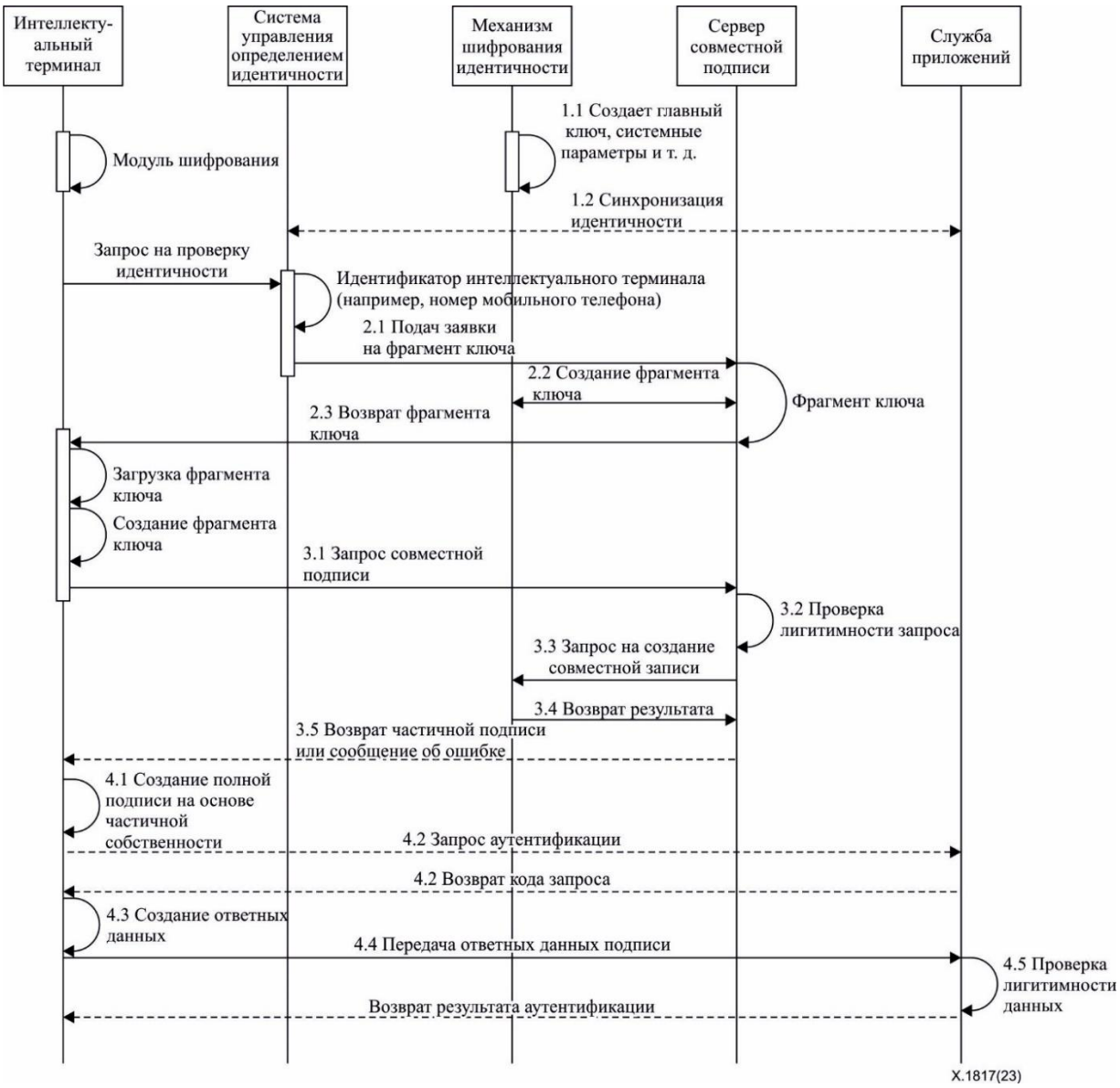

Рисунок 2 – Механизм совместной подписи для услуги обмена сообщениями 5G

Механизм совместной подписи, показанный на рисунке 2, используется для проверки идентичности сообщений 5G. Основной процесс выглядит следующим образом.

1) Механизм шифрования идентичности создает главный ключ, системные параметры и компонент ключа идентичности. Синхронизация идентичности между системой управления определением идентичности и службой приложений может выполняться на основе заранее заданного алгоритма в соответствии с главным ключом, системными параметрами и компонентом ключа идентичности. Заранее заданный алгоритм включает как минимум по одному из алгоритмов создания ключей, алгоритмов подписи и алгоритмов проверки. Выполняются следующие шаги.

- Шаг 1.1: Механизм шифрования идентичности создает главный ключ, системные параметры и компонент ключа идентичности.
- Шаг 1.2: Синхронизация идентичности между системой управления определением идентичности и службой приложений может выполняться на основе заранее заданного алгоритма в соответствии с главным ключом, системными параметрами и компонентом ключа идентичности.

2) После синхронизации идентичности между системой управления определением идентичности и службой приложений идентификатор интеллектуального терминала осуществляет проверку идентичности совместной подписи с сервером совместной подписи. Интеллектуальный терминал передает в систему управления определением идентичности идентификатор интеллектуального терминала (такой как номер мобильного телефона). Система управления определением идентичности направляет запрос ключа на сервер совместной подписи на основании идентификатора интеллектуального терминала. Сервер совместной подписи возвращает в интеллектуальный терминал фрагмент ключа на основе запроса ключа. Выполняются следующие шаги.

- Шаг 2.1: Интеллектуальный терминал инициирует запрос на проверку идентичности и запрашивает фрагмент ключа у сервера совместной подписи.
- Шаг 2.2: Сервер совместной подписи генерирует фрагмент ключа.
- Шаг 2.3: Сервер совместной подписи возвращает в интеллектуальный терминал фрагмент ключа на основе запроса ключа.

3) Интеллектуальный терминал загружает фрагмент ключа и генерирует соответствующий фрагмент подписи. Интеллектуальный терминал передает на сервер совместной подписи запрос совместной подписи на основе фрагмента подписи. Сервер совместной подписи проверяет легитимность запроса совместной подписи. Если проверка идентичности совместной подписи проходит успешно, то сервер совместной подписи перенаправляет запрос совместной подписи в механизм шифрования идентичности. Механизм шифрования идентичности генерирует частичную подпись в соответствии с запросом на совместную подпись, и сервер совместной подписи возвращает частичную подпись в интеллектуальный терминал. Выполняются следующие шаги.

- Шаг 3.1: Интеллектуальный терминал передает на сервер совместной подписи запрос совместной подписи на основе фрагмента подписи.
- Шаг 3.2: Сервер совместной подписи проверяет легитимность запроса совместной подписи.
- Шаг 3.3: Если проверка идентичности совместной подписи проходит успешно, то сервер совместной подписи перенаправляет запрос совместной подписи в механизм шифрования идентичности.
- Шаг 3.4: Механизм шифрования идентичности генерирует частичную подпись в соответствии с запросом на совместную подпись и возвращает частичную подпись на сервер совместной подписи.
- Шаг 3.5: Сервер совместной подписи возвращает частичную подпись в интеллектуальный терминал.

4) Интеллектуальный терминал генерирует полную подпись на основе частичной подписи. Процесс проверки идентичности совместной подписи со службой приложений на основе полной подписи выглядит следующим образом. Интеллектуальный терминал направляет запрос аутентификации на основе полной подписи в службу приложений. Служба приложений возвращает в интеллектуальный терминал код запроса на основе запроса аутентификации. Интеллектуальный терминал генерирует ответные данные в соответствии с фрагментом локального ключа и кодом запроса и направляет ответные данные в службу приложений. После получения ответных данных служба приложений проверяет легитимность ответных данных и идентичность интеллектуального терминала на основе полной подписи. Проверка идентичности совместной подписи завершена, и служба приложений возвращает результат аутентификации в интеллектуальный терминал. Выполняются следующие шаги.

- Шаг 4.1: Интеллектуальный терминал генерирует полную подпись на основе частичной подписи.
- Шаг 4.2: Интеллектуальный терминал направляет запрос аутентификации на основе полной подписи в службу приложений, а та отправляет в интеллектуальный терминал код запроса.
- Шаг 4.3: Интеллектуальный терминал генерирует ответные данные в соответствии с фрагментом локального ключа и кодом запроса. Фрагмент локального ключа – это фрагмент ключа, возвращаемый сервером совместной подписи.
- Шаг 4.4: Интеллектуальный терминал направляет ответные данные службе приложений.
- Шаг 4.5: Служба приложений проверяет легитимность ответных данных. Проверка идентичности совместной подписи завершена, и служба приложений возвращает результат аутентификации в интеллектуальный терминал.

7.2.2 Аутентификация сервера чат-бота

Прежде чем подключить чат-бот к платформе обмена сообщениями, чат-бот необходимо аутентифицировать. Для аутентификации используется сочетание аутентификации платформы и аутентификации на уровне приложения. Для аутентификации платформы может использоваться аутентификация цифрового сертификата на основе безопасного протокола передачи гипертекста (HTTPS), а для аутентификации на уровне приложения – метод аутентификации, основанный на имени пользователя и пароле.

Требуется, чтобы сервер чат-бота подал заявку на сертификат сервера через легитимный центр сертификации (ЦС) и предоставил платформе обмена сообщениями корневой сертификат ЦС, легитимное доменное имя или IP-адрес сервера чат-бота для проверки регистрации в процессе регистрации пользователя. По завершении регистрации платформа обмена сообщениями выполняет проверку идентичности на сервере чат-бота в процессе получения доступа к чат-боту. Аутентификация включает проверку сертификата сервера чат-бота, аутентификацию идентичности чат-бота.

7.3 Безопасность получения сообщений

Приложения для обмена сообщениями 5G могут взаимодействовать с системой терминала, чтобы гарантировать, что только приложения для обмена сообщениями 5G могут получать сообщения 5G, во избежание их злонамеренного использования и утечки личных данных из сообщений пользователей.

7.4 Безопасность передачи сообщений

Приложения для обмена сообщениями 5G могут взаимодействовать с системой терминала, чтобы гарантировать, что только приложения для обмена сообщениями 5G могут отправлять сообщения 5G, и во избежание злонамеренного использования таких сообщений разрешение на их передачу не может быть получено никакими другими приложениями.

7.5 Безопасность доступа к сообщениям

Приложения для обмена сообщениями 5G могут взаимодействовать с системами терминала для ограничения возможности санкционированного доступа к сообщениям 5G. Требуется, чтобы файл сообщения на стороне терминала читался только приложением для обмена сообщениями 5G; то же относится к другим операциям управления (таким как удаление и резервное копирование). Рекомендуется, чтобы на стороне платформы обеспечивалась возможность запроса и чтения сообщений (включая данные, относящиеся к журналу регистрации событий) только для владельца сообщения и чтобы другим пользователям (включая администраторов) доступ был, как правило, запрещен.

8 Требования безопасности при управлении услугами обмена сообщениями 5G

8.1 Безопасность управления пользователями

8.1.1 Разделение ролей и разрешений

Система безопасности управления пользователями разделяет платформу услуг на уровни и зоны в соответствии с функциями зонирования и привилегиями модулей обслуживания. Рекомендуется настроить учетную запись администратора в соответствии с различными привилегиями, включая привилегии суперадминистратора, администратора услуги и контролера.

a) Суперадминистраторы обладают расширенными полномочиями по управлению платформой функций услуги, то есть могут управлять администраторами и контролерами услуги.

b) Администраторы услуги имеют частичные или полные полномочия для управления услугой и ее функционированием. Однако администраторы услуги не могут получить права контроля или управления по отношению к другим администраторам услуг.

c) Контролеры имеют полномочия на проведение проверок регистрации и функционирования, но не на обработку услуг.

8.1.2 Мониторинг аномального поведения

Мониторинг и контроль некоторых аномальных действий, таких как аномальный вход в систему, одновременный вход из нескольких мест, отправка чрезмерного количества сообщений (чтобы классифицировать действие как спам). В случае таких видов аномального поведения необходимо предпринять соответствующие меры (например, добавить учетную запись в черный список и заблокировать ее), чтобы ограничить возможности таких аномальных пользователей.

8.2 Управление ключами и сертификатами

8.2.1 Управление ключами

Управление ключами – это механизм управления, с помощью которого терминал обмена сообщениями 5G и платформа услуги управляют своими ключами шифрования конфиденциальных данных. Рекомендуется иметь в наличии набор различных ключей шифрования для разных типов конфиденциальных данных, которые можно использовать, когда на стороне платформы или на стороне терминала осуществляется хранение зашифрованных конфиденциальных данных. Рекомендуется, чтобы требования к управлению ключами соответствовали [ISO/IEC 11770-1].

Система обмена сообщениями 5G может создавать соответствующие ключи для защиты различных объектов, включая как минимум типы ключей, указанные в таблице 2.

Таблица 2 – Типы и описания ключей системы обмена сообщениями 5G

Тип	Описание
Ключ безопасного хранения данных	Защищает сохраненные важные данные и конфиденциальную информацию
Ключ безопасной передачи данных	Ключ GBA генерируется в процессе аутентификации при входе в систему терминала и ряда платформ посредством процесса GBA (специальный метод генерирования), и рекомендуется, чтобы требования соответствовали требованиям аутентификации GBA [ETSI TS 129 109]
Ключ шифрования удостоверяющей информации пользователя	Защита удостоверяющей информации пользователя
Ключ шифрования данных ключей	Защита данных, относящихся к ключам
Ключ безопасной передачи данных	Защищает важные данные и конфиденциальную информацию при передаче

8.2.2 Управление сертификатами

Для реализации безопасных соединений HTTPS в веб-сервере должен быть настроен цифровой сертификат, удостоверяющий способ использования сервера. Для серверов, в которых необходимо настроить цифровые сертификаты, при наличии нескольких доменных имен необходимо подать заявку на получение сертификата сервера для каждого доменного имени. Если для предоставления услуг сервер использует IP и имеет несколько IP-адресов, необходимо подать заявку на сертификат сервера для каждого IP-адреса; эти типы сертификатов указаны в таблице 3.

Таблица 3 – Описание конфигурации сертификатов сервера системы обмена сообщениями 5G

Наименование сервера	Способ доступа	Тип сертификата
5GMC	Доменное имя	Обычный SSL-сертификат (требуется, чтобы в терминале был предварительно установлен корневой сертификат ЦС)
Платформа обмена сообщениями	Доменное имя	Обычный SSL-сертификат (требуется, чтобы в терминале был предварительно установлен корневой сертификат ЦС)
Модуль управления платформой обмена сообщениями	Доменное имя	Обычный SSL-сертификат
Чат-бот	Доменное имя	Обычный SSL-сертификат

8.3 Контроль безопасности

Журналы регистрации событий – это записи о важных видах поведения пользователей, аномальном использовании системных ресурсов и использовании важных команд платформы. Записи могут включать дату и время, тип, идентификатор субъекта, идентификатор объекта и результаты события. Контент, который может быть записан в журнал регистрации событий безопасности услуги, включает, помимо прочего, журналы регистрации действий пользователей, журналы регистрации действий администраторов и журналы регистрации событий, относящихся к услуге.

a) Журналы регистрации действий пользователей. В них записываются действия и их результаты, относящиеся к учетной записи, действия и их результаты, относящиеся к услуге, и т. п. Журналы регистрации действий пользователей могут включать информацию о пользователе, действиях пользователя, объектах этих действий, времени действий, результатах действий, аномальных результатах и т. д.

b) Журналы регистрации действий администраторов. В них записываются действия и их результаты, относящиеся к учетной записи, действия и их результаты, относящиеся к услуге, и т. п. Журналы регистрации действий администраторов могут включать информацию об администраторе, действиях администратора, объектах этих действий, времени, результатах, аномальных результатах и т. д.

c) Журналы регистрации событий, относящихся к услуге. Рекомендуется, чтобы системы могли вести журналы регистрации событий, относящихся к услугам. Платформа может хранить все виды журналов в течение определенного времени для онлайн-запроса в зависимости от требований; для тех журналов, для которых требования ко времени онлайн-хранения недостаточно, можно указать время автономного хранения. Онлайн-журналы хранятся в базе данных или системным методом. Платформа услуг управляет правами доступа и может просматриваться, экспортироваться или проверяться только назначенным администратором (контролером); автономные журналы можно импортировать в систему или использовать специальные инструменты для запросов, проверки и других операций. После экспорта автономные журналы, содержащие конфиденциальные данные, могут храниться в зашифрованных файлах.

8.4 Безопасность управления программным обеспечением

8.4.1 Безопасность управления разработкой программного обеспечения для обмена сообщениями 5G

Требуется, чтобы принципы безопасного кодирования системы услуги обмена сообщениями 5G предусматривали:

a) проверку эффективности входных данных пользователя, фильтрацию конфиденциальных символов;

b) шифрование хранимых конфиденциальных данных, таких как пароли;

c) передачу конфиденциальных данных, таких как имена пользователей и пароли, по протоколу HTTPS;

d) запрет прямых обращений к системным ресурсам, таким как файлы;

e) запрет использования оболочек в кодах, относящихся к Web;

f) использование функции безопасности при программировании.

8.4.2 Безопасность управления работой системы обмена сообщениями 5G

Система обмена сообщениями 5G способна контролировать важные процессы и логику обработки услуг и подавать сигнал тревоги при обнаружении ошибок.

9 Требования безопасности при управлении услугой обмена сообщениями 5G

9.1 Ограничение возможностей услуги

К ограничениям возможностей услуги относятся ограничение количества участников группы, дифференцированное управление групповыми функциями и ограничение групповых чатов.

a) Ограничение количества участников группы. При групповой отправке сообщений 5G должен быть установлен верхний предел количества участников групповой отправки, чтобы ограничить возможные неблагоприятные последствия.

b) Дифференцированное управление групповыми функциями. Платформы услуг могут поддерживать дифференцированное управление количеством вызываемых пользователей групповой услуги.

c) Ограничения групповых чатов. Платформы услуг могут поддерживать ограничение масштаба использования групповых чатов, настройку параметров управления количеством пользователей в группе, а также ограничение на длину названия группы.

9.2 Черный список входящих сообщений

Для сообщений, исходящих от мобильных устройств (MO) 5G, необходимо добавить функцию контроля аутентификации по черному списку входящих сообщений, чтобы предотвратить риск бомбардировки сообщениями 5G. С помощью системы, контролирующей флейм (агрессивная дискуссия), в групповых чатах может быть создан механизм мониторинга, способный анализировать признаки вредоносных массовых сообщений, которые будут добавляться в черный список входящих сообщений автоматически, методом ручной проверки и другими способами. Тогда система управления черным списком входящих сообщений сможет перехватывать вредоносные сообщения, направляемые в группу, и управлять ими.

9.3 Черный список исходящих сообщений

Для сообщений, направляемых в мобильные устройства (MT) 5G, необходимо добавить так называемый черный список исходящих сообщений, чтобы уменьшить вероятность жалоб пользователей приемных мобильных устройств. Отдельные пользователи могут пожаловаться или составить черный список исходящих сообщений, позвонив в службу поддержки клиентов, войдя в интерфейс самообслуживания, посетив зал обслуживания и другими способами. С помощью системы, контролирующей флейм, или соответствующих систем, относящихся к услуге, может быть создан механизм управления черным списком исходящих сообщений, способный перехватывать сообщения пользователей, соответствующие указанному пользователю или типу услуги.

Библиография

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

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2024 г.