ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

UIT-T X.1817 (09/2023)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Sécurité des IMT-2020

Exigences de sécurité relatives au service de messagerie de la 5G

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	X.1100-X.1199
APPLICATIONS ET SERVICES SÉCURISÉS (1)	X.1200-X.1299
SÉCURITÉ DU CYBERESPACE	X.1300-X.1499
APPLICATIONS ET SERVICES SÉCURISÉS (2)	X.1500-X.1599
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	X.1600-X.1699
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	X.1700-X.1729
COMMUNICATIONS QUANTIQUES	X.1750-X.1799
SÉCURITÉ DES DONNÉES	X.1100-X.1199
SÉCURITÉ DES IMT-2020	**X.1800–X.1819**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1817

Exigences de sécurité relatives au service de messagerie de la 5G

Résumé

La Recommandation UIT-T X.1817 énonce les exigences de sécurité relatives au service de messagerie de la 5G, y compris les exigences en matière d'utilisation sécurisée, les exigences en matière de gestion sécurisée et les exigences en matière de contrôle sécurisé relatives au service de messagerie de la 5G.

Historique[*]

Édition	Recommandation	Approbation	Commission d'études	ID unique
1.0	UIT-T X.1817	08-09-2023	17	11.1002/1000/15524

Mots clés

Service de messagerie de la 5G, cadre de sécurité, exigence de sécurité.

[*] Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur web, suivi de l'identifiant unique.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1817

Exigences de sécurité relatives au service de messagerie de la 5G

1 Domaine d'application

Le service de messagerie de la 5G est une amélioration du service de messages courts (SMS). Il s'agit de l'un des services de télécommunications d'entreprises de base, qui comprend le service de messages courts (SMS) défini par le 3GPP, et le service de communication enrichi (RCS) défini par la GSMA. Il prend notamment en charge les messages entre personnes ou entre applications et personnes, ainsi que divers médias (texte long, image, vidéo, audio, fichier et position). La présente Recommandation décrit les exigences de sécurité susceptibles d'atténuer les menaces et les problèmes de sécurité liés au service de messagerie de la 5G. La présente Recommandation énonce les exigences de sécurité relatives au service de messagerie de la 5G, y compris les exigences en matière d'accès sécurisé, les exigences en matière de gestion sécurisée et les exigences en matière de contrôle sécurisé relatives au service de messagerie de la 5G. La présente Recommandation décrit également les différences fonctionnelles entre les exigences de sécurité du service de messagerie de la 5G et celles des services 4G/3G/5G/WLAN.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont donc invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[ETSI TS 123 040] ETSI TS 123 040 v17.2.0 (2022), *système de télécommunication numérique cellulaire (phase 2+) GSM; système de télécommunications mobiles universelles (UMTS); LTE; 5G; réalisation technique du service de messages courts (SMS).*

[ETSI TS 124 229] ETSI TS 124 229 (2017), *système de télécommunication numérique cellulaire (phase 2+); système de télécommunications mobiles universelles (UMTS); LTE; protocole de commande d'appel multimédia IP fondé sur le protocole d'initiation de session (SIP) et sur le protocole de description de session (SDP); stade 3.*

[ETSI TS 129 109] ETSI TS 129 109 (2018), s*ystème de télécommunication cellulaire numérique (phase 2+); système de télécommunications mobiles universelles (UMTS); LTE; architecture d'authentification générique (GAA); interfaces Zh et Zn basées sur le protocole Diameter; stade 3.*

[ISO/CEI 11770-1] ISO/CEI 11770-1:2010, *Technologies de l'information – Techniques de sécurité – Gestion de clés – Partie 1*: *Cadre général*.

3 Définitions

3.1 Termes définis ailleurs

La présente recommandation utilise le terme suivant défini ailleurs:

3.1.1 agent conversationnel [b-GSMA RCC.71]: service automatisé basé sur le service de messagerie enrichi (*Rich Communication Service*, RCS) fourni aux utilisateurs et dont les résultats sont présentés sous forme de conversation.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 centre de messagerie 5G: serveur fournissant le service de messagerie de la 5G.

3.2.2 plate-forme de messagerie: plate-forme permettant aux applications tierces de se connecter au centre de messagerie 5G.

3.2.3 équipement d'utilisateur (*user equipment*, UE) de messagerie 5G: équipement d'utilisateur (UE) 5G dont l'application de messagerie prend en charge à la fois le service de messages courts (SMS) et le service de communication enrichi (RCS).

3.2.4 service de messagerie de la 5G: service de messagerie 5G comprenant un service de messages courts (SMS) et un service de communication enrichi (RCS). Le service de messagerie de la 5G prend en charge les messages entre les personnes ou entre les applications et les personnes, ainsi que divers médias (texte long, image, vidéo, audio, fichier et position).

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

3GPP Projet de partenariat de 3ème génération (*3rd generation partnership project*)

A2P de l'application à la personne (*application to person*)

AKA authentification et concordance de clés (*authentication and key agreement*)

GBA architecture d'amorçage générique (*generic bootstrapping architecture*)

GSMA Global System for Mobile communications Association

HSS service d'abonné de rattachement (*home subscriber service*)

HTTPS protocole de transport hypertexte sécurisé (*hypertext transfer protocol secure*)

IMS sous-système multimédia IP (*IP multimedia subsystem*)

MO au départ du mobile (*mobile originate*)

MT à destination d'un mobile (*mobile terminate*)

OTP mot de passe à usage unique (*one time password*)

P2P de personne à personne (*person to person*)

RCS service de communication enrichi (*rich communication service*)

SIM module d'identité d'abonné (*subscriber identity module*)

SIP protocole d'initiation de session (*session initiation protocol*)

SMS service de messages courts (*short message service*)

UE équipement d'utilisateur (*user equipment*)

UDM gestion de données unifiée (*unified data management*)

VoLTE téléphonie utilisant la technologie LTE (évolution à long terme) (*voice over long term evolution*)

WLAN réseau local sans fil (*wireless local area network*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

L'expression "**il est obligatoire**" indique une exigence qui doit être strictement suivie, et par rapport à laquelle aucun écart n'est autorisé pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "**il est recommandé**" indique une exigence qui est recommandée mais qui n'est pas absolument obligatoire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

6 Vue d'ensemble

6.1 Service de messagerie de la 5G

Le service de messagerie de la 5G, qui suit le profil universel du service de communication enrichi (RCS) de la GSMA, fournit des services avancés tels que la messagerie multimédia, les conversations de groupe et la plate-forme de messagerie. Le service de messagerie de la 5G est basé sur le portail natif du service de messages courts (SMS) du terminal, permettant aux utilisateurs d'envoyer et de recevoir du texte, des images, de l'audio, de la vidéo, des données de localisation, des informations sur les contacts et d'autres contenus multimédias, y compris les fonctions de service suivantes:

- Messages de personne à personne (P2P)

Les messages P2P sont des messages envoyés entre utilisateurs individuels, qui prennent en charge les contenus média suivants: texte (y compris les émoticônes), images, audio, vidéo, localisation, contacts (vCard) et documents.

- Messages du groupe

Un message de groupe est un message envoyé par un utilisateur individuel à plusieurs autres utilisateurs individuels en même temps. L'utilisateur peut saisir plusieurs numéros de contact à la fois ou sélectionner plusieurs destinataires dans le carnet d'adresses pour envoyer un message groupé à plusieurs destinataires. Chaque destinataire reçoit un message dans lequel apparaît le même contenu, le numéro de l'expéditeur est son véritable numéro de téléphone mobile, et le destinataire peut répondre directement au message à l'expéditeur dans un message P2P.

- Messages de conversation de groupe

Un message de conversation de groupe est un message interactif entre tous les utilisateurs individuels qui rejoignent le groupe.

- Messages d'application à personne (A2P)

Tout message créé à l'aide d'une application et destiné à un équipement mobile détenu par une personne est appelé messagerie A2P. La messagerie A2P permet aux marques de communiquer avec les utilisateurs par le biais d'un agent conversationnel. Les utilisateurs peuvent envoyer des messages RCS à l'agent conversationnel, notamment du texte (y compris des émoticônes), des images, de l'audio, de la vidéo, des données de localisation, des contacts (vCard) et des documents. Les agents conversationnels peuvent envoyer des messages aux utilisateurs en mode "point à point" ou "point à multipoint", et envoyer des messages enrichis comprenant du texte (y compris des émoticônes), des images, de l'audio, de la vidéo, des données de localisation, des contacts (vCard) et des documents. L'agent conversationnel peut envoyer des "cartes enrichies" qui fournissent une "liste de puces suggérées" composée de "réponses et d'actions suggérées".

6.2 Architecture des exigences de sécurité relatives au service de messagerie de la 5G

La Figure 1 montre l'architecture des exigences de sécurité relatives au service de messagerie de la 5G, qui comprend les exigences de sécurité du plan utilisateur, les exigences de sécurité relatives au plan de gestion et les exigences de sécurité relatives au plan de contrôle du service de messagerie de la 5G.

Les exigences de sécurité relatives au plan utilisateur du service de messagerie de la 5G comprennent l'exigence de sécurité d'une carte d'utilisateur destinée à la configuration ou à la modification, l'authentification de l'utilisateur, la réception sécurisée des messages, l'envoi sécurisé des messages et l'accès sécurisé aux messages.

Les exigences de sécurité relatives au plan de gestion du service de messagerie de la 5G comprennent la sécurité de la gestion des utilisateurs, la gestion des clés et des certificats, l'audit de sécurité et la sécurité de la gestion des logiciels.

Les exigences de sécurité relatives au plan de contrôle du service de messagerie de la 5G comprennent la restriction de la capacité de service, le contrôle de la liste noire des appelants et le contrôle de la liste noire des utilisateurs appelés.

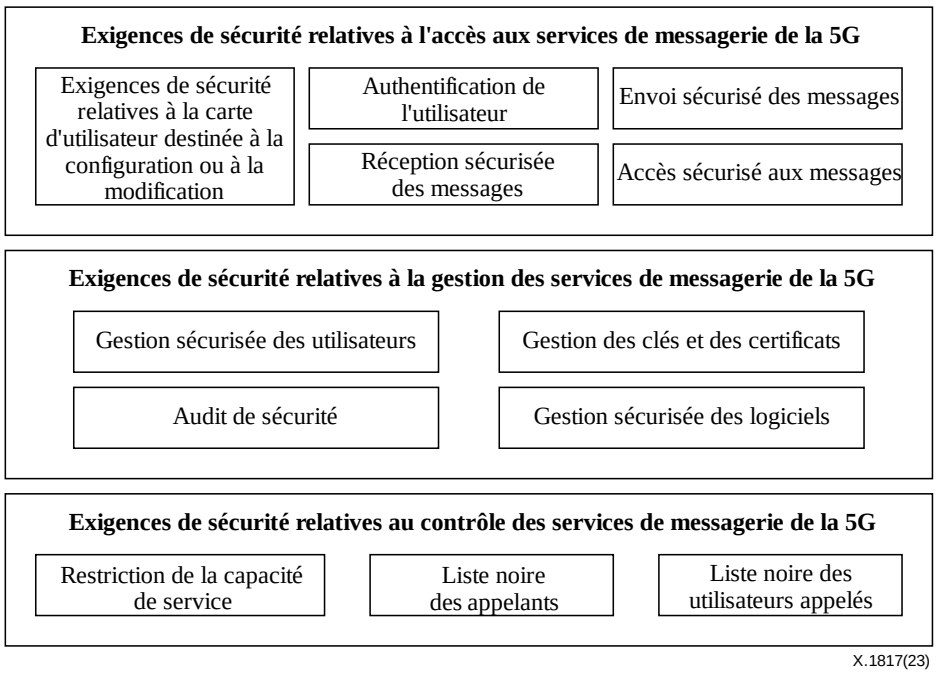

Figure 1 – Architecture des exigences de sécurité relatives au service de messagerie de la 5G

6.3 Différence fonctionnelle entre les exigences de sécurité relatives aux services de messagerie 5G et 4G/3G/5G/WLAN

La différence entre le service de messagerie de la 5G et le message SMS traditionnel réside en ce que le SMS traditionnel ne peut envoyer que du texte, tandis que le message 5G peut envoyer une variété de types de médias, notamment du texte (y compris des émoticônes), des vignettes, des images, de l'audio, de la vidéo, des données de localisation, des contacts et des documents.

Lors de l'utilisation des services de messagerie de la 5G, les terminaux peuvent accéder aux modules de fonction via les réseaux 3G, 4G, 5G ou le réseau local sans fil (WLAN). Après avoir accédé au réseau, les terminaux obtiennent d'abord les paramètres de service auprès du serveur de configuration, puis lancent une procédure d'enregistrement du protocole d'initiation de session (SIP) auprès du point d'accès. Une fois l'enregistrement réussi, les terminaux peuvent envoyer et recevoir des messages 5G, y compris des messages personnels et des messages sectoriels.

L'architecture des exigences de sécurité relatives aux messages de la 5G décrite dans le § 6.2 précise l'architecture de protection de la sécurité des messages de la 5G. Les services de messagerie de la 5G seront protégés quel que soit le mode de réseau par lequel les terminaux sont accessibles.

7 Exigences de sécurité relatives à l'accès aux services de messagerie de la 5G

7.1 Exigences de sécurité relatives à la carte d'utilisateur destinée à la configuration ou à la modification

Concernant les utilisateurs de la téléphonie utilisant la technologie LTE (évolution à long terme) (VoLTE) et du service de messagerie de la 5G qui doivent changer leur module d'identité d'abonné (carte SIM) en raison de la perte irrémédiable de la carte SIM perdue ou volée, il est recommandé que le centre de messagerie 5G mette à jour/rafraîchisse les informations correspondantes, afin que les utilisateurs puissent utiliser le service de messagerie de la 5G dans de bonnes conditions après avoir changé de carte SIM.

7.2 Authentification de l'utilisateur

Il est obligatoire que l'authentification de l'utilisateur entre l'expéditeur et le destinataire du message remplisse les conditions d'authentification, et que la plate-forme de service n'ouvre le service de messagerie 5G qu'aux utilisateurs authentifiés.

7.2.1 Authentification personnelle de l'utilisateur

Les messages 5G impliquent une variété de méthodes de mise en œuvre des services, correspondant à une variété de mécanismes d'authentification des utilisateurs. Les types de services de messagerie de la 5G et les exigences d'authentification sécurisée correspondantes sont présentés dans le Tableau 1.

Tableau 1 – Exigences en matière d'authentification sécurisée des services de messagerie de la 5G

Service de messagerie de la 5G	Exigences en matière d'authentification sécurisée
Messagerie 5G (diverses interactions de messagerie instantanée, y compris la messagerie P2P, les conversations de groupe, la messagerie par agent conversationnel et autres signalisations et médias connexes)	USIM IMS AKA (l'enregistrement SIP prend en charge l'authentification AKA)
Messagerie 5G (stockage des messages, y compris le chargement et le téléchargement de contenus multimédias dans les messages)	USIM GBA_ME
Découverte d'agents conversationnels	
Demande d'informations par un agent conversationnel	
Gestion de la configuration des terminaux	Pour la première fois, utilisation de l'authentification par insertion du numéro de téléphone mobile (réseau cellulaire) ou mot de passe à usage unique (OTP) par SMS (réseau non cellulaire). Lors du processus ultérieur d'obtention de la configuration, la gestion de la configuration du terminal peut choisir l'authentification par l'architecture d'amorçage générique (GBA) en fonction des besoins. Elle peut également sélectionner le mécanisme de signature

Tableau 1 – Exigences en matière d'authentification sécurisée des services de messagerie de la 5G

Service de messagerie de la 5G	Exigences en matière d'authentification sécurisée
	collaborative pour l'authentification. Il est recommandé que le mot de passe à usage unique envoyé par SMS soit conforme à [ETSI TS 123 040 v17.2.0].

Les méthodes d'authentification sont décrites ci-dessous:

a) USIM IMS AKA: Pour un utilisateur de messages 5G, pendant l'enregistrement du sous-système multimédia IP (IMS) auprès du centre de messagerie 5G, le centre de messagerie 5G obtient le vecteur d'authentification et de concordance de clés (AKA) de l'utilisateur auprès du HSS/UDM de l'utilisateur par l'intermédiaire de l'interface Zh, et procède à l'authentification IMS AKA de l'utilisateur sur la base du vecteur d'authentification. Il est recommandé que la certification AKA soit conforme à [ETSI TS 124 229].

b) USIM GBA_ME: Les terminaux qui prennent en charge les messages 5G doivent être dotés d'interfaces GBA. Les serveurs d'application non-SIP du système de messagerie 5G doivent prendre en charge les interfaces GBA Zn. Il est recommandé que la certification ACS soit conforme à [ETSI TS 124 229].

c) Gestion de la configuration des terminaux: Pour la première fois, utilisation de l'authentification par insertion du numéro de téléphone mobile (réseau cellulaire) ou SMS OTP (réseau non cellulaire), dans le processus ultérieur d'obtention de la configuration. Pour protéger les clés contre les fuites, elle peut utiliser le mécanisme de signature collaborative.

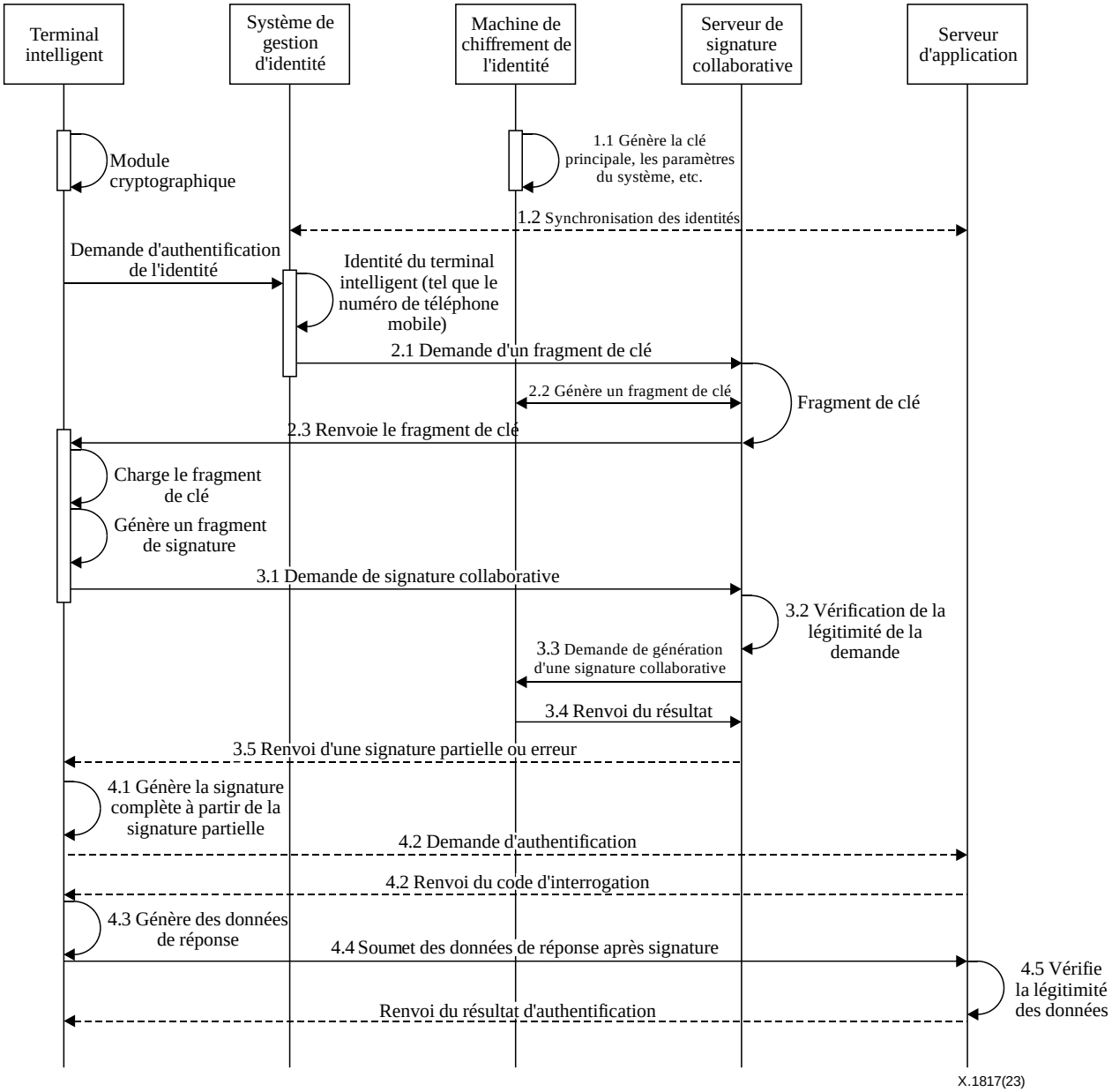

Figure 2 – Mécanisme de signature collaborative pour le service de messagerie de la 5G

Le mécanisme de signature collaborative illustré à la Figure 2 est utilisé dans le cadre de l'authentification de l'identité dans les messages 5G. Le processus principal est le suivant:

1) La machine de chiffrement de l'identité génère la clé principale, les paramètres du système et le composant de la clé d'identité. La synchronisation de l'identité entre le système de gestion de l'identité et le service d'application peut être effectuée sur la base de l'algorithme prédéfini en fonction de la clé principale, des paramètres du système et du composant de la clé d'identité. L'algorithme prédéfini comprend au moins l'un des algorithmes de génération de clés, de signature et de vérification. Les étapes sont décrites ci-dessous:
   - Étape 1.1: La machine de chiffrement de l'identité génère la clé principale, les paramètres du système et le composant de la clé d'identité.
   - Étape 1.2: La synchronisation de l'identité entre le système de gestion de l'identité et le service d'application peut être effectuée sur la base de l'algorithme prédéfini en fonction de la clé principale, des paramètres du système et du composant de la clé d'identité.

2) Après synchronisation de l'identité entre le système de gestion de l'identité et le service d'application, l'identité du terminal intelligent est utilisée pour l'authentification de l'identité de la signature collaborative avec le serveur de signature collaborative. Le terminal intelligent envoie l'identité du terminal intelligent (tel que le numéro de téléphone mobile) au système de gestion de l'identité. Le système de gestion de l'identité envoie la demande de clé au serveur de signature collaborative selon l'identité du terminal intelligent. Le serveur de signature collaborative renvoie le fragment de clé au terminal intelligent en fonction de la demande de clé. Les étapes sont décrites ci-dessous:

- Étape 2.1: Le terminal intelligent lance une demande d'authentification d'identité et demande un fragment de clé au serveur de signature collaborative.
- Étape 2.2: Le serveur de signature collaborative génère le fragment de clé.
- Étape 2.3: Le serveur de signature collaborative renvoie le fragment de clé au terminal intelligent en fonction de la demande de clé.

3) Le terminal intelligent charge le fragment de clé et génère le fragment de signature correspondant. Le terminal intelligent envoie une demande de signature collaborative au serveur de signature collaborative sur la base du fragment de signature. Le serveur de signature collaborative vérifie la légitimité de la demande de signature collaborative. Lorsque l'authentification de l'identité de la signature collaborative est réussie, le serveur de signature collaborative transmet la demande de signature collaborative à la machine de chiffrement de l'identité. La machine de chiffrement de l'identité génère une signature partielle en fonction de la demande de signature collaborative, et le serveur de signature collaborative renvoie la signature partielle au terminal intelligent. Les étapes sont décrites ci-dessous:

- Étape 3.1: Le terminal intelligent envoie une demande de signature collaborative au serveur de signature collaborative sur la base du fragment de signature.
- Étape 3.2: Le serveur de signature collaborative vérifie la légitimité de la demande de signature collaborative.
- Étape 3.3: Lorsque l'authentification de l'identité de la signature collaborative est réussie, le serveur de signature collaborative transmet la demande de signature collaborative à la machine de chiffrement de l'identité.
- Étape 3.4: La machine de chiffrement de l'identité génère une signature partielle en fonction de la demande de signature collaborative, et renvoie la signature partielle au terminal intelligent.
- Étape 3.5: Le serveur de signature collaborative renvoie la signature partielle au terminal intelligent.

4) Le terminal intelligent génère une signature complète sur la base de la signature partielle. Le processus d'authentification de l'identité par signature conjointe avec le service d'application basé sur la signature complète est le suivant. Le terminal intelligent envoie une demande d'authentification au service d'application sur la base de la signature complète. Le service d'application renvoie un code d'interrogation au terminal intelligent en fonction de la demande d'authentification. Le terminal intelligent génère des données de réponse en fonction du fragment de clé locale et du code d'interrogation, et envoie les données de réponse au service d'application. Après avoir reçu les données de réponse, le service d'application vérifie la légitimité des données de réponse et l'identité du terminal intelligent sur la base de la signature complète. L'authentification de l'identité par signature conjointe est terminée et le service d'application renvoie le résultat de l'authentification au terminal intelligent. Les étapes sont décrites ci-dessous:

- Étape 4.1: Le terminal intelligent génère la signature complète à partir de la signature partielle.

- Étape 4.2: Le terminal intelligent envoie une demande d'authentification au service d'application sur la base de la signature complète, et le service d'application envoie un code d'interrogation au terminal intelligent.
- Étape 4.3: Le terminal intelligent génère des données de réponse en fonction du fragment de clé locale et du code d'interrogation. Le fragment de clé locale est le fragment de clé qui est renvoyé par le serveur de signature collaboratif.
- Étape 4.4: Le terminal intelligent envoie les données de réponse au service d'application.
- Étape 4.5: Le service d'application vérifie la légitimité des données de réponse. L'authentification de l'identité par signature conjointe est terminée et le service d'application renvoie le résultat de l'authentification au terminal intelligent.

7.2.2 Authentification du serveur de l'agent conversationnel

Avant que l'agent conversationnel ne soit connecté à la plate-forme de messagerie, il doit être authentifié. L'authentification adopte une combinaison d'authentification de plate-forme et d'authentification de couche d'application. L'authentification de la plate-forme peut utiliser l'authentification par certificat numérique basée sur le protocole de transfert hypertexte sécurisé (HTTPS), et l'authentification de la couche application peut utiliser l'authentification basée sur un nom d'utilisateur et un mot de passe.

Le serveur de l'agent conversationnel doit demander un certificat de serveur auprès d'une autorité de certification (CA) légale et fournir le certificat racine de la CA, le nom de domaine légal ou l'adresse IP du serveur de l'agent conversationnel à la plate-forme de messagerie pour examen de l'enregistrement au cours de la procédure d'enregistrement de l'utilisateur. Une fois l'enregistrement terminé, la plate-forme de messagerie procède à l'authentification de l'identité sur le serveur de l'agent conversationnel au cours de la procédure d'accès à l'agent conversationnel. L'authentification comprend la vérification du certificat du serveur de l'agent conversationnel, l'authentification de l'identité de l'agent conversationnel, etc.

7.3 Réception sécurisée des messages

Les applications de messagerie 5G pourraient coopérer avec le système terminal pour s'assurer que seules les applications de messagerie 5G puissent recevoir des messages 5G, afin de garantir qu'ils ne seront pas utilisés de manière malveillante et que les données privées des messages des utilisateurs ne soient pas divulguées.

7.4 Envoi sécurisé des messages

Les applications de messagerie 5G pourraient coopérer avec le système terminal pour s'assurer que seules les applications de messagerie 5G puissent envoyer des messages 5G, et que la permission d'envoyer des messages ne peut pas être accordée à d'autres applications afin de garantir qu'elles ne soient pas utilisées à des fins malveillantes.

7.5 Accès sécurisé aux messages

Les applications de messagerie 5G pourraient coopérer avec les systèmes de terminaux pour restreindre les capacités d'accès autorisé aux messages 5G. Il est obligatoire que le fichier de messages du côté du terminal ne soit lu que par l'application de messagerie 5G ou effectue d'autres opérations de gestion (telles que la suppression et la sauvegarde). Il est recommandé que le message du côté de la plate-forme permette la consultation et la lecture (y compris les données liées au journal) pour le propriétaire du message, et que les autres utilisateurs (y compris les administrateurs) n'y aient généralement pas accès.

8 Exigences de sécurité relatives à la gestion des services de messagerie de la 5G

8.1 Sécurité de la gestion des utilisateurs

8.1.1 Répartition des rôles et des permissions

La sécurité de la gestion des utilisateurs divise la plate-forme de services en couches et en zones selon les fonctions de zonage et de privilège des modules de services. Il est recommandé de définir un compte d'administrateur en fonction de différents privilèges, notamment super administrateur, administrateur de services et auditeur:

a) Super administrateurs: ils disposent d'une autorité de gestion avancée concernant la plate-forme de fonction de service, ce qui signifie qu'ils peuvent gérer les administrateurs de service et les auditeurs.

b) Administrateurs de services: ils sont partiellement ou totalement responsables de la gestion et de l'exploitation des services. Cependant, les administrateurs de services ne sont pas responsables de l'audit ou de la gestion d'autres administrateurs de services.

c) Auditeurs: ils sont habilités à effectuer des audits d'enregistrement et des audits de fonctionnement, sans toutefois pouvoir traiter des services.

8.1.2 Contrôle des comportements anormaux

Surveillance et audit de certains comportements anormaux tels que les connexions anormales, les connexions à plusieurs endroits en même temps, l'envoi de messages au-delà d'un certain seuil (pour catégoriser l'action comme du spam). Concernant ces comportements anormaux, il est nécessaire de prendre des mesures (par exemple, ajouter à la liste noire et geler le compte), afin de restreindre ces utilisateurs aux comportements anormaux.

8.2 Gestion des clés et des certificats

8.2.1 Gestion des clés

La gestion des clés est le mécanisme de gestion par lequel le terminal de messagerie 5G et la plate-forme de service gèrent leurs clés de chiffrement de données sensibles. Il est recommandé de disposer d'un ensemble de clés de chiffrement différentes pour les différents types de données sensibles, qui pourraient être utilisées lorsque la plate-forme ou le terminal stocke les données sensibles de manière chiffrée. Il est recommandé que les exigences en matière de gestion des clés soient conformes à la norme [ISO/IEC 11770-1].

Le système de messagerie 5G pourrait concevoir des clés correspondantes pour protéger différents objets, y compris au moins les types de clés suivants présentés dans le Tableau 2:

Tableau 2 – Types et descriptions des clés du système de messagerie 5G

Types	Descriptions
Clé de stockage sécurisé des données	Protéger les données importantes stockées et les informations sensibles.
Clé de communication sécurisée	La clé GBA est générée au cours du processus d'authentification de connexion du terminal et des plates-formes multiples par le biais du processus GBA (méthode de génération spécifique). En outre, il est recommandé que les exigences soient conformes à l'authentification GBA dans [ETSI TS 129 109].
Clé de chiffrement des informations d'identification de l'utilisateur	Protéger les informations d'identification de l'utilisateur.

Tableau 2 – Types et descriptions des clés du système de messagerie 5G

Types	Descriptions
Clé de chiffrement des données	Protéger les données liées aux clés.
Clé de transfert sécurisé des données	Protéger les données importantes et les informations sensibles en transit.

8.2.2 Gestion des certificats

Pour mettre en œuvre les connexions sécurisées HTTPS, le serveur web doit être configuré avec un certificat numérique qui certifie le type d'utilisation du serveur. Pour les serveurs qui doivent être configurés avec des certificats numériques, s'il y a plusieurs noms de domaine, il est nécessaire de demander un certificat de serveur pour chaque nom de domaine. Lorsqu'un serveur utilise l'IP pour fournir des services, s'il y a plusieurs IP, il est nécessaire de demander un certificat de serveur pour chaque IP. Ces types de certificats sont présentés dans le Tableau 3.

Tableau 3 – Description de la configuration du certificat de serveur du système de messagerie de la 5G

Nom du serveur	Méthode d'accès	Type de certificat
5GMC	Nom de domaine	Certificat SSL ordinaire (requiert le terminal pour prédéfinir le certificat racine CA)
Plate-forme de messagerie	Nom de domaine	Certificat SSL ordinaire (requiert le terminal pour prédéfinir le certificat racine CA)
Module de gestion de la plate-forme de messagerie	Nom de domaine	Certificat SSL ordinaire
Agent conversationnel	Nom de domaine	Certificat SSL ordinaire

8.3 Audit de sécurité

Les journaux sont des enregistrements des comportements importants des utilisateurs, de l'utilisation anormale des ressources du système et de l'utilisation de commandes importantes de la plate-forme. Les enregistrements peuvent inclure la date et l'heure, le type, l'identification du sujet, l'identification de l'objet et les résultats de l'événement. Les contenus susceptibles d'être enregistrés dans le journal de sécurité des services comprennent, sans s'y limiter, les journaux des opérations des utilisateurs, les journaux des opérations des administrateurs et les journaux des services.

a) Journaux des opérations de l'utilisateur: ils enregistrent les opérations et les résultats des comptes, les opérations et les résultats des services, etc. Les journaux des opérations de l'utilisateur peuvent comprendre des informations sur l'utilisateur, des opérations de l'utilisateur, des objets d'opération, la durée de l'opération, les résultats de l'opération, les résultats anormaux, etc.

b) Journaux des opérations de l'administrateur: ils enregistrent les opérations et les résultats des comptes, les opérations et les résultats des services, etc. Les journaux des opérations de l'administrateur peuvent inclure les informations de l'administrateur, les opérations de l'administrateur, les objets de l'opération, le temps de l'opération, les résultats de l'opération, les résultats anormaux, etc.

c) Journaux de service: il est recommandé que les systèmes puissent enregistrer leurs journaux de service. La plate-forme peut stocker tous les types de journaux dans un délai déterminé pour une consultation en ligne en fonction de la demande; concernant les journaux qui dépassent le délai de stockage en ligne, le délai de stockage hors ligne peut être spécifié. Les

journaux en ligne sont stockés dans une base de données ou selon une méthode désignée par le système. La plate-forme de services gère les droits d'accès et ne peut être consultée, exportée ou auditée que par un administrateur désigné (auditeur); concernant les journaux hors ligne, ils peuvent être importés dans le système ou utiliser des outils spéciaux pour l'interrogation, l'audit et d'autres opérations. Les journaux hors ligne contenant des données sensibles pourraient être stockés dans des fichiers chiffrés après avoir été exportés.

8.4 Sécurité de la gestion des logiciels

8.4.1 Sécurité de la gestion du développement logiciel pour la messagerie 5G

Les principes de codage sécurisé du système de messagerie 5G doivent comprendre les éléments suivants:

a) Contrôle de l'efficacité des données saisies par l'utilisateur, filtrage des symboles sensibles.

b) Chiffrement des données sensibles de stockage, telles que les mots de passe.

c) Transmission des données sensibles par HTTPS, telles que les noms d'utilisateur et les mots de passe.

d) Interdiction d'accéder directement aux ressources du système, telles que les fichiers.

e) Interdiction d'utiliser des coquilles dans les codes associés au web.

f) Utilisation d'une fonction de sécurité pour la programmation.

8.4.2 Sécurité de la gestion des opérations pour le système de messagerie 5G

Le système de messagerie 5G peut surveiller les processus importants et la logique du traitement des services, et émettra une alarme en cas d'anomalie.

9 Exigences de sécurité relatives au contrôle des services de messagerie 5G

9.1 Restrictions de la capacité de service

Les restrictions de la capacité de service comprennent la limitation du nombre de personnes dans un groupe, le contrôle différencié des fonctions de groupe et la limitation des discussions de groupe.

a) Limitation du nombre de personnes dans un groupe: les opérations d'envoi de messages 5G par un groupe doivent fixer la limite supérieure du nombre d'envois par le groupe, afin de limiter les effets négatifs potentiels à une plage restreinte.

b) Contrôle différencié des fonctions de groupe: les plates-formes de services pourraient permettre le contrôle différencié du nombre d'utilisateurs appelés d'un service de groupe.

c) Limitation des conversations de groupe: les plates-formes de services peuvent prendre en charge la restriction de l'échelle des utilisateurs des conversations de groupe, les paramètres du nombre d'utilisateurs du groupe peuvent être configurés, les plates-formes de services peuvent prendre en charge la restriction de la longueur du nom du groupe.

9.2 Liste noire des appelants

Pour les messages 5G au départ du mobile (MO), il est nécessaire d'ajouter une fonction de contrôle de l'authentification de la liste noire des appelants pour prévenir les risques de bombardement de messages 5G. Un système de contrôle de l'activité pourrait mettre en place un mécanisme de surveillance des conversations de groupe, qui pourrait analyser les actions des messages de masse malveillants qui seront ajoutés à une liste noire d'appelants, par ajout automatique, examen manuel ou d'autres manières. Le contrôle de la liste noire des appelants pourrait alors intercepter et contrôler les actions des messages de groupe malveillants.

9.3 Liste noire des utilisateurs appelés

Pour les messages 5G à destination d'un mobile (MT), il est nécessaire d'ajouter un contrôle de liste noire des utilisateurs appelés afin de réduire le risque de plaintes de la part des utilisateurs de terminaux. Les utilisateurs personnels peuvent se plaindre ou établir une liste noire en appelant le service clientèle, en se connectant à une interface en libre-service, en se rendant dans un centre de services ou par d'autres moyens. Un système de contrôle de l'activité ou des systèmes de service connexes pourraient mettre en place un contrôle de la liste noire des utilisateurs appelés qui pourrait intercepter les messages des utilisateurs en fonction d'un type d'utilisateur ou de service donné.

Bibliographie

[b-GSMA RCC.71] GSM Association (2019), *Document de définition du service de profil universel RCS.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Publié en Suisse
Genève, 2024