(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 139 966***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 09495**

(51) Int Cl[8] : ***H 04 W 80/00*** *(2022.01), H 04 W 24/02, H 04 W 40/24, H 04 W 12/10*

(12) **BREVET D'INVENTION** **B1**

(54) Procédé d'établissement de session MCData IPCON.

(22) **Date de dépôt :** 20.09.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.03.24 Bulletin 24/12.

(45) **Date de la mise à disposition du public du brevet d'invention :** 28.02.25 Bulletin 25/09.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *AIRBUS DS SLC Société par actions simplifiée à associé unique* — FR.

(72) **Inventeur(s) :** Paterour Olivier et Piroard François.

(73) **Titulaire(s) :** AIRBUS DS SLC Société par actions simplifiée à associé unique.

(74) **Mandataire(s) :** Cabinet Camus Lebkiri.

FR 3 139 966 - B1

Description

Titre de l'invention : Procédé d'établissement de session MCData IPCON

DOMAINE TECHNIQUE DE L'INVENTION

[0001] Le domaine technique de l'invention est celui des télécommunications.

[0002] La présente invention concerne un procédé d'établissement de session MCData Internet Protocol Connectivity (IPCON) et en particulier un procédé d'établissement de session IPCON dans un réseau de communication selon le standard 3GPP MCS « 3rd Generation Partnership Program Mission-Critical System ».

ARRIERE-PLAN TECHNOLOGIQUE DE L'INVENTION

[0003] Les normes de radiocommunication PMR (selon la dénomination anglo-saxonne « Professional Mobile Radio » pour « Radio Mobile Professionnelle ») TETRAPOL®, TETRA® ou encore P25® permettent la mise en œuvre de réseaux professionnels sécurisés. Ces réseaux à bande étroite sont des réseaux nationaux ou locaux : ils sont implémentés par exemple au sein d'une organisation telle qu'une entreprise, au sein d'un pays par exemple pour les communications des pompiers, des forces de l'ordre, des militaires etc.

[0004] Ces réseaux évoluent vers une prise en charge d'échanges en large bande. Le standard 3GPP régissant les réseaux mobiles de type « GSM » selon la dénomination anglo-saxonne « Global System for Mobile Communications », notamment dans leurs troisième, quatrième et cinquième générations respectivement appelées « 3G », « 4G » et « 5G », et générations suivantes, et plus particulièrement dans les déploiements faisant appel à des services de communications critiques définis par le 3GPP appelés « MCS » selon la dénomination anglo-saxonne « Mission Critical Services » permet ces échanges sécurisés en large bande. Un réseau 3G, 4G ou 5G met en œuvre un équipement terminal 3G/4G/5G (appelé UE de l'anglais « User Equipement »), un réseau d'accès radio RAN (de l'anglais « Radio Access Network ») 3G/4G/5G et un cœur de réseau (3G/4G/5G). Les déploiements des services MCS en large bande ne se limitent bien entendu pas aux réseaux mobiles 3G/4G/5G mais incluent aussi des déploiements dans des réseaux IP (de l'anglais « Internet Protocol ») fixes et mobiles, par exemple des WLAN, de l'anglais « Wide Local Area Network ».

[0005] On entend par « réseau de communication selon le standard 3GPP MCS », un réseau de communication compatible avec le standard 3GPP MCS et plus particulièrement avec la version actuelle du 3GPP qui est la version 17 et avec les versions suivantes intégrant toutes les caractéristiques de l'invention.

[0006] Dans le standard 3GPP MCS, les services de communication suivants sont définis :

- MCPTT, de l'anglais « Mission Critical Push To Talk » pour « Appuyer Pour Parler en Mission Critique » en français, qui permet de réaliser des communications voix,
- MCVideo, qui permet de réaliser des communications vidéo,
- MCData, qui comprend trois sous-services :
  - SDS de l'anglais « Short Data Service » pour « Service de données courtes » en français et
  - FD de l'anglais « File Distribution » pour « Distribution de fichier » en français,
  - IPCON de l'anglais « IP Connectivity » pour « Connectivité IP » en français.

[0007] Le service MCData SDS permet le transport de données utiles (dans sa dénomination anglaise « payload ») ayant une taille variable. Le service MCData SDS couvre les fonctionalités de status et messaging. Il peut s'agir d'un texte ou d'un message étendu, d'un lien hypertexte permettant aux utilisateurs d'accéder à un contenu lié et accessible comme un fichier volumineux, des données de connaissance de la situation, des informations de localisation ou des instructions de commande.

[0008] Le service MCData IPCON concerne l'envoi de données utiles, entre deux clients MCData. Il faut souligner que, contrairement au service MCData SDS, le service MCData IPCON est un service de transport agnostique à la nature des échanges applicatifs. Ainsi, le service MCData IPCON permet l'échange de données IP en utilisant le service de transport MCData comme intermédiaire et assure le transport des données IP pour, par exemple, les hôtes de données, les serveurs, etc. L'échange des données n'est pas limité à une transaction.

[0009] La [Fig.1] est une représentation schématique d'un système pouvant servir à la mise en œuvre du service MCData IPCON. Les clients MCData 220 permettent la communication bidirectionnelle de données IP 200 avec le soutien du service de connectivité IP qui constitue ainsi la passerelle vers les hôtes 210 ou serveurs de données 210. Le client MCData 220 émetteur demande au service de transport MCData 230 une exigence de qualité de service et la priorité de communication associées. Le tunnel IP « Internet Protocol » 240 entre les deux clients MCData 220 est un tunnel de routage IP de données 200, notamment des données média. Chacun des deux clients MCData 220 est connecté 250 au service de transport MCData 230.

[0010] Il faut noter qu'un client MCData, qui prend en charge les capacités de connectivité IP, est en mesure d'interdire les demandes de connectivité IP entrantes, soit à la demande, soit en fournissant une liste d'origines exclues identifiées par l'identifiant MCData et, si possible, par l'alias fonctionnel.

[0011] Les spécifications actuelles, définies dans le document de spécifications techniques

TS 23.282 du standard 3GPP pour les communications MCData IPCON comprennent l'établissement et la suppression d'un tunnel IP 240 entre deux clients MCData 220.

[0012] Aucune sécurité n'est pour l'instant prévue pour le tunnel IP entre deux clients MCData. Ainsi, à l'heure actuelle, la sécurité des données 200 transportées à travers le tunnel IP 240 s'appuie sur la sécurité des données appliquée par les serveurs applicatifs 210.

[0013] Toutefois, la sécurité des données appliquée par les serveurs applicatifs 210 n'est parfois pas suffisante voire totalement absente. Pour l'instant, aucune solution n'a été trouvée concernant les communications MCData IPCON dans les documents de spécifications techniques TS 23.282 du standard 3GPP dédié à l'architecture fonctionnelle et les procédures et TS 24.282 du standard 3GPP de stage 3 dédié au protocole et à l'implémentation.

[0014] Il existe donc un besoin de fournir un procédé respectant les spécifications 3GPP R17 proposant une sécurité des communications MCData IPCON. En d'autres termes, une sécurité du contenu à transporter de bout en bout entre les clients MCData mettant en œuvre le tunnel IP doit être fournie. De plus, cette sécurité doit être activable et désactivable.

[0015] Le procédé doit aussi permettre la gestion de données média. Le tunnel IP, établi sur le plan média entre des clients MCData IP, permet d'échanger des données média entre des entités applicatives externes. Les clients MCData IP doivent donc pouvoir contrôler l'accès à ce tunnel IP : ceci est fait sur le plan de contrôle MCData au préalable et sur le plan média en sécurisant les données transitant par ce tunnel IP.

[0016] Afin d'assurer la gestion de données média, le procédé doit être compatible avec des tunnels GRE in UDP comme préconisé dans le document de spécifications techniques TS 24.582 du standard 3GPP concernant la gestion des données média à la clause 13.4. L'encapsulation GRE dans UDP est décrite dans le document IETF RFC 8086 « Internet Engineering Task Force Request for Comments: 8086 ». Le format d'encapsulation GRE-in-UDP contient un entête UDP et un entête GRE. Il faut noter que ces éléments d'entête ne doivent pas être altérés par le procédé permettant la sécurité des communications MCData IPCON.

[0017] Enfin, à l'heure actuelle, les communications MCData IPCON concernent uniquement les communications de point à point. Ainsi, les communications MCData IPCON de groupe n'existent pas. Un groupe peut être défini comme étant un groupe virtuel regroupant plusieurs dispositifs utilisateurs pouvant interagir entre eux une fois autorisés par le réseau de communication, par exemple authentifiés à un serveur de gestion de groupe du réseau de communication, permettant ainsi l'accès au groupe de communication.

[0018] Ainsi, l'invention vise à fournir un procédé permettant d'établir des communications

MCData IPCON sécurisées de bout en bout, à la fois pour les communications de point à point et les communications de groupe.

Résumé de l'invention

[0019] L'invention offre une solution aux problèmes évoqués précédemment, en définissant un mécanisme de génération, de distribution et de dérivation de clés pour le service MCData IPCON, ainsi qu'un mécanisme de chiffrement du contenu MCData IPCON.

[0020] Un aspect de l'invention concerne un procédé d'établissement de session MCData IPCON « Mission Critical Data IP Connectivity » dans un réseau de communication selon le standard 3GPP MCS « 3rd Generation Partnership Program Mission Critical System », le réseau comprenant :

- une entité MCData émettrice ;
- une entité MCData destinataire ; et
- un service de transport MCData connecté aux entités MCData émettrice et destinataire ;

le procédé comprenant :

- obtenir, par l'entité MCData émettrice, une clé DPPK « MCData Payload Protection Key » et un identifiant de la clé DPPK-ID « MCData Payload Protection Key Identifier »;
- transmettre, par l'entité MCData émettrice à l'entité MCData destinataire via le service de transport MCData un message SIP-INVITE comprenant la clé DPPK et l'identifiant de la clé DPPK-IK ;
- authentifier, par l'entité MCData destinataire, le message ;
- déterminer, par l'entité MCData destinataire, la clé DPPK et l'identifiant de la clé DPPK-ID et établir un tunnel IP entre l'entité MCData émettrice et l'entité MCData destinataire.

[0021] Grâce à l'invention, la sécurité de bout en bout est assurée entre deux entités MCData dans une communication IPCON. Ainsi, même si le contenu à envoyer n'est pas sécurisé par les serveurs applicatifs lorsque celui-ci est reçu par l'entité émettrice, l'invention permettra de sécuriser la transmission du contenu entre l'entité émettrice et l'entité destinataire.

[0022] Outre les caractéristiques qui viennent d'être évoquées dans le paragraphe précédent, le procédé selon un aspect de l'invention peut présenter une ou plusieurs caractéristiques complémentaires parmi les suivantes, considérées individuellement ou selon toutes les combinaisons techniquement possibles :

- Procédé selon l'invention dans lequel l'entité MCData émettrice est connectée à une entité applicative émettrice et l'entité MCData destinataire est connectée à au moins une entité applicative destinataire, le procédé comprenant en outre,

les étapes finales :

- Transmettre, par l'entité applicative émettrice, des données utiles à l'entité MCData émettrice.
- Générer, par l'entité MCData émettrice, un paquet de données comprenant :

- les données utiles chiffrées en utilisant la clé DPPK et l'identifiant de la clé DPPK-ID ; et
- un entête ;
- Envoyer, par l'entité MCData émettrice, le paquet de données généré à l'entité MCData destinataire via le tunnel IP établi ;
- Retirer, par l'entité MCData destinataire, l'entête du paquet de données généré et déchiffrer les données utiles chiffrées en utilisant la clé DPPK et l'identifiant de la clé DPPK-ID ; et
- Transmettre, par l'entité MCData destinataire, les données utiles déchiffrées à la au moins une entité applicative destinataire.
- Procédé selon l'invention dans lequel :
  - le tunnel IP est un tunnel GRE « Generic Routing Encapsulation » dans le protocole UDP « User Datagram Protocol » ; et
  - l'entête est un entête de type GRE et UDP.
- Procédé selon l'invention comprenant en outre les étapes préalables :
  - obtenir des informations
- d'autorisation d'établissement de session MCData IPCON, configurée avec un plan média MCData, entre l'entité MCData émettrice et l'entité MCData destinataire ; et
- de la nécessité de mettre en place le procédé selon l'invention ; et
- Mettre en œuvre le procédé d'établissement de session MCData IPCON « Mission Critical Data IP Connectivity » selon l'invention lorsque l'établissement de session MCData IPCON, configurée avec le plan média MCData, entre l'entité MCData émettrice et l'entité MCData destinataire est autorisé et si la mise en place du procédé selon l'invention est nécessaire.
- Procédé selon l'invention dans lequel :
  - ledit procédé est un procédé d'établissement de session MCData IPCON de groupe ;
  - l'entité MCData émettrice est un client MCData appartenant à un groupe MCData ;
  - l'entité MCData destinataire est un ensemble de clients MCData appartenant à un même groupe MCData que l'entité MCData émettrice ; et

- la clé DPPK est une clé de type GMK « Group Master Key » et l'identifiant de la clé DPPK-ID est de type GMK-ID « Group Master Key Identifier ».

- Procédé dans lequel :
  - ledit procédé est un procédé d'établissement de session MCData IPCON point à point ;
  - l'entité MCData émettrice et l'entité MCData destinataire sont des clients MCData ; et
  - la clé DPPK est une clé privée de type PCK « Private Call Key » et l'identifiant de la clé DPPK-ID est de type PCK-ID « Private Call Key Identifier » et la clé PCK comprenant le chiffrement de l'identité de l'entité MCData destinataire ;
  - une étape initiale d'obtention , par l'entité MCData émettrice et l'entité MCData destinataire, des éléments de chiffrement ;
  - l'obtention à l'étape, par l'entité MCData émettrice, de la clé PCK et de l'identifiant de la clé PCK-ID consiste en une génération de la clé PCK et de l'identifiant PCK-ID en utilisant les éléments de chiffrement obtenus à l'étape;
  - le message SIP-INVITE transmis à l'étape par l'entité MCData émettrice à l'entité MCData destinataire, comprend un conteneur MIKEY-SAKKE I-MESSAGE « Multimedia Internet KEYing-Sakai-Kasahara Key Encryption », le conteneur MIKEY-SAKKE I-MESSAGE comprenant la clé DPPK chiffrée avec une méthode de chiffrement SAKKE ; et l'identifiant de la clé DPPK-ID ; et
  - la détermination par l'entité MCData destinataire, de la clé PCK et de l'identifiant de la clé PCK-ID est effectué en utilisant les éléments de chiffrement obtenus à l'étape initiale.

[0023] Un autre aspect de l'invention concerne un réseau de communication selon le standard 3GPP MCS « 3rd Generation Partnership Program Mission-Critical System », le réseau de communication comprenant :

- une entité MCData émettrice ;
- une entité MCData destinataire ;
- un service de transport MCData connecté aux entités MCData émettrice et destinataire ;

le réseau de communication étant configuré pour mettre en œuvre le procédé selon l'invention.

[0024] Outre les caractéristiques qui viennent d'être évoquées dans le paragraphe précédent, le réseau de communication selon un aspect de l'invention peut présenter la caracté-

ristique suivante :

- réseau selon l'invention dans lequel l'entité MCData destinataire est :
  - un ensemble de clients MCData appartenant au même groupe MCData que l'entité MCData émettrice ; ou
  - un client MCData.

[0025] Selon un troisième aspect de l'invention, il est proposé un produit programme d'ordinateur comprenant des instructions qui conduisent le système selon l'invention à exécuter le procédé selon l'invention.

[0026] Selon un quatrième aspect de l'invention, il est proposé un support lisible par ordinateur, sur lequel est enregistré le programme d'ordinateur selon l'invention.

[0027] L'invention et ses différentes applications seront mieux comprises à la lecture de la description qui suit et à l'examen des figures qui l'accompagnent.

BREVE DESCRIPTION DES FIGURES

[0028] Les figures sont présentées à titre indicatif et nullement limitatif de l'invention.

- La [Fig.1] montre une représentation schématique d'un système pour la mise en œuvre du service MCData IPCON de l'art antérieur.
- La [Fig.2] est un schéma synoptique illustrant l'enchaînement des étapes du procédé selon l'invention.
- Les figures 3 et 4 sont des schémas synoptiques illustrant l'enchaînement des étapes du procédé selon deux variantes de l'invention.
- La [Fig.5] montre une représentation schématique d'un système configuré pour la mise en œuvre du service MCData IPCON selon l'invention.
- La [Fig.6] montre une représentation schématique d'un système configuré pour la mise en œuvre du service MCData IPCON de groupe selon un mode d'implémentation de l'invention.

DESCRIPTION DETAILLEE

[0029] Sauf précision contraire, un même élément apparaissant sur des figures différentes présente une référence unique.

[0030] La [Fig.5] est une représentation schématique d'un procédé d'établissement de session MCData IPCON « Mission Critical Data IP Connectivity » selon l'invention. L'entité MCData émettrice 320 et l'entité MCData destinataire 370 sont connectées 350 au service de transport MCData 330. Le service de transport MCData 330 comprend un ou plusieurs serveurs MCData. L'entité MCData émettrice 320 est connectée à une entité applicative émettrice 310. L'entité applicative émettrice 310 est par exemple un serveur applicatif émetteur. L'entité MCData destinataire 370 est connectée à une entité applicative destinataire 360. L'entité applicative destinataire 360 est par exemple un serveur applicatif destinataire. Le tunnel IP 340 permet le

routage IP de données 300, notamment des données média de l'entité applicative émettrice 310 à l'entité applicative destinataire 360 en passant par les entités MCData 320 et 370.

[0031] Le réseau de communication de la [Fig.5] est configuré pour mettre en œuvre le service MCData IPCON. Les entités MCData émettrice 320 et destinataire 370 sont interchangeables, c'est-à-dire qu'une entité MCData peut être émettrice 320 sur une période puis destinataire 370 sur une autre période. Chacune de ces entités MCData a une identité au sein du réseau de communication. Cette identité permet d'identifier l'entité au sein du réseau de communication. Par exemple, l'identité peut être un identifiant unique au sein du réseau de communication.

[0032] La [Fig.2] est un schéma synoptique illustrant l'enchaînement des étapes du procédé selon l'invention.

[0033] Dans une première étape 20, l'entité MCData émettrice 320 obtient une clé DPPK « MCData Payload Protection Key » et un identifiant de la clé DPPK-ID « MCData Payload Protection Key Identifier ». L'obtention de la clé DPPK peut consister en une réception de la clé DPPK et de l'identifiant DPPK-ID. L'obtention de la clé DPPK peut aussi consister en une génération de la clé DPPK en utilisant les éléments de chiffrement. Il faut noter que la clé DPPK n'est pas un type de clé particulier. En effet le terme DPPK regroupe les types de clés existants dans MCData, par exemple une clé privée PCK « Private Call Key » et une clé GMK « Group Master Key », utilisées pour la protection dans le procédé MCData respectivement pour les communications point-à-point et pour les communications de groupe. Par conséquent, plusieurs clés DPPK peuvent être utilisées dans un procédé 1 d'établissement de session MCData IPCON en fonction du canal de communication. De plus, bien qu'une clé privée PCK et une clé GMK puissent toutes deux être utilisées comme clé DPPK pour protéger le procédé MCData dans différents canaux, la clé privée PCK et la clé GMK ne sont pas la même clé et ne seront pas utilisées dans les mêmes canaux.

[0034] Le procédé 1 selon l'invention comprend une seconde étape de transmission 30, par l'entité MCData émettrice 320 à l'entité MCData destinataire 370 via le service de transport MCData, d'un message SIP-INVITE comprenant la clé DPPK et l'identifiant de la clé DPPK-IK.

[0035] La transmission 30 s'effectue selon le protocole SDP « Session Description Protocol ». Le protocole SDP est un protocole de communication de description de paramètres d'initialisation d'une session de diffusion en flux. Le protocole SDP ne comprend pas la livraison du média. Il est utilisé par l'émetteur et le destinataire pour la négociation du type et du format du média, et les propriétés associées. La transmission 30 s'effectue par l'embarquement d'une charge SDP dans le corps d'un message SIP INVITE. Le message SIP INVITE est envoyé par l'entité MCData

émettrice 320 à l'entité MCData destinataire 370. L'entité MCData destinataire 370 répond ensuite si elle accepte ou non l'établissement d'une session MCData IPCON avec l'entité MCData émettrice 320.

[0036] Dans une troisième étape 40, l'entité MCData destinataire 370 authentifie le message SIP-INVITE. L'authentification a pour finalité de vérifier que le message SIP-INVITE provient bien de l'entité MCData émettrice et qu'il n'est pas corrompu. L'authentification peut être facilitée par des procédures d'authentification effectuées préalablement à la mise en œuvre du procédé selon l'invention. Ainsi, dans ce cas, l'authentification peut consister à vérifier que le message a bien été envoyé par l'entité MC Data émettrice. L'authentification peut aussi consister à vérifier la signature d'un élément contenu dans le message. La validité de la signature peut être déterminée en vérifiant que l'identité de l'entité MCData émettrice 320 existe dans la liste des identités de confiance de l'entité MCData destinataire 370 et l'intégrité du document.

[0037] Le procédé 1 selon l'invention comprend une dernière étape de détermination 50, par l'entité MCData destinataire 370, de la clé DPPK et l'identifiant de la clé DPPK-ID.

[0038] La [Fig.3] est un schéma synoptique illustrant l'enchaînement des étapes du procédé selon une variante de l'invention. Dans cette variante, le procédé comprend en outre des étapes finales 60, 70, 80, 90 et 100. Cette variante permet l'envoi sécurisé de bout en bout de données entre deux entités applicatives. Chaque entité applicative est par exemple un serveur applicatif. Une première entité applicative 310 est connectée à une entité MCData émettrice 320 et une seconde entité applicative 360 est connectée à une entité MCData destinataire 370.

[0039] A l'étape 60, l'entité applicative émettrice 310 transmet des données utiles à l'entité MCData émettrice 320. Ces données utiles peuvent être chiffrées ou non.

[0040] Ensuite, l'entité MCData émettrice 320 génère à une étape 70 un paquet de données comprenant les données utiles chiffrées en utilisant la clé DPPK et l'identifiant de la clé DPPK-ID et un entête. Ainsi, avant la génération 70, les données utiles sont chiffrées. Afin d'effectuer le chiffrement, une dérivation de la clé DPPK peut être nécessaire. Par exemple, la clé DPPK est hachée par une fonction de dérivation de clé pour produire une clé de chiffrement DPCK « MCData Payload Cipher Key » des données utiles. Un exemple de format de données protégées compatible avec l'invention est décrit à la clause 8.5.4.1 dans le document de spécifications techniques TS 33.180 du standard 3GPP.

[0041] L'étape 80 consiste à envoyer, par l'entité MCData émettrice 320, le paquet de données généré 70 à l'entité MCData destinataire 370. L'entité MCData destinataire 370 retire ensuite à une étape 90 l'entête du paquet de données généré à l'étape 70 et déchiffre les données utiles chiffrées en utilisant la clé DPPK et l'identifiant de la clé DPPK-ID. Enfin, l'entité MCData destinataire 370 transmet à une étape 100 les

données utiles déchiffrées à l'entité applicative destinataire 360. Il faut noter que les serveurs MCData du service de transport MCData 330 assurent le transport entre l'entité MCData émettrice 320 et l'entité MCData destinataire 370. Ces serveurs MCData pourront notamment utiliser l'entête du paquet de données généré à l'étape 70 pour identifier l'entité MCData destinataire 370.

[0042] Dans une variante compatible avec la variante décrite ci-dessus, le tunnel IP 340 est un tunnel GRE « Generic Routing Encapsulation » dans le protocole UDP « User Datagram Protocol » et l'entête est un entête de type GRE et UDP. Le tunnel GRE in UDP est configuré entre l'entité MCData émettrice 320 et l'entité MCData destinataire 370, chaque entité MCData 320 et 370 agissant comme une extrémité du tunnel IP 340. Les entités MCData 320 et 370 sont configurées pour envoyer et recevoir les paquets GRE directement entre eux. Les serveurs MCData du système de transport MCData 330 situés entre ces deux entités MCData 320 et 370 n'ouvriront pas les paquets de données encapsulés. Ils ne se réfèreront qu'aux entêtes entourant les paquets encapsulés pour pouvoir les transmettre. Ainsi, cette encapsulation permet notamment de ne pas affecter la sécurité des paquets de données encapsulés.

[0043] La [Fig.4] est un schéma synoptique illustrant l'enchaînement des étapes du procédé selon une variante de l'invention. Dans cette variante, compatible avec les variantes précédentes, le procédé comprend en outre les étapes préalables 110 et 120. A l'étape 110, l'entité MCData émettrice 320 et l'entité MCData destinataire 370 obtiennent 110 des informations d'autorisation d'établissement de session MCData IPCON, configurée avec un plan média MCData, entre l'entité MCData émettrice et l'entité MCData destinataire 370 et des informations concernant la nécessité de mettre en place un procédé assurant la sécurité des données envoyées. Les informations concernant la nécessité de mettre en place le procédé assurant la sécurité des données envoyées peuvent donc être utilisées pour activer ou désactiver la mise en place du procédé par exemple en fonction de la sécurité des données appliquées par les serveurs applicatifs.

[0044] Le service MCData IPCON fournit un plan média pour l'échange de tout type de données IP entre des applications IP. Ces applications IP peuvent résider sur des hôtes externes au réseau 3GPP connectés par une interface IP à l'entité MCData ou peuvent être exécutées directement par l'entité MCData. Un plan média pouvant être utilisé dans l'invention est détaillé dans le document de spécifications techniques TS 24.582.

[0045] Les informations d'autorisation d'établissement de session MCData IPCON et concernant la nécessité de mettre en place le procédé assurant la sécurité des données envoyées peuvent être insérées dans le document de profil des entités MCData émettrice et destinataire.

[0046] En fonction de ces informations, le procédé est mis en œuvre à une étape 120 ou non. Ainsi si les informations autorisent l'établissement de session MCData IPCON,

configurée avec un plan média MCData, entre l'entité MCData émettrice 320 et l'entité MCData destinataire 370 et confirme la nécessité de mettre en place le procédé assurant la sécurité des données envoyées, alors le procédé selon, l'invention est mis en œuvre à une étape 120.

[0047] Dans un premier mode d'implémentation, le procédé selon l'invention est un procédé d'établissement de session MCData IPCON de groupe. L'entité MCData émettrice est un client MCData émetteur 420 appartenant à un groupe MCData 480, l'entité MCData destinataire est un ensemble de clients MCData destinataires 470 appartenant à un même groupe MCData 480 que le client MCData émetteur 420, la clé DPPK est une clé de type GMK « Group Master Key » et l'identifiant de la clé DPPK-ID est de type GMK-ID « Group Master Key Identifier ».

[0048] Dans ce premier mode d'implémentation, la clé GMK et l'identifiant de la clé GMK-ID sont obtenues à l'étape 20. Cette obtention par l'entité MCData émettrice consiste à recevoir la clé GMK et l'identifiant de la clé GMK-ID. La clé GMK et l'identifiant de la clé GMK-ID peuvent être fournis par un serveur GMS « Group Master Server ».

[0049] A l'étape 30, la transmission du conteneur s'effectue d'un client MCData émetteur 420 vers les autres membres du groupe qui sont donc des clients MCData destinataires 470.

[0050] Ensuite, à l'étape 40, chaque client MCData destinataire authentifie le message SIP-INVITE en vérifiant que le conteneur a bien pour origine le client appartenant au même groupe. Dans ce premier mode d'implémentation, l'authentification est facilitée par des procédures d'authentification effectuées préalablement à la mise en œuvre du procédé selon l'invention. Ainsi, dans ce cas, l'authentification peut consister à vérifier que le message a bien été envoyé par l'entité MC Data émettrice par exemple en accédant à un sous élément du document de groupe qui comporte toutes les informations relatives au groupe. Enfin, à l'étape 50, le client MCData destinataire détermine la clé GMK et l'identifiant de la clé GMK-ID. Par exemple, le message SIP-INVITE peut contenir un identifiant de groupe, par exemple une adresse URL « Uniform Resource Locator », qui permet d'accéder à un document de groupe contenant le GMK et GMK ID.

[0051] Une fois la session de communication de groupe établie, un client MCData émetteur qui souhaite transmettre un paquet de données vers les autres membres du groupe doit chiffrer ce paquet de données. Un exemple de chiffrement utilisable dans l'invention est celui décrit dans le document de spécifications techniques TS 33.180, avec notamment une dérivation de la clé GMK telle que définie dans la clause 8.5.3 et un format de données protégées décrit dans la clause 8.5.4.1 dans le document de spécifications techniques TS 33.180, avant de lui ajouter les entêtes nécessaires. Un exemple d'entête utilisable est un entête GRE et UDP. Ensuite, de manière optionnelle,

les clients MCData destinataires 470 effectuent l'opération inverse avant de transmettre le paquet déchiffré au data host visé.

[0052] La [Fig.6] est une représentation schématique d'un système pouvant servir à la mise en œuvre de ce premier mode d'implémentation. Le client MCData émetteur 420 et les clients MCData destinataires 470 appartiennent au même groupe MCData 480. Chaque client MCData 420 et 470 est connecté 450 au service de transport MCData 430. Le service de transport MCData 430 comprend un ou plusieurs serveurs MCData Le client MCData 420 est connecté à une entité applicative émettrice 410. Chaque client MCData destinataire 470 est connecté à une entité applicative destinataire 460. Le tunnel IP 440 permet le routage IP de données 400, notamment des données média, de l'entité applicative 410 aux entités applicatives 460.

[0053] Dans un second mode d'implémentation, le procédé selon l'invention est un procédé d'établissement de session MCData IPCON point à point. L'entité MCData émettrice 320 et l'entité MCData destinataire 370 sont des clients MCData. La clé DPPK est une clé privée de type PCK « Private Call Key » et l'identifiant de la clé DPPK-ID est de type PCK-ID « Private Call Key Identifier ».

[0054] Dans la première étape 10, les clients MCData émetteur 320 et destinataire 370 obtiennent des éléments de chiffrement. Ces éléments de chiffrement permettent l'obtention et la détermination de la clé PCK et de l'identification de la clé PCK-ID. Ces éléments de chiffrement peuvent être fournis par un serveur KMS « Key Management Server ». Les éléments de chiffrement venant du serveur KMS sont par exemple la clé privée SSK « Secret Signing Key », la clé publique « Public Validation Token » PVT ou la clé d'authentification publique KPAK «KMS Public Authentication Key »."

[0055] Dans la seconde étape 20, le client MCData émetteur obtient une clé privée PCK et un identifiant de la clé privée PCK-ID. Cette obtention consiste à générer la clé privée PCK et l'identifiant de la clé privée PCK-ID en utilisant les éléments de chiffrement obtenus à l'étape 10. Afin d'effectuer le chiffrement, une dérivation de la clé PCK peut être nécessaire. Un exemple de dérivation utilisable dans l'invention est défini dans la clause 8.3 du document de spécifications techniques TS 33.180.

[0056] La clé PCK obtenue à l'étape 20 comprend le chiffrement de l'identité de l'entité MCData destinataire 370. Ainsi la clé PCK permet, après extraction, d'obtenir l'entité MCData destinataire 370.

[0057] Dans la troisième étape 30, le MCData émetteur transmet la clé privée PCK et l'identifiant de la clé privée PCK-ID dans le message SIP-INVITE. Le message SIP-INVITE comprend un conteneur MIKEY-SAKKE I-MESSAGE « Multimedia Internet KEYing-Sakai-Kasahara Key Encryption », le conteneur MIKEY-SAKKE I-MESSAGE comprenant la clé DPPK chiffrée avec une méthode de chiffrement

SAKKE ; et l'identifiant de la clé DPPK-ID.

[0058] Le conteneur MIKEY-SAKKE I-MESSAGE est notamment utilisé pour transporter la clé DPPK. La clé DPPK peut par exemple être d'une longueur de 16 octets. La clé DPPK est encapsulée dans le conteneur avec une méthode de chiffrement SAKKE. Un exemple d'implémentation des messages MIKEY-SAKKE I-MESSAGE adaptés pour la mise en œuvre de l'invention est défini dans le document IETF RFC 6509 « Internet Engineering Task Force Request for Comments : 6509 ».

[0059] L'authentification du message SIP-INVITE peut consister à valider la signature du message SIP-INVITE. La signature du message SIP-INVITE consiste à signer le conteneur. Le conteneur signé permet au client MCData destinataire d'authentifier le conteneur en validant la signature. Par exemple, le conteneur est signé à l'aide d'une signature permettant d'authentifier l'origine du conteneur par le client MCData destinataire.

[0060] La transmission du conteneur s'effectue d'un client MCData émetteur vers un client MCData destinataire. Le message MIKEY-SAKKE I-MESSAGE comprend la clé privée PCK. Un exemple de structure possible du message MIKEY-SAKKE I-MESSAGE pour ce mode de réalisation est décrit à l'annexe E.3 dans le document de spécifications techniques TS 33.180.

[0061] Dans la quatrième étape 40, le client MCData destinataire authentifie le conteneur comprenant le message MIKEY-SAKKE I-MESSAGE en validant la signature de l'appelant.

[0062] Dans la cinquième étape 50, le client MCData destinataire détermine la clé privée PCK et l'identifiant de la clé privée PCK-ID. La détermination est effectuée par extraction en utilisant les éléments de chiffrement obtenus à l'étape 10

[0063] Le trafic subséquent sur la session MCData IPCON établie, c'est-à-dire le contenu envoyé par une entité applicative émettrice à une autre entité applicative destinataire, est chiffré par le MCData client émetteur et déchiffré par le MCData destinataire en utilisant la clé PCK. Un exemple de chiffrement et de déchiffrement utilisables pour une implémentation de l'invention sont décrits dans le document de spécifications techniques TS 33.180, avec notamment une dérivation de la clé PCK tel que défini dans la clause 8.5.3 et un format de données protégées décrit dans la clause 8.5.4.1 dans le document de spécifications techniques TS 33.180, avant de lui ajouter les entêtes nécessaires. Ce contenu chiffré est transporté dans le tunnel établi entre les deux clients MCData par exemple un tunnel GRE in UDP. Ainsi, après avoir chiffré le contenu reçu de l'entité applicative émettrice, le client MCData émetteur ajoute un entête par exemple un entête GRE et UDP avant de transmettre le paquet de données au client MCData destinataire, qui retire ces entêtes ajoutés avant de déchiffrer le contenu puis de transmettre le contenu déchiffré à l'entité applicative destinataire.

Revendications

[Revendication 1] Procédé (1) d'établissement de session MCData IPCON « Mission Critical Data Internet Protocol Connectivity » dans un réseau de communication selon le standard 3GPP MCS « 3rd Generation Partnership Program Mission Critical System », le réseau comprenant :

- une entité MCData émettrice est connectée à un entité applicative émettrice ;
- une entité MCData destinataire est connectée à au moins un serveur applicatif destinataire ; et
- un service de transport MCData connecté aux entités MCData émettrice et destinataire ;

le procédé comprenant :

- Obtenir (20), par l'entité MCData émettrice, une clé DPPK « MCData Payload Protection Key » et un identifiant de la clé DPPK-ID « MCData Payload Protection Key Identifier » ;
- Transmettre (30), par l'entité MCData émettrice à l'entité MCData destinataire via le service de transport MCData, un message SIP-INVITE comprenant la clé DPPK et l'identifiant de la clé DPPK-IK ;

- Authentifier (40), par l'entité MCData destinataire, le message ; et
- Déterminer (50), par l'entité MCData destinataire, la clé DPPK et l'identifiant de la clé DPPK-ID et établir un tunnel GRE « Generic Routing Encapsulation » entre l'entité MCData émettrice et l'entité MCData destinataire, le tunnel GRE « Generic Routing Encapsulation » étant établis dans un protocole UDP « User Datagram Protocol »,

- Transmettre (60), par le serveur applicatif émetteur, des données utiles à l'entité MCData émettrice,
- Générer (70), par l'entité MCData émettrice, un paquet de données comprenant :
  - les données utiles chiffrées en utilisant la clé DPPK et

l'identifiant de la clé DPPK-ID ; et
- un entête de type GRE et UDP ;

- Envoyer (80), par l'entité MCData émettrice, le paquet de données généré (70) à l'entité MCData destinataire via le tunnel GRE établi ;
- Retirer (90), par l'entité MCData destinataire, l'entête du paquet de données généré (70) et déchiffrer les données utiles chiffrées en utilisant la clé DPPK et l'identifiant de la clé DPPK-ID ; et
- Transmettre (100), par l'entité MCData destinataire, les données utiles déchiffrées à la au moins une entité applicative.

[Revendication 2] Procédé selon l'une quelconque des revendications précédentes comprenant en outre les étapes préalables:

- Obtenir (110) des informations :
  - d'autorisation d'établissement de session MCData IPCON, configurée avec un plan média MCData, entre l'entité MCData émettrice et l'entité MCData destinataire ; et
  - de la nécessité de mettre en place le procédé selon l'une quelconque des revendications précédentes ; et
- Mettre en œuvre (120) le procédé de la revendication 1 lorsque l'établissement de session MCData IPCON, configurée avec le plan média MCData, entre l'entité MCData émettrice et l'entité MCData destinataire est autorisé et si la mise en place du procédé selon l'une quelconque des revendications pré-cédentes est nécessaire.

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes dans lequel :

- Ledit procédé est un procédé d'établissement de session MCData IPCON de groupe ;
- L'entité MCData émettrice est un client MCData appartenant à un groupe MCData ;
- L'entité MCData destinataire est un ensemble de clients MCData appartenant à un même groupe MCData que l'entité

MCData émettrice ; et

- La clé DPPK est une clé de type GMK « Group Master Key » et l'identifiant de la clé DPPK-ID est de type GMK-ID « Group Master Key Identifier ».

[Revendication 4] Procédé selon les revendications 1 à 4 dans lequel :

- Ledit procédé est un procédé d'établissement de session MCData IPCON point à point ;
- L'entité MCData émettrice et l'entité MCData destinataire sont des clients MCData ; et
- La clé DPPK est une clé privée de type PCK « Private Call Key », l'identifiant de la clé DPPK-ID est de type PCK-ID « Private Call Key Identifier » et la clé PCK comprenant le chiffrement de l'identité de l'entité MCData destinataire ;
- Une étape initiale d'obtention (10), par l'entité MCData émettrice et l'entité MCData destinataire, des éléments de chiffrement ;
- L'obtention à l'étape (20), par l'entité MCData émettrice, de la clé PCK et de l'identifiant de la clé PCK-ID consiste en une génération de la clé PCK et de l'identifiant PCK-ID en utilisant les éléments de chiffrement obtenus à l'étape (10);
- Le message SIP-INVITE transmis à l'étape (30) par l'entité MCData émettrice à l'entité MCData destinataire, comprend un conteneur MIKEY-SAKKE I-MESSAGE « Multimedia Internet KEYing-Sakai-Kasahara Key Encryption », le conteneur MIKEY-SAKKE I-MESSAGE comprenant la clé DPPK chiffrée avec une méthode de chiffrement SAKKE ; et l'identifiant de la clé DPPK-ID ; et
- La détermination (50) par l'entité MCData destinataire, de la clé PCK et de l'identifiant de la clé PCK-ID est effectuée en utilisant les éléments de chiffrement obtenus à l'étape 10.

[Revendication 5] Réseau de communication selon le standard 3GPP MCS « 3rd Generation Partnership Program Mission-Critical System », le réseau de communication comprenant:

- Une entité MCData émettrice ;

- Une entité MCData destinataire ; et
- Un service de transport MCData connecté aux entités MCData émettrice et destinataire ;

le réseau de communication étant configuré pour mettre en œuvre le procédé (1) selon l'une quelconque des revendication précédentes.

[Revendication 6] Réseau selon la revendication précédente caractérisé en ce que l'entité MCData destinataire est :

- Un ensemble de clients MCData appartenant au même groupe MCData que l'entité MCData émettrice ; ou
- Un client MCData.

[Revendication 7] Produit programme d'ordinateur comprenant des instructions qui conduisent le réseau selon la revendication 8 à exécuter les étapes de la méthode selon l'une des revendications 1 à 6.

[Revendication 8] Support lisible par ordinateur, sur lequel est enregistré le programme d'ordinateur selon la revendication 9.

[Fig. 1]

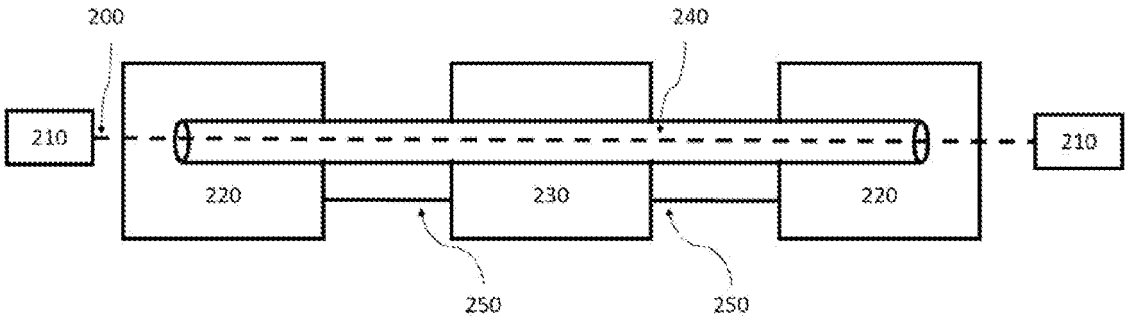

Fig. 1

[Fig. 2]

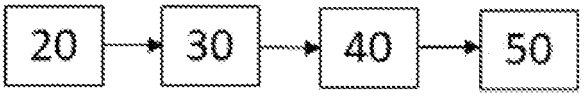

Fig. 2

[Fig. 3]

Fig. 3

[Fig. 4]

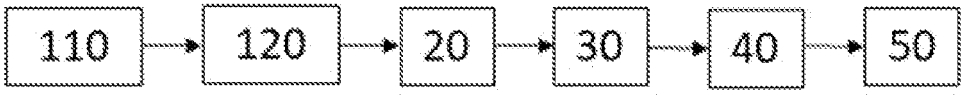

Fig. 4

[Fig. 5]

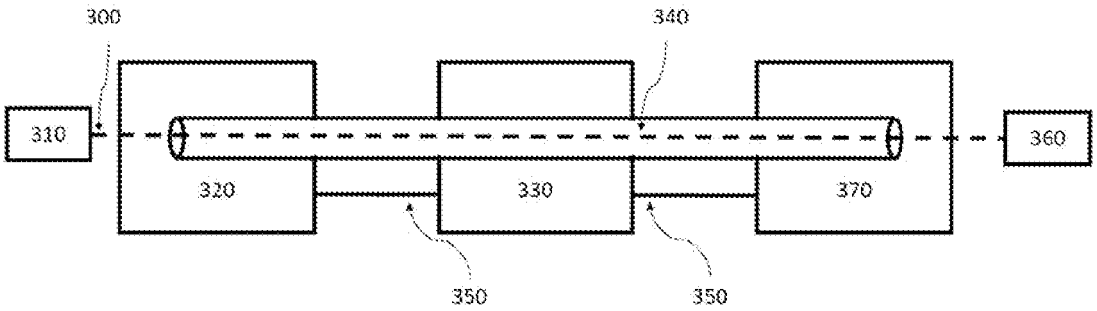

Fig. 5

[Fig. 6]

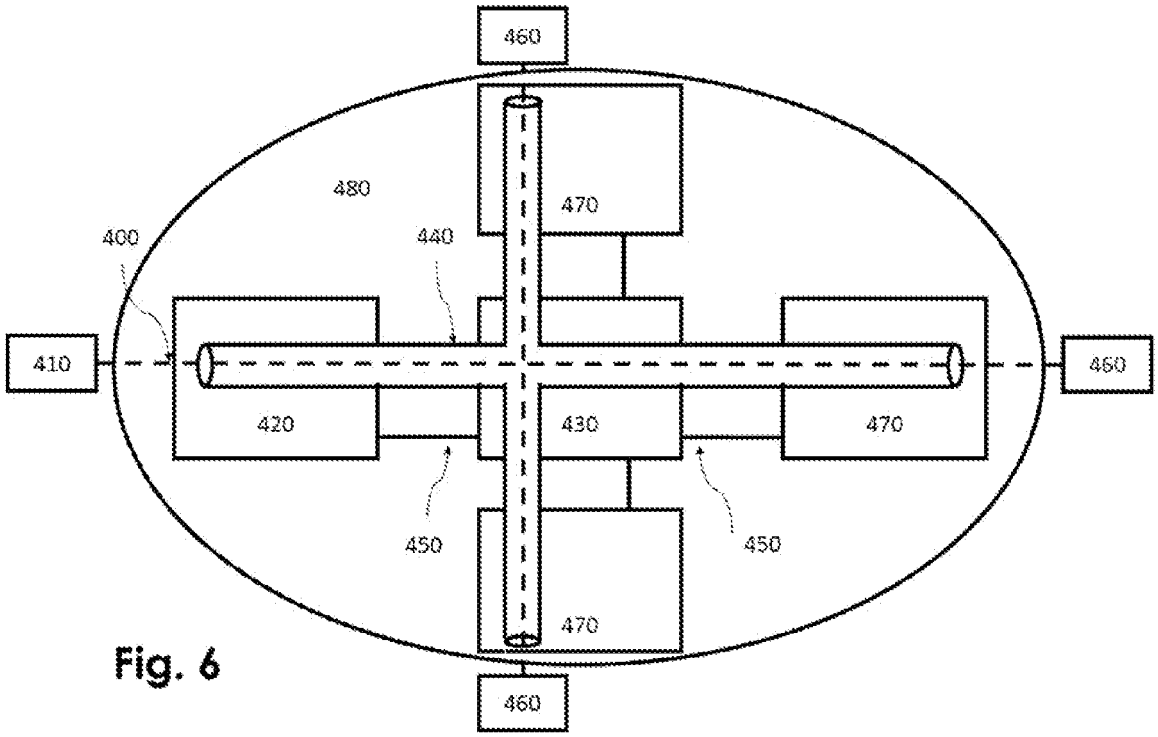

Fig. 6

N° d'enregistrement national : FR2209495 N° de publication : FR3139966

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

"3rd Generation Partnership Project;
Technical Specification Group Services and
System Aspects; Security of the mission
critical service; (Release 14)",
3GPP STANDARD ; TECHNICAL SPECIFICATION ;
3GPP TS 33.180, 3RD GENERATION PARTNERSHIP
PROJECT (3GPP), MOBILE COMPETENCE CENTRE ;
650, ROUTE DES LUCIOLES ; F-06921
SOPHIA-ANTIPOLIS CEDEX ; FRANCE,
vol. SA WG3, no. V14.0.0,
15 juin 2017 (2017-06-15), pages 1-118,
XP051298598,
[extrait le 2017-06-15]

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

"3rd Generation Partnership Project;
Technical Specification Group Core Network
and Terminals; Mission Critical Data
(MCData) media plane control; Protocol
specification (Release 17)",
3GPP STANDARD; TECHNICAL SPECIFICATION;
3GPP TS 24.582, 3RD GENERATION PARTNERSHIP
PROJECT (3GPP), MOBILE COMPETENCE CENTRE ;
650, ROUTE DES LUCIOLES ; F-06921
SOPHIA-ANTIPOLIS CEDEX ; FRANCE
,
vol. CT WG1, no. V17.2.0
24 juin 2022 (2022-06-24), pages 1-50,
XP052183246,
Extrait de l'Internet:
URL:https://ftp.3gpp.org/Specs/archive/24_
series/24.582/24582-h20.zip 24582-h20.docx
[extrait le 2022-06-24]

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT