(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 086 830**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **18 58873**

(51) Int Cl[8] : ***H 04 L 9/32*** *(2019.01)*

(12) BREVET D'INVENTION B1

(54) SYNCHRONISATION TEMPORELLE SECURISEE.

(22) **Date de dépôt :** 27.09.18.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 03.04.20 Bulletin 20/14.

(45) **Date de la mise à disposition du public du brevet d'invention :** 06.01.23 Bulletin 23/01.

(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) :** *GORGY TIMING Société par actions simplifiée* —FR, *INSTITUT POLYTECHNIQUE DE GRENOBLE Etablissement public* FR, *UNIVERSITE GRENOBLE ALPES Etablissement public* FR et *CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE* — FR.

(72) **Inventeur(s) :** DUDA ANDRZEJ et MKACHER FATEN.

(73) **Titulaire(s) :** INSTITUT POLYTECHNIQUE DE GRENOBLE Etablissement public, CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE, SCPTime Société par actions simplifiée, UNIVERSITE GRENOBLE ALPES Etablissement public national à caractère scientifique, culturel et professionnel.

(74) **Mandataire(s) :** Cabinet BEAUMONT.

FR 3 086 830 - B1

DESCRIPTION

TITRE : SYNCHRONISATION TEMPORELLE SECURISEE

Domaine technique

[0001] La présente invention concerne en générale les dispositifs électroniques adaptés à communiquer par des réseaux de communication, un protocole de synchronisation temporelle sécurisé et un dispositif et un procédé d'obtention sécurisée d'une estimation temporelle.

Technique antérieure

[0002] La figure 1 illustre schématiquement un système 100 de synchronisation temporelle. Le système comprend un serveur de synchronisation (TS) et un dispositif client de synchronisation (TC) qui communiquent à travers un réseau de communication. Le dispositif client de synchronisation TC est une entité de réseau qui souhaite obtenir une synchronisation temporelle sécurisée, par exemple, pour synchroniser son horloge locale 102 avec une référence précise. Pour ce faire, il contacte le serveur de synchronisation TS par l'intermédiaire du réseau de communication au moyen d'un protocole de synchronisation temporelle (TIME SYNC), tel que le protocole d'heure réseau (NTP : network time protocol).

[0003] Ce serveur de synchronisation TS comprend par exemple une source de synchronisation précise 104, telle qu'un oscillateur micro-atomique ou d'autres moyens de maintien d'une référence temporelle précise.

[0004] Le dispositif client de synchronisation TC peut demander une synchronisation temporelle au serveur de synchronisation TS pendant une phase d'initialisation suivant une première activation du client de synchronisation TC, cette opération pouvant être répétée à intervalles réguliers pour assurer une synchronisation

temporelle entre l'horloge locale 102 du dispositif client de synchronisation TC et la source de synchronisation précise 104 du serveur de synchronisation TS.

[0005] La figure 1 illustre le cas d'un seul dispositif client de synchronisation TC. Toutefois, le dispositif client de synchronisation TC et le serveur de synchronisation TS peuvent faire partie d'un réseau relativement grand dans lequel se trouvent de nombreux dispositifs clients de synchronisation TC servis par le serveur de synchronisation TS. Par exemple, pour les applications telles que la dissémination de temps légal certifié pour les transactions commerciales, il peut exister de nombreux points de vente demandant une synchronisation temporelle. Cependant, on a observé que lorsqu'un serveur de synchronisation TS doit fournir des services à de nombreux dispositifs clients de synchronisation, les capacités du serveur de synchronisation TS peuvent se trouver surchargées et entraîner des retards de synchronisation ou même des échecs de synchronisation. La fourniture d'un système adapté à traiter des demandes en provenance de nombreux dispositifs clients de synchronisation dans un réseau pose un problème technique.

[0006] Un autre problème technique du système de la figure 1 est que pour authentifier le serveur de synchronisation, il faut généralement vérifier le certificat du serveur, y compris sa période de validité. Cependant, lors de l'activation initiale du dispositif client de synchronisation TC, ce dispositif peut n'avoir aucune notion du temps. Ceci entraîne une situation Catch-22 dans laquelle le dispositif client de synchronisation TC devrait avoir une notion préalable de l'heure pour valider le certificat du serveur de synchronisation mais où l'obtention d'informations temporelles en provenance du serveur de

synchronisation TS demande une validation préalable du certificat.

Résumé de l'invention

[0007] Un objet de modes de réalisation de la présente description est de répondre à un ou plusieurs problèmes de l'art antérieur.

[0008] Selon un aspect, la présente invention prévoit un dispositif client de synchronisation comprenant une interface de réseau pour communiquer à travers un réseau de communication, le client de synchronisation étant configuré de manière à : recevoir, à travers le réseau de communication, en provenance d'un serveur d'authentification, une première clé et une première valeur contenant la première clé sous forme cryptée ; produire une deuxième valeur au moyen de la première clé ; et pendant une phase de synchronisation temporelle, transmettre à un serveur de synchronisation les première et deuxième valeurs.

[0009] Selon un mode de réalisation, le dispositif client de synchronisation est configuré, pendant la phase de synchronisation temporelle, de manière à : transmettre la première valeur au serveur de synchronisation dans un premier message comprenant un premier horodatage ; et transmettre la deuxième valeur au serveur de synchronisation dans un deuxième message.

[0010] Selon un mode de réalisation, la deuxième valeur est un code d'authentification de message du premier message produit au moyen de la première clé.

[0011] Selon un mode de réalisation, la première valeur contient en outre une indication de l'algorithme de cryptage à utiliser pour produire la deuxième valeur.

[0012] Selon un mode de réalisation, le dispositif client de synchronisation est par ailleurs configuré de manière à transmettre à travers le réseau de communication une requête à un serveur d'authentification pour obtenir la première clé et la première valeur, cette requête contenant un identifiant du dispositif client de synchronisation, l'identifiant étant par exemple une adresse IP (Internet Protocol : Protocole internet).

[0013] Selon un mode de réalisation, le dispositif client de synchronisation est configuré de manière à comprendre par ailleurs dans la requête un identifiant du serveur de synchronisation, l'identifiant du serveur de synchronisation étant par exemple une adresse IP.

[0014] Selon un mode de réalisation, la première valeur est cryptée au moyen d'une deuxième clé inconnue du dispositif client de synchronisation.

[0015] Selon un mode de réalisation, le dispositif client de synchronisation est de plus configuré de manière à : recevoir du serveur de synchronisation un troisième message contenant un ou plusieurs horodatages ; recevoir du serveur de synchronisation une troisième valeur correspondant à : un premier code d'authentification d'au moins une partie du premier message et/ou d'au moins une partie du troisième message produit au moyen de la première clé ; ou une signature numérique d'au moins une partie du premier message et/ou d'au moins une partie du troisième message produit à partir d'une clé privée ; et l'authentification du troisième message en vérifiant la troisième valeur à partir de la première clé ou d'une clé publique.

[0016] Selon un mode de réalisation, le dispositif client de synchronisation est de plus configuré de manière à : produire une estimation temporelle en demandant à un nœud

d'un réseau de chaînes de blocs des en-têtes d'une série de blocs d'une chaîne de blocs, extraire un horodatage de l'en-tête d'un bloc le plus récent de la série ; et produire l'estimation temporelle à partir de l'horodatage extrait ; et valider un certificat d'authentification du serveur d'authentification à partir de l'estimation temporelle.

[0017] Selon un autre aspect, la présente invention prévoit un système de synchronisation temporelle comprenant : un serveur d'authentification comprenant une interface de réseau pour communiquer à travers un réseau de communication, le serveur d'authentification étant configuré de manière à transmettre à travers le réseau de communication à une premier dispositif client de synchronisation une première clé et une première valeur contenant la première clé sous forme cryptée ; et un serveur de synchronisation configuré de manière à recevoir du premier dispositif client de synchronisation, lors d'une phase de synchronisation temporelle, la première valeur et une deuxième valeur produite au moyen de la première clé, le serveur de synchronisation étant configuré de manière à authentifier le premier dispositif client de synchronisation à partir de la deuxième valeur.

[0018] Selon un mode de réalisation : le serveur d'authentification est par ailleurs configuré de manière à transmettre à travers le réseau de communication à un deuxième dispositif client de synchronisation une troisième clé et une troisième valeur contenant la troisième clé sous forme cryptée ; et le serveur de synchronisation est par ailleurs configuré de manière à recevoir du deuxième dispositif client de synchronisation, pendant une phase de synchronisation temporelle, la troisième valeur et une quatrième valeur produite au moyen de la troisième clé, le serveur de synchronisation étant configuré de manière à

authentifier le deuxième dispositif client de synchronisation à partir de la quatrième valeur.

[0019] Selon un autre aspect, la présente invention prévoit un procédé d'obtention d'une synchronisation temporelle par un dispositif client de synchronisation comprenant une interface de réseau pour communiquer à travers un réseau de communication, ce procédé comprenant : la réception, à travers le réseau de communication en provenance d'un serveur d'authentification, d'une première clé et d'une première valeur contenant la première clé sous forme cryptée ; la production, par le dispositif client de synchronisation, d'une deuxième valeur au moyen de la première clé ; et pendant une phase de synchronisation temporelle, la transmission par le dispositif client de synchronisation des première et deuxième valeurs à un serveur de synchronisation.

[0020] Selon encore un autre aspect, la présente invention prévoit un procédé de synchronisation temporelle par un système de synchronisation temporelle, ce procédé comprenant : la transmission, par un serveur d'authentification à travers un réseau de communication à un dispositif client de synchronisation, d'une première clé et d'une première valeur contenant la première clé sous forme cryptée ; pendant une phase de synchronisation temporelle, la réception par un serveur de synchronisation en provenance du dispositif client de synchronisation de la première valeur et d'une deuxième valeur produite au moyen de la première clé ; et l'authentification, par le serveur de synchronisation, du dispositif client de synchronisation à partir de la deuxième valeur.

[0021] Selon un autre aspect, la présente invention prévoit un procédé de production d'une estimation temporelle au

moyen d'un dispositif électronique comprenant une interface de réseau pour communiquer à travers un réseau de communication, ce procédé comprenant : la demande, par le dispositif électronique à un nœud d'un réseau de chaînes de blocs, d'en-têtes d'une série de blocs d'une chaîne de blocs ; l'extraction d'un horodatage de l'en-tête d'un bloc le plus récent de la série ; et produire une estimation temporelle à partir de l'horodatage extrait.

[0022] Selon un mode de réalisation, le procédé consiste en outre à : demander à un autre nœud du réseau de chaînes de blocs des en-têtes de la série de blocs de la chaîne de blocs ; et extraire un autre horodatage de l'en-tête du bloc le plus récent de la série, dans lequel la production de l'estimation temporelle est en outre basée sur l'autre horodatage.

[0023] Selon un mode de réalisation, la chaîne de blocs comprend une chaîne de blocs allant d'un bloc d'origine à un N-ème bloc produit le plus récemment, l'en-tête du bloc le plus récent de la série étant un (N-j)-ème bloc de la chaîne de blocs, j étant compris entre 6 et 15.

[0024] Selon un mode de réalisation, chaque bloc de la chaîne de blocs, hormis le bloc d'origine, comprend une empreinte d'un bloc précédent de la chaîne.

[0025] Selon un mode de réalisation, la chaîne de blocs est la chaîne de blocs d'une crypto-monnaie.

[0026] Selon un autre aspect, la présente invention prévoit un procédé de vérification d'un certificat d'authentification comprenant : la production d'une estimation temporelle selon le procédé ci-dessus ; et la vérification par le dispositif électronique de la validité temporelle du certificat d'authentification à partir de l'estimation temporelle produite.

[0027] Selon encore un autre aspect, la présente invention prévoit un dispositif électronique comprenant une interface de réseau pour communiquer à travers un réseau de communication, le dispositif électronique étant configuré de manière à : demander à un nœud d'un réseau de chaînes de blocs des en-têtes d'une série de blocs d'une chaîne de blocs ; extraire un horodatage de l'en-tête d'un bloc le plus récent de la série ; et produire une estimation temporelles à partir de l'horodatage extrait.

[0028] Selon un mode de réalisation, le dispositif électronique est de plus configuré de manière à : demander à un autre nœud du réseau de chaînes de blocs des en-têtes de la série de blocs de la chaîne de blocs ; et extraire un autre horodatage de l'en-tête du bloc le plus récent de la série, dans lequel la production de l'estimation temporelle s'effectue en outre à partir de l'autre horodatage.

[0029] Selon un mode de réalisation, la chaîne de blocs comprend une chaîne de blocs allant d'un bloc d'origine à un N-ème bloc produit le plus récemment, l'en-tête du bloc le plus récent de la série étant un (N-j)-ème bloc de la chaîne de blocs, j étant compris entre 6 et 15.

[0030] Selon un mode de réalisation, le dispositif électronique est par ailleurs configuré de manière à vérifier la validité temporelle d'un certificat d'authentification à partir de l'estimation temporelle produite.

Brève description des dessins

[0031] Ces caractéristiques et avantages, ainsi que d'autres, seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

[0032] [Fig. 1] la figure 1 (décrite ci-dessus) illustre schématiquement un système de synchronisation temporelle ;

[0033] [Fig. 2] la figure 2 illustre schématiquement un système de synchronisation temporelle selon un exemple de réalisation de la présente invention ;

[0034] [Fig. 3] la figure 3 représente des communications entre entités de réseau dans le système de la figure 2 selon un exemple de réalisation de la présente invention ;

[0035] [Fig. 4] la figure 4 illustre schématiquement un système de production sécurisée d'une estimation temporelle selon un exemple de réalisation de la présente invention ;

[0036] [Fig. 5] la figure 5 représente une chaîne de blocs selon un exemple de réalisation de la présente invention ;

[0037] [Fig. 6] la figure 6 est un organigramme représentant des opérations d'un procédé de production sécurisée d'une estimation temporelle selon un exemple de réalisation de la présente invention ; et

[0038] [Fig. 7] la figure 7 illustre schématiquement un dispositif client de synchronisation selon un exemple de réalisation de la présente invention.

Description des modes de réalisation

[0039] De mêmes éléments ont été désignés par de mêmes références dans les différentes figures. En particulier, les éléments structurels et/ou fonctionnels communs aux différents modes de réalisation peuvent présenter les mêmes références et peuvent disposer de propriétés structurelles, dimensionnelles et matérielles identiques.

[0040] Sauf indication contraire, on utilise le terme "connecté" pour désigner une connexion électrique directe entre éléments de circuit, tandis que l'on utilise le terme "relié" ou "couplé" pour désigner une connexion électrique

entre éléments de circuit qui peut être directe ou s'effectuer par l'intermédiaire d'un ou plusieurs éléments.

[0041] Sauf précision contraire, les expressions "environ", "approximativement", "sensiblement" et "de l'ordre de" signifient à 10% près, de préférence à 5% près.

[0042] La figure 2 illustre schématiquement un système 200 de synchronisation temporelle selon un exemple de réalisation de la présente invention.

[0043] Le système 200 comprend des dispositifs clients de synchronisation TC1 et TC2 comprenant chacun une horloge locale 102 semblable à celle du dispositif client de synchronisation TC de la figure 1. En outre, chacun des dispositifs TC1, TC2 comprend par exemple une interface de réseau pour communiquer à travers un réseau avec un serveur de synchronisation TS. Ce réseau est par exemple un réseau à commutation de paquets comprenant par exemple un ou plusieurs réseaux locaux (LAN), réseaux locaux sans fil (WLAN) et/ou internet. Bien que l'exemple illustré comprenne deux dispositifs clients de synchronisation, en pratique, le serveur de synchronisation TS peut servir de nombreux dispositif client de synchronisation, par exemple des centaines ou même des milliers de tels dispositifs. Dans un exemple de réalisation, les dispositifs clients de synchronisation TC1, TC2 sont des points de vente et le serveur de synchronisation TS dissémine du temps légal certifié aux points de vente pour les transactions commerciales.

[0044] Le serveur de synchronisation TS est semblable au serveur de synchronisation de la figure 1 et comprend une source de synchronisation 104 relativement précise, qui comprend par exemple un micro-oscillateur atomique ou d'autres moyens de maintien d'une référence temporelle

précise. Dans certains modes de réalisation, la source de synchronisation 104 est basée sur un oscillateur au rubidium ou un OCXO (oscillateur à quartz thermostaté), mais d'autres types d'oscillateur sont possibles.

[0045] Le système 200 comprend en outre un serveur d'authentification AS, comprenant par exemple une horloge locale précise 202.

[0046] Chacun des clients de synchronisation TC1 et TC2 peut demander une synchronisation temporelle au serveur de synchronisation TS. Par exemple, de telles demandes peuvent se produire quand le dispositif TC1 ou TC2 est activé pour la première fois et/ou à intervalles réguliers au cours de la vie des dispositifs TC1 et TC2 pour maintenir la synchronisation temporelle. En effet, l'horloge locale 102 de chaque dispositif client de synchronisation TC1, TC2 dérive par exemple dans une certaine mesure au cours du temps, de sorte qu'en se resynchronisant avec le serveur de synchronisation TS, les dispositifs TC1 et TC2 peuvent maintenir une heure relativement précise, par exemple avec une précision de quelques millisecondes par rapport au temps universel coordonné.

[0047] Pour permettre une synchronisation temporelle sécurisée entre les dispositifs clients de synchronisation TC1 et TC2 et le serveur de synchronisation TS, une phase de configuration (CONFIG) est par exemple mise en œuvre au moyen du serveur d'authentification AS. Ceci implique par exemple des communications entre le serveur d'authentification AS et le serveur de synchronisation TS et entre le serveur d'authentification AS et chaque dispositif client de synchronisation TC1, TC2. On va à présent décrire plus en détail un procédé de mise en œuvre de cette phase de configuration et d'une phase ultérieure de

synchronisation temporelle (TIME SYNC) avec le dispositif client de synchronisation TC1 en référence à la figure 3. Un procédé semblable pourrait être mis en œuvre pour le dispositif client de synchronisation TC2.

[0048] La figure 3 représente les communications entre le dispositif client de synchronisation TC1, le serveur d'authentification AS et le serveur de synchronisation TS de la figure 2 selon un exemple de réalisation de la présente invention.

[0049] Avant le début des communications entre les parties, une opération de réglage (SETUP) a par exemple lieu, pendant laquelle une authentification mutuelle à partir de certificats est mise en œuvre entre le dispositif client de synchronisation TC1 et le serveur d'authentification AS et entre le serveur de synchronisation TS et le serveur d'authentification AS. Ceci implique par exemple l'établissement d'une session DTLS (datagram transport layer security : Sécurité de la couche de transport en mode datagramme), de façon connue de l'homme de l'art. La session DTLS crée des canaux sécurisés qui sont utilisés pour échanger des messages pendant la phase de configuration.

[0050] La phase de configuration (CONFIG) entre le serveur de synchronisation TS et le serveur d'authentification AS est par exemple mise en œuvre une fois ou à intervalles relativement peu fréquents, par exemple une fois par mois pour rafraîchir les matériaux cryptographiques utilisé pendant la synchronisation temporelle. Pendant cette phase, le serveur de synchronisation TS transmet par exemple au serveur d'authentification AS les algorithmes cryptographiques ALGO_TS pris en charge, y compris, dans certains modes de réalisation, les codes d'authentification de

message (MAC : message authentication code) pris en charge et/ou les signatures numériques (DS : digital signature) prises en charge.

[0051] Le serveur d'authentification AS répond en produisant et en transmettant au serveur de synchronisation TS une clé S qui est par exemple un secret à long terme destiné à être utilisé par le serveur de synchronisation TS. Au cas où une infrastructure de clé publique (PKI : Public Key Infrastructure) doit être utilisée pour signer les messages au client de synchronisation, le serveur d'authentification AS produit et transmet par exemple également au serveur de synchronisation TS un couple clé privée/clé publique Ke/Kd. Les mêmes clés S, Ke et Kd sont par exemple utilisées pour les communications avec chaque dispositif client de synchronisation, de sorte que le serveur de synchronisation TS n'a pas besoin de mémoriser une clé différente à utiliser avec chaque dispositif client de synchronisation.

[0052] La phase de configuration (CONFIG) entre le dispositif client de synchronisation TC1 et le serveur d'authentification AS (et entre les autres dispositifs clients de synchronisation et le serveur d'authentification) est par exemple mise en œuvre après la phase de configuration avec le serveur de synchronisation TS décrit ci-dessus. Le dispositif client de synchronisation TC1 initie par exemple la phase de configuration en transmettant au serveur d'authentification AS : son identifiant TCID, qui se présente par exemple sous la forme d'une adresse IP du dispositif client de synchronisation automatiquement contenue dans le message transmis ; un identifiant TSID du serveur de synchronisation TS avec lequel le dispositif client de synchronisation TC1 souhaite réaliser une synchronisation temporelle ; et les algorithmes cryptographiques ALGO_TC pris en charge, y compris, dans certains

modes de réalisation, les codes MAC pris en charge et/ou la signature numérique DS prise en charge. Dans des variantes de réalisation, le dispositif client de synchronisation TC1 ne transmet pas l'identifiant TSID du serveur de synchronisation TS mais, au lieu de cela, le serveur d'authentification AS propose un serveur de synchronisation TS au dispositif client de synchronisation TC1.

[0053] Comme on le décrira plus en détail ci-dessous, le serveur de synchronisation TS est par exemple configuré pour authentifier les messages de synchronisation temporelle qu'il envoie au client de synchronisation TC1 au moyen, soit d'un code MAC produit au moyen d'une clé symétrique K, soit d'une signature numérique DS produite au moyen de la clé privée Kd.

[0054] En supposant qu'au moins l'un des algorithmes cryptographiques pris en charge par le serveur de synchronisation TS est également pris en charge par le dispositif client de synchronisation TC1, le serveur d'authentification AS répond par exemple en fournissant au client de synchronisation TC1 la clé symétrique K et, dans certains cas, la clé d'accès public Ke du serveur de synchronisation TS, ainsi que le ou les algorithme(s) cryptographique(s) négocié(s) ALOG_TC_TS compatible(s) à la fois avec le serveur de synchronisation TS et le dispositif client de synchronisation TC1 et à utiliser pour les communications entre eux. Pour ce faire, le serveur d'authentification AS comprend par exemple une mémoire stockant, pour chaque dispositif client de synchronisation et pour chaque serveur de synchronisation TS dans le cas où il en en a plus d'un, les relations TSID-[S,(Ke,Kd)] et TCID-[K,C], dans lesquelles les identifiants TSID et TCID peuvent correspondre à des adresses IP du serveur de

synchronisation et du dispositif client de synchronisation, respectivement.

[0055] Le serveur d'authentification AS fournit par exemple au dispositif client de synchronisation TC1 un état C, sous forme d'une valeur cryptée. En particulier, l'état C correspond par exemple à la clé symétrique K et dans certains modes de réalisation, à une ou plusieurs valeurs, toutes cryptées au moyen de la clé S du serveur de synchronisation TS. La clé K est par exemple unique pour chaque dispositif client de synchronisation et l'utilisation de l'état C permet par exemple au serveur de synchronisation d'être sans état, c'est-à-dire qu'il n'a pas besoin de mémoriser la clé K associée à chaque dispositif client de synchronisation, comme on le décrira plus en détail ci-dessous. La clé S est par exemple inconnue du dispositif client de synchronisation TC1, qui ne peut par conséquent pas décrypter ou modifier l'état C. Seul le serveur de synchronisation TS est par exemple adapté à décrypter l'état C. Les autres valeurs cryptées dans l'état C peuvent comprendre une valeur indiquant le ou les algorithme(s) négocié(s) ALOG_TC_TS choisi(s) pour être utilisé(s) dans les communications entre le dispositif client de synchronisation TC1 et le serveur de synchronisation TS.

[0056] Par exemple, l'algorithme négocié pour les communications entre le dispositif client de synchronisation TC1 et le serveur de synchronisation TS est la primitive cryptographique connue sous le nom d'algorithme AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) ou un réseau de Feistel.

[0057] Les algorithmes MAC pris en charge par le serveur de synchronisation et/ou par le dispositif client de

synchronisation TC1 comprennent par exemple l'algorithme HMAC-SHA256 (Hash-based Message Authentication Code - Secure Hash Algorithm) et/ou l'algorithme AES-CMAC (Advanced Encryption Standard - Cipher-based Message Authentication Code) et/ou l'algorithme HMAC-MD5 (HMAC - Message Digest 5).

[0058] La signature numérique DS prise en charge par le serveur de synchronisation et/ou par le dispositif client de synchronisation TC1 comprend par exemple la signature Ed25519, qui est une signature EdDSA (Edwards-curve Digital Signature Algorithm) utilisant SHA-512 et Curve25519, et/ou la signature MQQ-SIG (Multivariate Quadratic Quasigroups Signature).

[0059] Pour initier une phase de synchronisation temporelle (TIME SYNC), le dispositif client de synchronisation TC1 transmet par exemple un message m1 au serveur de synchronisation TS. Le message m1 comprend par exemple des données correspondant au protocole particulier à utiliser pour la synchronisation temporelle. Par exemple, dans le cas du protocole NTP, le message comprend un horodatage T1 correspondant à l'horodatage du dispositif client de synchronisation TC1 à l'instant où le message m1 est produit et transmis. En outre, le message m1 comprend par exemple un nonce n, ainsi que l'état C. Le nonce n est par exemple une valeur aléatoire comprise dans chaque message m1 et assure une protection contre les attaques par rejeu. Par exemple, le serveur de synchronisation TS comprend ce nonce n, ou un code MAC ou une signature numérique basé sur ce nonce, dans un message de réponse ultérieur (décrit plus en détail ci-dessous) au dispositif client de synchronisation, qui peut alors vérifier que le nonce n est le même.

[0060] Le dispositif client de synchronisation TC1 transmet par exemple également au serveur de synchronisation TS un deuxième message m2 comprenant une valeur τ1 correspondant par exemple à une valeur de code MAC MAC_K(m1) produite au moyen de la clé symétrique K. Par exemple, cette valeur de code MAC est un code produit à partir du premier message m1 déjà reçu par le serveur de synchronisation TS. A titre de variante, il pourrait être produit à partir d'une partie du message m1 seulement, par exemple, à partir de l'état C ou du nonce n.

[0061] Les messages m1 et m2 sont par exemple transmis de manière indépendante, de sorte que le serveur de synchronisation TS peut traiter le message initial m1 aussitôt qu'il est reçu sans vérifier préalablement le code MAC. Ainsi, on améliore la qualité de l'opération de synchronisation temporelle. Toutefois, dans des variantes de réalisation, les messages m1 et m2 pourraient être transmis en un seul message.

[0062] Le serveur de synchronisation TS répond par exemple au message m1 en produisant et en transmettant au dispositif client de synchronisation TC1 un message m3 contenant l'horodatage T1 ainsi que les horodatages T2 et T3 conformément au protocole NTP. Par exemple, l'horodatage T2 correspond à l'instant de réception du message m1 par le serveur de synchronisation TS et l'horodatage T3 correspond à l'instant de transmission du message m3 au dispositif client de synchronisation TC1.

[0063] Le serveur de synchronisation TS décrypte également par exemple la valeur cryptée C à partir de sa clé secrète S et en extrait la clé symétrique K et, dans certains modes de réalisation, l'algorithme négocié ALGO_TC_TS. Le serveur de synchronisation TS est ensuite par exemple en mesure de

vérifier le code d'authentification de message MAC MAC_K(m1) fourni dans le message m2 à partir de la clé symétrique K.

[0064] Le serveur de synchronisation TS transmet également par exemple un message m4 au dispositif client de synchronisation TC1 après le message m3, le message m4 étant utilisé pour l'authentification. Par exemple, le message m4 comprend une valeur τ2 correspondant par exemple à un code MAC MAC_K(m1||m3) produit au moyen de la clé symétrique K et à partir d'au moins un des messages m1 et m3, et de préférence à partir des deux messages m1 et m3. A titre de variante, l'authentification pourrait être réalisée par une signature numérique DS_kd(m1||m3), correspondant à une signature d'au moins l'un des messages m1 et m3, et de préférence à partir des deux messages m1 et m3. Cette signature numérique est par exemple produite au moyen de la clé privée Kd du serveur de synchronisation TS. Dans certains cas, le serveur de synchronisation TS est adapté à produire à la fois le code MAC MAC_K(m1||m3) et la signature numérique DS_kd(m1||m3) et une sélection est effectuée, par exemple par le dispositif client de synchronisation TC1, entre ces deux sortes de types d'authentification de message selon que la propriété de non répudiation est souhaitée ou non.

[0065] Dans des variantes de réalisation, le code MAC et/ou la signature numérique pourraient être produits à partir d'une partie seulement des messages m1 et m3, par exemple à partir du nonce du message m1 seulement et/ou des horodatages T2 et T3 du message m3 seulement.

[0066] Le dispositif client de synchronisation TC1 est alors en mesure de déterminer une estimation relativement précise du temps en calculant le décalage temporel de son horloge

locale 102 par rapport à l'horloge 104 du serveur de synchronisation TS et le temps de propagation aller et retour RTT des communications entre le client de synchronisation TC1 et le serveur de synchronisation TS, qui sont par exemple déterminés par les équations suivantes :

[0067] [Math 1]

$$Offset = \frac{(T2 - T1) - (T4 - T3)}{2}$$

[0068]

[Math 2]

$$RTT = (T4 - T1) - (T3 - T2)$$

où T4 est un horodatage correspondant à l'instant de réception du message m3 par le dispositif client de synchronisation TC1.

[0069] Le dispositif client de synchronisation TC1 est par exemple configuré pour régler son horloge à partir des valeurs calculées d'Offset et de RTT. Comme le comprendra l'homme de l'art, dans certains cas, l'opération de synchronisation est répétée plusieurs fois et le réglage d'horloge se fait à partir d'un filtrage et/ou d'une analyse statistique de l'ensemble calculé de valeurs d'Offset et de RTT. En outre, dans certains modes de réali-sation, la valeur de RTT est comparée à un paramètre de seuil Δ, et le dispositif client de synchronisation TC1 est configuré pour rejeter le message m4 et/ou faire avorter la synchronisation temporelle si la valeur de RTT dépasse le paramètre de seuil Δ, assurant ainsi la défense contre les attaques par introduction d'un retard.

[0070] Le dispositif client de synchronisation TC1 authentifie également par exemple les informations temporelles fournies par le serveur de synchronisation TS en vérifiant

le code d'authentification ou la signature numérique fournis avec le message m4. Dans le cas où le message m4 comprend le code MAC MAC_K(m1||m3), le dispositif client de synchronisation TC1 vérifie par exemple ce code à partir de la clé symétrique K, par exemple en recalculant le code MAC et en comparant le code MAC recalculé avec celui fourni avec le message m4. Dans le cas où le message m4 comprend la signature numérique DS_kd(m1||m3), le dispositif client de synchronisation TC1 vérifie par exemple cette signature en décryptant la signature au moyen de sa clé publique Ke.

[0071] Comme on l'a décrit ci-dessus en relation avec la figure 3, les communications initiales entre le serveur d'authentification AS et le dispositif client de synchronisation TC1 et le serveur de synchronisation TS correspondent à une phase de réglage pendant laquelle une authentification mutuelle est effectuée, par exemple à partir d'un échange de certificats. Toutefois, le dispositif client de synchronisation TC1 peut être un dispositif dépourvu d'horloge synchrone et qui n'a donc pas de notion de l'heure à sa première mise sous tension.

[0072] On va à présent décrire un système et un procédé d'obtention sécurisée d'une estimation temporelle en référence aux figures 4 à 6. Le dispositif électronique pourrait correspondre à un dispositif client de synchronisation TC1 ou TC2 de la figure 2 à des fins de validation de certificat ou à tout dispositif électronique souhaitant obtenir une estimation de l'heure actuelle.

[0073] La figure 4 illustre schématiquement un système 400 de production d'une estimation temporelle selon un exemple de réalisation de la présente invention.

[0074] Dans le système 400, un dispositif électronique 402 souhaite obtenir une estimation de l'heure actuelle. Par

exemple, le dispositif 402 est un dispositif dépourvu d'interface utilisateur ou pourvu d'une interface utilisateur ne permettant pas la saisie d'informations temporelles. Dans certains modes de réalisation, le dispositif 402 est un dispositif électronique portable adapté à des communications sans fil, tel qu'un dispositif IoT (Internet of Things : Internet des objets).

[0075] Selon les modes de réalisation décrits ici, l'estimation temporelle est obtenue en utilisant un réseau de chaînes de blocs 406. Le réseau de chaînes de blocs 406 comprend par exemple J nœuds, chacun mémorisant des versions semblables d'une même chaîne de blocs BC. Le nombre J de nœuds est par exemple égal à au moins 2 et pourrait être égal à des centaines ou à des milliers. Le dispositif 402 demande certaines données de la chaîne de blocs BC à un nœud 404 d'un réseau de chaînes de blocs 406.

[0076] La chaîne de blocs BC est par exemple une chaîne de blocs publique immuable, telle que la chaîne de blocs d'une crypto-monnaie telle que le Bitcoin ou équivalent (le nom "Bitcoin" est susceptible de correspondre à une marque déposée). De manière connue de l'homme de l'art, un réseau de chaînes de blocs constitue de par sa conception une source de confiance, du fait de sa structure particulière.

[0077] Un horodatage est par exemple obtenue par le dispositif 402 à partir d'un ou plusieurs blocs de la chaîne de blocs par un accès de pair à pair. Un accès de pair à pair à la chaîne de blocs Bitcoin est par exemple décrit plus en détail dans la publication de S. Nakamoto intitulée "Bitcoin: A peer-to-peer Electronic Cash System", mai 2011. Dans certains modes de réalisation, le dispositif 402 demande les en-têtes d'une série de blocs de la chaîne de blocs BC et extrait un horodatage de l'un de ces en-têtes.

[0078] La figure 5 représente la chaîne de blocs BC de la figure 4 selon un exemple de réalisation. La chaîne de blocs BC comprend par exemple les blocs B0 à BN, le bloc B0 étant un bloc d'origine de la chaîne de blocs BC et le bloc BN étant le bloc le plus récent de la chaîne de blocs BC. Chaque bloc comprend par exemple un en-tête (HEADER) contenant un identifiant (BLOCK 0 à BLOCK N) du bloc, ainsi qu'un horodatage (TIMESTAMP). Chaque bloc comprend en outre des données qui, dans le cas du bloc de crypto-monnaie, correspondent par exemple à des données de grand livre comptable (LEDGER DATA). En outre, le bloc d'origine B0 comprend une empreinte (HASH) de son propre contenu et chaque autre bloc comprend en outre une empreinte du bloc précédent (HASH (PREV)), rendant ainsi difficile la modification des blocs les plus anciens sans approbation de la majorité des nœuds du réseau de chaînes de blocs.

[0079] La figure 6 est un organigramme illustrant des étapes d'un procédé de production d'une estimation temporelle selon un exemple de réalisation de la présente invention.

[0080] On suppose que le dispositif 402 a par exemple identifié le nœud 404 en tant que pair dans le réseau de chaînes de blocs 406 et connaît l'adresse IP de ce pair. Par exemple, le dispositif 402 a réalisé une opération de découverte de pair, en utilisant par exemple plusieurs graines DNS ou adresses IP codées en dur.

[0081] A une opération 601, le dispositif électronique 402 demande une série d'en-têtes au pair 404. Une commande "GetHeaders" (récupérer les en-têtes) est par exemple utilisée. Cette commande se présente par exemple sous la forme *GetHeaders(X,L)*, X étant l'identifiant du dernier bloc demandé et L étant le nombre d'en-têtes demandés. Dans

le cas de nœuds de Bitcoin, un maximum de 2 000 en-têtes peut être fourni.

[0082] Dans certains modes de réalisation, un certain nombre d'en-têtes des blocs les plus récents, qui peuvent rester sujets à changement et ne sont pas nécessairement immuables, sont exclus de la demande. Par exemple, l'en-tête du bloc le plus récent demandé est l'en-tête du (N-j)-ème bloc, le N-ème bloc étant le bloc le plus récent, et j étant compris entre 6 et 15, et dans un exemple égal à 10.

[0083] Le pair 404 prend par exemple l'empreinte du (N-j)-ème bloc et répond au dispositif 402 avec la série demandée d'en-têtes en chaîne après le block N-j. Le dispositif 402 répète alors par exemple la synchronisation des en-têtes pour atteindre la fin de la chaîne de blocs et identifie l'en-tête du bloc le plus récent N-j de la série.

[0084] A une opération 602, le dispositif électronique 402 extrait l'horodatage de l'en-tête du bloc le plus récent N-j. Dans certains modes de réalisation, cet horodatage a le même format que l'horodatage sur 64 bits utilisé en NTP, tandis que dans d'autres modes de réalisation, le format de l'horodatage de chaîne de bloc pourrait être différent et converti dans le format approprié.

[0085] Comme le représente la flèche en traits tiretés de la figure 6, les opérations 601 et 602 peuvent être répétées pour un ou plusieurs nœuds ou pairs de la chaîne de blocs pour assurer d'autres vérifications de l'authenticité des en-têtes et pour assurer une protection contre les attaques MITM (man-in-the-middle : par hôte interposé) et par usurpation d'identité. Ceci implique par exemple de demander les en-têtes de la série de blocs à un autre pair, d'identifier l'en-tête du bloc le plus récent de la série,

qui est par exemple à nouveau l'en-tête du (N-j)-ème bloc, puis d'extraire l'horodatage de cet en-tête. Le nouvel horodatage est par exemple comparé à l'horodatage extrait précédemment pour vérifier qu'ils sont identiques, vérifiant de la sorte l'horodatage à partir de deux nœuds séparés.

[0086] A une opération 603, une heure actuelle est estimée à partir du ou des horodatage(s) extrait(s) et une horloge locale 102 du dispositif électronique 402 est par exemple synchronisée à partir de l'estimation temporelle.

[0087] Comme l'horodatage sur laquelle on s'appuie n'est pas celui du bloc le plus récent de la chaîne de blocs, il peut y avoir un décalage temporel entre l'heure de l'horodatage extrait et l'heure réelle, qui dépendra de la valeur de j. Les présents inventeurs ont cependant observé qu'il est généralement possible de choisir une valeur de j qui fournisse une heure précise à quelques heures près, ce qui suffit généralement pour valider un certificat d'authentification. En effet, de tels certificats sont généralement valides jusqu'à une certaine date. Le choix du paramètre j se fonde par exemple sur la propriété de validité de l'horodatage dans la chaîne de blocs.

[0088] A une opération 604, un certificat est par exemple validé à partir de l'estimation temporelle. Ainsi, un certificat révoqué peut être identifié et rejeté par le dispositif 402. A titre de variante, d'autres utilisations de l'estimation temporelle produite pourraient être faites.

[0089] La figure 7 illustre schématiquement le dispositif client de synchronisation TC1 de la figure 2 plus en détail selon un exemple de réalisation.

[0090] Le dispositif TC1 comprend par exemple un processeur (P) 702 comprenant un ou plusieurs cœurs de processeur. Le

processeur 702 est par exemple couplé à une horloge locale (LOCAL CLOCK) 102, qui comprend par exemple un oscillateur local, tel qu'un oscillateur à quartz ou équivalent, ainsi qu'un ou plusieurs compteurs. Le dispositif TC1 comprend également par exemple une interface de réseau (NETWORK INTERFACE) 704 et une mémoire (MEMORY) 706 couplées au processeur 702.

[0091] La mémoire 706 stocke par exemple des instructions qui, lorsqu'elles sont exécutées par le processeur 702, provoquent la mise en œuvre des opérations du dispositif client de synchronisation TC1 décrites ci-dessus en relation avec la figure 3.

[0092] Le dispositif client de synchronisation TC2, le serveur d'authentification AS et le dispositif électronique 402 de la figure 4 sont par exemple réalisés par des circuits semblables à celui de la figure 2. Le serveur de synchronisation TS est également par exemple mis en œuvre par un circuit semblable, si ce n'est que, au lieu ou en plus de l'horloge locale 102, le serveur de synchronisation TS comprend la source de synchronisation sécurisée 104. En outre, dans le cas du dispositif 402, sa mémoire stocke par exemple des instructions qui mettent en œuvre le procédé décrit ci-dessus en relation avec la figure 6. En ce qui concerne le serveur de synchronisation TS et le serveur d'authentification AS, ces dispositifs comprennent également des mémoires stockant des instructions qui mettent en œuvre les opérations de ces dispositifs décrits ci-dessus en relation avec la figure 3.

[0093] Un avantage des modes de réalisation décrits en relation avec les figures 2 et 3 est que le serveur d'authentification AS soulage le serveur de synchronisation TS d'une quantité importante de sa charge, en particulier

la négociation d'algorithme et les échanges de clé. Ceci permet au serveur de synchronisation TS de manipuler les opérations de synchronisation temporelle avec un nombre relativement élevé de dispositifs clients de synchronisation et assure une disponibilité relativement élevée du serveur de synchronisation TS. Malgré l'utilisation du serveur d'authentification AS, les échanges entre le dispositif client de synchronisation et le serveur de synchronisation TS sont sécurisés par la production et la transmission au serveur de synchronisation d'un code d'authentification par le dispositif client de synchronisation à partir de la clé symétrique K fournie par le serveur d'authentification AS. En outre, en permettant au serveur de synchronisation TS d'être authentifié au moyen d'une signature numérique à partir de clés asymétriques, la non répudiation peut être prise en charge, tandis que les opérations critiques du point de vue temporel continuent de s'appuyer sur une cryptographie symétrique au moyen de la clé symétrique K.

[0094] Un avantage des modes de réalisation décrits en relation avec les figures 4 à 6 est qu'il est possible d'obtenir une estimation temporelle sûre de manière simple et sécurisée.

[0095] Divers modes de réalisation et variantes ont été décrits. L'homme de l'art comprendra qu'il est possible de combiner certaines caractéristiques de ces modes de réalisation et d'autres variantes apparaîtront à l'homme de l'art. Il apparaîtra en particulier à l'homme de l'art que bien que l'on ait décrit des modes de réalisation en relation avec le protocole NTP, les principes décrits ici peuvent s'appliquer à n'importe quel protocole de synchronisation temporelle. En outre, bien que des modes de réalisation aient été décrits dans lesquels un ou

plusieurs algorithmes cryptographiques à utiliser dans les communications entre un dispositif client de synchronisation et le serveur de synchronisation sont négociés, une telle négociation peut être omise dans des variantes de réalisation, si par exemple un seul algorithme cryptographique est désigné pour être utilisé par tous les dispositifs clients de synchronisation pour chaque opération cryptographique particulière (cryptage, production de code MAC, production de signature DS).

[0096] En outre, bien que la figure 5 donne un exemple de chaîne de blocs, les principes décrits ici peuvent être appliqués à une vaste gamme de types de chaînes de blocs dans lesquelles chaque bloc comprend un horodatage.

[0097] Il apparaîtra également à l'homme de l'art qu'il est possible de combiner le mode de réalisation de la figure 2 avec le mode de réalisation de la figure 4, le dispositif client de synchronisation TC1 étant capable d'obtenir une estimation temporelle pour valider un certificat d'authentification, par exemple en relation avec un session DTLS, avant la phase de configuration par le serveur d'authentification AS.

REVENDICATIONS

1. Dispositif client de synchronisation comprenant une interface de réseau pour communiquer à travers un réseau de communication, le dispositif client de synchronisation étant configuré de manière à :
- recevoir, à travers le réseau de communication en provenance d'un serveur d'authentification (AS), une première clé (K) et une première valeur (C) contenant la première clé (K) sous forme cryptée ;
- produire une deuxième valeur (MAC_K(m1)) au moyen de la première clé (K); et
- pendant une phase de synchronisation temporelle, transmettre à un serveur de synchronisation (TS) les première et deuxième valeurs (C, MAC_K(m1)).

2. Dispositif client de synchronisation selon la revendication 1, configuré, pendant la phase de synchronisation temporelle, de manière à :
- transmettre la première valeur (C) au serveur de synchronisation (TS) dans un premier message (m1) comprenant un premier horodatage (T1) et ;
- transmettre la deuxième valeur (MAC_K(m1)) au serveur de synchronisation (TS) dans un deuxième message (m2).

3. Dispositif client de synchronisation selon la revendication 2, dans lequel la deuxième valeur est un code d'authentification de message (MAC_K(m1)) du premier message (m1) produit au moyen de la première clé (K).

4. Dispositif client de synchronisation selon l'une quelconque des revendications 1 à 3, dans lequel la première valeur (C) contient en outre une indication d'un algorithme de cryptage (ALGO_TC_TS) à utiliser pour produire la deuxième valeur (MAC_K(m1)).

5. Dispositif client de synchronisation selon l'une quelconque des revendications 1 à 4, par ailleurs configuré de manière à transmettre à travers le réseau de communication une requête à un serveur d'authentification (AS) pour obtenir la première clé (K) et la première valeur (C), la requête contenant un identifiant (TCID) du dispositif client de synchronisation, l'identifiant étant par exemple une adresse IP (Internet Protocol : Protocole internet).

6. Dispositif client de synchronisation selon la revendication 5, configuré de manière à comprendre par ailleurs dans la requête un identifiant (TSID) du serveur de synchronisation (TS), l'identifiant du serveur de synchronisation (TS) étant par exemple une adresse IP.

7. Dispositif client de synchronisation selon l'une quelconque des revendications 1 à 6, dans lequel la première valeur (C) est cryptée au moyen d'une deuxième clé (S) inconnue du dispositif client de synchronisation.

8. Dispositif client de synchronisation selon l'une quelconque des revendications 1 à 7, par ailleurs configuré de manière à :

   - recevoir du serveur de synchronisation (TS) un troisième message (m3) contenant un ou plusieurs horodatages (T2, T3) ;

   - recevoir du serveur de synchronisation (TS) une troisième valeur (MAC_K(m1||m3), DS_Kd(m1||m3)) correspondant à : un code d'authentification de message d'au moins une partie du premier message (m1) et/ou d'au moins une partie du troisième message (m3) produit au moyen de la première clé (K) ; ou une signature numérique d'au moins une partie du premier message (m1) et/ou d'au moins une partie du troisième message (m3) produite à partir d'une clé privée (Kd) ; et

- authentifier le troisième message en vérifiant la troisième valeur (MAC_K(m1||m3), DS_Kd(m1||m3)) à partir de la première clé (K) ou d'une clé publique (Ke).

9. Dispositif client de synchronisation selon l'une quelconque des revendications 1 à 8, par ailleurs configuré de manière à :

- produire une estimation temporelle en demandant à un nœud (404) d'un réseau de chaînes de blocs (406) des en-têtes d'une série de blocs (B0 à BN) d'une chaîne de blocs (BC), extraire un horodatage de l'en-tête d'un bloc le plus récent de la série ; et produire l'estimation temporelle à partir de l'horodatage extrait ; et
- valider un certificat d'authentification du serveur d'authentification (AS) à partir de l'estimation temporelle.

10. Système de synchronisation temporelle comprenant :

- un serveur d'authentification (AS) comprenant une interface de réseau pour communiquer à travers un réseau de communication, le serveur d'authentification (AS) étant configuré de manière à transmettre à travers le réseau de communication à un premier dispositif client de synchronisation (TC1) une première clé (K) et une première valeur (C) contenant la première clé (K) sous forme cryptée ; et

- un serveur de synchronisation (TS) configuré de manière à recevoir du premier dispositif client de synchronisation (TC1), lors d'une phase de synchronisation temporelle, la première valeur (C) et une deuxième valeur (MAC_K(m1)) produite au moyen de la première clé (K), le serveur de synchronisation étant configuré de manière à authentifier le premier dispositif client de synchronisation (TC1) à partir de la deuxième valeur (MAC_K(m1)).

11. Système de synchronisation temporelle selon la revendication 10, dans lequel:

- le serveur d'authentification (AS) est par ailleurs configuré de manière à transmettre, à travers le réseau de communication à un deuxième dispositif client de synchronisation (TC2), une troisième clé (K) et une troisième valeur (C) contenant la troisième clé (K) sous forme cryptée ; et

- le serveur de synchronisation (TS) est par ailleurs configuré de manière à recevoir du deuxième dispositif client de synchronisation (TC2), pendant une phase de synchronisation temporelle, la troisième valeur (C) et une quatrième valeur (MAC_K(m1)) produite au moyen de la troisième clé (K), le serveur de synchronisation étant configuré de manière à authentifier le deuxième dispositif client de synchronisation (TC2) à partir de la quatrième valeur (MAC_K(m1)).

12. Procédé d'obtention d'une synchronisation temporelle par un dispositif client de synchronisation (TC1) comprenant une interface de réseau pour communiquer à travers un réseau de communication, ce procédé comprenant :

- la réception, à travers le réseau de communication en provenance d'un serveur d'authentification (AS), d'une première clé (K) et une première valeur (C) contenant la première clé (K) sous forme cryptée ;

- la production, par le dispositif client de synchronisation (TC1), d'une deuxième valeur (MAC_K(m1)) au moyen de la première clé (K) ; et

- pendant une phase de synchronisation temporelle, la transmission par le dispositif client de synchronisation des première et deuxième valeurs (C, MAC_K(m1)) à un serveur de synchronisation (TS).

13. Procédé de synchronisation temporelle par un système de synchronisation temporelle, ce procédé comprenant :

- la transmission, par un serveur d'authentification (AS) à travers un réseau de communication à un dispositif client de synchronisation (TC1), d'une première clé (K) et d'une première valeur (C) contenant la première clé (K) sous forme cryptée ;

- pendant une phase de synchronisation temporelle, la réception par un serveur de synchronisation (TS) en provenance du dispositif client de synchronisation (TC1) de la première valeur (C) et d'une deuxième valeur (MAC_K(m1)) produite au moyen de la première clé (K) ; et

- l'authentification par le serveur de synchronisation (TS) du dispositif client de synchronisation (TC1) à partir de la deuxième valeur (MAC_K(m1)).

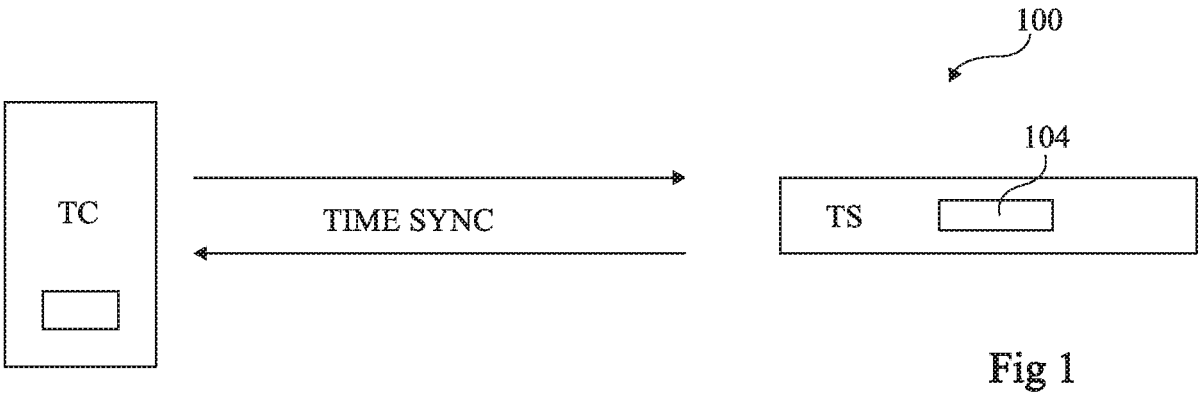
100
104
TC
TIME SYNC
TS

Fig 1

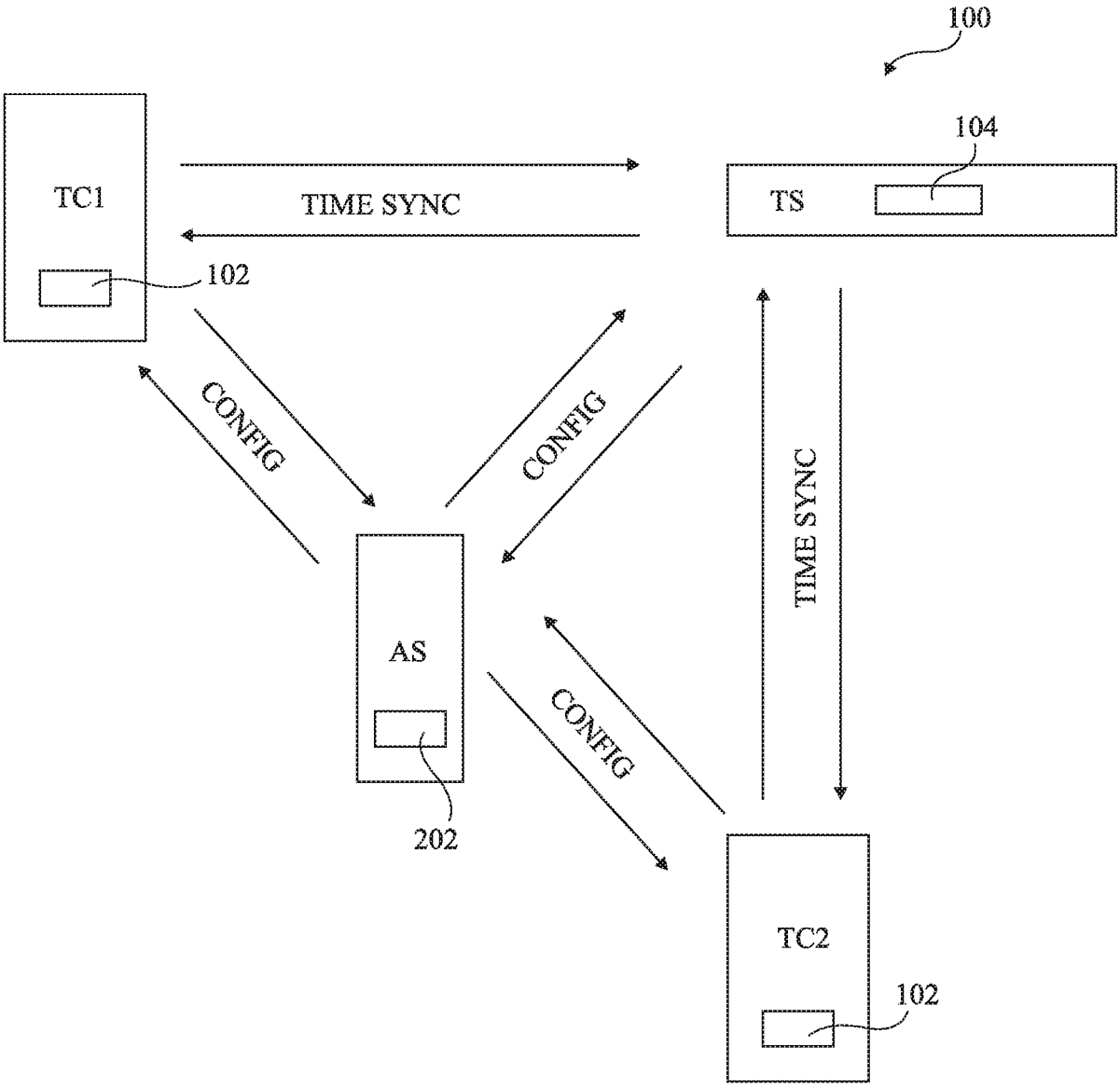
100
104
TC1
TIME SYNC
TS
102
CONFIG
CONFIG
TIME SYNC
AS
CONFIG
202
TC2
102

Fig 2

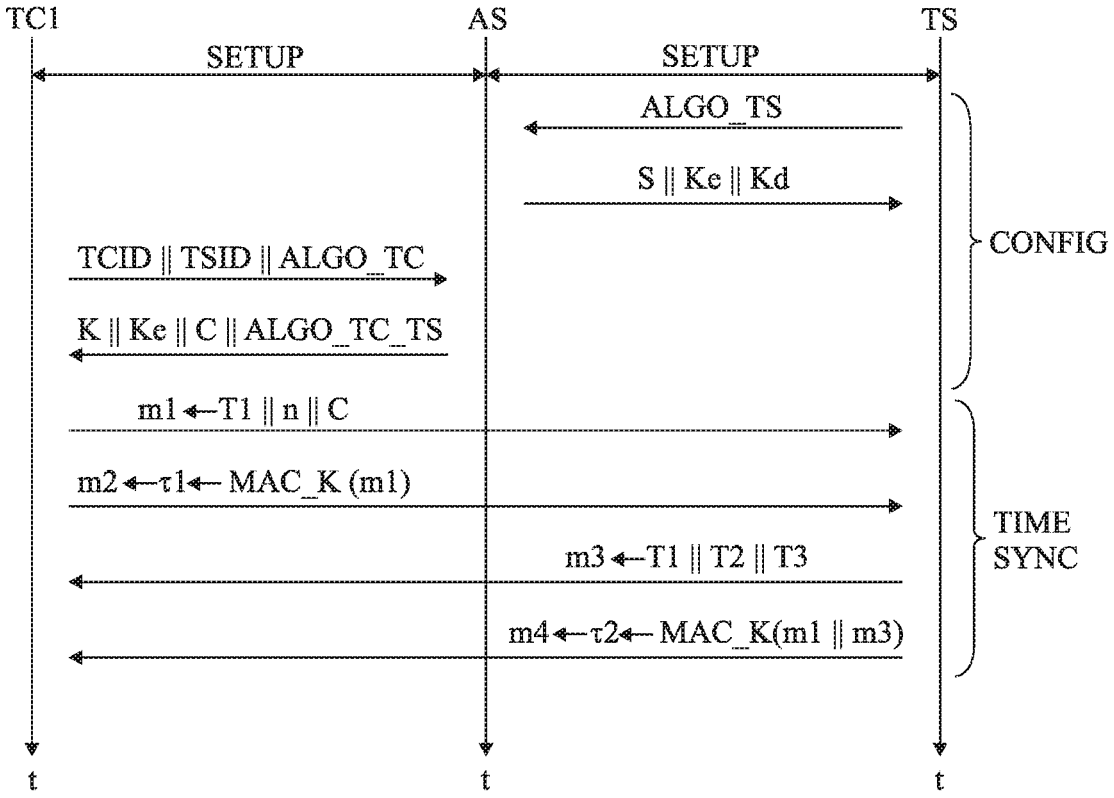
TC1
AS
TS
SETUP
SETUP
ALGO_TS
S || Ke || Kd
CONFIG
TCID || TSID || ALGO_TC
K || Ke || C || ALGO_TC_TS
m1←T1 || n || C
m2←τ1← MAC_K (m1)
TIME SYNC
m3←T1 || T2 || T3
m4←τ2← MAC_K(m1 || m3)
t
t
t

Fig 3

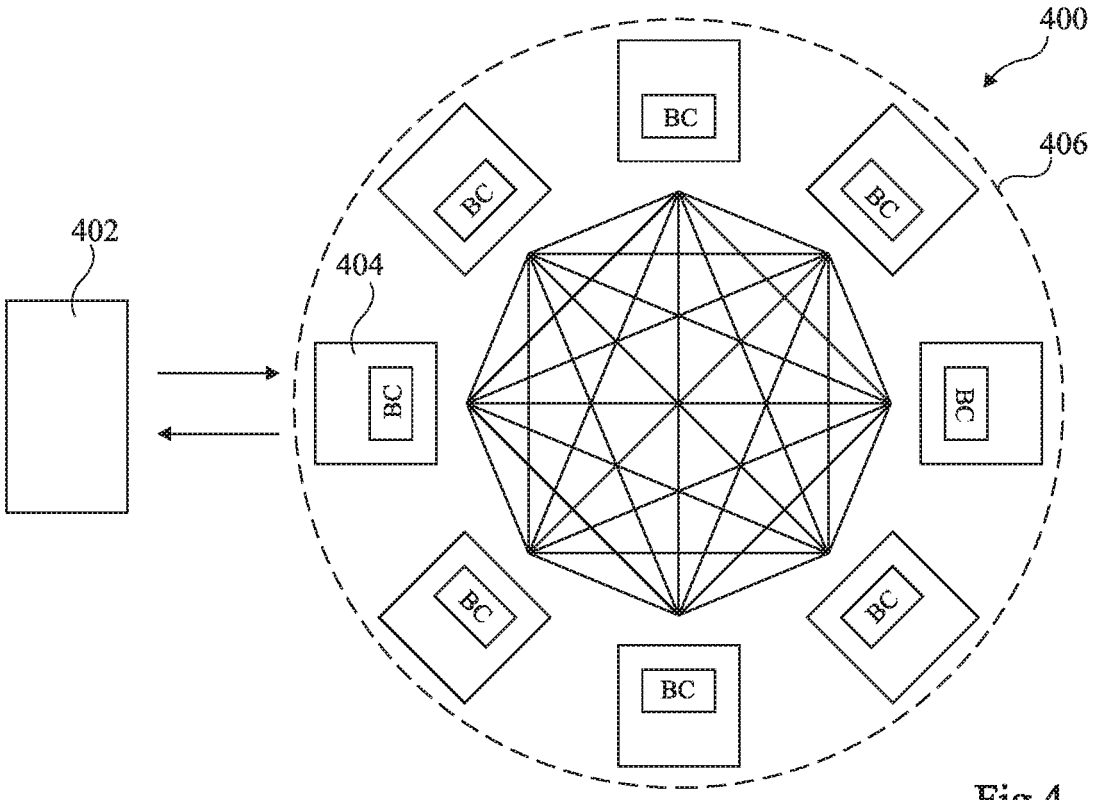
400
406
402
404
BC
BC
BC
BC
BC
BC
BC
BC

Fig 4

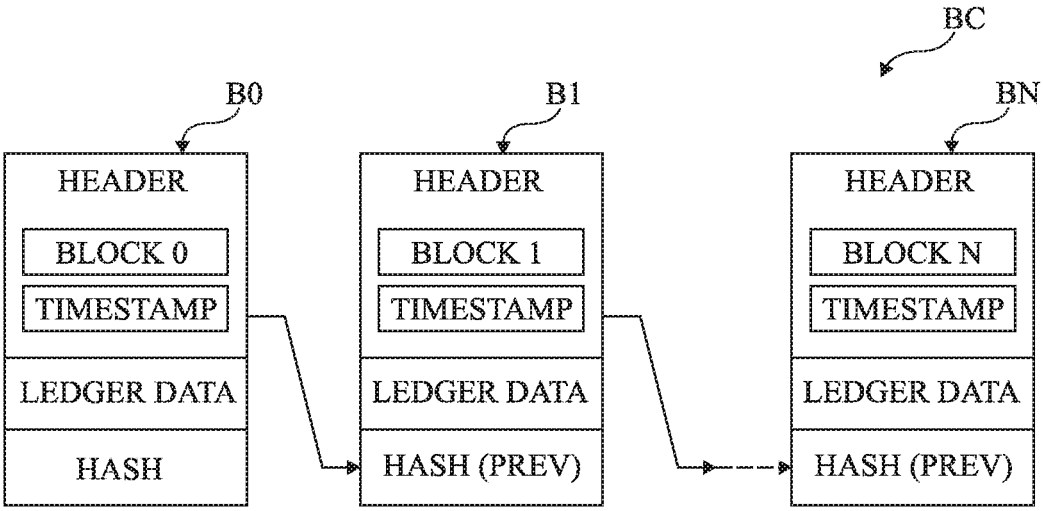

Fig 5

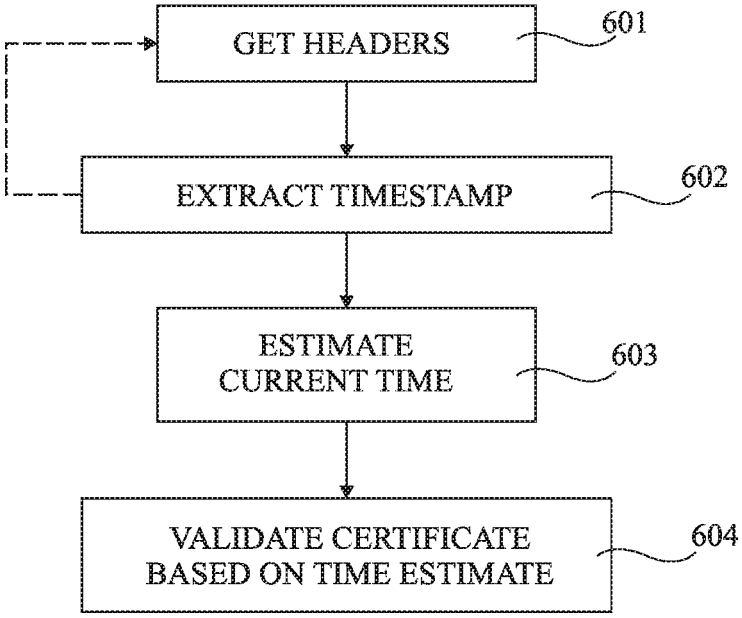

Fig 6

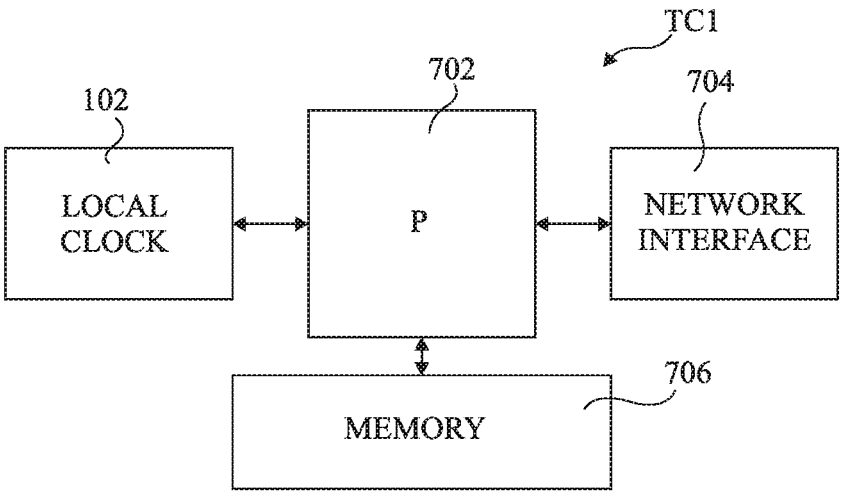

Fig 7

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.

[x] Le demandeur a maintenu les revendications.

☐ 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.

☐ 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

US 2005/251603 A1 (ISHII TAMOTSU [JP] ET AL) 10 novembre 2005 (2005-11-10)

FAN KAI ET AL: "Secure Time Synchronization Scheme in IoT Based on Blockchain", 2018 IEEE INTERNATIONAL CONFERENCE ON INTERNET OF THINGS (ITHINGS) AND IEEE GREEN COMPUTING AND COMMUNICATIONS (GREENCOM) AND IEEE CYBER, PHYSICAL AND SOCIAL COMPUTING (CPSCOM) AND IEEE SMART DATA (SMARTDATA), IEEE, 30 juillet 2018 (2018-07-30), pages 1063-1068, XP033556393, DOI: 10.1109/CYBERMATICS_2018.2018.00196 [extrait le 2019-05-30]

STENN D MILLS P PRINDEVILLE NETWORK TIME FOUNDATION H: "Network Time Protocol: Secure Network Time; draft-stenn-ntp-secure-network-time-00.txt ", NETWORK TIME PROTOCOL: SECURE NETWORK TIME; DRAFT-STENN-NTP-SECURE-NETWORK-TIME-00.TXT ; INTERNET-DRAFT: INTERNET ENGINEERING TASK FORCE, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205, 2 juillet 2018 (2018-07-02), pages 1-4, XP015127553, [extrait le 2018-07-02]

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

NEANT

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

NEANT