(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 144 730***

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

(21) **N° d'enregistrement national :** **22 14622**

(51) Int Cl[8] : ***H 04 L 9/30*** *(2023.01), H 04 L 9/22, H 04 W 12/069, G 06 F 21/64, 21/44*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 29.12.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 05.07.24 Bulletin 24/27.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *THALES Société anonyme* — FR.

(72) **Inventeur(s) :** GILLES Olivier, GRACIA-PEREZ Daniel et FAURA David José.

(73) **Titulaire(s) :** THALES Société anonyme.

(74) **Mandataire(s) :** ATOUT PI LAPLACE.

(54) Procédé de transmission sécurisée d'un élément secret entre un premier équipement de télécommunication et au moins un deuxième équipement de télécommunication.

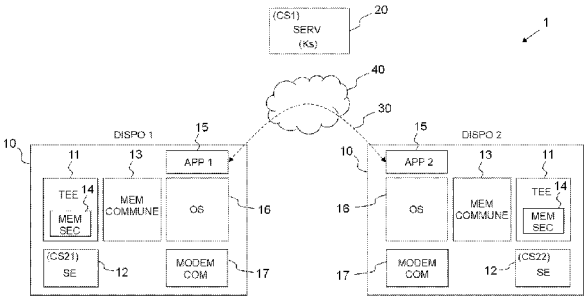
(57) L'invention concerne une transmission sécurisée d'un élément secret entre un serveur de clefs (SERV) et un dispositif de télécommunication (DISPO1) comprenant un module cryptographique sécurisé (SE), avec une authentification réciproque comprenant notamment:

par le serveur: génération d'une première valeur aléatoire; chiffrement de ladite première valeur aléatoire avec la clef publique du dispositif; détermination d'une première signature, par utilisation de la clef privée du serveur, de ladite première valeur aléatoire chiffrée; transmission à destination du dispositif d'un message comportant ladite première valeur aléatoire chiffrée et ladite première signature ;

par le dispositif, en mode sécurisé :

vérification de l'authenticité du serveur en fonction de ladite première valeur aléatoire chiffrée, de la première signature et de la clef publique du dispositif ; puis déchiffrement, par le module cryptographique sécurisé (SE) et au moyen de la clef privée du serveur, de ladite première valeur aléatoire chiffrée et stockage de la première valeur aléatoire déchiffrée dans la mémoire sécurisée ;chiffrement d'une deuxième valeur aléatoire avec la clef publique du serveur; détermination d'une deuxième signature par le module cryptographique sécurisé (SE), avec la clef privée du dispositif stockée dans le ledit module, de ladite deuxième valeur aléatoire chiffrée.

Figure pour l'abrégé: Fig. 1



FR 3 144 730 - A1

Description

Titre de l'invention : Procédé de transmission sécurisée d'un élément secret entre un premier équipement de télécommunication et au moins un deuxième équipement de télécommunication

Domaine technique

[0001] L'invention concerne l'établissement d'un canal de communication sécurisé entre deux équipements, permettant d'échanger des données secrètes, par exemple une clef temporaire, entre les deux équipements, et ce sans intervention d'une tierce partie, par opposition à la distribution de clef par une autorité de confiance.

[0002] L'invention s'applique particulièrement aux systèmes embarqués critiques (SEC).

Technique antérieure

[0003] Les systèmes de contrôle industriels (ICS) par exemple tels que SCADA, sont des systèmes distribués par nature, connectant capteurs et actuateurs à un superviseur via des bus spécialisés (bus de terrain). Historiquement, l'ensemble de ces équipements formaient un réseau isolé et étaient circonscrits dans une zone sécurisée d'un bâtiment de l'entreprise, où des mesures physiques et organisationnelles permettaient d'assurer leur sécurité, physique et informatique. A partir des années 90, l'Ethernet Industriel permit une plus grande interopérabilité de ces systèmes, et leur ouverture sur des réseaux IT. A partir de 2010 environ, la maturation de protocoles de communication légers et décentralisés tels que OPC UA PubSub ou MQTT a permis d'envisager un Internet des Objets Industriels (IIoT), où les équipements industriels sont présents hors de l'emprise de leurs opérateurs, et communiquent entre eux via des réseaux publics, non sécurisés.

[0004] L'établissement d'un canal sécurisé, pour l'échange d'un élément secret tels que l'échange de clefs Diffie-Hellman, est applicable dans les systèmes informatiques de la plupart des industries telles que l'automobile, le ferroviaire ou l'automatique. Il présente un intérêt tout particulier dans le cas des infrastructures dites « IIoT » (Industrial Internet of Things, ou internet des objets industriels), où la connectivité des équipements ne peut être établie avant la phase de déploiement, et peut évoluer au cours du cycle de vie. La sécurité de ce canal de communication est particulièrement critique lorsqu'il est établi dans le but de procéder à l'enrôlement d'un équipement connecté (l'un des équipements participant au canal est alors un serveur de clefs distribuant les clefs de session permettant ensuite à l'autre équipement d'établir les sessions de communication avec les autres membres du groupe).

[0005] Or, les systèmes embarqués sont aujourd'hui déployés dans un environnement de moins en moins maîtrisé par leurs opérateurs légitimes, et de plus en plus accessibles à

des attaquants. Si un ensemble de techniques tant au niveau réseau (pare-feu, DMZ…) qu'au niveau équipement (contrôle de flot d'exécution) a considérablement augmenté la sécurité de ces systèmes, le risque de compromission d'un équipement reste majeur, au regard de la criticité inhérente aux SECs. La compromission (lecture ou modification) d'une clef de session par un attaquant, permet à ce dernier de contrôler tous les échanges entre deux équipements. Les techniques d'échange de clef existantes (Diffie-Hellman RSA ou ECC) sont généralement efficaces pour protéger la sécurité des communications contre un attaquant présent sur le réseau mais n'offrent pas de protection contre un attaquant ayant la capacité d'accéder à la mémoire de l'équipement (par exemple via la compromission d'un processus sur celui-ci). En effet, les participants à la communication calculent une clef de chiffrement temporaire, qui est stockée dans sa mémoire. Une fois la clef de chiffrement temporaire lue par un attaquant, celui-ci sera en mesure de lire ou de falsifier les informations passant par ce canal – par exemple des clefs de session, dans le cadre d'une communication avec un serveur de clef. L'attaquant sera ensuite en mesure de fournir ou falsifier toute donnée passant sur le réseau en provenance, ou à destination de la machine compromise. Dans le cas où les clefs de session sont des clefs de groupe, ce pouvoir s'étendra à toutes les machines du groupe.

[0006] Il existe donc un besoin d'accroître la protection des télécommunications dans les systèmes de télécommunication notamment du type SEC.

Résumé de l'invention

[0007] A cet effet, suivant un premier aspect, la présente invention décrit un procédé de transmission sécurisée d'un élément secret entre un premier équipement de télécommunication et au moins un deuxième équipement de télécommunication, un couple respectif clef privée – clef publique étant associé à chacun desdits premier et deuxième équipements

[0008] le deuxième équipement comprenant un module cryptographique sécurisé, adapté pour exécuter des fonctions cryptographiques prédéfinies, pour stocker des informations cryptographiques dont la clef privée du deuxième équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ;

[0009] le deuxième équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée et une mémoire commune et des fonctions logicielles s'exécutant sur le processeur, ledit deuxième équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à

l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;

[0010] ledit procédé comprenant les étapes suivantes :

[0011] i/ authentification réciproque entre le premier équipement et le deuxième équipement, ladite authentification comprenant :

[0012] i-1/ par le premier équipement : génération d'une première valeur aléatoire et stockage de ladite première valeur aléatoire ; chiffrement de ladite première valeur aléatoire avec la clef publique du deuxième équipement préalablement obtenue ; détermination d'une première signature par utilisation de la clef privée du premier équipement de ladite première valeur aléatoire chiffrée ; transmission à destination du deuxième équipement d'un message comportant ladite première valeur aléatoire chiffrée et ladite première signature ;

[0013] i-2/ par le deuxième équipement :

[0014] dans le mode non sécurisé :

[0015] réception du message et copie dudit message dans la mémoire commune ;

[0016] puis en mode sécurisé :

[0017] vérification de l'authenticité du premier équipement en fonction de ladite première valeur aléatoire chiffrée, de la première signature et de la clef publique du premier équipement préalablement obtenue ; puis

[0018] si l'authenticité a été vérifiée, déchiffrement, par le module cryptographique sécurisé et au moyen de la clef privée du deuxième équipement stockée dans ledit module, de ladite première valeur aléatoire chiffrée et stockage de la première valeur aléatoire déchiffrée dans la mémoire sécurisée ;

[0019] obtention d'une deuxième valeur aléatoire et stockage de ladite deuxième valeur aléatoire dans la mémoire sécurisée ; chiffrement de ladite deuxième valeur aléatoire avec la clef publique du premier équipement préalablement obtenue ; détermination d'une deuxième signature par le module cryptographique sécurisé, avec la clef privée du deuxième équipement stockée dans le ledit module, de ladite deuxième valeur aléatoire chiffrée ; copie dans la mémoire commune de ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

[0020] dans le mode non sécurisé :

[0021] préparation, pour transmission à destination du premier équipement, d'un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

[0022] transmission à destination du premier équipement, du message ;

[0023] i-3/ par le premier équipement :

[0024] réception du message contenant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

[0025] vérification de l'authenticité du deuxième équipement en fonction de ladite deuxième

valeur aléatoire chiffrée, de ladite deuxième signature et de la clef publique du deuxième équipement préalablement obtenue ; puis

[0026] si l'authenticité a été vérifiée, déchiffrement de ladite deuxième valeur aléatoire chiffrée en fonction de la clef privée du premier équipement ;

[0027] ii/ détermination par le premier équipement d'une clef de chiffrement symétrique, dite clef d'initialisation en fonction de la première valeur aléatoire stockée à l'étape i-1 et de la deuxième valeur aléatoire déchiffrée à l'étape i-3, en mettant en œuvre une fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires ;

[0028] iii/ détermination par le deuxième équipement en mode sécurisé de ladite clef d'initialisation en fonction de la première valeur aléatoire stockée à l'étape i-2 et de la deuxième valeur aléatoire stockée à l'étape i-2, en mettant en œuvre ladite fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires et dont le résultat sera de façon strictement déterministe la clef d'initialisation également calculée par le premier équipement ; et stockage de ladite clef d'initialisation dans la mémoire sécurisée;

[0029] iv/ chiffrement de l'élément secret par le premier équipement avec ladite clef d'initialisation déterminée à l'étape ii ; et transmission dudit élément secret chiffré au deuxième équipement ;

[0030] v/ réception par le deuxième équipement dudit élément secret chiffré ; déchiffrement, en mode sécurisé, dudit élément secret à l'aide de la clef d'initialisation stockée à l'étape iii et stockage dudit élément secret dans la mémoire sécurisée ou dans le module cryptographique sécurisé.

[0031] On entend par élément d'information secret des données sensibles, typiquement des clefs cryptographiques, utilisées par les fonctions cryptographiques, par exemple pour chiffrer, déchiffrer, signer et/ou authentifier une signature et dont l'obtention par un tiers malveillant porterait atteinte à la sécurité des communications mises en œuvre notamment par le deuxième équipement.

[0032] Un tel procédé permet d'accroître la protection des télécommunications dans les systèmes de télécommunication notamment de deuxièmes équipements SEC.

[0033] Le principe de l'invention est de proposer une architecture de sécurité reposant sur des capacités d'éléments matériels et qui assure la mitigation de la compromission logicielle et/ou matérielle d'un deuxième équipement, y compris en cas de prise de contrôle non détectée. En particulier, l'invention assure à un système de télécommunication comportant des deuxièmes équipements en réseau et qui implémentent l'invention les propriétés suivantes :

- un deuxième équipement, compromis ou non, ne peut pas divulguer l'élément secret (typiquement une clef temporaire) ;

– dans le cadre d'un usage pour l'enrôlement des deuxièmes équipements : un deuxième équipement, compromis ou non, ne peut pas divulguer la clef de chiffrement (typiquement clef de session chiffrée de l'élément secret) ;

[0034] un équipement, compromis ou non, ne peut recevoir de clef pour communiquer avec les autres seconds équipements que d'un serveur de clef valide.

[0035] Dans des modes de réalisation, un tel procédé comprendra en outre l'une au moins des caractéristiques suivantes :

[0036] le premier équipement est un serveur de clefs, l'élément secret comporte au moins une clef de session et ledit procédé comprenant en outre les étapes suivantes :

[0037] les étapes i/ à v/ sont mises en œuvre par le serveur de clefs avec une pluralité de deuxièmes équipements pour transmettre auxdits deuxièmes équipements ladite même clef de session ;

[0038] une session de télécommunication est ensuite établie entre au moins deux desdits deuxièmes équipements en fonction de ladite clé de session stockée dans chacun desdits deuxièmes équipements suite à leur transmission par le serveur de clefs ;

[0039] - le premier équipement est un serveur de clefs, l'élément secret comporte au moins une clef de session et ledit procédé comprenant en outre les étapes suivantes :

[0040] les étapes i/ à v/ sont mises en œuvre par le serveur avec une pluralité d'applications logicielles d'un même deuxième équipement pour transmettre auxdits applications ladite même clef de session ;

[0041] une session de télécommunication est ensuite établie entre au moins deux desdites applications en fonction d'au moins lesdites copies de ladite clé de session stockées suite à leur transmission par le serveur de clefs ;

[0042] - le module cryptographique sécurisé du deuxième équipement est un module discret et/ou le module cryptographique sécurisé du deuxième équipement est adapté pour ne pouvoir échanger qu'au sein du deuxième équipement et uniquement en mode sécurisé ;

[0043] – le procédé de transmission sécurisée comprend avant l'étape i-1, une étape i-0 comprenant :

[0044] la transmission par le deuxième équipement au premier équipement du certificat du deuxième équipement établi par une autorité de certification et comprenant au moins la clef publique du deuxième équipement et une signature de ladite clef publique par la clef privée de l'autorité de certification ;

[0045] par le premier équipement : vérification de la validité du certificat du deuxième équipement transmis et stockage de la clef publique du deuxième équipement ;

[0046] et le message transmis par le premier équipement comprend en outre le certificat du premier équipement comprenant la clef publique du premier équipement ; et

[0047] dans l'étape i-2, après basculement en mode sécurisé : avant la mise en œuvre de la

vérification de l'authenticité du premier équipement, le certificat du premier équipement reçu dans le message est vérifié à l'aide du module cryptographique sécurisé, en fonction de la clef publique de l'autorité de certification préalablement stockée en mode sécurisé dans le module cryptographique sécurisé ;

[0048] - le premier équipement comprenant un module cryptographique sécurisé, adapté pour exécuter des fonctions cryptographiques prédéfinies, pour stocker des informations cryptographiques dont la clef privée du premier équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ; le premier équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée et une mémoire commune et des fonctions logicielles s'exécutant sur le processeur, ledit premier équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;

[0049] et les étapes décrites relativement au premier équipement, respectivement au deuxième équipement, sont en outre mises en œuvre symétriquement, i.e. cette fois par le deuxième équipement, respectivement par le premier équipement.

[0050] Suivant un autre aspect, l'invention décrit un système de télécommunication comprenant un premier équipement de télécommunication et au moins un deuxième équipement de télécommunication, un couple respectif clef privée – clef publique étant associé à chacun desdits premier et deuxième équipements

[0051] le deuxième équipement comprenant un module cryptographique sécurisé, adapté pour exécuter des fonctions cryptographiques prédéfinies, pour stocker des informations cryptographiques dont la clef privée du deuxième équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ;

[0052] le deuxième équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée et une mémoire commune et des fonctions logicielles s'exécutant sur le processeur, ledit deuxième équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;

[0053] lesdits premier équipement de télécommunication et au moins deuxième équipement de télécommunication étant adaptés pour mettre en œuvre entre eux une opération

d'authentification au cours de laquelle

[0054] le premier équipement est adapté pour générer une première valeur aléatoire et pour stocker ladite première valeur aléatoire, pour chiffrer ladite première valeur aléatoire avec la clef publique du deuxième équipement préalablement obtenue, pour déterminer une première signature, par utilisation de la clef privée du premier équipement, de ladite première valeur aléatoire chiffrée, pour transmettre à destination du deuxième équipement un message comportant ladite première valeur aléatoire chiffrée et ladite première signature ;

[0055] - le deuxième équipement est adapté, dans le mode non sécurisé, pour recevoir ledit message et copier ledit message dans la mémoire commune,

[0056] - puis le deuxième équipement est adapté, en mode sécurisé, pour vérifier l'authenticité du premier équipement en fonction de ladite première valeur aléatoire chiffrée, de la première signature et de la clef publique du premier équipement préalablement obtenue, puis si l'authenticité a été vérifiée, pour que le module cryptographique sécurisé déchiffre, au moyen de la clef privée du deuxième équipement stockée dans ledit module, ladite première valeur aléatoire chiffrée, pour stocker la première valeur aléatoire déchiffrée dans la mémoire sécurisée ; le deuxième équipement étant adapté pour, en mode sécurisé, obtenir une deuxième valeur aléatoire et stocker ladite deuxième valeur aléatoire dans la mémoire sécurisée, pour chiffrer ladite deuxième valeur aléatoire avec la clef publique du premier équipement préalablement obtenue, pour que le module cryptographique sécurisé détermine une deuxième signature, avec la clef privée du deuxième équipement stockée dans le ledit module, de ladite deuxième valeur aléatoire chiffrée, et pour copier dans la mémoire commune ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

[0057] le deuxième équipement est adapté pour, dans le mode non sécurisé, préparer, pour transmission à destination du premier équipement, un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature, transmettre à destination du premier équipement, ledit message ;

[0058] le premier équipement étant adapté pour recevoir ledit message contenant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature, pour vérifier l'authenticité du deuxième équipement en fonction de ladite deuxième valeur aléatoire chiffrée, de ladite deuxième signature et de la clef publique du deuxième équipement préalablement obtenue, puis si l'authenticité a été vérifiée, pour déchiffrer ladite deuxième valeur aléatoire chiffrée en fonction de la clef privée du premier équipement ;

[0059] le premier équipement étant adapté pour déterminer une clef de chiffrement symétrique, dite clef d'initialisation en fonction de ladite première valeur aléatoire stockée et de ladite deuxième valeur aléatoire déchiffrée, en mettant en œuvre une

fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires ;

[0060] le deuxième équipement est adapté pour, en mode sécurisé, déterminer ladite clef d'initialisation en fonction de ladite première valeur aléatoire stockée et de la deuxième valeur aléatoire stockée, en mettant en œuvre ladite fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires et dont le résultat sera de façon strictement déterministe la clef d'initialisation également calculée par le premier équipement, et stocker de ladite clef d'initialisation dans la mémoire sécurisée;

[0061] le premier équipement étant adapté pour chiffrer l'élément secret avec ladite clef d'initialisation qu'il a déterminée, et pour transmettre ledit élément secret chiffré au deuxième équipement ;

[0062] le deuxième équipement étant adapté pour recevoir ledit élément secret chiffré, pour déchiffrer, en mode sécurisé, ledit élément secret à l'aide de la clef d'initialisation stockée et pour stocker ledit élément secret dans la mémoire sécurisée ou dans le module cryptographique sécurisé.

[0063] Dans des modes de réalisation, le système de télécommunication comprendra en outre l'une au moins des caractéristiques suivantes :

[0064] - le premier équipement est un serveur de clefs, l'élément secret comporte au moins une clef de session et l'opération d'authentification est mise en œuvre par le serveur de clefs avec une pluralité de deuxièmes équipements pour transmettre auxdits deuxièmes équipements ladite même clef de session ;

[0065] au moins deux desdits deuxièmes équipements étant adaptés pour établir entre eux une session de télécommunication en fonction de ladite clé de session stockée dans chacun desdits deuxièmes équipements suite à leur transmission par le serveur de clefs ;

[0066] - le premier équipement est un serveur de clefs, l'élément secret comporte au moins une clef de session et l'opération d'authentification est mise en œuvre par le serveur avec une pluralité d'applications logicielles d'un même deuxième équipement pour transmettre auxdits applications ladite même clef de session ;

[0067] au moins deux desdites applications étant adaptées pour établir entre elles une session de télécommunication en fonction d'au moins lesdites copies de ladite clé de session stockées suite à leur transmission par le serveur de clefs ;

[0068] - le module cryptographique sécurisé du deuxième équipement est un module discret et/ou le module cryptographique sécurisé du deuxième équipement est adapté pour ne pouvoir échanger qu'au sein du deuxième équipement et uniquement en mode sécurisé.

Brève description des dessins

[0069] L'invention sera mieux comprise et d'autres caractéristiques, détails et avantages apparaîtront mieux à la lecture de la description qui suit, donnée à titre non limitatif, et grâce aux figures annexées, données à titre d'exemple.

[0070] [Fig.1] La [Fig.1] est une illustration d'un système de télécommunication dans un mode de réalisation de l'invention ;

[0071] [Fig.2] La [Fig.2] représente les étapes d'un procédé transmission sécurisée d'un élément secret dans un mode de réalisation de l'invention ;

[0072] [Fig.3] La [Fig.3] illustre une application au domaine ferroviaire d'un mode de réalisation de l'invention.

[0073] Des références identiques peuvent être utilisées dans des figures différentes lorsqu'elles désignent des éléments identiques ou comparables.

Description des modes de réalisation

[0074] En [Fig.1] est représenté un système de télécommunication 1 distribué dans un mode de réalisation de l'invention. Ce système 1 comporte une pluralité de dispositifs de télécommunication 10, un serveur (nommé SERV) 20 et un réseau de liaisons de télécommunication 40.

[0075] De façon connue, à chacun du serveur 20 et des dispositifs 10 est associé un couple clef privée/clef publique permettant un mécanisme de chiffrement asymétrique : la clef publique peut être distribuée au public tandis que la clef privée doit impérativement rester secrète et n'être utilisée que par l'équipement 10 (ou son utilisateur) auquel elle a été affectée. La propriété des algorithmes asymétriques est qu'un message chiffré par une clé privée sera lisible par tous ceux qui possèdent la clé publique correspondante. À l'inverse, un message chiffré par une clé publique n'est lisible que par le propriétaire de la clé privée correspondante. Typiquement la clef privée permet également de signer des messages.

[0076] Dans le mode de réalisation considéré, le serveur 20 et chaque dispositif 10 dispose d'un certificat numérique respectif, signé et émis par une autorité de certification CA tierce, qui permet de vérifier leur authenticité. Un certificat contient des informations identifiant de façon unique le propriétaire du certificat, telles que le nom, sa clé publique, le nom distinctif de l'autorité de certification CA, une signature numérique, par l'autorité de certification, à l'aide de sa propre clef privée, ou d'un tiers de confiance affilié des informations précédentes (en effet, la vérification de cette signature, à l'aide de la clef publique de la CA permet ainsi de valider ensuite que le certificat a été émis par une autorité de certification reconnue).

[0077] Le réseau 40 est adapté pour mettre à disposition des liaisons de télécommunication filaires et/ou sans fil aux dispositifs de télécommunication 10 et au serveur 20.

[0078] Les dispositifs de télécommunication 10, par exemple nommés DISPO1, DISPO2…,

sont des dispositifs électroniques adaptés pour établir entre eux des sessions de télécommunication via le réseau de télécommunication 40, par exemple pour échanger des données utiles (de type fournies par des capteurs dans des dispositifs 10 ou à destination d'actuateurs dans des dispositifs 10 ou des données stockées dans une base de données distante comprise dans un dispositif 10). Une ou des applications métier 15 (APP1 dans DISPO1, APP2 dans DISPO2) s'exécutant dans le dispositif électronique 10 échange(nt) avec une ou des applications métiers d'autres dispositifs 10 ou du serveur 20.

[0079] Chaque dispositif de télécommunication 10 est en outre adapté pour échanger avec le serveur 20 via le réseau de télécommunication 40.

[0080] Le serveur 20 comporte un générateur d'aléas, une mémoire, un processeur un bloc de télécommunication comprenant notamment, dans le mode de réalisation considéré, un modem, une antenne d'émission-réception RF, (non représenté).

[0081] Chaque dispositif 10 comporte un TEE 11, un Elément Sécurisé (SE) 12, une mémoire commune 13 et une mémoire sécurisée 14, une application métier 15, un système d'exploitation 16 et un Modem 17 (,) et non représentés : un processeur permettant l'exécution de l'application métier, du TEE, de l'OS, etc, un étage RF et un générateur d'aléas. …

[0082] Le TEE 11 est un environnement d'exécution sécurisé (« Trusted Execution Environment ») adapté pour permettre l'exécution de fonctions critiques dans la mémoire sécurisée 14 (au moyen par exemple d'un bit de contrôle dans le champ d'adressage, par exemple mis alors à 0) et qui est séparé du reste du système (correspondant au bit de contrôle mis à 1).

[0083] Le dispositif 10 et notamment son processeur, est ainsi doté d'un mécanisme lui permettant de basculer entre deux modes de fonctionnement alternatifs : un mode non sécurisé et un mode TEE, sécurisé, tel que dans le mode non sécurisé, le processeur et les fonctions logicielles exécutées sont interdits d'accès à la zone mémoire sécurisée 14 et accèdent à la mémoire commune 13 tandis que dans le mode sécurisé, seul un sous-ensemble très réduit, prédéfini, de fonctionnalités disponibles est autorisé à s'exécuter (rendant plus facile l'analyse du comportement des fonctions critiques) sur le processeur, et la mémoire sécurisée 14 et la mémoire commune 13 sont accessibles. Par exemple, dans le cas présent, ce sous-ensemble comporte exclusivement les opérations cryptographiques et logiques nécessaires à la réception d'une clef provenant d'un serveur de clef, en incluant toutes les vérifications qui sont l'objet de la présente invention, ainsi que l'usage de cette clef pour établir et sécuriser la communication avec d'autres seconds équipements.

[0084] Le SE 12 (« Secure Element ») est un module électronique, par exemple discret (sur une puce électronique qui lui est propre par exemple, séparée du reste des composants

du dispositif), qui assure des opérations cryptographiques de base (chiffrement, déchiffrement, signature, vérification de signature) à l'aide de secrets et permet de stocker, dans une mémoire inviolable du SE 12, et d'utiliser, des secrets (notamment la clef privée du dispositif 10) sans qu'ils puissent être accédés par aucun utilisateur (par exemple, parce que le SE 12 est adapté pour ne pas délivrer ces secrets : pas d'interfaces, pas de fonctionnalités le permettant). Le provisionnement des secrets dans le SE 12 est par exemple effectué en usine où les secrets sont générés dans le SE 12 ; il est aussi possible d'ajouter dynamiquement un secret. Aucune connexion directe depuis l'application métier 15 vers le SE 12 n'est autorisée. Dans le mode de réalisation considéré, optionnel, il n'est possible d'échanger avec le SE 12 au sein du dispositif 10 qu'en mode TEE. L'application métier 15 communique via la mémoire commune 13 avec une application « TEE Trusted Application » exécutée dans le TEE 11, qui est elle-même connectée au SE 12 chargé d'effectuer les opérations cryptographiques.

[0085] Typiquement un élément de sécurité TPM est utilisable pour mettre en œuvre le SE. Il existe plusieurs types de SE utilisables : ST33® de STM, le chip A700x® de NXP etc.

[0086] Dans le mode de réalisation considéré de l'invention, il est souhaité l'établissement de canaux de télécommunication sécurisés entre les dispositifs 10 via le réseau 40, et sur lesquels des messages chiffrés seront échangés. Un canal de communication sécurisé permettra de protéger la sécurité des communications contre un attaquant présent sur le réseau ou face à un attaquant disposant d'un accès physique à ces derniers.

[0087] L'établissement du canal de communication sécurisé entre les dispositifs 10 implique deux phases, en référence à la [Fig.2] :

– récupération des clefs de session par les dispositifs 10 (phase 1), qui implique trois étapes que chaque dispositif 10 doit réaliser indépendamment :

authentification réciproque entre le dispositif 10 et le serveur (étape 100i) ;

[0088] construction d'un canal de communication sécurisé temporaire entre le serveur et le dispositif 10 (sous-étapes 100ii et 100iii) ;

[0089] transmission des clefs de session (sous-étapes 100iv et 100v) ;

– exploitation du canal de communication sécurisé par les dispositifs 10 grâce aux clefs de session (phase 2).

[0090] L'authenticité réciproque (étape 100i) peut faire l'objet de nombreuses hypothèses plus ou moins simplificatrices. Nous nous plaçons ici dans le cadre le plus général – et le plus sûr – où le dispositif 10 connaît le serveur 20, mais sans lui faire confiance (i.e. il ne possède pas encore son certificat), et où le serveur ne connaît pas le dispositif 10, mais connaît (et fait confiance) à son autorité de certification CA.

[0091] Ci-dessous est exposé un mécanisme d'authentification réciproque reflétant une mise en œuvre particulière (nommément le modèle de sécurité de OPC UA), mais les grandes étapes se retrouvent quelles que soient les approches, même si l'ordre d'exécution peut varier :

- Identification du dispositif 10 (typiquement sous la forme d'un envoi de certificat) et vérification de la validité du dispositif 10 par le serveur 20 (auprès de l'autorité de certification CA) ;
- Preuve d'authenticité du serveur 20 (par émission d'un message signé) ;
- Vérification de la validité et de la preuve d'authenticité du serveur 20 par le dispositif 10 (vérification de la signature) ;
- Preuve d'authenticité du dispositif 10 (par émission d'un message signé) ;
- Vérification de la preuve d'authenticité du dispositif 10 par le serveur 20 (vérification de la signature).

[0092] Ainsi en référence à la [Fig.2], les étapes d'un procédé selon l'invention sont maintenant détaillées. Le dispositif 10 DISPO1 comporte sa clef privée CS21 ainsi que la clef publique de la CA, toutes deux stockées dans son SE 12.

[0093] Au cours du procédé, si à un moment quelconque une authentification ou vérification de validité, de signature etc. échoue, le processus se termine et les étapes ultérieures ne sont pas réalisées.

[0094] Une étape 100i-0 d'Identification du dispositif 10 (typiquement sous la forme d'un envoi de certificat) et de vérification de la validité du dispositif 10 par le serveur 20 (auprès d'une autorité de certification) comprend :

- la transmission par le dispositif 10 DISPO1 au serveur 20 du certificat du dispositif 10 établi par l'autorité de certification CA et comprenant au moins la clef publique CP21 du dispositif 10 et une signature de notamment ladite clef publique par la clef privée de l'autorité de certification CA ;
- vérification par le serveur 20 de la validité du certificat du dispositif 10 transmis (en l'authentifiant auprès de la CA ou avec la clef publique de la CA stockée dans le serveur 20) et stockage de la clef publique du dispositif 10 par le serveur 20.

Dans un mode de réalisation le certificat du dispositif 10 est stocké dans le SE 12 qui l'extrait en mode TEE avant son envoi au serveur 20, ce qui assure l'intégrité du certificat dans le dispositif 10. Dans un autre mode de réalisation, il est stocké dans la mémoire sécurisée 14 ou la mémoire commune 13 (dans ce cas le hash du certificat doit être stocké dans la mémoire sécurisée ou dans le SE).

[0095] Une étape 100i-1 de preuve d'authenticité du serveur 20 (par émission d'un message signé) mise en œuvre par le serveur 20 comprend :

- génération d'une première valeur aléatoire, aléa1, et stockage de ladite

première valeur aléatoire aléa1 ;

- chiffrement de ladite première valeur aléatoire aléa1 avec la clef publique CP21 du dispositif 10 DISPO1 préalablement obtenue dans le certificat reçu ;
- détermination d'une première signature par chiffrement avec la clef privée CS1 du serveur de l'agrégat de ladite première valeur aléatoire aléa1 chiffrée ;
- transmission à destination du dispositif 10 d'un message comportant ladite première valeur aléatoire aléa1 chiffrée, ladite première signature et le certificat du serveur 20.

[0096] Une étape 100i-2-1 de vérification de la validité et de la preuve d'authenticité du serveur 20 par le dispositif 10 (vérification de la signature) mise en œuvre par le dispositif 10 DISPO1 comprend la réception du message, et après basculement en mode TEE :

- le certificat du serveur 20 reçu dans le message est fourni au SE 12 pour authentification dudit certificat par le SE 12 en fonction de la clef publique de l'autorité de certification CA préalablement stockée dans le SE 12 (dans un mode de réalisation alternatif, la CA est stockée dans la mémoire sécurisée, et le SE n'est pas impliqué dans l'authentification du serveur et il l'est dans l'authentification du client auprès du serveur) ;
- vérification de l'authenticité du serveur 20 en fonction de ladite première valeur aléatoire aléa1 chiffrée, de la première signature et de la clef publique du serveur 20 figurant dans le certificat du serveur 20 authenticité : le dispositif 10 calcule à son tour un agrégat de la valeur aléa1, puis le compare avec la signature déchiffrée par la clef publique du serveur CP1 contenue dans le certificat): ceci permet de confirmer, en cas d'égalité des termes comparés que le serveur avait la clef privée nécessaire pour effectuer la signature et prouver son authenticité; puis
- seulement si l'authenticité a été vérifiée avec succès, déchiffrement par le SE 12, en fonction de la clef privée, CS21, du dispositif 10 stockée dans le SE 12, de ladite première valeur aléatoire aléa1 chiffrée et stockage de la première valeur aléatoire déchiffrée, aléa1, dans la mémoire sécurisée 14.

[0097] Grâce à l'utilisation du SE proposé dans l'invention, l'intégrité de la clef publique du CA et de la clef privée CS21 du dispositif 10 est assurée, ainsi que la confidentialité de cette dernière. De plus, grâce à l'utilisation du TEE le secret aléa1 transmis par le serveur 20 reste confidentiel (les applications non associées au TEE dans le dispositif 10 n'y ont pas d'accès) et la séquence d'opérations est exécutée de manière atomique (en cela que la séquence d'opérations du processus mis en œuvre en mode TEE ne peuvent pas être compromis).

[0098] Dans une étape 100i-2-2 de preuve d'authenticité du dispositif 10 (par émission d'un

message signé), ce dernier met en œuvre les étapes suivantes, en mode TEE :

- génération d'une deuxième valeur aléatoire, aléa2, (optionnellement le SE peut être utilisé pour générer au moins partiellement cette valeur et optionnellement, cette deuxième valeur aléatoire est à usage unique) et stockage de ladite deuxième valeur aléatoire dans la mémoire sécurisée 14 ;
- chiffrement de ladite deuxième valeur aléatoire aléa2 avec la clef publique CP1 du serveur 20 contenue dans le certificat reçu ;
- détermination d'une deuxième signature cryptographique par le SE 12 avec la clef privée du dispositif 10, stockée dans le SE 12, de ladite deuxième valeur aléatoire aléa2 chiffrée.

[0099] Il est fourni, par exemple via la mémoire commune 13, à l'application métier 15 un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature.

[0100] Puis l'application métier 15, en mode non sécurisé, transmet à destination du serveur 20, un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature.

[0101] Grâce à l'usage du SE 12 proposé dans l'invention, l'intégrité et la confidentialité de la clef privée CS21 du dispositif 10 sont assurées. Grace à l'usage du TEE 11, la confidentialité du secret aléa2 généré reste assurée ; à nouveau, aucune application dans le dispositif 10 ne peut connaître le contenu du secret car ce dernier est manipulé dans la TEE 11 et le SE 12. Finalement, l'exécution atomique de toutes les opérations est assurée par le TEE selon l'invention.

[0102] Dans une étape 100i-3 de vérification de la preuve d'authenticité du dispositif 10 par le serveur 20 (vérification de la signature), le serveur 20 met en œuvre les étapes suivantes :

- vérification de l'authenticité du dispositif 10 en fonction de ladite deuxième valeur aléatoire aléa2 chiffrée et de ladite deuxième signature présentes dans le message reçu et de la clef publique CP21 du dispositif 10 préalablement obtenue (pour vérifier que le dispositif 10 a bien utilisé la clef privée CS21 correspondante pour signer) ; puis
- seulement si l'authenticité a été vérifiée avec succès, déchiffrement de ladite deuxième valeur aléatoire aléa2 chiffrée en fonction de la clef privée CS1 du serveur 20 puis stockage.

[0103] Dans une étape de construction d'un canal de communication sécurisé temporaire entre le serveur 20 et le dispositif 10, les sous-étapes 100ii et 100iii sont mises en œuvre, en parallèle ou non. Cette « construction » correspond à celle d'une clef d'initialisation, par exemple symétrique (typiquement AES256). On parle de « construction de canal sécurisé » pour l'ensemble des opérations qui permettent à

plusieurs participants (deux ou plus) de partager une clef sans que celle-ci ne soit exposée en ligne. Ces échanges reposent sur la possession d'un secret commun, calculé (et non pas échangé) par chaque participant.

[0104] Ainsi dans la sous-étape 100ii, le serveur 20 détermine une clef de chiffrement, ici symétrique, dite clef d'initialisation, nommée K_{init}, en fonction de la première valeur aléatoire aléa1 stockée à l'étape 100i-1 et de la deuxième valeur aléatoire aléa2 déchiffrée à l'étape 100i-3, en mettant en œuvre une fonction de calcul de clef d'initialisation ayant pour variables les première et deuxième valeurs aléatoires aléa1 et aléa2.

[0105] Et dans la sous-étape 100iii, le dispositif 10 détermine également, en mode TEE, la clef d'initialisation K_{init} en fonction de la première valeur aléatoire aléa1 stockée à l'étape 100i-2-1 et de la deuxième valeur aléatoire aléa2 stockée à l'étape 100i-2-2, en mettant en œuvre ladite fonction de calcul de clef d'initialisation qui est commune au serveur et aux dispositifs 10 ; et stockage de la clef d'initialisation K_{init} dans la mémoire sécurisée 14 ou dans le module cryptographique sécurisé (SE12). Grâce au calcul en mode TEE et au stockage ainsi sécurisé, la confidentialité de la clef K_{init} est supérieure aux implémentations purement logicielles.

[0106] Dans une étape de transmission des clefs de session $\{K_S\}$ dans le canal sécurisé temporaire comportant les sous-étapes 100iv et 100v, les clefs de session chiffrées avec la clef d'initialisation sont transmises. Un attaquant de type man-in-the-middle n'obtiendra que des informations chiffrées, et donc inexploitables si le niveau de chiffrement est suffisant et les données échangées sont inconnues.

[0107] Dans la sous-étape 100iv, le serveur 20 chiffre les clefs de session $\{K_S\}$ avec la clef d'initialisation K_{init} déterminée à la sous-étape 100ii et transmet les clefs de session ainsi chiffrées au dispositif 1.

[0108] Dans la sous-étape 100v, le dispositif 10 reçoit les clefs de session chiffrées, puis les déchiffre, en mode TEE, à l'aide de la clef d'initialisation K_{init} stockée à la sous-étape 100iii, puis stocke les clefs de session déchiffrées $\{K_S\}$ dans la mémoire sécurisée 14 ou dans le SE 12.

[0109] L'information échangée dans ce contexte doit donc avoir une entropie suffisante (non-prédictabilité en vue de résister à une cryptanalyse). Typiquement, cet échange initial est limité à un ensemble de clef(s) de chiffrement et/ou de signature, que l'on a désigné collectivement par « clefs de session ». Ces clefs sont par exemple symétriques, pour des raisons de performances, mais pas nécessairement identiques (pour deux dispositifs 10 distincts notamment) dans le cas des clefs de signatures.

[0110] Echouer à cette étape (typiquement la conséquence d'un échec à l'étape antérieure de calcul des clefs) interrompt toute possibilité de communication avec le tiers, sauf à reprendre depuis le début du processus d'authentification.

[0111] Dans un mode de réalisation de l'invention s'appliquant à la classe des objets communicants bas débits, les clefs de sessions sont alors provisionnées dans le SE 12 et toute trace en mémoire (y compris dans la TEE 11) est effacée. Dans un mode de réalisation de l'invention s'appliquant à la classe des objets communicants haut débit, la clef est conservée dans l'espace mémoire (la mémoire sécurisée 14 pour la persistance).

[0112] Il est rappelé ci-après la différence entre ces classes.

[0113] Certains SEC communiquent via des réseaux à faible ou très faible débit, pour des raisons de portée, de coût, d'autonomie ou de robustesse aux perturbations électromagnétiques (y compris face à des menaces de type guerre électronique). De plus, les plateformes matérielles peuvent ne disposer que de ressources de calcul limitées – toujours pour les mêmes raisons. De ce fait, le chiffrement des données peut ne pas être nécessaire ni possible au regard des capacités et des besoins du système. L'intégrité des données, cependant, est d'autant plus nécessaire que la criticité de ces systèmes est typiquement supérieure à celle des SEC plus génériques décrits ci-dessous.

[0114] Des exemples d'applications relevant de cette classe de besoins sont les équipements impliqués dans le champ de bataille connecté, les capteurs et actuateurs en milieu à forte activité électromagnétique (nucléaire, spatial) ou les équipements médicaux invasifs (type pacemaker).

[0115] La classe des SEC connectés haut débit, plus répandue que la précédente, concerne les systèmes communiquant des données confidentielles et offrant des ressources (capacité de calcul, communication haut débit) suffisantes pour mettre en œuvre du chiffrement.

[0116] Les étapes de la phase 1 décrite précédemment ayant été mises en œuvre entre le serveur 20 et plusieurs dispositifs 10, ces derniers ont ainsi obtenu les clefs de session leur permettant, dans une phase 2, la mise en place d'une session de communication entre eux.

[0117] Par exemple un canal de communication sécurisé 30 est mis en œuvre entre les dispositifs DISPO1 et DISPO2, tel que les données échangées entre eux sur le réseau 30 entre les applications métier APP1 et APP2 sont chiffrées, en mode TEE, à l'aide d'une des clefs de session, et/ou sont signées à l'aide d'une autre clef de session. Par exemple, pour la classe des objets communicants haut débit, le déchiffrement/chiffrement est effectué dans la TEE en exploitant les clefs de session et dans le cas de la classe des objets communicants bas-débits, le déchiffrement/chiffrement n'est pas fait en TEE, mais dans le SE 12 qui seul conserve la clef de session. L'accès au Secure Element est par contre bien effectué en mode TEE.

[0118] Le TEE 11 et le SE 12 dans le dispositif 10 sont exploités par l'invention pour

assurer une confidentialité et intégrité forte des différents secrets impliqués dans les étapes du procédé incluant les clefs de session.

[0119] Il a été décrit ci-dessus, dans un mode de réalisation particulier de la présente invention, un procédé de transmission sécurisée des clefs de session entre un premier équipement, de type serveur de clefs, et un deuxième équipement, de type dispositif de communication d'un réseau de terminaux de communication, permettant ainsi une protection accrue des communications ultérieures mises en œuvre entre les dispositifs du réseau. L'invention peut bien sûr être mise en œuvre pour la transmission d'éléments secrets autres que des clefs de session entre deux équipements de télécommunication : par exemple des informations concernant la configuration d'un dispositif et/ou la mise à jour de son logiciel.

[0120] Comme vu précédemment, pour protéger le secret des communications et l'intégrité des équipements, un certain nombre de secrets sont nécessaires. Ces secrets sont suivant les cas partagés avec des tiers ou exclusifs au dispositif 10.

[0121] Une classification des secrets en fonction de leur persistance et de leur usage est proposée ici :

[0122] [Tableaux1]

Type de secret	*Secret source / Secret cible*	*Clef d'initialisation*	*Clef de session*	*Clef privée*
Durée de vie	Quelques secondes	Quelques secondes	Quelques heures à quelques mois	Permanente
Utilisation	Opération arbitraire (génération de la clef temporaire)	Chiffrement symétrique	Chiffrement et signature symétrique	Déchiffrement et signature asymétrique
Placement	TEE	TEE	SE ou TEE	SE

[0123] De cette classification, il ressort plusieurs éléments :

[0124] Le couple secret source / secret cible (appelé ci-dessus aléa1/aléa2) et la clef d'initialisation ne sont pas conservés dans un SE dans un mode de réalisation de l'invention car les temps de chargement de ceux-ci seraient trop importants aujourd'hui au regard de leur durée de vie (du moins pour les TPM2 – ce point pourrait changer avec l'évolution des SE) ;

[0125] Les opérations arbitraires appliquées au couple secret source / secret cible sont difficilement compatibles avec le fonctionnement d'un SE (sauf personnalisation, qui nuirait à la confiance que l'on pourrait accorder au SE) ;

[0126] La durée de vie des clefs privées rend tout indiqué l'usage d'un SE ;

[0127] Les clefs de session, qui ont une durée de vie très variable, pourraient être protégées par un SE ou dans la TEE selon le besoin opérationnel.

[0128] De façon générale, plus un secret est éphémère, moins il est protégé dans les architectures actuelles. Or, les secrets éphémères permettent d'inférer les secrets plus permanents : le couple secret cible/secret source permet de calculer de façon certaine la clef temporaire, qui permet de déchiffrer la clef de session. L'invention permet de protéger tous les secrets (la protection de la clef privée de l'équipement dans un Secure Element ne suffit pas : cela protège cette clef, mais n'empêche pas d'accéder aux clefs de session) : quelle que soit leur durée de vie, avec des moyens compatibles avec leur utilisation opérationnelle et sans induire de restriction importante des capacités temps-réel et/ou embarqué pour le système final.

[0129] De plus, l'invention permet de protéger l'intégrité des certificats, qui dans l'art antérieur sont rarement protégés, parce qu'ils ne sont pas confidentiels (négligeant qu'un attaquant qui modifierait ces certificats pourrait cependant initier une connexion avec un équipement malveillant : un exemple classique et particulièrement critique est d'autoriser un serveur de mise à jour malveillant, qui permet de transformer la compromission d'un processus en installation d'un logiciel malveillant – et donc à rendre la compromission persistante).

[0130] L'invention apporte aux équipements connectés qui la mettent en œuvre le bénéfice d'un canal sécurisé protégé par le couple SE et TEE.

[0131] Dans le cas général où le canal sécurisé est utilisé pour échanger un secret, l'invention offre les bénéfices suivants :

- exécution des opérations cryptographiques dans la TEE et le SE : capacité de mettre en œuvre des vérifications sur la nature des données, la source et/ou la destination dans un environnement de confiance, protection face au risque du vol de clef privée ;
- protection de l'intégrité des certificats : protection contre l'injection de certificats.

[0132] Application à la distribution de clef : tous les avantages généraux de l'invention décrits ci-dessus sont également fournis, avec de plus les avantages suivants :

- dans le cas principal (SEC Connecté haute confidentialité forte bande passante) :

protection des clefs tout au long du cycle de vie : mitigation du risque de compromission de l'équipement, meilleure protection des secrets reçus, meilleure protection des équipements distants face à la contrefaçon de données, meilleure protection contre le vol de clef privée de l'équipement ;

[0133] protection de l'intégrité des certificats : mitigation du risque de compromission de l'équipement, protection contre l'injection de certificats ;

[0134] couplée avec une solution de pare-feu de niveau 4, l'invention assure également une meilleure protection contre l'exfiltration d'information de l'équipement ;

[0135] Datalake de Confiance : en protégeant l'intégrité des données sur les équipements et en transit, l'invention permet d'avoir confiance dans les données présentes dans le datalake, et donc de les utiliser dans le cadre d'applications critiques.

- dans le cas variante (SEC Connecté haute intégrité faible bande passante), les propriétés décrites dans le cas principal sont assurées, mise à part l'amélioration de la propriété de protection des clefs tout au long du cycle de vie, car la clef de session est stockée dans le SE 12 plutôt que dans la TEE 14.

Dans les deux cas, ces bénéfices s'appliquent y compris si l'attaquant a un accès physique à la mémoire de l'équipement.

[0136] L'invention permet en outre de s'adapter au cycle de vie des secrets. Elle permet une isolation logique des flux de communication sans fil, et permet non seulement de chiffrer une ou des communications entre deux équipements distants, mais aussi entre deux applications situées sur le même équipement 10, ou encore entre une application sur un équipement 10 et une base de données locale à l'équipement 10 ou distante.

[0137] Dans un mode de réalisation, l'invention est mise en œuvre pour sécuriser les communications dans une architecture producteur-consommateur (encore appelée publisher/suscriber), où les informations sont organisées par groupes (ou topics) pouvant admettre un ou plusieurs producteurs, et un ou plusieurs consommateurs. Dans ce type d'architecture, les clefs de chiffrements sont partagées entre les différents équipements abonnés au groupe, ce qui rend la compromission d'un équipement particulièrement intéressante pour un attaquant (car lui permettant de compromettre ensuite tout le groupe). L'usage de notre invention, grâce à l'utilisation judicieuse d'éléments matériels sécurisés (TEE et SE) dans le calculateur idéalement de toutes les entités communicantes, permet de sécuriser l'échange et la confidentialité à l'exécution, y compris contre un attaquant ayant un accès physique à un des équipements protégé par l'invention.

[0138] Le protocole OPC UA PubSub (OPC UA Specification, part 14, version 1.04, 2018/02 https://reference.opcfoundation.org/v104/Core/docs/Part14/) est utilisé pour mettre en œuvre les communications. Il décrit le mécanisme de distribution des clefs de chiffrement au moyen d'un serveur dédié, le Security Key Service. Celui-ci authentifie les clients demandant un abonnement à une donnée, établit un canal sécurisé de communication et distribue les clefs de chiffrement via ce canal. Les communications sont ensuite chiffrées par les producteurs au moyen de ces clefs, envoyées à un broker 204 (potentiellement implémenté via des émissions de type multicast), transmises par ce dernier aux consommateurs et déchiffrées par les consommateurs. Le broker ne manipule que des messages chiffrés, et donc ne joue pas de rôle dans le

maintien de l'intégrité des données.

[0139] Dans le cas SEC connecté haute confidentialité haut débit, une plateforme matérielle dans chaque dispositif communicant (producteur et/ou consommateur) comporte une carte i.MX8M de NXP (incluant une TEE ARM TrustZone) et l'élément sécurisé TPM2 ST33.

[0140] Cette plateforme est exploitée avec la pile logicielle suivante (en mode non sécurisé) :

[0141] Système d'exploitation : Linux embarqué

[0142] Bibliothèque cryptographique : mbedTLS

[0143] Communications : UDP/IP + OPC UA PubSub + MQTT

[0144] En mode sécurisé, plusieurs options sont possibles, par exemple OP-TEE. Par ailleurs l'accès au TPM doit être réalisé dans la TrustZone. A cette fin, il est proposé de réaliser cet accès à partir d'une pile open-source TSS2 ou WolfTPM.

[0145] Dans ce contexte, les différentes clefs sont protégées et utilisées de la façon suivante, en suivant le mode de réalisation principal :

[0146] [Tableaux2]

Type de secret	Secret source / Secret cible	Clef temporaire	Clef de session	Clef privée
Protection	TrustZone	TrustZone	TrustZone	TPM2
Usage	TrustZone	TrustZone	TrustZone	TPM2

[0147] Les paramètres cryptographiques sont les suivants :

[0148] Le TPM2 de l'équipement protégé par l'invention va utiliser sa clef privée pour signer la connexion initiant le canal sécurisé avec un chiffrement asymétrique RSA2048.

[0149] Le TPM2 de l'équipement protégé par l'invention va utiliser sa clef privée pour dé-chiffrer aléa 1 envoyé par l'équipement distant avec un chiffrement asymétrique RSA2048.

[0150] La TrustZone de l'équipement protégé par l'invention va générer le secret aléa 2, et utiliser la clef publique de l'équipement distant pour chiffrer ce secret.

[0151] La TrustZone de l'équipement protégé par l'invention va calculer la clef temporaire au moyen des secrets aléa1 et aléa2.

[0152] La TrustZone de l'équipement protégé par l'invention va utiliser sa clef temporaire pour chiffrer le canal sécurisé avec un chiffrement symétrique AES256.

[0153] La TrustZone de l'équipement protégé par l'invention va utiliser sa clef de session (ou de groupe) pour chiffrer les messages avec un chiffrement symétrique AES256.

[0154] La TrustZone de l'équipement protégé par l'invention va utiliser sa clef de session

(ou de groupe) pour signer les messages avec la politique OPC UA PubSub Basic256Sha256.

[0155] Dans le cas SEC connecté haute intégrité faible débit et portant des clefs à longue durée de vie (deux paramètres généralement fortement liés), un placement différent des fonctions est proposé. La clef de session, au lieu d'être enregistrée dans la TrustZone, ne fait que transiter dans cette mémoire et est chargée puis conservée et utilisée dans le TPM2.

[0156] Cette variante peut être réalisée avec la même architecture matérielle et logicielle que la précédente.

[0157] Dans ce cadre, l'usage de la clef de session (pour le chiffrement, le déchiffrement, la vérification et la signature) est effectué par le TPM2.

[0158] [Tableaux3]

Type de secret	Secret source / Secret cible	Clef temporaire	Clef de session	Clef privée
Protection	TrustZone	TrustZone	TrustZone (ms) et TPM2 (heures/jours/semaines)	TPM2
Usage	TrustZone	TrustZone	TPM2	TPM2

[0159] Comparativement au cas général, la clef de session est moins exposée à des canaux cachés (elle n'est présente que quelques millisecondes dans la TrustZone, avant le chargement dans le TPM2). Cependant, le TPM2 étant typiquement moins efficace qu'un accélérateur cryptographique ou qu'un CPU, elle ne pourra traiter qu'une fréquence limitée de débit de données – ce pourquoi nous limitons cette architecture aux SEC à faible bande passante.

[0160] Les paramètres cryptographiques sont les suivants :

[0161] Le TPM2 de l'équipement protégé par notre invention va utiliser sa clef privée pour signer la connexion initiant le canal sécurisé avec un chiffrement asymétrique RSA2048.

[0162] Le TPM2 de l'équipement protégé par l'invention va utiliser sa clef privée pour dé-chiffrer aléa 1 envoyé par l'équipement distant avec un chiffrement asymétrique RSA2048.

[0163] La TrustZone de l'équipement protégé par l'invention va générer le secret aléa 2, et utiliser la clef publique de l'équipement distant pour chiffrer ce secret.

[0164] La TrustZone de l'équipement protégé par l'invention va calculer la clef temporaire au moyen des secrets aléa1 et aléa2.

[0165] La TrustZone de l'équipement protégé par notre invention va utiliser sa clef temporaire pour chiffrer le canal sécurisé avec un chiffrement symétrique AES256.

[0166] Le TPM2 de l'équipement protégé par notre invention va utiliser sa clef de session (ou de groupe) pour chiffrer les messages avec un chiffrement symétrique AES256.

[0167] Le TPM2 de l'équipement protégé par l'invention va utiliser sa clef de session (ou de groupe) pour signer les messages avec la politique de sécurité OPC UA PubSub Basic256Sha256.

[0168] Dans l'architecture choisie pour l'équipement 10, une application passerelle sécurisée 205 exécute le code applicatif en mode non sécurisé, au sein d'un système d'exploitation généraliste. TEE Trusted Application exécute le code critique pour l'établissement de la communication, tandis que les opérations de chiffrement asymétriques sont effectuées uniquement par le SE sur requête de la TEE. En mode non sécurisé, un pare-feu applicatif filtre tous les envois de données, et n'accepte que les messages signés par une clef de chiffrement valide. Pour cela, la vérification de celle-ci est déléguée à la TEE (TrustZone). Cette protection n'est pas absolue, puisque le pare-feu peut être compromis, mais permet de limiter le risque d'exfiltration d'informations, et donc d'ajouter une couche de défense en profondeur.

[0169] Considérons la mise en œuvre de cette application de l'invention dans le domaine ferroviaire, pour une application de maintenance prédictive, en référence à la [Fig.3]. Une application de type big data 202 exploite des données remontées de capteurs 206 en vue de présenter à un expert en maintenance une vue en temps réel souple de l'état de voies ferroviaires (rails, caténaires, etc.). L'opérateur ferroviaire a exprimé le besoin de sécuriser les communications sur le réseau public, y compris entre la passerelle sécurisée 205 et l'APN 203 (Access Public Network, fourni par un opérateur télécom), sans sacrifier la flexibilité de l'architecture (facilité de déploiement et d'enrôlement de l'équipement). Pour cela, la passerelle sécurisée doit se connecter à un serveur de clef, le Security Key Server 201 (SKS), suivant le protocole OPC UA PubSub. Cet échange permet au nouveau client d'obtenir les clefs de groupe (ou clefs de session). Dans ce cadre, les clefs de sessions sont particulièrement sensibles, puisqu'elles sont partagées entre tous les membres d'un groupe et l'implémentation de l'invention permet de bénéficier des avantages cités plus haut.

[0170] Au niveau opérationnel, en protégeant la confidentialité des données, l'invention assure le respect des exigences de confidentialité du client, ainsi que la protection contre le vol d'un actif de l'entreprise, qui peut ensuite être valorisé (y compris vendu). En protégeant l'intégrité des données sur les équipements et en transit, l'invention permet d'avoir confiance dans les données présentes dans le datalake, et donc de les utiliser pour la maintenance et l'optimisation du système 200 ainsi présenté en référence à la [Fig.3].

Revendications

[Revendication 1] Procédé de transmission sécurisée d'un élément secret entre un premier équipement de télécommunication (SERV) et au moins un deuxième équipement de télécommunication (DISPO1), un couple respectif clef privée – clef publique étant associé à chacun desdits premier et deuxième équipements

le deuxième équipement comprenant un module cryptographique sécurisé (SE), adapté pour exécuter des fonctions cryptographiques pré-définies, pour stocker des informations cryptographiques dont la clef privée du deuxième équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ;

le deuxième équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée (14) et une mémoire commune (13) et des fonctions logicielles s'exécutant sur le processeur, ledit deuxième équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;

ledit procédé comprenant les étapes suivantes :

i/ authentification réciproque entre le premier équipement (SERV) et le deuxième équipement (DISPO1), ladite authentification comprenant :

i-1/ par le premier équipement (SERV) : génération d'une première valeur aléatoire et stockage de ladite première valeur aléatoire ; chiffrement de ladite première valeur aléatoire avec la clef publique du deuxième équipement préalablement obtenue ; détermination d'une première signature par utilisation de la clef privée du premier équipement (SERV) de ladite première valeur aléatoire chiffrée ; transmission à destination du deuxième équipement (DISPO1) d'un message comportant ladite première valeur aléatoire chiffrée et ladite première signature ;

i-2/ par le deuxième équipement (DISPO1) :

dans le mode non sécurisé :

– réception du message et copie dudit message dans la mémoire commune ;

puis en mode sécurisé :

- vérification de l'authenticité du premier équipement en fonction de ladite première valeur aléatoire chiffrée, de la première signature et de la clef publique du premier équipement préalablement obtenue ; puis
- si l'authenticité a été vérifiée, déchiffrement, par le module cryptographique sécurisé (SE) et au moyen de la clef privée du deuxième équipement stockée dans ledit module, de ladite première valeur aléatoire chiffrée et stockage de la première valeur aléatoire déchiffrée dans la mémoire sécurisée ;
- obtention d'une deuxième valeur aléatoire et stockage de ladite deuxième valeur aléatoire dans la mémoire sécurisée ; chiffrement de ladite deuxième valeur aléatoire avec la clef publique du premier équipement préalablement obtenue ; détermination d'une deuxième signature par le module cryptographique sécurisé (SE), avec la clef privée du deuxième équipement stockée dans le ledit module, de ladite deuxième valeur aléatoire chiffrée ; copie dans la mémoire commune de ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

dans le mode non sécurisé :
préparation, pour transmission à destination du premier équipement (SERV), d'un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

- transmission à destination du premier équipement (SERV), du message ;

i-3/ par le premier équipement (SERV) :

- réception du message contenant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;
- vérification de l'authenticité du deuxième équipement en fonction de ladite deuxième valeur aléatoire chiffrée, de ladite deuxième signature et de la clef publique du deuxième équipement préalablement obtenue ; puis

– si l'authenticité a été vérifiée, déchiffrement de ladite deuxième valeur aléatoire chiffrée en fonction de la clef privée du premier équipement ;

ii/ détermination par le premier équipement d'une clef de chiffrement symétrique, dite clef d'initialisation en fonction de la première valeur aléatoire stockée à l'étape i-1 et de la deuxième valeur aléatoire déchiffrée à l'étape i-3, en mettant en œuvre une fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires ;
iii/ détermination par le deuxième équipement en mode sécurisé de ladite clef d'initialisation en fonction de la première valeur aléatoire stockée à l'étape i-2 et de la deuxième valeur aléatoire stockée à l'étape i-2, en mettant en œuvre ladite fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires et dont le résultat sera de façon strictement déterministe la clef d'initialisation également calculée par le premier équipement ; et stockage de ladite clef d'initialisation dans la mémoire sécurisée;
iv/ chiffrement de l'élément secret par le premier équipement (SERV) avec ladite clef d'initialisation déterminée à l'étape ii ; et transmission dudit élément secret chiffré au deuxième équipement (DISPO1) ;
v/ réception par le deuxième équipement (DISPO1) dudit élément secret chiffré ; déchiffrement, en mode sécurisé, dudit élément secret à l'aide de la clef d'initialisation stockée à l'étape iii et stockage dudit élément secret dans la mémoire sécurisée ou dans le module cryptographique sécurisé (SE).

[Revendication 2] Procédé de transmission sécurisée selon la revendication 1, selon lequel le premier équipement (SERV) est un serveur de clefs, l'élément secret comporte au moins une clef de session et ledit procédé comprenant en outre les étapes suivantes :

– les étapes i/ à v/ sont mises en œuvre par le serveur de clefs avec une pluralité de deuxièmes équipements (DISPO1, DISPO2, ...) pour transmettre auxdits deuxièmes équipements ladite même clef de session ;
– une session de télécommunication est ensuite établie entre au moins deux desdits deuxièmes équipements (DISPO1, DISPO2, ...) en fonction de ladite clé de session stockée dans

chacun desdits deuxièmes équipements suite à leur transmission par le serveur de clefs.

[Revendication 3] Procédé de transmission sécurisée selon la revendication 1 ou 2, selon lequel le premier équipement (SERV) est un serveur de clefs, l'élément secret comporte au moins une clef de session et ledit procédé comprenant en outre les étapes suivantes :

- les étapes i/ à v/ sont mises en œuvre par le serveur avec une pluralité d'applications logicielles d'un même deuxième équipement pour transmettre auxdits applications ladite même clef de session ;
- une session de télécommunication est ensuite établie entre au moins deux desdites applications en fonction d'au moins lesdites copies de ladite clé de session stockées suite à leur transmission par le serveur de clefs.

[Revendication 4] Procédé de transmission sécurisée selon l'une quelconque des revendications précédentes, selon lequel le module cryptographique sécurisé (SE) du deuxième équipement (DISPO1) est un module discret et/ou le module cryptographique sécurisé (SE) du deuxième équipement (DISPO1) est adapté pour ne pouvoir échanger qu'au sein du deuxième équipement et uniquement en mode sécurisé.

[Revendication 5] Procédé de transmission sécurisée selon l'une quelconque des revendications précédentes, comprenant avant l'étape i-1, une étape i-0 comprenant :

- la transmission par le deuxième équipement (DISPO1) au premier équipement (SERV) du certificat du deuxième équipement établi par une autorité de certification et comprenant au moins la clef publique du deuxième équipement et une signature de ladite clef publique par la clef privée de l'autorité de certification ;
- par le premier équipement : vérification de la validité du certificat du deuxième équipement transmis et stockage de la clef publique du deuxième équipement ;

et selon lequel le message transmis par le premier équipement

(SERV) comprend en outre le certificat du premier équipement comprenant la clef publique du premier équipement ; et
dans l'étape i-2, après basculement en mode sécurisé :

- avant la mise en œuvre de la vérification de l'authenticité du premier équipement, le certificat du premier équipement reçu dans le message est vérifié à l'aide du module cryptographique sécurisé (SE), en fonction de la clef publique de l'autorité de certification préalablement stockée en mode sécurisé dans le module cryptographique sécurisé (SE).

[Revendication 6] Procédé de transmission sécurisée selon l'une quelconque des revendications précédentes, le premier équipement comprenant un module cryptographique sécurisé (SE), adapté pour exécuter des fonctions cryptographiques prédéfinies, pour stocker des informations cryptographiques dont la clef privée du premier équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ; le premier équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée (14) et une mémoire commune (13) et des fonctions logicielles s'exécutant sur le processeur, ledit premier équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;
et les étapes décrites relativement au premier équipement, respectivement au deuxième équipement, sont en outre mises en œuvre symétriquement, i.e. cette fois par le deuxième équipement, respectivement par le premier équipement.

[Revendication 7] Système de télécommunication (1) comprenant un premier équipement de télécommunication (SERV) et au moins un deuxième équipement de télécommunication (DISPO1), un couple respectif clef privée – clef publique étant associé à chacun desdits premier et deuxième équipements
le deuxième équipement comprenant un module cryptographique sécurisé (SE), adapté pour exécuter des fonctions cryptographiques pré-

définies, pour stocker des informations cryptographiques dont la clef privée du deuxième équipement et pour ne pas pouvoir délivrer certaines au moins desdites informations cryptographiques stockées ;
le deuxième équipement comportant un processeur, au moins deux zones mémoires comprenant une mémoire sécurisée (14) et une mémoire commune (13) et des fonctions logicielles s'exécutant sur le processeur, ledit deuxième équipement étant adapté pour opérer alternativement selon un premier mode dit mode non sécurisé et un deuxième mode dit mode sécurisé, tel que les fonctions logicielles s'exécutant dans le mode non sécurisé du processeur peuvent seulement accéder à la mémoire commune, tandis qu'à l'inverse, les fonctions logicielles s'exécutant dans le mode sécurisé du processeur peuvent accéder à la mémoire sécurisée et à la mémoire commune ;
lesdits premier équipement de télécommunication (SERV) et au moins deuxième équipement de télécommunication (DISPO1) étant adaptés pour mettre en œuvre entre eux une opération d'authentification au cours de laquelle

– le premier équipement (SERV) est adapté pour générer une première valeur aléatoire et pour stocker ladite première valeur aléatoire, pour chiffrer ladite première valeur aléatoire avec la clef publique du deuxième équipement préalablement obtenue, pour déterminer une première signature, par utilisation de la clef privée du premier équipement (SERV), de ladite première valeur aléatoire chiffrée, pour transmettre à destination du deuxième équipement (DISPO1) un message comportant ladite première valeur aléatoire chiffrée et ladite première signature ;

- le deuxième équipement (DISPO1) est adapté, dans le mode non sécurisé, pour recevoir ledit message et copier ledit message dans la mémoire commune,
- puis le deuxième équipement (DISPO1) est adapté, en mode sécurisé, pour vérifier l'authenticité du premier équipement en fonction de ladite première valeur aléatoire chiffrée, de la première signature et de la clef publique du premier équipement préalablement obtenue, puis si l'authenticité a été vérifiée, pour que le module cryptographique sécurisé (SE) déchiffre, au moyen de la clef privée du deuxième

équipement stockée dans ledit module, ladite première valeur aléatoire chiffrée, pour stocker la première valeur aléatoire déchiffrée dans la mémoire sécurisée ; le deuxième équipement (DISPO1) étant adapté pour, en mode sécurisé, obtenir une deuxième valeur aléatoire et stocker ladite deuxième valeur aléatoire dans la mémoire sécurisée, pour chiffrer ladite deuxième valeur aléatoire avec la clef publique du premier équipement préalablement obtenue, pour que le module cryptographique sécurisé (SE) détermine une deuxième signature, avec la clef privée du deuxième équipement stockée dans le ledit module, de ladite deuxième valeur aléatoire chiffrée, et pour copier dans la mémoire commune ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature ;

le deuxième équipement (DISPO1) est adapté pour, dans le mode non sécurisé, préparer, pour transmission à destination du premier équipement (SERV), un message comportant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature, transmettre à destination du premier équipement (SERV), ledit message ;

le premier équipement (SERV) étant adapté pour recevoir ledit message contenant ladite deuxième valeur aléatoire chiffrée et ladite deuxième signature, pour vérifier l'authenticité du deuxième équipement en fonction de ladite deuxième valeur aléatoire chiffrée, de ladite deuxième signature et de la clef publique du deuxième équipement préalablement obtenue, puis si l'authenticité a été vérifiée, pour déchiffrer ladite deuxième valeur aléatoire chiffrée en fonction de la clef privée du premier équipement ;

le premier équipement (SERV) étant adapté pour déterminer une clef de chiffrement symétrique, dite clef d'initialisation en fonction de ladite première valeur aléatoire stockée et de ladite deuxième valeur aléatoire déchiffrée, en mettant en œuvre une fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires ;

le deuxième équipement est adapté pour, en mode sécurisé, déterminer ladite clef d'initialisation en fonction de ladite première valeur aléatoire stockée et de la deuxième valeur aléatoire stockée, en mettant en œuvre ladite fonction de calcul de clef d'initialisation ayant pour variables lesdites première et deuxième valeurs aléatoires et dont le résultat sera de façon strictement déterministe la clef d'initialisation également calculée par le premier équipement, et stocker de ladite clef

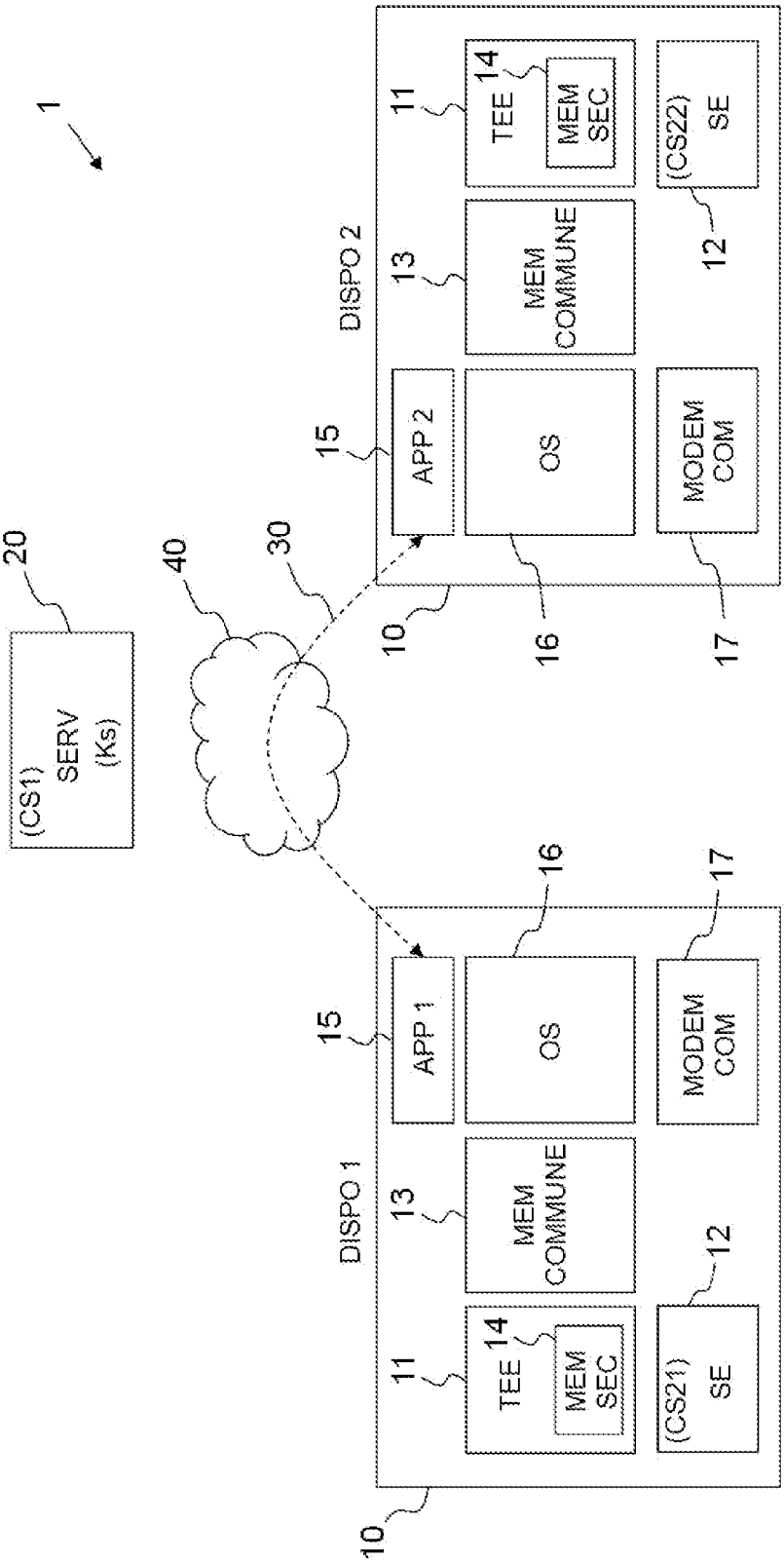
d'initialisation dans la mémoire sécurisée;
le premier équipement (SERV) étant adapté pour chiffrer l'élément secret avec ladite clef d'initialisation qu'il a déterminée, et pour transmettre ledit élément secret chiffré au deuxième équipement (DISPO1) ;
le deuxième équipement (DISPO1) étant adapté pour recevoir ledit élément secret chiffré, pour déchiffrer, en mode sécurisé, ledit élément secret à l'aide de la clef d'initialisation stockée et pour stocker ledit élément secret dans la mémoire sécurisée ou dans le module cryptographique sécurisé (SE).

[Revendication 8] Système de télécommunication (1) selon la revendication 7, dans lequel le premier équipement (SERV) est un serveur de clefs, l'élément secret comporte au moins une clef de session et l'opération d'authentification est mise en œuvre par le serveur de clefs avec une pluralité de deuxièmes équipements (DISPO1, DISPO2, ...) pour transmettre auxdits deuxièmes équipements ladite même clef de session ;
au moins deux desdits deuxièmes équipements (DISPO1, DISPO2, ...) étant adaptés pour établir entre eux une session de télécommunication en fonction de ladite clé de session stockée dans chacun desdits deuxièmes équipements suite à leur transmission par le serveur de clefs.

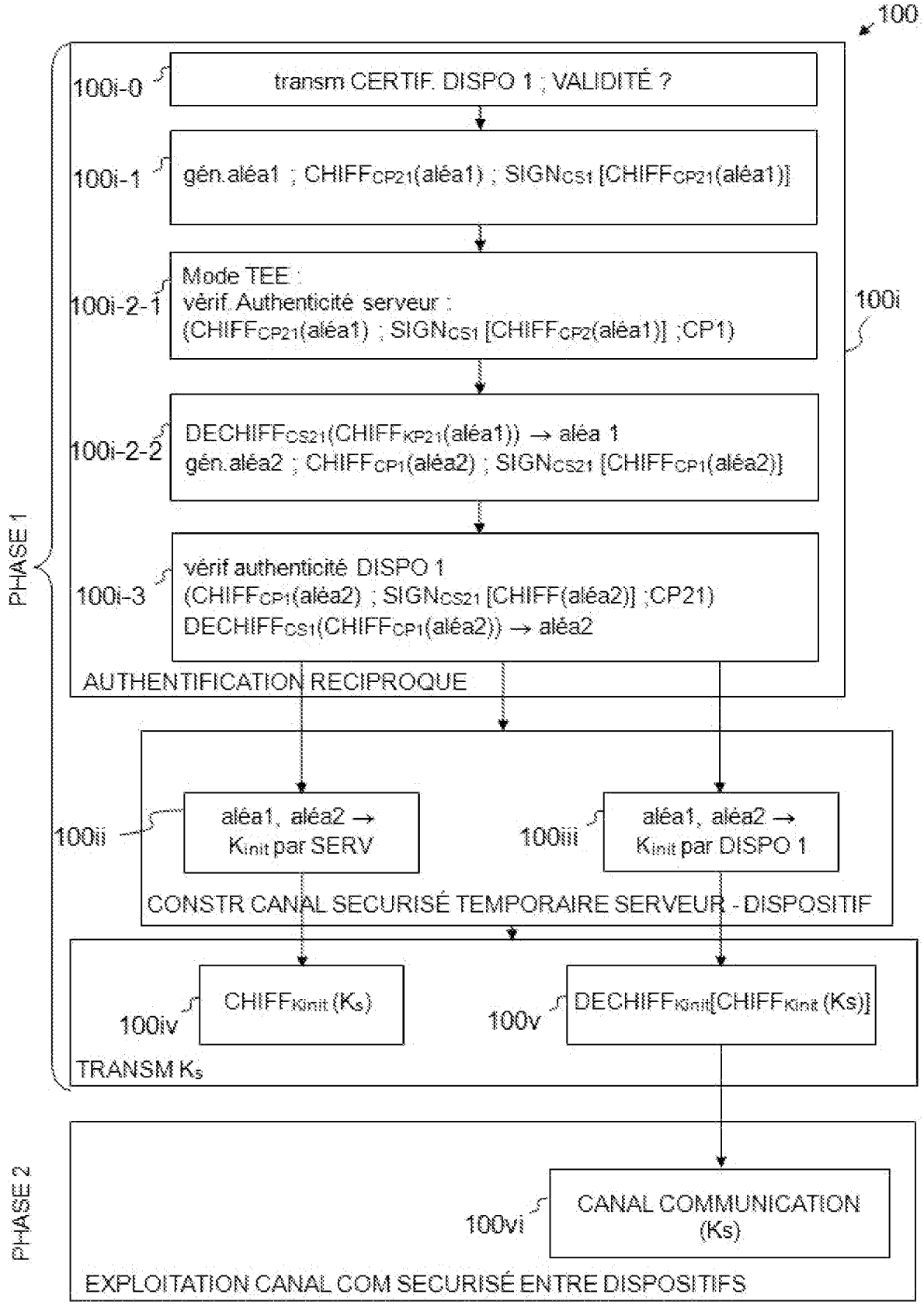
[Revendication 9] Système de télécommunication (1) selon la revendication 7 ou 8, dans lequel le premier équipement (SERV) est un serveur de clefs, l'élément secret comporte au moins une clef de session et l'opération d'authentification est mise en œuvre par le serveur avec une pluralité d'applications logicielles d'un même deuxième équipement pour transmettre auxdits applications ladite même clef de session ;
au moins deux desdites applications étant adaptées pour établir entre elles une session de télécommunication en fonction d'au moins lesdites copies de ladite clé de session stockées suite à leur transmission par le serveur de clefs.

[Revendication 10] Système de télécommunication (1) selon l'une quelconque des revendications 7 à 9, dans lequel le module cryptographique sécurisé (SE) du deuxième équipement (DISPO1) est un module discret et/ou le module cryptographique sécurisé (SE) du deuxième équipement (DISPO1) est adapté pour ne pouvoir échanger qu'au sein du deuxième équipement et uniquement en mode sécurisé.

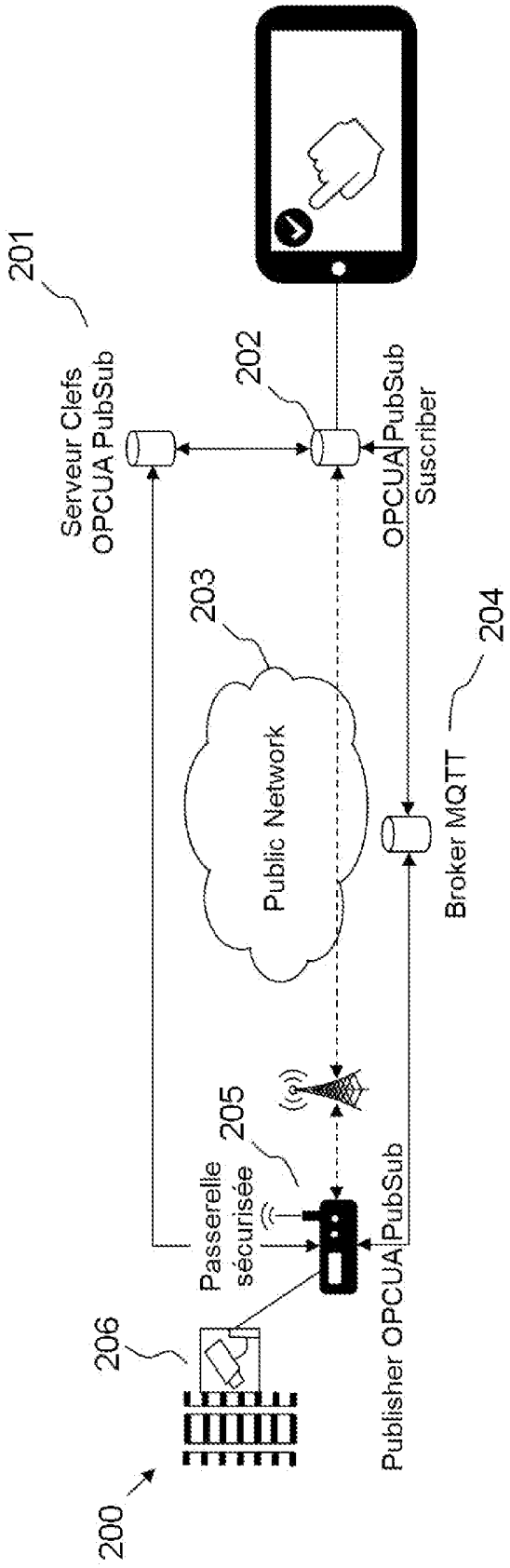
[Fig. 1]


1
DISPO 2
DISPO 1
11
TEE
14
MEM SEC
13
MEM COMMUNE
12
(CS22) SE
(CS21) SE
15
APP 2
APP 1
OS
16
MODEM COM
17
10
20
(CS1) SERV (Ks)
40
30

[Fig. 2]


100
100i-0
transm CERTIF. DISPO 1 ; VALIDITÉ ?
100i-1
gén.aléa1 ; CHIFF$_{CP21}$(aléa1) ; SIGN$_{CS1}$ [CHIFF$_{CP21}$(aléa1)]
100i-2-1
Mode TEE :
vérif. Authenticité serveur :
(CHIFF$_{CP21}$(aléa1) ; SIGN$_{CS1}$ [CHIFF$_{CP2}$(aléa1)] ;CP1)
100i
100i-2-2
DECHIFF$_{CS21}$(CHIFF$_{KP21}$(aléa1)) → aléa 1
gén.aléa2 ; CHIFF$_{CP1}$(aléa2) ; SIGN$_{CS21}$ [CHIFF$_{CP1}$(aléa2)]
100i-3
vérif authenticité DISPO 1
(CHIFF$_{CP1}$(aléa2) ; SIGN$_{CS21}$ [CHIFF(aléa2)] ;CP21)
DECHIFF$_{CS1}$(CHIFF$_{CP1}$(aléa2)) → aléa2
AUTHENTIFICATION RECIPROQUE
PHASE 1
100ii
aléa1, aléa2 → K_{init} par SERV
100iii
aléa1, aléa2 → K_{init} par DISPO 1
CONSTR CANAL SECURISÉ TEMPORAIRE SERVEUR - DISPOSITIF
100iv
CHIFF$_{Kinit}$ (K_S)
100v
DECHIFF$_{Kinit}$[CHIFF$_{Kinit}$ (K_S)]
TRANSM K_S
PHASE 2
100vi
CANAL COMMUNICATION (K_S)
EXPLOITATION CANAL COM SECURISÉ ENTRE DISPOSITIFS

[Fig. 3]


201
Serveur Clefs
OPCUA PubSub
202
OPCUA PubSub
Suscriber
203
Public Network
204
Broker MQTT
205
Passerelle
sécurisée
Publisher OPCUA PubSub
206
200

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 917603
FR 2214622

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 7 568 223 B2 (GEN INSTRUMENT CORP [US]) 28 juillet 2009 (2009-07-28) * colonne 7, ligne 9 - colonne 8, ligne 64; figures 1-2C * * colonne 2, lignes 20-39 * -----	1-10	G06F 21/44 G06F 21/64 H04L 9/30 H04W 12/069 H04L 9/22
T	"Chapter 12: Key Establishment Protocols ED - Menezes A J; Van Oorschot P C; Vanstone S A", HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], CRC PRESS, BOCA RATON, FL, US, PAGE(S) 489 - 541 , 1 octobre 1996 (1996-10-01), XP001525012, ISBN: 978-0-8493-8523-0 Extrait de l'Internet: URL:http://www.cacr.math.uwaterloo.ca/hac/ * section 12.5.2 (iii) and (iv) section 12.6.1 * -----		

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L

Date d'achèvement de la recherche	Examinateur
30 octobre 2023	Manet, Pascal

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
.....
& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 2214622 FA 917603

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 30-10-2023
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 7568223 B2	28-07-2009	AT E313200 T1	15-12-2005
		AU 4079200 A	14-11-2000
		AU 4213600 A	14-11-2000
		CA 2365856 A1	19-10-2000
		CA 2370471 A1	19-10-2000
		CN 1346563 A	24-04-2002
		DE 60024800 T2	06-07-2006
		EP 1169833 A1	09-01-2002
		EP 1171989 A2	16-01-2002
		HK 1045917 A1	13-12-2002
		US 2005027985 A1	03-02-2005
		US 2009323954 A1	31-12-2009
		WO 0062507 A1	19-10-2000
		WO 0062519 A2	19-10-2000

EPO FORM P0465