(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 062 013***

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

(21) **N° d'enregistrement national :** **17 50326**

(51) Int Cl[8] : ***H 04 N 21/23*** *(2017.01), H 04 L 9/00, 29/06*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 16.01.17.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.07.18 Bulletin 18/29.

(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) :** *ORANGE Société anonyme* — FR.

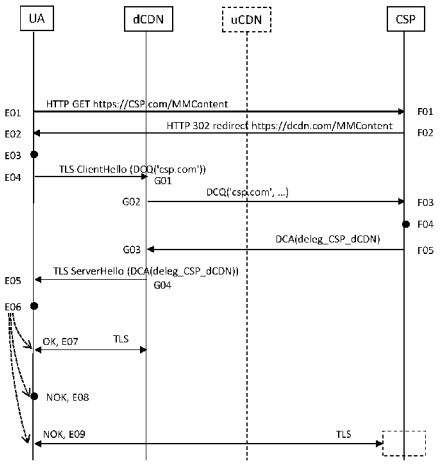
(72) **Inventeur(s) :** STEPHAN EMILE et FIEAU FREDERIC.

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

(74) **Mandataire(s) :** ORANGE.

(54) PROCEDES ET DISPOSITIFS DE VERIFICATION DE LA VALIDITE D'UNE DELEGATION DE DIFFUSION DE CONTENUS CHIFFRES.

(57) L'invention concerne un procédé de vérification d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA).



FR 3 062 013 - A1

Procédés et dispositifs de vérification de la validité d'une délégation de diffusion de contenus chiffrés

1. Domaine de l'invention

La demande d'invention se situe dans le domaine des réseaux de distribution de contenus, et plus particulièrement pour les contenus chiffrés.

2. Etat de la technique antérieure

Une part de plus en plus grande du trafic Internet est transportée sur le protocole TLS (Transport Layer Security, sécurité de la couche de transport, en anglais), un protocole standardisé par l'IETF dans le RFC 5346 et permettant de sécuriser les échanges entre un client et un serveur.

TLS permet d'authentifier le serveur ou le client, de chiffrer le contenu des échanges entre eux et d'en vérifier l'intégrité.

Lorsqu'un utilisateur souhaite consommer un contenu sur Internet par le biais du navigateur de son terminal client, une requête est émise à un serveur d'un fournisseur de contenu. Le plus souvent, ce fournisseur de contenu délègue la livraison du contenu à un autre serveur, choisi en fonction de plusieurs critères, comme par exemple la localisation du terminal du client et les termes du contrat entre le fournisseur de contenu et l'opérateur de l'autre serveur, lorsque ce contrat existe.

Malgré la sécurité apportée par TLS, le terminal client n'a aucun moyen de vérifier la validité de cette délégation. Ceci est d'autant plus problématique que les CDN (Content Delivery Network, réseau de distribution de contenu, en anglais), auxquels est déléguée la livraison du contenu, sont de plus en plus nombreux, et peuvent se déléguer entre eux la délégation qu'ils ont reçue d'un fournisseur de contenu, sans que ce dernier nécessairement le sache.

Un des buts de l'invention est de remédier à ces inconvénients de l'état de la technique.

3. Exposé de l'invention

L'invention vient améliorer la situation à l'aide d'un procédé de vérification d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client, le procédé comprenant les étapes suivantes mises en œuvre par le terminal :

- émission d'un premier message de requête du contenu, à destination du premier serveur, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- réception d'un message de redirection, comprenant au moins un identifiant d'un serveur tiers,
- obtention d'une adresse du second serveur, à partir de l'au moins un identifiant reçu dans le message de redirection,
- émission d'une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur.

Le procédé de vérification est particulier en ce qu'il comprend en outre les étapes suivantes :

- réception d'un message de certification en provenance du second serveur, comprenant un certificat de délégation signé par le premier serveur, au travers de la seconde connexion chiffrée,
- vérification du certificat de délégation à l'aide de la clé de chiffrement associée au premier serveur,
- émission d'un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

Le procédé de vérification selon l'invention permet au terminal de vérifier si la

délégation de livraison du contenu par une connexion chiffrée est bien valable.

Lorsqu'un terminal requiert un contenu à un serveur de contenu, et que ce serveur a délégué la livraison de ce contenu à un serveur tiers, le terminal reçoit du premier serveur un message de redirection comprenant un identifiant de ce serveur tiers, à qui il a délégué la livraison du contenu. Avec cet identifiant, le terminal obtient une adresse, qui peut être celle correspondant à l'identifiant, mais qui peut aussi être celle d'un autre serveur, à qui le serveur tiers a lui-même délégué son rôle. On parle alors de délégation multiple. Cette seconde délégation à cet autre serveur, en cascade de la première, peut se faire par exemple à l'aide d'une simple redirection DNS, invisible du premier serveur.

Dans la technique antérieure, par exemple basée sur https, sur le DNS, et sur un protocole de vérification de certificat tel que OCSP (Online Certificate Status Protocol, ou protocole de statut de certificat en ligne, en anglais) ou sa variante OCSP Stapling, le terminal peut s'assurer que tous les serveurs impliqués dans la chaine de délégation sont authentifiés par une autorité de certification, mais rien ne lui permet de vérifier la validité de la seconde délégation, ou a fortiori la validité de toute délégation suivante, en cas de délégation multiple à plus de deux niveaux.

Grâce au procédé de vérification selon l'invention, le terminal reçoit du second serveur un certificat de délégation, lui permettant de décider d'accéder au contenu ou non, en fonction de sa vérification du certificat. Cette vérification se faisant à l'aide d'une clé publique propre au premier serveur, le terminal peut vérifier que le certificat de délégation reçu du second serveur a été établi avec l'accord du premier serveur.

Même dans le cas le plus simple, où il n'y a pas de délégation multiple en cascade, c'est-à-dire dans le cas où le second serveur qui livre le contenu est le serveur tiers connu du premier serveur, il se peut que la délégation ait été révoquée entretemps par le premier serveur, pour une raison quelconque. Grâce à ce procédé selon l'invention, le terminal peut vérifier que le certificat de délégation reçu du second serveur établi valablement à un instant donné avec l'accord du premier serveur, est encore valable à l'instant où le terminal requiert le contenu. De plus, dans ce cas, ce procédé donne une occasion au second serveur de renouveler son certificat de

délégation auprès du premier serveur s'il est devenu trop ancien.

Selon un aspect de l'invention, l'étape d'obtention d'une adresse du second serveur comprend une étape de sélection de l'adresse parmi les identifiants de serveurs tiers, et/ou une étape d'interrogation d'un serveur de résolution d'adresse avec un identifiant.

Avantageusement, si le message de redirection en provenance du premier serveur comprend une liste d'identifiants ou d'adresses, le terminal peut en sélectionner une selon ses propres critères. De même si le message de redirection en provenance du premier serveur comprend un nom de domaine, le terminal peut obtenir une adresse à partir de ce nom en effectuant une requête DNS.

Selon un aspect de l'invention, le procédé comprend en outre une étape d'émission d'un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

Avantageusement, le terminal client consomme le contenu demandé au travers d'une connexion avec le second serveur, auquel le premier serveur a légitimement délégué la livraison.

Selon un aspect de l'invention, le message de certification comprend en outre une instruction de redirection et où le procédé comprend en outre une étape de redirection du terminal vers un troisième serveur.

Que le certificat de délégation soit valable ou non, c'est-à-dire que le premier serveur ait accepté ou non de déléguer la livraison au second serveur, le premier serveur peut inviter le terminal à se connecter à un serveur autre que le second serveur plutôt que de rester connecté au second serveur. Ce serveur de redirection peut être le premier serveur, ou un site ou un serveur déterminé par le premier serveur. Le site peut par exemple être une page d'information avertissant que le second serveur n'est pas un serveur approprié pour livrer le contenu demandé. Le serveur peut être un

serveur de livraison alternatif, préférable au second serveur.

Les différents aspects du procédé de vérification qui viennent d'être décrits peuvent être mis en œuvre indépendamment les uns des autres ou en combinaison les uns avec les autres.

L'invention concerne aussi un procédé de production d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client, le procédé comprenant les étapes suivantes mises en œuvre par le premier serveur:

- réception d'un message de requête du contenu, en provenance du terminal, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- émission d'un message de redirection à destination du terminal, comprenant au moins un identifiant d'un serveur tiers,

Le procédé de production est particulier en ce qu'il comprend en outre les étapes suivantes :

- réception d'un message de demande d'un certificat de délégation, en provenance d'un second serveur, comprenant un certificat d'authenticité du second serveur,
- analyse de la demande d'un certificat de délégation,
- en fonction du résultat de l'analyse, émission d'un message de réponse de certificat de délégation, à destination du second serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide de la clé de chiffrement.

Grâce au procédé de production selon l'invention, le premier serveur peut décider, si cela est approprié selon des critères propres au premier serveur, de fournir à un second serveur qui n'est pas forcément le serveur tiers auquel le premier serveur a éventuellement déjà délégué la livraison du contenu, une information concernant la délégation du premier au second serveur. Cette information ne peut pas être modifiée

par le second serveur, mais peut être vérifiée par le terminal auquel le second serveur la transmet.

Selon un aspect de l'invention, le message de demande d'un certificat de délégation comprend en outre une adresse du terminal client.

Avantageusement, le premier serveur peut ainsi prendre en compte, lors de l'étape d'analyse, l'adresse du terminal demandant le contenu. Ceci est utile car avec l'adresse il est possible de déterminer la localisation géographique, et, connaissant celle du second serveur, le premier serveur peut déterminer si la distance entre le terminal et le second serveur est propice à une livraison satisfaisante du contenu.

Selon un aspect de l'invention, le message de demande d'un certificat de délégation comprend en outre une signature du serveur tiers.

Avantageusement, le premier serveur peut ainsi prendre en compte, lors de l'étape d'analyse, la signature du serveur tiers. Ceci est utile car ce serveur tiers dispose normalement d'une délégation valable de la part du premier serveur, ou en a en tout cas déjà disposé. Le second serveur peut donc déduire que le second serveur a obtenu une délégation du serveur tiers, ce qui renforce la légitimité du second serveur auprès du premier serveur.

Selon un aspect de l'invention, le message de réponse de certificat de délégation comprend en outre une instruction de redirection pour le terminal client.

Que le premier serveur ait décidé ou non de déléguer la livraison au second serveur, le premier serveur peut inviter le terminal à se connecter à un site déterminé par le premier serveur, plutôt que de rester connecté au second serveur. Ce site peut par exemple être une page d'information avertissant que le second serveur n'est pas un serveur approprié pour livrer le contenu demandé, ou être un serveur de livraison alternatif, préférable au second serveur par exemple en raison de performances supérieures.

Les différents aspects du procédé de production qui viennent d'être décrits

peuvent être mis en œuvre indépendamment les uns des autres ou en combinaison les uns avec les autres.

L'invention concerne encore un procédé de demande d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA), le procédé comprenant les étapes suivantes mises en œuvre par le second serveur :

- réception d'une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur.

Le procédé de demande est particulier en ce qu'il comprend en outre les étapes suivantes :

- émission d'un message de demande d'un certificat de délégation, à destination du premier serveur, comprenant un certificat d'authenticité du second serveur,
- réception d'un message de réponse de certificat de délégation, en provenance du premier serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide d'une clé de chiffrement associée au premier serveur,
- émission d'un message de certification à destination du terminal, comprenant le certificat de délégation, au travers de la seconde connexion chiffrée, le terminal ayant préalablement obtenu une clé de chiffrement associée au premier serveur, au moyen d'une première connexion chiffrée entre le terminal et le premier serveur.

Ainsi, lorsque le second serveur reçoit une demande d'établissement d'une connexion d'un terminal souhaitant consommer un contenu référencé sur le premier serveur, le second serveur est en mesure de prouver qu'il a obtenu une délégation valable de la part du premier serveur.

L'invention concerne encore un dispositif de vérification d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client, le dispositif comprenant une machine de calcul reprogrammable ou une machine de

calcul dédiée, apte à et configurée pour :

- émettre un premier message de requête du contenu, à destination du premier serveur, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- recevoir un message de redirection en provenance du premier serveur, comprenant au moins un identifiant d'un serveur tiers,
- obtenir une adresse du second serveur, à partir de l'au moins un identifiant reçu dans le message de redirection,
- émettre une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur,
- recevoir un message de certification en provenance du second serveur, comprenant un certificat de délégation signé par le premier serveur, au travers de la seconde connexion chiffrée,
- vérifier le certificat de délégation à l'aide de la clé de chiffrement associée au premier serveur,
- émettre un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

Ce dispositif de vérification, apte à mettre en œuvre dans tous ses modes de réalisation le procédé de vérification qui vient d'être décrit, est destiné à être mis en œuvre dans un terminal client ou dans une application comprise dans le terminal telle qu'un navigateur (browser en anglais).

L'invention concerne encore un dispositif de production d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client, le dispositif comprenant une machine de calcul reprogrammable ou une machine de calcul dédiée, apte à et configurée pour :

- recevoir un message de requête du contenu, en provenance du terminal, au

travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,

- émettre un message de redirection à destination du terminal, comprenant au moins un identifiant d'un serveur tiers,
- recevoir un message de demande d'un certificat de délégation, en provenance d'un second serveur, comprenant un certificat d'authenticité du second serveur,
- analyser la demande d'un certificat de délégation,
- en fonction du résultat de l'analyse, émettre un message de réponse de certificat de délégation, à destination du second serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide de la clé de chiffrement.

Ce dispositif de production, apte à mettre en œuvre dans tous ses modes de réalisation le procédé de production qui vient d'être décrit, est destiné à être mis en œuvre par exemple dans un serveur de référencement de contenu.

L'invention concerne aussi un dispositif de demande d'un certificat de délégation, la délégation étant d'un premier serveur à un second serveur, pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client, le dispositif comprenant une machine de calcul reprogrammable ou une machine de calcul dédiée, apte à et configurée pour :

- recevoir une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur,
- émettre un message de demande d'un certificat de délégation, à destination du premier serveur, comprenant un certificat d'authenticité du second serveur,
- recevoir un message de réponse de certificat de délégation, en provenance du premier serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide d'une clé de chiffrement associée au premier serveur,
- émettre un message de certification à destination du terminal, comprenant le certificat de délégation, au travers de la seconde connexion chiffrée, le terminal ayant préalablement obtenu une clé de chiffrement associée au premier serveur,

au moyen d'une première connexion chiffrée entre le terminal et le premier serveur.

Ce dispositif de demande, apte à mettre en œuvre dans tous ses modes de réalisation le procédé de demande qui vient d'être décrit, est destiné à être mis en œuvre par exemple dans un serveur de diffusion de contenu.

L'invention concerne aussi un système de vérification d'un certificat de délégation, comprenant un dispositif de vérification, un dispositif de production et un dispositif de demande d'un certificat de délégation.

L'invention vise enfin :

- un programme d'ordinateur comprenant des instructions pour la mise en œuvre des étapes du procédé de vérification qui vient d'être décrit, lorsque ce programme est exécuté par un processeur, ainsi qu'un support d'informations lisible par un terminal client, et comportant des instructions de ce programme d'ordinateur,
- un programme d'ordinateur comprenant des instructions pour la mise en œuvre des étapes du procédé de production qui vient d'être décrit, lorsque ce programme est exécuté par un processeur, ainsi qu'un support d'informations lisible par un serveur de référencement de contenu, et comportant des instructions de ce programme d'ordinateur,
- un programme d'ordinateur comprenant des instructions pour la mise en œuvre des étapes du procédé de demande qui vient d'être décrit, lorsque ce programme est exécuté par un processeur, ainsi qu'un support d'informations lisible par un serveur de diffusion de contenu, et comportant des instructions de ce programme d'ordinateur.

Ces programmes peuvent utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

Les supports d'informations peuvent être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, un tel support peut comporter un

moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, un tel support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Un programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, un support d'informations selon l'invention peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution des procédés en question.

4. Présentation des figures

D'autres avantages et caractéristiques de l'invention apparaitront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier de l'invention, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 illustre une configuration réseau situant les entités impliquées dans la technique décrite,
- la figure 2 présente un exemple d'enchainement et de mise en œuvre des étapes du procédé de demande d'un certificat de délégation, du procédé de vérification d'un certificat de délégation et du procédé de production d'un certificat de délégation, selon un aspect de l'invention,
- la figure 3 présente un exemple de structure d'un dispositif de vérification d'un certificat de délégation, selon un aspect de l'invention,
- la figure 4 présente un exemple de structure d'un dispositif de production d'un certificat de délégation, selon un aspect de l'invention,
- la figure 5 présente un exemple de structure d'un dispositif de demande d'un certificat de délégation, selon un aspect de l'invention.

5. Description détaillée d'au moins un mode de réalisation de l'invention

Dans la suite de la description, on présente des exemples de plusieurs modes de réalisation de l'invention se basant sur les protocoles TLS et https, mais l'invention peut se baser sur d'autres protocoles, tel que par exemple les protocoles HTTP1.1, SPDY, HTTP2, SCTP, DTLS et QUIC.

On décrit maintenant, en relation avec la **figure 1**, une configuration réseau situant les entités impliquées dans la technique décrite. Plus particulièrement, les entités suivantes sont illustrées :

- un serveur CSP d'un fournisseur de contenu référençant différents contenus (par exemple du contenu multimédia, du type comprenant des sons, des images ou des vidéos, ou des fichiers exécutables) destinés à être distribués à des terminaux clients d'utilisateurs finaux ;
- un terminal client UA, par exemple un ordinateur, un smartphone d'un utilisateur, cherchant à obtenir un contenu auprès du fournisseur de contenu, un tel terminal client UA pouvant embarquer un ou plusieurs agents clients ("User Agent" en anglais) du type http (pour "HyperText Transfer Protocol" en anglais) ou HTTPS (pour "HyperText Transfer Protocol Secure" en anglais) ou encore du type navigateur Internet ;
- un serveur de livraison de contenu uCDN auquel le serveur CSP du fournisseur de contenu a délégué la livraison du contenu en question et qui est connu du serveur CSP du fournisseur de contenu à l'aide d'un nom de domaine ;
- un secondaire de livraison de contenu dCDN auquel le primaire de livraison de contenu uCDN a potentiellement délégué la livraison du contenu recherché par l'utilisateur du terminal client UA dans un contexte de double délégation. ;
- un serveur de résolution de nom de domaine DNS permettant d'associer un nom de domaine à une adresse réseau ;
- un serveur CA d'une autorité de certification permettant de délivrer des certificats, par exemple selon le protocole HTTPS (pour « HyperText Transfer Protocol

Secure » en anglais), aux serveurs en question.

Les différentes entités présentées ci-dessus sont alors connectées entre elles via un réseau 100 de télécommunications pour la transmission de données, par exemple basé sur un protocole internet.

Dans certains modes de réalisation, un serveur de résolution de nom de domaine local LDNS fait appel à un serveur DNS central.

Dans certains modes de réalisation, plusieurs serveurs CA d'autorités de certification sont utilisés, chaque serveur pouvant faire appel à un serveur CA différent.

Dans d'autres modes de réalisation, les serveurs de livraison uCDN et dCDN peuvent être regroupés dans une seule et même entité matérielle.

Dans encore d'autres modes de réalisation, davantage de serveurs de livraison sont présents, par exemple dans un contexte de délégations en cascade.

La **figure 2** présente un exemple d'enchainement et de mise en œuvre des étapes du procédé de demande d'un certificat de délégation, du procédé de vérification d'un certificat de délégation et du procédé de production d'un certificat de délégation, selon un aspect de l'invention.

Un utilisateur d'un terminal UA souhaite consommer un contenu multimédia MMContent, référencé par un fournisseur de contenu, dont il connait ou a obtenu l'identité d'une façon quelconque.

Dans une phase initiale non illustrée, par exemple à l'aide d'un moteur de recherche et une recherche à partir d'un nom du contenu ou à partir du nom du fournisseur de contenu, le terminal UA récupère le nom de domaine d'un serveur CSP associé au fournisseur de contenu, sur lequel est référencé le contenu MMContent. Cette adresse est par exemple sous forme d'url (Uniform Resource Locator, ou localisateur uniforme de ressource, en anglais), telle que 'csp.com'.

Lors d'une étape **E01**, connue, à l'aide d'une application spécifique ou d'un navigateur générique, le terminal UA émet une requête pour obtenir le contenu MMContent. Par souci de simplicité le terme "terminal" est utilisé dans ce document, mais il peut représenter une telle application ou un tel navigateur (appelé "browser" en

anglais), installée ou installé sur le terminal.

Cette requête pour obtenir le contenu est par exemple une requête http utilisant le protocole https, telle que:

"http GET https://csp.com/MMContent".

Cette requête fait suite à une procédure d'établissement d'un tunnel sécurisé TLS entre le terminal UA et le serveur CSP. Cette procédure comprend l'envoi d'un message TLS ClientHello par l'UA. Le serveur CSP émet en réponse vers le terminal UA un message ServerHello comprenant du matériel cryptographique comme par exemple une clé publique à laquelle est associée une clé privée conservée par l'administrateur du domaine CSP, ou encore un ticket de session SessionTicket (tel que décrit dans le RFC5077). La clé publique est en général attachée à un certificat du serveur CSP, que le serveur CSP a obtenu après d'une autorité de certification quelconque. Ce matériel permettra au terminal UA de déchiffrer ultérieurement du contenu chiffré par le serveur CSP ou par un autre serveur du même domaine 'csp.com'

Lors d'une étape **F01**, connue, le serveur CSP reçoit la requête http GET et identifie un serveur tiers, avec lequel une relation d'ordre contractuel existe. Ce serveur est sélectionné par le serveur CSP selon divers critères, tels que par exemple une proximité en termes de réseau avec le terminal UA, ou un profil utilisateur du terminal UA.

Lors d'une étape **F02**, connue, L'UA est redirigé de proche en proche vers le serveur en charge d'effectuer la livraison du contenu.

Dans le cas où la délégation est simple, le serveur tiers est celui qui effectue la livraison du contenu au terminal UA. Le serveur tiers est alors le serveur dCDN.

Dans le cas où la délégation est multiple, c'est-à-dire le cas où le serveur tiers n'effectue pas la livraison du contenu mais l'a déléguée à un autre serveur, le serveur tiers est le serveur uCDN et cet autre serveur est le serveur dCDN.

Dans le cas à délégation simple, lors de l'étape **F02**, le serveur CSP émet aussi vers le terminal UA un message de redirection en réponse à la requête "http GET

https://csp.com/MMContent", comprenant l'adresse du serveur dCDN, "dcdn.com". Ce message de redirection est par exemple :

"http 302 redirect https://dcdn.com/MMContent",

que le terminal UA reçoit lors d'une étape **E02**.

Dans le cas à délégation multiple, plusieurs méthodes connues, basées sur des redirections obligatoires HTTP et DNS, ou sur des redirections alternatives, ou sur une combinaison des deux, ont pour résultat final que le terminal UA dispose d'une adresse du serveur dCDN, sous forme d'adresse url ou d'adresse IP. Le message de redirection émis lors de l'étape **F02** est alors, par exemple :

"http 302 redirect https://dcdn.com/MMContent",

que le terminal UA reçoit lors de l'étape **E02**.

Dans ce cas, lors d'une étape **E03**, le terminal UA obtient l'adresse IP du serveur dCDN par une requête DNS sur le nom de domaine "dcdn.com".

Il se peut également qu'un des serveurs impliqués dans la redirection, par exemple le serveur CSP, insère une liste de plusieurs adresses de serveur dans un message de redirection alternative émis lors de l'étape **F02**. Dans ce cas, lors de l'étape **E03**, le terminal UA obtient l'adresse IP du serveur dCDN après avoir effectué une sélection parmi les adresses de serveur comprises dans la réponse, sur des critères tels que par exemple la proximité entre le terminal UA et les serveurs de la liste, la liste étant comprise dans une réponse de type out-of-band encoding tel que décrit dans le document "https://tools.ietf.org/html/draft-reschke-http-oob-encoding-08.txt".

Dans tous les cas présentés ci-dessus, en fin d'étape E03 le terminal UA dispose d'une url vers le domaine 'dCDN.com' et de l'adresse IP d'un serveur de 'dCDN.com', le serveur dCDN.

Lorsque le terminal UA a obtenu l'adresse du serveur dCDN, il demande, lors d'une étape **E04**, l'établissement d'une session chiffrée entre lui-même et le serveur dCDN. Il s'agit par exemple d'un tunnel sécurisé TLS entre le terminal UA et le serveur dCDN. Cette procédure comprend l'envoi d'un message TLS ClientHello par le terminal UA. Pour ce faire, ce message est émis par le terminal UA, reçu par le serveur dCDN lors d'une étape **G01**, comprenant, dans un mode préféré de réalisation de l'invention,

une requête au serveur dCDN de prouver qu'il a obtenu une délégation valable de la part d'un serveur du domaine 'csp.com'. Ce message peut être par exemple un message selon une modification du protocole TLS, comprenant une requête de certificat de délégation DCQ (pour Delegation Challenge Query, ou requête de preuve de délégation, en anglais), tel que :

"TLS ClientHello (DCQ('csp.com', options) ; SNI='dCDN.com')".

Optionnellement, le contenu du message est signé à l'aide d'une clé préalablement obtenue par le terminal UA, comme par exemple une clé de type SessionTicket, afin que le serveur dCDN ne puisse pas modifier le contenu de la requête DCQ.

Afin d'obtenir cette preuve exigée par le terminal UA, appelée certificat de délégation, le serveur dCDN doit la requérir, ou l'avoir préalablement requise, de la part du domaine 'csp.com'.

Dans un mode dit **synchrone**, la requête de certificat de délégation émise par le serveur dCDN lors d'une étape **G02** est déclenchée par l'étape **E04**. Ce mode est utile lorsque par exemple aucune relation n'existe préalablement entre le serveur CSP et le serveur dCDN, ou lorsque le certificat de délégation en possession du serveur dCDN est ancien et doit être renouvelé. Dans ce mode, optionnellement, le terminal UA peut insérer une information reçue au préalable, tel que par exemple :

- une signature de l'URL de redirection insérée par le serveur uCDN, dont le but est de prouver au serveur dCDN que la requête reçue du terminal UA provient effectivement d'une redirection initiée par le serveur uCDN;
- un SessionTicket reçu du serveur CSP, dont le but est de permettre la reprise rapide d'une connexion TLS entre le terminal UA et le serveur CSP.

Dans un second mode de réalisation de l'invention, dit **mode asynchrone**, le serveur dCDN requiert périodiquement ce certificat de délégation, indépendamment de l'étape **E04**, afin d'être prêt à fournir à tout moment, sur demande d'un terminal tel que le terminal UA, une preuve de délégation récente. Dans ce mode asynchrone l'étape **G02** n'est pas déclenchée par l'étape **E04**, mais effectuée indépendamment du procédé de vérification d'une délégation selon l'invention, ou encore dans une requête

delegChallengeQuery('csp.com', options) effectuée préalablement par un autre terminal que le terminal UA.

Les étapes **G02**, **F03**, **F04**, **F05** et **G03**, décrites ci-dessous décrivent le procédé de production d'un certificat de délégation et sont similaires en mode synchrone ou asynchrone.

Lors de l'étape G02, le serveur dCDN se connecte au server CSP via une connexion sécurisé de type TLS où les 2 entités s'authentifient mutuellement par exemple en échangeant des certificats X.509. Le serveur dCDN insère, dans un message qu'il émet vers le serveur CSP, la demande de certificat de délégation DCQ('csp.com', options) reçue du terminal dans le message TLS ClientHello(). Optionnellement la demande de délégation peut être transmise à l'aide d'un protocole applicatif tel que http (notamment en mode API REST), smtp ou ldap.

Lors d'une étape **F03**, le serveur CSP reçoit du serveur dCDN le message émis lors de l'étape **G02**. Il est à noter que le serveur recevant ce message peut être un serveur du domaine 'csp.com' différent de celui ayant reçu lors de l'étape F01 la requête de contenu de la part du terminal UA. Par simplicité ces deux serveurs, qui sont du même domaine 'csp.com' et peuvent être confondus en un seul serveur, sont appelé tous les deux "serveur CSP".

Ce message comprend une requête de certificat de délégation telle que

"DCQ('csp.com', options)",

comprenant par exemple :

- 'csp.com' est le nom du domaine délégant, fourni par le terminal UA;
- "options" comprend un enregistrement OCSP du certificat X.509 de dCDN obtenu préalablement par le serveur dCDN auprès d'une autorité de certification, noté "dCDN_OCSP_Stapling"

Optionnellement le serveur CSP peut obtenir directement de l'entête TLS l'enregistrement dCDN_OCSP_Stapling, ou l'obtenir en interrogeant l'autorité de certification qui a produit le certificat X.509 du domaine 'dCDN.com'.

Lors d'une étape **F04**, le serveur CSP analyse la demande de certificat de délégation reçue.

Optionnellement, en mode synchrone, au cas où la délégation est multiple, la demande de certificat de délégation comprend en outre un champ 'URL Signing' ajouté par uCDN préalablement à l'étape **E02**, et que le terminal UA a transmis au serveur dCDN lors de l'étape **E04**. Ainsi, le serveur CSP peut vérifier que le serveur uCDN a effectivement délégué la livraison du contenu à un autre serveur de livraison.

Optionnellement, en mode synchrone, au cas où un champ SessionTicket est compris dans la requête DCQ, le serveur CSP peut alors vérifier l'authenticité de la requête de certificat de délégation, afin d'identifier qu'elle provient d'un terminal UA connu préalablement, ou mesurer le temps de redirection quand la délégation est multiple, afin de déterminer si la livraison de contenu par le serveur dCDN satisfait une exigence de performance minimale.

Optionnellement, en mode synchrone, la demande de certificat de délégation comprend en outre une adresse IP du terminal UA obtenue par le serveur dCDN lors de l'étape **G01.** L'adresse IP du serveur dCDN étant visible du serveur CSP, le serveur CSP est ainsi en mesure de déterminer les localisations géographiques respectives du terminal UA et du serveur dCDN, et d'estimer la qualité de service résultant de la diffusion du contenu MMContent du serveur dCDN vers le terminal UA. Si cette qualité est jugée insuffisante par le serveur CSP, il peut décider de ne pas attribuer de délégation au serveur dCDN.

Lors d'une étape **F05**, le serveur CSP émet vers le serveur dCDN une réponse de certificat de délégation à la demande émise lors de l'étape **G02**, que le serveur dCDN reçoit lors de l'étape **G03**. Ce message de réponse prend la forme d'une réponse utilisant le même protocole que la requête :

"DCA(deleg_CSP_dCDN)".

Si le serveur CSP, lors de l'étape d'analyse **F04**, a décidé d'autoriser la délégation de la livraison du contenu au serveur dCDN, le message de réponse comprend le certificat de délégation signé par le serveur CSP :

- "dCDN_OCSP_Stapling": l'enregistrement récent OCSP du certificat X.509 du serveur dCDN ;
- "CSP_OCSP_Stapling": un enregistrement récent OCSP du certificat X.509 du

serveur CSP obtenu préalablement par le serveur CSP auprès d'une autorité de certification;

- une signature par le serveur CSP du certificat de délégation: CSP calcule une empreinte des deux enregistrements "dCDN_OCSP_Stapling" et "CSP_OCSP_Stapling" à l'aide d'une fonction de hashage (SHA256), qu'il signe à l'aide de la clé privée de son certificat X.509 .

Ces trois éléments constituent ce qui est appelé le certificat de délégation.

Si dans le cas contraire, pour une raison ou une autre, le serveur CSP a décidé lors de l'étape d'analyse **F04** de refuser d'attribuer une délégation au serveur dCDN, le message de réponse peut être vide, ou comprendre un jeton correspondant à un refus de délégation, signé à l'aide de la clé privée du certificat X.509 de 'csp.com'.

Dans une variante avantageuse, le message de réponse peut, dans le cas d'un refus de délégation, comprendre un lien vers un site ou un serveur alternatif, auquel le serveur CSP fait confiance, et vers lequel le terminal UA peut se diriger. Ce serveur alternatif peut être par exemple un serveur plus adapté au type de terminal, dans le cas où le protocole utilisé en le terminal UA et le serveur dCDN est le protocole QUIC (le serveur dCDN ajoute alors le champ UAID du CHO, équivalent QUIC au message TLS ClientHello, dans la requête DCQuery). Dans ce cas le message de réponse est un type de redirection HTTPS contenant une URL, ce qui présente l'avantage de constituer une solution de remplacement à une annulation complète de la livraison par le serveur dCDN du contenu demandé.

Lors d'une étape **G04**, le serveur dCDN répond à la demande de certificat de délégation que le terminal UA a émise lors de l'étape **E04**. Ce message de réponse peut être par exemple un message selon une modification du protocole TLS, tel que :

"TLS ServerHello (DCA(deleg_CSP_dCDN))",

ou "TLS ServerHello (DCA(PoD))".

Ce message comprend la réponse à la requête de certificat de délégation, signée par le serveur CSP, que le serveur dCDN a reçue lors de l'étape **G03**.

Le terminal UA reçoit ce message lors d'une étape **E05**. Lors d'une étape **E06**, le terminal UA vérifie la signature du certificat de délégation : il déchiffre l'empreinte à

l'aide de la clé publique du certificat X.509 de 'csp.com' reçue lors de l'étape **E02**, et calcule une empreinte à l'aide de la même fonction de hachage que celle utilisée par le signataire, et vérifie que l'empreinte déchiffrée et l'empreinte calculée sont bien identiques.

Si le certificat de délégation est authentique, lors d'une étape **E07**, le terminal UA finalise l'établissement du tunnel TLS avec le serveur dCDN, ce qui permet la livraison du contenu MMContent du serveur dCDN au terminal UA.

Si le certificat de délégation n'est pas valable, lors d'une étape **E08**, le terminal UA ferme le tunnel TLS avec le serveur dCDN, et le contenu MMContent n'est pas livré au terminal UA.

Dans une variante avantageuse, si la signature du certificat de délégation est authentique et que le message de réponse contient une instruction de redirection vers un site ou un serveur alternatif, alors, lors d'une étape **E09**, le terminal UA ferme le tunnel TLS avec le serveur dCDN, et émet une requête adaptée afin qu'il soit dirigé vers le site ou le serveur alternatif.

La **figure 3** présente un exemple de structure de dispositif de vérification d'un certificat de délégation 300, permettant la mise en œuvre d'un procédé de vérification d'un certificat de délégation selon l'un quelconque des modes de réalisation décrits ci-dessus en relation avec la figure 2.

Le dispositif de validation 300 comprend une mémoire vive 303 (par exemple une mémoire RAM), une unité de traitement 302, équipée par exemple d'un processeur, et pilotée par un programme d'ordinateur stocké dans une mémoire morte 301 (par exemple une mémoire ROM ou un disque dur). A l'initialisation, les instructions de code du programme d'ordinateur sont par exemple chargées dans la mémoire vive 303 avant d'être exécutées par le processeur de l'unité de traitement 302.

La figure 3 illustre seulement un mode particulier de réalisation, parmi plusieurs modes particuliers de réalisation possibles, du procédé de vérification d'un certificat de délégation détaillé ci-dessus, en relation avec la figure 2. En effet, la technique de l'invention se réalise indifféremment sur une machine de calcul reprogrammable (un

ordinateur PC, un processeur DSP ou un microcontrôleur) exécutant un programme comprenant une séquence d'instructions, ou sur une machine de calcul dédiée (par exemple un ensemble de portes logiques comme un FPGA ou un ASIC, ou tout autre module matériel).

Dans le cas où l'invention est implantée sur une machine de calcul reprogrammable, le programme correspondant (c'est-à-dire la séquence d'instructions) pourra être stocké dans un médium de stockage amovible ou non, ce médium de stockage étant lisible partiellement ou totalement par un ordinateur ou un processeur.

Le dispositif de validation comprend également un module de communication (COM) adapté pour émettre des messages de requête de contenu, et des demandes d'établissement de connexion, et pour recevoir des messages de redirection, et des messages de certification.

Selon un mode particulier de réalisation de l'invention, l'unité de traitement comprend un module logiciel de navigation Internet ("browser" en anglais) ou client HTTP adapté à mettre en œuvre le procédé de vérification d'un certificat de délégation selon l'un quelconque des modes particuliers décrits précédemment.

Selon un mode de réalisation, un tel dispositif de vérification d'un certificat de délégation est compris dans un terminal client.

La **figure 4** présente un exemple de structure de dispositif de production d'un certificat de délégation 400, permettant la mise en œuvre d'un procédé de production d'un certificat de délégation selon l'un quelconque des modes de réalisation décrit ci-dessus en relation avec la figure 2.

Le dispositif de production d'un certificat de délégation 400 comprend une mémoire vive 403 (par exemple une mémoire RAM), une unité de traitement 402, équipée par exemple d'un processeur, et pilotée par un programme d'ordinateur stocké dans une mémoire morte 401 (par exemple une mémoire ROM ou un disque dur). A l'initialisation, les instructions de code du programme d'ordinateur sont par exemple chargées dans la mémoire vive 403 avant d'être exécutées par le processeur de l'unité de traitement 402.

La figure 4 illustre seulement une manière particulière, parmi plusieurs possibles, de mise en œuvre le procédé de production d'un certificat de délégation détaillé ci-dessus, en relation avec la figure 2. En effet, la technique de l'invention se réalise indifféremment sur une machine de calcul reprogrammable (un ordinateur PC, un processeur DSP ou un microcontrôleur) exécutant un programme comprenant une séquence d'instructions, ou sur une machine de calcul dédiée (par exemple un ensemble de portes logiques comme un FPGA ou un ASIC, ou tout autre module matériel).

Dans le cas où l'invention est implantée sur une machine de calcul reprogrammable, le programme correspondant (c'est-à-dire la séquence d'instructions) pourra être stocké dans un médium de stockage amovible ou non, ce médium de stockage étant lisible partiellement ou totalement par un ordinateur ou un processeur.

Le dispositif de production d'un certificat de délégation comprend également un module de communication (COM') adapté pour émettre des messages de réponse de certificat de délégation, et des messages de redirection, et pour recevoir des messages de requête de contenu, et des messages de demande d'un certificat de délégation.

Dans un mode de réalisation, un tel dispositif de production d'un certificat de délégation est compris dans un serveur, par exemple un serveur d'un fournisseur de contenu apte à référencer ledit contenu.

La **figure 5** présente un exemple de structure de dispositif de demande d'un certificat de délégation 500, permettant la mise en œuvre d'un procédé de demande d'un certificat de délégation selon l'un quelconque des modes de réalisation décrit ci-dessus en relation avec la figure 2.

Le dispositif de production d'un certificat de délégation 500 comprend une mémoire vive 503 (par exemple une mémoire RAM), une unité de traitement 502, équipée par exemple d'un processeur, et pilotée par un programme d'ordinateur stocké dans une mémoire morte 501 (par exemple une mémoire ROM ou un disque dur). A l'initialisation, les instructions de code du programme d'ordinateur sont par exemple

chargées dans la mémoire vive 503 avant d'être exécutées par le processeur de l'unité de traitement 502.

La figure 5 illustre seulement une manière particulière, parmi plusieurs possibles, de mise en œuvre le procédé de demande d'un certificat de délégation détaillé ci-dessus, en relation avec la figure 2. En effet, la technique de l'invention se réalise indifféremment sur une machine de calcul reprogrammable (un ordinateur PC, un processeur DSP ou un microcontrôleur) exécutant un programme comprenant une séquence d'instructions, ou sur une machine de calcul dédiée (par exemple un ensemble de portes logiques comme un FPGA ou un ASIC, ou tout autre module matériel).

Dans le cas où l'invention est implantée sur une machine de calcul reprogrammable, le programme correspondant (c'est-à-dire la séquence d'instructions) pourra être stocké dans un médium de stockage amovible ou non, ce médium de stockage étant lisible partiellement ou totalement par un ordinateur ou un processeur.

Le dispositif de demande d'un certificat de délégation comprend également un module de communication (COM") adapté pour émettre des messages de demande d'un certificat de délégation, et des messages de certification, et pour recevoir des messages de réponse de certificat de délégation, et des demandes d'établissement d'une connexion.

Dans un mode de réalisation, un tel dispositif de demande d'un certificat de délégation est compris dans un serveur de diffusion de contenu, par exemple un serveur de cache apte à diffuser du contenu.

REVENDICATIONS

1. Procédé de vérification d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA),

le procédé comprenant les étapes suivantes **mises en œuvre par le terminal** :

- émission (E01) d'un premier message de requête du contenu, à destination du premier serveur, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- réception (E02) d'un message de redirection, comprenant au moins un identifiant d'un serveur tiers (dCDN, uCDN),
- obtention (E03) d'une adresse du second serveur, à partir de l'au moins un identifiant reçu dans le message de redirection,
- émission (E04) d'une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur,

le procédé étant **caractérisé** en ce qu'il comprend en outre les étapes suivantes :

- réception (E05) d'un message de certification en provenance du second serveur, comprenant un certificat de délégation signé par le premier serveur, au travers de la seconde connexion chiffrée,
- vérification (E06) du certificat de délégation à l'aide de la clé de chiffrement associée au premier serveur,
- émission (E07) d'un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

2. Procédé de vérification selon la revendication 1, où l'étape d'obtention d'une adresse du second serveur comprend une étape de sélection de l'adresse parmi les identifiants de serveurs tiers, et/ou une étape d'interrogation d'un serveur de résolution

d'adresse avec un identifiant.

3. Procédé de vérification selon l'une des revendications précédentes, comprenant en outre une étape d'émission (E07) d'un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

4. Procédé de vérification selon l'une des revendications précédentes, où le message de certification comprend en outre une instruction de redirection et où le procédé comprend en outre une étape de redirection (E09) du terminal vers un troisième serveur.

5. Procédé de production d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA),

le procédé comprenant les étapes suivantes **mises en œuvre par le premier serveur**:

- réception (F01) d'un message de requête du contenu, en provenance du terminal, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- émission (F02) d'un message de redirection à destination du terminal, comprenant au moins un identifiant d'un serveur tiers (dCDN, uCDN),

le procédé étant **caractérisé** en ce qu'il comprend en outre les étapes suivantes :

- réception (F03) d'un message de demande d'un certificat de délégation, en provenance d'un second serveur, comprenant un certificat d'authenticité du second serveur,
- analyse (F04) de la demande d'un certificat de délégation,
- en fonction du résultat de l'analyse, émission (F05) d'un message de réponse de certificat de délégation, à destination du second serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide de la clé de

chiffrement.

6. Procédé de production selon la revendication précédente, où le message de demande d'un certificat de délégation comprend en outre une adresse du terminal client (UA).

7. Procédé de production selon l'un des revendications 5 à 6, où le message de demande d'un certificat de délégation comprend en outre une signature du serveur tiers (uCDN).

8. Procédé de production selon l'une des revendications 5 à 7, où le message de réponse de certificat de délégation comprend en outre une instruction de redirection pour le terminal client.

9. Dispositif de vérification d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA), le dispositif comprenant une machine de calcul reprogrammable (302) ou une machine de calcul dédiée, apte à et configurée pour :

- émettre un premier message de requête du contenu, à destination du premier serveur, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- recevoir un message de redirection, comprenant au moins un identifiant d'un serveur tiers (dCDN, uCDN),
- obtenir une adresse du second serveur, à partir de l'au moins un identifiant reçu dans le message de redirection,
- émettre une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur,

le dispositif étant **caractérisé** en ce que ladite machine de calcul reprogrammable (302)

ou ladite machine de calcul dédiée, est en outre apte à et configurée pour :

- recevoir un message de certification en provenance du second serveur, comprenant un certificat de délégation signé par le premier serveur, au travers de la seconde connexion chiffrée,
- vérifier le certificat de délégation à l'aide de la clé de chiffrement associée au premier serveur,
- émettre un second message de requête du contenu, à destination du second serveur, au travers de la seconde connexion chiffrée, si le certificat de délégation vérifié est valable.

10. Dispositif de production d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA), le dispositif comprenant une machine de calcul reprogrammable (402) ou une machine de calcul dédiée, apte à et configurée pour :

- recevoir un message de requête du contenu, en provenance du terminal, au travers d'une première connexion chiffrée entre le terminal et le premier serveur, au moyen de laquelle le terminal a préalablement obtenu une clé de chiffrement associée au premier serveur,
- émettre un message de redirection à destination du terminal, comprenant au moins un identifiant d'un serveur tiers (dCDN, uCDN),

le dispositif étant **caractérisé** en ce que ladite machine de calcul reprogrammable (402) ou ladite machine de calcul dédiée, est en outre apte à et configurée pour :

- recevoir un message de demande d'un certificat de délégation, en provenance d'un second serveur, comprenant un certificat d'authenticité du second serveur,
- analyser la demande d'un certificat de délégation,
- en fonction du résultat de l'analyse, émettre un message de réponse de certificat de délégation, à destination du second serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide de la clé de chiffrement.

11. Système de vérification d'un certificat de délégation comprenant un dispositif conforme à la revendication 9, un dispositif conforme à la revendication 10 et un dispositif de demande d'un certificat de délégation, la délégation étant d'un premier serveur (CSP) à un second serveur (dCDN), pour une livraison d'un contenu référencé sur le premier serveur, et destiné à un terminal client (UA), le dispositif de demande comprenant une machine de calcul reprogrammable (502) ou une machine de calcul dédiée, apte à et configurée pour :

- recevoir une demande d'établissement d'une seconde connexion chiffrée entre le terminal et le second serveur, comprenant un identifiant du premier serveur,

le système étant en outre **caractérisé** en ce que ladite machine de calcul reprogrammable (502) ou ladite machine de calcul dédiée, est en outre apte à et configurée pour :

- émettre un message de demande d'un certificat de délégation, à destination du premier serveur, comprenant un certificat d'authenticité du second serveur,
- recevoir un message de réponse de certificat de délégation, en provenance du premier serveur, comprenant un certificat de délégation signé par le premier serveur, vérifiable à l'aide d'une clé de chiffrement associée au premier serveur,
- émettre un message de certification à destination du terminal, comprenant le certificat de délégation, au travers de la seconde connexion chiffrée, le terminal ayant préalablement obtenu une clé de chiffrement associée au premier serveur, au moyen d'une première connexion chiffrée entre le terminal et le premier serveur.

12. Produit programme d'ordinateur, comprenant des instructions de code de programme pour la mise en œuvre du procédé de vérification d'un certificat de délégation selon l'une quelconque des revendications 1 à 4, lorsque ledit programme est exécuté sur un ordinateur.

13. Support d'enregistrement lisible par un terminal client (UA) sur lequel est enregistré le programme selon la revendication 12.

14. Produit programme d'ordinateur, comprenant des instructions de code de programme pour la mise en œuvre du procédé de production d'un certificat de délégation selon l'une quelconque des revendications 5 à 8, lorsque ledit programme est exécuté sur un ordinateur.

15. Support d'enregistrement lisible par un serveur de contenu (CSP) sur lequel est enregistré le programme selon la revendication 14.

Fig 1

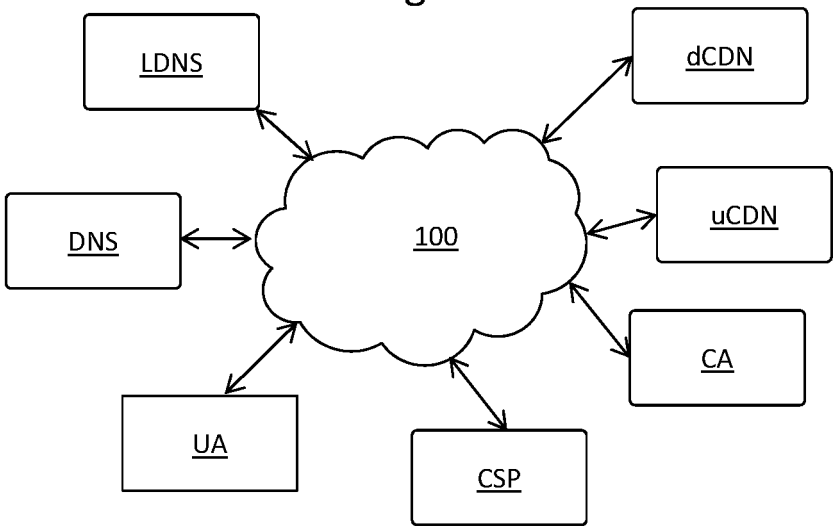


Fig 3

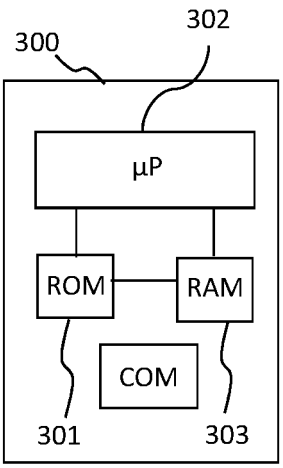


Fig 4

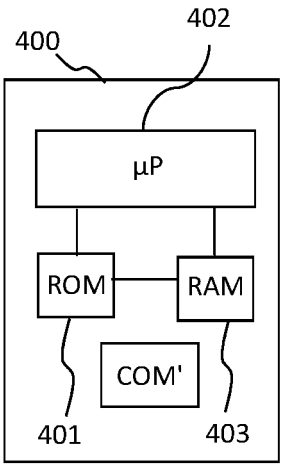


Fig 5

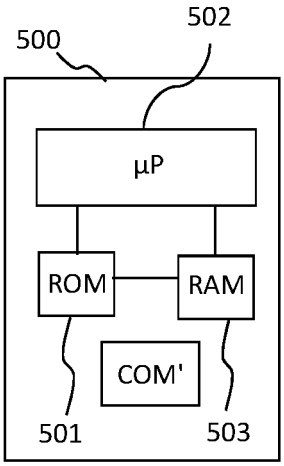
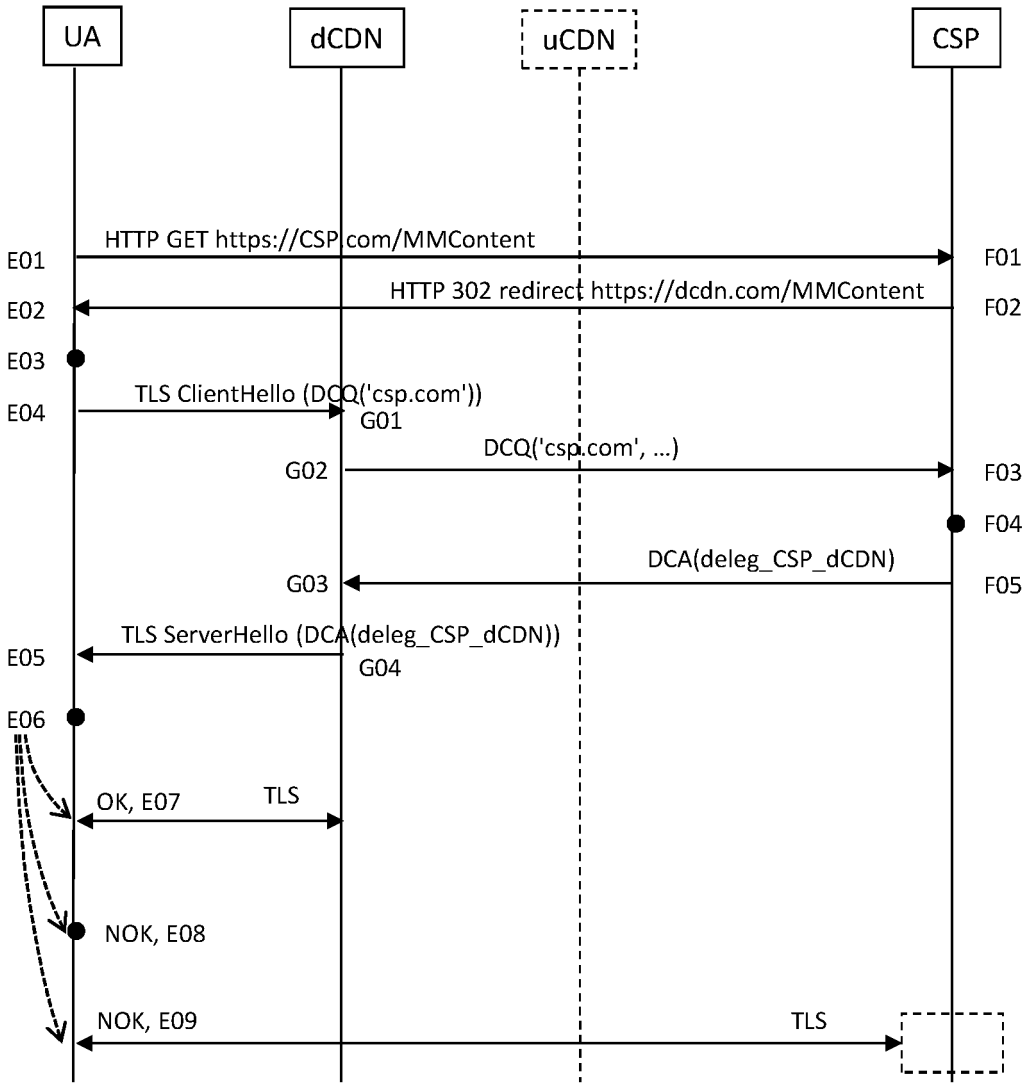


Fig 2


UA
dCDN
uCDN
CSP
HTTP GET https://CSP.com/MMContent
E01
F01
HTTP 302 redirect https://dcdn.com/MMContent
E02
F02
E03
TLS ClientHello (DCQ('csp.com'))
E04
G01
DCQ('csp.com', ...)
G02
F03
F04
DCA(deleg_CSP_dCDN)
G03
F05
TLS ServerHello (DCA(deleg_CSP_dCDN))
E05
G04
E06
OK, E07
TLS
NOK, E08
NOK, E09
TLS

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 837909
FR 1750326

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	LIANG JINJIN ET AL: "When HTTPS Meets CDN: A Case of Authentication in Delegated Service", 2014 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, IEEE, 18 mai 2014 (2014-05-18), pages 67-82, XP032686141, ISSN: 1081-6011, DOI: 10.1109/SP.2014.12 [extrait le 2014-11-13] * pages 73,76,77; figures 1-7 *	1-15	H04N21/23 H04L9/00 H04L29/06
X	US 2003/014503 A1 (LEGOUT ARNAUD [FR] ET AL) 16 janvier 2003 (2003-01-16) * alinéas [0117] - [0122] *	1-15	
X	KIM H ET AL: "A robust and flexible digital rights management system for home networks", JOURNAL OF SYSTEMS & SOFTWARE, ELSEVIER NORTH HOLLAND, NEW YORK, NY, US, vol. 83, no. 12, 1 décembre 2010 (2010-12-01), pages 2431-2440, XP027449644, ISSN: 0164-1212, DOI: 10.1016/J.JSS.2010.04.064 [extrait le 2010-06-15] * pages 3-5 *	1-15	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04N

Date d'achèvement de la recherche	Examinateur
9 octobre 2017	Folea, Octavian

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 1750326 FA 837909

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 09-10-2017
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 2003014503 A1	16-01-2003	AT 241820 T	15-06-2003
		DE 60100317 D1	03-07-2003
		DE 60100317 T2	29-04-2004
		EP 1278112 A1	22-01-2003
		JP 2003122724 A	25-04-2003
		US 2003014503 A1	16-01-2003

EPO FORM P0465