

⑤④ SECURISATION DE L'ACCES A UN SERVICE.

②② Date de dépôt : 04.10.17.

③③ Priorité :

④③ Date de mise à la disposition du public
de la demande : 05.04.19 Bulletin 19/14.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 25.10.19 Bulletin 19/43.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑥① Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦① Demandeur(s) : *OBERTHUR TECHNOLOGIES
Société anonyme —FR et AIRTAG Société anonyme
— FR.*

⑦② Inventeur(s) : DOTTAX EMMANUELLE, SOUMAH
CHRISTOPHE et PORTERET CYRIL.

⑦③ Titulaire(s) : OBERTHUR TECHNOLOGIES Société
anonyme, AIRTAG Société anonyme.

⑦④ Mandataire(s) : CABINET BEAU DE LOMENIE.



5

Arrière-plan de l'invention

10 La présente invention concerne le contrôle d'accès à un service et porte plus particulièrement sur la gestion de l'accès d'utilisateurs à un service à l'aide de clés cryptographiques.

Les services d'authentification et de sécurité visant à contrôler l'accès à de
quelconques services, au moyen par exemple d'une communication NFC ou autre, se
15 sont considérablement développés ces dernières années. Ces services se manifestent notamment dans de nombreuses applications de la vie courante telles que le contrôle des portes d'une maison ou d'un véhicule, le contrôle de portiques de sécurité, l'accès aux transports ou à des services Internet...

Il est par exemple possible aujourd'hui de contrôler l'accès à une voiture de sorte que
20 son utilisation (ouverture des portes, démarrage etc.) ne soit autorisée qu'au travers d'une clé électronique (ou clé numérique) détenue par le propriétaire du véhicule. De nombreuses fonctions, ou « services », peuvent être déclenchées à l'aide d'une telle clé, telles que le contrôle du démarrage du moteur, de la fonction GPS, de l'autoradio du véhicule etc.

25 Pour déclencher ces services, il est nécessaire de posséder les droits d'accès (ou droits d'utilisation) appropriés. Typiquement, le propriétaire d'un véhicule utilise un dispositif portable, un téléphone portable par exemple, sur lequel est hébergée une application dédiée qui communique avec le fournisseur de services correspondant (i.e. le véhicule, dans le cas présent). Ce dispositif de contrôle permet au propriétaire de
30 s'identifier auprès du fournisseur de services et de requérir l'accès à des services conformément aux droits d'accès dont il dispose.

Dans le cas du contrôle d'accès à un véhicule, par exemple, les droits d'accès sont typiquement attribués en premier lieu au propriétaire. Les tiers ne sont généralement pas en mesure d'obtenir librement les droits d'accès à un service, en particulier si celui-ci est
35 payant ou privatif. Le propriétaire d'une voiture peut toutefois souhaiter prêter certains de ses droits d'accès à un tiers de confiance afin que celui-ci en bénéficie également.

Le document FR 2 989 799 décrit par exemple une méthode permettant au titulaire de droits d'accès à un service de déléguer tout ou partie de ses droits à un tiers. Cette

délégation prend la forme d'un prêt de certains droits à un tiers. Pour ce faire, le titulaire transmet au tiers des données signées à l'aide de sa clé privée cryptographique. Ces données signées peuvent ensuite être utilisées par le tiers pour accéder de façon sécurisée au service concerné.

- 5 Il est souhaitable d'améliorer encore d'avantage la sécurisation de l'accès à des services, afin notamment d'éviter tous accès ou usages non autorisés dudit service.

Objet et résumé de l'invention

10 A cet effet, la présente invention concerne un procédé de contrôle, mis en œuvre par un système de contrôle, pour contrôler l'accès à un service, le procédé comprenant les étapes suivantes :

- envoi d'une première donnée de défi à un premier terminal ;
- réception, en réponse audit envoi, d'un premier code MAC généré par le premier terminal accompagné d'un identifiant (ID1) du premier terminal et de premiers
- 15 droits d'accès pour accéder au service ;
- dérivation d'une première clé mère cryptographique à partir d'une clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;
- dérivation d'une première clé temporaire cryptographique à partir de la première
- 20 clé mère cryptographique ;
- génération d'un deuxième code MAC à partir de la première clé temporaire cryptographique, des premiers droits d'accès et de la première donnée de défi ;
- et
- gestion de l'accès du premier terminal au service à partir d'une comparaison des
- 25 premier et deuxième codes MAC.

La présente invention permet ainsi de sécuriser l'accès d'un service en fournissant à des utilisateurs une ou des clés temporaires cryptographiques pour bénéficier de certains droits d'accès. Ces clés temporaires sont issues d'une clé maîtresse cryptographique au travers d'une double dérivation de clé. L'usage de clés temporaires cryptographiques est

30 avantageux en ce que celles-ci peuvent être renouvelées régulièrement, rendant ainsi plus difficile tous accès illicites à un service donné. En effet, un tiers malveillant ne disposera que d'un temps restreint pour obtenir l'accès au service pendant qu'une clé temporaire est en cours de validité, réduisant ainsi les risques de fraudes. Chaque changement de clé temporaire rend plus difficile l'accès frauduleux à un service.

35 De manière avantageuse, on peut définir la période de validité d'une clé temporaire de sorte à ce qu'une tentative d'accès frauduleuse ait peu de chance d'aboutir avant expiration de la clé temporaire en cours de validité.

L'invention permet aussi de faciliter la révocation des droits d'accès susceptibles d'avoir été attribués à un utilisateur.

Selon un mode de réalisation particulier, au cours de l'étape de gestion d'accès, le système de contrôle autorise l'accès du premier terminal au service selon les premiers
5 droits d'accès seulement s'il est déterminé lors de ladite comparaison que les premier et deuxième codes MAC coïncident.

Selon un mode de réalisation particulier, la première clé temporaire cryptographique est dérivée de sorte qu'elle ne soit considérée comme valide par le système de contrôle que pour une période de temps prédéfinie.

10 Selon un mode de réalisation particulier, le procédé de contrôle comprend, préalablement à l'envoi de la première donnée de défi, un enrôlement comprenant les étapes suivantes :

- réception, en provenance du premier terminal, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ;
- 15 - dérivation de la première clé mère cryptographique à partir de la clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ; et
- envoi, au premier terminal, de la première clé mère cryptographique de sorte à permettre au premier terminal d'accéder au service selon les premiers droits si
20 les premier et deuxième codes MAC coïncident.

Selon un mode de réalisation particulier, le procédé de contrôle comprend :

- réception en provenance du premier terminal, en réponse à l'envoi de la première donnée de défi, d'une donnée de dérivation, d'une donnée temporelle indiquant la validité dans le temps du premier code MAC reçu, et d'une donnée
25 d'authentification du premier code MAC reçu ;
- génération d'un code MAC additionnel à partir d'une clé mère cryptographique dérivée de la clé maîtresse cryptographique et à partir de la donnée de dérivation et de la donnée temporelle ;
- vérification que le code MAC additionnel coïncide avec la donnée
30 d'authentification reçue ; et
- dans l'affirmative, détermination de la première clé temporaire cryptographique par dérivation à partir de la première clé mère cryptographique et de la donnée de dérivation.

Selon un mode de réalisation particulier, le procédé de contrôle comprend,
35 préalablement à l'envoi de la première donnée de défi, un enrôlement comprenant les étapes suivantes :

- réception, en provenance du premier terminal, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ;

- dérivation de la première clé mère cryptographique à partir de la clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;
- dérivation de la clé première temporaire cryptographique à partir de la première clé mère cryptographique et de la donnée de dérivation ;
- détermination de la donnée d'authentification en calculant un code MAC à partir d'une clé mère cryptographique dérivée de la clé maîtresse cryptographique et à partir de la donnée de dérivation et de la donnée temporelle ;
- envoi, au premier terminal, de la première clé temporaire cryptographique et de la donnée d'authentification de sorte à permettre au premier terminal d'accéder au service selon les premiers droits d'accès si les premier et deuxième codes MAC coïncident.

Selon un mode de réalisation particulier, la première clé temporaire cryptographique est dérivée à partir de la première clé mère cryptographique et d'une donnée temporelle.

Selon un mode de réalisation particulier, la donnée temporelle est une donnée déterminée à partir d'un point courant dans le temps, la donnée temporelle définissant une durée de temps pendant laquelle la première clé temporaire cryptographique est valide.

Selon un mode de réalisation particulier, le procédé de contrôle comprend, préalablement à l'envoi de la première donnée de défi, un enrôlement comprenant les étapes suivantes :

- réception, en provenance du premier terminal, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ;
- dérivation de la première clé mère cryptographique à partir de la clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;
- dérivation de la première clé temporaire cryptographique à partir de la première clé mère cryptographique et d'une donnée temporelle ;
- envoi, au premier terminal, de la première clé temporaire cryptographique de sorte à permettre au premier terminal d'accéder au service selon les premiers droits si les premier et deuxième codes MAC coïncident.

Selon un mode de réalisation particulier, la première clé temporaire cryptographique est déterminée par dérivation à partir de la première clé mère cryptographique, de la donnée temporelle et d'une donnée de dérivation correspondant à ladite première clé temporaire cryptographique parmi une pluralité de clés temporaires cryptographique susceptibles d'être obtenues par dérivation à partir de la première clé mère cryptographique et de ladite donnée temporelle ;

ladite donnée de dérivation étant reçue du premier terminal en réponse de l'envoi de la première donnée de défi.

Selon un mode de réalisation particulier, le procédé de contrôle comprend, préalablement à l'envoi de la première donnée de défi, un enrôlement comprenant les

5 étapes suivantes :

- réception, en provenance du premier terminal, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ;
- dérivation de la première clé mère cryptographique à partir de la clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits
- 10 d'accès ;
- dérivation de la première clé temporaire cryptographique à partir de la première clé mère cryptographique, de la donnée temporelle et de la donnée dérivation ; et
- envoi, au premier terminal, de la première clé temporaire cryptographique de
- 15 sorte à permettre au premier terminal d'accéder au service selon les premiers droits si les premier et deuxième codes MAC coïncident.

Dans un mode particulier de réalisation, les différentes étapes du procédé de contrôle sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi au moins un programme d'ordinateur sur un

20 support d'informations correspondant, chaque programme étant susceptible d'être mis en œuvre dans un dispositif tel qu'un ordinateur, ou plus généralement dans un système de contrôle, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de contrôle tel que défini ci-dessus.

L'invention vise aussi un support d'enregistrement (ou support d'informations) lisible

25 par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

L'invention concerne également un procédé de traitement, mis en œuvre par un premier terminal, pour accéder à un service dont l'accès est contrôlé par un système de

contrôle, comprenant :

- réception d'une donnée de défi en provenance du système de contrôle ;
- génération d'un premier code MAC à partir de la donnée de défi et de premiers droits d'accès au service et à partir d'une première clé temporaire cryptographique dérivée de la première clé mère cryptographique ; et
- envoi, au système de contrôle, du premier code MAC accompagné d'un
- 30 identifiant du premier terminal et des premiers droits d'accès, de sorte à
- 35 permettre au système de contrôle de contrôler si le premier terminal est autorisé à accéder au service selon les premiers droits d'accès.

Selon un mode de réalisation particulier, le procédé de traitement comprend, en réponse à l'envoi du premier code MAC, la réception d'une réponse du système de contrôle indiquant si le premier terminal T1 est autorisé à accéder au service selon les premiers droits d'accès.

5 Selon un mode de réalisation particulier, le procédé de traitement comprend, préalablement à la génération du premier code MAC, un enrôlement comprenant :

- envoi, au système de contrôle, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ; et
- réception, en provenance du système de contrôle, de la première clé mère cryptographique dérivée à partir d'une clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ; et
- dérivation de la première clé temporaire cryptographique à partir de la première clé mère cryptographique.

10 Selon un mode de réalisation particulier, le procédé de traitement comprend, préalablement à la génération du premier code MAC :

- détermination d'une donnée temporelle et d'une donnée de dérivation, la donnée temporelle étant représentative de la validité dans le temps du premier code MAC ;
- détermination d'une donnée d'authentification du premier code MAC en calculant un code MAC à partir d'une clé mère cryptographique dérivée de la clé maîtresse cryptographique et à partir de la donnée de dérivation et de la donnée temporelle ;

la première clé temporaire cryptographique étant dérivée à partir de la première clé mère cryptographique et de la donnée de dérivation ; et

25 - envoi au système de contrôle, en réponse à la donnée de défi, de la donnée temporelle, de la donnée de dérivation et de la donnée d'authentification.

30 Selon un mode de réalisation particulier, le procédé de traitement comprend, préalablement à la génération du premier code MAC, la réception, en provenance du système de contrôle, d'une deuxième clé mère cryptographique, différente de la première clé mère cryptographique, dérivée à partir de la clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;

dans lequel la donnée d'authentification est déterminée en tant que code MAC à partir de la deuxième clé mère cryptographique, de la donnée de dérivation et de la donnée temporelle.

35 Selon un mode de réalisation particulier, le procédé de traitement comprend, préalablement à la génération du premier code MAC, la détermination d'une donnée temporelle ;

la première clé temporaire cryptographique étant dérivée à partir de la première clé mère cryptographique et de la donnée temporelle.

Selon un mode de réalisation particulier, la première clé temporaire cryptographique est déterminée par dérivation à partir de la première clé mère cryptographique, de la
5 première donnée temporelle et d'une donnée de dérivation correspondant à ladite première clé temporaire cryptographique parmi une pluralité de clés temporaires cryptographique susceptibles d'être obtenues par dérivation à partir de la première clé mère cryptographique et de la première donnée temporelle,

le procédé comprenant un envoi de la donnée de dérivation au système de contrôle
10 en réponse à la donnée de défi.

Selon un mode de réalisation particulier, le procédé de traitement comprend, préalablement à la génération du premier code MAC, un enrôlement comprenant :

- envoi, au système de contrôle, de l'identifiant du premier terminal et des premiers droits d'accès pour accéder au service ; et
- 15 - réception, en provenance du système de contrôle, de la première clé temporaire cryptographique.

Selon un mode de réalisation particulier, lors dudit enrôlement, le premier terminal reçoit une pluralité de clés temporaires cryptographiques,

le procédé comprenant une étape de sélection, parmi les clés temporaires
20 cryptographiques reçues, d'une clé en tant que première clé temporaire cryptographique.

Dans un mode particulier de réalisation, les différentes étapes du procédé de traitement sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi au moins un programme d'ordinateur sur un support d'informations correspondant, chaque programme étant susceptible d'être mis en
25 œuvre dans un terminal ou un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de traitement tel que défini ci-dessus.

L'invention vise aussi un support d'enregistrement (ou support d'informations) lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que
30 mentionné ci-dessus.

A noter que les programmes mentionnés dans le présent exposé 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.

35 De plus, les supports d'enregistrement mentionnés ci-avant peuvent être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le 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.

5 D'autre part, les supports d'enregistrement peuvent correspondre à 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. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, les supports d'enregistrement peuvent correspondre à un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

10 L'invention vise également un système de contrôle pour contrôler l'accès à un service, le système de contrôle comprenant :

- un module de communication configuré pour envoyer une première donnée de défi à un premier terminal et pour recevoir, en réponse audit envoi, un premier code MAC généré par le premier terminal accompagné d'un identifiant du premier terminal et de premiers droits d'accès pour accéder au service ;
- 15 - un module de traitement configuré pour :
 - dériver une première clé mère cryptographique à partir d'une clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;
 - 20 ○ dériver une première clé temporaire cryptographique à partir de la première clé mère cryptographique ;
 - générer un deuxième code MAC à partir de la première clé temporaire cryptographique, des premiers droits d'accès et de la première donnée de défi ; et
 - 25 - un module de contrôle configuré pour gérer l'accès du premier terminal au service à partir d'une comparaison des premier et deuxième codes MAC.

L'invention vise également un terminal, dit premier terminal, pour accéder à un service dont l'accès est contrôlé par un système de contrôle, ledit premier terminal comprenant :

- 30 - un module de communication configuré pour recevoir une donnée de défi en provenance du système de contrôle ; et
- un module de traitement configuré pour :
 - générer un premier code MAC à partir de la donnée de défi et de premiers droits d'accès au service et à partir d'une première clé temporaire cryptographique dérivée de la première clé mère cryptographique ; et
 - 35 ○ envoyer, au système de contrôle, le premier code MAC accompagné d'un identifiant du premier terminal et des premiers droits d'accès, de sorte à

permettre au système de contrôle de contrôler si le premier terminal est autorisé à accéder au service selon les premiers droits d'accès.

Selon un mode de réalisation, l'invention est mise en œuvre au moyen de composants logiciels et/ou matériels. Dans cette optique, le terme « module » peut correspondre dans ce document aussi bien à un composant logiciel, qu'à un composant matériel ou à un ensemble de composants matériels et logiciels.

A noter que les différents modes de réalisation définis ci-avant en relation avec le procédé de contrôle, d'une part, et avec le procédé de traitement, d'autre part, ainsi que les avantages associés à ces procédés, s'appliquent par analogie au système de contrôle et au premier terminal tels que définis ci-avant.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent des exemples de réalisation dépourvus de tout caractère limitatif. Sur les figures:

- la figure 1 déjà décrite représente schématiquement un environnement comprenant un système de contrôle et un terminal selon un mode de réalisation particulier de l'invention ;
- la figure 2 représente schématiquement la structure d'un serveur compris dans le système de contrôle représenté en figure 1, selon un mode de réalisation particulier de l'invention ;
- la figure 3 représente schématiquement la structure d'un dispositif électronique compris dans le système de contrôle représenté en figure 1, selon un mode de réalisation particulier de l'invention ;
- la figure 4 représente schématiquement la structure d'un terminal de communication, selon un mode de réalisation particulier de l'invention ;
- la figure 5 représente, sous forme d'un diagramme, les étapes d'un procédé de contrôle et les étapes d'un procédé de traitement, selon un premier mode de réalisation de l'invention ;
- la figure 6 représente, sous forme d'un diagramme, une variante du premier mode de réalisation illustré en figure 5 ;
- la figure 7 représente, sous forme d'un diagramme, les étapes d'un procédé de contrôle et les étapes d'un procédé de traitement, selon un deuxième mode de réalisation de l'invention ;
- la figure 8 représente, sous forme d'un diagramme, une variante du deuxième mode de réalisation illustré en figure 7 ;

- la figure 9 représente, sous forme d'un diagramme, les étapes d'un procédé de contrôle et les étapes d'un procédé de traitement, selon un troisième mode de réalisation de l'invention ; et
- la figure 10 représente, sous forme d'un diagramme, une variante du troisième mode de réalisation illustré en figure 9.

Description détaillée de plusieurs modes de réalisation

Comme indiqué précédemment, le présent exposé concerne le contrôle de l'accès à des services par des utilisateurs. Divers modes de réalisation de l'invention sont à présent décrits ci-après.

Les modes de réalisation décrit ci-dessous s'inscrivent dans le cadre d'un contrôle d'accès à un véhicule tel qu'une voiture par exemple, et notamment pour l'accès à certaines fonctionnalités d'une telle voiture. On comprend toutefois que la présente invention s'applique plus généralement au contrôle d'accès à un quelconque service ou à diverses fonctionnalités d'un tel service. A titre d'exemple, le service géré dans le cadre de l'invention peut ainsi concerner le contrôle des portes d'une maison ou d'un véhicule, le contrôle de portiques de sécurité, l'accès à des transports ou encore l'accès à des services Internet. Le service concerné peut également prendre la forme d'un quelconque dispositif électronique ou électromécanique, telle qu'une télévision ou une console de jeux vidéo par exemple, dont l'accès ou le déclenchement de fonctionnalités est contrôlé grâce à l'invention.

L'invention propose d'améliorer le contrôle d'accès d'utilisateurs à un service donné, à savoir l'utilisation d'une voiture dans le cas présent. Pour ce faire, le principe de l'invention repose sur la génération de clés cryptographiques, et notamment de clés cryptographiques temporaires, par dérivation d'une clé cryptographique maîtresse de façon à permettre à des utilisateurs d'accéder au service considéré.

Plus particulièrement, l'invention, selon différents modes de réalisation, concerne un procédé de contrôle, mis en œuvre par un système de contrôle, pour contrôler l'accès à un service, le procédé comprenant les étapes suivantes :

- envoi d'une première donnée de défi à un premier terminal ;
- réception, en réponse audit envoi, d'un premier code MAC (pour « Code d'Authentification de Message ») généré par le premier terminal accompagné d'un identifiant du premier terminal et de premiers droits d'accès pour accéder au service ;
- dérivation d'une première clé mère cryptographique à partir d'une clé maîtresse cryptographique, de l'identifiant du premier terminal et des premiers droits d'accès ;

- dérivation d'une première clé temporaire cryptographique à partir de la première clé mère cryptographique ;
- génération d'un deuxième code MAC à partir de la première clé temporaire cryptographique, des premiers droits d'accès et de la première donnée de défi ;
- 5 et
- gestion de l'accès du premier terminal au service à partir d'une comparaison des premier et deuxième codes MAC.

L'invention concerne également le système de contrôle correspondant.

10 En outre, l'invention, selon différents modes de réalisation, concerne un procédé de traitement, mis en œuvre par un premier terminal, pour accéder à un service dont l'accès est contrôlé par un système de contrôle, comprenant :

- réception d'une donnée de défi en provenance du système de contrôle ;
- génération d'un premier code MAC à partir de la donnée de défi et de premiers droits d'accès au service et à partir d'une première clé temporaire
- 15 cryptographique dérivée de la première clé mère cryptographique ; et
- envoi, au système de contrôle, du premier code MAC accompagné d'un identifiant du premier terminal et des premiers droits d'accès, de sorte à permettre au système de contrôle de contrôler si le premier terminal est autorisé à accéder au service selon les premiers droits d'accès.

20 L'invention concerne également le premier terminal correspondant.

D'autres aspects et avantages de la présente invention ressortiront des exemples de réalisation décrits ci-dessous en référence aux dessins mentionnés ci-avant.

Sauf indications contraires, les éléments communs ou analogues à plusieurs figures portent les mêmes signes de référence et présentent des caractéristiques identiques ou

25 analogues, de sorte que ces éléments communs ne sont généralement pas à nouveau décrits par souci de simplicité.

La **figure 1** représente, de manière schématique, un environnement comprenant un système de contrôle SY, contrôlant l'accès à un service SR, et un terminal de communication T1. Comme déjà indiqué, le service SR correspond ici à une voiture dont

30 certaines fonctionnalités sont contrôlées par le système de contrôle SY. Le type du ou des fonctionnalités dont l'accès est contrôlé peut varier selon le cas.

Dans cet exemple, un utilisateur U1 utilise le terminal T1 pour accéder au service SR. Le terminal T1 peut être un quelconque terminal de communication, tel qu'un terminal mobile par exemple. On suppose ici que ce terminal T1 est un téléphone portable de type

35 smartphone.

Le système de contrôle SY comporte ici un dispositif électronique DP1 et un serveur DP2. Le dispositif DP1 est configuré pour gérer l'accès de l'utilisateur U1 au service SR. Le dispositif DP1 peut être disposé dans la voiture ou, alternativement, hors de la voiture, de

sorte à permettre le contrôle de certaines fonctionnalités de la voiture, telles que le contrôle du mécanisme d'ouverture des portes, le contrôle du démarrage du moteur, le contrôle de la fonction GPS ou encore de l'autoradio, etc. Le dispositif DP1 se présente par exemple sous la forme d'un boîtier électronique fixé ou non à la voiture SR. La structure du dispositif DP1, selon un exemple particulier, est décrite plus en détail ci-après en référence à la **figure 3**.

Par ailleurs, le serveur DP2 est configuré pour interagir avec l'utilisateur U1 afin de fournir notamment la ou les clés cryptographiques adéquates pour accéder au service SR. Dans l'exemple représenté en **figure 1**, le serveur SV2 et le dispositif DP1 sont deux équipements séparés. Selon une variante, le serveur DP2 et le dispositif DP1 forment un seul et même dispositif. La structure du serveur DP2, selon un exemple particulier, est décrite plus en détail ci-après en référence à la **figure 2**.

La **figure 2** représente schématiquement la structure du serveur DP2 conformément à un mode de réalisation particulier de l'invention.

Plus précisément, le serveur DP2 comprend dans cet exemple au moins un processeur 10, une première mémoire non volatile 12, une deuxième mémoire non volatile 14 et une interface de communication 16. Le serveur DP2 peut en outre comprendre d'autres éléments non représentés, tels qu'une mémoire volatile réinscriptible (RAM), qui sont bien connus de l'homme du métier.

La mémoire 12 est une mémoire non volatile réinscriptible ou une mémoire morte (ROM), cette mémoire constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le serveur DP2, et sur lequel est enregistré un programme d'ordinateur PG1 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG1 comporte des instructions pour l'exécution d'étapes d'un procédé de contrôle selon un mode de réalisation particulier, comme décrit ultérieurement.

Dans l'exemple envisagé ici, la mémoire 14 est une mémoire non volatile réinscriptible configuré pour stocker en particulier la clé maîtresse cryptographique CMK_0 dont l'usage sera décrit ultérieurement. Selon un exemple particulier de réalisation, la clé maîtresse cryptographique CMK_0, et toutes autres éventuelles clés cryptographiques, sont gérées par un HSM (pour « Hardware Security Module ») au niveau du serveur.

Le processeur 10 piloté par le programme d'ordinateur PG1, met ici en œuvre un module de communication MD2 et un module de traitement MD4.

Le module de communication MD2 est configuré pour assurer la communication avec l'extérieur et notamment le terminal utilisateur T1. Cette communication est réalisée ici en utilisant l'interface 16 qui peut être tout type d'interface de communication approprié (filaire ou sans fil) pour communiquer avec le terminal T1. Dans l'exemple considéré ici, ces communications sont assurées via Internet.

Le module de de traitement MD4 est configuré pour réaliser un certain nombre de traitements conformes à l'invention qui seront décrits ultérieurement dans différentes modes de réalisation. Dans cet exemple, le module de traitement MD4 est en particulier configuré pour déterminer une ou des clés cryptographiques dérivées de la clé maîtresse CMK_0. Selon un exemple particulier, le module de traitement MD4 est implémenté dans un HSM, comme déjà mentionné ci-dessus.

La **figure 3** représente schématiquement la structure du dispositif électronique DP1 conformément à un mode de réalisation particulier de l'invention.

Plus précisément, le dispositif DP1 comprend dans cet exemple au moins un processeur 20, une première mémoire non volatile 22, une deuxième mémoire non volatile 24 et une interface de communication 26. Le dispositif DP1 peut en outre comprendre d'autres éléments non représentés, tels qu'une mémoire volatile réinscriptible (RAM), qui sont bien connus de l'homme du métier.

La mémoire 22 est une mémoire non volatile réinscriptible ou une mémoire morte (ROM), cette mémoire constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le dispositif DP1, et sur lequel est enregistré un programme d'ordinateur PG2 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG2 comporte des instructions pour l'exécution d'étapes d'un procédé de contrôle selon un mode de réalisation particulier, comme décrit ultérieurement.

Dans l'exemple envisagé ici, la mémoire 24 est une mémoire non volatile réinscriptible configuré pour stocker en particulier la clé maîtresse cryptographique CMK_0 dont l'usage sera décrit ultérieurement. Cette mémoire 24 peut être située, par exemple, dans une partie sécurisée du processeur 20 ou dans un mémoire sécurisée distincte du processeur 20, tel que dans un élément sécurisé (ou « secure element »).

Le processeur 20 piloté par le programme d'ordinateur PG2, met ici en œuvre un certain nombre de modules, à savoir : un module de communication MD10, un module de traitement MD12 et un module de contrôle d'accès MD14.

Le module de communication MD10 est configuré pour assurer la communication avec l'extérieur et notamment le terminal utilisateur T1. Cette communication est réalisée ici en utilisant l'interface 26 qui peut être tout type d'interface de communication approprié (filaire ou sans fil) pour communiquer avec le terminal T1. Dans l'exemple considéré ici, ces communications sont des communications sans fil de type NFC, Bluetooth ou autre.

Le module de traitement MD12 est configuré pour réaliser un certain nombre de traitements qui seront décrits ultérieurement dans différents modes de réalisation. Dans cet exemple, le module de traitement MD12 est en particulier configuré pour vérifier si un code MAC transmis par le terminal utilisateur T1 est valide. Pour ce faire, le module de

traitement MD12 dérive la clé maîtresse cryptographique CMK_0 et utilise la clé ainsi obtenue par dérivation pour générer un code MAC qu'il compare avec un autre code MAC fourni par le terminal T1, comme expliqué plus en détail ultérieurement. Selon un exemple particulier, le module de traitement MD12 est implémenté dans un élément sécurisé, comme déjà mentionné ci-dessus.

Le module de contrôle d'accès MD14 est configuré pour contrôler (ou gérer) l'accès du terminal T1 au service SR considéré. Ce contrôle est réalisé à partir du résultat de la vérification effectuée au préalable par le module de traitement MD12. Le contrôle d'accès réalisé par le module MD14 peut notamment conduire à autoriser, l'utilisateur U1 par exemple, à accéder à tout ou partie du service SR ou peut conduire au refus de l'accès de tout ou partie du service SR.

La **figure 4** représente schématiquement la structure du terminal T1 conformément à un mode de réalisation particulier de l'invention.

Plus précisément, le terminal T1 comprend dans cet exemple au moins un processeur 30, une première mémoire non volatile 32, une deuxième mémoire non volatile 34, une interface de communication 36 et une deuxième interface de communication 38. Le terminal T1 peut en outre comprendre d'autres éléments non représentés, tels qu'une mémoire volatile réinscriptible (RAM) ou une interface homme-machine, qui sont bien connus de l'homme du métier.

La mémoire 32 est une mémoire non volatile réinscriptible ou une mémoire morte (ROM), cette mémoire constituant un support d'enregistrement (ou support d'informations) conforme à un mode de réalisation particulier, lisible par le terminal T1, et sur lequel est enregistré un programme d'ordinateur PG3 conforme à un mode de réalisation particulier. Ce programme d'ordinateur PG2 comporte des instructions pour l'exécution d'étapes d'un procédé de traitement selon un mode de réalisation particulier, comme décrit ultérieurement.

Dans l'exemple envisagé ici, la mémoire 34 est une mémoire non volatile réinscriptible configuré pour stocker en particulier une ou des clés cryptographiques, comme décrit plus en détail ultérieurement dans différents modes de réalisation. La mémoire 34 peut en outre enregistrer d'autres données utiles au terminal T1 telles que par exemple un identifiant ID1 du terminal T1.

La première interface de communication 36 est configurée pour permettre la communication entre le terminal T1 et l'interface de communication 16 du serveur DP2.

La deuxième interface de communication 38 configurée pour permettre la communication entre le terminal T1 et le dispositif DP1 (et plus particulièrement avec l'interface de communication 26 de ce dernier).

Le processeur 30 piloté par le programme d'ordinateur PG3, met ici en œuvre un certain nombre de modules, à savoir : un module de communication MD20 et un module de traitement MD22.

5 Le module de communication MD20 est configuré pour assurer les communications avec l'extérieur et notamment avec le serveur DP2 (en utilisant l'interface 36) et avec le terminal utilisateur T1 (en utilisant l'interface 38). Dans l'exemple considéré ici, les communications avec le serveur DP2 sont réalisées par Internet tandis que les communications avec le dispositif DP1 sont de type NFC, Bluetooth ou autre.

10 Le module de traitement MD22 est configuré pour réaliser un certain nombre de traitements qui seront décrits plus en détails ultérieurement dans différents modes de réalisation. Dans cet exemple, le module de traitement MD22 est en particulier configuré pour générer un code MAC destiné à être transmis au dispositif DP1 du système de contrôle SY en vue d'accéder au service SR. La génération d'un tel code MAC, qui s'effectue notamment à partir d'une donnée de défi envoyée au préalable par le dispositif
15 DP1, sera décrite plus en détail ultérieurement dans des exemples particuliers. Selon un exemple particulier, le module de traitement MD22 est implémenté dans un élément sécurisé. Le terminal T1 est par exemple un téléphone portable, type smartphone, et l'élément sécurisé est par exemple une carte SIM ou un module eUICC (pour « *embedded Universal Integrated Circuit Card* »). Cet élément sécurisé peut être configuré pour
20 stocker des données secrètes telles que des clés cryptographiques et pour exécuter des fonctions cryptographiques.

L'envoi d'un tel code MAC par le module de communication MD20 au dispositif DP1 permet de requérir l'accès au service SR, c'est-à-dire l'accès à certaines fonctionnalités de la voiture du propriétaire U1 dans cet exemple.

25 Dans un mode de réalisation particulier, les modules MD20 et MD22 sont contrôlés à l'aide d'une application logicielle (ou « app ») spécifique mis en œuvre dans le terminal T1.

On comprendra que les modules MD2, MD4 (**figure 2**), MD10-MD14 (**figure 3**) et MD20, MD22 (**figure 4**) décrits ci-avant ne représentent que des exemples de mise en
30 œuvre non limitatifs de l'invention.

Plus généralement, on comprendra que certains éléments généralement présents dans un serveur, dans un terminal de communication, ou encore dans un dispositif électronique destiné à coopérer avec un tel terminal, ont été volontairement omis car ils ne sont pas utiles à la compréhension de la présente invention.

35 Plus généralement, le système de contrôle SY et les terminaux T1 et T2 représentés en **figures 1-4** ne constituent que des exemples de réalisation non limitatifs, d'autres mises en œuvre étant possibles dans le cadre de l'invention. L'homme du métier comprendra en particulier que certains éléments du système de contrôle SY et du terminal

T1 ne sont décrits ici que pour faciliter la compréhension de l'invention, ces éléments n'étant pas nécessaires pour mettre en œuvre l'invention.

Divers exemples de réalisation de l'invention sont à présent décrits à partir des **figures 5 à 10**.

5

Figure 5 : premier mode de réalisation

Un mode de réalisation particulier est à présent décrit en référence à la **figure 5**. Plus précisément, le dispositif DP1 et le serveur DP2 mettent collectivement en œuvre un procédé de contrôle en exécutant respectivement les programmes d'ordinateur PG1 et
10 PG2. En parallèle, le terminal T1 met en œuvre un procédé de traitement en exécutant le programme d'ordinateur PG3.

Dans un premier temps, le terminal T1 de l'utilisateur U1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d'enrôlement (étapes E2-E8). On suppose ici que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque le propriétaire U1
15 vient de faire l'acquisition de sa voiture SR et configure son terminal T1 en interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa voiture. D'autres modes de réalisation sont toutefois possibles.

Comme représenté en **figure 5**, lors de cet enrôlement initial, le terminal T1 envoie (E2) au serveur DP2 une requête d'enrôlement comportant l'identifiant ID1 du terminal T1
20 et, éventuellement, des droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au service SR.

Dans les différents modes de réalisation décrits dans ce document, les droits d'accès RG1 peuvent se présenter par exemple sous la forme d'un identifiant ou d'un code correspondant aux droits d'accès requis. Ces droits d'accès spécifient par exemple les
25 fonctionnalités auxquelles l'utilisateur U1 souhaite accéder (c.-à-d. utiliser), et éventuellement aussi la durée ou la période de temps pendant laquelle chacune de ces fonctionnalités peuvent être accédées.

Le serveur DP2 reçoit (E2) la requête d'enrôlement en provenance du terminal T1 puis détermine (E4) une première clé mère cryptographique OK_0. Pour ce faire, le
30 serveur DP2 récupère la clé maîtresse cryptographique CMK_0 dans sa mémoire et dérive la clé mère cryptographique OK_0 à partir de la clé maîtresse CMK_0, de l'identifiant ID1 et des droits d'accès RG1. Autrement dit, le serveur DP2 détermine en E4 la première clé mère cryptographique OK_0 par dérivation à partir de la clé maîtresse CMK_0 et en prenant en entrée l'identifiant ID1 et les droits d'accès RG1. Cette dérivation est réalisée
35 par calcul en exécutant un algorithme de dérivation approprié dont le choix et l'implémentation sont définis par l'homme du métier.

Dans un exemple particulier, la requête d'enrôlement envoyée par le terminal T1 en E2 comporte en outre un identifiant du service SR, c'est-à-dire identifiant de la voiture de

l'utilisateur U1 dans cet exemple. Le serveur DP2 peut prendre également en compte cet identifiant du service SR pour déterminer en E4 la clé mère OK_0 (et éventuellement aussi la clé mère OK_0_bis1 déterminée en E6 comme expliqué ci-après). De cette manière, lorsqu'une pluralité de services sont possibles, le serveur DP2 peut déterminer la clé mère

5 OK_0 propre au service SR considéré.

Dans ce document, on nommera « DERIV » l'algorithme de dérivation utilisé pour effectuer les différentes opérations de dérivation de clés cryptographiques. Cet algorithme prend en entrée certains paramètres pour dériver une clé cryptographique d'un certain ordre (ou rang) de sorte à obtenir une clé cryptographique d'un ordre (ou rang) inférieur.

10 On considère ici que la clé CMK_0 est une clé maîtresse dans le sens où c'est la clé à partir de laquelle toutes les autres clés utilisées, pour un service donné SR, sont dérivées directement ou indirectement, comme expliqué tout au long du présent exposé. Une clé d'ordre inférieur présente un lien intrinsèque avec la clé d'ordre immédiatement supérieur dont elle est issue, et également avec chaque autre clé d'ordre encore supérieure dont

15 elle est éventuellement indirectement issue. Ce lien, qui résulte du mécanisme de dérivation utilisé, permet de contrôler efficacement la validité des différentes clés cryptographiques attribuées aux utilisateurs. En particulier, l'expiration ou la révocation d'une première clé cryptographique a pour conséquence de rendre invalide, non seulement ladite première clé, mais également toutes éventuelles clés d'ordre inférieur qui

20 sont dérivées directement ou indirectement à partir de ladite première clé.

Avant de calculer (E4) la clé première mère OK_0, le serveur DP2 peut coopérer avec le terminal T1 pour réaliser une procédure d'authentification appropriée du terminal T1 pour vérifier que le terminal T1 est autorisé à recevoir la clé mère OK_0.

Selon une variante, le terminal T1 ne fournit pas les droits d'accès RG1 en E2. C'est le

25 serveur DP2 qui détermine lui-même les droits d'accès RG1 auxquels l'utilisateur U1 peut prétendre et qui utilise ceux-ci en E4 pour calculer la clé mère OK_0.

Comme représenté en **figure 5**, le serveur DP2 détermine (E6) ensuite une deuxième clé mère cryptographique OK_0_bis1, différente de la première clé mère OK_0 obtenue en E4. Pour ce faire, le serveur DP2 dérive en E6 la deuxième clé mère OK_0_bis1 à partir de

30 la clé maîtresse CMK_0, de l'identifiant ID1 et des droits d'accès RG1. Autrement dit, le serveur DP2 détermine en E6 la deuxième clé mère OK_0_bis1 par dérivation à partir de la clé maîtresse CMK_0 et en prenant en entrée l'identifiant ID1 et les droits d'accès RG1, de façon analogue au calcul de la première clé mère OK_0 en E4. Cette deuxième dérivation E6 est également réalisée par calcul en exécutant l'algorithme de dérivation

35 DERIV. Afin de garantir que la clé mère OK_0_bis1 obtenue en E6 est différente de la mère OK_0 obtenue en E4, les dérivations réalisées en E4 et E6 peuvent prendre en entrée une donnée supplémentaire, appelée par exemple « type de clé », et qui prendrait

différentes valeurs selon que l'on veut obtenir par dérivation OK_0 (en E4) ou OK_0bis1 (en E6).

Le serveur DP2 envoie (E8) ensuite au terminal T1 les clés mères cryptographiques OK_0 et OK_0_bis1 obtenues respectivement en E4 et E6. Dans cet exemple, cet envoi E8 comprend en outre les droits d'accès RG1. Cet envoi est fait de préférence de façon sécurisée.

Une fois reçus (E8), le terminal T1 enregistre (E10) les clés mères OK_0 et OK_0_bis1 et les droits d'accès RG1 dans sa mémoire 34 (**figure 4**). Dans un exemple particulier, le premier terminal T1 est un terminal de télécommunications, de type smartphone par exemple, et la mémoire locale 34 est une mémoire sécurisée d'un élément sécurisé (ou dispositif sécurisé), d'une carte SIM ou d'un module d'identité de souscripteur embarqué (de type eUICC pour « *embedded Universal Integrated Circuit Card* »).

Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire les clés mères OK_0 et OK_0_bis1 obtenues chacune par dérivation à partir de la clé maîtresse CMK_0. Ces clés mères OK_0 et OK_0_bis1 peuvent être utilisées par le terminal T1 lors de chaque accès au service SR.

On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique DP1 (**figure 1**).

Le dispositif DP1 envoie (E12) alors au terminal T1 une donnée de défi (ou « challenge » en anglais) notée c10.

Dans le présent exposé, cette donnée de défi c10 et toutes autres données de défi considérées ultérieurement peuvent se présenter sous une quelconque forme appropriée exploitable par un terminal destinataire pour générer un code MAC comme expliqué ci-après. Une telle donnée de défi peut notamment prendre la forme d'une série d'au moins un caractère, de type alphanumérique ou autre par exemple. Cette donnée de défi c1, comme toutes les données de défi évoquées dans ce document, se caractérise en ce qu'elle est de préférence imprédictible, ou du moins difficile à prédire, pour une entité extérieure afin de rendre difficile tout accès non autorisé au service SR.

Comme représenté en **figure 5**, une fois la donnée de défi c10 reçue (E12), le terminal T1 détermine (E14) une donnée d'authentification AUTH_D1 en calculant un code MAC à partir de la deuxième clé mère cryptographique OK_0_bis1 et à partir d'une donnée de dérivation DERIV_D et d'une donnée temporelle TIME_V. Pour ce faire, le terminal T1 détermine au préalable la donnée de dérivation DERIV_D et la donnée temporelle TIME_V selon une quelconque manière appropriée.

Plus précisément, la donnée temporelle TIME_V est une donnée représentative de la validité dans le temps d'une clé temporaire cryptographique OK_0_T1 qui est déterminée ici en E16 (**figure 5**). Par ailleurs, la donnée de dérivation DERIV_D est ici une donnée choisie par le terminal T1 et qui intervient ultérieurement dans le calcul de la clé temporaire cryptographique OK_0_T1, comme expliqué ci-après.

Le terminal T1 dérive (E16) ensuite la clé temporaire cryptographique OK_0_T1 mentionnée ci-dessus, à partir de la première clé mère cryptographique OK_0 et de la donnée de dérivation DERIV_D. Autrement dit, la clé temporaire cryptographique OK_0_T1 est déterminée en E16 par dérivation à partir de la première clé mère OK_0 et en prenant en entrée la donnée de dérivation DERIV_D. La clé temporaire OK_0_T1 déterminée en E16 peut donc varier en fonction notamment de la donnée de dérivation DERIV_D choisie par le terminal T1.

Dans le présent exposé, une « clé temporaire cryptographique » (ou clé provisoire cryptographique) désigne une clé cryptographique dont la validité dans le temps est limitée. Une telle clé temporaire n'est valide que pendant une période de temps prédéfinie.

Dans le mode de réalisation décrit ici, le terminal T1 utilise (E16) la donnée de dérivation DERIV_D pour dériver la clé temporaire OK_0_T1. Comme décrit ci-dessus en E14, cette donnée de dérivation DERIV_D est en outre prise en entrée avec la donnée temporelle TIME_V pour déterminer la donnée d'authentification AUTH_D1. Comme expliqué par la suite, l'usage combiné de la donnée de dérivation DERIV_D et de la donnée temporelle TIME_V permet de conférer une validité limitée dans le temps à la clé temporaire OK_0_T1.

Lors d'une étape de calcul E18, le terminal T1 génère un code MAC, noté MC10, à partir de la clé temporaire OK_0_T1 et de la donnée de défi c10.

De façon bien connue, un code MAC (pour « Code d'Authentification de Message ») est un code pouvant accompagner des données dans le but d'assurer l'intégrité de ces dernières, permettant ainsi de vérifier que celles-ci n'ont subi aucune modification, après une transmission par exemple. Dans le présent document, le calcul du code MAC MC10 et de tous les autres codes MAC considérés ultérieurement est réalisé en exécutant un algorithme (noté « MAC » dans les figures) à partir d'une clé secrète, à savoir la clé temporaire OK_0_T1 dans cet exemple. L'utilisation d'un tel code MAC permet d'authentifier son expéditeur. Le choix et l'implémentation du calcul d'un tel code MAC sont définis par l'homme du métier selon chaque cas d'usage.

Lors d'une étape d'envoi E20, le terminal T1 envoie au dispositif DP1 le code MAC MC10 ainsi que l'identifiant ID1 du terminal T1, les droits d'accès RG1, la donnée de dérivation DERIV_D, la donnée temporelle TIME_V et la donnée d'authentification AUTH_D1. Une fois ces données reçues (E20), le dispositif DP1 procède à l'étape E22.

Lors de l'étape E22, le dispositif DP1 dérive la première clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1. Autrement dit, le dispositif DP1 détermine en E22 la première clé mère cryptographique OK_0 par dérivation à partir de la clé maîtresse CMK_0 et en prenant en entrée l'identifiant ID1 et les droits d'accès RG1. Cette dérivation est réalisée en exécutant l'algorithme de dérivation DERIV de la même manière que lors de l'étape de dérivation E4 réalisée par le serveur DP2.

Le dispositif DP1 dérive (E24) également la deuxième clé mère cryptographique OK_0_bis1 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1. Autrement dit, le dispositif DP1 détermine en E24 la deuxième clé mère cryptographique OK_0_bis1 par dérivation à partir de la clé maîtresse CMK_0 et en prenant en entrée l'identifiant ID1 et les droits d'accès RG1, de la même manière que lors de l'étape de dérivation E6 réalisée par le serveur DP2.

Au cours d'une étape de vérification E26, le dispositif DP1 vérifie la donnée d'authentification AUTH_D1 reçue en E20. Pour ce faire, le dispositif DP1 recalcule la donnée d'authentification AUTH_D1 en générant un code MAC à partir de la deuxième clé mère OK_0_bis1 obtenu en E24 et à partir de la donnée de dérivation DERIV_D et de la donnée temporelle TIME_V reçues en E20. Le calcul de ce code MAC est réalisé de la même manière que lors du calcul E14 réalisée par le terminal T1 (**figure 5**). Si le code MAC ainsi obtenu en E26 est identique à la donnée d'authentification AUTH_D1 reçue en E20, le dispositif DP1 détecte que la donnée d'authentification AUTH_D1 est valide et procède à l'étape E28. Dans le cas contraire, le procédé prend fin et le dispositif DP1 informe éventuellement le terminal T1 que les données reçues sont invalides.

Au cours d'une étape de vérification E28, le dispositif DP1 vérifie la validité de la donnée temporelle TIME_V. Pour ce faire, le dispositif DP1 détermine dans cet exemple un point courant dans le temps, tel que par exemple une date courante et/ou une heure courante, et détermine si la donnée temporelle TIME_V est valide à partir de ce point courant dans le temps. Dans un exemple particulier, le dispositif DP1 détermine à partir de la donnée temporelle TIME_V une période de temps (période d'une heure ou d'un jour, par exemple) pendant laquelle l'utilisateur U1 est autorisé à accéder au service SR, et détecte que la donnée temporelle TIME_V est valide si la date et l'heure courantes définissent un point courant dans le temps compris dans cette période de temps prédéterminée. Autrement dit, la validité dans le temps des données envoyées par le terminal T1 en E20, et en particulier de la donnée d'authentification AUTH_D1, est déterminée par la donnée temporelle TIME_V.

Le dispositif DP1 dérive (E30) ensuite la clé temporaire cryptographique OK_0_T1 à partir de la première clé mère OK_0 et de la donnée de dérivation DERIV_D. Pour ce faire, le dispositif DP1 détermine la clé temporaire OK_0_T1 par dérivation à partir de la

clé mère OK_0 et en prenant en entrée la donnée de dérivation DERIV_D reçue en E20. La vérification préalable de la donnée de dérivation DERIV_D (E26) et de la donnée temporelle TIME_V (E28) permet de s'assurer que la clé temporaire OK_0_T1 est toujours valide au moment du traitement.

5 Lors d'une étape E32, le dispositif DP1 génère à son tour un code MAC, noté ici MC11, à partir de la clé temporaire cryptographique OK_0_T1 obtenue en E30 et de la donnée de défi c10 envoyée en E12. Ce code MAC MC12 est obtenu en effectuant le même calcul que lors de l'étape de calcul E18 réalisée par le terminal T1.

10 Le dispositif DP1 compare (E34) ensuite le code MAC MC10 reçu en E20 avec le code MAC MC11 calculé en E30 et détermine si ces deux codes MAC coïncident. Dans cet exemple, le dispositif DP1 vérifie si MC1 et MC2 sont identiques.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E34 entre les codes MAC MC10 et MC11.

15 Plus précisément, lors d'une étape E36, le dispositif DP1 détermine à partir du résultat de la comparaison réalisée en E34 si le terminal T1 est autorisé à accéder au service SR selon les droits d'accès RG1. Autrement dit, le dispositif DP1 contrôle l'accès au service SR en fonction du résultat obtenu en E34 ($MC10 = MC11$?). Ce contrôle peut se concrétiser par une autorisation d'accès ou par un blocage.

20 Le dispositif DP1 peut également envoyer (E38) au terminal T1 une réponse DEC10 indiquant sa décision concernant la demande d'accès du terminal T1 au service SR.

Dans cet exemple, s'il est détecté en E34 que les codes MAC MC10 et MC11 sont identiques, le dispositif DP1 autorise (E36) l'accès au service SR selon les droits d'accès RG1 et envoie (E38) une réponse DEC10 positive au terminal T1. Dans le cas contraire (codes MAC MC10 et MC11 différents), le dispositif DP1 bloque l'accès du terminal T1 au service SR et envoie une réponse DEC10 négative en E38 au terminal T1.

25 La présente invention permet ainsi de sécuriser l'accès d'un service en fournissant à des utilisateurs une ou des clés temporaires cryptographiques pour bénéficier de certains droits d'accès. Ces clés temporaires sont issues d'une clé maîtresse cryptographique au travers d'une double dérivation de clé, comme décrit ci-avant dans un exemple particulier (dérivation de CMK_0 puis de OK_0). L'usage de clés temporaires cryptographiques est avantageux en ce que celles-ci peuvent être renouvelées régulièrement, rendant ainsi plus difficile tous accès illicites à un service donné. En effet, un tiers malveillant ne disposera que d'un temps restreint pour obtenir l'accès au service pendant qu'une clé temporaire est en cours de validité, réduisant ainsi les risques de fraudes. Chaque changement de clé temporaire rend plus difficile l'accès frauduleux à un service.

35 De manière avantageuse, on peut définir la période de validité d'une clé temporaire de sorte à ce qu'une tentative d'accès frauduleuse ait peu de chance d'aboutir avant expiration de la clé temporaire en cours de validité.

Lorsqu'un utilisateur souhaite accéder au service, il transmet au système de contrôle, via son terminal, un code MAC généré à partir de sa clé temporaire cryptographique. En revanche, l'utilisateur ne transmet pas sa clé temporaire cryptographique, ni même sa clé mère cryptographique OK_0, puisque le système de contrôle est capable de retrouver lui-même ces clés par calcul. Ce procédé permet ainsi de sécuriser l'accès au service tout en limitant la diffusion des clés cryptographiques. Dans l'exemple ci-dessus, les clés mères cryptographiques OK_0 et OK_0_bis1 ne sont diffusées qu'une fois, lors de l'enrôlement.

L'invention permet aussi de faciliter la révocation des droits d'accès susceptibles d'avoir été attribués à un utilisateur. Par exemple, si la clé maîtresse CMK_0 est révoquée ou a expiré, le système de contrôle SY calcule en E22 et E24 (**figure 5**) des clés mères différentes des clés OK_0 et OK_0_bis1 et en déduit ensuite que la demande d'accès du terminal T1 doit être rejetée.

Le système SY, et en particulier le véhicule SR, n'est pas forcément au courant que la clé maîtresse CMK_0 a été révoquée ou n'est plus valide. Cependant, si une procédure de révocation a modifié CMK_0 de sorte que c'est une nouvelle clé maîtresse CMK_1 qui est à présent utilisée par le véhicule SR à la place de CMK_0, alors toutes les clés dérivées à partir de la clé CMK_0 produiront des codes MACs invalides. Dans cet exemple, une procédure de révocation consiste à changer la clé maîtresse (en remplaçant CMK_0 par CMK_1 par exemple).

Dans le mode réalisation représenté en **figure 5**, une deuxième clé mère cryptographique OK_0_bis1 est utilisée (E14) pour générer le code MAC correspondant à la donnée d'authentification AUTH_D1. L'usage de cette clé additionnelle OK_0_bis1, différente de la première clé mère OK_0 utilisée en E18 pour calculer le code MAC MC10, permet de sécuriser encore d'avantage l'accès au service SR.

Selon une variante de réalisation, on utilise la première clé mère OK_0 en E14 (**figure 5**), à la place de la deuxième clé mère OK_0_bis1, pour calculer aussi la donnée d'authentification AUTH_D1. De la même manière, la première clé mère OK_0 est utilisée en E26 par le dispositif DP1 pour recalculer la donnée d'authentification AUTH_D1. Dans ce cas, les étapes E6 et E24 représentées en **figure 5** visant à déterminer cette deuxième clé mère OK_0_bis1 ne sont pas réalisées. Cette variante permet de simplifier quelque peu les traitements réalisés par le système de contrôle SY.

Figure 6 : variante du premier mode de réalisation

Dans le mode de réalisation représenté en **figure 5**, le terminal T1 reçoit notamment la clé mère cryptographique OK_0 lui permettant de déterminer un clé temporaire cryptographique en fonction notamment de la date et de l'heure courantes. Le terminal T1 choisit la donnée temporelle TIME_V et la donnée de dérivation DERIV_D de sorte que la clé temporaire OK_0_T1 soit valide pendant une période de temps suffisamment longue

pour calculer le code MAC (étape E18, figure 5) et pour que le système de contrôle SY vérifie ensuite (étapes E22-E38) le code MAC reçu avec cette même clé temporaire OK_0_T1.

5 L'envoi E8 (**figure 5**) de la clé mère cryptographique OK_0 suppose toutefois que le terminal T1 soit un terminal de confiance. En particulier, on optera de préférence pour ce mode de réalisation si le terminal T1 dispose d'une mémoire suffisamment sécurisée pour stocker la clé mère OK_0 et, éventuellement, la clé mère OK_0_bis1.

10 Une variante du mode de réalisation de la **figure 5** est à présent décrite en référence à la **figure 6**. On suppose ici que le terminal T1 ne présente pas le niveau de confiance requis pour recevoir et stocker en sécurité la clé mère cryptographique OK_0 et, éventuellement, la clé mère OK_0_bis1. C'est le cas par exemple lorsque le terminal T1 ne contient pas d'élément sécurisé tel qu'une carte SIM ou un module eUICC. Aussi, cette variante diffère du mode de réalisation de la **figure 5** en ce que le serveur DP2 ne fournit pas la clé mère OK_0, et éventuellement la clé mère OK_0_bis1, au terminal T1 mais

15 fournit directement à celui-ci une ou une pluralité de clés temporaires cryptographiques ainsi qu'une donnée d'authentification associée à chaque clé temporaire fournie, de sorte à permettre au terminal T1 d'accéder ensuite au service SR considéré. Le serveur DP2 détermine chaque clé temporaire de la même manière que la clé temporaire OK_0_T1 déterminée par le terminal T1 dans le mode de réalisation de la **figure 5** (étape E16).

20 Plus particulièrement, comme représenté en **figure 6**, le terminal T1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d' enrôlement (étapes E50-E58). On suppose ici que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque l'utilisateur U1 vient de faire l'acquisition de sa voiture SR et configure son terminal T1 en interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa

25 voiture. D'autres modes de réalisation sont toutefois possibles.

Lors de cet enrôlement initial, le terminal T1 envoie (E50) au serveur DP2 une requête d' enrôlement de façon identique à l'étape E2 représenté en **figure 5**. Cette requête d' enrôlement comporte l'identifiant ID1 du terminal T1 et, éventuellement, des droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au

30 service SR. Ces droits d'accès RG1 se caractérisent de la même manière que décrit précédemment en référence à la **figure 5**.

Le serveur DP2 reçoit (E50) la requête d' enrôlement en provenance du terminal T1 puis détermine une première clé mère cryptographique OK_0 (étape E52) et une deuxième clé mère cryptographique OK_0_bis1 (étape E54) de la même manière que

35 décrit précédemment en référence respectivement aux étapes E4 et E6 de la **figure 5**.

Le serveur DP2 détermine (E56) ensuite au moins une clé temporaire cryptographique par dérivation à partir de la première clé mère OK_0. Comme représenté en **figure 6**, on suppose ici que le serveur DP2 détermine en E56 les clés temporaires

cryptographiques OK_0_T1, OK_0_T2 et OK_0_T3 par dérivation à partir de la clé mère OK_0 et d'une donnée de dérivation DERIV_D respective. Pour ce faire, le serveur DP2 détermine au préalable les données de dérivation DERIV_D puis détermine les clés temporaires OK_0_T1, OK_0_T2 et OK_0_T3 de façon analogue au calcul E16 décrit ci-

5 avant en référence à la **figure 5**. Au cours de cette étape de traitement E56 (**figure 6**), le serveur DP2 détermine également, de façon analogue à l'étape E14 représentée en **figure 5**, des données d'authentification AUTH_D1, AUTH_D2 et AUTH_D3 associées respectivement aux clés temporaires OK_0_T1, OK_0_T2 et OK_0_T3. Dans cette

10 exemple, chacune des données d'authentification AUTH_D1, AUTH_D2 et AUTH_D3 est donc déterminée en calculant un code MAC correspondant, à partir de la deuxième clé mère OK_0_bis1, d'une donnée temporelle TIME_V et d'une donnée de dérivation DERIV_D.

Les données temporelles TIME_V et les données de dérivation DERIV_D se caractérisent de la même manière que décrit précédemment en référence à la **figure 5**.

15 Comme représenté en **figure 6**, le serveur DP2 envoie (E58) ensuite au terminal T1 un ensemble de données PCK1 comprenant les clés temporaires OK_0_T1, OK_0_T2 et OK_0_T3 ainsi que les données d'authentification associées AUTH_D1, AUTH_D2 et AUTH_D3.

Une fois reçues (E58), le terminal T1 enregistre (E59) ces données dans sa mémoire

20 34 (**figure 4**).

Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire des clés temporaires cryptographiques déterminées par double dérivation à partir de la clé maîtresse CMK_0. Ces clés temporaires OK_0_T1,

25 OK_0_T2 et OK_0_T3 peuvent être utilisées par le terminal T1 pour accéder au service SR.

On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique

30 DP1 (**figure 1**).

Le dispositif DP1 envoie (E60) au terminal T1 une donnée de défi notée ici c11.

Comme représenté en **figure 6**, une fois la donnée de défi c1 reçue (E60), le terminal T1 détermine (E62) un point courant dans le temps, à savoir dans cet exemple : la date courante et/ou l'heure courante (données temporelles).

35 Le terminal T1 sélectionne (E64) alors, en fonction du point courant dans le temps déterminée en E62, une clé applicable parmi les clés temporaires OK_0_T1, OK_0_T2 et OK_0_T3 reçues en E60. Dans cette exemple, on suppose que le terminal T1 détermine,

en fonction des date et/ou heure courantes, que la clé temporaire OK_0_T2 est celle à utiliser et sélectionne donc celle-ci au cours de l'étape E64.

Lors d'une étape de calcul E66, le terminal T1 génère un code MAC, noté MC12, à partir de la clé temporaire OK_0_T2 sélectionnée en E64 et à partir de la donnée de défi c11 reçue en E60. La génération E66 de ce code MAC MC12 s'effectue de façon analogue au calcul E18 décrit ci-avant en référence à la **figure 5**.

Lors d'une étape d'envoi E68, le terminal T1 envoie au dispositif DP1 le code MAC MC12 ainsi que l'identifiant ID1 du terminal T1, les droits d'accès RG1, la donnée de dérivation DERIV_D associée à la clé temporaire OK_0_T2, la donnée temporelle TIME_V associée à la clé temporaire OK_0_T2, et également la donnée d'authentification AUTH_D2 associée à la clé temporaire OK_0_T2. Une fois ces données reçues (E68), le dispositif DP1 réalise un traitement (étapes E70-E86) analogue à celui décrit précédemment en référence aux étapes E22-E38 (**figure 5**).

Plus particulièrement, lors de l'étape de dérivation E70, le dispositif DP1 dérive la première clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1 de la même manière que lors de l'étape de dérivation E52 réalisée par le serveur DP2.

Le dispositif DP1 dérive (E72) également la deuxième clé mère cryptographique OK_0_bis1 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1 de la même manière que lors de l'étape de dérivation E54 réalisée par le serveur DP2.

Au cours d'une étape de vérification E74, le dispositif DP1 vérifie la donnée d'authentification AUTH_D2, de la même manière que lors de l'étape de calcul E56 réalisée par le serveur DP2. Le dispositif DP1 génère ainsi un code MAC à partir de la deuxième clé mère OK_0_bis1 et à partir de la donnée de dérivation DERIV_D et de la donnée temporelle TIME_V reçues en E68. Si le code MAC ainsi obtenu en E74 est identique à la donnée d'authentification AUTH_D2 reçue en E68, le dispositif DP1 détecte que la donnée d'authentification AUTH_D2 est valide et procède à l'étape E76. Dans le cas contraire, le procédé prend fin et le dispositif DP1 informe éventuellement le terminal T1 que les données reçues sont invalides.

Au cours d'une étape de vérification E76, le dispositif DP1 vérifie la validité de la donnée temporelle TIME_V reçue en E68, de façon identique à l'étape E28 représentée en **figure 5**. Le dispositif DP1 détermine par exemple un point courant dans le temps, tel que par exemple une date courante et/ou une heure courante, et détermine si la donnée temporelle TIME_V est valide à partir de ce point courant dans le temps.

Toujours en référence à la **figure 6**, le dispositif DP1 dérive (E78) ensuite la clé temporaire cryptographique OK_0_T2 à partir de la première clé mère OK_0 obtenue en

E70 et de la donnée de dérivation DERIV_D reçue en E68, de la même manière que lors de l'étape E56 réalisée par le serveur DP2.

Lors d'une étape de calcul E80, le dispositif DP1 génère à son tour un code MAC, noté ici MC13, à partir de la clé temporaire cryptographique OK_0_T2 obtenue en E78 et de la donnée de défi c11 envoyée en E60. Ce code MAC MC13 est ici obtenu en effectuant le même calcul que lors de l'étape de calcul E66 réalisée par le terminal T1 pour générer le code MAC MC12.

Le dispositif DP1 compare (E82) ensuite le code MAC MC12 reçu en E68 avec le code MAC MC13 calculé en E80 et détermine si ces deux codes MAC sont identiques (ou coïncident), ce façon analogue à l'étape E34 représentée en **figure 5**.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E82 entre les codes MAC MC12 et MC13. Pour ce faire, le dispositif DP1 réalise les étapes E84 et E86 de façon analogue aux étapes E36 et E38 représentées en **figure 5**. En particulier, comme représenté en **figure 6**, le dispositif DP1 autorise ou bloque l'accès du terminal T1 au service SR (étape E84) et envoie une décision DEC11 positive ou négative au terminal T1 (étape E86).

La variante représentée en **figure 6** permet ainsi avantageusement de mettre à profit les ressources disponibles au niveau du système de contrôle SY, et plus précisément ici du serveur DP2, pour déterminer une ou des clés temporaires cryptographiques susceptibles d'être utilisées par le terminal T1 pour accéder au service SR. En outre, cela permet de ne pas diffuser une ou des clés mères cryptographiques, au caractère sensible, depuis le système de contrôle SY vers un terminal client lorsque ce dernier ne présente pas un niveau de confiance suffisant.

De la même façon que pour la **figure 5**, il est possible d'utiliser aussi en E56 (**figure 6**) la première clé mère cryptographique OK_0 pour calculer les données d'authentification AUTH_D1, AUTH_D2 et AUTH_D3.

Figure 7 : deuxième mode de réalisation

Un autre mode de réalisation est à présent décrit en référence à la **figure 7**. Plus précisément, le dispositif DP1 et le serveur DP2 mettent collectivement en œuvre un procédé de contrôle en exécutant respectivement les programmes d'ordinateur PG1 et PG2. En parallèle, le terminal T1 met en œuvre un procédé de traitement en exécutant le programme d'ordinateur PG3.

Dans un premier temps, le terminal T1 de l'utilisateur U1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d'enrôlement (étapes E90-E96) de façon similaire aux étapes E2-E8 représentées en **figure 5**, à la différence qu'aucune deuxième clé temporaire OK_0_bis1 n'est ici utilisée.

On suppose ici aussi que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque le propriétaire U1 vient de faire l'acquisition de sa voiture SR et configure son terminal T1 en interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa voiture. D'autres modes de réalisation sont toutefois possibles.

5 Comme représenté en **figure 7**, le terminal T1 envoie (E90) au serveur DP2, lors de cet enrôlement initial, une requête d'enrôlement comportant l'identifiant ID1 du terminal T1 et, éventuellement, des droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au service SR.

10 Le serveur DP2 dérive (E92) une première clé mère cryptographique OK_0 à partir de la clé maîtresse CMK_0, de l'identifiant ID1 et des droits d'accès RG1, de façon identique à l'étape E4 représentée en **figure 5**.

Le serveur DP2 envoie (E96) ensuite la clé mère cryptographique OK_0, et éventuellement les droits d'accès RG1, au terminal T1.

15 Une fois reçus (E96), le terminal T1 enregistre (E98) la clé mère OK_0 et les droits d'accès RG1 dans sa mémoire 34 (**figure 4**). Dans un exemple particulier, le premier terminal T1 est un terminal de télécommunications, de type smartphone par exemple, et la mémoire locale 34 est une mémoire sécurisée d'une carte SIM ou d'un module d'identité de souscripteur embarqué (de type eUICC pour « *embedded Universal Integrated Circuit Card* »).

20 Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire la clé mère OK_0 obtenue par dérivation à partir de la clé maîtresse CMK_0. Cette clé mère OK_0 peut être utilisée par le terminal T1 lors de chaque accès au service SR.

25 On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique DP1 (**figure 1**).

Le dispositif DP1 envoie (E100) au terminal T1 une donnée de défi notée c12.

30 Lors d'une étape E102, le terminal T1 détermine une donnée temporelle DT1 représentative de la validité dans le temps d'une clé temporaire cryptographique OK_0_T5 calculée ici en E104 (**figure 7**). Pour ce faire, le terminal T1 détermine au préalable la donnée temporelle DT1 selon une quelconque manière appropriée.

35 Plus particulièrement, dans cet exemple de réalisation, le terminal T1 détermine un point courant dans le temps, défini ici par la date courante et/ou l'heure courante. Le terminal T1 détermine alors en E102 la donnée temporelle DT1 en fonction de la date courante et/ou de l'heure courante.

Au cours d'une étape E104, le terminal T1 dérive une clé temporaire cryptographique OK_0_T5 (déjà mentionnée ci-avant) à partir de la clé mère OK_0 reçue en E96 et de la donnée temporelle DT1 déterminée en E102. Autrement dit, la clé temporaire OK_0_T5 est déterminée par dérivation à partir de la clé mère OK_0 et en prenant en entrée la donnée temporelle DT1.

Le terminal T1 génère ensuite un code MAC, noté MC14, à partir de la clé temporaire OK_0_T5 et de la donnée de défi c12, de façon analogue à l'étape E18 (**figure 5**) ou à l'étape E66 (**figure 6**).

Lors d'une étape d'envoi E108, le terminal T1 envoie au dispositif DP1 le code MAC MC14 ainsi que l'identifiant ID1 du terminal T1 et les droits d'accès RG1. Une fois ces données reçues (E108), le dispositif DP1 procède à l'étape E110.

Lors de l'étape E110, le dispositif DP1 dérive la clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1, de façon identique à l'étape E22 (**figure 5**) ou à l'étape E92 (**figure 7**).

Le dispositif DP2 détermine (E112) en outre une donnée temporelle, notée ici DT2, en fonction d'un point courant dans le temps. Pour ce faire, le dispositif DP2 détermine dans cet exemple la date courante et/ou l'heure courante, et en déduit la donnée temporelle DT2. Dans un exemple particulier, le dispositif DP2 (et plus généralement, le système de contrôle SY) est configuré pour que la donnée temporelle DT2 déterminée en E112 corresponde à une période de temps prédéfinie, c'est-à-dire une fenêtre (ou créneau) temporelle, pendant laquelle une clé temporaire cryptographique (OK_0_T5, dans cet exemple) est valide.

Dans l'exemple considéré ici, on suppose que la donnée temporelle DT2 est identique à la donnée temporelle DT1. Cela peut toutefois ne pas être le cas si le terminal T1 tarde trop longtemps avant d'envoyer son code MAC MC14 en E108 au dispositif DP1.

Le dispositif DP1 dérive (E114) alors la clé temporaire cryptographique OK_0_T5 à partir de la clé mère OK_0 et de la donnée temporelle DT2. Pour ce faire, le dispositif DP1 détermine la clé temporaire OK_0_T5 par dérivation à partir de la clé mère OK_0 et en prenant en entrée la donnée temporelle DT2 déterminée en E112. L'obtention préalable de la donnée temporelle DT2 permet de déterminer la clé temporaire OK_0_T5 qui est en cours de validité au moment du traitement.

Selon un exemple particulier, on fixe une durée de validité prédéfinie pour différentes clés temporaires. Cette durée de validité est fixée à 1 heure par exemple. Les données temporelles associées à chacune des clés temporaires correspondent à des heures fixes pleines, par exemple les heures « 13h00 », « 14h00 », « 15h00 »... Ainsi, toutes les heures, une nouvelle clé temporaire est valable pendant 1 heure. Le système de contrôle SY vérifie ainsi de la manière suivante : il regarde quelle heure il est en E112 et en déduit

la valeur de la donnée temporelle DT6. Si l'heure courante est « 13h45 », il en déduit que la donnée temporelle DT2 correspond à l'heure de « 13h00 ». Selon une variante, la valeur de la donnée temporelle DT2 peut être également envoyée par le terminal T1, et le système de contrôle SY vérifie que cette date et/ou heure n'a pas expirée par rapport à la durée de validité fixée.

Selon une variante, la donnée temporelle DT2 est différente de la donnée temporelle DT1 mais suffisamment proche pour que le dispositif DP1 obtienne en E114 la même clé temporaire cryptographique OK_0_T5 que celle déterminée par le terminal T1 en E104.

Lors d'une étape E116, le dispositif DP1 génère à son tour un code MAC, noté ici MC15, à partir de la clé temporaire cryptographique OK_0_T5 obtenue en E114 et de la donnée de défi c12 envoyé en E100. Ce code MAC MC15 est obtenu en effectuant le même calcul que lors de l'étape de calcul E106 réalisée par le terminal T1.

Le dispositif DP1 compare (E118) ensuite le code MAC MC14 reçu en E108 avec le code MAC MC15 calculé en E116 et détermine si ces deux codes MAC coïncident. Dans cet exemple, le dispositif DP1 vérifie si MC14 et MC15 sont identiques.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E118 entre les codes MAC MC14 et MC15, de façon analogue aux étapes E34-E38 décrites ci-avant en référence à la **figure 5**.

Plus précisément, lors d'une étape de traitement E120, le dispositif DP1 détermine à partir du résultat de la comparaison réalisée en E118 si le terminal T1 est autorisé à accéder au service SR selon les droits d'accès RG1. Autrement dit, le dispositif DP1 contrôle l'accès au service SR en fonction du résultat obtenu en E118 (MC14 = MC15 ?). Ce contrôle peut se concrétiser par une autorisation d'accès ou par un blocage.

Le dispositif DP1 peut également envoyer (E122) au terminal T1 une réponse DEC12 indiquant sa décision concernant la demande d'accès du terminal T1 au service SR.

Dans cet exemple, s'il est détecté en E118 que les codes MAC MC14 et MC15 sont identiques, le dispositif DP1 autorise (E120) l'accès au service SR selon les droits d'accès RG1 et envoie (E122) une réponse DEC12 positive au terminal T1. Dans le cas contraire (codes MAC MC14 et MC15 différents), le dispositif DP1 bloque (E120) l'accès du terminal T1 au service SR et envoie (E122) une réponse DEC12 négative pour en informer le terminal T1.

Ce mode de réalisation particulier permet avantageusement à un terminal de confiance de garder en mémoire une clé mère cryptographique à partir de laquelle peut être déterminée une clé temporaire applicable pour une période de temps donnée. Le terminal peut ainsi, dans cette période de temps, utiliser cette clé temporaire pour obtenir l'accès au service concerné.

Figure 8 : variante du deuxième mode de réalisation

Dans le mode de réalisation représenté en **figure 7**, l'envoi E96 de la clé mère cryptographique OK_0 suppose toutefois que le terminal T1 soit un terminal de confiance. En particulier, on optera de préférence pour ce mode de réalisation si le terminal T1 dispose d'une mémoire suffisamment sécurisée pour stocker la clé mère OK_0.

5 Une variante du mode de réalisation de la **figure 7** est à présent décrite en référence à la **figure 8**. On suppose ici que le terminal T1 ne présente pas le niveau de confiance requis pour recevoir et stocker en sécurité la clé mère cryptographique OK_0. C'est le cas par exemple lorsque le terminal T1 ne contient pas d'élément sécurisé tel qu'une carte SIM ou un module eUICC. Aussi, cette variante diffère du mode de réalisation de la

10 **figure 7** en ce que le serveur DP2 ne fournit pas la clé mère OK_0 au terminal T1 mais fournit directement à celui-ci une ou une pluralité de clés temporaires cryptographiques, de sorte à permettre au terminal T1 d'accéder ensuite au service SR considéré. Le serveur DP2 détermine chaque clé temporaire de la même manière que la clé temporaire OK_0_T5 déterminée par le terminal T1 dans le mode de réalisation de la **figure 7** (étape

15 E104).

Plus particulièrement, comme représenté en **figure 8**, le terminal T1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d'enrôlement (étapes E130-E136). On suppose ici que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque l'utilisateur U1 vient de faire l'acquisition de sa voiture SR et configure son terminal T1 en

20 interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa voiture. D'autres modes de réalisation sont toutefois possibles.

Lors de cet enrôlement initial, le terminal T1 envoie (E130) au serveur DP2 une requête d'enrôlement de façon identique à l'étape E90 représentée en **figure 7**. Cette requête d'enrôlement comporte l'identifiant ID1 du terminal T1 et, éventuellement, des

25 droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au service SR. Ces droits d'accès RG1 se caractérisent de la même manière que décrit précédemment.

Le serveur DP2 reçoit (E130) la requête d'enrôlement en provenance du terminal T1 puis détermine une première clé mère cryptographique OK_0 (étape E132) de la même

30 manière que lors de l'étape E92 représentée en **figure 7**.

Le serveur DP2 détermine (E134) ensuite au moins une clé temporaire cryptographique par dérivation à partir de la première clé mère OK_0 et d'une donnée temporelle. Comme représenté en **figure 8**, on suppose ici que le serveur DP2 détermine en E134 les clés temporaires cryptographiques OK_0_T5, OK_0_T6 et OK_0_T7 par

35 dérivation à partir de la clé mère OK_0 et de données temporelles respectives. Pour ce faire, le serveur DP2 détermine au préalable les données temporelles puis détermine les clés temporaires OK_0_T5, OK_0_T6 et OK_0_T7 de façon analogue à l'étape E104 représentée en **figure 7**. Chaque donnée temporelle est représentative de la période de

temps (ou fenêtre temporelle) pendant laquelle la clé temporaire correspondante est valide. La donnée temporelle correspondant à chacune des clés temporaires OK_0_T5, OK_0_T6 et OK_0_T7 peut être choisie de façon arbitraire. La période de temps pendant laquelle une clé temporaire est valide peut être fixée à 1 heure ou 1 jour par exemple.

- 5 Comme représenté en **figure 8**, le serveur DP2 envoie (E136) ensuite au terminal T1 un ensemble de données PCK2 comprenant les clés temporaires OK_0_T5, OK_0_T6 et OK_0_T7.

Une fois reçues (E136), le terminal T1 enregistre (E138) ces données dans sa mémoire 34 (**figure 4**).

- 10 Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire des clés temporaires cryptographiques déterminées par double dérivation à partir de la clé maîtresse CMK_0. Ces clés temporaires OK_0_T5, OK_0_T6 et OK_0_T7 peuvent être utilisées par le terminal T1 pour accéder au service SR.
- 15

On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique DP1 (**figure 1**).

- 20 Le dispositif DP1 envoie (E140) alors au terminal T1 une donnée de défi notée c13.

Lors d'une étape E142, le terminal T1 détermine un point courant dans le temps, à savoir dans cet exemple : la date courante et/ou l'heure courante, constituant une donnée temporelle.

- Le terminal T1 sélectionne (E144) alors, en fonction du point courant dans le temps déterminée en E142, une clé applicable parmi les clés temporaires OK_0_T5, OK_0_T6 et OK_0_T7 reçues en E136. Dans cette exemple, on suppose que le terminal T1 détermine, en fonction des date et/ou heure courantes, que la clé temporaire OK_0_T6 est celle à utiliser et sélectionne donc celle-ci au cours de l'étape E144.
- 25

- Lors d'une étape de calcul E146, le terminal T1 génère un code MAC, noté MC16, à partir de la clé temporaire OK_0_T6 sélectionnée en E144 et à partir de la donnée de défi c13 reçue en E140. La génération E146 de ce code MAC MC16 s'effectue de façon analogue au calcul E106 représenté en **figure 7**.
- 30

- Lors d'une étape d'envoi E148, le terminal T1 envoie au dispositif DP1 le code MAC MC16 ainsi que l'identifiant ID1 du terminal T1 et les droits d'accès RG1. Une fois ces données reçues (E148), le dispositif DP1 réalise un traitement (étapes E150-E162) analogue à celui décrit précédemment en référence aux étapes E110-E122 (**figure 7**).
- 35

Plus précisément, lors de l'étape E150, le dispositif DP1 dérive la clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant

ID1 du terminal T1 et des droits d'accès RG1, de façon identique à l'étape E22 (**figure 5**) ou à l'étape E132 (**figure 8**) par exemple.

Le dispositif DP2 détermine (E152) en outre une donnée temporelle, notée ici DT3, représentative d'un point courant dans le temps. Pour ce faire, le dispositif DP2 détermine dans cet exemple la date courante et/ou l'heure courante, et en déduit la donnée temporelle DT3. Dans un exemple particulier, le dispositif DP2 est configuré pour que la donnée temporelle DT3 déterminée en E152 corresponde à une période de temps prédéfinie, c'est-à-dire une fenêtre (ou créneau) temporelle, dans laquelle se situe le point courant dans le temps. Ainsi, la donnée temporelle DT3 peut varier selon la fenêtre temporelle dans laquelle se situe le dispositif DP2 lors de son traitement au cours des étapes E150-E162. La donnée temporelle DT3 est par exemple déterminée de la même façon que la donnée temporelle DT2, comme décrit précédemment en référence à l'étape E112 (**figure 7**).

Le dispositif DP1 dérive (E154) alors la clé temporaire cryptographique OK_0_T6 à partir de la clé mère OK_0 et de la donnée temporelle DT3. Pour ce faire, le dispositif DP1 détermine la clé temporaire OK_0_T6 par dérivation à partir de la clé mère OK_0 et en prenant en entrée la donnée temporelle DT3 déterminée en E152. L'obtention préalable de la donnée temporelle DT3 permet de déterminer la clé temporaire OK_0_T6 qui est en cours de validité au moment du traitement. On suppose dans le cas présent que la donnée temporelle DT3 est ici identique à la donnée temporelle précédemment utilisée en E134 par le serveur DP2 pour obtenir, par dérivation de la clé mère OK_0, la clé temporaire OK_0_T6. Le dispositif DP1 obtient donc ici en E154 la clé temporaire OK_0_T6.

Lors d'une étape E156, le dispositif DP1 génère à son tour un code MAC, noté ici MC17, à partir de la clé temporaire cryptographique OK_0_T6 obtenue en E154 et de la donnée de défi c13 envoyée en E140. Ce code MAC MC17 est obtenu en effectuant le même calcul que celui réalisé par le serveur DP2, lors de l'étape E134, pour déterminer la clé temporaire OK_0_T6.

Le dispositif DP1 compare (E158) ensuite le code MAC MC16 reçu en E148 avec le code MAC MC17 calculé en E156 et détermine si ces deux codes MAC coïncident. Dans cet exemple, le dispositif DP1 vérifie si MC16 et MC17 sont identiques.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E158 entre les codes MAC MC16 et MC17, de façon analogue aux étapes E118-E122 décrites ci-avant en référence à la **figure 7**.

Plus précisément, lors d'une étape E160, le dispositif DP1 détermine à partir du résultat de la comparaison réalisée en E158 si le terminal T1 est autorisé à accéder au service SR selon les droits d'accès RG1. Autrement dit, le dispositif DP1 contrôle l'accès au

service SR en fonction du résultat obtenu en E158 (MC16 = MC17 ?). Ce contrôle peut se concrétiser par une autorisation d'accès ou par un blocage.

Le dispositif DP1 peut également envoyer (E162) au terminal T1 une réponse DEC13 indiquant sa décision concernant la demande d'accès du terminal T1 au service SR.

5 Dans cet exemple, s'il est détecté en E158 que les codes MAC MC16 et MC17 sont identiques, le dispositif DP1 autorise (E160) l'accès au service SR selon les droits d'accès RG1 et envoie (E162) une réponse DEC13 positive au terminal T1. Dans le cas contraire (codes MAC MC16 et MC17 différents), le dispositif DP1 bloque (E160) l'accès du terminal T1 au service SR et envoie (E162) une réponse DEC13 négative pour en informer le
10 terminal T1.

La variante représentée en **figure 8** permet ainsi avantageusement de mettre à profit les ressources disponibles au niveau du système de contrôle SY, et plus précisément ici du serveur DP2, pour déterminer une ou des clés temporaires cryptographiques susceptibles d'être utilisées par le terminal T1 pour accéder au service SR. En outre, cela
15 permet de ne pas diffuser une clé mère cryptographique, au caractère sensible, depuis le système de contrôle SY vers terminal client lorsque ce dernier ne présente pas un niveau de confiance suffisant.

Les modes de réalisation des **figures 7** et **8** sont avantageux en ce qu'il n'est pas nécessaire de déterminer une donnée d'authentification pour chaque clé temporaire
20 cryptographique, comme cela est le cas dans les modes de réalisation des **figures 5** et **6** par exemple, rendant ainsi les traitements moins complexes et plus économes en ressources.

Figure 9 : troisième mode de réalisation

25 Un autre mode de réalisation, proche de celui représenté en **figure 7**, est à présent décrit en référence à la **figure 9**. Plus précisément, le dispositif DP1 et le serveur DP2 mettent collectivement en œuvre un procédé de contrôle en exécutant respectivement les programmes d'ordinateur PG1 et PG2. En parallèle, le terminal T1 met en œuvre un procédé de traitement en exécutant le programme d'ordinateur PG3.

30 Comme décrit ci-après, ce mode de réalisation diffère de celui représenté en **figure 7** en ce qu'une donnée de dérivation DERIV_D est en outre utilisée pour déterminer la ou les clés temporaires cryptographiques.

Dans un premier temps, on suppose que le terminal T1 de l'utilisateur U1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d'enrôlement (étapes E170-
35 E174) de façon identique aux étapes E90-E96 représentées en **figures 7**.

On suppose ici aussi que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque le propriétaire U1 vient de faire l'acquisition de sa voiture SR et configure son

terminal T1 en interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa voiture. D'autres modes de réalisation sont toutefois possibles.

Comme représenté en **figure 9**, le terminal T1 envoie (E170) au serveur DP2, lors de cet enrôlement initial, une requête d'enrôlement comportant l'identifiant ID1 du terminal T1 et, éventuellement, des droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au service SR. Ces droits d'accès RG1 se caractérisent comme déjà décrits ci-avant en référence aux précédents modes de réalisation.

Le serveur DP2 dérive (E172) une première clé mère cryptographique OK_0 à partir de la clé maîtresse CMK_0, de l'identifiant ID1 et des droits d'accès RG1, de façon identique à l'étape E4 représentée en **figure 5** ou à l'étape E92 représentée en **figure 7**.

Le serveur DP2 envoie (E174) ensuite la clé mère cryptographique OK_0, et éventuellement les droits d'accès RG1, au terminal T1.

Une fois reçus (E174), le terminal T1 enregistre (E176) la clé mère OK_0 et les droits d'accès RG1 dans sa mémoire 34 (**figure 4**). Dans un exemple particulier, le premier terminal T1 est un terminal de télécommunications, de type smartphone par exemple, et la mémoire locale 34 est une mémoire sécurisée d'une carte SIM ou d'un module d'identité de souscripteur embarqué (de type eUICC pour « *embedded Universal Integrated Circuit Card* »).

Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire la clé mère OK_0 obtenue par dérivation à partir de la clé maîtresse CMK_0. Cette clé mère OK_0 peut être utilisée par le terminal T1 lors de chaque accès au service SR.

On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique DP1 (**figure 1**).

Le dispositif DP1 envoie (E178) alors au terminal T1 une donnée de défi notée c14.

Lors d'une étape E180, le terminal T1 détermine une donnée temporelle DT5 de façon analogue à l'étape E102 (**figure 7**). Cette donnée temporelle DT5 est représentative de la validité dans le temps d'une clé temporaire cryptographique OK_0_T8 calculée ici en E184. Pour ce faire, le terminal T1 détermine au préalable la donnée temporelle DT5 selon une quelconque manière appropriée.

Plus particulièrement, dans cet exemple de réalisation, le terminal T1 détermine un point courant dans le temps, défini ici par la date courante et/ou l'heure courante. Le terminal T1 détermine alors en E180 la donnée temporelle DT5 en fonction de la date courante et/ou de l'heure courante.

Ce mode de réalisation diffère de celui représenté en **figure 7** en ce que le terminal T1 détermine (E182) en outre une donnée de dérivation DERIV_D et utilise celle-ci lors d'une étape de dérivation E184 pour déterminer la clé temporaire cryptographique OK_0_T8 déjà mentionnée ci-avant.

5 Plus précisément, le terminal T1 sélectionne en E182 une donnée de dérivation DERIV_D selon une quelconque méthode appropriée. Le terminal T1 dérive (E184) ensuite la clé temporaire cryptographique OK_0_T8 à partir de la clé mère OK_0, de la donnée temporelle DT5 obtenue en E180 et la donnée de dérivation DERIV_D obtenue en E182. Autrement dit, la clé temporaire OK_0_T8 est déterminée par dérivation à partir de
10 la clé mère OK_0 et en prenant en entrée la donnée temporelle DT5 et la donnée de dérivation DERIV_D.

La donnée DERIV_D est par exemple choisie (E182) par le terminal T1 en fonction de la donnée temporelle DT5 déterminés en E180 et/ou en fonction d'un historique de clés temporaires générées dans le passé par le terminal T1. Selon un exemple particulier, le
15 terminal T1 peut générer jusqu'à un nombre maximum prédéfini de clés temporaires différentes applicables pour une même une période de temps (ou fenêtre temporelle) prédéterminée. A chaque demande d'accès au service SR, le terminal T1 peut par exemple générer une nouvelle clé temporaire. Dans un exemple particulier, un maximum de n clés temporaires distinctes peuvent être générées successivement par le terminal T1
20 pour accéder à différents moments au service SR dans une période de temps prédéfinie (n = 10, par exemple). L'utilisation d'une telle donnée de dérivation DERIV_D permet donc au terminal T1 de déterminer une nouvelle clé temporaire applicable pour une période de temps prédéfinie à chaque itération de l'étape E184.

Le terminal T1 génère (E186) ensuite un code MAC, noté MC18, à partir de la clé
25 temporaire OK_0_T8 et de la donnée de défi c14, de façon analogue à l'étape E18 (figure 5) ou à l'étape E106 (figure 7) par exemple.

Lors d'une étape d'envoi E188, le terminal T1 envoie au dispositif DP1 le code MAC MC18 ainsi que l'identifiant ID1 du terminal T1, les droits d'accès RG1 et la donnée de dérivation DERIV_D déterminée en E182. Une fois ces données reçues (E188), le dispositif
30 DP1 procède à l'étape E190.

Lors de l'étape E190, le dispositif DP1 dérive la clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant ID1 du terminal T1 et des droits d'accès RG1, de façon identique à l'étape E172, ou encore à l'étape E22 (figure 5) ou à l'étape E92 (figure 7) par exemple.

35 Le dispositif DP2 détermine (E192) en outre, de façon analogue à l'étape E112 (figure 7), une donnée temporelle, notée ici DT6, représentative d'un point courant dans le temps. Pour ce faire, le dispositif DP2 détermine dans cet exemple la date courante et/ou l'heure courante, et en déduit la donnée temporelle DT6. Dans un exemple

particulier, le dispositif DP2 est configuré pour que la donnée temporelle DT6 déterminée en E192 corresponde à une période de temps prédéfinie, c'est-à-dire une fenêtre (ou créneau) temporelle, dans laquelle se situe le point courant dans le temps. Ainsi, la donnée temporelle DT6 peut varier selon la fenêtre temporelle dans laquelle se situe le

5 dispositif DP2 lors de son traitement au cours des étapes E188-E202.

Dans l'exemple considéré ici, on suppose que la donnée temporelle DT6 est identique à la donnée temporelle DT5. Cela peut toutefois ne pas être le cas si le terminal T1 tarde trop longtemps avant d'envoyer au dispositif DP1 son code MAC MC18 en E188 (**figure 9**) ou si le terminal T1 utilise une clé obsolète en E184.

10 Le dispositif DP1 dérive (E194) alors la clé temporaire cryptographique OK_0_T8 à partir de la clé mère OK_0, de la donnée temporelle DT6 et de la donnée de dérivation DERIV_D. Autrement dit, le dispositif DP1 détermine la clé temporaire OK_0_T8 par dérivation à partir de la clé mère OK_0 et en prenant en entrée la donnée temporelle DT6 déterminée en E192 et de la donnée de dérivation DERIV_D reçue en E188. L'obtention

15 préalable de la donnée temporelle DT6 et de la donnée de dérivation DERIV_D permet ainsi de déterminer la clé temporaire OK_0_T6 qui est en cours de validité au moment du traitement.

Selon un exemple particulier, on fixe auprès du système de contrôle SY une durée de validité prédéfinie pour chaque clé temporaire. Cette durée de validité est fixée à 1 heure par exemple. Les données temporelles associées à chacune des clés temporaires correspondent à des heures fixes pleines, par exemple les heures « 13h00 », « 14h00 », « 15h00 »... Ainsi, toutes les heures, une nouvelle clé temporaire est valable pendant 1

20 heure. Le système de contrôle SY vérifie ainsi de la manière suivante : il regarde quelle heure il est en E192 et en déduit la valeur de la donnée temporelle DT6. Si l'heure courante est « 13h45 », il en déduit que la donnée temporelle DT6 correspond à l'heure de « 13h00 ». Selon une variante, la valeur de la donnée temporelle DT6 pourrait être également envoyée par le terminal T1, et le système de contrôle SY vérifie que cette date

25 et/ou heure n'a pas expirée par rapport à la durée de validité fixée.

Lors d'une étape de calcul E196 (**figure 9**), le dispositif DP1 génère à son tour un

30 code MAC, noté ici MC19, à partir de la clé temporaire cryptographique OK_0_T8 obtenue en E194 et de la donnée de défi c14 envoyé en E178. Ce code MAC MC19 est obtenu en effectuant le même calcul que lors de l'étape de calcul E186 réalisée par le terminal T1.

Le dispositif DP1 compare (E198) ensuite le code MAC MC18 reçu en E188 avec le code MAC MC19 calculé en E196 et détermine si ces deux codes MAC coïncident. Dans cet

35 exemple, le dispositif DP1 vérifie si MC18 et MC19 sont identiques.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E198 entre les codes MAC MC18 et MC19, de façon

analogue aux étapes E34-E38 (**figure 5**) ou aux étapes E118-E122 (**figure 7**) par exemple.

Plus précisément, lors d'une étape E200, le dispositif DP1 détermine à partir du résultat de la comparaison réalisée en E198 si le terminal T1 est autorisé à accéder au service SR selon les droits d'accès RG1. Autrement dit, le dispositif DP1 contrôle l'accès au service SR en fonction du résultat obtenu en E198 (MC18 = MC19 ?). Ce contrôle peut se concrétiser par une autorisation d'accès ou par un blocage.

Le dispositif DP1 peut également envoyer (E202) au terminal T1 une réponse DEC14 indiquant sa décision concernant la demande d'accès du terminal T1 au service SR.

Dans cet exemple, s'il est détecté en E198 que les codes MAC MC18 et MC19 sont identiques, le dispositif DP1 autorise (E200) l'accès au service SR selon les droits d'accès RG1 et envoie (E202) une réponse DEC14 positive au terminal T1. Dans le cas contraire (codes MAC MC18 et MC19 différents), le dispositif DP1 bloque (E200) l'accès du terminal T1 au service SR et envoie (E202) une réponse DEC14 négative pour en informer le terminal T1.

Comme décrit précédemment, l'utilisation d'une donnée de dérivation DERIV_D lors des étapes E184 et E194 (**figure 9**) permet avantageusement de générer plusieurs clés temporaires cryptographiques applicables pour une période de temps prédéfinie. Ainsi, le terminal T1 peut générer et utiliser une nouvelle clé temporaire cryptographique à chaque fois qu'il demande l'accès au service SR dans une période de temps prédéfinie. Il est de ce fait plus difficile pour un tiers malveillant de déterminer la clé temporaire applicable à un instant donné, ce qui sécurise encore d'avantage l'accès au service considéré.

Figure 10 : variante du troisième mode de réalisation

Dans le mode de réalisation représenté en **figure 9**, l'envoi E174 de la clé mère cryptographique OK_0 suppose toutefois que le terminal T1 soit un terminal de confiance. En particulier, on optera de préférence pour ce mode de réalisation si le terminal T1 dispose d'une mémoire suffisamment sécurisée pour stocker la clé mère OK_0.

Une variante du mode de réalisation de la **figure 9** est à présent décrite en référence à la **figure 10**. On suppose ici que le terminal T1 ne présente pas le niveau de confiance requis pour recevoir et stocker en sécurité la clé mère cryptographique OK_0. C'est le cas par exemple lorsque le terminal T1 ne contient pas d'élément sécurisé tel qu'une carte SIM ou un module eUICC. Aussi, cette variante diffère du mode de réalisation de la **figure 9** en que le serveur DP2 ne fournit pas la clé mère OK_0 au terminal T1 mais fournit directement à celui-ci une ou une pluralité de clés temporaires cryptographiques, de sorte à permettre au terminal T1 d'accéder ensuite au service SR considéré. Le serveur DP2 détermine chaque clé temporaire de la même manière que la clé temporaire

OK_0_T8 déterminée par le terminal T1 dans le mode de réalisation de la **figure 9** (étape E184).

Plus particulièrement, comme représenté en **figure 10**, le terminal T1 et le serveur DP2 coopèrent ensemble pour réaliser une phase dite d'enrôlement (étapes E210-E216).

5 On suppose ici que cet enrôlement ne se produit qu'une seule fois, par exemple lorsque l'utilisateur U1 vient de faire l'acquisition de sa voiture SR et configure son terminal T1 en interagissant avec le serveur DP2 afin de pouvoir accéder par la suite librement à sa voiture. D'autres modes de réalisation sont toutefois possibles.

10 Lors de cet enrôlement initial, le terminal T1 envoie (E210) au serveur DP2 une requête d'enrôlement de façon identique à l'étape E2 représentée en **figure 5** ou encore à l'étape E170 représentée en **figure 9**. Cette requête d'enrôlement comporte l'identifiant ID1 du terminal T1 et, éventuellement, des droits d'accès RG1 représentatifs des droits que requière l'utilisateur U1 pour accéder au service SR. Ces droits d'accès RG1 se caractérisent de la même manière que décrit dans les modes de réalisation précédents.

15 Le serveur DP2 reçoit (E210) la requête d'enrôlement en provenance du terminal T1 puis détermine une première clé mère cryptographique OK_0 (étape E212) de façon identique à l'étape E4 représentée en **figure 5** ou encore à l'étape E172 représentée en **figure 9**.

20 Le serveur DP2 détermine (E214) ensuite au moins une clé temporaire cryptographique par dérivation à partir de la première clé mère OK_0, d'une donnée temporelle et d'une donnée de dérivation. Comme représenté en **figure 10**, on suppose ici que le serveur DP2 détermine en E214 les clés temporaires cryptographiques suivantes :

- 25 - les clés temporaires OK_0_T81 et OK_0_T82 applicables pendant une première période de temps prédéfinie ;
- les clés temporaires OK_0_T91 et OK_0_T92 applicables pendant une deuxième période de temps prédéfinie ;
- les clés temporaires OK_0_T101 et OK_0_T102 applicables pendant une troisième période de temps prédéfinie.

30 Chacune de ces clés temporaires OK_0_T81, OK_0_T82, OK_0_T91, OK_0_T92, OK_0_T101 et OK_0_T102 est déterminée par le serveur DP2 par dérivation à partir de la clé mère OK_0, d'une donnée temporelle respective et d'une donnée de dérivation respective. Pour ce faire, le serveur DP2 détermine au préalable les données temporelles et les données de dérivation puis détermine les clés temporaires listées ci-dessus de façon analogue à l'étape E184 représentée en **figure 9**.

35 Comme représenté en **figure 10**, le serveur DP2 envoie (E216) ensuite au terminal T1 un ensemble de données PCK3 comprenant les clés temporaires OK_0_T81, OK_0_T82, OK_0_T91, OK_0_T92, OK_0_T101 et OK_0_T102 déterminées à l'étape

E214. Dans l'exemple considéré ici, le serveur DP2 ne fournit au terminal T1 ni les données temporelles ni les données de dérivation correspondant aux clés temporaires transmises, ce qui permet de renforcer la sécurité du contrôle d'accès au service SR.

Une fois reçues (E216), le terminal T1 enregistre (E218) les données PCK3 dans sa
 5 mémoire 34 (**figure 4**).

Le terminal T1 est ainsi enrôlé auprès du serveur DP2, et plus généralement du système de contrôle SY, dans le sens où le terminal T1 s'est identifié auprès du serveur DP2 et détient à présent en mémoire des clés temporaires cryptographiques déterminées par double dérivation à partir de la clé maîtresse CMK_0. Ces clés temporaires OK_0_T81,
 10 OK_0_T82 etc. peuvent être utilisées par le terminal T1 pour accéder au service SR.

On suppose que l'utilisateur U1 souhaite à présent accéder au service SR considéré. Pour ce faire, l'utilisateur U1 positionne par exemple son terminal T1 à proximité de sa voiture SR de sorte à ce que le terminal T1 puisse coopérer avec le dispositif électronique DP1 (**figure 1**).

15 Le dispositif DP1 envoie (E220) alors au terminal T1 une donnée de défi notée c15.

Lors d'une étape E222, le terminal T1 détermine un point courant dans le temps, à savoir dans cet exemple : la date courante et/ou l'heure courante, constituant une donnée temporelle.

Le terminal T1 sélectionne (E224) alors, en fonction du point courant dans le temps
 20 déterminée en E222, une clé applicable parmi les clés temporaires reçues en E216 dans les données PCK3. Dans cette exemple, on suppose que le terminal T1 détermine, en fonction de la date courante et/ou de l'heure courante, que la clé temporaire OK_0_T91 doit être utilisée et sélectionne donc celle-ci au cours de l'étape E224.

Lors d'une étape de calcul E226, le terminal T1 génère un code MAC, noté MC20, à
 25 partir de la clé temporaire OK_0_T91 sélectionnée en E224 et à partir de la donnée de défi c15 reçue en E220. La génération E226 de ce code MAC MC20 s'effectue de façon analogue à l'étape E18 (**figure 5**) ou à l'étape E186 (**figure 9**) par exemple.

Lors d'une étape d'envoi E228, le terminal T1 envoie au dispositif DP1 le code MAC MC20, l'identifiant ID1 du terminal T1, les droits d'accès RG1 ainsi qu'une donnée de
 30 dérivation DERIV_D correspondant à la clé temporaire cryptographique OK_0_91 sélectionnée en E224. Une fois ces données reçues (E228), le dispositif DP1 réalise les étapes E230-E242 décrites ci-après.

Plus précisément, lors de l'étape E230, le dispositif DP1 dérive la clé mère cryptographique OK_0 à partir de la clé maîtresse cryptographique CMK_0, de l'identifiant
 35 ID1 du terminal T1 et des droits d'accès RG1, de façon identique à l'étape E212 (**figure 10**), à l'étape E22 (**figure 5**) ou encore à l'étape E190 (**figure 9**) par exemple.

Le dispositif DP2 détermine (E232) en outre une donnée temporelle, notée ici DT8, représentative d'un point courant dans le temps. Pour ce faire, le dispositif DP2 détermine

dans cet exemple la date courante et/ou l'heure courante, et en déduit la donnée temporelle DT8. Dans un exemple particulier, le dispositif DP2 est configuré pour que la donnée temporelle DT8 déterminée en E232 corresponde à une période de temps prédéfinie, c'est-à-dire une fenêtre (ou créneau) temporelle, dans laquelle se situe le point courant dans le temps. Ainsi, la donnée temporelle DT8 peut varier selon la fenêtre temporelle dans laquelle se situe le dispositif DP2 lors de son traitement au cours des étapes E230-E242. La donnée temporelle DT8 est par exemple déterminée de la même façon que la donnée temporelle DT6, comme décrit précédemment en référence à l'étape E192 (**figure 7**).

Le dispositif DP1 dérive (E234) alors la clé temporaire cryptographique OK_0_T91 à partir de la clé mère OK_0, de la donnée temporelle DT8 et de la donnée de dérivation DERIV_D. Pour ce faire, le dispositif DP1 détermine la clé temporaire OK_0_T91 par dérivation à partir de la clé mère OK_0 et en prenant en entrée la donnée temporelle DT8 déterminée en E232 et la donnée de dérivation DERIV_D reçue en E228. L'obtention préalable de la donnée temporelle DT8 permet de déterminer la clé temporaire qui est en cours de validité au moment du traitement. On suppose que le dispositif DP1 obtient ici en E234 la clé temporaire OK_0_T91 dans la mesure où le terminal T1 a transmis suffisamment rapidement son code MAC MC20 (E228) au dispositif DP1.

Lors d'une étape E236, le dispositif DP1 génère à son tour un code MAC, noté ici MC21, à partir de la clé temporaire cryptographique OK_0_T91 obtenue en E234 et de la donnée de défi c15 envoyée en E220. Ce code MAC MC21 est obtenu en effectuant le même calcul que celui réalisé par le serveur DP2, lors de l'étape E214, pour déterminer la clé temporaire OK_0_T91.

Le dispositif DP1 compare (E238) ensuite le code MAC MC20 reçu en E228 avec le code MAC MC21 calculé en E236 et détermine si ces deux codes MAC coïncident. Dans cet exemple, le dispositif DP1 vérifie si MC20 et MC21 sont identiques.

Le dispositif DP1 gère ensuite l'accès du terminal T1 au service SR à partir du résultat de la comparaison effectuée en E238 entre les codes MAC MC20 et MC21, de façon analogue aux étapes E34-E38 représentées en **figure 5** ou aux étapes E198-E202 représentées en **figure 9**.

Plus précisément, lors d'une étape E240, le dispositif DP1 détermine à partir du résultat de la comparaison réalisée en E238 si le terminal T1 est autorisé à accéder au service SR selon les droits d'accès RG1. Autrement dit, le dispositif DP1 contrôle l'accès au service SR en fonction du résultat obtenu en E238 (MC20 = MC21 ?). Ce contrôle peut se concrétiser par une autorisation d'accès ou par un blocage. Pour ce faire, le dispositif DP1 peut si besoin se reporter à une base de données dans laquelle est enregistré l'identifiant de chaque utilisateur et les droits d'accès associés.

Le dispositif DP1 peut également envoyer (E242) au terminal T1 une réponse DEC15 indiquant sa décision concernant la demande d'accès du terminal T1 au service SR.

Dans cet exemple, s'il est détecté en E238 que les codes MAC MC20 et MC21 sont identiques, le dispositif DP1 autorise (E240) l'accès au service SR selon les droits d'accès
5 RG1 et envoie (E242) une réponse DEC15 positive au terminal T1. Dans le cas contraire (codes MAC MC20 et MC21 différents), le dispositif DP1 bloque (E240) l'accès du terminal T1 au service SR et envoie (E242) une réponse DEC15 négative pour en informer le terminal T1.

10 A noter que, dans les différents modes de réalisation et variantes décrits ci-avant, l'ordre dans lequel sont réalisées les différentes étapes n'est pas limitatif, d'autres séquences d'exécution des étapes étant possibles dans le cadre de l'invention.

Selon une variante de réalisation, le dispositif DP1 et le serveur DP2 forment un seul et même dispositif. Dans ce cas, le système de contrôle peut stocker notamment la clé
15 mère OK_0 de sorte qu'il ne soit pas nécessaire de la recalculer ultérieurement (lors des étapes E22, E70, E110, E150, E190 et E230, par exemple). Cette variante s'applique à tous les modes de réalisation et variantes décrits ci-avant.

Dans les modes de réalisation et variantes décrits ci-avant, les codes MAC générés par le terminal client T1, ainsi que par le système de contrôle SY, sont obtenus à partir
20 d'une clé cryptographique et d'une donnée de défi. Selon une variante, le calcul de chaque code MAC peut prendre également en entrée une donnée additionnelle (ou donnée d'information), dont la nature et le format peuvent être adaptés selon le cas. Cette donnée additionnelle peut par exemple spécifier les fonctionnalités (ou actions) que l'utilisateur est autorisé à exécuter en lien avec le service SR considéré (ouvrir le véhicule
25 avec droit de démarrage, ouvrir le coffre seulement...).

Un homme du métier comprendra que les modes de réalisation et variantes décrits ci-avant ne constituent que des exemples non limitatifs de mise en œuvre de l'invention. En particulier, l'homme du métier pourra envisager une quelconque adaptation ou combinaison des modes de réalisation et variantes décrits ci-avant afin de répondre à un
30 besoin bien particulier.

REVENDEICATIONS

- 5 1. Procédé de contrôle, mis en œuvre par un système de contrôle (SY), pour contrôler l'accès à un service (SR), le procédé comprenant les étapes suivantes :
- envoi d'une première donnée de défi (c10-c15) à un premier terminal (T1) ;
 - réception, en réponse audit envoi, d'un premier code MAC (MC10 ; MC12 ; MC14 ; MC16 ; MC18 ; MC20) généré par le premier terminal accompagné d'un
- 10 identifiant (ID1) du premier terminal et de premiers droits d'accès (RG1) pour accéder au service ;
- dérivation d'une première clé mère cryptographique (OK_0) à partir d'une clé maîtresse cryptographique (CMK_0), de l'identifiant du premier terminal et des premiers droits d'accès ;
- 15 - dérivation d'une première clé temporaire cryptographique (OK_0_T1 ; OK_0_T2 ; OK_0_T5 ; OK_0_T6 ; OK_0_T8 ; OK_0_T91) à partir de la première clé mère cryptographique (OK_0) ;
- génération d'un deuxième code MAC (MC11 ; MC13 ; MC15 ; MC17 ; MC19 ; MC21) à partir de la première clé temporaire cryptographique et de la première
- 20 donnée de défi (c1) ; et
- gestion de l'accès du premier terminal au service à partir d'une comparaison des premier et deuxième codes MAC.
- 25 2. Procédé selon la revendication 1, dans lequel, au cours de l'étape de gestion d'accès, le système de contrôle autorise l'accès du premier terminal (T1) au service (SR) selon les premiers droits d'accès (RG1) seulement s'il est déterminé lors de ladite comparaison que les premier et deuxième codes MAC coïncident.
- 30 3. Procédé selon la revendication 1 ou 2, dans lequel la première clé temporaire cryptographique est dérivée de sorte qu'elle ne soit considérée comme valide par le système de contrôle que pour une période de temps prédéfinie.
- 35 4. Procédé selon l'une quelconque des revendications 1 à 3, comprenant, préalablement à l'envoi de la première donnée de défi (c1), un enrôlement comprenant les étapes suivantes :
- réception, en provenance du premier terminal (T1), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ;

- dérivation de la première clé mère cryptographique (OK_0) à partir de la clé maîtresse cryptographique (CMK_0), de l'identifiant du premier terminal et des premiers droits d'accès ; et
 - envoi, au premier terminal, de la première clé mère cryptographique (OK_0) de sorte à permettre au premier terminal d'accéder au service (SR) selon les premiers droits si les premier et deuxième codes MAC coïncident.
- 5
5. Procédé selon l'une quelconque des revendications 1 à 4, comprenant :
- réception en provenance du premier terminal (T1), en réponse à l'envoi de la première donnée de défi (c10 ; c11), d'une donnée de dérivation (DERIV_D), d'une donnée temporelle (TIME_V) indiquant la validité dans le temps du premier code MAC (MC10) reçu, et d'une donnée d'authentification (AUTH_D1 ; AUTH_D2) du premier code MAC (MC10) reçu ;
 - génération d'un code MAC additionnel à partir d'une clé mère cryptographique (OK_0 ; OK_0bis) dérivée de la clé maîtresse cryptographique (CMK_0) et à partir de la donnée de dérivation (DERIV_D1 ; DERIV_D2) et de la donnée temporelle (TIME_V) ;
 - vérification que le code MAC additionnel coïncide avec la donnée d'authentification (AUTH_D1 ; AUTH_D2) reçue ; et
 - dans l'affirmative, détermination de la première clé temporaire cryptographique (OK_0_T1 ; OK_0_T2) par dérivation à partir de la première clé mère cryptographique (OK_0) et de la donnée de dérivation (DERIV_D1 ; DERIV_D2).
- 10
- 15
- 20
6. Procédé selon la revendication 5, comprenant, préalablement à l'envoi de la première donnée de défi (c11), un enrôlement comprenant les étapes suivantes :
- réception, en provenance du premier terminal (T1), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ;
 - dérivation de la première clé mère cryptographique (OK_0) à partir de la clé maîtresse cryptographique (CMK_0), de l'identifiant du premier terminal et des premiers droits d'accès ;
 - dérivation (E56) de la clé première temporaire cryptographique (OK_0_T2) à partir de la première clé mère cryptographique (OK_0) et de la donnée de dérivation (DERIV_D) ;
 - détermination (E56) de la donnée d'authentification (AUTH_D2) en calculant un code MAC à partir d'une clé mère cryptographique (OK_0 ; OK_0bis) dérivée de la clé maîtresse cryptographique (CMK_0) et à partir de la donnée de dérivation (DERIV_D) et de la donnée temporelle (TIME_V) ;
- 25
- 30
- 35

- envoi (E58), au premier terminal, de la première clé temporaire cryptographique (OK_0_T2) et de la donnée d'authentification (AUTH_D2) de sorte à permettre au premier terminal d'accéder au service (SR) selon les premiers droits d'accès si les premier et deuxième codes MAC coïncident.

5

7. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel la première clé temporaire cryptographique (OK_0_T5 ; OK_0_T6) est dérivée à partir de la première clé mère cryptographique (OK_0) et d'une donnée temporelle (DT2 ; DT3 ; DT6 ; DT8).

10

8. Procédé selon la revendication 7, dans lequel la donnée temporelle (DT2) est une donnée déterminée à partir d'un point courant dans le temps, la donnée temporelle définissant une durée de temps pendant laquelle la première clé temporaire cryptographique est valide.

15

9. Procédé selon la revendication 7 ou 8, comprenant, préalablement à l'envoi de la première donnée de défi (c13), un enrôlement comprenant les étapes suivantes :

- réception, en provenance du premier terminal (T1), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ;
- dérivation de la première clé mère cryptographique (OK_0) à partir de la clé maîtresse cryptographique (CMK_0), de l'identifiant du premier terminal et des premiers droits d'accès ;
- dérivation de la première clé temporaire cryptographique (OK_0_T6) à partir de la première clé mère cryptographique (OK_0) et d'une donnée temporelle ;
- envoi, au premier terminal, de la première clé temporaire cryptographique (OK_0_T6) de sorte à permettre au premier terminal d'accéder au service (SR) selon les premiers droits si les premier et deuxième codes MAC coïncident.

20

25

10. Procédé selon l'une quelconque des revendications 7 à 9 dans lequel la première clé temporaire cryptographique (OK_0_T8 ; OK_0_T91) est déterminée par dérivation à partir de la première clé mère cryptographique (OK_0), de la donnée temporelle (DT6 ; DT8) et d'une donnée de dérivation (DERIV_D) correspondant à ladite première clé temporaire cryptographique parmi une pluralité de clés temporaires cryptographique susceptibles d'être obtenues par dérivation à partir de la première clé mère cryptographique (OK_0) et de ladite donnée temporelle (DT6 ; DT8) ;

ladite donnée de dérivation (DERIV_D) étant reçue du premier terminal (T1) en réponse de l'envoi de la première donnée de défi (c14 ; c15).

30

35

11. Procédé selon la revendication 10, comprenant, préalablement à l'envoi de la première donnée de défi (c15), un enrôlement comprenant les étapes suivantes :

- réception, en provenance du premier terminal (T1), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ;
- dérivation de la première clé mère cryptographique (OK_0) à partir de la clé maîtresse cryptographique (CMK_0), de l'identifiant du premier terminal et des premiers droits d'accès ;
- dérivation de la première clé temporaire cryptographique (OK_0_T91) à partir de la première clé mère cryptographique (OK_0), de la donnée temporelle (DT8) et de la donnée dérivation (DERIV_D) ; et
- envoi, au premier terminal, de la première clé temporaire cryptographique (OK_0_T91) de sorte à permettre au premier terminal d'accéder au service (SR) selon les premiers droits si les premier et deuxième codes MAC coïncident.

12. Procédé de traitement, mis en œuvre par un premier terminal (T1), pour accéder à un service (SR) dont l'accès est contrôlé par un système de contrôle (SY), comprenant :

- réception d'une donnée de défi (c10-c15) en provenance du système de contrôle ;
- génération d'un premier code MAC (MC10 ; MC12 ; MC14 ; MC16 ; MC18 ; MC20) à partir de la donnée de défi et à partir d'une première clé temporaire cryptographique (OK_0_T1 ; OK_0_T2 ; OK_0_T5 ; OK_0_T6 ; OK_0_T8 ; OK_0_T91) dérivée d'une première clé mère cryptographique (OK_0) ; et
- envoi, au système de contrôle, du premier code MAC accompagné d'un identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1), de sorte à permettre au système de contrôle de contrôler si le premier terminal est autorisé à accéder au service selon les premiers droits d'accès.

13. Procédé selon la revendication 12, comprenant, en réponse à l'envoi du premier code MAC, la réception d'une réponse du système de contrôle (SY) indiquant si le premier terminal T1 est autorisé à accéder au service selon les premiers droits d'accès.

14. Procédé selon la revendication 12 ou 13, comprenant, préalablement à la génération du premier code MAC, un enrôlement comprenant :

- envoi, au système de contrôle (SY), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ; et
- réception, en provenance du système de contrôle, de la première clé mère cryptographique (OK_0) dérivée à partir d'une clé maîtresse cryptographique

(CMK_0), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) ; et

- dérivation de la première clé temporaire cryptographique (OK_0_T1 ; OK_0_T5 ; OK_0_T8) à partir de la première clé mère cryptographique (OK_0).

5

15. Procédé selon la revendication 14, comprenant, préalablement à la génération du premier code MAC :

- détermination d'une donnée temporelle (TIME_V) et d'une donnée de dérivation (DERIV_D), la donnée temporelle étant représentative de la validité dans le temps du premier code MAC (MC10) ;

10

- détermination d'une donnée d'authentification (AUTH_D1) du premier code MAC (MC10) en calculant un code MAC à partir d'une clé mère cryptographique (OK_0 ; OK_0bis) dérivée de la clé maîtresse cryptographique (CMK_0) et à partir de la donnée de dérivation (DERIV_D) et de la donnée temporelle (TIME_V) ;

15

la première clé temporaire cryptographique (OK_0_T1) étant dérivée à partir de la première clé mère cryptographique (OK_0) et de la donnée de dérivation (DERIV_D) ; et

- envoi au système de contrôle, en réponse à la donnée de défi (C10), de la donnée temporelle (TIME_V), de la donnée de dérivation (DERIV_D) et de la donnée d'authentification (AUTH_D1).

20

16. Procédé selon la revendication 15, comprenant, préalablement à la génération du premier code MAC, la réception, en provenance du système de contrôle, d'une deuxième clé mère cryptographique (OK_0_bis1), différente de la première clé mère cryptographique (OK_0), dérivée à partir de la clé maîtresse cryptographique (CMK_0), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) ;

25

dans lequel la donnée d'authentification (AUTH_D1) est déterminée en tant que code MAC à partir de la deuxième clé mère cryptographique (OK_0_bis1), de la donnée de dérivation (DERIV_D) et de la donnée temporelle (TIME_V).

30

17. Procédé selon la revendication 14, comprenant, préalablement à la génération du premier code MAC, la détermination d'une donnée temporelle (DT1 ; DT5) ;

la première clé temporaire cryptographique (OK_0_T5) étant dérivée à partir de la première clé mère cryptographique (OK_0) et de la donnée temporelle (DT1).

35

18. Procédé selon la revendication 17, dans lequel la première clé temporaire cryptographique (OK_0_T8) est déterminée par dérivation à partir de la première clé mère

cryptographique (OK_0), de la première donnée temporelle (DT5) et d'une donnée de dérivation (DERIV_DATA) correspondant à ladite première clé temporaire cryptographique parmi une pluralité de clés temporaires cryptographique susceptibles d'être obtenues par dérivation à partir de la première clé mère cryptographique (OK_0) et de la première donnée temporelle (DT5),

le procédé comprenant un envoi de la donnée de dérivation (DERIV_DATA) au système de contrôle en réponse à la donnée de défi (c14).

19. Procédé selon la revendication 12 ou 13, comprenant, préalablement à la génération du premier code MAC, un enrôlement comprenant :

- envoi, au système de contrôle (SY), de l'identifiant (ID1) du premier terminal et des premiers droits d'accès (RG1) pour accéder au service ; et
- réception, en provenance du système de contrôle, de la première clé temporaire cryptographique (OK_0_T2 ; OK_0_T6 ; OK_0_T91).

20. Procédé selon la revendication 19, dans lequel, lors dudit enrôlement, le premier terminal (T1) reçoit une pluralité de clés temporaires cryptographiques (OK_0_T1-OK_0_T3 ; OK_0_T5-OK_0_T7 ; OK_0_T81-OK_0_T102),

le procédé comprenant une étape de sélection, parmi les clés temporaires cryptographiques reçues, d'une clé en tant que première clé temporaire cryptographique.

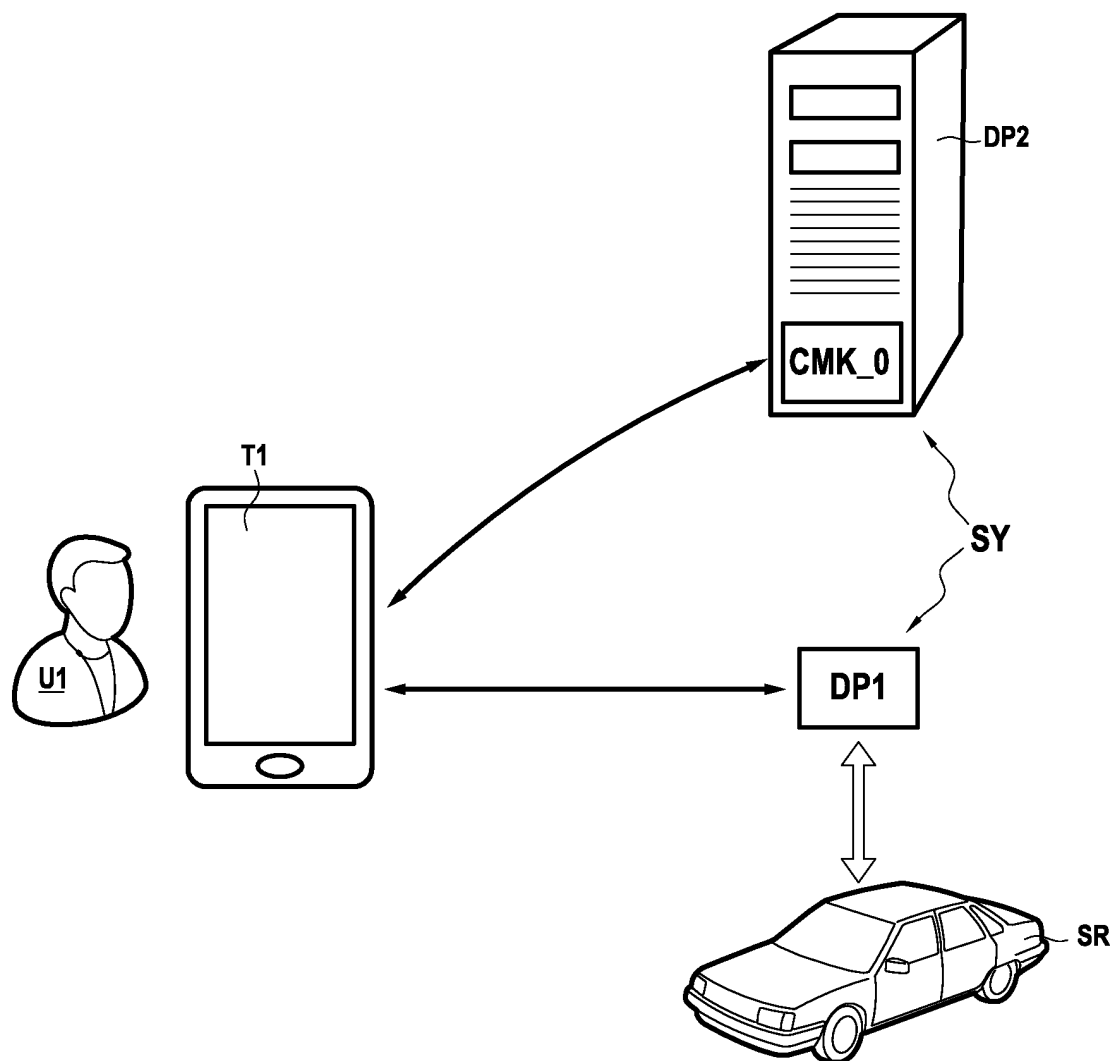


FIG.1

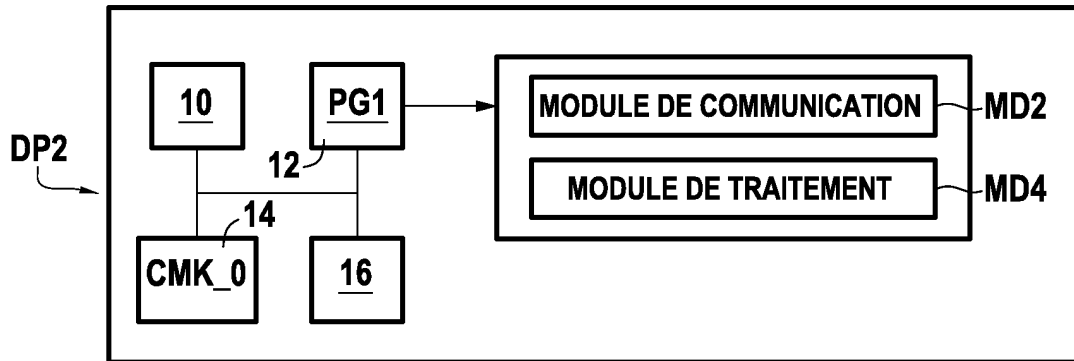


FIG.2

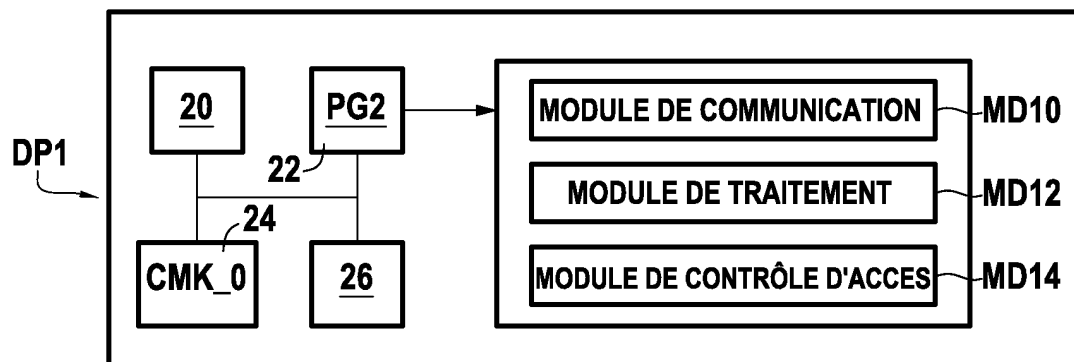


FIG.3

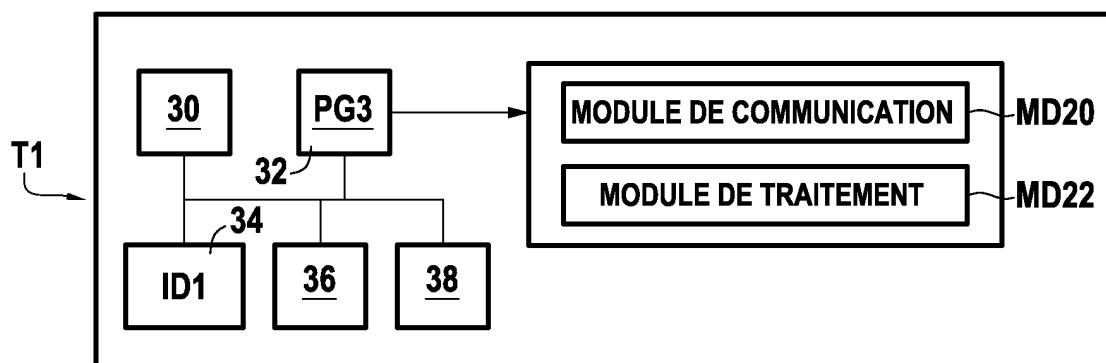
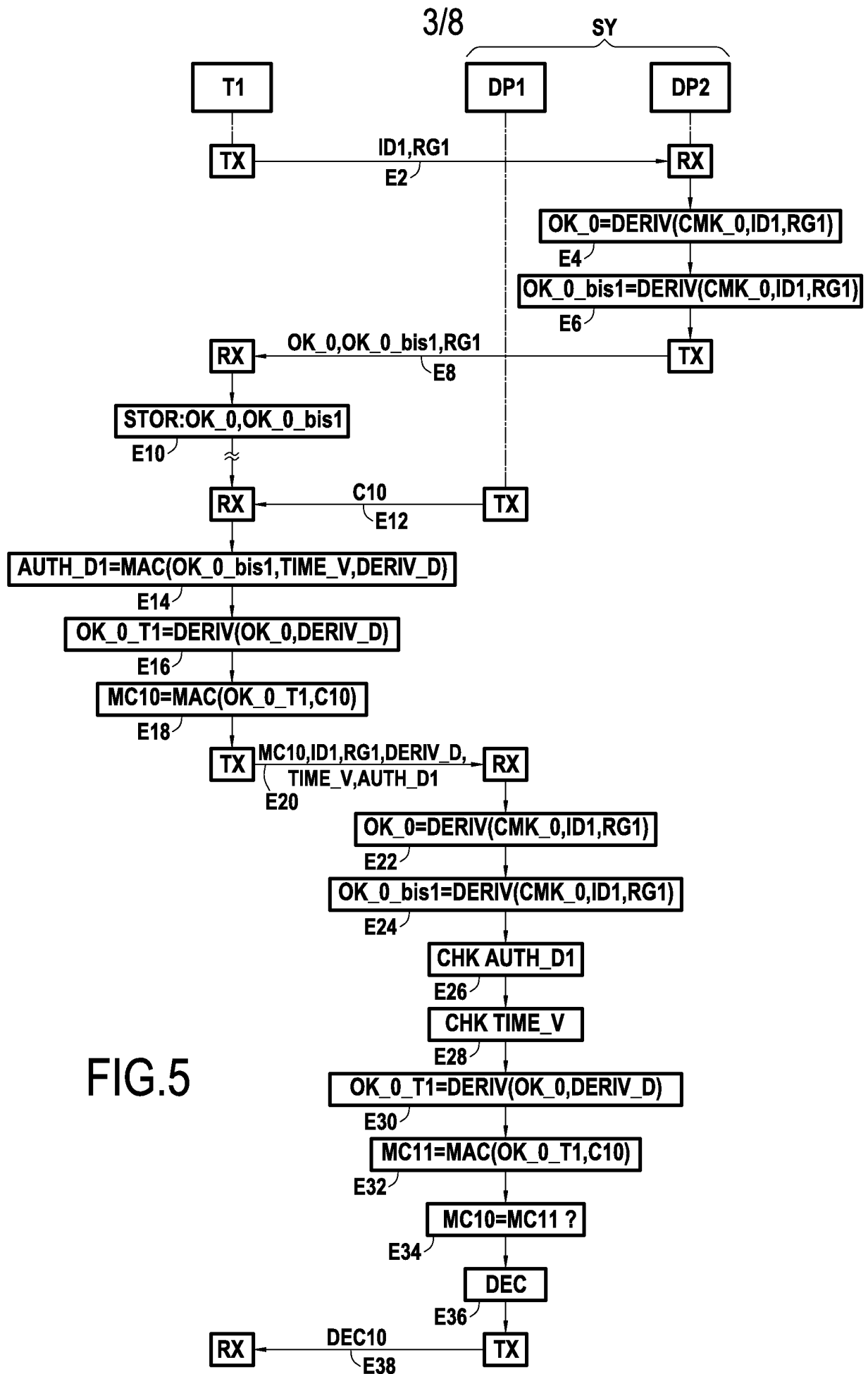
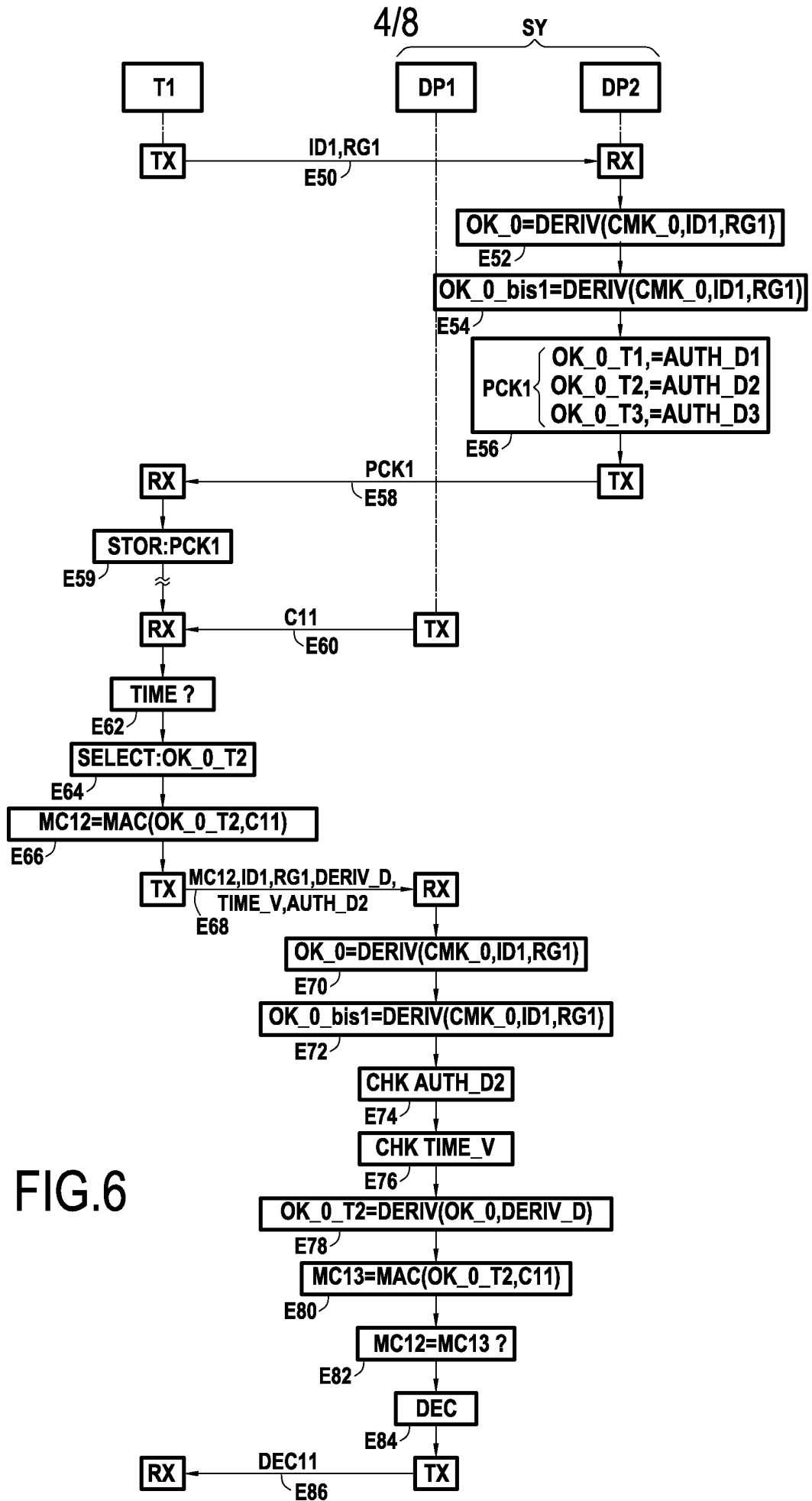


FIG.4





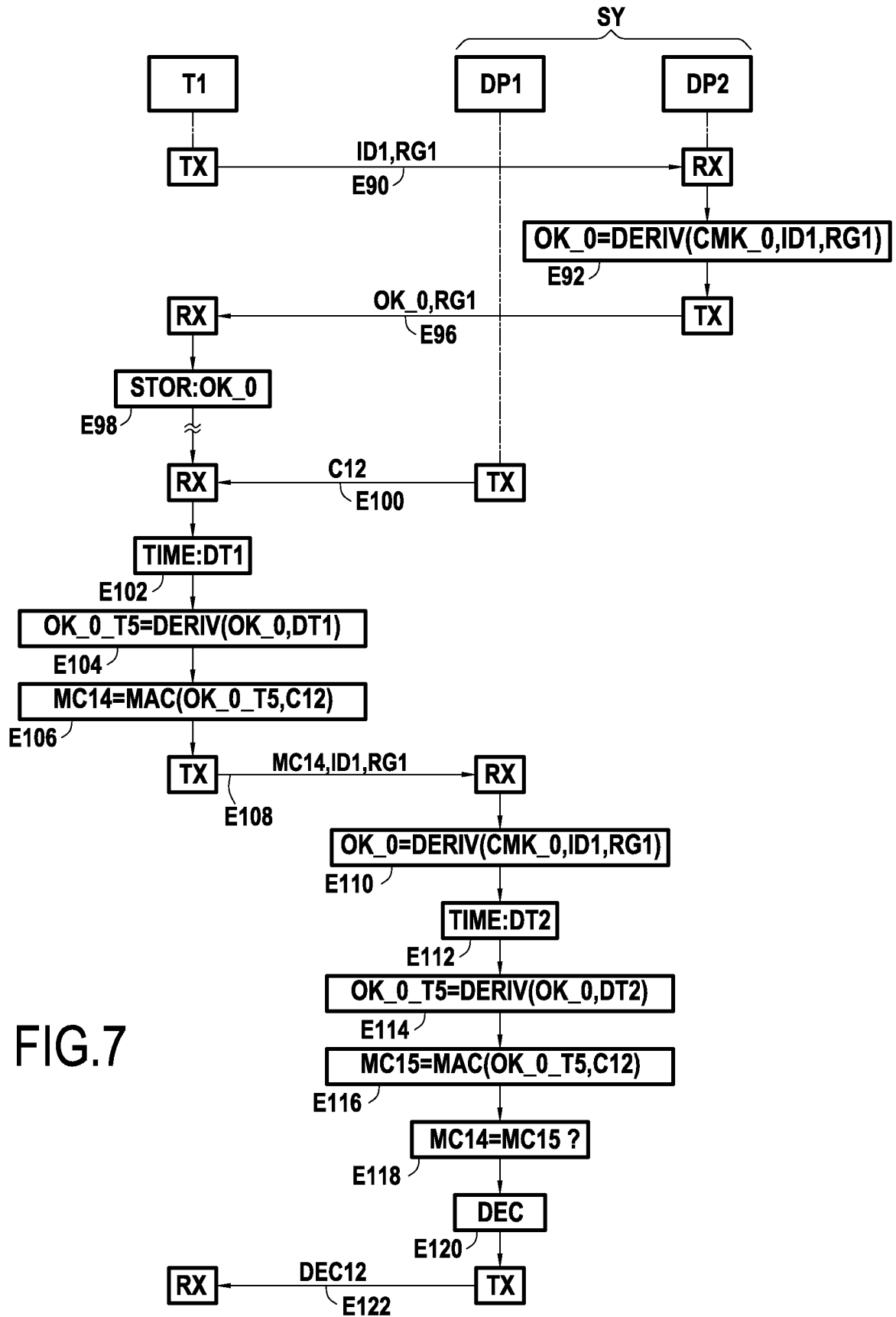


FIG.7

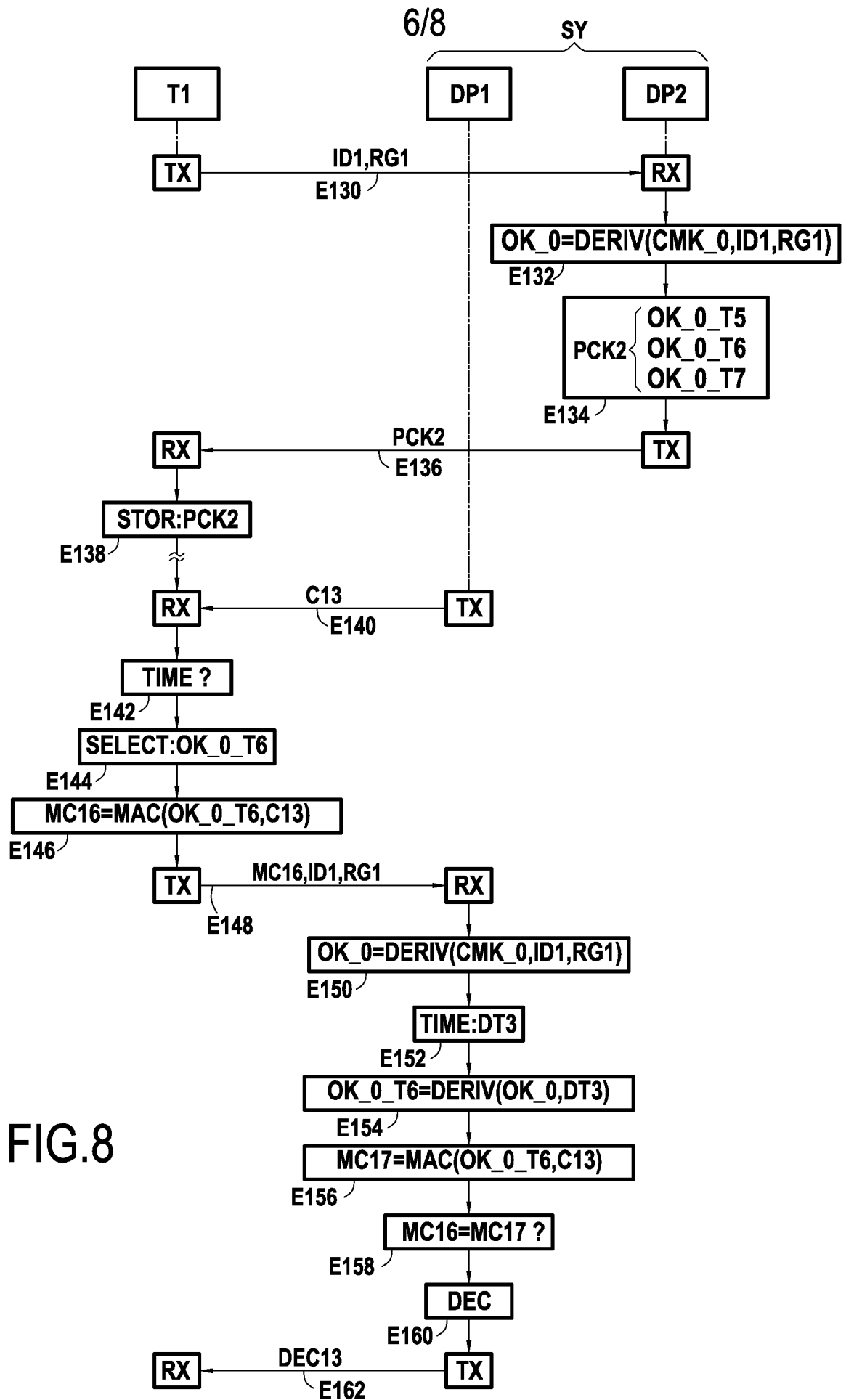
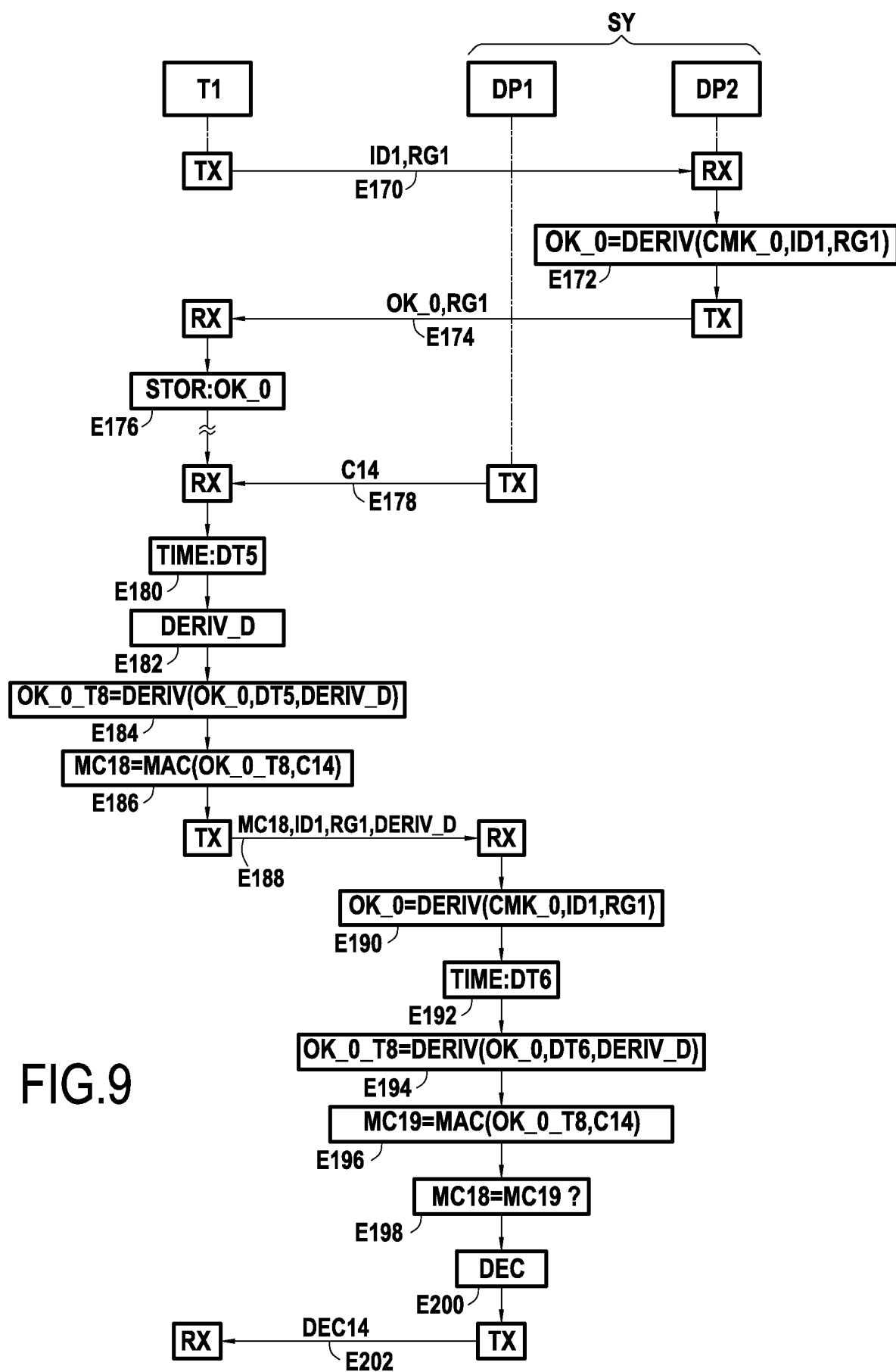
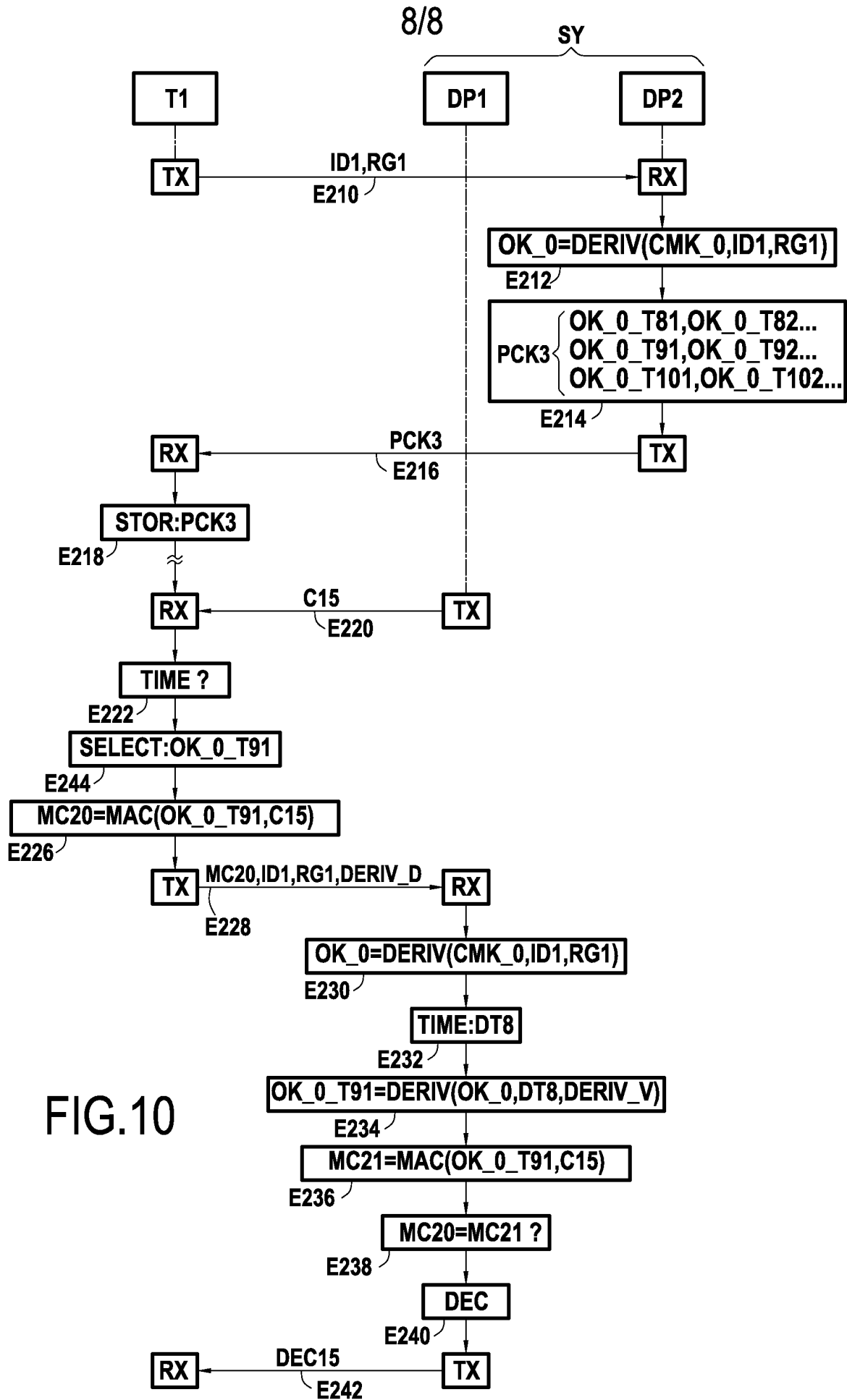


FIG. 8





RAPPORT DE RECHERCHE

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

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveau) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

☒ Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

☒ Le demandeur a modifié les revendications.

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

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

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

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

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

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

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

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

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

US 2007/021105 A1 (PATEL SARVAR M [US]) 25 janvier 2007 (2007-01-25)

GUILLOU L C ET AL: "Cryptographic authentication protocols for smart cards", COMPUTER NETW, ELSEVIER, AMSTERDAM, NL, vol. 36, no. 4, 16 juillet 2001 (2001-07-16), pages 437-451, XP004304908, ISSN: 1389-1286, DOI: 10.1016/S1389-1286(01)00165-7

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

US 2006/155822 A1 (YANG JEN-SHUN [TW] ET AL) 13 juillet 2006 (2006-07-13)

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

NEANT