Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2221016 C 2007/10/23

(11)(21) 2 221 016

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(22) Date de dépôt/Filing Date: 1997/11/03

(41) Mise à la disp. pub./Open to Public Insp.: 1998/06/04

(45) Date de délivrance/Issue Date: 2007/10/23

(30) Priorité/Priority: 1996/12/04 (FR96 14858)

(51) Cl.Int./Int.Cl. *H04L 9/30* (2006.01),
H04L 9/08 (2006.01)

(72) Inventeur/Inventor:
PINKAS, DENIS, FR

(73) Propriétaire/Owner:
BULL S.A., FR

(74) Agent: GOUDREAU GAGE DUBUC

(54) Titre : PROCEDE DE RECUPERATION DE CLES MIS EN OEUVRE POUR UN CHIFFREMENT FORT DE MESSAGE

(54) Title: PROCESS FOR RECOVERING KEYS IMPLEMENTED FOR HIGHLY ENCRYPTING MESSAGES

(57) Abrégé/Abstract:
La présente invention concerne un procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message émis par une entité, message soit à stocker localement soit à transmettre à une autre entité, la lecture d'un message nécessitant une clé de déchiffrement qui peut être reconstruite au moins par une tierce partie de confiance de récupération de clés tandis que sont rajoutés au message un champ de compensation et un champ de contrôle obligatoire comportant lui-même au moins un champ de récupération de clé pour permettre à au moins une tierce partie de confiance de fournir les clés de déchiffrement autorisant la lecture du message chiffré. Ce procédé de récupération de clés est remarquable en ce que, le champ de contrôle obligatoire comporte de plus, en clair, la date du jour ainsi que le numéro d'agrément du matériel/logiciel de chiffrement et chiffrée sous une clé journalière intermédiaire la clé de dialogue. Chaque champ de récupération de clé comporte en outre, d'abord l'identifiant de la tierce partie de confiance de récupération de clés adéquate, fonction du type de l'application, ensuite une clé de dialogue chiffrée sous la clé publique de ladite tierce partie de confiance et enfin, chiffrés sous la clé publique de ladite tierce partie de confiance, le numéro de série du matériel/logiciel agréé, de manière optionnelle l'identifiant de l'entité et de son gestionnaire, une clé de travail servant au calcul de la clé journalière intermédiaire et la période de validité de cette clé de travail. Enfin, de manière également remarquable, pendant la période de validité de la clé de travail, ladite clé de travail permet, seul le champ de contrôle obligatoire étant fourni, de calculer à l'avance pour la tranche de temps où l'écoute est autorisée, grâce à une formule imposée, des clés journalières intermédiaires utilisées pour déchiffrer les clés de dialogue elle-mêmes utilisées pour calculer à partir du champ de compensation et du champ de contrôle obligatoire les clés aléatoires de déchiffrement des messages.

Abrégé descriptif:

Procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message.

La présente invention concerne un procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message émis par une entité, message soit à stocker localement soit à transmettre à une autre entité, la lecture d'un message nécessitant une clé de déchiffrement qui peut être reconstruite au moins par une tierce partie de confiance de récupération de clés tandis que sont rajoutés au message un champ de compensation et un champ de contrôle obligatoire comportant lui-même au moins un champ de récupération de clé pour permettre à au moins une tierce partie de confiance de fournir les clés de déchiffrement autorisant la lecture du message chiffré. Ce procédé de récupération de clés est remarquable en ce que, le champ de contrôle obligatoire comporte de plus, en clair, la date du jour ainsi que le numéro d'agrément du matériel/logiciel de chiffrement et chiffrée sous une clé journalière intermédiaire la clé de dialogue. Chaque champ de récupération de clé comporte en outre, d'abord l'identifiant de la tierce partie de confiance de récupération de clés adéquate, fonction du type de l'application, ensuite une clé de dialogue chiffrée sous la clé publique de ladite tierce partie de confiance et enfin, chiffrés sous la clé publique de ladite tierce partie de confiance, le numéro de série du matériel/logiciel agréé, de manière optionnelle l'identifiant de l'entité et de son gestionnaire, une clé de travail servant au calcul de la clé journalière intermédiaire et la période de validité de cette clé de travail. Enfin, de manière également remarquable, pendant la période de validité de la clé de travail, ladite clé de travail permet, seul le champ de contrôle obligatoire étant fourni, de calculer à l'avance pour la tranche de temps où l'écoute est autorisée, grâce à une formule imposée, des clés journalières intermédiaires utilisées pour déchiffrer les clés de dialogue elle-mêmes utilisées pour calculer à partir du champ de compensation et du champ de contrôle obligatoire les clés aléatoires de déchiffrement des messages.

Procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message.

La présente invention concerne un procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message émis par une entité, message soit à stocker localement soit à transmettre à une autre entité, la lecture d'un message nécessitant une clé de déchiffrement fournie à au moins une tierce partie de confiance de récupération de clés tandis que le message comporte un champ de contrôle obligatoire comportant lui-même au moins un champ de récupération de clé pour permettre à au moins une tierce partie de confiance de fournir les informations de déchiffrement autorisant la lecture du message chiffré.

Il est tout d'abord précisé qu'il est admis par convention, qu'un chiffrement est considéré fort lorsque son déchiffrement ne peut être effectué, sans disposer de la clé, dans un temps raisonnable.

De manière générale, avec les progrès constants dans le domaine de l'informatisation, un besoin de plus en plus immédiat est engendré en ce qui concerne la protection de l'information. La sécurité informatique fait à présent partie intégrante des problèmes épineux à résoudre dans ce domaine. Ainsi et entre autres, un problème se pose lorsqu'il est désiré utiliser des techniques de chiffrement pour protéger efficacement des informations sensibles. En effet, dans de nombreux pays, la diffusion des informations chiffrées sur les réseaux publics est soumise à autorisations au cas par cas, alors que la nécessité d'exploiter de telles techniques s'y fait réellement sentir. La tendance des instances gouvernementales internationales est toutefois aujourd'hui d'autoriser à quiconque l'usage d'un chiffrement fort. En contrepartie de cette autorisation, les autorités nationales entendent conserver un droit de regard c'est-à-dire être en mesure de déchiffrer de telles communications.

Avec ce type de technique, le message stocké ou transmis ne peut être déchiffré que lorsque la clé de déchiffrement utilisée est connue. L'objet ou le problème technique particulier est ici de faire connaître la clé de déchiffrement à une autorité de récupération de clés déterminée, autorité qui dans la suite est appelée "tierce partie de confiance" de récupération de clés. Deux techniques sont généralement utilisées pour y parvenir.

La première technique consiste à déposer une clé de déchiffrement de longue durée qui servira elle-même à déchiffrer les clés de travail ou de déchiffrement. Un matériel ou un logiciel de déchiffrement (indiqué dans la suite, dans un but de simplification et de concision, par «matériel/logiciel de déchiffrement») utilise alors ladite clé pour déchiffrer à son tour les clés de déchiffrement d'un message et ainsi toute personne qui désire déchiffrer le message doit posséder le double de ladite clé. Cette technique s'avère efficace et praticable, par exemple à l'intérieur d'un même pays, mais présente de sérieux inconvénients relativement à la sécurité dès lors que la communication est internationale et/ou qu'une autorité d'un des pays concernés souhaite écouter et comprendre un message émis dans l'un desdits pays concernés par une personne suspectée. En effet, la tierce partie de confiance de récupération de clés d'un pays doit obligatoirement demander à la tierce partie de confiance de récupération de clés d'un autre pays ou à la personne possédant le double de la clé de la lui fournir pour pouvoir déchiffrer le message. Dans le cas où cette dernière est d'accord, ce qui est une première restriction, d'une part l'écoute est "avouée" à la tierce partie de confiance de récupération de clés de l'autre pays alors que ce type d'intervention se veut plutôt discret et même confidentiel et, d'autre part une perte de temps significative est inévitablement provoquée pour obtenir le double de la clé, ce qui est tout à fait inopportun car le message doit être rapidement compris si il est désiré intervenir rapidement auprès de la personne suspectée avant que cette dernière n'ait pu s'échapper ou disparaître. Cette technique présente donc d'importantes limitations pour être utilisée à un niveau international compte tenu de la contrepartie exigée par les instances gouvernementales internationales pour autoriser l'échange de ce type de communications à moins que les gouvernements intéressés ne souscrivent entre eux à des agréments de réciprocité, ce qui dans ce domaine, loin s'en faut, n'est pas toujours souhaité.

La seconde technique consiste elle à ne pas déposer une clé de déchiffrement de longue durée mais à permettre le déchiffrement de la clé de déchiffrement par la tierce partie de confiance de récupération de clés et donc la clé de chiffrement du message que cette clé soit une clé asymétrique ou une clé symétrique. Pour cela, est ajouté dans le message deux champs supplémentaires, appelés dans ce qui suit, champ de compensation et champ de contrôle obligatoire, comportant lui-même, entres autres informations, au moins un champ destiné à la récupération de la clé auprès d'un gardien de clés autorisé, qui est la ci-dessus appelée "tierce partie de confiance" de récupération de clés. Ainsi, dans le cas plus particulier du stockage local d'un message mémorisé chiffré, par

exemple sur un disque, une seule tierce partie de confiance de récupération de clés est impliquée et donc un seul champ de récupération de clé est nécessaire. Par contre, dans le cas plus général de la transmission d'un message entre deux utilisateurs ou de manière plus générale entre deux entités communicantes, deux champs de récupération de clé sont nécessaires puisque deux tierces parties de confiance de récupération de clés sont impliquées, d'une part celle du pays de l'émetteur du message et d'autre part celle du pays du destinataire du message. Ainsi, une conversation internationale entre deux interlocuteurs respectivement d'un pays A et d'un pays B peut être écoutée, si cette écoute est autorisée, par les autorités d'interception adéquates respectivement du pays A et du pays B sans jamais pouvoir l'être par les autorités de tout autre pays. Par conséquent, lorsqu'une écoute est légalement autorisée, le premier champ de récupération de clé du champ de contrôle obligatoire permet l'écoute par l'intermédiaire de l'autorité agréée du pays A alors que le second champ de récupération de clé permet l'écoute par l'intermédiaire de l'autorité agréée du pays B. Ces deux autorités agréées peuvent être soit, des autorités nationales situées dans les pays où se trouvent physiquement les entités communicantes, soit également, des autorités nationales de la même nationalité que celle des entités communicantes. En fait, pour permettre le déchiffrement, l'un de ces deux champs de récupération de clé présents dans le message est d'abord remis à une tierce partie de confiance de récupération de clé, puis la clé de déchiffrement est remise par ladite tierce partie de confiance à l'autorité nationale lui permettant ainsi de déchiffrer le message dans son intégralité. Actuellement, il est prévu que chaque pays agrée un certain nombre de tierces parties de confiance de récupération de clés qui seront donc nationales et chacune de préférence spécifique d'un domaine, de cette manière c'est la tierce partie de confiance agréée par une instance gouvernementale qui contrôle et permet le déchiffrement et non directement l'instance gouvernementale. Une telle technique est décrite dans la brochure "Commercial Key Escrow (CKE, marque de Trusted Information Systems, Inc.) : The path to global information security". Cette seconde technique présente cependant elle aussi un certain nombre d'inconvénients. Un premier sérieux inconvénient est inhérent au fait qu'il est impossible de s'apercevoir, de manière simple, qu'une tentative de fraude par modification du champ de contrôle obligatoire ou modification du matériel/logiciel de chiffrement a été perpétrée. De plus, cette technique ne permet pas non plus de fournir à l'avance des clés journalières de déchiffrement utilisables à l'intérieur, et seulement à l'intérieur, d'une tranche de temps prédéterminée, ce qui est un second notable inconvénient relativement à la sécurité. Enfin, un autre

inconvénient existe du fait que les entités communicantes ne sont pas identifiées ce qui ne permet pas de discriminer facilement entre des écoutes légales ou illégales.

La présente invention a pour but de remédier aux divers inconvénients des différentes techniques connues de l'art antérieur et propose un procédé de récupération de clés efficace, aisé à mettre en oeuvre, qui permet de détecter toute modification, même minime, du champ de contrôle obligatoire et qui autorise la fourniture, même à l'avance, de clés journalières de déchiffrement utilisables uniquement à l'intérieur d'une tranche de temps prédéterminée.

Pour cela, le procédé de récupération de clés mis en oeuvre pour un chiffrement fort de message mentionné dans le préambule est remarquable en ce que le champ de contrôle obligatoire comporte de plus, d'une part, en clair, la date du jour ainsi que le numéro d'agrément du matériel/logiciel de chiffrement et d'autre part, une clé de dialogue chiffrée sous une clé intermédiaire journalière, clé intermédiaire qui est une clé calculée à partir de certains éléments du champ de contrôle obligatoire selon une formule qui est explicitée plus loin.

Ainsi selon l'idée de l'invention et grâce à la technique employée, qui va être décrite ci-après, la modification ultérieurement à sa génération du champ de contrôle obligatoire correctement généré par l'émetteur rend le déchiffrement par le destinataire impossible. En fait, une altération de certaines données du champ de contrôle obligatoire qui viserait à empêcher la récupération de la clé de déchiffrement du message par l'une quelconque des tierces parties de confiance entraîne l'impossibilité de déchiffrer le message. Le numéro d'agrément du matériel/logiciel de chiffrement permet en outre, à l'autorité nationale autorisant les tierces parties de confiance de récupération de clés à donner les clés de déchiffrement, en premier lieu d'identifier le matériel/logiciel à utiliser pour déchiffrer le message. Enfin, la date du jour permet, d'abord, d'assurer que le message à déchiffrer est transmis dans la bonne tranche de temps, une date incorrecte étant détectée automatiquement et immédiatement sans même devoir faire appel à la tierce partie de confiance de récupération de clés, mais également et surtout, d'être le fondement même de la technique permettant de fournir à l'avance des clés de déchiffrement ainsi qu'il sera expliqué ci-après.

Selon une autre caractéristique propre à la présente invention, le procédé de récupération de clés est remarquable en ce que chaque champ de récupération

de clé comporte d'abord, en clair, l'identifiant de la tierce partie de confiance de récupération de clés adéquate, fonction du type de l'application, ensuite une clé de dialogue chiffrée sous la clé publique de ladite tierce partie de confiance et enfin, chiffrés sous la clé publique de ladite tierce partie de confiance, le numéro de série du matériel/logiciel agréé, une clé de travail et la période de validité de cette clé de travail.

En outre, selon une variante, chaque champ de récupération de clé comporte de plus dans le dernier champ précité l'identifiant de l'entité utilisatrice ou du gestionnaire de ce matériel/logiciel également chiffré sous la clé publique de la tierce partie de confiance de récupération de clés adéquate. Grâce à cet identifiant, avantageusement et de la manière précisée dans la suite, la tierce partie de confiance de récupération de clés peut connaître directement l'identité de l'entité utilisatrice ou du gestionnaire sans en référer au fournisseur du matériel/logiciel ou son représentant ni à une autorité d'enregistrement des entités utilisatrices.

Enfin, de manière caractéristique, la clé de travail combinée, entre autres, avec la date est utilisée pour calculer la clé intermédiaire journalière alors que ladite clé intermédiaire est utilisée pour chiffrer la clé de dialogue.

Ainsi, le choix de la tierce partie de confiance de récupération de clés est laissé à l'application, c'est donc un choix dynamique qui est fonction du type de l'application ou du contexte, c'est-à-dire spécifique d'un domaine. De cette manière, le matériel/logiciel agréé peut "connaître" le choix et par conséquent le nom des tierces parties de confiance de récupération de clés adéquates, nom qui peut être déterminé à partir du contexte de l'application ou de données de l'utilisateur, à partir des pays d'origine et de destination ou encore à partir d'éléments de la structure hiérarchique des noms. Ce principe même de choix dynamique fait donc que la tierce partie de confiance ne peut connaître à l'avance ce choix. L'identifiant de tierce partie de confiance de récupération de clés permet, à l'autorité nationale autorisant les tierces parties de confiance à donner les clés de déchiffrement, d'identifier la tierce partie de confiance de récupération de clés choisie. Afin de vérifier que le champ de contrôle obligatoire construit par l'émetteur a été constitué pour rendre effectivement accessible la clé de déchiffrement du message aux différentes tierces parties de confiance, le matériel/logiciel du récepteur récalcule une partie de ce champ de contrôle obligatoire, à savoir qu'il réchiffre la clé de dialogue, qu'il obtient par ailleurs au

moyen du protocole d'échange des clés propre à l'application, sous la clé publique de chaque tierce partie de confiance et vérifie qu'il obtient un résultat identique. Si ce n'est pas le cas, il s'abstient de déchiffrer le message.

Ce procédé n'empêche toutefois pas un matériel/logiciel du récepteur modifié en conséquence de passer outre à ce contrôle et de ne pas s'abstenir de déchiffrer. Ainsi qu'il sera expliqué plus loin, une des originalités de l'invention réside dans le fait que la modification, durant leur transfert, des champs de contrôle obligatoire et de compensation correctement générés, empêche le receveur, quelque soit le logiciel / matériel receveur utilisé (conforme ou modifié), de déchiffrer le message.

De manière habituelle, les systèmes classiques de récupération de clés se contentent de chiffrer directement la clé de déchiffrement du message sous la clé de chaque tierce partie de confiance. Ceci a pour conséquence qu'il est nécessaire de faire appel à une tierce partie de confiance pour déchiffrer chaque clé individuelle de déchiffrement. Ainsi qu'il va en être expliqué ci-après, une autre originalité de l'invention réside dans le fait qu'i va être possible de fournir à l'avance aux autorités de déchiffrement des clés journalières intermédiaires ce qui évite aux autorités de déchiffrement d'avoir recours aux services d'une tierce partie de confiance pour déchiffrer chaque message. Afin de permettre aux autorités de recevoir à l'avance des données permettant de reconstruire les clés de déchiffrement, contrairement aux techniques connues, le procédé juxtapose à la méthode directe de récupération de la clé de dialogue au moyen de la clé publique de chiffrement de la tierce partie de confiance une seconde méthode de récupération de la clé de dialogue, utilisant une hiérarchie de clés à quatre niveaux, où d'abord la clé de travail, le numéro de série du matériel/logiciel agréé, la période de validité de ladite clé de travail, et de manière optionnelle selon la variante ci-dessus présentée, l'identifiant de l'utilisateur ou du gestionnaire de ce matériel/logiciel sont chiffrés sous chaque clé publique de tierce partie de confiance de récupération de clés, où ensuite la clé de travail combinée en particulier à la date, est utilisée pour calculer la clé intermédiaire journalière où ensuite la clé intermédiaire journalière est utilisée pour chiffrer une clé de dialogue. La clé de travail étant chiffrée sous la clé publique de la tierce partie de confiance de récupération de clés, celle-ci est déchiffrable par cette tierce partie de confiance et par elle seule, sachant qu'en outre, cette clé de travail ne peut servir directement mais seulement indirectement à déchiffrer le message. En conséquence, de manière caractéristique, le matériel/logiciel de déchiffrement agréé va calculer la clé intermédiaire journalière au moyen d'une

fonction à sens unique (appelée “one-way function" ou bien "one-way-hash function” par l’homme du métier) à partir de la clé de travail, et du champ de contrôle obligatoire, à savoir, de la date du jour, du numéro d’agrément et des deux champs de récupération de clé. Les deux entités communiquantes échangent habituellement une clé de déchiffrement selon un protocole qui leur est propre. Selon la méthode utilisée, la clé échangée n'est plus considérée comme étant cette clé de déchiffrement mais comme étant précisemment la clé de dialogue mentionnée ci-dessus. Cette clé de dialogue est donc aussi accessible aux tierces parties de confiance désignées d'une part de manière directe, car chiffrée directement sous leur clé publique mais aussi du fait que cette clé de dialogue est aussi chiffrée sous une clé journalière intermédiaire. Les deux entités communiquantes vont calculer la clé de déchiffrement à partir d'une fonction à sens unique utilisant comme paramètres la clé de dialogue et le résultat d'une fonction à sens unique résistante aux collisions calculée sur l'ensemble des composants du champ de contrôle obligatoire, le dedit résultat étant ensuite combiné au champ de compensation au moyen d'un OU exclusif.

Chacune des tierces parties de confiance effectue le calcul de la clé de déchiffrement de la même manière et est donc à même de calculer la clé de déchiffrement. Le champ de compensation permet d'utiliser une clé de déchiffrement de valeur quelconque, qui peut être du type "clé privée" pour un algorithme asymmétrique ou du type "clé secrète" pour un algoritme symmétrique. En effet, l'émetteur du message ajuste la valeur de la clé au moyen du champ de compensation car le résultat de la fonction à sens unique utilisant comme paramètres la clé de dialogue et le résultat d'une fonction à sens unique résistante aux collisions calculée sur l'ensemble des composants du champ de contrôle obligatoire ne peut être prédictible. Donc, du fait que la clé de déchiffrement est fonction du champ de contrôle obligatoire et du champ de compensation, utilisé conjointement par les entités communiquantes et les tierces parties de confiance, et comme cela a été précisé ci-avant, une quelconque altération du champ de contrôle obligatoire normalement constitué à l'origine par l'émetteur entraîne l’impossibilité de déchiffrer le message, le but, et ceci est fondamental, étant de rendre la clé de déchiffrement fausse pour le receveur du message suite à une quelconque modification. En effet, une modification, même minime, d’un quelconque des champs du champ de contrôle obligatoire a pour résultat de modifier la clé de déchiffrement et d’interdire ainsi le déchiffrement et donc de comprendre la sémantique du message. Il est important de constater que le présent procédé permet de choisir, pour chaque message, une clé de déchiffrement différente et parfaitement aléatoire.

Pour une meilleure appréhension de l'idée de l'invention, la description suivante, qui n'est bien entendu pas limitative, fera bien comprendre, en précisant le vocabulaire employé par l'homme du métier et les différents intervenants dans les différentes phases de mise en oeuvre, dans quel environnement l'invention s'insère et comment elle peut être réalisée.

Ainsi une première phase consiste en la demande d'agrément du matériel/logiciel de déchiffrement. Pour cela, de manière caractéristique, le fournisseur du matériel/logiciel de déchiffrement requiert un agrément à l'autorité d'agrément des matériels/logiciels (par exemple, en France le SCSSI - Service Central de la Sécurité des Systèmes d'Information) celle-ci lui procurant en retour, dans la mesure où le matériel/logiciel est effectivement agréé, un numéro d'agrément pour ledit matériel/logiciel de déchiffrement. Le fournisseur doit fournir, outre le matériel/logiciel de déchiffrement, deux matériels/logiciels spécifiques, un premier matériel/logiciel utilisé par une autorité nationale de déchiffrement, autorité ci-après appelée pour des besoins de concision «autorité de déchiffrement» et un second matériel/logiciel utilisé par la tierce partie de confiance de récupération de clés. L'autorité de déchiffrement utilise le premier matériel/logiciel pour extraire la partie utile du champ de contrôle obligatoire et ensuite, à partir des données renvoyées par la tierce partie de confiance de récupération de clés, permettre de déchiffrer les données chiffrées. La tierce partie de confiance de récupération de clés utilise elle le second matériel/logiciel pour fournir la clé ou les clés de déchiffrement à l'autorité de déchiffrement. En effet, le numéro d'agrément figure en clair dans le champ de contrôle obligatoire afin de permettre tant à l'autorité de déchiffrement qu'à la tierce partie de confiance de récupération de clés d'identifier les matériels/logiciels à utiliser pour exploiter le message.

Une seconde phase consiste en la demande d'enregistrement d'une entité utilisatrice de chiffrement fort auprès d'un fournisseur de matériel/logiciel ou de son représentant ou encore auprès d'une autorité d'enregistrement des entités utilisatrices qui a reçu délégation de la part du fournisseur pour effectuer cette opération. A titre d'exemple, en France, la loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications en son article 17 dispose que "...l'autorisation peut être subordonnée à l'obligation pour le fournisseur de communiquer l'identité de l'acquéreur...". Une déclaration préalable d'utilisation du matériel/logiciel par chaque utilisateur est donc nécessaire. De manière

remarquable, pour permettre son enregistrement l'entité utilisatrice communique au fournisseur de matériel/logiciel, son représentant ou une autorité d'enregistrement des entités utilisatrices le numéro d'agrément du matériel/logiciel, le numéro de série du matériel/logiciel, son nom d'entité utilisatrice, les coordonnées du gestionnaire de l'entité et la date du jour qui seront utilisés pour la validation du matériel/logiciel de déchiffrement. Il est ici à noter que la clé maître propre au matériel/logiciel concerné permet, à partir du numéro de série du matériel/logiciel, de calculer une clé dite diversifiée et de valider chaque matériel/logiciel pour autoriser son utilisation durant une période donnée. L'objet de la clé maître n'est pas de permettre le déchiffrement des messages mais de permettre d'associer le numéro du matériel/logiciel à un nom d'entité ou d'utilisateur et d'autoriser l'utilisation du matériel/logiciel agréé seulement après un enregistrement préalable et donc communication de l'identité de l'entité utilisatrice. Le fournisseur de matériel/logiciel, son représentant ou une autorité d'enregistrement des entités utilisatrices répond à l'entité utilisatrice en lui communiquant le droit d'utilisation du matériel/logiciel ainsi que, ce qui est également fondamental, des informations permettant de personnaliser le matériel/logiciel après sa mise en vente, et tout particulièrement la clé publique de l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés. Le droit d'utilisation qui est valable pour une période déterminée est fourni sous la forme d'une clé qui est en fait une chaîne de caractères à rentrer par exemple sur le clavier d'un ordinateur et qui, si elle est correcte, permet d'autoriser le matériel/logiciel à fonctionner pour la tranche de temps autorisée. Ce droit d'utilisation qui est scellé sous la clé dite diversifiée, l'intégrité étant donc garantie du fait de ce scellement sous la clé dite diversifiée, est constitué d'une part d'une période d'utilisation et d'autre part de la clé publique d'une autorité nationale d'agrément des tierces parties de confiance de récupération de clés qui peut ainsi être ajoutée après l'achat du logiciel/matériel. En effet, le matériel/logiciel peut être vendu de deux façons, soit prêt à être utilisé dans un pays et alors il comprend la clé publique d'une autorité nationale d'agrément des tierces parties de confiance de récupération de clés, soit prêt à être utilisé dans tout pays qui le reconnaîtrait valable et dans ce cas, c'est au moment de la mise en service que cette clé publique est communiquée. La clé publique de l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés permet au matériel/logiciel de vérifier les certificats des tierces parties de confiance de récupération de clés agréées pour les pays où le matériel/logiciel est agréé ainsi qu'il est expliqué plus loin. Un tel certificat peut prendre en particulier la forme d'un certificat X.509 tel que décrit dans la norme

ITU-T (ex CCITT) du même nom. Il permet à l'autorité d'agrément des tierces parties de confiance de récupération de clés de garantir, pour une durée donnée, l'association entre le nom d'une tierce partie de confiance de récupération de clés, la valeur de sa clé publique et l'algorithme de chiffrement à utiliser. Le fournisseur de matériel/logiciel, son représentant ou une autorité d'enregistrement des entités utilisatrices garde la trace, dans un fichier d'audit, de l'enregistrement de cette entité utilisatrice en mémorisant le numéro d'agrément de matériel/logiciel, le numéro de série du matériel/logiciel, le nom de l'entité et les coordonnées du gestionnaire de l'entité. Le fournisseur de matériel/logiciel, son représentant ou une autorité d'enregistrement des entités utilisatrices peut aussi être tenu de transmettre ce fichier d'audit de manière régulière (ou sur demande expresse) à une autorité gouvernementale nationale. Ce fichier peut donc être obtenu soit, auprès du fournisseur de matériel/logiciel, de son représentant, d'une autorité d'enregistrement des entités utilisatrices soit encore, auprès de cette autorité gouvernementale nationale. De manière particulière, il est possible, mais non indispensable, pour un même organisme de cumuler les rôles de tierce partie de confiance de récupération de clés et d'autorité d'enregistrement des entités utilisatrices.

En outre, selon la variante ci-avant proposée, le droit d'utilisation comprend une information supplémentaire, elle aussi scellée sous la clé diversifiée. Cette information supplémentaire est constituée de l'identifiant de l'entité utilisatrice ou de celui du gestionnaire du matériel/logiciel de chiffrement agréé. L'identifiant pourra selon les cas et les pays prendre des valeurs différentes. Cela peut être, à titre d'exemples, le numéro d'une carte d'identité nationale, le numéro d'un passeport ou même dans le cas des États Unis d'Amérique un numéro de permis de conduire ("Driving License number"). Lorsque cette information supplémentaire est retournée avec le droit d'utilisation, alors le matériel/logiciel de chiffrement agréé la reporte dans la partie chiffrée de chaque champ de récupération de clé ainsi qu'il a été expliqué auparavant. Dans ce cas, la tierce partie de confiance de récupération de clés peut, au moyen dudit identifiant, connaître directement l'identité de l'entité utilisatrice ou du gestionnaire sans en référer au fournisseur ou son représentant ni à une autorité d'enregistrement des entités utilisatrices.

Egalement, toute tierce partie de confiance de récupération de clés doit demander son agrément auprès de l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés. Lorsqu'une tierce partie de

confiance de récupération de clés est agréée par cette autorité, elle est ajoutée à la liste d'un répertoire des tierces parties de confiance de récupération de clés agréées et un certificat d'agrément est produit sous forme électronique, par exemple sous forme d'un certificat au format X 509, pour garantir l'identité de la tierce partie de confiance de récupération de clés, la valeur de la clé publique de la tierce partie de confiance de récupération de clés, l'algorithme de chiffrement à utiliser et la durée de cette garantie. L'autorité nationale d'agrément des tierces parties de confiance de récupération de clés délivre aussi, mais de manière indirecte, des certificats d'agrément internationaux à des tierces parties de confiance de récupération de clés internationales par l'intermédiaire des autorités nationales d'agrément de tierces parties de confiance de récupération de clés d'autres pays avec lesquels une reconnaissance existe. Ceci est effectué lorsqu'une autorité nationale d'agrément des tierces parties de confiance de récupération de clés reconnaît une autre autorité nationale d'agrément des tierces parties de confiance de récupération de clés. Dans ce cas, cette autorité nationale d'agrément des tierces parties de confiance de récupération de clés émet un certificat (par exemple au format X.509) garantissant la valeur de la clé de l'autre autorité nationale d'agrément des tierces parties de confiance de récupération de clés. Ainsi, de proche en proche, selon une technique connue sous le nom de "chaînage des certificats", il est possible, connaissant la clé publique de l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés d'un pays, de valider la clé publique de l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés d'un autre pays, cet autre pays validant lui-même la clé publique d'une tierce partie de confiance de récupération de clés de cet autre pays. De manière indirecte, la clé publique de la tierce partie de confiance de récupération de clés d'un autre pays se trouve ainsi validée uniquement par la connaissance d'une seule clé publique spécifique à l'autorité nationale d'agrément des tierces parties de confiance de récupération de clés d'un seul pays. C'est cette unique clé publique qui est transmise lors de la validation du logiciel/matériel.

Le fonctionnement du matériel/logiciel de déchiffrement agréé est maintenant décrit ci-après. Il peut être mis en oeuvre sans qu'aucun dépôt préalable de clé n'ait été réalisé. Le matériel/logiciel de déchiffrement agréé comme explicité précédemment, pour son utilisation par une entité communicante, va à partir des identifiants des pays d'origine, obtenir et ceci pour chaque pays communicant, les clés publiques de tierces parties de confiance de récupération de clés adéquates qui dans certains cas pourront être choisies par défaut, chaque tierce

partie de confiance de récupération de clés étant pourvue d'un certificat (par exemple au format X.509) délivré par l'autorité nationale d'agrément et listé dans un répertoire. Une fois les clés publiques des deux tierces parties de confiance de récupération de clés adéquates ainsi obtenues, le matériel/logiciel peut créer le champ de contrôle obligatoire conforme aux caractéristiques de la présente invention.

De la description préalable il découle divers principes concernant cette technique. Ainsi, tout matériel/logiciel agréé n'est pas opérationnel lors de l'achat mais doit être validé par le fournisseur de matériel/logiciel, son représentant ou une autorité d'enregistrement des entités utilisatrices exerçant dans un pays, une entité utilisatrice devant nécessairement obtenir une autorisation pour utiliser un matériel/logiciel agréé en s'adressant à l'un quelconque des pays où il est agréé. Egalement, le droit d'utilisation du matériel/logiciel est valable non seulement pour le pays où il a été agréé mais aussi pour les autres pays avec lesquels une reconnaissance existe. A tout moment un pays peut être reconnu sans qu'il soit besoin de recontacter l'autorité d'enregistrement des entités, ceci étant obtenu par une certification de clés avec deux niveaux de hiérarchie. De même, il est impossible d'utiliser un matériel/logiciel agréé sans que deux tierces parties de confiance de récupération de clés nationales ou nationale et internationale agréées ne soient utilisées.

Une caractéristique également fondamentale peut être ci-après explicitée, caractéristique relative à la fréquence de changement de la clé de travail. Selon le procédé de récupération de clés conforme à l'invention, pendant la période de validité de la clé de travail, ladite clé de travail permet, en utilisant seulement le champ de contrôle obligatoire, de calculer et de fournir à l'avance des clés journalières intermédiaires permettant de déchiffrer chaque clé individuelle de dialogue et par là même de déchiffrer l'ensemble des messages pour la tranche de temps indiquée par la période de validité de la clé de travail, qui est chiffrée sous la clé publique de chaque tierce partie de confiance de récupération de clés, cette période étant à mettre en regard de la période d'écoute légale demandée par l'autorité de déchiffrement afin de pouvoir délivrer à l'avance l'ensemble ou le sous-ensemble des clés journalières intermédiaires demandées.

En effet, la fréquence de changement de la clé de travail influe sur la rapidité du déchiffrement et les impératifs de communication en temps réel entre l'autorité de déchiffrement et la tierce partie de confiance de récupération de clés.

Plusieurs possibilités sont à envisager. Une première possibilité consiste à conserver la même clé de travail durant une session, une session pouvant durer par exemple de 2 à 3 heures, et ainsi chiffrer chaque message avec une clé différente. Dans ce cas, il convient de reconsulter la tierce partie de confiance de récupération de clés pour chaque nouvelle session, donc pour chaque session demander une clé, ce qui est particulièrement lourd et gênant. Une possibilité antagoniste consiste à, indéfiniment ou au moins très longtemps, conserver une même clé pour chiffrer tous les messages, mais cette solution est dangereuse du fait qu'une autorité qui posséderait une telle clé pourrait continuer d'écouter et déchiffrer tout message même lorsque la durée d'écoute autorisée, qui elle est limitée dans le temps, serait achevée, ceci irait totalement à l'encontre du but recherché. Une solution moyenne et qui dans certains cas, en particulier lorsque la granularité de la durée d'écoute est la journée, apparaît convenable peut être de conserver une même clé durant toute une journée pour éviter d'avoir à consulter maintes fois la tierce partie de confiance de récupération de clés pour permettre le déchiffrement de tous les messages de la journée. Enfin, la solution la plus avantageuse et qui est ici recommandée chaque fois que cela s'avérera possible, consiste à conserver une même clé de travail durant une période de temps au moins égale à une semaine. En effet, dans ce cas la clé de travail, permet de calculer à l'avance des clés journalières de déchiffrement de l'ensemble des messages pour la tranche de temps indiquée par la période de validité de la clé de travail, qui est chiffrée sous la clé publique de chaque tierce partie de confiance. Cette période est à mettre en regard de la période d'écoute légale demandée par l'autorité de déchiffrement afin de pouvoir délivrer à l'avance l'ensemble ou le sous-ensemble des clés de déchiffrement demandées. Cette solution préférée, est véritablement originale et particulièrement avantageuse, car elle autorise la remise de la totalité des clés nécessaires au déchiffrement des messages pour l'ensemble d'une période d'écoute considérée, pour obtenir ces clés, il suffit de fournir un seul champ de contrôle obligatoire. Plus précisément, l'autorité de déchiffrement qui déclare désirer écouter une entité donnée pour une période déterminée fournit à une tierce partie de confiance le champ de contrôle obligatoire, la clé journalière intermédiaire étant définie comme étant une fonction, entre autres, de la clé de travail et de la date du jour. La tierce partie de confiance de récupération de clés qui connaît donc la clé de travail, lorsqu'elle prend connaissance que cette autorité désire écouter l'entité donnée pour la période déterminée, cette autorité lui transmettant le champ de contrôle obligatoire, peut fournir un ensemble de clés journalières intermédiaires (mais ne fournira en aucun cas la clé de travail).

A présent, il peut être donné un exemple d'interception et de déchiffrement par une autorité d'interception lors d'une phase d'écoute légale. Au tout début, l'autorité judiciaire (en France, le juge d'instruction ou en ce qui concerne les «interceptions de sécurité» le Premier ministre) sur requête, autorise une interception pour une entité donnée et une tranche de temps donnée. Lorsque l'autorité d'interception s'aperçoit que les informations interceptées sont chiffrées, celle-ci doit alors déterminer le nom de l'autorité de déchiffrement habilitée pour lui transmettre l'ordre judiciaire et les données interceptées. L'autorité de déchiffrement doit à son tour déterminer la tierce partie de confiance de récupération de clés adéquate en consultant l'en-tête du champ de contrôle obligatoire qui contient, en particulier l'un des champs de récupération de clé où figure en clair le nom de l'organisme agréé sélectionné. L'autorité de déchiffrement communique la durée souhaitée pour le déchiffrement et de manière optionnelle le nom ou l'identifiant de l'entité à écouter accompagné du nom de son gestionnaire, sachant que le message chiffré n'a jamais besoin d'être communiqué. De plus, il n'est pas de la compétence de la tierce partie de confiance de récupération de clés, qui n'a pas à avoir connaissance de l'ordre judiciaire et ne connaît que la période de déchiffrement demandée et autorisée et de manière optionnelle le nom ou l'identifiant de l'entité à écouter accompagné du nom de son gestionnaire, d'apprécier la validité de l'écoute demandée. Il est ici à noter, que la connaissance de la période d'écoute souhaitée permet d'instituer un contrôle a posteriori, par une commission de contrôle, du contenu et du bien-fondé de la demande exprimée par l'autorité de déchiffrement, ce contrôle est possible relativement à l'identité de l'entité écoutée et à la durée de la période d'écoute, la commission de contrôle étant par exemple en France la Commission de Contrôle des Interceptions de Sécurité (CCIS). Dans le cas où l'identifiant de l'entité utilisatrice ne figure pas dans la partie chiffrée du champ de récupération de clé, alors la commission de contrôle demande également soit, au fournisseur d'origine, à son représentant, ou à l'autorité d'enregistrement des entités utilisatrices, soit à une autorité gouvernementale nationale de lui fournir la relation entre le nom d'entité et les numéros d'agrément et de série des matériels/logiciels. De son côté et selon la durée d'écoute souhaitée, la tierce partie de confiance de récupération de clés délivre, à l'autorité de déchiffrement, la clé de déchiffrement du message ou les clés journalières intermédiaires permettant de déchiffrer chaque clé individuelle de déchiffrement des messages pour la période considérée. La tierce partie de confiance de récupération de clés effectue également l'audit des informations communiquées par l'autorité de

déchiffrement en les stockant dans un fichier d'audit et tout particulièrement la période de déchiffrement demandée avec, s'ils sont communiqués, le nom ou l'identifiant de l'entité à écouter accompagné du nom de son gestionnaire, en y associant le numéro de matériel/logiciel agréé, le numéro de série de ce matériel/logiciel et la durée d'écoute. Le contrôle a posteriori effectué par la commission de contrôle est donc fait d'une part, au moyen du fichier d'audit ainsi constitué et mis à sa disposition par la tierce partie de confiance de récupération de clés et d'autre part, dans le cas où l'identifiant de l'entité utilisatrice ne figure pas dans la partie chiffrée du champ de récupération de clé, de la relation entre le numéro de série du matériel/logiciel et l'entité utilisatrice mis à disposition par le fournisseur, son représentant ou l'autorité d'enregistrement des entités utilisatrices en rapprochant ces informations des informations fournies par l'autorité de déchiffrement, en particulier de l'ordre judiciaire d'origine. Selon la variante proposée précédemment, le contrôle a posteriori effectué par la commission de contrôle est réalisé directement en rapprochant les informations contenues dans le fichier d'audit constitué par la tierce partie de confiance de récupération de clés des informations du fichier d'audit tenu par l'autorité de déchiffrement et finalement de l'ordre judiciaire d'origine produit par l'autorité de déchiffrement. Dans les deux cas, l'autorité de déchiffrement devra ainsi éventuellement justifier ses écoutes en montrant que ces dernières correspondent bien à celles prévues par l'ordre judiciaire d'origine, toutes ces informations étant mises à la disposition de l'autorité de contrôle.

Il est tout à fait remarquable de constater que le numéro de série du matériel/logiciel ainsi qu'éventuellement le nom ou l'identifiant de l'entité à écouter accompagné du nom de son gestionnaire apparaissent dans chaque partie chiffrée sous la clé publique d'une tierce partie de confiance de récupération de clés et non dans le champ en clair. Ceci empêche les entités qui ne sont pas habilitées à écouter de pouvoir identifier les intervenants grâce au champ de contrôle obligatoire. Si cette caractéristique n'est pas nécessaire, alors ces informations peuvent être mises dans la partie "en clair" mais doivent alors être prises en compte dans le calcul de la clé de chiffrement. Ces informations, une fois déchiffrées par la tierce partie de confiance de récupération de clés, sont remises systématiquement à l'autorité de déchiffrement. Lorsque seul le numéro de série du matériel/logiciel figure dans la partie chiffrée, il permet, au moyen d'un accès au fichier tenu par l'autorité d'enregistrement des entités utilisatrices ou par le fournisseur de matériel/logiciel ou son représentant d'identifier l'entité et le gestionnaire de l'entité.

Il est également à remarquer qu'il est apporté un certain nombre de limitations aux pouvoirs des autorités d'interception et de déchiffrement concernant la légalité des écoutes. Ainsi, il convient de contrôler a posteriori, mais non d'empêcher, que ces autorités n'ont pas d'une part, eu accès à la sémantique des communications relatives à une entité n'entrant pas dans le cadre d'un contrôle judiciaire et d'autre part, eu accès à la sémantique de communications en dehors des périodes autorisées par l'autorité judiciaire. Pour cela et relativement à l'accès à la sémantique des communications relatives à une autre entité, soit le numéro de série du matériel/logiciel agréé permet indirectement de s'assurer de l'identité de l'entité ou de la personne sous écoute en les rapprochant des informations fournies par l'autorité d'enregistrement des entités utilisatrices ou le fournisseur de matériel/logiciel ou son représentant qui sont constituées du numéro de série du matériel/logiciel agréé associé à une liste d'entités, soit l'identifiant de l'entité ou celui de son gestionnaire, lorsqu'il est présent dans chaque partie chiffrée du champ de contrôle obligatoire, permet de s'assurer directement de l'identité de l'entité ou de la personne sous écoute. La relation entre le numéro de série du matériel/logiciel agréé et le nom des entités est maintenue par les autorités d'enregistrement des entités utilisatrices. La commission de contrôle peut demander le contenu de cette relation auprès des autorités d'enregistrement des entités tant nationales qu'étrangères. Il est bien entendu qu'en ce qui concerne les pays étrangers, cette garantie de contrôle a posteriori dépend de la bonne volonté du fournisseur étranger ou de l'autorité étrangère d'enregistrement des entités de fournir ladite relation. Si un fournisseur ou une autorité d'enregistrement des entités d'un pays étranger refuse de fournir cette relation, le contrôle a posteriori ne peut être réalisé et par conséquent la garantie que des écoutes illégales ne sont pas perpétrées ne peut être offerte à ce pays. Pour ce qui est de l'accès à des communications non comprises dans la tranche d'écoute autorisée c'est l'information de la date du jour qui est systématiquement utilisée lors du calcul de la clé de chiffrement et donc de déchiffrement.

Pour conclure, selon l'idée de l'invention et grâce à la technique employée, une quelconque altération d'un élément du champ de contrôle obligatoire normalement constitué à l'origine par l'émetteur entraîne l'impossibilité de déchiffrer le message, le but étant de rendre la clé de déchiffrement fausse suite à une quelconque modification d'un champ de contrôle initialement correct. En effet, une modification, même minime, d'un quelconque des champs du champ

de contrôle obligatoire a pour résultat de modifier la clé de déchiffrement et d'interdire ainsi le déchiffrement et donc l'écoute du message. Le numéro d'agrément du matériel/logiciel permet, à l'autorité nationale de déchiffrement, d'identifier le matériel/logiciel à utiliser pour déchiffrer le message. Enfin, la date du jour permet d'assurer que le message à déchiffrer est transmis dans la bonne tranche de temps, une date incorrecte étant automatiquement détectée. Le choix de la tierce partie de confiance de récupération de clés est laissé à l'application, c'est donc un choix dynamique qui est fonction du type de l'application. De cette manière, le matériel/logiciel agréé peut "connaître" le choix et par conséquent le nom des tierces parties de confiance de récupération de clés adéquates. Ce principe même de choix dynamique fait donc que la tierce partie de confiance ne peut connaître à l'avance ce choix. L'identifiant de tierce partie de confiance de récupération de clés permet, à l'autorité nationale autorisant les tierces parties de confiance, d'identifier la tierce partie de confiance de récupération de clés choisie. La clé de dialogue est chiffrée sous la clé publique de la tierce partie de confiance de récupération de clés, elle est donc déchiffrable par cette tierce partie de confiance. Egalement, la clé de travail est chiffrée séparément sous la clé publique de la tierce partie de confiance de récupération de clés, elle est donc déchiffrable par cette tierce partie de confiance et par elle seule. De plus, la fréquence de changement de la clé de travail doit être judicieusement choisie, la solution la plus avantageuse et qui est ici préconisée, consiste à conserver une même clé de travail durant une période de temps au moins égale à une semaine. Dans ce cas, la clé de travail permet de calculer à l'avance des clés journalières intermédiaires permettant de reconstruire chaque clé individuelle de déchiffrement de l'ensemble des messages pour la tranche de temps où l'écoute est autorisée et ceci durant la période de temps choisie. Cette solution, est originale et avantageuse car elle autorise la remise de la totalité des clés nécessaires au déchiffrement des messages pour l'ensemble d'une période d'écoute considérée, il suffit pour obtenir ces clés de fournir le champ de contrôle obligatoire et la période d'écoute souhaitée. De même, selon la présente invention il est permis de discriminer, de manière indirecte mais aisée, entre des écoutes légales et illégales. Enfin, selon une variante, pour laquelle chaque champ de récupération de clé comporte de plus l'identifiant de l'entité utilisatrice ou du gestionnaire du matériel/logiciel, la tierce partie de confiance de récupération de clés peut connaître directement l'identité de l'entité utilisatrice ou du gestionnaire sans en référer au fournisseur du matériel/logiciel ni à une autorité d'enregistrement des entités utilisatrices.

Revendications:

1. Procédé de récupération de clés pour un chiffrement fort d'un message émis par une première entité, le message étant soit à stocker localement soit à transmettre à une seconde entité, une lecture du message nécessitant une clé de déchiffrement qui peut être reconstruite au moins par une tierce partie de confiance de récupération de clés, comprenant l'étape de former le message avec un champ de compensation et un champ de contrôle obligatoire, le champ de contrôle obligatoire comprenant au moins un champ de récupération de clés pour permettre à la tierce partie de confiance de fournir la clé de déchiffrement, caractérisé en ce que le champ de contrôle obligatoire comprend de plus, d'une part, en clair, la date du jour ainsi qu'un numéro d'agrément d'un matériel/logiciel de chiffrement et d'autre part, une clé de dialogue chiffrée sous une clé journalière intermédiaire.

2. Le procédé de récupération de clés selon la revendication 1, caractérisé en ce que chaque champ de récupération de clés comporte, en clair, un premier identifiant de la tierce partie de confiance, le premier identifiant étant fonction d'un type d'application, une clé de dialogue chiffré sous une clé publique de la tierce partie de confiance et, chiffrés sous la clé publique de la tierce partie de confiance, un numéro de série du matériel/logiciel agréé, une clé de travail et une période de validité de la clé de travail.

3. Le procédé de récupération de clés selon la revendication 2, caractérisé en ce que chaque champ comporte de plus un second identifiant de l'une de : i) une entité utilisatrice et ii) un gestionnaire du matériel/logiciel agréé, le second identifiant également chiffré sous la clé publique de la tierce partie de confiance.

4. Le procédé de récupération de clés selon l'une quelconque des revendications 2 et 3, caractérisé en ce que la clé de travail, combinée au moins avec la date du jour, est utilisée pour calculer la clé journalière

intermédiaire, la clé journalière intermédiaire étant utilisée pour chiffrer la clé de dialogue, ce qui permet à la tierce partie de confiance de calculer la clé journalière intermédiaire à l'avance et de la remettre à une autorité de déchiffrement durant une période d'écoute légale.

5. Le procédé de récupération de clés selon la revendication 3, caractérisé en ce qu'un matériel/logiciel de déchiffrement agréé calcule la clé de déchiffrement au moyen d'une fonction à sens unique utilisant comme paramètres la clé de dialogue échangée par ailleurs dans un protocole, ainsi qu'un résultat d'une fonction à sens unique résistante à des collisions calculée sur un ensemble de composants du champ de contrôle obligatoire, ce résultat étant combiné au champ de compensation au moyen d'un OU exclusif, ce qui permet d'utiliser une clé de déchiffrement de valeur quelconque, qui peut être de l'un d'un type : i) "clé privée", pour un algorithme asymétrique, et ii) "clé secrète", pour un algorithme symétrique, car un émetteur du message peut ajuster une valeur de la clé de déchiffrement au moyen du champ de compensation.

6. Le procédé de récupération de clés selon la revendication 4, caractérisé en ce que la tierce partie de confiance est en mesure de calculer la clé de déchiffrement au moyen d'une fonction à sens unique utilisant comme paramètres la clé de dialogue soit i) chiffrée sous sa propre clé publique soit ii) chiffrée sous la clé journalière intermédiaire et un résultat d'une fonction à sens unique résistante à des collisions calculée sur un ensemble de composants du champ de contrôle obligatoire, ce résultat étant combiné au champ de compensation au moyen d'un OU exclusif.

7. Le procédé de récupération de clés selon la revendication 4, caractérisé en ce que la tierce partie de confiance et un récepteur utilisent un même procédé de calcul pour la clé de déchiffrement qui est une fonction du champ de contrôle obligatoire et du champ de compensation, et dès lors une altération

même minime de ces champs empêche un déchiffrement correct par un destinataire du message chiffré à l'aide de cette clé de déchiffrement.

8. Le procédé de récupération de clés selon l'une quelconque des revendications 1 à 7, caractérisé en ce q'il utilise deux matériels/logiciels, d'une part un premier matériel/logiciel utilisé par une autorité nationale de déchiffrement pour extraire une partie utile du champ de contrôle obligatoire et ensuite, à partir de données renvoyées par la tierce partie de confiance, permettre de déchiffrer des données chiffrées, et d'autre part un second matériel/logiciel utilisé par la tierce partie de confiance pour fournir la clé de déchiffrement à l'autorité nationale de déchiffrement.

9. Le procédé de récupération de clés selon l'une quelconque des revendications 1 à 8, caractérisé en ce qu'une entité utilisatrice de chiffrement fort qui demande son enregistrement auprès de l'une de : i) un fournisseur de matériel/logiciel, ii) son représentant et iii) une autorité d'enregistrement des entités utilisatrices, communique, pour une validation du matériel/logiciel de chiffrement/déchiffrement, au fournisseur de matériel/logiciel, son représentant ou autorité d'enregistrement des entités utilisatrices un numéro d'agrément du matériel/logiciel de chiffrement/déchiffrement, un numéro de série du matériel/logiciel de chiffrement/déchiffrement, un nom d'entité, des coordonnées d'un gestionnaire de l'entité et la date du jour.

10. Le procédé de récupération de clés selon la revendication 9, caractérisé en ce que, lors de l'enregistrement de l'entité utilisatrice, le numéro d'agrément du matériel/logiciel de chiffrement/déchiffrement, le numéro de série du matériel/logiciel de chiffrement/déchiffrement, le nom de l'entité et les coordonnées du gestionnaire de l'entité sont mémorisés par le fournisseur dans un fichier d'audit.

11. Le procédé de récupération de clés selon l'une quelconque des revendications 9 et 10, caractérisé en ce que, pour valider une utilisation de

chaque matériel/logiciel de chiffrement/déchiffrement durant une période déterminée, une clé maître propre au matériel/logiciel de chiffrement/déchiffrement concerné est utilisée pour calculer, à partir du numéro de série du matériel/logiciel de chiffrement/déchiffrement, une clé dite diversifiée, le fournisseur du matériel/logiciel de chiffrement/déchiffrement, son représentant ou l'autorité d'enregistrement des entités utilisatrices communiquant alors à l'entité utilisatrice un droit d'utilisation du matériel/logiciel de chiffrement/déchiffrement valable pour la période déterminée ainsi que des informations permettant de personnaliser le matériel/logiciel de chiffrement/déchiffrement, le droit d'utilisation du matériel/logiciel de chiffrement/déchiffrement autorisant le matériel/logiciel de chiffrement/déchiffrement à fonctionner pour la période déterminée étant fourni sous une forme d'informations scellées sous la clé dite diversifiée et constituées d'une période d'utilisation, d'une clé publique d'une autorité nationale d'agrément de tierces parties de confiance et de l'identifiant de l'utilisateur ou du gestionnaire du matériel/logiciel de chiffrement/déchiffrement.

12. Le procédé de récupération de clés selon la revendication 11, caractérisé en ce que toute tierce partie de confiance demande son agrément auprès de l'autorité nationale d'agrément des tierces parties de confiance et lorsqu'une tierce partie de confiance de récupération de clés est agréée par cette autorité, elle est ajoutée à une liste d'un répertoire de tierces parties de confiance agréées tandis qu'un certificat d'agrément est produit sous forme électronique pour garantir une identité de la tierce partie de confiance, une valeur de la clé publique de la tierce partie de confiance, un algorithme de chiffrement à utiliser et une durée de cette garantie.

13. Le procédé de récupération de clés selon la revendication 12, caractérisé en ce que la clé publique de l'autorité nationale d'agrément des tierces parties de confiance permet au matériel/logiciel de chiffrement/déchiffrement de vérifier des certificats de tierces parties de confiance agréées pour des pays où le matériel/logiciel de

chiffrement/déchiffrement est agréé, de tels certificats permettant, en outre, à l'autorité nationale d'agrément des tierces parties de confiance de garantir, pour une durée donnée, une association entre un nom d'une tierce partie de confiance, une valeur de sa clé publique et un algorithme de chiffrement à utiliser.

14. Le procédé de récupération de clés selon la revendication 13, caractérisé en ce que, à partir d'une connaissance d'une seule clé publique spécifique à une autorité nationale d'agrément des tierces parties de confiance d'un seul pays, cette autorité nationale d'agrément délivre, de manière indirecte, des certificats d'agréments internationaux à des tierces parties de confiance par l'intermédiaire d'autorités nationales d'agrément de tierces parties de confiance d'autres pays avec lesquels une reconnaissance existe, de telle manière que lorsqu'une première autorité nationale d'agrément des tierces parties de confiance reconnaît une seconde autorité nationale d'agrément des tierces parties de confiance, cette première autorité nationale émet un certificat garantissant une valeur d'une clé de la seconde autorité nationale d'agrément des tierces parties de confiance et ainsi, de proche en proche, connaissant une clé publique de l'autorité nationale d'agrément des tierces parties de confiance d'un premier pays, une clé publique de l'autorité nationale d'agrément des tierces parties de confiance d'un second pays est validée, ce second pays validant lui-même une clé publique d'une tierce partie de confiance de récupération de clés de ce second pays.

15. Le procédé de récupération de clés selon la revendication 14, caractérisée en ce que, lorsque le matériel/logiciel de déchiffrement agréé est mis en oeuvre sans qu'aucun dépôt préalable de clé n'ait été réalisé, ce matériel/logiciel, pour son utilisation par une entité communicante, va, à partir d'identifiants de pays d'origine, obtenir, et ceci pour chaque pays communicant, des clés publiques de tierces parties de confiance qui dans certains cas pourront être choisies par défaut, chaque tierce partie de confiance étant pourvue d'un certificat délivré par l'autorité nationale d'agrément et listée dans

un répertoire, et, une fois les clés publiques de deux tierces parties de confiance de récupération de clés adéquates ainsi obtenues, le matériel/logiciel peut créer le champ de contrôle obligatoire.

16. Le procédé de récupération de clés selon la revendication 15, caractérisé en ce que, pendant une période de validité de la clé de travail, la clé de travail permet, en utilisant seulement le champ de contrôle obligatoire, de calculer et de fournir à l'avance des clés journalières intermédiaires permettant de déchiffrer toute clé individuelle de dialogue et par là même de déchiffrer un ensemble de messages pour une tranche de temps indiquée par la période de validité de la clé de travail, qui est chiffrée sous la clé publique de chaque tierce partie de confiance, cette période étant à mettre en regard de la période d'écoute légale demandée par l'autorité de déchiffrement afin de pouvoir délivrer à l'avance un ensemble ou un sous-ensemble de clés journalières intermédiaires demandées.

17. Le procédé de récupération de clés selon l'une quelconque des revendications 4 à 16, caractérisé en ce qu'un contrôle à posteriori, par une commission de contrôle, d'un contenu et d'un bien-fondé d'une demande exprimée par l'autorité de déchiffrement est effectué relativement à une identité d'une entité écoutée et à la durée de la période d'écoute, la commission de contrôle pour cela demandant soit au fournisseur, soit à l'autorité d'enregistrement des entités de lui fournir une relation entre le nom d'entité et les numéros d'agrément et de série des matériels/logiciels, tandis que de son côté la tierce partie de confiance effectue également un audit d'informations communiquées par l'autorité de déchiffrement en les stockant dans un fichier d'audit, en y associant le numéro de matériel/logiciel agréé, le numéro de série de ce matériel/logiciel et la durée d'écoute, le contrôle a posteriori étant effectué par la commission de contrôle au moyen d'une part, du fichier d'audit ainsi constitué et mis à sa disposition par la tierce partie de confiance et d'autre part, d'une relation entre le numéro de série du matériel/logiciel et l'entité utilisatrice mis à disposition par le fournisseur ou l'autorité d'enregistrement des

entités en rapprochant ces informations des informations fournies par l'autorité de déchiffrement.

18. Le procédé récupération de clés selon l'une quelconque des revendications 1 à 16, caractérisé en ce qu'un contrôle a posteriori, par une commission de contrôle, d'un contenu et d'un bien-fondé d'une demande exprimée par l'autorité nationale de déchiffrement est effectué relativement à une identité d'une entité écoutée et à la durée de la période d'écoute, la commission de contrôle pour cela demandant à la tierce partie de confiance l'identifiant de l'entité et de son gestionnaire, le numéro d'agrément et de série du matériel/logiciel, des informations communiquées par l'autorité nationale de déchiffrement et en particulier la durée d'écoute demandée par l'autorité de déchiffrement, toutes ces informations étant stockées dans un fichier d'audit tenu par la tierce partie de confiance, le contrôle a posteriori étant effectué par la commission de contrôle au moyen du fichier d'audit ainsi constitué et mis à sa disposition par la tierce partie de confiance, du fichier d'audit tenu par l'autorité nationale de déchiffrement et finalement d'un ordre judiciaire d'origine produit par l'autorité nationale de déchiffrement.

19. Le procédé de récupération de clés selon l'une quelconque des revendications 17 et 18, caractérisé en ce que la commission de contrôle peut contrôler a posteriori que des autorités de déchiffrement n'ont pas eu accès à une sémantique de communications relatives à une entité n'entrant pas dans un cadre d'un contrôle judiciaire, pour cela, soit le numéro de série du matériel/logiciel agréé permet indirectement de s'assurer de l'identité de l'entité sous écoute en rapprochant les informations fournies par l'autorité d'enregistrement des entités ou le fournisseur qui sont constituées du numéro de série du matériel/logiciel agréé associé à une liste d'entités, soit un identifiant d'une entité ou celui d'un gestionnaire, lorsqu'il est présent dans chaque partie chiffrée du champ de contrôle obligatoire, permet de s'assurer directement d'une identité d'une entité ou d'une personne sous écoute, un contenu de cette relation pouvant être demandé par la commission de contrôle

auprès des autorités d'enregistrement des entités tant nationales qu'étrangères.

20. Le procédé de récupération de clés selon l'une quelconque des revendications 17 à 19, caractérisé en ce que la commission de contrôle peut contrôler a posteriori que les autorités de déchiffrement n'ont pas eu accès à la sémantique de communications en dehors de périodes autorisées par une autorité judiciaire, grâce à la date du jour qui est systématiquement utilisée lors du calcul de la clé de chiffrement et donc de la clé de déchiffrement.