Introduction

OpenPGP GnuPG GPG GPL GNU PGP ...

Cryptographie cryptage chiffrement cryptanalyse ...

Licence logiciel libre audit algorithme brevet ...

Une introduction pour clarifier les concepts et la combinatoire complexe de tous ces termes !

SOMMAIRE

MOTS-CLÉS

- OpenPGP
- PGP Corporation
- GnuPG
- GPG
- GPL

L'histoire du système cryptographique PGP et du long procès de son fondateur

La cryptographie est une science ancienne, mais il a fallu attendre la diffusion d'ordinateurs rapides pour qu'elle soit largement adoptée. Les autorités nationales ont suivi cette évolution avec une inquiétude croissante. En effet, s'il existe de nombreux usages légitimes pour la cryptographie, elle constitue également un outil pouvant être exploité à des fins illicites. En 1991, un projet de loi du Sénat américain portant le numéro 266, qui concernait la lutte contre la criminalité d'une manière générale, comportait une disposition obligeant tous les outils de chiffrement à comporter une « porte dérobée » donnant aux autorités l'accès aux messages chiffrés. Alors même que les débats parlementaires sur cette loi étaient en cours, Phil Zimmermann combina plusieurs méthodes de chiffrement existantes pour créer un logiciel qu'il nomma « Pretty Good Privacy », ou PGP.

Si les principes mathématiques sur lesquels reposait PGP étaient connus depuis longtemps, l'innovation de Phil Zimmermann a consisté à rendre ces outils accessibles à tout propriétaire d'un ordinateur domestique. Dès ses premières versions, PGP permettait aux utilisateurs de MS-DOS de disposer d'un système de chiffrement en principe impossible à casser, tel qu'il est employé par les militaires. Tandis que les débats législatifs sur le projet de loi 266 se poursuivaient, un ami de Zimmermann se mit à distribuer PGP avec l'objectif de mettre le chiffrement fort à disposition d'un aussi grand nombre de personnes que possible. Il utilisa pour cela des systèmes BBS (des ordinateurs permettant le téléchargement de fichiers) ainsi qu'Internet, qui était à l'époque pour l'essentiel un réseau employé par les chercheurs et les universités. Ce militantisme actif contribua à l'abandon du projet de loi.

Zimmermann, qui était depuis longtemps un militant antinucléaire, était convaincu que PGP pourrait être utile aux dissidents, aux contestataires et à toute autre personne exposée à des risques en raison de ses convictions, soit un grand nombre de personnes à la fois aux États-Unis et à l'étranger. Depuis la Seconde Guerre mondiale, les États-Unis considéraient le chiffrement fort comme une menace importante pour leur sécurité interne et interdisaient son exportation. L'exportation de logiciels de chiffrement, PGP y compris, nécessitait de disposer d'une licence délivrée par le Département d'état, l'exportation vers certains

JARGON Cyptographie, chiffrer, déchiffrer

Quelques précisions terminologiques ne sont peut-être pas de trop ici.

La *cryptographie* désigne en principe une écriture secrète, mais par extension, le terme est maintenant employé pour désigner l'art de créer de telles écritures. C'est dans ce sens que nous l'utilisons dans ce livre.

La transformation d'un message pour le rendre incompréhensible à ceux qui ne disposent pas de la clé adéquate se nomme *chiffrement*, le *déchiffrement* étant l'opération inverse. Les verbes correspondants sont *chiffrer* et *déchiffrer*. Les termes cryptage/décryptage, plus récents, ainsi que les termes codage/décodage (et les verbes correspondants) ont des sens similaires et sont parfois contestés. Pour éviter toute confusion, nous n'y aurons pas recours dans ce livre.

pays étant interdite dans tous les cas. Les outils de chiffrement étaient ni plus ni moins classifiés comme des armes de guerre.

Zimmermann décida alors de contourner les restrictions à l'exportation en exploitant la différence entre écrit et logiciel. Initialement, PGP a été écrit sous forme de texte, ou « code source », qu'il faut ensuite convertir en un programme utilisable par l'ordinateur à l'aide d'outils informatiques. C'est une pratique très courante en informatique. Le texte lui-même n'est pas un logiciel, pas plus que les plans d'une voiture ne sont une voiture, mais il est tout aussi indispensable pour obtenir le produit final. Zimmermann eut donc l'idée de publier sous forme de livre le texte (le code) sur lequel reposait PGP. Bien que de nombreux livres traitant de cryptographie aient été soumis à des restrictions à l'exportation, Zimmermann réussit à obtenir une licence pour son livre de code source. C'est ainsi que PGP se diffusa dans le monde entier et devint rapidement une norme *de facto* pour le chiffrement de données.

BON À SAVOIR Exception juridique

Les livres ne sont pas considérés comme des logiciels, même lorsqu'ils contiennent du « code source », ces instructions grâce auxquelles un ordinateur peut créer un programme. Et les livres ne sont pas des armes non plus (mais vous êtes peut-être d'un autre avis si vous avez déjà laissé tomber sur votre pied l'un de ces pavés informatiques de 1 500 pages).

Bien entendu, les autorités américaines ne furent pas dupes de la manœuvre et intentèrent un procès à Zimmermann, qui dura trois ans. Ce procès fit de lui une sorte de héros de la communauté informatique. De nombreux utilisateurs téléchargèrent PGP uniquement pour avoir une meilleure idée de ce dont il était question, et finirent par l'utiliser régulièrement pour leurs propres besoins. Au cours d'auditions parlementaires, Zimmermann lut des lettres qu'il avait reçues de personnes vivant sous des régimes autoritaires ou dans des zones de guerre expliquant comment leur vie avait été sauvée par PGP, ce qui permit au public de prendre conscience de l'importance de son travail. Par ailleurs, dans la mesure où PGP avait été diffusé sur Internet avant la publication

du livre, le code était déjà disponible partout dans le monde (pour peu qu'on dispose d'une connexion Internet, ce qui n'était pas donné à tout le monde au début des années 1990). Le livre était simplement un moyen pour les personnes résidant à l'extérieur des États-Unis d'utiliser PGP en respectant les lois américaines.

L'histoire du procès de PGP est fascinante et pourrait facilement remplir tout ce livre. Pour Zimmermann et ses défenseurs, le contenu du livre était de la « parole ». Or, le Premier amendement à la Constitution des États-Unis garantit la liberté de parole. D'où d'intéressantes considérations, par exemple pour savoir où se situe la limite entre la parole et le code informatique. Par ailleurs, PGP n'avait pas été distribué par Zimmermann lui-même, mais par d'autres. Si quelqu'un en Libye téléchargeait PGP depuis le serveur du *Massachusetts Institute of Technology*, Zimmermann en était-il responsable ? Ces questions furent longuement débattues par les avocats des deux bords, mais lorsqu'il apparut que les tribunaux considéraient le Premier amendement comme ayant plus de poids que la réglementation fédérale, les autorités américaines firent marche arrière. Ce recul évita des frais juridiques supplémentaires (et la perspective d'une défaite humiliante) dans une affaire qui paraissait mal engagée pour le gouvernement et surtout, il coupa court au risque de l'établissement d'une jurisprudence qui aurait rendu plus généralement légale toute exportation en matière cryptographique. Un futur gouvernement américain pourrait toutefois remettre l'affaire sur la table s'il considère les circonstances comme plus favorables pour lui.

Que recouvrent les termes PGP, GPG et OpenPGP ?

Pour éviter toute confusion entre les sigles PGP, GPG et OpenPGP, un petit résumé peut être utile :

- OpenPGP est une norme à laquelle se conforment PGP et GnuPG, et aussi d'autres logiciels. En effet, de nombreux éditeurs de logiciels intègrent des fonctions OpenPGP à leurs produits, même si aucun n'est aussi connu ou reconnu que PGP ou GnuPG.
- PGP désigne exclusivement le produit du même nom de la société PGP Corporation. Lorsque vous voyez le mot PGP, il ne peut désigner que ce produit, et non GnuPG ni aucune autre mise en œuvre d'OpenPGP.
- Les expressions GnuPG et GPG s'appliquent spécifiquement au logiciel libre Gnu Privacy Guard.

La norme OpenPGP

PGP n'était pas seulement confronté à un procès, mais présentait certains problèmes techniques, que des cryptographes dans le monde entier ne tardèrent pas à soulever. Le problème le plus manifeste était l'utilisation par PGP des techniques de chiffrement RSA (Rivest Shamir Adleman) et IDEA (International Data Encryption Algorithm), qui étaient brevetées. En conséquence, toute utilisation commerciale de PGP nécessitait le paiement de droits aux détenteurs des brevets. Pour beaucoup d'informaticiens et de spécialistes de la sécurité, le recours à ces techniques brevetées était inacceptable parce qu'il représentait un obstacle à l'utilisation de PGP, tant pour le grand public que pour les entreprises.

Zimmermann proposa une solution en 1988, lorsque sa société, PGP Corporation, proposa une version revue et corrigée de PGP, OpenPGP, à l'IETF (*Internet Engineering Task Force*, l'organisme chargé d'élaborer les normes d'Internet). OpenPGP définit les normes selon lesquelles différents programmes peuvent communiquer entre eux, librement mais de manière sécurisée, en utilisant une version améliorée du protocole PGP et différents algorithmes de chiffrement. Ce qui permit à diverses personnes et entreprises de créer leurs propres mises en œuvre d'OpenPGP à partir de zéro en les adaptant à leurs besoins particuliers.

Un système reposant sur OpenPGP est-il vraiment sûr ?

S'il fallait une preuve du niveau de sécurité que peut offrir OpenPGP, il suffirait d'évoquer le fait que les meilleurs spécialistes en sécurité informatique y font appel, ainsi que de très nombreuses administrations nationales, grandes entreprises ou hôpitaux.

Avec une puissance de calcul suffisante, il est possible de casser le chiffrement utilisé par n'importe quelle application OpenPGP. La National Security Agency, l'agence de renseignement américaine responsable de la collecte et de l'analyse de l'information (www.nsa.gov) disposerait d'ordinateurs spécialement conçus pour casser ce type de chiffrement. Toutefois, si quelqu'un est prêt à dépenser des millions pour accéder à vos informations, il existe sans doute pour lui des moyens plus simples d'y parvenir. On peut donc dire sans risquer de se tromper que lorsqu'OpenPGP est correctement configuré et employé, il est suffisamment sûr pour inciter ceux qui s'intéressent à vos informations à choisir un autre moyen d'y accéder plutôt que de tenter de casser le chiffrement.

ATTENTION Vous avez dit sécurité ?

OpenPGP n'est pas la garantie d'une sécurité absolue. Mal mis en pratique, il peut même affaiblir votre sécurité en vous donnant l'impression que vos informations sont protégées alors qu'elles ne le sont pas. Le fait de ne pas adopter les bonnes pratiques en matière de sécurité informatique revient à fermer sa maison à clé en partant en vacances tout en laissant la clé sous le paillasson, là où n'importe qui peut la trouver.

PGP Corporation aujourd'hui

BUSINESS PGP Corporation

Pendant quelques années, PGP Corporation a appartenu à Network Associates, mais c'est aujourd'hui une société indépendante comptant parmi ses partenaires de nombreux acteurs importants du marché informatique.

Aujourd'hui, PGP Corporation est un acteur important du monde de la cryptographie et de la sécurité de l'information qui fournit des logiciels PGP pour de nombreuses plates-formes, de l'ordinateur au PDA, et pour de nombreuses applications, du courrier électronique aux dossiers médicaux en passant par la messagerie instantanée. Elle propose des versions d'OpenPGP pour la plupart des systèmes d'exploitation courants, ainsi qu'un système PGP qui s'intègre de manière transparente aux logiciels de courrier électronique les plus employés.

PGP est un produit commercial et PGP Corporation propose une large gamme de services en rapport avec ce produit. Dans ce livre, nous traiterons de la version de base, PGP Desktop ; les solutions PGP pour l'entreprise pourraient remplir un livre à elles seules. Dans la mesure où PGP est un produit commercial, il n'est pas gratuit.

Le logiciel libre GnuPG

GnuPG est un logiciel libre qui met en œuvre la norme OpenPGP et les algorithmes qu'elle désigne. Elle a été mise à disposition du public en 1999 par le développeur allemand Werner Koch, et elle est disponible dans des versions Windows et Unix, dont Linux et Mac OS X.

La licence GPL

- http://www.gnu.org/licenses/gpl.html

Dans la mesure où GnuPG respecte la norme OpenPGP (utilisable donc sans restriction car il ne se sert pas de l'algorithme breveté IDEA), il peut être employé pour communiquer avec des utilisateurs employant d'autres logiciels conformes à cette norme. « Librement disponible » signifie ici que l'on peut se le procurer gratuitement, accéder au code source qui a servi à créer le programme et que vous pouvez en faire ce que bon vous semble, comme l'énonce sa licence GPL. L'accès au code source n'intéresse sans doute qu'une minorité de lecteurs, mais elle est essentielle pour ceux qui ont besoin de l'examiner et de le modifier, condition au combien importante pour que le logiciel soit sûr.

Le nom officiel du logiciel est GnuPG, mais ce nom est fréquemment abrégé en GPG. Quel que soit le nom que vous utilisiez, les personnes connaissant OpenPGP sauront de quoi vous parlez.

PGP ou GnuPG ?

GnuPG est gratuit et libre, tandis que PGP ne l'est pas mais présente certains avantages notamment en termes de langues disponibles, de simplicité d'emploi, d'assistance technique et d'algorithmes pris en charge. Vous allez toutefois constater que pour le moment, le choix d'un logiciel de cryptographie peut s'avérer cornélien dans la mesure où chaque solution présente des avantages et des inconvénients importants.

GnuPG sous licence GPL

GnuPG est un logiciel libre. Vous pouvez l'employer comme bon vous semble, à titre privé ou professionnel. Néanmoins, si vous l'intégrez à un produit professionnel que vous revendez ensuite, lisez attentivement la licence GPL (General Public License) et respectez-la ! Vous constaterez notamment que dès lors qu'un produit utilise du code GPL, il est soumis à certaines obligations, notamment celle de reverser le code source amélioré à la communauté dont il est issu.

- http://www.gnu.org/licenses/gpl.html

VERSIONS
Langues disponibles de PGP

À l'heure actuelle, PGP n'a pas été traduit en français, uniquement en allemand et en japonais. Il se peut que cette situation change, et peut-être une version localisée sera-t-elle disponible lorsque vous lirez ces lignes. Si ce n'est pas le cas, vous devez accepter une moindre convivialité du logiciel dès lors que vous ou vos utilisateurs n'êtes pas familiarisés avec la langue de Shakespeare.

GnuPG est disponible en français. Cependant, dans la mesure où il fonctionne depuis l'invite de commande, la question de la langue a une importance moindre que s'il disposait d'une interface graphique. Vous verrez toutefois que des interfaces graphiques ont été créées *a posteriori* pour GnuPG et que l'une des meilleures d'entre elles, Enigmail, a été traduite en français.

Enigmail est une extension de Mozilla Thunderbird, un logiciel de courrier électronique gratuit d'excellente qualité. Sans vouloir trop approfondir ici (ce sera l'objet du reste du livre), retenez toutefois qu'il est possible d'utiliser GnuPG par l'intermédiaire d'une interface graphique entièrement en français, mais à condition d'utiliser le logiciel de courrier électronique Mozilla Thunderbird, lui aussi en français.

OUTIL Un logiciel libre de courrier électronique

- *Mozilla Thunderbird, le mail sûr et sans spam*, D. Garance, Eyrolles 2005.

Simplicité d'emploi

Un utilisateur de GnuPG ne doit pas avoir peur de « mettre la main dans le cambouis » de temps à autre et de faire appel à l'invite de commande de son système d'exploitation. Il existe bien pour GnuPG des modules supplémentaires qui offrent une interface plus conviviale (voir ci-dessus),

mais ceux-ci ne permettent pas toujours d'accéder à toutes les fonctions de GnuPG. De plus, lors des mises à jours de GnuPG, il n'est pas certain que ces interfaces soient également mises à niveau. Il n'est donc peut-être pas recommandé d'installer GnuPG chez son grand-père, sauf si on est prêt à lui rendre visite souvent pour régler des problèmes de configuration et d'utilisation.

C'est pourquoi, on pourra préférer utiliser PGP de PGP Corporation qui fait tout son possible pour que ses produits fonctionnent de manière transparente du point de vue de l'utilisateur final, à la manière de n'importe quel autre logiciel commercial. C'est un avantage déterminant. Si vous aviez à mettre en place une solution cryptographique unique pour le service commercial, la comptabilité et le service marketing de votre entreprise, et à condition que la langue de l'interface soit sans importance, nous vous conseillerions sans hésitation de choisir PGP, la simplicité d'emploi étant alors un facteur pertinent.

La transparence, garantie de qualité

On attribue la qualité de transparence à un logiciel selon que son fonctionnement interne est plus ou moins connu et accessible. Pour la plupart des utilisateurs, c'est un facteur sans importance : ce qu'ils souhaitent, c'est que leur logiciel fonctionne sans poser de problèmes. En revanche, pour les professionnels de la sécurité, la transparence est un facteur critique.

En effet, celle-ci leur offre une liberté, une opportunité rares : ces professionnels, leur équipes, ou d'autres personnes mandatées, pourront vérifier le code source des programmes. Ainsi, ils s'assureront qu'ils ne contiennent pas de code malveillant ou de porte dérobée (backdoor) permettant un contrôle non souhaité pendant leur exécution, et à l'insu des utilisateurs, par des individus voués à des buts non louables.

Les logiciels dont le code est ouvert peuvent être audités par de nombreux utilisateurs à travers la planète, passionnés et intéressés par les progrès qu'apportent les logiciels libres. Quel meilleur audit que celui réalisé par des centaines de bénévoles et professionnels dont les seuls buts sont de faire progresser ces outils qui permettent de protéger notre vie privée. Utiliser de tels logiciels, dont le code source est ouvert et dont les fonctionnements sont connus est un gage de sécurité et de pérennité.

TERMINOLOGIE Audit de sécurité

Les personnes qui prennent la sécurité au sérieux, dans des contextes où des vies humaines ou d'importantes sommes d'argent dépendent de la confidentialité des informations, font appel à des spécialistes pour faire examiner leurs logiciels de sécurité et s'assurer de l'absence de problèmes. Un tel processus d'examen d'un logiciel se nomme « audit ».

Sachant qu'il y a plus d'individus bienveillants que le contraire, la transparence est synonyme d'ouverture, de confiance, de sécurité.

La cryptographie est un art ancien, et l'une de ses règles essentielles est que la connaissance du fonctionnement d'un bon système cryptographique n'aide pas pour autant à le casser. Les seuls systèmes de chiffrement que les professionnels de la cryptographie prennent au sérieux sont ceux dont le fonctionnement est au contraire connu. C'est le cas du système cryptographique d'OpenPGP, parfaitement audité de manière continue depuis dix ans par des personnes qui seraient ravies d'y trouver une faille. Ce serait pour eux la gloire assurée au sein de la communauté des cryptanalystes, un peu comme pour un ingénieur d'inventer un moteur hautes performances ne consommant que deux litres d'essence aux cent kilomètres.

Toutefois, PGP et GnuPG ne se limitent pas au code des algorithmes utilisés par OpenPGP. Il y a autour de ces algorithmes une bonne quantité de code source. Un individu malveillant pourrait trouver dans le code source une faille permettant de passer outre les protections qu'offre le logiciel. Le code source nécessite d'être audité par des professionnels talentueux pour s'assurer de sa fiabilité. De par sa qualité de logiciel libre, le code source de GnuPG est librement accessible par tout un chacun, et vérifié par des personnes aux compétences de tous niveaux. Quant au code source de PGP, il est accessible aussi, mais exclusivement à ses clients ; ces derniers font toutefois fréquemment appel à des spécialistes très pointus pour l'auditer.

Algorithmes pris en charge

Les premières versions de PGP faisaient appel à des algorithmes qui étaient soumis à des brevets à l'époque de la création de PGP. Certaines de ces méthodes de chiffrement sont maintenant dans le domaine public, mais l'une d'entre elles, IDEA, est protégée par des brevets en Europe. OpenPGP est passé à des algorithmes plus récents, mais vous trouverez des références aux anciens algorithmes dans les premières versions de PGP. Vous n'avez pas besoin de comprendre ce qu'est IDEA, mais vous devez savoir le reconnaître si vous y avez affaire un jour.

GnuPG ne prend pas en charge la méthode de chiffrement IDEA parce qu'elle n'est pas entièrement libre, bien que les termes de sa licence soient très généreux : son emploi est gratuit pour une utilisation non

ATTENTION

IDEA, un composant breveté

L'algorithme IDEA étant soumis à un brevet, nous vous déconseillons fortement de l'utiliser. Si d'aventure vous receviez un élément chiffré avec l'algorithme IDEA, la meilleure attitude à adopter serait de demander à votre correspondant de vous renvoyer les informations chiffrées avec un autre algorithme. Cela ne devrait poser aucun problème à votre émetteur et vous évitera par la même d'implémenter un algorithme breveté dont l'utilisation va à l'encontre de la transparence et de l'ouverture des logiciels libres.

AVANCÉ Installation d'IDEA pour GnuPG

Si vous choisissez d'employer GnuPG et n'avez d'autre choix que d'utiliser l'algorithme IDEA, installez le module correspondant. Son code source est téléchargeable depuis l'adresse :

- ftp://ftp.gnupg.dk/pub/contrib-dk/idea.c.gz

et le fichier DLL correspondant, compilé pour Windows, depuis ftp://ftp.gnupg.dk/pub/contrib-dk/ideadll.zip. Décompressez le fichier et placez-le fichier dans le répertoire de l'application GnuPG (sous Unix, Linux, etc., vous devrez au préalable compiler le source). Ajoutez ensuite la ligne `load-extension idea` au fichier `gnupg.conf` pour disposer d'IDEA sous GnuPG. Retenez bien, toutefois, que ce module n'a rien d'officiel et que ses concepteurs n'offrent aucune garantie quant à son fonctionnement.

commerciale, et il suffit d'avoir acheté une seule fois un produit incluant IDEA pour disposer d'une licence à vie pour ce produit. Dans le cas contraire, vous pouvez acquérir en ligne une licence IDEA pour la modique somme de 15 euros. Aussi généreux qu'ils soient, ces termes de licence restent incompatibles avec celle de GnuPG. Il est possible de modifier GnuPG pour le rendre compatible avec IDEA, mais l'équipe de développement de GnuPG ne le fera pas pour vous. PGP Corporation a quant à elle payé le détenteur du brevet (la société suisse Mediacrypt). En conséquence, lorsque vous achetez PGP, vous disposez automatiquement d'une licence IDEA. Heureusement, OpenPGP ne nécessite plus d'utiliser IDEA, mais pour certaines entreprises, cette licence est néanmoins nécessaire. Si vous trouvez un fichier chiffré vieux de dix ans que vous souhaitez ouvrir, il est possible que vous ayez besoin d'IDEA. Sinon, il est superflu.

OpenPGP et la loi

OpenPGP utilise certains des algorithmes de chiffrement à clé publique les plus forts disponibles actuellement. « Fort » signifie ici que les forces de l'ordre ne pourront accéder à un fichier correctement protégé avec GnuPG, ce qui n'est pas du goût de la plupart des autorités nationales. Certains pays autorisent leurs citoyens à utiliser des algorithmes de chiffrement forts, mais d'une manière limitée seulement, et qui puissent être cassés. D'autres exigent que toutes les clés de chiffrement soient déposées auprès d'une « autorité de séquestre ».

Ainsi, si un jour vous deveniez un dangereux criminel, il suffirait aux forces de l'ordre de demander votre clé à cette autorité pour être en mesure de déchiffrer les messages qui vous incriminent. C'est un peu comme demander à un cambrioleur de fournir volontairement ses empreintes digitales avant d'effectuer un cambriolage, et tout aussi efficace.

Pour compliquer encore les choses, les lois changent régulièrement. Si vous avez des doutes concernant la législation dans ce domaine concernant votre propre pays, renseignez-vous auprès d'un spécialiste local de la sécurité ou d'un avocat. Une recherche Google portant sur « lois cryptographie » donnera plusieurs résultats intéressants ; vous pouvez aussi vous rendre sur le site http://rechten.uvt.nl/koops/cryptolaw, en anglais mais très complet. D'autres implications légales d'OpenPGP seront traitées au chapitre 11.

CONTEXTE La loi en France

Si les États-Unis appliquaient des restrictions à la diffusion de la cryptographie, la France n'était pas en reste : à l'époque du procès de PGP, c'était l'un des pays au monde les plus restrictifs en la matière, puisque le chiffrement y était tout simplement interdit sans autorisation préalable des autorités. Depuis, il a été libéralisé et il peut être employé sans risque de poursuites judiciaires. Toutefois, les autorités françaises restent extrêmement méfiantes vis-à-vis des procédés cryptographiques, comme vous le découvrirez au chapitre 11.