# Projet ICare

# La notion de PKI et le Droit

**Référence :** ICARE/CAB/TPC/DOC_5/v1
**Type :** Note de travail
**Diffusion :** Générale

**Date :** 02/05/2002
**Titre :** **ICare – La notion de PKI et le Droit**

**Auteur(s) :** Thierry Piette-Coudol, avocat

**Résumé :**
Ce document expose comment la notion de PKI est traitée (ou non traitée) dans le droit français

**TABLE DES MATIERES**

# 1. Préambule

La présente note de travail présente une réflexion actualisée sur la notion de PKI face au Droit.

Cette contribution a vocation, avec d'autres contributions sur des thèmes complémentaires ou connexes, a être intégrée dans le document "*Etat de l'art – Déliverable 1.4.*", préparé par l'ENST dans le cadre du projet ICARE, plus particulièrement dans sa 5ème partie.

# 2. Statut juridique de la PKI

## 1.1 La question de la définition légale de la PKI

Pour une gestion optimale des clés publiques, l'existence des AC est généralement ressentie comme indispensable. Par contre, l'opinion générale est plus fluctuante en ce qui concerne le besoin d'une PKI. Les divergences sont grandes sur le point de savoir si les Pouvoirs Publics et la Loi doivent se mêler de la création de la PKI ou de son exploitation.

### 2.1.1. Pour ou contre un statut juridique de la PKI

D'un côté, certains auteurs remarquent que si le besoin est manifeste pour la signature électronique et les AC qui la mettent en œuvre, l'absence de législation occasionne un véritable manque de visibilité[1]. Les candidats potentiels aux fonctions de AC sont aux prises avec trop de textes juridiques de différentes natures, ce qui les empêchent d'avoir une vision claire de leur responsabilité. Une législation spécifique sur la PKI pourrait préciser et stabiliser la matière. Mais les partisans du "moins d'Etat" rétorquent qu'il est trop tôt pour conclure que le marché ne saura pas produire des AC satisfaisants. Le danger est que le législateur ou les juristes qui l'inspirent se montrent incapables de comprendre la situation et le contexte global du Commerce Electronique y compris la connexité du débat avec les autres questions, cryptographie et signature électronique.

### 2.1.2. La coexistence de deux types de Tiers Certificateurs

Si une loi vient intervenir pour instaurer une PKI, que penser des AC qui ne se réclameraient pas de cette structure légale. En effet, certains secteurs professionnels fonctionnant en groupe fermé d'utilisateurs sont déjà en voie de créer des services à valeur ajoutée pris en charge par une entité spécifique. Dit d'une autre façon, ils créeront une AC "propriétaire". Ce type d'AC ou d'Infrastructure ne serait pas pour autant dépourvu de base juridique, mais le fondement serait contractuel et non plus légal c'est-à-dire provenant d'une loi.

La Loi de réforme des télécommunications de décembre 1990 a déjà intronisé les *groupes fermés d'utilisateurs* (GFU) qui bénéficient de la plus grande liberté à l'intérieur du groupe. Ainsi un statut d'origine légale ne s'appliquerait pas obligatoirement à une PKI de groupe fermé. On ne peut cependant pas penser qu'aucune interconnexion technique ne serait jamais établie entre le groupe fermé et les utilisateurs des réseaux ouverts et que les utilisateurs d'une PKI fermée ne rencontreraient pas ceux d'autres PKI. Faudra-t-il alors déclarer PKI pionnières hors-la-loi ?

La Commission Nationales des Nations Unies pour le Développement du Commerce International (CNUDCI) a développé une autre position[2]. Pour la Commission, la coexistence de deux types d'infrastructure, Infrastructure

[1] Cf. "*Public Key Infrastructure and Digital Signature legislation : Ten Public Questions*" par Bradford BIDDLE dans Cyberspace Lawyer, 1997 vol.2, n°2

[2] Voir le Rapport du Groupe de Travail sur le Commerce Electronique, 31ème session, New York 18-28 février 1997, A/CN.9/437, 12 mars 1997.

de fondement légal ou sans fondement légal va devenir une réalité. Naturellement la Commission y voit une différence : toute PKI instrumentée par une Loi pourra bénéficier des effets conjugués de cette loi et des textes portant sur des matières et des questions connexes, notamment la validation juridique de la signature électronique. Rien n'est moins sûr pour une PKI de groupe fermé. Cependant il faudra gérer l'interopérabilité entre les deux mondes. L'interopérabilité se produira au niveau des certificats électroniques. La CNUDCI estime que si la PKI fermée produit des certificats dans des conditions acceptables pour les PKI nationales, la validité de ces certificats devrait être reconnue. Mais par quelle Autorité ?

**2.1.3. Quel rôle pour l'Etat ?**

En définitive, cette dernière question renvoie à la détermination du rôle de l'Etat. L'Etat comme dans de nombreux domaines techniques joue plusieurs instruments dans la même partition : rôle de régulateur, rôle de prescripteur et rôle d'utilisateur. Mais souvent dans son rôle de régulateur qui s'analyse autant en régulation économique et sociale qu'en réglementation juridique, la problématique consiste à déterminer s'il doit agir ou non. La 9ème recommandation du Livre Blanc de IALTA indiquait que l'Etat doit réglementer les échanges dont il est partie prenante, mais qu'il ne doit pas s'impliquer dans les autres types d'échange, en dehors de faire respecter le cadre juridique existant. (par exemple, dans le cas de relations entreprises/consommateurs, cela pourrait se traduire par l'élaboration de règles minimales pour les AC et CPS).

**2.1.4. Définition et structure de la PKI**

Il n'y a pas en l'état actuel de définition légale de la PKI, ni dans la Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques ni dans la loi française n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

Une définition "officielle" de la PKI peut être recherchée dans des sources extérieure. On peut relever celle du Service de Sécurité des Télécommunications du Gouvernement fédéral du Québec qui définit la PKI ainsi qu'il suit :

*Qu'est-ce qu'une Infrastructure de Clés Publiques ?*

*Il s'agit d'un système de gestion de clés de chiffrement et de délivrance de certificats qui permet les transactions financières électroniques et l'échange d'information de nature délicate entre deux étrangers et ce, en toute sûreté. Une PKI offrira des services de protection de la vie privée, contrôle d'accès, d'intégrité, d'authentification et de non-répudiation pour les applications informatiques et les transactions de commerce électronique. Une PKI assurera*

- *la gestion de la génération et de la distribution des paires de clés publique/privée ;*
- *la publication de la clé publique et de l'identité de chaque utilisateur sous forme de "certificats" dans des babillards ouverts (les répertoires X.500).*

*Une PKI permet, avec un haut niveau de confiance :*

- *d'assurer la protection des clés privées ;*
- *de veiller à ce que des clés publiques données soient véritablement reliées à des clés privées données ;*
- *de vérifier que la partie qui possède une paire de clés publique/privée est bien qui elle prétend être.*

## 1.2 La PKI en pratique

### 2.2.1. Le besoin d'une PKI

#### 1.2.1.1 Une infrastructure pour répondre aux besoins des utilisateurs

Les juristes américains de l'American Bar Association aux Etats-Unis se sont les premiers saisis d'une matière qui relèvent davantage du management global des Systèmes d'Information que du Droit. L'ABA a édité les *Signature Guidelines* accompagnés de l'*US Model Digital Signature Law* en 1995. Cette Loi modèle ensuite portée à la CNUDCI (Commission des Nations Unies pour le Droit Commercial International) est devenue une des bases pour la préparation de sa *Loi-Modèle pour le Commerce Electronique*. La CNUDCI continue ses travaux sur le thème de la certification et de la signature électronique, tandis que la Chambre de Commerce Internationale à Paris, sous la férule des juristes américains, a préparé l'implémentation technique des éléments de management juridique dans le projet *Guidec*. Il est remarquable que tous ces éléments et travaux concourent à la satisfaction des mêmes besoins, bien qu'il manque un modèle général permettant de les intégrer, aussi bien au plus haut niveau qu'à celui des utilisateurs de base.

Des réflexions ont été menées sur cette question en plusieurs endroits du monde et le modèle de management pratique que constitue la PKI a été défini s'appliquant tant aux travaux des groupes nationaux ou internationaux qu'aux AC. La PKI favorise l'émergence de la signature électronique. Sans préjuger des effets juridiques finaux de la signature électronique, cette dernière doit rester conforme aux règles et normes tout au long de l'échange électronique, tant au niveau de l'authentification que de l'intégrité. La cryptographie joue sur ces points un rôle essentiel. La PKI est transversale aux technologies de la communication : contrairement aux premiers travaux de la signature électronique qui visaient principalement l'EDI, la PKI est neutre au point de vue technologie car elle ne vise qu'à organiser le contexte d'utilisation du certificat. Les avantages de la PKI valent pour l'EDI autant que pour Internet (email et WEB). Comme la structure a pour but d'organiser la nouvelle profession et de veiller à la déontologie générale tant entre les Tiers, qu'entre les Tiers et leurs clients et qu'entre les Tiers et les Pouvoirs Publics, la structure est communément hiérarchisée sans que cela ne soit une obligation.

#### 1.2.1.2 La PKI entre technique et management

Aujourd'hui, une PKI est un système de gestion de clés de chiffrement et de délivrance de certificats qui permet les transactions commerciales et financières en toute sécurité. Une PKI offre des services de protection de la vie privée, contrôle d'accès, d'intégrité, d'authentification et de non-répudiation pour les applications informatiques et les transactions de commerce électronique. Pour tenter de synthétiser le tout, une PKI est un ensemble cohérent de matériel, logiciel, base de données, réseaux, procédures de sécurité et d'exigences légales. Dans le monde technique, l'authentification s'est rapprochée de l'intégrité avec la signature électronique. La PKI est aujourd'hui designée et réalisée dans le cadre de la signature électronique. La dimension technique est déclinée et traduite en solution pour l'utilisateur final. Avec les aspects juridiques auxquels font appel la signature électronique, on s'éloigne encore un peu de la sphère technique.

La PKI doit être apte à inclure l'AC ou les AC ainsi que les d'autres Tiers de Confiance. Elle organise la pratique professionnelle et de veille à la déontologie générale entre les tiers de confiance, qu'entre les Tiers et leurs clients et qu'entre les Tiers et les Pouvoirs Publics :

- La PKI est garante de la compétence professionnelle des Tiers. D'une part, elle fournit les éléments d'information nécessaires pour que les entités intéressées deviennent AC. D'autre part, elle permet l'intégration des Tiers dans la structure. Le modèle organise l'interopérabilité dans les échanges de certificats électroniques ;
- Ce modèle crée et maintient l'expertise et la déontologie entre les Tiers permettant le développement de la "confiance" chez l'utilisateur en ce qui concerne la portée des services fournis et la responsabilité encourue ;
- Le modèle est un exercice théorique dont la Loi n'a pas à susciter obligatoirement la création. Cependant par la suite, la Loi peut reconnaître le modèle ou sa mise en pratique.

**2.2.2. Le concept de PKI dans le monde**

Si l'intérêt d'une PKI n'est pas à démontrer pour les spécialistes, force est de constater qu'il existe peu de PKI déclarées, alors que la Directive communautaire pour un cadre commun de la signature électronique n'en dit pas un mot, quoique qu'elle traite des AC.

### 1.2.1.3 La difficulté de dresser un bilan international

Actuellement il semble que les moyens et mesures techniques à mettre en œuvre dans la PKI sont définis et suffisamment stables. La préoccupation principale devient la régulation de l'infrastructure et de son contexte. Une partie de la régulation concerne le savoir-faire technique et peut être organisée par les techniciens et les utilisateurs finaux. Mais d'autres questions sont du ressort de la régulation juridique c'est-à-dire de la Loi ou éventuellement du contrat. Les PKI ont pour mission de sécuriser les échanges électroniques en général et en particulier, le Commerce Electronique. Aussi une grande part de la régulation juridique sera-t-elle placée sous les auspices du droit commercial, national ou international, quoique la cryptographie fasse l'objet d'un traitement juridique. La plupart du temps, la cryptographie est le seul pan de la régulation juridique existante, alors que les autres sont à établir. La PKI dans l'immaturité du concept soutient la comparaison avec l'iceberg. La plus grande partie est immergée et manque de transparence pour l'utilisateur final, alors que la partie visible est la régulation juridique, le plus souvent la réglementation de la cryptographie.

Dresser un bilan des PKI revient à tenter une synthèse de débats et travaux, principalement dans le domaine juridique, dans trois domaines différents qui sont : les PKI elles-mêmes, la cryptographie et les AC, le Commerce Electronique. Les initiatives dans ce domaine se situent à tous les niveaux territoriaux. Il existe des initiatives "internationales" qui sont le fait d'organisations internationales comme celles qui ont déjà été citées. Il y de nombreuses initiatives nationales en Utah (USA), en France, au Canada, au Québec. On ne peut faire autrement que de qualifier d'initiatives" des actions qui sont de différentes natures : des Lois ou projet de lois, des "Lois modèles" provenant d'organisations internationales et proposées au législateur national, des instruments juridiques de référence préparés dans des groupes de travail internationaux et proposés aux utilisateurs nationaux, par exemple les Guidelines de l'ABA, les normes ou prénommes issues d'organisation de normalisation, les projets et les réalisations techniques, enfin les études générales, nationales ou sectorielles.

### 1.2.1.4 L'Union Européenne et la PKI

La position de l'Union Européenne en matière d'Infrastructure a été exprimée dans sa Communication COM(97)503 "*Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et la cryptographie"*. Au chapitre des mesures, le texte annonce les intentions de la Commission :

> *La Commission encourage l'industrie et les organisations internationales de normalisation à développer des normes techniques et d'infrastructure pour les signatures numériques et le chiffrement, afin d'assurer un usage sûr et en confiance des réseaux, et de respecter les obligations en matière de protection de la vie privée et des données. La Commission va réfléchir à des mandats spécifiques ou des obligations en matière de normalisation, et proposer, en étroite collaboration avec les Etats membres, l'industrie et la communauté des usagers (entreprises, consommateurs, citoyens), des mesures permettant de soutenir les travaux dans ce domaine.*

La Commission ne se reconnaît pas un pouvoir d'action directe en la matière. Classiquement pour tout ce qui concerne les normes techniques, elle renvoie aux organisations spécialisées, UIT ou ISO au niveau international ou le CEN-CENELEC (Centre Européen de Normalisation) ou l'ETSI (organisme de normalisation des télécommunications) au niveau européen. Elle peut par contre soutenir les projets techniques initiés par l'industrie européenne. A travers plusieurs programmes de la Commission, on peut relever le soutien et des subventions versées à des projets comme DEDICA, ICE-TEL, E2S.

Le projet FAST des chambres de commerce européennes pour construire une PKI européenne peut également être signalé. FAST (pour *First Attempt to Secure Trade*) est un projet abouti du programme TEDIS 2 (programme de promotion de l'EDI) de la Commission de Bruxelles concernant la branche "Autorités d'Enregistrement et de Certification. Le consortium d'études était formé de diverses chambres de commerce européennes, d'opérateurs postaux et de télécommunications, d'opérateurs EDI et de fournisseurs de RVA et de consultants. Ce projet visait déjà au début des années 1990 à établir sur une base européenne un réseau de

certificateurs électroniques pour le monde EDI. On y prévoyait que la fonction de certification électronique, employée à l'occasion de la signature électronique apposée sur les messages EDI afin d'en sécuriser l'échange, serait confiée aux chambres de Commerce. Le projet illustrait bien l'organisation hiérarchique de l'infrastructure globale (à clé publique) par l'enregistrement et l'accréditation des chambres de commerce locales par la chambre de commerce (ou l'organisme assimilé) nationale, les structures nationales étant chapeautées par la Chambre de Commerce Internationale dont le siège est à Paris. Le projet a éprouvé des difficultés pour passer du stade du pilote expérimental à celui de l'exploitation en grandeur réelle, avec pour principale raison le développement continu des concepts, des protocoles et des standards.

On voit aussi apparaître dans citation ci-dessus, un point important de l'auto-limitation de la Commission, la distinction signature électronique / chiffrement. En termes de finalité, la Commission parie que la signature électronique participera à la validité des échanges électroniques, en particulier dans le Commerce Electronique. Cet objectif rentre dans la mission générale de l'Union Européenne pour le bénéfice des Etats-membres. A l'opposé en prétendant réguler la confidentialité des échanges électroniques, elle rencontrerait l'opposition de certains Etats-membres qui mettraient en avant les impératifs de la sûreté intérieure et de la défense nationale. Cette situation explique que la Commission est prête à participer à la régulation des infrastructures, sous réserve de la compétence de normalisation technique des organisations internationale, largement en matière de signature électronique mais plus prudemment en matière de chiffrement. Comme exposé dans le document COM 503 :

*Le Traité CEE et le Traité d'Union européenne respectent pleinement la compétence des Etats membres dans les domaines de la sécurité nationale et de l'application du droit. Si des restrictions nationales sont établies, elles doivent rester compatibles avec la législation communautaire. La Commission va examiner si des restrictions nationales peuvent être totalement ou partiellement justifiées, en particulier au vu des dispositions du Traité en matière de libre circulation et des dispositions de la Directive communautaire sur la protection des données.*

Comme le concept de PKI intéresse principalement les AC dans un cadre précis, celui de la signature électronique, on se serait attendu à une position plus précise dans les discussions autour de la Directive signature électronique. Même si certains des éléments d'une PKI sont présents dans la proposition de Directive sur la signature électronique, la notion de PKI n'est ni imposée ni même suggérée. Ce qu'on peut trouver étrange ou regrettable compte tenu des aspects juridiques particulièrement significatifs de cette Directive. La Commission ne renvoie pas au standard X.509 v.3. mais préfère un système technique plus vague comportant tout de même des certificats, mais sans faire référence au modèle d'organisation de la cryptographie à clé publique, la PKI.

#### 1.2.1.5 De la PKI à l'ICG

Le concept de PKI est donc intimement lié à la signature électronique. Le concept se montre alors étriqué parce qu'il ne s'étend pas aux Tiers de Confidentialité (chiffrement des messages) et qu'il laisse de côté la cryptographie symétrique en se centrant sur la gestion des clés publiques / clés privées. L'usage de la cryptographie est une question transversale au modèle de la PKI. La réglementation française, fort riche sur la question de la cryptographie n'apporte pas d'information sur une éventuelle PKI qui serait présente derrière les applications utilisant la cryptographie. La réglementation est minimale en ce qui concerne l'utilisation de la cryptographie dans le cadre de la signature électronique. Aussi on ne s'étonne pas que dans ce domaine non plus, la PKI ne soit n'y imposée ni même suggérée.

Dans le cas français, la réglementation sur la cryptographie est une forme de régulation juridique produite par l'administration, à son bénéfice exclusif en terme de contrôle. On se trouve dans la sphère d'un droit administratif général (encadrement des activités professionnelles) qui fut longtemps droit administratif spécial (affaires militaires). La PKI a une toute autre vocation : l'établissement concret des moyens susceptibles d'asseoir les relations de confiance entre les AC et leurs utilisateurs, une confiance qui constitue le liant des relations d'affaires. On se trouve dans la sphère du droit commercial. L'obligation réglementaire est-elle suffisante pour rendre compte des relations entre les deux organismes agréés et des relations des organismes agréés avec leurs clients ? D'autres concepts sont prêts à prendre la relève avec une finalité beaucoup plus fédératrice. Le Département de la Défense (DoD) des USA a ainsi élaboré le concept de KMI. Dans une présentation disponible sur le Web, le DoD définit les différents concepts d'infrastructure utilisables pour la sécurité des échanges électroniques et montre comment ils procèdent l'un de l'autre.

A partir de cette modélisation, on peut avancer les contenus suivants pour les structures :

- L'Infrastructure de Clé Publique ("PKI") : les cadre et services qui fournissent la génération, la diffusion, la production, le contrôle et la dimension financière des certificats de clé publique (lié à la signature électronique).

- L'Infrastructure de Gestion de Clé ("KMI") : les cadre et services qui fournissent la génération, la diffusion, la production, le contrôle et la dimension financière des certificats de clé publique et les clés de cryptographie symétrique.
- L'Infrastructure de Gestion de la sécurité ("SMI") : tous les services d'une KMI plus des services supplémentaires associés au téléchargement de logiciel, à l'audit, à la détection d'intrusion et à la gestion de mot de passe.

Selon le Département américain de la Défense, les services fournis par une IGC seraient les suivants :
- Certification de clés publiques (Autorités de Certification, serveurs de certificats)
- Distribution de Clés Publiques (répertoire de clés)
- Gestion de clés, demande de clés, génération et production de clés
- Dénombrement des clés, révocation de certificats, recouvrement de clés
- Développement des Politiques, évaluation et mise en application

D'un autre point de vue, on dira qu'il réconcilie le monde de la cryptographie, en intégrant la cryptographie symétrique et les Tiers de confidentialité. Le concept d'IGC est sans doute le plus fédérateur : il devrait permettre d'intégrer à leur heure tous les autres types de Tiers comme les "Tiers Archiveurs", les "Tiers Horodateurs" et autres "Tiers assureurs" (rapport Lorentz). La normalisation ISO réalisée par le JAC1/SC27 ou le AC68/SC2, l'approche de l'ETSI groupe STAG et celle de la DGXIII dans les projets ETS montrent que de nombreuses autres fonctions ou services peuvent s'intégrer dans les Infrastructures, pris en charge par des Tiers spécifiques ou non.

### 2.2.3. Le concept de PKI en France

En ce qui concerne la France, la notion de PKI y est connue. D'autres part, certaines études françaises parlent d'une "*Infrastructure de Gestion de Clés*" (IGC) qui semble correspondre au concept américain de KMI. Il est difficile actuellement d'être plus précis faute d'une référence au niveau international. Les instances internationales de normalisation, comme l'UIT et l'IETF pourraient être saisies prochainement de propositions pour une définition commune et standard des KMI/IGC.

Le concept d'IGC a fait son apparition en France dans les milieux administratifs. Il est tout d'abord au centre des travaux de la Commission Interministérielle pour la Sécurité de Systèmes d'Information (SSII). Ainsi le document "*Procédures et Politiques de certification de clés*" dit PC2 établit-il un début de régulation interne d'une Infrastructure de Gestion de Clés. Cependant le contenu du document ne permet pas de déterminer avec exactitude si l'IGC visée est bien différente de la classique PKI. Pourtant certains schémas laissent voir des Tiers de séquestre dans le réseau hiérarchisé d'une PKI à côté des AC. Il existe une intention d'intégrer dans un ensemble cohérent les systèmes de chiffrement par cryptographie symétrique, qui semblent encore la majorité sur le marché. Le marché ne présente pas une offre de logiciels et services de signature électronique très importante mais plusieurs produits permettent simultanément l'authentification, l'intégrité et la confidentialité à partir de moyens de cryptographie asymétrique. Comme on le voit, l'IGC fédère toutes les variétés de Tiers, Tiers de certification (signature électronique et chiffrement) et Tiers de confiance (tiers de séquestre des clés pour le chiffrement), sans oublier les Autorités d'enregistrement.

Les études récentes de l'ATICA montrent tout l'intérêt de l'administration pour les IGC.

Pour le secteur privé, même s'il n'est pas nommé, le concept d'IGC est naturellement en œuvre dans les travaux e-business préparés notamment par Electronic Commerce Europe[3] (EcE). Cette association prépare au niveau européen et en concertation avec la Commission des études et projets qui mêlent *e-commerce*, *e-administration* et *e-finances*. Les concepteurs sont des professionnels issus de grands groupes industriels et commerciaux européens. Leur point de vue est pratique ; ils visent à l'efficacité commerciale dans leurs travaux. Sur la base d'*extranet sécurisé*, les projets de l'EcE proposent des solutions en termes commerciaux et les fonctions de certification et de notarisation balisent le domaine électronique pour apporter aux acteurs de maximum de sécurité. Le profil des membres explique la maturité des propositions de l'EcE : en matière de certification

[3] Electronic Commerce Europe est une association européenne non lucrative de droit belge dont le siège est à Bruxelles. Son objet est de contribuer à l'expansion du Commerce Electronique en Europe. L'association se veut l'émanation des grandes entreprises industrielles et commerciales et des communautés professionnelles d'utilisateurs. La vision globalisante et fédératrice des travaux des membres sont remarquables dans les projets e.TRANS.@ction et SYNAPSE.
URL : http:WWW.ec-europe.org

électronique également, il faudra sortir rapidement des aspects purement techniques pour raisonner en termes de solution.

Les professionnels intéressés, réunis dans des communautés professionnelles d'utilisateurs, ont en général la préoccupation moins de réaliser une IGC qu'une *PKI orientée utilisateur*.