

Distr.  
GÉNÉRALE

CES/SEM.47/12  
1 mars 2002

FRANCAIS seulement

**COMMISSION STATISTIQUE et  
COMMISSION ÉCONOMIQUE POUR L'EUROPE**

**COMMISSION DES COMMUNAUTÉS  
EUROPÉENES**

**CONFÉRENCE DES STATISTICIENS  
EUROPÉENS**

**EUROSTAT**

**Séminaire commun CEE-Eurostat sur les  
Systèmes intégrés d'information statistique  
et les questions connexes (ISIS 2002)**  
(Genève, Suisse, 17-19 avril 2002)

Point II: Sécurité des communications et confidentialité des données

## **UTILISATION DES INFRASTRUCTURES DE CLÉS PUBLIQUES À L'INSEE**

### **Communication sollicitée**

Rapport envoyé par l'INSEE, France <sup>1</sup>

## **I. INTRODUCTION**

1. On vise dans cet article à dresser un panorama rapide des utilisations à l'INSEE, effectives ou prévues, des infrastructures de clés publiques (ICP) et des technologies associées. Ces utilisations, quoique modestes et se situant dans un contexte encore balbutiant, mettent en lumière des problématiques variées qui peuvent intéresser d'autres instituts de statistiques.

2. Après quelques rappels rapides, on indique le contexte général dans lequel se situe l'institut en matière d'ICP, puis les principes d'utilisation qu'il s'est fixé. On décrit ensuite quelques cas d'utilisation des techniques de certification électronique, pour des entités dépendant de l'INSEE et pour des entités extérieures. Une rapide conclusion tente de tirer quelques enseignements à ce stade encore précoce.

### **A. Statistique et sécurité**

3. Comme tout institut statistique, l'INSEE collecte, traite, stocke et diffuse un grand volume de données, et entretient pour ce faire des flux d'information nombreux et variés avec une large gamme de partenaires. Ces données et ces flux requièrent des services de sécurité différenciés, notamment en matière de confidentialité et d'intégrité. En particulier, le secret de certaines informations est garanti par la loi.

---

<sup>1</sup> INSEE: Institut National de la Statistique et des Études Économiques; communication préparé par Franck Cotton (franck.cotton@insee.fr).

4. Tout en laissant de côté les aspects de disponibilité des données, on peut donner quelques indications sur les services de sécurité pertinents lors des différentes phases de l'activité statistique :

- Lors de la collecte d'information, il est nécessaire d'assurer l'authentification du fournisseur de données, de même que celle de l'institut comme destinataire de l'information ; par ailleurs, l'intégrité des informations doit être garantie ainsi, assez fréquemment que leur confidentialité (données individuelles, financières, etc.).
- Lors du traitement de l'information, les mêmes services d'intégrité et de confidentialité doivent être assurés ; en outre, pour certaines données sensibles, les questions de gestion des droits d'accès et d'authentification des agents autorisés se posent avec une acuité particulière.
- Lors de la diffusion de l'information, l'institut doit être authentifié comme émetteur, voire comme propriétaire de l'information ; l'authentification du destinataire de l'information peut également être nécessaire (retour d'information personnalisé, diffusion commerciale, etc.) ; de plus, les questions d'intégrité et de confidentialité peuvent se poser en des termes renouvelés (non altération des produits, respect du secret statistique et de la réglementation en matière de gestion de données individuelles, gestion d'embargo, propriété intellectuelle, ...).

5. Avec la dématérialisation des échanges, ces questions de sécurité se posent de manière radicalement nouvelle : des systèmes de confiance souvent relativement informels, basés sur les contacts en face à face, l'écrit, les services postaux, téléphoniques, etc., doivent trouver leur équivalent dans le monde numérique, et il ne fait pas de doute pour beaucoup que les techniques de certification électronique joueront un rôle crucial dans ce changement.

## **B. Certification électronique - Rappels**

6. On rappelle rapidement dans ce paragraphe quelques principes de fonctionnement des techniques de certification électronique et des ICP. Le lecteur familiarisé avec ces notions pourra passer directement à la partie suivante.

7. Les infrastructures de clés publiques s'appuient sur la cryptographie asymétrique, concept datant du milieu des années 1970, en vertu duquel chaque entité dispose d'une paire de clés liées mathématiquement et telles que tout message chiffré, selon un algorithme adapté, avec l'une des clés ne peut être déchiffré qu'avec l'autre. L'une des clés est publique, par exemple stockée dans un annuaire à accès libre ; l'autre, souvent nommée clé privée, est secrète et ne peut être déduite de la clé publique.

8. Pour expédier confidentiellement un message à un correspondant, il suffit de le chiffrer avec la clé publique de ce dernier : il sera seul à pouvoir déchiffrer le message, et ce grâce à sa clé secrète. Inversement, en chiffrant un message (ou le plus souvent une empreinte de ce message) par sa clé privée, un correspondant garantit son origine, et cela peut être vérifié par tout le monde grâce à la clé publique du signataire.

9. La cryptographie asymétrique possède de nombreux avantages par rapport à la cryptographie classique (dite symétrique) dans laquelle la même clé sert à chiffrer et déchiffrer le message. En particulier, elle évite d'avoir à convenir de clés secrètes avec ses correspondants, et donc permet d'envoyer des messages confidentiels à des destinataires sans contact préalable, fonctionnalité indispensable au développement des échanges dématérialisés. Elle dispense par ailleurs d'avoir à gérer autant de clés secrètes que de correspondants : chaque entité n'a que deux clés. De plus, elle est la seule à pouvoir fournir des services fiables de signature électronique, du fait de l'existence d'une clé secrète individuelle : en cryptographie symétrique, toute clé est connue par au moins deux intervenants.

10. Les algorithmes de cryptographie asymétrique sont toutefois très consommateurs de ressources de calcul, ce qui explique qu'ils sont le plus souvent utilisés en association avec des algorithmes classiques : ils ne servent alors que pour l'établissement d'une clé symétrique temporaire (le cas typique est celui du protocole SSL, très utilisé sur l'Internet). Beaucoup plus grave, le concept même de clé publique rend la cryptographie asymétrique sensible aux attaques par interception : une personne mal intentionnée peut se faire passer pour une autre et substituer sa clé publique à celle de cette autre personne <sup>2</sup>, ce qui peut lui permettre d'intercepter et de déchiffrer les messages confidentiels adressés à sa victime.

11. C'est pour éviter les attaques par interception qu'a été introduite la notion de certificat numérique : celui-ci associe, en général pour une durée et un usage donnés, une clé publique et une identité. Cette association est garantie (c'est-à-dire signée numériquement) par un tiers de confiance, l'autorité de certification, dans le respect d'une politique de qualité, la politique de certification, qui précise notamment la nature des vérifications qu'effectue l'autorité avant de délivrer le certificat (contrôle de l'identité du demandeur, preuve de possession de la clé privée, etc.).

12. C'est l'ensemble des matériels, logiciels, personnes, règles et procédures mis en œuvre par une autorité de certification pour créer, gérer, stocker, distribuer et révoquer des certificats basés sur la cryptographie à clés publiques qui est appelé une infrastructure de clés publiques. Afin de signer les certificats qu'elle fournit, l'autorité de certification possède elle-même un certificat, qu'elle peut s'être attribué elle-même, ou qui peut lui avoir été fourni par une autre autorité de certification : on peut par ce biais construire des relations d'approbation entre autorités de certification ou entre ICP, voire de véritables hiérarchies ou réseaux de confiance permettant de relier des entités qui peuvent ne pas se connaître *a priori*.

## II. LE CONTEXTE

13. Pour prendre en compte le développement des échanges dématérialisés, l'INSEE a décidé dès 1999 d'investir dans les technologies liées à la certification, accompagnant en cela les évolutions en cours dans la société française en général et dans la sphère administrative en particulier. Le contexte national est en effet marqué par la transposition en droit français de la directive européenne de décembre 1999 sur la signature électronique, qui est en cours, ainsi que par de nombreuses initiatives de l'État pour promouvoir la « e-administration », initiatives stimulées par un plan gouvernemental annoncé début 1998 et relayé depuis par de nombreuses mesures (en particulier en matière de libéralisation de la cryptographie).

14. Parmi ces initiatives, il faut noter celle du ministère de l'économie, des finances et de l'industrie (MINÉFI), dont l'INSEE est une Direction générale, qui a mis en œuvre une politique très volontariste de développement des téléprocédures ; ainsi, les plus grandes entreprises sont, depuis le début de l'année 2002, contraintes par la loi de déclarer et de payer leur TVA en ligne : 25 000 télédéclarations ont été enregistrées pour le mois de janvier 2002, et une forte montée en charge est attendue d'ici la fin de l'année. La dématérialisation d'autres procédures, concernant les entreprises ou les particuliers, est également prévue.

15. Le cadre général de ces opérations a été défini il y a quelques années ; en particulier, la réflexion transversale portant sur la sécurité a conduit à qualifier les besoins en matière d'authentification des intervenants et en matière d'intégrité et de confidentialité des données échangées, et en conséquence à établir l'utilisation de certificats électroniques comme l'un des principes directeurs pour la sécurisation des téléprocédures.

16. À l'appui de cette politique, le MINÉFI, plutôt que d'attribuer lui-même des certificats numériques aux entreprises, a mis au point un dispositif de référencement de certificats fournis par des ICP externes, commerciales ou corporatives. Un document public, la politique de certification-type, définit les critères de référencement des certificats et un processus d'évaluation reposant sur un questionnaire très détaillé permet

---

<sup>2</sup> Par exemple dans l'annuaire où sont publiées les clés publiques, ou dans un message destiné à une tierce personne.

de vérifier la conformité à cette politique et à la réglementation des certificats et des services fournis par une ICP externe, ainsi plus généralement que leur niveau de qualité.

17. Cette initiative a largement contribué à développer le marché de la certification pour les entreprises, et l'on compte maintenant une vingtaine de fournisseurs de services de certification commerciaux en France, dont la plupart des grands réseaux bancaires, parmi lesquels une bonne dizaine sont référencés par le MINÉFI. Il faut noter par ailleurs que d'autres organismes publics retiennent des approches comparables à celle du MINÉFI (cas du ministère de l'intérieur pour la communication sécurisée avec les collectivités territoriales), voire se proposent d'adopter purement et simplement sa politique de référencement.

18. Pour ce qui est de ses besoins propres, en particulier la certification des serveurs de téléprocédures et de leurs opérateurs, le MINÉFI a entamé le déploiement d'une infrastructure privée de gestion de clés. Il est prévu que cette ICP ait une structure fédérative, chacune des grandes directions du ministère étant responsable de sa propre ICP et l'ensemble étant regroupé sous la coupe d'une ICP racine commune. Des projets sont par ailleurs en cours au niveau gouvernemental pour la mise en place d'une autorité de certification qui pourrait servir de racine pour toutes les autorités de l'administration.

### **III. L'ICP DE L'INSEE – PRINCIPES ET ÉTAT D'AVANCEMENT**

19. Pour sa part, l'INSEE s'inscrit naturellement dans la politique générale de développement de l'économie numérique conduite par le gouvernement. Une infrastructure de clés publiques interne a été construite à partir de la fin 1999, et diverses applications utilisant les techniques de certification ont été réalisées ou sont à l'étude. Pour cadrer les développements dans ce domaine assez nouveau, deux lignes directrices ont été fixées, en cohérence avec les orientations générales que le MINÉFI précisait à la même période ou a indiquées depuis :

- L'INSEE couvre lui-même ses besoins de certification internes, c'est-à-dire notamment qu'il certifie ses personnels et ses ressources informatiques.
- Pour la certification des entités externes avec lesquelles il est amené à entrer en relation, l'INSEE se repose sur l'utilisation de services de certification extérieurs, dont il peut être préalablement amené à vérifier l'adéquation par une procédure d'homologation plus ou moins formalisée.

20. Bien entendu, ces propositions doivent être déclinées et adaptées dans les différentes situations réelles, ainsi qu'on le verra dans la suite. En particulier, le niveau de développement des schémas de certification externes et l'état des méthodes et des outils permettant de mettre en pratique leur homologation peuvent parfois conduire à adopter des solutions qui n'obéissent pas pleinement aux principes ci-dessus.

21. L'ICP interne est opérationnelle depuis le début de l'année 2001, après une phase de préparation et de test d'environ une année. Elle est organisée en une autorité de certification racine et quatre autorités filles, dont deux à vocation interne (consacrées respectivement aux personnes et aux équipements informatiques), et deux autres dédiées à la certification d'entités externes<sup>3</sup>. Il faut en outre mentionner une autorité de certification fille supplémentaire, utilisée pour les tests. L'autorité racine est actuellement autocertifiée, mais il est prévu de l'intégrer dans l'ICP interne du MINÉFI dès que les critères et procédures permettant de mener à bien cette opération auront été précisés.

22. La coordination de l'ensemble du système est confiée, par délégation du comité de direction de l'INSEE, au responsable de la sécurité des systèmes d'information. La responsabilité sur les différentes

---

<sup>3</sup> Ces deux autorités « externes », dont l'existence contredit les principes mentionnés plus haut, fournissent deux exemples d'adaptation à des cas concrets des grandes orientations générales ; ces exemples seront détaillés ci-dessous.

autorités de certification a de même été déléguée aux autorités compétentes au sein de l'institut (par exemple au responsable des ressources humaines pour ce qui est de l'autorité de certification des personnes).

#### **IV. CERTIFICATION DES ENTITÉS INTERNES**

##### **A. Équipements informatiques**

23. On l'a vu, l'ICP de l'INSEE permet de fournir des certificats aux personnels et aux ressources informatiques, par le biais de deux autorités de certifications spécialisées. Parmi celles-ci l'autorité « informatique » est celle dont le développement est le plus avancé ; sa fonction principale est de distribuer aux serveurs web internes des certificats leur permettant d'engager avec leurs clients des sessions sécurisées via le protocole HTTPS. Elle pourrait également, quoique ce ne soit pas prévu à court terme, certifier d'autres types de matériels (équipements de réseau, par exemple).

24. C'est également l'autorité informatique qui certifie quelques personnes particulières, qui sont d'ailleurs plutôt des rôles organisationnels : d'une part les administrateurs de l'ICP elle-même, d'autre part un signataire de code logiciel. Ce dernier est chargé, en fonction d'une politique définie (qui inclut notamment des procédures de vérification de qualité par des experts désignés), d'apposer la signature de l'INSEE sur des programmes ou éléments logiciels (contrôles ActiveX, appliquestes Java, etc.) développés en interne. Ceci permet par exemple d'utiliser en Intranet des éléments actifs qui, faute de signature, déclencheraient des alertes de sécurité compte tenu du paramétrage de nos navigateurs. Ce service peut également permettre de garantir des programmes que l'INSEE fournit à des utilisateurs ou des clients externes (installateurs de cédérom, par exemple).

25. Il est à noter toutefois que les serveurs web de l'INSEE délivrant des services destinés au grand public sont actuellement sécurisés par des certificats fournis par une autorité de certification commerciale. Ceci vise à éviter les inconvénients liés à l'absence de reconnaissance en standard par les navigateurs courants des certificats émis par l'INSEE<sup>4</sup>. On peut citer l'exemple du serveur de diffusion commerciale de l'INSEE (« web commerce »), qui permet, via des transactions sécurisées, l'achat en ligne et le paiement par portefeuille électronique ou carte bancaire de produits (livres, cédéroms) ou de données (fichiers, publications électroniques, etc.).

##### **B. Personnes**

26. Les développements de la seconde autorité interne, celle qui est dédiée aux personnes, sont beaucoup moins avancés. À dire vrai, la définition de la stratégie générale en matière de fourniture de certificats aux personnels de l'INSEE vient seulement d'être engagée. Les principes qui ont été retenus sont de distinguer les certificats de signature (permettant de s'authentifier) et les certificats de confidentialité (permettant de chiffrer des données), de déployer prioritairement les certificats de signature sur des supports matériels de type carte à puce, et globalement de procéder par étapes, en s'appuyant sur les évolutions générales en cours en matière de sécurité des systèmes d'information.

27. L'INSEE a récemment amélioré la formalisation de sa politique de classification des données ; on distingue désormais trois niveaux de sensibilité pour les données internes (accès libre, accès restreint, haute protection). À chaque niveau doivent être associées des modalités particulières de contrôle d'accès. En particulier, seules les personnes fortement authentifiées (par certificat) pourront accéder aux données sous haute protection. Le travail de classement effectif par les directions opérationnelles de chacune des

---

<sup>4</sup> Lorsqu'il reçoit un certificat émis par une autorité qu'il ne connaît pas, le navigateur en avertit son utilisateur. L'ajout d'une autorité de confiance aux (trop) nombreuses autorités installées par défaut dans les navigateurs peut être réalisé par l'internaute, et on peut d'ailleurs considérer que c'est le responsabiliser que de lui demander d'effectuer explicitement cette procédure. Toutefois, l'état de maturité des produits et du grand public a conduit pour l'instant à adopter la certification par une autorité « préinstallée ».

nombreuses sources de données de l'INSEE dans l'un des trois niveaux de sensibilité est en voie d'achèvement. Sur la base de ce travail, l'une des sources sera prochainement sélectionnée afin d'engager une expérience d'intégration d'une authentification par carte à puce des utilisateurs des applications permettant d'accéder à cette source.

28. D'un point de vue technique, l'intégration de l'authentification forte ne pose pas de difficulté, à partir du moment où l'application fait usage de technologies suffisamment récentes. En revanche, c'est l'organisation en matière d'autorisations d'accès qu'il convient d'expérimenter sérieusement. Il est inutile, voire trompeur, de s'appuyer sur des authentifications par certificats si, par exemple, les droits d'accès attribués à des utilisateurs ne sont pas supprimés dans des délais acceptables lorsque ces utilisateurs changent de fonction. Pour concrétiser ce préalable indispensable, l'INSEE a mis en place une organisation de gestion des droits applicatifs basée sur l'utilisation d'un annuaire LDAP centralisé ; cet annuaire fait d'ailleurs également fonction de service de publication pour l'infrastructure de clés publiques.

29. L'autorité de certification des personnes peut distribuer des certificats de signature ou des certificats de confidentialité (principe de séparation des clés). Toutefois, les services de chiffrement soulèvent des questions souvent plus complexes que les services d'authentification. Une de ces questions est celle de la gestion des clés privées, qui se pose en des termes tout à fait différents pour les clés de chiffrement et pour les clés de signature : que faire lorsqu'un individu perd sa clé de chiffrement, et ne peut de ce fait plus accéder à ses propres fichiers ou à ses messages ? ou s'il quitte l'institution sans rendre sa clé, empêchant ainsi la récupération de données qui peuvent être importantes ?

30. Des services dits de recouvrement de clés ont été définis pour éviter ce type de situation, mais leur mise en œuvre est extrêmement délicate, d'un point de vue technique aussi bien qu'organisationnel. L'opportunité de la mise en place de ce type de services fait partie des thèmes qui feront l'objet prochainement de discussions stratégiques au niveau ministériel. En attendant, l'ouverture aux utilisateurs internes de l'INSEE de fonctions de chiffrement articulées avec l'infrastructure de clés publiques restera limitée, et se fera essentiellement dans le cadre de la messagerie.

31. Il est parfois difficile d'éviter que des entités internes soient certifiées par des autorités externes, on l'a vu plus haut dans le cas des serveurs web publics. Pour ce qui est des personnes, on peut citer l'exemple d'un important projet interministériel destiné à la gestion de la dépense publique, qui est en cours de déploiement dans toute l'administration française (plusieurs dizaines d'utilisateurs sont concernés à l'INSEE). Ce projet utilise une infrastructure de clés publiques qui lui est propre, et donc des profils de certificats et des méthodes d'enregistrement particuliers. Les certificats que fournira cette ICP seront enregistrés sur une carte à puce dédiée, et il n'est pas tout à fait assuré à l'heure actuelle qu'il ne faudra pas équiper tous les utilisateurs concernés de lecteurs de cartes dédiés.

32. Il est clair que ce type d'approche fermé et propriétaire n'est pas globalement optimal, et ne saurait éventuellement se justifier que dans la situation transitoire où l'état de développement des services de certification au sein des différents ministères est très variable. Avec de telles démarches, les utilisateurs se retrouveront demain dotés d'un certificat par application, tout comme actuellement ils ont souvent un mot de passe par application. Il est bien préférable, même si cela peut être plus difficile, de s'appuyer sur des systèmes de certification existants ou à développer dans les services, au plus près des utilisateurs. Cela nécessite d'établir un cahier des charges spécifiant les exigences de l'application en termes de profils de certificats ou de qualité des procédures, puis de laisser chaque service attribuer lui-même des certificats respectant les contraintes ainsi fixées. C'est ce type de démarche que l'INSEE favorise pour ses contacts avec des partenaires extérieurs.

## V. CERTIFICATION DES ENTITÉS EXTERNES

### A. Reconnaissance de certificats externes

33. Pour les besoins d'échanges sécurisés avec des partenaires identifiés, notamment fournisseurs d'information, l'INSEE privilégie des solutions d'accréditation de systèmes de certification externes. On peut citer l'exemple d'un projet en cours de développement pour attribuer en temps réel aux entreprises qui se créent leur numéro d'identification (numéro SIREN). Ceci nécessite la mise en place de liens sûrs avec les CFE, centres de formalités des entreprises, où ces dernières viennent effectuer leurs démarches administratives (ces CFE sont situés par exemple dans les chambres de commerce et d'industrie ou les chambres de métiers). Pour cela, l'INSEE préfère accompagner la mise en place de systèmes de certification des CFE par leurs organismes de tutelle que de leur attribuer lui-même des certificats.

34. La reconnaissance de certificats externes pour les besoins de sécurisation d'une application est une démarche nécessaire (chaque application, on l'a vu, ne doit pas être déployée avec son propre système de certification), mais également assez complexe. Des méthodologies d'accord entre une application et une ICP externe sont d'ailleurs en train d'apparaître, à côté des méthodologies plus « classiques » d'accord entre ICP. Le niveau de contrainte demandé par l'application quant aux caractéristiques des certificats reflète un positionnement sur une échelle de compromis entre généralité des certificats et nécessité de procédures supplémentaires d'inscription :

- Si le certificat identifie très exactement un type d'entité donné, par exemple par une caractéristique particulière du certificat (présence d'un identifiant spécial, autorité de certification dédiée, etc.), l'accès à l'application peut parfois être donné au seul vu du certificat. Éventuellement, l'application peut récupérer certaines informations du certificat pour personnaliser son comportement.
- Inversement, si les certificats des clients sont peu contraints, il est le plus souvent nécessaire de gérer une procédure spécifique d'inscription à l'application, qui permet de lier dans un annuaire local l'identité d'un utilisateur à un certificat donné (repéré par son empreinte, son numéro de série, etc.).

35. Il n'est pas prévu pour le moment d'utiliser une authentification par certificat pour les personnes physiques ou les entreprises directement clientes des systèmes d'information de l'INSEE. On peut citer à titre d'illustration les projets d'enquêtes par Internet auprès des entreprises, actuellement en cours de développement : il s'agit dans un premier temps des enquêtes de conjoncture, puis des enquêtes sur les prix de vente industriels (qui font intervenir des informations plus sensibles). Dans l'état actuel des réflexions, une authentification par mot de passe paraît suffisante : seul le serveur de l'INSEE sera certifié (les échanges seront naturellement chiffrés).

36. Néanmoins, il est clair qu'il faudra rapidement être en mesure d'accepter les demandes de clients ou de répondants qui souhaiteraient élever le niveau de sécurité et s'authentifier par certificat. En particulier, les entreprises qui se sont équipées d'un certificat reconnu par le MINÉFI pour s'acquitter en ligne de leur TVA peuvent légitimement prétendre à utiliser ce même certificat pour répondre à un questionnaire électronique de l'INSEE. Pour se préparer à satisfaire cette demande, l'INSEE participe à la réflexion du MINÉFI sur la mise en œuvre au sein du ministère de services mutualisés de validation de certificats : il est en effet indispensable que la politique d'accréditation du MINÉFI se traduise par des pratiques uniformes d'acceptation ou de refus des certificats dans l'ensemble de ses services.

37. Un problème de reconnaissance de certificats externes se posera également lorsque l'INSEE souhaitera banaliser les possibilités d'accès à son système d'information par des partenaires privilégiés<sup>5</sup>, notamment les services statistiques des ministères. Actuellement, ces accès se font par réseaux dédiés ou sécurisés, et la tendance est d'abandonner les modes de connexion dédiés en faveur de l'utilisation de l'Internet. Il est toutefois clair qu'un dispositif d'authentification à base de certificats devra accompagner cette ouverture, et qu'il n'est pas souhaitable là non plus d'imposer un système de certification géré par l'INSEE. On n'en est sur cette question aussi qu'aux réflexions préliminaires.

## **B. Attribution de certificats à des entités externes**

38. Dans certains cas, l'INSEE peut être amené à certifier lui-même des entités externes. Cela peut être dû à des conditions particulières d'utilisation des certificats, ou à des situations transitoires, avec des partenaires dont les schémas de certification sont insuffisamment développés. On fournit dans ce paragraphe deux exemples de ce type de situations.

39. Dans le cadre d'un projet pilote de transmission en ligne de données d'état civil, l'Institut prévoit d'attribuer des certificats permettant d'authentifier les mairies qui participent à l'expérience : une autorité de certification dédiée à cette fonction a été créée au sein de l'ICP privée : c'est l'une des deux autorités « externes » citées plus haut. Cependant, l'INSEE n'a pas vocation à être organisme de certification des mairies, et des dispositifs de certification pilotés par le ministère de l'intérieur sont par ailleurs en cours de construction : lorsque le projet arrivera en phase de déploiement effectif, ce sont ces dispositifs qui seront utilisés.

40. L'autre cas d'autorité de certification à vocation externe est lié à l'ouverture prochaine d'un service payant de consultation du répertoire SIRENE<sup>6</sup> par échange sécurisé de requêtes XML via l'Internet. Dans le cadre de l'abonnement à ce service, l'INSEE fournit un logiciel permettant de regrouper les requêtes de divers formats provenant du système d'information du client, d'établir les liaisons sécurisées avec le serveur de l'INSEE, de mettre en forme les demandes XML et d'interpréter les réponses. Ce service est destiné à de gros clients (banques, grandes compagnies, etc.), et un contrat individuel est signé avec chacun d'eux. Dans ce cas précis, l'authentification du client se fait par un certificat fourni par l'INSEE, et ce pour plusieurs raisons : l'enregistrement pour l'attribution du certificat a été entièrement intégré dans le déroulement du contact commercial avec le client (et tout particulièrement dans les procédures de signature du contrat) ; par ailleurs le certificat est complètement caché dans le logiciel client livré ; enfin, cette solution permet un contrôle du profil du certificat (durée de vie et modalités de renouvellement alignées sur celles du contrat, numéro de contrat inclus dans le certificat, etc.) qui n'aurait pas pu être réalisé autrement.

## **VI. CONCLUSION**

41. Comme l'illustrent les paragraphes précédents pour ce qui est du cas français (mais le constat est probablement valable dans de nombreux autres pays), le domaine de la certification électronique est encore en pleine mutation : les premières expériences réelles de terrain commencent tout juste à apporter leurs enseignements, les stratégies politiques et commerciales se dessinent, les initiatives se multiplient, pas toujours dans la cohérence la plus complète.

42. Ce contexte bouillonnant peut inciter à la prudence, voire à la réserve. Toutefois, la conviction d'une généralisation prochaine de ces technologies a maintenant débordé le cercle des techniciens de la sécurité pour atteindre les principaux acteurs politiques et économiques. Il est donc important de s'y préparer, en développant à la fois une stratégie générale pour canaliser le foisonnement des demandes, mais en même

---

<sup>5</sup> Le système statistique public français est décentralisé : y participent de nombreux organismes présents dans les différents ministères ; l'INSEE en assure la coordination, et entretient par ailleurs des liens privilégiés avec des organismes divers publics ou non (Banque de France, instituts et centres de recherche, etc.).

<sup>6</sup> Répertoire français des entreprises et des établissements.

temps une démarche volontariste : il ne s'agit pas d'attendre indéfiniment pour se lancer que les évolutions en cours se stabilisent, que les normes et protocoles s'affinent ou que les outils mûrissent.

43. Un point crucial à noter est que les projets utilisant la certification sont à la fois techniques et organisationnels, voire politiques : les questions d'identification font généralement intervenir des enjeux de pouvoir. Il est donc essentiel que les projets soient portés au bon niveau de décision au sein de l'organisation, et la pédagogie envers les décideurs interne est souvent un des facteurs clés à développer.

44. On peut également souligner la position particulière qui est celle d'un institut de statistique vis-à-vis de ces problématiques, notamment, comme c'est le cas à l'INSEE, quand cet institut est également chargé de la gestion des grands répertoires nationaux. D'une part, on l'a vu en introduction, la sécurité et la dématérialisation des échanges représentent des enjeux importants pour des organismes dont la matière première, l'information, est déjà immatérielle. D'autre part, les instituts statistiques peuvent souvent contribuer utilement aux réflexions relatives à l'organisation des services de certification, en faisant valoir leur expérience théorique et pratique en matière de définition de concepts, d'identification, de nommage et d'autres services indispensables à l'essor de ces systèmes.