Distr.
GÉNÉRALE

CSE/AC.71/2004/3
16 mars 2004

FRANCAIS
ANGLAIS et FRANÇAIS seulement

**COMMISSION DE STATISTIQUE DES NATIONS UNIES et COMMISSION ÉCONOMIQUE POUR L'EUROPE (CEE) CONFÉRENCE DES STATISTICIENS EUROPÉENS**

**COMMISSION EUROPÉENNE OFFICE STATISTIQUE DES COMMUNAUTÉS EUROPÉENNES (EUROSTAT)**

**ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE) DIRECTION DES STATISTIQUES**

**Réunion conjointe CEE / EUROSTAT / OCDE sur la gestion des systèmes d'information statistique (GSIS)**
(Genève, 17 au 19 mai 2004)

Sujet (i) : La technologie Web et les systèmes d'information statistique

# UTILISATION DE L'ICP POUR LE RECENSEMENT

**Communication sollicitée**

Présentée par Statistique Canada[1]

## I. INTRODUCTION

### A. Infrastructure commune du gouvernement du Canada

1. Le gouvernement du Canada, dans le cadre de son projet *Gouvernement en direct (GED)* lancé en 2000, a mis en place une infrastructure commune appelée *Voie de communication protégée* qui est utilisée par près de 200 ministères et organismes. Cette infrastructure offre un réseau de base sûr pour l'offre de services électroniques aux citoyens et aux entreprises sur Internet.

2. Outre les services réseau fiables et de grande capacité, la Voie de communication protégée offre des services de sécurité dont l'Infrastructure à clés publiques (ICP) et une autorité de certification (AC) commune. Les différents ministères doivent se servir de cette infrastructure pour développer et exploiter des services publics.

3. Statistique Canada a collaboré étroitement avec les organismes centraux du Canada et le consortium (qui avait à sa tête les Entreprises Bell Canada (BCE)) qui a construit l'infrastructure commune, en vue de la mise sur pied d'un service ICP spécial convenant aux exigences particulières du recensement. Ces exigences, ainsi que le nouveau service qui a été conçu, sont décrits dans le présent document.

[1] Préparé par Mel Turner et Lise Duquet de Statistique Canada.

### B. Recensement de la population et Recensement de l'agriculture

4. À titre de bureau national de la statistique du Canada, Statistique Canada a la responsabilité d'effectuer aux cinq ans un Recensement de la population et un Recensement de l'agriculture. Pour le prochain recensement, en 2006, nous souhaitons offrir à tous les citoyens la possibilité d'entrer leurs réponses en direct, sur Internet, et garantir à ceux-ci que leur confidentialité sera entièrement assurée. En ce qui concerne Internet, la confidentialité comprend la protection des données des réponses contre toute indiscrétion et altération durant les communications avec Statistique Canada. Le présent document explique les exigences du recensement ainsi que les raisons qui ont motivé le choix de la technologie ICP pour le système.

5. En mai 2004, Statistique Canada effectuera une répétition générale en vue du Recensement de 2006, notamment en ce qui concerne l'utilisation d'Internet pour l'envoi des réponses. Le gouvernement du Canada a amélioré son infrastructure commune afin d'offrir un service ICP anonyme qui aidera à respecter les exigences du recensement. Par ailleurs, la répétition générale du recensement permettra de démontrer de quelle façon cette méthode peut être utilisée dans d'autres situations.

6. Il s'agira de l'une des premières utilisations au monde de l'ICP pour un recensement, car on estime que les processus habituels d'inscription en vue de l'obtention d'un certificat d'ICP sont trop coûteux pour une seule utilisation. En ayant recours à une technique unique permettant la réutilisation des certificats, Statistique Canada croit qu'elle a trouvé une méthode pratique.

7. Pour le Recensement de 2001, Statistique Canada a offert un service expérimental en direct : le répondant devait alors télécharger et configurer un logiciel spécial de saisie et d'envoi des réponses. On devait se servir de ce logiciel pour assurer le degré de sécurité (par un chiffrement) jugé nécessaire pour la collecte des données du recensement. On a estimé que cette méthode n'est pas pratique sur une grande échelle, en raison de la taille du logiciel à télécharger et du nombre de demandes de renseignements de la part des répondants. Toutefois, cette expérience a été déterminante : elle a en effet contribué à définir les exigences à cet égard pour le Recensement de 2006

## II. OBJECTIFS ET EXIGENCES

### A. Objectifs du recensement

8. Le gouvernement du Canada réalise une initiative de taille visant à offrir en direct tous les services fréquemment utilisés d'ici 2005. Appelé *Gouvernement en direct (GED)*, ce projet a pour but de rehausser la satisfaction du public en rendant les services plus faciles d'accès et plus conviviaux.

9. Nous souhaitons offrir à tous les Canadiens et les Canadiennes la possibilité d'entrer en direct les réponses du Recensement de 2006, en partie pour respecter l'objectif de GED mais également parce que nous croyons qu'une part importante du public exigera ce service. Ainsi, ce projet n'était pas motivé au départ par des raisons d'économie de coûts mais plutôt par la demande du public (ou la demande perçue). Nos sondages sur la pénétration d'Internet ont révélé que la plupart des Canadiens et Canadiennes ont accès à Internet à la maison, au travail ou encore par le recours à des points d'accès publics (bibliothèques, écoles, etc.) et qu'ils optent pour des services en direct pour l'entrée des réponses si ces méthodes permettent de gagner du temps ou si elles sont plus pratiques que la méthode traditionnelle.

10. Le Recensement de la population porte sur environ 13,5 millions de ménages, tandis que le Recensement de l'agriculture vise plus de 300 000 exploitations agricoles. Ces recensements doivent être réalisés simultanément en mai 2006. Ils comprendront un certain nombre de changements quant à la méthode, par rapport aux recensements précédents : en effet, en plus d'offrir un service en direct, il s'agira de la première fois que nous utilisons au Canada une méthode d'envoi et retour par la poste (auparavant, les questionnaires du recensement étaient distribués puis renvoyés par la poste) pour les régions urbaines. En outre, nous mettons en

place une nouvelle technologie de numérisation (balayage) et de reconnaissance pour la saisie des données. En raison de tous ces changements, nous allons effectuer une répétition générale complète des processus de collecte en mai 2004. Cette répétition portera sur environ 300 000 ménages et 20 000 exploitations agricoles de trois régions géographiques représentatives du pays.

11. La prévision du degré d'acceptation du service en direct pour une enquête unique comme le recensement est très difficile, étant donné la nature du processus et les préférences des citoyens qui changent sans cesse quant à l'utilisation d'Internet. Nous croyons que grâce à des stratégies efficaces de communication au public et de conception d'interface environ 20 à 25 % des ménages vont opter pour le service en direct. Toutefois, pour atteindre cet objectif, il sera crucial d'offrir un service pratique et convivial. Pour la répétition générale nous n'aurons pas recours à la même campagne média que pour le recensement véritable. Ainsi, les documents d'information qui vont accompagner le questionnaire constitueront le seul moyen employé pour faire connaître l'existence du service en direct.

12. Le fait de garantir la confidentialité et la sécurité des réponses est un objectif primordial de toutes nos enquêtes. En raison de l'envergure et de l'ampleur des recensements, ceux-ci suscitent un examen minutieux de la part du public. En fait, certains avancent que bien des citoyens choisiront sans doute le service en direct car ils estiment que cette méthode est plus *confidentielle* que le formulaire papier qui est manipulé par plusieurs personnes dans le cadre du processus de collecte. Toutefois, nous devons également composer avec la perception du public au sujet de la vulnérabilité d'Internet quant aux accès non autorisés et le fait que le recensement constitue certes une cible de choix pour les pirates de l'électronique. Dans ce contexte, nous souhaitons utiliser des méthodes de chiffrement sans égal pour assurer la confidentialité des réponses au recensement. Ainsi, nous visons à offrir des caractéristiques supérieures à celles généralement proposées pour le commerce électronique et susciter une confiance élevée de la part du public canadien.

## B. Exigences du recensement

13. La transposition des objectifs administratifs cités plus haut, en tenant compte de l'expérience de 2001, afin de déterminer les besoins techniques et en matière d'application pouvant être comblés, a consisté en un processus exécuté à plusieurs reprises. Il a fallu collaborer étroitement avec des fournisseurs de logiciels commerciaux, des organismes centraux responsables de l'infrastructure commune, des fournisseurs de services d'infrastructure et des entrepreneurs participant aux travaux sur le logiciel du recensement. Ces interactions ont été complexes, mais les exigences fondamentales se sont avérées étonnamment simples. Notre réussite jusqu'à maintenant a été possible car nous avons fait en sorte que ces besoins soient directs et compris de tous les intervenants.

### i. Accès simple et unique

14. Même si les exigences sur le plan de la confidentialité indiquaient dès le début d'avoir recours à l'ICP, le processus d'inscription commun imposé alors pour l'obtention d'un certificat d'ICP était jugé trop coûteux pour une initiative unique comme le recensement. Nous avions besoin d'une méthode d'accès simple afin que le processus d'identification ne cause pas d'inconvénients aux répondants et ne les dissuade pas d'utiliser le service en direct. Le point important à cet égard a trait au fait qu'on s'est aperçu que ce processus n'effectuait *pas* l'authentification de la personne (caractéristique normale pour l'ICP) mais que dans le cadre d'un événement unique, il l'associait à un formulaire particulier (le questionnaire du recensement). Aucune inscription préalable n'était exigée : un code d'accès unique imprimé sur chaque formulaire permettait d'exécuter un processus d'identification en une étape.

### ii. Pratique et convivial

15. La nécessité d'une méthode pratique pour les répondants a été établie principalement suite à l'expérience de 2001. Par exemple, le répondant ne doit pas avoir à télécharger (ou acheter) un logiciel en plus des navigateurs Web courants. Ainsi, on pourrait utiliser des points d'accès à Internet communs, comme des bibliothèques et des kiosques, en plus de se conformer à la façon dont l'ordinateur de la plupart des utilisateurs d'information est configuré.

16. Nous souhaitions de plus éviter de modifier la configuration de l'ordinateur de l'utilisateur (en ne laissant aucune trace). Par conséquent, aucun élément (donnée du recensement ou logiciel) ne peut demeurer dans le poste de travail une fois que la session est terminée.

17. En raison de cet aspect, en plus de l'obligation de permettre aux utilisateurs de reprendre une session interrompue sur un ordinateur *différent* de l'ordinateur initial (ce qu'on appelle l'*itinérance*), les questionnaires partiellement remplis doivent être enregistrés dans le serveur d'applications et non dans le poste de travail.

18. La possibilité d'interrompre et de reprendre une session était particulièrement importante pour le long formulaire du recensement, car dans ce cas un ménage comportant plusieurs personnes peut prendre un certain temps à remplir ce formulaire. Nous avons estimé la durée de la session à 25 à 30 minutes pour un ménage d'une taille moyenne qui remplit le formulaire du recensement de la population (formulaire 2B) et de 40 à 60 minutes pour le Recensement de l'agriculture.

#### iii. Capacité de manipuler des volumes importants

19. Les habitudes quant aux réponses en direct pour un recensement de la population ne sont pas connues pour le moment, mais nous prévoyons qu'ils seront semblables à celles prévalant pour les formulaires papier. Autrement dit, les réponses vont être envoyées à l'approche du jour du recensement ou le jour même du recensement : ainsi, une capacité de traitement importante sera nécessaire en vue du traitement des données transmises pendant la période de pointe. Nous modifierons peut-être nos estimations suite à la répétition générale de mai 2004, mais pour le Recensement de 2006 nous prévoyons, en période de pointe, devoir prendre en charge 50 000 sessions simultanées. Il s'agit d'un facteur qui influe grandement sur les coûts de la capacité d'infrastructure requise. En ayant recours à une installation commune du gouvernement, plutôt que d'accroître notre propre capacité utilisée pour les enquêtes périodiques, nous espérons éviter les goulots d'étranglement.

20. L'infrastructure commune, qui a été réalisée pour le gouvernement du Canada par un consortium ayant à sa tête les Entreprises Bell Canada (BCE), est appelée la *Voie de communication protégée*. Cette voie offre des services réseau de grande capacité et à grande disponibilité, y compris des services ICP. De plus, les exploitants de la Voie de communication protégée[2] étaient disposés à établir un partenariat avec Statistique Canada en vue de la mise en place d'un service ICP spécial pour le logiciel du recensement.

### C. Exigences en matière de sécurité et de confidentialité

21. L'exigence concernant la confidentialité des données du recensement est primordiale et Statistique Canada a pour politique de protéger par un chiffrement les données confidentielles transmises. Le logiciel du recensement, conformément à ce qui a été expliqué plus haut, doit permettre d'interrompre et de reprendre une session : ainsi, les premières réponses doivent être retransmises au répondant afin qu'il puisse les consulter ou encore les modifier. De plus, nous souhaitions offrir aux répondants des commentaires ou des instructions en temps réel, qui peuvent comprendre des renseignements délicats. Il fallait donc assurer à tout prix un chiffrement de bout en bout et bidirectionnel.

22. Certes, en raison de la nécessité d'effectuer un chiffrement, l'ICP semblait le choix idéal, mais les services existants comportaient une caractéristique importante en matière d'authentification, qui exigeait l'inscription préalable des participants. Nous souhaitions éviter le recours à un processus d'inscription pour plus de commodité pour les répondants et pour des raisons de confidentialité. Le Canada ne dispose pas d'un *registre de la population* et le fait d'exiger un processus de la sorte pourrait être controversé sur le plan politique.

23. Les systèmes de chiffrement à clés publiques offrent deux fonctions distinctes : la protection de la confidentialité et des signatures numériques en vue de l'authentification. Normalement, des paires de clés distinctes sont produites pour chacune de ces fonctions. Le logiciel du recensement n'exigeait que la protection

[2] Travaux publics et Services gouvernementaux Canada (TPSGC), qui a passé un contrat avec le consortium *Équipe BCE*.

de la confidentialité; ainsi, Statistique Canada a suggéré la création d'un nouveau service de production de certificats d'ICP *anonymes* (et par conséquent de clés de signature).

24. Une dernière exigence prévalait, soit l'« invisibilité » de l'interface de sécurité pour l'utilisateur. Nous souhaitions que le dialogue de l'utilisateur soit entièrement régi par le logiciel du recensement, sans interpellation de la part des services de sécurité communs. Statistique Canada estime qu'il est important, pour susciter la confiance du public envers l'indépendance statistique, que son identité soit distincte de l'identité générale du gouvernement lorsqu'il s'agit d'un dialogue en direct. Pour souligner la distinction entre la collecte de données statistiques et les opérations administratives, Statistique Canada est autorisée, en vertu de la politique du gouvernement, à émettre des certificats d'ICP qui ne font pas l'objet d'une intercertification avec d'autres organismes.

## III. LA SOLUTION

### A. SCEAU – Service ICP anonyme

25. Le nouveau service est appelé *SCEAU* (*Session avec Chiffrement et Enregistrement AUtomatique*). En raison du volet *automatisé d'ouverture de session* de ce service, le logiciel du recensement peut demander l'utilisation de la Voie de communication protégée afin d'établir une session sûre sans qu'il y ait de dialogue d'ouverture de session avec l'utilisateur. Cette méthode concorde avec notre volonté de disposer d'un processus d'identification en une étape et d'une interface invisible. De plus, il n'était plus nécessaire de disposer d'un répertoire supplémentaire, qui aurait été nécessaire dans le cas d'un très grand nombre d'utilisateurs uniques.

26. On assure l'anonymat en prévoyant un ensemble prédéfini d'identificateurs d'utilisateur, de mots de passe et de noms distinctifs en ce qui concerne l'ICP. Toutefois, ces éléments ne sont jamais vus par l'utilisateur : ils sont utilisés en coulisse et ils servent à définir la session et à établir les mécanismes de sécurité. Cette séquence est appelée *ouverture de session automatique*.

27. Puisque les certificats ICP sont anonymes, le service SCEAU conserve une base de données des certificats générée à l'avance. Ces certificats peuvent être associés dynamiquement à une session d'utilisateur, puis être recyclés et réutilisés une fois que la session est terminée. Autrement dit, le certificat n'est utilisé que pour un moment, soit pour la transmission. Une fois que les données ont été reçues et que la session est terminée, il est impossible de retracer le certificat qui a été utilisé.

28. Il n'y a aucune association à long terme entre un répondant et un certificat d'ICP particulier. L'utilisateur n'est sans doute pas au courant qu'un certificat a été produit, car celui-ci est provisoire et, par conséquent, l'utilisateur ne doit pas le conserver. Cette méthode diffère des expériences habituelles que les utilisateurs ont avec l'ICP, car dans ces cas ils doivent composer avec un processus d'inscription (exigeant souvent une authentification indépendante de l'identité) ainsi qu'avec des services de définition et de récupération de mot de passe.

29. Étant donné que l'utilisateur de la session est anonyme, le service SCEAU dispose d'une autorité de certification (AC) réservée qui ne fait pas l'objet d'une intercertification avec une autre AC. Ainsi, le service SCEAU est entièrement indépendant des autres services communs offerts par le gouvernement du Canada et il renforce la perception que la collecte de données statistiques est distincte des opérations et des services administratifs.

30. Le service SCEAU fait appel à une technologie d'Entrust, Inc., une société canadienne qui est l'un des chefs de file mondiaux des logiciels de sécurité. Plus particulièrement, on s'est servi du logiciel Entrust TruePass$^{MC}$ car celui-ci n'a pas à être installé dans l'ordinateur de l'utilisateur et, de plus, toutes les caractéristiques de sécurité et les mises à jour sont gérées en un point central (site Web). Le logiciel Entrust TruePass prend en compte la vulnérabilité des opérations sur le Web en assurant un chiffrement de bout en bout

transparent de l'information transmise sur le Web. Lorsque l'information transite entre le serveur Web et le navigateur Web de l'utilisateur, elle est en fait chiffrée deux fois : une fois par SSL (fonction propre aux navigateurs et utilisée à grande échelle pour le commerce électronique) et une autre fois par le logiciel Entrust TruePass.

31. Le logiciel Entrust TruePass télécharge dynamiquement une mini-application Java et le certificat d'ICP dans un poste de travail, afin de permettre le chiffrement de bout en bout. Une fois que la session est terminée, la mini-application est automatiquement supprimée. Statistique Canada a collaboré directement avec Entrust en 2003 afin de s'assurer que la version 7 du logiciel TruePass, qui offre la fonction de chiffrement bidirectionnel, est prête à temps pour la mise en place du service SCEAU.

32. La logique du service SCEAU est décrite en détail à la prochaine section. Elle concorde à merveille avec les exigences du recensement quant à l'offre d'un chiffrement de bout en bout bidirectionnel tout en demeurant essentiellement invisible pour l'utilisateur. Dans ce cas, pour l'utilisateur, le contact se fait au départ avec le « recensement » et non avec le service SCEAU.

## B. Utilisation du service SCEAU dans la pratique

33. On peut mieux comprendre le service SCEAU en suivant la séquence logique du logiciel du recensement. Nous allons examiner les opérations génériques des séquences « d'ouverture de session » et de « transmission des données » afin de déterminer quels composants prennent part à ces opérations et de quelle façon fonctionne la protection de la confidentialité. Dans les descriptions ci-après, nous nous penchons sur les interactions entre le *navigateur de l'utilisateur*, l'*infrastructure ICP commune* et le *logiciel du recensement*. Ces éléments se trouvent à des endroits différents : le navigateur de l'utilisateur peut être situé n'importe où au Canada, les services d'infrastructure sont offerts depuis Thornhill en Ontario et le logiciel du recensement se trouve dans les locaux de Statistique Canada à Ottawa.

### i. Ouverture de session pour le recensement

34. La séquence débute lorsqu'un utilisateur accède à l'adresse URL du recensement. Cette adresse URL est imprimée sur le formulaire qui est posté au répondant et elle est également présentée sous forme de lien à notre site Web public. Tout accès à cette adresse URL est immédiatement dirigé vers l'infrastructure commune, en vue de l'établissement d'un environnement de sécurité local au sein du navigateur de l'utilisateur, qui est appelé *ensemble de cadres TruePass*. Ce processus est invisible pour l'utilisateur, sauf en ce qui concerne le léger retard et l'affichage d'une icône de cadenas à la partie inférieure de l'écran.

35. L'ensemble de cadres TruePass comprend une applet Java qui offre des services de chiffrement et qui communique avec le navigateur à titre de module externe. Cet ensemble comprend des cadres dissimulés qui renferment temporairement la version chiffrée des éléments affichés à l'écran. Les pages affichées peuvent accéder à ces cadres dissimulés à l'aide du logiciel Javascript intégré aux éléments HTML et du modèle de référence DOM[3]. Ainsi, le certificat qui représente Statistique Canada (et qui contient la clé publique de Statistique Canada) est installé dans le navigateur.

36. En plus de l'établissement de l'ensemble de cadres, la communication est protégée à l'aide du protocole de sécurisation (SSL à 128 bits) et du protocole HTTPS avant la transmission de la commande au logiciel du recensement.

37. Un *code d'accès à Internet (CAI)* unique de 15 chiffres (regroupés en cinq ensembles de trois chiffres) est imprimé sur chaque questionnaire du recensement. Ce CAI est généré aléatoirement et il est associé à un identificateur géographique qui est relié à notre registre des adresses. Il contient de plus des chiffres de contrôle qui servent à repérer les erreurs de saisie. Le CAI est conçu de façon à ce qu'il soit difficile de le deviner ou d'effectuer un accès en choisissant des chiffres au hasard. Le premier écran affiché à l'intention de l'utilisateur

[3] DOM = modèle objet de document défini par le W3C.

exécute un contrôle du navigateur qui sert à s'assurer que les caractéristiques requises sont supportées activées. Une fois que le navigateur est correctement configuré, le logiciel demande à l'utilisateur d'entrer le CAI qui figure sur le questionnaire.

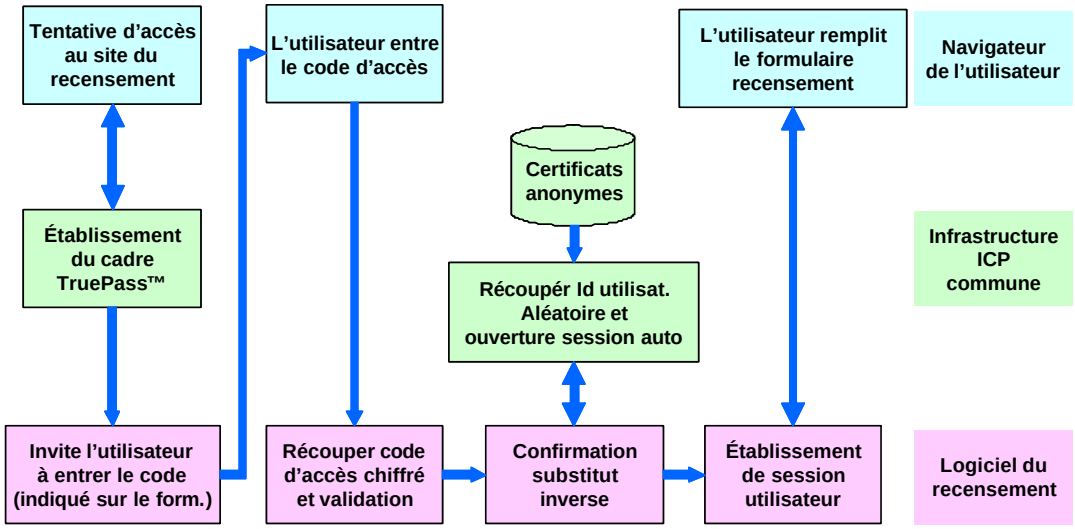


*Figure 1 – Séquence d'ouverture de session*

38. Le code d'accès chiffré est transmis directement au logiciel du recensement en vue d'une vérification. Le logiciel peut déterminer si le code a été entré correctement et, en consultant une base de données, il établit l'état actuel de cet identificateur. Par exemple, il peut s'agir d'une session interrompue qui est reprise ou encore des données peuvent avoir déjà été entrées, ou encore la collecte de données en direct pour ce ménage peut être déjà terminée.

39. Si l'identificateur est valide, le logiciel peut demander à l'infrastructure qu'elle effectue l'ouverture de session automatique. Cette opération est invisible pour l'utilisateur, grâce à un mécanisme appelé *substitution inverse*. Essentiellement, il s'agit d'un service d'arrière-plan qui permet au logiciel de faire appel à des services privés au sein de l'infrastructure de manière sûre.

40. La demande d'ouverture de session autorise l'infrastructure à sélectionner aléatoirement un ensemble de justificatifs d'identité de pseudo-utilisateur et d'exécuter l'ouverture de session automatique. Ainsi, un certificat anonyme est sélectionné parmi un grand nombre de certificats qui ont été produits préalablement, puis la clé publique de l'utilisateur est envoyée au logiciel du recensement. Avec ces justificatifs d'identité, la session de l'utilisateur est complètement établie et le navigateur peut interagir avec le logiciel de manière entièrement sûre. Le chiffrement ICP se sert de clés uniques de 1 024 bits, des clés distinctes étant prévues pour l'envoi et la réception des données.

41. Précisons que pour l'utilisateur, il s'agit d'un processus très léger et transparent. Si aucun problème de compatibilité ou de configuration de navigateur ne prévaut, il suffit d'entrer le numéro d'identification fourni pour débuter la session.

### ii. Envoi des données des réponses

42. Une fois qu'une session SCEAU a été établie, l'infrastructure ne participe plus de façon importante aux interactions. Toutefois, en raison des volumes prévus pour le recensement, nous avons tiré avantage de la capacité de l'infrastructure commune (serveurs et largeur de bande) afin d'adjoindre certaines pages Web non confidentielles à cet endroit. Par exemple, les pages qui renferment des instructions communes (pages d'aide) sur la façon de remplir les questionnaires du recensement ou encore les instructions affichées en réponse à des

erreurs peuvent être présentées directement plutôt que par un recours au logiciel. De cette façon, on améliore en général les performances en réduisant le délai d'exécution entre l'infrastructure et le logiciel du recensement.

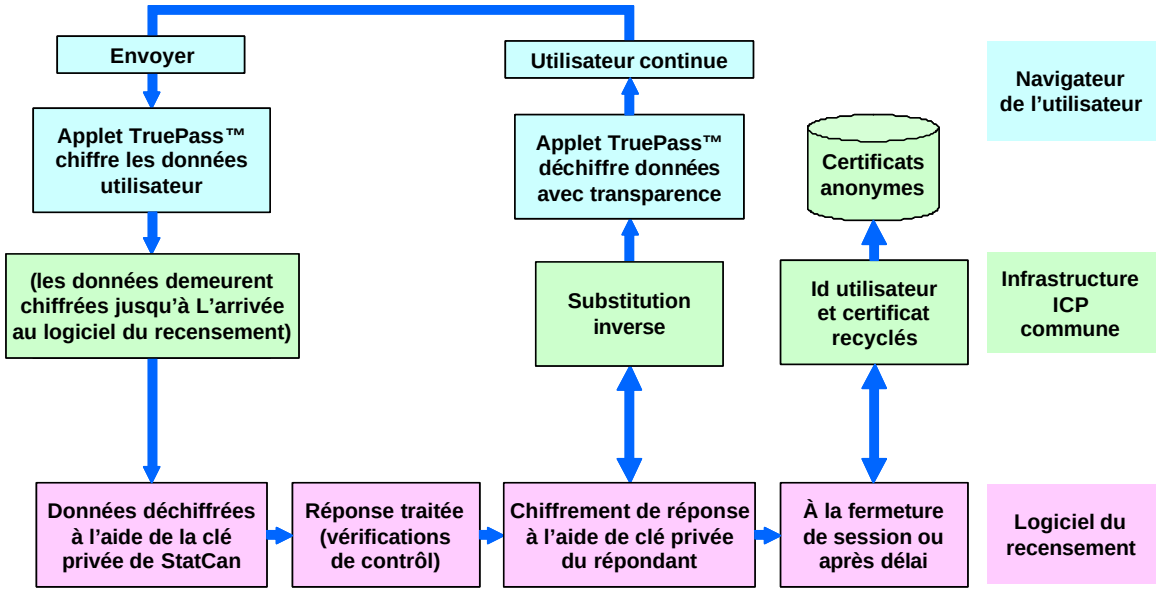


*Figure 2– Séquence d'échange de données*

43. Les dialogues de réponse du recensement sont répartis en pages, chacune de celles-ci contenant un petit nombre de questions (en général deux ou trois). À la fin de chaque page, l'utilisateur a la possibilité de *continuer* ou d'*interrompre* la session (dans le cas du long formulaire) : dans les deux cas, les données figurant à la page sont transmises. La séquence représentée à la figure 2 est la *boucle de transmission* qui effectue la progression dans le formulaire. (L'utilisateur peut également *revenir* en arrière et passer en revue les pages affichées précédemment, mais cette opération n'est pas différente, quant au concept, de la logique indiquée). Nous entrons dans la séquence à l'intersection où l'utilisateur a terminé une page de questions et cliqué sur *continuer* (étape « Envoyer » dans la figure).

44. Le processus d'*envoi* appelle l'applet TruePass en vue du chiffrement des données à l'aide de la clé publique de Statistique Canada. La page entière d'éléments entrés est chiffrée et stockée temporairement dans un cadre dissimulé de l'ensemble de cadres. Parallèlement, les données entrées qui ne sont pas chiffrées sont effacées. Une fois que les données sont chiffrées, les zones dissimulées sont transmises au logiciel du recensement.

45. Les données de l'utilisateur demeurent chiffrées jusqu'à ce qu'elles arrivent au logiciel. L'infrastructure ne peut pas accéder aux données en transit : elle fait simplement office de mécanisme de transmission.

46. Une fois que les données ont été reçues par le logiciel, elles sont déchiffrées à l'aide de la clé privée de Statistique Canada avant tout traitement devant être effectué par le logiciel. Les données du recensement font l'objet d'un contrôle de la cohérence, mais cette opération est minime. Le point important consiste à gérer la liste des membres du ménage (voir le paragraphe suivant) et à faire progresser l'utilisateur dans l'ensemble de questions portant sur chaque membre du ménage. De plus, les questions jugées sans objet d'après les réponses aux questions précédentes sont sautées.

47. On demande au répondant de préciser les membres du ménage dès le début de la session et, par la suite, les questions sont modifiées afin que le nom de la personne en question y figure. On vise ainsi à aider le répondant à être cohérent et à éviter qu'il oublie des membres du ménage. On a conçu cette méthode à l'aide d'essais de convivialité et de sorte que les différences avec le questionnaire papier soient moindres. (Le

questionnaire papier est disposé en colonnes et une colonne est utilisée pour chaque membre du ménage. En raison de l'espace offert à l'écran, il est impossible de procéder de cette façon).

48. Une fois qu'une page de questions a été traitée par le serveur, le logiciel produit la prochaine page de questions et il chiffre son contenu à l'aide de la clé publique du répondant (le logiciel TruePass offre des sous-programmes qui sont stockés dans le serveur et qui exécutent cette tâche). Ce chiffrement en sortie est important, car les données ainsi chiffrées peuvent contenir des données du recensement qui ont été entrées précédemment, en réponse à des questions personnalisées ou encore à une demande de l'utilisateur quant à l'affichage d'une page précédente.

49. Les données chiffrées sont envoyées au navigateur du répondant par l'entremise de l'infrastructure. Sous le navigateur, la clé privée du répondant sert à déchiffrer les données : la page des données chiffrées est placée dans un cadre dissimulé et les données correspondantes servent à remplir les zones affichées. Cette opération est transparente pour l'utilisateur et celui-ci continue à passer en revue la page ou à répondre aux questions de la nouvelle page pendant que le cycle de transmission s'exécute.

50. Le cycle prend fin lorsque le délai accordé est terminé ou lorsque l'utilisateur demande à interrompre la session ou à mettre un terme à celle-ci. En tel cas, le logiciel du recensement avise l'infrastructure (par une substitution inverse) que la session prend fin. L'infrastructure peut alors effectuer une fermeture de session automatique et renvoyer le certificat anonyme à l'ensemble de certificats. Ce certificat peut ensuite être réutilisé et être sélectionné aléatoirement pour un autre répondant.

51. La base de données du recensement qui conserve l'état du recensement est également mise à jour afin qu'elle indique si l'entrée des données dans le formulaire du recensement a été interrompue, si le formulaire est terminé ou s'il est incomplet (délai dépassé). Cette base de données de l'état est intégrée à toutes les voies de collecte afin que les procédures de suivi puissent être lancées au moment adéquat.

## C. Utilisation du service SCEAU à d'autres fins

52. Même s'il est quelque peu prématuré d'envisager le recours au service SCEAU pour une autre utilisation que le recensement, il importe de préciser qu'on a pris soin de concevoir un service indépendant plutôt qu'un simple élément appuyant le Recensement de 2006.

53. Il importe de faire remarquer que l'infrastructure commune appelée *Voie de communication protégée* a été conçue à titre de pierre angulaire de l'initiative canadienne *Gouvernement en direct (GED)*. Le projet GED a été lancé en 2000, dans le but d'améliorer l'accès des Canadiens et Canadiennes à l'information et aux services du gouvernement en tout temps, depuis n'importe quel endroit et dans la langue officielle de leur choix, d'ici 2005.

54. En plus de l'infrastructure commune de la Voie de communication protégée, le projet GED a permis de disposer d'un financement de lancement pour les réalisations ministérielles dans le domaine de l'offre de services électroniques aux Canadiens et Canadiennes. Les ministères se faisaient concurrence pour ces fonds en fonction de la portée (pénétration) et de l'innovation dont faisaient preuve leurs propositions.

55. Statistique Canada s'est imposé comme chef de file dans le projet GED et a reçu à obtenir des fonds pour son expérience initiale de collecte électronique des données (CED) pour le secteur privé : il s'agissait de donner aux entreprises la possibilité de répondre à nos enquêtes par l'intermédiaire d'Internet plutôt que par l'envoi par la poste des questionnaires papier. Par ailleurs, les responsables du projet du Recensement de la population de 2006 souhaitaient participer à l'initiative GED, mais ils devaient tenir également compte des risques quant à la disponibilité de l'infrastructure commune pour la répétition générale de 2004 ainsi que de certains problèmes de financement pour le volet en direct.

56. Un accord de partenariat entre Statistique Canada et la Voie de communication protégée a été conclu en juillet 2003 : celui-ci comprenait un financement de type partagé en vue de la mise sur pied du service

SCEAU. La part des coûts supportés par l'infrastructure commune correspondait à la possibilité de la réutilisation du service SCEAU par d'autres applications du gouvernement.

57. Pour pouvoir utiliser le service SCEAU pour d'autres utilisations, il suffit de revoir ses attributs de clé. Par-dessus tout, le service SCEAU offre un chiffrement de bout en bout bidirectionnel qui fait appel à des certificats d'ICP anonymes. Ainsi, on peut assurer un échange sûr de données confidentielles ou délicates pour lequel *l'identité de la personne n'a aucune importance*. Dans bien des situations c'est le cas : certaines personnes pourraient même avancer que cette situation prévaut la plupart du temps pour les services gouvernementaux. Par exemple, bon nombre d'opérations se font entre des « substituts » plutôt qu'entre les véritables personnes qui effectuent la transaction. Ces substituts agissent en notre nom et envoient des formulaires ou négocient des services.

58. De même, bien des opérations se fondent sur des justificatifs d'identité qui sont déjà en place et qui ne sont pas en rapport avec l'ICP. Par exemple, pour chacune des ventes par carte de crédit il suffit de disposer du numéro de la carte et parfois d'un code d'accès. Si vous choisissez de communiquer ces justificatifs d'identité à quelqu'un, cette personne peut effectuer la transaction. Toutefois, dans ce cas, on pourrait toujours s'attendre à ce que l'information de la carte de crédit et les détails de la transaction fassent l'objet d'un traitement confidentiel. On pourrait se servir du service SCEAU à cet effet.

59. En raison de sa nature bidirectionnelle, le service SCEAU est plus avantageux que le service courant de chiffrement NIP/SSL. Avec l'ICP, l'information délicate reçue et transmise est chiffrée, mais à l'aide de paires de clés différentes. Les données de sortie sont chiffrées à l'aide d'une clé qui est unique au répondant en question. On doit procéder ainsi pour la plupart des formulaires en direct pour lesquels des données entrées et transmises précédemment doivent être affichées ou lorsque des mises à jour en temps réel sont partagées.

60. En revanche, lorsqu'on doit disposer de la véritable identité de la personne qui effectue la transaction parce que la signature électronique a une portée légale ou parce qu'une authentification est exigée pour des raisons de sécurité, le service SCEAU ne convient pas. Le concept de protection des données confidentielles par un *SCEAU, sans signature*, est simple à expliquer au public.

61. On peut se servir du service SCEAU pour assurer une meilleure confidentialité à l'utilisateur général d'information, pour des services comme le courriel confidentiel. À l'instar de l'enveloppe sous double pli cacheté, les utilisateurs peuvent être assurés que le contenu n'a pas été vu par des tiers.

62. Des arguments d'ordre économique prévalent également en ce qui concerne l'utilisation à plus grande échelle d'un service semblable à SCEAU. En effet, ce service offre une voie confidentielle qui entraîne essentiellement des frais indirects moindres qu'un système ICP complet. Le besoin de répertoires et de services de gestion de clés étant moindre, le coût par transaction est donc normalement moins élevé. De plus, le service est beaucoup moins importun pour l'utilisateur que dans le cas d'une inscription à l'ICP et d'une authentification complète.

63. Même si le service SCEAU ne faisait pas partie au départ du plan de la Voie de communication protégée, son utilisation pour le recensement a suscité un intérêt au sein d'autres ministères et il deviendra sans doute un service d'utilisation générale.

## IV. CONCLUSION

64. Dans le présent document, nous avons décrit le service SCEAU, qui consiste en une utilisation spéciale de la technologie ICP. On a conçu ce service tout particulièrement en fonction du Recensement de la population canadienne, mais il pourra servir à d'autres utilisations. Même s'il convient tout particulièrement aux enquêtes statistiques, il peut s'avérer utile pour les transactions sur Internet, pour lesquelles la confidentialité est une exigence primordiale.

65. En même temps que le présent document est distribué pour la première fois (mai 2004), la répétition générale du recensement se fera à trois endroits au Canada. Les résultats de cette expérience serviront à peaufiner notre méthode pour les services en direct pour les enquêtes sociales ainsi qu'à sonder l'acceptation générale quant à ce type de protection de données. Il reste à voir si la confiance du public envers un service en direct peut être rehaussée.

- - - - -