AU DELÀ DE LA CARTE

POUR OFFRIR AU CITOYEN UNE GAMME INTÉGRÉE DE SERVICES :

L INFRASTRUCTURE NÉCESSAIRE

13 février 1997

TABLE DES MATIÈRES

---

1. INTRODUCTION

1.1 Rappel des faits et des enjeux

- Dans le contexte du déploiement des autoroutes de l information et de la multiplication des points de services électroniques aux citoyens, le CRISP a proposé au gouvernement en avril 1995 l adoption d une carte multiservices intelligente. Une telle carte permettrait à n importe lequel ministère ou organisme d offrir des services personnalisés à chaque citoyen désireux de transiger avec son gouvernement par l entremise de points de services électroniques et contribuerait à simplifier les relations entre l État et le citoyen.

  En décembre 1995, le CRISP déposait au Secrétariat de l autoroute de l information (SAI) un inventaire d exemples de façons de faire qui pourraient être transformées et simplifiées dans certains ministères ou organismes avec l avènement des inforoutes si on disposait d un moyen fiable d identification du citoyen.

  À l automne 1996, la Régie de l assurance-maladie annonce le lancement d une carte " santé ". Pour les membres du CRISP, l application santé est considérée comme étant la principale application porteuse introduisant une carte d accès aux services de l État, à la condition toutefois que le "design" de la carte

permette une évolution dans une perspective multiservices.

Parallèlement, la Commission de la culture lançait deux opérations visant à recueillir l opinion des citoyens sur les enjeux du développement des autoroutes de l information et sur les problèmes relatifs à l identification des québécois.

Le CRISP se sent concerné par ces problématiques, dans la mesure où les banques d informations électroniques détenues par les ministères et organismes du gouvernement du Québec et les systèmes informatiques qui les soutiennent sont sous la responsabilité opérationnelle de ses membres. Les technologies pour offrir des services personnalisés à distance, par l entremise de guichets automatisés de services, d Internet ou de la télévision interactive sont en déploiement au Québec comme partout dans le monde. Ces technologies peuvent transformer et simplifier les relations entre l État et ses citoyens.

Les autoroutes de l information viennent définitivement modifier la façon dont les ministères et organismes offrent leurs services aux citoyens, permettent d organiser autrement l offre gouvernementale de ces services et exigent d autres moyens pour identifier à distance un citoyen qui a droit à un service. Le CRISP insiste sur l importance de viser à simplifier l offre de services plutôt que d en accroître la complexité : la prolifération de services électroniques risque d accentuer l image du " labyrinthe " trop souvent accolée au gouvernement, et de décupler les contrôles d identité inhérents à ce type de services. La carte multiservices est un des moyens permettant d atteindre cette simplicité.

1.2 Le mandat

- Dans la poursuite de cette réflexion, le CRISP cherche à illustrer l infrastructure requise pour qu un citoyen puisse accéder facilement et de façon transparente à un ensemble d informations et de services gouvernementaux le plus grand possible, à partir d une variété de points de services et en utilisant une carte multiservices.

1.3 Les hypothèses de travail

- Le CRISP a appuyé sa réflexion sur un certain nombre d hypothèses ou conditions souhaitables, qui vont constituer les balises des solutions à retenir : souhaitables,
    - une seule carte par citoyen;souhaitables, qui vont constituer les balises des solutions à retenir :
    - une seule carte pour tous les services offerts par les différents ministères et organismes ;
    - une carte permettant d obtenir des services personnalisés à partir d une variété de points de services électroniques;
    - une seule et unique procédure d'utilisation pour réaliser l'ensemble des transactions électroniques avec l'État, et ce peu importe le moyen ou le canal utilisé;

- une seule transaction pour rejoindre plusieurs ministères ou organismes, par exemple pour un changement d'adresse;
- un citoyen peut obtenir une vue synthèse de ses dossiers détenus par les organismes publics;
- les informations publiques relatives à l identification d une personne qui sont détenues par plusieurs ministères et organismes sont partageables;
- le niveau actuel de sécurité et de fiabilité est augmenté.

1.4 Le groupe de travail

- Afin de réaliser cette tâche, le CRISP a mis sur pied un groupe de travail formé de gestionnaires et de professionnels provenant des ministères et organismes suivants :
  - Commission administrative des régimes de retraite et d assurance
  - Directeur de l État civil
  - Directeur général des élections
  - Ministère de l Emploi, de la Solidarité et de la Condition féminine
  - Ministère de l Environnement et de la Faune
  - Ministère de la Santé et des Services sociaux
  - Ministère des Relations avec les citoyens et de l Immigration
  - Ministère du Revenu
  - Régie de l assurance-maladie du Québec
  - Régie des rentes du Québec
  - Société d assurance automobile du Québec

  En outre, des représentants du Secrétariat à l autoroute de l information ont été consultés à quelques reprises par le groupe de travail.

---

2. LES OBJECTIFS

2.1 L objectif principal

- À quoi servirait donc une carte multiservices? En quoi cette carte pourrait-elle être utile pour un citoyen? Comment fonctionne ce type de carte? Qu est-ce qu une telle carte vient changer dans les façons de faire des ministères et organismes? Voilà les questions auxquelles s est attaqué le CRISP.

  Le groupe de travail s est donné pour objectif d illustrer comment les différents ministères et organismes pourraient supporter conjointement et globalement l offre gouvernementale des services au citoyen si celui-ci disposait d une carte multiservices lui permettant d obtenir des services personnalisés à partir de points de services électroniques.

2.2 Les objectifs spécifiques

Afin de rencontrer cet objectif, les membres du groupe ont convenu ensuite de :

1. définir les contours de l autoroute de l information et des exigences de son utilisation pour les services gouvernementaux;
2. illustrer les technologies des cartes à puce derrière le concept de la carte multiservices;
3. illustrer le contenu d une carte multiservices gouvernementale, les exigences liées à son émission et à son utilisation;
4. proposer différentes alternatives d infrastructures possibles et de comparer les exigences et les gains qui y sont reliés;
5. souligner quelques uns des éléments critiques que le gouvernement doit prendre en compte.

2.3 Les limites du mandat

- Dans cette réflexion, le CRISP met d abord l accent sur la réalisation de **transactions personnelles par l entremise de points de services électroniques** entre le citoyen et l'État. Il n'aborde donc pas la diffusion d'informations d'intérêt général de la part de l'État vers l'ensemble de la population. De plus, seuls les citoyens ont été considérés, les personnes morales ayant été, par conséquent, volontairement écartées du périmètre d'analyse du mandat. Les services aux entreprises par le biais des autoroutes de l information nécessitent en soi une analyse qui pourrait faire l objet d un autre mandat.

  Les transactions personnelles réalisées par l entremise de points de services électroniques peuvent avoir ou non des implications monétaires. Par exemple, une transaction personnelle peut s'apparenter à une demande d'indemnisation de toute nature, au renouvellement de droits, à l'acquisition de permis divers, à la consultation et à la mise à jour de dossiers moyennant un déboursé. Cet aspect ne sera que brièvement abordé et mériterait également une étude spécifique.

  Les propositions de scénarios ne s'attarderont pas à identifier les acteurs qui devraient réaliser les fonctions inhérentes à chacun d'entre eux. Il est prématuré à ce stade d identifier des responsables et ces décisions appartiendront à d'autres instances.

---

3. LES BESOINS D IDENTIFICATION " ÉLECTRONIQUE "

- L identification, ou le besoin de s identifier, nous rappelle la Commission de l accès à l information dans son mémoire d octobre 1996, n est pas un fait nouveau propre au Québec et est né de deux objectifs poursuivis tout autant par le secteur public que par le secteur privé :

- identifier une personne pour s'assurer de son éligibilité à un bien ou à un service;

- retracer les fraudeurs ou les personnes qui ne s'acquittent pas de leurs obligations sociales ou financières.

- Une " carte d identité " au sens où on l entend généralement utilise des éléments informationnels (photo, nom, prénom, numéro, etc.) utilisables dans un contexte d identification en " face à face ". Une carte conçue pour une authentification par mode électronique commande un autre type d informations, électroniques celles-là, permettant à un automate de reconnaître l utilisateur de la carte.

  Les ministères et les organismes qui veulent offrir des services personnalisés à un citoyen par l entremise de points de services électroniques font face à une problématique complexe pour s assurer de l identité de la personne " au bout du fil " et pour garantir la sécurité des transactions :

- **Certifier l identité** des utilisateurs (établir l identité des personnes)

- **Authentifier** les utilisateurs (la transaction provient du bon expéditeur de qui elle est censée provenir)

- Garantir la **confidentialité** de l information (seul le destinataire d un message confidentiel sera en mesure de le lire)

- Préserver l **intégrité** de l information (le contenu du message n est pas modifié entre l émission et la réception)

- Garantir l **origine** du message et sa **non-répudiation** (la signature)

- **Contrôler l accès** aux informations

- Les besoins d identification peuvent être en partie rencontrés en utilisant des techniques de vérification croisée, en demandant par exemple à chaque interlocuteur de fournir certaines informations connues de lui seul (le prénom de sa mère, le montant inscrit à la 12e ligne dans son rapport d impôt). Ces moyens sont largement utilisés, au téléphone, mais sont souvent plus difficiles à mettre au point avec des points de services électroniques, le niveau de sécurité qui leur est associé est extrêmement variable et les ministères et organismes qui les utilisent doivent évaluer à chaque fois le niveau de risque qu ils sont prêts à assumer.

  La multiplication de ces demandes d informations apparaît vite tatillonne pour le citoyen, et ne contribue pas à simplifier les relations qu il entretient avec son gouvernement.

  Il faut ajouter à cette série d exigences toutes les contraintes rattachées à la sécurité des transactions, plus particulièrement lorsque les informations ont un caractère confidentiel, stratégique ou financier, dans la mesure où le citoyen

voudra rapidement compléter des transactions monétaires par l entremise des points électroniques de services.

La carte multiservices ne doit donc pas être assimilée à une "carte d'identité ", quoiqu elle réponde à un besoin d identification dans un réseau informatique. Toutefois, si l'État optait éventuellement pour une carte d'identité, la carte multiservices pourrait être retenue comme support physique de cette carte d'identité.

---

4. LES AUTOROUTES DE L INFORMATION

- Pourquoi doit-on se préoccuper de questions d identification et de sécurité sur les autoroutes de l information? Comment peut-on répondre aux besoins des ministères et organismes et permettre à un citoyen des communications sécuritaires? Où en sont à cet égard les réseaux informatisés qui supportent les autoroutes?

- Les premiers réseaux informatiques reliaient les entreprises entre elles et des succursales à un ordinateur central. Encore aujourd hui, ces réseaux fonctionnent dans un environnement contrôlé et sont utilisés sous supervision par du personnel réservé. Leur sécurité repose essentiellement sur l identification de l utilisateur à l aide d un code d usager et d un mot de passe. La route est privée et protégée. La majorité des réseaux informatiques gouvernementaux à usage interne appartiennent à cette catégorie.

- Aucune carte n est nécessaire, la sécurité est assurée avec des solutions logicielles.

- Le monde bancaire a introduit la seconde génération de réseaux, notamment avec les **guichets automatiques** et les **terminaux point de vente (débit)**. Les guichets sont utilisés sans supervision, par une clientèle diversifiée, mais les guichets tout comme les terminaux point de vente sont des appareils physiquement sécuritaires. L **authentification** de l utilisateur devient obligatoire avant de donner accès aux fonctions bancaires et la partie la plus sensible du message est **chiffrée** pour assurer la **confidentialité**. Il n y a pas comme tel de signature des messages.

- Les solutions sécuritaires mises en place jumellent une carte à piste magnétique (" élément possédé ") et un NIP (" élément connu "). Il faut aussi noter que dans les réseaux bancaires, le consommateur a signé avec son institution une convention qui vient fixer les conditions d utilisation de la carte et responsabilise son détenteur.

- D autres **autoroutes privées,** plus récentes, prévoient habituellement une sécurité à la fine pointe. Ces réseaux peuvent être ouverts au grand public (UBI ou SIRIUS) ou réservés à une clientèle pré-identifiée (le réseau de la RAMQ ou de la CSST par exemple). Ces réseaux privés et sécuritaires doivent cependant, tôt ou tard, se relier aux autres réseaux à sécurité variable (réseaux

bancaires, Internet). Différents autres réseaux privés de **guichets de services** (ex. bornes télématiques TouchNet) viennent aussi se greffer sur ces réseaux de même que sur les réseaux bancaires.

- **Internet** est un réseau public, ouvert à tous les types d appareils et de postes de travail, à toutes les catégories d utilisateurs et pour toutes sortes d usages.

- Pour protéger l information lors de son transport, les exigences déjà présentes à un moindre degré dans les réseaux précédents deviennent incontournables : il faut assurer la sécurité des transactions de bout-en-bout, de leur point d origine à leur point d arrivée. Comme on ne peut pas protéger la route, il font donc blinder les messages.

  Les autoroutes de l information ou les inforoutes, selon la terminologie utilisée, sont composées de tous ces types de réseaux : l inforoute est un **réseau de réseaux**. Le niveau de sécurité d une transaction qui les emprunte ne peut être plus élevé que le niveau de sécurité du maillon le plus faible du réseau sur lequel elle transite.

  Un ministère ou un organisme doit donc évaluer les risques et s assurer du niveau de sécurité adéquat de la transaction personnelle qu il veut offrir à un citoyen par l entremise d un point de service électronique, en fonction du ou des réseaux sur lesquels cette transaction est appelée à transiter.

---

5. LA CARTE MULTISERVICES

- Il existe toute une panoplie de cartes informatiques, utilisant différentes techniques pour reconnaître ou lire des informations. La carte à microprocesseur représente dans l état actuel de l avancement des technologies la carte sinon la plus répandue du moins la plus prometteuse.

5.1 Les différentes cartes et leurs caractéristiques

Ve

- La **carte munie d un code à bâtonnets ("code à barre")** est largement répandue. C est une carte munie d un code graphique lisible par un lecteur optique. Ce type de code apparaît sur le permis de conduire et est utilisé par les corps policiers.

  La **carte à piste magnétique** est une carte pourvue d une surface magnétisable sur laquelle sont stockées des informations. Les cartes bancaires de crédit et de débit sont des cartes à piste magnétique.

  Il existe sur le marché trois grands types de " vraies " cartes à puce : la **carte à**

mémoire, la **carte à logique câblée** et la **carte à microprocesseur**. Elles ont chacune été conçues pour des usages spécifiques et elles ne permettent pas toutes le même niveau de sécurité.

La **carte à mémoire** et la **carte à logique câblée** disposent d une " mémoire " sous forme de jetons qui sont " grillés " au fur et à mesure de leur consommation. Ce sont des cartes jetables. La carte *La Puce* de Bell Canada appartient à cette catégorie.

La **carte à microprocesseur** est dotée d un microprocesseur comparable à ceux des micro-ordinateurs, mais avec des capacités beaucoup plus limitées. Elle est programmable, dispose d une unité de calcul pour l exécution de commandes, d un système d exploitation, d une mémoire découpée en répertoires et fichiers dont les accès sont contrôlés en lecture, écriture, et effacement . Elle est dotée de mécanismes d accès (par l utilisation de mots de passe ou de NIP) et de sécurité cryptographique. Elle peut être personnalisée comme la carte à piste. Elle n est pas reproductible, elle conserve les secrets, l information et les clés de façon sûre, et permet l ajout de nouvelles applications. De plus, son développement et son évolution font l objet d une normalisation ISO.

La carte à microprocesseur est un outil d authentification utilisée pour les cartes bancaires (Europay, Mastercard, Mondex), les cartes de téléphonie cellulaire (Fido) et les cartes santé (France, Espagne, Allemagne).

Le tableau qui suit, adapté d un document produit par le SAI, compare les caractéristiques de ces différentes cartes.

Tableau comparatif des caractéristiques des principales cartes

BM = carte à bande magnétique M = carte à mémoire et à logique câblée **MP = carte à microprocesseur**	**BM**	**M** **LC**	**MP**
Caractéristiques			
Respect du principe élément possédé / élément connu	X	X	X
Carte non reproductible		X	X
Conservation de secrets de façon physiquement sûre		X	X
Conservation d informations		X	X
Carte pouvant être personnalisée	X	X	X
Carte programmable			X
Carte pouvant effectuer des opérations cryptographiques dynamiques			X
Pouvant contenir des clés de chiffrement en toute sécurité			X

Pouvant contenir des certificats			X
Solution évolutive permettant l ajout de nouvelles applications			X

- Toutes ces cartes, quelle que soit la technologie qu elles utilisent, doivent bien sûr pouvoir être lues par un périphérique lecteur de carte. Ces appareils se répandent rapidement et obéissent à des normes sévères qui garantissent leur utilisation à l échelle mondiale. Tous les appareils ayant accès aux autoroutes de l information (micro-ordinateur, télévision interactive, guichets automatisés de services, téléphones, etc.) ont d ores et déjà commencé à être dotés de lecteurs capables de lire les cartes à microprocesseur. Par ailleurs, plusieurs cartes juxtaposent plus d une technologie : des cartes à piste sont dotées de codes à bâtonnets et des cartes à puces ont aussi une piste magnétique.

5.2 Le contenu d une carte multiservices et ses variantes

- Une **carte à microprocesseur** utilisée comme support pour une carte multiservices gouvernementale permet d imaginer une carte véhiculant des informations visibles et non visibles, aux fins d identification d un citoyen désireux de transiger avec son gouvernement par l entremise de points de services électroniques, sur les autoroutes de l information quelles qu elles soient.

  Les **informations visibles** (nom, photo ou numéro,) présentes sur la carte ne le sont que pour permettre au détenteur de reconnaître sa propre carte parmi d autres ou encore de s identifier auprès d une personne physique.

  Du strict point de vue technologique, aucune information n a besoin d être visible **sur** la carte, puisqu un point de service électronique (une machine) ne peut lire que des informations qui sont dans la puce. Cette hypothèse, absurde lorsque poussée à cet extrême, illustre bien que la carte multiservices n a pas besoin d être une carte d identité au sens où on l entend généralement. Elle ne l est que pour des besoins strictement électroniques.

  En tout état de cause et compte tenu qu une telle carte devra satisfaire aux exigences spécifiques de cartes comme la carte d assurance-maladie ou le permis de conduire, les informations d identification "publiques" requises pour ces cartes devraient y être inscrites ou embossées. Il faudra également prendre en compte le caractère temporaire d éléments d informations comme l adresse postale, par exemple, qu il pourrait être coûteux de vouloir maintenir à jour sur la carte.

  Les informations **non visibles** (électroniques) sont celles qui permettent à un système électronique de reconnaître le détenteur de la carte et qui garantissent la sécurité de ses transactions personnelles électroniques. Une partie de ces informations sont fixes, alors que d autres ont un caractère plus volatile.

- Un **authentifiant** (le plus souvent un NIP, ou encore une empreinte) permet au détenteur d "activer" sa carte, et d être le seul à pouvoir le faire. Il faut noter ici que cet authentifiant n est pas conservé ailleurs que dans la puce de la carte et qu il n est ni nécessaire ni souhaitable de maintenir un registre central des NIP.

- Un **certificat** et des **clés,** attribués au détenteur de la carte par une **autorité de certification** reconnue, permettent l usage d une **signature électronique** pour garantir l origine, l intégrité et la non-répudiation d une transaction ou d un message.

- Des **éléments de cryptographie** pour chiffrer et encrypter un message ou des informations en fonction de besoins accrus de confidentialité et d intégrité de certains types de messages ou de transactions.

- Un fichier d **informations communes** pouvant contenir des informations qui sont les mêmes pour tous les ministères et organismes , comme les informations nominatives à déclaration obligatoire ou un numéro commun. Rappelons que la technologie de la carte à microprocesseur permet d ajouter, de corriger et de détruire des informations.

- Les adresses du citoyen pourraient être inscrites au besoin dans cette partie commune, mais la pertinence de le faire devra être évaluée plus à fond. Un même citoyen peut détenir plusieurs adresses postales : domicile principal ou secondaire, adresse temporaire, adresses d affaires, auxquelles s ajoutent les différents numéros de téléphone et de télécopieur sans compter les adresses électroniques. Outre le caractère volatile de plusieurs de ces éléments, il faut souligner que les adresses sont utilisées par plusieurs ministères ou organismes pour évaluer l admissibilité d un citoyen à un droit ou un service. Ne mentionnons à titre d exemple que le Directeur général des élections.

- Des **répertoires ou fichiers spécialisés** pouvant contenir des informations spécifiques comme les droits et les privilèges du détenteur de la carte, permettent à chaque fournisseur de service (chaque ministère, chaque organisme) d autoriser celui-ci à accéder à des informations personnelles ou à des services particuliers.

- La technologie de la carte à microprocesseur permet de structurer des répertoires sans aucun lien entre eux, et d en réserver l accès aux seules personnes ou organismes autorisés (les hôpitaux pour les informations Santé ou les policiers de la route pour les informations sur le permis de conduire par exemple).

  La carte à microprocesseur permet de conserver et transporter en toute sécurité un minimum d information relative à l utilisateur et aux services auxquels il a droit. Cependant, compte tenu que la capacité de stockage est malgré tout limitée et que la carte peut être perdue ou détruite, il faut que ces informations soient conservées " en double " dans une ou plusieurs banques de données traditionnelles.

  On peut aussi ajouter sur la carte de nouveaux répertoires et de nouvelles informations au fur et à mesure que de nouveaux services voient le jour afin d éviter d émettre de nouveau des cartes à chaque fois qu on veut modifier ou

ajouter un service.

Il faudra là aussi évaluer plus à fond la pertinence d inscrire dans la carte des droits ou des privilèges temporaires ou révocables qu il pourrait être difficile ou coûteux de maintenir à jour. La carte pourrait tout aussi bien ne contenir que les informations communes et laisser aux organisations le soin de gérer dans les banques centralisées chez eux les droits et les privilèges de leurs clients, ou de n y inscrire que des informations à caractère plus permanent.

Ajoutons enfin qu un numéro de série unique et normalisé est attribué à chaque puce lors de la fabrication, comme dans le cas des moteurs d automobile.

5.3 L émission d une carte multiservices par un gouvernement

- **L émission** d une carte multiservices par un gouvernement fait intervenir toute une série d opérations pour s assurer de l identité des personnes à qui une carte est émise, des droits accordés à cette personne par les différents ministères et organismes, de même qu aux mécanismes nécessaires pour assurer la sécurité et la protection des messages et des transactions initiées avec la carte .

  Le gouvernement doit donc en premier lieu établir l identité de la personne à qui il désire émettre une carte, et lui attribuer les éléments de sécurité qui lui seront nécessaires**.**

  On appelle **certification** ce processus formel d identification qui fait intervenir une tierce partie impartiale et indépendante qui garantit , à divers niveaux et suivant des normes préétablies, l identité de parties transigeant à distance. Une **autorité de certification** reconnue devra établir formellement l identité du citoyen et autoriser l émission d une carte dotée de ses **informations visibles et invisibles.** Le gouvernement devra mandater un organisme responsable qui pourrait être une organisation qui détient déjà des responsabilités dans ce domaine, comme la direction de l État civil par exemple.

  Un **certificat d identification** est associé à la carte, sorte de document électronique qui lie le détenteur de la carte à une paire de **clés** qui constitue l élément de base de sa **signature électronique,** nécessaire pour garantir l origine, l intégrité et la non-répudiation des transactions effectuées sur les autoroutes de l information.

  La tenue d un **registre central** des cartes émises est incontournable pour s assurer qu un citoyen ne peut avoir qu une seule carte, pour assurer le remplacement des cartes perdues ou volées, et pour permettre le renouvellement des cartes à échéance. Ce registre ne devrait contenir que les informations nominatives à déclaration obligatoire et les certificats octroyés pour permettre des transactions électroniques. Dans le concept d une carte multiservices " volontaire ", seuls les citoyens désirant se prévaloir de ce privilège seraient inscrits dans ce répertoire.

  Encore ici, il faudra statuer sur la pertinence de conserver la ou les adresses du citoyen dans le registre central eu égard aux besoins spécifiques des différents ministères et organismes.

Les informations confidentielles administrées par les différents organismes autorisés (santé, revenu, justice, rentes, assurances) sont détenues, comme aujourd hui, par ces seuls organismes, dans des fichiers sous leur seule responsabilité.

Les **droits et privilèges** accordés à un citoyen d avoir accès à des données ou à des services déterminés pourraient être inscrits de façon électronique sur la carte ou conservés dans chaque ministère ou organisme. Le terme **habilitation** est souvent utilisé pour désigner l ensemble des droits et privilèges d un détenteur de carte. Ces droits sont accordés par chaque ministère ou organisme public fournisseur de services en fonction des lois qu il administre et de ses règles propres. L inscription des droits sur la carte, si on décidait de le faire, pourrait également être faite par l autorité de certification, autorisée préalablement par chaque ministère et organisme dont c est la responsabilité.

Le processus de certification, l inscription des droits et privilèges, la remise de la carte dans les mains du détenteur et son activation, sans compter la fabrication de la carte elle même, font intervenir toute une série d opérations qui se réalisent de différentes façons et ne peuvent souffrent d aucune faiblesse. Il faut retenir que cette étape est cruciale et peut-être le maillon le plus faible de la sécurité des autoroutes de l information.

5.4 L utilisation d une carte multiservices par un citoyen

- L usage d une carte multiservices permet à tout citoyen de communiquer et de transiger simplement avec son gouvernement par l entremise de points de services électroniques. Il n appartient pas au CRISP de statuer sur le caractère obligatoire d une telle carte pour cet usage comme pour tout autre type d usage.

  La vérification de l identité du client transigeant à distance avec un ministère ou un organisme par l entremise d un point de services électroniques, son **authentification,** fait intervenir plusieurs niveaux de vérification.

  Le premier niveau de vérification se fait au point d entrée électronique (guichet, Internet, UBI) pour vérifier que la carte est bien entre les mains du bon détenteur . Cette première **authentification** est basée sur la vérification que l objet possédé (la carte) correspond à l élément connu de la seule personne qui détient la carte (NIP ou empreinte digitale). La généralisation éventuelle de la carte multiservices pose le problème de la mémorisation du NIP par une partie de la population. L examen d une donnée biométrique en substitution au NIP apparaît prometteur à plusieurs égards.

  Le second niveau de vérification vise à s assurer de la provenance de la transaction. Dans les systèmes bancaires sécurisés, c est le même authentifiant (NIP) qui est utilisé. Dans les réseaux publics, où chaque transaction doit porter son propre mécanisme de sécurité, c est un des rôles dévolu à la **signature numérique** et aux mécanismes de **clés privées et publiques** qui la soutiennent.

Le système de **signature numérique** sert donc à garantir la **provenance** du message (la transaction vient de la bonne personne) et sa **non-répudiation** (l émetteur de pourra nier plus tard en être l auteur).

Le troisième niveau de vérification consiste à s assurer de l **habilitation** du client, i.e. s assurer des **droits d accès** à un service ou à un autre du détenteur de la carte.

Le système de **signature numérique** servira aussi à encrypter certaines transactions qui nécessitent un niveau de confidentialité plus élevé, et à garantir la **confidentialité** de la transaction (seul le destinataire peut lire le contenu) et son **intégrité** (le contenu n est pas modifié).

Ces caractéristiques imposent rapidement des choix stratégiques pour le gouvernement et seront mis en lumière dans les deux alternatives décrites dans les scénarios d infrastructures du chapitre 6 :

L authentification devrait-il prendre la forme

- d un processus unique et d un mécanisme unique pour tous les fournisseurs gouvernementaux, sous la responsabilité d une autorité centrale gouvernementale ?
- d un processus unique pour tous les fournisseurs gouvernementaux, mais sous la responsabilité de chaque ministère ou organisme fournisseur de service?
- d un processus propre à chaque ministère et organisme fournisseur de services?

- Ces choix sont stratégiques à plusieurs égards, autant en termes des services offerts au citoyen qu en matière de répartition des responsabilités qui devront être assumées par les ministères et des investissements technologiques qu ils devront engager.

---

6. L INFRASTRUCTURE

6.1 Prémisses et conditions universelles

- Avant même de présenter des scénarios possibles en matière d'infrastructure relative à la carte multiservices, un certain nombre de prémisses ou de conditions universelles à tous les scénarios sont nécessaires et inévitables. En effet, la mise en place d une carte partagée par tous les ministères et organismes exige une mise en commun minimale d informations, de spécifications et de fonctionnalités, et ce indépendamment des scénarios technologiques et fonctionnels retenus.

  Voici au moins quatre éléments communs :

Facture de la carte multiservices

L apparence physique de la carte multiservices et les informations lisibles qu elle doit offrir doivent être normalisées. En effet, des éléments d information lisibles devront être disponibles sur la carte étant donné qu elle devra probablement être utilisée pour la réalisation de transactions en face à face et en l absence d équipements pouvant lire les informations contenues électroniquement dans celle-ci.

Ces informations lisibles seront le résultat de la recherche du plus petit dénominateur commun entre les ministères et les organismes. Par exemple, si la carte se veut un substitut au permis de conduire et à la carte d assurance-maladie, elle devra au moins contenir une photo pour les transactions en face à face et des données permettant de reconnaître cette pièce comme étant un permis de conduire à l extérieur du Québec.

Architecture relative à la carte multiservices

Les éléments technologiques entourant le concept de la carte multiservices doivent faire l objet d une standardisation. Ces éléments ont trait au choix comme tel du type de carte à microprocesseurs (système d exploitation, architecture interne), au système de cryptographie retenu (système de biclé privé et public, système de clés symétriques) et aux canaux transactionnels possibles et à leurs spécificités.

Procédures de certification et d authentification

La procédure de certification nécessaire avant de procéder à l émission d une carte doit être unique et rigoureuse. Cette procédure cruciale ne peut pas faire l objet de raccourcis.

De la même façon, la procédure d authentification de l utilisateur de la carte doit être uniforme afin de respecter le concept de la carte multiservices suggéré.

Banques de données

Dans le but d assurer l unicité des cartes actives, un répertoire doit être créé. Celle-ci doit contenir les données minimales pour être en mesure de procéder à la vérification des cartes en usage avant d en émettre une nouvelle. Les données conservées actuellement dans le registre d'état civil constituent, à priori, une grappe de données intéressantes et minimales.

Ce répertoire ne contient pas nécessairement les identifiants de chacun des ministères et organismes susceptibles d être intéressés par la carte multiservices. Cet ajout fait partie intégrante d'un scénario fonctionnel.

6.2 Description et explication des scénarios

- La reconnaissance de la nécessité d'une mise en commun de plusieurs

éléments relatifs à l'implantation d'une carte multiservices nous amène inévitablement à considérer dans cette même foulée l'introduction d'une entité virtuelle ou administrative qui assumerait les responsabilités relatives au maintien de ces quatre conditions de base.

Voici donc deux scénarios qui ont été conçus autour d'une variation du degré de partage des responsabilités et des tâches entre les ministères et organismes et cette entité appelée "Infrastructure commune" . Les scénarios décrivent deux approches diamétralement opposées et sont présentés en prenant pour acquis que les éléments communs sont respectés.

Le premier scénario préconise la plus grande autonomie possible des ministères et des organismes fournisseurs de service et un minimum d informations, de fonctionnalités et de structures mises en commun. C est un scénario basé sur la plus grande **décentralisation** possible des responsabilités des ministères et organismes tout en offrant au citoyen une image cohérente de ses relations avec l État.

Le second scénario prône le maximum de mise en commun des informations, des fonctionnalités et des structures. C est un scénario basé sur la rationalisation et l i**ntégration** de structures administratives et technologiques actuelles au profit d une offre intégrée de services au citoyen.

Le tableau suivant présente et compare les deux scénarios retenus : la **décentralisation** et l **intégration.** Après avoir décrit sommairement chacun des scénarios, ceux-ci sont présentés en fonction de 12 caractéristiques pouvant les différencier:

1. Le contenu de la carte
2. L émission de la carte (certification)
3. Le répertoire d informations communes
4. L attribution des droits d accès
5. L authentification du client lors de l'utilisation
6. La sécurité du dialogue transactionnel
7. Les services spécifiques
8. Les services génériques
9. Le portefeuille de services
10. La navigation à travers les services offerts
11. Les informations publiques d identification qui sont communes aux ministères et organismes
12. Les fonctions de paiement

- Les deux scénarios présentent des visions volontairement opposées, pour bien illustrer que la carte multiservices permet de simplifier un peu, ou beaucoup, l offre de services gouvernementaux au citoyen, tout comme elle permet de modifier un peu, ou radicalement, la façon dont le gouvernement organise son offre de services.

Il importe cependant de souligner que peu importe le scénario les informations confidentielles administrées par les différents organismes autorisés (santé, revenu, justice, rentes, assurances) sont détenues et protégées par ces seuls organismes, dans des fichiers sous leur seule responsabilité.

Une représentation graphique des deux scénarios est annexée (voir annexe 1).

6.3 Les scénarios comparés

Caractéristiques	**Scénario** **DÉCENTRALISATION**	**Scénario** **INTÉGRATION**
Description sommaire	Ce scénario préconise la plus grande autonomie possible des ministères et des organismes fournisseurs de service et le minimum d informations, de fonctionnalités et de structures mises en commun. Dans ce cas-ci, l'infrastructure commune assure le volet normalisation de la carte et s'assure de l'existence d un répertoire central des données minimales. Le citoyen fait affaires comme aujourd hui avec des ministères et des organismes distincts.	Ce scénario prône le maximum de mise en commun des informations, des fonctionnalités et des structures. Ici, l'infrastructure commune est omniprésente et assure tout le dialogue entre les ministères et organismes et les citoyens. Le délestage de plusieurs fonctions, qui dans le scénario décentralisation sont sous le contrôle de chacune des organisations, sont maintenant réalisées au profit de leur intégration au sein d'une infrastructure commune à développer. Quoiqu il continue à faire affaires avec des ministères et des organismes distincts, le citoyen a l impression de communiquer avec un gouvernement.
1. **Contenu de la carte** (voir point 5.2)	Des **informations sur la carte :** nom, prénom, photographie, sexe, date de naissance, date d'expiration, etc. pour être en mesure de réaliser également des transactions en mode face à face, en fonction des besoins minimaux communs des ministères et organismes. Des **informations dans la puce** : • les mêmes identifiants que ceux lisibles sur la	Idem. Par définition, la carte et son contenu sont normalisés.

	carte; • un mot de passe **(**NIP, données biométriques, etc.) qui permet d ouvrir la carte; • des données relatives à la sécurité des transactions comme une **clé privée** qui, jumelée à une clé publique émise par une autorité de certification permet de composer une **signature électronique;** • et le cas échéant des **droits d accès :** nas, nam, no permis de conduire, no client, no de dossier, etc.	
Émission de la carte **(certification)** (voir point 5.3)	Chaque ministère ou organisme fournisseur de services émet la carte multiservices en fonction des procédures et des standards établis. Par conséquent, chaque entité possède la capacité de certification. Le citoyen peut obtenir sa carte de l un ou l autre ministère ou organisme avec lequel il fait affaires, et s assurer auprès des autres que ses droits et privilèges y sont inscrits.	Le processus de certification est sous le contrôle d'un seul organisme responsable. Celui-ci peut s'adjoindre au besoin des partenaires tout en gardant le pouvoir sur la totalité du processus. Le citoyen obtient sa carte auprès d un organisme unique ou de ses mandataires aptes à certifier l identification des citoyens et d émettre les cartes.

Répertoire d informations communes	La création d un registre central des cartes émises est incontournable pour s assurer qu un citoyen ne peut avoir qu une seule carte, pour assurer le remplacement des cartes perdues ou volées, et pour permettre le renouvellement des cartes à échéance. S y ajoutent les certificats et les clés. Dans ce scénario, seules les données essentielles à ce type de contrôle sont conservées.	Ce scénario implique obligatoirement la mise en place d'un répertoire d informations communes qui contiendrait les données nécessaires à l'identification d'un citoyen, son identifiant électronique, tous les identifiants spécifiques à chacune des organisations, la date d'expiration de la carte et toute autre donnée commune jugée utile. Des liens permanents sont développés entre toutes les organisations et cette infrastructure commune afin de garantir la mise à jour en temps réel du répertoire en ce qui concerne les identifiants.
Attribution des droits d accès	Chaque organisation inscrit son ou ses identifiant(s) et les données qu'elle juge nécessaires sur la carte. Ceci dans le but de simplifier les communications et de devoir répéter sans cesse la procédure de demande d'identifiants auprès du citoyen. Le contenu du répertoire central étant minimal, une organisation ne pourra pas s'y référer	L'architecture de la carte multiservices devrait prévoir qu'une organisation puisse inscrire ses identifiants sur la carte multiservices du citoyen désirant faire affaires électroniquement avec elle. La décision de l'inscrire revient, en bout de piste, à chacune des organisations. En procédant ainsi, une organisation évite de devoir consulter constamment la banque centrale des données pour connaître l'identification de l'utilisateur qui désire transiger avec elle. Il n'est pas exclu qu'à l'émission de la carte, l'agent responsable puisse immédiatement inscrire des identifiants majeurs sur la carte après vérification. Le répertoire central contient, au minimum, un jumelage entre l identifiant électronique et chacun des identifiants locaux des ministères et des organismes.

Authentification du client lors de l'utilisation	Le processus d'authentification est assumé entièrement par chaque ministère et organisme. Les liens entre l'identifiant électronique et les identifiants locaux sont sous le contrôle absolu de chaque organisation.	L'infrastructure commune gère le mécanisme d'authentification. De ce fait, les communications entre les citoyens et l'infrastructure commune sont prises en charge par celle-ci. Par la suite, l'infrastructure accomplit le relais avec l'organisme concerné. Lors d'une communication, si les identifiants d'une organisation en particulier ne sont pas présents sur la carte, ce scénario n'exclut pas la possibilité d'exiger du citoyen des identifiants ou des clés additionnelles.
Sécurité du dialogue transactionnel	La sécurité dans la transmission des données est entièrement assurée par chacun des organismes. Pour le citoyen, le niveau de sécurité peut varier en fonction des transactions ou des informations qu il échange et des exigences de chaque organisation avec laquelle il transige.	Toute la sécurité des communications est assumée par l'infrastructure commune (système de clés privé, publique, asymétrique). Pour le citoyen, le niveau de sécurité de ses transactions est identique, quel que soit le ministère ou l organisme fournisseur de services.
Services spécifiques	Chaque ministère ou organisme reste maître d'oeuvre de la configuration de ses interfaces et des scénarios transactionnels avec les citoyens (''design'' des panoramas, enchaînement des transactions, etc.). En d'autre mots, la situation actuelle demeure à l'effet que chaque organisme contrôle totalement les communications avec les citoyens. Aucune normalisation n'est à prévoir. Comme aujourd hui, le citoyen doit composer avec les	Les interfaces fournies aux citoyens sont normalisées et relèvent de l'infrastructure commune. De plus, les liens entre l'identifiant électronique et le dossier du citoyen sont assurés par l'infrastructure commune. Lorsqu un ministère ou un organisme est mis en contact pour réaliser une transaction électronique, il est assuré que la personne qui désire effectuer cette transaction est effectivement la bonne. L'infrastructure commune gère la totalité du dialogue et les systèmes locaux

	"formulaires" propres à chaque ministère et organisme.	deviennent comme des serveurs répondant à des commandes de l'infrastructure commune. Pour le citoyen, quel que soit le ministère ou l organisme avec lequel il fait affaires, le dialogue est normalisé et les "formulaires" à l écran ont un air de famille.
Services génériques	Chaque organisme contrôle ses propres transactions avec les citoyens. Aucune mise en commun n'est prévue. Comme aujourd hui le citoyen est appelé à répéter auprès de chaque ministère et organisme les informations qui sont nécessaires à ces administrations pour lui offrir un service.	Une transaction, comme un changement d'adresse, est centralisée. À la limite, les adresses qui sont contenues dans les banques de données des organisations sont déchargées le répertoire d informations communes. Un citoyen n a pas à répéter à chaque ministère ou organisme fournisseurs de services les mêmes informations.
Portefeuille de services	Ce scénario ne permet pas de vision globale de l ensemble des services accessibles par un citoyen avec sa carte. Comme c est le cas actuellement, le citoyen fait affaires avec des ministères et des organismes distincts, en mode "silo" ou "cheminée", qui lui dispensent des services indépendamment les uns des autres.	Le scénario d intégration permet d obtenir un portrait global des droits et privilèges décernés à un citoyen par son gouvernement. Le citoyen peut obtenir une vue d ensemble des dossiers que les organisations publiques détiennent à son endroit.

Navigation à travers les services offerts	Comme les transactions sont conçues en mode indépendant, il devient très difficile d'organiser une forme de navigation à travers les services offerts. Le citoyen continue de faire affaires avec des ministères et des organismes distincts.	La prise en charge de l'ensemble du scénario transactionnel par l'infrastructure commune permet d'offrir une véritable navigation parmi les services offerts par l'état. Le citoyen fait affaires avec le Gouvernement d abord et avant tout.
Les échanges d informations entre les ministères et les organismes	Les formules actuelles demeurent inchangées, et les échanges pour des fins administratives se font sous la supervision de la Commission d accès à l information. Le citoyen, comme aujourd hui, ne peut savoir que les informations qu il a transmises à un organisme sont retransmises à un autre. Toutefois, ces échanges ne peuvent se faire sans l autorisation de la Commission d accès à l information.	L'existence d'un répertoire d informations communes ouvre la porte à un nouveau mode d organisation des informations publiques relatives à l identification d un citoyen. Le répertoire faciliterait une utilisation ordonnée et sécuritaire de ces données en assurant qu'elles concernent la même personne, sans échanges ou croisement. Le citoyen est assuré que l information qu il transmet au gouvernement ne peut être altérée par des échanges. Il peut aussi obtenir le portrait de ses dossiers détenus dans les ministères et organismes.
Fonctions de paiement	Les fonctions de paiement électronique sont assurées localement, i.e. que chaque ministère et organisme développe et met à la disposition de sa clientèle les outils électroniques nécessaires pour percevoir les paiements qui lui sont acheminés. Le citoyen réalise ses transactions financières auprès de chaque ministère et organisme, suivant les modalités offertes par chacun d eux.	L'intégration inclut les modalités de paiement. L infrastructure centrale met à la disposition de l ensemble des ministères et des organismes les dispositifs nécessaires pour percevoir et acheminer les paiements. Un citoyen réalise ses transactions financières selon un mode uniforme et ses transactions sont automatiquement aiguillés vers le bon ministère ou organisme.

- On pourrait facilement développer toute une série de scénarios intermédiaires pour illustrer encore mieux comment une carte multiservices pourrait modifier et simplifier les façons pour un citoyen de transiger avec les ministères et organismes de son gouvernement.

  On pourrait aussi agencer de plusieurs autres manières les 12 éléments placés ici en opposition si on voulait évaluer dès maintenant toutes les alternatives et tous les scénarios qui décriraient comment le gouvernement pourrait organiser autrement son offre de services aux citoyens. Nous n avons voulu ici qu illustrer jusqu où pourrait aller cette réforme, à partir d un moyen technologique porteur comme la carte multiservices à microprocesseur. Nous avons aussi voulu montrer qu une telle technologie doit être vue de façon globale, pour l ensemble des ministères et organismes.

  Chacun des 12 éléments brièvement analysés soulève des questions auxquelles les membres du CRISP, ne prétendent pas apporter de réponses :

  1. Que devrait contenir une carte multiservices? sur la carte? dans la puce?
  2. Qui devrait émettre la carte? comment?
  3. Que devrait contenir le répertoire d informations communes? qui devrait le gérer?
  4. Devrait-on y inscrire les droits et les privilèges? Comment doit-on les attribuer et gérer?
  5. Jusqu où doit-on aller pour s assurer de l authentification du client lors de l'utilisation?
  6. Jusqu où doit-on assurer la sécurité du dialogue transactionnel ? qui ?
  7. Comment organiser l offre de services spécifiques?
  8. Quels services génériques devraient-on offrir?
  9. Doit-on offrir un portefeuille de services? jusqu où et comment?
  10. Doit-on offrir une navigation à travers les services offerts? jusqu à quel point?
  11. Quelles sont les informations publiques d identification qui sont communes aux ministères et organismes?
  12. Comment organiser les fonctions de paiement?

- Il faudra de toute évidence poursuivre les réflexions pour chacun des 12 éléments identifiés, de façon à mieux cerner les impacts organisationnels, économiques et législatifs soulevés par chacun d eux.

---

7. LES BÉNÉFICES

- Les bénéfices associés à la carte multiservices vont varier en fonction du scénario retenu et du niveau de sophistication des infrastructures qui seront

mises en place. Ces bénéfices se regroupent sous les deux thèmes classiquement accolés à tout bénéfice : la réduction des coûts et l amélioration du service.

Les caractéristiques intrinsèques de la carte multiservices et des infrastructures qui pourraient être mises en place permettent toutefois de regrouper autrement les bénéfices. On l a dit déjà, l usage d une carte multiservices permet à tout citoyen de transiger avec son gouvernement par l entremise de points de services électroniques pour avoir accès à des informations ou y obtenir des services personnels. L utilisation d une carte multiservices permet donc non seulement d offrir en toute sécurité des services "personnalisés" à la clientèle de l État, mais aussi de modifier les modes traditionnels d offres de services du gouvernement, permettant à la fois de simplifier et d améliorer les services et de diminuer les coûts.

7.1 Pour le citoyen

- Ainsi, un citoyen transigeant avec l État au moyen de sa carte multiservices obtiendrait, à un degré variable selon le scénario qui serait retenu :

- **un accès normalisé aux services offerts par les ministères et organismes** : un citoyen n aurait besoin de connaître qu'une seule et unique procédure d'utilisation pour être en mesure de réaliser l'ensemble de ses transactions électroniques personnelles avec l'État, et ce peu importe le moyen ou le canal utilisé;

- **un usage standardisé** peu importe le ministère ou l organisme avec lequel il transige : tous les échanges électroniques entre les citoyens et l'État pourraient être identiques. En d'autres mots, les interfaces sont tous standardisés y compris les transactions de paiement;

- **une transaction rejoignant plusieurs ministères ou organismes** : les transactions de même nature entre le citoyen et l'État pourraient être réduites au minimum. Le cas d'un changement d'adresse est exemplaire à cet égard;

- **une vision globale de ses droits et services**: le citoyen pourrait obtenir une vue synthèse des dossiers que les organismes publics détiennent à son endroit;

- **une meilleure garantie de sécurité des informations confiées à son gouvernement** : l'infrastructure à développer pourrait inclure des mécanismes ou des fonctionnalités pouvant sécuriser les informations publiques relatives à l identification d une personne détenues par plusieurs ministères et organismes tout en augmentant leur niveau de fiabilité.

- **une confiance accrue dans les services publics,** liée au décloisonnement des services, d une part, et rattachée au fait que le resserrement des contrôles entraînerait une meilleure garantie que les deniers publics servent à ceux qui y ont droit selon les lois en vigueur.

- D autres bénéfices sont plus généraux et déjà largement associés aux autoroutes de l information et aux points de services électroniques :

- **une meilleure facilité d accès aux services** : des services gouvernementaux disponibles 24 heures sur 24, 7 jours par semaine, partout sur le territoire y incluant directement de son domicile;

- **une réduction des délais** pour l obtention d un service.

- Enfin, le remplacement des multiples cartes de plastique (surtout dans le domaine de la santé) par une seule carte multiservices gouvernementale constitue pour le citoyen un bénéfice en soi.

7.2 Pour l État

- La mise à la disposition des ministères et organismes d une carte unique offre plusieurs avantages pour le gouvernement. Comme le souligne avec raison le SAI, pris un à un, rares sont les organismes qui peuvent justifier les coûts associés à la mise en place de moyens efficaces et sécuritaires pour réaliser des transactions sur les inforoutes.

  Mais les inforoutes et le moyen sécuritaire d y accéder avec une carte multiservices à microprocesseur autorise et justifie, comme le démontre le second scénario, un renouvellement complet de la façon dont le gouvernement a traditionnellement offert ses services à la population en amenant :

- **une mise en commun des infrastructures "informationnelles"**
  - répertoire d informations publiques relatives à l identification d une personne
  - "interfaces d'application"
  - points de services électroniques

- **un décloisonnement des services gouvernementaux**

- **une réduction des coûts au niveau de la manipulation papier**
  - création, duplication, remplacement, transport, conservation, etc.

- **une élimination des duplications/redondances**
  - transactions
  - contrôles
  - stockage de données
  - traitement des données

- **une qualité d'information accrue**
  - réduction des erreurs et des reprises de traitement
  - contribue à l'élimination d informations délibérément faussées

- **une diminution des recherches d'individu et des vérifications d'identité**
  - meilleure protection des renseignements personnels
  - information au bon endroit, au bon moment et en tout temps.

- réduction potentielle des abus de système

- **une réduction des coûts**
  - la réduction des coûts pour la prestation d un service donné
  - la réduction des coûts générée par la réduction des intervenants dans le dossier, donc réduction de l appareil gouvernemental
  - la réduction des coûts de production d un service permet de rencontrer les objectifs de compressions budgétaires et de diminution des effectifs

- **une amélioration du service**
  - réduction des délais dans la prestation d un service
  - avec une meilleure organisation des informations publiques d identification communes aux ministères et organismes, réduction des démarches répétitives d un citoyen

- **une réduction de la fraude**
  - plus grande assurance de la conformité du service avec les droits réels des citoyens réclamant le service

---

8. LES RECOMMANDATIONS

- Une infrastructure administrative et technologique doit être mise en place pour permettre l utilisation par le citoyen d une carte multiservices et pour soutenir l offre gouvernementale de services personnalisés disponibles par l entremise de points de services électroniques et des autoroutes de l information.

  Selon les choix qui seront fait, l infrastructure qui soutiendra la carte multiservices permettra de simplifier un peu, ou beaucoup, l offre de services gouvernementaux au citoyen. Ces choix offrent aussi au gouvernement l opportunité de modifier un peu, ou radicalement, la façon dont il organise son offre de services.

  Dans le contexte actuel où le gouvernement s interroge sur les enjeux des autoroutes de l information et sur la question des cartes d identité, où le renouvellement des services publics devient impérieux et les compressions budgétaires incontournables, au moment enfin où la carte d assurance-maladie se transforme en carte santé à microprocesseur, le CRISP recommande aux autorités gouvernementales

- d évaluer, au-delà de la carte, le potentiel de renouvellement de l offre de services gouvernementaux aux citoyens;

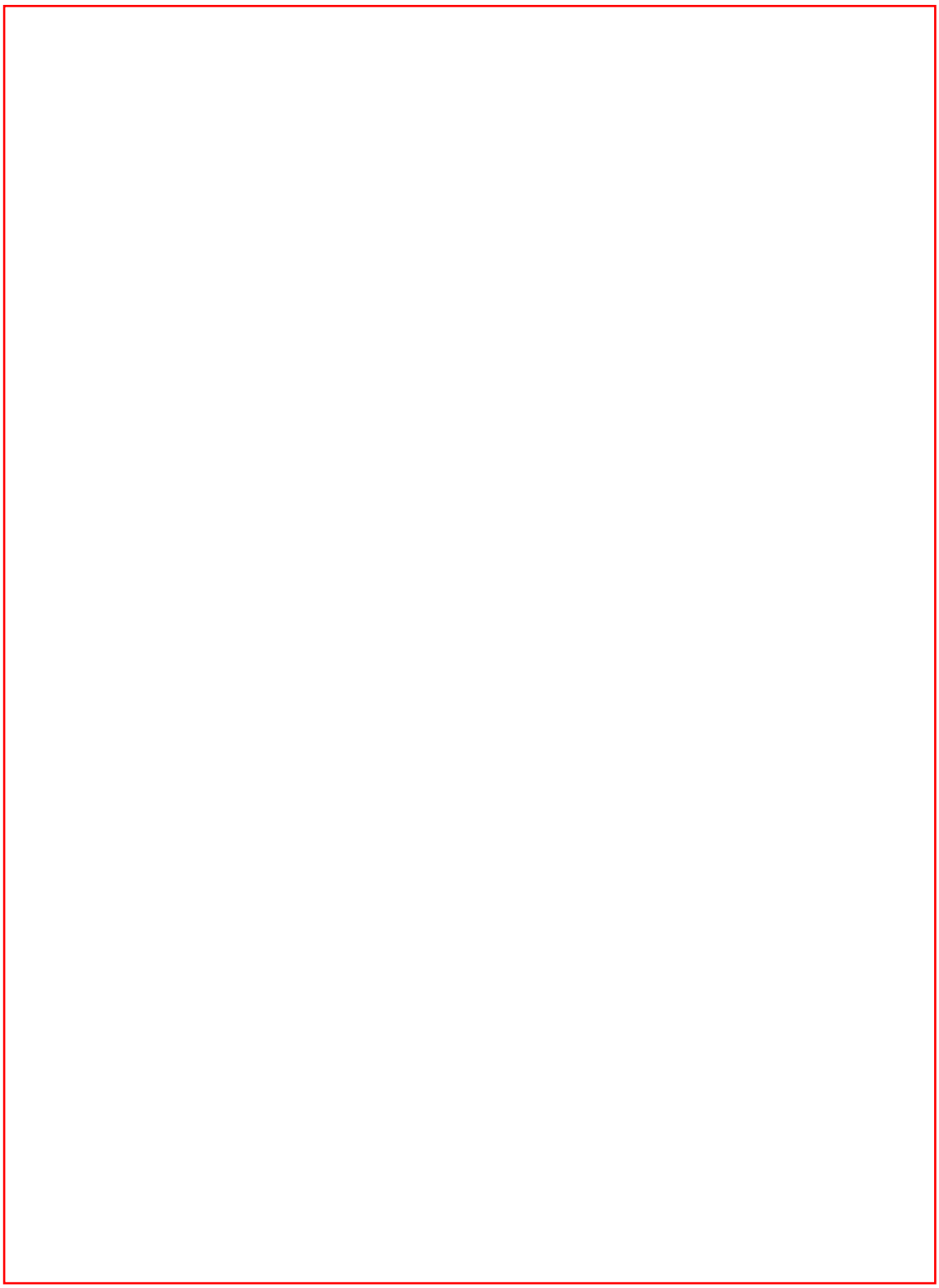
- d entreprendre dès maintenant les études visant à évaluer les alternatives et les impacts organisationnels, économiques et législatifs liés

  1. au contenu de la carte;
  2. à l émission de la carte;

3. au répertoire d informations communes;
4. à l attribution des droits d accès;
5. à l authentification du client lors de l'utilisation;
6. à la sécurité du dialogue;
7. aux services spécifiques;
8. aux services génériques;
9. au portefeuille de services;
10. à la navigation à travers les services offerts;
11. à l organisation des informations publiques d identification détenues par les ministères et les organismes;
12. aux modalités de paiement.

- de s assurer que les projets spécifiques qui s apprêtent à offrir des services sur les autoroutes de l information et par l entremise de points de services électroniques le sont dans un contexte d offre globale de services à un citoyen par son gouvernement.

Annexe 1



Annexe 2

BIBLIOGRAPHIE

Plusieurs documents ont été consultés et utilisés par les membres du groupe de travail dans leur travail de réflexion et de recherche. Cette liste n est pas exhaustive et énumère des documents voire des parties de documents qui ont souvent été utilisés dans leur version préliminaire et à l état de projet.

1. SIGNATURE NUMÉRIQUE ET SÉCURITÉ SUR INTERNET

Richard Parent
Service de la prospective
SCT
4 décembre 1995

2. LA SÉCURISATION DES TRANSACTIONS D AFFAIRES ET DES ENVIRONNEMENTS INFORMATIQUES ET DE TÉLÉCOMMUNICATIONS AU GOUVERNEMENT DU QUÉBEC
(document de travail)

Annexe B - Les particularités de l EDI touchant la sécurité

Yvan Lauzon
Service de la prospective
SCT
1996

3. POUR UNE MODERNISATION DU FONCTIONNEMENT DES AFFAIRES GRÂCE À UNE INFRASTRUCTURE DE CLÉS PUBLIQUES AU QUÉBEC (document de travail)

Richard Parent
Service de la prospective
SCT
30 septembre 1996

4. PROJET DE RÉPERTOIRE GOUVERNEMENTAL (document de travail)

René Lortie
Service de la prospective
SCT
30 septembre 1996

5. L EDI ET LA SIGNATURE ÉLECTRONIQUE

Ross Lamarre
Ministère du Revenu du Québec
in MOT DE PASSE
Bulletin de la sécurité informatique
Vol. 9, no 4 - décembre 1995

6. LA CRYPTOGRAPHIE À CLEF PUBLIQUE

Anonyme
2 pages + 4 pages d illustrations

7. L AVOCARTE

L expérience du Barreau de Paris
(Recueilli et transmis par Yvan Lauzon)

8 LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AU NOUVEAU-BRUNSWICK (document de travail)

Juillet 1996

9. POUR UNE CARTE D IDENTIFICATION ÉLECTRONIQUE UNIVERSELLE
(document de travail)

Ministère de la Culture et des Communications
Secrétariat à l autoroute de l information
Septembre 1996

10. RÉPERTOIRE GOUVERNEMENTAL (QUÉBEC)

Pages Vertes : un format pour les entrées référencées
Proposé par le Comité avis, expertise et représentation, Groupe des responsables de la gestion documentaires (GRGD)
Version préliminaire, 5 juin 1996

11. VOCABULAIRE GÉNÉRAL DE LA SÉCURITÉ INFORMATIQUE

Carole Verreault
Office de la langue française

12. LA TÉLÉMESSAGERIE

Gilbert Labonté et Pierre-P. Tremblay
Direction générale des télécommunications
Juillet 1996

13. POUR AMÉLIORER LES RELATIONS ENTRE L ÉTAT ET LES CITOYENS : UN RÉSEAU DE CENTRES DE SERVICES GOUVERNEMENTAUX (projet de mémoire)

Direction générale de l information
Communication-Québec
9 août 1996

14. DOCUMENT DE RÉFLEXION SUR LA QUESTION DES CARTES D IDENTITÉ AU QUÉBEC

Commission d accès à l information du Québec
Octobre 1996

15. L IMPLANTATION RÉUSSIE DES INFOROUTES DANS L ORGANISATION QUÉBÉCOISE : AVANT TOUTE CHOSE, UNE AFFAIRE DE CULTURE

Mémoire présenté par le CEFRIO et la CEVEIL à la Commission de la culture portant sur les enjeux du développement de l inforoute québécoise
9 octobre 1996

16. POCHETTE D INFORMATION UNISYS SUR LA CARTE À PUCES

29 NOVEMBRE 1996

17. GUIDE DE DIFFUSION DE L INFORMATION GOUVERNEMENTALE SUR INTERNET (Document de travail)

Direction de la diffusion sur les inforoutes

Ministère des Relations avec les citoyens et de l Immigration
19 décembre 1996

18. LA MONNAIE ÉLECTRONIQUE

L Informatique Professionnelle, no 149
Décembre 1996

19. L UTILISATION DE LA CARTE A MICROPROCESSEUR PAR LE GOUVERNEMENT DU QUÉBEC (document de travail)

Secrétariat de l autoroute de l information
Janvier 1997

20. MOYENS DE PAIEMENT ÉLECTRONIQUE

Programme de sensibilisation et d information sur l EDI et le Commerce électronique en milieu gouvernemental - Activité thématique 43 - Compte rendu des présentations
27 janvier 1997
