www.inforoute-gouvernementale.qc

Architecture gouvernementale de la sécurité de l'information numérique (AGSIN)

Architecture cible globale sommaire

L'inforoute gouvernement@le

Secrétariat du Conseil du trésor
Québec

Secrétariat du Conseil du trésor

ARCHITECTURE GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE (AGSIN)

ARCHITECTURE CIBLE GLOBALE

SOMMAIRE

version 1.0

BL3sommaire_sct_v1.0p2.7.doc

DIFFUSION RESTREINTE

Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles

Québec

Septembre 2001

Table des matières

1. INTRODUCTION

Les technologies de l'information affectent profondément les façons de faire de l'État et ont des impacts sur l'ensemble des secteurs d'activités du gouvernement. C'est actuellement le cas, en particulier, de l'Internet et de la prestation électronique de services (PES). Reconnaissant cette révolution technologique dans la façon dont l'État produira et dispensera désormais ses services aux individus (citoyens) et aux entreprises, le Secrétariat du Conseil du trésor (SCT) cherche à en tirer pleinement profit dans son plan d'action gouvernemental.

Dans ce but, le SCT a entrepris, en collaboration avec les ministères et organismes (M/O), un exercice d'architecture à haut niveau nommé architecture d'entreprise gouvernementale (AEG). En fonction des grands objectifs gouvernementaux, l'AEG vise à comprendre et illustrer ce que sera la nouvelle prestation de services et les impacts qu'elle aura sur les grands processus et les ressources informationnelles.

L'architecture d'entreprise gouvernementale comporte plusieurs volets et segments dont l'un est l'architecture gouvernementale de la sécurité de l'information numérique (AGSIN) qui vise, d'une part, à assurer la sécurité des renseignements personnels et la confiance des individus à l'égard de la protection de ces renseignements et de la vie privée et, d'autre part, à supporter la mise en place des grandes orientations gouvernementales.

Outre l'AGSIN, plusieurs initiatives ont été prises par la SCT afin d'appuyer les ministères et organismes dans la mise en œuvre de la sécurité de l'information numérique. Notamment, la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* a été adoptée en novembre 1999. Un groupe de travail a été formé sur la sécurité et ses travaux ont conduit à réviser cette directive et à mettre en place divers mécanismes de gouverne.

Le troisième bien livrable du projet d'élaboration de l'AGSIN, qui présente l'architecture cible globale, est résumé dans ce sommaire.

2. PERSPECTIVES CONTEXTUELLES

2.1 Tendances de l'industrie

La sécurisation des échanges d'informations numériques soulève une problématique, liée au développement du commerce électronique, qui est à considérer sous plusieurs dimensions : juridique, organisationnelle[1] et technologique.

En ce qui concerne la **dimension juridique**, la communauté internationale jette depuis plusieurs années les bases du cadre légal du commerce électronique et aborde les questions de sécurité. La loi type sur le commerce électronique, établie en 1996 par la Commission des Nations-Unies pour le droit commercial international (CNUDCI), a probablement été l'initiative la plus influente. La CNUDCI a aussi entrepris en 1997 des travaux sur la signature électronique.

[1] L'importance des aspects humains dans l'architecture cible de l'AGSIN a conduit à identifier également une "dimension humaine", séparée de la dimension organisationnelle.

Aux États-Unis, le Uniform electronic Transactions Act (UETA), qui date de 1999, devrait avoir été adopté par environ 35 états en 2001. Il élimine tout doute sur la valeur exécutoire des transactions électroniques. Le gouvernement américain a aussi adopté en 2000 une loi renforçant la validité des enregistrements et de la signature électroniques et travaille à deux autres projets visant à favoriser les affaires électroniques.

En Europe, outre les législations nationales, le parlement européen a adopté en 1999 la Directive sur un cadre commun pour les signatures électroniques.

Au Canada, le gouvernement fédéral a adopté en 1999 la Loi sur la protection des renseignements personnels et des documents électroniques (C-6). En parallèle, la Conférence pour l'harmonisation des lois au Canada propose un projet de loi uniforme sur le commerce électronique. Mais ce projet de loi uniforme semble supplanté par la loi C-6 et les nombreuses initiatives (lois ou projets de loi) déjà prises par les provinces et les territoires. La loi C-6 a son pendant dans les provinces comme loi sur la protection de l'information. Cependant, les organisations relèvent de la compétence provinciale et les transactions conclues à l'intérieur de la province sont soustraites à l'application de cette loi.

Bien que souvent négligées dans l'élaboration d'une architecture de sécurité, **les dimensions organisationnelle et humaine** sont essentielles pour mettre en place et gérer la sécurité. Un cadre de gestion de la sécurité permet aussi de mesurer l'efficacité des processus et des solutions technologiques. Les normes générales de sécurité prennent en compte cet aspect.

Selon la firme Gartner, un développement par étapes doit permettre de définir l'ensemble des éléments du cadre de gestion, où l'on retrouvera, par exemple, les politiques et les directives de sécurité, l'organisation et les processus, les mécanismes de suivi et de contrôle.

En ce qui concerne **la dimension technologique**, une architecture de sécurité englobe un certain nombre de composantes physiques et de solutions technologiques qui ont pour but d'assurer la sécurité des informations numériques et des échanges électroniques, ainsi que des équipements et infrastructures d'échange et de traitement de l'information numérique. Ces logiciels, équipements et moyens de communication permettent d'assurer des fonctionnalités qui sont regroupées en « fonctions » (ou services) de sécurité. Ces fonctions sont présentées plus en détails à la section 3.3 de ce sommaire.

Il faut aussi tenir compte des nouveaux besoins que fait apparaître le développement rapide de la technologie sans fil. Ainsi, les téléphones cellulaires seront de plus en plus utilisés pour la PES, ainsi que les assistants numériques personnels ou autres nouveaux appareils de ce type.

2.2 Tendances gouvernementales hors Québec

L'accès d'une proportion croissante de la population à l'Internet a amené un grand nombre de gouvernements à développer la prestation de leurs services par voie électronique aux individus et entreprises.

Des initiatives de prestation électronique de services (PES) se multiplient ainsi, particulièrement dans les pays industrialisés, dans des domaines comme l'enseignement à distance, la déclaration et le paiement des taxes, factures ou contraventions, la votation en ligne, le renouvellement des permis, les enregistrements ou les inscriptions, l'obtention de documents d'état-civil, etc.

Les gouvernements qui développent la PES dans plusieurs domaines sont amenés à structurer leurs moyens et leur organisation, et des travaux intenses sont en cours à travers le monde pour développer des

architectures gouvernementales de sécurité dans le cadre plus général d'une architecture d'entreprise gouvernementale.

2.3 Tendances au gouvernement du Québec

Diverses initiatives ont déjà été prises par le gouvernement relativement à la sécurité de l'information numérique. La politique québécoise de l'autoroute de l'information a été adoptée en 1998. La Directive sur la sécurité a été énoncée en 1993 et actualisée en 1999. Plusieurs projets sont en cours pour faciliter son application, dont celui sur la catégorisation de l'information numérique. En avril 1999, un groupe de travail sur la sécurité de l'information a déposé un rapport qui établissait les défis de la gestion de cette sécurité et proposait un cadre pour sa gestion.

Toute solution de sécurité doit respecter les sources de droit en vigueur : la législation générale en vigueur aux niveaux provincial et fédéral, la législation sectorielle, les lois cadres (comme la Loi sur les archives) et, enfin, les exigences contractuelles et conventionnelles. Des ajustements importants à ces différentes sources pourraient être nécessaires afin d'accommoder la sécurité de l'information numérique et des échanges électroniques. La loi concernant le cadre juridique des technologies de l'information, adoptée en juin 2001, a pour objet principal d'assurer la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et la reconnaissance de leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers.

Les différentes composantes physiques et solutions technologiques de sécurité peuvent être regroupées en mécanismes pour assurer la protection, la détection et la correction, ainsi que pour assurer le respect des critères de DICAI de la directive sur la sécurité. Un certain nombre de ces mécanismes sont utilisés dans les chantiers centraux du gouvernement : l'ICPG, le Répertoire gouvernemental, la carte santé, SERTIR, GIRES et le serveur de paiement.

Les chantiers centraux du gouvernement

Autorisée par le Conseil du trésor en juin 1999 et en cours d'implantation, **l'infrastructure à clés publiques gouvernementale (ICPG)** permettra à des individus (ou des processus), par l'usage de certificats et de la cryptographie, de se reconnaître à distance, d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information numérique sensible.

Pour l'implantation progressive (sur 5 ans) de l'ICPG, un certain nombre de travaux ont été menés ou vont l'être. Par contre, le projet de politique québécoise de cryptographie et d'identification électronique (PCIE), qui émane également de la politique sur l'autoroute de l'information, est suspendu au MCC, de même que les cadres organisationnels et techniques au SCT.

La loi concernant le cadre juridique des technologies de l'information contient des dispositions pour baliser la prestation de services de certification. Le modèle fonctionnel de l'ICPG adopté par le CT propose un découpage des responsabilités, dont certaines ont déjà été confiées à un organisme central pour la gestion des clés et des certificats. Un cadre de gestion de l'ICPG devra être clairement défini.

Le **répertoire gouvernemental**, accessible par Internet, a pour but de permettre aux individus et aux entreprises d'avoir accès à la description des services offerts, aux références de documents gouvernementaux et aux coordonnées des employés de l'État. La conception détaillée du répertoire a été publiée en 1997. Les travaux relatifs au répertoire s'exécutent actuellement selon une approche expérimentale, mais sans stratégie d'ensemble.

Compte tenu de la nature des informations que renferme le répertoire, il doit lui-même être hautement protégé. Cette sécurité est d'autant plus nécessaire qu'on y retrouve des informations essentielles à la gestion de la sécurité de l'information numérique, comme les certificats de chiffrement (passeports et visas électroniques) des employés de l'état.

Comme pour l'ICPG, la loi concernant le cadre juridique des technologies de l'information contient des dispositions touchant plus particulièrement le répertoire. D'autres lois pourraient également s'y appliquer selon la nature des informations emmagasinées. Encore assez imprécise, les modalités de gestion du répertoire devront être reprises.

Un projet est mené depuis 1998 sous la coordination de la RAMQ sur un nouveau système de **carte santé** à microprocesseur dans le cadre de la programmation régionale des services ambulatoires (PRSA). Son but est de démontrer le potentiel de la carte à puce dans le domaine de la santé. Étant donné que l'usage de la carte santé n'est pas encore défini clairement, il n'est pas possible d'exprimer les besoins précis en matière de sécurité à son sujet.

Le **Service transactionnel d'information et de repérage (SERTIR)** est un serveur Web mis à la disposition des M/O par les services gouvernementaux (DGSIG) pour l'offre de services transactionnels et de commerce électronique. Présenté aux M/O en 1999, le SERTIR continue à être développé.

Du point de vue technologique, les besoins relatifs à la continuité 24/7 du fonctionnement sont généralement comblés par la DGSIG, mais des besoins demeurent quant à la sécurité entourant le SERTIR, relativement à la disponibilité des applications, à l'identification/authentification et l'habilitation/contrôle d'accès, au chiffrement des informations numériques et à la prévention des intrusions. Le cadre de gestion de la sécurité est encore peu développé et le partage des responsabilités entre la DGSIG et les M/O est à préciser.

Pour son projet de **gestion intégrée des ressources (GIRES)**, qui vise notamment le remplacement de systèmes de gestion du personnel et de système de gestion budgétaire et comptable, le gouvernement a choisi en 1999 le progiciel d'Oracle. Puisque GIRES servira à gérer centralement (à la DGSIG) les informations relatives aux ressources gouvernementales, un très haut niveau d'attention et de protection doit lui être accordé, d'autant plus que GIRES alimentera potentiellement le répertoire gouvernemental.

L'organisation de la gestion de la sécurité demandera de prendre de nombreuses mesures dans le projet GIRES, notamment pour la définition des rôles et responsabilités, l'élaboration des politiques, directives et procédures de sécurité, le cadre de gestion de l'exploitation, la sécurité physique des équipements. Du point de vue technologique, GIRES devra être protégé contre les intrusions : chiffrement des échanges entre les postes de travail et les serveurs, authentification forte (à l'étude), robustesse des infrastructures pour garantir la disponibilité.

Comme **serveur de paiement**, plusieurs M/O utilisent le service *P@iement en ligne* offert par le MFQ et exploité par la Banque nationale du Canada. Les divers besoins immédiats et futurs relatifs à la sécurisation des transactions et de paiements semblent avoir été pris en compte par le MFQ et la BNC.

Situation des ministères et organismes

Les informations sur la situation dans les M/O proviennent d'ateliers tenus en février et mars 2001 avec 16 M/O et aux cueillettes effectuées en février 2001 auprès de 12 M/O représentatifs.

Une grande majorité des M/O rencontrés indique que les lois et règlements applicables ne semblent pas adaptés à la PES ou aux échanges. La loi concernant le cadre juridique des technologies de l'information facilitera la reconnaissance légale des documents sur support informatique.

Les M/O rencontrés se sont engagés dans la prestation électronique de services à leur clientèle, la plupart étant au début du processus. Par contre, tous ces M/O effectuent des échanges d'informations numériques avec un ou plusieurs d'entre eux. La majorité des M/O consultés connaissent relativement bien leurs vulnérabilités et la plupart d'entre eux ont élaboré des politiques, normes ou procédures en matière de sécurité mais pour la moitié d'entre eux, le cadre de gestion de la sécurité n'est pas adapté à la PES.

Les principales vulnérabilités organisationnelles constatées proviennent de l'absence de catégorisation de l'information numérique, d'un plan global de sécurité, de mécanismes de contrôle et de suivi, d'un processus d'habilitation, de formation, de plans de relève.

Presque tous les M/O consultés se sont occupés de concevoir une architecture de sécurité et la moitié travaille à l'élaboration ou à l'adaptation de leur architecture de sécurité. Ces architectures sont beaucoup orientées vers la dimension technologique de la sécurité.

Cependant, certaines vulnérabilités ont tout de même été constatées au niveau technologique. Celles-ci proviennent de l'absence de chiffrement du trafic, d'outils d'analyse des vulnérabilités, ainsi que de l'absence d'outils ou de services de détection des intrusions, de journalisation, de surveillance (outre la détection des virus) ou de garantie de haute disponibilité.

Infrastructures centrales

Ossature de l'inforoute gouvernementale, le Réseau intégré de communications informatiques et bureautiques (RICIB) est géré par les services gouvernementaux (DGT). Un appel d'offres a été lancé par le Conseil du trésor en janvier 2001 pour réaliser un réseau de plus grande capacité, le réseau de télécommunication multimédia (RETEM). Le **RICIB** et le **RETEM** doivent permettre de garantir la sécurisation des infrastructures technologiques, applications et informations numériques qui transitent sur le réseau. Un certain nombre d'améliorations y apparaissent souhaitables : par exemple, dans sa dimension organisationnelle, à l'égard des rôles et responsabilités du personnel chargé de la sécurité, des politiques et directives sur la sécurité, ou des guides et procédures de sécurité ; et dans sa dimension technologique, à l'égard des coupe-feu, du système d'exploitation sécurisé, de la détection des intrusions, ou encore de la détection des virus.

À titre de **serveur informatique gouvernemental**, la Direction générale des services informatiques gouvernementaux (DGSIG) fournit aux M/O des services informatiques sur diverses plates-formes. Elle est responsable de la sécurisation initiale des environnements des M/O qu'elle dessert. Chaque M/O utilisateur est responsable de la sécurité de ses applications et de la gestion des identifiants et profils des utilisateurs, mais il n'existe pas de guide pour les assister dans cette tâche.

La réglementation encadrant les activités de la DGSIG n'est pas adaptée à un contexte de PES protégée. Des ajustements seront nécessaires, par exemple à l'égard des responsabilités des employés d'intervenants externes à qui des M/O ont confié l'hébergement de données. Les contrats entre la DGSIG et les M/O devront être révisés. De plus, la DGSIG devra probablement adapter son cadre de gestion pour assurer la protection des informations numériques dans le cadre des PES, ou encore pour couvrir l'offre par la DGSIG des outils et services communs partagés ou réutilisables.

2.4 Rappel des exigences architecturales et des principes en matière de sécurité de l'information

L'AEG a élaboré des stratégies d'affaires et des exigences architecturales dont certaines concernent la sécurité de l'information numérique. Ces exigences, plus quelques autres qui peuvent y être ajoutées, peuvent être classées selon les trois grands axes d'intervention de la Loi sur l'administration publique : la qualité de la prestation des services aux individus ; la performance de l'administration publique ; le développement de la société québécoise.

Les principes en matière de sécurité de l'information sont ceux énoncés dans la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale auxquels se sont ajoutés des principes complémentaires élaborés dans le cadre du projet AGSIN.

Les ministères et organismes doivent gérer les risques et les impacts à l'égard des principes de « DICAI » de la directive sur la sécurité : la disponibilité de l'information à une personne autorisée, l'intégrité de l'information, la confidentialité de l'information, l'authentification des personnes, l'irrévocabilité. Il est essentiel que ces critères soient respectés dans chacune des étapes du cycle de vie de l'information.

De plus, la gestion de la sécurité doit respecter des principes de vision commune, de cohérence, de responsabilité et d'imputabilité, d'évolution et d'universalité.

Les principes de la Directive, de même que les principes complémentaires, ont des implications pour tous les M/O mais en particulier pour certains d'entre eux : le Conseil du trésor et son secrétariat, le MJQ, le MRCI, les Archives nationales du Québec, le Contrôleur des finances, la Sûreté du Québec.

3. MODÈLE GÉNÉRAL DE L'ARCHITECTURE GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE (AGSIN)

3.1 Cadre global de référence

Se doter d'un cadre global de référence permet de manière simple et efficace de visualiser les éléments dominants à considérer dans la sécurité de l'information numérique. De plus, ceci permet la mise en contexte des différents éléments du concept d'espace sécurisé introduit dans la première version de l'architecture d'entreprise gouvernementale.

Ainsi le cadre global de référence met en perspective :

- les clientèles visées;
- les dimensions (juridique, humaine, organisationnel et technologique) de la sécurité;
- les fonctions de sécurité, supportées par un ensemble de mécanismes de sécurité et de solutions technologiques;
- le cycle de vie de l'information;
- les besoins d'affaires;
- la valeur de l'information.

3.2 Les dimensions de la sécurité

Dimension juridique

Les préoccupations de sécurité de l'information numérique sont trop facilement centrées sur la recherche de solutions techniques alors que de nombreux éléments organisationnels et juridiques sont tout aussi importants.

Un certain nombre de lois du Québec imposent des actions ou des règles qui concernent la sécurité de l'information et tout particulièrement les suivantes :

- Loi sur l'administration publique ;
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ;
- Loi sur les archives ;
- Loi concernant le cadre juridique des technologies de l'information.

De plus, outre leur importance générale, les chartes canadienne et québécoise sur les droits et libertés sont à considérer particulièrement puisqu'elles rappellent le droit au respect de la vie privée.

Enfin, les contrats, ententes et conventions sont des sources de droits et d'obligations : il faut notamment vérifier les liens contractuels, les clauses relatives à la sécurité et à la protection de la vie privée, analyser les clauses de non-responsabilité.

Dimension humaine

La sécurité de l'information numérique soulève des questions suffisamment importantes relativement aux personnes pour traiter de la dimension humaine séparément de la dimension organisationnelle.

L'organisation de la sécurité informatique exige la structuration et la définition de politiques de sécurité à l'égard du personnel qui devront traiter, notamment, de l'enquête de sécurité, l'habilitation sécuritaire du personnel, la sensibilisation à la sécurité et la formation.

Dans cette dimension humaine on classera également les questions d'éthique, de pratique professionnelle et d'imputabilité. Tout le personnel de l'organisation, de la haute direction à l'utilisateur final, a des obligations relatives à la sécurité afin que la solution de sécurité soit appliquée efficacement et atteigne les objectifs de son implantation.

Dimension organisationnelle

La sécurité administrative varie d'une organisation à l'autre, mais on portera une attention particulière aux politiques, normes, standards et directives de sécurité, aux rôles et responsabilités du personnel chargé de la sécurité, à la catégorisation de l'information, à l'évaluation de la vulnérabilité, aux registres et dossiers de sécurité et à la gestion du consentement.

La sécurité physique et du milieu vise principalement la sécurité du lieu physique (bâtiment, structure, support portable), du lieu géographique (catastrophes naturelles, cambriolage) et des dispositifs auxiliaires (chauffage, électricité, climatisation).

La sécurité matérielle porte sur un ensemble de mécanismes de protection, de détection et de réponse pour contrôler l'accès aux biens et aux informations sensibles ainsi que sur les modalités de la sécurité du matériel (inventaire, entretien, contrôle de qualité, etc.).

La sécurité des opérations vise la constance des opérations, le contrôle des accès aux systèmes et aux logiciels, la surveillance des actions sur les systèmes, les infrastructures et les installations, et la gestion des supports (utilisation, disposition, envoi, transport, etc.).

Dimension technologique

En premier lieu, les solutions technologiques doivent supporter les fonctions et composantes de la sécurité qui font l'objet de la section 3.3 qui suit. Mais il y a aussi d'autres éléments technologiques auxquels on tend à porter moins d'attention, comme le développement des applications ou la sélection et mise en œuvre des applications et des équipements.

Dans le développement des applications, les préoccupations de sécurité se retrouveront dès la conception et lors du choix des outils et langages de programmation. Les revues de code et les essais tiendront compte de la sécurité. L'environnement de développement sera sécurisé et l'utilisation de modules externes sera surveillée.

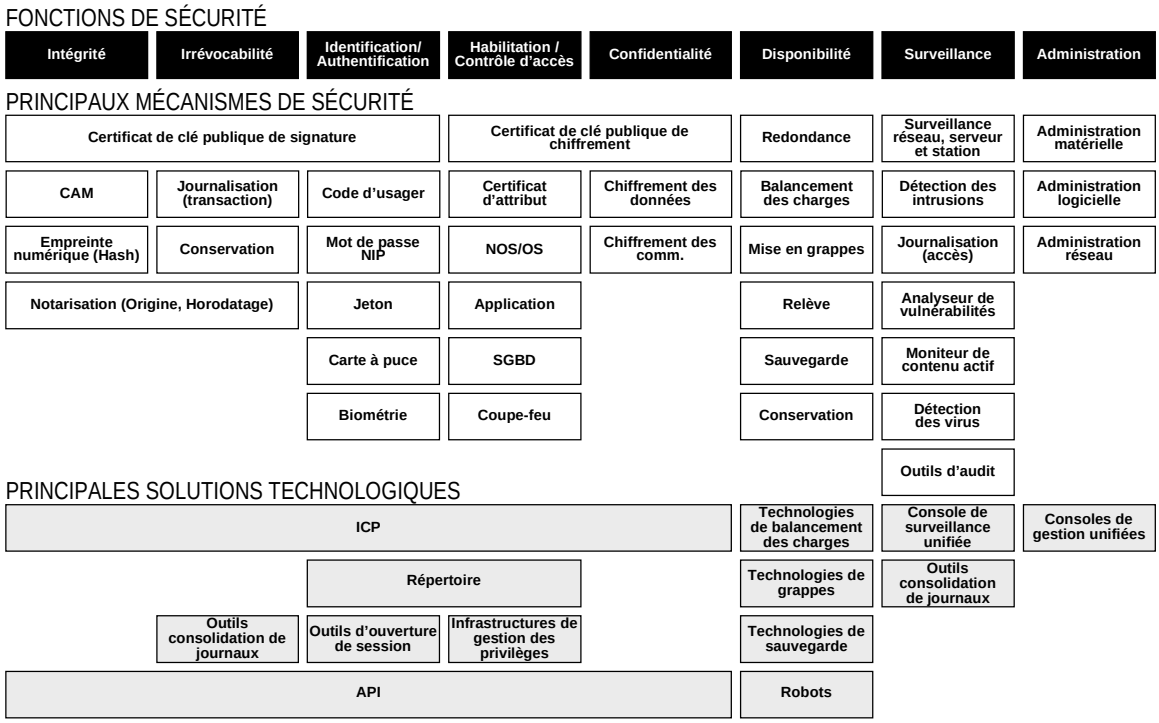
Lors de la sélection des applications et équipements, on s'assurera qu'ils sont sécuritaires par la réalisation d'une analyse des produits, par leur évaluation à l'aide de critères standards d'évaluation de la sécurité, par leur essai dans un contexte reproduisant le contexte d'utilisation réelle.

Les préoccupations de sécurité seront aussi présentes lors de l'installation et de la configuration des applications et équipements, de la mise à jour des systèmes d'exploitation et des applications, de la configuration des postes de travail.

3.3 Les fonctions et composantes de la sécurité

On identifie 8 fonctions de sécurité de l'information numérique, qui s'appuient chacune sur des mécanismes de sécurité et des solutions technologiques. La figure ci-dessous présente ces éléments :

FONCTIONS DE SÉCURITÉ



La fonction d'intégrité est responsable d'assurer qu'une information n'a pas été modifiée ou détruite sans autorisation de façon volontaire ou accidentelle.

La fonction d'irrévocabilité assure qu'une action ou qu'un document est indéniable et clairement attribué à l'entité qui l'a généré. A la différence des autres fonctions, cette fonction vise la protection mutuelle des entités impliquées dans un échange ou une transaction et non la protection contre une tierce partie.

La fonction d'identification / authentification sert d'une part, à identifier une entité (personne ou autre) i.e. répondre à la question « Qui est cette entité? » et, d'autre part, à l'authentifier auprès du système pour qu'il accorde un accès : « Cette entité est-elle celle qu'elle dit être? ».

La fonction d'habilitation / contrôle d'accès définit une liste de ressources et de données auxquelles une entité peut avoir accès une fois qu'elle a été dûment authentifiée, et contrôle à qui le droit d'accès est accordé et pour poser quels gestes.

La fonction de confidentialité assure qu'une information n'est pas divulguée ou mise à la disposition d'une entité ou d'un traitement non autorisé.

La fonction de disponibilité assure que les informations numériques et les systèmes sont accessibles en temps voulu et de la manière requise par une entité autorisée.

La fonction de surveillance met en évidence les vulnérabilités, offre des pistes de vérification et permet la protection contre les tentatives d'intrusion et les programme malicieux.

La fonction d'administration permet l'administration sécuritaire des logiciels, ainsi que des équipements informatiques et de réseautique. Elle inclut autant les processus (réalisation du schéma de configuration, inventaire, tenue des dossiers, etc.) que des outils.

Il existe des liens de dépendance entre ces fonctions. Par exemple, toutes les fonctions sont dépendantes de l'administration et de la surveillance qui sont elles-mêmes intimement liées. La fonction d'habilitation/contrôle d'accès est dépendante de la fonction d'identification/authentification, etc. Ces dépendances démontrent bien que l'on ne peut envisager d'utiliser seuls les différents fonctions et mécanismes de sécurité.

3.4 La valeur des attributs de l'information numérique au gouvernement du Québec

Dans le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité», le SCT explique la démarche pour réaliser cette catégorisation et établir des mesures de sécurité à mettre en place selon le contexte d'utilisation. Les informations sont évaluées pour chacun des attributs DICAI et chaque attribut reçoit une valeur (élevée, moyenne ou basse).

Pour chacun des cinq attributs de DICAI, ainsi que pour les fonctions d'habilitation/contrôle d'accès, la surveillance et l'administration, des mécanismes et solutions technologiques différents pourront être utilisés selon l'évaluation qui aura été ainsi faite : la valeur « élevée » d'un attribut demandera la mise en œuvre de moyens plus forts pour assurer la sécurité voulue.

Les moyens à mettre en œuvre pour assurer la sécurité d'une information varieront également en fonction du contexte d'utilisation et au long de son cycle de vie, depuis sa définition jusqu'à sa destruction.

3.5 Le modèle général de l'AGSIN

Prestation électronique de services (PES) et échanges électroniques protégés

L'AGSIN étant un segment de l'architecture d'entreprise gouvernementale (AEG), le modèle général de l'AGSIN se doit de respecter le modèle général de prestation électronique de services (PES), élaboré dans la première version de l'AEG.

L'AGSIN ayant une portée plus large que celle retenue dans la première version de l'AEG, le modèle général de la PES a dû être adapté afin d'inclure les services aux autres clientèles (partenaires, mandataires, fournisseurs, autres gouvernements, etc.), les services aux employé(e)s, les interactions entre les M/O, les accès sécuritaires (plutôt qu'uniquement les moyens d'identification) et les différents modes d'accès. Ceci conduit à un nouveau modèle, le modèle général des échanges électroniques.

Le lien entre la vision d'affaires de l'AEG et la vision de la sécurité de l'information numérique de l'AGSIN s'établit grâce au concept des domaines de confiance. Un domaine de confiance inhérent à la sécurité se définit comme un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité et un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité en matière de sécurité.

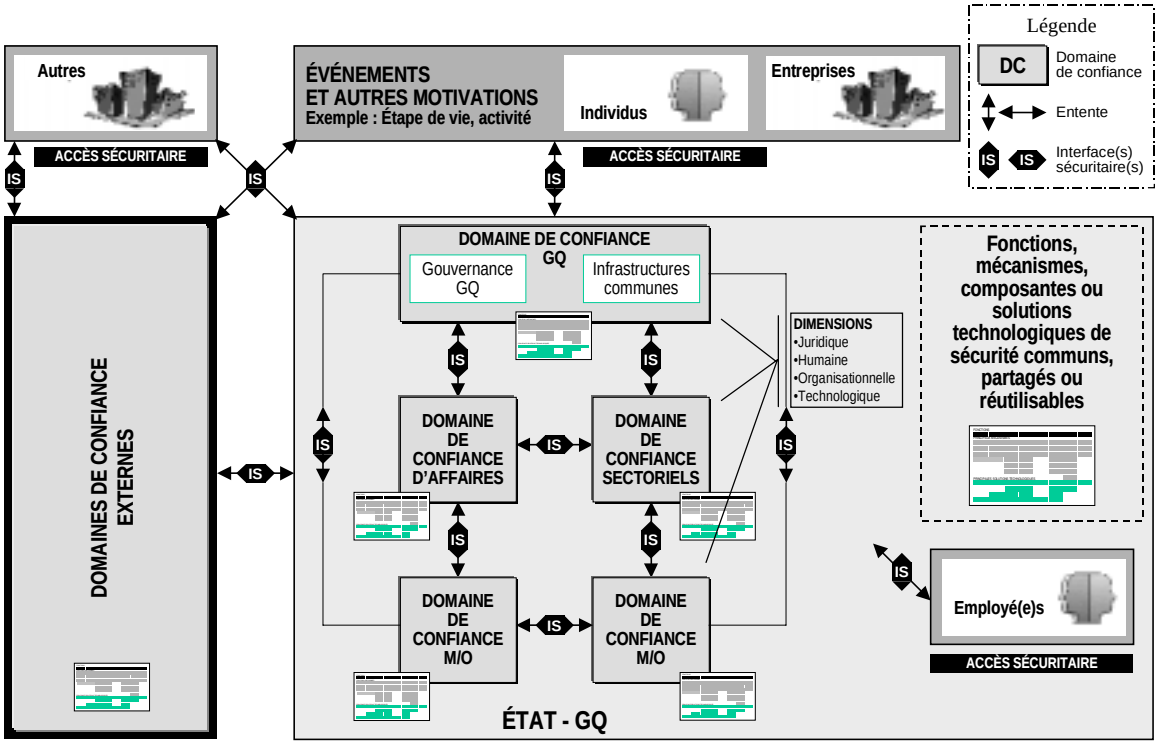
Le modèle général des échanges électroniques protégés au gouvernement du Québec propose cinq types de domaines de confiance : les domaines de confiance des M/O (ex. : MTQ, CSST, etc.), les domaines de confiance d'affaires (ex. : MIC pour la trousse de démarrage d'entreprise), les domaines de confiance sectoriels (ex. : secteur de la santé), les domaines de confiance du gouvernement du Québec (ex.: Infrastructure commune au niveau des services gouvernementaux (SG), gouvernance au niveau du SCT, etc) et, enfin, les domaines de confiances externes (ex. : Association canadienne de paiement (CPA), Gouvernement du Canada).

Le modèle de l'architecture gouvernementale de sécurité (AGSIN)

Le modèle général de l'AGSIN fait ressortir les interactions entre les domaines de confiance et les clientèles visées. Il repose notamment sur des orientations et principes en matière de sécurité de l'information numérique, sur le portrait et les besoins gouvernementaux en matière de sécurité de l'information numérique et sur les normes portant sur les fonctions de sécurité pour les systèmes ouverts.

MODÈLE GÉNÉRAL DE L'AGSIN

VUE – AFFAIRES



L'AGSIN présente les fonctions de sécurité, les mécanismes de sécurité et les composantes ou solutions technologiques nécessaires pour assurer un niveau adéquat de sécurité de l'information numérique tout au

long de son cycle de vie. Ce sont ces mêmes fonctions de sécurité qui, au besoin, sont à la base des accès sécuritaires entre le gouvernement du Québec et les différentes clientèles.

L'AGSIN ne présuppose pas l'utilisation de produits particuliers en matière de sécurité mais propose des solutions conformes aux normes et ayant fait leurs preuves sur le marché.

Les organisations doivent planifier en fonction de l'hétérogénéité et être sélectives dans l'application des architectures technologiques. Les standards doivent être mis à jour régulièrement et l'architecture doit permettre une variété de standards afin d'accommoder différents contextes. L'AGSIN doit ainsi faire partie d'un processus continu et évolutif. Son succès repose moins sur le contenu que sur son actualisation.

Dans le modèle, chaque domaine de confiance définit sa propre politique de sécurité et élabore un cadre de gestion correspondant en s'assurant de couvrir l'ensemble des dimensions de la sécurité. Dans le domaine de confiance, les informations numériques doivent être protégées au niveau adéquat par des fonctions de sécurité dont les mécanismes de sécurité dépendront de la valeur des informations à protéger et des risques qu'elles encourent. Lorsque les informations numériques transitent dans un domaine de confiance ayant des mesures de sécurité de niveau inférieur, des mesures spéciales doivent être mises en œuvre pour conserver le niveau voulu de sécurité.

Une entente définit les règles qui régissent les interactions entre les domaines de confiance ainsi qu'avec les clientèles. Elle permet également de délimiter les champs de compétence entre les domaines de confiance. Une entente contient au minimum une Interface sécuritaire.

Une interface sécuritaire définit les modalités techniques de sécurisation de l'information numérique. Elle est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et standards et les fonctions et mécanismes de sécurité nécessaires pour assurer la connectivité et l'interopérabilité entre les domaines de confiance ainsi qu'avec les clientèles.

Les ententes et interfaces sécuritaires feront l'objet d'un contenu type à l'intention des organisations.

4. LES VUES SPÉCIFIQUES DE L'AGSIN

Ces vues permettent de présenter, selon les différents volets de l'AEG, les concepts du modèle général de l'AGSIN et d'identifier le potentiel de mise en commun, de partage et de réutilisation[2] des ressources en matière de sécurité. Les quatre volets présentés dans cette section sont les suivants :

- Volet affaires;
- Volet information;
- Volet application;
- Volet infrastructure technologique.

Ce découpage en volets respecte le cadre méthodologique en vigueur au sein du Secrétariat du Conseil du trésor et utilisé pour l'élaboration de l'architecture d'entreprise gouvernementale à haut niveau. En tant que segment de l'AEG, l'AGSIN se conforme à cette démarche.

[2] L'environnement commun comprendra les composantes qui seront communes pour l'ensemble de la communauté gouvernementale. L'environnement partagé entre plusieurs M/O réunira les composantes propres à une grappe de services. Les composantes réutilisables pourront être celles développées par un M/O et pouvant être réutilisées par d'autres M/O.

4.1 Volet affaires

La vue affaires du modèle général de l'AGSIN correspond en tout point au modèle général de l'AGSIN présenté à la section 3.5 de ce sommaire. Pour ce volet, le plan de mise en œuvre devra traiter notamment de la gouvernance (application, évolution et communication de l'AGSIN), et de la reconnaissance des domaines de confiance (guides d'élaboration d'une politique de sécurité, du cadre de gestion de la sécurité, d'une entente, d'une interface sécuritaire).

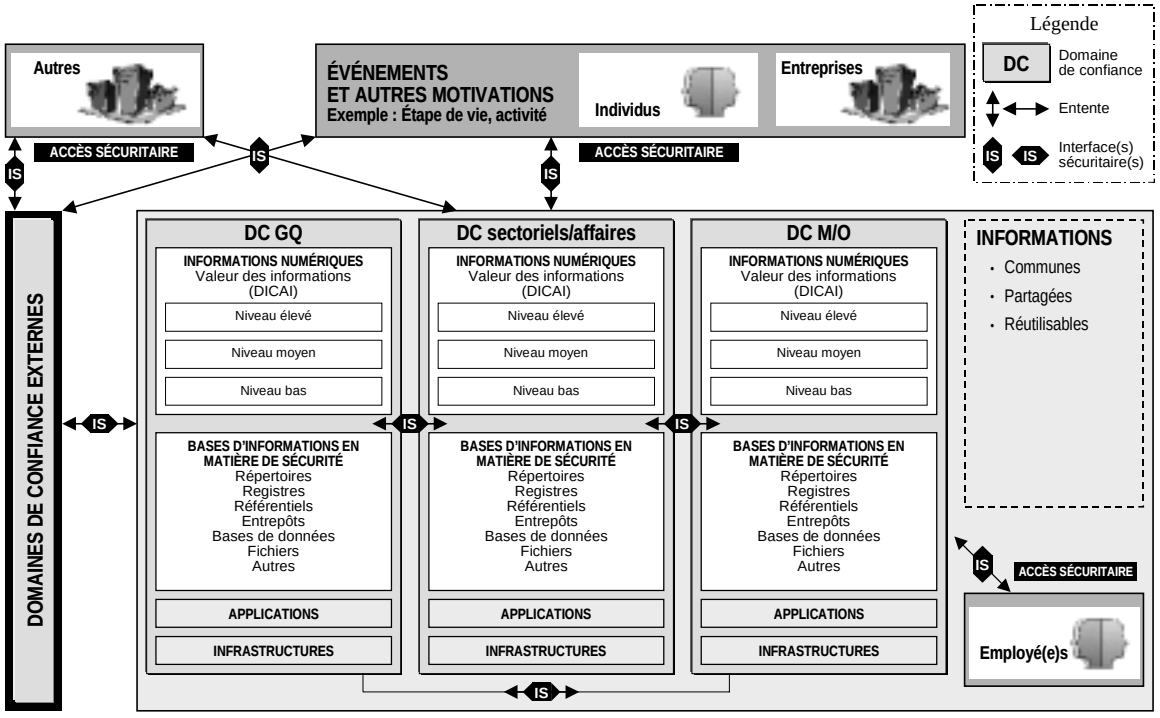
On peut identifier plusieurs éléments d'affaires en matière de sécurité qui ont un potentiel de mise en commun, de partage ou de réutilisation. Ces potentiels devront être validés. À titre d'exemple :

- **Mise en commun** : Ententes et interfaces sécuritaires, Processus d'identification, d'authentification, de signature.
- **Partage** : Ententes et interfaces sécuritaires des secteurs de la santé, de l'Éducation et municipal, Ententes et interfaces sécuritaires élaborées par les organismes responsables d'une grappe de services, Processus propres à un secteur ou à une grappe. .
- **Réutilisation** : Ententes et interfaces sécuritaires des M/O, Processus propres à un M/O.

4.2 Volet information

MODÈLE GÉNÉRAL DE L'AGSIN

VUE – INFORMATION



Afin d'assurer un niveau adéquat de sécurité en fonction de la valeur de l'information numérique, une base d'informations en matière de sécurité est nécessaire pour la gestion des mécanismes de sécurité et des solutions technologiques supportant les fonctions de sécurité. Ces informations en matière de sécurité possèdent une valeur élevée et nécessitent donc elles-mêmes des mécanismes de sécurité et des solutions technologiques assurant un niveau élevé de sécurité.

La base d'informations en matière de sécurité est principalement constituée des informations relatives à la gestion des informations numériques, des applications relatives à la sécurité et des infrastructures technologiques nécessaires à la sécurité. Elle peut donner lieu à la création de schémas, de tableaux, de fichiers, de données, de règles, etc. qui doivent être emmagasinés et échangés de manière sécuritaire. Parmi ce type d'informations, notons les certificats de clés publiques de chiffrement, les informations d'identification/authentification des entités, les profils d'habilitation/contrôle d'accès, les règles de surveillance, les règles de définition des virus, les règles de définition des accès des coupe-feux, les métadonnées en matière de sécurité, etc.

La base d'informations en matière de sécurité d'un domaine de confiance peut faire appel à des informations en matière de sécurité d'un ou de plusieurs autres domaines de confiance. Il faut donc accorder une attention particulière à la protection des échanges d'informations en matière de sécurité entre les domaines de confiance de façon à ne pas affaiblir le niveau de protection prévu. À cet effet, des ententes et des interfaces sécuritaires particulières relatives à l'échange d'informations entre les bases d'information en matière de sécurité sont nécessaires.

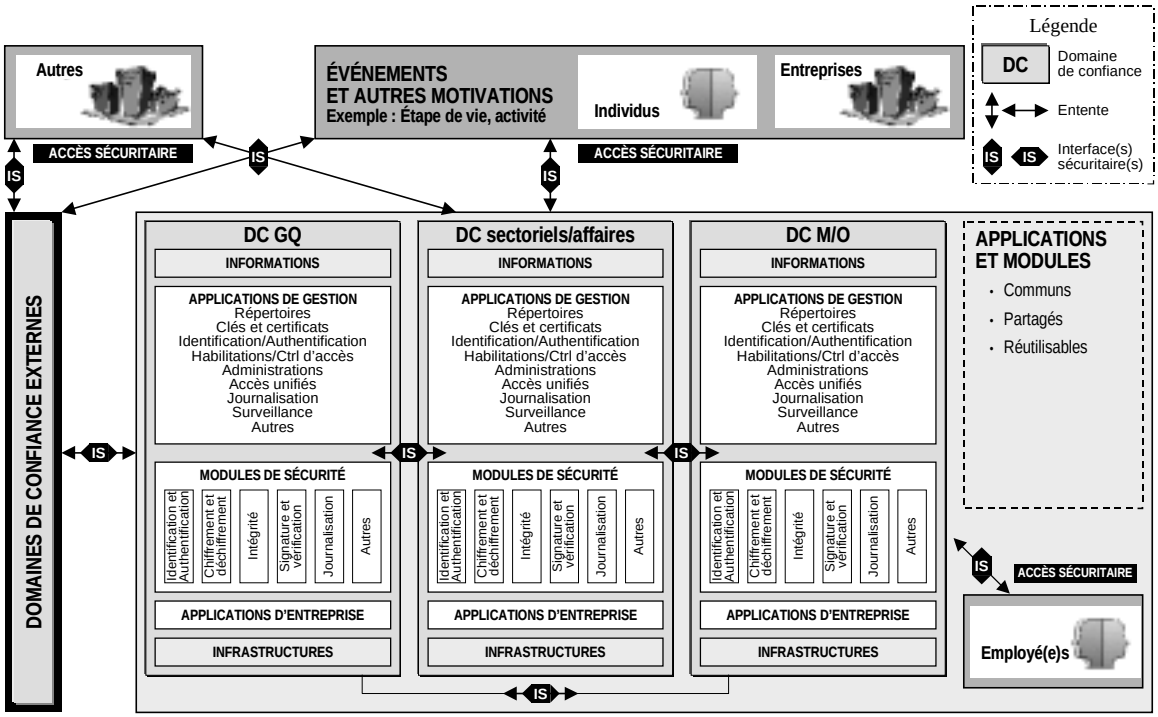
On peut identifier plusieurs éléments d'informations en matière de sécurité qui ont un potentiel de mise en commun, de partage ou de réutilisation. Ces potentiels devront être validés. À titre d'exemple :

- **Mise en commun** : Répertoire(s) gouvernemental(aux) des informations relatives aux employés et aux partenaires/mandataires et certificats de clés publiques de chiffrement associés, base de données de GIRES des informations relatives aux employés et aux partenaires/mandataires, base de données et fichiers des règles de sécurité du RICIB et du RETEM.
- **Partage** : Registre-référentiel des schémas XML de sécurité normalisés, Base de données et fichiers des règles de sécurité des secteurs de la santé, de l'Éducation et municipal, Registres-référentiels particuliers XML des secteurs ou grappes, Bases de données des règles de sécurité des secteurs ou grappes.
- **Réutilisation** : Registres-référentiels particuliers XML des M/O, Bases de données des règles de sécurité des M/O, Formulaires électroniques vierges.

4.3 Volet applications

MODÈLE GÉNÉRAL DE L'AGSIN

VUE – APPLICATION



La base d'informations en matière de sécurité requiert une gestion adaptée à la valeur des informations qu'elle contient. À cet effet, chaque domaine de confiance doit mettre en place des applications relatives à la gestion de la sécurité. La base d'informations en matière de sécurité étant répartie, les domaines de confiances doivent sélectionner et/ou développer des produits facilitant une gestion centralisée de ces informations.

Les applications relatives à la gestion de la sécurité traitent donc de la gestion des mécanismes de sécurité et des solutions technologiques assurant les fonctions de sécurité. Ces applications doivent être conformes aux normes, autant si elles sont acquises que si elles sont développées sur mesure. Dans l'éventualité où elles sont acquises, elles devront avoir fait leurs preuves dans l'industrie et être certifiées par des organismes reconnus, si pertinent.

Parmi ces applications, on retrouvera notamment celles assurant la gestion des répertoires, des clés et des certificats, de l'identification/authentification, de l'habilitation/contrôle d'accès, de l'administration (des logiciels et du matériel), des accès (unifiés), de la journalisation, de la surveillance, etc.

Les modules de sécurité visent à intégrer les fonctions de sécurité aux applications d'entreprise. Ils portent principalement sur l'identification/authentification, le chiffrement et le déchiffrement, l'intégrité, la signature et la vérification et la journalisation.

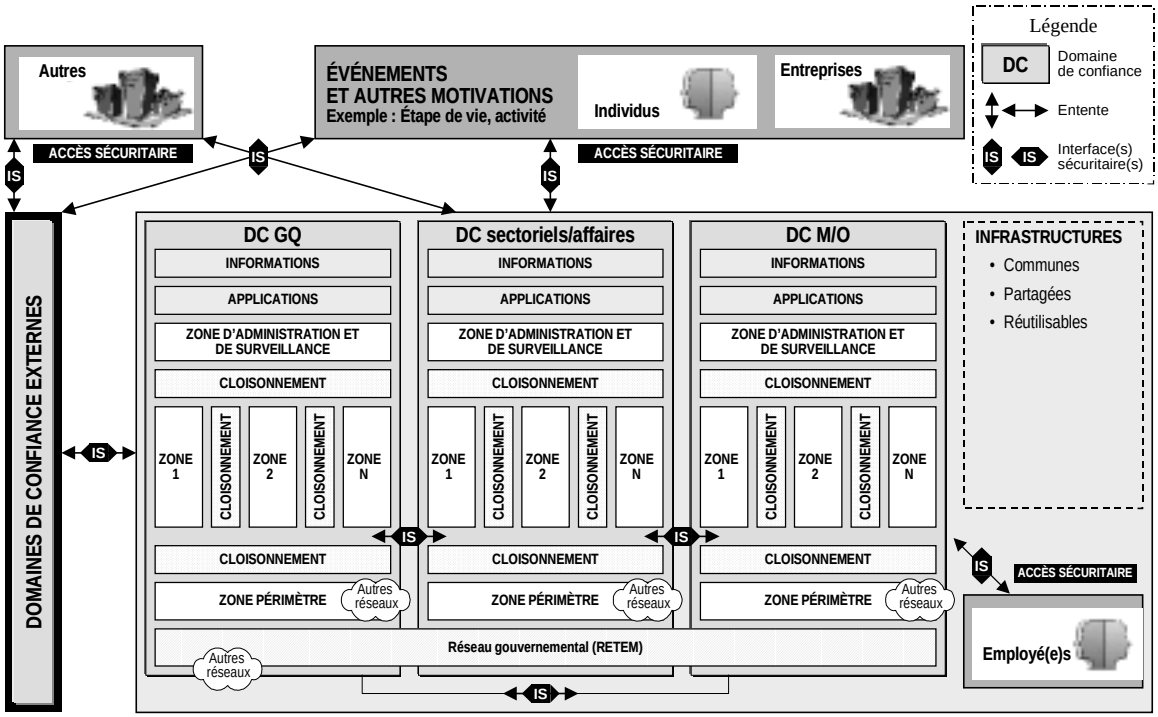
On peut identifier plusieurs applications (et modules) qui ont un potentiel de mise en commun, de partage ou de réutilisation. À titre d'exemple :

- **Mise en commun** : Applications relatives à la gestion de la sécurité et les modules de sécurité (gestion du répertoire gouvernemental, gestion des clés et des certificats ICPG, gestion de l'administration, de la journalisation et de la surveillance du RICIB et du RETEM, gestion de l'administration des applications gouvernementales et des serveurs gouvernementaux, module(s) d'identification et d'authentification, module(s) de chiffrement et déchiffrement, etc.)
- **Partage** : Applications relatives à la gestion de la sécurité et les modules de sécurité dans les secteurs de la santé, de l'Éducation et municipal (gestion de l'administration, de la journalisation et de la surveillance des réseaux sectoriels, module(s) d'identification et d'authentification, module(s) de chiffrement et déchiffrement, etc.), Applications et modules de sécurité propres à une grappe.
- **Réutilisation** : Modules de sécurité propres à un M/O (journalisation , vérification d'intégrité, etc.).

4.4 Volet infrastructure technologique

MODÈLE GÉNÉRAL DE L'AGSIN

VUE – INFRASTRUCTURE TECHNOLOGIQUE



Cette figure du volet Infrastructure technologique de l'AGSIN introduit les concepts de cloisonnements et de zones.

Le concept de cloisonnement de l'AGSIN permet le découpage en zones de manière à gérer adéquatement les accès à celles-ci. Les équipements assurant le cloisonnement permettent une connexité sécuritaire entre les zones, entre les domaines de confiance et avec les clientèles en acceptant seulement les connexions autorisées. Les coupe-feu et/ou les routeurs sont généralement utilisés pour protéger les zones.

Le découpage en zones facilite la protection des informations numériques au niveau approprié. Chaque zone contient un ensemble d'équipements informatiques de réseautique et de logiciels regroupés en fonction de certaines considérations telles que le type d'équipements et de logiciels, le type d'informations emmagasinées, le type de services offerts et le type d'accès autorisés.

Les interfaces sécuritaires du modèle général utilisent les services fournis par les équipements et logiciels des zones et des cloisonnements afin d'offrir les fonctions de sécurité qu'elles requièrent.

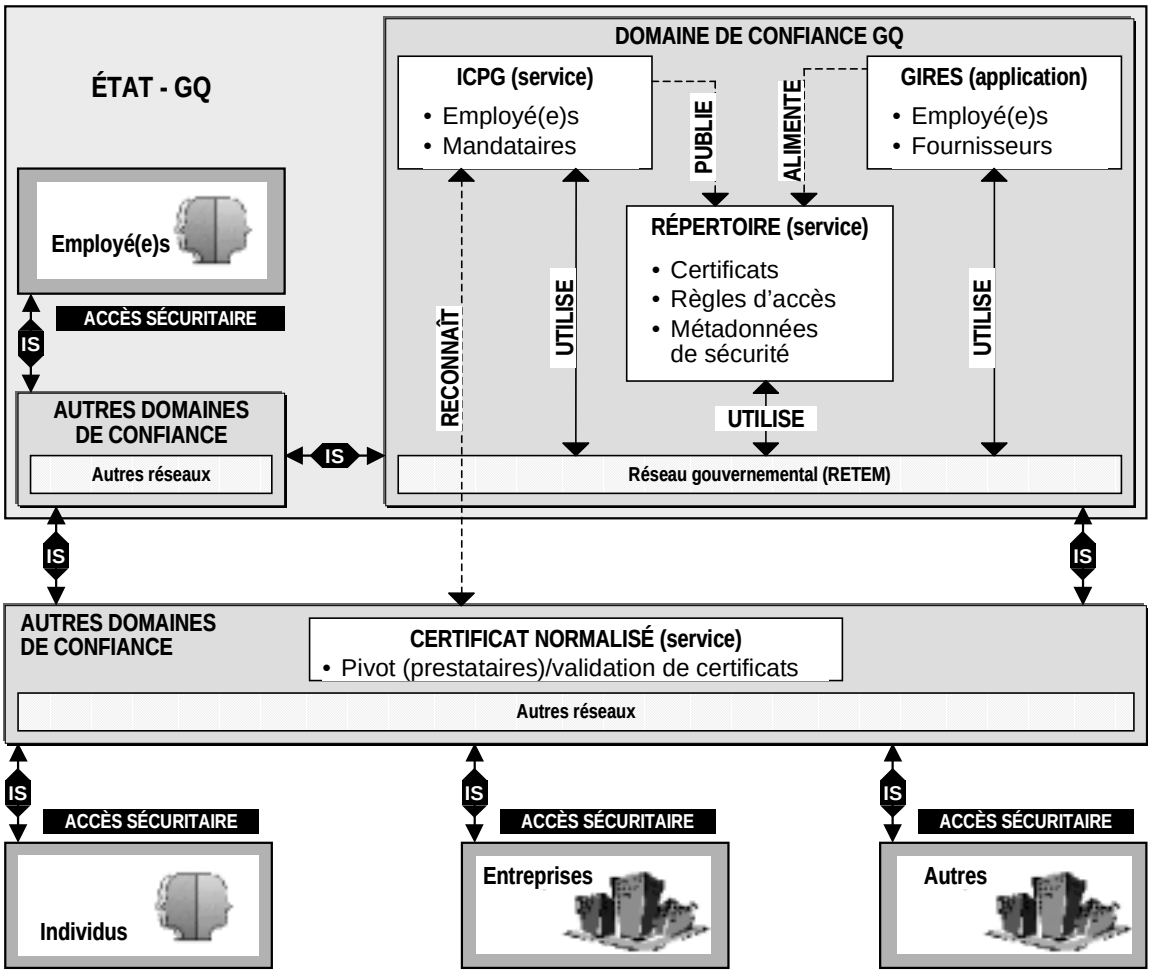
Les réseaux de transport permettent l'échange des informations numériques et des informations de la base d'information en matière de sécurité. En portant une attention particulière aux réseaux de transport, en particulier au RICIB et au RETEM, on permettra de ne pas affaiblir la sécurité des domaines de confiance.

On peut identifier plusieurs éléments d'infrastructure technologique qui ont un potentiel de mise en commun ou de partage. À titre d'exemple :

- **Mise en commun** : Solutions technologiques supportant les mécanismes de sécurité (serveur(s) du répertoire gouvernemental, serveur(s) de gestion des clés et des certificats, serveur(s) de détecteurs d'intrusions réseau et de virus du RICIB et du RETEM, serveur(s) coupe-feu du RICIB et du RETEM, serveur(s) de détecteurs des virus, serveur(s) coupe-feu de l'intranet gouvernemental, serveur(s) de contrôle d'accès (unifiés), détecteur(s) d'intrusions serveur, etc.
- **Partage** : Serveur(s) du registre-référentiel de schémas XML de sécurité normalisés, infrastructures technologiques en matière de sécurité des secteurs de la santé, de l'Éducation et municipal (serveur(s) de détecteurs des intrusions réseau et de virus des réseaux sectoriels, analyseur(s) de vulnérabilité des réseaux sectoriels, serveur(s) coupe-feu des réseaux sectoriels, etc.), Infrastructures technologiques en matière de sécurité propres à une grappe.

5. POSITIONNEMENT DES PROJETS SPÉCIFIQUES

La figure suivante illustre la vision gouvernementale cible des relations anticipées entre l'ICPG, le répertoire gouvernemental, GIRES et le réseau gouvernemental RETEM par rapport à l'architecture gouvernementale de la sécurité de l'information numérique.



VISION GOUVERNEMENTALE CIBLE
Relations ICPG – Répertoire – GIRES – RETEM
Aspect sécurité

5.1 ICPG

Élaborée à l'intérieur de la Politique québécoise de l'autoroute de l'information, l'infrastructure à clés publiques gouvernementale (ICPG) a vu son institution autorisée par le Conseil du trésor le 29 juin 1999. Des orientations fondamentales ont alors été adoptées pour assurer la cohérence et l'optimisation des ressources lors de son implantation. Un modèle fonctionnel adapté au fonctionnement gouvernemental a été choisi.

L'usage de l'ICPG sera conséquent au résultat des travaux relatifs à la catégorisation de l'information numérique de manière à sécuriser cette information en fonction de la valeur établie.

Principalement, l'ICPG répond à plusieurs des fonctions de sécurité et implique l'utilisation des mécanismes correspondants. De plus, en termes d'arrimage avec l'AGSIN, il faudra tenir compte des travaux inhérents aux certificats normalisés en cours d'élaboration. Bien que la figure précédente puisse laisser croire que le pivot sera à l'extérieur du gouvernement, sa localisation (interne, externe ou en partenariat) reste à déterminer.

Lorsque applicable (c'est-à-dire selon la valeur de l'information numérique à protéger), l'ICPG est la seule solution de sécurité retenue par le SCT garantissant l'authentification forte et l'irrévocabilité.

5.2 Le répertoire gouvernemental

Le répertoire gouvernemental repose sur une organisation de l'information qui en permet la désignation unique, la gestion, le partage et la réutilisation. Il est conçu pour offrir des services de consultation (coordonnées des employés des M/O, structures et activités des M/O, fournisseurs du gouvernement) et de soutien aux applications (comme la messagerie, la sécurité, …).

Étant donné son rôle central, le répertoire gouvernemental doit être hautement protégé.

Selon la conception détaillée qui en est faite, le répertoire est conforme aux principes de l'AGSIN. Il est réaliste d'utiliser le répertoire gouvernemental comme élément essentiel à la sécurité pour assurer les fonctions d'identification/authentification et d'habilitation/contrôle d'accès. Ceci doit cependant entraîner divers travaux d'architecture et de gouvernance.

5.3 La solution GIRES

Dans le contexte actuel, la solution GIRES a pris en compte ou considéré dans la liste des travaux à réaliser tous les éléments visant à assurer la sécurité de l'information numérique et des échanges électroniques conformément à l'AGSIN.

Selon ses orientations actuelles, la solution GIRES n'a pas besoin, a priori, d'une infrastructure à clé publique. Toutefois, d'après les orientations gouvernementales, il est probable qu'une ICP soit nécessaire dans un mode de fonctionnement sans papier.

Si la solution GIRES doit devenir le principal fournisseur du répertoire gouvernemental afin de supporter les fonctions de sécurité reliés à l'identification/authentification et à l'habilitation/contrôle d'accès des employés, il faudra revoir la position (centralisée ou non) des pratiques ainsi que le partage des responsabilités à l'égard de la sécurité, de l'efficience, de l'efficacité et de la qualité du service.

5.4 Le RICIB et le RETEM

Épine dorsale des échanges électroniques au gouvernement du Québec, le RICIB (et son remplaçant le RETEM) doivent être hautement protégés. La DGT, qui le gère, offre divers mécanismes et éléments de sécurité, mais des ajouts ou améliorations seront nécessaires à l'égard de la technologie (ex. : système d'exploitation sécurisé, coupe-feu de nouvelle génération, outils de surveillance réseau, accès à distance chiffré, etc.) et de l'organisation (politiques, normes et directives de sécurité, guides et procédures, plan

d'urgence et de relève, contrôle de l'accès physique, …) pour garantir que les attributs de sécurité atteignent le niveau élevé qui est nécessaire.

6. ZONES ET OBJETS DE NORMALISATION

Des zones et objets de normalisation potentiels ainsi que des normes ouvertes, de facto ou émergentes pertinentes aux différents volets du modèle général de l'AGSIN sont identifiés afin de fournir un guide et un cadre de référence aux intervenants en matière de sécurité au gouvernement du Québec. Il faut noter toutefois qu'un effort de la part des M/O pour l'adoption de cette normalisation sera nécessaire afin d'assurer la nécessaire cohérence gouvernementale et se protéger contre les risques associés aux normes non reconnues.

Ces champs de normalisation potentiels (seuls les normes et standards dominants les plus pertinents sont identifiés) peuvent correspondre à des documents, des règles, des critères, des mécanismes de sécurité, des solutions technologiques ou des processus.

7. PRINCIPAUX IMPACTS RELATIFS À LA MISE EN ŒUVRE DE L'AGSIN

L'AGSIN propose une nouvelle vision de la sécurité de l'information numérique au sein de l'appareil gouvernemental québécois. De ce fait, elle engendre des nouveaux paradigmes en matière de sécurité qui découlent principalement des nouvelles possibilités d'affaires et des nouveaux canaux de distribution que sont les réseaux ouverts.

Il est essentiel que le gouvernement du Québec intègre l'AGSIN dans son modèle de gouvernance de la sécurité et dans le cadre de gestion des TI et de la PES sans lesquels elle ne peut tenir la route. Une très grande importance devra être apportée au cadre de gouvernance afin que les architectes qui utiliseront l'AGSIN dans le processus d'élaboration d'une architecture de sécurité numérique spécifique puissent connaître leur contexte de travail.