ANNEXE 15 - ORIENTATIONS (BESOINS) DE SÉCURITÉ

1. INTRODUCTION

Conformément à la démarche proposée dans l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN), le SIIJ doit définir la portée de son autorité en matière de sécurité, de même que celle des différentes organisations impliquées dans sa prestation de service. Ce document ramène le concept de domaine de confiance de l'AGSIN et présente ceux qui seront directement impliqués dans le SIIJ.

Pour être en mesure de déterminer les solutions de sécurité qui seront appliquées au SIIJ, des orientations sont énoncées pour chacune des fonctions de sécurité de l'AGSIN. Ces orientations devront être considérées dans la sélection, la réalisation et la mise en place de chacun des systèmes de l'environnement du SIIJ.

AVIS.
Toute mention de produits (Microsoft, Suite .NET ou de ses composantes ou de tout autre produit), n'est indiquée qu'à titre d'exemple, d'hypothèse de travail ou à des fins d'évaluation de coût, seulement. La mention d'un produit ne peut ni doit être interprétée comme constituant un choix privilégié par le SIIJ.

2. DOMAINE DE CONFIANCE

Un domaine de confiance se définit comme étant un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique. Un cadre de gestion de la sécurité est un ensemble d'activités pertinentes à la sécurité. Ces activités sont assujetties à une politique de sécurité administrée par une seule autorité en matière de sécurité. Ce concept est appuyé par des ententes de sécurité et des interfaces sécuritaires dans le but d'installer la confiance dans les échanges électroniques. Ces différents éléments relatifs à un domaine de confiance sont présentés plus en détails à la section 2.1.

2.1 Les domaines de confiance du SIIJ

Le SIIJ implique principalement six domaines de confiance :

1. ***Le domaine de confiance du noyau*** **:** ce domaine de confiance regroupe tous les systèmes du noyau d'échange et d'intégration ainsi que les systèmes qui doivent

soutenir les opérations. De plus, ce domaine de confiance, pourrait être « impartiteur » de certains systèmes sous l'autorité d'autres domaines de confiance, tels que le ministère de la Sécurité publique du Québec (MSP) et le ministère de la Justice du Québec (MJQ).

2. ***Le domaine de confiance du ministère de la Sécurité publique du Québec (MSP)***[122] **:** ce domaine de confiance a autorité sur les systèmes ayant pour mission de gérer les dossiers des services correctionnels du Québec (SCQ) et ceux de la Commission québécoise des libérations conditionnelles (CQLC).

   Les systèmes ayant pour mission de gérer les dossiers de poursuites criminelles des services de police sont particuliers, car ils relèvent, en matière d'autorité, de chacun des corps de police qui y entreposent de l'information. Il s'avère que le morcellement de ces systèmes serait peu efficient et complexe à mettre en œuvre. Le domaine de confiance du MSP semble donc être le candidat le plus évident pour chapeauter ces systèmes.

3. ***Le domaine de confiance du ministère de la Justice du Québec*** **:** ce domaine de confiance regroupe les applications ayant les missions suivantes :

   - gérer les dossiers et les activités de la Cour d'appel;
   - gérer les dossiers des substituts du procureur général (SPG);
   - gérer les dossiers et les activités des tribunaux;
   - gérer les infractions et la perception des amendes;
   - gérer les données financières.

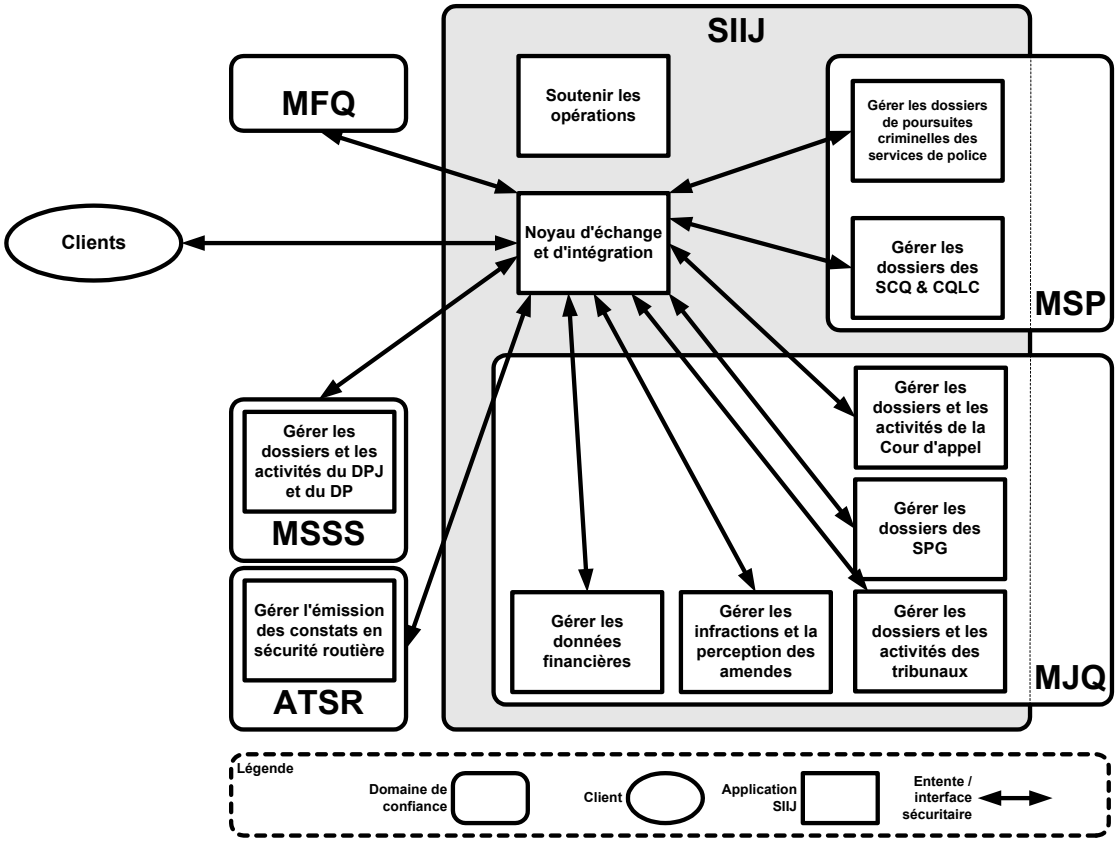
4. ***Le domaine de confiance de l'ATSR*** **:** ce domaine de confiance a autorité sur les systèmes ayant pour mission de gérer l'émission des constats en sécurité routière (l'ATSR).

5. ***Le domaine de confiance du ministère de la Santé et des Services sociaux*** **:** ce domaine de confiance a autorité sur les systèmes ayant pour mission de gérer les dossiers et les activités du Directeur de la protection de la jeunesse (DPJ) et du Directeur de la protection (DP).

6. ***Le domaine de confiance du serveur de paiement (MFQ)*** : ce domaine de confiance possède autorité sur le serveur de paiement gouvernemental. Ce système, hébergé par le ministère des Finances, permet de gérer l'encaissement des paiements pour les transactions gouvernementales réalisées à partir d'Internet, des réseaux privés et de l'inforoute gouvernementale.

[122] Le regroupement de tous les corps policiers québécois à l'intérieur du domaine de confiance du MSP est une hypothèse de travail qui devra être confirmée.

La figure suivante montre la portée de l'autorité de chacune des organisations impliquées dans le SIIJ, de même que les ententes devant être élaborées pour assurer la sécurité dans le cadre du SIIJ.



Il est à noter, dans la figure précédente, que certains systèmes se retrouvent dans plus d'un domaine de confiance. Cette représentation montre qu'un système peut appartenir à un domaine de confiance tout en étant imparti ou hébergé par le domaine de confiance du noyau. Dans ce cas, le domaine de confiance qui détient l'autorité sur le système à la responsabilité d'assurer la sécurité des informations numériques de ce système. Le domaine du SIIJ, quant à lui, à la responsabilité d'assurer la sécurité de l'environnement physique du système, notamment la sécurité des locaux, l'alimentation électrique, la maintenance des infrastructures et équipements (serveur, aiguilleurs, câblage, etc.). Des ententes devront être conclues pour déterminer les responsabilités de chacun des domaines de confiance impliqués tant au niveau de la mise en œuvre, de l'évolution que de l'exploitation.

Il est nécessaire de mentionner, de plus, que les domaines de confiance du MSP et du MJQ dépassent les limites du domaine de confiance du noyau. Ceci s'explique par le fait que certains systèmes de ces deux entités ne sont pas concernés par le projet SIIJ et ne peuvent donc être inclus dans le domaine de confiance du noyau. Les systèmes de

gestion des ressources financières, matérielles et humaines des deux entités sont des exemples de ce type de systèmes.

2.2 Éléments relatifs à un domaine de confiance

Cette section présente les différents éléments composant un domaine de confiance (autorité en matière de sécurité, cadre de gestion de la sécurité et politique de sécurité), de même que les éléments qui permettent de régir les échanges entre les différents domaines de confiances touchés par le SIIJ (entente de sécurité, interface sécuritaire).

2.2.1 Autorité en matière de sécurité

Une autorité en matière de sécurité est l'entité responsable de l'élaboration, de l'implantation et de l'application de la politique de sécurité et du cadre de gestion de la sécurité.

De façon spécifique pour le domaine de confiance du noyau, une autorité en matière de sécurité devra être identifiée ou définie[123] pour assurer la sécurité de celui-ci. De plus, pour les domaines de confiance afférents à celui du SIIJ, l'autorité en matière de sécurité devra être clairement identifiée et connue.

2.2.2 Cadre de gestion de la sécurité

Le cadre de gestion de la sécurité documente tous les éléments de la gestion de la sécurité. Il couvre les actifs devant être protégés, la démarche du domaine de confiance en matière de gestion des risques, les objectifs et les mesures de contrôle ainsi que le niveau d'assurance requis.

Le domaine de confiance du noyau devra se doter d'un cadre de gestion pour assurer la sécurité des systèmes qu'il détient et dont il a l'autorité, ainsi que ceux dont il est l'impartiteur.

2.2.3 Politique de sécurité

Une politique de sécurité exprime, en termes généraux, les exigences en matière de sécurité d'un domaine de confiance. Elle définit notamment ce qui est permis, ce qui est prohibé, la façon dont une activité peut être réalisée, etc.

Le domaine de confiance du noyau devra se doter d'une politique de sécurité pour assurer la sécurité des systèmes qu'il détient et dont il a l'autorité, ainsi que ceux dont il est l'impartiteur.

[123] À confirmer selon le modèle de gouvernance qui sera retenu.

2.2.4 Entente de sécurité

Une entente de sécurité vise à définir 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.

Le domaine de confiance du noyau devra ratifier des ententes avec les différents domaines de confiance impliqués dans le SIIJ, de même qu'avec plusieurs clientèles externes telles les organisations périphériques, municipales et fédérales.

2.2.5 Interface sécuritaire

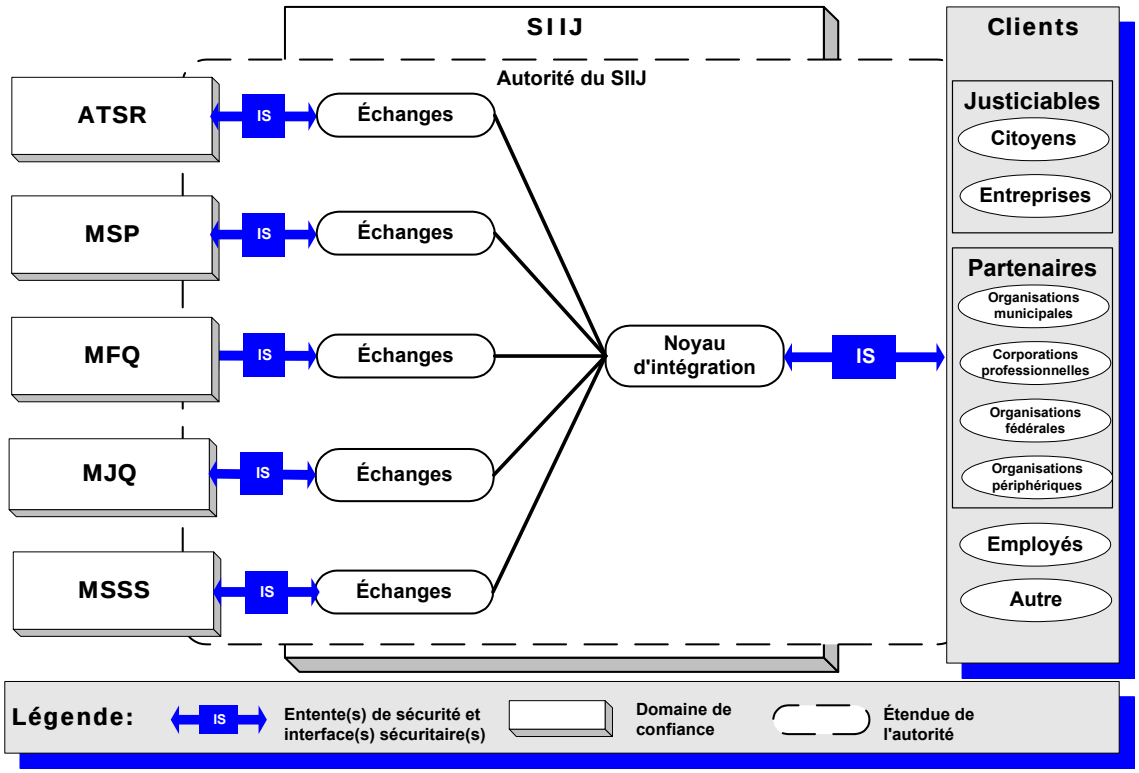
Une interface sécuritaire présente les modalités techniques de sécurisation de l'information numérique. Elle est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et les fonctions de sécurité nécessaires pour assurer la connectivité et l'interopérabilité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

Le domaine de confiance du noyau devra développer une série d'interfaces sécuritaires en collaboration avec les domaines de confiance touchés par le projet SIIJ et les clientèles externes. Ces interfaces accompagneront les différentes ententes de sécurité ratifiées avec ces domaines de confiance et ces clientèles.

2.3 Modèle de confiance

Le modèle de confiance montre la portée potentielle de l'autorité d'un domaine de confiance pour son offre de services aux clientèles visées et ses échanges avec d'autres domaines de confiance. Tels que définis précédemment, les services et les échanges sont encadrés par des ententes de sécurité comprenant une ou plusieurs interfaces sécuritaires. Il est important de noter que le modèle de confiance comprend le domaine de confiance du noyau, mais aussi des ententes de sécurité et des interfaces sécuritaires. Celles-ci permettront au domaine de confiance du noyau d'assurer une protection de bout en bout de l'information dont elle est responsable.

La figure suivante illustre le modèle de confiance sommaire pour le SIIJ :



Au centre de cette figure se trouvent les services fournis par le noyau d'intégration du SIIJ. Celui-ci est un regroupement de services qui nécessitent des échanges avec chacun des domaines de confiance sous l'autorité des différents intervenants présentés à gauche de la figure (MSP, MJQ, MSSS, MFQ et ATSR). Chaque domaine de confiance génère un nombre important d'échanges et de types d'échanges (échanges possédant les mêmes caractéristiques. Exemples : l'envoi d'une DIP, la diffusion du rôle, etc.). Ces différents types d'échanges se doivent d'être spécifiés et encadrés par des ententes de sécurité (aspects organisationnels et légaux) et des interfaces sécuritaires (aspects techniques). Chaque relation entre les domaines de confiance des intervenants et celui du SIIJ peut faire l'objet d'une ou de plusieurs ententes de sécurité et interfaces sécuritaires régissant chacune plusieurs échanges.

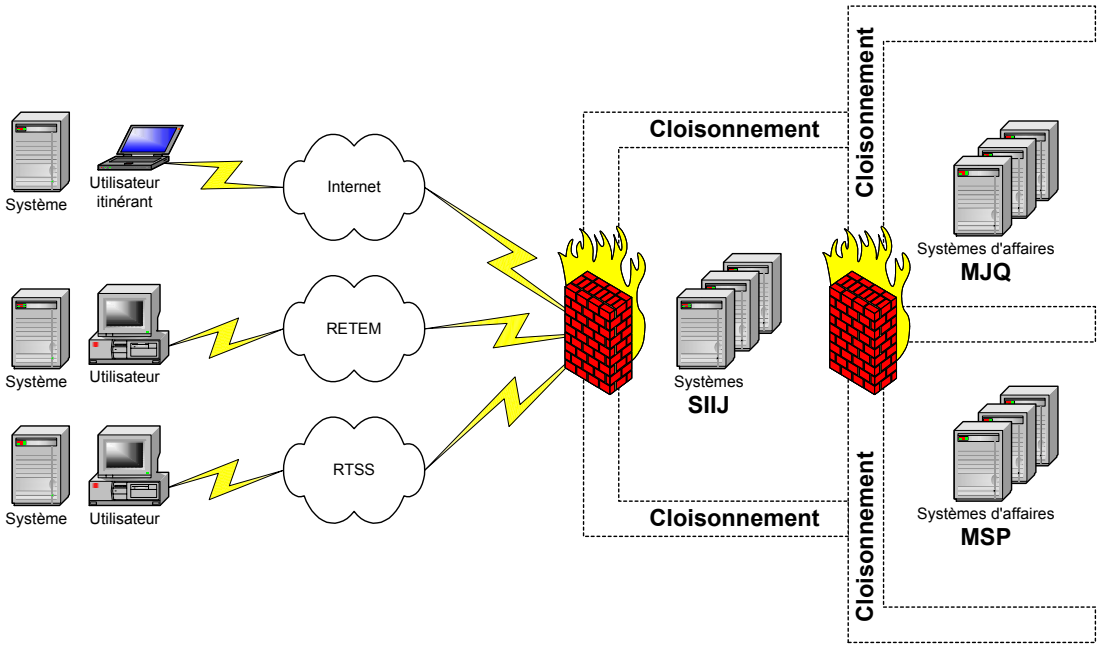
Les relations avec les différentes clientèles du SIIJ présentées à droite de la figure doivent être, elles aussi, régies par des ententes de sécurité et des interfaces sécuritaires. Celles-ci ne seront cependant pas de même nature que celles touchant les domaines de confiance impliqués directement dans le SIIJ. Elles prendront plutôt la forme de convention d'utilisation et d'exigences techniques génériques. Plusieurs versions de ces documents pourront être développées en fonction des différents groupes de clientèles et d'utilisateurs. Ainsi, les avocats et les organisations municipales pourront se voir imposer des exigences auxquelles les justiciables n'auront pas à répondre, conformément aux ententes relatives à chacun. Par exemple, il pourrait être exigé des

premiers de protéger l'information se trouvant sur les postes de travail, mais les derniers ne se verraient pas dans l'obligation de répondre à une telle exigence.

3. ARCHITECTURE SOMMAIRE

Le concept de domaine de confiance vise à créer des frontières entre les organisations impliquées dans le SIIJ. Cette approche doit se refléter dans l'architecture du SIIJ.

La figure suivante représente l'architecture sommaire de la sécurité du SIIJ[124]. Alors que la section 2 présente la vision conceptuelle et logique de la sécurité, cette figure présente la vision technologique à haut niveau de la sécurité.



Comme l'illustre la figure, la technique du cloisonnement permet de faire le découpage en zones, de manière à gérer adéquatement les accès à celles-ci. Les équipements assurant le cloisonnement (principalement, mais pas exclusivement, des coupe-feux) permettent une connexion sécuritaire entre les zones, entre les domaines de confiance et avec les clientèles qui accèdent à distance (par Internet, le RETEM ou le RTSS) aux systèmes du SIIJ, en acceptant seulement les connexions autorisées. Chaque zone contient des systèmes de mission, de même qu'un ensemble d'équipements informatiques et de réseautique. Les systèmes de mission ainsi que les systèmes du noyau d'échange et d'intégration à l'intérieur de ces zones sont sur des réseaux locaux

[124] L'architecture technologique centralisée dans un seul lieu physique du SIIJ est une hypothèse de travail. Puisque cette hypothèse dépend de facteurs externes à l'analyse préliminaire, elle devra être confirmée avant la phase de réalisation, lorsque les décisions concernant la gouverne auront été prises et lorsque les discussions concernant SERTIR auront été complétées.

indépendants. L'architecture sommaire du SIIJ propose trois zones principales, soit celles du noyau d'échange et d'intégration du SIIJ, du MJQ et du MSP.

Étant donné que les systèmes de l'ATSR, du MFQ et du MSSS ne seront pas hébergés par le domaine de confiance du noyau, ils ne sont pas représentés sous forme de zones. Ils apparaissent plutôt parmi les systèmes présentés à gauche de la figure. Ceux-ci utilisent principalement le RETEM (systèmes de l'ATSR et du MFQ) et le RTSS (uniquement dans le cas des systèmes du MSSS) pour échanger avec le SIIJ. Le fait qu'aucun cloisonnement n'apparaisse aux côtés de ces systèmes ne signifie évidemment pas qu'ils ne sont pas protégés, mais bien que les décisions en matière de sécurité pour ces systèmes relèvent des domaines de confiance de ces trois intervenants. Les ententes de sécurité et les interfaces sécuritaires ratifiées entre ces domaines de confiance et le domaine de confiance du noyau permettront de s'assurer que les mécanismes de sécurité mis en place sont acceptables.

4. ORIENTATIONS ET SOLUTIONS DE SÉCURITÉ

Cette section présente les orientations, en ce qui a trait au SIIJ, de chacune des fonctions de sécurité énoncées dans l'AGSIN. Selon ces orientations, les solutions nécessaires pour assurer la sécurité du SIIJ sont présentées[125].

4.1 Identification et authentification

La fonction d'identification[126] permet d'identifier un client (utilisateur et système) ou encore de répondre à la question « Qui est ce client? ». L'authentification sert à authentifier un client ou encore de répondre à la question « Ce client est-il celui qu'il dit être? »

4.1.1 Orientations

- Chacune des organisations est responsable d'identifier adéquatement (selon ses politiques en vigueur) ses utilisateurs avant de leur attribuer un identifiant/mot de passe, un certificat numérique ou tout autre moyen permettant au SIIJ de les authentifier. Avant de se voir attribuer un moyen d'accéder au SIIJ, il importe de vérifier l'identité du requérant. Cette responsabilité devra être assumée par chacune des organisations selon un protocole approuvé par le SIIJ (exemple, la directive de l'ICPG prévoit l'utilisation d'agent de vérification de l'identité (AVI);

[125] Les éléments relatifs à la volumétrie seront abordés dans la description détaillée de chacune des solutions.
[126] Adapté de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

- Chaque organisation est responsable de créer ses utilisateurs, ou groupes d'utilisateurs et de leur attribuer leurs rôles;

- Certains cas d'utilisation ne nécessitent pas d'identification pour émettre un identifiant/mot de passe à un justiciable (par exemple, le dépôt d'une plainte);

- Lorsqu'il est nécessaire de vérifier formellement l'identité d'un justiciable, ce dernier devra se présenter physiquement chez un mandataire autorisé avec une pièce d'identité valable, afin de se voir attribuer un identifiant/mot de passe, un certificat numérique ou tout autre moyen permettant au SIIJ de l'authentifier (la directive de l'ICPG prévoit par exemple l'utilisation d'agent de vérification de l'identité (AVI);

- Les clients (utilisateurs et systèmes) devant accéder ou transmettre de l'information confidentielle ou stratégique au SIIJ doivent être dûment authentifiés;

- Le SIIJ permet à l'utilisateur de s'authentifier une seule fois pour accéder à l'ensemble des ressources auxquelles il est autorisé. Ceci implique donc que toutes les ressources, incluant les systèmes d'affaires, doivent faire confiance à la fonction d'authentification du système Sécurité de l'information numérique. Cependant, ceci n'implique pas qu'il ne puisse y avoir d'autres authentifications durant une session. En effet, les ressources peuvent solliciter une nouvelle authentification pour des raisons de sécurité (par exemple, un consentement lors d'une transaction);

- Les méthodes d'authentification permises pour accéder à une ressource seront déterminées en fonction de la valeur de l'information à laquelle un utilisateur doit accéder. L'annexe 16 permet d'illustrer le degré de sensibilité de l'information traitée par le SIIJ;

- La méthode d'authentification sera attribuée par rôle à l'intérieur du SIIJ plutôt que par usager nommé. Ainsi, à titre d'exemple, tous les juges utiliseront la même méthode d'authentification, sauf exception.

4.1.2 Solutions

Les solutions d'identification et d'authentification qui suivent ont été retenues. Le recours à l'une ou l'autre de ces solutions dépendra de la valeur de l'information à laquelle un utilisateur doit accéder et du contexte d'utilisation (ex. sur un portable, à distance, dans le « périmètre du SIIJ », etc.) :

- ***Code d'usager/mot de passe*** : cette solution permet d'authentifier l'utilisateur en acceptant le code d'usager (unique à chaque utilisateur) et le mot de passe, ceci en comparant ce dernier au mot de passe correspondant dans une base de données ou un répertoire. Cette solution d'identification/authentification très répandue assure un

niveau de sécurité peu élevé, en particulier si un faible contrôle de l'identification est réalisé (par exemple : à l'émission d'un code usager/mot de passe sur Internet);

- ***Certificat numérique*** : cette solution consiste à utiliser un certificat numérique permettant d'effectuer l'identification et l'authentification de son propriétaire, de même que la signature et le chiffrement de documents. L'utilisation de cette solution, qui permet d'assurer un niveau moyen ou élevé de sécurité, implique de stocker le certificat numérique sur le poste de l'utilisateur (niveau de sécurité moyen) ou sur une carte à puce (niveau de sécurité élevé). Cette dernière alternative implique l'installation d'un lecteur de carte à puce sur chaque ordinateur qui permettra d'accéder aux informations pertinentes. Considérant l'investissement important qu'elle demande, cette solution devra être utilisée dans les cas où les informations sont particulièrement confidentielles ou stratégiques.

4.2 Habilitation et contrôle d'accès

La fonction d'habilitation/contrôle d'accès[127] (« Que m'est-il permis de faire? ») définit une liste de ressources et d'informations auxquelles un client (utilisateur et système) peut accéder une fois qu'il a été dûment authentifié. Les mécanismes de contrôle de l'accès permettent aux systèmes de contrôler exactement à qui le droit d'accès est accordé, pour quelles ressources et de quelle façon.

4.2.1 Orientations

- Chaque système (noyau ou affaires) du SIIJ est responsable d'appliquer le contrôle d'accès aux transactions qu'il offre et aux informations qu'il détient;

- Une liste des systèmes (noyau ou affaires) sur laquelle un utilisateur ou un système peut accéder, une fois qu'il a été dûment authentifié, doit être définie et maintenue à jour à l'intérieur du noyau d'échange et d'intégration;

- Les systèmes (noyau ou affaires) doivent fournir et maintenir à jour la liste des groupes d'utilisateurs (rôles) qui sont autorisés à leur accéder;

- Le noyau d'échange et d'intégration est responsable de fournir aux systèmes (noyau ou affaires) l'identité et le, ou les rôles, de l'utilisateur qui requiert l'accès à une ressource du SIIJ;

- Les accès aux systèmes du SIIJ par un client (utilisateur et système) et aux systèmes d'affaires par un système du noyau, sont contrôlés par des coupe-feux, et seuls les

[127] Extrait de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

protocoles prévus peuvent circuler à travers ceux-ci (exemples : protocoles SMTP, HTTP, HTTPS, etc.);

- Les serveurs Web sont les seuls systèmes du SIIJ directement exposés aux clients (utilisateurs et systèmes). Les serveurs Web se chargent de recevoir les requêtes des clients, d'envoyer l'information aux systèmes du SIIJ, de recevoir les réponses et de les acheminer aux clients. Toutes ces opérations s'effectuent de façon transparente aux yeux des utilisateurs.

4.2.2 Solutions

Les solutions suivantes d'habilitation et de contrôle d'accès ont été retenues :

- Outil de répertoire d'entreprise (par exemple, Microsoft Active Directory) permettant d'entreposer des coordonnées d'entités (utilisateurs, systèmes, autres ressources) en fonction de certaines hiérarchies (groupes, organisations, domaines de confiance);
- Outil centralisé de gestion des droits d'accès (cet outil pourrait être à même l'outil de répertoire d'entreprise);
- Outil de cloisonnement (coupe-feu).

4.3 Confidentialité

La fonction de confidentialité[128] permet de s'assurer qu'une information n'est pas divulguée ou mise à la disposition d'un client (utilisateur et système) qui n'a pas l'autorisation d'y accéder. Cette fonction est généralement remplie par des solutions de chiffrement.

4.3.1 Orientations

- Les informations doivent seulement être divulguées ou mises à la disposition des clients (utilisateurs et systèmes) autorisés;

- Le SIIJ met en place les mécanismes pour garantir la confidentialité des informations numériques qui sont entreposées, ou qui circulent dans les systèmes sous son autorité;

- Chaque organisation a l'obligation de mettre en place les mécanismes de sécurité locaux pour garantir la confidentialité des informations numériques qui sont entreposées ou qui circulent dans les systèmes sous son autorité. Bien que des

[128] Adapté de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

fonctions du noyau peuvent être sollicitées dans quelques cas, certains mécanismes devront être implantés à l'intérieur de chacune des organisations (exemples : chiffrement sur les postes mobiles et chiffrement des courriels);

- Toute information confidentielle ou stratégique doit être chiffrée lorsqu'elle circule, ou est susceptible de circuler, dans un réseau public ou non sécuritaire. Ceci fait référence à deux médiums de transmission différents :
  - Internet : l'utilisation du SIIJ au moyen de l'Internet se fait à travers une connexion chiffrée, à l'exception des pages informationnelles disponibles au grand public et qui ne nécessitent pas d'authentification;
  - Courriel : les documents contenant de l'information confidentielle ou stratégique envoyés par courriel doivent être chiffrés ou doivent être envoyés dans un courriel chiffré.

- Toute information confidentielle ou stratégique doit être chiffrée lorsqu'elle est entreposée sur un système ou un média dont le contrôle d'accès n'est pas adéquat pour la valeur de celle-ci (exemples : ordinateur portable, disquette).

4.3.2 Solutions

Les solutions de chiffrement qui suivent ont été retenues. Le recours à l'une ou l'autre de ces solutions dépendra de la valeur de l'information à laquelle un utilisateur doit accéder et, surtout, du contexte d'utilisation (exemples : accès à distance, accès dans le « périmètre » du SIIJ, accès pour la maintenance des systèmes, etc.) :

- ***Connections Web chiffrées (SSL)*** : solution permettant d'établir des connexions point à point (des postes des utilisateurs au SIIJ) sur le réseau Internet. Elle fournit une protection contre la surveillance électronique, la manipulation et la contrefaçon des données au niveau des communications. Contrairement à la solution du tunnel chiffré qui garde en sécurité les données en créant un canal sécurisé sur le réseau où elles circulent, SSL garde en sécurité les données uniquement entre deux applications. Cette solution de chiffrement multi plate-formes et intégrée directement dans les fureteurs Web est certainement la plus répandue sur Internet;

- ***Tunnel chiffré (réseau virtuel privé RVP)*** : solution qui permet de créer un tunnel (réseau virtuel privé) à l'intérieur d'un réseau public tel qu'Internet. Les données qui y circulent sont chiffrées de bout en bout (de l'émetteur au récepteur). Cette solution permet non seulement d'assurer la confidentialité des accès au SIIJ à partir d'un fureteur Web, mais aussi à partir d'autres applications (exemples : outils d'entretien des systèmes, certains traitements en lots). Cette solution, qui peut nécessiter l'installation d'un logiciel sur les postes des utilisateurs, sera déployée de façon restreinte par les services du RETEM;

- ***Chiffrement des documents numériques - composant pour poste client*** : solution permettant de chiffrer et de déchiffrer des documents numériques entreposés sur les postes de travail des utilisateurs. Cette solution peut prendre la forme de logiciels commerciaux ou d'une fonction intégrée au système d'exploitation (Windows 2000 et XP). Cette solution est utilisée pour des besoins spécifiques et ciblés. À titre d'exemple d'utilisation, peuvent être mentionnées la protection de documents de jugement sur des portables ou la protection de preuves sur des postes de travail à la maison. Il est nécessaire de rappeler que la mise en place d'une solution de chiffrement des postes de travail est du ressort des intervenants, et non de l'autorité du SIIJ. L'autorité du SIIJ pourra cependant recommander une solution;

- ***Chiffrement des documents numériques - composant pour serveur applicatif*** : solution permettant de chiffrer et de déchiffrer des documents numériques en circulation ou entreposés dans les systèmes du SIIJ. Cette solution est offerte par des serveurs applicatifs tels que BizTalk de Microsoft à l'aide de CryptoAPI notamment. Cette solution sera utilisée pour tous les besoins de chiffrement de documents du SIIJ;

- ***Chiffrement des courriers électroniques*** : solution permettant le chiffrement des courriers électroniques et des documents numériques y étant attachés. Cette solution se greffe à un logiciel standard de courrier électronique. Elle sera utilisée systématiquement lorsque des informations confidentielles ou stratégiques seront transmises par courrier électronique. Il est à noter que, selon les orientations, la mise en place d'une solution de chiffrement des courriels est du ressort des intervenants et non de l'autorité du SIIJ. L'autorité du SIIJ pourra cependant recommander une solution.

4.4 Intégrité et irrévocabilité

La fonction d'intégrité[129] permet d'assurer qu'une information n'a pas été modifiée ou détruite sans autorisation, de façon volontaire ou accidentelle. La fonction

[129] Adapté de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).

d'irrévocabilité[130] fait en sorte qu'une action ou un document soit indéniable et clairement attribué à l'entité qui l'a généré.

4.4.1 Orientations

- Pour certains documents, un mécanisme doit être mis en place pour garantir que l'information échangée par voie électronique est complète et n'a pas été modifiée.

- Pour certains documents, un mécanisme doit être mis en place pour garantir que ces documents soient indéniables et clairement attribués à l'entité qui les a générés (exemples : jugement, rapport de police, demande d'intenter une procédure, etc.).

- Pour certains documents transmis par un client (utilisateur et système), un mécanisme doit être mis en place pour permettre la signature d'un tiers autorisé.

- Pour certains documents reçus par voie électronique, un mécanisme doit être mis en place pour permettre d'apposer une date de tombée.

- La solution de signature de documents doit supporter :
  - plusieurs types de documents, notamment Microsoft Word et Adobe Acrobat;
  - une marque visible semblable à la signature manuscrite;
  - la signature multiple d'un document.

- La solution de signature de dossiers doit supporter :
  - l'inclusion de multiples documents à l'intérieur d'un dossier;
  - la signature multiple d'un dossier.
- Le SIIJ ne supporte pas la signature numérique pour les justiciables, tant que ces derniers ne disposeront pas d'une clé publique de signature reconnue par le gouvernement du Québec[131].

4.4.2 Solutions

Les besoins d'irrévocabilité nécessitent la mise en place d'une solution de signature numérique. Plus spécifiquement, cette solution vise à combler les besoins suivants :

- Signer et vérifier la signature de documents électroniques;

[130] Adapté de l'Architecture gouvernementale de la sécurité de l'information numérique (AGSIN).
[131] Le projet de Service québécois d'authentification gouvernementale (SQAG) pourrait fournir des éléments de solution en ce sens.

- Signer et vérifier la signature de dossiers électroniques (groupe de documents);
- Signer et vérifier la signature de courriers électroniques;
- Effectuer de la « notarisation » (signature de documents par une tierce partie de confiance qui peut être un individu ou un système);
- Effectuer de l'horodatage (apposition d'une date et d'une heure sur les documents).

4.4.2.1 Hypothèses des certificats numériques

Il ressort clairement que plusieurs certificats numériques seront nécessaires pour assurer la sécurité de l'information numérique du SIIJ. L'organisation du SIIJ ne se dotera pas d'une infrastructure à clés publiques (ICP). Le SIIJ utilisera plutôt les ICP en place dans chacune des organisations impliquées (exemples : ICPG, Notarius, etc.). Par conséquent, ces dernières seront responsables de déterminer et mettre en œuvre les moyens adéquats pour protéger les clés privées de leurs usagers par une carte à puce ou par un autre moyen jugé suffisamment sécuritaire selon la valeur de l'information à laquelle ils doivent accéder. Il est donc évident que certains enjeux découlent de cette hypothèse. Parmi ces enjeux, il y a, entre autres :

- ***Mise en place d'un pivot*** : la mise en place d'un pivot est primordiale pour faire le pont entre les différentes ICP impliquées. Les travaux de mise en œuvre du projet SIIJ devront donc s'arrimer étroitement à ceux du pivot gouvernemental pour s'assurer d'offrir une solution adéquate qui sera disponible selon les échéanciers prévus;
- ***Distribution des certificats aux utilisateurs du SIIJ*** : le responsable de l'infrastructure à clés publiques gouvernementale (ICPG) doit prévoir les processus et les infrastructures lui permettant de distribuer des certificats à un grand nombre d'utilisateurs du SIIJ. Ces processus devront tenir compte du fait que les utilisateurs du SIIJ ne sont pas tous des employés du gouvernement ou des mandataires tels qu'ils sont actuellement définis dans la mission de l'ICPG (exemples : avocats, huissiers, municipalités, etc.);
- ***Multiplicité des certificats*** : dans la mesure où plusieurs ICP sont déployées, il pourrait survenir des cas où un même individu possède un certificat dans plus d'une ICP. L'utilisation d'un certificat numérique unique par utilisateur devrait être favorisée pour le SIIJ.

4.5 Disponibilité, surveillance, et administration

Ces fonctions sont présentées dans les architectures détaillées des systèmes Pilotage et exploitation et Journalisation.

4.6 Résumé des solutions de sécurité

Ce tableau résume les solutions technologiques devant être déployées pour assurer la sécurité du SIIJ selon les orientations retenues.

SOLUTIONS TECHNOLOGIQUES DE SÉCURITÉ

Identification et authentification	▪ Certificat numérique. ▪ Code d'usager/mot de passe.
Habilitation et contrôle d'accès	▪ Outil de répertoire d'entreprise. ▪ Outil centralisé de gestion des droits d'accès (pourrait être à même l'outil de répertoire d'entreprise). ▪ Outil de cloisonnement; coupe-feu.

Confidentialité	▪ Connections Web chiffrées (SSL/TSL).
	▪ Tunnel chiffré (réseau virtuel privé RVP).
	▪ Chiffrement des documents numériques.
	  ▪ Composant pour poste client.
	  ▪ Composant pour serveur applicatif.
	▪ Chiffrement des courriers électroniques.

Intégrité/Irrévocabilité	▪ Outil de signature de documents électroniques. ▪ Outil de signature de dossiers électroniques. ▪ Outil de signature de courriers électroniques. ▪ Outil de notarisation. ▪ Outil d'horodatage.