

ANNEXE 2 - SÉCURITÉ DE L'INFORMATION NUMÉRIQUE

5. STRUCTURE DU NIVEAU ENTREPRISE

5.1 Système Sécurité de l'information numérique

Le système Sécurité de l'information numérique est constitué des mécanismes de sécurité et des solutions technologiques qui garantissent, au niveau approprié et tout au long du cycle de vie de l'information, les fonctions de sécurité suivantes, telles que définies dans l'Architecture gouvernementale de sécurité de l'information numérique (AGSIN) :

- Identification/Authentification;
- Habilitation/Contrôle d'accès;
- Intégrité;
- Irrévocabilité;
- Confidentialité.

Les mécanismes de sécurité et les solutions technologiques des autres fonctions de sécurité (disponibilité, surveillance et administration) sont couverts par les systèmes du noyau Pilotage et exploitation et Journalisation.

Le système Sécurité de l'information numérique oblige les utilisateurs ou systèmes qui sollicitent l'utilisation du SIIJ à s'authentifier afin de confirmer leur identité. Cette authentification est requise lors d'une demande d'accès à des actifs informationnels dont le contenu est confidentiel ou stratégique. Bien que la presque totalité du SIIJ nécessite que l'utilisateur soit authentifié pour procéder, certaines fonctions offertes aux justiciables pourraient être sollicitées de façon anonyme (par exemple, la consultation de documentation d'ordre public).

Le mécanisme de sécurité (mot de passe ou certificat numérique) préconisé pour l'authentification sera déterminé en fonction de la valeur de l'information à laquelle l'utilisateur ou le système doit accéder.

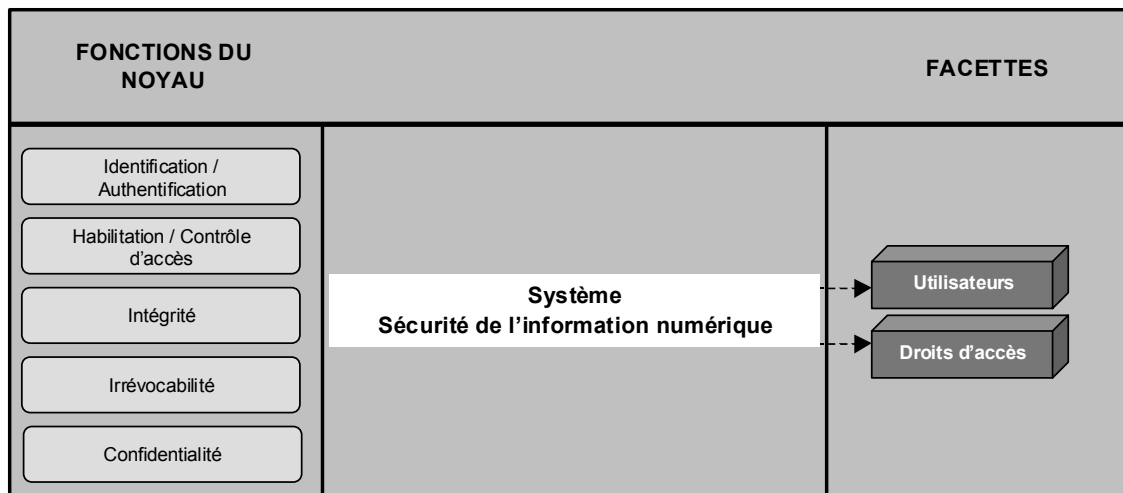
Le système Sécurité de l'information numérique doit contrôler les accès aux ressources du SIIJ; conséquemment, il permet aux utilisateurs (individus ou systèmes) d'être autorisés à utiliser une ressource. Il conviendra de nommer ressource tout élément d'un

système informatisé du SIIJ (exemples : système, élément d'information, transaction, serveur, imprimante, etc.). Ce système devra être en mesure de gérer les utilisateurs et les ressources du SIIJ ainsi que les droits d'accès des utilisateurs aux ressources⁴⁵.

Ce système permet de réaliser la signature et le chiffrement d'informations numériques, de même que leur contrepartie, soit le déchiffrement et la vérification de signatures d'informations numériques. Pour ce faire, l'utilisation de certificats numériques est incontournable.

Finalement, ce système permet à un utilisateur de déposer un document pour qu'une heure de tombée lui soit apposée.

La figure suivante illustre l'arrimage des fonctions du noyau et du système Sécurité de l'information numérique.



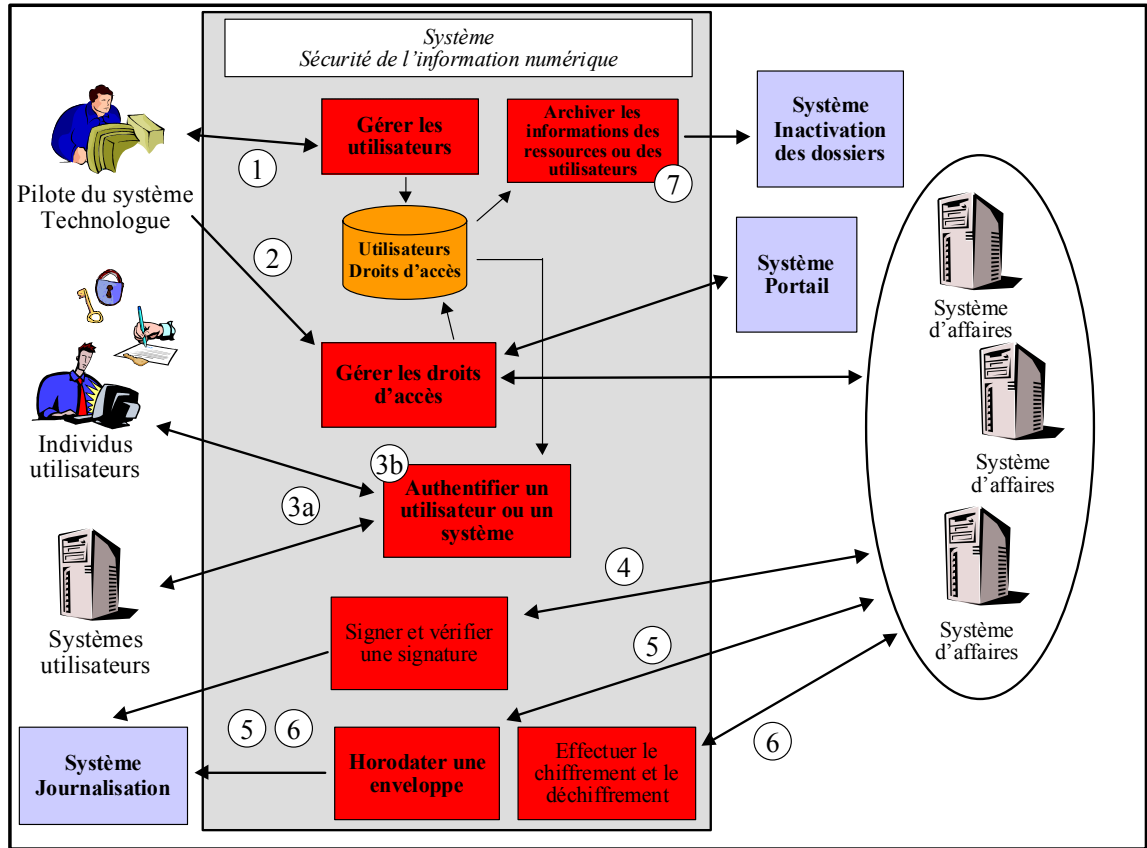
Le système Sécurité de l'information numérique est constitué des fonctions suivantes :

- Authentifier;
- Gérer les utilisateurs;
- Gérer les droits d'accès;
- Effectuer le chiffrement et le déchiffrement;
- Signer et vérifier une signature;
- Horodater;

⁴⁵ Le système Sécurité de l'information numérique contrôle uniquement les accès aux systèmes d'affaires et du noyau, aux serveurs, aux imprimantes, etc. L'accès aux éléments plus fins, tels que les transactions et les éléments spécifiques d'information, ne sera pas géré par ce système, mais bien par les systèmes d'affaires et du noyau. S'ils en offrent la possibilité, ces derniers pourront cependant utiliser l'information contenue dans le système Sécurité de l'information numérique pour la gestion des contrôles d'accès aux éléments plus fins.

- Archiver les données de sécurité.

Le diagramme suivant présente le fonctionnement général du système Sécurité de l'information numérique.



8. L'information sur les utilisateurs du SIIJ est entrée manuellement par le pilote ou importée par lots à partir des différents systèmes de ressources humaines des intervenants impliqués dans le SIIJ. Les pilotes peuvent par la suite créer des groupes d'utilisateurs, effectuer la mise à jour de l'information sur les utilisateurs, l'activation et la désactivation des utilisateurs et la réinitialisation des mots de passe.
9. L'information sur les ressources et groupes de ressources auxquels un groupe d'utilisateurs peut accéder une fois que l'utilisateur a été dûment authentifié est entrée dans le système par le technologue. Celui-ci peut modifier ou supprimer une ressource ou un groupe de ressources. Cette fonction permet également au pilote de décider qui a le droit d'accéder à quelles ressources.

10. Authentifier :

- c. Le système authentifie un utilisateur ou un système qui tente d'accéder à une ressource sécurisée du SIIJ. Elle permet à la fois d'authentifier les utilisateurs et les systèmes utilisant un mot de passe et ceux utilisant un certificat numérique. Dans le cas où l'utilisateur est un individu, le résultat de la vérification lui est par la suite retourné. Si le résultat est positif, l'individu sera dirigé vers la ressource demandée, généralement le système Portail. Dans le cas où l'utilisateur est un système, celui-ci sera dirigé vers la ressource demandée.
 - d. Suite à une authentification réussie, l'utilisateur ou le système se verra remettre un billet Kerberos. Ce billet, qui contient des informations de sécurité, sera par la suite utilisé pour chacune des autorisations d'accès aux systèmes d'affaires et du noyau du SIIJ. L'utilisateur n'aura donc pas à s'authentifier de nouveau.
11. Lorsque nécessaire, une signature numérique peut être apposée sur une enveloppe (« contenants » renfermant un ou plusieurs documents) dans le but de garantir à la fois l'origine et l'intégrité de l'information. Cette fonction permet aussi de vérifier la validité d'une signature apposée sur une enveloppe et de générer une entrée dans le système Journalisation.
12. Lorsque nécessaire, la date et l'heure peut être apposée sur une enveloppe. Un accusé de réception confirmant qu'elle a bel et bien transité par le noyau d'intégration du SIIJ est alors émis et une entrée est effectuée dans le système Journalisation.
13. Lorsque nécessaire, une enveloppe peut être chiffrée de façon à substituer, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé numérique permettant de le ramener à sa forme initiale. Cette fonction permet aussi de déchiffrer une enveloppe.
14. Lorsque nécessaire, le système peut fournir au système Inactivation des dossiers la clé publique du ou des utilisateurs ayant signé numériquement un document. Cette copie archivée de la clé publique pourra être jointe aux documents signés par l'utilisateur, ce qui permettra de vérifier ultérieurement la validité de sa signature.

Il est à noter que la conception, la réalisation et l'exploitation de ce système doivent tenir compte d'un certain nombre de concepts (tirés de l'AGSIN) et d'orientations générales de sécurité présentés à l'annexe 15.

Les niveaux de sécurité requis pour chacun des groupes (rôles) d'utilisateurs doivent aussi être considérés. Ceux-ci ont été établis par les conseillers du SIIJ en fonction de trois facteurs : valeur de l'information numérique, valeur des transactions numériques et valeur de la signature numérique. Le premier concerne la sensibilité de l'information à laquelle les utilisateurs ont accès (publique à hautement confidentielle). Le second concerne la nature des actions posées en regard des informations qui sont manipulées ou

détenues (transaction grand public à transaction critique). Finalement, le troisième concerne le mécanisme de signature numérique requis par un utilisateur du SIIJ pour signer un document (aucune solution à solution forte). Des cotes de 1 à 4 ont été fournies pour chacun de ces facteurs et la cote la plus élevée a été retenue pour le choix du niveau de solution correspondant. Ces niveaux de solution sont :

5. Aucune solution.
6. Solution faible, par exemple : code d'utilisateur et mot de passe.
7. Solution moyenne, par exemple : un certificat sur le poste de travail.
8. Solution forte, où l'on envisage un certificat sur support matériel (carte « à puces ») qui doit demeurer en possession du détenteur en tout temps.

Le tableau suivant fournit une synthèse des niveaux de solution pour chaque principal groupe d'utilisateurs du SIIJ, ainsi que le nombre d'utilisateurs approximatif appartenant à ce groupe.

Organisation	Rôle	Nombre	Niveau
Services policiers	Agente de secrétariat	850	4
	Agent de liaison	178	4
	Directeur des unités responsables des poursuites	800	4
	Enquêteur et gestionnaire d'enquêtes	2431	4
	Patrouilleur	7200	4
	Soutien opérationnel	750	4
SPG	Substituts en chef et en chef-adjoint	40	4
	Recherchistes – Bureau du SPG	10	4
	SPG	290	4
	Agents de secrétariat – Bureau du SPG	190	4
Tribunaux (usagers internes)	Gestionnaire des services judiciaires	125	2
	Greffier adjudicateur	200	4
	Greffier audiencier	500	4
	Greffier, personnel de soutien	600	3
	Greffier, services financiers	100	3
	Greffier, technicien	200	3
	Huissier audiencier	300	2
	Juge et secrétaire	900	4
	Juge en chef et coordonateur	50	4
	Juge de paix	100	4
	Maître des rôles	75	3
	Shérif (civil)	50	3
	Tribunaux (usagers internes)	Shérif (criminel)	50
Tribunaux (usagers externes)	Avocat	12 000	3

*Analyse préliminaire du Système d'intégration d'information de justice
Architecture générale des systèmes d'information*

Organisation	Rôle	Nombre	Niveau
	Expert psycho-sociaux	60	3
	Huissier	535	3
	Médiateur	887	3
	Notaire	2500	3
	Sténographe	200	3
	Syndic	251	3
SCQ (milieu ouvert)	Agent de probation (professionnel)	299	4
	DESMO et secrétaires	38	4
	Dir. Régional - gestionnaire	12	4
	Secrétaires - Dir. Régional	12	3
	Conseillers (professionnels)	20	4
	Directeur des Services administratifs	12	4
SCQ et CQLC (milieu fermé)	Agents des services correctionnels	1458	4
	Chef d'unité - Agent des services correctionnels	252	4
	Personnel de bureau / technicien administratif	69	3
	Agent de probation	39	4
	Direction générale des services correctionnels	60	4
	Administrateur/ Directeur des Services en détention	18	4
	Commission Québécoise des libérations conditionnelles	20	4

Le tableau suivant présente le nombre total par organisation et le nombre total toutes organisations confondues d'utilisateurs qui devront avoir recours à chacun des niveaux de sécurité.

Organisation	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Total
Services policiers	0	0	0	12209	12209
SPG	0	0	0	530	530
Tribunaux (usagers internes)	0	425	1025	1800	3250
Tribunaux (usagers externes)	0	0	16433	0	16433
SCQ (milieu ouvert)	0	0	12	381	393
SCQ et CQLC (milieu fermé)	0	0	69	1847	1916
Total	0	425	17 539	16767	34731

Le tableau démontre bien que les solutions de niveau 3 et 4 seront les plus utilisées dans le cadre du SIIJ. Les solutions d'ICP retenues dans le cadre du SIIJ (ICPG, Notarius, etc.) devront donc en tenir compte.

Les détails sur les niveaux de sécurité requis sont présentés à l'annexe 16.

Le système Sécurité de l'information numérique vise à respecter les orientations suivantes :

- La sélection de technologies la plus conviviale possible pour répondre aux besoins des utilisateurs et capables d'évoluer en fonction des besoins.
- L'information transmise par le système n'est pas modifiable, sauf par les mécanismes prévus d'amendements, de remplacements ou d'ajouts.
- Permettre au justiciable qui choisit d'agir seul devant les tribunaux, d'utiliser le système pour produire ses documents à l'intérieur de balises définies.
- L'utilisation de progiciels éprouvés sera privilégiée pour le développement du SIIJ.
- Le système SIIJ doit profiter des services communs offerts par le gouvernement du Québec lorsque applicable.
- Seuls les intervenants de justice doivent avoir accès à distance aux dossiers des tribunaux. Le justiciable aura cependant accès à distance à son propre dossier.
- Le système SIIJ donnera la prépondérance au français et supportera l'anglais lorsque requis.
- Le système SIIJ doit s'appuyer sur les infrastructures technologiques déjà en place dans les M/O.
- Des mécanismes simples et efficaces d'authentification et d'identification conforme à la Loi concernant le cadre juridique des technologies de l'information (L.Q. 2001, ch. 32) sont introduits.
- Le système SIIJ devra assurer une circulation sécuritaire de l'information empêchant toute intrusion ainsi que toute altération des données.
- Tout en respectant la propriété de l'information générée par chacune des organisations, tout utilisateur doit avoir accès, dans la mesure où il y a droit, à toute l'information pertinente dont il a besoin. Par ailleurs, chaque organisation doit pouvoir compter sur l'échange mutuel d'information afin de maximiser son efficacité et son efficience.
- Le système SIIJ doit permettre la conservation de la trace de certaines transactions.
- Les orientations technologiques du SIIJ seront établies sur la base de la primauté des besoins et intérêts communs du projet SIIJ et non sur les intérêts spécifiques des partenaires.
- Le système SIIJ doit s'appuyer sur les infrastructures technologiques déjà en place dans les M/O.
- Le système SIIJ doit tirer profit des fonctionnalités du réseau Internet.
- L'infrastructure technologique du SIIJ sera moderne mais basée sur des technologies éprouvées.
- La priorité sera accordée aux standards ouverts plutôt qu'aux standards propriétaires.

- Les normes technologiques du SIIJ impliquant des échanges d'informations seront harmonisées à celles du gouvernement fédéral.
- La démarche de l'architecture gouvernementale de la sécurité de l'information numérique (AGSIN) servira à déterminer les besoins de sécurité ainsi que les mécanismes et solutions technologiques afférentes.

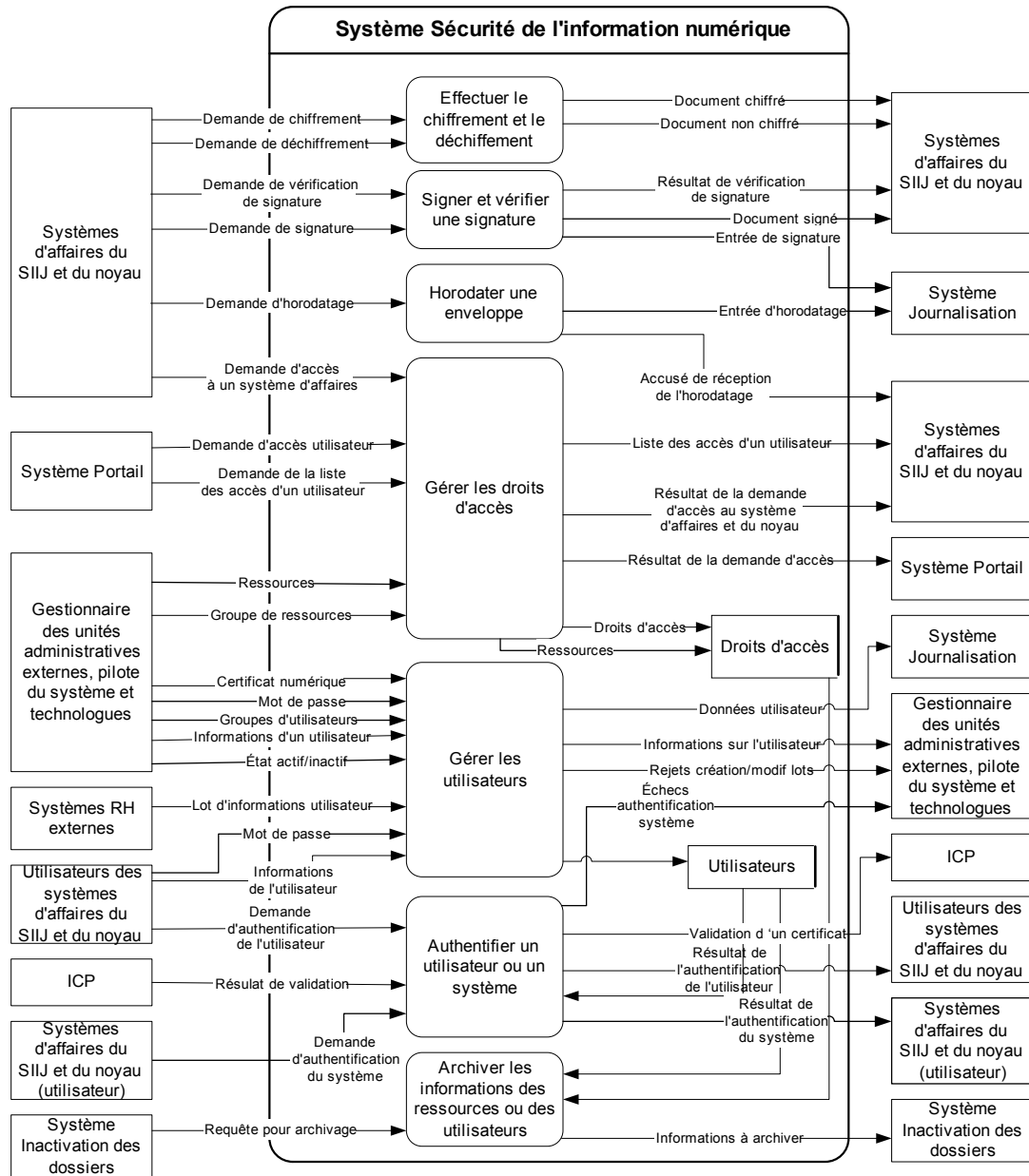
6. STRUCTURE DU SYSTÈME

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.

6.1 Modèle du système

Le diagramme suivant présente le modèle du système Sécurité de l'information numérique. Il contient toutes les fonctions du système, les relations entre ces fonctions, les utilisateurs du système, les systèmes du SIIJ et les facettes de données, de même que les principaux flux de données entre ces divers éléments.



Les sections suivantes présentent les fonctions du système Sécurité de l'information numérique et les unités de tâche qui les composent, les facettes de données, les interfaces utilisées par les divers utilisateurs du système et les catégories d'utilisateurs du système.

6.2 Description et définition des fonctions du système

6.2.1 Fonction Authentifier

6.2.1.1 Description

Cette fonction permet de vérifier l'identité d'un utilisateur (individu ou système), ou encore de répondre à la question « Qui est cet utilisateur? », et de garantir que cet utilisateur est bien celui qu'il dit être. Cette fonction est utilisée à chaque fois qu'un utilisateur ou qu'un système veut accéder à une ressource du SIIJ. Elle permet à la fois d'authentifier les utilisateurs et les systèmes utilisant un mot de passe et ceux utilisant un certificat numérique. Dans le premier cas, le système de sécurité comparera le mot de passe fourni par l'utilisateur avec celui contenu dans le répertoire des utilisateurs. Dans le second cas, le système vérifiera la validité du certificat par l'entremise d'une infrastructure à clé publique, gérée par une tierce partie de confiance (exemples : ICPG, Notarius, etc.) et l'associera à l'utilisateur correspondant du répertoire des utilisateurs.

Conformément aux orientations de sécurité retenues, le SIIJ permettra à l'utilisateur de ne s'authentifier qu'une seule fois sur le portail afin d'accéder à l'ensemble des ressources auxquelles il est autorisé. Ceci implique donc que toutes les ressources, incluant les systèmes d'affaires, devront faire confiance à la fonction Authentifier du système Sécurité de l'information numérique. Une fois l'utilisateur authentifié, un billet Kerberos lui est remis, pour ensuite être utilisé par les autres systèmes du SIIJ (d'affaires et du noyau) lors de l'autorisation d'accès de cet utilisateur.

Cependant, ceci n'implique pas qu'il ne puisse y avoir d'autres authentifications durant une session. En effet, les ressources pourront solliciter une nouvelle authentification pour des raisons de sécurité particulières (par exemple, un consentement lors d'une transaction particulièrement sensible).

Cette fonction est constituée des unités de tâche suivantes :

- Authentifier un utilisateur utilisant un mot de passe;
- Authentifier un utilisateur utilisant un certificat numérique;
- Émettre le billet Kerberos de l'utilisateur.

6.2.1.2 Définition des unités de tâche

Unité de tâche Authentifier un utilisateur utilisant un mot de passe

Cette unité de tâche sera initiée à la suite de la demande d'accès à une ressource sécurisée du SIIJ par un utilisateur (individu ou système interne ou externe au SIIJ). L'utilisateur devra alors fournir son nom d'utilisateur ainsi que son mot de passe.

L'unité de tâche procédera à la recherche de l'utilisateur dans le répertoire des utilisateurs. Si l'utilisateur existe, elle vérifiera la concordance du mot de passe saisi avec celui du répertoire.

Dans le cas où l'utilisateur est un individu, le résultat de la vérification (positif ou négatif) lui sera par la suite retourné. Si le résultat est positif, l'individu sera dirigé vers la ressource demandée, généralement le système Portail. Sinon, l'individu sera invité à s'authentifier de nouveau. Le nombre d'essais consécutifs devra être limité à l'aide d'un paramètre géré par le système Sécurité de l'information numérique. Dans le cas où l'utilisateur est un système, celui-ci sera dirigé vers la ressource demandée, généralement le système Gestion des interfaces, si le résultat est positif. Sinon, la session sera interrompue et le pilote du système sera averti.

Unité de tâche Authentifier un utilisateur utilisant un certificat numérique

Cette unité de tâche sera initiée à la suite de la demande d'accès à une ressource sécurisée du SIIJ par un utilisateur (individu ou système interne ou externe au SIIJ). L'utilisateur devra alors fournir son certificat numérique selon la procédure prévue par l'autorité de certification émettrice (ICPG, Notarius, etc.).

L'unité de tâche procédera à la recherche de l'utilisateur dans le répertoire des utilisateurs. Si l'utilisateur existe, elle vérifiera la concordance du certificat numérique présenté avec celui du répertoire. Par la suite, le système vérifiera la validité du certificat auprès de l'autorité de certification émettrice (ICPG, Notarius, etc.) de celui-ci.

Dans le cas où l'utilisateur est un individu, le résultat de la vérification (positif ou négatif) lui sera par la suite retourné. Si le résultat est positif, l'individu sera dirigé vers la ressource demandée, généralement le système Portail. Sinon, l'individu sera invité à s'authentifier de nouveau. Le nombre d'essais consécutifs devra être limité à l'aide d'un paramètre géré par le système Sécurité de l'information numérique. Dans le cas d'un système, il sera dirigé vers la ressource demandée, généralement le système Gestion des interfaces, si le résultat est positif. Sinon, la session sera interrompue et le pilote du système sera averti.

Unité de tâche Émettre le billet Kerberos de l'utilisateur

Cette unité de tâche sera initiée à la suite d'une authentification réussie d'un utilisateur ou d'un système qui se verra remettre un billet Kerberos. Ce billet contient des informations de sécurité et sera utilisé pour chacune des autorisations d'accès aux systèmes d'affaires et du noyau du SIIJ. Le document *RFC 1510 : The Kerberos Network Authentication Service (V5)* (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>) détaille les règles d'utilisation de Kerberos.

Description sommaire de Kerberos⁴⁶

⁴⁶ Source : Documentation en ligne de Microsoft Windows 2000 Advanced
http://www.microsoft.com/windows2000/fr/advanced/help/default.asp?url=/windows2000/fr/advanced/help/sag_SEconceptsUnAuthKerb.htm

Authentification Kerberos V5 : Kerberos V5 est le protocole de sécurité principal pour les authentifications réalisées dans un domaine. Il vérifie l'identité de l'utilisateur et les services de réseau. Cette double vérification est appelée authentification mutuelle.

Mode de fonctionnement de Kerberos V5 : Le mécanisme d'authentification Kerberos V5 émet des tickets d'accès aux services de réseau. Ces tickets contiennent des données cryptées, dont un mot de passe crypté, qui confirment auprès du service demandé l'identité de l'utilisateur. À l'exception du mot de passe qu'il doit fournir ou de son identification par carte à puce, l'utilisateur ne voit rien du processus d'authentification.

Kerberos V5 dispose d'un service important, le centre de distribution de clés (KDC, Key Distribution Center). Le KDC fonctionne sur chaque contrôleur de domaine dans le cadre de Active Directory, qui stocke tous les mots de passe et toutes les autres informations relatives aux comptes.

Le processus d'authentification Kerberos V5 fonctionne de la manière suivante :

- À l'aide d'un mot de passe ou d'une carte à puce, l'utilisateur du système client s'authentifie auprès du KDC.
- Le KDC émet un TGT (Ticket Granting Ticket) spécial pour le client. Avec ce TGT, le système client accède au TGS (Ticket Granting Service), qui fait partie du mécanisme d'authentification Kerberos V5 du contrôleur de domaine.
- Ensuite, le TGS émet un ticket de service à l'intention du client.
- Le client présente ce ticket de service au service de réseau demandé. Le ticket de service prouve à la fois l'identité de l'utilisateur au service et l'identité du service à l'utilisateur.

6.2.2 Fonction Gérer les utilisateurs

6.2.2.1 Description

Cette fonction permet principalement d'effectuer la gestion des utilisateurs⁴⁷ du SIIJ à l'aide du répertoire utilisateur du SIIJ. Elle permet, dans un premier cas, d'importer par lots des informations sur les utilisateurs provenant des systèmes de ressources humaines des intervenants impliqués dans le SIIJ (MJQ, MSP, MSSS, avocats, huissiers, etc.). Dans un deuxième cas, elle permet de faire la saisie manuelle unitaire de cette information dans le système. Cette fonction permet de plus d'ajouter au « dossier » de l'utilisateur⁴⁸ des informations propres à la sécurité, telles que la clé publique de chiffrement et de signature, le nom d'utilisateur et le mot de passe.

⁴⁷ Un utilisateur peut être un individu ou un système d'affaires, du noyau ou un système externe.

⁴⁸ Le dossier utilisateur réfère à l'ensemble de l'information portant sur un utilisateur donné du SIIJ: nom, coordonnées, code d'usager, mot de passe, certificat numérique, etc.

Cette fonction permet aussi de créer, de modifier et de supprimer des groupes composés d'utilisateurs définis dans le répertoire du SIIJ. Un groupe est composé d'utilisateurs possédant les mêmes caractéristiques (exemples : rôle ou localisation physique) et les mêmes droits d'accès aux ressources.

De plus, elle permet d'effectuer la mise à jour de l'information sur les utilisateurs, l'activation et la désactivation des utilisateurs et la réinitialisation des mots de passe. Finalement, cette fonction permet de gérer les requêtes au répertoire qui sert de mécanisme de stockage des « dossiers » d'utilisateurs.

Cette fonction implique la production de fichiers de ressources humaines par les systèmes qui les gèrent, par exemple GIRES. Les ententes relatives à la production de ces fichiers devront être prises dans le cadre de la phase de réalisation du système Sécurité de l'information numérique.

Cette fonction est constituée des unités de tâche suivantes :

- Créer/modifier un utilisateur en mode unitaire;
- Créer/modifier un utilisateur en lot;
- Joindre un certificat numérique à l'utilisateur;
- Créer/modifier/supprimer un groupe d'utilisateurs;
- Répondre aux requêtes d'information sur l'utilisateur;
- Réinitialiser le mot de passe.

Cette fonction ne permet pas à un utilisateur d'obtenir lui-même, en ligne, un code d'utilisateur et un mot de passe. Toutefois, une analyse plus approfondie des besoins des systèmes d'affaires pourrait éventuellement établir la pertinence d'un tel service.

6.2.2.2 Définition des unités de tâche

Unité de tâche Créer/modifier un utilisateur en mode unitaire

Cette unité de tâche sera initiée à la suite de la demande de création d'un utilisateur ou de modification de ses informations. Lors d'une création, le gestionnaire d'une unité administrative ou le pilote de système doit fournir un identifiant unique (cette unicité devra être validée par le système⁴⁹), les informations de bases obligatoires (exemples : nom, prénom, courriel, etc.) ainsi que les informations relatives à la sécurité (exemples : mot de passe, groupe, etc.)⁵⁰. Ces informations sont stockées dans le répertoire utilisateur du SIIJ. Pour une modification, l'utilisateur de l'unité de tâche doit fournir

⁴⁹ L'identifiant demeure celui qui est utilisé dans chacune des organisations. Pour rendre cela possible le répertoire devra prévoir un domaine pour chacune des organisations. Lorsqu'un utilisateur demande l'accès au SIIJ, il devra fournir son UPN (unique principal name) dont le format rappelle celui d'un courriel (jean.tremblay@mjq.gouv.qc.ca)

⁵⁰ Le mot de passe initial devra être changé dès la première utilisation.

l'identifiant de l'utilisateur visé ou l'obtenir au moyen d'une recherche pour, par la suite, procéder à la mise à jour des informations.

De plus, cette unité de tâche permettra au gestionnaire d'une unité administrative, du pilote de système ou d'un système d'affaires ou du noyau de faire basculer la propriété d'état d'un utilisateur d'actif à inactif, et vice versa.

Unité de tâche Créer/modifier un utilisateur en lot

Cette unité de tâche sera initiée à la suite du dépôt d'un lot de création d'utilisateurs ou de modification de leurs informations. Ce lot peut prendre la forme d'un fichier ou d'un message. Le lot doit fournir l'identifiant unique⁵¹ (cette unicité devra être validée par le système) de chaque utilisateur, les informations de base obligatoires (exemples : nom, prénom, courriel, etc.) ainsi que les informations relatives à la sécurité (exemples : mot de passe, rôle, etc.). Ces informations sont stockées dans le répertoire utilisateur du SIIJ. Pour une modification, l'utilisateur doit fournir les mêmes informations que lors d'une création.

Unité de tâche Créer/modifier/supprimer un groupe d'utilisateurs

Cette unité de tâche sera initiée à la suite de la demande de création, de modification ou de suppression d'un groupe d'utilisateurs provenant du gestionnaire de l'unité administrative ou du pilote de système. Lors de la création, l'utilisateur doit fournir un identifiant unique pour le groupe; cet identifiant sera utilisé pour la recherche du groupe lors d'une modification ou d'une suppression. L'interface utilisateur de gestion des utilisateurs et groupes d'utilisateurs devra permettre d'ajouter et de retirer des utilisateurs comme membres du groupe, et ce, à partir du répertoire d'utilisateur. La suppression d'un groupe sera supportée, bien que l'utilisation de la propriété de désactivation soit privilégiée. Seuls les groupes n'étant pas utilisés peuvent être supprimés.

Unité de tâche Répondre aux requêtes d'information sur l'utilisateur

Cette unité de tâche sera initiée à la suite d'une demande d'information sur un utilisateur provenant d'un système ou d'un opérateur. Les informations demandées seront retournées au requérant lorsque celui dispose des droits d'accès nécessaire. Les requêtes doivent être formulées selon la norme de répertoire LDAP (Lightweight Directory Access Protocol). Elles peuvent être de tout type : À quel prénom/nom correspond un nom d'utilisateur? Quel numéro de téléphone correspond à tel prénom/nom? À quelle unité administrative appartient tel individu? Etc.

Unité de tâche Réinitialiser le mot de passe

⁵¹ Cet identifiant doit être unique à l'organisation requérante et conforme aux normes du répertoire du SIIJ.

Cette unité de tâche sera initiée à la suite de la demande de changement du mot de passe d'un utilisateur provenant du gestionnaire de l'unité administrative, du pilote de système ou directement de l'utilisateur. Cette unité présente une interface utilisateur permettant au gestionnaire de l'unité administrative ou au pilote de système de saisir le nouveau mot de passe. Dans le cas où un utilisateur changerait lui-même son mot de passe, il devra aussi fournir, à l'aide d'une interface utilisateur qui lui est destinée, son ancien mot de passe pour que la modification soit acceptée. Dans tous les cas, le nouveau mot de passe doit satisfaire à la politique de sécurité sur les mots de passe du SIIJ (longueur, format, etc.).

Unité de tâche Joindre un certificat numérique à l'utilisateur

Cette unité de tâche sera initiée à la suite de la demande d'ajout ou de changement de certificat numérique d'un utilisateur provenant du gestionnaire de l'unité administrative, du pilote de système ou directement de l'utilisateur. Cette unité met à jour les propriétés relatives au certificat numérique contenues dans le répertoire utilisateur, notamment les clés publiques de chiffrement et de signature. Les modalités permettant de faire le lien avec l'ICP utilisée par les organisations impliquées (ICPG, Notarius, etc.) devront être déterminées.

6.2.3 Fonction Gérer les droits d'accès

6.2.3.1 Description

La fonction Gérer les droits d'accès permet de définir, de modifier ou de supprimer une ressource ou un groupe de ressources auxquelles un groupe d'utilisateurs peut accéder une fois que l'utilisateur a été dûment authentifié⁵².

Cette fonction permet également de décider qui a le droit d'accéder à quelles ressources. De façon plus concrète, un groupe est créé dans le répertoire d'entreprise pour chacun des systèmes d'affaires et du noyau, et les groupes d'utilisateurs (rôle) autorisés à accéder à ceux-ci devront être membres de ce groupe. Cette fonction est constituée des unités de tâche suivantes :

- Créer/modifier/supprimer une ressource;
- Créer/modifier/supprimer un groupe de ressources;
- Créer/modifier/supprimer un droit d'accès;
- Autoriser un utilisateur.

6.2.3.2 Définition des unités de tâche

Unité de tâche Créer/modifier/supprimer une ressource

Cette unité de tâche sera initiée à la suite de la demande de création d'une ressource ou de modification de ses informations. Lors d'une création, le pilote de système ou le technologue doit fournir un identifiant unique (cette unicité devra être validée par le système), les informations de base obligatoires (exemples : nom, localisation, etc.) ainsi que les informations relatives à la sécurité (exemples : groupe d'accès, rôle, etc.). Ces informations sont stockées dans le répertoire des ressources⁵³ du SIIJ. Pour une modification, l'utilisateur de l'unité de tâche doit fournir l'identifiant de la ressource ou l'obtenir au moyen d'une recherche pour, par la suite, procéder à la mise à jour des informations.

⁵² Il est nécessaire de rappeler que le système Sécurité de l'information numérique contrôle uniquement les accès aux systèmes d'affaires et du noyau, aux serveurs, aux imprimantes, etc. L'accès aux éléments plus fins, tels que les transactions et les éléments spécifiques d'information, ne sera pas géré par ce système, mais bien par les systèmes d'affaires et du noyau. S'ils en offrent la possibilité, ces derniers pourront cependant utiliser l'information contenue dans le système Sécurité de l'information numérique pour la gestion des contrôles d'accès aux éléments plus fins.

⁵³ L'implantation du répertoire des ressources se fera dans le même répertoire physique que celui des utilisateurs, soit le répertoire d'entreprise du SIIJ.

Unité de tâche Créer/modifier/supprimer un groupe de ressources

Cette unité de tâche sera initiée à la suite de la demande de création, de modification ou de suppression d'un groupe de ressources provenant d'un technologue ou du pilote d'un système d'affaires ou du noyau. Lors de la création, l'utilisateur doit fournir un identifiant unique pour le groupe. Cet identifiant sera utilisé pour la recherche du groupe lors d'une modification ou d'une suppression. L'interface utilisateur qui permet de créer et de modifier devra supporter l'ajout et le retrait de ressources comme membres du groupe, et ce, à partir du répertoire de ressources. La suppression d'un groupe sera supportée, bien que l'utilisation de la propriété de désactivation soit privilégiée. Seul les groupes n'étant pas utilisés peuvent être supprimés.

Unité de tâche Créer/modifier/supprimer un droit d'accès

Cette unité de tâche sera initiée à la suite de la demande de création, de modification ou de suppression d'un droit d'accès provenant d'un pilote de système. Ce droit d'accès se traduit dans le répertoire par un groupe. Lors de la création, l'utilisateur doit fournir un identifiant unique pour le groupe. Cet identifiant sera utilisé pour la recherche du groupe lors d'une modification ou d'une suppression. L'interface utilisateur de gestion des utilisateurs et groupes d'utilisateurs devra permettre d'ajouter et de retirer des groupes d'utilisateurs comme membres du groupe, et ce, à partir du répertoire des utilisateurs. La suppression d'un groupe sera supportée, bien que l'utilisation de la propriété de désactivation soit privilégiée. Seuls les groupes n'étant pas utilisés peuvent être supprimés.

Unité de tâche Autoriser un utilisateur

Cette unité de tâche sera initiée à la suite d'une demande de validation d'un billet Kerberos de la part d'un système d'affaires ou du noyau auquel un utilisateur (individu ou système) déjà authentifié tente d'accéder. Lorsque ce dernier tente d'accéder à un système d'affaires ou du noyau, ce système fournit à l'unité de tâche Autoriser un utilisateur le billet Kerberos remis par l'utilisateur. L'unité de tâche détermine la validité de celui-ci et autorise ou non l'utilisateur qui détient le billet Kerberos à accéder au système visé. Le résultat de la vérification (positif ou négatif) sera par la suite retourné au système requérant. Cette unité de tâche permet à un utilisateur qui a déjà été authentifié de ne pas avoir à s'authentifier de nouveau pour accéder à un autre système.

Le document *RFC 1510: The Kerberos Network Authentication Service (V5)* (<http://www.ietf.org/rfc/rfc1510.txt?number=1510>) détaille les règles d'utilisation de Kerberos.

6.2.4 Fonction Effectuer le chiffrement et le déchiffrement

6.2.4.1 Description

La fonction Effectuer le chiffrement et le déchiffrement vise à s'assurer qu'une information n'est pas divulguée ou mise à la disposition d'un utilisateur (individu ou système) ou de toute autre entité qui n'est pas autorisée à y accéder. De façon plus précise, le chiffrement consiste en l'application d'un algorithme mathématique permettant de substituer, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé numérique permettant de le ramener à sa forme initiale. Cette fonction permet donc de chiffrer des enveloppes (« contenant » renfermant un ou plusieurs documents) et de les déchiffrer⁵⁴.

Cette fonction est constituée des unités de tâche suivantes :

- Chiffrer une enveloppe;
- Déchiffrer une enveloppe.

6.2.4.2 Définition des unités de tâche

Unité de tâche Chiffrer une enveloppe

Cette unité de tâche sera initiée à la suite de la demande de chiffrement d'une enveloppe de la part d'un système d'affaires ou du noyau. Dans un premier temps, l'enveloppe vide est créée. Par la suite, les informations sont déposées dans l'enveloppe, qui est finalement chiffrée à partir du certificat numérique fourni par le système requérant. L'enveloppe ainsi créée est retournée au système requérant une fois que le chiffrement est complété. Il est à noter que cette fonction est sollicitée lors d'un échange avec un système externe au SIIJ qui requiert l'utilisation d'une file de message. Elle n'est toutefois pas utilisée lors d'un échange entre deux systèmes à l'intérieur du SIIJ.

Unité de tâche Déchiffrer une enveloppe

Cette unité de tâche sera initiée à la suite de la demande de déchiffrement d'une enveloppe de la part d'un système d'affaires ou du noyau. Cette unité extrait le contenu de l'enveloppe et en vérifie l'intégrité à l'aide du certificat numérique fourni par le système du requérant. S'il est intègre, le contenu de l'enveloppe est retourné au système requérant une fois que le déchiffrement est complété. Il est à noter que cette fonction est sollicitée lors d'un échange avec un système externe au SIIJ qui requiert l'utilisation d'une file de message. Elle n'est toutefois pas utilisée lors d'un échange entre deux systèmes à l'intérieur du SIIJ.

6.2.5 Fonction Signer et vérifier une signature

⁵⁴ Les solutions de chiffrement du canal de transmission (Web SSL et réseau virtuel privé) sont intégrées aux solutions de télécommunication.

6.2.5.1 Description

Cette fonction du système permet à un utilisateur ou à un système d'apposer une signature numérique à une enveloppe dans le but de garantir à la fois l'origine et l'intégrité de l'information, rendant ainsi impossible son éventuelle révocabilité après émission ou sa contrefaçon par un tiers. Cette fonction permet aussi de vérifier cette signature afin de s'assurer de son authenticité.

La signature s'effectue en appliquant un algorithme mathématique sur l'ensemble du contenu de l'enveloppe à signer avec la clé privée de signature du requérant, ce qui produit un résultat appelé *hash*. Ce résultat constitue l'élément clé de la signature. Il est par la suite utilisé pour vérifier l'intégrité de l'enveloppe, de même que l'identité du signataire. La vérification de la signature s'effectue en appliquant un algorithme mathématique sur l'ensemble du contenu de l'enveloppe à signer avec la clé publique de signature du signataire et en comparant le résultat avec celui préalablement obtenu lors de la signature. Des vérifications seront faites auprès de l'autorité de certification émettrice (ICPG, Notarius, etc.) du certificat pour s'assurer de la validité de celui-ci lors de la signature.

Cette fonction est constituée des unités de tâche suivantes :

- Signer une enveloppe;
- Vérifier la signature d'une enveloppe.

6.2.5.2 Définition des unités de tâche

Unité de tâche Signer une enveloppe

Cette unité de tâche sera initiée à la suite de la demande de signature d'une enveloppe de la part d'un système d'affaires ou du noyau⁵⁵. Dans un premier temps, l'enveloppe vide est créée. Par la suite, les informations sont déposées dans l'enveloppe, qui est finalement signée à partir du certificat numérique fourni par le système requérant. L'enveloppe ainsi créée est retournée au système requérant une fois que la signature est complétée. Une fois créée, une enveloppe ne peut être scindée. Il importe donc que le requérant regroupe les documents selon leur destination. La signature d'un document plutôt que d'une enveloppe est faite à l'extérieur du système, à l'aide d'une application spécialisée⁵⁶ et déployée sur les postes des utilisateurs.

⁵⁵ La solution technique est présentée au chapitre 4.2.3.

⁵⁶ La description de l'outil de signature est fournie à la section 4.2.3 de l'annexe.

La signature d'une enveloppe donnera lieu à une entrée dans le journal des transactions (voir le système Journalisation). Cette entrée⁵⁷ peut être utilisée afin de prouver que l'action de signer une enveloppe a bel et bien été réalisée par la fonction de signature.

Unité de tâche Vérifier la signature d'une enveloppe

Cette unité de tâche sera initiée à la suite de la demande de vérification de la signature d'une enveloppe de la part d'un système d'affaires ou du noyau. Cette unité vérifie l'intégrité de l'enveloppe à l'aide du certificat numérique fourni par le système du requérant. Le résultat de la vérification (positif ou négatif) sera par la suite retourné au système requérant.

6.2.6 Fonction Horodater une enveloppe

6.2.6.1 Description

Cette fonction, initiée par les systèmes d'affaires et du noyau, permet d'apposer électroniquement la date et l'heure sur une enveloppe et d'émettre un accusé de réception confirmant qu'elle a bel et bien transité par le noyau d'intégration du SIIJ. Cet accusé de réception contient une référence à l'enveloppe, de même que la date et l'heure de son passage dans le SIIJ. L'enveloppe peut être signée numériquement par la fonction Horodater, en faisant appel à la fonction Signer et vérifier une signature. La fonction Horodater est constituée des unités de tâche suivantes :

- Horodater une enveloppe;
- Émettre un accusé de réception.

6.2.6.2 Définition des unités de tâche

Unité de tâche Horodater une enveloppe

Cette unité de tâche sera initiée à la suite de la demande d'horodatage d'un document ou d'un ensemble de documents (enveloppe), de la part d'un système d'affaires ou du noyau. Dans un premier temps, une enveloppe vide est créée. Par la suite, les informations sont déposées dans l'enveloppe, qui est finalement horodatée à partir de l'heure du SIIJ. L'enveloppe ainsi créée est retournée au système requérant, une fois que l'horodatage est complété. Une fois créée, une enveloppe ne peut être scindée. Il importe donc que le requérant regroupe les documents selon leur destination. Dans le cas où l'accusé de réception doit être signé, il sera mis dans une nouvelle enveloppe par la fonction de signature.

⁵⁷ Cette entrée contiendra les éléments suivants : numéro de l'événement, identifiant de l'enveloppe signée, identifiant du système requérant, date et heure de la signature.

Unité de tâche Émettre un accusé de réception

Cette unité de tâche sera initiée à la suite de la demande d'horodatage de la part d'un système d'affaires ou du noyau. Les informations relatives à l'horodatage⁵⁸ seront retournées au système requérant, et la transaction donnera lieu à une entrée dans le journal des transactions (voir le système Journalisation).

6.2.7 Fonction Supporter l'archivage des données de sécurité

6.2.7.1 Description

Cette fonction permet de recevoir des requêtes d'information du système Inactivation des dossiers et de lui fournir, aux fins d'archivage, les résultats de ces requêtes, soit la clé publique du ou des utilisateurs ayant signé numériquement un document. Cette copie archivée de la clé publique pourra être jointe aux documents signés par l'utilisateur, ce qui permettra de vérifier ultérieurement la validité de sa signature.

Cette fonction est constituée des unités de tâche suivantes :

- Recevoir les requêtes d'information à archiver;
- Fournir les informations à archiver.

6.2.7.2 Définition des unités de tâche

Unité de tâche Recevoir les requêtes d'information à archiver

Cette unité de tâche sera initiée à la suite d'une demande d'information à archiver provenant du système Inactivation des dossiers. Les informations demandées seront retournées au système Inactivation des dossiers, tout en respectant les droits d'accès à ces informations. Les requêtes doivent être formulées selon la norme LDAP.

⁵⁸ Numéro de l'événement, identifiant de l'enveloppe horodatée, identifiant du système requérant, date et heure de l'horodatage.

Unité de tâche Fournir les informations à archiver

Cette unité de tâche sera initiée à intervalle fixe dans le temps. Les informations spécifiées seront retournées au système Inactivation des dossiers.

6.3 Description et définition des facettes du système

Le stockage des données du système Sécurité de l'information numérique repose essentiellement sur un répertoire d'entreprise.

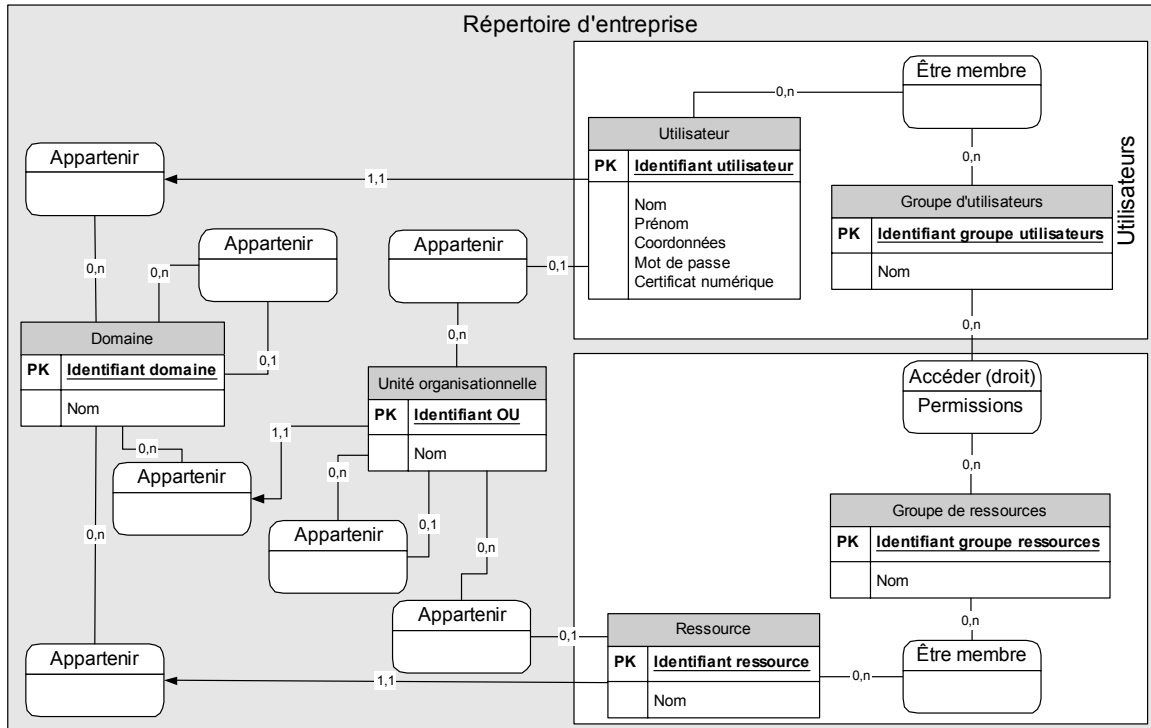
Un répertoire d'entreprise est un recueil de données qui permet de retrouver facilement des entités (généralement des personnes, des organisations, des ressources, etc.) à l'aide de critères spécifiques.

Les répertoires d'entreprise sont un type de base de données spécialisée permettant de stocker des informations de manière hiérarchique et offrant des mécanismes simples pour rechercher l'information, la trier et l'organiser selon un nombre des critères spécifiques.

L'utilisation d'un répertoire d'entreprise ne se limite pas à la recherche de personnes ou de ressources. En effet, un répertoire d'entreprise peut servir à :

- Constituer un carnet d'adresses;
- Supporter l'authentification des utilisateurs (grâce à un mot de passe ou autre);
- Définir les droits d'accès de chaque utilisateur;
- Recenser des informations sur un parc matériel (ordinateurs, serveurs, leurs adresses IP et adresses MAC, etc.);
- Décrire les applications disponibles.
- Etc.

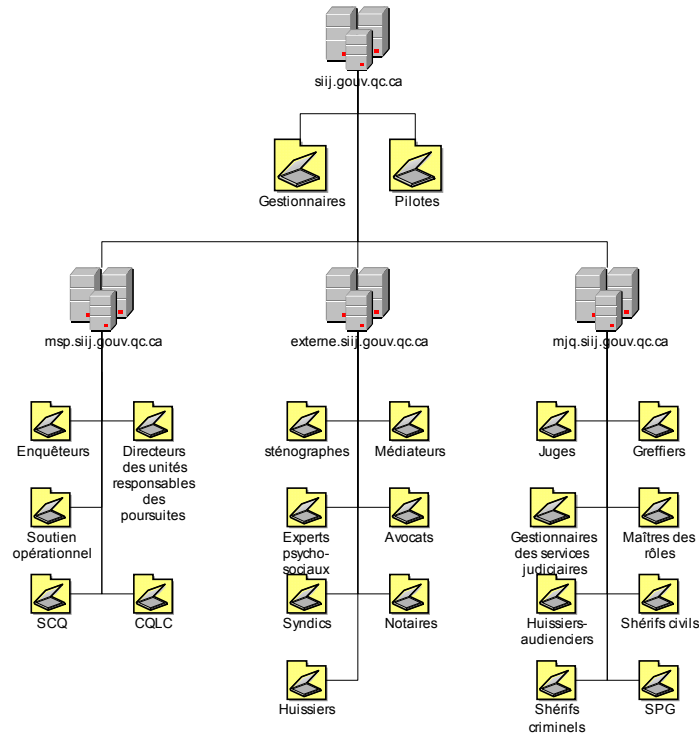
Le diagramme suivant présente sommairement les classes entreposées à l'intérieur du répertoire d'entreprise du SIIJ.



Voici les orientations qui devront guider la conception du répertoire :

- Le répertoire d'entreprise du SIIJ et de ses partenaires gouvernementaux doit s'arrimer au projet de répertoire d'entreprise gouvernemental;
- Chacun des domaines de confiance du SIIJ doit avoir son propre répertoire d'entreprise;
- Le répertoire d'entreprise du SIIJ contient un annuaire global qui réfère au répertoire de chaque domaine de confiance. De plus, il contient l'information sur les utilisateurs appartenant au domaine de confiance du noyau ainsi que sur les groupes d'utilisateurs liés à plus d'un domaine de confiance.

Le diagramme suivant présente un aperçu de ce à quoi pourrait ressembler l'architecture du répertoire d'entreprise SIIJ. L'architecture détaillée devra être définie dans le cadre des activités de réalisation du SIIJ.



Il a été nécessaire de définir une interface normalisée permettant d'accéder de façon standard aux services du répertoire d'entreprise. Le protocole LDAP⁵⁹ remplit cette mission en fournissant un moyen unique (standard ouvert) d'effectuer des requêtes sur un annuaire (compatible LDAP).

Le modèle d'information du protocole LDAP définit le type de données pouvant être stockées dans un répertoire LDAP.

Est appelé entrée (en anglais *entry*) l'élément de base du répertoire d'entreprise. Chaque entrée du répertoire LDAP correspond à un objet abstrait ou réel (exemples : une personne, un objet matériel, des paramètres). Chaque entrée est constituée d'un ensemble d'attributs (paires clé/valeur) permettant de caractériser l'objet que l'entrée permet de définir.

⁵⁹ Le protocole LDAP en est actuellement à sa version 3 et a été normalisé par l'IETF (Internet Engineering Task Force). Il existe une RFC pour chaque version de LDAP : RFC 1487 pour LDAP v. 1 standard, RFC 1777 pour LDAP v. 2 standard (1994) et RFC 2251 pour LDAP v. 3 standard (1997).

Le tableau suivant présente une liste non exhaustive des principaux attributs utilisateurs définis par le standard LDAP v3 et pertinents pour les utilisateurs du système Sécurité de l'information numérique.

Attribut	Description
aliasedObjectName	DN de l'objet dont celui en cours est un alias
authorityRevocationList	Liste de certificats révoqués par l'autorité chargée de les réguler
businessCategory	Activité professionnelle d'une entreprise ou d'une personne
c	Code du pays en deux lettres (respectant le standard ISO 3166)
caCertificate	Certificat de l'autorité de régulation
certificateRevocationList	Liste des certificats révoqués par l'autorité de régulation
cn	Nom de l'objet (<i>common name</i>)
description	Description de l'objet
distinguishedName	Nom distingué (utilisé par d'autres attributs par héritage)
givenName	Prénom de la personne
houseIdentifier	Identifiant d'un bâtiment
initials	Initiales d'une personne
l	Localité de l'objet (géographique)
member	Nom distingué (DistinguishedName) des membres
name	Nom (utilisé par d'autres attributs par héritage)
o	Nom de l'organisation
objectClass	Classe d'objets
ou	Unité organisationnelle (branche de l'organisation)
owner	Nom du propriétaire de l'objet
postalAddress	Adresse postale (sans le code postal)
postalCode	Code postal
serialNumber	Numéro de série de l'objet
sn	Nom de famille de la personne (<i>surname</i>)
st	État ou région (<i>state</i>)
street	Nom de la rue et assimilé (boulevard, etc.)
telephoneNumber	Numéro de téléphone
telexNumber	Numéro de télex
title	Titre de la personne (différent de fonction)
uid	Identifiant unique de l'objet
userCertificate	Certificat de l'utilisateur
userPassword	Mot de passe de l'utilisateur

6.3.1 Facette Utilisateurs

6.3.1.1 Description

Cette facette permet de stocker l'information sur tous les utilisateurs des systèmes du SIIJ de même que sur les groupes d'utilisateurs.

La facette regroupe les classes d'information (entités) suivantes :

- Utilisateurs;
- Groupe d'utilisateurs.

6.3.1.2 Modèle de facette

Le diagramme présenté à la section 2.3 illustre la facette Utilisateurs, ses principales entités ainsi que les relations qu'elle entretient avec les autres facettes du SIIJ.

6.3.1.3 Définition des classes d'information et de contrôle utilisateur

Utilisateurs

Cette classe (entité) de données est un répertoire des utilisateurs du système. Elle contient les informations générales de l'utilisateur, de même que les informations relatives à la sécurité. Les utilisateurs sont classés dans le répertoire selon la hiérarchie⁶⁰ (domaine, unité organisationnelle) établie.

La classe sera décrite au moyen des attributs (propriétés) suivants :

- Identifiant utilisateur;
- Nom d'utilisateur;
- Nom;
- Prénom;
- Coordonnées;
- Mot de passe;
- Certificat numérique.

Les principaux services du noyau de cette classe seront les suivants :

- Créer/modifier un utilisateur;

⁶⁰ Définition: Modèle de base de données dans lequel les différentes informations sont organisées en arborescence.

- Activer/désactiver un utilisateur;
- Répondre aux requêtes d'information sur l'utilisateur;
- Réinitialiser le mot de passe;
- Joindre un certificat numérique à l'utilisateur.

Groupe d'utilisateurs

Cette classe (entité) de données est un regroupement d'utilisateurs dans le répertoire des utilisateurs du système.

La classe sera décrite au moyen des attributs (propriétés) suivants :

- Identifiant groupe utilisateurs;
- Nom;
- Description.

Le principal service du noyau de cette classe sera le suivant :

- Créer/modifier/supprimer un groupe d'utilisateurs.

6.3.2 Facette Droits d'accès

6.3.2.1 Description

Cette facette permet de stocker l'information sur les droits d'accès du SIIJ. Un droit d'accès est constitué d'un groupe d'utilisateurs ayant accès à un groupe de ressources avec un certain niveau de privilège. De plus, cette facette permet de stocker l'information sur toutes les ressources du SIIJ, de même que sur les regroupements de ressources.

6.3.2.2 Modèle de facette

Le diagramme présenté à la section 2.3 illustre la facette Droits d'accès, ses principales entités, ainsi que les relations qu'elle entretient avec les autres facettes du SIIJ.

6.3.2.3 Définition des classes d'information et de contrôle utilisateur

Ressources

Cette classe (entité) de données est un répertoire des ressources du système. Elle contient les informations générales de la ressource classée dans le répertoire selon la hiérarchie établie (domaine, unité organisationnelle).

La classe sera décrite au moyen des attributs (propriétés) suivants :

- Identifiant ressource;
- Nom;
- Description.

Les principaux services du noyau de cette classe seront les suivants :

- Créer/modifier/supprimer une ressource.

Groupe de ressources

Cette classe (entité) de données est un regroupement de ressources dans le répertoire des ressources du système.

La classe sera décrite au moyen des attributs (propriétés) suivants :

- Identifiant groupe ressources;
- Nom;
- Description.

Le principal service du noyau de cette classe sera le suivant :

- Créer/modifier/supprimer un groupe de ressources.

Droits d'accès

Cette classe (entité) de données est une table des droits d'accès aux ressources du système. Elle contient, pour chaque groupe de ressources, les groupes utilisateurs y ayant accès ainsi que les permissions attribuées à chacun.

La classe sera décrite au moyen des attributs (propriétés) suivants :

- Identifiant groupe ressources;
- Identifiant groupe utilisateurs;
- Nom du droit;
- Description.

Le principal service du noyau de cette classe sera le suivant :

- Créer/modifier/supprimer un droit d'accès.

6.4 Description et définition des interfaces utilisateur

Les différents utilisateurs du SIIJ interagissent avec le système Sécurité de l'information numérique au moyen des interfaces utilisateur suivantes :

- Authentification des utilisateurs;
- Gestion des utilisateurs et groupes d'utilisateurs;
- Gestion des ressources et groupes de ressources.

6.4.1 Interface Authentification des utilisateurs

6.4.1.1 Description

Cette interface permet aux utilisateurs qui désirent accéder aux ressources du SIIJ de s'identifier et de s'authentifier.

Fonction implantée : Authentifier.

Particularité : cette interface doit être développée à partir des services d'Active Directory.

6.4.2 Interface Gestion des utilisateurs et groupes d'utilisateurs

6.4.2.1 Description

Cette interface permet aux responsables chargés de la gestion des utilisateurs du SIIJ (gestionnaires des unités administratives et pilotes) d'ajouter, de mettre à jour et de supprimer les informations sur les utilisateurs et les groupes d'utilisateurs. Elle permet aussi aux gestionnaires et pilotes d'activer et de désactiver les utilisateurs, de leurs joindre un certificat numérique et de réinitialiser leur mot de passe. Cette interface est également accessible aux utilisateurs pour modifier leur propre profil.

Fonction implantée : Gérer les utilisateurs.

Particularité : cette interface doit être développée à partir des services d'Active Directory.

6.4.3 Interface Gestion des ressources et groupes de ressources

6.4.3.1 Description

Cette interface permet aux technologues chargés de la gestion des ressources du SIIJ de créer, de modifier et de supprimer l'information sur les différentes ressources et groupes de ressources qui seront utilisés par les utilisateurs du SIIJ.

Fonction implantée : Gérer les droits d'accès.

Particularité : cette interface doit être développée à partir des services d'Active Directory.

6.5 Description et définition des catégories d'acteurs

Cette section identifie et décrit brièvement les catégories d'acteurs (utilisateurs) qui seront directement affectés par le système Sécurité de l'information numérique, soit :

- Utilisateurs du SIIJ;
- Gestionnaires des unités administratives;
- Pilotes du système;
- Technologues;
- Systèmes d'affaires.

6.5.1 Catégorie d'acteurs Utilisateurs du SIIJ

6.5.1.1 Description

Les utilisateurs ont recours au système dans le cadre d'une demande d'authentification lors d'une connexion au système et lorsqu'ils doivent effectuer une modification de leur profil (incluant une réinitialisation de leur mot de passe). Il est à noter que les autres catégories d'acteurs du système Sécurité de l'information numérique sont aussi considérées comme des utilisateurs du SIIJ.

6.5.2 Catégorie d'acteurs Gestionnaires des unités administratives

6.5.2.1 Description

Les gestionnaires des unités administratives ou les responsables locaux de la sécurité ont la responsabilité de faire la gestion des utilisateurs, des groupes d'utilisateurs et des droits d'accès. Ils peuvent réaliser eux-mêmes les tâches reliées à ces fonctions ou les confier aux pilotes du système.

6.5.3 Catégorie d'acteurs Pilotes du système

6.5.3.1 Description

Les pilotes du système ont la responsabilité de faire la gestion des utilisateurs, des groupes d'utilisateurs, des droits d'accès et des paramètres du système de sécurité. Ils interviennent donc dans la gestion applicative des systèmes.

6.5.4 Catégorie d'acteurs Technologues

6.5.4.1 Description

Les technologues doivent définir et enregistrer dans le système les différentes ressources techniques (systèmes, serveurs, imprimantes, etc.) et groupes de ressources auxquels auront accès les utilisateurs du SIIJ. Ils interviennent donc dans la gestion technique des systèmes. Ces technologues peuvent être des techniciens ou des gestionnaires de réseau.

6.5.5 Catégorie d'acteurs Systèmes d'affaires

6.5.5.1 Description

Cette catégorie d'acteurs concerne l'ensemble des systèmes d'affaires du SIIJ qui sont habilités à faire appel aux différentes fonctions du système Sécurité de l'information numérique.

7. DYNAMIQUE DU SYSTÈME

Le système Sécurité de l'information numérique est concerné par les processus de travail suivants :

- Définir les utilisateurs et les groupes d'utilisateurs;
- Définir les ressources et les groupes de ressources.

7.1 Processus de travail Définir les utilisateurs et les groupes d'utilisateurs

7.1.1 Raison d'être

La raison d'être de ce processus est de définir, dans le système Sécurité de l'information numérique, les utilisateurs et les groupes d'utilisateurs qui auront accès aux diverses ressources du SIIJ.

7.1.2 Description

Ce processus de travail permet aux gestionnaires et pilotes des différentes organisations touchées par le SIIJ d'identifier et de fournir au SIIJ les données concernant chacun des utilisateurs qui auront accès aux ressources du SIIJ. Ces acteurs auront tout d'abord la responsabilité de définir si un membre de l'organisation sera ou non un utilisateur du SIIJ. Si c'est le cas, le gestionnaire ou le pilote devra vérifier que le rôle (ou groupe de responsabilité) occupé par l'individu nécessite l'utilisation d'un certificat numérique ou non⁶¹.

Dans le cas où un certificat numérique n'est pas requis⁶², le gestionnaire ou le pilote créera directement l'utilisateur à l'aide de la fonction Gérer les utilisateurs. Les données qui définissent les utilisateurs pourront être entrées manuellement à l'aide de l'unité de tâche Créer/modifier un utilisateur en mode unitaire et de l'interface utilisateur Gestion des utilisateurs et groupes d'utilisateurs prévue à cet effet. Dans le cas où une partie de cette information existe dans un autre système de l'organisation impliquée (exemples :

⁶¹ L'annexe 16 - *Établissement des niveaux de sécurité requis*, ou tout document qui pourra en découler, permettra de définir si un rôle nécessite le recours à un certificat ou non.

⁶² Niveau 1 ou 2, selon l'annexe 16 - *Établissement des niveaux de sécurité requis*.

dans un répertoire, une base de données ou même un chiffrier électronique), elle est exportée automatiquement vers le système Sécurité de l'information numérique à l'aide de l'unité de tâche Créer/modifier un utilisateur en lot et l'information manquante est complétée manuellement par les responsables à l'aide de l'unité de tâche Créer/modifier un utilisateur en mode unitaire et de l'interface utilisateur Gestion des utilisateurs et groupes d'utilisateurs.

Dans le cas où un certificat numérique est requis⁶³, une demande de certificat devra être déposée au responsable de l'ICP chargé d'émettre des certificats aux membres de l'organisation à laquelle appartient l'utilisateur du SIIJ. En accord avec le cadre de gestion propre à chacune des ICP, des vérifications d'identité seront effectuées par celle-ci. L'ampleur de ces vérifications variera selon que le certificat émis est un certificat de niveau 3 ou de niveau 4. L'émission d'un certificat de niveau 4 nécessitera des vérifications plus poussées. Dans l'éventualité où la demande d'émission de certificat est refusée, le gestionnaire responsable de la demande se verra expliquer les motifs de refus. Dans l'éventualité où la demande est acceptée, le certificat sera émis et acheminé à l'utilisateur. Une copie de la clé publique sera jointe par le gestionnaire ou pilote responsable de la demande aux informations sur l'utilisateur qui auront préalablement été entrées dans le système Sécurité de l'information numérique tel que décrit précédemment.

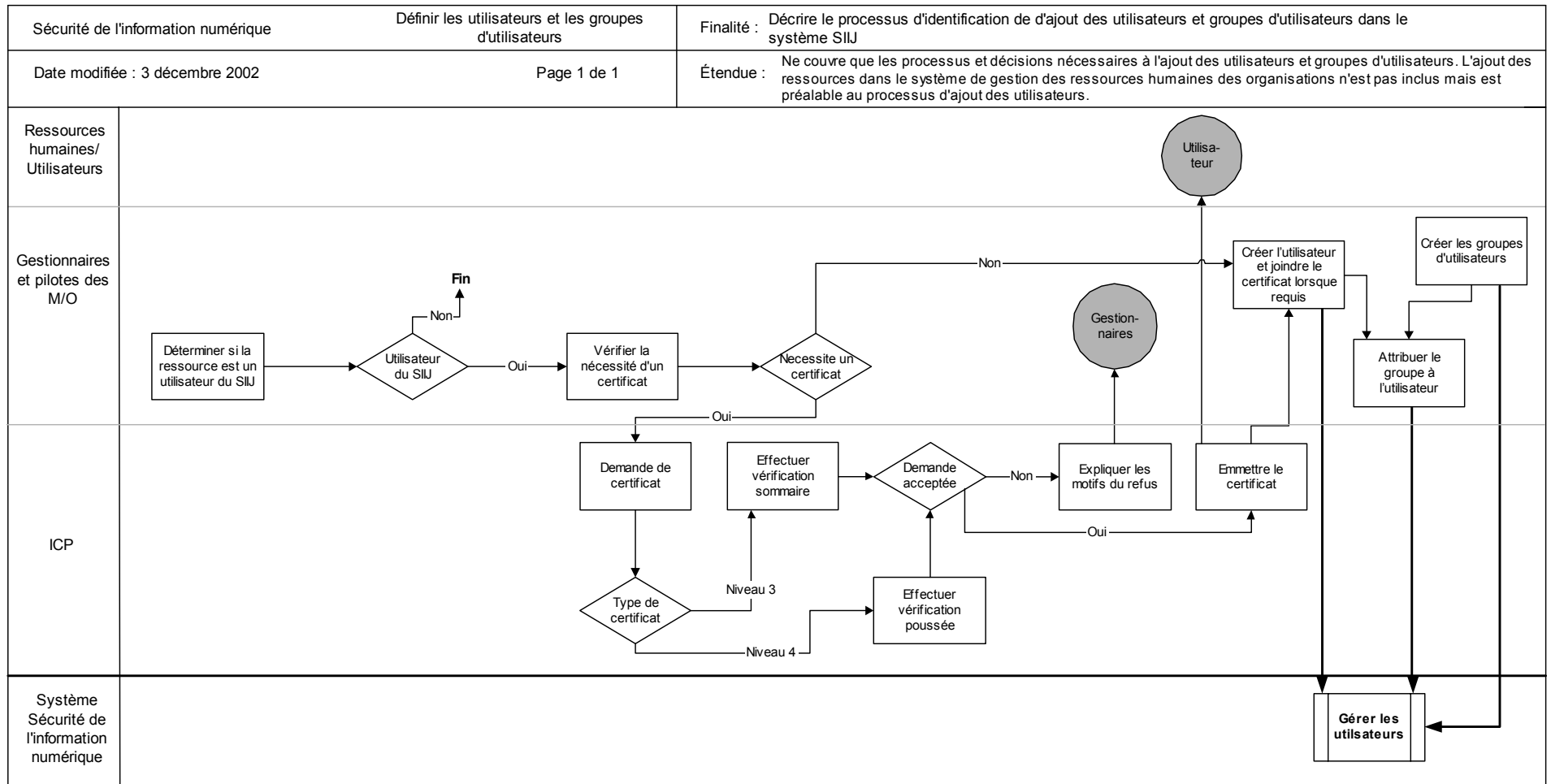
Ce processus de travail implique aussi la définition et l'attribution des groupes d'utilisateurs à l'intérieur du système Sécurité de l'information numérique⁶⁴. Ces groupes d'utilisateurs sont créés et attribués manuellement par les gestionnaires ou les pilotes des différentes organisations touchées par le SIIJ. Les gestionnaires ou les pilotes utilisent l'unité de tâche Créer/modifier un utilisateur en mode unitaire et l'interface utilisateur Gestion des utilisateurs et groupes d'utilisateurs prévus à cet effet. Des scripts de création de groupes peuvent aussi être utilisés par les pilotes (ou les technologues) pour l'entrée des données dans le système Sécurité de l'information numérique.

Chaque organisation qui possède des utilisateurs dans le SIIJ est responsable d'effectuer la définition des utilisateurs et des groupes d'utilisateurs du SIIJ qui en font partie. L'entité SIIJ n'est pas habilitée à définir les utilisateurs des organisations (à l'exception des utilisateurs directs des systèmes du noyau).

Le diagramme suivant présente le processus de définition des utilisateurs et groupes d'utilisateurs

⁶³ Niveau 3 ou 4, selon l'annexe 16 - *Établissement des niveaux de sécurité requis*.

⁶⁴ Un groupe d'utilisateur peut être un groupe de responsabilité (rôle), un groupe d'appartenance (structure organisationnelle), un groupe géographique (localisation), etc. Le type de groupe le plus pertinent dans ce contexte est cependant le groupe de responsabilité (rôle).



7.1.3 Pré-conditions

- Les utilisateurs doivent avoir été identifiés par les gestionnaires ou les pilotes des organisations auxquelles ils appartiennent.
- Chaque utilisateur doit posséder un identifiant unique qui sera validé par le système, de même que des informations de base obligatoires (exemples : nom, prénom, courriel, etc.).

7.1.4 Post-conditions

Aucune post-condition

7.1.5 Type

Ce processus est à la fois manuel et automatisé.

7.1.6 Critères de qualité

- Le processus de définition des utilisateurs et des groupes d'utilisateurs doit être le plus simple possible afin qu'il soit effectué par des gestionnaires et des pilotes qui ne sont pas nécessairement des spécialistes en informatique. Afin de contribuer à cet objectif, l'interface utilisateur qui supporte le processus doit être ergonomique, et intuitive.
- L'interface utilisateur employée pour supporter le processus doit être performante et permettre de faire l'ajout, la modification et la suppression rapides des utilisateurs et des groupes d'utilisateurs.

7.2 Processus de travail Définir les ressources et les groupes de ressources

7.2.1 Raison d'être

La raison d'être de ce processus est de définir dans le système Sécurité de l'information numérique les ressources et les groupes de ressources qui seront accessibles aux utilisateurs du SIIJ.

7.2.2 Description

Ce processus de travail permet aux technologues du SIIJ et aux organisations touchées par le SIIJ de définir les données concernant chacune des ressources qui seront accessibles par le SIIJ. Les technologues auront la responsabilité de recenser les ressources et les données qui les définissent et d'entrer manuellement l'information dans le système Sécurité de l'information numérique à l'aide de l'interface Gestion des ressources et groupes de ressources prévues à cet effet.

Ce processus de travail implique aussi la définition des groupes de ressources à l'intérieur du système Sécurité de l'information numérique. Ces groupes de ressources sont créés manuellement par les technologues du SIIJ et des organisations touchées par le SIIJ. Ces technologues se servent de l'interface utilisateur Gestion des ressources et groupes de ressources conçue à cette fin. Des scripts de création de groupes peuvent aussi être utilisés.

7.2.3 Pré-conditions

- Les ressources doivent avoir été identifiées par les technologues des organisations auxquelles elles appartiennent (SIIJ ou autres organisations).
- Chaque ressource doit posséder un identifiant unique qui sera validé par le système, de même que les informations de base obligatoires (exemples : nom, localisation, etc.).

7.2.4 Post-conditions

Aucune post-condition.

7.2.5 Type

Ce processus est à la fois automatisé et manuel.

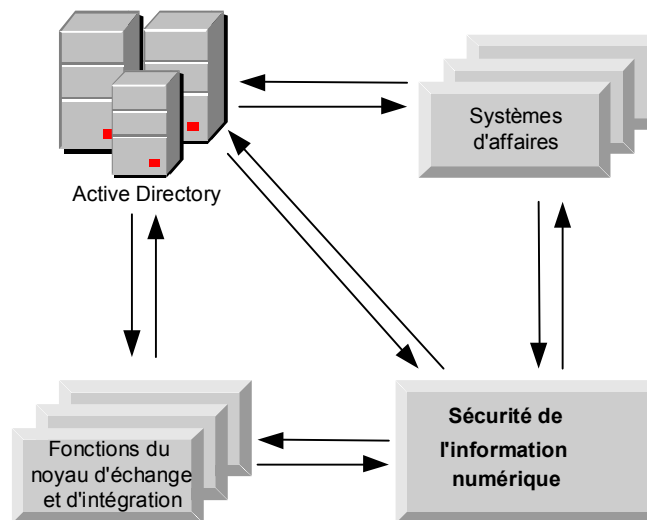
7.2.6 Critères de qualité

- L'interface utilisateur employée pour supporter le processus doit être performante et permettre de faire l'ajout, la modification et la suppression rapides des utilisateurs et des groupes d'utilisateurs.

8. ARCHITECTURE LOGICIELLE

8.1 Modèle d'architecture du logiciel

Le diagramme suivant présente les éléments du système Sécurité de l'information numérique ainsi que leur répartition entre les plate-formes et les infrastructures génériques du SIIJ.



8.1.1 Description de l'architecture logicielle du système Sécurité de l'information numérique

L'architecture logicielle du système Sécurité de l'information numérique repose principalement sur le système d'exploitation Windows serveur de Microsoft, son

répertoire d'entreprise Active Directory et ses outils cryptographiques CryptoAPI et CAPICOM. Les systèmes du noyau et les systèmes d'affaires sollicitent généralement les fonctions de sécurité par l'entremise du système Sécurité de l'information numérique. Les requêtes au répertoire Active Directory pourront être faites directement afin de ne pas alourdir inutilement le système.

8.1.1.1 Critères de qualité

Les critères de qualité de la réalisation sont les suivants :

- La sécurité du système (développement et déploiement tenant compte des meilleures pratiques de sécurité : utilisation de modules ou d'objets éprouvés, revue de code incluant des critères de sécurité, environnement de développement sécurisé, essai des produits dans un contexte reproduisant le contexte réel d'utilisation, etc.);
- La conformité aux besoins à être exprimés par les gestionnaires des unités administratives, les pilotes du système et les technologues;
- La robustesse et la stabilité du système (résistance aux bris, niveau de service, capacité d'accepter plusieurs milliers d'utilisateurs en même temps);
- La performance des services interactifs du système;
- L'ergonomie et la facilité d'utilisation des interfaces utilisateur;
- L'adaptabilité et la facilité d'installation;
- La qualité de la documentation.

8.1.1.2 Interfaces

Les services suivants seront mis à la disposition des autres systèmes :

- Authentifier un utilisateur utilisant un mot de passe;
- Authentifier un utilisateur utilisant un certificat numérique;
- Présenter les informations relatives à un utilisateur (coordonnées, droits d'accès, etc.);
- Chiffrer une enveloppe;
- Déchiffrer une enveloppe;
- Signer une enveloppe;
- Vérifier la signature d'une enveloppe;
- Horodater une enveloppe;
- Recevoir les requêtes d'information à archiver.

8.2 Identification et description des progiciels commerciaux

Le système Sécurité de l'information numérique est constitué des progiciels commerciaux suivants :

- Active Directory de Microsoft;
- CryptoAPI de Microsoft;
- ApproveIt Desktop de Silanis.

8.2.1 Progiciel commercial Active Directory de Microsoft

8.2.1.1 Identification

Microsoft Active Directory (composante de Windows 2000 de Microsoft), version la plus récente.

8.2.1.2 Description

Le service Active Directory de Microsoft est une composante centrale du système d'exploitation Windows 2000. Ce progiciel permet de créer un répertoire d'entreprise centralisé contenant les données sur les utilisateurs, les groupes d'utilisateurs, les ressources, les groupes de ressources et les droits d'accès aux ressources alloués aux différents utilisateurs ou groupes d'utilisateurs.

8.2.1.3 Orientations d'implantation

Aucune orientation d'implantation précise.

8.2.2 Progiciel commercial CryptoAPI de Microsoft

8.2.2.1 Identification

Microsoft CryptoAPI, version la plus récente.

8.2.2.2 Description

CryptoAPI fournit des services permettant aux développeurs d'applications d'ajouter des fonctions de chiffrement/déchiffrement de données. CryptoAPI supporte plusieurs algorithmes de chiffrement à travers différents modules appelés « fournisseurs de services cryptographiques ».

8.2.2.3 Orientations d'implantation

Aucune orientation d'implantation précise.

8.2.3 Progiciel commercial Approvelt Desktop de Silanis

8.2.3.1 Identification

Éditeur : Silanis Approvelt Desktop, version 5 ou suivante.

8.2.3.2 Description

Approvelt Desktop de Silanis permet d'apposer une signature numérique et une image protégée de la signature manuscrite correspondant à la signature numérique sur tout document généré par des applications standard (Word et Excel de Microsoft, Acrobat d'Adobe, ReachForms d'Accelio, etc.).

8.2.3.3 Orientations d'implantation

Silanis Approvelt Desktop doit être déployé sur chacun des postes de travail des utilisateurs qui auront à signer des documents ou à vérifier la signature apposés sur ces documents.

8.3 Identification et description des logiciels importés

Le système Sécurité de l'information numérique n'est pas constitué de logiciels importés.

8.4 Identification et description des sous-systèmes à programmer

Le système Sécurité de l'information numérique est constitué du sous-système Sécurité de l'information numérique.

8.4.1 Sous-système Sécurité de l'information numérique

8.4.1.1 Description

Le tableau suivant présente le travail de programmation à effectuer pour chacune des unités de traitement du sous-système Sécurité de l'information numérique.

Unité de tâche	Travail de programmation à effectuer ⁶⁵			
	Interface à développer	À programmer	Fourni par le logiciel	Logiciel à configurer
Fonction Authentifier				
Authentifier un utilisateur utilisant un mot de passe	X			
Authentifier un utilisateur utilisant un certificat numérique	X			
Émettre le billet Kerberos				Serveur Web et Active Directory
Fonction Gérer les utilisateurs				
Créer/modifier un utilisateur en mode unitaire	X			
Créer/modifier un utilisateur en lot		X		
Joindre un certificat numérique à l'utilisateur	X			
Créer/modifier/supprimer un groupe d'utilisateurs	X			
Répondre aux requêtes d'information sur l'utilisateur			Active Directory	
Réinitialiser le mot de passe	X			
Fonction Gérer les droits d'accès				
Créer/modifier/supprimer une ressource	X			
Créer/modifier/supprimer un groupe de ressources	X			
Créer/modifier/supprimer un droit d'accès	X			

⁶⁵ Interface à développer : la majeure partie de l'unité de tâche est effectuée par un logiciel, cependant, il faut la personnaliser ou lui ajouter une interface.
 À programmer : la majeure partie de l'unité de tâche doit être programmée.
 Fourni par le logiciel : l'unité de tâche est entièrement effectuée par un logiciel.
 Logiciel à configurer : l'unité de tâche fonctionne en configurant de façon adéquate un logiciel.

Unité de tâche	Travail de programmation à effectuer ⁶⁵			
	Interface à développer	À programmer	Fourni par le logiciel	Logiciel à configurer
Autoriser un utilisateur				Serveur Web et Active Directory
Fonction Effectuer le chiffrement et le déchiffrement				
Chiffrer une enveloppe			CryptoAPI	
Déchiffrer une enveloppe			CryptoAPI	
Fonction Signer et vérifier une signature				
Signer une enveloppe			CryptoAPI	
Vérifier la signature d'une enveloppe			CryptoAPI	
Fonction Horodater				
Horodater une enveloppe		X		
Émettre un accusé de réception		X		
Fonction Archiver les données de sécurité				
Recevoir les requêtes d'information à archiver			Active Directory	
Fournir les informations à archiver			Active Directory	

8.4.1.2 Structure

La structure organique du système sera réalisée sur la base du modèle organique général qui sera produit lors des activités préalables à la réalisation des systèmes du SIIJ.

8.4.1.3 Dynamique

Ce système n'implique pas de processus complexes. La dynamique sera donc prise en charge dans le cadre de l'analyse fonctionnelle du système.

8.4.1.4 Intégration technologique

L'intégration technologique sera réalisée lorsque les choix technologiques et le modèle organique général auront été réalisés.

9. STRATÉGIE DE CONCEPTION ET DE RÉALISATION

9.1 Critères de découpage

La stratégie de conception et de réalisation vise à permettre de réaliser et d'implanter progressivement le système. Sommairement, le système Sécurité de l'information numérique est constitué de deux éléments : l'authentification/contrôle d'accès et la cryptographie/horodatage. Les infrastructures technologiques de ces derniers n'ont que très peu de liens entre elles. L'authentification/contrôle d'accès s'opère autour du répertoire d'entreprise Active Directory de Microsoft tandis que la cryptographie/horodatage s'appuie sur CryptoAPI de Microsoft. C'est donc sur cette base que le découpage des deux phases est déterminé.

9.2 Groupes d'intégration

Le système Sécurité de l'information numérique sera conçu et réalisé selon les deux groupes d'intégration suivants :

- Authentification/contrôle d'accès;
- Cryptographie/horodatage.

9.2.1 Description des groupes d'intégration

9.2.1.1 Groupe d'intégration Authentification/contrôle d'accès

Ce groupe d'intégration comprend les fonctions suivantes :

- Authentifier;
- Gérer les utilisateurs;
- Gérer les droits d'accès.

Le groupe d'intégration Authentification/contrôle d'accès est le premier groupe de ce système qui doit être implanté. Ce groupe met en place le répertoire d'entreprise qui est sollicité par la cryptographie. De plus, le groupe d'intégration Authentification/contrôle d'accès doit être disponible dès l'implantation du premier système d'affaires du SIIJ afin de permettre aux utilisateurs d'y accéder.

9.2.1.2 Groupe d'intégration Cryptographie/horodatage

Ce groupe d'intégration comprend les fonctions suivantes :

- Effectuer le chiffrement et le déchiffrement;
- Signer et vérifier une signature;
- Horodater;
- Supporter l'archivage des données de sécurité.

Le groupe d'intégration Cryptographie/horodatage est le deuxième groupe de ce système qui doit être implanté, car il dépend du répertoire d'entreprise et des infrastructures technologiques du premier groupe d'intégration. Il doit être disponible dès l'implantation du premier système d'affaires du SIIJ qui nécessite la signature numérique, le chiffrement ou l'horodatage.

9.2.2 Constitution des groupes d'intégration

Le tableau suivant présente la séquence de réalisation et d'implantation des unités de tâches du système Sécurité de l'information numérique. Le tableau fait référence aux groupes d'intégration décrits précédemment, soit :

- « A » : Authentification/contrôle d'accès;
- « B » : Cryptographie/horodatage.

Traitement		Groupe d'intégration
Système Sécurité de l'information numérique		
Fonction Authentifier		
	Unité de tâche Authentifier un utilisateur utilisant un mot de passe	A
	Unité de tâche Authentifier un utilisateur utilisant un certificat numérique	A
	Unité de tâche Émettre le billet Kerberos de l'utilisateur	A
Fonction Gérer les utilisateurs		
	Unité de tâche Créer/modifier un utilisateur en mode unitaire	A
	Unité de tâche Créer/modifier un utilisateur en lot	A
	Unité de tâche Joindre un certificat numérique à l'utilisateur	A
	Unité de tâche Créer/modifier/supprimer un groupe d'utilisateurs	A
	Unité de tâche Répondre aux requêtes d'information sur l'utilisateur	A
	Unité de tâche Réinitialiser le mot de passe	A
Fonction Gérer les droits d'accès		
	Unité de tâche Créer/modifier/supprimer une ressource	A
	Unité de tâche Créer/modifier/supprimer un groupe de ressources	A
	Unité de tâche Créer/modifier/supprimer un droit d'accès	A
	Unité de tâche Autoriser un utilisateur	A
Fonction Effectuer le chiffrement et le déchiffrement		
	Unité de tâche Chiffrer une enveloppe	B
	Unité de tâche Déchiffrer une enveloppe	B
Fonction Signer et vérifier une signature		
	Unité de tâche Signer une enveloppe	B
	Unité de tâche Vérifier la signature d'une enveloppe	B
Fonction Horodater		
	Unité de tâche Horodater une enveloppe	B
	Unité de tâche Émettre un accusé de réception	B
Fonction Archiver les données de sécurité		
	Unité de tâche Recevoir les requêtes d'information à archiver	B
	Unité de tâche Fournir les informations à archiver	B

10. RÈGLES RÉALISATEUR

10.1 Règles de l'architecture réalisateur

10.1.1 Règles de l'architecture logicielle

L'architecture réalisateur devra tenir compte, dans la définition de l'architecture logicielle, d'un certain nombre de règles applicables au système Sécurité de l'information numérique. Ces règles concernent principalement la portée de la solution et les principes de fonctionnement découlant de la solution. Elles s'énoncent comme suit :

- Des ententes techniques (interfaces de sécurité, telles que définies dans l'AGSIN) doivent être prises avec les intervenants afin d'endosser certains choix technologiques réalisés dans cette architecture;
- Toutes les demandes d'authentification et d'accès aux ressources du SIIJ de la part des utilisateurs (individus et systèmes) doivent s'effectuer en passant par le système Sécurité de l'information numérique. Celui-ci permet à l'utilisateur de s'authentifier une seule fois afin d'accéder à l'ensemble des ressources auxquelles il est autorisé. De plus, les ressources peuvent solliciter une nouvelle authentification pour des raisons de sécurité (par exemple, consentement lors d'une transaction);
- L'ICPG, ou toute autre ICP approuvée par le gouvernement du Québec, est responsable de l'émission et de la gestion des certificats numériques utilisés dans le cadre du SIIJ. Les règles de certification de celles-ci s'appliquent donc.
- La méthode d'authentification sera attribuée par rôle et par responsabilité à l'intérieur du SIIJ plutôt que par utilisateur nommé. Ainsi, à titre d'exemple, tous les juges utiliseront la même méthode d'authentification, sauf exception;
- Le système Sécurité de l'information numérique est responsable de régir l'accès aux systèmes d'affaires du SIIJ. Le contrôle de l'accès aux transactions que ces systèmes d'affaires offrent et aux informations qu'ils détiennent est régi par les systèmes d'affaires eux-mêmes;
- Une liste des ressources auxquelles un utilisateur (individu ou système) peut accéder une fois qu'il a été dûment authentifié doit être définie et maintenue à l'intérieur du système Sécurité de l'information numérique;
- Le système Sécurité de l'information numérique est responsable de fournir aux systèmes du SIIJ l'identité et le ou les rôles de l'utilisateur qui requiert l'accès à une ressource du SIIJ;
- La solution de signature de document doit supporter :
 - plusieurs types de documents, notamment Microsoft Word et Adobe Acrobat,
 - une image protégée de la signature manuscrite (pour certains types de documents),
 - de multiples signatures d'un document;
- 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;
- Chaque organisation a l'obligation de mettre en place certains mécanismes locaux de sécurité afin de garantir la confidentialité des informations numériques qui sont

entreposées ou qui transitent par les systèmes sous son autorité. Les solutions suivantes devront être déployées par les organisations :

- solution de signature électronique pour poste de travail (solution permettant de signer des documents se trouvant sur les postes de travail et d'inclure une image reproduisant la signature manuscrite),
- solution de chiffrement du courriel,
- solution de chiffrement pour poste de travail (solution permettant de chiffrer l'information stockée sur les postes de travail),
- coupe-feu,
- etc.

10.1.2 Règles de l'architecture technologique

Le système Sécurité de l'information numérique reposera sur les éléments d'infrastructure logicielle suivants :

- Système d'exploitation **Microsoft Advanced Server 2000**;
- Fonctions d'émission et de gestion des certificats numériques, fournies par **l'ICPG ou par toute autre ICP externe**, dont les certificats sont acceptés par le pivot du gouvernement du Québec;
- L'outil de répertoire d'entreprise **Microsoft Active Directory** permettant d'entreposer des données d'entités en fonction de hiérarchies;
- Solution de signature électronique sur poste de travail **ApproveIt Desktop de Silanis**;
- Solution d'horodatage;
- Solution de chiffrement de connexion **Web SSL**;
- Solution de chiffrement **CryptoAPI** fournie par les serveurs BizTalk.

En plus de ces choix technologiques, les règles d'architecture technologique suivantes devront être considérées :

- Les accès aux systèmes du SIIJ par un utilisateur (individu ou système) et aux systèmes d'affaires par un système du noyau sont contrôlés par des coupe-feux, et seuls les protocoles prévus peuvent circuler à travers ceux-ci (exemples : protocoles SMTP, HTTP, HTTPS, etc.). Ces protocoles sont décrits à la section Infrastructure technologique
- Les serveurs Web sont les seuls systèmes du SIIJ directement exposés aux utilisateurs (individus ou systèmes). Les serveurs Web se chargent de recevoir les requêtes des utilisateurs, d'envoyer l'information aux systèmes du SIIJ, de recevoir

les réponses et de les acheminer aux utilisateurs. Toutes ces opérations s'effectuent de façon transparente aux yeux des utilisateurs.

10.1.3 Règles de la structure d'information persistante

L'architecture réalisateur devra tenir compte d'une orientation dans la définition de la structure d'information persistante applicable au système Sécurité de l'information numérique. Cette orientation est la suivante :

- L'outil de répertoire d'entreprise Microsoft Active Directory sera utilisé afin d'entreposer l'information persistante sur les utilisateurs, les groupes d'utilisateurs, les ressources, les groupes de ressources et les droits d'accès.

10.2 Règles des spécifications réalisateur

10.2.1 Règles des composants logiciels

- L'interaction avec Active Directory devra s'effectuer par ADSI ou par requête LDAP exclusivement.
- Le structure proposée devra être déterminée sur la base de celle qui sera proposée par le projet de répertoire d'entreprise qui est en cours au Secrétariat du Conseil du trésor.

11. STRUCTURE DE L'INFORMATION PERSISTANTE

Le système sera supporté par le répertoire d'entreprise Active Directory qui constitue une composante du système d'exploitation Windows 2000. La structure d'Active Directory est basée sur la norme X.500.

Un répertoire d'entreprise repose sur une organisation hiérarchique (en réseau) des données. Il utilise des entités (« contenants ») pour représenter des organisations ou des collections d'objets (incluant des individus) tels que des utilisateurs, des systèmes, des serveurs, etc. Les objets et contenants sont organisés à l'intérieur d'une structure en forme d'arbre. Il est à noter qu'une activité de conception du répertoire d'entreprise du SIIJ devra être réalisée afin de définir plus en détails sa structure.

11.1 Architecture des bases de données

Sans objet, puisque le système Sécurité de l'information numérique s'appuie sur un répertoire d'entreprise et non sur des bases de données.

11.2 Modèles des bases de données

La structure détaillée du répertoire d'entreprise sera une adaptation du modèle de base de Active Directory. La structure finale sera établie sur la base des travaux du Secrétariat du conseil du trésor relativement au répertoire d'entreprise gouvernemental. De plus, elle sera fortement affectée par le modèle de gouverne qui sera retenu pour le SIIJ.

12. INFRASTRUCTURE TECHNOLOGIQUE

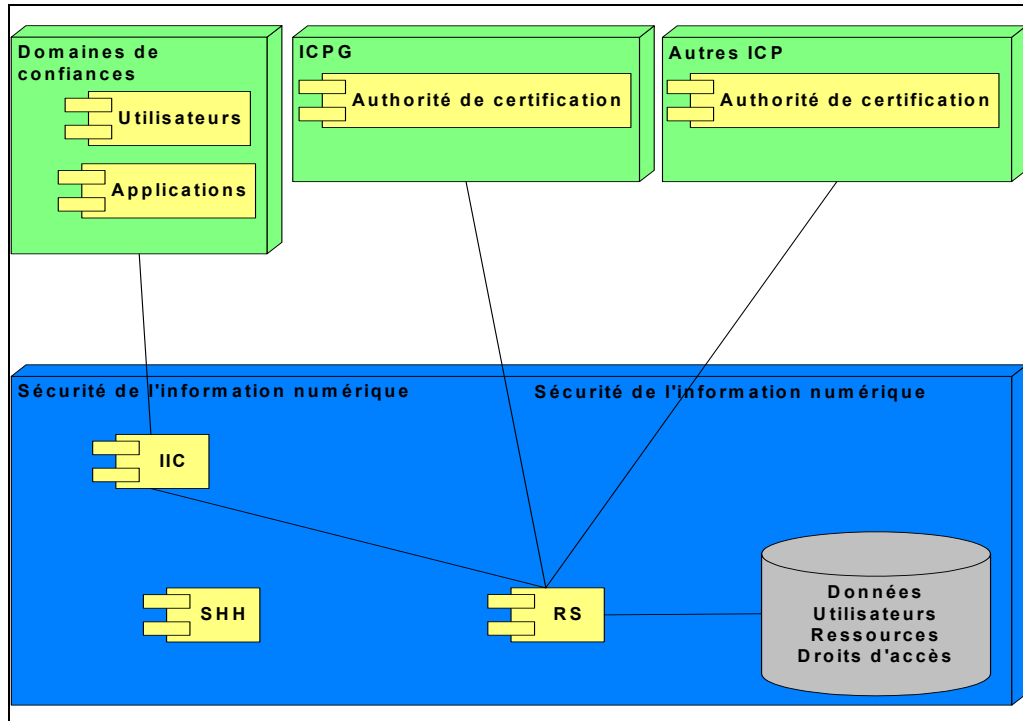
Cette section décrit l'infrastructure technologique nécessaire au soutien du système Sécurité de l'information numérique. Elle décrit le matériel, les logiciels ainsi que les services de soutien qui permettront d'exploiter le système Sécurité de l'information numérique. Elle documente la répartition physique de l'infrastructure sous le volet de la réalisation, soit l'environnement de production.

12.1 Infrastructure de production

Afin de soutenir l'exploitation des systèmes d'information, une infrastructure technologique devra être mise en place. Les sections ci-dessous présentent les configurations d'infrastructure, c'est-à-dire ordinateurs, périphériques, équipement de communication, logiciels ainsi que la manière dont ces dernières sont reliées entre elles.

Le diagramme de déploiement suivant présente les composantes d'infrastructure technologique nécessaires au support du système Sécurité de l'information numérique. La description des composantes qui sont graphiquement représentées dans ce diagramme se trouve à la section 8.2 intitulée Configurations de l'infrastructure technologique.

*Analyse préliminaire du Système d'intégration d'information de justice
Architecture générale des systèmes d'information*



12.2 Configurations de l'infrastructure technologique

Dans le but de supporter l'environnement de production du SIIJ, trois nœuds différents sont recommandés. Les sections suivantes décrivent la configuration de ces environnements.

- Le nœud nommé Répertoire Sécurisé (RS) agira comme point d'entrée pour toutes les requêtes de sécurité liées au répertoire d'entreprise centralisé qui contient les données sur les utilisateurs, les groupes d'utilisateurs, les ressources, les groupes de ressources et les droits d'accès. De plus, ce nœud supportera les fonctions directement liées aux aspects cryptographiques.
- Le nœud Intégrité, Irrévocabilité et Confidentialité (IIC) ne fait pas directement partie du noyau d'échange et d'intégration. Il représente les équipements nécessaires devant être déployés dans les différents points de services faisant partie du SIIJ. Cette composante d'équipement est, en fait, une application permettant d'apposer sur tout document une signature numérique et une image protégée de la signature manuscrite correspondant à la signature numérique.
- Le dernier nœud, Horodatage (SHH), supportera la fonction permettant d'apposer électroniquement la date et l'heure sur une enveloppe et d'émettre un accusé de réception.

Ce nœud est implanté à la place du système d'horodatage qui est basé sur la fonction maître d'opérations « émulateur de PDC » puisque la fonction d'horodatage doit pouvoir servir de preuve légale. Il serait donc inopportun de disperser cette fonction sur un ensemble trop grand d'équipements. La vérification du processus d'horodatage devra être rigoureuse pour assurer la validité de celui-ci.

12.2.1 Définition des configurations physiques

Cette section décrit les caractéristiques de chaque configuration d'infrastructure technologique qui se réfèrent à chacun des trois nœuds.

Nœud – RS

Matériel

- Serveur à 2 processeurs Intel Pentium III Xeon 900 MHz
- 2 Go de mémoire vive
- Disque rigide de 2x72 Go en configuration RAID 1
- 4 Contrôleurs réseau Ethernet 100 Base T
- Contrôleurs E-S Fast Wide SCSI-3
- Lecteur de disques compacts

Logiciel

- Système d'exploitation Microsoft Advanced Server 2000
- Composante Microsoft Active Directory
- Composante Microsoft CryptoAPI

Nœud – IIC

Matériel

- Poste de travail Pentium III ou IV ou compatible
- Logiciel
- Système d'exploitation Microsoft Windows
 - Silanis ApproveIt Desktop

Nœud – SHH

Matériel

- Serveur à 2 processeurs Intel Pentium III 1,266 GHz
- 1 Go de mémoire vive
- Disque rigide de 2x72 Go en configuration RAID 1
- 4 Contrôleurs réseau Ethernet 100 Base T
- Contrôleurs E-S Fast Wide SCSI-3
- Lecteur de disques compacts

Logiciel

- Système d'exploitation Microsoft Advanced Server 2000
- Composante Microsoft SNTP
- Composante d'horodatage

12.2.2 Volumes des configurations physiques

Cette section permet de déterminer le nombre de configurations d'infrastructure technologique nécessaires et l'affectation de chaque configuration à un emplacement d'exploitation et à un environnement de travail particulier.

Description du nœud	Emplacement	Nombre
Nœud – RS	Centre de traitement	2
Nœud – IIC	Chaque poste de travail devant apposer une signature électronique	1 par poste de travail
Nœud – SHH	Centre de traitement	2

12.3 Répartition

Cette section présente la répartition des sous-systèmes et des composants logiciels au déploiement et à l'exécution dans les configurations d'infrastructure technologique.

12.3.1 Répartition du logiciel

La répartition des sous-systèmes et des composants logiciels est représentée dans les configurations d'infrastructure technologique de la section précédente.

12.3.2 Utilisation de l'infrastructure de communication

L'utilisation prévue de l'infrastructure de communication ne déborde pas du cadre interne du noyau d'échange et d'intégration.

12.4 Hypothèses

Afin d'évaluer la charge générée sur les composantes technologiques et sur le réseau par les applications, trois types de profils d'applications ont été établis. Ainsi, ces différents profils permettront d'établir des configurations physiques basées sur les performances attendues.

Les qualificatifs énumérés ci-dessous ont été utilisés afin de classifier les types de profils des applications.

Critère	Faible	Moyen	Élevé
Mémoire statique et dynamique utilisée par l'application	1 gigaoctet et moins	De 1 à 4 gigaoctets	4 gigaoctets et plus
Opération de traitement utilisée par l'application	Très peu	Appariement, diffusion, gestion	Traitement intensif de type compression-décompression, chiffrement, signature, calcul vectoriel, conversion, aiguillage, recherche
Concurrence de l'application	Aucune	Quelques traitements concurrents	Concurrence des traitements de manière régulière
Modèle d'accès des données de l'application	Lecture de données seulement	Lecture et écriture de données	Principalement écriture de données
Modèle d'accès des données de l'application	Séquentiel	Principalement séquentiel, quelque peu aléatoire	Principalement aléatoire

Critère	Faible	Moyen	Élevé
Volume d'accès des données de l'application	2 mégaoctets et moins	De 2 à 10 mégaoctets	10 mégaoctets et plus
Utilisation de ressources distribuées	Aucune	Une très faible partie des données	La majeure partie des données
Débit d'accès réseau de l'application	10 kilooctets et moins par seconde	De 10 à 200 kilooctets par seconde	200 kilooctets et plus par seconde

Trois types de profils d'applications sont présentés ci-dessous. Les profils ont été élaborés selon les qualificatifs de ressources énumérées dans le tableau précédent. La classification des différentes applications devant être déployées sur l'infrastructure technologique sera donc basée sur ces définitions.

Application de faible exigence	Application d'exigence moyenne	Application d'exigence élevée
Utilisation de la mémoire peu sollicitée	Consommation de la mémoire plus ou moins restreinte	Forte utilisation de la mémoire
Emploi modeste de l'unité de traitement et faible concurrence des traitements	Utilisation plus élevée de l'unité de traitement et de la concurrence des traitements	L'unité de traitement et la concurrence des traitements sont couramment utilisées
Effectue principalement des accès de données en lecture séquentielle dont le volume et la fréquence sont peu élevés	Effectue habituellement des accès en lecture et en écriture séquentielles et parfois aléatoires. Le volume et la fréquence des accès de données sont en général restreints	En général, les accès de données sont en mode d'écriture et souvent de façon aléatoire. Le volume et la fréquence sont élevés. Les ressources distribuées sont utilisées régulièrement
Utilisation faible de la bande passante réseau	Utilisation plus ou moins persistante de la bande passante réseau	Le réseau est utilisé de façon persistante
Temps réponse des traitements rapide	Temps réponse des traitements d'ordinaire assez court	Le temps réponse des traitements est de manière générale long

La classification des différents types de serveurs devant être déployés sur l'infrastructure technologique sera basée sur les classifications des différents types d'applications.

Description	Faible exigence	Exigence moyenne	Exigence élevée
Type de serveur	1	2	3
Type de processeur	Intel Pentium III à 1,266 GHz	Intel Pentium III Xeon à 900 MHz	Intel Pentium III Xeon à 900 MHz
Nombre maximal de processeurs	Capacité bi processeurs	Capacité quadruple processeurs	Capacité octuple processeurs
Capacité mémoire	256 Mo extensible à 6 Go	1 Go extensible à 16 Go	2 Go extensible à 16 Go
Capacité disques	Deux porte-unités Wide Ultra2/Ultra3 SCSI (6 x 1 po) enfichables à chaud	Deux porte-unités Wide Ultra2/Ultra3 SCSI (6 x 1 po) enfichables à chaud	Un porte-unité Wide Ultra2/Ultra3 SCSI (4 x 1 po) enfichables à chaud
Capacité totale de stockage	Maximum de 582,4 Go	Maximum de 873,6 Go	Maximum interne de 145,6 Go
Expansion	6 connecteurs PCI dont 2 enfichables à chaud	6 connecteurs PCI dont 4 enfichables à chaud	11 connecteurs PCI enfichables à chaud
Composantes redondantes et enfichables à chaud	Connecteur PCI, Systèmes d'alimentation, Ventilateurs, Mémoire de secours en ligne	Connecteur PCI, Systèmes d'alimentation, Ventilateurs, Mémoire de secours en ligne	Connecteur PCI, Systèmes d'alimentation, Ventilateurs, Mémoire de secours en ligne

Les exigences sur l'infrastructure des différentes applications sont présentées dans le tableau suivant. Les définitions énumérées précédemment ont servi à établir ces hypothèses.

Application	Exigence sur l'infrastructure
Microsoft Active Directory	Moyenne
Composante Microsoft CryptoAPI	Élevée
Silanis ApproveIt Desktop ⁶⁶	Moyenne
Composante Microsoft Sntp	Légère
Composante d'horodatage	Légère

Les hypothèses volumétriques suivantes ont été formulées pour le système Sécurité de l'information numérique.

Paramètre	Valeur
Nombre de transactions annuelles	139 927 604
Nombre de transactions annuelles de gestion de contexte	34 981 901
Nombre total d'utilisateurs	47 246
Nombre annuel de gestions de profil	47 246

⁶⁶ Cet outil est présenté à titre d'exemple.

Le tableau suivant présente les hypothèses ayant trait au nombre de transactions qui seront effectuées pour chaque service offert par le système Sécurité de l'information numérique.

Fonction	Nombre de transactions annuelles
Sécurité de l'information numérique	139 927 604

Le tableau suivant présente les hypothèses utilisées par type de logiciel à l'exécution pour la configuration des nœuds de l'environnement de production. Les exigences requises par le système d'exploitation sont exclues du tableau ci-dessous.

Logiciel	Nombre de transactions par heure de pointe	Mémoire vive requise (gigaoctets)	Espace disque requis (gigaoctets)	Bande passante requise (méga-bit/sec)
Microsoft Active Directory	312 338	1	40	100
Composante Microsoft CryptoAPI	83 215	1	10	100
Silanis ApproveIt Desktop	5 131	0,25	1	100
Composante Microsoft SNTP	1	0,25	1	100
Composante d'horodatage	5 131	0,512	1	100

Les paramètres suivants ont été utilisés afin d'effectuer la conversion sur les périodes de pointes. Le tableau suivant les décrit.

Paramètre	Pourcentage
Transactions d'un mois de pointe en % de l'année	10,4 %
Transactions d'un jour de pointe en % du mois	7,5 %
Transactions d'une heure de pointe en % d'une journée	29 %