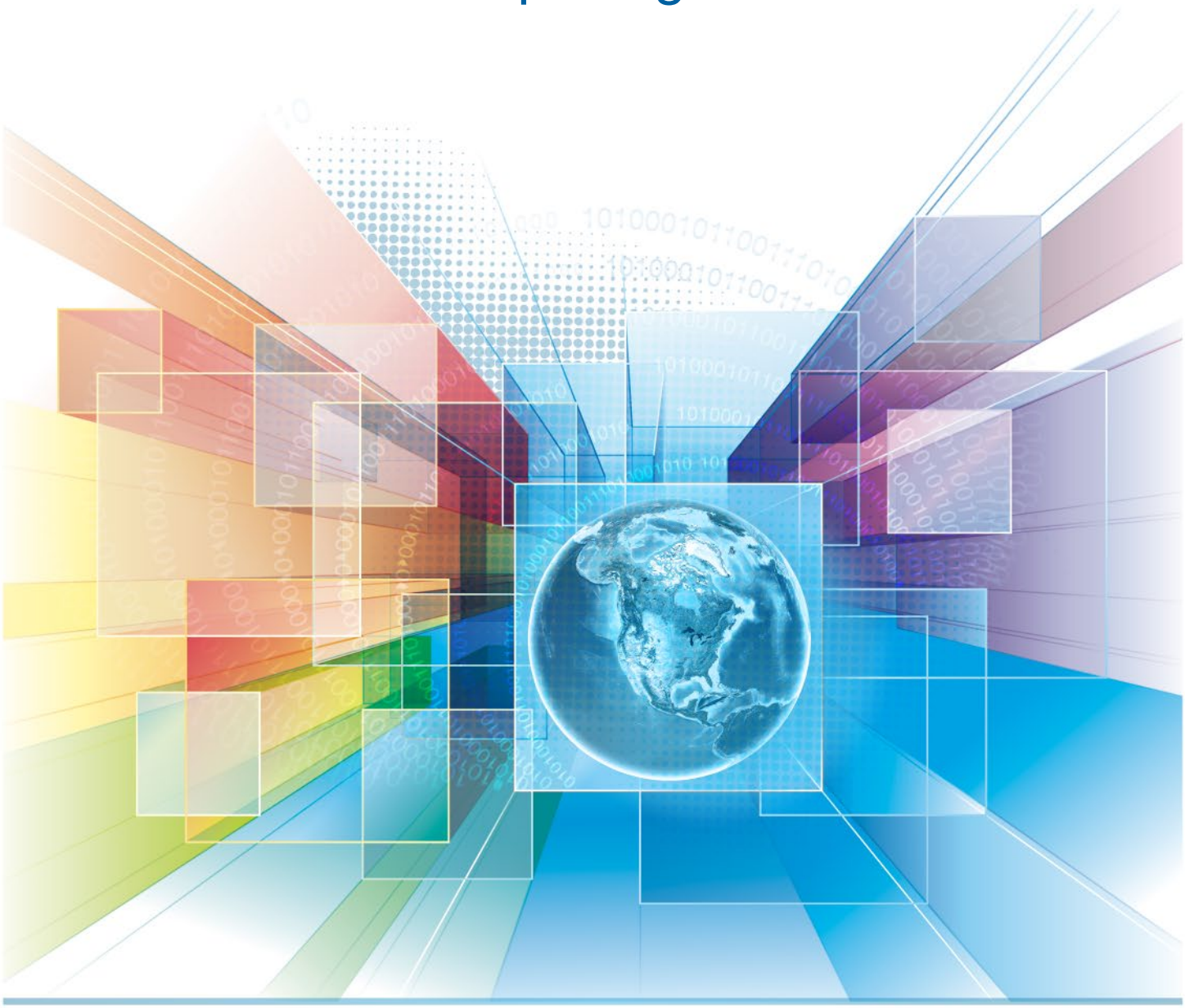
Cadre commun d'interopérabilité du gouvernement du Québec

Architecture d'entreprise gouvernementale 3.2



ENSEMBLE on fait avancer le Québec

Québec

Cadre commun d'interopérabilité du gouvernement du Québec

Architecture d’entreprise gouvernementale 3.2

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite par la Direction des communications.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – Juillet 2016
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-76154-9 (en ligne)

Table des matières

Liste des figures

Sigles et acronymes

3DES *Triple Data Encryption Standard*

AEG Architecture d'entreprise gouvernementale

AES *Advanced Encryption Standard*

AFNOR Association française de normalisation

ASCII *American Standard for Information Interchange*

CAST5 *Carlisle Adams Stafford Tavares version 5*

CCI Cadre commun d'interopérabilité

CCIGQ Cadre commun d'interopérabilité du gouvernement du Québec

CGRI Cadre de gestion des ressources informationnelles

CSS *Cascading Style Sheets* (feuilles de style en cascade)

CSV *Comma Separated Values*

DAOT Direction de l'architecture et des orientations technologiques

DNS *Domain Name Service*

DNSsec *Domain Name System Security Extensions*

DOM *Document Object Model*

DPI Dirigeant principal de l'information

DSA *Digital Signature Algorithm*

DSS *Digital Signature Standard*

DTLS *Datagram Transport Layer Security*

EAP *Extensible Authentication Protocol*

ECC *Elliptic Curve Cryptography*

ECDSA *Elliptic Curve Digital Signature Algorithm*

FLAC *Free Lossless Audio Codec*

FTP *File Transfer Protocol*

FTPS *FTP/SSL (Secure Socket Layer)*

GIF *Graphics Interchange Format* (format GIF)

GML *Geography Markup Language*

HTML *HyperText Markup Language* (langage HTML)

HTTP *HyperText Transport Protocol* (protocole HTTP)

HTTPS *HyperText Transport Protocol Secure*

ID-WSF *Identity Web Services Framework*

IDEA *International Data Encryption Algorithm*

IEEE *Institute of Electrical and Electronics Engineers*

IETF *Internet Engineering Task Force*

IKE *Internet Key Exchange*

IMAP *Internet Access Message Protocol*

IP *Internet Protocol*

IPSEC *Internet Protocol Security*

ISO Organisation internationale de normalisation

JPEG *Joint Photography Experts Group* (norme JPEG)

JSON *JavaScript Object Notation*

KML *Keyhole Markup Language*

LAN *Local Area Network*

LDAP *Lightweight Directory Access Protocol*

LGGRI Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement

LZMA *Lempel-Ziv-Markov chain-Algorithm*

MCCD Modèle corporatif conceptuel de données

MGCD Modèle gouvernemental conceptuel de données

MGCP *Media Gateway Control Protocol*

MIME *Multipurpose Internet Mail Extensions* (protocole MIME)

MP3 *MPEG-1/2 Audio Layer 3*

MTOM *Message Transmission Optimization Mechanism*

NFS *Network File System*

OASIS *Organization for the Advancement of Structured Information Standards*

ODF *Open Document Format*

OP Organismes publics

OSI *Open Systems Interconnection*

PDF *Portable Document Format* (format PDF)

PES Prestation électronique de services

PGP *Pretty Good Privacy*

PGRI Plan de gestion des ressources informationnelles

PNG *Portable Network Graphics* (format PNG)

RADIUS *Remote Authentication Dial-In User Service*

RDF *Resource Description Framework* (système RDF)

REST *Representational State Transfert*

RFC *Request for Comment*

RI Ressources informationnelles

RSA Rivest Shamir Adleman

RTP *Real Time Protocol* (protocole RTP)

RTSP *Real Time Streaming Protocol*

SAML *Security Assertion Markup Language*

SCIM *System for Cross-Domain Identity Management*

SFTP *Secure File Transfer Protocol*

SGQR Standard gouvernemental en ressources informationnelles

SGQRI Standard du gouvernement du Québec pour les ressources informationnelles

SHA *Secure Hash Algorithm*

SHP *Shapefile*

SI Système d'information

SIP Session Initiation Protocol

SMB *Server Message Block*

S/MIME *Secure-Multipurpose Internet Mail Extensions*

SMTP *Simple Mail Transfer Protocol*

SOAP *Simple Object Access Protocol*

SSH *Secure Shell*

SSL *Secure Socket Layer*

SVG *Scalable Vector Graphics*

TACACS *Terminal Access Controller Access-Control System*

TACACS+ *Terminal Access Controller Access-Control System Plus*

TAR *Tape Archive*

TCP *Transmission Control Protocol*

TI Technologies de l'information

TIFF *Tagged Image File Format* (format TIFF)

TLS *Transport Layer Security*

TOGAF *The Open Group Architecture Framework*

UDDI *Universal Description Discovery and Integration*

UDP *User Datagram Protocol*

UIT Union internationale des télécommunications

URI *Uniform Resource Identifier*

UTF *Unicode Transformation Format*

W3C *Consortium W3C*

WFS *Web Feature Service*

WMS *Web Map Service*

WS-I *Web Services Interoperability*

WSDL *Web Service Description Language*

WTLS *Wireless Transport Layer Security*

XACML *eXtensible Access Control Markup Language*

XADES *XML Advanced Electronic Signatures*

XHTML *eXtensible HyperText Markup Language*

XKMS *XML Key Management Specification*

XML *eXtended Markup Language* (langage XML)

XMLdec *XML Decryption*

XMLenc *XML Encryption*

XOP *XML-binary Optimized Packaging*

XSL *eXtended Stylesheet Language*

XSLT *eXtensible Stylesheet Language Transformations*

Historique des versions

Version de l'AEG	Statut	Modification
3.0	Novembre 2014	Publication de la première édition
3.1	Mars 2015	Aucune modification
3.2	Juillet 2016	Aucune modification

La version en vigueur est disponible à cette adresse :

http://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/

Avertissement

Ce document s'inspire des meilleures pratiques dans une variété de champs d'expertise existant présentement sur le marché de la normalisation et de l'architecture d'entreprise, et il ne souscrit à aucune méthode ni à aucun outil propriétaire en particulier. Édité une première fois en avril 2014, cette version à été revue afin d'ajouter le volet sécurité.

Destinataires

L'objectif de ce document est de servir de cadre normatif de référence pour tout acteur d'un organisme public jouant un rôle dans la conception, le développement et la gestion d'un système d'information. Il peut servir comme intrant et matériel de référence à l'architecture d'entreprise gouvernementale et à l'architecture d'entreprise corporative.

Connaissances préalables

Ce document s'insère dans le cadre des travaux de l'architecture d'entreprise gouvernementale 3.0. Afin de bénéficier pleinement du contenu de ce produit livrable, il est fortement recommandé d'avoir une connaissance sommaire de ce qui suit :

- L'ancienne version du Cadre commun d'interopérabilité ;
- La normalisation ;
- Les standards du gouvernement du Québec en ressources informationnelles (SGQRI) ;
- L'Architecture d'entreprise gouvernementale 3.0 ;
- Le Cadre d'architecture d'entreprise TOGAF 9 de l'*Open Group* ;
- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et ses implications pour le développement des systèmes d'information.

Statut

Ce document constitue une pratique recommandée au gouvernement du Québec. Toutefois, le respect du Cadre commun d'interopérabilité du gouvernement du Québec sera considéré dans l'analyse des projets soumis au Sous-secrétariat du dirigeant principal de l'information. Ainsi, le cadre représente un référentiel commun devant être adopté par les organismes publics. On verra, à l'usage, s'il est nécessaire d'obtenir un statut obligatoire pour le présent cadre.

Sommaire exécutif

Offrir une prestation électronique de services (PES) à un citoyen, à une entreprise, à un organisme public ou à un partenaire implique des échanges de données et de services informatiques entre les systèmes de toutes les parties engagées, qui doivent donc « interopérer[1] ». En effet, l'interopérabilité est un aspect incontournable de l'intégration technologique des services en ligne, lesquels demandent d'ouvrir et de faire coopérer les systèmes d'information des différents organismes public (OP). De nombreux gouvernements, notamment ceux du Royaume-Uni, de la France, de l'Australie, des Pays-Bas et de l'Allemagne, appliquent déjà leur propre cadre commun d'interopérabilité ; ils sont persuadés de l'avantage qu'il représente dans le passage à une administration électronique.

Devant cette préoccupation et conformément à la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) et à la politique-cadre, le dirigeant principal de l'information (DPI) propose le Cadre commun d'interopérabilité du gouvernement du Québec (CCIGQ). Véritable référentiel en matière de technologies de l'information, le CCIGQ est un ensemble de normes et de standards[2] relatifs aux ressources informationnelles, qui vise à soutenir l'interopérabilité des systèmes de l'administration publique du Québec.

Le CCIGQ se veut ainsi une référence qui permet la réalisation des objectifs de la planification stratégique gouvernementale. Ce cadre contribue à l'amélioration des services offerts par l'ensemble des organismes publics à leurs clients, et cela en établissant une vision commune de l'interopérabilité au sein de l'administration publique et en favorisant la simplification et l'intégration des services offerts. L'élaboration du cadre est tributaire de l'architecture d'entreprise gouvernementale (AEG 3.0) ayant comme objectif l'amélioration du service offert par le gouvernement à ses cinq types de clients (citoyen, entreprise, employé de l'État, organisme public, fournisseur partenaire). Cette version du CCIGQ couvre les normes applicatives et technologiques applicables aux processus d'échanges d'information entre organismes publics.

1. Nous retenons la définition suivante de l'interopérabilité : La possibilité pour des systèmes informatiques hétérogènes d'échanger des données et des services informatiques. Une définition équivalente de l'interopérabilité, donnée par l'Office québécois de la langue française, est la faculté qu'ont des systèmes de fonctionner conjointement et de donner accès à leurs ressources de façon réciproque.

2. Une norme désigne un ensemble de spécifications décrivant un objet, un être ou une manière d'opérer et qui est approuvée et publiée par un organisme de normalisation national ou international (ISO, IETF, AFNOR, etc.). Attention à la confusion entre un standard et une norme. Le standard résulte d'un consensus plus restreint que pour la norme, il est élaboré entre des industriels au sein de consortiums (W3C, etc.) et non par des organismes nationaux ou internationaux. La différence est cependant faible et les Anglo-Saxons utilisent le terme « standard » pour désigner une norme.

1. Cadre commun d’interopérabilité du gouvernement du Québec

1.1 Introduction

La gouvernance et la gestion des ressources informationnelles à l'échelle du gouvernement du Québec représentent des enjeux majeurs pour les citoyens, les entreprises, les organismes et l'administration publique. À cet égard, la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement poursuit cinq objectifs, à savoir :

- Tirer profit des ressources informationnelles en tant que levier de transformation ;
- Investir de façon optimale et rigoureuse ;
- Optimiser la gestion de l'expertise et du savoir-faire ;
- Assurer la sécurité de l'information ;
- Tirer profit des logiciels libres.

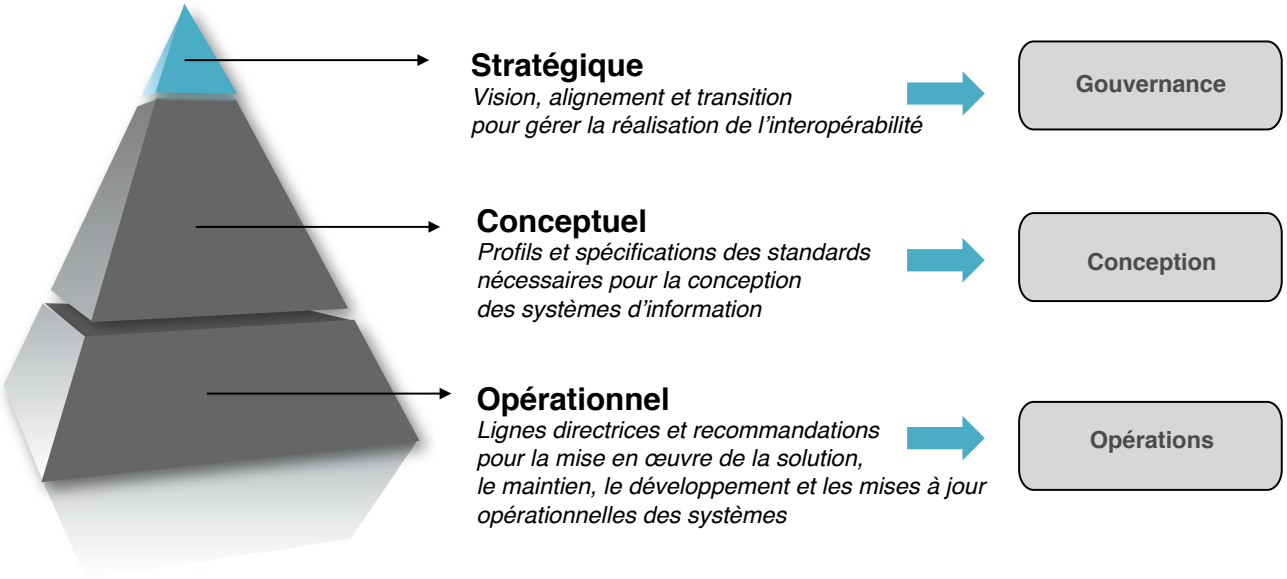
Pour réaliser ces objectifs et dans une perspective d'amélioration de la planification gouvernementale, le gouvernement a mis en place un ensemble de règles claires s'appuyant sur la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) sanctionnée le 13 juin 2011. Ces règles remplacent désormais celles édictées par certaines dispositions de la Loi sur l'administration publique (chapitre A-6.01) et de la Loi sur le ministère des Services gouvernementaux (chapitre M-26.1).

Avec la politique-cadre et la loi qui lui confère la portée requise, l'administration publique québécoise met à la disposition des dirigeants les outils nécessaires afin qu'ils puissent se soumettre aux orientations gouvernementales en termes d'amélioration des services, d'efficience en matière de ressources informationnelles et de pérennité du patrimoine numérique de leur organisation respective.

La pertinence de se doter d'un cadre normatif dans le contexte d'une initiative d'interopérabilité au sein du gouvernement du Québec se traduit selon plusieurs points de vue (figure 1):

- Point de vue stratégique – L'interopérabilité sur le plan stratégique est un moyen qui concrétise la vision gouvernementale en ce qui a trait à la gestion des ressources informationnelles (RI). Dans le contexte actuel marqué par des compressions budgétaires et l'orientation vers une gestion optimisée des projets en RI, la mise en place d'un cadre normalisant la réalisation de ces projets garantira le respect des objectifs stratégiques en termes de gouvernance.
- Point de vue conceptuel – L'adoption d'un cadre normatif définissant les profils et les spécifications des standards nécessaires pour la conception des systèmes d'information favorisera les interactions interorganisationnelles. En jouant un rôle de régulateur, ce cadre aidera à pallier la difficulté des échanges entre les systèmes et les organismes et permettra une meilleure exploitation des possibilités de partage et de réutilisation des RI et, de ce fait, une meilleure prestation électronique de services intégrée.
- Point de vue opérationnel – L'opérationnalisation du CCIGQ permet de simplifier, d'optimiser et d'intégrer les services proposés par les OP et, ainsi, de contribuer à l'amélioration des services rendus aux citoyens et aux entreprises. En plus, le respect des normes et des standards rend compatibles les différentes solutions technologiques et permet le choix entre les solutions commerciales et les solutions alternatives constituées par des logiciels libres dont la conformité aux normes est souvent excellente

- **Figure 1 Pertinence d'une initiative d'interopérabilité**



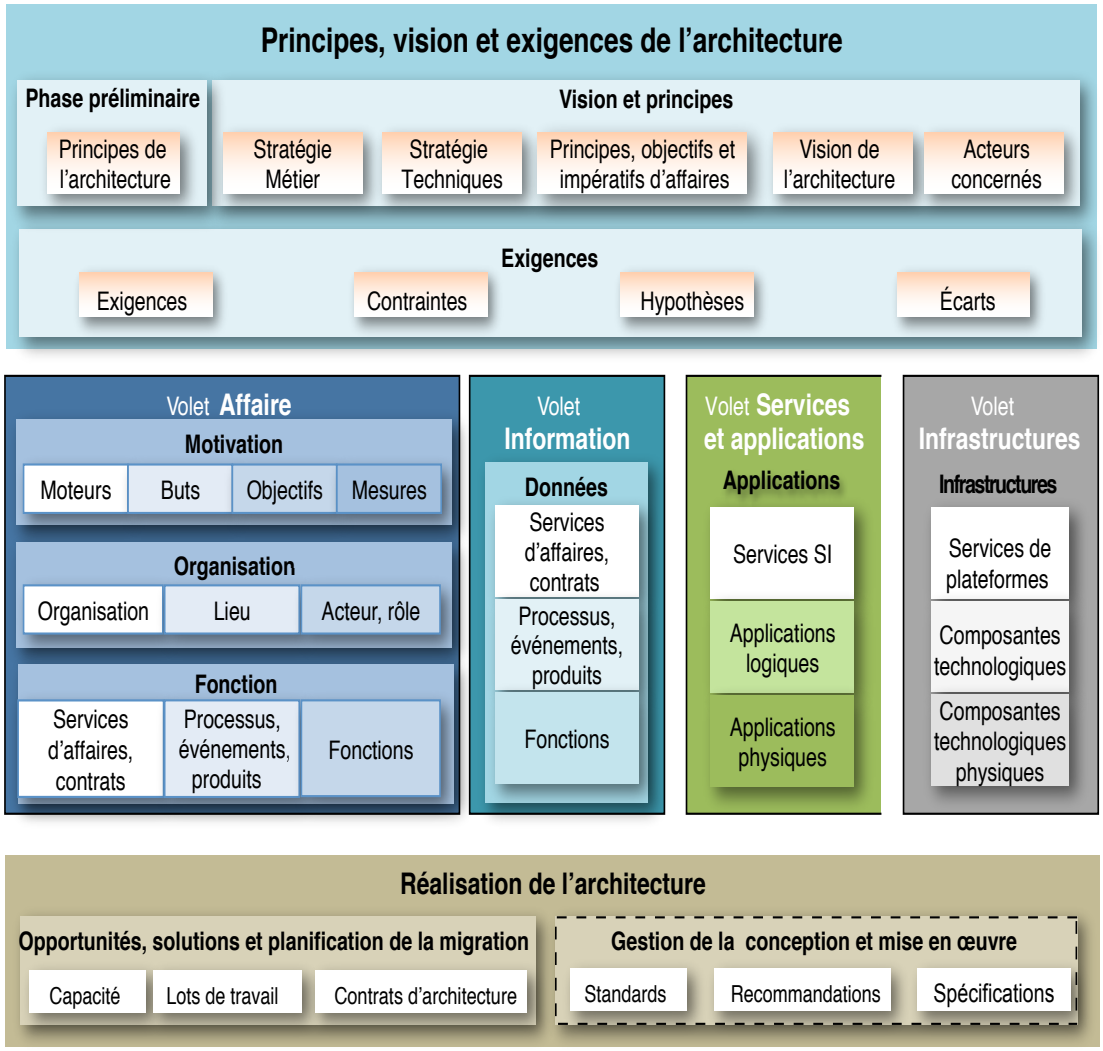
Fonder le CCIGQ sur des normes et des standards permet de conférer aux orientations une certaine pérennité qu'il est nécessaire de réévaluer chaque année. En effet, les normes évoluent et les besoins du gouvernement également. Tout comme la première version du CCIGQ, cette version résulte pour une part importante d'un travail interministériel. Les versions ultérieures devront évoluer également grâce à la contribution des différents organismes publics.

1.2 Interopérabilité dans l'écosystème gouvernemental québécois

Le CCIGQ est mis en application alors que de nombreuses réalisations en matière d'orientations gouvernementales sont déjà à l'œuvre. Dans sa version actuelle, il s'arrime au cadre de référence de l'architecture d'entreprise gouvernementale en version 3 (AEG 3.0). En particulier, chaque composante du CCIGQ est mise en relation avec le ou les volets auxquels elle se rapporte : Affaires, Services et applications, Information ou Technologie.

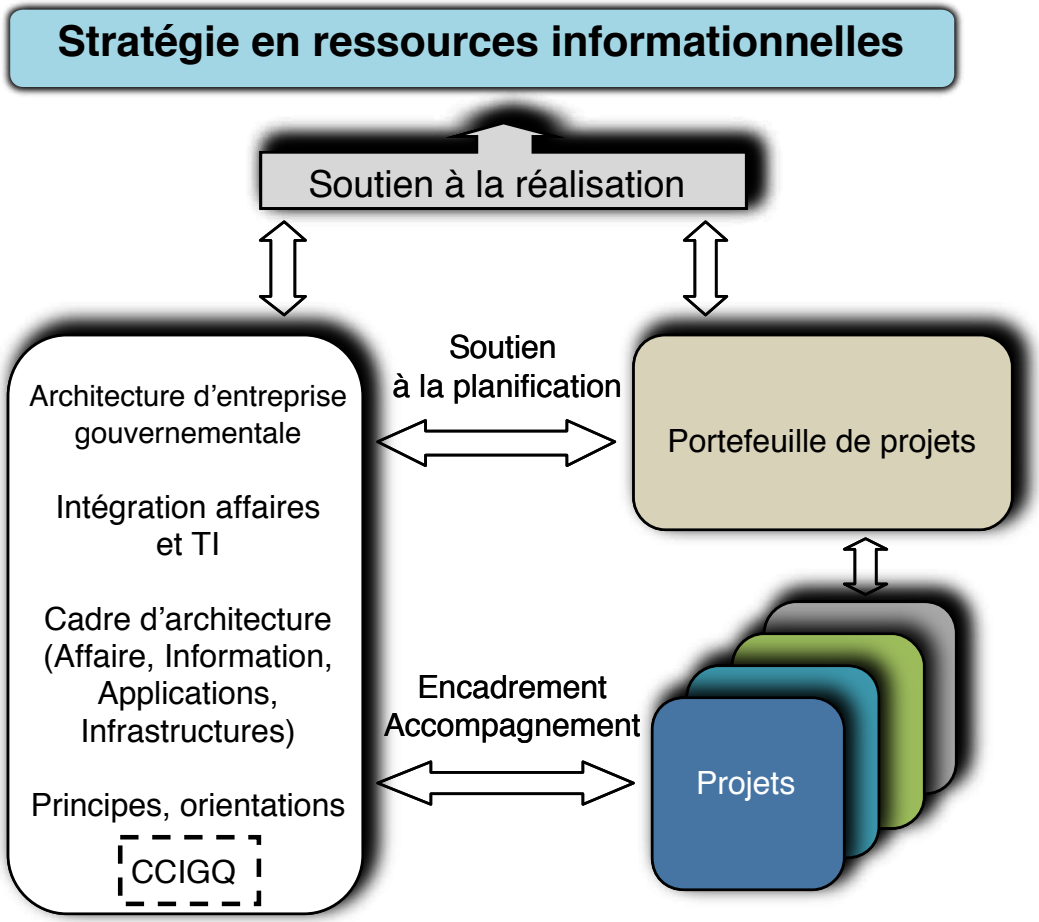
The Open Group Architecture Framework (TOGAF) est le cadre d'architecture adopté par le gouvernement du Québec. Dans sa version 9.1, il positionne l'interopérabilité sur le plan de la réalisation de l'architecture et, plus précisément, dans la gestion de la conception et de la mise en œuvre comme élément de fondation indispensable pour l'élaboration d'une architecture d'entreprise.

Figure 2 Positionnement du CCIGQ dans le cadre d'architecture proposé par le TOGAF 9.1



Dans le contexte du gouvernement du Québec, l'AEG 3.0 est un processus d'organisation visant à mettre en relation les orientations, les stratégies gouvernementales, les ressources informationnelles et les technologies de l'information et des communications. La figure qui suit met en évidence les relations entre ces différents éléments, notamment la stratégie en RI, le portefeuille de projets, le cadre d'architecture gouvernemental, les architectures à l'intérieur des OP et la mise en œuvre des différents projets.

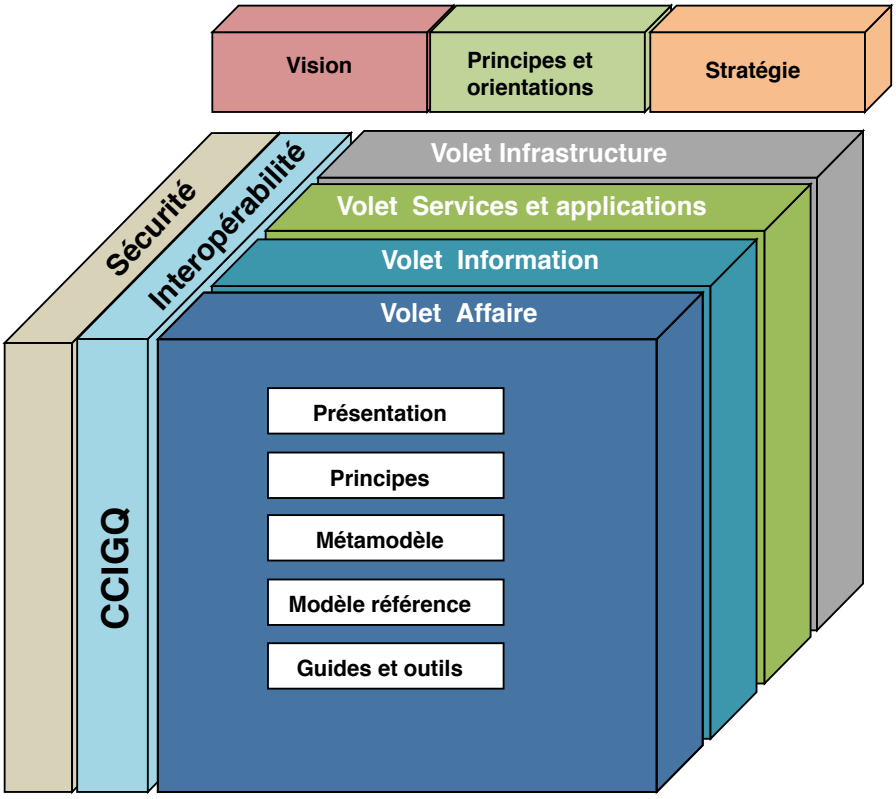
Figure 3 Portée de l'Architecture d'entreprise gouvernementale (AEG)



L'AEG soutient la réalisation de la stratégie gouvernementale, et ce, en contribuant à une gestion efficiente des budgets et des projets (portefeuille de projets) selon une vision intégrée des solutions d'affaires et des technologies associées au plan stratégique. L'AEG agit également comme un guide qui permet d'encadrer les OP dans le processus de réalisation de leurs projets en RI. Le CCIGQ étant un élément de fondation important de l'AEG, il apporte un soutien à la réalisation de ces projets en favorisant une cohérence et une meilleure exploitation des possibilités de partage et de réutilisation des RI.

L'AEG dans sa troisième version (AEG 3.0) est une structure composée de quatre volets, à savoir les volets Affaire, Information, Services et applications, et Infrastructures, et de deux segments : Interopérabilité et Sécurité (figure 4). Chaque volet contient une description, des principes, une vue du métamodèle de l'AEG 3.0, des modèles de référence, des guides et des outils.

Figure 4 Positionnement du CCIGQ dans l'AEG



En tant que segment transversal aux différents volets de l'AEG, l'interopérabilité couvre les normes, les standards, les pratiques et les méthodologies nécessaires pour chaque volet encadrant les OP qui souhaitent mettre en œuvre leur propre architecture d'entreprise corporative à travers des projets, favorisant ainsi leur arrimage avec l'AEG.

Dans la même perspective de normalisation des technologies de l'information, le DPI a élaboré un ensemble de standards touchant les RI (SGQRI), qui sont regroupés sur le site du Secrétariat du Conseil du trésor[3]. Ces derniers viennent complémenter le CCIGQ en couvrant d'autres champs : la sécurité, la navigabilité des sites Web, etc.

Si le CCIGQ tisse la toile de fond entre les normes et les standards internationaux ayant une incidence sur l'interopérabilité, il ne peut en revanche prétendre à l'exhaustivité en matière d'interopérabilité dans l'administration publique. Par exemple, des standards du gouvernement québécois pourront compléter le cadre commun d'interopérabilité par des rapports techniques, des pratiques recommandées ou des standards consensuels dans les cas suivants :

- En l'absence de normes et de standards à l'échelle internationale ;
- Lorsqu'un degré de détail plus fin est requis (notamment quant à la mise en œuvre de la norme et à l'évaluation de la conformité) ;
- Lorsque l'ajustement au contexte gouvernemental d'une norme ou d'un standard existant dans un profil est nécessaire.

3. http://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/standards-et-normes/

1.3 Portée

Le CCIGQ est considéré comme une référence qui contribue à l'amélioration des services offerts par l'ensemble des OP à leurs clients, et cela en établissant une vision commune de l'interopérabilité au sein de l'administration publique et en favorisant la simplification et l'intégration des services offerts. L'élaboration du cadre est tributaire de l'AEG 3.0 ; elle permet de répondre à cet objectif et, ultimement, d'améliorer le service que le gouvernement rend à ses cinq types de clients :

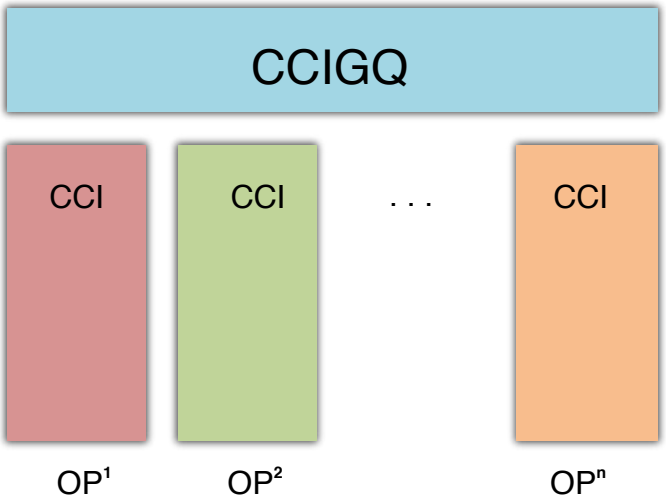
- Citoyen ;
- Entreprise ;
- Employé de l'État ;
- Organisme public ;
- Fournisseur partenaire.

Bien que les normes et les standards présents dans le CCIGQ contribuent à l'interopérabilité, il est pratiquement impossible de faire un catalogue qui couvre tout ce qui est requis pour l'implémentation et la configuration des systèmes d'information sans que ce catalogue soit difficile à lire et à mettre en application. Par conséquent, il est important de savoir que le CCIGQ en soi n'est pas suffisant pour réaliser l'interopérabilité.

Dans le présent cadre, les normes et les standards d'interopérabilité propres aux organismes publics ne font pas partie du CCIGQ qui a une portée gouvernementale et un caractère transversal. Par conséquent, les normes et les standards appliqués dans certains domaines comme la santé (p. ex. : HL7, SNOMED CT, etc.) ou l'éducation (p. ex. : MARC, LODE, etc.) ne font pas partie du CCIGQ (figure 5), mais ils doivent être intégrés aux cadres communs d'interopérabilité (CCI) corporatifs des organisations[4].

4. On entend ici par CCI corporatif le cadre normatif de l'organisme public garantissant l'interopérabilité interne.

Figure 5 Portée du CCIGQ



Les CCI propres aux OP sont considérés comme des prolongements du CCIGQ. Il est donc important que les deux cadres soient cohérents et complémentaires. Si un élément d'un CCI d'organisation devient commun à tous les organismes publics, il sera un candidat potentiel pour faire partie du CCIGQ.

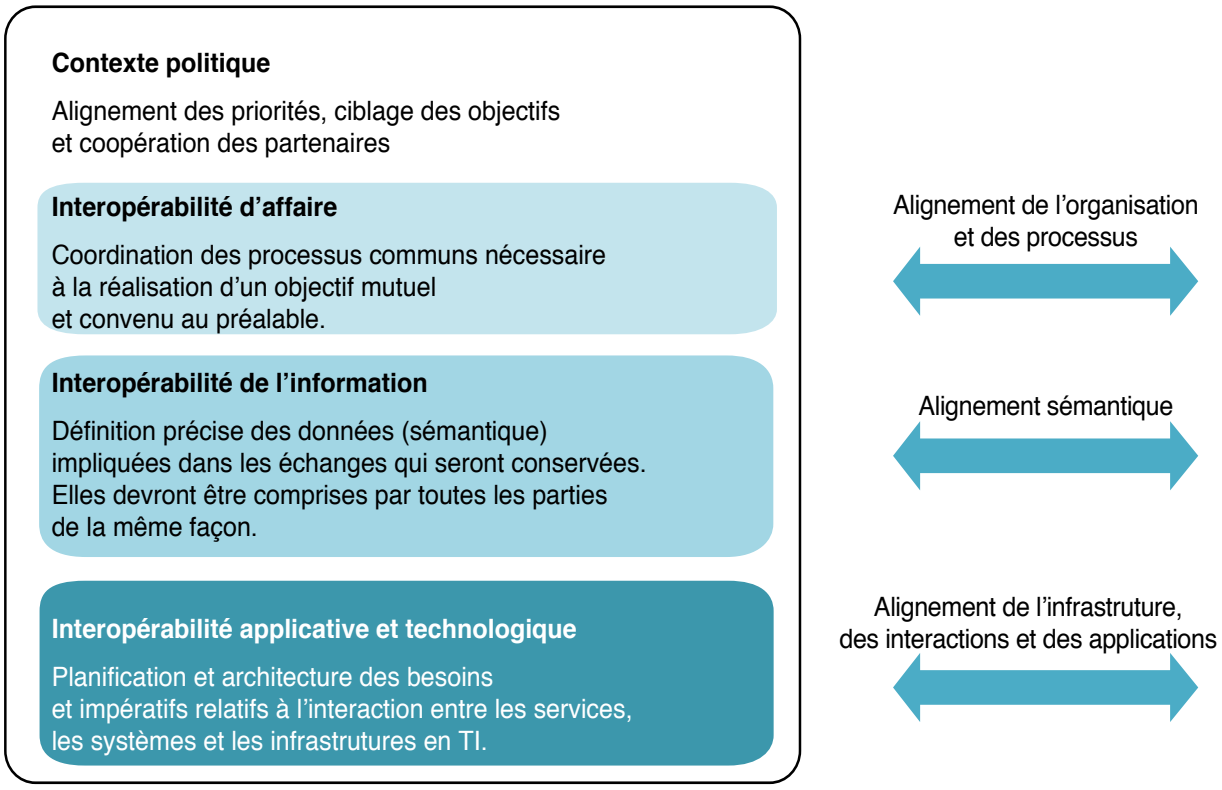
Le document n'explique pas les critères qui garantissent la bonne utilisation des normes et des standards spécifiés. L'aspect de leur utilisation est plutôt couvert dans les documents de référence à ces normes et à ces standards, tels que décrits par l'organisme de normalisation qui s'en charge. Cependant, le CCIGQ souligne, lorsque cela est jugé important, les points qui pourraient constituer des entraves à l'interopérabilité ou bien les aspects qui se rapportent à la coexistence des normes et des standards préconisés. La mise en œuvre du contenu du CCIGQ n'a pas été traitée dans le présent cadre, mais elle le sera dans des versions ultérieures.

1.4 Structure et contenu du CCIGQ

Dans son contenu, le CCIGQ découpe le système d'information du gouvernement du Québec en trois volets[5] soutenus par une sécurité transversale. Il sélectionne pour chacun les normes, les standards, les démarches et les méthodologies qui permettront d'assurer une interopérabilité technologique, informationnelle et organisationnelle.

5. Le volet 1 traite de l'interopérabilité sur le plan des affaires, le volet 2 de l'interopérabilité de l'information et le volet 3 de l'interopérabilité technologique.

Figure 6 Modèle de référence du CCIGQ



Le CCIGQ s'inscrit dans le cadre de l'AEG et reflète ainsi sa structure d'architecture à quatre volets. Dans cette version, le volet Services et applications et le volet Infrastructure ont été fusionnés en un seul volet d'interopérabilité nommé « Interopérabilité applicative et technologique ».

1.4.1 Interopérabilité d'affaires

L'objectif de ce volet d'interopérabilité est, d'une part, de fournir un cadre fonctionnel permettant de guider et d'accompagner les conseillers en architecture d'entreprise afin d'assurer la compréhension commune des différents processus d'affaires gouvernementaux et, d'autre part, d'offrir aux organismes publics les éléments permettant la communication entre les méthodes de conception de systèmes et les supports de modélisation. En plus, la notion de processus – de bout en bout, dans une vision client de l'organisation de services d'affaires – est proposée pour assurer une vision unique et cohérente de la prestation de services intégrée, tout en masquant la complexité organisationnelle des entités des organismes publics qui la composent.

1.4.2 Interopérabilité de l'information

Avoir une compréhension commune de l'ensemble des données utilisées à l'occasion des échanges interorganisationnels est désormais une nécessité pour le gouvernement du Québec. Ce dernier considère l'information gouvernementale comme un actif stratégique dont l'organisation cohérente et la gestion efficace contribuent à la transformation et à l'amélioration continue de l'administration publique ainsi que de la prestation des services. Se doter d'un cadre

de référence permettant de normaliser cette information gouvernementale est un atout pour la réutilisation et le partage de l'information conformément à la vision gouvernementale. Dans la présente version du CCIGQ, seul l'aspect sémantique de l'interopérabilité de l'information est considéré. Une démarche basée sur des concepts présentés dans le volet Information de l'AEG 3.0[6] (modèle gouvernemental conceptuel de données [MGCD], modèle corporatif conceptuel de données [MCCD], modèle de lien, etc.) est présentée.

1.4.3 Interopérabilité applicative et technologique

Dans ce cadre sont réunis l'ensemble des normes et des standards relatifs aux enjeux d'interopérabilité associés aux volets Applications et Infrastructures de l'AEG 3.0. Des critères de sélection et des orientations ont été utilisés et une classification inspirée de différents modèles de référence reconnus internationalement a été élaborée pour présenter les normes et les standards inventoriés. Un modèle a été conçu pour illustrer la classification des normes par niveau ainsi que les interrelations entre les niveaux.

Dans un premier temps, le modèle *Open Systems Interconnection*[7] (OSI) a été utilisé pour définir le niveau « interconnexion ». Ce niveau regroupe les normes associées à l'interconnexion de systèmes hétérogènes afin d'assurer une communication efficace entre systèmes ouverts[8]. Toutefois, ce modèle seul ne peut pas couvrir tous les niveaux d'interopérabilité technique, en particulier ceux associés aux services Web qui sont plus larges qu'une simple connexion entre deux entités ou composantes.

Au niveau précédent a été ajouté le niveau « intégration » qui traite des normes et mécanismes assurant l'intégration des données des applications et des services Web. Les modèles SOAP/XML[9], WSDL[10], etc. ont été utilisés ensuite pour présenter les normes et les standards associés aux services Web, des modèles conçus pour permettre la création d'un riche environnement de services.

De plus, un troisième niveau, « formats et structures », a été proposé pour identifier les normes sur le plan des caractéristiques de l'information à échanger, tant du point de vue transactionnel que de celui de la gestion de processus. Finalement, cette section est complétée par les « profils de services » qui cartographient les normes et les mécanismes technologiques qui seront utilisés par différents types de services gouvernementaux. Ils sont présentés sous la forme de profils normatifs.

---

6. Pour plus d'information, sur le document intitulé *AEG 3.0 : volet Information, modèle de référence et guide de conception* (418 643-0875, poste 5021).
7. http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=17473
8. Le terme système ouvert désigne dans ce document des systèmes informatiques qui fournissent un ensemble d'avantages en interopérabilité, portabilité, et standards ouverts de logiciel (Wikipedia).
9. **S**OAP, **S**imp**l**e Obje**ct** A**cc**e**ss** Prot**oc**o**l**, e**st** une **sp**é**cifica**ti**o**n de pro**t**o**co**l**e pour é**ch**anger de**s i**nforma**ti**o**ns st**ruc**t**urée**s** dan**s l**a m**i**s**e** en œu**v**re de **s**er**vice**s** Web **s**ur de**s** ré**s**eaux **i**nforma**ti**que**s**. E**ll**e **s**'appu**i**e **s**ur **l**e XML, *Ext**ens**ible Mar**k**up Language*, pour **l**a déf**ini**t**i**on du forma**t** de me**ss**age, e**t** repo**s**e généra**l**emen**t s**ur d'au**tre**s pro**t**o**co**l**e**s de **l**a **c**ou**ch**e d'app**lica**t**i**on du Modè**l**e O**SI** (H**TT**P ou **S**M**T**P) pour **l**a négo**cia**t**i**on de **l**a **c**onnexi**o**n e**t l**a **t**ran**s**m**issi**on de do**c**umen**t** XML.
10. WSDL : *Web Service Description Language*.

1.4.4 Sécurité

La sécurité et la protection des renseignements personnels ou autrement confidentiels sont des obligations importantes pour les OP qui administrent des services publics. D'où la nécessité d'utiliser des normes et standards de sécurité adéquats et interopérables afin d'accroître l'efficacité et la cohérence des actions en la matière.

Comme le montre la figure 6, la sécurité a une portée transversale aux trois volets mentionnés précédemment. Ainsi, au volet Affaires, elle contribue à la définition des processus de collaboration entre les OP et leurs partenaires afin de réaliser les objectifs de sécurité fixés pour le service commun d'échanges sur le Web, tout en prenant en considération les risques et les objectifs d'affaires. Au volet Information, elle établit la définition précise des informations de sécurité (normalisation) associées aux processus, aux applications ainsi qu'aux activités de supervision et de reddition de comptes. Au volet Applications et Technologie, elle vise l'identification des services et mécanismes de sécurité afin d'assurer la sécurité des services d'échanges sur le Web relativement aux aspects techniques suivants : interfaces ouvertes, interconnexion, intégration des données, présentation et échange des données de même que l'accessibilité.

Finalement, il faut rappeler que le cadre normatif de sécurité du service d'échanges sur le Web à mettre en place sera tributaire du contexte propre aux différentes parties prenantes. Au préalable, celles-ci devront s'entendre sur les visions, les objectifs, les principes, les orientations et les niveaux de sécurité requis pour protéger les informations échangées.

1.5 Évolution du document

Chaque année, une réévaluation de l'actualité et de la modernité du contenu du CCIGQ est réalisée et, selon le degré de désuétude des normes et des standards qui le constituent, la décision de le mettre à jour sera prise.

Les OP, en tant que partenaires, sont appelés à participer à la mise à jour du CCIGQ afin que le cadre commun réponde davantage à leurs besoins, et cela, dans la limite de la portée du cadre, la cible étant de faire en sorte que le CCI des organisations devienne la source qui alimente, d'une façon dynamique, les normes et les standards du CCIGQ.

À l'occasion d'une demande de modification ou d'un ajout dans le CCIGQ, il faut s'assurer que le changement demandé n'enfreint pas les règles et les principes adoptés dans le cadre. Le DPI se réserve le droit de rejeter toute demande de changement jugée non conforme aux règles et aux principes énumérés dans le présent cadre.

À plus long terme, la cible serait de faire en sorte que le cadre commun d'interopérabilité des organisations devienne la source qui alimente, d'une façon dynamique, les normes et les standards du CCIGQ.

2. Interopérabilité applicative et technologique

2.1 Introduction

L'interopérabilité a besoin de plus qu'une connectivité technique reposant sur un ensemble de protocoles (réseaux, transfert, transport, etc.). Elle repose sur l'utilisation des interfaces de programmation, des formats de données standardisés et des profils de normes et de standards spécialisés pour assurer des services communs sécuritaires et utiles à l'ensemble de l'administration publique.

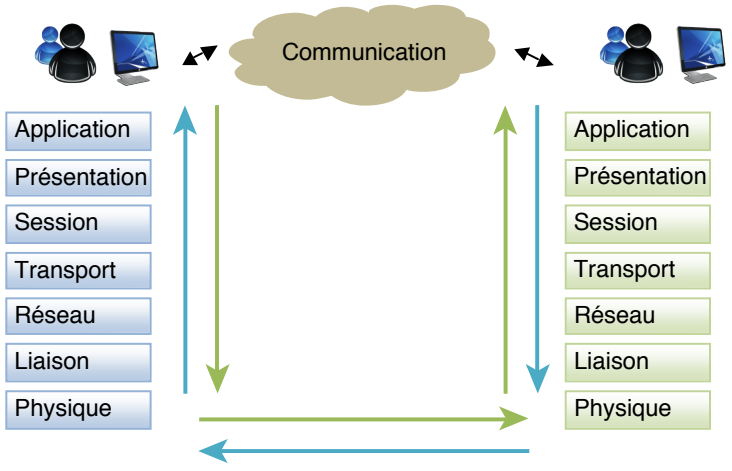
L'interopérabilité définie ici est applicative et technologique. Dans cette version du CCIGQ, les volets d'interopérabilité relatifs à l'architecture technologique, aux services et aux applications sont fusionnés. L'idée d'avoir deux sections indépendantes dépend fortement de l'avancement des travaux de l'AEG 3.0.

Ce volet de l'interopérabilité recense l'ensemble des normes et des standards techniques utilisés dans une communication inter-organisationnelle. La portée de cette version du CCIGQ couvre seulement les interactions entre OP. Un élargissement de la portée est envisageable dans les prochaines versions pour englober les clients du gouvernement, c'est-à-dire les citoyens et les entreprises.

2.2 Catégorisation

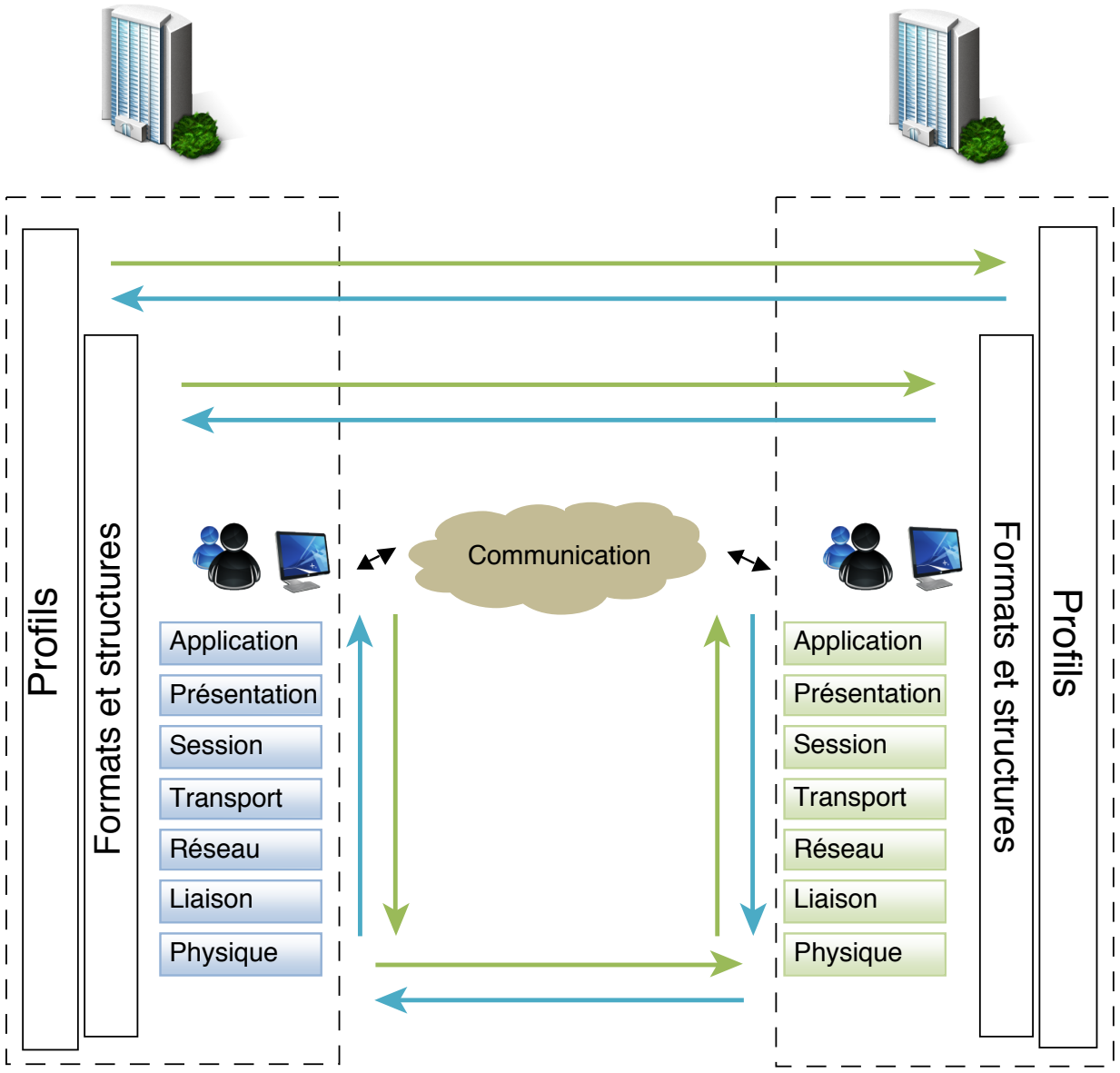
Pour bien positionner le volet applicatif et technologique du CCIGQ dans son cadre et pour faciliter sa lecture, et surtout son utilisation, les normes et les standards qui le composent sont classés selon leur fonction et leur contenu. Cette classification est faite de telle sorte qu'ils interagissent tout au long d'un processus de communication ou d'échange de données. À cet effet, un modèle de référence a été élaboré selon une structure s'inspirant des protocoles d'Internet. Il s'agit notamment de la norme OSI (*Open System Interconnexion,* ISO 7498) indiquée à la figure 7. De plus, de par la portée de l'interopérabilité, il était nécessaire d'enrichir le modèle en considérant d'autres protocoles d'Internet ainsi que ceux propres à la sécurité. Il s'agit des protocoles Web W3C et OASIS.

Figure 7 Modèle OSI



La figure suivante illustre le découpage retenu pour le modèle d'interopérabilité des services et des échanges d'information au gouvernement du Québec.

Figure 8 Modèle de référence pour le volet Applications et Infrastructures du CCIGQ



Ce découpage a permis de faire ressortir les principales composantes du modèle de référence. Il en résulte trois niveaux d'interopérabilité, un aspect de sécurité transversal ainsi que les profils normatifs des services.

1. Niveaux d'interopérabilité

Ce niveau traite des exigences d'interopérabilité auxquelles doivent se soumettre les composantes des systèmes informatiques et les systèmes de télécommunications des organismes publics du

gouvernement du Québec pour pouvoir communiquer entre eux, notamment pour le soutien des services internes et pour la prestation électronique de services.

Interconnexion

L'interconnexion couvre principalement les normes et les standards associés aux différentes couches du modèle OSI :

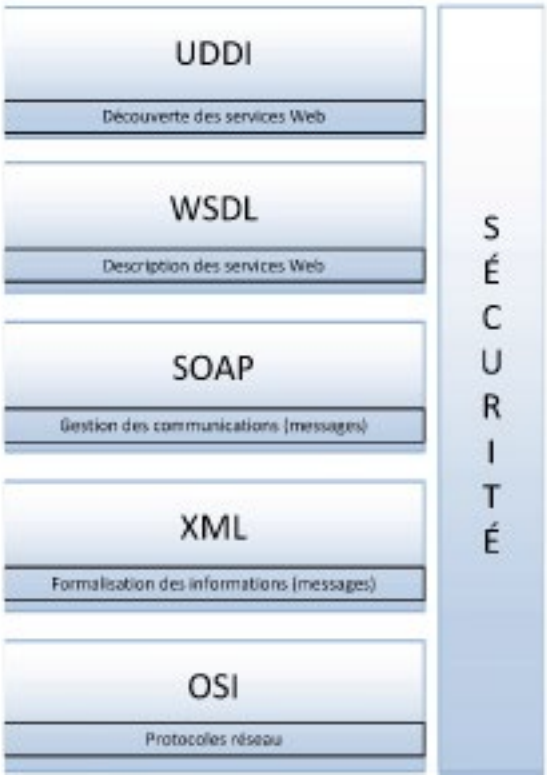
- Couche physique ;
- Couche liaison ;
- Couche réseau ;
- Couche de transport ;
- Couche de session ;
- Couche présentation ;
- Couche d'application ;

Intégration

Les services basés sur Internet, y compris les services électroniques gouvernementaux, sont disponibles dans une multitude de formes et d'apparences et offrent une variété de possibilités d'interaction. L'interopérabilité technique couvre, en plus, des aspects techniques de connexion pour l'échange d'information entre un fournisseur et un consommateur d'information ainsi que la liaison des applications. Ce niveau gère les interactions entre les applications[11] ; il repose sur une infrastructure de communication (SOAP/HTTP) et supporte un ensemble de standards de services Web (XML, WSDL) tel que présenté à la figure 9. Ce niveau comprend les aspects clés tels que la communication entre programmes, les échanges de messages, les interfaces ouvertes et normalisées, les intergiciels, la gestion des processus, la présentation des données ainsi que l'accessibilité.

11. C'est à ce même niveau que l'on retrouverait les normes et standards associés au modèle Corba si le cadre traitait du modèle de coopération entre objets répartis.

Figure 9 Normes des services Web (W3C et OASIS)



Formats et structures

Ce niveau s'intéresse aux normes et aux standards qui permettent de présenter du contenu aux utilisateurs. Les normes et les standards touchant l'aspect de la présentation favorisent l'échange et le partage d'information (documents textes, graphiques, multimédias, etc.) entre les systèmes. Les aspects couverts principalement par ce niveau sont :

- Format ;
- Encodage ;
- Structuration et traitement des données structurées.

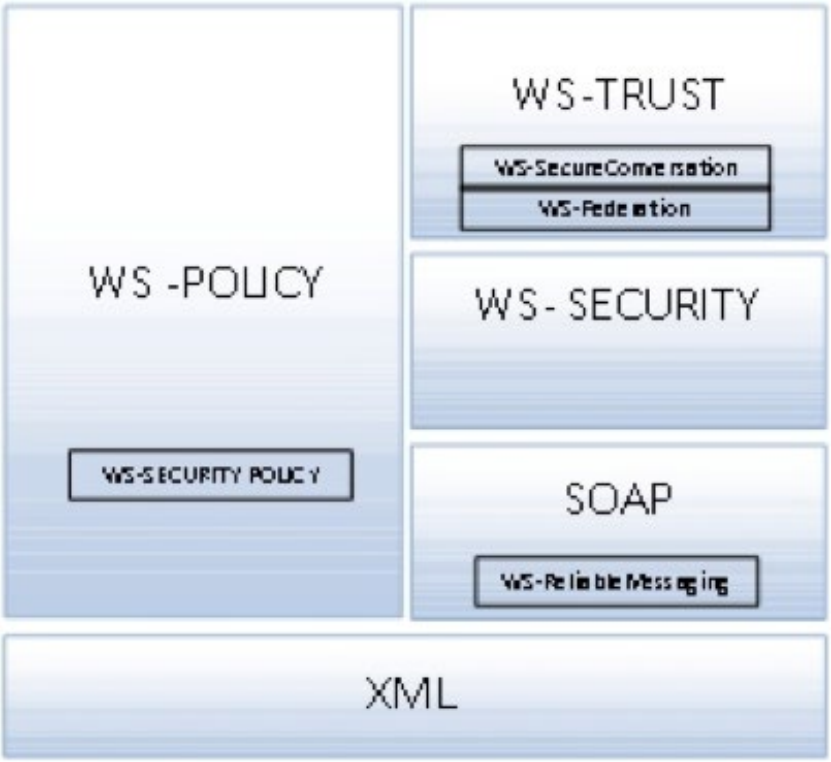
2. Sécurité

La sécurité repose sur les normes et standards permettant d'assurer la sécurité des plateformes de services d'échange ou Web tout en veillant à la protection des renseignements personnels et la confiance des usagers à l'égard de ces services. La figure 10 présente les normes associées aux services Web, auxquelles il faut ajouter les protocoles relatifs aux différentes couches du modèle OSI ainsi que les mécanismes de chiffrement.

Les normes et protocoles retenus le sont en partant du principe de conformité aux normes internationales communément admises en matière de sécurité des communications et des services. De plus, une analyse comparative des normes et des spécifications mentionnées dans les cadres nationaux d'interopérabilité, principalement de France, d'Allemagne, du Royaume-Uni et de l'Australie, a été réalisée. Le travail d'analyse a permis d'examiner les aspects techniques

des différents cadres nationaux clés, dont la sécurité. L'exercice a mis en évidence le grand degré de convergence dans les choix techniques que ces pays ont faits.

Figure 10 Normes de sécurité des services Web de type SOAP



3. Profils normatifs de service

Les profils des normes et des standards soutiennent l'ensemble des services gouvernementaux. Dans cette version, seuls quelques types de services sont considérés. Toutefois, une fois les principaux services communs gouvernementaux cartographiés, le même exercice sera fait pour tous les services.

Les types de services considérés par ce niveau sont :

- Services de messagerie électronique;
- Services multimédias;
- Architecture orientée services[12].

Le choix de cette approche de découpage répond à un double objectif. En plus de regrouper les normes et les standards selon leur fonction en catégories claires et logiques, ce découpage garantit la traçabilité facile des différents standards et normes.

Afin de simplifier la lecture et surtout l'évolution du cadre, la version d'une norme ou d'un standard est précisée seulement dans les spécifications. Ainsi, le changement d'une version, qui est plus

12. Il est possible de définir l'architecture orientée services (AOS) d'un point de vue d'architecture d'entreprise comme un style architectural visant à organiser et à utiliser des services (Web ou autres) afin de soutenir l'interopérabilité entre les données et les applications de l'organisation.

fréquent que le cycle de mise à jour du CCIGQ, ne constituera pas une contrainte nécessitant la relance du processus de normalisation.

2.2.1 Critères de sélection

Pour faire partie du volet applicatif et technologique du CCIGQ, une norme ou un standard doit être :

1. Ouvert

L'utilisation de standards et de formats ouverts offre plusieurs avantages comme :

- Assurer l'interopérabilité des systèmes ;
- Éviter la dépendance exclusive à l'égard de fournisseurs et ainsi favoriser un marché compétitif ;
- Assurer la pérennité des données ;
- Offrir la liberté de choix aux clients et aux partenaires qui interagissent avec le gouvernement.

Cependant, il n'existe pas de définition universelle du terme « standard ouvert ». Il apparaît donc important que le gouvernement statue sur sa propre définition du standard ouvert et qu'il utilise cette définition dans le choix des standards qu'il retiendra.

Le choix d'une bonne définition est essentiel, car plusieurs administrations publiques ont, par le passé, été critiquées par les éditeurs de produits propriétaires. Il a été convenu d'utiliser une définition existante, soit celle adoptée par la France (2004), pour sa simplicité, et d'y ajouter les caractéristiques retenues par le Royaume-Uni, lesquelles ont fait l'objet d'une longue et sérieuse consultation en 2011-2012.

Définition :

On entend par « standard ouvert » tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérables, dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre.

Caractéristiques :

- Collaboration – le standard est élaboré par un processus décisionnel collaboratif sur la base d'un consensus indépendant de tout fournisseur. L'engagement dans le développement et l'évolution du standard est ouvert à toutes les parties intéressées ;
- Transparence – le processus décisionnel est transparent (accessible au public) et fait l'objet d'un examen par des experts en la matière ;
- Procédure régulière – le standard est adopté par un organisme de normalisation, un forum ou un consortium, et un processus de rétroaction ainsi que d'approbation permet d'en assurer la qualité ;
- Accès équitable – le standard est publié, soigneusement documenté et accessible au public, soit gratuitement, soit pour un coût modique ;

- Soutien du marché – à l'exception d'un contexte de solutions innovantes, le standard est mature, il a le soutien du marché et il a démontré son indépendance par rapport aux plateformes, aux applications et aux fournisseurs ;
- Droits – pour assurer notamment l'interface avec d'autres implémentations qui ont adopté le même standard, les droits essentiels à la mise en œuvre du standard sont autorisés sur une base libre de redevances qui est compatible avec les solutions en logiciels libres et les solutions sous licences propriétaires. Ces droits doivent être irrévocables, sauf en cas de violation des conditions de la licence.

L'adoption de ce critère de sélection tire son origine de l'orientation gouvernementale à considérer le logiciel libre au même titre que le logiciel propriétaire. Pour concrétiser cette orientation, il est proposé que le choix des normes et des standards à retenir dans le CCIGQ donne la priorité aux normes et aux standards ouverts selon la définition adoptée par le gouvernement du Québec.

2. Pertinent

La pertinence, au sens gouvernemental, d'une norme ou d'un standard fait référence à son utilité et à sa nécessité quant à une interaction interorganisationnelle, et cela, indépendamment du fait que la norme ou le standard est reconnu ou non.

3. Mature

La maturité d'une norme ou d'un standard est définie selon les meilleures pratiques de gestion et par rapport à un ensemble clair de références externes. Dans le contexte gouvernemental québécois, une norme ou un standard est dit mature si, en plus d'être bien établi et soutenu par les infrastructures technologiques, il a démontré sa fiabilité à la suite de son application.

4. Indépendant

Une norme ou un standard faisant partie du CCIGQ devrait être indépendant de toute infrastructure technologique, logiciel ou bien matériel. Son choix ne devra pas imposer des restrictions d'acquisition à l'organisme qui l'adopte.

5. Facile à déployer

Le déploiement d'une norme ou d'un standard du CCIGQ ne doit pas être contraignant et engendrer des coûts de déploiement supplémentaires. Le respect de ce critère assurera une meilleure application du CCIGQ.

6. Soutenu par l'industrie

Une norme ou un standard répondant à ce critère de sélection doit être bien établi dans l'industrie et s'être bâti une solide réputation dans le domaine auquel il se rattache. On entend ici par « soutien de l'industrie » l'adoption de la norme ou du standard ainsi que le soutien qu'il offre.

2.2.2 Statuts adoptés

Pour les éléments de chaque couche, un tour d'horizon est accompli pour reconnaître les normes et les standards en considérant leur maturité pour gérer le risque lié à leur adoption. Un statut est attribué à chaque norme ou standard sélectionné dans un objectif de flexibilité d'application du CCIGQ. Pour tout ce qui existe déjà, la conformité à un seul choix de standard s'avérerait restrictive, contraignante et elle nécessiterait parfois même une refonte du système. Avoir recours aux statuts garantira la transition entre les différentes versions d'une même norme ou d'un même standard. Pour alléger cette version, le statut « admissible dans une version antérieure » utilisé dans l'ancienne version du CCIGQ a été omis. Les statuts retenus pour la présente version sont les suivants :

- Statut « À considérer »

Les normes et les standards sont à prendre en considération s'ils ont été essayés et testés. Ces normes et standards sont à privilégier dans la mesure du possible. Leurs applications ne doivent pas être contraignantes ou nécessiter des travaux majeurs comme une refonte du système. De plus, dans certains cas, une norme ou un standard peut ne pas être assez mature pour être retenu. En revanche, cette maturité peut se développer avec le temps, permettant ainsi une potentielle admissibilité.

- Statut « À retenir »

Les normes et les standards sont à retenir s'ils ont été essayés, testés, considérés comme la solution privilégiée, s'ils sont établis sur le marché et répondent à tous les objectifs du CCIGQ. Ces normes et standards doivent être respectés et appliqués en priorité.

2.2.3 Gabarit de présentation des normes et standards

Chaque élément du CCIGQ est présenté de la même façon. Dans cette version, afin de simplifier le texte en l'axant sur l'orientation à préconiser, les éléments d'analyse et de contexte ont été enlevés. On considère seulement l'orientation et les spécifications de la norme ou du standard sélectionné. Quant aux spécifications des normes et des standards, on précise l'origine, l'organisme qui les soutient, ses fonctions ainsi que les avantages de leur utilisation.

3. Normes et standards du volet applications et infrastructures

3.1 Niveau interconnexion

3.1.1 Couche réseau

IPv6 – À prendre en considération

IPv6 est la nouvelle génération de protocole Internet ; il est en train de remplacer IPv4. Il apporte de nombreuses améliorations, notamment :

- La simplification du routage et des en-têtes ;
- L'adressage plus large : espace d'adresse sur 128 bits versus 32 bits pour IPv4 ;
- La sécurité intégrée ;
- L'amélioration de l'autoconfiguration des réseaux.

Dans un contexte marqué par la tendance générale sur le marché vers une conversion à l'IPv6, il est fortement suggéré de :

- Retenir IPv6 qui est assez mature pour être déployé et prendre en considération la version IPv4, compte tenu du parc installé ;
- Vérifier, avant tout nouveau déploiement de solutions (interconnexion de réseaux, mise en œuvre de nouveaux services réseaux), que le soutien d'IPv6 est assuré et que l'interopérabilité avec IPv4 est fonctionnelle ;
- Envisager les scénarios de migration d'IPv4 vers IPv6.

IPv4 – À retenir

Les adresses IPv4 sont quasiment épuisées ; il est donc fortement suggéré aux organismes publics de migrer vers la version IPv6 et de tenir compte de l'interopérabilité d'IPv4 au moment des échanges. L'adressage interne des organismes publics doit être conforme au *Request for Comment* RFC 1918. Aucune adresse IP (du RFC 1918) ne doit circuler sur Internet.

IPsec – À prendre en considération

Voir la section sur la sécurité.

3.1.2 Couche transport

RTP / RTCP – À retenir

Real-Time Transport Protocol (RTP) est un protocole de communication, intégré dans H323, permettant le transport de données en temps réel. Il est à utiliser dans le cadre d'un déploiement de la voix sur IP ou d'applications multimédias. Il fait partie de la recommandation H.323, plus particulièrement de la recommandation H.225, UIT-T SG16 portant sur les protocoles de signalisation et de « paquétisation »[13] des flux multimédias issus d'un système H.323. Ce protocole serait à retenir même hors du contexte H.323/H.225 (avec SIP [*Session Initiation Protocol*], par exemple).

TCP – À retenir

La suite TCP/IP est le standard commun pour les interconnexions entre réseaux de technologies variées. TCP contrôle l'état de la transmission entre deux machines et le séquencement des paquets IP grâce au système d'accusés de réception. TCP est à retenir puisqu'il demeure le vecteur le plus fiable de HTTP, de SMTP et de FTP.

UDP – À retenir

UDP est l'un des principaux protocoles de télécommunication utilisés par Internet. Il possède des en-têtes beaucoup moins lourds que TCP. Cependant, il n'offre aucun contrôle sur le flux d'information, mais il reste très utilisé dans les applications multimédias.

3.1.3 Couche session

Open SSH – À retenir

SSH (*Secure Shell*) est un protocole recommandé aux organismes publics pour assurer la sécurité des connexions entre deux systèmes. C'est un protocole bien établi. Il existe tant en version commerciale qu'en version libre (*Open SSH*). Le protocole SSH est approprié pour accéder à tout type de serveur lorsque le chiffrement de la session est nécessaire.

3.1.4 Couche présentation

Voir les sections 3.3.1 Formats (Contenu Web) et 3.3.3 Structuration et traitement des données structurées.

13. La « paquétisation » désigne l'opération de transformation du flux en paquet transmis séparément à la couche réseau (couche 3 du modèle OSI).

3.1.5 Couche application

- ### Protocoles de communication

HTTP 1.1 – À retenir

HTTP est un protocole de communication client-serveur. Il est recommandé d'utiliser HTTP 1.1 dans tout nouveau développement et de conserver FTP uniquement pour les échanges qui n'ont pas besoin d'être sécurisés. La RFC 2774 propose un cadre d'extension au protocole HTTP qui va prendre une importance considérable avec les services Web. La RFC 2965 introduit un mécanisme de maintien de sessions nécessaire aux services Web.

HTTPS – À retenir

Voir la section sur la sécurité.

FTP – À retenir

FTP (*File Transfer Protocol*) est un protocole de communication destiné à l'échange de fichiers sur un réseau TCP/IP. Le protocole FTP ne permet pas toujours d'assurer l'interopérabilité entre plateformes différentes. Seuls les logiciels serveur et client respectant le standard RFC 2640 en donnent la garantie grâce à l'utilisation de l'encodage UTF-8 et, accessoirement, d'une nouvelle commande LANG qui permet de choisir la langue des messages retournés par le serveur au cours de la session FTP.

FTPS – À retenir

Voir la section sur la sécurité.

SFTP – À retenir

Voir la section sur la sécurité.

SMB 2 – À retenir

SMB (*Server Message Block*) est un protocole réseau utilisé principalement pour fournir un accès partagé aux fichiers, aux imprimantes, aux ports série et aux divers échanges entre les nœuds d'un réseau. En 2006, avec l'arrivée de Windows Vista puis de Windows 7, Microsoft a mis au point une version 2 du protocole, plus rapide. Le standard SMB est à retenir car il peut cohabiter avec le standard FTP dans les cas d'intégration et d'échange de fichiers. Exemple : un serveur FTP avec un serveur SMB-SAMBA.

- ### Protocoles orientés multimédia

RTSP – À retenir

Les protocoles RTSP (*Real Time Streaming Protocol*) sont destinés aux systèmes de contenu multimédia en temps réel (*streaming media*). Ils permettent de contrôler un serveur de média à distance. RTSP ne transporte pas les données elles-mêmes et doit être associé à un protocole de transport comme RTP pour exécuter cette tâche. Ces protocoles seraient à retenir même hors du contexte H.323/H.225 (avec SIP, par exemple).

SIP – À considérer

Session Initiation Protocol (dont le sigle est SIP) est un protocole de la couche applicative et non de la couche session comme son nom pourrait le laisser croire. Il est normalisé et standardisé par l'IETF (*Internet Engineering Task Force*), décrit par le RFC 3261, qui rend obsolète le RFC 2543, et il est complété par le RFC 3265 qui a été conçu pour établir, modifier et terminer des sessions multimédias.

H.323 – À retenir

H.323 développé par l'UIT-T, défini comme « Systèmes de communication multimédia en mode paquet », est le protocole le plus stable et le plus utilisé en téléphonie. Il concerne principalement les standards de visioconférence sur les réseaux locaux. En plus, il est largement implanté sur le marché.

MGCP – À retenir

Le protocole MGCP (*Media Gateway Control Protocol*) permet de contrôler les passerelles multimédias (*Media Gateways*) qui assurent la conversion de la voix et de la vidéo entre les réseaux IP et le réseau téléphonique commuté (RTC). Il peut être utilisé en interface avec le monde de la téléphonie classique.

H.245 – À retenir

H.245 est le canal de contrôle qui gouverne l'entité H.323. Il définit les protocoles de contrôle pour les communications multimédias. Il est à retenir pour un système H.323.

T.120 – À retenir

La recommandation T.120 adoptée par l'UIT-T donne les grandes lignes d'autres standards[14] dans les séries T.12x et T.13x qui régissent les échanges de données en multipoint et en temps réel en marge d'une conférence multimédia. T.120 s'appuie sur les recommandations T.121 à T.127.

Les possibilités ouvertes par T.120 comprennent :

- Le partage d'un tableau blanc, c'est-à-dire une fenêtre dans laquelle tous les participants à une conférence peuvent écrire (partie de T.126) ;
- L'échange de fichiers (T.127) ;
- Le partage d'applications, c'est-à-dire l'utilisation conjointe d'un programme (T.128).

T.126 – À retenir

T.126 est le protocole du service multipoint d'imagerie fixe et d'annotation.

T.127 – À retenir

T.127 est le protocole de transfert multipoint de fichiers binaires.

14. http://www.itu.int/rec/T-REC-T.120/fr

T.128 – À retenir

T.128 est le protocole de partage d'applications en multipoint.

Protocoles orientés messagerie

✓ Protocole de structuration des courriels

MIME – À retenir

MIME est utilisé par la majorité des outils de communication (nouvelles, courriels, etc.).

✓ Protocole de structuration sécurisée des courriels

S/MIME 3 – À retenir

Voir la section sur la sécurité.

• Protocoles d'exploitation

DNS – À retenir

Le DNS (*Domain Name Service*) est un service qui permet d'assurer le nommage et l'échange des renseignements des domaines. Une version libre du serveur, BIND (*Berkeley Internet Name Domain*), est utilisée dans la plupart des installations UNIX. Cependant, BIND n'est pas un produit, mais plutôt un morceau de code. Afin d'en faire une solution utilisable, les organismes publics doivent faire un important investissement pour inclure les fonctions manquantes, notamment celles ayant trait à la sécurité. Dans le contexte gouvernemental, c'est le DNS qui est à retenir.

• Protocoles d'accès

LDAP v3 – À retenir

Standard de l'IETF, LDAP est le modèle d'information à retenir. La plupart des fournisseurs de logiciels de messagerie électronique, de services d'annuaires ainsi que des constructeurs informatiques ont adapté leurs produits au protocole LDAP. LDAP, dans sa version 3, est à retenir.

NFS 4.0 – À retenir

NFS (*Network File System*) est un protocole développé par *Sun Microsystems* en 1984. Il permet à un ordinateur d'accéder à des systèmes de fichiers par l'intermédiaire d'un réseau favorisant le partage des données, principalement entre systèmes UNIX. Des versions existent pour Macintosh ou *Microsoft Windows*. NFS est compatible avec IPv6 sur la plupart des systèmes.

WMS 1.3 – À retenir

WMS (*Web Map Service*) est un protocole de communication standard qui permet de se connecter, par une interface HTTP, à une base de données géographiques et d'en extraire les images de cartes géographiques appropriées.

WFS 2.0 – À retenir

Le standard WFS est un protocole décrit dans des spécifications maintenues par l'*Open Geospatial Consortium* (OGC), qui permet de mettre en ligne des services de géocollaboration dans les processus de mise à jour des données cartographiques. Il donne accès à l'information géographique se trouvant sur un serveur, et cela d'une façon « granulaire » afin de cibler des fonctionnalités et des propriétés de fonctionnalités particulières au lieu de l'intégralité d'un fichier. Pour l'accès à l'information géographique, WFS 2.0 est à retenir.

GeoRSS (simple et GML) – À retenir

Des standards facilitant l'accessibilité temporelle et le partage d'information, comme un fil de nouvelles, entre les bases de données sont désormais disponibles et améliorent le bilan de l'interopérabilité des organisations de mesures d'urgence[15]. Ils sont définis selon l'approche du Système interorganisationnel de connaissance de la situation au Québec (SICS-QC) qui est cohérent avec le système québécois de sécurité civile. On entend par approche du SICS-QC l'utilisation d'une structure de messages selon la complémentarité du profil canadien du Protocole d'alerte commun (PAC-PC) et de la configuration géographique du GeoRSS GML et du *GeoRSS Simple*[16]. Ces deux protocoles GeoRSS (*Geographic Really Simple Syndication*) permettent la circulation standardisée (uniforme et cohérente) des messages PAC-PC dans le réseau de sécurité civile sous forme de flux de contenu avec possibilité de filtres.

WMTS 1.0.0 – À retenir

Le *World Map Tile Service* (WMTS) est défini par l'OGC. Il permet d'obtenir des cartes géoréférencées tuilées à partir d'un serveur de données sur le réseau. On peut y déposer des requêtes complexes (dont la « reprojection » ou la symbolisation de données vecteur) nécessitant une certaine puissance de calcul côté serveur. Le WMTS met l'accent sur la performance et ne permet de demander que des images préalablement calculées (tuiles) appartenant à des dallages prédéfinis. Le Centre de services partagés (CSPQ) a produit le fond de carte officielle du gouvernement du Québec en WMTS, et plusieurs ministères et organismes l'utilisent.

CSW – À retenir

Le Service de catalogue Web (CSW) offre l'accès à des registres permettant la recherche et la publication de collections de renseignements descriptifs (métadonnées) sur des données, services et objets d'information connexes qui décrivent les caractéristiques de ces ressources et qui peuvent être soumises à des requêtes ou à l'évaluation d'utilisateurs oude logiciels. Les services de catalogue Web sont essentiels à la recherche et à la création de liens entre

15. http://www.ogcnetwork.net/SWE_Common_Spec
16. http://fr.wikipedia.org/wiki/GeoRSS

les ressources documentées d'une communauté d'information. Ce standard est supporté par le logiciel GeoNetwork utilisé dans l'administration publique québécoise.

WPS 1.0.0 – À retenir

Un service de géotraitement Web (WPS) donne accès à des calculs ou à des modèles sur les données géoréférencées. Le WPS peut réaliser des analyses spatiales comme la soustraction d'un jeu de nombres géo-référencés d'un autre jeu (p. ex. pour déterminer la différence dans le nombre de cas de grippe au cours de deux saisons distinctes). Les données nécessaires au service peuvent être accessibles sur un réseau ou un serveur (WFS, CSW) et respecter les standards d'identification et d'échange des données. Le standard du service de traitement Web dispose d'un mécanisme pour déterminer les données géoréférencées nécessaires au calcul, lancer le calcul et gérer les résultats afin que le client puisse y accéder.

Aide-mémoire

Interconnexion

Catégorie	Sous-catégorie	Norme Standard	Statut
Couche réseau		IPv4	À retenir
		IPv6	À considérer
Couche de transport		RTP/RTCP	À retenir
		TCP	À retenir
		UDP	À retenir
Couche de session		SSH	À retenir
Protocoles d'application	Protocoles multimédias	RTSP	À retenir
		H.323	À retenir
		SIP	À considérer
		MGCP	À retenir
		H.245	À retenir
		T.120	À retenir
		T.126	À retenir
		T.127	À retenir
		T.128	À retenir
	Protocoles de transfert	FTP	À retenir
		SMB 2	À considérer
		HTTP 1.1	À retenir
		HTTPS	À retenir
		FTPS	À retenir
		SFTP	À retenir
	Protocoles de messagerie	MIME	À retenir
		S/MIME 3	À retenir
	Protocoles d'exploitation	DNS	À retenir
	Protocoles d'accès	LDAP v3	À retenir
		NFS 4.0	À retenir
		WMS 1.3	À retenir
		WFS 2.0	À retenir

3.2 Niveau intégration

3.2.1 Services Web

- Messagerie

SOAP 1.1 – À retenir

SOAP est un protocole XML qui permet, à travers un appel de procédure à distance, d'envoyer des messages en utilisant le protocole de transport HTTP ou SMTP. SOAP présente plusieurs avantages. En plus d'être assez ouvert pour s'adapter à différents protocoles de transport, il est indépendant de la plateforme et du langage. SOAP 1.1 est à retenir.

SOAP 1.2 – À considérer

SOAP 1.2 n'est pas encore arrivé à maturité ; il est donc à prendre en considération.

MTOM – À retenir

MTOM est un standard qui permet l'envoi des données binaires dans leur taille d'origine. Il permet ainsi d'éviter l'encodage des données en texte, ce qui fait augmenter leur taille. MTOM est à retenir.

XOP – À retenir

Le standard MTOM est utilisé conjointement avec le standard XOP qui permet l'extraction des données binaires des fichiers XML afin d'optimiser les échanges. XOP est à retenir.

- Répertoire de publication

UDDI v3 – À retenir

La version 3 d'UDDI est retenue pour la localisation des services Web. La V3 accepte le double encodage (UTF-8 et UTF-16) et elle est conforme aux spécifications XML qui exigent que les parseurs XML acceptent les deux formats d'encodage. Les spécifications XML ont préséance sur les spécifications UDDI.

- Langage de description

WSDL 2.0– À retenir

WSDL (*Web Service Description Language*) est un document XML considéré comme un élément essentiel dans une architecture orientée services, et ce, en ce qui concerne la description des fonctionnalités offertes par un service Web. WSDL 1.1 et 2.0 sont les deux versions retenues pour la description des services Web. Il est toutefois recommandé d'utiliser la version WSDL 2.0.

WSDL 1.1 – À considérer

Cette version de WSDL est à prendre en considération.

- ## Orchestration

WS-BPEL2.0 – À retenir

WS- (BPEL *Web Services Business Process Execution Language)* est un dérivé à la fois de WSFL (*Web Services Flow Language)* d'IBM et de XLang de Microsoft, qu'il a remplacé, devenant de fait le standard de l'orchestration des services Web. C'est un langage de programmation basé sur XML pour décrire les processus d'affaires de haut niveau. La version 2.0 de WS-BPEL est à retenir.

WS-CDL – À retenir

La chorégraphie de service, contrairement à l'orchestration qui suppose l'existence d'un chef d'orchestre (WS-BPEL est un langage d'orchestration), implique des interactions pair-à-pair. En ce qui concerne la chorégraphie des services Web, WS-CDL est à retenir.

- ## Gestion transactionnelle

XAML – À retenir

XAML est une spécification de développement pour des services Web, qui tire son nom du protocole XA (*Transaction Authority*) qui a donné le *Transaction Authority Markup Language.* Les spécifications XAML permettent en effet à une transaction Web de gérer l'intégrité transactionnelle. XAML est à retenir.

Aide-mémoire

Intégration

Catégorie	Sous-catégorie	Norme Standard	Statut
Service Web	Messagerie	SOAP1.1	À retenir
		SOAP1.2	À considérer
		MTOM	À retenir
		XOP	À retenir
	Répertoire de publication	UDDI v3	À retenir
	Langage de description	WSDL1.1	À considérer
		WSDL 2.0	À retenir
	Orchestration	WS-BPEL 2.0	À retenir
		WS-CDL	À retenir
	Gestion transactionnelle	XAML	À retenir

3.3 Niveau formats et structures

3.3.1 Formats

- Contenu textuel

PDF – À retenir

Le format PDF, langage de description de pages créé par la société *Adobe Systems,* est largement utilisé à l'échelle gouvernementale. En janvier 2007, l'intégralité des spécifications du format PDF ont été communiquées à l'Organisation internationale de normalisation (ISO), rendant ainsi le format PDF ouvert (ISO 32000-1) en janvier 2008. Il est recommandé d'utiliser .pdf comme format pour la diffusion des documents destinés à la consultation (non appelés à être modifiés).

ODF 1.2 – À retenir

L'*Open Document Format* est une norme destinée aux applications de bureau, qui regroupe les formats suivants (avec les extensions de documents associées). Ces formats sont éditables avec toute application de bureau qui reconnaît la norme. Ils offrent la possibilité de collaborer autant à l'intérieur qu'à l'extérieur des organisations sans imposer l'achat d'outils bureautiques précis. Le format *Open Document* regroupe les formats suivants (avec les extensions de documents associées) :

- Texte formaté .odt
- Tableur .ods
- Présentation .odp
- Dessin .odg
- Diagramme .odc
- Formule .odf
- Base de données .odb
- Image .odi
- Document principal .odm

DOC, DOCX – À considérer

Le format de document DOC est un format propriétaire développé par Microsoft. Ses spécifications n'appartiennent pas au domaine public. Ce n'est donc pas un format ouvert. Par contre le format de document DOCX qui est une concrétisation de la norme *Office Open* XML développée à l'origine par Microsoft pour concurrencer la solution *Open Document* (suffixes .odt) est un format ouvert mais qui pose des problème de rétrocompatibilité. Compte tenu de leur large utilisation, les organismes publics peuvent continuer à les utiliser en attendant la pénétration sur le marché des suites bureautiques supportant ODF. Toutefois, les polices de caractères C*, soit les nouvelles polices de Microsoft dont le nom commence par un C (Calibri, Cambria, Candara, Consolas, Constantia et Corbel), doivent être évitées au niveau du traitement du texte puisqu'elles sont soumises à une licence qui en permet l'affichage seulement avec la suite *MS Office*. Dans ce cas, des polices libres ne peuvent pas en émuler l'aspect et tous les documents utilisant ces polices seraient mal affichés ce qui causera un problème d'interopérabilité.

PostScript – À retenir

PostScript (PS) est un langage de description de page développé par Adobe. Il repose sur des formulations vectorielles de la plupart de ses éléments. Ce langage entre plateformes permet d'obtenir un fichier unique comportant tous les éléments décrivant la page (textes, images, polices, couleurs, etc.). Lorsqu'il s'agit de documents destinés aux imprimantes, le format PS (*PostScript*) est à retenir.

TXT – À retenir

Les fichiers texte (extension .txt) sont largement utilisés. Ce format s'applique à des données brutes. Il est utilisé pour les textes sans mise en forme respectant le code ASCII. À l'échelle gouvernementale, le TXT est à retenir.

• Contenu Web

HTML 4.1 – À retenir

HTML (*Hypertext Markup Language*) est un langage de balisage permettant d'écrire de l'hypertexte, de structurer sémantiquement et de mettre en forme le contenu des pages, d'intégrer des objets multimédias ainsi que des formulaires de saisie de même que des programmes informatiques. Il permet de créer des documents interopérables qui seront

conformes aux exigences des standards d'accessibilité du Web (SGQRI 008). HTML 4.1 est le format de contenu Web le plus utilisé à l'échelle gouvernementale.

HTML 5 – À considérer

HTML 5 est désormais une recommandation du W3C, et cela depuis 2014. Des organismes publics utilisent de plus en plus HTML 5 qui offre plus de fonctionnalités et qui est plus compatible avec d'autres standards gouvernementaux, notamment l'accessibilité du Web (SGQRI 008). Pour le moment, c'est une version à prendre en considération.

CSS 2.1 – À retenir

CSS est un langage informatique qui sert à décrire la présentation des documents HTML et XML. Les spécifications définissant CSS sont définies par le W3C. CSS n'a pas de « versions », mais des « niveaux ». Le niveau 2.1 (niveau 2, première révision) est à retenir. Le niveau 3 (CSS 3) est encore non normatif à la date de rédaction du présent cadre commun d'interopérabilité. Toutefois, des modules complétés de CSS 3 peuvent être utilisés avec le niveau 2.1.

XHTML 1.1 – À retenir

Dans le but de rapprocher HTML de XML, de les rendre compatibles et d'ajouter des extensions à HTML particulièrement en ce qui concerne les formulaires, le W3C a élaboré le XHTML (*eXtended* HTML), profitant ainsi du fait que HTML est la façon la plus simple de produire des objets affichables. La version la plus mature est XHTML 1.1, qui est à retenir.

XHTML 2.0 – À considérer

La version XHTML 2.0 n'est pas largement répandue, donc elle est à prendre en considération.

- ### Contenu multimédia

  - ✓ #### Graphisme

    ##### PNG – À retenir

    PNG (*Portable Network Graphics*) est un format de fichier graphique matriciel utilisant une compression dite sans perte ; il est recommandé pour les images avec des palettes de couleurs prédéfinies (p. ex. : des icônes, des logos). Il est supérieur au GIF.

    ##### TIFF – À retenir

    TIFF (*Tagged Image File Format*) est un format de fichier graphique matriciel dont Adobe est le dépositaire et le propriétaire initial. Il est adapté pour les images de taille importante et de haute qualité.

    ##### JPEG – À retenir

    Le format JPEG (*Joint Photography Experts Group*) fournit des fichiers très compacts grâce à son algorithme de compression efficace, mais il entraîne des pertes d'information.

Il peut être utilisé pour produire des photos et des images texturées dans les pages Web. JPEG est largement utilisé au gouvernement du Québec.

GIF – À retenir

GIF (*Graphic Interchange Format*) est un format de fichier graphique matriciel qui est largement utilisé par la communauté gouvernementale. Il utilise une compression dite sans perte « LZW ». Il permet de créer des images animées.

SVG 1.1 seconde édition – À retenir

SVG (*Scalable Vector Graphics*) est un format de données conçu pour décrire des ensembles de graphiques vectoriels et basés sur XML. Ce format inspiré est spécifié par le W3C. SVG permet de présenter des graphiques vectoriels et de les animer. SVG est déjà largement utilisé.

SVGMobile – À retenir

SVGMobile prend en considération les spécificités des appareils mobiles.

✓ Audio

OGG – À retenir

Le format libre de compression-décompression OGG (CODEC Vorbis) offre une meilleure qualité et une plus grande compression que d'autres formats tels que le format audio connu MP3 (propriétaire). Pour le contenu audio et vidéo, le format OGG est à retenir.

MP3 – À considérer

MP3 (ISO 11172-3) est un algorithme de compression capable de réduire fortement la quantité de données nécessaires à la restitution d'un son monophonique ou stéréophonique. MP3, puisqu'il est déjà pas mal établi au gouvernement, est à prendre en considération en ce qui concerne l'échange, la diffusion et la conservation des séquences sonores.

MKV – À retenir

Le format MKV est un conteneur vidéo qui peut regrouper au sein d'un même fichier (généralement avec l'extension .mkv) plusieurs pistes vidéo et audio ainsi que des sous-titres et des chapitres. Il partage avec le format WebM certaines spécificités. MKV est à retenir.

✓ Vidéo

THEORA – À retenir

THEORA est un format de compression vidéo ouvert et sans brevet. C'est un des composants du projet de format d'encapsulation OGG, qui a pour but de créer un ensemble de standards ouverts concernant le traitement de signaux multimédias (son, vidéo). THEORA fournit la vidéo, utilise une licence de type BSD et se fonde sur le codec

libre VP3 de On2 Technologies. THEORA entre en compétition avec des codecs tels que MPEG-4 (p. ex. : Xvid et DivX), Windows Media Video ou RealVideo.

Contrairement au codec Xvid, le codec THEORA n'est soumis à aucun brevet appartenant au MPEG-4. Le THEORA est tout de même soumis à des brevets appartenant à On2 Technologies, mais On2 a donné le droit irrévocable d'utiliser les brevets en question sans aucune restriction. Le format THEORA est à retenir.

WebM À retenir

WebM est un format de conteneur multimédia ouvert principalement destiné à un usage sur le Web ; il regroupe les flux vidéo du codec VP8 et les flux audio du codec Vorbis.

Le WebM fait partie des formats vidéo proposés pour la balise <video> de HTML5. Il est amené à remplacer le premier format ouvert proposé, THEORA, et il fait concurrence au format fermé H.264. WebM est à retenir.

MP4 – À considérer

MP4 est une partie de la norme MPEG-4 qui utilise H.264 comme norme de compression vidéo ; elle est la plus couramment utilisée pour l'enregistrement, la compression et la distribution de vidéo en haute définition. MP4, soumis à des brevets mais largement utilisé au gouvernement, est à prendre en considération pour l'enregistrement, la compression et la distribution de vidéo en haute définition.

✓ Contenu géospatial

SHP – À retenir

Shapefile (SHP) est un format de contenu géospatial issu du monde des systèmes d'informations géographiques (SIG). Ce format est désormais devenu un standard de facto largement utilisé par un grand nombre de logiciels libres (*MapServer*, *Grass*, *Udig*, *MapGuide OpenSource*, *GmapCreator*, *QGIS*, *GvSIG*, etc.).

KML 2.2 – À retenir

Le standard KML (*Keyhole Markup Language*) est un langage qui permet d'encoder le contenu géographique afin de le visualiser. Il est basé sur le formalisme XML et destiné à la gestion de l'affichage de données géospatiales. La version 2.2 de KML est à retenir.

✓ Identifiant de ressource

URI – À retenir

Le format utilisé pour identifier une ressource est unique dans le Web. Il s'agit de l'URI (*Uniform Resource Identifier*). Un URI peut identifier une ressource ou ses méthodes. Il est recommandé aux organismes publics de se conformer au standard du W3C et de l'*Internet Engineering Task Force* (IETF) en matière d'URI et d'URL, et d'utiliser les produits qui s'y conforment. Les organismes publics doivent se reporter aux standards SGQRI en ce qui concerne le cas particulier des URL d'adresses de noms de domaine et de courriel.

3.3.2 Encodage

- Caractère

Unicode 6.2.0 – À retenir

Le standard Unicode permet des échanges de textes dans différentes langues, à un niveau mondial. Il est développé par le *Consortium Unicode* qui vise à permettre le codage de texte écrit en donnant à tout caractère de n'importe quel système d'écriture un nom et un identifiant numérique, et ce, de manière unifiée, quelle que soit la plateforme informatique ou le logiciel utilisé. La dernière version, Unicode 6.2.0, publiée le 26 septembre 2012, est à retenir.

Dans l'administration publique québécoise, il faut se reporter au standard SGRQI 3[17] qui définit le jeu de caractères adopté et décrit dans l'ISO-Latin n°9, ou ISO/CEI 8859-15. Ce jeu de caractères permet d'écrire, outre en français, dans les langues suivantes : albanais, allemand, anglais, basque, breton, catalan, danois, espagnol, estonien, féroïen, finnois, frison, gaélique écossais, gaélique irlandais (nouvelle orthographe), galicien, gallois, groenlandais, islandais, italien, latin, luxembourgeois, néerlandais, norvégien, portugais, romanche et suédois.

- Audio

Vorbis (OGG) – À retenir

Vorbis est un codec audionumérique, sans brevet, ouvert et libre, plus performant en termes de qualité et de taux de compression que le format MP3, mais moins populaire que ce dernier. C'est un des composants du projet OGG qui a pour but de créer un ensemble de formats et codecs multimédias ouverts (son, vidéo) libre de tout brevet. Ce codec est à retenir.

FLAC – À retenir

FLAC est un algorithme de compression audio sans perte. Il n'enlève aucune information du flux audio tout en réduisant la taille des fichiers. À utiliser pour l'échange, la diffusion et la conservation des séquences sonores de haute qualité, et ce, sans aucune perte.

- Vidéo

H.261 et H.263 – À retenir

H.261 et H.263 sont des recommandations de compression vidéo de l'UIT-T. Ces codecs s'appuient sur RTP et RTCP pour communiquer. H.261 définit la compression de l'information vidéo sur réseau à faible bande passante. H.263 est une variante de H.261. Il est adapté pour les faibles vitesses de transmission (64 kbp/s à 128 kbp/s). Ces standards font partie de la recommandation H.323. Ces deux codecs sont à prendre en considération mais, si c'est possible, on doit éviter les solutions propriétaires.

17. http://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/standards_relatifs_interoperabilite/SGQRI003.pdf

VP8 – À retenir

Pour la compression vidéo, le format ouvert de compression VP8 devrait être utilisé étant donné qu'il offre une meilleure qualité de compression que les standards H261 et H263. Il est également à retenir pour la diffusion en direct (*streaming*).

VP9 – À considérer

VP9 est un codec ouvert et libre de droits développé par Google. Il était nommé au début de son développement *Next Gen Open Video* (NGOV) et *VP-Next*. VP9 sera le successeur de VP8 ; il est donc à prendre en considération.

• Compression

ZIP – À retenir

ZIP est un format de compression largement utilisé. Pour échanger des fichiers avec des utilisateurs qui ont un système d'exploitation autre que Linux, il est recommandé d'utiliser ZIP pour éviter les problèmes d'interopérabilité.

TAR 1.26 – À retenir

TAR (*File Archiver*) est couramment utilisé pour recueillir plusieurs fichiers pour ensuite les consolider en un seul fichier destiné à la distribution ou à l'archivage, et ce, tout en préservant l'information du système de fichiers. Il est important de noter que TAR exclut la partie compression de fichiers. TAR est à retenir pour la distribution et l'archivage de fichiers.

GZIP 4.3 – À retenir

GZIP (*Gnu Zip*) est un logiciel libre de compression qui a été créé à partir de 1991 pour remplacer le programme *Compress* d'UNIX. Le format manipulé par GZIP (GZ) est un format de compression ouvert utilisé avec l'outil TAR. En effet, l'outil TAR regroupe différents fichiers dans une archive .tar, et l'outil GZIP est en mesure de les compresser. L'extension .gz créée par GZIP est ajoutée à celle du fichier. Il est donc possible de trouver des fichiers du type Fichier.txt.gz ou Fichier.tar.gz. GZIP est à retenir.

LZMA 2 – À retenir

LZMA (*Lempel-Ziv-Markov chain-Algorithm*) est un algorithme de compression de données sans perte utilisé dans le format 7z du programme 7-Zip. Il offre un fort taux de compression (en général plus fort que le Bzip2). La nouvelle version de LZMA, LZMA2, est mieux appropriée et elle possède de nouvelles fonctionnalités, notamment la vérification d'intégrité.

3.3.3 Structuration et traitement des données structurées

- Structuration des données

XML 1.0 – À retenir

XML (*Extensible Markup Language*) permet de stocker dans un document des données structurées. Les données sont indépendantes de l'affichage. Ainsi, à partir d'un seul fichier XML, on pourra créer divers documents. XML permet d'utiliser le potentiel de toute la famille XML : schémas, XSLT et XHTML, y compris ses langages modulaires spécialisés (SVG, XML SIG, etc.). XML est un pilier de l'interopérabilité, que ce soit sur le plan de l'échange de données entre les organismes publics ou avec les citoyens et les partenaires. La version XML 1.0 est à retenir car elle garantit la compatibilité avec d'autres standards (p. ex. : WSDL 1.1).

XSLT 2.0 – À retenir

XSLT est un langage de transformation dont la syntaxe est XML, qui réalise (de manière transparente) l'analyse du document XML pour le transformer en un arbre DOM, trouve les nœuds satisfaisant aux règles XSL, régénère un DOM et génère le document dans le format approprié (HTML, PDF, etc.) grâce à la feuille de style XSL-FO. La version 2 de XSLT est à retenir.

JSON – À retenir

JSON (*JavaScript Object Notation*) est un format de données textuelles, générique, dérivé de la notation des objets du langage ECMAScript. Il permet de représenter de l'information structurée. Il est à retenir pour des échanges particuliers tels que les favoris Internet (*bookmarks*). Par contre, il doit être pris en considération dans une communication du style REST.

DOM niveau 3 – À retenir

DOM (*Document Object Model*), standard du W3C construit un arbre complet du document constitué de nœuds de différents types : document, élément, attribut, commentaires, etc. Le DOM de niveau 3 permet à l'API de charger et de sauvegarder les arbres manipulés. DOM est utilisé notamment par XSLT et Xpath. Les organismes publics doivent baser leurs composantes de système et scripts sur DOM niveau 3 ou sur SAX v2. Il faut noter que certains éléments du DOM niveau 3 ne sont pas supportés sur tous les navigateurs.

SAX 2.0 – À retenir

SAX (*Simple API for XML*) découpe le flux d'entrée en jetons et retourne des événements à chaque élément, attribut ou texte rencontré. Il est efficace, car il ne peut renvoyer à l'application qui s'appuie sur lui que les nœuds nécessaires ; il permet donc de traiter un volume de données important avec peu de mémoire. La version 2 de SAX permet de prendre en considération les espaces de noms XML. Les organismes publics doivent baser leurs composantes de système et scripts sur DOM niveau 3 ou sur SAX v2.

CSV – À considérer

Le format d'échange tabulé CSV (*Comma Separated Values*) permet l'exportation d'un ensemble de données vers un fichier ASCII tabulé par des virgules ou d'autres formes de séparations, et vice versa. En raison du fait que la séparation entre les champs n'est pas régie par une règle claire (virgule, tabulation, etc.), le format CSV n'est pas considéré comme un standard en soi mais plutôt comme une pratique (largement répandue). Ainsi, CSV est à prendre en considération, mais il est préférable d'utiliser XML en ce qui a trait au format d'échange.

RDF – À retenir

RDF (*Ressource Description Framework*) est utilisé comme une méthode générale pour la description ou la modélisation conceptuelle de l'information qui est mise en œuvre dans les ressources Web, en utilisant une variété de formats de syntaxe. L'adoption de RDF favorise l'établissement des liens sémantiques entre les données (*linkdata*), ce qui est très utile pour la gestion de l'information gouvernementale.

GML 3.2.1 – À retenir

GML est un langage basé sur XML, qui permet d'encoder et d'échanger de l'information géospatiale. Le format GML est utilisé par les protocoles de communication WMS et WFS.

SFA – À retenir

Simple Features (*officially Simple Feature Access*) est en même temps un standard de l'OGC et de l'ISO (ISO 19125). Il définit un modèle de stockage des données géographiques. La structuration de la plupart des bases de données permettant d'intégrer des données géospatiales (Oracle, SqlServer, MySQL, PostGIS) implémente une partie ou la totalité du standard *Simple Feature Traitment* des données structurées.

Protocole d'alerte commun – profil canadien (PAC-PC) – À retenir

Le Profil canadien du Protocole d'alerte commun (PAC) constitue un ensemble de règles et de listes gérées de valeurs, dont l'utilisation est recommandée au Canada par les ministres responsables de la sécurité publique du fédéral, des provinces et des territoires.

Le Profil canadien est conforme au Protocole d'alerte commun (le « standard de référence ») administré et géré par l'Organization for the Advancement of Structured Information Standards (OASIS). Un message valide du PC-PAC constitue donc également un message valide du PAC.

Lors d'un sinistre, nombreuses sont les décisions qui devront être prises pour répondre aux besoins dictés par la situation afin de réduire les effets et d'en atténuer les conséquences. La circulation de l'information est actuellement possible entre les diverses organisations, mais elle repose surtout sur des moyens traditionnels (téléphone de vive voix, courriels, télécopies, réunions en personne ou téléconférence). Il n'y a pas de processus systématique d'échange d'information en temps réel.

- ## Traitement des données structurées

XLink 1.1, XPath 2.0, XQuery 1.0, XPointer 1.0, XInclude 1.0 (2e édition) – À retenir

Le langage XML approuvé par le W3C et la famille des standards (*XLink, XPointer*, XSL, etc.) améliorent l'interopérabilité entre les systèmes des organismes publics. Utilisés dans le traitement des documents, XML, XPath, *XQuery, XLink, XInclude et XPointer* permettent de pointer sur le fragment (nœud ou attribut) le plus fin d'un document XML, d'agréger divers fragments XML et de naviguer dans les structures XML.

- *XPath* est un langage qui sélectionne à l'aide de prédicats une partie d'un document XML.
- *XQuery* et *XPath* sont complémentaires.
- *XPointer* pointe un document XML et peut sélectionner une partie de ce document à l'aide de *XPath*.
- *XLink* décrit des liens entre des « *Xpointers* ».
- *XInclude* permet de construire des documents composites à partir d'autres documents ou fragments XML.

Cette famille de standards est à retenir. Il est recommandé aux organismes publics de faire les traitements XML du côté serveur afin d'éviter une grande disparité de l'affichage du résultat final dans les fureteurs des utilisateurs.

Espaces de noms XML – À retenir

Un document XML utilise fréquemment des vocabulaires issus de domaines et d'applications différents, ce qui peut entraîner des collisions au moment de la validation du document par le schéma. Les espaces nominatifs définis par le W3C ont pour rôle de lever toute ambiguïté en qualifiant chaque terme utilisé (en lui donnant un contexte, en quelque sorte).

Les espaces nominatifs sont référencés dans le document XML par un URI et factorisés par un préfixe plus facile d'utilisation. Ce préfixe qualifie chaque élément et attribut ambigus du document. Les organismes publics doivent utiliser les espaces nominatifs XML.

Aide-mémoire

Formats

Catégorie	Sous-catégorie	Norme	Standard	Statut
Texte		PDF		À retenir
		ODF	odt	À retenir
			ods	À retenir
			odp	À retenir
			odg	À retenir
			odc	À retenir
			odf	À retenir
			odb	À retenir
			odi	À retenir
			odm	À retenir
		TXT		À retenir
		DOC, DOCX		À considérer
Web		HTML 4.1		À retenir
		HTML 5		À considérer
		XHTML 1.1		À retenir
		XHTML 2.0		À considérer
		XSLT 2.0		À retenir
		CSS 2		À retenir
Multimédia	Audio	OGG		À retenir
		MP3		À considérer
		MKV		À retenir
	Vidéo	OGV/THEORA		À retenir
		WebM		À retenir
		H.264		À considérer
	Graphisme	PNG		À retenir
		GIF		À retenir
		JPEG		À retenir
		TIFF		À retenir
		SVG		À retenir
		SVG Mobile		À retenir
Géospatial		SHP		À retenir
		KML 2.2		À retenir

Structures

Encodage Traitement	Catégorie	Norme Standard	Statut
Encodage	Caractère	UNICODE	À retenir
	Audio	Vorbis (OGG)	À retenir
		FLAC	À retenir
	Vidéo	H261/H263	À retenir
		VP8	À retenir
		VP9	À considérer
	Compression	ZIP	À retenir
		GZIP	À retenir
		TAR	À retenir
		LZMA 2	À retenir
Structuration et traitement des données structurées	Structuration	XML 1.0	À retenir
		JSON	À retenir
		DOM (niveau 3)	À retenir
		CSV	À considérer
		SAX 2.0	À retenir
		GML 3.2.1	À retenir
		RDF	À retenir
	Traitement des données structurées	*XLink* 1.0	À retenir
		XQuerry 1.0	À retenir
		XPath 2.0	À retenir
		XInclude 1.0	À retenir
		XPointer 1.0	À retenir

3.4 Sécurité

Pour les fins de ce document, la sécurité est considérée comme une caractéristique souhaitable d'un service interopérable d'échange ou Web rendu par un organisme public. Toutefois, un service sécurisé doit considérer tous les aspects suivants :

- la sécurité des services et mécanismes d'échange ;
- la sécurité des services Web ;
- la sécurité technique connexe (sécurité des réseaux avec pare-feu, IPS, protection contre les virus, etc.) ;
- l'utilisation des services de sécurité communs (ICPG, ClicSéqur) ;
- les pratiques complémentaires de sécurité (gestion opérationnelle).

L'objectif principal de la présente section du cadre est de promouvoir l'interopérabilité, la neutralité et la sécurité des plateformes de services d'échanges sur le Web tout en assurant la protection des renseignements personnels et en préservant la confiance des usagers envers ces services. Elle est destinée également à inventorier un ensemble de normes susceptibles d'être applicables au sein des OP. Les éléments de sécurité traités peuvent être mobilisés pour sécuriser les niveaux « interconnexion » ou « intégration » du modèle présenté à la section 2.2.

3.4.1 Considérations de sécurité

La confiance est un principe directeur de la vision de l'AEG 3.0. Afin de promouvoir ce principe dans les services gouvernementaux, il est nécessaire, dès la conception d'un service et pour souligner la transparence, que la sécurité et la confidentialité de ce service soient prises en considération ou assurées.

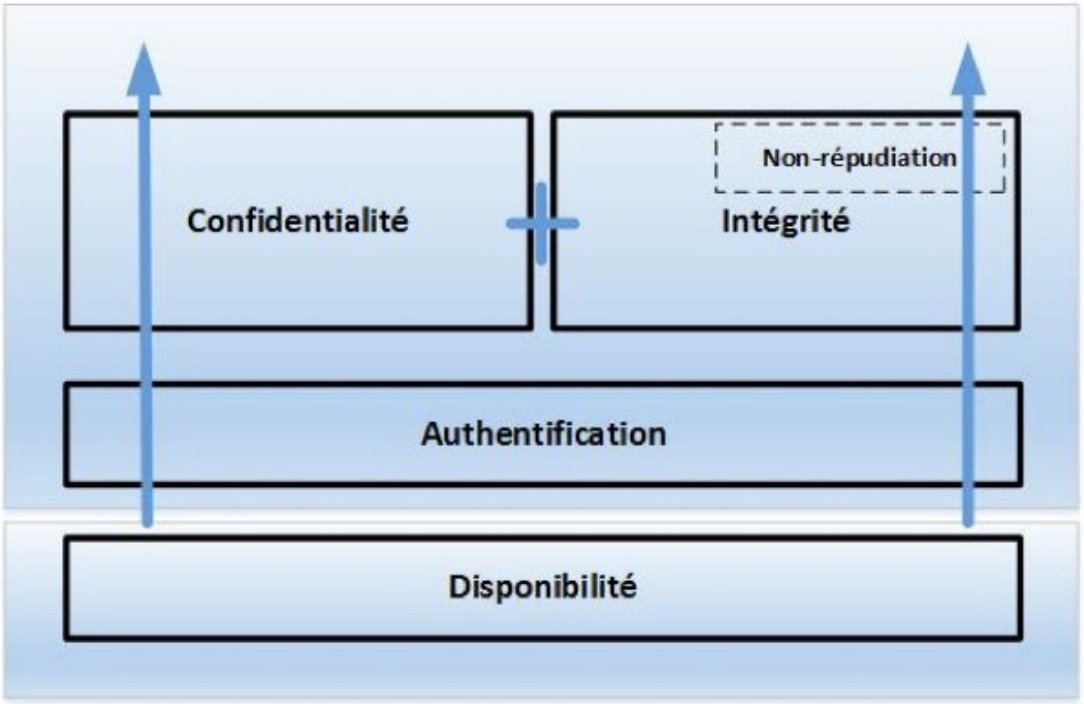
Ce cadre énonce des normes de sécurité utiles pour assurer la confidentialité et l'intégrité de l'information traitée par des services d'échanges sur le Web. Il traite également des normes portant sur les considérations de sécurité associées à l'authentification des entités et à la non-répudiation des renseignements ou des événements.

En ce qui a trait à la disponibilité, le travail d'analyse n'a pas permis de repérer de normes particulières la concernant[18]. Toutefois, la capacité à gérer les événements de disponibilité demeure une qualité essentielle d'un service d'échanges sur le Web. Afin de garantir la disponibilité des services, il est nécessaire de connaître quand et pourquoi cette disponibilité est compromise. Les conditions de sa maintenance doivent être établies entre le client et le ou les prestataires de services au moyen d'ententes établissant les niveaux de service requis.

La figure 11 illustre les relations de dépendance entre les propriétés de sécurité. On note que la disponibilité est l'assise de l'interopérabilité et qu'elle est une notion préalable, que la confidentialité est indépendante de l'intégrité alors que la non-répudiation implique l'intégrité ou encore qu'il peut être nécessaire, afin de garantir la confidentialité ou l'intégrité, que les entités soient authentifiées, etc.

18. L'indisponibilité des services d'échanges ou Web est la situation dans laquelle une application, ou un système subit une dégradation ou une interruption de son service à la suite de la défaillance d'une ou plusieurs de ses parties.

Figure 11 Propriétés de sécurité



Les normes peuvent donc être utilisées de différentes façons, comme des blocs de construction, pour l'élaboration de services sécurisés d'échanges ou Web. Elles ont aussi comme autre propriété l'adaptabilité à une grande variété de modèles de sécurité. Elles peuvent, entre autres, permettre à différents domaines de sécurité de se connecter et d'échanger de l'information de façon sécuritaire ou de se fédérer de telle sorte que l'accès à des ressources gérées dans un domaine sont accessibles à des entités (personnes ou dispositifs) dont l'identité et les attributs de sécurité sont gérés par d'autres domaines de sécurité.

Lors de l'élaboration de l'architecture des services, il est important d'adopter une démarche d'analyse qui comprendra, entre autres, ce qui suit :

- Obtenir une compréhension des aspects clés des services d'échanges ou Web afin d'établir des besoins et des exigences de sécurité, entre autres par l'identification du maillon faible de la chaîne des composantes d'un service (failles de sécurité potentielles) ;
- Identifier les propriétés de sécurité requises en fonction de la catégorisation des données ainsi que leurs configurations de mise en œuvre ;
- Effectuer une analyse des risques pour chaque propriété de sécurité de service Web afin de déterminer les niveaux de robustesse requis ;
- Adopter des scénarios, des modèles de solution appropriés pour la sélection des normes afférentes et la sécurisation des services d'échange ou Web.

Rappelons que l'AGSIN propose une démarche de sécurisation des échanges[19] et que l'ISO 7498-2[20] traite avec précision le sujet des propriétés de sécurité, des normes de sécurité ainsi que des possibilités de combinaison afin d'obtenir le niveau de sécurité requis.

Par ailleurs, les solutions techniques adoptées pour ces services doivent respecter la capacité de chaque partenaire concerné pour organiser ses systèmes et réseaux de traitement de données d'une manière qui convient le mieux à ses pratiques (c'est-à-dire l'approche technologique, le cadre juridique, les principes de gestion, la sécurité, etc.). Du point de vue de l'utilisateur, les fonctions liées à la sécurité (identification, authentification, non-répudiation, confidentialité) doivent bénéficier d'un maximum de transparence, nécessiter un minimum d'efforts et, en même temps, fournir le niveau de sécurité convenu.

Lors de la mise en œuvre du CCI, les questions de sécurité devront être considérées et traitées. Il est impératif que les OP se dotent d'un ensemble de pratiques et d'activités pour les appuyer dans la mise en œuvre du cadre d'interopérabilité, en partie ou dans sa totalité, et qui doit reposer sur :

- La gestion des risques et des menaces associés à la mise en œuvre du cadre d'interopérabilité ;
- La détermination et la mise en œuvre d'un ensemble de mesures de sécurité nécessaires afin d'assurer la disponibilité, la confidentialité, l'intégrité, l'authenticité et la non-répudiation de l'information, conformément à sa catégorisation et à sa sensibilité ;
- La prise en considération, par les processus de gestion, des enjeux associés au cadre d'interopérabilité afin d'établir la gouvernance ;
- La définition et l'attribution des rôles et responsabilités de gestion du cadre et de la sécurité ;
- La conformité aux différentes normes et aux niveaux de sécurité des différentes parties prenantes d'un service ;
- La définition et la gestion des relations, les niveaux d'interopérabilité entre les parties prenantes à un service ;
- La connaissance du niveau et des restrictions relatives à la catégorisation et à la sensibilité de l'information traitée ;
- La définition et la gestion de la façon dont le cadre technique d'interopérabilité s'inscrit dans d'autres cadres et les soutient ;
- Le repérage et la gestion des problèmes de sécurité liés à la mise en place d'éléments de ce cadre ;
- Le contrôle et la connaissance de ce qui est autorisé, de l'usager qui se connecte et des ressources auxquelles il accède ;
- La gestion des changements apportés aux configurations ;
- La prévision de l'intégration aux systèmes existants ;
- La permanence de la validité et de l'efficacité des normes utilisées ;
- La connaissance des évolutions.

19. Pour plus d'information sur ce point, consultez «La chaîne des mécanismes de sécurité».

20. ISO 7498-2 *Information processing systems – Open Systems Interconnection – Basic reference Model – Part2 : Security Architecture.*

3.4.2 Protocoles de sécurité associés au niveau interconnexion

- Protocoles contribuant à l'identification, à l'authentification ou à l'autorisation

EAP – À retenir

Le protocole EAP (*Extensible Authentication Protocol)* est une norme de l'IETF décrite dans la RFC 3748. Il fournit un cadre d'authentification flexible pour l'accès au réseau et prend en charge plusieurs méthodes d'authentification. Quand le protocole EAP est utilisé en conjonction avec un point d'accès réseau compatible 802.1X (sans fil ou filaire), certaines méthodes EAP permettent de « négocier » une clé PMK (*Pair-wise Master Key*) entre le client et le point d'accès. Cette clé PMK peut ensuite être utilisée pour chiffrer les sessions TKIP ou CCMP. Il est à noter que, bien qu'il soit utilisable sur des réseaux filaires, ce mécanisme est le plus souvent employé dans les réseaux sans fil.

IEEE 802.1X – À retenir

Le standard 802.1X est lié à la sécurité des réseaux informatiques ; il a été mis au point par l'IEEE. Il permet de contrôler l'accès aux équipements d'infrastructures réseau et, par leur intermédiaire, de relayer l'information liée aux dispositifs d'identification en place. Il s'appuie sur le protocole EAP pour le transport des renseignements portant sur l'identification en mode client/serveur. Le déploiement de l'IEEE 802.1X fournit une couche de sécurité pour l'utilisation des réseaux câblés et sans fil. Si un équipement réseau actif, tel qu'un commutateur réseau ou une borne Wi-Fi, est compatible avec la norme IEEE 802.1X, il est possible de contrôler l'accès à chacun de ses ports (PAE) indépendamment du type de connexion.

SAML 2.0 – À retenir

Security Assertion Markup Language (SAML) est un standard pour l'échange d'information sur l'authentification et l'autorisation entre des domaines de sécurité ; en d'autres termes la « prolifération de l'identité ». Il est basé sur le langage XML et permet notamment l'implémentation de l'authentification unique SSO (single sign on). Développée par le consortium international OASIS, la version actuelle de SAML 2.0 constitue la convergence de SAML 1.1, l'*Identity Federation Framework (Liberty Alliance*) et le cadre Shibboleth 1.3.

XACML V3.0 – À retenir

L'*eXtensible Access Control Markup Language* (XACML) est un standard de W3C qui spécifie un langage pour le contrôle d'accès, la circulation des règles et l'administration de la politique de sécurité des systèmes d'information. XACML est souvent utilisé pour assurer la fonction d'autorisation dans les architectures SOA.

LDAPv3 – À retenir

Le *Lightweight Directory Access Protocol* (LDAP) est décrit dans la RFC 4510. Il permet de gérer des annuaires, c'est-à-dire d'accéder à des bases d'information sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. En termes de sécurité, LDAP est un moyen d'authentification et il peut assurer la confidentialité et l'intégrité des échanges dans une communication en utilisant TLS.

RADIUS – À retenir

Le *Remote Authentication Dial-In User Service* (RADIUS) est un protocole client-serveur permettant de centraliser des données d'authentification, d'autorisation et de gestion des comptes lors d'un accès à distance, que ce soit pour le réseau filaire ou sans fil. La dernière version du protocole RADIUS est normalisée par l'IETF : les RFC 2865 (*RADIUS Authentification*) et RFC 2866 (*RADIUS Accounting*) de juin 2000.

DIAMETER – À retenir

Le Diameter est un protocole d'authentification, successeur du protocole RADIUS. Il est défini par la RFC 3588. Il est basé sur TCP alors que RADIUS est en UDP. Il exerce trois fonctions : l'authentification, l'autorisation et la traçabilité (AAA en anglais : *Authentification, Authorization, Accounting/Auditing*) et il est destiné aux échanges entre serveurs sur des liaisons sûres. Il est notamment utilisé dans les réseaux de téléphonie mobile pour accéder aux bases de données HLR et HSS afin d'identifier, d'authentifier et de localiser les abonnés mobiles 3G et LTE /4G ; les serveurs Diameter, sont généralement compatibles avec RADIUS.

TACACS – À retenir

Le *Terminal Access Controller Access-Control System* (TACACS) est un protocole d'authentification distante utilisé pour communiquer avec un serveur d'authentification, généralement employé dans des réseaux UNIX. TACACS permet à un serveur d'accès distant de communiquer avec un serveur d'authentification afin de déterminer si l'utilisateur a le droit d'accéder au réseau. (À noter : c'est un protocole propriétaire.)

TACACS+ – À retenir

Le *Terminal Access Controller Access-Control System Plus* (TACACS+) est un protocole permettant de fournir du contrôle d'accès pour les routeurs, les accès réseau et autres équipements réseau grâce à un ou plusieurs serveurs centralisés. TACACS+ assure l'authentification, l'autorisation et la traçabilité. Ce protocole est incompatible avec TACACS. (À noter : c'est un protocole propriétaire.)

KERBEROS V5 – À retenir

Le Kerberos est un système d'authentification unifié, décrit par la RFC 4120, utilisant un serveur central authentifiant les utilisateurs, appelé KDC (*Key Distribution Center*). Un utilisateur se voit délivrer un jeton (*ticket*) d'une durée de vie limitée ; celui-ci sert de preuve d'authentification pour accéder aux différents services disponibles. Un client utilisant l'authentification Kerberos envoie des jetons dans les requêtes destinées au serveur cible. Ce processus est exécuté automatiquement par les applications supportant Kerberos.

OPENID – À considérer

L'*OpenID* est un système d'authentification décentralisé géré par l'*OpenID Foundation*. Il permet l'authentification unique et le partage d'attributs. Ainsi, un utilisateur peut s'authentifier auprès de plusieurs sites Web en utilisant chaque fois un unique identifiant *OpenID*. Le modèle se base sur des liens de confiance préalablement établis entre les fournisseurs de services et les fournisseurs d'identité.

OPENID CONNECT 1.0 – À considérer

L'*OpenID Connect 1.0* est une simple couche d'identité sur le dessus du protocole OAuth 2.0. Elle permet aux clients de vérifier l'identité de l'utilisateur final sur la base de l'authentification effectuée par un serveur d'autorisation, afin obtenir des informations de base sur le profil de l'utilisateur final de manière interopérable. Ce protocole supporte les applications mobiles.

OAuth 2.0 – À considérer

L'OAuth est un protocole libre d'autorisation défini dans le RFC 6749, qui permet à une application tierce d'accéder à l'information d'un utilisateur tout en protégeant son pseudonyme et son mot de passe. Plusieurs organisations utilisent ce protocole, à l'image de Facebook, Google et PayPal.

SCIM – À considérer

Le System for *Cross-Domain Identity Management* (SCIM) a été soumis à l'IETF en mars 2014. Il est actuellement en version de travail (draft). Ce protocole permet de gérer facilement l'identité des utilisateurs dans des applications et services d'infonuagique.

BIOAPI 2.0 – À considérer

La première version de BIOAPI est une API (*Application Programming Interface*) qui a fait l'objet d'une norme internationale ISO 19784. Le but du BIOAPI est de promouvoir l'interopérabilité des systèmes applicatifs qui utilisent des données biométriques. Ainsi, ces systèmes pourront intégrer des composants fournis par différents fournisseurs.

- ## Protocoles contribuant à la mise en œuvre du chiffrement

IPSec – À retenir

Internet Protocol Security (IPSec) a été développé pour assurer la confidentialité du flux de paquets de données sur des réseaux IP. Il a été conçu pour assurer des communications privées et protégées sur ces réseaux. Il fournit un service de sécurisation des échanges par cryptographie comprenant le contrôle de l'intégrité, le contrôle d'accès et la confidentialité. Le protocole décrit comment intégrer, à la couche réseau, le chiffrement des paquets IP ; toutefois, il ne spécifie pas d'algorithme particulier de chiffrement à employer. Le chiffrement peut être appliqué selon deux approches : transport ou tunnel. Ce protocole est utilisé pour créer des réseaux privés virtuels (VPN) et, autre avantage, il peut aussi garantir l'authenticité des différents équipements composant le réseau VPN. Toutefois, n'ayant aucun moyen de communiquer avec la couche application, il ne peut offrir d'assurance quant à la permanence de l'application de ce mécanisme.

TLSv1.2 – À retenir

Le *Transport Layer Security* (TLS) est un protocole de sécurisation des échanges sur Internet utilisant la cryptographie ; il a été décrit dans la RFC5246. Le TLS remplace son prédécesseur le SSL. Il fonctionne suivant un mode client-serveur et satisfait aux quatre mesures de sécurité suivantes : authentification du serveur, confidentialité des données échangées, intégrité des données échangées et authentification du client, et ce, de manière optionnelle. Le TLS se situe entre la couche application (comme HTTP, FTP, SMTP) et la couche transport TCP. Le

protocole est implémenté par les protocoles applicatifs de la pile Internet pour sécuriser les échanges s'appuyant sur des protocoles applicatifs (FTP, http, LDAP, VPN etc.).

DTLS v1.2 – À retenir

Bien que TLS soit largement utilisé, il ne peut être utilisé pour les protocoles datagramme comme UDP et DCCP. En effet, les datagrammes ne fournissent aucune garantie quant à la réception des paquets de données, ce qui rend difficile l'utilisation de TLS pour sécuriser les communications. Pour remédier à ce problème, l'IETF a proposé le DTLS (*Datagram Transport Layer Security*) dans la RFC 6347. Ce protocole offre une sécurité des échanges, comparable à celle de TLS, basée sur des protocoles en mode datagramme.

WTLS – À retenir

Le *Wireless Transport Layer Security* (WTLS) est un composant du protocole de communication WAP (*Wireless Application Protocol*) qui permet d'accéder à Internet à partir d'un appareil de transmission sans fil, comme un téléphone portable ou un assistant personnel. WTLS est dérivé de TLS et adapté aux appareils à faible bande passante. Il utilise des algorithmes de la cryptographie moderne et, comme TLS, il permet des communications chiffrées entre un client et un serveur.

SSH v2 – À retenir

Le *Secure Shell* (SSH) est un protocole de communication qui sécurise l'échange entre client et serveur en créant un tunnel chiffré. Il est défini dans la RFC 4251 et existe tant en version commerciale qu'en version libre (*Open SSH*). Le protocole SSH est approprié pour accéder à distance à tout type de serveur lorsque le chiffrement de la session est nécessaire, comme avec SFTP.

X.509 – À retenir

Le X.509 est un cadre architectural pour la réalisation d'un service d'authentification basé sur l'usage de certificats numériques (infrastructure à clé publique). X.509 a fait l'objet d'une RFC 5280 qui définit la structure du certificat électronique, et un algorithme assurant la validation du chemin de la certification. Le cadre supporte plusieurs algorithmes de chiffrement (RSA, DSA, etc.).

DNSsec – À retenir

Le *Domain Name System Security Extensions* (DNSsec) est un protocole de l'IETF permettant de garantir l'authenticité et l'intégrité des données DNS. Les spécifications sont publiées dans la RFC 4033. Le protocole utilise la cryptographie avec clé publique pour signer les données DNS, ce qui assure l'intégrité des données de bout en bout. Il faut noter que ce protocole n'assure pas la confidentialité des données.

IKE/ISAKMP – À retenir

Le protocole *Internet Key Exchange* (IKE) a été défini dans le RFC 4306 comme IKEv2. Ce protocole est chargé de négocier la connexion. Avant qu'une transmission IPSec puisse être faite, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées. Ce protocole permet deux types d'authentification, PSK (*Pre-Shared Key*

ou secret partagé) pour la génération de clés de session RSA ou à l'aide de certificats. Le protocole *Internet Security Association and Key Management Protocol* (ISAKMP) est défini comme un cadre pour établir, négocier, modifier et supprimer des associations de sécurité (AS) entre deux parties. IPsec utilise une association de sécurité pour indiquer comment les parties vont faire usage des en-têtes d'authentification et de l'encapsulation d'un paquet.

HTTPS 1.1– À retenir

L'*HyperText Transfer Protocol Secure* (HTTPS) est une version sécurisée de HTTP. HTTPS permet à l'usager de vérifier l'identité du site Web auquel il accède, grâce à un certificat d'authentification délivré par une autorité tierce, réputée fiable. Il peut permettre de valider l'identité de l'usager si celui-ci utilise également un certificat d'authentification client. Il est à retenir pour les échanges sécurisés.

FTPS – À retenir

Le *File Transfer Protocol Secure* (FTPS) est la variante de FTP protégée par les protocoles SSL. Il permet à l'usager de vérifier l'identité du serveur auquel il accède, grâce à un certificat d'authentification. Il permet également de chiffrer la communication. FTPS est à retenir dans le cas d'échanges de fichiers sur un réseau non sécurisé.

SFTP – À retenir

Le *SSH File Transfer Protocol* (SFTP) est un protocole sécurisé de transport de fichiers qui utilise SSH pour ses connexions. Le transport des fichiers bénéficie ainsi de la meilleure sécurité possible. Il y a deux avantages à utiliser SFTP au lieu de FTP : les mots de passe ne sont jamais transférés d'une façon lisible, ce qui empêche toute attaque de type écoute passive, et les données sont chiffrées pendant le transfert, ce qui rend difficile l'espionnage ou la modification de la connexion.

STARTTLS – À retenir

Le STARTTLS est une extension utilisée, entre autres, par le protocole SMTP (RFC 3207) afin de sécuriser une transaction en créant un tunnel TLS (chiffré) entre deux serveurs de messagerie. Avec STARTTLS, la session commence en clair, le serveur annonce qu'il supporte SSL et l'usager peut passer tout de suite en mode chiffrement sur le même port initial. La session est intégralement en SSL. Il est recommandé de proposer l'extension ESMTP STARTTLS sur les serveurs de messagerie, mais sans exiger que les usagers l'utilisent. Le STARTTLS est employé aussi par IMAP, POP3, FTP, LDAP, etc.

S/MIME 3.2 – À retenir

Le protocole *Secure/Multipurpose Mail Internet Extensions* (S/MIME) est une extension de MIME définie dans la RFC 5751. Il permet de signer et de chiffrer le contenu des courriers électroniques avec fichiers joints. Grâce à un mécanisme de cryptographie et à une infrastructure à clé publique, S/MIME offre les services de sécurité suivants : authentification, intégrité et confidentialité.

OpenPGP – À retenir

L'*Open Pretty Good Privacy* (OpenPGP) est un protocole proposé par l'IETF dans la RFC 4880 et servait initialement au chiffrement et à l'authentification du courriel. Il fournit un cadre de format afin de sécuriser l'échange et le stockage de données. Il définit le format des messages, signatures ou certificats qui peuvent être utilisés.

XML SIGNATURE v1.1 – À retenir

XML SIGNATURE est un ensemble de spécifications qui précisent les règles de syntaxe et de traitement pour créer et représenter les signatures numériques. C'est une recommandation flexible de W3C pour signer des documents de différente nature. Il est même possible de signer des portions particulières d'un même document.

XADES v1.4.1 – À retenir

Le *XML Advanced Electronic Signatures* (XAdES) est une extension de *XML SIGNATURE* proposée par l'Institut européen des standards en télécommunication (ETSI). Cette extension permet surtout au document signé de rester valide pendant une longue période.

XMLenc v1.1 – À retenir

Élaboré par le W3C, le *XML ENCRYPTION* (XMLenc) spécifie un procédé pour chiffrer des données et les représenter en format XML. Les données peuvent être de différente nature, document XML, un ou plusieurs éléments XML ou même le contenu d'un élément XML. *XML SIGNATURE* et *XMLenc* constituent un cadre de référence largement utilisé par les standards de l'industrie (WSS, SAML, etc.).

XML Decryption Transform – À retenir

Le *XML Decryption Transform* (Transformé de déchiffrement XML) est une spécification du W3C qui permet de vérifier, lorsqu'une partie d'un document XML est chiffrée, si le chiffrement a été appliqué avant ou après la signature XML.

3.4.3 Protocoles de sécurité associés au niveau intégration

WS-I Basic Security Profile v1.1 – À retenir

La *Web Services Interoperability Organization* (WS-I () a élaboré le *Basic Security Profile* v1.1 qui représente une extension du Basic Profile v1.0 traitant des spécifications de sécurité. Le *Basic Security Profile* v1.1 est conçu pour supporter l'ajout de fonctionnalités de sécurité aux enveloppes et messages SOAP ainsi qu'au niveau de la couche de transport des services Web pour favoriser l'interopérabilité.

WS-Security v1.1 – À retenir

Le *Web Service Security v1.1* est un standard de l'OASIS qui ajoute aux spécifications existantes une structure pour incorporer des mécanismes d'authentification, de signature et de chiffrement dans un message SOAP, mécanismes utilisables lors de l'implémentation de services Web. Cette spécification est flexible et conçue pour sécuriser les services Web avec une grande variété de modèles de sécurité, entre autres l'utilisation de SAML, de Kerberos et de certificats X.509. Il

décrit comment *XML Encryption* et *XML Signature* doivent être appliqués aux documents ou messages SOAP.

WS-Policy – À retenir

La *WS-Policy* définit un cadre et un modèle pour la spécification des propriétés des services Web sous la forme de politiques ou règles (policies). Elle est une spécification qui permet, entre autres, de préciser les possibilités ou les contraintes associées à un service Web particulier, de sécurité ou autre (algorithmes de chiffrement supportés, certificat exigé, etc.).

WS-Security Policy v1.2 – À retenir

La *WS-Security Policy* est une spécification de services Web qui est devenue un standard de l'OASIS à partir de la version 1.2. Elle étend les spécifications de sécurité des protocoles *WS-Security*, *WS-Trust* et *WS-SecureConversation*. Elle permet de spécifier qui est autorisé à accéder un service et comment il peut y accéder. Elle peut aussi déterminer les méthodes d'authentification ainsi que le niveau de chiffrement, etc.

WS- SecureConversation – À retenir

WS-SecureConversation est une spécification de services Web qui travaille en collaboration avec *WS-Security, WS-Trust* et *WS-Policy* afin de créer et de partager des contextes de sécurité assurant l'établissement des clés, l'efficacité du chiffrement et la vérification d'intégrité des messages SOAP échangés. Cette spécification définit un cadre pour la demande et la délivrance des jetons de sécurité et la négociation des relations de confiance.

WS-Trust v1.3 – À retenir

WS-Trust est une extension de *WS-Security* qui est un protocole permettant de délivrer, de renouveler ou de valider les jetons de sécurité. Cette spécification est destinée à fournir un ensemble flexible de mécanismes qui peuvent être utilisés pour supporter une série de protocoles de sécurité. En utilisant les extensions définies dans *WS-Trust*, les applications peuvent s'engager dans une communication sécurisée, conçue pour travailler dans le cadre de services Web.

WS-Federation v1.2 – À retenir

WS-Federation est une spécification du consortium OASIS, qui spécifie et définit des mécanismes de fédération de domaines de confiance hétérogènes. WS-Federation est une extension de *WS-Trust* et elle s'appuie sur les autres spécifications de la famille WS- d'OASIS, notamment *WS-Security*, *WS-Policy* et *WS-SecureConversation*. C'est un langage de description de règles de confiance qui permet de gérer les relations de confiance entre des environnements hétérogènes. Concrètement, elle permet d'effectuer l'authentification mutuelle d'applications utilisant des approches de sécurité différentes (authentification Kerberos, X.509, etc.).

ID-WSF 2.0 – À retenir

L'*Identity Web Services Framework* (ID-WSF) est une spécification de l'organisation Liberty Alliance qui définit l'interopérabilité des identités entre services Web dans un environnement d'identité fédéré. Sa particularité est qu'il supporte le standard SAML 2.0, ce qui doit faciliter son implémentation.

XKMS 2.0 – À retenir

Le *XML Key Management Specification* (XKMS) est un protocole de W3C pour enregistrer, localiser, distribuer et valider une clé de chiffrement publique. Il est utilisé conjointement avec *XML Signature* et *XMLenc*. XKMS est composé de deux parties : XKISS pour les requêtes de localisation et de validation des clés publiques et XKRSS pour enregistrer, renouveler, révoquer et obtenir des clés.

3.4.4 Mécanismes de chiffrement

- **Algorithmes de chiffrement asymétrique**

RSA – À retenir

Le *Rivest Shamir Aldeman* (RSA) est un algorithme de chiffrement asymétrique très connu, qui utilise une paire de clés composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Lorsqu'il est utilisé, l'algorithme garantit la confidentialité, l'intégrité et la non-répudiation. Cet algorithme peut être aussi utilisé pour la signature numérique, dans ce cas, la clé privé sert à chiffrer tandis que la clé publique est utilisée à déchiffrer les données. La longueur de la clé du chiffrement dépend de la valeur des données à protéger. Par exemple, pour de l'information très confidentielle, il est recommandé d'utilisé au minimum 2048 bits.

Exponiation dans un corps fini (Diffie-Hellman) – À retenir

Les publications 800-56a du NIST et FIPS 186.3 indiquent les protocoles d'établissement de clés à partir d'une méthode à base de logarithmes discrets ainsi que la spécification des paramètres. Le logarithme discret est utilisé pour le chiffrement à clé publique, (échange de clés Diffie-Hellman et le chiffrement El Gamal). Ils interviennent également dans la conception des chiffrements à clé symétrique (secrète) comme le standard AES.

ECC – À retenir

L'*Elliptic Curve Cryptography* (ECC) est un algorithme à clé publique de cryptographie de courbe elliptique. L'algorithme ECC accepte la création de signatures numériques et l'échange de clés pour chiffrer ou authentifier le contenu. La définition du traitement de l'algorithme se fonde sur la norme ANSI X9.62, développée par le groupe de travail ANSI X9F1, sur la norme IEEE 1363 et la norme SEC 1.

- **Algorithmes de chiffrement symétrique**

3DES – À retenir

Le *Triple Data Encryption Standard* (3DES) est un algorithme de chiffrement symétrique par blocs appliquant successivement trois fois l'algorithme DES avec deux ou trois clés différentes, d'où son nom. Il a été publié en 1999 par IBM. Le chiffrement symétrique utilise la même clé pour chiffrer et déchiffrer les données, ce qui rend ces algorithmes plus rapides que les algorithmes asymétriques.

AES – À retenir

L'*Advanced Encryption Standard* (AES) est un algorithme de chiffrement symétrique par blocs fixes de 128 bits, publié en 2001 par le NIST dans le FIPS PUB197. La longueur de la clé de chiffrement peut être de 128,192 ou 256 bits.

CAST5 – À retenir

Le *Carlisle Adams/Stafford Tavares* (CAST-128 ou CAST5) est un algorithme de chiffrement symétrique par blocs utilisé par plusieurs logiciels, dont certaines versions de PGP. Il a été approuvé au Canada par le *Communications Security Establishment* pour une utilisation gouvernementale. Malgré un brevet déposé par Entrust sur la conception CAST, CAST-128 est disponible partout sans frais pour des applications commerciales ou non commerciales.

IDEA – À retenir

L'*International Data Encryption Algorithm* (IDEA) est un algorithme de chiffrement symétrique suisse publié en 1991. Il utilise une clé de chiffrement de 128 bits pour chiffrer et déchiffrer des blocs de données de 64 bits. L'algorithme applique huit fois une même transformation suivie d'une transformation finale.

- ## Algorithmes de signature numérique

DSS – À retenir

Le *Digital Signature Standard* (DSS) est un standard américain du FISP 186-4 (*Federal Information Processing Standard*). Le standard a été publié la première fois en 1994 et révisé plusieurs fois par la suite. Il spécifie une série d'algorithmes qui peuvent être utilisés pour la signature numérique. Il s'agit de RSA, DSA et ECDSA.

RSA – À retenir

Tel que spécifié précédemment, l'algorithme RSA peut être utilisé pour signer numériquement des données selon les normes ANSI X9.31 et RSA PKCS #1 v2.1 et les directives du FIPS 186-3. Le module doit être d'au moins 2048 bits.

DSA – À retenir

Le *Digital Signature Algorithm* (DSA) est un algorithme de signature numérique standardisé par le NIST. Cet algorithme fait partie de la spécification DSS pour *Digital Signature Standard* adoptée en 1993 (FIPS 186). Le standard a été amélioré en 2002 dans FIPS 186-2. Il est couvert par un brevet, mais il peut être utilisé gratuitement. Le protocole de signature est défini dans la norme FIPS 186-3. La longueur du module doit être d'au moins 2048 bits.

Exponiation dans un corps fini – À retenir

La cardinalité du corps doit être un nombre premier et elle doit être d'une longueur d'au moins 2048 bits.

ECDSA – À retenir

L'*Elliptic Curve Digital Signature Algorithm* (ECDSA) est un algorithme asymétrique de signature numérique décrit dans la norme ANSI X9.62, qui doit être mis en œuvre selon les directives du FIPS 186-3. Il est basé sur l'algorithme DSA et utilise la théorie des courbes elliptiques. Pour un niveau de sécurité comparable à celui des algorithmes RSA et DSA, la signature avec ECDSA utilise des clés plus courtes, ce qui rend les opérations de signature plus rapides et plus performantes.

- ### Algorithmes de hachage

SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512) – À retenir

Le *Secure Hash Algorithm* (SHA-2) est une famille de fonctions de hachage qui ont été conçues par la *National Security Agency* des États-Unis (NSA). Les algorithmes de la famille SHA-2, SHA-256, SHA-384 et SHA-512 sont décrits et publiés en compagnie de SHA-1 dans le FIPS 180-2 (*Secure Hash Standard*) datant de 2002. La fonction SHA-224 a été ajoutée un peu plus tard. En 2005, des problèmes de sécurité de SHA-1 sont apparus. Bien que l'algorithme de SHA-2 partage des similarités avec celui de SHA-1, ces attaques n'ont pas pu être étendues à SHA-2 jusqu'à maintenant.

SHA-3 – À considérer

La SHA-3 est une nouvelle fonction de hachage cryptographique qui a été sélectionnée en octobre 2012 par le NIST en raison des faiblesses découvertes sur MD-5 et SHA-1, qui laissaient craindre une fragilité de SHA-2 qui est construit sur le même schéma. Elle est basée sur un principe différent de celui des fonctions MD5, SHA-1 et SHA-2. Elle n'est pas destinée à remplacer SHA-2, qui n'a à l'heure actuelle pas été compromise par une attaque significative, mais à fournir une solution de remplacement considérant les possibilités d'attaques contre les standards MD5, SHA-0 et SHA-1. Elle possède des variantes qui peuvent produire un hachage de 224, 256, 384 et 512 bits.

AES – À retenir

L'algorithme AES peut être utilisé pour le hachage (128 bits et plus).

3DES – À retenir

L'algorithme 3DES, connu aussi sous le nom de 3DEA, peut être utilisé pour le hachage (clés à double longueur au minimum).

RSA – À retenir

L'algorithme RSA peut être utilisé pour le hachage (1024 bits et plus).

ECC – À retenir

L'algorithme ECC peut être utilisé pour le hachage (160 bits et plus).

ElGamal – À retenir

L'algorithme basé sur l'exponiation dans un corps fini (ElGamal) peut être utilisé pour le hachage (1024 bits et plus).

- ## Algorithmes d'intégrité des données

HMAC – À retenir

Le HMAC est un code d'authentification de message basé sur la fonction de hachage. Il sert à assurer l'intégrité des données et l'authentification de l'origine des données. Il est défini dans la norme FIPS 198 et la norme ANSI X9.71.

CMAC – À retenir

Le CMAC est un code d'authentification de message basé sur la fonction de chiffrement. Il sert à assurer l'intégrité des données et l'authentification de l'origine de ces données. Il doit être utilisé avec l'algorithme AES dont la longueur d'étiquette doit être au minimum de 122 bits (voir les prescriptions de la publication du 800-38B du NIST).

Aide-mémoire

Sécurité

Niveau	Catégorie	Sous-catégorie	Norme / Standard	Statut	Propriétés de sécurité				
					D	I	C	A	N-R
Interconnection	Couche physique	-	-	-	-	-	-	-	-
	Couche liaison	Identification & authentification	EAP	À retenir	-	X	X	-	-
			IEEE 802.1X	À retenir	-	X	X	-	-
	Couche réseau	Chiffrement	IPSec	À retenir	-	X	X	X	-
	Couche transport	-	-	-	-	-	-	-	-
	Couche Session		TLS v1.2	À retenir	-	X	X	X	X
		Chiffrement	DTLS v1.2	À retenir	-	X	X	X	-
			WTLS	À retenir	-	X	X	X	-
			SSH v2	À retenir	-	X	X	X	-
	Couche présentation	Chiffrement	XML SIGNATURE v1.1	À retenir	-	X	-	-	-
			XADES v1.4.1	À retenir	-	-	X	-	-
			XMLenc v1.1	À retenir	-	-	X	-	-
			XML Decryption transform	À retenir	-	X	X	-	-
			XKMS 2.0	À retenir	-	X	X	-	-
		ICP	X.509	À retenir	-	X	X	X	-
		Authentification & autorisation	SAML 2.0	À retenir	-	X	X	X	-
			XACML v3.0	À retenir	-	X	X	X	-
	Couche application	Chiffrement	IKE/ISAKMP	À retenir	-	-	X	-	-
			DNSsec	À retenir	-	X	X	-	-
			HTTPS	À retenir	-	X	X	-	-
			FTPS	À retenir	-	X	X	-	-
			SFTP	À retenir	-	X	X	-	-
			STARTTLS	À retenir	-	X	X	-	-
			S/MIME v3.2	À retenir	-	-	X	X	-
			OpenPGP	À retenir	-	X	X	X	X
		Identification, authentification, autorisation	LDAP v3	À retenir	-	X	X	X	-
			RADIUS	À retenir	-	X	X	X	-
			KERBEROS v5	À retenir	-	X	X	X	-
			TACACS	À retenir	-	X	X	X	-

D: Disponibilité, I: Intégrité, C: Confidentialité, A: Authentification, N-R: Non Répudiation

Niveau	Catégorie	Sous-catégorie	Norme / Standard	Statut	Propriétés de sécurité				
					D	I	C	A	N-R
Interconnection	Couche application	Identification, authentification, autorisation	TACACS+	À retenir	-	X	X	X	-
			DIAMETER	À retenir	-	X	X	X	-
			Open ID	À considérer	-	-	X	X	-
			Open ID Connect v1.0	À considérer	-	X	X	X	-
			0Auth 2.0	À considérer	-	X	X	X	-
			SCIM	À considérer	-	X	X	X	-
		Biométrie	BIOAPI v2.0	À considérer	-	X	X	X	-
Intégration	Services Web	Architecture SOAP	WS-I Basic Security Profil v1.1	À retenir	-	X	X	-	-
			WS-Security v1.1	À retenir	-	X	X	X	-
			WS-Policy	À retenir	-	X	X	-	-
			WS-Security Policy	À retenir	-	X	X	-	-
			WS-Secure Conversations	À retenir	-	X	X	-	-
			WS-Trust v1.3	À retenir	-	X	X	X	-
			WS-Federation v1.2	À retenir	-	X	X	X	-
			ID WSF v2.0	À retenir	-	X	X	X	-
S/O	Chiffrement	Asymétrique	RSA	À retenir	-	-	X	-	-
			Exponiation dans un corps fini	À retenir	-	-	X	-	-
			ECC	À retenir	-	-	X	-	-
		Symétrique	3DES	À retenir	-	-	X	-	-
			AES	À retenir	-	-	X	-	-
			CAST5	À retenir	-	-	X	-	-
			IDEA	À retenir	-	-	X	-	-
		Signature numérique	DSS	À retenir	-	X	X	X	X
			RSA	À retenir	-	X	X	X	X
			DSA	À retenir	-	X	X	X	-
			Exponiation dans un corps fini	À retenir	-	-	X	-	-
			ECDSA	À retenir	-	X	-	-	-
		Hachage	SHA v2	À retenir	-	X	-	-	-
			SHA v3	À considérer	-	X	-	-	-

D: Disponibilité, I: Intégrité, C: Confidentialité, A: Authentification, N-R: Non Répudiation

Niveau	Catégorie	Sous-catégorie	Norme / Standard	Statut	Propriétés de sécurité				
					D	I	C	A	N-R
S/O	Chiffrement	Hachage	AES	À retenir	-	X	-	-	-
			RSA	À retenir	-	X	-	-	-
			ECC	À retenir	-	X	-	-	-
			ElGamal	À retenir	-	X	-	-	-
		Intégrité des données	HMAC	À retenir	-	X	-	-	-
			CMAC	À retenir	-	X	-	-	-

D: Disponibilité, I: Intégrité, C: Confidentialité, A: Authentification, N-R: Non Répudiation

3.5 Profils normatifs de service

3.5.1 Services de messagerie électronique

- Protocoles de transfert de courriels

SMTP – À retenir

SMTP est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique. Il doit s'appliquer dans les communications avec l'extérieur comme protocole de passerelle entre systèmes et entre organismes publics en passant par Internet.

- Protocoles de manipulation de courriels

POP 3 – À retenir

Le protocole POP 3 (*Post Office Protocol*) permet à un client de récupérer ses messages sur un serveur de courriels distant. Le RFC 1939 définit les spécifications de POP 3, version actuelle. Quant au RFC 2449, il ajoute quelques extensions à la version précédente, notamment celles permettant d'améliorer la sécurité par la commande d'authentification. Pour les clients de messageries, l'utilisation de clients POP 3 est à retenir par les organismes publics. Partant du fait que le niveau de sécurité du protocole POP 3 est relativement faible, il est fortement recommandé de n'utiliser POP 3 qu'avec SSL.

IMAP 4.1 – À retenir

Le protocole IMAP (*Internet Message Access Protocol*), comme POP3, permet à un client de messagerie de lire et de manipuler ses messages sur un serveur de courriels distant. Ce sont deux manières fonctionnellement différentes d'aller chercher du courrier électronique sur un serveur, la différence essentielle étant qu'avec IMAP une copie des messages reste sur le serveur. Pour les clients de messageries, l'utilisation de clients d'IMAP 4.1 est à retenir et même préférée à POP 3 par les organismes publics.

3.5.2 Services multimédias

- Visioconférence

H.320 – À retenir

H.320 est un protocole et une recommandation définie par l'UIT-T. Il définit les terminaux, type téléphone, station de visioconférence, etc. connectés sur le réseau RNIS. Les principaux protocoles appartenant à cette suite sont H.221, H.230 et H.242. Les codecs audio comme G.711 et vidéo comme H.261 et H.263. H.320 spécifient les caractéristiques techniques des systèmes et équipements de terminaux visiophoniques à bande passante étroite typiquement pour des services de visioconférence et de visiophonie.

La spécification d'une bande passante se définit par un débit variant de 64 kbit à 1920 kbit.

H.323 – À retenir

H.323 regroupe un ensemble de protocoles de communication de la voix, de l'image et de données sur IP. C'est un protocole développé par l'UIT-T qui le définit comme un « Systèmes de communication multimédia en mode paquet ». Il est dérivé du protocole utilisé sur RNIS.

Plus qu'un protocole, H.323 ressemble davantage à une association de plusieurs protocoles différents qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec et le transport de l'information.

- Pour le contrôle et la signalisation : H.225, H.245, Q.931, RTCP.
- Pour la voix : G.711, G.722, G.723, G.726, G.728, G.729.
- Pour la vidéo : H.261, H.263, H.264.
- Pour les données : T.123, T.124, T.125.

3.5.3 Architecture orientée services

- Messagerie

SOAP 1.1 – À retenir

(Voir section 3.2)

SOAP 1.2 – À considérer

(Voir section 3.2)

MTOM – À retenir

(Voir section 3.2)

XOP – À retenir

(Voir section 3.2)

- Répertoire de publication

  UDDI v3 – À retenir

  (Voir section 3.2)

- Langage de description

  WSDL 2.0 – À retenir

  (Voir section 3.2)

  WSDL 1.1 – À considérer

  (Voir section 3.2)

- Structure des données échangées

  XML – À retenir

  (Voir section 3.3)

- Transport des données

  HTTP - TCP/IP – À retenir

  (Voir section 3.1)

- Orchestration

  WS-BPEL2.0 – À retenir

  (Voir section 3.2)

  WS-CDL – À retenir

  (Voir section 3.2)

- Gestion transactionnelle

  XAML – À retenir

  (Voir section 3.2)

Aide-mémoire

Profils normatifs de service

Architecture	Catégorie	Sous-catégorie	Norme Standard	Statut
Services de messagerie électronique	Protocole de transfert		SMTP	À retenir
	Protocole de manipulation		POP 3	À retenir
			IMAP 4.1	À retenir
Services multimédias	Visioconférence		H.320	À retenir
			H.323	À retenir
	Codecs	Audio	Vorbis (OGG)	À retenir
			FLAC	À retenir
		Vidéo	H.261/H.263	À retenir
			VP8	À retenir
			VP9	À considérer
Architecture orientée services	Messagerie		SOAP 1.1	À retenir
			SOAP 1.2	À considérer
			MTOM	À retenir
			XOP	À retenir
	Répertoire de publication		UDDI	À retenir
	Langage de description		WSDL 1.1	À considérer
			WSDL 2.0	À retenir
	Structure des données échangées		XML	À retenir
	Transport des données		HTTP-TCP/IP	À retenir
	Orchestration		WS-BPEL 2.0	À retenir
			WS-CDL	À retenir
	Gestion transactionnelle		XAML	À retenir

Annexe

Composition du comité interministériel responsable de l'élaboration du Cadre commun d'interopérabilité du gouvernement du Québec

Lors des travaux du comité interministériel, les organismes publics membres du comité étaient représentés par les personnes suivantes :

Responsable et rédacteur du projet

Talel Korkobi, Yassine Maghlout
Secrétariat du Conseil du trésor

Comité interministériel

• Stéphane Asselin	Centre de services partagés du Québec
• Dominic Pagé	Commission de la santé et de la sécurité du travail
• Dawn Angele Alexander	Ministère de l'Agriculture, des Pêcheries et de l'Alimentation
• Luigi Matei	Ministère de l'Emploi et de la Solidarité sociale
• Hugues Bernard	Ministère de la Famille
• Frédéric Serrault	Ministère des Finances et de l'Économie
• Gaston Gagné	Ministère des Ressources naturelles
• Pena Gerardo	Ministère des Ressources naturelles
• Johnson-Marcelino Darcelin	Ministère de la Santé et des Services sociaux
• Daniel Bouchard	Ministère des Transports
• Michel Bouchard	Ministère des Transports
• Hugues Beaudoin	Régie de l'assurance maladie du Québec
• Robert Trudel	Régie de l'assurance maladie du Québec
• Sylvie Marcotte	Régie des rentes du Québec
• Jalil Emmanuel	Secrétariat du Conseil du trésor
• Josée Gauthier	Secrétariat du Conseil du trésor
• Dave Tanguy	Secrétariat du Conseil du trésor
• Michel Plaisance	Société de l'assurance automobile du Québec
• Yves Sicard	Société de l'assurance automobile du Québec

D’autres comités ont collaboré aux travaux d’élaboration du CCIGQ, notamment :

Table des conseillers en architecture d’entreprise

• Diane Thibault	Commission de la santé et de la sécurité du travail
• Stéphane Vachon	Commission de la santé et de la sécurité du travail
• Simon Cloutier	Directeur de l’état civil
• Zouheir Naja	Directeur général des élections du Québec
• Dominic Bégin	Ministère du Conseil exécutif
• Sylvie Guay	Ministère du Développement durable de l’Environnement, de la Faune et des Parcs
• Patrick Bédard	Ministère des Finances et de l’Économie
• Julio Brito	Ministère des Finances et de l’Économie
• Caroline Moyen	Ministère des Finances et de l’Économie
• Jacques St-Hilaire	Ministère des Relations internationales de la Francophonie et du Commerce extérieur
• Louise Légaré	Ministère de la Santé et des Services sociaux
• Daniel Bouchard	Ministère des Transports
• Marie-Andrée Lefebvre	Régie des rentes du Québec
• Louis Mimeault	Régie des rentes du Québec
• Guy Carigna	Revenu Québec
• Myriam Cyr	Services Québec
• Alain Martel	Services Québec
• Hugo Roberge	Société de l’assurance automobile du Québec
• Gisèle Léger	Sûreté du Québec

Sous-groupes de la Table des conseillers en architecture d'entreprise

- Brigitte Fournier — Centre de services partagés du Québec
- Claire Lemoine — Centre de services partagés du Québec
- Alexandre Paquette-Dussault — Centre de services partagés du Québec
- Gérard Guité — Commission de la santé et de la sécurité du travail
- Dominic Pag — Commission de la santé et de la sécurité du travail
- Jean Arsenault — Ministère de l'Éducation, du Loisir et du Sport
- Richard Pelletier — Ministère des Ressources naturelles
- Louise Légaré — Ministère de la Santé et des Services sociaux
- Sylvie Marcotte — Régie des rentes du Québec
- Guy Carignan — Revenu Québec
- Diane Bernier — Services Québec
- Yves Dumas — Services Québec

Table de concertation du logiciel libre

- Martin Durand — Cégep de Sainte-Foy
- Claire Lemoine — Centre de services partagés du Québec
- Abdallah Benabbes — Commission des droits de la personne et des droits de la jeunesse
- Mario Gagnon — Commission scolaire des Affluents
- Serey-Pheak Sea — Ministère de l'Agriculture, des Pêcheries et de l'Alimentation
- François Maltais — Ministère de la Famille
- Mateus Fernandes — Ministère des Finances et de l'Économie
- Daniel Pelletier — Ministère de la Santé et des Services sociaux
- Michel Rochette — Ministère de la Santé et des Services sociaux
- Nicolas Gignac — Ministère de la Sécurité publique
- Carl Pelletier — Ministère des Ressources naturelles
- Hugues Beaudoin — Régie de l'assurance maladie du Québec
- Benoît des Ligneris — Révolution Linux
- Gabriel Cossette — Services partagés Canada
- Éric Marcoux — Université Laval

Comité interministériel (volet sécurité)

• Stéphane Fleurant	Centre de services partagés du Québec
• Nicolas Tanguay	Commission de la santé et de la sécurité du travail
• Jean-François Laverdière	Régie de l'assurance maladie du Québec
• Ayda Saidane	Revenu Québec
• Daniel Faucher	Ministère de l'Emploi et de la Solidarité sociale
• Benoît Dicaire	Ministère de la Justice
• Imed Masmoudi	Ministère de la Justice
• Ghyslain Garceau	Ministère du Transport
• Jean Rhéaume	Secrétariat du Conseil du trésor
• Ilario Pedron	Sûreté de Québec

Secrétariat
du Conseil du trésor
Québec