



ENTRUST.NET

***Énoncé de pratiques de certification pour serveurs
Web SSL***

Version: 2.02
1^{er} janvier 2002

Copyright © Entrust.net Inc., 1999-2002. Tous droits réservés.

Versions antérieures

Version	Date	Changements apportés
1.0	26 mai 1999	Première version
2.0	1 ^{er} juillet 2000	Ajout de dispositions portant sur des entités subordonnées (par exemple, des tierces autorités d'enregistrement) dans l'infrastructure à clé publique Entrust.net pour serveurs Web SSL. Révision de nombreuses autres modalités.
2.02	1 ^{er} janvier 2002	Révisions mineures concernant le remplacement du Certificat co-certifié.

TABLE DES MATIÈRES

1.	Introduction	1
1.1	Aperçu	1
1.2	Titre.....	1
1.3	Communauté et application.....	1
1.3.1	Autorités de certification	1
1.4	Renseignements.....	3
1.4.1	Mise en œuvre.....	3
1.4.2	Renseignements	3
2.	Dispositions générales.....	4
2.1	Obligations.....	4
2.1.1	Obligations de l'autorité de certification	4
2.1.2	Obligations de l'autorité d'enregistrement.....	4
2.1.3	Obligations de l'abonné.....	5
2.1.4	Obligations de la partie utilisatrice	7
2.1.5	Obligations de l'entité responsable du Répertoire	8
2.2	Responsabilité	9
2.2.1	Responsabilité des AC	9
2.2.1.1	Garanties et limitations des garanties.....	9
2.2.1.2	Dénégations.....	10
2.2.1.3	Plafond des pertes	10
2.2.1.4	Autres exclusions	12
2.2.1.5	Activités dangereuses.....	13
2.2.2	Responsabilité des AE	13
2.3	Responsabilité financière.....	13
2.3.1	Garantie offerte par les parties utilisatrices.....	13
2.3.2	Rapports de fiduciaire.....	15
2.3.3	Processus administratifs.....	15
2.4	Interprétation et application	15
2.4.1	Lois applicables	15
2.4.2	Dissociabilité, maintien, regroupement et avis	16
2.4.3	Règlement des différends.....	19
2.5	Honoraires	20
2.5.1	Frais d'émission ou de renouvellement d'un certificat.....	20
2.5.2	Frais d'accès.....	20
2.5.3	Frais d'accès à des renseignements concernant la révocation ou l'état	20
2.5.4	Frais pour autres services comme des renseignements sur les politiques.....	20
2.5.5	Politique de remboursement	20
2.6	Publication et répertoires	21
2.6.1	Publication de renseignements sur les AC	21
2.6.2	Fréquence de la publication	21
2.6.3	Contrôles en matière d'accès.....	21
2.6.4	Répertoires.....	21
2.7	Vérification de conformité.....	21
2.7.1	Fréquence des vérifications de conformité d'une entité	22
2.7.2	Identité/compétences du vérificateur	22

2.7.3	Rapports entre le vérificateur et la partie qui fait l'objet d'une vérification	22
2.7.4	Objet de la vérification	22
2.7.5	Mesures correctrices	22
2.7.6	Communication des résultats	22
2.8	Caractère confidentiel	22
2.8.1	Renseignements confidentiels	23
2.8.2	Renseignements non confidentiels	23
2.8.3	Divulgence de renseignements sur la révocation ou la suspension d'un certificat	23
2.8.4	Divulgence aux responsables de l'application de la loi	23
2.8.5	Divulgence dans le cadre de procédures au civil	23
2.8.6	Divulgence à la demande du propriétaire	24
2.8.7	Autres circonstances dans lesquelles sont divulgués des renseignements	24
2.9	Droits de propriété intellectuelle	24
3	Identification et Authentification	26
3.1	Enregistrement initial	26
3.1.1	Types de noms	26
3.1.2	Noms significatifs	27
3.1.3	Règles d'interprétation des différentes formes de noms	27
3.1.4	Caractère unique des noms	27
3.1.5	Règlement des différends en matière de revendication d'un nom	27
3.1.6	Reconnaissance, authentification et rôle des marques de commerce	27
3.1.7	Preuve de la possession d'une clé privée	29
3.1.8	Authentification de l'identité de l'organisation	29
3.1.9	Authentification de l'identité du particulier	29
3.2	Mise à jour régulière des clés	29
3.3	Mise à jour suivant une révocation	30
3.4	Demande de révocation	30
4	Exigences opérationnelles	31
4.1	Demande de certificat	31
4.2	Émission d'un certificat	31
4.3	Acceptation d'un certificat	31
4.4	Suspension et révocation d'un certificat	31
4.4.1	Circonstances donnant lieu à une révocation	31
4.4.2	Auteur de la demande de révocation	32
4.4.3	Procédure de demande de révocation	32
4.4.4	Délai de grâce	33
4.4.5	Circonstances donnant lieu à une suspension	33
4.4.6	Auteur de la demande de suspension	33
4.4.7	Procédure de demande de suspension	33
4.4.8	Limites relatives à la période de suspension	33
4.4.9	Fréquence de la publication d'une LCR	33
4.4.10	Obligation de vérifier la LCR	33
4.4.11	Révocation en ligne/Disponibilité du service de vérification de l'état	33
4.4.12	Obligation de vérifier les révocations en ligne	33
4.4.13	Autres formes disponibles de publicité des révocations	33
4.4.14	Obligation de vérification relative à d'autres formes de publicité des révocations	34
4.4.15	Obligations spéciales relatives à la compromission d'une clé	34

4.5	Procédures d'audit de sécurité.....	34
4.6	Archivage des dossiers.....	34
4.7	Changement des clés	34
4.8	Reprise en cas de compromission et de sinistre	34
4.9	Cessation des activités des AC	35
5	<i>Contrôles de sécurité des lieux, des procédures administratives et du personnel.....</i>	<i>36</i>
5.1	Contrôles de sécurité des lieux.....	36
5.2	Contrôles de sécurité des procédures administratives	36
5.3	Contrôles de sécurité du personnel	36
6	<i>Contrôles de sécurité technique</i>	<i>37</i>
6.1	Génération et installation de la biclé.....	37
6.1.1	Génération de la biclé	37
6.1.2	Livraison de la clé privée à une entité.....	37
6.1.3	Livraison de la clé publique à l'émetteur de certificats	37
6.1.4	Livraison de la clé publique des AC aux utilisateurs	37
6.1.5	Taille des clés	37
6.1.6	Génération des paramètres de la clé publique.....	37
6.1.7	Vérification de la qualité des paramètres.....	37
6.1.8	Génération des clés par matériel et/ou logiciel	37
6.1.9	Objets de l'utilisation des clés.....	37
6.2	Protection des clés privées	38
6.3	Autres aspects de la gestion des biclés.....	38
6.4	Données d'activation	38
6.5	Contrôles de sécurité des ordinateurs	38
6.6	Contrôles techniques du cycle de vie.....	38
6.7	Contrôles de sécurité réseau	38
6.8	Contrôles d'ingénierie du module cryptographique	38
7	<i>Profils du certificat et de la LCR.....</i>	<i>39</i>
7.1	Profil du certificat	39
7.2	Profil de la LCR.....	39
8	<i>Administration.....</i>	<i>40</i>
8.1	Renseignements.....	40
8.2	Procédures de modification	40
8.3	Politiques en matière de publication et d'avis	40
8.4	Approbation de l'ÉPC.....	40
9	<i>Acronymes</i>	<i>41</i>
10	<i>Définitions</i>	<i>42</i>

1. Introduction

Les autorités de certification Entrust.net pour serveurs Web SSL émettent des certificats Entrust.net pour serveurs Web SSL en vue de contribuer à une protection accrue des communications entre les serveurs et les navigateurs pour le Web qui utilisent le protocole SSL (Secure Sockets Layer). Entrust.net utilise le logiciel primé Entrust/PKI(mc) d'Entrust afin d'offrir des certificats numériques conformes aux normes en la matière permettant une protection accrue des communications en ligne.

1.1 Aperçu

Le présent énoncé de pratiques de certification pour serveurs Web SSL décrit les pratiques et les procédures suivies par (i) les autorités de certification Entrust.net pour serveurs Web SSL et (ii) les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL. Il décrit également les modalités conformément auxquelles Entrust.net offre les services des autorités d'enregistrement et de certification en ce qui concerne les certificats Entrust.net pour serveurs Web SSL. Le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL s'applique à toutes les personnes, entités et organisations, y compris, sans limiter la portée de ce qui précède, à tous les demandeurs, les abonnés, les parties utilisatrices, les revendeurs et les covendeurs et à toute autre personne, entité ou organisation ayant des rapports avec (i) Entrust.net relativement à des certificats Entrust.net pour serveurs Web SSL ou à des services fournis par Entrust.net relativement à des certificats Entrust.net pour serveurs Web SSL ou (ii) toute autorité d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL ou tous les revendeurs ou covendeurs fournissant des services relativement à des certificats Entrust.net pour serveurs Web SSL. Le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL est incorporé par renvoi à tous les certificats Entrust.net pour serveurs Web SSL émis par des autorités de certification Entrust.net pour serveurs Web SSL. Il énonce, à l'intention des demandeurs, des abonnés, des parties utilisatrices, des revendeurs, des covendeurs et autres personnes, entités et organisations, les pratiques et les politiques suivies par les autorités de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL. Le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL prévoit également les droits et obligations d'Entrust.net, de toute tierce autorité d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL, des demandeurs, des abonnés, des parties utilisatrices, des revendeurs et des covendeurs et des personnes, entités ou organisations susceptibles d'utiliser des certificats Entrust.net pour serveurs Web SSL ou de s'y fier ou ayant des rapports avec une autorité de certification Entrust.net pour serveurs Web SSL ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL relativement aux certificats Entrust.net pour serveurs Web SSL ou tout service relatif aux certificats Entrust.net pour serveurs Web SSL.

1.2 Titre

Le présent document est intitulé « Énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ».

1.3 Communauté et application

L'utilisation des certificats Entrust.net pour serveurs Web SSL est restreinte aux serveurs pour le Web utilisant le protocole Secure Sockets Layer. Toute autre utilisation des certificats Entrust.net pour serveurs Web SSL est interdite.

1.3.1 Autorités de certification

Dans l'infrastructure à clé publique Entrust.net pour serveurs Web SSL, les autorités de certification peuvent accepter les DSC et les clés publiques des demandeurs dont l'identité a été vérifiée ainsi qu'il est prévu aux présentes par une autorité d'enregistrement exploitée par Entrust.net ou par une tierce autorité

d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL. Si une demande de certificat Entrust.net pour serveurs Web SSL est vérifiée, l'autorité d'enregistrement qui effectue la vérification demande à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre un certificat Entrust.net pour serveurs Web SSL. L'autorité de certification Entrust.net pour serveurs Web SSL crée un certificat Entrust.net pour serveurs Web SSL contenant la clé publique et les renseignements d'identification contenus dans la demande d'émission que lui a adressée l'autorité d'enregistrement. Le certificat Entrust.net pour serveurs Web SSL créé par suite de la demande sera signé numériquement par l'autorité de certification Entrust.net pour serveurs Web SSL.

Seules les autorités de certification autorisées par Entrust.net peuvent émettre des certificats Entrust.net pour serveurs Web SSL. Si plusieurs autorités de certification sont autorisées à émettre des certificats Entrust.net pour serveurs Web SSL, Entrust.net en affiche la liste dans son répertoire.

1.3.2 Autorités d'enregistrement

Dans l'infrastructure à clé publique Entrust.net pour serveurs Web SSL, les autorités d'enregistrement qui relèvent des autorités de certification Entrust.net pour serveurs Web SSL peuvent accepter les demandes de certificats Entrust.net pour serveurs Web SSL des demandeurs et effectuer une vérification limitée des renseignements contenus dans ces demandes. Si les renseignements fournis sont vérifiés conformément aux procédures établies par l'autorité de politiques d'Entrust.net, l'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL peut demander à cette dernière d'émettre au demandeur un certificat Entrust.net pour serveurs Web SSL.

Seules les autorités d'enregistrement autorisées par Entrust.net peuvent demander à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre des certificats Entrust.net pour serveurs Web SSL. Si plusieurs autorités d'enregistrement sont autorisées à présenter une telle demande, Entrust.net en affiche la liste dans son répertoire.

1.3.3 Entités finales

Les entités finales aux fins de l'infrastructure à clé publique Entrust.net pour serveurs Web SSL sont les suivantes :

1. **Demandeur** - Le demandeur est la personne, l'entité ou l'organisation ayant demandé un certificat Entrust.net pour serveurs Web SSL, mais à qui aucun certificat n'a encore été émis.
2. **Abonné** - L'abonné est la personne, l'entité ou l'organisation à qui un certificat Entrust.net pour serveurs Web SSL a été émis.
3. **Partie utilisatrice** – La partie utilisatrice est la personne, l'entité ou l'organisation qui se fie à un certificat Entrust.net pour serveurs Web SSL ou à tout autre renseignement fourni dans un répertoire Entrust.net ou utilise ceux-ci pour vérifier l'identité et la clé publique d'un abonné, ou qui utilise cette clé publique pour faire parvenir des communications cryptographiées à un abonné ou pour en recevoir de celui-ci.

1.3.4 Applicabilité

Le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL s'applique aux certificats Entrust.net pour serveurs Web SSL émis par des autorités de certification Entrust.net pour serveurs Web SSL. Les certificats Entrust.net pour serveurs Web SSL sont émis par des autorités de certification Entrust.net pour serveurs Web SSL pour usage par des serveurs pour le Web fournissant des services basés sur le protocole SSL. Les certificats Entrust.net pour serveurs Web SSL sont conformes à la norme X.509 v3 avec des champs additionnels pour le protocole SSL.

1.4 Renseignements**1.4.1 Mise en œuvre**

L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL est mis en œuvre par l'autorité opérationnelle d'Entrust.net et repose sur les politiques établies par l'autorité de politiques d'Entrust.net.

1.4.2 Renseignements

Les demandes de renseignement sur les certificats Entrust.net pour serveurs Web SSL sont adressées à :

Entrust.net Inquiries
1000, promenade Innovation,
Ottawa (Ontario) K2K 1A7
Téléphone : 1 (877) 368-7483
Télécopieur : 1 (877) 839-3538
Email: tsite.entrust@Entrust.net

2. Dispositions générales

2.1 Obligations

2.1.1 Obligations de l'autorité de certification

L'autorité de certification Entrust.net pour serveurs Web SSL doit :

- (i) fournir des services d'autorité de certification conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (ii) sur réception d'une demande d'une autorité d'enregistrement relevant d'elle, émettre un certificat Entrust.net pour serveurs Web SSL conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (iii) communiquer les renseignements sur la révocation de certificats Entrust.net pour serveurs Web SSL en émettant des certificats Entrust.net pour serveurs Web SSL et en publiant des LCR de certificats Entrust.net pour serveurs Web SSL dans un répertoire Entrust.net conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (iv) publier des LCR de certificats Entrust.net pour serveurs Web SSL régulièrement conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (v) sur réception d'une demande de révocation adressée par une autorité d'enregistrement relevant d'elle, révoquer le certificat Entrust.net pour serveurs Web SSL en question conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

Aux fins de l'exploitation des autorités de certification Entrust.net pour serveurs Web SSL, Entrust.net peut avoir recours à un ou plusieurs représentants ou mandataires pour s'acquitter de ses obligations aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice; Entrust.net demeure cependant responsable de l'exécution de ces obligations.

2.1.2 Obligations de l'autorité d'enregistrement

L'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL doit :

- (i) prendre connaissance des demandes de certificat Entrust.net pour serveurs Web SSL conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (ii) effectuer une vérification limitée des renseignements fournis par les demandeurs dans leur demande de certificat Entrust.net pour serveurs Web SSL et, si cette étape est franchie avec succès, demander à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre un certificat Entrust.net pour serveurs Web SSL, le tout conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (iii) prendre connaissance des demandes de révocation de certificats Entrust.net pour serveurs Web SSL présentées par les abonnés et effectuer une vérification de ces demandes, et, si cette étape est franchie avec succès, demander à une autorité de certification Entrust.net pour serveurs Web SSL de révoquer le certificat Entrust.net pour serveurs Web SSL en cause, le tout conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (iv) conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, aviser les abonnés de l'émission à leur intention d'un certificat Entrust.net pour serveurs Web SSL;

- (v) conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, aviser les abonnés de la révocation ou de l'expiration à brève échéance du certificat Entrust.net pour serveurs Web SSL qui leur a été émis.

Entrust.net peut avoir recours à un ou plusieurs représentants ou mandataires pour s'acquitter de ses obligations relativement à une autorité d'enregistrement exploitée par Entrust.net prévues à l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans une entente d'abonnement ou dans un contrat avec une partie utilisatrice; elle demeure cependant responsable de l'exécution de ses obligations par ces représentants ou mandataires aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Entrust.net peut désigner des tierces parties indépendantes pour agir à titre d'autorités d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL. Ces tierces autorités d'enregistrement indépendantes sont responsables de l'exécution de leurs fonctions aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Entrust.net n'est pas responsable de l'exécution de leurs fonctions par ces tierces autorités d'enregistrement indépendantes. Celles-ci peuvent avoir recours aux services d'un ou de plusieurs représentants ou mandataires pour s'acquitter de leurs obligations à titre d'autorités d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL. Elles demeurent responsables de l'exécution de leurs fonctions par ces représentants ou mandataires aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Entrust.net peut désigner des revendeurs et des covendeurs aux fins (i) des certificats Entrust.net pour serveurs Web SSL et (ii) des services fournis relativement aux certificats Entrust.net pour serveurs Web SSL. Ces revendeurs et covendeurs sont responsables de l'exécution de leurs fonctions aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Entrust.net n'est pas responsable de l'exécution de leurs fonctions par les revendeurs et les covendeurs. Ces derniers peuvent recourir aux services d'un ou de plusieurs représentants ou mandataires pour s'acquitter de leurs obligations aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Ils sont responsables de l'exécution de leurs fonctions par ses représentants ou mandataires aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de toute entente d'abonnement ou de tout contrat avec une partie utilisatrice. Les tierces autorités d'enregistrement indépendantes, les revendeurs et les covendeurs bénéficient pleinement de toutes (i) les dénégations de déclarations, de garanties, et de conditions, (ii) les limitations de responsabilité, (iii) les déclarations et les garanties des demandeurs, des abonnés et des parties utilisatrices, et (iv) les indemnités des demandeurs, des abonnés et des parties utilisatrices, prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, toute entente d'abonnement et tout contrat avec une partie utilisatrice.

2.1.3 Obligations de l'abonné

Les abonnés et les demandeurs doivent :

- (i) comprendre la cryptographie à clé publique et les certificats, y compris les certificats Entrust.net pour serveurs Web SSL et, si nécessaire, obtenir la formation nécessaire aux fins de l'utilisation de ceux-ci;
- (ii) fournir, dans toute communication avec Entrust.net ou avec une tierce autorité d'enregistrement indépendante, des renseignements exacts ne comprenant aucune erreur, fausse déclaration ou omission;
- (iii) générer une nouvelle clé sûre par des techniques cryptographiques établies aux fins de son utilisation en association avec le certificat Entrust.net pour serveurs Web SSL (dans le cas de l'abonné) ou avec la demande de certificat Entrust.net pour serveurs Web SSL (dans le cas du demandeur);
- (iv) lire et accepter toutes les modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et de l'entente d'abonnement;

- (v) s'abstenir de modifier le contenu d'un certificat Entrust.net pour serveurs Web SSL;
- (vi) utiliser les certificats Entrust.net pour serveurs Web SSL aux seuls fins légales autorisées dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, et conformément aux lois applicables;
- (vii) n'utiliser un certificat Entrust.net pour serveurs Web SSL que pour le compte de la personne, de l'entité ou de l'organisation dont le nom figure comme sujet dans le certificat Entrust.net pour serveurs Web SSL en question;
- (viii) protéger leurs clés privées en les mettant en mémoire sur un jeton matériel ou une disquette et en tenant ce support distinct de leur ordinateur lorsqu'il n'est pas utilisé;
- (ix) aviser Entrust.net ou, si le demandeur a présenté sa demande de certificat Entrust.net pour serveurs Web SSL à une tierce autorité d'enregistrement indépendante, aviser cette autorité, dès qu'il est raisonnablement possible de le faire, de tout changement des renseignements fournis dans sa demande de certificat Entrust.net pour serveurs Web SSL ou de tout changement des circonstances ayant pour effet de rendre trompeuse ou inexacte sa demande de certificat Entrust.net pour serveurs Web SSL;
- (x) aviser Entrust.net ou, si l'abonné a reçu son certificat Entrust.net pour serveurs Web SSL d'une tierce autorité d'enregistrement indépendante, aviser cette autorité, dès qu'il est raisonnablement possible de le faire, de tout changement des renseignements fournis dans son certificat Entrust.net pour serveurs Web SSL ou de tout changement des circonstances ayant pour effet de rendre trompeurs ou inexacts les renseignements contenus dans son certificat Entrust.net pour serveurs Web SSL;
- (xi) cesser immédiatement d'utiliser un certificat Entrust.net pour serveurs Web SSL si des renseignements qui y sont contenus sont trompeurs ou inexacts ou si un changement de circonstances aurait pour effet de rendre trompeurs ou inexacts des renseignements qui y sont contenus;
- (xii) aviser Entrust.net ou, si l'abonné a reçu son certificat Entrust.net pour serveurs Web SSL d'une tierce autorité d'enregistrement indépendante, aviser cette autorité immédiatement de toute compromission réelle ou soupçonnée des clés privées de l'abonné ou du demandeur et demander la révocation du certificat en question;
- (xiii) cesser d'utiliser le certificat Entrust.net pour serveurs Web SSL de l'abonné a) dès qu'il est expiré ou révoqué ou, b) dès qu'il y a compromission réelle ou soupçonnée de la clé privée correspondant à la clé publique contenue dans le certificat en cause, et retirer celui-ci des supports ou logiciels sur lesquels il a été installé;
- (xiv) n'utiliser le certificat Entrust.net pour serveurs Web SSL de l'abonné que sur un (1) serveur pour le Web à la fois;
- (xv) s'abstenir d'utiliser la clé privée de l'abonné correspondant à la clé publique contenue dans le certificat Entrust.net pour serveurs Web SSL de l'abonné pour signer d'autres certificats;
- (xvi) faire preuve de discernement déterminer si, étant donné le lien de confiance et de sécurité qu'offre un certificat Entrust.net pour serveurs Web SSL, il convient d'utiliser un certificat Entrust.net pour serveurs Web SSL en toute circonstance.

L'exportation, l'importation et l'utilisation des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes peuvent être assujetties à certaines restrictions. L'abonné doit se conformer à l'ensemble des lois et règlements applicables à son droit d'exporter, d'importer ou d'utiliser des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes. Il doit obtenir toutes les licences et autorisations requises aux fins de l'exportation, de l'importation ou de l'utilisation des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes. L'exportation, l'importation et l'utilisation de certains logiciels, techniques cryptographiques, matériels informatiques et micrologiciels (« technologie ») qui peuvent être utilisés dans le traitement des certificats Entrust.net pour serveurs Web SSL ou en conjonction avec ceux-ci peuvent être assujetties à certaines restrictions. L'abonné doit se conformer à l'ensemble des lois et règlements applicables à son droit d'exporter, d'importer ou d'utiliser cette technologie et ces renseignements connexes. Il doit obtenir toutes les licences et autorisations requises aux fins de l'exportation, de l'importation ou de l'utilisation de cette technologie et de ces renseignements connexes.

2.1.3.1 Déclarations et garanties de l'abonné et du demandeur

L'abonné et le demandeur déclarent et garantissent ce qui suit à Entrust.net :

- (i) tous les renseignements fournis par l'abonné ou le demandeur à Entrust.net ou à une tierce autorité d'enregistrement indépendante sont exacts et ne contiennent aucune erreur, omission ou fausse déclaration;
- (ii) la clé privée correspondant à la clé publique soumise par l'abonné ou le demandeur dans une demande de certificat Entrust.net pour serveurs Web SSL a été générée au moyen de techniques cryptographiques établies et n'a pas été compromise;
- (iii) les renseignements fournis par l'abonné ou le demandeur à Entrust.net ou à une tierce autorité d'enregistrement indépendante ne violent pas ni ne détournent ou affaiblissent les droits de propriété intellectuelle ou autres de toute personne, entité ou organisation dans quelque administration que ce soit, ni n'entrent injustement en concurrence avec ces droits ou y portent par ailleurs atteinte;
- (iv) le demandeur avise Entrust.net ou, s'il a adressé sa demande de certificat Entrust.net pour serveurs Web SSL à une tierce autorité d'enregistrement indépendante, il avise cette autorité, dès qu'il est en mesure de le faire, du changement des renseignements fournis dans sa demande de certificat Entrust.net pour serveurs Web SSL ou du fait que des changements de circonstances rendent trompeurs ou inexacts les renseignements fournis dans sa demande de certificat Entrust.net pour serveurs Web SSL;
- (v) l'abonné cesse immédiatement d'utiliser son certificat Entrust.net pour serveurs Web SSL si des renseignements contenus dans celui-ci changent ou que des changements de circonstances rendent trompeurs ou inexacts les renseignements qui y sont contenus;
- (vi) l'abonné cesse d'utiliser son certificat Entrust.net pour serveurs Web SSL a) dès que celui-ci est expiré ou révoqué, ou b) dès qu'il y a compromission réelle ou soupçonnée de la clé privée correspondant à la clé publique contenue dans le certificat en cause, et retire celui-ci de tout support ou logiciel sur lequel il a été installé;
- (vii) l'abonné et le demandeur n'utilisent pas les certificats Entrust.net pour serveurs Web SSL à des fins dangereuses ou illégales (y compris à des fins délictuelles).

2.1.3.2 Avis

L'abonné affiche l'avis suivant dans un endroit bien en vu sur son site Web, que les parties utilisatrices peuvent voir (par exemple, dans la section « dispositions légales » ou « dénégations » de son site Web) :

L'utilisation des certificats Entrust.net pour serveurs Web SSL est assujettie aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL (www.entrust.net/ÉPC) et du contrat avec une partie utilisatrice (www.entrust.net/customer/relyingparty.htm). L'utilisation d'un certificat Entrust.net pour serveurs Web SSL constitue une acceptation des modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et du contrat avec une partie utilisatrice. »

2.1.4 Obligations de la partie utilisatrice

La partie utilisatrice doit :

- (i) comprendre la cryptographie à clé publique et les certificats, y compris les certificats Entrust.net pour serveurs Web SSL, et, si nécessaire, obtenir la formation nécessaire aux fins de l'utilisation de ceux-ci;
- (ii) lire et accepter toutes les modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et du contrat avec une partie utilisatrice;
- (iii) vérifier les certificats Entrust.net pour serveurs Web SSL, notamment en consultant les LCR, conformément à la procédure de validation du chemin de certification défini dans la

- recommandation UIT-T X.509:1997 | ISO/IEC 9594-8 (1997), en prenant en considération tout champ additionnel « critical » et rectificatif technique approuvé le cas échéant;
- (iv) ne se fier à un certificat Entrust.net pour serveurs Web SSL et ne l'utiliser que si celui-ci n'est pas expiré ou n'a pas été révoqué et que si une chaîne de confiance satisfaisante peut être établie par rapport à une autorité de certification principale fiable;
 - (v) faire preuve de jugement et ne se fier à un certificat Entrust.net pour serveurs Web SSL que si cette confiance est raisonnable dans les circonstances, notamment en déterminant si cette confiance est raisonnable étant donné le lien de confiance et de sécurité qu'offre un certificat Entrust.net pour serveurs Web SSL et la valeur de toute transaction pouvant nécessiter l'utilisation d'un certificat Entrust.net pour serveurs Web SSL.

L'exportation, l'importation et l'utilisation des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes peuvent être assujetties à certaines restrictions. La partie utilisatrice doit se conformer à l'ensemble des lois et règlements applicables à son droit d'utiliser des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes. Elle doit obtenir toutes les licences et autorisations requises aux fins de l'exportation, de l'importation et de l'utilisation des certificats Entrust.net pour serveurs Web SSL et des renseignements connexes. L'exportation, l'importation et l'utilisation de certains logiciels, techniques cryptographiques, matériels informatiques et micrologiciels (« technologie ») qui peuvent être utilisés dans le traitement des certificats Entrust.net pour serveurs Web SSL ou en conjonction avec ceux-ci peuvent être assujetties à certaines restrictions. La partie utilisatrice doit se conformer à l'ensemble des lois et règlements applicables à son droit d'exporter, d'importer et d'utiliser cette technologie et ces renseignements connexes. Elle doit obtenir toutes les licences et autorisations requises aux fins de l'exportation, de l'importation et de l'utilisation de cette technologie et de ces renseignements connexes.

2.1.4.1 Déclarations et garanties de la partie utilisatrice

La partie utilisatrice déclare et garantit ce qui suit à Entrust.net :

- (i) elle valide de façon satisfaisante un certificat Entrust.net pour serveurs Web SSL avant de déterminer si elle s'y fiera, notamment en obtenant la confirmation que le certificat Entrust.net pour serveurs Web SSL n'est pas expiré ou n'a pas été révoqué et qu'une chaîne de confiance satisfaisante peut être établie par rapport à une autorité de certification principale fiable;
- (ii) elle ne se fie à aucun certificat Entrust.net pour serveurs Web SSL expiré ou révoqué;
- (iii) elle ne se fie à aucun certificat Entrust.net pour serveurs Web SSL qu'il est impossible de valider par rapport à une autorité de certification principale fiable;
- (iv) elle fait preuve de discernement pour déterminer s'il est raisonnable, compte tenu des circonstances, de se fier à un certificat Entrust.net pour serveurs Web SSL, notamment en déterminant si cette utilisation est raisonnable étant donné le lien de confiance et de sécurité qu'offre un certificat Entrust.net pour serveurs Web SSL et la valeur de toute transaction pouvant nécessiter l'utilisation d'un certificat Entrust.net pour serveurs Web SSL;
- (v) elle n'utilise aucun certificat Entrust.net pour serveurs Web SSL à des fins dangereuses ou illégales (y compris à des fins délictueuses).

2.1.5 Obligations de l'entité responsable du Répertoire

L'entité responsable du Répertoire Entrust.net doit :

- (i) conformément aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, communiquer les renseignements relatifs à la révocation de certificats Entrust.net pour serveurs Web SSL publiés par une autorité de certification Entrust.net pour serveurs Web SSL;
- (ii) communiquer une copie de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et d'autres renseignements liés aux produits et aux services fournis par les autorités de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL.

2.2 Responsabilité

LE PLAFOND DE LA RESPONSABILITÉ CUMULATIVE D'ENTRUST.NET, DES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT D'AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, DES REVENDEURS OU COVENDEURS, DES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES OU FOURNISSEURS ET DE LEURS EMPLOYÉS OU ADMINISTRATEURS, ENVERS UN DEMANDEUR, UN ABONNÉ, UNE PARTIE UTILISATRICE OU TOUTE AUTRE PERSONNE, ENTITÉ OU ORGANISATION, POUR LES PERTES, LES FRAIS, LES DÉPENSES, LES OBLIGATIONS, LES DOMMAGES-INTÉRÊTS, LES RÉCLAMATIONS OU LES MONTANTS FIXÉS DANS UN RÈGLEMENT DÉCOULANT DE L'UTILISATION D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU DES SERVICES FOURNIS RELATIVEMENT À UN TEL CERTIFICAT, OU S'Y RAPPORTANT, EST LIMITÉ PAR LE PRÉSENT ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, QUI CONTIENT ÉGALEMENT DES GARANTIES LIMITÉES, DES LIMITATIONS DE LA RESPONSABILITÉ ET DES DÉNÉGATIONS DE DÉCLARATIONS, DE GARANTIES ET DE CONDITIONS.

2.2.1 Responsabilité des AC

2.2.1.1 Garanties et limitations des garanties

Entrust.net offre aux abonnés les garanties limitées suivantes relativement à l'utilisation des autorités de certification Entrust.net pour serveurs Web SSL :

- (i) les autorités de certification Entrust.net pour serveurs Web SSL fournissent des services de répertoire conformes aux pratiques et aux procédures prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (ii) les autorités de certification Entrust.net pour serveurs Web SSL émettent des certificats Entrust.net pour serveurs Web SSL conformément aux procédures prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (iii) les autorités de certification Entrust.net pour serveurs Web SSL fournissent des services de révocation conformes aux procédures prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

Nonobstant ce qui précède, Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés ou administrateurs ne font aucune déclaration, ne fournissent aucune garantie et ne formulent aucune condition à des demandeurs, des abonnés, des parties utilisatrices ou autres personnes, entités ou organisations relativement (i) aux techniques utilisées aux fins de la génération et de la mise en mémoire de la clé privée correspondant à la clé publique contenue dans un certificat Entrust.net pour serveurs Web SSL, notamment sur la question de savoir si la clé privée en question a été compromise ou si elle a été générée au moyen de techniques cryptographiques établies, (ii) à la fiabilité des techniques ou méthodes cryptographiques utilisées pour accomplir un acte, une transaction ou un processus nécessitant ou utilisant un certificat Entrust.net pour serveurs Web SSL, (iii) à tout logiciel, ou (iv) à la non-répudiation d'un certificat Entrust.net pour serveurs Web SSL ou d'une transaction facilitée par l'utilisation d'un certificat Entrust.net pour serveurs Web SSL, puisqu'il s'agit d'une détermination relevant des lois applicables.

Les demandeurs, les abonnés et les parties utilisatrices reconnaissent et conviennent que les opérations relatives aux certificats Entrust.net pour serveurs Web SSL et aux demandes de certificats Entrust.net pour serveurs Web SSL dépendent de la transmission de renseignements sur des infrastructures de communication comme, sans limiter la portée de ce qui précède, l'Internet, des lignes téléphoniques et des

lignes et réseaux de télécommunication, des serveurs, des garde-barrières, des agents « proxy » (aussi appelés mandataires), des routeurs, des commutateurs et des ponts (« matériel de télécommunication »), et que ce matériel de télécommunication n'est pas sous le contrôle de Entrust.net ni sous celui des tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, des revendeurs ou covendeurs, des sous-entrepreneurs, distributeurs, mandataires ou fournisseurs ou de leurs employés ou administrateurs. Ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, ni les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs ou leurs employés ou administrateurs, ne sont responsables des erreurs, défaillances, retards, interruptions, vices ou corruptions liés à un certificat Entrust.net pour serveurs Web SSL, à une LCR de certificats Entrust.net pour serveurs Web SSL ou à une demande de certificat Entrust.net pour serveurs Web SSL, dans la mesure où l'erreur, la défaillance, le retard, l'interruption, le vice ou la corruption est causé par le matériel de télécommunication

2.2.1.2 Dénégations

SAUF CE QUI EST EXPRESSÉMENT PRÉVU À L'ARTICLE 2.2.1.1, ENTRUST.NET, LES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS OU COVENDEURS, LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES OU FOURNISSEURS ET LEURS EMPLOYÉS OU ADMINISTRATEURS NE FONT AUCUNE DÉCLARATION, N'OFFRENT AUCUNE GARANTIE ET NE FORMULENT AUCUNE CONDITION EXPLICITE, IMPLICITE, LÉGISLATIVE, FONDÉE SUR L'USAGE DU COMMERCE OU AUTRE, ET ILS DÉSAVOUENT EXPRESSÉMENT TOUTE DÉCLARATION, GARANTIE ET CONDITION DE COMMERCIALISABILITÉ, D'ABSENCE DE CONTREFAÇON, DE TITRE, DE QUALITÉ SATISFAISANTE OU DE CONFORMITÉ À UN OBJET.

2.2.1.3 Plafond des pertes

LA RESPONSABILITÉ CUMULATIVE D'ENTRUST.NET, DES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, DES REVENDEURS OU COVENDEURS, DES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES OU FOURNISSEURS OU DE LEURS EMPLOYÉS ET ADMINISTRATEURS, ENVERS UN DEMANDEUR, UN ABONNÉ, UNE PARTIE UTILISATRICE OU TOUTE AUTRE PERSONNE, ENTITÉ OU ORGANISATION, DÉCOULANT D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU DE TOUT SERVICE FOURNI RELATIVEMENT À UN TEL CERTIFICAT, OU S'Y RAPPORTANT, Y COMPRIS LA RESPONSABILITÉ DÉCOULANT DU FAIT D'UTILISER UN TEL CERTIFICAT OU DE S'Y FIER, N'EXCÈDE EN AUCUN CAS MILLE DOLLARS AMÉRICAINS (1 000 \$ US) (« PLAFOND DES DOMMAGES-INTÉRÊTS CUMULATIFS »). CETTE LIMITATION S'APPLIQUE À CHAQUE CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, SANS ÉGARD AU NOMBRE DE TRANSACTIONS OU DE CAUSES D'ACTION DÉCOULANT DU CERTIFICAT OU D'UN SERVICE FOURNI RELATIVEMENT À CELUI-CI, OU S'Y RAPPORTANT. LES LIMITATIONS QUI PRÉCÈDENT S'APPLIQUENT À TOUTE FORME DE RESPONSABILITÉ, QU'ELLE SOIT BASÉE SUR UN CONTRAT (NOTAMMENT POUR MANQUEMENT À UNE DISPOSITION ESSENTIELLE), UN DÉLIT (DONT LA NÉGLIGENCE), LA LOI OU TOUTE AUTRE THÉORIE DE LA RESPONSABILITÉ, CE QUI COMPREND LES DOMMAGES-INTÉRÊTS DIRECTS, INDIRECTS, EXTRAORDINAIRES, LÉGAUX, PUNITIFS, EXEMPLAIRES, CONSÉCUTIFS, DÉCOULANT DES ACTES DE CONFIANCE OU ACCESSOIRES.

SI LA RESPONSABILITÉ DÉCOULANT D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU D'UN SERVICE FOURNI RELATIVEMENT À UN TEL

CERTIFICAT, OU S'Y RAPPORTANT, EXCÈDE LE PLAFOND DES DOMMAGES-INTÉRÊTS CUMULATIFS FIXÉ DANS L'ARTICLE PRÉCÉDENT, LES MONTANTS CONSTITUANT LE PLAFOND DES DOMMAGES-INTÉRÊTS CUMULATIFS SONT ATTRIBUÉS D'ABORD AUX PREMIERS DEMANDEURS EN VUE D'ARRIVER À UNE RÉOLUTION DÉFINITIVE DU DIFFÉREND, À MOINS D'UNE ORDONNANCE CONTRAIRE RENDUE PAR UN TRIBUNAL COMPÉTENT. ENTRUST.NET, LES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS ET COVENDEURS, LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES ET FOURNISSEURS OU LEURS EMPLOYÉS ET ADMINISTRATEURS, NE SONT EN AUCUN CAS TENUS DE PAYER UN MONTANT SUPÉRIEUR AU PLAFOND DES DOMMAGES-INTÉRÊTS CUMULATIFS POUR CHAQUE CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU POUR TOUT SERVICE FOURNI RELATIVEMENT À UN TEL CERTIFICAT, SANS ÉGARD À LA RÉPARTITION DES MONTANTS ENTRE LES DEMANDEURS.

ENTRUST.NET, LES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS ET COVENDEURS, LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES ET FOURNISSEURS OU LEURS EMPLOYÉS ET ADMINISTRATEURS, NE PEUVENT EN AUCUN CAS ÊTRE TENUS DE PAYER DES DOMMAGES-INTÉRÊTS ACCESSOIRES, EXTRAORDINAIRES, LÉGAUX, PUNITIFS, EXEMPLAIRES, INDIRECTS, DÉCOULANT DES ACTES DE CONFIANCE OU CONSÉCUTIFS (Y COMPRIS, SANS LIMITER LA PORTÉE DE CE QUI PRÉCÈDE, DES DOMMAGES-INTÉRÊTS POUR PERTE DE CHIFFRE D'AFFAIRES, D'OCCASIONS D'AFFAIRES, DE CLIENTÈLE ET DE PROFITS, POUR PERTE D'EXPLOITATION, DE DONNÉES OU D'ÉCONOMIES OU POUR TOUTE AUTRE PERTE PÉCUNIAIRE SEMBLABLE), QU'ILS DÉCOULENT D'UN CONTRAT (Y COMPRIS POUR MANQUEMENT À UNE DISPOSITION ESSENTIELLE), D'UN DÉLIT (DONT LA NÉGLIGENCE), DE LA LOI OU DE TOUTE AUTRE THÉORIE DE LA RESPONSABILITÉ.

LES LIMITATIONS QUI PRÉCÈDENT S'APPLIQUENT MÊME EN CAS D'ÉCHEC DE TOUT RECOURS LIMITÉ PRÉVU DANS LES PRÉSENTES ET MÊME SI ENTRUST.NET OU LES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS OU COVENDEURS, LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES OU FOURNISSEURS ET LEURS EMPLOYÉS OU ADMINISTRATEURS ONT ÉTÉ INFORMÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

CERTAINES ADMINISTRATIONS NE PERMETTANT PAS LA DÉNÉGATION OU LA LIMITATION DE RESPONSABILITÉ POUR DES DOMMAGES-INTÉRÊTS CONSÉCUTIFS OU ACCESSOIRES, LES LIMITATIONS PRÉVUES CI-DESSUS PEUVENT NE PAS S'APPLIQUER À CERTAINS DEMANDEURS, ABONNÉS, PARTIES UTILISATRICES OU À TOUTE AUTRE PERSONNE, ENTITÉ OU ORGANISATION. LES DÉNÉGATIONS DE DÉCLARATIONS, DE GARANTIES ET DE CONDITIONS ET LES LIMITATIONS DE RESPONSABILITÉ DANS LE PRÉSENT ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL SONT DES ÉLÉMENTS ESSENTIELS DE L'ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, DE TOUTE ENTENTE D'ABONNEMENT ET DE TOUT CONTRAT AVEC UNE PARTIE UTILISATRICE. TOUS LES DEMANDEURS, LES ABONNÉS, LES PARTIES UTILISATRICES ET AUTRES PERSONNES, ENTITÉS ET ORGANISATIONS RECONNAISSENT D'UNE PART QUE, EN L'ABSENCE DE TELLES DÉNÉGATIONS DE DÉCLARATIONS, DE GARANTIES OU DE CONDITIONS, ET SANS LES LIMITATIONS DE RESPONSABILITÉ, ENTRUST.NET N'ÉMETTRAIT AUX ABONNÉS AUCUN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, ET NI ENTRUST.NET, NI LES TIERCES AUTORITÉS D'ENREGISTREMENT INDÉPENDANTES RELEVANT DES AUTORITÉS DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB

SSL, NI LES REVENDEURS OU COVENDEURS, NI LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES OU FOURNISSEURS, NI LEURS EMPLOYÉS OU ADMINISTRATEURS, NE FOURNIRAIENT DE SERVICE RELATIVEMENT À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, ET, D'AUTRE PART, QUE LA RÉPARTITION DU RISQUE PRÉVUE DANS LES PRÉSENTES DISPOSITIONS EST RAISONNABLE.

2.2.1.4 Autres exclusions

Sans que cela emporte quelque restriction que ce soit, ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, ni les revendeurs ou covendeurs, ni les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs, ni leurs employés ou administrateurs, ne sont responsables envers les demandeurs, les abonnés, les parties utilisatrices ou les autres personnes, entités ou organisations relativement aux pertes, frais, dépenses, obligations, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant de l'utilisation d'un certificat Entrust.net pour serveurs Web SSL ou de tout service fourni relativement à un certificat Entrust.net pour serveurs Web SSL, ou s'y rapportant, dans les cas suivants :

- (i) le certificat Entrust.net pour serveurs Web SSL a été émis par suite d'erreurs, de fausses déclarations ou d'autres actes ou omissions d'un abonné ou de toute autre personne, entité ou organisation;
- (ii) le certificat Entrust.net pour serveurs Web SSL est expiré ou a été révoqué;
- (iii) le certificat Entrust.net pour serveurs Web SSL a été modifié ou par ailleurs transformé;
- (iv) l'abonné a omis de cesser d'utiliser un certificat Entrust.net pour serveurs Web SSL alors que les renseignements qui y sont contenus ont changé ou que les circonstances ont changé de façon que les renseignements en question sont devenus trompeurs ou inexacts;
- (v) un abonné a manqué à l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ou à l'entente d'abonnement qu'il a conclue, ou une partie utilisatrice a manqué à l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ou au contrat qu'elle a conclu en tant que partie utilisatrice;
- (vi) la clé privée associée au certificat Entrust.net pour serveurs Web SSL a été compromise;
- (vii) le certificat Entrust.net pour serveurs Web SSL est utilisé à une fin non permise dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ou en contravention avec les lois applicables.

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés ou administrateurs, ne peuvent en aucun cas être tenus responsables envers un demandeur, un abonné ou toute autre personne, entité ou organisation, des pertes, frais, obligations, dépenses, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant du refus de Entrust.net, des tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, des revendeurs ou covendeurs, des sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et de leurs employés ou administrateurs, ou s'y rapportant, d'émettre un certificat Entrust.net pour serveurs Web SSL ou d'en demander l'émission. Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés ou administrateurs, ne peuvent en aucun cas être tenus responsables envers un demandeur, un abonné ou toute autre personne, entité ou organisation, des pertes, frais, obligations, dépenses, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant de tout retard de Entrust.net, des tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, des revendeurs ou covendeurs, des sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et de leurs employés ou administrateurs, ou s'y rapportant, mis à émettre un certificat Entrust.net pour serveurs Web SSL ou à en demander l'émission.

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés ou administrateurs, ne peuvent en aucun cas être tenus responsables envers un abonné, une partie utilisatrice ou toute autre personne, entité ou organisation des pertes, frais, obligations, dépenses, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant de toute allégation ou de toute procédure dans laquelle il est allégué, ou s'y rapportant, qu'un certificat Entrust.net pour serveurs Web SSL ou certains des renseignements qui y sont contenus violent, détournent ou affaiblissent un brevet d'invention, une marque de commerce, un droit d'auteur, un secret de fabrication ou tout autre droit de propriété intellectuelle ou autre de toute personne, entité ou organisation dans quelque administration que ce soit, entrent injustement en concurrence avec ce droit ou y portent par ailleurs atteinte.

2.2.1.5 Activités dangereuses

Les certificats Entrust.net pour serveurs Web SSL et les services fournis par Entrust.net relativement aux certificats Entrust.net pour serveurs Web SSL ne sont pas conçus ou fabriqués pour être utilisés dans le cadre d'activités dangereuses ou autres utilisations exigeant un rendement à toute épreuve, ou en conjonction avec celles-ci, y compris aux fins du fonctionnement d'installations nucléaires ou de systèmes de navigation aérienne ou de communication, de contrôle de la circulation aérienne, d'appareils médicaux ou d'équipements de survie. Entrust.net, les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés ou administrateurs, désavouent expressément toute déclaration, garantie et condition relative à ces utilisations, qu'elle soit explicite, implicite, statutaire, fondée sur l'usage du commerce ou autre.

2.2.2 Responsabilité des AE

Les mêmes dispositions relatives à la responsabilité prévues à l'article 2.2.1 concernant les autorités de certification Entrust.net pour serveurs Web SSL s'appliquent aux autorités d'enregistrement exploitées par Entrust.net, aux tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, aux revendeurs, covendeurs et sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et à leurs employés ou administrateurs.

2.3 Responsabilité financière

Les abonnés et les parties utilisatrices sont responsables des conséquences financières qu'ils subissent et que toute autre personne, entité ou organisation subit par suite de transactions auxquelles les abonnés ou les parties utilisatrices prennent part et dans le cadre desquelles sont utilisés des certificats Entrust.net pour serveurs Web SSL, ou par suite de services fournis relativement à des certificats Entrust.net pour serveurs Web SSL. Entrust.net ne fait aucune déclaration, n'offre aucune garantie et ne formule aucune condition concernant l'efficacité financière des transactions effectuées au moyen d'un certificat Entrust.net pour serveurs Web SSL ou des services fournis relativement à des certificats Entrust.net pour serveurs Web SSL, et ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant d'autorités de certification Entrust.net pour serveurs Web SSL, ni les revendeurs ou covendeurs, ni les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs, ni leurs employés ou administrateurs, n'encourent de responsabilité, exception faite de ce qui est expressément prévu dans les présentes relativement à l'utilisation d'un certificat Entrust.net pour serveurs Web SSL ou au fait de s'y fier, ou à des services fournis relativement à des certificats Entrust.net pour serveurs Web SSL.

2.3.1 Garantie offerte par les parties utilisatrices

LES PARTIES UTILISATRICES GARANTISSENT ENTRUST.NET, LES TIERCES AUTORITÉS INDÉPENDANTES RELEVANT D'UNE AUTORITÉ DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS ET COVENDEURS, SOUS-ENTREPRENEURS,

DISTRIBUTEURS, MANDATAIRES ET FOURNISSEURS ET LEURS EMPLOYÉS ET ADMINISTRATEURS (COLLECTIVEMENT, LES « PARTIES BÉNÉFICIAIRES DE LA GARANTIE ») CONTRE TOUTE RESPONSABILITÉ RELATIVEMENT AUX OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS, MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERTS) DÉCOULANT DE L'UTILISATION PAR UNE PARTIE UTILISATRICE D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, OU DU FAIT QU'ELLE S'Y EST FIÉE, OU DE TOUT SERVICE FOURNI RELATIVEMENT À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, Y COMPRIS (I) DE L'ABSENCE DE VALIDATION SATISFAISANTE D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL PAR UNE PARTIE UTILISATRICE, (II) DU FAIT POUR LA PARTIE UTILISATRICE DE SE FIER À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL EXPIRÉ OU RÉVOQUÉ, (III) DE L'UTILISATION D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL À DES FINS NON PERMISES DANS L'ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, DANS L'ENTENTE D'ABONNEMENT OU DANS TOUT CONTRAT AVEC UNE PARTIE UTILISATRICE, ET DANS LES LOIS APPLICABLES, (IV) DE L'OMISSION PAR UNE PARTIE UTILISATRICE DE FAIRE PREUVE DE DISCERNEMENT DANS LES CIRCONSTANCES EN SE FIANTE À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, OU (V) DE TOUTE RÉCLAMATION OU ALLÉGATION SELON LAQUELLE LE FAIT POUR UNE PARTIE UTILISATRICE DE SE FIER À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU AUX RENSEIGNEMENTS CONTENUS DANS CE CERTIFICAT VIOLE, DÉTOURNE OU AFFAIBLIT LES DROITS, NOTAMMENT LES DROITS DE PROPRIÉTÉ INTELLECTUELLE OU AUTRE DE QUI QUE CE SOIT DANS QUELQUE ADMINISTRATION QUE CE SOIT, ENTRE INJUSTEMENT EN CONCURRENCE AVEC CES DROITS OU Y PORTE PAR AILLEURS ATTEINTE. NONOBTANT CE QUI PRÉCÈDE, LES PARTIES UTILISATRICES NE SONT PAS TENUES DE GARANTIR UNE PARTIE BÉNÉFICIAIRE DE LA GARANTIE CONTRE LES OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS ET MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERT) DANS LA MESURE OÙ CES OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS ET MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERT) DÉCOULENT D'UNE ACTION FAUTIVE INTENTIONNELLE DE LA PARTIE BÉNÉFICIAIRE DE LA GARANTIE, OU S'Y RAPPORTENT.

2.3.1.1 Garantie offerte par les abonnés

LES ABONNÉS GARANTISSENT ENTRUST.NET, LES TIERCES AUTORITÉS INDÉPENDANTES RELEVANT D'UNE AUTORITÉ DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, LES REVENDEURS ET COVENDEURS, LES SOUS-ENTREPRENEURS, DISTRIBUTEURS, MANDATAIRES ET FOURNISSEURS ET LEURS EMPLOYÉS OU ADMINISTRATEURS (COLLECTIVEMENT, LES « PARTIES BÉNÉFICIAIRES DE LA GARANTIE ») CONTRE TOUTE RESPONSABILITÉ RELATIVEMENT AUX OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS OU MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERTS) DÉCOULANT DU FAIT POUR UNE PARTIE UTILISATRICE DE SE FIER À UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL OU DES SERVICES FOURNIS RELATIVEMENT À CE CERTIFICAT, OU S'Y RAPPORTANT, Y COMPRIS (I) D'UNE ERREUR, DE FAUSSES DÉCLARATIONS OU D'UNE OMISSION PAR UN ABONNÉ LORSQU'IL UTILISE OU DEMANDE UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, (II) DE LA MODIFICATION PAR UN ABONNÉ DES RENSEIGNEMENTS CONTENUS DANS UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, (III) DE L'UTILISATION D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL À DES FINS NON PERMISES DANS L'ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, DANS

L'ENTENTE D'ABONNEMENT OU DANS TOUT CONTRAT AVEC UNE PARTIE UTILISATRICE, ET DANS LES LOIS APPLICABLES, (IV) DE L'OMISSION D'UN ABONNÉ DE PRENDRE LES PRÉCAUTIONS NÉCESSAIRES POUR PRÉVENIR LA PERTE, LA DIVULGATION, LA COMPROMISSION OU L'UTILISATION NON AUTORISÉE DE LA CLÉ PRIVÉE CORRESPONDANT À LA CLÉ PUBLIQUE CONTENUE DANS CE CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL, OU (V) DE L'ALLÉGATION QUE L'UTILISATION D'UN CERTIFICAT ENTRUST.NET POUR SERVEURS WEB SSL D'UN ABONNÉ OU DES RENSEIGNEMENTS CONTENUS DANS CELUI-CI VIOLE, DÉTOURNE OU AFFAIBLIT LES DROITS, NOTAMMENT LES DROITS DE PROPRIÉTÉ INTELLECTUELLE OU AUTRES DE QUI QUE CE SOIT DANS QUELQUE ADMINISTRATION QUE CE SOIT, ENTRE INJUSTEMENT EN CONCURRENCE AVEC CES DROITS OU Y PORTE PAR AILLEURS ATTEINTE. NONOBTANT CE QUI PRÉCÈDE, L'ABONNÉ N'EST PAS TENU DE GARANTIR UNE PARTIE BÉNÉFICIAIRE D'UNE GARANTIE CONTRE LES OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS ET MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERT) DANS LA MESURE OÙ CES OBLIGATIONS, PERTES, FRAIS, DÉPENSES, DOMMAGES-INTÉRÊTS, RÉCLAMATIONS ET MONTANTS FIXÉS DANS UN RÈGLEMENT (NOTAMMENT LES HONORAIRES D'AVOCAT RAISONNABLES, LES FRAIS JUDICIAIRES ET LES HONORAIRES D'EXPERT) DÉCOULENT D'UNE ACTION FAUTIVE INTENTIONNELLE DE CETTE PARTIE BÉNÉFICIAIRE D'UNE GARANTIE, OU S'Y RAPPORTENT.

2.3.2 Rapports de fiduciaire

Aucune disposition du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice, n'est réputée faire d'Entrust.net, d'une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, d'un revendeur ou covendeur, d'un sous-entrepreneur, distributeur, mandataire ou fournisseur et de leurs employés ou administrateurs, le fiduciaire, l'associé, le mandataire, le syndic ou l'ayant droit d'un demandeur, d'un abonné ou d'une partie utilisatrice ou d'une autre personne, entité ou organisation, ni créer à quelque fin que ce soit de rapports de fiduciaire entre, d'une part, Entrust.net ou une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, ou un revendeur ou covendeur, un sous-entrepreneur, distributeur, mandataire ou fournisseur et leurs employés ou administrateurs, et, d'autre part, tout abonné, tout demandeur, toute partie utilisatrice ou toute autre personne, entité ou organisation. Aucune disposition de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice ne confère à un abonné, un demandeur, une partie utilisatrice ou à toute autre tierce partie quelque pouvoir d'agir, de créer et d'assumer une obligation ou une responsabilité ou de faire quelque déclaration que ce soit pour le compte d'Entrust.net, d'une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, d'un revendeur ou covendeur, d'un sous-entrepreneur, distributeur, mandataire ou fournisseur et de leurs employés ou administrateurs, ou de lier ceux-ci.

2.3.3 Processus administratifs

Aucune disposition.

2.4 Interprétation et application

2.4.1 Lois applicables

Les lois de la province de l'Ontario, Canada, sans renvoi à leurs règles en matière de conflits des lois, régissent l'interprétation, la validité, le caractère exécutoire et l'application de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, des ententes d'abonnement et des contrats avec des parties

utilisatrices. L'application de la Convention des Nations Unies sur les contrats de vente internationale de marchandises à l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, aux ententes d'abonnement et aux contrats avec une partie utilisatrice, est expressément exclue. Les litiges découlant de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice, ou s'y rapportant, ou se rapportant à des certificats Entrust.net pour serveurs Web SSL ou à des services fournis relativement à ceux-ci, qui ne sont pas résolus dans le cadre d'un mode de règlement extrajudiciaire des conflits, sont soumis à la cour provinciale ou à la cour fédérale siégeant à Ottawa (Ontario), et chaque personne, entité ou organisation admet par les présentes que de tels litiges relèvent de la compétence personnelle et exclusive de ces tribunaux. Si une affaire est soumise à une cour provinciale ou à une cour fédérale, les demandeurs, les abonnés et les parties utilisatrices renoncent aux droits qu'ils peuvent avoir à un procès avec jury.

2.4.1.1 Force majeure

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, les revendeurs ou covendeurs, les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs et leurs employés et administrateurs ne sont pas en défaillance aux termes des présentes et ne sont pas responsables des pertes, frais, dépenses, obligations, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant des retards dans l'exécution des modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice ou de l'omission d'exécuter ou de respecter ces modalités, ou s'y rapportant, pour des motifs échappant raisonnablement à leur contrôle, lesquels motifs incluent les cas fortuits ou l'ennemi public, les émeutes et insurrections, les guerres, accidents, incendies, grèves et autres conflits de travail (peu importe que Entrust.net soit en mesure ou non d'accéder aux demandes), les embargos et les actions en justice, l'omission de toute autorité de certification supérieure, l'omission d'obtenir les permis ou les autorisations d'exportation, la main-d'œuvre, les matériaux, l'énergie, les services publics, les composantes ou la machinerie nécessaires, et les actes d'autorités civiles ou militaires.

2.4.1.2 Interprétation

Tous les renvois dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL à des « articles » se rapportent à des articles du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Les pronoms neutres et toute variation de ceux-ci utilisés dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL sont réputés inclure le féminin et le masculin, et tous les termes utilisés au singulier sont réputés inclure le pluriel, et vice versa, selon le contexte. Les termes « des présentes », « dans les présentes », « ci-après » et autres termes semblables renvoient au présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL dans son ensemble, lequel peut être à l'occasion modifié ou complété, et non à une section contenue dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Les termes « notamment » ou « y compris » utilisés dans les présentes ne sont pas exclusifs et signifient « notamment, sans restreindre la portée de ce qui précède ».

2.4.2 Dissociabilité, maintien, regroupement et avis

2.4.2.1 Dissociabilité

Dans la mesure du possible, chaque disposition de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement et d'un contrat avec une partie utilisatrice est interprétée de manière à être exécutoire et valide sous le régime des lois applicables. Si l'application à des circonstances ou à des faits donnés de l'ensemble ou d'une partie de l'une des dispositions de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice est jugée invalide ou non exécutoire par un arbitre ou un tribunal compétent, (i) l'application de la disposition en question à tout autre circonstance ou fait donné demeure valide et exécutoire, et la validité des autres dispositions de l'énoncé de pratique de certification Entrust.net SSL Web Server, d'une entente

d'abonnement ou d'un contrat avec une partie utilisatrice n'en est aucunement compromise, et (ii) la disposition en question doit être appliquée dans la mesure possible de façon à en respecter l'esprit et elle doit être modifiée dans la seule mesure nécessaire pour la rendre valide et exécutoire.

IL EST EXPRESSÉMENT ENTENDU ET CONVENU QUE CHAQUE DISPOSITION DE L'ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET SSL WEB SERVER, D'UNE ENTENTE D'ABONNEMENT OU D'UN CONTRAT AVEC UNE PARTIE UTILISATRICE PORTANT SUR (I) LA LIMITATION DE RESPONSABILITÉ OU DES DOMMAGES-INTÉRÊTS, SUR (II) LES DÉNÉGATIONS DE DÉCLARATIONS, DE GARANTIES, DE CONDITIONS OU DE RESPONSABILITÉS, OU SUR (III) L'INDEMNISATION, SE VEUT EXPRESSÉMENT DISSOCIABLE DE TOUTE AUTRE DISPOSITION DE L'ÉNONCÉ DE PRATIQUES DE CERTIFICATION ENTRUST.NET POUR SERVEURS WEB SSL, D'UNE ENTENTE D'ABONNEMENT OU D'UN CONTRAT AVEC UNE PARTIE UTILISATRICE, ET DOIT ÊTRE INTERPRÉTÉE ET APPLIQUÉE DANS CE SENS.

2.4.2.2 Maintien

Les dispositions de l'article intitulé « Définitions » et les articles 2.1.3.1, 2.1.4.1, 2.2, 2.3, 2.4, 2.8, 2.9, 3.1.5, 3.1.6, 4.6 et 8.2 subsistent en cas de résiliation ou d'expiration de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice. Tous les renvois à des articles qui subsistent en cas de résiliation de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice, incluent tous les paragraphes de ces articles. Toutes les obligations de paiement subsistent en cas de résiliation ou d'expiration de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice.

2.4.2.3 Regroupement

L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, les ententes d'abonnement et les contrats avec une partie utilisatrice énoncent tous les droits et obligations d'Entrust.net, des tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, des revendeurs et covendeurs, des sous-entrepreneurs, distributeurs, mandataires et fournisseurs et de leurs employés ou administrateurs, et de tout demandeur, tout abonné ou toute partie utilisatrice ou autre personne, entité ou organisation relativement à l'objet des présentes et des autres ententes mentionnées, et il ne peut être ajouté ou dérogé à ces droits et obligations par des contrats, des communications ou des ententes antérieures de quelque nature que ce soit, qu'elles soient verbales ou écrites. Les droits et obligations d'Entrust.net, des tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, des revendeurs et covendeurs, des sous-entrepreneurs, distributeurs, mandataires et fournisseurs et de leurs employés et administrateurs ne peuvent être modifiés ou faire l'objet d'une renonciation par entente verbale et ne peuvent être modifiés qu'au moyen d'un document signé ou certifié authentique par un représentant dûment autorisé d'Entrust.net.

2.4.2.4 Dispositions conflictuelles

En cas de conflit entre les dispositions de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et de toute entente écrite explicite conclue entre Entrust.net ou une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL et un abonné ou une partie utilisatrice relativement aux certificats Entrust.net pour serveurs Web SSL ou à tout service fourni relativement aux certificats Entrust.net pour serveurs Web SSL, cette autre entente écrite explicite prévaut. En cas d'incompatibilité entre les dispositions de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et les dispositions d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice, les modalités du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL prévalent.

2.4.2.5 Renonciation

L'omission par Entrust.net de faire appliquer à tout moment l'une ou l'autre disposition du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement conclue avec Entrust.net ou d'un contrat conclu entre une partie utilisatrice et Entrust.net, ou l'omission d'Entrust.net d'exiger à quelque moment que ce soit l'exécution par un demandeur, un abonné, une partie utilisatrice ou par toute autre personne, entité ou organisation de l'une ou l'autre disposition du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement conclue avec Entrust.net ou d'un contrat conclu entre une partie utilisatrice et Entrust.net, ne doivent pas être considérées comme une renonciation présente ou future à l'application de cette disposition, ni ne compromettent de quelque façon que ce soit le droit d'Entrust.net de faire appliquer cette disposition par la suite. La renonciation expresse d'Entrust.net à toute disposition, condition ou exigence prévue dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans une entente d'abonnement conclue avec Entrust.net ou dans un contrat conclu entre une partie utilisatrice et Entrust.net, ne constitue pas une renonciation à une obligation éventuelle de respecter cette disposition, condition ou exigence. L'omission d'une tierce autorité d'enregistrement indépendante ou d'un revendeur relevant d'une autorité de certification Entrust.net pour serveurs Web SSL (« autorité d'enregistrement ») de faire appliquer à quelque moment que ce soit l'une ou l'autre disposition du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement conclue avec cette autorité d'enregistrement ou de tout contrat conclu entre une partie utilisatrice et cette autorité d'enregistrement, ou l'omission de cette autorité d'enregistrement d'exiger à quelque moment que ce soit l'exécution par un demandeur, un abonné, une partie utilisatrice ou par toute autre personne, entité ou organisation, du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement conclue avec cette autorité d'enregistrement ou d'un contrat conclu entre une partie utilisatrice et cette autorité d'enregistrement, ne doivent d'aucune façon être considérées comme une renonciation présente ou future à l'application de cette disposition, ni ne compromettent de quelque façon que ce soit le droit de cette autorité d'enregistrement de faire appliquer cette disposition par la suite. La renonciation expresse d'une autorité d'enregistrement à toute disposition, condition ou exigence prévue dans une entente d'abonnement conclue avec cette autorité d'enregistrement ou dans un contrat conclu entre une partie utilisatrice et cette autorité d'enregistrement ne constitue pas une renonciation à une obligation éventuelle de respecter cette disposition, condition ou exigence.

2.4.2.6 Avis

Tout avis d'un abonné, un demandeur ou une partie utilisatrice à Entrust.net aux termes du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice est donné par écrit à l'adresse précisée ci-dessous par courrier affranchi avec accusé de réception, par télécopieur ou par service de messagerie de 24 h, et il est valide à compter, (i) dans le cas d'un envoi par télécopieur ou par service de messagerie, le jour ouvrable suivant et, (ii) dans le cas d'un envoi par courrier avec accusé de réception, cinq (5) jours ouvrables suivant la date de mise à la poste. Tout avis d'Entrust.net aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice est donné par courrier électronique ou par télécopieur ou service de messagerie à la dernière adresse, adresse électronique ou au dernier numéro de télécopieur de l'abonné contenu dans le dossier d'Entrust.net. En cas d'avis par courrier électronique, l'avis est valable le jour ouvrable suivant. En cas d'avis par courrier affranchi avec accusé de réception, par télécopieur ou par service de messagerie de 24 h, l'avis est valable ainsi qu'il est prévu aux points (i) ou (ii), selon le moyen utilisé.

Adresse de Entrust.net:	Entrust.net Inc.
aux fins d'un avis	1000, promenade Innovation
	Ottawa (Ontario)
	Canada, K2K 3E7
	Attention : Directeur des opérations, Entrust.net
	Télécopieur : 1 (877) 839-3538

2.4.2.7 Cession

Les certificats Entrust.net pour serveurs Web SSL et les droits accordés aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice appartiennent personnellement au demandeur, à l'abonné ou à la partie utilisatrice qui a conclu l'entente d'abonnement ou le contrat avec une partie utilisatrice, et ne peuvent être cédés, vendus, transférés ou faire l'objet d'une disposition, volontairement ou involontairement, par effet de la loi ou autrement, sans le consentement préalable écrit d'Entrust.net ou de l'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL avec laquelle le demandeur, l'abonné ou la partie utilisatrice a conclu un contrat. Toute tentative de cession ou de transfert sans ce consentement est nulle et met fin immédiatement aux droits du demandeur, de l'abonné ou de la partie utilisatrice prévus dans l'énoncé de pratique de certification Entrust.net SSL Web Server, l'entente d'abonnement ou le contrat avec une partie utilisatrice. Entrust.net peut céder, vendre ou transférer l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, une entente d'abonnement ou un contrat avec une partie utilisatrice, ou en disposer autrement, ainsi que tous ses droits et obligations prévus dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, une entente d'abonnement ou un contrat avec une partie utilisatrice (i) à une société liée ou (ii) dans le cadre d'une vente, d'une fusion ou de tout autre transfert de la totalité ou presque des éléments d'actifs ou des stocks de l'entreprise d'Entrust.net auxquels se rapportent l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, les ententes d'abonnement et les contrats avec une partie utilisatrice. Sous réserve des limitations qui précèdent, la présente entente lie les successeurs et les ayant droit autorisés d'Entrust.net, les tierces autorités d'enregistrement relevant des autorités de certification Entrust.net, les demandeurs, les abonnés ou les parties utilisatrices, le cas échéant, et profitent à ceux-ci.

2.4.3 Règlement des différends

Tout différend entre un abonné ou un demandeur et Entrust.net ou toute tierce autorité d'enregistrement relevant des autorités de certification Entrust.net, ou une partie utilisatrice et Entrust.net ou toute tierce autorité d'enregistrement agissant en conformité avec les autorités de certification Entrust.net est assujéti à une procédure de médiation conformément aux Règles de médiation en matière commerciale de l'Association américaine d'arbitrage, qui doit se tenir, en anglais, à Ottawa (Ontario). Si la médiation ne permet pas de régler le différend dans un délai de trente (30) jours, celui-ci est soumis à l'arbitrage obligatoire. L'arbitre a le droit de trancher toutes les questions relatives à l'arbitrabilité. Le différend est définitivement réglé à l'arbitrage conformément aux règles de l'Association américaine d'arbitrage, modifiées par la présente disposition. Cet arbitrage doit se tenir, en anglais, à Ottawa (Ontario), devant un seul arbitre choisi par l'Association américaine d'arbitrage (AAA) parmi un groupe d'arbitres spécialisés en technologie, qui connaît raisonnablement bien les différends en matière de commerce électronique. L'arbitre applique les lois de la province de l'Ontario, sans égard à ses règles en matière de conflits des lois, et rend une décision écrite dans un délai de trente (30) jours à compter de la date de clôture de l'audition, mais au plus tard un (1) an suivant la date à laquelle la question a été soumise à l'arbitrage. La décision de l'arbitre est exécutoire et déterminante et peut être enregistrée auprès de tout tribunal compétent. Dans chaque procédure d'arbitrage, la partie qui obtient gain de cause a droit à une adjudication de la totalité ou d'une partie de ses frais découlant de l'arbitrage, y compris les honoraires d'avocat raisonnables effectivement payés. Rien dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans une entente d'abonnement ou un contrat avec une partie utilisatrice n'empêche Entrust.net ou une tierce autorité d'enregistrement relevant d'une autorité de certification Entrust.net de demander à un tribunal compétent une injonction temporaire ou permanente, sans enfreindre le présent article 2.4.3. et sans restreindre les pouvoirs de l'arbitre, relativement à (i) toute compromission alléguée ayant une incidence sur l'intégrité d'un certificat Entrust.net pour serveurs Web SSL, ou à (ii) tout manquement aux modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice. Le recours à l'arbitrage ou l'introduction d'une action ne soustraient pas le demandeur, l'abonné ou la partie utilisatrice à ses obligations aux termes de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice.

2.4.3.1 Délai de prescription en matière d'arbitrage et d'action

Toutes les procédures d'arbitrage et les actions en justice se rapportant à un certificat Entrust.net pour serveurs Web SSL ou à des services fournis relativement à un certificat Entrust.net pour serveurs Web SSL doivent être instituées avant l'expiration d'un délai de un (1) an suivant (i) l'expiration ou la révocation du certificat Entrust.net pour serveurs Web SSL Certificate en cause ou (ii) la date à laquelle le ou les services en cause sont fournis relativement au certificat Entrust.net pour serveurs Web SSL en litige, la date la plus rapprochée étant retenue. Il est interdit à toute partie d'instituer une procédure d'arbitrage ou une action se rapportant à un certificat Entrust.net pour serveurs Web SSL ou à un ou des services fournis relativement à un certificat Entrust.net pour serveurs Web SSL après l'expiration de ce délai.

2.5 Honoraires

Les honoraires facturés pour les services fournis par Entrust.net relativement à des certificats Entrust.net pour serveurs Web SSL sont énoncés dans le répertoire Entrust.net. Ces honoraires peuvent faire l'objet de modifications qui entrent en vigueur immédiatement après avoir été affichées dans le répertoire Entrust.net. Les honoraires facturés pour les services fournis par des tierces autorités d'enregistrement indépendantes, des revendeurs et des covendeurs relativement à des certificats Entrust.net pour serveurs Web SSL sont affichés sur les sites web exploités par ces autorités d'enregistrement, ces revendeurs et ces covendeurs. Les honoraires peuvent faire l'objet de modifications qui entrent en vigueur immédiatement après avoir été affichées sur ces sites web.

2.5.1 Frais d'émission ou de renouvellement d'un certificat

Voir le répertoire Entrust.net pour les frais réclamés par Entrust.net. Voir les sites web exploités par les autorités d'enregistrement relevant des autorités de certification Entrust.net, les revendeurs et les covendeurs pour les frais réclamés par ces autorités d'enregistrement, revendeurs et covendeurs.

2.5.2 Frais d'accès

Voir le répertoire Entrust.net pour les frais réclamés par Entrust.net. Voir les sites web exploités par les autorités d'enregistrement relevant des autorités de certification Entrust.net, les revendeurs et les covendeurs pour les frais réclamés par ces autorités d'enregistrement, revendeurs et covendeurs.

2.5.3 Frais d'accès à des renseignements concernant la révocation ou l'état

Voir le répertoire Entrust.net pour les frais réclamés par Entrust.net. Voir les sites web exploités par les autorités d'enregistrement relevant des autorités de certification Entrust.net, les revendeurs et les covendeurs pour les frais réclamés par ces autorités d'enregistrement, revendeurs et covendeurs.

2.5.4 Frais pour autres services comme des renseignements sur les politiques

Voir le répertoire Entrust.net pour les frais réclamés par Entrust.net. Voir les sites web exploités par les autorités d'enregistrement relevant des autorités de certification Entrust.net, les revendeurs et les covendeurs pour les frais réclamés par ces autorités d'enregistrement, revendeurs et covendeurs.

2.5.5 Politique de remboursement

Ni Entrust.net, ni les autorités d'enregistrement relevant des autorités de certification Entrust.net, ni les revendeurs ou covendeurs ne versent de remboursement relativement aux certificats Entrust.net pour serveurs Web SSL ou aux services fournis relativement à ces certificats.

2.6 Publication et répertoires

Entrust.net maintient le répertoire Entrust.net aux fins d'y conserver différents renseignements liés aux certificats Entrust.net pour serveurs Web SSL et à l'utilisation des autorités de certification Entrust.net pour serveurs Web SSL, des autorités d'enregistrement Entrust.net et des tierces autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL. L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et les divers autres renseignements connexes sont publiés dans le répertoire Entrust.net. Il est possible également d'obtenir l'énoncé de pratiques de certification Entrust.net SSL Web sur un support en papier en en faisant la demande à Entrust.net.

2.6.1 Publication de renseignements sur les AC

Les renseignements suivants sur les certificats Entrust.net pour serveurs Web SSL sont publiés dans le répertoire Entrust.net :

- (i) l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL;
- (ii) les renseignements et les ententes concernant l'abonnement à des certificats Entrust.net pour serveurs Web SSL et le fait de s'y fier;
- (iii) les révocations de certificats Entrust.net pour serveurs Web SSL effectuées par une autorité de certification Entrust.net pour serveurs Web SSL.

La présentation des données utilisée pour les certificats Entrust.net pour serveurs Web SSL et pour les listes de certificats révoqués dans le répertoire Entrust.net est conforme aux définitions connexes de schémas données dans la série de recommandations X.500 (édition de 1997) ainsi que certaines des améliorations définies dans cette même série de recommandations.

2.6.2 Fréquence de la publication

L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL peut être réédité et publié conformément à la politique énoncée à l'article 8 du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

2.6.3 Contrôles en matière d'accès

L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL est publié dans le répertoire Entrust.net. Tous les demandeurs, les abonnés et les parties utilisatrices ont accès à l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, qui ne peut cependant être modifié que par l'autorité de politiques d'Entrust.net.

2.6.4 Répertoires

Les autorités de certification Entrust.net pour serveurs Web SSL tiennent les répertoires Entrust.net pour permettre l'accès aux renseignements se rapportant aux certificats Entrust.net pour serveurs Web SSL et aux LCR. Les renseignements qui se trouvent dans les répertoires Entrust.net sont accessibles au moyen d'une interface web et sont régulièrement mis à jour ainsi qu'il est prévu dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Les répertoires Entrust.net constituent l'unique source reconnue de LCR et d'autres renseignements relatifs aux certificats Entrust.net pour serveurs Web SSL.

2.7 Vérification de conformité

Les autorités de certification Entrust.net pour serveurs Web SSL, les autorités d'enregistrement exploitées par Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL sont soumises à une vérification de conformité aux pratiques et aux procédures prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

2.7.1 Fréquence des vérifications de conformité d'une entité

Une fois par année civile, les autorités de certification Entrust.net pour serveurs Web SSL, les autorités d'enregistrement exploitées par Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL sont soumises à une vérification de conformité aux pratiques et aux procédures prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Si un rapport de vérification recommande qu'une mesure correctrice soit prise, Entrust.net ou la tierce autorité d'enregistrement indépendante concernée prend des mesures correctrices dans un délai de trente (30) jours de la réception du rapport de vérification.

2.7.2 Identité/compétences du vérificateur

La vérification de conformité est effectuée par un cabinet d'experts-comptables aux compétences reconnues en matière d'évaluation des autorités de certification et des autorités d'enregistrement. Le cabinet Deloitte & Touche LLP a été sélectionné en tant que vérificateur pour les autorités de certification Entrust.net et les autorités d'enregistrement exploitées par Entrust.net.

2.7.3 Rapports entre le vérificateur et la partie qui fait l'objet d'une vérification

Le cabinet d'experts-comptables sélectionné pour effectuer une vérification de conformité à l'égard des autorités de certification Entrust.net pour serveurs Web SSL, des autorités d'enregistrement exploitées par Entrust.net et des tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net n'a aucun lien avec l'entité qui fait l'objet de la vérification.

2.7.4 Objet de la vérification

La vérification de conformité permet de vérifier que les autorités de certification Entrust.net pour serveurs Web SSL, les autorités d'enregistrement exploitées par Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net respectent les politiques et les procédures prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

2.7.5 Mesures correctrices

Sur réception d'une vérification de conformité qui relève des manquements, les autorités de certification Entrust.net pour serveurs Web SSL, les autorités d'enregistrement exploitées par Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net prennent des moyens commercialement raisonnables pour remédier à ces manquements dans les plus brefs délais.

2.7.6 Communication des résultats

Les résultats de toute vérification de conformité sont communiqués, dans le cas des autorités de certification Entrust.net pour serveurs Web SSL et des autorités d'enregistrement exploitées par Entrust.net, à l'autorité opérationnelle d'Entrust.net et, dans le cas des tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net, à l'autorité opérationnelle de cette autorité d'enregistrement.

2.8 Caractère confidentiel

Ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net, ni les revendeurs et covendeurs ne peuvent divulguer ou vendre les noms d'un demandeur ou d'un abonné (ou tout autre renseignement fourni par un demandeur ou un abonné dans une demande de certificat Entrust.net pour serveurs Web SSL), sauf conformément au présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, à une entente d'abonnement ou à un contrat avec une partie utilisatrice. Entrust.net et toutes les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net et tous les revendeurs et covendeurs exercent un soin raisonnable pour prévenir l'utilisation ou la divulgation de ces renseignements à des fins autres que celles qui sont prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans une entente d'abonnement ou dans un contrat avec une partie utilisatrice. Nonobstant ce qui précède, les demandeurs et les abonnés reconnaissent que certains des renseignements fournis dans une demande de certificat Entrust.net pour serveurs Web SSL sont incorporés aux certificats Entrust.net pour serveurs Web SSL et que Entrust.net, les

tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net et les revendeurs et covendeurs ont le droit de rendre ces renseignements accessibles au public.

2.8.1 Renseignements confidentiels

Les renseignements qui sont fournis par les demandeurs, les abonnés ou les parties utilisatrices aux fins de l'abonnement à un certificat Entrust.net pour serveurs Web SSL ou de son utilisation, qui ne font pas partie des renseignements décrits à l'article 2.8.2 ci-après, sont considérés confidentiels. Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net ont le droit de divulguer ces renseignements à des sous-entrepreneurs ou mandataires qui participent avec Entrust.net à la vérification des renseignements fournis dans les demandes de certificats Entrust.net pour serveurs Web SSL ou à l'exploitation des autorités de certification Entrust.net pour serveurs Web SSL ou des autorités d'enregistrement exploitées par Entrust.net. Les renseignements considérés confidentiels ne peuvent être divulgués que si cette divulgation est rendue obligatoire par suite de procédures légales, judiciaires ou administratives ou qu'elle est par ailleurs obligatoire en droit. Entrust.net et les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net ont le droit de divulguer des renseignements considérés confidentiels aux conseillers juridiques ou financiers dont les services sont retenus dans le cadre de procédures légales, judiciaires ou administratives ou autres procédures obligatoires en droit, à des acheteurs potentiels, des avocats, des comptables, des banques et des sources de financement et à leurs conseillers relativement à des fusions, des acquisitions ou des restructurations.

2.8.2 Renseignements non confidentiels

Les renseignements inclus dans un certificat Entrust.net pour serveurs Web SSL ou une liste des certificats révoqués ne sont pas considérés confidentiels. Les renseignements contenus dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ne sont pas considérés confidentiels. Sans limiter la portée de ce qui précède, les renseignements (i) qui étaient ou deviennent connus sans qu'Entrust.net, une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, un revendeur ou covendeur soit en faute, (ii) dont Entrust.net, une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, un revendeur ou un covendeur prend ou a pris connaissance légitimement sans qu'il y ait une restriction quant au caractère confidentiel ou à l'exclusivité par une source autre que l'abonné, (iii) qui sont conçus de façon indépendante par Entrust.net, une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, un revendeur ou un covendeur, ou (iv) dont la divulgation est approuvée par un abonné, ne sont pas considérés confidentiels.

2.8.3 Divulgence de renseignements sur la révocation ou la suspension d'un certificat

Si un certificat Entrust.net pour serveurs Web SSL est révoqué par une autorité de certification Entrust.net pour serveurs Web SSL, un numéro de série est inclus dans l'entrée de la liste des certificats révoqués visant les certificats Entrust.net pour serveurs Web SSL révoqués.

2.8.4 Divulgence aux responsables de l'application de la loi

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs et les covendeurs ont le droit de divulguer des renseignements considérés confidentiels à des responsables de l'application de la loi conformément aux lois applicables.

2.8.5 Divulgence dans le cadre de procédures au civil

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs et les covendeurs peuvent divulguer des renseignements considérés confidentiels dans le cadre de procédures d'arbitrage, d'un litige ou de toute autre procédure légale, judiciaire ou administrative se rapportant à ces renseignements. Cette divulgation est permise à condition que Entrust.net, la tierce autorité d'enregistrement indépendante, le revendeur ou le covendeur prennent des moyens commercialement raisonnables pour obtenir une ordonnance préventive enregistrée auprès d'un tribunal restreignant l'utilisation et la divulgation de ces renseignements aux seuls

renseignements raisonnablement nécessaires aux fins de l'arbitrage, du litige ou de toute autre procédure légale, judiciaire ou administrative.

2.8.6 Divulgateion à la demande du propriétaire

Entrust.net, la tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, les revendeurs et les covendeurs peuvent divulguer des renseignements qui leur sont fournis par un demandeur, un abonné ou une partie utilisatrice à la demande de ces derniers.

2.8.7 Autres circonstances dans lesquelles sont divulgués des renseignements

Aucune disposition.

2.9 Droits de propriété intellectuelle

Entrust.net conserve tous les droits, titres et intérêts (y compris tous les droits de propriété intellectuelle) sur tous les certificats Entrust.net pour serveurs Web SSL, exception faite des renseignements fournis par un demandeur ou un abonné qui sont inclus dans un certificat Entrust.net pour serveurs Web SSL, lesquels renseignements demeurent la propriété du demandeur ou de l'abonné. Tous les demandeurs et abonnés accordent à Entrust.net et à toute autorité d'enregistrement relevant d'une autorité de certification Entrust.net l'autorisation non exclusive, internationale, acquittée et libre de toute redevance d'utiliser, de copier, de modifier, d'afficher en public et de distribuer ces renseignements, par tous les moyens et sous toute forme actuels ou futurs aux fins prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans l'entente d'abonnement de l'abonné et dans tout contrat avec une partie utilisatrice. Entrust.net et les autorités d'enregistrement relevant des autorités de certification Entrust.net ont le droit de transférer, de transporter ou de céder cette autorisation en conjugaison avec tout transfert, transport ou cession visé à l'article 2.4.2.7. Entrust.net accorde aux abonnés et aux parties utilisatrices l'autorisation non exclusive et incessible d'utiliser, de copier et de distribuer des certificats Entrust.net pour serveurs Web SSL, à condition que ces certificats soient utilisés aux fins prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans l'entente d'abonnement de l'abonné et dans tout contrat avec une partie utilisatrice, et qu'ils soient reproduits entièrement et fidèlement et qu'ils ne soient pas publiés dans une base de données, un répertoire ou un annuaire accessibles au public sans l'autorisation écrite expresse d'Entrust.net. En dehors des conditions précédemment citées, aucun autre droit n'est et ne devrait être accordé, de manière implicite ou explicite. En fonction de leur disponibilité, Entrust.net peut à sa discrétion fournir des copies de un ou plusieurs Certificats Co-certifiés à ses abonnés pour usage uniquement avec les certificats Entrust.net pour serveurs Web SSL émises aux-dits abonnés. Entrust.net conserve tous les droits et titres (incluant tous les droits de propriété intellectuelle) dans et sous le Certificat Co-certifié.

Entrust.net autorise la reproduction de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL à condition que (i) l'avis de droit d'auteur figurant sur la première page du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL figure sur toute copie de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, et que (ii) l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL soit reproduit entièrement et fidèlement. Entrust.net conserve tous les droits, titres et intérêts (y compris tous les droits de propriété intellectuelle) sur l'énoncé de pratiques de certification Entrust.net SSL Web Server.

Entrust.net, les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, les revendeurs et covendeurs, les sous-entrepreneurs, distributeurs, mandataires et fournisseurs ou leurs employés et administrateurs ne peuvent en aucun cas être tenus responsables envers un demandeur, un abonné ou une partie utilisatrice ou tout autre tiers des pertes, frais, obligations, dépenses, dommages-intérêts, réclamations ou montants fixés dans un règlement découlant de toute allégation, ou s'y rapportant, de contrefaçon, de détournement, d'affaiblissement, de concurrence injuste ou de toute autre violation d'un brevet, d'une marque de commerce, d'un droit d'auteur, d'un secret de fabrication ou de tout autre droit de propriété intellectuelle ou autre d'une personne, entité ou organisation

dans quelque administration que ce soit, découlant d'un certificat Entrust.net pour serveurs Web SSL ou des services fournis relativement à un certificat Entrust.net pour serveurs Web SSL, ou s'y rapportant.

3 Identification et Authentification

3.1 Enregistrement initial

Pour obtenir un certificat Entrust.net pour serveurs Web SSL, le demandeur doit : (i) générer une bicle sûre par des techniques cryptographiques établies, (ii) accepter toutes les modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et de l'entente d'abonnement, (iii) remplir et présenter une demande de certificat Entrust.net pour serveurs Web SSL contenant tous les renseignements requis par une autorité d'enregistrement exploitée par Entrust.net ou par une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL (une « autorité d'enregistrement »), et ne contenant aucune erreur, fausse déclaration ou omission. Une fois que le demandeur a rempli la demande de certificat Entrust.net pour serveurs Web SSL et qu'il a accepté les modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et de l'entente d'abonnement, une autorité d'enregistrement ou un tiers autorisé par une autorité d'enregistrement effectue une vérification limitée de certains des renseignements fournis dans la demande de certificat Entrust.net pour serveurs Web SSL. Si l'étape de la vérification limitée effectuée par une autorité d'enregistrement est franchie avec succès, l'autorité d'enregistrement peut, à sa seule discrétion, demander à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre au demandeur un certificat Entrust.net pour serveurs Web SSL. Si elle refuse de demander l'émission d'un certificat Entrust.net pour serveurs Web SSL, l'autorité d'enregistrement (i) prend des moyens commercialement raisonnables pour informer le demandeur par courrier électronique des raisons de son refus et (ii) rembourse rapidement les montants qui ont été payés relativement à la demande de certificat Entrust.net pour serveurs Web SSL. Si une demande de certificat Entrust.net pour serveurs Web SSL franchit l'étape de la vérification avec succès, l'autorité d'enregistrement demande à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre un certificat Entrust.net pour serveurs Web SSL et avise le demandeur par courrier électronique de l'émission d'un certificat Entrust.net pour serveurs Web SSL par l'autorité de certification Entrust.net pour serveurs Web SSL. Le demandeur recevra un URL qu'il peut utiliser pour récupérer le certificat Entrust.net pour serveurs Web SSL. Une fois émis le certificat Entrust.net pour serveurs Web SSL, ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant des autorités de certification Entrust.net pour serveurs Web SSL, ni les revendeurs ou covendeurs, ni les sous-entrepreneurs, distributeurs, mandataires ou fournisseurs, ni leurs employés et administrateurs n'ont l'obligation d'effectuer une surveillance, une enquête ou une vérification constante des renseignements fournis dans une demande de certificat Entrust.net pour serveurs Web SSL.

3.1.1 Types de noms

Les noms du sujet dans un certificat Entrust.net pour serveurs Web SSL sont conformes au format des noms distinctifs (DN) défini dans la norme X.500. Les autorités de certification Entrust.net pour serveurs Web SSL utilisent une règle d'affectation unique des noms ainsi qu'il est exposé ci-après. Chaque certificat Entrust.net pour serveurs Web SSL doit contenir les renseignements suivants :

- (i) le « nom du pays » (C), c'est-à-dire le code de deux lettres selon ISO 3166 pour le pays dans lequel le demandeur se trouve et prévoit héberger le serveur pour le Web sur lequel il a l'intention d'installer le certificat Entrust.net pour serveurs Web SSL;
- (ii) le « nom de l'organisation » (O), c'est-à-dire le nom de l'organisation dans le cas d'une société, d'une association de personnes ou d'une autre entité. Dans le cas d'une entreprise individuelle, le nom de l'organisation peut être celui du demandeur;
- (iii) le « nom de l'unité organisationnelle » (OU), qui est un champ optionnel. Le champ OU peut être utilisé pour établir une distinction entre différents groupes organisationnels au sein d'une organisation (par exemple, pour faire la distinction entre les ressources humaines, le marketing et le développement);
- (iv) le « nom commun » (CN), c'est-à-dire le nom de l'hôte ou du chemin d'accès complet utilisé dans le DNS du serveur pour Web sur lequel le demandeur a l'intention d'installer le certificat Entrust.net pour serveurs Web SSL.

3.1.2 Noms significatifs

La valeur du nom commun utilisé dans un certificat Entrust.net pour serveurs Web SSL est le nom de l'hôte ou du chemin d'accès complet du demandeur utilisé dans le DNS du serveur pour Web sur lequel il a l'intention d'installer le certificat Entrust.net pour serveurs Web SSL.

3.1.3 Règles d'interprétation des différentes formes de noms

Les noms du sujet pour les certificats Entrust.net pour serveurs Web SSL sont interprétés conformément aux articles 3.1.1 et 3.1.2.

3.1.4 Caractère unique des noms

Les noms sont définis sans ambiguïté pour chaque sujet dans un répertoire Entrust.net. L'attribut Nom distinctif devrait être exclusif au serveur pour Web relativement auquel il est attribué, et il vise à empêcher que le même nom de sujet soit attribué à deux certificats Entrust.net pour serveurs Web SSL. Un numéro de série unique est attribué à chaque certificat Entrust.net pour serveurs Web SSL.

3.1.5 Règlement des différends en matière de revendication d'un nom

Les noms des sujets dans les certificats Entrust.net pour serveurs Web SSL sont attribués selon le principe du « premier arrivé, premier servi ». Lorsqu'elle accepte un nom de sujet en vue de son incorporation dans un certificat Entrust.net pour serveurs Web SSL, l'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL ne se prononce pas sur la question de savoir si l'utilisation de tels renseignements viole, détourne ou affaiblit des droits de propriété intellectuelle ou autres d'une personne, entité ou organisation, ou entre injustement en concurrence avec ces droits ou y porte par ailleurs atteinte. Les autorités de certification Entrust.net et les autorités d'enregistrement relevant des autorités de certification Entrust.net n'agissent pas à titre d'arbitres ni ne règlent les différends entre des abonnés ou entre des abonnés et des plaignants tiers relativement à l'utilisation de renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL. L'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ne confère aucun droit procédural ou fondamental à un abonné ou un tiers plaignant relativement à des renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL. Il n'est d'aucune façon interdit aux autorités de certification Entrust.net et aux autorités d'enregistrement relevant des autorités de certification Entrust.net de demander des mesures de redressement en droit ou en equity (y compris une injonction) concernant un différend entre abonnés ou entre abonnés et plaignants tiers ou un différend entre des abonnés et une autorité de certification Entrust.net pour serveurs Web SSL ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, ou entre un tiers plaignant et une autorité de certification Entrust.net pour serveurs Web SSL ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, découlant de renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL. Les autorités de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL ont respectivement le droit de révoquer des certificats Entrust.net pour serveurs Web SSL et celui d'en demander la révocation sur réception d'une ordonnance dûment authentifiée d'un arbitre ou d'un tribunal compétent exigeant la révocation d'un certificat Entrust.net pour serveurs Web SSL.

3.1.6 Reconnaissance, authentification et rôle des marques de commerce

Une autorité de certification Entrust.net pour serveurs Web SSL ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL peut, dans certaines circonstances, prendre des mesures à l'égard d'un certificat Entrust.net pour serveurs Web SSL contenant des renseignements susceptibles de violer les droits de propriété intellectuelle et commerciale d'un tiers plaignant. Si un tiers plaignant fournit à une autorité de certification Entrust.net pour serveurs Web SSL ou à une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL (i) une copie certifiée datant de moins de trois (3) mois de l'enregistrement d'une marque de commerce par le bureau principal des marques de commerce des États-Unis, du Canada, du Japon, de l'Australie ou de l'un ou l'autre des pays membres de l'Union européenne, à condition que cet enregistrement soit encore valide, (ii) une copie d'un avis écrit préalable adressé à l'abonné du certificat Entrust.net pour serveurs Web SSL en

litige indiquant que le plaignant estime que des renseignements contenus dans le certificat Entrust.net pour serveurs Web SSL de l'abonné violent ses droits de propriété intellectuelle et commerciale, et (iii) une déclaration par le plaignant indiquant le moyen par lequel un avis a été adressé à l'abonné et ses motifs de croire que l'abonné du certificat Entrust.net pour serveurs Web SSL en litige a reçu cet avis, une autorité de certification Entrust.net pour serveurs Web SSL ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL peut prendre les mesures suivantes. L'autorité de certification Entrust.net pour serveurs Web SSL ou l'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL peut déterminer si la date d'émission du certificat Entrust.net pour serveurs Web SSL de l'abonné est antérieure à la date d'enregistrement qui figure sur l'enregistrement de la marque de commerce fourni par le plaignant. Si la date d'émission du certificat Entrust.net pour serveurs Web SSL de l'abonné est antérieure à la date d'enregistrement de la marque de commerce, l'autorité de certification Entrust.net pour serveurs Web SSL ou l'autorité d'enregistrement relevant de l'autorité de certification Entrust.net pour serveurs Web SSL ne prend aucune autre mesure à moins qu'on lui présente une ordonnance authentifiée d'un arbitre ou d'un tribunal compétent. Si la date d'émission du certificat Entrust.net pour serveurs Web SSL est postérieure à la date d'enregistrement qui figure sur l'enregistrement de la marque de commerce fourni par le plaignant, l'autorité de certification Entrust.net pour serveurs Web SSL ou l'autorité d'enregistrement relevant de l'autorité de certification Entrust.net pour serveurs Web SSL demande à l'abonné de fournir une preuve de propriété de l'enregistrement de la marque de commerce correspondant par le bureau principal des marques de commerce des États-Unis, du Canada, du Japon, de l'Australie ou de l'un ou l'autre des pays membres de l'Union européenne. Si l'abonné peut fournir une copie certifiée, ainsi qu'il est mentionné ci-dessus, délivrée avant l'enregistrement de la marque de commerce du plaignant ou le même jour, l'autorité de certification Entrust.net pour serveurs Web SSL ou l'autorité d'enregistrement relevant de l'autorité de certification Entrust.net pour serveurs Web SSL ne prend aucune autre mesure à moins qu'on lui présente une ordonnance authentifiée d'un arbitre ou d'un tribunal compétent. Si l'abonné ne répond pas dans les dix (10) jours ouvrables ou si la date de la copie certifiée de l'enregistrement de la marque de commerce fournie par l'abonné est postérieure à la copie certifiée de l'enregistrement de la marque de commerce fournie par le plaignant, l'autorité de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant de cette autorité de certification Entrust.net pour serveurs Web SSL peuvent respectivement révoquer le certificat Entrust.net pour serveurs Web SSL en litige ou en demander la révocation.

Si un abonné institue des procédures contre un plaignant, ou si un plaignant institue des procédures contre un abonné, et que ces procédures se rapportent à des renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL délivré, et si la partie qui institue les procédures fournit à une autorité de certification Entrust.net pour serveurs Web SSL ou à une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL une copie de la plainte ou de la déclaration estampillée, l'autorité de certification Entrust.net pour serveurs Web SSL maintient en l'état actuel le certificat Entrust.net pour serveurs Web SSL, ou l'autorité d'enregistrement relevant de l'autorité de certification Entrust.net pour serveurs Web SSL demande à l'autorité de certification Entrust.net pour serveurs Web SSL de maintenir en l'état actuel le certificat Entrust.net pour serveurs Web SSL, sous réserve des obligations de changer l'état de ce certificat Entrust.net pour serveurs Web SSL par ailleurs prévues dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, dans une entente d'abonnement ou dans un contrat avec une partie utilisatrice. Quand des procédures sont en cours, une autorité de certification Entrust.net pour serveurs Web SSL ne révoque pas le certificat Entrust.net pour serveurs Web SSL en litige, et une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL n'en demande pas la révocation, à moins qu'elle en reçoive l'ordre par un arbitre ou un tribunal compétent ou qu'elle y soit tenue par une disposition du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, d'une entente d'abonnement ou d'un contrat avec une partie utilisatrice. Dans le cas où des procédures sont instituées conformément à ce qui est mentionné précédemment, les autorités de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL se conforment à toute directive d'un tribunal compétent relativement à un certificat Entrust.net pour serveurs Web SSL en litige sans qu'elles soient nécessairement nommées comme parties aux procédures. Si elles sont nommées comme parties à des procédures relatives à un certificat Entrust.net pour serveurs Web SSL, Entrust.net et/ou les tierces parties exploitant une autorité

d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL ont le droit de prendre les mesures jugées nécessaires pour répondre à ces procédures ou y opposer une défense. Les abonnés ou les parties utilisatrices qui prennent part à des procédures relatives à un certificat Entrust.net pour serveurs Web SSL demeurent assujettis à toutes les modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de l'entente d'abonnement conclue par l'abonné et du contrat conclu par la partie utilisatrice à titre de partie utilisatrice.

Les autorités d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL avisent celle-ci de tout différend dont elles sont au courant et qui se rapporte à des renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL dont elles ont demandé l'émission.

3.1.7 Preuve de la possession d'une clé privée

Les autorités d'enregistrement vérifient la preuve de possession des DSC créées au moyen des algorithmes asymétriques réversibles (comme RSA) par validation de la signature sur la DSC soumise par le demandeur avec sa demande de certificat Entrust.net pour serveurs Web SSL.

3.1.8 Authentification de l'identité de l'organisation

Les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL effectuent une vérification limitée de toute identité organisationnelle soumise par un demandeur ou un abonné. Les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL déterminent si l'identité, l'adresse et le nom de domaine de l'organisation fournis dans une demande de certificat Entrust.net pour serveurs Web SSL sont conformes aux renseignements contenus dans des bases de données de tiers ou des sources gouvernementales. Les renseignements et les sources utilisés aux fins de la vérification limitée des demandes de certificat Entrust.net pour serveurs Web SSL peuvent varier selon le pays du demandeur ou de l'abonné. Si des identités organisationnelles ne sont enregistrées auprès d'aucune source gouvernementale, les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL prennent des moyens commercialement raisonnables pour confirmer l'existence de l'organisation en cause. Elles peuvent notamment s'informer auprès de banques et d'autres personnes ou établissements dignes de foi. Les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL doivent se conformer à toutes les pratiques de vérification formulées par l'autorité de politiques d'Entrust.net.

L'autorité de politiques d'Entrust.net peut, à sa discrétion, mettre les pratiques de vérification à jour afin d'améliorer le processus de vérification de l'identité de l'organisation. Tout changement des pratiques de vérification est publié conformément aux procédures normales de mise à jour de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

3.1.9 Authentification de l'identité du particulier

Les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL effectuent une vérification limitée de l'identité du particulier soumise par un demandeur ou un abonné. Aux fins d'établir l'exactitude de l'identité d'un particulier, celui-ci doit comparaître devant un représentant d'une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL ou un notaire dans le pays du demandeur. Le particulier doit présenter trois (3) pièces d'identité avec photographie. Le genre de pièce d'identité acceptable aux fins d'une identification en règle dépend du pays du demandeur.

L'autorité de politiques d'Entrust.net peut, à sa discrétion, mettre les pratiques de vérification à jour afin d'améliorer le processus de vérification de l'identité du particulier. Tout changement des pratiques de vérification est publié conformément aux procédures normales de mise à jour de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

3.2 Mise à jour régulière des clés

Chaque certificat Entrust.net pour serveurs Web SSL contient une date d'expiration afin de réduire au minimum l'exposition de la clé associée au certificat. Pour cette raison, lorsqu'elle traite une commande

de certificat Entrust.net pour serveurs Web SSL, Entrust.net exige qu'une nouvelle clé soit générée et que la nouvelle clé publique de cette clé soit soumise avec la demande de certificat Entrust.net pour serveurs Web SSL du demandeur. Entrust.net ne renouvelle aucun certificat Entrust.net pour serveurs Web SSL. Par conséquent, s'il souhaite continuer d'utiliser un certificat Entrust.net pour serveurs Web SSL après la date d'expiration de celui-ci, l'abonné doit obtenir un nouveau certificat Entrust.net pour serveurs Web SSL et remplacer le certificat Entrust.net pour serveurs Web SSL expiré. Les abonnés soumettant une demande pour un nouveau certificat Entrust.net pour serveurs Web SSL, doivent franchir l'étape initiale de la demande prévue à l'article 3.1, notamment générer une nouvelle clé et soumettre tous les renseignements requis aux fins d'une demande initiale de certificat Entrust.net pour serveurs Web SSL. L'autorité d'enregistrement qui a traité la demande de certificat Entrust.net pour serveurs Web SSL de l'abonné prend des moyens commercialement raisonnables pour aviser l'abonné de l'expiration à brève échéance de son certificat Entrust.net SSL Web en faisant parvenir un message par courrier électronique à la personne-ressource en matière technique dont le nom figure dans la demande de certificat Entrust.net pour serveurs Web SSL correspondante. L'abonné cesse immédiatement d'utiliser un certificat Entrust.net pour serveurs Web SSL expiré et le retire de tout support ou logiciel sur lequel il l'a installé.

3.3 Mise à jour suivant une révocation

Les autorités de certification Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL ne renouvellent aucun certificat Entrust.net pour serveurs Web SSL qui a été révoqué. S'il souhaite utiliser un certificat Entrust.net pour serveurs Web SSL après la révocation de celui-ci, l'abonné doit demander un nouveau certificat Entrust.net pour serveurs Web SSL et remplacer celui qui a été révoqué. Pour obtenir un nouveau certificat Entrust.net pour serveurs Web SSL, l'abonné doit franchir l'étape initiale de la demande prévue à l'article 3.1, notamment générer une nouvelle clé et soumettre tous les renseignements requis aux fins d'une demande initiale de certificat Entrust.net pour serveurs Web SSL. L'abonné cesse immédiatement d'utiliser un certificat Entrust.net pour serveurs Web SSL révoqué et retire celui-ci de tout support ou logiciel sur lequel il l'a installé.

3.4 Demande de révocation

L'abonné peut demander la révocation de son certificat Entrust.net pour serveurs Web SSL en tout temps à la condition qu'il puisse prouver à l'autorité d'enregistrement qui a traité sa demande de certificat Entrust.net pour serveurs Web SSL qu'il est la personne, l'organisation ou l'entité à qui le certificat Entrust.net pour serveurs Web SSL a été émis. L'autorité d'enregistrement authentifie la demande de révocation d'un certificat Entrust.net pour serveurs Web SSL d'un abonné en exigeant la phrase de passe soumise par l'abonné dans sa demande de certificat Entrust.net pour serveurs Web SSL ou une partie des renseignements fournis par l'abonné dans sa demande de certificat Entrust.net pour serveurs Web SSL. Sur réception et confirmation de ces renseignements, l'autorité d'enregistrement demande la révocation du certificat Entrust.net pour serveurs Web SSL de l'abonné dans un délai de quarante-huit (48) heures de la validation de la demande de révocation, et une autorité de certification Entrust.net pour serveurs Web SSL inscrit subséquemment le numéro de série du certificat Entrust.net pour serveurs Web SSL révoqué à la LCR d'un répertoire Entrust.net. Les autorités d'enregistrement relevant de l'autorité de certification Entrust.net pour serveurs Web SSL prennent des moyens commercialement raisonnables pour aviser l'abonné de la révocation de son certificat Entrust.net pour serveurs Web SSL en faisant parvenir un message par courrier électronique aux personnes-ressources en matière technique et de sécurité dont les noms figurent dans la demande de certificat Entrust.net pour serveurs Web SSL de l'abonné.

4 Exigences opérationnelles

4.1 Demande de certificat

Pour obtenir un certificat Entrust.net pour serveurs Web SSL, le demandeur doit suivre les procédures décrites à l'article 3.1 de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Une autorité d'enregistrement exploitée par Entrust.net ou une tierce autorité d'enregistrement indépendante relevant d'une autorité de certification Entrust.net pour serveurs Web SSL suit les procédures prévues aux articles 3.1.8 et 3.1.9 aux fins d'une vérification limitée de l'identité du demandeur.

4.2 Émission d'un certificat

Après la vérification limitée des renseignements fournis par un demandeur dans une demande de certificat Entrust.net pour serveurs Web SSL, une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL peut demander à une autorité de certification Entrust.net pour serveurs Web SSL d'émettre un certificat Entrust.net pour serveurs Web SSL. Sur réception de cette demande, l'autorité de certification Entrust.net pour serveurs Web SSL peut générer et signer numériquement un certificat Entrust.net pour serveurs Web SSL conformément au profil du certificat décrit à l'article 7 du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

4.3 Acceptation d'un certificat

Une fois le certificat Entrust.net pour serveurs Web SSL généré et archivé dans un répertoire Entrust.net, l'autorité d'enregistrement qui en a demandé l'émission prend des moyens commercialement raisonnables pour aviser le demandeur par courrier électronique que son certificat Entrust.net pour serveurs Web SSL est disponible. Le message par courrier électronique contient un URL au moyen duquel le demandeur peut récupérer le certificat Entrust.net pour serveurs Web SSL.

4.4 Suspension et révocation d'un certificat

Une autorité de certification Entrust.net pour serveurs Web SSL révoque un certificat Entrust.net pour serveurs Web SSL après avoir reçu une demande de révocation valide de la part d'une autorité d'enregistrement relevant de cette autorité de certification Entrust.net pour serveurs Web SSL. L'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL qui reçoit une demande de révocation valide de la part de l'abonné de son certificat Entrust.net pour serveurs Web SSL est habilitée à demander et peut demander à l'autorité de certification dont elle relève de révoquer le certificat Entrust.net pour serveurs Web SSL en question. L'autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL qui apprend l'existence d'un événement nécessitant qu'un abonné cesse d'utiliser son certificat Entrust.net pour serveurs Web SSL est habilitée à demander et demande à l'autorité de certification Entrust.net pour serveurs Web SSL dont elle relève de révoquer le certificat Entrust.net pour serveurs Web SSL en question. Les autorités de certification Entrust.net pour serveurs Web SSL ne permettent pas la suspension de certificats Entrust.net pour serveurs Web SSL.

4.4.1 Circonstances donnant lieu à une révocation

Une autorité de certification Entrust.net pour serveurs Web SSL est habilitée à révoquer et peut révoquer le certificat Entrust.net pour serveurs Web SSL d'un abonné, et une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL est habilitée à en demander la révocation et en demande la révocation si cette autorité de certification Entrust.net pour serveurs Web SSL ou cette autorité d'enregistrement sait ou a des motifs raisonnables de croire que l'un ou l'autre des événements suivants s'est produit :

- (i) la clé privée de cette autorité de certification Entrust.net pour serveurs Web SSL ou la clé privée d'une autorité de certification supérieure a été compromise;

- (ii) l'abonné a manqué à l'une ou l'autre des modalités de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ou de l'entente d'abonnement qu'il a conclue;
- (iii) les renseignements contenus dans un certificat Entrust.net pour serveurs Web SSL émis à un abonné ont changé;
- (v) les frais d'un certificat Entrust.net pour serveurs Web SSL ou les frais de services n'ont pas été acquittés;
- (vi) il a été déterminé qu'un certificat Entrust.net pour serveurs Web SSL n'a pas été émis conformément aux exigences prévues dans l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL ou dans l'entente d'abonnement conclue par l'abonné;
- (vi) il existe d'autres raisons raisonnablement susceptibles de compromettre l'intégrité, la sécurité ou la fiabilité d'un certificat Entrust.net pour serveurs Web SSL ou d'une autorité de certification Entrust.net pour serveurs Web SSL.

L'abonné demande la révocation de son certificat Entrust.net pour serveurs Web SSL s'il soupçonne ou sait que sa clé privée est compromise ou qu'il y a eu changement des renseignements contenus dans son certificat Entrust.net pour serveurs Web SSL ou changement des circonstances qui rend inexacts, incomplets ou trompeurs les renseignements contenus dans son certificat Entrust.net pour serveurs Web SSL. Cette demande de révocation est soumise par l'abonné à l'autorité d'enregistrement qui a traité sa demande de certificat Entrust.net pour serveurs Web SSL. Si le certificat Entrust.net pour serveurs Web SSL d'un abonné est révoqué pour quelque motif que ce soit, l'autorité d'enregistrement qui a traité la demande de certificat Entrust.net pour serveurs Web SSL de l'abonné prend des moyens commercialement raisonnables pour aviser l'abonné concerné par courrier électronique adressé aux personnes-ressources en matière technique et de sécurité dont les noms figurent dans la demande de certificat Entrust.net pour serveurs Web SSL. La révocation d'un certificat Entrust.net pour serveurs Web SSL ne change rien aux obligations contractuelles de l'abonné aux termes du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, de l'entente d'abonnement qu'il a conclue et de tout contrat avec une partie utilisatrice.

4.4.2 Auteur de la demande de révocation

L'abonné peut demander la révocation de son certificat Entrust.net pour serveurs Web SSL en tout temps pour n'importe quelle raison. S'il demande la révocation de son certificat Entrust.net pour serveurs Web SSL, l'abonné doit pouvoir prouver son identité, ainsi qu'il est prévu à l'article 3.4, à l'autorité d'enregistrement qui a traité sa demande de certificat Entrust.net pour serveurs Web SSL. Les autorités de certification Entrust.net pour serveurs Web SSL ne sont tenues de révoquer un certificat Entrust.net pour serveurs Web SSL et les autorités d'enregistrement relevant des autorités de certification Entrust.net pour serveurs Web SSL ne sont tenues d'en demander la révocation que si un abonné peut prouver son identité de façon satisfaisante ainsi qu'il est prévu aux articles 3.4 et 4.4.3. Une autorité de certification Entrust.net pour serveurs Web SSL est habilitée à révoquer et révoque le certificat Entrust.net pour serveurs Web SSL d'un abonné, et une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL a le droit d'en demander la révocation et en demande la révocation en tout temps, pour l'une ou l'autre des raisons énumérées à l'article 4.4.1.

4.4.3 Procédure de demande de révocation

Une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL authentifie la demande de révocation de certificat Entrust.net SSL Web Server d'un abonné en demandant à l'abonné de fournir (i) une partie des renseignements qu'il a fournis dans sa demande de certificat Entrust.net pour serveurs Web SSL, ou (ii) la phrase de passe qu'il a soumise avec sa demande de certificat Entrust.net pour serveurs Web SSL, ou en exigeant une vérification par une personne-ressource de l'abonné. Sur réception et confirmation de ces renseignements, l'autorité d'enregistrement envoie une demande de révocation à l'autorité de certification Entrust.net pour serveurs Web SSL qui a émis le certificat Entrust.net pour serveurs Web SSL en question. L'autorité de certification Entrust.net pour serveurs Web SSL qui reçoit la demande de révocation doit, dans un délai de quarante-huit (48) heures suivant la réception de la demande, inscrire le numéro de série du certificat Entrust.net pour serveurs Web SSL révoqué à la LCR d'un répertoire Entrust.net. Si le certificat Entrust.net pour serveurs Web SSL d'un abonné est révoqué pour

quelque raison que ce soit, l'autorité d'enregistrement qui a demandé la révocation du certificat Entrust.net pour serveurs Web SSL de l'abonné prend des moyens commercialement raisonnables pour en aviser ce dernier par courrier électronique adressé aux personnes-ressources en matière technique et de sécurité dont les noms figurent dans la demande de certificat Entrust.net SSL Web de l'abonné.

4.4.4 Délai de grâce

Immédiatement après avoir découvert l'existence d'une compromission réelle ou soupçonnée d'une clé privée, l'abonné demande la révocation du certificat Entrust.net pour serveurs Web SSL correspondant. Les demandes de révocation pour autres motifs requis sont présentées dès la première occasion raisonnable.

4.4.5 Circonstances donnant lieu à une suspension

Les autorités de certification Entrust.net pour serveurs Web SSL ne suspendent pas les certificats Entrust.net pour serveurs Web SSL.

4.4.6 Auteur de la demande de suspension

Les autorités de certification Entrust.net pour serveurs Web SSL ne suspendent pas les certificats Entrust.net pour serveurs Web SSL.

4.4.7 Procédure de demande de suspension

Les autorités de certification Entrust.net pour serveurs Web SSL ne suspendent pas les certificats Entrust.net pour serveurs Web SSL.

4.4.8 Limites relatives à la période de suspension

Les autorités de certification Entrust.net pour serveurs Web SSL ne suspendent pas les certificats Entrust.net pour serveurs Web SSL.

4.4.9 Fréquence de la publication d'une LCR

Les autorités de certification Entrust.net pour serveurs Web SSL prennent des moyens commercialement raisonnables pour publier une LCR au moins toutes les vingt-quatre (24) heures. La LCR est généralement publiée autour de minuit. Dans certaines circonstances, elle peut aussi être publiée dans l'intervalle, comme lorsqu'il y a détection d'une grave compromission.

4.4.10 Obligation de vérifier la LCR

La partie utilisatrice doit vérifier si le certificat Entrust.net pour serveurs Web SSL auquel elle entend se fier a été révoqué. Elle doit vérifier les listes de certificats révoqués qui se trouvent dans le répertoire pertinent pour déterminer si le certificat Entrust.net SSL Web Server auquel elle entend se fier a été révoqué. Entrust.net, les tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, les revendeurs et covendeurs, les sous-entrepreneurs, distributeurs, mandataires et fournisseurs et leurs employés et administrateurs ne peuvent en aucun cas être tenus responsables des dommages, de quelque nature qu'ils soient, causés par (i) l'omission d'une partie utilisatrice de vérifier si un certificat Entrust.net pour serveurs Web SSL a été révoqué ou est expiré, ou (ii) le fait pour une partie utilisatrice de se fier à un certificat Entrust.net pour serveurs Web SSL qui a été révoqué ou qui est expiré.

4.4.11 Révocation en ligne/Disponibilité du service de vérification de l'état

Les LCR qui se trouvent dans un répertoire Entrust.net peuvent être recherchées par numéro de série.

4.4.12 Obligation de vérifier les révocations en ligne

Voir l'article 4.4.10.

4.4.13 Autres formes disponibles de publicité des révocations

Aucun autre moyen n'est prévu.

4.4.14 Obligation de vérification relative à d'autres formes de publicité des révocations

Aucune disposition.

4.4.15 Obligations spéciales relatives à la compromission d'une clé

S'il soupçonne ou sait que la clé privée correspondant à la clé publique contenue dans son certificat Entrust.net pour serveurs Web SSL a été compromise, l'abonné avise immédiatement l'autorité d'enregistrement qui a traité sa demande de certificat Entrust.net pour serveurs Web SSL de la compromission réelle ou soupçonnée en suivant les procédures énoncées à l'article 4.4.3. L'abonné cesse immédiatement d'utiliser ce certificat Entrust.net pour serveurs Web SSL et le retire de tout support ou logiciel sur lequel il l'a installé. L'abonné doit vérifier les circonstances entourant la compromission réelle ou soupçonnée et aviser les parties utilisatrices qui ont pu être touchées par la compromission réelle ou soupçonnée.

4.5 Procédures d'audit de sécurité

Les événements importants en matière de sécurité dans les systèmes des autorités de certification Entrust.net pour serveurs Web SSL sont automatiquement horodatés et enregistrés sous forme de journaux d'audit dans les fichiers de la piste d'audit. Les fichiers de la piste d'audit sont traités (examinés pour déterminer s'il y a eu violation des politiques ou autres événements importants) régulièrement. Des codes d'authentification sont utilisés en conjonction avec les fichiers de la piste d'audit pour prévenir la modification des journaux d'audit. Les fichiers de la piste d'audit sont archivés périodiquement. Tous les fichiers, y compris le fichier de la piste d'audit le plus récent, sont déplacés sur des supports de sauvegarde et conservés dans une installation d'archivage sûre.

4.6 Archivage des dossiers

Les fichiers de la piste d'audit et les bases de données pour les autorités de certification Entrust.net pour serveurs Web SSL sont tous archivés. Les archives de la base de données d'une autorité de certification Entrust.net pour serveurs Web SSL sont conservées pendant au moins trois (3) ans. Les archives des fichiers de la piste d'audit sont conservés pendant au moins un (1) an. Les bases de données des autorités de certification Entrust.net pour serveurs Web SSL sont chiffrées et protégées par les clés maîtresses logicielles d'Entrust. Le support d'archivage est protégé en étant conservé dans une installation à accès restreint à laquelle seul le personnel autorisé d'Entrust.net a accès. Les fichiers d'archivage sont sauvegardés à mesure qu'ils sont créés. Les originaux sont conservés sur place et hébergés avec un système d'autorité de certification Entrust.net pour serveurs Web SSL. Les fichiers de sauvegarde sont conservés dans un endroit sûr et géographiquement distinct.

4.7 Changement des clés

Les abonnés reçoivent des certificats Entrust.net pour serveurs Web SSL qui expirent après une période déterminée pour réduire au minimum l'exposition de la bicyclée associée. Pour cette raison, une nouvelle bicyclée doit être créée et cette nouvelle clé publique doit être soumise avec chaque commande d'un certificat Entrust.net pour serveurs Web SSL pour remplacer un certificat Entrust.net pour serveurs Web SSL sur le point d'expirer. Le processus de renouvellement d'un certificat Entrust.net pour serveurs Web SSL est décrit à l'article 3.2.

4.8 Reprise en cas de compromission et de sinistre

Les autorités de certification Entrust.net pour serveurs Web SSL ont un plan de reprise en cas de sinistre qui permet la reprise rapide des services s'il y a panne de système.

Entrust.net requiert des contrôles de sécurité rigoureux pour maintenir l'intégrité des autorités de certification Entrust.net pour serveurs Web SSL. Entrust.net estime peu probable la compromission de la

clé privée utilisée par une autorité de certification Entrust.net pour serveurs Web SSL. Cependant, Entrust.net dispose de politiques et de procédures qui seront utilisées en cas d'une telle compromission. À tout le moins, tous les abonnés sont informés dès que possible d'une telle compromission, et les renseignements pertinents sont affichés dans le répertoire Entrust.net.

4.9 Cessation des activités des AC

Si une autorité de certification Entrust.net pour serveurs Web SSL met fin à ses activités, tous les certificats Entrust.net pour serveurs Web SSL qu'elle a émis sont révoqués.

5 Contrôles de sécurité des lieux, des procédures administratives et du personnel

5.1 Contrôles de sécurité des lieux

Le logiciel Entrust/Authority(mc) est utilisé comme composante logicielle des autorités de certification Entrust.net pour serveurs Web SSL. Le matériel informatique et le logiciel d'une autorité de certification Entrust.net pour serveurs Web SSL est situé dans un endroit sûr dont les procédures de contrôle de sécurité et d'accès répondent aux normes de l'industrie en la matière ou excèdent celles-ci. La pièce qui contient le logiciel Entrust/Authority est désignée comme une zone à deux (2) personnes, et des contrôles sont exercés pour prévenir qu'une personne entre dans la pièce seule. Des systèmes d'alarme sont utilisés pour aviser le personnel de sécurité de toute violation des règles d'accès à une autorité de certification Entrust.net pour serveurs Web SSL.

5.2 Contrôles de sécurité des procédures administratives

Une autorité de certification Entrust.net pour serveurs Web SSL assume un certain nombre de rôles jugés fiables aux fins d'opérations de nature délicate de ses logiciels. Pour obtenir accès à un logiciel Entrust/Authority utilisé par une autorité de certification Entrust.net pour serveurs Web SSL, le personnel opérationnel doit se soumettre à des vérifications des antécédents. Les opérations de l'autorité de certification Entrust.net pour serveurs Web SSL relatives à l'ajout d'un personnel administratif ou au changement des paramètres de la politique des autorités de certification nécessitent plus d'une (1) personne.

5.3 Contrôles de sécurité du personnel

Le personnel opérationnel affecté à une autorité de certification Entrust.net pour serveurs Web SSL ne se verra confier aucune responsabilité qui entre en conflit avec les responsabilités opérationnelles qu'il assume pour l'autorité de certification Entrust.net pour serveurs Web SSL. Les privilèges attribués au personnel opérationnel affecté à une autorité de certification Entrust.net pour serveurs Web SSL sont limités au minimum nécessaire pour permettre à celui-ci d'exécuter ses fonctions.

6 Contrôles de sécurité technique

6.1 Génération et installation de la biclé

6.1.1 Génération de la biclé

La biclé de signature d'une autorité de certification Entrust.net pour serveurs Web SSL est créée au cours du démarrage initial de l'application Entrust/Master Control et protégée par la clé maîtresse de cette autorité de certification Entrust.net pour serveurs Web SSL. On a recours à des dispositifs matériels pour générer des clés, ce qui est conforme au moins au niveau 3 de la norme FIPS 140-1.

6.1.2 Livraison de la clé privée à une entité

Non pertinent.

6.1.3 Livraison de la clé publique à l'émetteur de certificats

La clé publique contenue dans un certificat Entrust.net pour serveurs Web SSL est livrée aux autorités de certification Entrust.net pour serveurs Web SSL dans une demande de signature de certificat (DSC) dans le cadre du processus de demande de certificat Entrust.net pour serveurs Web SSL.

6.1.4 Livraison de la clé publique des AC aux utilisateurs

Le certificat de clé publique des autorités de certification Entrust.net pour serveurs Web SSL est cocertifié par l'autorité de certification GTE Corporation («GTE»). Le certificat de clé publique autosigné pour l'autorité de certification GTE est installé à l'avance dans un navigateur et logiciel de serveur Web communs par les fabricants de logiciels concernés.

6.1.5 Taille des clés

La taille des clés pour serveurs Web est déterminée par le logiciel de serveur Web de l'abonné.

6.1.6 Génération des paramètres de la clé publique

Le logiciel du serveur Web de l'abonné permet de déterminer quels paramètres de la clé publique sont utilisés.

6.1.7 Vérification de la qualité des paramètres

La qualité des paramètres de la clé publique est réglée par le logiciel du serveur Web de l'abonné qui génère les paramètres. Ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, ni les revendeurs et covendeurs, ni les sous-entrepreneurs, distributeurs, mandataires et fournisseurs, ni leurs employés et administrateurs ne font de déclaration, n'offrent de garantie, ne formulent de condition de quelque nature que ce soit relativement à la qualité de la clé publique contenue dans un certificat Entrust.net pour serveurs Web SSL.

6.1.8 Génération des clés par matériel et/ou logiciel

La méthode de génération de la biclé de l'abonné associée à un certificat Entrust.net pour serveurs Web SSL relève exclusivement de l'abonné, et ni Entrust.net, ni les tierces autorités d'enregistrement indépendantes relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, ni les revendeurs et covendeurs, ni les sous-entrepreneurs, distributeurs, mandataires et fournisseurs, ni leurs employés et administrateurs n'assument de responsabilité de quelque nature que ce soit pour ce qui est de la génération de la biclé de l'abonné.

6.1.9 Objets de l'utilisation des clés

Les certificats Entrust.net pour serveurs Web SSL émis par une autorité de certification Entrust.net pour serveurs Web SSL contiennent les champs additionnels keyUsage et extendkeyUsage limitant l'objet pour lequel un certificat Entrust.net pour serveurs Web SSL peut être utilisé. Les abonnés et les parties

utilisatrices n'utilisent des certificats Entrust.net pour serveurs Web SSL que conformément au présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et aux lois applicables.

6.2 Protection des clés privées

Les autorités de certification Entrust.net pour serveurs Web SSL utilisent le logiciel Authority/Entrust en conjonction avec du matériel informatique homologué selon le niveau 3 de la norme FIPS 140-1 pour protéger les clés privées des autorités de certification Entrust.net pour serveurs Web SSL. L'abonné assume la responsabilité de protéger la clé privée associée à la clé publique contenue dans son certificat Entrust.net pour serveurs Web SSL. Entrust.net n'entierce pas les clés privées des autorités de certification Entrust.net pour serveurs Web SSL.

6.3 Autres aspects de la gestion des bclés

Aucune disposition.

6.4 Données d'activation

Aucune disposition.

6.5 Contrôles de sécurité des ordinateurs

Les postes de travail sur lesquels les autorités de certification Entrust.net pour serveurs Web SSL sont utilisés sont visés par des mesures de protection des lieux, ainsi qu'il est décrit l'article 5.1 du présent énoncé de pratiques de certification pour serveurs Web SSL. Les systèmes d'exploitation installés sur les postes de travail sur lesquels les autorités de certification Entrust.net pour serveurs Web SSL sont utilisés exigent l'identification et l'authentification des utilisateurs. L'accès aux données de bases du logiciel Entrust/Authority et aux pistes d'audit est restreint conformément au présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL. Le personnel opérationnel ayant accès aux autorités de certification Entrust.net pour serveurs Web SSL est tenu d'utiliser des jetons matériels en conjonction avec un NIP pour obtenir accès à la pièce qui contient le logiciel Entrust/Authority utilisé aux fins de ces autorités de certification Entrust.net pour serveurs Web SSL.

6.6 Contrôles techniques du cycle de vie

L'efficacité et la justesse des paramètres de sécurité décrits dans le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL sont passées en revue une fois l'an. Une évaluation du risque et de la menace sera effectuée pour déterminer si la longueur des clés doit être accrue ou les procédures opérationnelles modifiées à l'occasion afin de maintenir la sécurité du système.

6.7 Contrôles de sécurité réseau

Le logiciel Entrust/Authority, accessible à distance par l'intermédiaire d'Entrust/Admin, est protégé à l'aide des fonctionnalités de sécurité offerts par le protocole SEP (Secure Exchange Protocol) et le logiciel Entrust/Session.

6.8 Contrôles d'ingénierie du module cryptographique

Le module cryptographique du logiciel Entrust/Authority est conçu pour satisfaire aux exigences du niveau 1 de la norme FIPS 140-1. Des jetons matériels optionnels peuvent être utilisés pour générer des bclés qui peuvent répondre à des niveaux supérieurs d'homologation FIPS, mais qui doivent répondre au moins au niveau 1.

7 Profils du certificat et de la LCR

7.1 Profil du certificat

Le profil des certificats Entrust.net pour serveurs Web SSL délivrés par une autorité de certification Entrust.net pour serveurs Web SSL répond aux spécifications du protocole Secure Sockets Layer.

7.2 Profil de la LCR

Les champs suivants du format des listes de certificats révoqués (LCR), selon la définition qui en est donnée dans la norme X.509 version 2, sont utilisés par les autorités de certification Entrust.net pour serveurs Web SSL :

- version: indiquer la valeur v2
- signature : identificateur de l'algorithme utilisé pour signer la LCR
- émetteur du certificat : le nom distinctif complet de l'autorité de certification publiant la LCR
- présente mise à jour : heure de la publication de la LCR
- prochaine mise à jour : heure de la prochaine mise à jour prévue de la LCR
- certificats révoqués : information sur la liste des certificats révoqués

8 Administration

8.1 Renseignements

Directeur des opérations, Entrust.net Inc.
Entrust.net Inc.
1000, promenade Innovation
Ottawa (Ontario)
K2K 3E7

Téléphone : (613) 270-3157
Adresse électronique : entrust.OA@entrust.net

8.2 Procédures de modification

Entrust.net peut, à sa discrétion, modifier à l'occasion l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et ses modalités. Les modifications de l'énoncé de pratique de certification Entrust.net pour serveurs Web SSL qui, de l'avis de Entrust.net, auront peu de conséquence, sinon aucune, pour les demandeurs, les abonnés ou les parties utilisatrices, peuvent être effectuées sans que soit changé le numéro de version de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et sans qu'un avis soit donné aux demandeurs, aux abonnés et aux parties utilisatrices. Ces modifications entrent en vigueur dès leur publication dans le répertoire Entrust.net.

Les modifications de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL qui, de l'avis de Entrust.net, sont susceptibles d'avoir des conséquences importantes pour les demandeurs, les abonnés et les parties utilisatrices, sont publiées dans le répertoire Entrust.net et entrent en vigueur quinze (15) jours après leur publication à moins qu'Entrust.net retire l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL avant cette date d'entrée en vigueur. Si Entrust.net effectue une modification importante de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL, le numéro de version de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL est mis à jour en conséquence. L'abonné est réputé avoir consenti aux modalités de la version mise à jour de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et il est lié par ces modalités, sauf s'il cesse d'utiliser son ou ses certificats Entrust.net pour serveurs Web SSL, le ou les retire et en demande la révocation avant la date à laquelle la version mise à jour de l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL entre en vigueur.

8.3 Politiques en matière de publication et d'avis

Toute modification importante du présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL est précédée d'un avis de la modification projetée dans le répertoire Entrust.net.

8.4 Approbation de l'ÉPC

Le présent énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et les changements subséquents sont approuvés par l'autorité de politiques d'Entrust.net.

9 Acronymes

AC	Autorité de certification
AE	Autorité d'enregistrement
AO	Autorité opérationnelle
AP	Autorité (responsable) des politiques
DN	Nom distinctif
DNS	Serveur de noms de domaine
DSA	Digital Signature Algorithm
DSC	Demande de signature de certificat
ÉPC	Énoncé de pratiques de certification
HTTP	Protocole de transfert hypertexte
ICP	Infrastructure à clé publique
IETF	Internet Engineering Task Force
ITU-T	Union internationale des télécommunications - Secteur de la normalisation des télécommunications
LCR	Liste de certificats révoqués
MAC	Code d'authentification des messages
NIP	Numéro d'identification personnel
OID	Identificateur d'objet
RDN	Nom distinctif relatif
RFC	Request for Comment
SEP	Secure Exchange Protocol
SSL	Secure Sockets Layer
URL	Universal Resource Locator

10 Définitions

Abonné : Personne, entité ou organisation ayant fait la demande d'un certificat Entrust.net pour serveurs Web SSL et à qui un certificat a été émis.

AR : Voir Autorité d'enregistrement.

Autorité d'enregistrement : Entité exécutant les deux fonctions suivantes : (1) elle accuse réception des renseignements fournis par le sujet qui sera nommé dans un certificat, et (2) effectue une vérification limitée des renseignements fournis par le sujet en regard des renseignements disponibles dans les bases de données de certains tiers. Si les renseignements fournis par un sujet correspondent aux renseignements contenus dans les bases de données de ces tiers, une autorité d'enregistrement peut demander à une autorité de certification de générer, de signer numériquement et d'émettre un certificat contenant les renseignements vérifiés par l'autorité d'enregistrement.

Autorité de certification : Entité ou organisation qui (i) crée et signe numériquement des certificats contenant notamment une clé publique du sujet et d'autres renseignements destinés à identifier le sujet, (ii) donne accès à des certificats afin de faciliter les communications avec le sujet identifié dans le certificat et (iii) crée et signe numériquement les listes de certificats révoqués contenant des renseignements sur les certificats qui ont été révoqués et qui ne doivent plus être utilisés.

Autorité de certification Entrust.net pour serveurs Web SSL : Autorité de certification exploitée par Entrust.net ou pour le compte de celle-ci aux fins d'émettre, d'administrer, de révoquer et de renouveler des certificats Entrust.net pour serveurs Web SSL et de donner accès à ceux-ci.

Autorité des politiques d'Entrust.net : Désigne le personnel qui travaille pour Entrust.net ou pour le compte de celle-ci et qui établit les politiques et les procédures qui règlent l'utilisation des autorités de certification Entrust.net pour serveurs Web SSL.

Autorité opérationnelle d'Entrust.net : Désigne le personnel qui travaille pour Entrust.net ou pour le compte de celle-ci et qui est responsable de l'utilisation des autorités de certification Entrust.net pour serveurs Web SSL.

Biclé Deux clés cryptographiques mathématiquement liées ayant pour caractéristiques (i) qu'une clé peut être utilisée pour chiffrer un message qui ne peut être déchiffré qu'au moyen de l'autre clé, et (ii) que, même connaissant une clé, il est impossible de découvrir l'autre clé par calcul.

Certificat cocertifié désigne un certificat qui (i) inclut la clé publique d'une paire de clé publique-clé privée générée par ou pour l'Autorité de Certification Entrust.net, (ii) inclut la signature digitale d'une Autorité de Certification gérée par GTE Corporation ("GTE") ou ses successeurs, (iii) autorise la vérification de la clé publique d'un certificat de serveur SSL d'un abonné par l'usage de la clé publique du certificat GTE, et (iv) a une date d'expiration le ou avant le 23 février 2006.

Certificat : Document numérique qui, à tout le moins : a) identifie l'autorité de certification émettrice, b) nomme un sujet ou le désigne par ailleurs, c) contient une clé publique d'une biclé, d) fixe la période de validité du certificat et e) contient un numéro de série et porte la signature numérique d'une autorité de certification.

Certificat Entrust.net pour serveurs Web SSL : Certificat SSL émis par une autorité de certification Entrust.net pour serveurs Web SSL aux fins de son utilisation sur des serveurs pour le Web.

Clé privée : Clé d'une biclé utilisée pour déchiffrer un message chiffré. Cette clé doit être gardée secrète.

Clé publique : Clé d'une biclé utilisée pour chiffrer un message. La clé publique peut être librement accessible à quiconque souhaite adresser un message chiffré au titulaire de la clé privée de la biclé. La clé publique est normalement disponible dans un certificat émis par une autorité de certification et est souvent obtenue en accédant à un répertoire ou à une base de données. La clé publique est utilisée pour chiffrer un message qui ne peut être déchiffré que par le titulaire de la clé privée correspondante.

Compromission : Perte, divulgation ou perte de contrôle réelle ou soupçonnée de données ou de renseignements de nature délicate.

Contrat avec une partie utilisatrice : Contrat conclu entre une partie utilisatrice et Entrust.net ou entre une partie utilisatrice et une tierce autorité d'enregistrement indépendante ou un revendeur relevant d'une autorité de certification Entrust.net pour serveurs Web SSL portant sur la communication et l'utilisation de certains renseignements et sur la prestation de certains services relativement aux certificats Entrust.net pour serveurs Web SSL.

Covendeur : Toute personne, entité ou organisation à qui Entrust.net ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL a accordé le droit de faire la promotion des certificats Entrust.net pour serveurs Web SSL.

Demande de certificat Entrust.net pour serveurs Web SSL : Formulaire et renseignements requis par une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL et fournis par un demandeur lorsqu'il demande l'émission d'un certificat Entrust.net pour serveurs Web SSL.

Demandeur : Personne, entité ou organisation qui fait la demande d'un certificat Entrust.net pour serveurs Web SSL, mais à qui il n'a encore été émis aucun certificat, personne, entité ou organisation qui détient à l'heure actuelle un ou plusieurs certificats Entrust.net pour serveurs Web SSL et qui demande le renouvellement de ce ou ces certificats ou l'émission d'un ou de plusieurs certificats Entrust.net pour serveurs Web SSL additionnels.

Énoncé de pratiques de certification : Énoncé des pratiques auxquelles se conforme l'autorité de certification aux fins d'émettre, d'administrer, de révoquer et de renouveler des certificats et de donner accès à ceux-ci, et modalités aux termes desquelles l'autorité de certification offre ces services.

Énoncé de pratiques de certification Entrust.net pour serveurs Web SSL : Le présent document.

Entente d'abonnement : Entente conclue entre un abonné et Entrust.net ou entre un abonné et une tierce autorité d'enregistrement indépendante ou un revendeur relevant d'une autorité de certification Entrust.net pour serveurs Web SSL concernant d'une part l'émission et l'administration d'un certificat Entrust.net pour serveurs Web SSL et le fait de rendre celui-ci accessible, et d'autre part la prestation d'autres services relativement à ce certificat.

Entrust.net: Entrust.net Inc.

ÉPC : Voir Énoncé de pratiques de certification.

ÉPC Entrust.net pour serveurs Web SSL : Voir Énoncé de pratiques de certification Entrust.net pour serveurs Web SSL.

FIPS: Federal Information Processing Standards. Il s'agit de normes gouvernementales américaines qui prescrivent les exigences relatives au rendement, les méthodes, les formats, les protocoles de communication et autres exigences aux fins de l'utilisation de matériel informatique, de logiciels, de données et de télécommunications.

Identificateur d'objet : Suite formatée de nombres enregistrée conformément à des procédures d'enregistrement d'identificateur d'objet reconnues au niveau international.

IETF: Internet Engineering Task Force. Communauté internationale de concepteurs, d'exploitants et de vendeurs de réseaux et de chercheurs qui s'intéressent à l'architecture Internet et à l'exploitation efficace de l'Internet.

IO: Voir Identificateur d'objet.

Jour ouvrable : Tous les jours de la semaine sauf le samedi, le dimanche et les jours fériés, y compris les jours fériés dans la municipalité d'Ottawa (Ontario).

LCR : Voir Liste de certificats révoqués.

Liste de certificats révoqués : Liste horodatée des numéros de série des certificats révoqués portant la signature numérique d'une autorité de certification.

Partie utilisatrice : Personne, entité ou organisation qui utilise un certificat Entrust.net pour serveurs Web SSL ou tout renseignement fourni dans un Répertoire relevant d'une autorité de certification Entrust.net pour serveurs Web SSL, ou s'y fie, pour obtenir et confirmer la clé publique et l'identité d'un abonné.

Période opérationnelle : Période de validité d'un certificat. La période opérationnelle commence habituellement le jour de l'émission du certificat (ou à toute autre date ultérieure précisée dans le certificat) et se termine le jour et l'heure de son expiration prévue dans le certificat ou avant si le certificat est révoqué.

PKIX : Groupe de travail de la IETF élaborant des spécifications techniques des composantes des ICP basées sur les certificats conformes à la norme X.509 Version 3.

Répertoire : Collection de bases de données et de sites web contenant des renseignements sur les certificats émis par une autorité de certification, y compris notamment sur les types de certificats et de services fournis par l'autorité de certification et les frais facturés pour les certificats et pour les services fournis par l'autorité de certification, des listes de certificats révoqués, la description des pratiques et procédures de l'autorité de certification et autres renseignements et ententes portant sur l'utilisation des certificats émis par l'autorité de certification.

Répertoire Entrust.net : Collection de bases de données et de sites web contenant des renseignements sur les certificats Entrust.net pour serveurs Web SSL et les services fournis par Entrust.net relativement à des certificats Entrust.net pour serveurs Web SSL, y compris notamment sur les types de certificats Entrust.net pour serveurs Web SSL émis par les autorités de certification Entrust.net pour serveurs Web SSL, les services fournis par Entrust.net relativement aux certificats Entrust.net pour serveurs Web SSL et les frais facturés par Entrust.net pour les certificats Entrust.net pour serveurs Web SSL et pour les services fournis par Entrust.net relativement à ceux-ci, des listes de certificats révoqués, l'énoncé de pratiques de certification Entrust.net pour serveurs Web SSL et d'autres renseignements et ententes portant sur l'utilisation des certificats Entrust.net pour serveurs Web SSL.

Revendeur : Toute personne, entité ou organisation à qui Entrust.net ou une autorité d'enregistrement relevant d'une autorité de certification Entrust.net pour serveurs Web SSL a accordé le droit d'utiliser les certificats Entrust.net pour serveurs Web SSL.

Révoquer ou révocation : Mettre fin prématurément à la période opérationnelle d'un certificat à compter d'une date donnée.

Société liée : Entrust et toute société ou autre entité que Entrust contrôle directement ou indirectement. Dans le présent contexte, une partie contrôle une société ou autre entité si elle détient ou contrôle directement ou indirectement cinquante pour cent (50 %) ou plus des droits de vote aux fins du conseil d'administration ou de tout autre mécanisme de contrôle.

Sujet : Personne, entité ou organisation dont la clé publique est contenue dans un certificat.