



**Bell Canada**

# **Politique de certification**

## **AC de base de Bell**

**Date:** Le 25 janvier 2008

**Approuvé par :**

**Version:** 1.0

## HISTORIQUE DE Révision

Version	Description	Date émis	Date approuvé
1.0	Version finale 1.0	25 janvier 2008	

## TABLE DES MATIÈRES

1.	Introduction.....	6
1.1.	Aperçu .....	6
1.2.	Nom et identification du document.....	6
1.3.	Participants à l'ICP .....	6
1.4.	Utilisation des certificats .....	7
1.5.	Administration de la politique.....	7
1.6.	Définitions et sigles.....	7
2.	Responsabilités concernant la publication et les référentiels.....	10
3.	Identification et authentification.....	11
3.1.	Nom.....	11
3.2.	Validation initiale de l'identité.....	11
3.3.	Identification et authentification des demandes de renouvellement de clés .....	11
3.4.	Identification et authentification des demandes de révocation.....	11
4.	Exigences opérationnelles du cycle de vie des certificats.....	12
4.1.	Demande de certificat .....	12
4.2.	Traitement des demandes de certificat .....	12
4.3.	Délivrance des certificats .....	12
4.4.	Acceptation d'un certificat.....	12
4.5.	Utilisation des paires de clés et des certificats .....	12
4.6.	Renouvellement d'un certificat .....	12
4.7.	Renouvellement des clés de certificats.....	12
4.8.	Modification d'un certificat .....	13
4.9.	Révocation ou suspension d'un certificat.....	13
4.10.	Services d'état des certificats .....	13
4.11.	Fin de l'abonnement.....	13
4.12.	Séquestre et récupération des clés .....	13
5.	Installations, gestion et contrôle opérationnels .....	14
5.1.	Contrôles physiques.....	14
5.1.1	Emplacement et construction des installations .....	14
5.1.2	Accès physique .....	14
5.1.3	Alimentation électrique et climatisation.....	14
5.1.4	Exposition à l'eau.....	14
5.1.5	Prévention et protection contre les incendies.....	14
5.1.6	Stockage des supports .....	14
5.1.7	Mise au rebut des déchets .....	15

5.1.8	Sauvegarde hors site.....	15
5.2.	Contrôles procéduraux.....	15
5.3.	Contrôles du personnel.....	15
5.4.	Procédures de journalisation à des fins de vérification .....	16
5.5.	Archivage des documents .....	16
5.6.	Renouvellement des clés .....	16
5.7.	Compromission et reprise après sinistre.....	16
5.8.	Cessation des activités de l'AC ou d'une AE.....	16
6.	Contrôles techniques de sécurité .....	17
6.1.	Production et installation des paires de clés.....	17
6.2.	Protection des clés privées et contrôles techniques des modules cryptographiques .....	17
6.3.	Autres aspects de la gestion des paires de clés.....	18
6.4.	Données d'activation.....	18
6.5.	Contrôle de la sécurité informatique.....	18
6.6.	Contrôle de sécurité du cycle de vie.....	18
6.7.	Contrôle de sécurité réseau.....	18
6.8.	Horodatage .....	18
7.	Profils des certificats, des LCR et OCSP.....	19
7.1.	Profil des certificats .....	19
7.2.	Profil des LCR.....	20
7.3.	Profil OCSP.....	20
8.	Vérification de conformité et autres évaluations.....	21
9.	Autres questions juridiques et de gestion .....	22
9.1.	Redevances.....	22
9.2.	Responsabilité financière .....	22
9.3.	Confidentialité des renseignements d'entreprise .....	22
9.4.	Confidentialité des renseignements personnels.....	22
9.5.	Droits de propriété intellectuelle .....	22
9.6.	Déclarations et garanties .....	22
9.7.	Exonération de garanties .....	24
9.8.	Limitations de la responsabilité.....	24
9.9.	Indemnités .....	26
9.10.	Période de validité et cessation des activités .....	26
9.11.	Avis individuels et communications avec les participants .....	26
9.12.	Modifications .....	26
9.13.	Dispositions concernant le règlement des différends.....	26
9.14.	Lois applicables .....	26
9.15.	Conformité aux lois applicables.....	27

9.16.	Accord intégral .....	27
9.17.	Cession.....	27
9.18.	Cas de force majeure .....	27

## 1. Introduction

### 1.1. Aperçu

Le présent document définit la politique de certification (PC) pour la signature numérique – assurance de niveau moyen (conformément aux normes du gouvernement canadien) – que doit utiliser l'autorité de certification (AC) de base de Bell. Le présent document est conforme à la partie IV (*Certificate Policy and Certification Practice Statement Framework*) de la norme *Public Key Infrastructure X.509*, élaborée par l'*Internet Engineering Task Force* (groupe de travail IETF PKIX).

La politique de certification définie dans le présent document est destinée à être utilisée par Bell Canada et ses filiales. Les utilisateurs de ce document doivent consulter l'AC émettrice afin d'obtenir plus de détails sur la mise en œuvre de cette politique.

La présente PC vise la gestion et l'utilisation des certificats contenant des clés publiques utilisées pour les mécanismes d'authentification. Plus particulièrement, les certificats délivrés en vertu de ces politiques serviront à vérifier l'identité des AC subordonnées chez Bell Canada.

L'abonné n'est pas autorisé à faire des transactions commerciales au nom de l'organisation qui exploite l'AC.

L'AC sera assujettie aux lois canadiennes et aux lois provinciales pertinentes touchant l'application, l'élaboration, l'interprétation et la validité de la présente politique de certification.

Toute exception à la présente PC doit être approuvée par écrit par le comité directeur ICP de Bell.

Bell Canada se réserve le droit de ne pas conclure d'entente de certification croisée (ou « cocertification ») avec une autorité de certification externe.

### 1.2. Nom et identification du document

bell-pki-certpcy-RootCA -digitalSignature ::= { joint-iso-itut-t (2) country (16) Canada (124) Bell (113565) pki (3) CertificatePolicy (1) Root CA (1) DigitalSignature (1) }

### 1.3. Participants à l'ICP

La présente politique reconnaît les participants suivants :

- l'autorité de certification (AC), qui signe et délivre les certificats;
- l'autorité d'enregistrement (AE), qui est responsable d'assurer la légitimité des demandes de certificats;
- les abonnés, qui seront des AC subordonnées;
- les parties utilisatrices, qui peuvent être des personnes physiques ou morales, chez Bell ou ailleurs, qui cherchent à vérifier l'authenticité d'une AC subordonnée.

#### 1.4. Utilisation des certificats

Les certificats délivrés par une AC exploitée en vertu de la présente politique ne doivent être utilisés que par les AC subordonnées. Les AC subordonnées ne peuvent utiliser les certificats qui leur sont délivrés par l'AC de base de Bell que pour signer les certificats qu'elles délivrent ou (après avoir obtenu l'approbation du comité directeur ICP de Bell) pour cocertifier une AC externe.

#### 1.5. Administration de la politique

L'organisation responsable de la rédaction, de l'enregistrement, de la tenue et de la mise à jour de la présente politique de certification est le comité directeur ICP de Bell, avec lequel on peut communiquer par courriel, à l'adresse [bellpki@bell.ca](mailto:bellpki@bell.ca).

#### 1.6. Définitions et sigles

Expression	Définition
Comité directeur ICP de Bell	Ensemble des procédés et des structures mises en œuvre par le conseil pour guider, diriger, gérer et surveiller les activités de l'organisation en vue d'atteindre ses objectifs.
Autorité de certification	Entité de confiance reconnue par un ou plusieurs utilisateurs pour la gestion et la délivrance des certificats de clé publique X.509 et des LRC.
Politique de certification	Politique administrative spécialisée visant les transactions électroniques effectuées dans le cadre de la gestion des certificats. La politique de certification aborde tous les aspects liés à la production, à la distribution, à la comptabilité, à l'exécution, à la récupération et à l'administration des certificats numériques. Indirectement, la politique de certification peut également régir les transactions effectuées à l'aide d'un système de communication protégé par un système de sécurité fondé sur les certificats. En contrôlant les extensions de certificats critiques, la politique de certification et les technologies d'application associées peuvent appuyer la prestation des services de sécurité exigés pour des applications particulières.
Liste des certificats révoqués	Liste émise et actualisée par l'autorité de certification et indiquant les certificats qu'elle a délivrés mais qui ont été révoqués avant leur délai prévu d'expiration.
Énoncé de pratiques de certification	Énoncé des pratiques qu'applique une autorité de certification pour délivrer, suspendre, révoquer et renouveler les certificats et y donner accès, d'une manière qui satisfait aux exigences contenues dans une politique de certification ou un contrat de services.
Nom distinctif	Ensemble de paires attributs-valeurs qui identifie de façon unique un objet dans un référentiel donné.
Module matériel autonome	Dispositif de matériel servant à générer et à stocker des clés cryptographiques d'une façon sécuritaire.

Norme de cryptographie à clé publique n° 10 (NCCP n° 10)	Format des messages envoyés à l'autorité de certification pour demander la certification d'une clé publique.
Infrastructure à clé publique	Ensemble de politiques, procédés, plateformes de serveurs et logiciels utilisés pour gérer des certificats et des paires de clés publique-privée, ainsi que pour délivrer, tenir à jour et révoquer des certificats de clé publique.
Infrastructure à clé publique X.509	Norme IETF ( <a href="#">RFC 3280</a> ) qui définit le format d'un certificat numérique.
Autorité d'enregistrement	Organisation responsable de l'identification et de l'authentification des détenteurs de certificat numérique, mais qui ne signe ni ne délivre de certificats. L'AC peut demander à l'AE d'exécuter certaines tâches.
Partie utilisatrice	Toute personne physique ou morale ou tout ordinateur qui juge fiable l'authenticité du lien entre la clé publique et le nom distinctif dans un certificat numérique.

<b>Sigle</b>	<b>Explication</b>
AC	Autorité de certification
PC	Politique de certification
EPC	Énoncé de pratiques de certification
LCR	Liste des certificats révoqués
ND	Nom distinctif
HSM	Module matériel autonome
IETF	<i>Internet Engineering Task Force</i> (groupe de travail IETF)
NCCP	Norme de cryptographie à clé publique
ICP	Infrastructure à clé publique
PKIX	Infrastructure à clé publique X.509
AE	Autorité d'enregistrement

RSA	Rivest-Shamir-Adleman
-----	-----------------------

## **2. Responsabilités concernant la publication et les référentiels**

L'AC émettrice assume des responsabilités liées à la publication des certificats qu'elle délivre. Elle doit :

- publier sa PC sur un site Web accessible à toutes les parties utilisatrices (la maintenance du site Web peut être assurée par l'AC ou une autre partie agissant en son nom, mais le choix du site Web doit être approuvé par le comité directeur ICP de Bell), lorsque le comité directeur ICP de Bell a approuvé la PC;
- inclure dans tout certificat qu'elle délivre l'adresse URL du site Web contenant la PC;
- s'assurer que le système d'exploitation et les contrôles d'accès au référentiel sont configurés de telle sorte que seul le personnel autorisé de l'AC peut écrire dans la version en ligne de la PC ou la modifier;
- fournir au besoin la version texte complète de l'EPC, aux fins de vérification, d'inspection, d'accréditation ou de certification croisée.

L'AC peut, à sa discrétion, mettre en place des mécanismes de contrôle de l'accès aux certificats ou à la vérification en ligne de l'état des certificats (si ce dernier service est fourni par l'AC). Il faut publier rapidement les certificats dès leur délivrance. L'AC doit garantir, directement ou au moyen d'une entente avec un référentiel, l'accès sans restriction aux LCR.

### **3. Identification et authentification**

#### **3.1. Nom**

Le certificat de signature de l'AC de base doit avoir comme nom distinctif (ND) « C=CA,O=Bell,OU= Bell Root CA ». Les certificats délivrés par l'AC de base de Bell doivent avoir un nom distinctif (ND) unique et clairement distinct dans le champ sujet du certificat, conformément à la partie I de la PKIX. Ce nom doit se présenter sous la forme d'une chaîne imprimable X.501 et ne doit pas être vide. Les noms distinctifs des certificats délivrés doivent avoir un lien avec le nom organisationnel de l'AC subordonnée et être approuvés par le comité directeur ICP de Bell avant la délivrance des certificats.

#### **3.2. Validation initiale de l'identité**

L'AC de base de Bell ne délivrera de certificat à une AC subordonnée qu'à la réception de l'autorisation appropriée du comité directeur ICP de Bell (voir la section 4.1). Le processus utilisé doit fournir une assurance de niveau élevé (et pas seulement une assurance de niveau moyen) à l'effet que l'AC subordonnée possède effectivement la clé privée correspondant à la clé publique faisant l'objet de la demande.

Le processus doit également fournir une assurance de niveau élevé à l'effet que le certificat que reçoit l'AC subordonnée a bel et bien été délivré par l'AC de base de Bell.

#### **3.3. Identification et authentification des demandes de renouvellement de clés**

L'AC de base de Bell ne traitera de demande de renouvellement de clé de certificat de signature d'une AC subordonnée qu'à la réception de l'autorisation appropriée du comité directeur ICP de Bell (voir la section 4.7). Le nouveau certificat doit fournir le même niveau élevé d'assurance quant à son authenticité que celui décrit à la section 3.2.

#### **3.4. Identification et authentification des demandes de révocation**

L'AC de base de Bell ne traitera de demande de révocation de certificat de signature d'une AC subordonnée qu'à la réception de l'autorisation appropriée du comité directeur ICP de Bell (voir la section 4.9). Le processus de révocation doit fournir le même niveau élevé d'assurance quant à l'authenticité du certificat que celui décrit à la section 3.2.

## **4. Exigences opérationnelles du cycle de vie des certificats**

### **4.1. Demande de certificat**

La demande pour faire signer un certificat de signature d'une AC subordonnée par l'AC de base de Bell doit être faite conformément aux procédés décrits dans la charte du comité directeur ICP de Bell. Tout directeur de niveau B de Bell (niveau chef) peut soumettre une demande de certification d'AC par l'AC de base de Bell.

### **4.2. Traitement des demandes de certificat**

Les demandes de certificats doivent être traitées conformément à la charte du comité directeur ICP de Bell.

### **4.3. Délivrance des certificats**

Le processus de délivrance de certificats de l'AC de base de Bell doit fournir le même niveau d'assurance élevé quant à l'authenticité des certificats que celui décrit à la section 3.2.

### **4.4. Acceptation d'un certificat**

L'AC subordonnée doit indiquer son intention de ne pas accepter un certificat qui lui a été délivré par l'AC de base de Bell dans un délai d'un (1) jour ouvrable. Si l'AC subordonnée n'indique pas son intention de ne pas accepter le certificat, l'AC subordonnée sera considérée avoir accepté le certificat.

Lorsqu'un certificat est accepté, l'AC de base de Bell doit veiller à la publication du certificat dans un référentiel accessible à toutes les parties utilisatrices.

### **4.5. Utilisation des paires de clés et des certificats**

Les AC subordonnées abonnés ne doivent utiliser les certificats délivrés par l'AC de base de Bell que pour signer les certificats qu'elles délivrent ou (après avoir obtenu l'approbation écrite du comité directeur ICP de Bell) pour cocertifier une AC externe. Les parties utilisatrices ne peuvent utiliser les certificats délivrés par l'AC de base de Bell que pour vérifier que les certificats qu'elles jugent fiables ont bel et bien été signés par l'AC subordonnée, tel que stipulé.

### **4.6. Renouvellement d'un certificat**

Les demandes de renouvellement de certificats doivent être adressées au comité directeur ICP de Bell et suivre le même processus que celui applicable aux demandes de certificats (voir la section 4.1ff).

### **4.7. Renouvellement des clés de certificats**

Les demandes de renouvellement de clés doivent être adressées au comité directeur ICP de Bell et suivre le même processus que celui applicable aux demandes de certificats (voir la section 4.1ff).

#### **4.8. Modification d'un certificat**

L'AC de base de Bell ne traite pas les modifications de certificats. Les demandes de modification de certificats seront traitées comme des demandes de nouveaux certificats.

#### **4.9. Révocation ou suspension d'un certificat**

Les demandes de révocation ou de suspension de certificats doivent être approuvées par le comité directeur ICP de Bell. Le processus de révocation doit fournir un niveau d'assurance élevé quant à l'authenticité des certificats, tel que décrit à la section 3.4. L'AC de base de Bell doit s'assurer que le certificat révoqué ou suspendu est publié dans une LCR qui sera accessible à toutes les parties utilisatrices. Les demandes de suspension et de révocation doivent être publiées dans les deux (2) et cinq (5) jours ouvrables suivant leur approbation, respectivement. La section 7.2 décrit les exigences relatives au contenu de la LCR.

#### **4.10. Services d'état des certificats**

L'AC de base de Bell doit publier une LCR en ligne, qui doit être accessible à toutes les parties utilisatrices. Sur demande, le comité directeur ICP de Bell mettra à la disposition de toute partie utilisatrice le contrat de niveau de service concernant la disponibilité de la LCR.

#### **4.11. Fin de l'abonnement**

L'AC subordonnée qui souhaite mettre fin à son abonnement doit en faire la demande au comité directeur ICP de Bell. Si la demande est approuvée, un quorum (voir la section 5.2) de registraires de l'AC de base de Bell doit révoquer le certificat de signature de l'AC subordonnée.

#### **4.12. Séquestre et récupération des clés**

L'AC de base de Bell ne doit pas utiliser les services de tierces parties pour le séquestre et la récupération des clés des certificats qu'elle délivre.

## **5. Installations, gestion et contrôle opérationnels**

### **5.1. Contrôles physiques**

Les contrôles physiques des installations qui hébergent l'AC de base de Bell doivent être conformes aux dispositions de la présente politique, ainsi qu'aux politiques, pratiques, normes et procédures de sécurité pertinentes de Bell, aux règlements gouvernementaux et à toutes les lois applicables.

#### **5.1.1 Emplacement et construction des installations**

L'emplacement et la construction des installations qui hébergent l'AC de base de Bell, lorsque d'autres mécanismes de contrôle de sécurité comme des gardes-barrière et des détecteurs d'intrusion y sont intégrés, doivent fournir une assurance de niveau moyen (conformément aux normes du gouvernement canadien) quant à la protection du matériel et des dossiers de l'AC de base de Bell contre un accès non autorisé.

#### **5.1.2 Accès physique**

L'AC de base de Bell doit toujours veiller à ce que son matériel soit protégé contre un accès non autorisé, surtout lorsque le module cryptographique est installé et activé.

Des contrôles d'accès physique doivent être mis en place de sorte à fournir une assurance de niveau moyen (conformément à la section 5.1.1) quant à la protection contre le risque de violation du matériel, même lorsque le module cryptographique n'est pas installé ni activé.

L'accès à l'équipement et au matériel cryptographiques de l'AC de base de Bell doit être réservé à des membres de confiance particuliers du personnel.

#### **5.1.3 Alimentation électrique et climatisation**

L'AC de base de Bell doit s'assurer que les installations d'alimentation électrique et de climatisation sont suffisantes pour permettre le bon fonctionnement du matériel de l'AC.

#### **5.1.4 Exposition à l'eau**

Le matériel de l'AC de base de Bell doit être installé de sorte à le protéger adéquatement contre une exposition à l'eau.

#### **5.1.5 Prévention et protection contre les incendies**

Un système d'extinction des incendies automatique doit être installé conformément aux politiques et codes locaux.

#### **5.1.6 Stockage des supports**

Les supports doivent être stockés de sorte à les protéger contre une détérioration accidentelle (p. ex. eau, feu et magnétisme). Les supports qui contiennent des données de vérification, des archives ou de l'information de sauvegarde doivent être copiés et stockés en sécurité dans un lieu séparé de l'AC de base, conformément à la section 5.1.8, doté d'une protection des supports équivalente à celle en vigueur dans les principales installations de l'AC de base de Bell.

### **5.1.7 Mise au rebut des déchets**

Les déchets doivent être enlevés ou détruits.

Les supports utilisés pour stocker de l'information sensible doivent être nettoyés, de sorte qu'il soit impossible de récupérer les données avant leur élimination.

### **5.1.8 Sauvegarde hors site**

L'AC de base de Bell doit effectuer des sauvegardes de système suffisantes pour récupérer d'une défaillance de système, selon un horaire régulier. L'AC de base de Bell doit utiliser des installations situées dans un lieu séparé de celui de son matériel pour des fins de sauvegarde et d'archivage, et s'assurer que ces installations ont le même niveau de contrôles physiques et procéduraux que les principales installations de l'AC de base de Bell. Les installations servant à la sauvegarde doivent se situer à une distance d'au moins 100 km des principales installations.

## **5.2. Contrôles procéduraux**

L'AC de base de Bell doit prévoir les rôles suivants pour assurer son exploitation :

- les administrateurs de système, qui sont responsables de la maintenance du système d'exploitation et des logiciels d'application pour le serveur qui exécute l'application de l'AC et les serveurs utilisés pour créer le ou les référentiels pour les certificats et les LCR émis par l'AC de base de Bell, ainsi que la présente politique, l'EPC associé et toute pièce justificative exigée. Les tâches d'administration du système peuvent être accomplies par tout administrateur de système autorisé; il n'y a pas de quorum exigé (contrairement aux administrateurs de l'AC et aux registraires);
- les administrateurs de l'AC, qui sont responsables de générer les clés privées de l'AC de base de Bell et d'autoriser les registraires. Tous les administrateurs de l'AC doivent assister à la création des clés privées de l'AC de base de Bell; il faut un quorum d'au moins trois administrateurs de l'AC pour autoriser un registraire;
- les registraires, qui sont responsables de signer les certificats délivrés par l'AC de base de Bell et d'activer les clés de signature privées de l'AC de base de Bell; il faut un quorum d'un quorum d'au moins trois registraires pour activer les clés de signature privées de l'AC de base de Bell.

Les administrateurs de l'AC peuvent également agir comme registraires. Cependant, une séparation stricte des tâches est exigée entre les administrateurs de système d'une part et les administrateurs de l'AC et les registraires d'autre part.

## **5.3. Contrôles du personnel**

Les administrateurs de système, les administrateurs de l'AC et les registraires de l'AC de base de Bell doivent se conformer à toutes les procédures de contrôle des RH pertinentes de Bell, en plus de se soumettre à une vérification des antécédents criminels, avant d'être autorisés à accomplir leurs tâches.

Les administrateurs de système, les administrateurs de l'AC et les registraires doivent recevoir une formation sur l'utilisation des logiciels et du matériel qu'ils utiliseront pour assumer leurs fonctions. Ils doivent également suivre un cours de recyclage chaque fois que paraît une nouvelle version qui se distingue de façon importante de la précédente.

#### **5.4. Procédures de journalisation à des fins de vérification**

Chaque fois qu'elle active une clé de signature privée, l'AC de base de Bell doit consigner ce fait dans un journal, en indiquant les noms des registraires qui l'ont activée, le but de l'activation, ainsi que le numéro de série et le nom distinctif du certificat.

L'AC doit tenir le journal des activations pendant toute sa durée utile, et seuls les administrateurs de l'AC, les registraires et les administrateurs de système de l'AC de base de Bell doivent être autorisés à le consulter. Le journal doit être protégé contre toute violation subséquente (p. ex. sur un support non réinscriptible, ou en signant numériquement toutes les entrées). L'AC doit sauvegarder tous les journaux dans les 24 heures suivant chaque nouvelle entrée, et cette copie de sauvegarde doit également être protégée contre toute violation. La copie de sauvegarde doit être conservée dans un lieu sûr et séparé, conformément à la section 5.1.

#### **5.5. Archivage des documents**

L'AC doit archiver tous les documents associés aux demandes de certificats, y compris les approbations, ainsi que tous les journaux de vérification, pendant toute sa durée utile, plus sept ans. L'accès aux archives doit être réservé aux administrateurs et aux registraires de l'AC.

#### **5.6. Renouvellement des clés**

Les procédures de renouvellements des clés de l'AC de base de Bell sont identiques aux procédures de production des clés; se reporter à la section 6.1. L'ancien certificat ne doit pas être révoqué ni retiré du référentiel, à moins que le comité directeur ICP de Bell ne juge qu'il existe un risque important de compromission de l'ancienne clé privée.

#### **5.7. Compromission et reprise après sinistre**

L'AC de base de Bell doit mettre en place un plan de reprise après sinistre qui lui permettra de reprendre ses activités dans les 30 jours suivant un sinistre. Si un sinistre ou une compromission a lieu, toutes les parties utilisatrices doivent en être avisées. L'AC de base de Bell doit se redéployer conformément à la section 6.6. Si la clé privée a subi une compromission, l'ancien certificat de signature de l'AC de base de Bell doit être révoqué, et une nouvelle paire de clés doit être générée conformément à la section 6.1.

#### **5.8. Cessation des activités de l'AC ou d'une AE**

Lorsqu'elle met fin à ses services, l'AC de base de Bell doit en aviser toutes les parties utilisatrices. Le comité directeur ICP de Bell deviendra alors détenteur de tout le matériel archivé, aussi longtemps que cela sera nécessaire.

## **6. Contrôles techniques de sécurité**

### **6.1. Production et installation des paires de clés**

L'AC de base de Bell doit s'assurer que ses paires de clés de signature numérique sont réalisées à l'aide d'un module matériel autonome (HSM) réservé à son usage exclusif. Le module doit être inviolable, ne présenter aucun signe d'altération et être installé conformément aux exigences de sécurité physique de Bell Canada. La production des paires de clés doit être exécutée à l'aide de l'algorithme RSA et compter au moins 4096 bits. Les certificats délivrés par l'AC de base de Bell doivent être signalés comme étant destinés à ne servir qu'aux fins de signature numérique (voir la section 7.1). Une fois que la paire de clés de signature a été générée, elle doit être copiée sur le module matériel autonome, lequel doit ensuite être mis en lieu sûr, conformément à la section 5.1.

Les paires de clés de l'AC subordonnée, dont les clés publiques doivent être intégrées aux certificats qui seront délivrés par l'AC de base de Bell, doivent être générées à l'aide de l'algorithme RSA et compter au moins 2048 bits. La clé publique de l'AC subordonnée doit être communiquée à l'AC de base de Bell, comme le décrit la section 3.2. Les certificats délivrés par l'AC de base de Bell doivent être signalés comme étant destinés à ne servir qu'aux fins de signature numérique (voir la section 7.1) et communiqués aux parties utilisatrices et au référentiel de certificats, comme l'expliquent les sections 3.2 et 4.4.

### **6.2. Protection des clés privées et contrôles techniques des modules cryptographiques**

Toute activité de maintenance ou d'activation effectuée sur le HSM de l'AC de base de Bell exige la présence d'un quorum (voir la section 5.2) de registraires et doit être exécutée dans un endroit sûr. Aucun employé seul de Bell Canada ne peut avoir accès à toutes les composantes de contrôle d'accès qui lui permettraient d'accéder à un module cryptographique individuellement. L'AC de base de Bell ne doit jamais entiercer ni archiver de clés privées (voir la section 6.1 sur les exigences concernant la sauvegarde des paires de clés).

La destruction des clés privées de l'AC de base de Bell exige la présence d'un quorum de registraires. La mise hors fonction du HSM de l'AC de base de Bell doit être réalisée en présence d'un quorum de registraires. Au moment de la mise hors fonction, tous les jetons HSM et les clés doivent être détruits.

Les NIP nécessaires à l'activation des clés privées de l'AC de base de Bell doivent contenir au moins huit chiffres.

Les composantes cryptographiques doivent être expédiées et reçues de façon sécuritaire, et une vérification de leur intégrité doit être effectuée dès leur réception. Les zones de stockage des HSM doivent être suffisamment sécuritaires pour protéger les HSM contre toute violation ou utilisation non autorisée pendant le stockage.

Les réparations au HSM effectuées sur place doivent être faites en présence d'au moins trois registraires ou administrateurs de l'AC. Les jetons HSM qui ont fait l'objet de réparations ne doivent être mis en service aux emplacements de l'ICP de Bell Canada que si le fournisseur atteste que les fonctions du HSM sont conformes aux exigences et que les jetons réparés équivalent à des jetons nouvellement achetés.

Les clés privées des AC subordonnées dont les certificats sont signés par l'AC de base de Bell ne doivent jamais être entières ni archivées.

### **6.3. Autres aspects de la gestion des paires de clés**

La période de validité du certificat de signature de l'AC de base de Bell est de 20 ans. La période de validité des certificats délivrés par l'AC de base de Bell est de 15 ans.

### **6.4. Données d'activation**

Chaque registraire doit avoir un NIP comportant au moins huit chiffres pour activer ses fonctions sur le module de cryptage de matériel.

### **6.5. Contrôle de la sécurité informatique**

La maintenance de l'ordinateur hébergeant l'AC de base de Bell doit être réalisée conformément aux politiques, pratiques, procédures et normes de sécurité pertinentes de Bell applicables à sa plateforme, à son système d'exploitation et à ses logiciels d'application.

### **6.6. Contrôle de sécurité du cycle de vie**

L'ordinateur hébergeant l'AC de base de Bell doit être déployé conformément aux pratiques de déploiement pertinentes de Bell. Les rustines de système d'exploitation et de logiciels doivent être installées conformément aux politiques, pratiques, procédures et normes de sécurité pertinentes de Bell.

### **6.7. Contrôle de sécurité réseau**

L'ordinateur hébergeant l'AC de base de Bell ne doit en aucun temps être relié à un réseau protocole Internet (protocole IP).

### **6.8. Horodatage**

La différence entre l'heure de l'ordinateur hébergeant l'AC de base de Bell et le temps légal des serveurs de Bell ne doit pas dépasser dix secondes.

## 7. Profils des certificats, des LCR et OCSP

### 7.1. Profil des certificats

Le profil des certificats de signature de l'AC de base de Bell doit contenir les champs suivants :

<b>Champ</b>	<b>Description</b>
<i>Version</i>	Version 3
<i>Serial number</i>	Numéro de série unique parmi tous les certificats délivrés par l'AC de base de Bell
<i>Signature algorithm identifier</i>	SHA-1
<i>Issuer ND</i>	C=CA,O=Bell,OU=Bell Root CA
<i>Valid from</i>	Date et heure de délivrance du certificat
<i>Valid to</i>	20 ans après la date précédente
<i>Subject ND</i>	C=CA,O=Bell,OU= Bell Root CA
<i>Key usage</i>	Signature numérique
<i>Basic constraints</i>	CA:TRUE
<i>Authority key identifier</i>	Empreinte numérique SHA-1 de 160 bits de la clé publique de l'AC de base de Bell
<i>Subject key identifier</i>	Empreinte numérique SHA-1 de 160 bits de la clé publique de l'AC subordonnée
<i>Certificate policies</i>	2.16.124.113565.3.1.1.1
<i>CRL distribution points</i>	Adresse URL de la LCR publiée par l'AC de base de Bell

Le profil des certificats délivrés par l'AC de base de Bell doit contenir les champs suivants :

<b>Champ</b>	<b>Description</b>
<i>Version</i>	Version 3
<i>Serial number</i>	Numéro de série unique parmi tous les certificats délivrés par l'AC de base de Bell

<i>Signature algorithm identifier</i>	SHA-1
<i>Issuer ND</i>	C=CA,O=Bell,OU= Bell Root CA
<i>Valid from</i>	Date et heure de délivrance du certificat
<i>Valid to</i>	15 ans après la date précédente
<i>Subject ND</i>	Nom distinctif approuvé de l'AC subordonnée
<i>Key usage</i>	Signature numérique
<i>Basic constraints</i>	CA:TRUE
<i>Authority key identifier</i>	Empreinte numérique SHA-1 de 160 bits de la clé publique de l'AC de base de Bell
<i>Subject key identifier</i>	Empreinte numérique SHA-1 de 160 bits de la clé publique de l'AC subordonnée
<i>Certificate policies</i>	2.16.124.113565.3.1.1.1
<i>CRL distribution points</i>	Adresse URL de la LCR de l'AC de base de Bell

## 7.2. Profil des LCR

Le profil des LCR publiées par l'AC de base de Bell doit comporter les champs suivants :

<b>Liste de révocation</b>	<b>Description</b>
<i>Serial number</i>	Numéro de série du certificat révoqué
<i>Revocation date</i>	Date de révocation du certificat
<i>CRL reason code</i>	Raison de la révocation (explication)

## 7.3. Profil OCSP

L'AC de base de Bell ne prend pas en charge le protocole OCSP (*On-line Certificate Status Protocol*).

## **8. Vérification de conformité et autres évaluations**

L'AC de base de Bell doit faire l'objet d'une vérification interne de Bell avant le début de ses activités, et au moins une fois par année par la suite. Elle peut également être soumise à une vérification en tout temps, à la discrétion du comité directeur ICP de Bell.

Les résultats de la vérification doivent être transmis au comité directeur ICP de Bell, mais doivent aussi être mis à la disposition de toutes les parties utilisatrices. Si une vérification signale des lacunes, l'AC de base de Bell doit, dans les deux semaines qui suivent, soumettre un plan au comité directeur ICP de Bell pour corriger ces lacunes. S'il juge les risques inacceptables, le comité directeur ICP de Bell peut demander à l'AC de base de Bell d'interrompre ses activités, soit jusqu'à ce que les risques reviennent à un niveau acceptable, soit de façon permanente.

## **9. Autres questions juridiques et de gestion**

### **9.1. Redevances**

L'AC de base de Bell ne prévoit pas imposer de redevances à quelque organisation de Bell, mais se réserve le droit de le faire, à sa discrétion, en tout temps.

### **9.2. Responsabilité financière**

L'AC de base de Bell n'accepte aucune responsabilité financière que ce soit.

Toute partie utilisatrice à la présente politique de certification (PC) (« partie utilisatrice ») doit souscrire une police d'assurance de dommages complète, couvrant les dommages corporels et les atteintes à la personne, dont le décès, et les dommages matériels, y compris toute perte d'utilisation découlant de la négligence de la partie utilisatrice.

### **9.3. Confidentialité des renseignements d'entreprise**

Tous les renseignements confidentiels communiqués à l'AC de base de Bell (comme de possibles renseignements confidentiels apparaissant dans une demande de certificat, et les parties confidentielle de l'EPC) ainsi que tous les renseignements contenus dans les journaux de pistes de vérification, les rapports vérification, les mesures de sécurité et les plans de reprise après sinistre, sont considérés confidentiels et doivent être traités conformément aux politiques de sécurité pertinentes de Bell et aux lois sur la vie privée pertinentes du Canada.

Toute AC subordonnée ou autre partie utilisatrice ayant accès à ces renseignements confidentiels ou les recevant doit les protéger contre un accès non autorisé, en assurer la confidentialité et éviter de les utiliser ou de les divulguer à des tiers.

### **9.4. Confidentialité des renseignements personnels**

Tous les renseignements personnels recueillis par l'AC de base de Bell seront traités conformément aux politiques de sécurité pertinentes de Bell et aux lois sur la vie privée pertinentes du Canada.

Les renseignements figurant dans les certificats et la liste des certificats révoqués (LCR) émis par l'AC de base de Bell ne sont pas considérés comme des renseignements personnels.

### **9.5. Droits de propriété intellectuelle**

Les droits de propriété intellectuelle découlant du déploiement de l'AC de base de Bell, y compris la PC, l'EPC, les certificats, les noms et les clés, ainsi que tout produit ou renseignement développé en vertu de la présente politique ou conformément à celle-ci, demeurent la propriété de Bell Canada.

### **9.6. Déclarations et garanties**

L'AE qui assume les fonctions d'enregistrement décrites dans la présente politique doit se conformer aux dispositions de la présente politique.

Chaque AC subordonnée de l'AC de base de Bell s'engage à faire ce qui suit :

- fournir à l'AC de base de Bell des renseignements exacts, exempts d'erreurs, d'omissions et de fausses déclarations;

- demander la révocation d'un certificat lorsque la clé correspondante n'est plus nécessaire, ou lorsque la sécurité de la clé a été compromise ou a pu être compromise;
- mémoriser plutôt que noter les mots de passe ou NIP nécessaires pour accéder aux clés privées ou aux jetons cryptographiques ou les utiliser;
- protéger avec diligence les clés privées et les jetons cryptographiques en tout temps contre la perte, le vol ou l'altération ou la violation;
- informer l'AC de base de Bell dans les 48 heures suivant tout changement aux renseignements apparaissant dans un certificat ou une demande de certificat;
- informer l'AC de base de Bell dans les 24 heures si elle soupçonne une compromission de la sécurité d'une ou de plusieurs de ses clés privées, des données d'activation ou du module matériel autonome ou de tout mot de passe ou NIP utilisé pour accéder à ses clés privées ou à ses jetons cryptographiques;
- comprendre les principes de base des certificats de clé publique et leur utilisation dans l'application de gestion;
- utiliser les certificats exclusivement à des fins légales et autorisées, conformément aux conditions de la présente politique et des lois applicables;
- utiliser les certificats uniquement pour le compte de la personne, de l'entité ou de l'organisation qui est indiquée comme étant le sujet du certificat;
- lire et comprendre toutes les conditions et restrictions contenues dans la présente politique et tout autre contrat conclu avec l'AC de base de Bell, et accepter d'y être liée.

Chaque partie utilisatrice s'engage envers l'AC de base de Bell à faire ce qui suit :

- utiliser les certificats exclusivement à des fins légales et autorisées, conformément aux lois applicables;
- comprendre et reconnaître qu'elle s'appuie sur la présente politique à ses risques, et que l'AC de Bell n'assume aucune responsabilité quant à la confiance accordée à la présente politique.

L'AC de base de Bell atteste qu'elle fait preuve de diligence raisonnable lorsqu'elle vérifie l'exactitude des renseignements apparaissant dans les certificats qu'elle délivre. Toutefois, l'AC de base de Bell ne fait aucune déclaration ni garantie relativement à ce qui suit :

- les techniques utilisées pour générer et stocker la clé privée qui correspond à la clé publique d'un certificat, que la sécurité de la clé privée ait été compromise ou que la clé ait été générée au moyen de techniques cryptographiques sûres;
- la fiabilité des techniques ou méthodes cryptographiques utilisée pour effectuer toute action, transaction ou processus mettant en cause ou utilisant un certificat;
- tout logiciel quel qu'il soit; ou
- la non-répudiation d'un certificat quelconque ou d'une signature numérique vérifiée à l'aide d'un certificat, puisque la détermination de non-répudiation dépend des lois applicables.

### 9.7. Exonération de garanties

L'AC de base de Bell décline toute garantie quant à l'utilisation de ses certificats à des fins autres que la vérification de l'identité de l'AC subordonnée.

L'AC de base de Bell ne peut être tenue responsable de l'une ou l'autre des pertes suivantes :

- perte découlant d'un manquement de toute partie utilisatrice à ses obligations, d'une perte de service causée par une guerre, une catastrophe naturelle, une grève, un lock-out, un conflit de travail ou tout autre facteur indépendant de sa volonté;
- perte subie entre la date de révocation d'un certificat et la publication suivante de la liste des certificats révoqués;
- perte liée à l'utilisation non autorisée des certificats délivrés par l'AC subordonnée;
- perte liée à l'utilisation des certificats au-delà des limites prescrites dans la PC en vertu de laquelle les certificats sont délivrés, ou perte liée à l'utilisation frauduleuse ou négligente des certificats et/ou de la LCR émis par l'AC subordonnée;
- perte liée à la divulgation de renseignements contenus dans les certificats et les LCR;
- perte découlant d'un défaut d'aviser la partie utilisatrice de la révocation de certificats. L'AC de base de Bell décline toute autre garantie ou obligation que ce soit, y compris toute garantie de qualité marchande, garantie de bon fonctionnement à une fin particulière et garantie d'exactitude de l'information fournie.

### 9.8. Limitations de la responsabilité

L'AC de base de Bell et ses employés, administrateurs ou fournisseurs, déclinent expressément toute responsabilité que ce soit à l'égard de toute AC subordonnée, partie utilisatrice ou autre personne ou entité, relativement à l'utilisation de ses certificats ou des services qu'elle fournit en lien avec les certificats ou à la confiance qui leur est accordée.

L'expression « niveau d'assurance moyen » ne doit pas être considérée comme étant une déclaration ou une garantie relative à la disponibilité des services de l'AC de base de Bell. Bell Canada ne garantit pas que les services de l'AC de base de Bell seront disponibles en tout temps.

La présente politique renferme également des garanties limitées et des exonérations des déclarations, garanties et conditions. Les parties utilisatrices reconnaissent que l'AC de base de Bell n'assume aucune responsabilité que ce soit relativement à des dommages subis par les parties utilisatrices ou tout tiers en raison d'une confiance excessive accordée à tout certificat. Chaque certificat de l'AC subordonnée doit contenir un avis de responsabilité limitée.

L'exonération de responsabilité qui précède s'applique à toute responsabilité contractuelle (y compris une inexécution fondamentale), délictuelle (y compris une négligence) ou à toute autre théorie de responsabilité, et s'applique indépendamment d'un manquement à l'objet essentiel de quelque recours limité que ce soit prévu dans les présentes, et même si l'AC de base de Bell a été informée de la possibilité de tels dommages.

L'AC de base de Bell n'offrira aucune compensation à qui que ce soit relativement à toute perte découlant de l'utilisation inappropriée ou frauduleuse de cette infrastructure à clé publique. L'AC de base de Bell décline toute responsabilité que ce soit en rapport avec un contrat ou une autre forme de réclamation concernant l'exportation ou l'importation de produits cryptographiques par des personnes ou des organisations qui utilisent les services de l'AC de base de Bell.

© 2008 Bell Canada

L'AC de base de Bell décline également toute responsabilité que ce soit en ce qui concerne les facteurs indépendants de sa volonté, y compris la disponibilité ou le fonctionnement d'Internet, des télécommunications ou d'autres systèmes d'infrastructure.

## **9.9. Indemnités**

Chaque AC subordonnée assume tous les risques et responsabilités liés à l'exécution de ses obligations en vertu des présentes et de celles de ses employés, sous-traitants et agents. Elle doit également prendre toutes les mesures nécessaires pour éviter tout dommage à l'AC de base de Bell et à toute autre personne concernée par les obligations décrites dans les présentes. À cet effet, l'AC subordonnée s'engage à indemniser l'AC de base de Bell et toute autre personne concernée par les obligations décrites de toute réclamation, demande, poursuite, action, cause d'action ou responsabilité, de quelque nature que ce soit, pour des dommages, pertes, coûts ou dépenses découlant de i) dommages à des personnes ou à des biens, atteintes à la personne ou décès causé par la négligence ou des actes volontaires ou des omissions de l'AC subordonnée ou de ses employés, sous-traitants et agents, en rapport avec la présente politique ou les services associés; et ii) toute violation par l'AC subordonnée de tout engagement, déclaration, garantie ou condition contenus dans la présente politique et faisant font partie des responsabilités de l'AC subordonnée.

## **9.10. Période de validité et cessation des activités**

La présente politique demeure en vigueur tant que l'AC de base de Bell continue d'exercer ses activités. Les sections 9.3, 9.8 et 9.9 demeureront en vigueur après la résiliation de la présente politique.

## **9.11. Avis individuels et communications avec les participants**

Les participants et les parties utilisatrices à la présente politique peuvent communiquer officiellement avec l'AC de base de Bell en envoyant un courriel à [bellrootca@bell.ca](mailto:bellrootca@bell.ca).

## **9.12. Modifications**

Toute modification apportée à la présente politique doit être approuvée au préalable par le comité directeur ICP de Bell. Il incombe également au comité de déterminer si la modification approuvée modifie l'acceptabilité des certificats délivrés en vertu de la PC à un degré qui justifie de modifier l'identificateur d'objet (OID) de la PC.

## **9.13. Dispositions concernant le règlement des différends**

Tout différend lié à la gestion des clés et des certificats au sein des entités de Bell sera résolu, en dernier ressort, par le comité directeur ICP de Bell. Si un différend entre Bell et une entité externe ne peut être réglé par la négociation ou la médiation, on devra recourir à l'arbitrage, conformément à la *Loi sur l'arbitrage commercial* du Canada.

## **9.14. Lois applicables**

Les lois de l'Ontario et les lois fédérales du Canada qui s'appliquent aux présentes, à l'exclusion des règlements relatifs aux conflits des lois, régissent l'interprétation, la validité et l'exécution de la présente politique, ainsi que tout autre contrat conclu par l'AC. Tout différend lié à la présente politique ou à tout contrat, ou à des certificats ou à tout service fourni par l'AC de base de Bell en lien avec les certificats, qui ne peut être résolu par un autre mécanisme de règlement des différends, sera porté devant les tribunaux de la province de l'Ontario, et toutes les personnes, entités ou organisations conviennent par les présentes que ces tribunaux auront une compétence personnelle et exclusive sur ces différends.

### **9.15. Conformité aux lois applicables**

Les participants à l'AC de base de Bell doivent se conformer à tous les codes, lois, ordonnances et règlements applicables des organismes gouvernementaux, qu'ils soient fédéraux, provinciaux, municipaux ou locaux, qui ont compétence sur les services fournis aux termes des présentes, y compris, sans s'y limiter, ceux en lien avec le traitement du matériel et des logiciels cryptographiques.

### **9.16. Accord intégral**

La présente politique et les documents auxquels elle renvoie constituent la politique de certification complète de l'AC de base de Bell et l'intégralité de l'entente intervenue entre l'AC subordonnée et l'AC de base de Bell en ce qui concerne l'objet des présentes, et annulent et remplacent tous les accords antérieurs et autres protocoles ou déclarations concernant l'AC de base de Bell.

S'il est établi qu'une partie de la présente politique est incorrecte ou invalide, le reste de la PC demeurera en vigueur.

### **9.17. Cession**

Les certificats et les droits octroyés en vertu de la présente politique ou de tout contrat appartiennent personnellement à l'AC subordonnée à laquelle le certificat a été délivré, et à la personne, à l'entité ou à l'organisation qui a signé un contrat avec l'AC de base de Bell; ils ne peuvent être cédés, vendus, transférés ni autrement aliénés, que ce soit volontairement ou involontairement, par effet de la loi ou autrement, sans l'accord écrit préalable de l'AC de base de Bell.

Toute tentative de cession ou de transfert sans ce consentement sera nulle et mettra automatiquement fin aux ces droits de l'AC subordonnée en vertu de la présente politique ou de tout contrat d'abonné. L'AC de base de Bell peut céder, vendre, transférer ou aliéner autrement la présente politique, ou tout contrat, ainsi que tous ses droits et obligations en vertu de la présente politique et de tout contrat, à une société affiliée.

### **9.18. Cas de force majeure**

L'AC de base de Bell ne peut être tenue responsable des pertes, coûts, dépenses, responsabilités, dommages ou réclamations, ou être considérée comme ayant failli aux modalités de la présente politique, de tout contrat ou de tout montant de règlement, lorsque des retards ou des manquements d'exécution sont imputables à des causes indépendantes de sa volonté, y compris, sans s'y limiter, les événements suivants : cas fortuit ou sabotage, émeute ou insurrection, guerre, attentat terroriste, épidémie, accident, feu, grève ou autre conflit de travail, embargo, demande en justice, manque de permis ou d'approbation d'exportation ou incapacité d'obtenir de tels permis, manque de main-d'œuvre, de matières premières, d'énergie ou de services publics nécessaires, de composantes ou de machinerie et actes des autorités civiles ou militaires.