Infrastructure à Clés Publiques de Rezel

Politique de Certification De Rezel

VERSION 0.2

Table des matières

1 Préambule

1.1 Aperçu

Ce document constitue la Politique de Certification (PC) de l'Autorité de Certification (AC) mise en place à Rezel. Il décrit les différentes dispositions qui d'une part, garantissent la fiabilité des certificats délivrés, et d'autre part, limitent le cadre juridique d'utilisation de ces certificats.
La présente PC régit l'ensemble des composantes de l'Infrastructure à Clés Publiques (ICP) de Rezel.

1.2 Version

La version de la présente politique de certification de Rezel est 0.1, datée du 9 mai 2007.

1.3 Publication

Ce document est publié sur le site Web de l'AC de Rezel (http://ca.rezel.net).

2 Introduction

2.1 Introduction Générale

2.1.1 Infrastructure à Clé Publique (ICP)

Une ICP est un ensemble d'outils destiné à fournir des services de sécurité basés sur la cryptographie asymétrique (clé privée/clé publique). Les clients utilisateurs font partie d'une même communauté désirant accéder à ces services de sécurité communs.
Le principe de la cryptographie asymétrique est simple : chaque utilisateur possède un jeu de deux clés, l'une publique et l'autre privée. Tout le monde peut utiliser la clé publique d'une autre personne (ou machine) pour chiffrer un message que seul cette personne (ou machine) possédant la clé privée correspondante pourra déchiffrer. La clé privée ne circule jamais dans le réseau, il est donc possible de s'échanger des messages ou documents électronique de façon sécurisée.
La cryptographie asymétrique à elle seule, étant facile à gérer, est bien adaptée à des échanges entre deux individus. Ce n'est pas le cas dans un environnement ouvert ou au sein d'une organisation, où plusieurs individus, ne se connaissant pas forcément, échangent des données sensibles ou effectuent des transactions électroniques.
Les infrastructures à clé publique sont destinées à répondre à ce besoin. Elles sont composées de plusieurs éléments dont l'AE (autorité d'enregistrement), la CA (autorité de certification) et un système de distribution et stockage des certificats.

2.1.2 Politique de Certification (PC)

Une politique de certification est un ensemble identifié de règles indiquant l'applicabilité d'un certificat à une collectivité en particulier et à une catégorie d'applications comportant des exigences de sécurité communes. Elle précise si le certificat de clé publique en question convient ou non à une fin ou à une application donnée.

Une autorité de certification peut adopter plusieurs politiques de certification, mais dans chaque cas, le document qu'est cette politique sert de pierre angulaire à l'établissement d'un lien de confiance à l'égard d'un certificat de clé publique. De plus, cette politique rend possible la co-certification.
En émettant un certificat, l'autorité de certification déclare à l'utilisateur du certificat qu'une clé publique donnée est associée à une entité dont l'identité a été authentifiée selon des règles établies par une politique de certification.
En somme les principaux rôles de la politique de certification sont :

- La définition du périmètre d'utilisation des certificats
- L'indication des obligations et responsabilités des entités (Utilisateur, CA, ...)
- La spécification des classes de certificats si différents niveaux de sécurité sont nécessaires, et les niveaux de contrôle qui leur sont associés

Ainsi, la politique de certification précise à la fois les conditions d'utilisation des certificats et les garanties offertes par ces certificats.

2.2 Rôles des composantes de l'ICP et des intervenants

2.2.1 Autorité de certification

C'est l'entité de l'ICP qui est responsable de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle définit une Politique de Certification (PC) et la fait appliquer par les différentes composantes de l'Infrastructure à Clé Publique.

2.2.2 Autorité d'Enregistrement

C'est l'entité de l'ICP qui est chargé de traiter les demandes de certificat et vérifier que le demandeur est bien la personne qu'il prétend être, conformément aux règles définies par l'Autorité de Certification. Elle garantit la validité des informations contenues dans le certificat.

2.2.3 Client de l'ICP

Client ou bien porteur de certificat, c'est la personne physique détentrice d'un certificat.

2.2.4 Tiers utilisateurs

C'est la personne qui souhaite authentifier un porteur de certificat, de vérifier une signature numérique et/ou de chiffrer des messages à l'intention d'un porteur de certificat.

2.2.5 Résumé de la Politique de Certification

2.2.5.1 Introduction

L'infrastructure à clé publique implémentée à Rezel délivrera dans un premier temps des certificats de signature de deux classes : des certificats de classe 1, destinés aux tests disponibles pour toute la communauté Internet, et des certificats de classe 3 réservés aux administrateurs de Rezel.

2.2.5.2 Certificats de classe 1

Selon la présente politique de certification, sont émis des certificats de test de classe 1 et leurs clés privées associées pour une fin de signature numérique de classe 1. Ils devront être utilisés pour des applications de type messagerie électronique ou navigation sur le Web, sans valeur marchande ou juridique associée, c'est à dire sans obligation de donner, de faire ou de ne pas faire quelque chose.
Lors de l'enregistrement initial, un lien entre le demandeur du certificat et son adresse électronique qui devrait être unique est établie.
Les certificats de classe 1 sont envoyés sous forme logiciel par voie électronique ou téléchargés du site de l'AC de Rezel.

2.2.5.3 Certificat classe 3

Selon la présente politique de certification, les certificats de classe 3 émis, et leurs clés privées associées, sont destinés à l'identification des individus désirant accéder à des données sensibles, par exemple la gestion des adhérents pour les administrateurs.
Lors de l'enregistrement initial, l'identité des détenteurs potentiels de ces certificats doit être vérifiée. Une authentification des demandeurs est effectuée lors de cette phase : seuls les administrateurs de Rezel peuvent obtenir ce certificat, ils doivent se présenter en personne auprès de l'administrateur de l'ICP.
Ces certificats et leurs clés privées associées sont stockés dans un support matériel (clé USB par exemple).

2.3 Personne responsable, coordonnées

2.3.1 Organisme responsable de la présente politique

La présente politique de certification est sous la responsabilité de Rezel

2.3.2 Personne Responsable

Administrateur ICP de Rezel
212 rue de Tolbiac
75013 Paris

2.4 Champs d'applications de la politique

Le présent document constitue la politique de certification de l'ICP mise en place à Rezel dans le cadre d'une expérimentation (projet d'INFRES357 – S2P3 2007). Elle s'applique à l'AC, à son responsable, à son personnel, aux certificats émis par l'AC, aux Listes de Certificats Révoqués

émises par l'AC, aux individus utilisant les services de l'AC et aux tiers utilisateurs des certificats émis par l'AC.

2.4.1 Liste des applications appropriées

2.4.1.1 Certificats de classe 1

Ce type de certificat doit être utilisé exclusivement à des fins de test et de familiarisation avec la technologie des certificats. Ils doivent être utilisés pour des applications de type messagerie électronique ou navigation sur le Web, sans valeur marchande ou juridique associée, c'est-à-dire sans obligation de donner, de faire ou de ne pas faire quelque chose.

2.4.1.2 Certificats de classe 3

Certificat à utiliser pour la signature et l'identification en vue d'accéder à des données sensibles, par exemple des données nominatives (gestion des adhérents), au sein de Rezel.

2.4.2 Liste des applications interdites

2.4.2.1 Certificats de classe 1

Toutes applications autres que celles définies par la disposition 2.4.1.1 est interdite. Toutes personnes ne respectant pas ceci, le fait sous sa propre responsabilité et à ses risques et périls.

2.4.2.2 Certificats de classe 3

Toutes applications autres que celles définies par la disposition 2.4.1.2 est interdite. Toutes personnes ne respectant pas ceci, le fait sous sa propre responsabilité et à ses risques et périls.

3 Dispositions générales

3.1 Obligations générales

Pour un bon fonctionnement et des services de sécurité fiables, les différentes composantes de l'ICP doivent respecter chacune ses obligations.

3.1.1 Obligations de l'AC

L'AC est responsable des opérations relatives aux services de certification réalisées par l'une quelconque des composantes de l'ICP.
L'AC doit en outre :

- Se conformer à toutes exigences de la présente Politique de Certification.
- Veiller à ce que toutes les composantes de l'ICP se conforment à toutes les modalités pertinentes de la présente Politique de Certification.
- Respecter les droits des porteurs de certificats et tiers utilisateurs de certificats à l'égard des lois et règlements en vigueur.
- Publier les LCR (Liste des Certificats Révoqués), les mettre à jour et préserver leur intégrité.

- Utiliser des moyens de génération des clés et certificats d'un niveau de sécurité compatible avec la classe des certificats émis.
- Mettre en place les moyens nécessaires pour assurer une protection maximale de l'infrastructure contre les désastres et l'accès non autorisé et toutes opérations qui peuvent nuire à la qualité des services offerts.
- Mettre en place les moyens nécessaires pour assurer une disponibilité maximale de l'ensemble des services.
- Informer les demandeurs de certificats des procédures à suivre correspondantes au cycle de vie des certificats.

3.1.2 Obligations de l'Autorité d'Enregistrement (AE)

L'AE doit se conformer à toutes les exigences de la présente politique de certification. Elle doit en outre :
- . Traiter les demandes de certificat dans des délais raisonnables.
- . Vérifier les données personnelles d'identification et les données contenues dans le certificat
- Mettre en place les moyens pour communiquer en sécurité avec les clients dans les différentes phases du cycle de vie de certificats.
- Respecter la loi en vigueur en ce qui concerne les données à caractère personnel et d'identification collectées lors des procédures d'enregistrement.
- Conserver et protéger en confidentialité et en intégrité toutes les données collectées, à caractère personnel.

3.1.3 Obligations du « client »

Toute personne possédant un certificat (de n'importe quelle classe) délivré par l'AC de Rezel, doit se conformer à toutes les exigences de la présente Politique de Certification.
Elle doit en outre :
- Garantir que les informations soumises à l'AC sont exactes, complètes et que les documents présentés sont valides.
- Aviser l'AC de la perte ou la compromission de sa clé privée le plus rapidement possible si cela arrive.

3.1.4 Obligations du tiers utilisateur

Le tiers utilisateur d'un certificat (personne qui se fie à un certificat signé par l'AC de Rezel) doit se conformer à toutes les exigences mentionnées dans le cadre de la présente Politique de Certification et de tout document contractuel associé qu'il reconnaît expressément avoir lu et approuvé.
L'AC de Rezel se dégage de toute responsabilité des conséquences résultantes de l'utilisation d'un certificat non valide ou révoqué non vérifié.
Le tiers utilisateur doit toujours vérifier que le certificat est utilisé à des fins pertinentes et conformément aux applications autorisées.

3.2 Responsabilités

Toutes les parties (l'AC, les composantes de l'ICP, les porteurs de certificats, et les tiers utilisateurs) sont responsables de tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente Politique de Certification.

3.2.1 Responsabilité de l'AC

L'AC étant en phase d'expérimentation, elle n'assume aucun engagement ni responsabilité quant aux conséquences qui pourraient résulter de l'interruption de ses activités provoquée par tout cas de force majeure.
Aucune responsabilité ne sera assumée par l'AC et par le personnel de l'AC pour l'utilisation d'un certificat dans des conditions qui ne seraient pas conformes ou non autorisées par la présente Politique de Certification.

3.2.2 Responsabilité de l'AE

La responsabilité de l'AE pourra être engagée uniquement par l'AC.

3.3 Interprétation et mise en application

3.3.1 Droit applicable

La loi française est applicable aux dispositions de la présente Politique de Certification, bien que les activités qui en découlent puissent être appliquées en partie en dehors de la France. Les certificats de test, notamment, peuvent être utilisés en dehors du territoire français.

3.3.2 Règlement des différends

Toute contestation relative aux dispositions du présent document et au service de certification sera soumise à une procédure à l'amiable préalablement à une instance judiciaire.

3.3.3 Permanence de la PC

Le fait que l'une des parties n'ait pas exigé l'application d'une clause quelconque du présent document ne pourra en aucun cas être considéré comme une renonciation aux droits de cette partie découlant de cette clause dont l'inapplication a été tolérée.

3.4 Publication et dépôt de documents

3.4.1 Informations publiées

Les documents disponibles au public (consultables sur le site Web de l'AC) sont la Politique de Certification et les formulaires de demande de certificat.
La Liste des Certificats Révoqués est publiée également.

3.4.2 Fréquence de diffusion

Les Listes de Certificats Révoqués seront mises à jour dans des délais que l'AC juge être raisonnables.
La PC publiée est mise à jour dès qu'une nouvelle version est mise au point.

3.4.3 Contrôle de l'accès

La Politique de Certification de l'AC ne sera accessible, pour création ou modification, qu'au personnel autorisé de l'AC, et ce à travers des contrôles d'accès appropriés généralement mis en place à Rezel.
Un système de contrôle d'accès est mis en place au niveau du service de publication pour protéger les documents publiés.

3.5 Contrôle de conformité à la PC

L'Autorité de Certification de Rezel a la responsabilité du bon fonctionnement des composantes de l'ICP, conformément aux dispositions énoncées dans le présent document. L'AC effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette ICP.

3.5.1 Fréquence du contrôle de conformité

Aucune exigence n'est spécifiée pour le moment, le contrôle devrait être réalisé au minimum une fois par an par la suite.

3.5.2 Périmètre du contrôle de conformité

Le périmètre de l'audit concerne toutes les procédures et tous les engagements stipulés par le présent document.

3.6 Politique de confidentialité

3.6.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :
- les clés privées des entités propriétaires de certificats,
- les journaux d'événements des composantes de l'AC et de l'AE,
- les données personnelles (à l'exception des informations à caractère personnel contenues dans les certificats),
- les rapports d'audit

3.6.2 Données à caractère personnel détenues par l'AC

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au contenu de tous les documents détenus ou transmis par l'AC.

L’AE collecte notamment des informations personnelles au moment de la requête des certificats de classe 3 qui devrait se faire en « face à face ».
Toutes les données collectées et détenues par l’AC sur une personne sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable de cette personne.

3.6.3 Données à caractère personnel contenues dans la LCR

Les Listes des Certificats Révoqués ne contiennent que les numéros d’enregistrement des certificats, et leur date de révocation.

3.6.4 Divulgation des causes de révocation de certificat

Les causes de révocation des certificats sont confidentielles, elles ne sont pas divulguées.

3.7 Droits relatifs à la propriété intellectuelle

Les éléments protégés par la législation sur les droits d'auteur resteront la propriété du détenteur des droits correspondants. Il n’est pas permis de mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des oeuvres dérivées ou copies de ceux-ci, sans l'autorisation préalable du détenteur des droits d'auteur.

3.8 Dispositions pénales

Ces dispositions ne sont pas définies pour le moment.

4 Identification et authentification

4.1 Enregistrement initial

4.1.1 Types de noms

Chaque certificat doit contenir dans le champ « Subject » un nom de forme distinctive et unique, de telle façon qu’il n’y ait pas d’ambiguïté dans la base de donnée de l’AC de Rezel.

4.1.2 Nécessité d'utilisation de noms distinctifs

Un nom doit présenter un caractère unique dans sa constitution au sein de la base de donnée de l’AC.
Le contenu des champs de nom Subject et Issuer doit avoir un lien explicite avec l'entité authentifiée.
Pour les certificats de test (Classe 1) : le nom distinctif doit contenir une adresse électronique.
Pour les certificats de classe 3 : le nom distinctif doit contenir soit une combinaison du prénom et du nom, soit un pseudonyme identifié comme tel (le login par exemple).

4.1.3 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC.
Cette dernière s'occupera de garantir l'unicité de l'attribut de sujet de certificat en lui assignant si nécessaire une valeur formée d'une combinaison d'informations relatives au porteur du certificat

4.1.4 Procédure de règlement des différends concernant des revendications relatives aux noms

Une partie qui demande un certificat doit préalablement avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer.
Tout différend est réglé par l'AC.

4.1.5 Méthode de vérification de la possession de la clé privée

L'AC doit vérifier que le demandeur est véritablement en possession de la clé privée associée à la clé publique objet de la certification. Cette vérification peut être réalisée à partir d'un paquet de demande de certificat au standard PKCS #10 dans le cas de certificat de test (classe 1). Pour la classe 3, la question ne se pose pas car la clé privée est générée par l'AC elle-même. Le tout, clés et certificat, est délivré en « face à face » dans un support digne de confiance.

4.2 Vérification aux fins de renouvellement périodique des clés

Le renouvellement est valable pour les certificats de classe 3. Il n'y a pas de renouvellement pour les certificats de test.
La vérification doit être la même que lors d'un enregistrement initial

4.3 Authentification des demandes de révocation

Il n'y a pas de révocation pour les certificats de classe 1. En ce qui concerne les certificats de classe 3, l'authentification des demandes de révocation est réalisée soit par la fourniture d'un secret (mot de passe) et d'autres informations directement à l'AC (serveur de l'AC), soit par une présence physique.
Si la demande émane d'un tiers, ce dernier doit être authentifié et la demande doit être justifiée.

4.4 Vérification aux fins de renouvellement des clés après une révocation

Si un certificat a été révoqué, il ne peut jamais y avoir de renouvellement. Il faut procéder à la certification de nouvelles clés de la même façon que pour un enregistrement initial.

5 Exigences opérationnelles en matière de gestion des certificats

5.1 Demande de certificat

Les demandeurs d'identification électronique doivent suivre et respecter les procédures publiées. Les informations suivantes doivent au moins figurer dans la demande de certificat :

- les informations qui seront inscrites dans le nom distinctif (DN) du certificat,
- . la clé publique à certifier (certificat de test et paire de clé générée par le demandeur),
- la preuve de possession de la clé privée.

Selon la classe du certificat demandé, la demande doit contenir les éléments suivants :

Classe de Certificat	**Informations requises dans les requêtes Et mode de communication**
Certificat de Test (classe 1)	Informations requises : - Nom, prénom - Adresse e-mail - Acceptation des procédures et politiques de certification. Mode de communication : Via le site Web de l'AC et la messagerie électronique.
Certificat de classe 3	Informations requises : - Nom, prénom - Adresse postale et téléphone - Preuve d'appartenance à l'organisation (ici administrateur de Rezel) : authentification (login et mot de passe) ou déclaration sur l'honneur d'un membre du bureau. - Adresse e-mail - Contrat et acceptation des procédures et politiques de certification. Mode de communication : Face-à-face

Chaque demande doit être accompagnée des éléments qui permettent de prouver l'identité et les pouvoirs des futurs porteurs de certificat conformément aux procédures applicables en fonction du type de certificat demandé.

5.2 Validation des demandes de certificat

5.2.1 Exigences de la validation des demandes de certificat

Les validations requises préalablement à l'émission d'un certificat sont :

- Établir que le demandeur du certificat est la personne identifiée dans la demande (en accord avec et dans la limite de la description des niveaux de certificat)
- Établir que le demandeur du certificat a le droit de détenir la clé privée correspondant à la clé publique mentionnée dans le certificat
- Établir que les informations appelées à figurer dans le certificat sont exactes.

5.2.2 Approbation des demandes de certificat

En cas de réussite de toutes les validations requises pour une demande de certificat, la demande est approuvée et le certificat demandé est délivré selon la procédure d'émission.

5.2.3 Refus d'une demande de certificat

En cas d'échec de la validation, le demandeur concerné est avertie sans délai de l'échec de la validation en mentionnant le motif de l'échec (sauf si la loi l'interdit).
La personne dont la demande de certificat est rejetée peut présenter une nouvelle requête.

5.3 Émission et distribution d'un certificat

Une demande de certificat n'oblige en aucune façon l'AC à émettre un certificat numérique.
L'émission d'un certificat par l'AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat.

5.4 Acceptation des certificats

5.4.1 Déclaration du client à l'acceptation

En acceptant un certificat, le « client » des services de l'AC de Rezel certifie et reconnaît vis-à-vis de cette AC, émettrice du certificat et de tous ceux qui font raisonnablement confiance à l'information contenue dans le certificat que :

- Toute signature numérique créée à l'aide de la clé privée correspondant à la clé publique qui figure dans le certificat et que le certificat a été accepté et est en cours de validité (ni expiré, ni révoqué) au moment de la signature numérique et qu'aucune personne non autorisée n'a eu accès à sa clé privée.
- Toutes les déclarations faites par le « client » concernant l'information contenue dans le certificat sont vraies.
- Le certificat est exclusivement utilisé à des fins légales et licites, conformes à la présente PC.

5.4.2 Obligation d'empêcher la divulgation de la clé privée

En acceptant un certificat, le « client » utilisateur des services de l'AC, est obligé de protéger sa clé privée en utilisant un système digne de confiance et de prendre les précautions raisonnables pour empêcher la perte, la divulgation, la modification ou l'usage abusif de sa clé privée.

5.4.3 Publication

La publication d'un certificat intervient après l'acceptation de ce dernier par la personne à qui il est destiné. Cette dernière peut aussi publier leurs certificats en utilisant leurs propres moyens.

5.5 Récupération des clés privées.

Les certificats générés par l'AC de Rezel sont des certificats de signature. La clé privée de signature ne se récupère donc jamais.

5.6 Suspension et révocation d'un certificat

5.6.1 Motifs généraux de révocation

Un certificat sera révoqué dans ces cas :
- Compromission ou violation de la clé privée du sujet du certificat
- Le sujet du certificat n'a pas respecté une obligation matérielle du présent document
- Départ ou changement du statut du sujet du certificat
- L'information contenue dans le certificat du sujet du certificat a été modifiée.

5.6.2 Révocation à la demande du « client »

L'AC doit révoquer un certificat à la demande du « client » une fois ce dernier est authentifié.

5.6.3 Révocation pour vice d'émission

L'AC révoquera sans retard un certificat non délivré conformément aux procédures stipulées par la présente PC.

5.6.4 Notification et confirmation de la révocation

L'AC s'engage à mettre à jour la LCR dés qu 'un certificat est révoqué et de fournir une confirmation de révocation si c'est le « client » qui en a fait la demande.

5.6.5 Effet de la révocation

La révocation d'un certificat induit les effets suivants :
- La période opératoire du certificat est immédiatement considérée comme terminée.
- Les obligations contractuelles stipulées par la présente PC ne sont pas affectées.
- La clé privée correspondant à la clé publique devra être détruite.

5.6.6 Délai de traitement d'une demande de révocation

L'ICP étant en phase d'expérimentation ce délai n'est pas encore fixé. Pour l'instant, les demandes de révocation des certificats de classe 3 sont traitées immédiatement dès réception des

demandes via le Web ou en se présentant physiquement auprès d'un administrateur de l'ICP. Les certificats de test ne sont pas révocables.

5.6.7 Fréquence de publication de la liste des certificats révoqués (LCR)

Dès que la révocation du certificat d'une entité identifiée est effective, l'AC générera et publiera dans un délais raisonnable une nouvelle LCR (Liste des Certificats Révoqués).

5.6.8 Publication des motifs de révocation

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit du porteur du certificat.

5.7 Sauvegarde et archivage

Dans le but d'assurer la continuité des services, l' « auditabilité » et la non-répudiation des opérations, les certificats de signatures émis et les LCR produites par l'AC sont archivés.
Ces donnés sont conservés pendant une durée que l'AC jugera être raisonnable, typiquement un an pour les opérations concernant les certificats de classe 1, et dix an pour celles concernant les certificats de classes 2, après leur expiration.

5.8 Renouvellement des clés

Les bi-clés sont périodiquement renouvelés afin de minimiser les attaques cryptographiques. L'enregistrement lors d'un renouvellement est identique à l'enregistrement initial.

5.9 Compromission et mesures anti-sinistre

Les mesures et procédures à suivre doivent être documentés par l'AC.

5.9.1 Corruption des ressources informatiques, des logiciels et (ou) des données

La seule activité critique que l'AC doit maintenir en fonctionnement, c'est la prise en compte et la publication des révocations de certificats.

L'AC doit établir des procédures visant à assurer le maintien des activités et décrire, dans ces procédures, les étapes prévues en cas de corruption ou de perte des ressources informatiques, logicielles ou de données nécessaires. Lorsque le dépôt de documents ne relève pas de l'AC, celle-ci doit s'assurer que tous les contrats conclus avec le dépositaire prévoient la mise en place, par celui-ci, de procédures visant à la préservation des données.
L'AC doit également envisager un plan de secours et de redémarrage de ses activités.
Le service étant en phase de test, ces mesures ne sont pas opérationnelles à l'heure actuelle.

5.9.2 Révocation de la clé publique d'une composante de l'ICP

Dans le cas où l'on doit révoquer le certificat de signature numérique d'une AC il faut :

- Aviser les porteurs de certificats concernés,
- Publier le numéro de série du certificat dans la LCR appropriée,
- Révoquer tous les certificats signés au moyen du certificat de signature numérique révoqué.

Après la correction des problèmes qui ont donné suite à la révocation, l'AC peut :

- Produire un nouveau bi-clé de signature et publier les certificats y associés,
- Émettre de nouveaux certificats à toutes les entités.

5.9.3 Compromission de la clé privée d'une composante de l'ICP

Si une composante de l'ICP soupçonne sa clé privée d'être compromise, elle doit avant de redéfinir un certificat au sein de l'ICP révoquer sa clé publique.

5.10 Fin d'abonnement

Les porteurs de certificats délivrés par l'AC de Rezel sont considérés comme abonnés aux services offerts par cette AC. Leur abonnement est valable tant que le certificat est en cours de validité ou qu'il a été renouvelé.
L'interruption d'un abonnement suite à une cause quelconque entraîne la révocation du certificat correspondant.
Les personnes qui peuvent demander la fin de l'abonnement sont les mêmes que celles pouvant demander la révocation du certificat.

6 Mesures de sécurité physique, des procédures et du personnel

6.1 Contrôles de sécurité physique

6.1.1 Situation géographique et construction des sites

L'ICP est installée dans une zone de sécurité et protégée contre l'accès non autorisé.

6.1.2 Accès physique

Les contrôles de sécurité physique mis en œuvre sont les suivants :

- Entrée au bâtiment protégé.
- Accès aux machines contrôlés.

6.1.3 Autres contrôles

Le niveau de protection des locaux techniques de l'AC est essentiel dans la garantie de la sécurité des moyens de certification et de l'exploitation de ces moyens.
Une fois l'AC mise en production, le personnel d'administration fera le nécessaire pour garantir une protection maximale contre les risques d'accident.
Il serra mis en place des systèmes garantissant le fonctionnement de l'infrastructure dans le meilleur cadre possible : par exemple mise en place d'un système de conditionnement de l'air pour la régulation de la température et de l'humidité.

6.2 Contrôles du personnel

Tous les membres du personnel de l'ICP doivent être des personnes de confiance, administrateurs de Rezel. Ils devraient être formés pour accomplir les taches qui leur sont attribuées et s'engager sur la non-divulgation de renseignements ayant trait à la sécurité de l'AC.

7 Mesures techniques de sécurité

7.1 Production et installations des bi-clés

7.1.1 Production des bi-clés et remise des clés privées

L'AC doit produire son propre bi-clé de signature numérique au moyen d'un algorithme de cryptographie par des moyens sûrs.
L'AC ne délivrant que des certificats de signature, dans le cas de certificats de test, le demandeur produit lui-même un bi-clé de signature numérique. Dans le cas d'un certificat de classe 3, le bi-clé de signature numérique est produit par l'AC est délivré à la personne concernée en face-à-face.

7.1.2 Remise de la clé publique à l'AC

Lors de l'enregistrement initial, pour les certificats de test, la clé publique d'un demandeur de certificat doit être remise à l'AC sous la forme d'un paquet attestant de la possession de la clé privée correspondante.

7.1.3 Remise de la clé publique de l'AC aux utilisateurs

Les utilisateurs peuvent télécharger sur le site de l'AC, sa clé publique de vérification sous la forme d'un certificat numérique.

7.1.4 Tailles des clés asymétriques

Tous les bi-clés des AC ont une durée de vie au moins égale à 10 ans, sont produits par l'algorithme RSA et ont une taille de clé d'au moins 2048 bits.
Les bi-clés délivrés aux demandeurs de certificats ont une durée de vie d'un an, sont produits en utilisant l'algorithme RSA et ont une taille qui varie de 512 à 2048.

7.1.5 Production des paramètres des clés publiques

Le moyen de génération de bi-clé doit utiliser des paramètres respectant les normes internationales de sécurité propres à l'algorithme considéré.

7.1.6 Nature de la ressource de production de clés

Les bi-clés de l'AC, et les bi-clés de signature numérique sont produits par un module cryptographique logiciel.

7.1.7 Utilisation de la clé publique

L'AC ne délivre que des certificats de signature numérique, la clé publique de vérification est utilisée à des fins d'identification, d'authentification, de non-répudiation et/ou d'intégrité. La clé publique de vérification de l'AC est la seule clé utilisable pour vérifier la signature des certificats.

7.2 Protection des clés privées

Les porteurs de certificats délivrés par l'AC de Rezel doivent protéger leurs clés privées afin qu'elles ne soient pas divulguées. Il leur appartiendra de choisir le matériel et les logiciels offrant une sécurité suffisante pour la protection et l'utilisation de leurs clés privées conformément à la présente politique de certification.

7.2.1 Récupération des clés privées

Pour le moment l'AC de Rezel ne délivre que des certificats de signature numérique, il n'y a pas de recouvrement pour tous les certificats.

7.2.2 Initialisation et conservation de la clé privée dans le module cryptographique

Les clés privées des AC sont générées dans le module cryptographique logiciel, elles sont conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.
Les clés privées des porteurs de certificats sont générées par un moyen local. Elles doivent être conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.

7.2.3 Méthode d'activation de la clé privée

Les demandeurs de certificats doivent être authentifiés avant que la clé privée ne soit activée. Cette authentification peut se faire sous forme de données d'activation (mot de passe) dans le cas de certificats de classe 1, et par présence physique dans le cas de certificats de classe 3.

7.2.4 Méthode de désactivation/destruction des clés privées

Lorsque les clés sont désactivées, ils doivent être effacer de la mémoire. Dans le cas ou le certificat de signature numérique arrive à expiration ou s'il est révoqué, la clé privée ne peut plus servir à aucune opération et doit être détruite.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

L'AC émettrice doit archiver toutes les clés publiques de vérification conformément à la stipulation définie au sous-paragraphe 5.7.

7.3.2 Périodes d'utilisation des clés publiques et privées

La période de validité de toutes les clés des porteurs de certificats est d'un an.
La période de validité des clés des éléments de l'ICP est de 10 ans.

7.4 Données d'activation

7.4.1 Génération et installation des données d'activation

Des données d'activation peuvent être utilisées lors de la livraison des certificats de classe 1 et 2. Ces données d'activation, générés par l'AC doivent être aléatoires.

7.4.2 Protection des données d'activation

Pour les systèmes de l'AC, les données d'activation doivent être protégées en intégrité et en confidentialité. Ceci est normalement prévu dans la suite logicielle que l'AC utilise pour la mise en place de son infrastructure.
Les porteurs de certificat sont responsables de l'intégrité et la confidentialité des données d'activation liée à leurs clés privées.

7.5 Contrôle des développements des systèmes

L'ICP mise en place à Rezel est en phase d'expérimentation pour le moment. Cette phase d'expérimentation peut déboucher sur une phase de production où de nombreuses modifications seront effectuées.
L'implémentation de l'ICP, la configuration de toutes ces composantes ainsi que toutes modifications ou installations ultérieures devront être documentées, respectées et contrôlées.

7.6 Mécanismes de contrôle de la sécurité réseau

L'ICP doit être protéger contre les attaques provenant d'Internet. Une telle protection doit être assurée par l'installation de passerelles de sécurité.

8 Forme et contenu des certificats et des listes de révocations

8.1 Forme et contenu des certificats

Les champs suivants doivent être complétés par le logiciel de l'AC :
- Version: version du certificat X.509
- Numéro de série unique du certificat
- Algorithme de signature de l'AC
- Emetteur: nom de l'AC émettrice
- Validités: dates d'activation, et d'expiration du certificat
- Sujet: nom distinctif de l'entité identifiée
- Algorithme d'usage de la clé publique, et valeur de la clé publique.
- Extensions: les extensions du certificat.

8.1.1 Signature du certificat

C'est l'empreinte numérique que l'AC appose, en utilisant sa clé privée sur le certificat. Par conséquent le certificat signé est l'ensemble des éléments suivants :

- L'ensemble des champs décrits à l'article 8.1,
- L'identifiant de l'algorithme utilisé pour produire la signature de l'AC,
- L'empreinte numérique de l'AC.

8.1.2 Champs d'extensions

L'AC supporte les extensions normalisées tels que spécifiés dans la recommandation X509.

8.2 Formes et contenu des LCR

Les LCR doivent contenir les champs de base tels que spécifiés dans la recommandation X 509 CRL Version 2 :
- Version: version de la liste de certificats révoqués X.509
- Signature: identifiant de l'algorithme de signature de l'AC
- Emetteur: nom de l'AC émettrice
- Date d'émission de cette LCR
- Date limite d'émission de la prochaine LCR
- Liste d'enregistrement de révocation
- Numéro de série unique du certificat révoqué
- Date de la révocation
- Extensions propres à cette révocation
- Extensions générales de la LCR

9 Administration de la politique de certification

9.1 Procédures de modifications

9.1.1 Délais de préavis

La présente Politique de Certification peut être modifiée sans préavis des porteurs de certificats et tiers utilisateurs si les changements n'ont aucune conséquences sur eux. Cependant un préavis que l'AC jugera raisonnable (typiquement 7 à 30 jours) sera donné selon l'importance de l'impact des modifications sur les porteurs de certificats et tiers utilisateurs.

9.1.2 Forme de diffusion des avis

Dans les cas nécessitant un préavis, les changements sont diffusés sur le site Web de l'AC, et les porteurs de certificats sont avisé (typiquement par courrier électronique).

9.1.3 Modifications nécessitant l'adoption d'une nouvelle politique

Dans le cas ou les modifications apportées à la politique ont un impact majeur sur les porteurs de certificats et/ou les tiers utilisateurs, une nouvelle politique de certification peut être instituée.

9.2 Procédure de publication

La présente Politique de Certification doit être publiée et accessible. L'ensemble de ces documents est publié sur le site Web de l'AC et une copie peut être obtenue par voie électronique.