Banque Populaire

Politique de Certification - AC ICG BP Client

Reference du document	
1.3.6.1.4.1.40559.1.0.1.1.111.1.0	1 juillet 2013

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 467 226 960 €.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13. RCS n°493 455 042.

Table des matières

1. INTRODUCTION

1.1. Présentation générale

BPCE SA, pour son réseau Banque Populaire, met en œuvre un service de dématérialisation des contrats intégrant un processus de signature électronique.

Dans le cadre de ce processus des certificats électroniques de signature sont générés à la volée et valable le temps de la transaction de signature électronique.

Dans ce cadre, le réseau Banque Populaire utilise une Autorité de Certification, interne au Groupe BPCE, pour émettre les certificats électroniques de signature auprès de Clients ou de Prospects.

Il s'agit de l' « AC ICG CE Client » qui a vocation à être certifiée conformément au référentiel ETSI 102042 pour le niveau LCP.

Le présent document constitue la Politique de Certification pour les certificats du profil « Signature » de l'Autorité de Certification « AC ICG CE Client ».

1.2. Identification du document

Le numéro d'OID du présent document est 1.3.6.1.4.1.40559.1.0.1.1.111.1.0

Le numéro d'OID de ce document répond aux principes de nommage suivants :

- iso(1)
- org(3)
- dod(6)
- internet(1)
- private(4)
- enterprise(1)
- bpce (40559)
- Service informatique (1)
- Programme de confiance numérique (0)
- Politiques de Certification (1)
- Politique de Certification IT-CE – ICG – Signature (1)
- Racine (1), Client (11), ICG-CE-Client(101), ICG--Entite(121), ICG-BP-Client(111), ICG-Tech(131),
- Environnement :
  - Production (1)
  - Qualification développement (2)
- Version (0)

1.3. Entités intervenant dans l'IGC

1.3.1. Autorité de Certification

L'Autorité de Certification est BPCE SA, dûment représentée par son responsable, le Directeur de la Sécurité des Systèmes d'informations Groupe.

L'Autorité de Certification est garante du niveau de confiance des certificats qu'elle émet. Ce niveau de confiance repose sur des mesures techniques et organisationnelles et sur une gouvernance, qui sont décrits dans la présente Politique de Certification. L'Autorité de Certification veille à l'application de la présente Politique de Certification

En particulier, l'AC a la responsabilité des fonctions suivantes :

- Mise en application de la PC.
- Gestion des certificats.
- Publication des Listes de Certificats Révoqués (LCR).
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'IGC.
- Réception et traitement des demandes de Révocation de Certificats.
- Archivage des dossiers de demande de Certificats ou de Révocation.

Elle peut déléguer opérationnellement une partie de ses responsabilités.

1.3.2. Autorité d'Enregistrement

Les rôles de l'Autorité d'Enregistrement sont répartis entre :

- D'une part, les Chargés de Clientèle,
- D'autre part, l'AE Technique.

La présente PC ne fait donc pas référence à l'Autorité d'Enregistrement, mais à l'une ou l'autre de ses composantes, ensemble des Chargés de Clientèle, ou AE Déléguée.

1) Le Chargé de Clientèle

Le Chargé de Clientèle appartient au réseau des Banque Populaire et réalise le face à face préalable avec le futur porteur de certificat.

Dans ce cadre, le Chargé de Clientèle a pour rôle de dérouler le processus de signature du contrat en présence du client. Ce processus intègre de manière transparente les étapes de demande, de génération et de destruction du certificat électronique délivré au porteur.

Le Chargé de Clientèle accompagne le Porteur dans le processus de signature et réalise les différentes étapes proposées par son application métier de signature de contrat.

Les différentes étapes techniques liées à ce processus amènent le chargé de clientèle à avoir accès à un coffre-fort électronique, elles lui permettent d'avoir accès aux contrats signés par le Porteur.

Le Chargé de Clientèle veille à la protection de la confidentialité et de l'intégrité des données qui lui parviennent ou qu'il transmet à d'autres fonctions de l'IGC au cours des processus de gestion du cycle de vie des certificats.

2) L'AE Technique

L'AE technique est appelée directement par les composants de signature utilisés par le Chargé de Clientèle en agence ou bien par un Client ou un Prospect directement en ligne. Ces appels permettent de :

- Générer des bi-clés pour le porteur au niveau de l'application de signature
- Réaliser la demande de certificat au nom du Porteur

Cette AE technique est donc « transparente » du point de vue du Porteur et du chargé de clientèle et est opérée par l'Opérateur de Service , IT-CE.

L'AE Technique est responsable de la gestion du cycle de vie des certificats. Elle gère pour le compte des Clients et Prospects:

- Les demandes d'enregistrement.
- Les demandes de révocation.
- L'archivage des dossiers d'enregistrement.

Elle joue le rôle d'interface auprès de l'Autorité de Certification pour mener à bien les actions ci-dessus.

L'AE Technique veille à la protection de la confidentialité et de l'intégrité des données qui lui parviennent ou qu'elle transmet à d'autres fonctions de l'IGC au cours des processus de gestion du cycle de vie des certificats.

1.3.3. Porteurs de certificats

Le Porteur de certificat est une personne physique, client de la Banque Populaire ou Prospect et souhaitant signer électroniquement un contrat. Il obtient dans ce cadre un certificat X.509 V3, dont les informations d'identification sont regroupées dans le champ "Objet".

1.3.4. Utilisateurs de certificats

Les utilisateurs de certificats, dans le cadre de la présente Politique de Certification, sont :

- Les services d'archivage constituant le dossier de preuve lié au contrat dématérialisé signé
- Les outils techniques mis à disposition des porteurs leur permettant de lire numériquement leur contrat signé et les propriétés de signature mises en œuvre dans le cadre de l'opération de signature de leur contrat.

1.3.5. Autres participants

1) Composantes de l'IGC

Les composantes techniques de l'IGC sont présentées dans la Déclaration des Pratiques de Certification et maintenues par l'opérateur de Service de Certification IT-CE.

2) Opérateur de Service de Certification (OSC)

L'Opérateur de Service de Certification est chargé de la délivrance du service technique correspondant aux fonctions de l'Autorité de Certification.

- Il héberge, exploite et maintient en conditions opérationnelles les composants d'infrastructure et les interfaces de gestion.

- Il s'engage sur le niveau de service de l'Autorité de Certification.

L'Opérateur de Service de Certification est IT-CE. Le personnel de l'OSC peut être amené à utiliser des certificats d'authentification ou de signature sur les composantes de l'IGC. Ces certificats sont émis par une Autorité de Certification propre à l'OSC. La présente Politique de Certification ne s'applique pas à ces certificats.

3) Mandataire de certification

Sans objet.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

1) Bi-clés et certificats des Porteurs

Les certificats concernés par cette PC sont des certificats de signature. Ils répondent aux besoins de signature électronique et de non répudiation des personnes physiques, clientes ou prospects du réseau Banque Populaire, et souhaitant réaliser une opération de signature électronique de leur contrat.

L'usage des certificats est rappelé dans les Conditions Générales d'Utilisation, qui sont soumises au Porteur durant le processus de signature de son contrat. Le Porteur approuve ces Conditions Générales d'Utilisation sans quoi le processus de signature de son contrat ne peut pas aboutir.

Les bi-clés associées aux certificats sont stockées sous format logiciel sur le serveur réalisant l'opération de signature.

2) Bi-clés et certificats d'AC et composantes

Le certificat de l' « AC ICG CE Client » est signé par l' « AC ICG BPCE » et est utilisable exclusivement pour :

- Signer des certificats Porteurs.

- Signer des LCRs.

La chaîne de certification mise en œuvre est la suivante :

- AC Racine BPCE

  - AC ICG BPCE

- AC ICG BP Client

1.4.2. Domaines d'utilisation interdits

L'AC décline toute responsabilité dans l'usage que ferait un Porteur d'un certificat dans le cadre d'une application non mentionnée au paragraphe 1.4.1, et pour toute opération illicite.

En cas de violation de cette obligation par le Porteur, BPCE SA et le réseau Banque Populaire ne pourraient voir leur responsabilité engagée vis-à-vis de quiconque.

Les actions résultant de l'utilisation du certificat ne peuvent être considérées comme ayant une valeur probante au sens de la directive européenne 1999/93/CE et des articles 1316 et suivants du Code civil.

1.5. Gestion de la PC

1.5.1. Entité gérant la PC

BPCE SA gère la PC via ses instances de pilotage et de décision de l'AC.

1.5.2. Point de contact

Les demandes d'informations ou questions concernant l'Autorité de Certification doivent être adressées à :

Directeur de la Sécurité des Systèmes d'informations Groupe (RSSI Goupe)

50 Rue Pierre Mendes France

75201 Paris Cedex 13

rssi-pssi-icg@bpce.fr

Ce point de contact est disponible et à jour sur le site de publication de l'Autorité de Certification (voir le paragraphe 2.2).

1.5.3. Entité déterminant la conformité d'une DPC avec cette PC

Le Comité Sécurité Groupe (COSSIG) sous la responsabilité du RSSI-Groupe détermine la conformité de la DPC à la présente PC.

1.5.4. Procédures d'approbation de la conformité de la DPC

L'approbation de la conformité de la DPC est mise à l'ordre du jour du COSSIG. Ce dernier se base sur des résultats d'audits menés par le contrôle RSSI IT-CE et sur les PV de mise en production. Deux niveaux de contrôles sont alors appliqués.

- Contrôle niveau 1 par les équipes opérationnelles d'IT-CE
- Contrôle niveau 2 par les équipes sécurité IT-CE

1.6. Définitions et acronymes

Les définitions et acronymes sont référencées dans le document annexe suivant : « Mesures communes, définitions et acronymes applicables à l'ICG ». Cette annexe est publiée au sein du même espace que la présente politique.

2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

2.1. Entités chargées de la mise à disposition des informations

L'Autorité de Certification est chargée de la mise à disposition des informations devant être publiées.

L'Opérateur de Service s'engage à fournir les informations devant être publiées dans les délais réglementaires, et à les publier au niveau du site Internet.

2.2. Informations devant être publiées

Les informations publiées par l'AC ICG BP Client sont les suivantes :

- La présente Politique de Certification.
- Les Conditions Générales d'Usage du service de signature
- Les points de contacts (adresses email, numéros de téléphone) avec l'Autorité de Certification
- La liste des certificats révoqués (LCR)
- Les certificats de l'AC ICG BP Client, de l'AC IGC BPCE et de l'AC Racine BPCE.
- L'empreinte du certificat de l'AC ICG BP Client.

Toutes ces informations sont publiées sur le site Internet du réseau des Banques Populaires : http://pro.d00.pki01.bpce.fr

2.3. Délais et fréquences de publication

Le site de publication a une disponibilité de 24h/24 7j/7.

La disponibilité, les délais et fréquence de publication des LCR sont précisés au paragraphe 4.9.

Le site de publication garantit l'intégrité des informations publiées.

2.4. Contrôle d'accès aux informations publiées

Les informations publiées sont mises à disposition en lecture à l'ensemble des accédants au site de publication (ouvert sur Internet).

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC.

Le personnel de l'OSC a accès aux informations y compris les informations d'état des certificats (ajout, suppression, modification), via une authentification par certificat, et selon une politique d'habilitation.

Le personnel d'exploitation du site de publication a accès aux informations y compris les informations d'état des certificats (ajout, suppression, modification), via une authentification à deux facteurs, et selon une politique d'habilitation.

Le transfert des informations devant être publiées de l'OSC vers le personnel d'exploitation du site de publication se fait de manière sécurisée en garantissant l'intégrité des données.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3 l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type X.501.

Le paragraphe 7 précise le format du DN.

3.1.2. Nécessité d'utilisation de noms explicites

La décomposition du DN est la suivante :

- Champ CN (Common Name) : contient le prénom suivi du nom du Porteur, tels qu'inscrit dans le référentiel d'identification des Clients de la Banque Populaire (cas d'un Client) ou que saisit par le Prospect.

Remarque : en cas d'homonymie, un deuxième prénom, tel que figurant sur le titre d'identité présenté, pourra être ajouté dans le champ CN.

- Champ OU (Organizational Unit) : contient le numéro de SIREN ou SIRET de l'organisation d'appartenance du Client, tel que renseigné dans le référentiel d'identification des Clients de la Banque Populaire (cas d'un Client) ou que saisit par le Prospect. S'il s'agit d'un particulier, le champ n'est pas positionné

- Champ O (Organization) : contient le libellé de l'organisation d'appartenance du Client tel que renseigné dans le référentiel d'identification des Clients de la Banque Populaire (cas d'un Client) ou que saisit par le Prospect ou rien s'il s'agit d'un particulier.

- Champ C (Country) : contient le pays où est basé le siège social de l'organisation d'appartenance du Client ou du Client lui-même tel que renseigné dans le référentiel d'identification des Clients de la Banque Populaire (cas d'un Client) ou que saisit par le Prospect.

.

Ces informations sont :

- recueillies par le Chargé de Clientèle, sur la base des informations déjà présentes dans le référentiel d'identification des Clients de la Banque Populaire, au moment de l'établissement du contrat avec le Client ou le Prospect s'il s'agit d'une souscription en agence,

- Recueillies, sur la base des informations déjà présentes dans le référentiel d'identification des Clients de la Banque Populaire, après l'identification du Client s'il s'agit d'une souscription en ligne,

- Saisies par le Prospect et après avoir été authentifié s'il s'agit de la souscription en ligne par un Prospect.

Le paragraphe 7 précise le format du DN.

3.1.3. Pseudonymisation des porteurs

Les pseudonymes ne sont pas autorisés par la présente Politique de Certification.

Remarque : les certificats anonymes ne sont pas non plus autorisés.

3.1.4. Règles d'interprétation des différentes formes de nom

Aucune interprétation particulière n'est à faire des informations portées dans le champ « Objet » des Certificats.

Ces informations sont établies par l'AC et reposent essentiellement sur les règles suivantes :

- Tous les caractères sont au format printableString, i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501.

- Les prénoms et noms composés sont séparés par des tirets " - ".

Les certificats respectent les exigences formulées dans le document [RFC 5280].

3.1.5. Unicité des noms

Les certificats des Porteurs de l'« AC IGC BP Client » pour le profil Signature sont identifiés de manière unique par la combinaison :

- Du DN du certificat.

  o Le DN contient le prénom, le nom et éventuellement l'organisation du Porteur.

- Le deuxième prénom du Porteur sera inscrit dans le champ CN (entre le premier prénom et le nom) en cas d'homonymie avec un Porteur existant.

- Du champ « Subject Alternative Name ».

  o Ce champ contient l'adresse email professionnelle du Porteur qui est unique au sein de son organisation.

- Du champ « Key Usage ».

  o Ce champ permet de distinguer le certificat d'un même Porteur pour des profils différents (Authentification ou Signature).

3.1.6. Identification, authentification et rôle des marques déposées

Sans objet.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

La clé privée est générée par la KI ICGau moment de la signature du dossier à signer. Cette clé privée n'est valable que pour la signature du dit dossier et est détruite définitivement du contexte à la fin de l'opération de signature. La preuve de possession de la clé privée se fait au moment de la génération d'une requête de certificat, conforme au standard PKCS#10.

3.2.2. Validation de l'identité d'un organisme

Cf. paragraphe 3.2.3.

3.2.3. Validation de l'identité d'un individu

1) Enregistrement d'un porteur [particulier]

Si le Porteur est un Client, il s'identifie et s'authentifie en Agence ou sur le portail de la Banque Populaire. Une fois le Client authentifié, les informations le concernant sont récupérées depuis le référentiel d'Informations des Clients de la Banque Populaire.

Si le Porteur est un Prospect, il s'identifie sur le portail de la Banque Populaire via le mécanisme proposé. Une fois identifié, il saisit les informations nécessaires à l'établissement de son certificat.

Le procédé d'identification du Porteur diffère suivant la Banque Populaire et le canal d'accès (Agence Internet, Téléphone,…).

2) Enregistrement d'un porteur [Entreprise] sans Mandataire de Certification

Dans le cas d'un Client [Entreprise], le référentiel d'identification des Clients de la Banque Populaire dispose des informations liées à l'entreprise :

- Identité du Signataire Client
- SIREN

Dans le cas d'un Prospect, les informations suivantes sont saisies au moment de l'inscription :

- Identité du Signataire Prospect
- SIREN

3) Enregistrement d'un Mandataire de Certification (ou Gestionnaire de Certificats)

Sans objet.

4) Enregistrement d'un porteur [Entreprise/Administration] via un Mandataire de Certification

Sans objet.

3.2.4. Informations non vérifiées du porteur

Sans objet.

3.2.5. Validation de l'autorité du demandeur

La validation de l'autorité du demandeur dépend de sa qualité de Client ou de Prospect. Notamment les documents qui peuvent être signés ne sont pas les mêmes suivant qu'il s'agisse d'un Client ou d'un Prospect.

3.2.6. Certification croisée d'AC

L'AC IGC CE Client ne fait l'objet d'aucune certification croisée avec une autre AC.

3.3. Identification et validation d'une demande de renouvellement des clés

Remarque : un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante.

Le processus de renouvellement dans le cadre de la présente PC n'est pas recevable du fait qu'il s'agit de certificat électronique éphémère à usage unique.

3.4. Identification et validation d'une demande de révocation

Remarque : Toute demande de révocation est authentifiée et validée par le Chargé de Clientèle. La demande de révocation n'est recevable que durant la durée de vie du certificat électronique qui est de 10 minutes. En dehors de cette période le certificat aura expiré et il ne sera pas possible de réaliser une opération de révocation.

Les acteurs suivants peuvent être à l'origine d'une demande de révocation :

- Le Porteur via une demande en agence auprès d'un chargé de clientèle.
- Le processus de signature dématérialisé dans le cadre d'une erreur rencontrée au cours du processus de signature électronique.

3.4.1. Cas d'une révocation par le Porteur

Le Porteur demande à son Chargé de Clientèle de révoquer son certificat. Cette demande n'est recevable que durant une période de 10 minutes après la signature de son contrat.

Le Chargé de Clientèle transmet un email à l'AC pour que la révocation soit prise en compte.

3.4.2. Cas d'une révocation via l'application de signature

Dans le cas où une erreur est rencontrée par l'application de signature une demande automatique de révocation du certificat est envoyée à l'AC.

4. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Une demande de certificat pour un Porteur doit émaner du serveur de signature utilisé par la Banque Populaire.

Cette demande ne peut donc provenir que pour un Client ou un Prospect du réseau Banque Populaire.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Les informations liées à la demande de certificats sont vérifiées sur la base :

- Des informations d'identité du porteur.
- Les informations d'identification d'entreprise du porteur, s'il s'agit d'une demande pour un certificat d'entreprise.

4.2. Traitement d'une demande de certificat

4.2.1. Exécution des processus d'identification et de validation de la demande

L'application de signature utilisée met en œuvre un processus automatique qui :

- Permet de récupérer automatiquement les informations d'identification à jour lorsqu'il s'agit d'un Client
- Utilise les informations saisies au moment de l'opération de signature lorsqu'il s'agit d'un Prospect
- Propose éventuellement au chargé de clientèle de mettre à jour certaines informations si ces dernières sont obsolètes ou non exploitables. Le chargé de clientèle peut demander au Client de fournir de nouveau ses justificatifs d'identité s'ils ne sont pas lisibles dans le référentiel de la banque.

S'il s'agit d'un Porteur entreprise, les informations nécessaires à la validation de l'entreprise sont également présentées suivant le même processus.

Il s'agit notamment dans ce cadre d'obtenir le numéro SIREN à jour de l'entreprise.

4.2.2. Acceptation ou rejet de la demande

L'étape de validation décrite au paragraphe précédent (paragraphe 4.2.1) peut conduire à l'acceptation ou au rejet de la demande.

En cas de rejet de la demande, l'AE informe le Porteur de la non-conformité rencontrée.

4.2.3. Durée d'établissement du certificat

Suite à la validation de la demande de signature du contrat, les opérations techniques de génération du certificat sont déclenchées instantanément. Ces opérations consistent notamment à :

- Générer une nouvelle clé privée
- Faire une demande de signature
- Faire signer cette demande par l'AC
- Emettre le certificat électronique correspondant
- Réaliser l'opération de signature du contrat
- Détruire la clé privée générée initialement

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Voir paragraphe précédent

4.3.2. Notification par l'AC de la délivrance du certificat au porteur

Il n'y a pas de notifications particulières de la délivrance du certificat au Porteur, du fait que le certificat est éphémère et utilisé directement dans les opérations de signature de son contrat.

Néanmoins ce certificat est intégré au document PDF matérialisant le contrat signé du Client.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Dans le processus de signature, le Porteur est amené à accepter les Conditions Générales d'Usage du service. Ces Conditions Générales d'Usage intègrent les Conditions Générales d'Utilisation du certificat.

Cette étape est obligatoire pour permettre la signature du contrat. En cas de refus par le Porteur, il ne lui sera pas possible de signer électroniquement son contrat.

L'étape de signature vaut donc acceptation explicite par le Porteur.

4.4.2. Publication du certificat

Les certificats ne sont pas publiés après leur délivrance.

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée et du certificat doit être conforme aux usages prévus au paragraphe 1.4.

Les Conditions Générales d'Utilisation incluses dans les Conditions Générales d'Usage du service de signature précisent également l'usage de la clé privée.

De plus, le certificat les mentionne explicitement dans des champs dédiés (voir le paragraphe 7).

4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificats doivent respecter les usages autorisés des certificats tels que prévus au paragraphe 1.4.

4.6. Renouvellement d'un certificat

La RFC 3647 définit l'opération de renouvellement d'un certificat comme la génération d'un certificat dont seules les dates de validité ont changé par rapport au certificat précédent.

Le processus de renouvellement est sans objet dans le cadre de la présente Politique de Certification.

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4. Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

4.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé

4.7.1. Causes possibles de changement d'une bi-clé

La signature d'un nouveau contrat entraîne systématiquement la génération d'une nouvelle bi-clé.

Il n'est donc pas opportun de parler de nouveau certificat puisque les processus sont identiques à ceux de la délivrance initiale.

4.7.2. Origine d'une demande d'un nouveau certificat

Sans objet.

4.7.3. Procédure de traitement d'une demande d'un nouveau certificat

Sans objet.

4.7.4. Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.7.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.7.6. Publication du nouveau certificat

Sans objet.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.8. Modification du certificat

Sans objet.

4.8.1. Causes possibles de modification d'un certificat

Sans objet.

4.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4. Notification au porteur de l'établissement du certificat modifié

Sans objet.

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6. Publication du certificat modifié

Sans objet.

4.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

4.9. Révocation et suspension des certificats

La révocation d'un certificat ne peut intervenir que durant la période de validité du certificat, c'est-à-dire pendant les 10 minutes après la génération du certificat.

Cette période extrêmement courte entraîne le fait que le processus de révocation sera difficilement probant dans le cadre de la présente Politique de Certification.

Néanmoins la PKI mise en œuvre permet de traiter manuellement les révocations.

4.9.1. Causes possibles d'une révocation

1) Certificats de Porteurs

Un certificat doit être révoqué dans les cas suivants :

- Non-respect de la PC et des Conditions Générales d'Utilisation.
- Les informations éronées relatives à l'identité du Porteur figurant dans le certificat
- La clé privée du Porteur est suspectée de compromission ou est compromise.
- Le certificat de l'AC est révoqué (ce qui entraîne la Révocation de tous les Certificats signés par la Clé Privée correspondante).
- Le Porteur,ou le chargé de clientèle fait une demande de révocation du certificat Porteur.

2) Certificats d'une composante de l'IGC

Un certificat de composante de l'IGC doit être révoqué dans les cas suivants :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante.
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec elle suite à un audit de qualification ou de conformité négatif).
- Cessation d'activité de l'entité opérant la composante.

4.9.2. Origine d'une demande de révocation

1) Certificats de Porteurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat de Porteur sont les suivantes :

- Le Porteur au nom duquel le certificat a été émis.
- Le Chargé de clientèle.
- Un Représentant légal du Porteur.
- L'AC émettrice du certificat.

Le Porteur est informé des personnes ou entités susceptibles d'effectuer une demande de révocation pour son certificat, via les Conditions Générales d'Utilisation.

2) Certificats d'une composante de l'IGC

La révocation du certificat de l'AC ne peut être décidée que par le responsable de l'AC ou par des autorités judiciaires via une décision de justice.

La révocation des certificats des autres composantes est décidée par l'entité opérant la composante concernée (l'OSC) qui doit en informer l'AC sans délai.

4.9.3. Procédure de traitement d'une demande de révocation

1) Révocation d'un certificat Porteur

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre 3.4.

La révocation d'un certificat Porteur peut être réalisée via un processus manuel de demande explicite auprès des équipes de l'OSC.

L'opération est enregistrée dans les journaux d'événement de l'AC.

2) Révocation d'un certificat d'une composante de l'IGC

La décision de révocation d'un certificat d'AC sera prise par le responsable de l'Autorité de Certification. Il en informera aussitôt les AE et l'OSC.

La décision de révoquer un certificat d'une autre composante de l'IGC (sous la responsabilité de l'OSC) devra être soumise par l'OSC au Responsable de l'Autorité de Certification au préalable. Les impacts de cette révocation seront étudiés, et des mesures prises en conséquence.

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

Dès que le Porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

Le délai ne pourra excéder 10 minutes après la génération du certificat.

4.9.5. Délai de traitement par l'AC d'une demande de révocation

1) Révocation d'un certificat Porteur

La demande sera traitée par les équipes de l'OSC dès sa réception et durant les heures et jours ouvrés.

2) Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'AC ou d'une composante de l'IGC est effectuée immédiatement par l'OSC dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat (voir paragraphe 4.9.2.2) et suite à la prise de décision du Responsable d'AC.

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

Dans le processus de signature électronique du contrat, le contrat signé est remis au Porteur. Cette signature intègre notamment un horodatage qui permet de s'assurer que le certificat utilisé pour la signature était valable à la date de l'horodatage.

Ces informations sont portées dans le document signé et peuvent être vérifiées par le lecteur du PDF utilisé.

4.9.7. Fréquence d'établissement des LCR

Les LCR sont établies et publiées toutes les 24 heures. Elles sont également générées après chaque révocation et publiées sous un délai de 3 heures.

4.9.8. Délai maximum de publication d'une LCR

Après sa génération, la LCR est publiée dans un délai maximum de 3 heures.

4.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Aucun service OSCP n'est mis en œuvre.

4.9.10. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de Porteurs, les entités autorisées à effectuer une demande de révocation l'effectuent dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site Internet de l'AC.

4.9.13. Causes possibles d'une suspension

La présente Politique de Certification n'autorise pas la suspension de certificats.

4.9.14. Origine d'une demande de suspension

Sans objet.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16. Limites de la période de suspension d'un certificat

Sans objet.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

Les LCR / LAR sont des LCR au format V2 et sont publiées sur le serveur web HTTP de publication.

Les accès en lecture aux LCR / LAR sont publics.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

4.10.3. Dispositifs optionnels

Sans objet.

4.11. Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le Porteur avant la fin de validité du certificat, pour une raison ou une autre, ce dernier est révoqué.

4.12. Séquestre de clé et recouvrement

Il n'est pas procédé à un séquestre de clé.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5. MESURES DE SÉCURITÉ NON TECHNIQUES

Les exigences de ce chapitre sont référencées dans le document annexe suivant : « Mesures communes applicables à l'ICG ». Cette annexe est publiée au sein du même espace que la présente politique.

6. MESURES DE SÉCURITÉ TECHNIQUES

Ce chapitre présente un ensemble de mesures techniques concernant la sécurité de l'IGC. Des précisions et des compléments sur la mise en œuvre de ces mesures sont donnés dans la DPC.

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

1) Clés d'AC

La génération des clés de signature de l'AC a lieu lors d'une *Key Ceremony* (cérémonie de clés*).* Cette cérémonie se déroule sous le contrôle du maître de cérémonie et en présence d'un huissier de justice qui atteste du bon déroulement des opérations sensibles.

Remarque : les différents rôles participant à la *Key Ceremony* sont cités dans la DPC et sont nommés dans la documentation relative à la *Key Ceremony*.

2) Clés Porteurs générées par l'AC

Les clés des Porteurs sont générées par l'AC sur le serveur de signature. A la fin de l'opération de signature les clés sont détruites du serveur.

3) Clés Porteurs générées par le Porteur

Sans objet.

6.1.2. Transmission de la clé privée à son propriétaire

La clé privée n'est pas transmise au Porteur et reste sur le serveur durant toute l'opération de signature. Il n'est pas possible d'exporter cette clé.

6.1.3. Transmission de la clé publique à l'AC

Les informations nécessaires à l'établissement du certificat sont récupérées par l'application de signature et transmise via une CSR (Certificate String Request). L'échange avec la PKI se fait sous la forme d'une requête au format PKCS#10.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

La clé publique de l'AC est mise à disposition des utilisateurs via le certificat de l'AC qui est téléchargeable publiquement tel que défini au paragraphe 2.2.

L'empreinte (*Thumbprint*) du certificat de la clé publique de l'AC est également publiée permet d'en établir l'authenticité.

6.1.5. Tailles des clés

La taille des clés de l'AC est de 4096 bits.

La taille des clés des Porteurs pour un certificat de signature est de 2048 bits.

6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Voir le paragraphe 7 pour les paramètres et les algorithmes liés à la génération des bi-clés.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats de Porteurs et de LCR.

L'utilisation de la clé privée de Porteur et du certificat de signature associé est strictement limitée aux usages définis au paragraphe 1.4.1.1).

6.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

1) Modules cryptographiques de l'AC

Le module cryptographique utilisé par l'AC pour générer et mettre en œuvre sa clé de signature répond aux exigences de sécurité attendues par l'ETSI 102042. Il est certifié conforme vis-à-vis des critères communs EAL4+.

2) Dispositifs de création de signature des Porteurs

Le dispositif utilisé est le magasin de certificat du serveur de signature.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC, pour les opérations d'export ou d'import hors ou dans un module cryptographique, est assuré par les Porteurs de secrets de l'AC (voir paragraphe 6.1.1.1) où la présence de trois Porteurs de secrets est nécessaire pour mettre en œuvre la clé privée de l'AC.

6.2.3. Séquestre de la clé privée

Il n'est procédé à aucun séquestre de clés privées, qu'il s'agisse de clé privée d'AC ou de porteur.

6.2.4. Copie de secours de la clé privée

La clé privée des Porteurs ne fait pas l'objet d'une copie de secours.

La clé privée de l'AC fait l'objet d'une copie de secours stockée dans un coffre-fort.

6.2.5. Archivage de la clé privée

Ni la clé privée de l'AC ni celles des Porteurs ne font l'objet d'un archivage.

6.2.6. Transfert de la clé privée vers / depuis le module cryptographique

La clé privée de l'AC est générée et stockée au sein du même module cryptographique.

Le transfert de la copie de secours de cette clé se fait de manière chiffrée et conformément aux exigences du chapitre 6.2.4.

6.2.7. Stockage de la clé privée dans un module cryptographique

La clé privée d'AC sont stockées dans des modules cryptographiques répondant aux exigences de sécurité de l'ETSI 102042 pour le niveau NCP+ (Voir paragraphes 6.2.1 et 6.2.4).

6.2.8. Méthode d'activation de la clé privée

1) Clé privée d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via une carte d'administration et fait intervenir au moins trois Porteurs de secrets.

2) Clés privée des Porteurs

L'activation de la clé privée se fait via un appel Webservice, intégré dans le processus de signature. L'utilisation de la clé privée ne peut avoir lieu en dehors de ce cadre.

6.2.9. Méthode de désactivation de la clé privée

1) Clé privée d'AC

La désactivation de la clé privée de l'AC dans le module cryptographique est contrôlée via une carte d'administration et fait intervenir au moins trois Porteurs de secrets.

La clé privée d'AC pourra être désactivée manuellement dès l'apparition d'un incident lié à l'évolution de l'environnement du module cryptographique, notamment en cas d'arrêt ou de déconnexion du module.

2) Clés privées de Porteurs

Sans objet.

6.2.10. Méthode de destruction des clés privées

1) Clé privée de l'AC

La destruction de la clé privée de l'AC ne peut être effectuée qu'à partir du module cryptographique (HSM).

2) Clés privées de Porteurs

La destruction de la clé privée consiste à effacer de manière sécurisée la clé privée correspondante du magasin de certificat du serveur de signature. Cette destruction peut avoir lieu :

- A la fin du processus de signature
- Au cours du processus de signature si jamais une erreur est rencontrée, suite à la génération de la clé.

6.2.11. Niveau de qualification du module cryptographique et des dispositifs de création de signature

Voir paragraphes 6.2.1 et 6.2.4.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques d'AC et les clés publiques de Porteurs sont archivées dans le cadre de la politique d'archivage des certificats (voir chapitre **Erreur ! Source du renvoi introuvable.**).

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et certificats des Porteurs couverts par la présente Politique de Certification ont une durée de vie de 10 minutes.

La durée de vie de la bi-clé de signature de l'AC est de 30 ans.

L'AC veillera à n'émettre des certificats que si leur date de fin de validité est antérieure à la date de fin de validité du certificat de l'AC (cf. paragraphe **Erreur ! Source du renvoi introuvable.**).

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

1) Génération et installation des données d'activation correspondant à la clé privée de l'AC

La génération et l'installation des données d'activation des modules cryptographiques stockant la clé privée de l'AC ainsi que les copies de cette clé se font lors de la phase d'initialisation et de personnalisation de ces modules (lors de la *Key Ceremony*).

Les Porteurs de secrets sont identifiés dans l'un des documents opérationnels de l'AC décrivant les rôles et l'organisation.

2) Génération et installation des données d'activation correspondant à la clé privée du Porteur

Sans objet.

6.4.2. Protection des données d'activation

1) Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation générées par l'AC pour les modules cryptographiques ne sont connues que par les responsables des données d'activation, qui en assurent la confidentialité, l'intégrité et la disponibilité.

2) Protection des données d'activation correspondant à la clé privée du Porteur

Sans objet.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. Mesures de sécurité des systèmes informatiques

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques supportant les fonctions de l'Autorité de Certification et mis à disposition par l'OSC sont encadrés par les mesures de sécurité suivantes :

- Identification et authentification pour l'accès au système.
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles).
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur).
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels.
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès.
- Protection du réseau contre toute intrusion d'une personne non autorisée.
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
- Fonctions d'audits (non-répudiation et nature des actions effectuées).
- Gestion des reprises sur erreur.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

La DPC décrit les moyens mis en œuvre pour implémenter chacune de ces mesures de sécurité. Ces mesures de sécurité sont explicitées dans des règles opérationnelles de sécurité et dans des documents d'exploitation utilisés par l'OSC.

6.5.2. Niveau de qualification des systèmes informatiques

Sans objet.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurité liées au développement des systèmes

La conception et le développement des systèmes informatiques supportant les fonctions de l'Autorité de Certification ont été réalisés dans le respect des normes et standards applicables.

Les aspects sécurité ont notamment été pris en compte.

La documentation existe et évolue en fonction des mises à jour.

Les systèmes informatiques sont testés dans un environnement de test dédié avant mise en production.

6.6.2. Mesures liées à la gestion de la sécurité

Le Comité Sécurité Groupe valide les évolutions à apporter aux systèmes afin de maintenir le niveau de sécurité de l'AC.

Ces évolutions donnent lieu à des tests et à une mise à jour de la documentation et des procédures d'exploitation.

6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7. Mesures de sécurité réseau

L'architecture réseau des systèmes informatiques supportant les fonctions de l'Autorité de Certification respecte les bonnes pratiques en matière de sécurité réseau : cloisonnement, séparation des environnements (test / production), règles de filtrage, robustesse des équipements réseau, gestion de la haute disponibilité…

Des audits périodiques suivis d'actions correctrices sont menés pour lutter contre les vulnérabilités.

La DPC donne plus de détails sur les règles mises en œuvre pour chacun des composants de l'architecture technique.

6.8. Horodatage / Système de datation

L'Autorité de Certification date les journaux d'événements avant de les envoyer vers l'archivage (voir Politique d'Horodatage /système de datation).

Le mécanisme de synchronisation est basé sur des flux NTP. La précision est inférieure à 1 seconde.

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1. Profil des certificats

Les certificats de l'AC sont au format X509v3.

7.1.1. Certificat de l'AC BPCE AC Racine

Le certificat de l'AC racine contient les informations suivantes.

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil
DN Émetteur	CN = BPCE AC Racine OU = 0002 49345504200025 O = BPCE C = FR
DN Objet	CN = BPCE AC Racine OU = 0002 49345504200025 O = BPCE C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 30 ans
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 4096 bits>

2) Extensions de base

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature de certificat, Signature de Liste de Révocation de Certificats
Stratégies de certificat	O	N	Identificateur de politique = AnyPolicy
Points de distribution des LCR	O	N	HTTP : URL=http://pro.d00.pki01.bpce.fr
Contraintes de base	O	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=0

7.1.2. Certificat de l'AC BPCE AC CLIENT

Le certificat de l'AC racine contient les informations suivantes.

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil

DN Émetteur	CN = BPCE AC Racine OU = 0002 49345504200025 O = BPCE C = FR
DN Objet	CN = BPCE AC CLIENT OU = 0002 49345504200025 O = BPCE C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 30 ans
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 4096 bits>

2) Extensions de base

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature de certificat, Signature de Liste de Révocation de Certificats
Stratégies de certificat	O	N	Identificateur de politique = AnyPolicy
Points de distribution des LCR	O	N	HTTP : URL=http://xxx
Contraintes de base	O	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=0

7.1.3. Certificat de l'AC SIGNATURE Banque Populaire DC9-99

Le certificat de l'AC racine contient les informations suivantes.

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil
DN Émetteur	CN = BPCE AC CLIENT

	OU = 0002 49345504200025 O = BPCE C = FR
DN Objet	CN = AC SIGNATURE Banque Populaire DC9-99 OU = 0002 49345504200025 O = BPCE C = FR
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 30 ans
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 4096 bits>

2) Extensions de base

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Signature de certificat, Signature de Liste de Révocation de Certificats
Stratégies de certificat	O	N	Identificateur de politique = AnyPolicy
Points de distribution des LCR	O	N	HTTP : URL=http://pro.d00.pki01.bpce.fr
Contraintes de base	O	O	Type d'objet=Autorité de certification Contrainte de longueur de chemin d'accès=0

7.1.4. Certificat des Porteurs

Les certificats de signature des Porteurs contiennent les informations suivantes :

1) Champs de base

Champ	Valeur
Version	2 (= V3)
Numéro de série	Défini par l'outil
DN Émetteur	CN = AC SIGNATURE Banque Populaire DC9-99

	OU = 0002 49345504200025 O = BPCE C = FR
DN Objet	CN = Michel DURAND OU = 0002 < SIREN (9 chiffres) ou SIRET (14 chiffres) > (optionnel) O = <Raison sociale du Client> (optionnel) C = < FR ou pays du Client >
Valide à partir du	YYMMDDHHMMSS
Valide jusqu'au	YYMMDDHHMMSS + 10 minutes
Algorithme de clé publique	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Clé publique	<valeur de la clé publique RSA de 2048 bits>

Remarque : les contraintes sur le format du champ OU du DN sont compatibles avec le format des numéros SIREN ou équivalent étranger (pas de contrainte sur le nombre de caractères).

2) Extensions Standard

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Identificateur de la clé du sujet	O	N	<Valeur de Hachage>
Identificateur de la clé de l'autorité	O	N	<Valeur de Hachage>
Utilisation de la clé	O	O	Non répudiation (40)
Stratégies de certificat	O	N	Identificateur de politique = 1.3.6.1.4.1.40559.1.0.1.1.111.1.0
Points de distribution des LCR	O	N	http= http://pro.d00.pki01.bpce.fr
Contraintes de base	O	O	Type d'objet=Entité finale Contrainte de longueur de chemin d'accès=N/A

3) Autres extensions

Champ	Obligatoire (O/N)	Critique (O/N)	Valeur
Subject Alternative Name (rfc822)	N	N	mdurand@societe.fr

7.2. Profil des Listes de Certificats Révoqués (LCR)

Les LCR émises présentent les caractéristiques suivantes :

Durée et fréquence de mise à jour

- Durée de validité : 7 jours
- Périodicité de mise à jour : 24 heures

Informations et principes de base

La version de la LCR est v2.

L'émetteur de la liste de révocation a comme DN le nom de l'Autorité de Certification signataire de cette LCR.

Les certificats révoqués sont listés.

Les certificats sont nommés par leur numéro de série.

La date de révocation est précisée.

Extensions

- Numéro de la LCR
- Authority Key Identifier : identifiant de la clé publique de l'AC

Lieux de publication

URL http de publication : http://pro.d00.pki01.bpce.fr

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Les exigences de ce chapitre sont référencées dans le document annexe suivant : « Mesures communes, définitions et acronymes applicables à l'Infrastructure de Confiance Groupe (ICG) ». Cette annexe est publiée au sein du même espace que la présente politique.