Politique et pratiques de certification

AC Racine BPCE

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 180 478 270€.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13.

RCS n° 493 455 042.

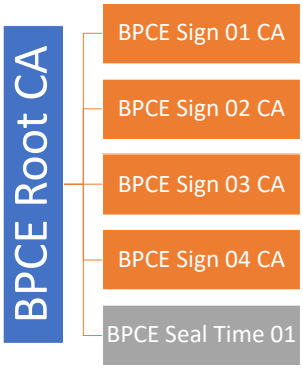
Table des matières

1 INTRODUCTION

1.1 Présentation générale

Le présent document, *Politique et pratiques de certification – AC Racine BPCE* présente les exigences spécifiques à la politique de certification de l'A.C. *BPCE Root CA* de l'I.G.C. de BPCE.

Cette A.C. est l'A.C. racine de la hiérarchie suivante :



Les mesures de sécurité applicables à l'A.C. racine sont décrites dans le document [MCOM].

Dans le cadre de cette P.C., les certificats émis sont des certificats d'A.C. finales.

1.2 Identification de la P.C.

Le numéro d'OID de la présente P.C. est : 1.3.6.1.4.1.40559.1.0.1.31.1.1.1

1.3 Usage des certificats

1.3.1 Domaines d'utilisation applicables

La présente A.C. ne délivre que des certificats d'A.C.

Une unique biclé est utilisée pour la signature des certificats des A.C. filles et de la L.A.R. sous la responsabilité de l'A.C.

1.3.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des biclés et des certificats sont définies au chapitre 4.5 ci-dessous.

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

Voir [MCOM].

2.1.1 Publication des L.A.R.

L'A.C. Racine publie la liste des autorités révoquées (L.A.R.). Ces L.A.R. sont publiées aux adresses suivantes :

http://pro.d00.pki02.bpce.fr/BPCERootCA.crl

http://pro.d01.pki02.bpce.fr/BPCERootCA.crl

http://pro.d02.pki02.bpce.fr/BPCERootCA.crl

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

Les noms choisis pour désigner les A.C. filles doivent être explicites.

Les noms des A.C. filles de l'A.C. Racine sont déterminés par celle-ci. Les A.C. sont identifiables par leurs DN, comme suit.

C=FR	Les certificats sont émis par une A.C. française
O=BPCE	Les A.C. filles sont rattachées au Groupe
OU=0002 493455042	SIREN de BPCE, précédé de « 0002 » et d'un espace (U+0020)
OI=NTRFR-493455042	SIREN de BPCE, précédé de « NTRFR » et d'un trait d'union (U+002D)
CN=...	Nom commun de l'A.C.

Les noms communs des A.C. de la hiérarchie sont les suivants :

- BPCE Sign 01 CA
- BPCE Sign 02 CA
- BPCE Sign 03 CA
- BPCE Sign 04 CA
- BPCE Seal Time 01

Le CN de l'A.C. Racine est : BPCE Root CA

3.1.1 Unicité des noms

Le DN du champ « *subject* » de chaque certificat d'A.C. fille doit permettre d'identifier de façon unique celle-ci au sein du domaine de l'A.C.

L'A.C. est garante de l'unicité des noms des A.C. filles.

3.1.2 Identification, authentification et rôle des marques déposées

L'A.C. s'engage quant à l'unicité des noms de ses A.C. filles, conformément au paragraphe précédent, ainsi qu'à résoudre tout litige portant sur la revendication d'utilisation d'un nom.

3.1.3 Validation initiale de l'identité

Agissant en tant qu'A.C., l'A.C. Racine est responsable et en charge de la validation de l'identité des A.C. filles.

3.1.4 Méthode pour prouver la possession de la clé privée

La possession de la clé privée est constatée durant la cérémonie des clés.

3.1.5 Validation de l'identité d'un organisme

Toutes les A.C. sont rattachées au groupe BPCE.

3.1.6 Validation de l'identité d'un individu

Les responsables des A.C. filles sont les mêmes que ceux de l'A.C. Racine.

3.1.7 Informations non vérifiées du porteur

Sans objet.

3.1.8 Validation de l'autorité du demandeur

Sans objet (cf. 3.1.6).

3.1.9 Certification croisée d'A.C.

Pas d'exigence en l'état actuel de la P.C.

3.2 Identification et validation d'une demande de renouvellement des clés

Le renouvellement d'une biclé donne lieu à une cérémonie de clés.

3.3 Identification et validation d'une demande de révocation

Une demande de révocation de clé pour une A.C. fille ne peut être effectuée et validée qu'à l'occasion d'une réunion du comité de gestion de l'I.G.C.

4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

Les demandes de certificat sont déposées et traitées dans le cadre d'une cérémonie de clés.

4.2 Traitement d'une demande de certificat

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

L'identification et la validation des demandes sont décrites dans le script de cérémonie des clés.

4.2.2 Acceptation ou rejet de la demande

Toutes les demandes sont acceptées lors de la cérémonie de clés, un refus ne pouvant se produire qu'en cas d'un incident durant celle-ci. L'incident sera alors consigné dans le procès-verbal de la cérémonie.

4.2.3 Durée d'établissement du certificat

Sauf incident, le certificat est établi à la fin de la cérémonie des clés.

4.3 Délivrance du certificat

4.3.1 Actions de l'A.C. concernant la délivrance du certificat

Se référer au script de la cérémonie des clés.

4.3.2 Notification de la délivrance du certificat au porteur (responsable d'une A.C. fille)

La remise du certificat doit se faire en mains propres (face-à-face).

Le certificat complet et exact doit être mis à la disposition de son porteur.

4.4 Acceptation du certificat

L'acceptation du certificat est formellement consignée dans le procès verbal de la cérémonie des clés.

4.4.1 Publication du certificat

Les certificats d'A.C. filles sont publiés sur le site Internet www.dossiers-securite.bpce.fr, et à une adresse indiquée dans leurs politiques de certification respectives (voir [PROFILS]).

4.4.2 Notification aux autres entités de la délivrance du certificat

Sans objet.

4.5 Usages de la biclé et du certificat

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

Pour les A.C. filles, l'utilisation des clés privées est limitée :

- À la signature des certificats
- À la signature des CRL.

Cet usage est indiqué explicitement dans les extensions des certificats (*keyCertSign, cRLSign*).

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

Les utilisateurs de ces certificats pourront vérifier la révocation ou l'expiration des certificats d'A.C. en analysant le contenu de ces certificats et la liste de révocation mise à disposition par la présente Autorité de Certification.

4.6 Renouvellement d'un certificat

Dans le cadre de la présente P.C., il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la biclé correspondante. Comme l'A.C. génère les biclés des A.C., elle garantit qu'un certificat correspondant à une biclé existante ne peut pas être renouvelé au sens du RFC3647.

Tout renouvellement s'effectue dans les mêmes conditions et selon les mêmes modalités que la demande initiale.

4.7 Délivrance d'un nouveau certificat suite à changement de la biclé

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont semblables aux opérations initiales.

4.8 Modification du certificat

La modification du certificat n'est pas admise.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'A.C. :

- Compromission, suspicion de compromission, perte ou vol de clé privée
- Cessation de l'activité de l'A.C. fille concernée
- Décision suite à un échec de contrôle de conformité
- Révocation de l'A.C. Racine
- Rupture technologique, nécessitant de procéder à la génération de nouvelles biclés (longueurs des clés trop faibles, algorithmes de hachage compromis).

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat d'A.C. sont les responsables de ces A.C.

4.9.3 Procédure de traitement d'une demande de révocation

Une fois la demande validée, l'A.C. Racine révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la publication sur l'état des certificats. L'information de révocation doit être diffusée au minimum via une L.A.R. signée par l'A.C. Racine. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'A.C.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat.

La révocation du certificat de l'A.C. Racine nécessite la réunion des porteurs de secrets pour procéder aux étapes de :

- Révocation du certificat d'A.C. et de l'ensemble des certificats d'A.C. filles
- Signature d'une nouvelle L.A.R.

L'ensemble des populations concernées par la révocation du certificat de l'A.C. Racine sera alors informé, soit directement, soit par une information sur le site institutionnel de l'A.C.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Sans objet.

4.9.5 Délais de traitement par l'A.C. d'une demande de révocation

Toute demande de révocation est traitée en urgence.

Il s'écoule au maximum 24 heures entre la demande de révocation par le responsable de l'A.C. et la publication de la nouvelle L.A.R. prenant en compte cette demande.

La révocation du certificat est planifiée immédiatement après la validation de cette procédure par le comité de pilotage et suite à la détection d'une des causes de révocation.

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

L'utilisateur d'un certificat émis par une A.C. fille est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

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

Les systèmes de révocation et de vérification ont un taux de disponibilité de 99,5 pour cent, et respectent une durée maximum d'indisponibilité de 4 heures.

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

Sans objet.

4.9.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.10 Exigences spécifiques en cas de compromission de la clé privée

La compromission de la clé privée d'un certificat d'A.C. fera l'objet d'une information claire sur le site de publication de l'A.C.

4.9.11 Suspension de certificats

La suspension de certificats n'est pas autorisée dans la présente P.C.

4.10Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de L.A.R. Ces L.A.R. sont des L.C.R. au format V2.

La L.A.R. est mise à jour annuellement et lors d'une révocation.

La L.A.R. est accessible à l'une des adresses suivantes :

http://pro.d00.pki02.bpce.fr/BPCERootCA.crl

http://pro.d01.pki02.bpce.fr/BPCERootCA.crl

http://pro.d02.pki02.bpce.fr/BPCERootCA.crl

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7.

5 ANNEXE : EXIGENCES DE SÉCURITÉ DU MODULE CRYPTOGRAPHIQUE DE L'A.C.

Dans la mesure où les certificats émis par la présente A.C. sont des certificats d'A.C. filles, les exigences de ce chapitre s'appliquent indifféremment à l'A.C. Racine et aux A.C. filles.

Le module cryptographique, utilisé par l'I.G.C. pour générer et mettre en œuvre les clés de signature de ses A.C. (pour la génération des certificats électroniques, des L.C.R. / L.A.R. et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les biclés des porteurs, doit répondre aux exigences de sécurité suivantes :

- garantir que la génération des biclés est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des biclés générées
- si les biclés de signature des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'A.C. et pendant leur transfert vers le dispositif de stockage matériel ou logiciel du porteur et assurer leur destruction sûre après ce transfert
- assurer la confidentialité et l'intégrité des clés privées de signature des A.C. durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie
- être capable d'identifier et d'authentifier ses utilisateurs
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur
- permettre de créer une signature électronique sécurisée pour signer les certificats générés par l'A.C., qui ne révèle pas les clés privées de l'A.C. et qui ne peut pas être falsifiée sans la connaissance de ces clés privées
- créer des enregistrements d'audit pour chaque modification concernant la sécurité
- si une fonction de sauvegarde et de restauration des clés privées de l'A.C. est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

6 RÉFÉRENCES

Les documents référencés sont les suivants :

- [CNIL] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
- [DIRSIG] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
- [SIGN] : Loi no 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

6.1 Documents normatifs

[ETSI_TSP]	ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.01.01_60/en_319401v020101p.pdf
[EIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE. http://www.europa.eu
[GDPR]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[RFC_3161]	Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) https://www.ietf.org/rfc/rfc3161.txt
[RFC_5816]	ESSCertIDv2 Update for RFC 3161 https://www.ietf.org/rfc/rfc5816.txt
[SOGIS-CRYPTO]	SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms – Version 1.0 – May 2016. http://sogis.org

6.2 Mesures communes

[MCOM] *Mesures communes*, publié à l'adresse www.dossiers-securite.bpce.fr

6.3 Profils de certificats et CRL

[PROFILS] *Description des profils de certificats et des CRL*, publié à l'adresse www.dossiers-securite.bpce.fr