SERVICES DE CONFIANCE EIDAS

PLAN DE FIN DE VIE

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.

SOMMAIRE

1 INTRODUCTION

1.1 Objet du document

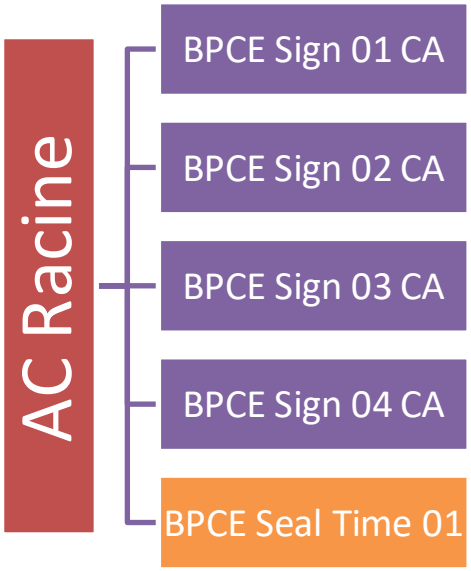
Ce document expose les étapes des procédures de cessation ou de transfert du service de certification de l'IGC.

La fin d'activité peut concerner une ou plusieurs AC simultanément, l'application de ce plan est à adapter selon le nombre et le niveau de certification des AC arrêtées.

1.2 Portée du document

Les services de confiance eIDAS, objets de ce document, sont déployés dans le cadre de solutions de signature électronique de document proposées par BPCE à ses clients. Ils assurent la délivrance de certificats X.509 certifiés *ETSI EN 319411-1*.

Les AC suivantes sont concernées par les présentes mesures :



Ces AC sont certifiées selon des normes ETSI **[EN 319 401]** et **[EN 319 411]** qui imposent des exigences vérifiées par ce plan.

Le plan de fin de vie détaille les dispositions mentionnées dans les politiques de certification des différentes AC (voir 1.3).

1.3 Documents de référence

[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 https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
[EN 319 401]	*ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*

	https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf
[EN 319 411]	*ETSI EN 319 411 V1.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;* https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.02_60/en_31941101v010202p.pdf
[ROOT]	Politique et pratiques de certification – AC Racine Document BPCE
[RR]	ICG – Qualification eiDAS, Rôles et responsabilités Document BPCE

2 CESSATION D'ACTIVITE DE L'AC

2.1 Généralités

La cessation d'activité d'une AC peut intervenir :

- Lors de l'expiration normale du certificat de cette AC ;
- Par révocation du certificat de l'AC (avec ou sans compromission de sa clé) ;
- Par transfert des porteurs vers une AC externe à BPCE.

L'AC considérée peut être l'AC Racine ou l'une des AC intermédiaires. La cessation de l'activité de l'AC Racine implique l'arrêt simultané de toutes ses AC filles.

Toute cessation d'activité est prise en charge par le comité de pilotage des services impactés, qui prépare alors les actions ci-dessous :

- Information des clients et des porteurs qui détiendront un certificat valide à la date de cessation d'activité de l'AC ;
- Génération d'une dernière LCR (*cf.* 3.1) ;
- Destruction des clés privées ;
- Maintien de la publication des informations de verification des certificats ;
- Conservation des éléments de preuve.

2.2 Cas de l'arrêt définitif du service

Que ce soit suite à l'expiration normale d'un certificat d'AC, après une compromission ou en corrolaire d'un transfert, un arrêt définitif d'une AC sans solution BPCE de poursuite à l'identique est une décision impactant fortement les clients du service.

Une telle décision ne peut être prise que par le responsable de l'AP (**[RR]**). Cette décision doit être prise le plus en amont possible de la date de cessation de l'AC, afin de permettre aux Clients et porteurs de trouver une solution de remplacement.

L'arrêt définitif implique :

- La recherche de solutions alternatives pour les clients actuels du service (*cf.* 3.5);
- L'information des tiers (*cf.* 3.6) ;
- L'arrêt des activités sous-traitées à des fournisseurs (*cf.* 3.7) ;
- L'organisation des procédures d'arrêt communes avec les autres cas de cessation d'activité.

2.3 Cessation d'activité de l'AC à expiration de son certificat

2.3.1 Date de cessation d'activité

La date de cessation d'activité est dans ce cas la date d'expiration du certificat de l'AC.

2.3.2 Continuité de l'activité juqu'à la cessation

L'émission de nouveaux certificats par l'AC cesse à partir du moment où la date de fin de validité du certificat émis dépasse la date de fin de validité du certificat de l'AC.

La possibilité de révoquer un certificat et a génération de listes de révocation se poursuivent juqu'à la date d'expiration du certificat de l'AC.

Les porteurs de certificats désirant renouveler leur certificat en fin de vie de l'AC sont orientés vers une nouvelle offre de certification équivalente chez BPCE, ou chez un autre prestataire (2.6).

2.3.3 Actions de finalisation de l'AC

Les actions nominales énumérées en 2.1 sont menées.

2.4 Cessation de l'activité de l'AC pour révocation de son certificat sans compromission

2.4.1 Date de cessation d'activité

La révocation d'un certificat d'AC peut être décidée par le comité de pilotage pour permettre par exemple un changement de caractéristiques des clés de l'AC sans qu'il n'y ait eu de compromission de la clé privée de l'AC.

La date de cessation est alors choisie par le comité de pilotage et peut être bien anticipée. La mise en place de la nouvelle est menée de front, et permet de proposer de nouveaux certificats aux porteurs impactés par le fin d'acrivité de l'AC visée.

2.4.2 Continuité de l'activité juqu'à la cessation

L'émission de nouveaux certificats par l'AC cesse à partir du moment où la date de fin de validité du certificat du porteur dépasse la date de cessation choisie.

Les porteurs de certificats désirant renouveler leur certificat sont orientés vers la nouvelle offre de certification équivalente chez BPCE, ou chez un autre prestataire (2.6).

La possibilité de révoquer un certificat et la génération de listes de révocation se poursuivent toujours juqu'à la date d'expiration du certificat de l'AC.

2.4.3 Actions de finalisation de l'AC

La nouvelle AC est mise en place avant la date de fin d'activité de l'AC.

Tous les certificats encore valides à la date de cessation d'activité de l'AC sont révoqués.

Les actions nominales énumérées en 2.1 sont menées.

2.5 Cessation de l'activité de l'AC pour révocation de son certificat après compromission

2.5.1 Date de cessation d'activité

La procédure est menée après détection d'un incident de sécurité menant à la suspicion ou la démonstration de la compromission de la clé privée de l'AC.

2.5.2 Actions de finalisation de l'AC

Les actions doivent alors être traitées dans l'urgence, et en prenant en compte les procédures de traitement d'incident déjà prévue (information des clients, porteurs et de l'ANSSI).

Les actions à mener sont :

- Révocation de tous les certificats émis par l'AC compromise ;
- Génération d'une dernière LCR (*cf.* 3.1) ;
- Révocation du certificat de l'AC ;
- L'information des clients et des porteurs de certificats venant d'être révoqués (*cf.* 3.6.1) ;
- Destruction des clés privées de l'AC (*cf.* 3.2);
- Maintien de la publication des informations de verification des certificats (*cf.* 3.3);
- Conservation des éléments de preuve (*cf.* 3.4).

Les opérations de communication, en particulier auprès des clients de l'AC, seront faites avec la plus grande précaution, pour prendre en compte l'impact potentiel pour eux et se mettre en capacité de limiter au maximum les impacts.

2.6 Transfert de l'AC à un autre PSCO

Au cours de la vie des AC, il se peut que l'entité propriétaire de l'AC fasse l'objet d'un rachat, d'une fusion, ou d'une transformation (changement de statut, de capital…).

La décision de transfert d'activité du service de certification ne peut être prise que par le responsable de l'AP (**[RR]**). Cette décision doit être prise le plus en amont possible de la date de fermeture prévue du service.

Préalablement au transfert d'activité, une étude doit être menée sur les conditions de transfert. S'il s'avère que les conditions d'exploitation sont identiques à celles en vigueur chez BPCE, les incidences sur l'activité de l'AC seront limitée à des impacts documentaires et contractuels, sans révocation ni renouvellement des certificats des porteurs. Sinon, des renouvellements anticipés des certificats des porteurs peuvent être envisagés, et la cessation de l'AC BPCE peut être décidée par une révocation de son certificat (cas de l'absence de compromission de sa clé) ou à sa date de fin de validité.

Cette décision est actée par le comité de pilotage des services impactés, qui prépare alors les actions déclinées dans ce plan de fin de vie :

- Définition des modalités de transfert de l'AC (transfert des clés privées de l'AC ou renouvellement anticipé des certificats sur l'AC du nouveau prestataire) ;
- Information des tiers (*cf.* 3.6) ;
- Organisation de l'arrêt de l'AC selon les modalités du transfert (reprise par le nouveau PSCO, cessation à expiration du certificat (*cf.* 2.3) ou révocation du certificat (*cf.* 2.4).

3 PROCEDURES DE FIN DE VIE

3.1 Génération de la dernière Liste de Certificats Révoqués

L'AC, pendant la période de fin de vie, continue de gérer la LCR dans les mêmes conditions et à la même fréquence qu'auparavant, et ce jusqu'à la fin de vie de l'AC.

Si, au moment de la cessation d'activité de l'AC, il subsiste des certificats encore valides, ils sont tous révoqués. Les éventuelles clés privées de porteurs conservées par BPCE sont alors détruites.

Pour les AC qualifiées ANSSI, il est obligatoire que l'AC génère une dernière LCR, avec comme fin de validité le 31 décembre 9999, 23h59m59s. Cette dernière LCR est publiée nominalement. Si l'AC n'est pas qualifiée auprès de l'ANSSI, cette action est facultative. Elle permet néanmoins de prolonger la durée de vie de l'AC, ce qui peut améliorer les résultats de certains outils de vérification de signature.

Dans le cas d'une AC BPCE, le processus pour les AC qualifiées ANSSI sera appliqué.

Pour rappel, aucune AC de l'IGC ne met en œuvre de service OCSP.

3.2 Destruction des clés privées

Dès que l'AC a généré sa dernière CRL, sa clé privée est détruite de façon définitive dans les HSM, ainsi que toutes ses sauvegardes.

Si le HSM virtuel dans lequel se trouvait la clé de l'AC est désormais vide, ce HSM virtuel est dépersonnalisé.

Un procès-verbal de destruction est établi par le responsable de l'AC.

3.3 Maintien de la publication des informations de verification des certificats

L'utilisation des certificats consiste à pouvoir en vérifier la validité, au minimum pendant toute la durée de vie de l'AC. Chaque AC publie ainsi sur des points de distribution précisés dans les Politiques de Certification et présents dans les certificats :

- Les certificats des Autorités de Certification ;
- Les listes de certificats révoqués (ARL et CRL).

Afin de respecter les engagements pris envers les clients, les porteurs et les utilisateurs de certificats, la publication de ces informations perdure, pour chaque AC, jusqu'à au minimum 1 an après la fin de période de validité du certificat de l'AC.

Les URL de ces points de distribution ne peuvent pas être modifiées dans les certificats déjà émis. Aussi, une solution technique doit être trouvée afin que les certificats et CRL puissent être téléchargées sur l'URL prévue y compris après un éventuel transfert ou arrêt de l'IGC BPCE.

3.4 Conservation des éléments de preuve

Une AC produit et conserve un ensemble d'éléments de preuve concernant les porteurs de certificats et l'exploitation de ses services. Ces preuves sont conservées pour une durée

de 10 ans à compter de l'émission d'un certificat par une AC. Les preuves archivées intègrent :

- Toutes les versions des CGU, politiques et pratiques des services de confiance
- Les accords contractuels entre les services de confiance et les souscripteurs
- Les dossiers d'enregistrement des porteurs de certificat
- La preuve d'acceptation des CGU par les souscripteurs
- Les certificats des AC et des autres composantes publiques de l'IGC
- Les listes de révocation émises par les AC, y compris le cas échéant la dernière CRL
- Les certificats émis pour les porteurs
- Les journaux d'évènements des différentes composantes (AC, AE, …)
- Les rapports d'audit

L'archivage de ces éléments est garanti, y compris après la fin de vie de l'AC, pour la durée prévue et pour 10 ans pour la dernière CRL émise.

3.5 Recherche de solutions alternatives

Lorsque BPCE arrête une AC sans la remplacer elle-même par une autre, le responsable des AC recherche pour les clients impactés d'autres prestataires de service de certification fournissant des certificats de même niveau. Pour cela, il consulte les listes de prestataires de confiance :

- Liste des PSCO qualifiés par l'ANSSI :

  https ://www.ssi.gouv.fr/en/regulation/eidas-regulation/trusted-list/
- Liste établie par LSTI :

  https ://www.lsti-certification.fr/index.php/fr/certification/eidas/eidas-trusted-list
- Liste au format XML sur le site de l'UE :

  https ://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

BPCE privilégiera les fournisseurs français mais pourra considérer les fournisseurs étrangers à défaut. BPCE communiquera à ses clients une liste des fournisseurs proposant un service équivalent à celui dont ils bénéficiait.

3.6 Information des tiers

3.6.1 Clients et Porteurs

BPCE s'engage à prévenir tous ses clients et les porteurs de certificats (excepté les porteurs de certificats éphémères) par courriel et par un message sur son site Internet au minimum au moins 3 mois avant la date effective de cessation d'activité de l'AC (sauf cas d'incident de sécurité).

BPCE expose à ses clients les solutions alternatives qu'il a identifiées et négocie avec eux les clauses contractuelles de cloture des contrats. En cas de transfert à une autre AC, les modalités exposées ci-après dans le document sont appliquées.

3.6.2 Organisme d'audit

BPCE prévient l'organisme d'audit ETSI qui a audité l'AC concernée de la fin de vie programmée de l'AC.

3.6.3 ANSSI

Lorsque l'AC arrêtée est qualifiée par l'ANSSI, il est nécessaire d'en informer sans délai l'ANSSI.

Dès que la décision d'arrêt du service est présentée en comité de pilotage, le responsable de l'AC est en charge d'en informer l'ANSSI. Selon les instructions du document **[QUAL_CONTACT]**, le responsable de l'AC adresse un courrier électronique à « qualification@ssi.gouv.fr » et indique le plan d'arrêt d'activité mis en place.

De plus, le responsable du service de l'AC pourra renforcer cette annonce par l'envoi d'un courrier postal à l'adresse suivante :

Agence nationale de la sécurité des systèmes d'information

Bureau qualification et agrément

51, boulevard de la Tour-Maubourg

75700 PARIS

3.7 Arrêt des activités sous-traitées

BPCE prévient ses fournisseurs de la cessation du service afin d'identifier et d'organiser, pour la date prévue, la fin des activités techniques et les modalités contractuelles en lien avec cet arrêt.

Note : À la date de rédaction du présent document, aucun sous-traitant n'est identifié dans la fourniture des services des AC.