Politique d'Acceptation Commune

PAC

Common Acceptance Policy

CAP

Réf. :
Version 3.1 Fr

SOMMAIRE

1. PREAMBULE

Les technologies Internet sont aujourd'hui au cœur des problématiques d'ouverture, d'interconnexion et de collaboration des systèmes d'information. Ces nouveaux concepts augmentent la portée de l'approche d'entreprise étendue, ensemble constitué de l'entreprise et de sa communauté : clients, partenaires (stratégiques et financiers), fournisseurs, Administration…

Les organisations cherchent à améliorer l'efficacité économique de leurs processus par la mise en œuvre d'applications de dématérialisation des données et des flux. Celles-ci permettent, au delà d'une réduction des coûts liés à la transformation du processus « papier » (charges de travail, coûts d'affranchissement, contraintes d'archivage…), d'améliorer la réactivité et la qualité de service et, surtout, de fluidifier les processus métier.

Ces applications de dématérialisation des flux sont naturellement multiples et concernent l'ensemble des secteurs de l'économie. Elles supposent de mettre en œuvre des espaces de confiance dans lesquels il faut pouvoir identifier et authentifier techniquement les différents acteurs et valider la qualité des transactions et de leurs émetteurs.

Le certificat électronique est un élément important dans la construction des espaces de confiance ; il permet à son porteur de s'authentifier (certificat d'identité), de signer (certificat de signature), d'établir une liaison sécurisée … Une application s'appuiera sur un certificat comme moyen d'identification de son porteur et de contrôle d'intégrité de l'information, dans des fonctions de contrôle d'accès ou de signature.

Les émetteurs de certificats sont aujourd'hui multiples (secteur bancaire, administration, entreprises…). Une application doit pouvoir accepter, en général, des certificats d'autorités de certification différentes ; dans un monde ouvert, il serait, en effet, à la fois trop coûteux et trop contraignant de demander à un même porteur d'obtenir un certificat par application.

Il est essentiel, lorsqu'un certificat est présenté à une organisation ou à une application, de connaître le niveau de sécurité de celui-ci (niveau 1, niveau 2…), le niveau d'engagement de l'Autorité de Certification associée et ses limites éventuelles (Assurance responsabilité, …).

Une Politique d'Acceptation est un ensemble de règles qui définit notamment les exigences auxquelles une Autorité de Certification doit se conformer pour que ses certificats soient acceptés par une communauté particulière et/ou une classe d'applications ayant des exigences de sécurité communes.

La Politique d'Acceptation Commune (PAC) a été définie, par le secteur bancaire français pour le secteur bancaire, afin de répondre aux besoins des promoteurs d'applications du secteur bancaire et permettre à ceux-ci d'utiliser, comme moyen d'identification et de signature, différentes familles de certificats (émis selon des politiques de certification différentes), en associant à ces certificats, un niveau minimum de qualité ; la Politique d'Acceptation fait, en particulier, intervenir la qualité des certificats acceptés et, donc, les Politiques de Certification (PC) qui définissent les conditions dans lesquelles sont émis ces certificats.

Le Comité PAC aura le souci de mettre à niveau la PAC, soit lorsque le marché fait évoluer ses exigences ou ses besoins, par exemple suite à une évolution de référentiel, soit lorsque c'est la communauté bancaire qui adapte ses exigences aux besoins bancaires. La nouvelle version PAC sera diffusée avec un délai suffisant de mise en œuvre pour permettre la réalisation des évolutions demandées.

En France, l'administration, en concertation avec l'ensemble des acteurs, a défini la PRIS/RGS (Politique de Référencement Intersectorielle de Sécurité / Référentiel Général de Sécurité) qui caractérise les éléments clés que doit respecter une PC, en fonction des niveaux de qualité des certificats auxquels elle est associée.

Les référentiels en vigueur cités dans ce document sont :

- La PRIS jusqu'au 19 mai 2016.
- le RGS V1 jusqu'au 1er juillet 2016.

Le CFONB, Comité Français d'Organisation et de Normalisation Bancaire, a adopté la PRIS/RGS comme référence commune pour le secteur bancaire en matière d'émission de certificats numériques. Cette référence à la PRIS/RGS permet de s'appuyer sur des travaux existants et de prévoir une coexistence et une cohérence avec les infrastructures de confiance mises en place dans le cadre des services en ligne et des télé-procédures de l'administration française.

L'obtention du référencement ou la fourniture d'une attestation de conformité à la PRIS/RGS d'une PC par un organisme accrédité COFRAC, ou équivalent, s'impose pour que l'AC soit référencée PAC. Il faut néanmoins tenir compte du caractère spécifique de la PRIS/RGS et pouvoir, chaque fois que nécessaire, intégrer d'autres référentiels nationaux ou européens.

La présente PAC sera mise à jour à l'aune du règlement européen 910/2014 dit eIDAS adopté le 23 juillet 2014 qui sera d'application à compter du 1er juillet 2016 une fois paru l'ensemble des actes d'implémentation et d'exécution.

La PAC définit un certain nombre de principes que les différents acteurs concernés par cette politique s'engagent à respecter.

La PAC répond aux besoins des promoteurs d'applications communes ou propres aux établissements bancaires et financiers déclarées comme acceptant des certificats PAC, mais peut être élargie à des applications spécifiques pour répondre à des besoins des :

- Établissements bancaires et financiers de pays tiers
- Partenaires tiers non bancaires (français ou de pays tiers)

La PAC n'adresse pas :

- Les principes de validation, qui sont définis au niveau du guide de bonnes pratiques en matière de validation des certificats de signature
- Les droits, les attributs et les limites associés au porteur, qui sont gérés au niveau des applications (et/ou, éventuellement, au niveau des certificats eux-mêmes)

Par ailleurs, la PAC permet à :

- Un émetteur de certificats attestés conformes à la PAC de plus largement diffuser ses certificats
- Un porteur de certificat d'élargir les cas d'usage de ses certificats

QUELQUES DEFINITIONS

Accepteur :

- L'organisation ou l'application qui, pour répondre à un niveau de risque évalué par le promoteur d'application, utilise des certificats attestés conformes à la PAC
- L'accepteur est, dans ce contexte de PAC, le promoteur de l'application utilisatrice de certificats

Application :

- Une application est un programme ou ensemble de programmes qui permettent de réaliser une ou plusieurs tâches

Applications communes :

- Applications communes aux établissements bancaires et financiers, ou dans la définition Banque de France, communes aux établissements de crédit et entreprises d'investissement (ex : applications COREP, COFINREP, BAFI).
  - Une application commune peut être une application développée spécifiquement par un établissement, répondant à un besoin commun et à une même finalité.
    - Les Applications communes incluent les applications interbancaires.

Applications propres :

- Applications propres à un établissement bancaire et financier ou à un établissement de crédit et entreprises d'investissement, autres qu'une Application commune (ex : gestion des titres).

Applications acceptant les certificats PAC :

Peuvent être déclarées acceptant les certificats PAC les applications

- communes aux établissements du secteur bancaire
- spécifiques répondant aux besoins des :
  - Établissements bancaires et financiers de pays tiers
  - Partenaires tiers non bancaires (français ou de pays tiers)
- propres à un établissement bancaire et financier adhérent à la PAC

Autorité de Certification (AC) :

- Organisme ayant la confiance d'une ou plusieurs entités pour gérer le cycle de vie d'un certificat : produire, distribuer, révoquer, suspendre, renouveler ou archiver des certificats numériques (Définition CFONB- 12/2003)
- ***Définition RGS*** : Au sein d'un prestataire de services de certification électronique (PSCE), une Autorité de Certification (AC) a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et identifiée comme tel, en tant qu'émetteur (champ « Issuer » du certificat), dans les certificats émis au titre de cette Politique de Certification.

Cadre de référence

Le cadre de référence définit les conditions applicables aux certificats permettant de s'assurer que leur conformité aux principes de la PAC.

Pour la France, le cadre de référence est la PRIS/RGS.

Certificat électronique :

- Attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne (article 2 de la Directive Européenne 1999/93/CE)
- Permet à son porteur de s'authentifier et de signer des transactions électroniques
- Est caractérisé par son niveau de sécurité associé (niveau 1, 2 ou 3)

Certificat qualifié :

- Un certificat qualifié est émis par un PSCE (Prestataire de Service de certification Électronique) qui répond aux exigences exprimées dans la directive européenne du 1999, transposée en droit français par la loi du 13 mars 2000 et le décret du n° 2001-272 du 30 mars 2001

Comité PAC

Ce comité est responsable de la définition de la PAC et de ses évolutions. Il définit le référentiel PAC et les procédures de traitement des demandes de conformité PAC.

L'adresse postale du Comité PAC :

CFONB

Comité PAC

18 rue Lafayette

75002 PARIS

Comité d'Enregistrement PAC

Ce Comité vérifie la conformité au référentiel PAC, défini par le Comité PAC, selon les procédures établies et prononce le référencement PAC d'une Autorité de Certification ou d'une famille de certificats, ou bien encore l'acceptation des certificats PAC par une application.

L'adresse postale du Comité PAC :

CFONB

Comité d'Enregistrement PAC

18 rue Lafayette

75002 PARIS

COFRAC :

- COmité FRançais d'ACcréditation : Association française chargée de l'accréditation des laboratoires, organismes certificateurs et d'inspection.

Conformité :

- La conformité concerne :
  - Une organisation, au travers d'une application acceptant les certificats PAC ou d'une AC ou d'une famille de certificats déclarée conforme ; l'organisation est alors adhérente à la PAC ;
  - Des AC ou des familles de certificats déclarées conformes ;
  - Des classes d'applications acceptant les certificats PAC.

Correspondant :

- Interlocuteur représentant de l'AC ou de l'application ayant mandat pour le compte de son établissement.

CRL ou LCR :

- Les CRL (Certificate Revocation List) ou LCR (Listes de Certificats Révoqués) répertorient les certificats qui ont été révoqués par l'autorité de certification.

eIDAS (electronic Identification And trusted Services) :

- Règlement UE 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 pour une entrée en application le 1er juillet 2016.

Émetteur :

- L'AC qui est en position d'émettre des certificats ou des familles de certificats.

Famille de certificats :

Ensemble de certificats, le cas échéant de différents niveaux, répondant chacune à une politique de certification bien déterminée de l'AC émettrice.

Niveau de qualité :

Le niveau de qualité d'un certificat est défini par :

- Le niveau de sécurité du certificat ;
- Le niveau d'engagement que prend l'organisation vis-à-vis des certificats dont elle est responsable.

Niveau d'engagement :

Le niveau d'engagement que prend l'organisation vis-à-vis des certificats dont elle est responsable est défini dans le cadre de la PC. L'organisation déclare que son niveau d'engagement comprend des garanties financières et des polices d'assurance adaptées à ses activités et aux responsabilités qui en découlent.

Niveau de sécurité :

3 niveaux de sécurité sont définis pour les certificats :

- Niveau 1 : Certificat logiciel, qui peut être délivré sans opération de face à face ;
- Niveau 2 : Certificat sur support matériel, délivré après une opération de face à face ;
- Niveau 3 : Certificat de très haut niveau de sécurité sur support matériel, pouvant justifier de la qualité de certificat qualifié permettant la mise en œuvre d'une signature avancée avec présomption de fiabilité.

OCSP :

(Online **C**ertificate **S**tatus **P**rotocol). Protocole de vérification en ligne du statut courant du certificat sans requérir de CRL.

Politique d'Acceptation :

- Une Politique d'Acceptation est un ensemble de règles qui définit notamment les exigences auxquelles une Autorité de Certification doit se conformer pour que ses certificats soient acceptés par une communauté particulière, notamment dans ce dossier cela concerne la communauté bancaire, et/ou une classe d'applications avec des exigences de sécurité communes

Politique de Certification (PC):

- La Politique de Certification, que l'Autorité de Certification a mise en place et s'engage à respecter, est un texte qui définit la qualité d'un certificat et, en particulier, son niveau de sécurité (niveau 1, 2, 3 équivalents aux niveaux 1, 2 ou 3 étoiles dans le référentiel PRIS/RGS)
- ***Définition extraite du RGS***: Ensemble de règles, identifiées par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment sur les porteurs et les utilisateurs de certificats.

Politique de Validation :

- La Politique de Validation est l'ensemble des textes qui établit les devoirs et responsabilités de l'entité (l'autorité de validation) chargée de la gérer.

Cette Politique de Validation pourra être mise en œuvre par une ou plusieurs entités, sur une ou plusieurs plates-formes physiques.
Les principales responsabilités de l'entité chargée de la validation vont porter sur :

- la définition de l'enchaînement des fonctions de gestion de la preuve selon l'application et le certificat utilisé ;
- l'administration des règles de gestion ;
- le contrôle de la chaîne de confiance pour le certificat ;
- le contrôle des données et des extensions ;
- le contrôle du statut du certificat ;
- la validation de la signature;
- le contrôle de la politique d'acceptation adoptée par l'application.

Prestataire de service de certification électronique (PSCE) :

- ***Définition PRIS/RGS*** : Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC, mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « Issuer » du certificat.

PRIS :

- PRIS : Politique de Référencement Intersectorielle de Sécurité, publiée initialement par l'ADAE (Agence de Développement de l'Administration Électronique) et reprise depuis par la DGME (Direction Générale de la Modernisation de l'État) ;
- Ce référentiel est historique. Il a été créé à l'origine pour permettre au secteur privé d'équiper les entreprises pour utiliser les télé-procédures faisant appel à la certification.

Programme :

- En informatique, un programme est une suite d'opérations prédéterminées destinées à être exécutées de manière automatique par un appareil informatique en vue d'effectuer des travaux et des calculs arithmétiques ou logiques ou simuler un fonctionnement.

Promoteur d'applications :

- Dans le contexte de la PAC, le promoteur d'applications a la charge d'une application qui utilise notamment des certificats référencés conformes à la PAC ;
- Le promoteur d'application est en position d'accepteur de certificats.

Référencement de conformité PAC

Une famille de certificats peut être référencée conforme à la PAC, suite à la demande faite par l'organisation supportant l'Autorité de Certification qui émet le certificat candidat à la conformité PAC.

Le référencement est délivré par le Comité d'Enregistrement PAC, selon les règles établies par le Comité PAC, au sein du document « Politique d'Acceptation Commune ».

RGS :

- RGS V1: Référentiel Général de Sécurité, publié par le décret n° 2010-112 du 2 février 2010, sous la responsabilité de la DGME et de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
- Le secteur bancaire français fait référence au RGS, successeur de la PRIS, sans qu'il y ait pour autant un alignement systématique de la PAC sur les versions futures du RGS ;
- Le Comité PAC étudiera, au cas par cas, l'intérêt de prendre en compte de nouveaux référentiels (en particulier, au niveau européen).

SSCD (Secure Signature Creation Device)

Support matériel cryptographique, utilisé par le porteur pour stocker et mettre en œuvre sa clef privée et dont le niveau de sécurité est défini par l'ANSSI.

Cf. : article 1 alinéa 6 du décret 2001-272 du 30 mars 2001.

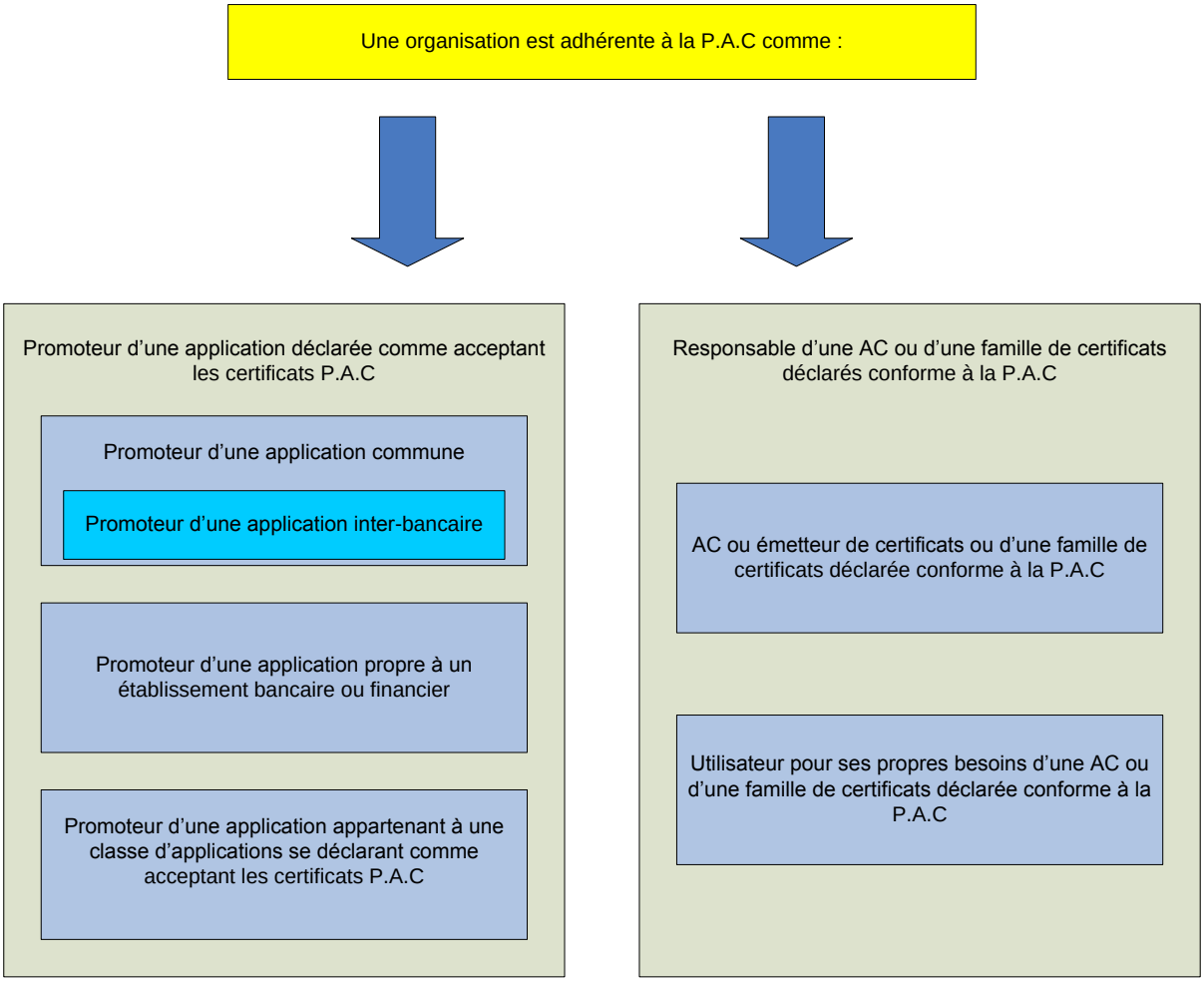
SCVP (Server based Certificate Validation Protocol)

Protocole standardisé (RFC 5055) permettant d'échanger les informations concernant la validité des certificats utilisés par une application. Cet échange protocolaire s'effectue entre l'application et un ou des serveurs de validation.

2. LA POLITIQUE D'ACCEPTATION COMMUNE

La Politique d'Acceptation Commune

La Politique d'Acceptation Commune (PAC) est définie par le secteur bancaire pour le secteur bancaire pour répondre aux besoins des promoteurs d'applications du secteur bancaire et leur permettre d'utiliser différentes familles de certificats (émis selon des politiques de certification différentes), en y associant, pour chacune de ces familles, un niveau minimum de qualité.



Il est indispensable de noter que la notion de conformité est différente pour les certificats et les applications utilisatrices :

- Les AC et les familles de certificats sont référencées conformes à la PAC ;
- Les applications utilisatrices se déclarent conformes, en faisant référence à la PAC.

Les objectifs de la PAC

La PAC est utilisée par:

- La profession bancaire dans la construction progressive d'un espace de confiance autour de la signature électronique, d'une démarche de multi-acceptance, et dans la recherche d'une meilleure maîtrise du risque ;
- Les promoteurs d'applications pourront ainsi :
  - Déterminer le niveau de qualité du certificat correspondant aux exigences de sécurité qu'ils jugeront nécessaires pour réduire ou couvrir leurs risques ;
  - Utiliser des certificats référencés conformes à la PAC.

Elle permet de renforcer le cadre de référence des espaces de confiance attachés à la Profession Bancaire.

La PAC permet aux différents acteurs de connaître:

- La liste des AC et des familles de certificats référencés appartenant ou non au secteur bancaire français.
- Les niveaux minima de sécurité et de qualité des certificats :
  - Niveau de sécurité 1, 2 ou 3 ;
  - Niveau d'engagement de l'émetteur.

La PAC concerne les certificats d'authentification, de signature et de chiffrement. Par référence à la PRIS/RGS, on acceptera des certificats « double usage » utilisés à la fois en authentification et en signature.

Les éléments constitutifs de la PAC

Pour faciliter les mises à jour, la PAC s'organise autour de :

- Un corps de document fixe qui précise :
  - Les critères que doivent respecter les familles de certificats et leurs émetteurs en fonction des niveaux de qualité ;
    - Politique de Certification, par référence à la PRIS/RGS ;
    - Niveau d'engagement de l'émetteur.
  - Les contrôles au minimum, que devront faire les applications sur les certificats
    - Ces contrôles sont obligatoires pour toutes les applications qui font référence à la PAC.
- Une série d'annexes à ce document :
  - Un rappel du contexte ;
  - Les exigences liées au niveau de sécurité du certificat ;
  - Les caractéristiques des certificats en fonction de leur niveau de sécurité ;
  - Les contrôles à effectuer sur le certificat dans le cadre de la PAC ;
  - Les documents de référence.
- Des listes publiées aux côtés de la PAC afin de préciser :
  - Une liste des AC et des familles de certificats référencées qui s'enrichira progressivement ;
    - Politique de Certification associée ;
    - Niveau d'engagement associé ;
    - Un correspondant ;
    - Une liste des applications acceptant les certificats PAC pour lesquelles un strict respect de la PAC est nécessaire.
  - Une liste des organisations adhérentes à la PAC:
    - Émettrices de certificats référencés PAC ;
    - Promoteurs d'applications acceptant les certificats PAC.
  - Une liste des sites officiels de publication.

Le corpus documentaire de référence

La PAC s'appuie sur :

- Les Politiques de Certification des banques (éventuellement des non banques) qui sont référencées PRIS/RGS, ou sont déclarées conformes à la PRIS/RGS suite à un audit d'une organisation agréée COFRAC, ou équivalent.
- Les documents définissant les gabarits des certificats
- Le cadre de référence déontologique défini par la PAC
  - Respect de la réglementation ;
  - Respect des principes déontologiques généraux définis dans le paragraphe « Principes de conformité ».

3. LES ELEMENTS CLES DE LA POLITIQUE COMMUNE D'ACCEPTATION

La PAC s'organise autour d'un ensemble de principes :

- Principes structurels
- Principes techniques
- Principes de qualité des certificats
- Principes d'organisation
- Principes de responsabilité
- Principes d'acceptation
- Principes de conformité
- Principes de publication
- Principes de défraiement
- Principes de renouvellement du référencement PAC

Tous les acteurs de la PAC s'engagent à strictement respecter ces principes.

Principes structurels

Les organisations

Une organisation sera dite adhérente à la PAC si, et seulement si, elle porte :

- Une application acceptant des certificats PAC
- Une AC ou une famille de certificats qui est référencée conforme à la PAC

En cas de suspicion (compromission des clés, fraude,…) le responsable de l'application et/ou l'AC en informe la communauté PAC via le Comité d'Enregistrement PAC, par tout moyen électronique (Information sur le serveur WEB du CFONB, mail de notification).

Les applications

Il est indispensable de très nettement séparer les différentes catégories d'applications :

- ***Les applications communes*** pour lesquelles les promoteurs de l'application commune concernée définiront, en relation avec les instances concernées, les niveaux de risque qu'ils sont prêts à accepter et les feront valider par la communauté
  - Le promoteur d'application s'engage à ce que ces applications communes respectent strictement les principes de la PAC, lorsque celle-ci utilise des certificats PAC.
- ***Des applications propres à un établissement bancaire ou financier adhérent à la PAC*** qui pourront utiliser la PAC comme référentiel
  - Chaque établissement reste maître, pour chacune des applications qui lui est propre, des risques qu'il est prêt à supporter et des familles de certificats qu'il acceptera
- Des applications pourront utiliser des certificats PAC sans être référencées mais elles ne pourront se réclamer de la PAC.
  - Le promoteur de cette application pourra a posteriori demander à être référencé PAC.

La Politique d'Acceptation Commune (PAC) est utilisée par un promoteur d'applications pour identifier les AC et les familles de certificats qui lui permettent de répondre au niveau de risque qu'il a évalué dans le cadre de son application.

L'analyse du niveau de risque associé à l'application et, en conséquence, le niveau de qualité des certificats à utiliser sont du strict ressort du promoteur d'applications.

Une AC référencée comme conforme à la PAC, ne pourra s'opposer à l'utilisation de ses familles de certificats par une application elle-même acceptant les certificats PAC.

Les AC et les familles de certificats

Pour être conforme à la PAC, l'AC ou la famille de certificats doit respecter l'une des règles suivantes :

- La Politique de Certification (PC) s'appuie sur le référentiel PRIS/RGS : l'AC étant qualifiée PRIS/RGS, elle doit produire l'attestation de qualification fourni, suite à un audit, par un organisme agréé COFRAC.

  On reconnaît, alors, le niveau de sécurité du certificat (niveau 1, 2 ou 3) en ligne avec les définitions de la PRIS/RGS.
- La PC s'appuie sur un référentiel autre que la PRIS/RGS
  - Si ce référentiel est déjà attesté conforme à la PAC (niveau de qualité de cette politique de référence attesté équivalent ou supérieur à celui de la PRIS/RGS), l'AC étant qualifiée sur ce référentiel, elle doit produire l'attestation de qualification fourni, suite à un audit, par un organisme agréé COFRAC ou équivalent.

    On reconnaît, alors, le niveau de sécurité du certificat (niveau 1, 2 ou 3) en ligne avec les définitions de ce référentiel.
  - Si ce référentiel n'est pas encore reconnu comme conforme à la PAC, il faudra d'abord définir les niveaux d'équivalence de ce référentiel avec les niveaux de la PAC. Ce nouveau référentiel avec ses écarts éventuels identifiés, sera intégré dans les référentiels PAC, après qu'un audit auprès d'un organisme agréé COFRAC ou équivalent ait été passé positivement. Le résultat de l'audit devra être fourni au Comité d'Enregistrement PAC.
- La PC ne s'appuie sur aucun référentiel et il n'y a pas de demande ou d'intérêt à créer un nouveau référentiel. L'AC doit fournir le résultat positif d'un audit réalisé auprès d'un organisme agréé COFRAC ou équivalent, selon le référentiel PAC.

Dans tous les cas, la PC, associée à l'AC ou à la famille de certificats, doit également respecter la PAC.

La conformité d'une AC ou d'une famille de certificats s'organisera autour de :

- Un audit de la PC associée, lorsque celle-ci ne s'appuie pas sur un cadre de référence (PRIS/RGS ou référentiel de niveau équivalent déjà reconnu par le comité PAC) ;
- La solidité financière de l'organisation émettrice ;
- Une évaluation du niveau d'engagement de l'organisation responsable ;
- La validation du respect des règles de conformité par l'organisation.
- La fourniture, le cas échéant, d'un certificat de recette sur support matériel, afin de vérifier l'interopérabilité avec les applications conformes à la PAC, (cf. Annexe 1).

Principes techniques

Fonctions 'Émetteur de certificats'

La PAC définit 3 niveaux de sécurité pour les certificats (niveau 1, 2 ou 3), sur les principes définis par l'administration française dans le cadre de la PRIS/RGS. Ces 3 niveaux sont spécifiques à la PAC et au domaine bancaire ; ils pourront, en particulier, diverger des définitions PRIS/RGS.

Chaque niveau constitue un sur ensemble du niveau inférieur ; ainsi, un certificat attesté conforme au niveau 2 pourra être utilisé aussi bien dans des applications demandant un niveau 1 qu'un niveau 2.

L'élément fondamental permettant de définir le niveau de sécurité d'un certificat est la Politique de Certification à laquelle il est associé.

Un promoteur d'applications acceptant les certificats d'une AC conforme à la PAC est assuré du niveau minimal de sécurité du certificat.

En dehors des contraintes liées à la conception et à la gestion de l'AC, les certificats de niveau 1, 2 et 3 seront, principalement caractérisés par les 3 critères suivants :

	Certificat niveau 1	Certificat niveau 2	Certificat niveau 3
Principe de remise	Tout moyen de remise offrant un minimum de sécurité peut être envisagé (face à face ou enregistrement à distance)	La remise se fait nécessairement en face à face	La remise se fait nécessairement en face à face
Dispositif de confinement du certificat	Certificat logiciel	Certificat sur support matériel cryptographique.	Certificat sur un équipement SSCD
Taille des clés[1]	RSA 1024 ou 2048 bits	RSA 2048 bits[2]	A minima, RSA 2048 bits

Pour plus d'information, voir l'annexe 4 et 5 du présent document.

La Politique de Certification (PC)[3] de l'AC candidate doit :

- s'appuyer sur un référentiel reconnu par le comité PAC comme permettant de s'assurer de la qualité des certificats émis :
- préciser les key Usages des certificats

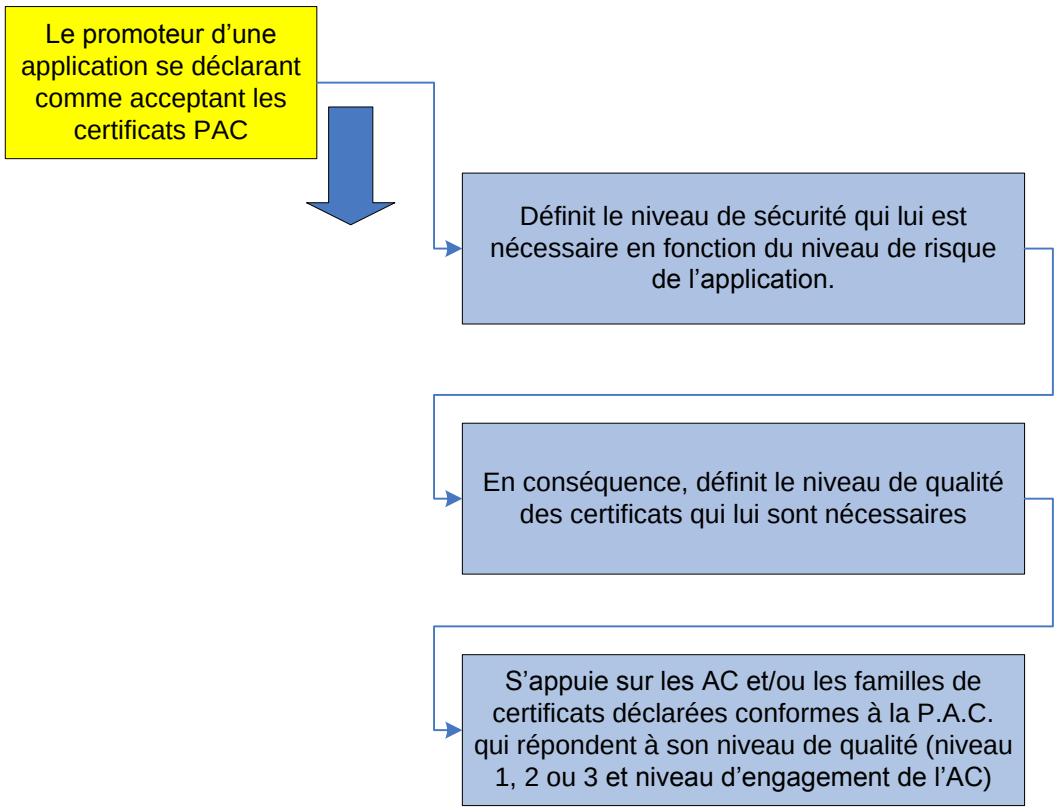
[1] L'émission de certificats avec des tailles de clé spécifiques est régie par l'ANSSI en France aujourd'hui.
[2] Une longueur de clef de 1024 bits est toléré dans une phase transitoire jusqu'au prochain renouvellement du certificat.
[3] La PC peut être spécifique à l'organisation

Le fait qu'une AC soit qualifiée/référencée PRIS/RGS permet de s'assurer du niveau de sécurité du certificat, sans que le Comité d'Enregistrement PAC n'ait à commanditer un audit spécifique et approfondi.

D'autres cadres de référence (notamment ceux de pays tiers) sont acceptables pour permettre de juger du niveau de sécurité du certificat. Dans ce cas, l'AC doit fournir le résultat de l'audit réalisé par un cabinet agréé COFRAC (ou équivalent pour les pays autres que la France) afin de s'assurer que ces référentiels permettent d'obtenir des niveaux de qualité au moins équivalents à ceux que définit la PRIS/RGS (NB : dans ce dernier cas, les frais seront à la charge de l'AC en quête de l'agrément PAC).

Fonctions 'promoteur d'applications'

Le promoteur de l'application mène une analyse de risques et définit le niveau de qualité des certificats (authentification et/ou signature, chiffrement) qui lui sont nécessaires.



Utilisation du certificat d'identification

Domaine	Certificat niveau 1	Certificat niveau 2	Certificat niveau 3
Contextes type d'utilisation	Les risques de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou biens ou pour pouvoir démontrer l'origine des données existent, mais sont moyens	Risques forts de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou biens ou pour pouvoir démontrer l'origine des données	Risques très forts de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou biens ou pour pouvoir démontrer l'origine des données

Utilisation du certificat de signature

Domaine	Certificat niveau 1	Certificat niveau 2	Certificat niveau 3
Contextes type d'utilisation	Les risques de tentative d'usurpation d'identité et de perte d'intégrité pour pouvoir signer indûment des données existent, mais sont moyens	Risques fort de tentative d'usurpation d'identité et de perte d'intégrité pour pouvoir signer indûment des données	Risques très forts de tentative d'usurpation d'identité et de perte d'intégrité pour pouvoir signer indûment des données

Utilisation du certificat de confidentialité

Domaine	Certificat niveau 1	Certificat niveau 2	Certificat niveau 3
Contextes type d'utilisation	assurer la confidentialité des données que ce soit lors de leur transport, ou de leur stockage Les risques de perte de confidentialité sont moyens et les besoins de recouvrement ne sont pas nécessaires	assurer la confidentialité des données stockées Les risques de perte de confidentialité et les besoins de recouvrement sont forts.	assurer la confidentialité des données stockées Les risques de perte de confidentialité sont très forts et le recouvrement est imposé.

Nota : Le certificat de confidentialité permet principalement d'échanger les clefs utilisées par les algorithmes de chiffrement de données tels que 3DES ou AES. Il peut également servir à chiffrer des données mais avec un niveau de performance qui limite son usage à des domaines spécifiques.

Le promoteur de l'application définit le niveau de sécurité nécessaire et s'appuie sur les AC et familles de certificats conformes à la PAC, en ligne avec ses besoins. On utilisera, en général, les certificats de :

- Niveau 1 pour se protéger contre des risques de niveau moyen ;
- Niveau 2 en face de risques élevés ;
- Niveau 3 en face de risques forts.

Le promoteur d'applications s'engage à ce que la politique de sécurité associée à l'application définisse un cadre technique, procédural et juridique prenant en compte le niveau de qualité des certificats et :

- l'utilisation de dispositifs sécurisés (SSCD), si nécessaire ;
- la vérification d'usage sur le certificat, en fonction des exigences de l'application (structure, key usage, date de validité…) ;
- la consultation du statut du certificat (CRL, OCSP, SCVP, …) ;
- l'utilisation d'outils certifiés, le cas échéant ;
- le référencement PAC de la famille de certificats de l'AC utilisée par l'application,
- …

Le promoteur d'applications s'assure des contrôles de sécurité à effectuer tels qu'habituellement définis dans la pratique en matière de certification et de transactions électroniques.

Le promoteur d'applications a la charge de s'assurer de la qualité du certificat tel que défini ci-après et de gérer la validation de celui-ci ; le contrôle des droits, des habilitations et des limites d'usage des différents utilisateurs ne font pas partie de la PAC.

Principes de qualité des certificats

Une organisation émettrice de certificats s'engage à respecter les principes suivants pour les AC et/ou familles de certificats qu'elle souhaite voir référencer :

- La Politique de Certification des AC et/ou familles de certificats respectant, *a minima*, les principes de la PRIS/RGS
  - La structure du certificat
    - Respect du format X509 V3
    - Respect des extensions (en particulier, au niveau des extensions critiques)
    - Respect des principes d'identification
  - La longueur des clés
  - Les principes de confinement du certificat :
    - Certificat logiciel (limité au niveau 1)
    - Certificat sur support matériel cryptographique, solution technique nécessaire pour un niveau 2 ou 3, (carte à puce, token…)
    - La durée de vie du certificat (et des clés d'AC de signature)
  - Les principes d'enregistrement et de distribution
    - Règles de nommage
    - Validation initiale de l'identité
    - Traitement de la demande de certificat
    - Délivrance en face à face pour des certificats de niveau 2 ou 3
  - La gestion du cycle de vie des certificats
    - Renouvellement et délivrance d'un nouveau certificat
  - La fonction d'information sur l'état des certificats
    - Gestion des CRL et/ou des requêtes/réponses OCSP
  - Les principes de gestion de l'AC
  - Les principes de sécurité et de gestion des éléments cryptographiques associés à l'AC

- Niveau d'engagement sur ses différentes familles de certificats.

Une application acceptant un certificat PAC doit, *a minima*, au niveau du contrôle de la qualité du certificat, respecter les principes suivants :

- Contrôle du gabarit, de la date de validité, des extensions
- Contrôle du statut du certificat

Principes d'organisation

Les correspondants

L'organisation adhérente à la PAC nomme :

- Un responsable et un suppléant pour l'ensemble des AC et des familles de certificats reconnues conformes, qui sera en mesure de :
  - Aider ses partenaires dans la mise en œuvre des certificats conformes
  - Être rapidement informé en cas d'incident
- Un responsable et un suppléant pour l'ensemble des applications acceptant des certificats PAC, auquel les partenaires pourront faire appel sur des problématiques d'usage des certificats.

La publication

Voir annexe 2

Principes de responsabilité

Les engagements que prend une AC sont définis dans sa Politique de Certification.

Incidents

Une organisation doit immédiatement prévenir le Comité d'Enregistrement PAC lors de la survenue d'un incident :

- Au niveau de l'émission d'un certificat
  - Secrets corrompus
  - Incidents au niveau de l'enregistrement
  - …
- Au niveau des contrôles effectués par une application acceptrice

Les obligations de l'organisation et les procédures à suivre en cas d'incident sont précisées par la PC associée à la famille de certificats ou par tout document y faisant référence.

Les changements d'organisation impactant la PAC doivent être communiqués aux adhérents.

Responsabilité du porteur

La responsabilité du porteur n'est pas régie par la PAC mais directement par l'émetteur de certificats (l'AC) dans sa relation avec le porteur.

Responsabilité d'un émetteur

Un émetteur de certificats déclarés conformes PAC doit, pour les AC et les familles de certificats, strictement respecter :

- Les PC associées aux AC et familles de certificats déclarées comme conformes
- Les critères de solidité financière de l'organisation
- Les niveaux d'engagement sur les certificats
- Les principes de sécurité, de responsabilité et de conformité définis dans la PAC
- Les principes de réciprocité

Responsabilité d'un promoteur d'applications

Un promoteur a la charge de :

- Définir le niveau de risque de son application et le niveau de qualité des certificats utilisables
- Respecter les contrôles de validité des certificats

La gestion des litiges

La gestion des conflits potentiels et des litiges se fait directement entre l'établissement accepteur et l'émetteur de certificats concerné.

Il ne peut être fait référence à la PAC en cas de litige par :

- Une organisation non adhérente à la PAC
- Une organisation adhérente pour des applications non déclarées conformes à la PAC.

Principes d'acceptation

Un tiers promoteur d'une application acceptant les certificats PAC pourra utiliser ces derniers sans que nécessairement tous les certificats acceptés par la dite application, ne soient conformes à la PAC.

Principes de conformité

L'organisation qui déclare une application conforme à la PAC s'engage à respecter *a minima* les principes suivants :

- La référence à la PAC et l'usage des certificats s'y rapportant au sein d'applications utilisatrices, ne peuvent être réalisés pour des applications considérées par la réglementation qui y est applicable, comme illégales ou illicites. Ce principe constitue un principe de base essentiel, l'organisation déclarant pleinement s'y conformer.
- Il incombe à l'organisation de s'assurer de la conformité de ses applications à la réglementation en vigueur. Le référencement ne peut en aucun cas être considéré comme attestant d'un contrôle de conformité par le Comité d'Enregistrement PAC. Ce contrôle relève de la seule responsabilité de l'organisation.

En cas de manquement à ces principes, le Comité d'Enregistrement PAC a la possibilité de demander à l'organisation qu'une application utilisatrice ne fasse pas référence à la PAC et qu'elle supprime en conséquence la possibilité d'usage des certificats s'y rapportant.

Il en est de même si c'est l'AC qui ne respecte pas les règles de la PAC.

Principes de publication

Peuvent utiliser la référence à la PAC ainsi que tout signe distinctif ou autre dénomination :

- les AC et les familles de certificats référencées PAC
- les promoteurs d'applications faisant partie d'une organisation adhérente à la PAC

Le cas échéant, une convention sera prévue à cet effet.

Le site du CFONB est le site de publication de référence de :

- La PAC dans sa version en vigueur et son historique de publication
- La liste des cadres de référence
- La liste des organisations adhérentes à la PAC (en référence à une application ou une AC ou une famille de certificats déclarée conforme)
- La liste des applications acceptant des certificats PAC
- La liste des AC et familles de certificats référencées PAC, commercialisées
  - Les niveaux minimum de sécurité et de qualité des certificats associés (niveau 1, 2, 3)
  - Un lien vers la Politique de Certification de l'AC (signée par l'AC afin d'en assurer l'intégrité technique)
- La liste des interlocuteurs et de leurs suppléants :
  - Responsables des AC et familles de certificats référencées PAC (un seul responsable et un suppléant par organisation)
  - Promoteurs d'applications

On se limitera à communiquer le nom du correspondant et l'adresse e-mail du responsable d'AC et du promoteur d'applications.

Principes de défraiement

Les travaux du Comité PAC et du Comité d'Enregistrement PAC ne font l'objet d'aucun défraiement :

- Par contre, toutes les charges d'audit, s'il y a lieu, sont supportées par les organisations faisant leur demande de référencement.

Principes de renouvellement du référencement PAC

Le référencement PAC est délivré pour une période d'**un an**.

Chaque année, avant la date anniversaire du référencement obtenu, l'AC doit fournir :

- une attestation de l'assurance Responsabilité Civile Professionnelle
- et
  - soit l'attestation de conformité correspondant à son cadre de référence
  - soit l'attestation du résultat positif d'un audit de contrôle de l'AC par rapport au référentiel PAC, si l'AC n'appuie pas son émission de certificats sur un cadre de référencement reconnu.

Dans le cas où le cadre de référence initialement utilisé par l'AC a évolué (par exemple nouvel OID), ce n'est pas un renouvellement qui doit être fait. Une nouvelle demande de référencement PAC doit être initiée.

La demande de renouvellement est à adresser au Comité d'Enregistrement PAC par courrier en remplissant la demande de renouvellement, accompagné de l'attestation telle que décrite ci-dessus.

4. LES PRINCIPES DE DEMANDE DE REFERENCEMENT

Les principes de référencement

On peut être adhérent à la PAC en tant que :

- Promoteur d'applications acceptant des certificats PAC
- Émetteur de certificats pour les AC et les familles de certificats déclarées conformes

A ce titre les promoteurs d'application ou les émetteurs de familles de certificats déclarés conformes ne peuvent se réclamer d'une conformité à la PAC que pour les seules applications ou familles de certificats référencées.

Seules les applications ou familles de certificats conformes à la PAC seront publiées sur le site du CFONB. Tous ceux qui ne sont pas référencés ne peuvent se prévaloir de la conformité PAC.

Lors de son adhésion, le demandeur d'un référencement précise le périmètre organisationnel concerné par la PAC, en termes de filiales, organismes mutualistes… Une organisation adhérente prévient le Comité d'Enregistrement PAC dans le cas où une modification de son périmètre organisationnel ou une modification sociale (par exemple changement de dénomination sociale) peut impacter le respect de la PAC.

Déclaration de référencement d'une application

Les certificats référencés PAC sont utilisés par des promoteurs des :

- Applications communes au secteur bancaire et financier français
- Applications propres à un établissement bancaire et financier déclaré conforme
- Applications appartenant à une classe d'applications déclarée conforme

Toute nouvelle application sera déclarée au Comité d'Enregistrement PAC qui mettra à jour la liste des applications acceptant des certificats PAC sur le site WEB du CFONB.

Une application pourra être déclarée conforme à la demande d'un promoteur d'applications :

- Du secteur bancaire et financier d'un pays tiers
- Du secteur non bancaire et financier (français ou d'un pays tiers)

Cette demande sera présentée au Comité d'Enregistrement PAC qui étudiera la qualité de la classe d'applications, en fonction des principes précédents énoncés, et sur la base d'une analyse documentaire.

Référencement d'une famille de certificats

En support de sa demande de référencement d'une famille de certificats, une organisation présente les AC et familles de certificats qu'elle entend faire déclarer conformes

Ces familles de certificats :

- Respectent la PRIS/RGS
- Ou ont été analysées par un auditeur référencé par un organisme tel que le COFRAC en France (www.cofrac.fr) ou l'European cooperation for Accreditation (EA).

  En dehors des organismes ci-dessus, les demandes seront étudiées au cas par cas.

Le processus de contrôle de référencement

Principes associés au dépôt de candidature

Les différents documents présentés pour la demande de référencement sont rédigés en français ou en anglais. Dans le cas où les documents ont été traduits en anglais, il est demandé que la qualité de la traduction soit attestée par un organisme indépendant reconnu dans son secteur d'activité et ayant une bonne connaissance du vocabulaire du métier de la certification électronique.

Processus associés au dépôt de candidature

Le processus de dépôt de candidature s'organise autour des étapes suivantes :

- Constitution du dossier de candidature organisé autour des documents suivants :
  - Références de la famille de certificats que l'organisation souhaiterait voir déclarer conforme
  - PC associées
  - Cadre de référence associé
- Envoi par l'établissement demandeur du dossier de demande de référencement au Comité d'Enregistrement PAC
- Accusé réception du dépôt envoyé par le Comité d'Enregistrement PAC
- Dans le cas des AC non-conformes PRIS/RGS, un audit doit être déclenché à l'initiative de l'organisation et sous sa responsabilité (la qualité de l'audit et la durée de la mission sont définis par le demandeur, sans que le Comité d'Enregistrement PAC ne prenne un quelconque engagement)
- Analyse de la demande, et dans le cas des AC non-conformes PRIS/RGS, en s'appuyant, sur le rapport d'audit.

Analyse de la candidature

La demande de référencement se fait pour:

- Une ou plusieurs fonctions émettrices (une ou plusieurs AC, une ou plusieurs familles de certificats, certificats de niveau 1, 2 ou 3) (attestation de conformité)
- Une ou plusieurs applications (déclaration)

Pour engager le processus de reconnaissance de référencement, l'organisation doit présenter :

- Pour un émetteur de certificats (voir dossier de référencement disponible sur site WEB du CFONB) :
  - La liste des AC et des familles de certificats
    - Les PC associées (et si nécessaire, les documents auxquels elles renvoient)
    - Son positionnement par rapport aux cadres de référence retenus pour les PC
    - Les attestations éventuellement déjà obtenues d'organismes officiels ou d'auditeurs attestant de la conformité de la famille de certificats à un référentiel d'audit
    - Les garanties financières associées aux certificats telles que précisées dans la PC, les polices d'assurance associées ou des documents complémentaires.

      Le Comité d'Enregistrement PAC analysera l'existence matérielle de ces documents et non pas leur consistance
    - Les coordonnées du correspondant et de son suppléant (nom et adresse email)

- Pour un accepteur (promoteur d'applications) :
  - Les classes d'applications candidates
  - Les coordonnées du correspondant (nom et adresse email)

Une organisation reconnue conforme (adhérente à la PAC) doit obtenir l'approbation du Comité d'Enregistrement PAC pour intégrer dans son périmètre :

- Une nouvelle AC ou famille de certificats
- Une nouvelle classe d'applications

L'analyse détaillée de la Politique de Certification du candidat est un élément clé du processus d'adhésion et du formulaire de référencement associé.

Les coûts d'audit sont à la charge de l'organisation demandant son adhésion, lorsque la PC n'est pas conforme au cadre de référence PAC (PRIS/RGS ou référentiel agréé de niveau équivalent) que ce soit pour l'évaluation de la PC du candidat ou pour l'évaluation de la PC de référence à laquelle renvoie sa propre PC.

L'adhérent s'engage à respecter strictement le cadre de la PAC.

Recours en cas de rejet de la candidature

Dans l'hypothèse où une organisation aura vu sa candidature à la demande de référencement refusée, elle pourra soumettre à nouveau sa candidature, après avoir corrigé les éléments ayant conduit à refuser sa candidature.

Le candidat est libre de présenter à nouveau sa candidature, en expliquant et mettant en valeur les évolutions qu'il propose par rapport à sa demande antérieure.

Gestion des évolutions

Il faut distinguer les évolutions provoquées par :

- Le Comité PAC qui fait évoluer le cadre de référence PAC
- L'organisation responsable de l'application déclarée conforme ou de l'AC ou de la famille de certificats attestée conforme

Lorsque le Comité PAC est responsable de l'évolution, il est à sa charge de définir le niveau de l'évolution (niveau mineur, ne demandant pas un nouveau référencement ou niveau majeur supposant un nouveau référencement des AC ou des familles de certificats)

- En cas de modification du cadre de référence PAC (par exemple, la suppression d'un référentiel reconnu, suite à une défaillance sécuritaire), le Comité d'Enregistrement PAC est tenu d'aviser les organisations reconnues conformes à la PAC sur le délai de prise en compte. Ce délai de prise en compte du nouveau référentiel devra être suffisant pour permettre au marché de se mettre en conformité. Les organisations reconnues devront s'être alignées sur le nouveau référentiel d'après le délai fixé pour sa mise en œuvre effective.
- Les organisations devront présenter leur demande de référencement ou de renouvellement de référencement sur le nouveau référentiel. Le délai de fin d'utilisation de l'ancien référentiel sera précisé à parution du nouveau référentiel, par le Comité PAC.

.

En cas d'évolution de la PAC, le comité PAC a, vis-à-vis du Bureau du Conseil du CFONB, la charge de :

- L'informer dans le cas d'une modification mineure
- Demander son approbation, dans le cas d'une évolution majeure

Dans le cas où l'évolution est provoquée par l'organisation adhérente, celle-ci est responsable de la qualification du niveau d'évolution (mineure ou majeure, une évolution majeure supposant en particulier, un changement de l'OID de la PC associée à l'AC ou la famille de certificats)

Lorsque l'organisation adhérente est responsable de l'évolution, il faut tenir compte des cas suivants :

- Arrêt de fonctionnement d'une application déclarée conforme ou d'une AC ou d'une famille de certificats attestée conforme ; l'organisation prévient le Comité d'Enregistrement PAC, 3 mois avant l'arrêt d'activité, sauf cas de force majeure. Dans ce dernier cas, l'organisation fera ses 'meilleurs efforts' pour prévenir dès que possible le Comité d'Enregistrement PAC

- Modifications mineures (donc sans évolution de l'OID) des conditions de fonctionnement (techniques et organisationnelles) de l'AC ou de l'application, sans que ces modifications n'altèrent le référencement PRIS/RGS (ou le référencement à un cadre de référence de niveau équivalent et reconnu par le Comité PAC dans le cadre de la PAC) ou une application déclarée conforme ; l'organisation n'est pas tenue de documenter et présenter ces évolutions au Comité d'Enregistrement PAC

- Modifications majeures (donc avec changement d'OID) des conditions de fonctionnement (techniques et organisationnelles) de l'AC ou de l'application, qui conduisent à avoir potentiellement un impact sur le référencement PRIS/RGS (ou le référencement à un cadre de référence de niveau équivalent et reconnu par le Comité PAC dans le cadre de la PAC) ou une application déclarée conforme ; dans les 6 mois précédant ces modifications, l'organisation est tenue de :
  - Déclarer ces évolutions au Comité d'Enregistrement PAC avant la diffusion des certificats comportant le nouvel OID ;
  - Demander la mise à jour de la date de fin de validité du référencement de la familles de certificats avec l'ancien OID, précisant ainsi pendant quelle durée cette famille[4] est utilisable (un délai raisonnable doit être prévu) **et** présenter l'attestation ou le rapport d'audit de la nouvelle famille de certificats qui lui permettront d'obtenir un nouveau référencement PAC.

  La liste des familles de certificats référencés PAC sera ainsi publiée avec l'historique de toutes les versions d'OID encore valides. Au minimum pendant la durée de validité de chaque famille de certificats, la PC correspondante doit rester accessible en ligne.

- Modification d'un cadre de référence tiers reconnu conforme à la PAC :
  - Dans l'hypothèse où le niveau de sécurité de ce référentiel reste *a minima* identique à celui de la PRIS/RGS, le promoteur de ce référentiel est simplement tenu d'aviser le Comité d'Enregistrement PAC des modifications
  - Dans l'hypothèse où le niveau de sécurité de ce référentiel n'est plus compatible avec celui de la PRIS/RGS, l'organisation adhérente à ce référentiel :
    - En avisera le Comité d'Enregistrement PAC, au moins 3 mois avant la date de mise en œuvre effective de ces modifications
    - Demandera le retrait de son référencement ou présentera les actions ou les raisons qui lui permettront de conserver celui-ci.

En face de ces différentes situations, le Comité d'Enregistrement PAC pourra :

- Maintenir son référencement ;
- Procéder au retrait de celui-ci ;

[4] La durée de validité d'une Autorité de Certification doit être au moins égale à la durée de vie du dernier certificat émis par cette AC.

- Demander un audit du nouveau référentiel, la charge de cet audit restant à l'organisation souhaitant conserver son référencement.

Les principes d'audit et de contrôle

En cas de changement opéré sur une AC déjà référencée, les principes d'audit et de contrôle s'imposent aux acteurs suivants :

- Les adhérents du CFONB
- Les tiers non adhérents du CFONB

Acteurs adhérents du CFONB

Le contrôle des conditions de mise en œuvre de la PAC est sous la responsabilité des Inspections Générales de chaque banque; le CFONB, en tant que garant de l'existence de la PAC, peut demander un avis à l'Inspection Générale de la banque participante, sur incident ou sur un événement spécifique.

Acteur non adhérents du CFONB

Un audit ou une procédure de contrôle peut être provoqué à la demande du Comité d'Enregistrement PAC, à la suite de :

- Une évolution du référentiel de l'organisation adhérente susceptible de réduire le niveau de sécurité et de rendre celui-ci inférieur au niveau défini par le cadre de référence.
- Un incident :
  - Corruption des secrets
  - Incidents sur les processus organisationnels (enregistrement, renouvellement, révocation…)
  - Utilisation frauduleuse d'un certificat valide dans une application acceptant les certificats PAC
  - …

Le processus d'audit ou de contrôle doit respecter les principes suivants :

- L'organisation a la charge de retenir un auditeur référencé/ recommandé par un organisme du type COFRAC ou équivalent
- Le périmètre de l'analyse est défini en fonction de la nature de la problématique, d'un commun accord entre les deux parties
- Les rapports et comptes rendus sont rédigés en français ou en anglais
- Le Comité d'Enregistrement PAC s'engage à garder confidentielles les informations obtenues sur l'organisation, ses applications, ses AC ou ses familles de certificats
- Dans tous les cas, les coûts d'audit sont à la charge de l'organisation qui se fait auditer

A la suite de ces missions de contrôle, l'auditeur rend ses conclusions à l'organisation auditée qui a la charge de les transmettre au Comité d'Enregistrement PAC.

Une démarche de mise en conformité peut être proposée par l'organisation, avec un planning et un renouvellement du processus de contrôle.

Dans le cas d'écarts trop importants avec le cadre de référence de la PAC (éventuellement, après que l'organisation ait tenté de corriger ces écarts), le référencement est retiré.

La saisine du Comité PAC

Tout établissement adhérent à la PAC peut saisir le Comité PAC et lui demander de convoquer une réunion d'urgence du Comité d'Enregistrement PAC, en particulier en cas de soupçon de fraude ou de malversation.

5. LE CAS DES ORGANISATIONS NON ADHERENTES A LA PAC

Faire référence à la PAC est autorisé aux organisations qui ne sont pas reconnues comme adhérentes à la PAC, uniquement dans des fonctions d'acceptation, c'est-à-dire dans un rôle de promoteur d'applications, à la condition que :

- L'organisation précise systématiquement et très clairement qu'elle n'est pas adhérente à la PAC ;
- Ses applications acceptent l'ensemble des certificats des AC référencés PAC ;
- L'organisation s'engage à respecter les évolutions de la PAC au niveau des fonctions d'émission : nouvelle AC référencée, suppression d'un AC ou d'une gamme de certificats… La mise à niveau doit se faire dans les 3 mois suivant la publication sur les sites officiels de la nouvelle version de la PAC ;
- L'organisation respecte les « Principes de conformité » associées à la PAC, tant au niveau de l'application acceptrice de certificats que de l'organisation elle-même ;
- L'organisation informe l'émetteur de certificats, en cas d'incidents ;
- L'organisation respecte les droits de propriété intellectuelle sur la PAC.

En aucun cas, une organisation non adhérente à la PAC ne peut engager la responsabilité d'une organisation adhérente, en faisant référence à la PAC.

6. LES PRINCIPES DE GOUVERNANCE

Le CFONB est en charge des missions suivantes :

- Au travers du Comité PAC :
  - Il est garant de la publication du référentiel et de ses évolutions
  - Il publie sur son site le référentiel de la PAC
  - Il revoit la PAC sur une base au moins annuelle et, en fonction des besoins, la réactualise, chaque fois que nécessaire
  - Il pilote les évolutions de la PAC (mise à jour, publication…)
- Au travers du Comité d'Enregistrement PAC :
  - Il publie la liste des AC référencées et des applications acceptant des certificats PAC
  - Il fait vivre la PAC et, en conséquence, il :
    - Reconnaît la conformité de nouvelles applications
    - Atteste de la conformité des AC ou des familles de certificats
  - Il étudie les dossiers de demande de référencement
  - Il demande, le cas échéant, des audits dans la phase d'analyse de la demande de référencement

Le CFONB est en charge des problématiques de propriété intellectuelle autour de la PAC et, en particulier, du dépôt et de la protection de tout signe distinctif et autres dénominations concernant la PAC (marque, « label », nom de domaine, …).

Il faut noter que le CFONB n'est en aucun cas, responsable :

- ni du respect de la PAC par les organisations, applications, AC ou familles de certificats reconnues conformes
- ni des conséquences directes ou indirectes qui pourraient en être induites.

Les auditeurs auront la charge de vérifier que les principes de la PAC sont appliqués, soit lors d'une demande de référencement initiale ou de son renouvellement, soit en contrôle ponctuel. Les charges d'audit sont, dans tous les cas, à la charge des établissements audités

Dans le cadre de leurs missions au titre de la PAC, les membres des Comité PAC et Comité d'Enregistrement PAC comme du CFONB sont tenus à une obligation de confidentialité.

7. ANNEXE 1 : RAPPEL DU CONTEXTE

Dans cette annexe, nous positionnons les unes par rapport aux autres :

- La politique de certification
- La politique d'acceptation
- La politique de validation

La Politique de Certification

La qualité d'un certificat est régie par la Politique de Certification que l'Autorité de Certification (AC) a défini et qu'elle s'engage à respecter.

Le CFONB a adopté la Politique de Référencement Intersectorielle de Sécurité (PRIS/RGS), réalisée par l'administration en concertation avec l'ensemble des acteurs, comme base commune pour le secteur bancaire en matière de certificats numériques, en particulier pour l'établissement des politiques de certification propres à chaque Établissement Financier. Cette référence à la PRIS/RGS permet de s'appuyer sur des travaux existants et de prévoir une coexistence et une cohérence avec les infrastructures de confiance mises en place dans le cadre des services en lignes et des télé-procédures de l'administration française.

Il faut noter que la PRIS/RGS distingue les natures de certificats : certificats d'identité, certificats de signature, certificats de chiffrement.

En s'appuyant sur ce cadre de référence, chaque Établissement établit sa propre politique de certification et en est seul responsable.

La PAC définit 3 niveaux de sécurité pour un certificat :

- Niveau 1, correspondant à un certificat logiciel pas nécessairement remis en face à face
- Niveau 2, niveau dit fort, correspondant schématiquement à des secrets stockés en carte à puce ou token et faisant intervenir un face à face
- Niveau 3, niveau dit qualifié, pour des applications supposant un très haut niveau de sécurité et/ou répondant généralement à des contraintes légales fortes

La PRIS/RGS définit les différents niveaux de sécurité, en s'appuyant sur les critères suivants :

- Les principes de confinement du certificat (certificat logiciel ou certificat sur carte à puce)
- Les principes d'enregistrement et de distribution
- Les principes de gestion de l'AC
- Les principes de publication et de révocation
- Les règles de gestion des listes de révocation
- Les principes de sécurité (en particulier, au niveau de la protection des secrets de signature des certificats)

La qualité du certificat est définie par :

- Son niveau de sécurité (niveau 1,2 ou 3)
- L'engagement que prend l'AC en cas de non-conformité par rapport aux principes énoncés dans la Politique de Certification (par exemple, niveau de la RC Professionnelle)

La Politique d'Acceptation (PA)

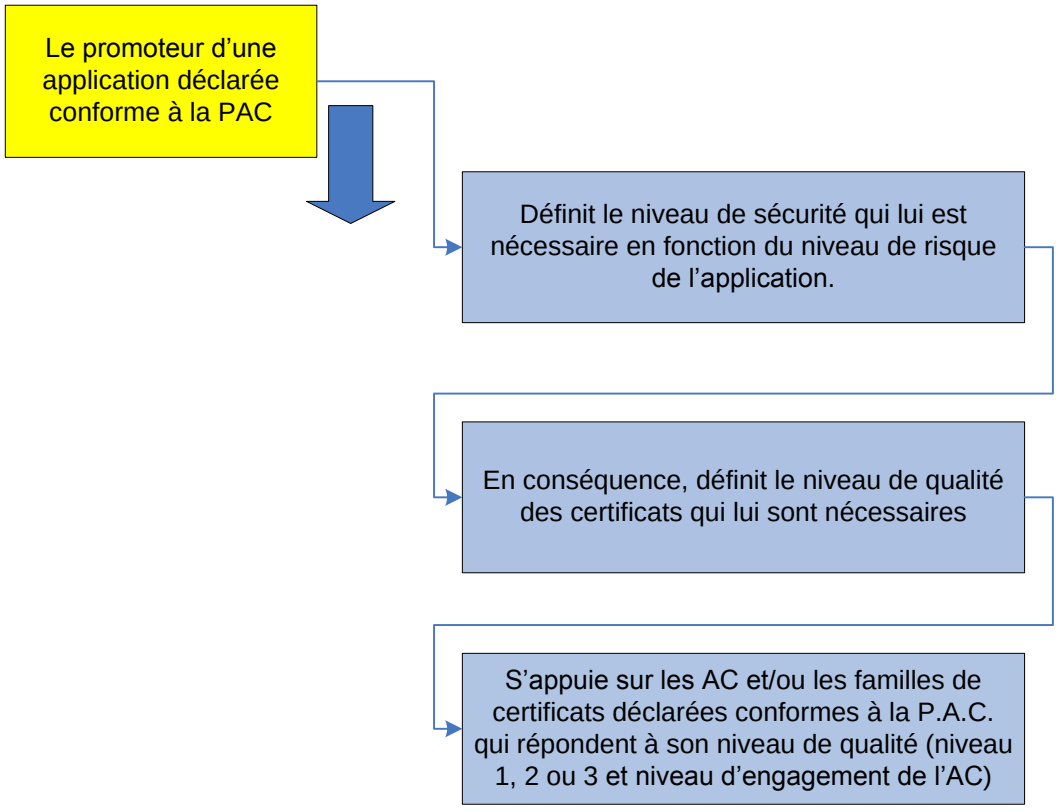
Les certificats et les bi clés associés seront utilisés par les applications pour identifier et authentifier leurs utilisateurs, dans des opérations de contrôle d'accès ou pour contrôler l'intégrité des instructions reçues dans des opérations de signature. En fonction du niveau de risque accepté au niveau des applications, il faudra identifier plus ou moins fortement les acteurs et/ou assurer un niveau de signature et, donc, utiliser des certificats d'un niveau de qualité adapté.

Une politique d'acceptation définit les règles que doit respecter une AC ou une famille de certificats pour que ses certificats soient acceptés par une application

Une politique d'acceptation permettra d'attester de la conformité des familles de certificats et de définir leur niveau de qualité et de sécurité ainsi que de la conformité des contrôles sur l'utilisation de ces certificats dans les applications définies.

Une politique d'acceptation adresse les besoins :

- Des promoteurs d'applications en leur permettant de s'appuyer sur des AC ou des familles de certificats attestées conformes et d'assurer un niveau de sécurité dans leurs services
- Des AC et des organisations émettrices de certificats de bâtir un espace de multi-acceptance dans lequel leurs familles de certificats référencées par la PAC sont reconnues par un ensemble d'applications portées par des acteurs différents
- Des porteurs qui seront naturellement bénéficiaires de la construction d'espaces de multi-acceptance



La Politique de Validation

Une politique de validation ne se limite pas aux principes permettant d'accepter un certificat ; elle doit pouvoir servir de référence à l'application pour permettre à celle-ci de valider une transaction ou une opération, en prolongeant la politique d'acceptation et en permettant de mettre celle-ci en œuvre.

La validation d'un mouvement ou d'une transaction se fait, en particulier, en exécutant les contrôles associés aux politiques d'acceptation et de validation. La vérification du référencement PAC du certificat utilisé étant implicite.

Domaines respectifs des politiques d'acceptation et de validation

Très schématiquement, la politique d'acceptation définit les critères que doivent respecter les certificats, en fonction du niveau de qualité recherché ainsi que les critères à respecter par les applications utilisatrices de ces certificats.

La politique d'acceptation définit un cadre de référence au niveau des certificats et de leurs utilisations, alors que l'objet de la politique de validation est de définir les moyens de mettre en œuvre cette politique d'acceptation (le 'comment' en prolongement du 'quoi'), dans un autre document.

La politique de validation définit les différentes opérations à effectuer pour s'assurer du niveau de qualité du certificat et de sa conformité au niveau demandé par l'application pour son référencement. Elle entre en jeu

- une fois la famille de certificats déclarée conformes à la PAC ;
- et ce, pour les applications acceptant les certificats PAC.

La politique de validation couvre un périmètre plus large que celui adressé par la politique d'acceptation, en particulier au niveau de la validation de la signature technique et de la gestion de la preuve des contrôles réalisés.

Contrôles	Politique d'acceptation	Politique de validation	Contrôles applicatifs
Famille de certificats utilisée	X	X	(X)
Gabarit du certificat	X	X	
Date de validité	X	X	
Longueur de clés	X	X	
Politique de certification associée	X	X	
Niveau 1, 2 ou 3	X	X	
Niveau d'engagement de l'émetteur	X	X	
Listes de révocation	X	X	
Key usage	X	X	
Signature		X	
Outils de signature		X	
Outils de validation de signature		X	
Intégrité de la signature		X	(X)
Conformité de la famille de certificats avec le niveau requis par l'application		X	X
Droits, habilitations et limites			X

8. ANNEXE 2 : LISTE DES SITES DE PUBLICATION DE REFERENCE

Le site de référence de publication de la PAC est aujourd'hui le site du CFONB :

http://www.cfonb.org

Le CFONB s'assure de la mise à jour de ce site sur les thèmes relatifs à la PAC.

9. ANNEXE 3 : ÉLEMENTS TECHNIQUES CONCERNES PAR LA PAC

La PRIS/RGS s'appuie sur et précise les exigences du RFC3280, RFC2560, RFC3739, RFC3647, CWA14167-1.

Le tableau suivant reprend la liste des postes sur lesquels porte l'analyse de conformité des AC et des familles de certificats ; sont identifiés :

- Les postes dont les spécifications sont précisées dans la PRIS/RGS
- Les postes dont les spécifications conditionnent le niveau de sécurité du certificat

Éléments techniques		Définition dans le cadre de la PRIS/RGS	Fonction du niveau de sécurité technique du certificat
Profils de certificats/LCR/OCSP et algorithmes			
Gabarit du certificat			
	Format (X509)	oui	Non
	Champs de base	oui	Non
	Contraintes sur les identifiants (AC, porteur…)	oui	Non
	Extensions	oui	Non
	Nature du certificat	oui	non
Format des CRL		oui	non
Protocoles État en ligne des Certificats (OCSP)		Oui-RFC 2560	non
Algorithmes et longueurs de clés		oui	oui
PC			
Définition des entités intervenant dans l'IGC		oui	non
Domaines d'utilisation applicables / interdits		oui	oui
Gestion de la PC		oui	non
Principes de mise à disposition des informations devant être publiées		oui	oui
Identification et nommage			
	Nommage	oui	non
	Validation initiale de l'identité	oui	oui
	Identification et validation d'une demande de renouvellement des clés	oui	oui
	Identification et validation d'une demande de révocation	oui	oui

Éléments techniques		Définition dans le cadre de la PRIS/RGS	Impact sur le niveau de sécurité technique du certificat
Exigences opérationnelles sur le cycle de vie des certificats			
	Demande de certificat	oui	oui
	Traitement d'une demande de certificat	oui	non
	Délivrance du certificat	oui	oui
	Acceptation du certificat	oui	oui
	Usage du bi clé et du certificat	oui	oui
	Renouvellement d'un certificat	oui	non
	Délivrance d'un nouveau certificat suite à changement du bi clé	oui	oui
	Modification du certificat	oui	non
	Révocation et suspension des certificats	oui	oui
	Fonction d'information sur l'état des certificats	oui	non
	Fin de la relation entre le porteur et l'AC	oui	non
Mesures de sécurité non techniques			
	Mesure de sécurité physique	oui	oui
	Mesures de sécurité procédurales	oui	oui
	Mesures de sécurité vis-à-vis du personnel	oui	non
	Archivage de données	oui	non
	Changement de clés d'AC	oui	non
	Reprise suite à compromission et sinistre	oui	non
	Fin de vie de l'IGC	oui	non

Éléments techniques		Définition dans le cadre de la PRIS/RGS	Impact sur le niveau de sécurité technique du certificat
Mesures de sécurité techniques			
	Génération et installation de bi clés	oui	oui
	Protection des clés privées et des modules cryptographiques	oui	oui
	Gestion des bi clés	oui	non
	Données d'activation	oui	non
	Sécurité des systèmes informatiques	oui	oui
	Sécurité des systèmes durant leur cycle de vie	oui	non
	Sécurité réseau	oui	non
	Horodatage / Système de datation	oui	non
Audits de conformité et autres évaluations			
	Fréquences et/ou circonstances des évaluations	oui	non
	Identités / qualifications des évaluateurs	oui	non
	Relations entre évaluateurs et entités évaluées	oui	non
	Sujets couverts par les évaluations	oui	non
	Actions prises suite aux conclusions des évaluations	oui	non
	Communication des résultats	oui	non

Éléments techniques		Définition dans le cadre de la PRIS/RGS	Impact sur le niveau de sécurité technique du certificat
Problématiques métiers et légales			
	Tarifs	non	non
	Responsabilité financière	non	non
	Confidentialité des données professionnelles	oui	non
	Protection des données personnelles	oui	non
	Droit sur la propriété intellectuelle et industrielle	non	non
	Interprétations contractuelles et garanties	oui	non
	Limite de garantie	non	non
	Limite de responsabilité	non	non
	Durée et fin anticipée de validité de la PC	oui	non
	Amendements à la PC	oui	non
	Dispositions concernant la résolution de conflits	non	non
	Juridictions compétentes	non	non
	Conformité aux législations et réglementations	non	non
	Dispositions diverses	non	non
	Autres dispositions	non	non
Exigences de sécurité du module cryptographique de l'AC			
Exigences sur les objectifs de sécurité		oui	oui
Exigences sur la certification		oui	oui
Exigences de sécurité du dispositif d'authentification et de signature			
Exigences sur les objectifs de sécurité		oui	non
Exigences sur la certification		oui	oui

10. ANNEXE 4 : EXIGENCES LIEES AU NIVEAU DE QUALITE DU CERTIFICAT

Les exigences sur les niveaux de sécurité des certificats sont définies par le secteur bancaire, en faisant référence au classement par étoiles de PRIS/RGS ; elles sont reprises dans le tableau ci-dessous :

Domaine	Niveau 1	Niveau 2	Niveau 3
Validation initiale de l'identité du porteur	Envoi du dossier d'enregistrement sous forme papier (avec copie des pièces d'identité) ou sous forme électronique (ex : signature avec un certificat et un outil **) ou communication d'un élément propre au futur porteur permettant de l'identifier au sein d'une base de données administrative pré-établie (1)	Contrôle de l'identité • en face à face • avec une signature électronique de niveau ** mais de préférence de niveau *** (recommandé)	Contrôle de l'identité • en face à face uniquement
Remise / acceptation d'un certificat	❑ Remise par message électronique ❑ Acceptation tacite	❑ Remise en face à face si l'authentification du porteur se fait en en face à face et que celui-ci n'a pas eu lieu à l'enregistrement ❑ Si possible, acceptation explicite du certificat par le porteur ❑ Au minimum, acceptation tacite à partir d'une date de remise suffisamment fiable	❑ Remise en face à face si l'authentification du porteur se fait en face à face et que celui-ci n'a pas eu lieu à l'enregistrement ❑ Si l'AC ne génère pas le bi clé, vérification que le certificat est bien associé à la clé privée correspondante (chargement à distance sur une carte à puce ou un token) ❑ Acceptation explicite du certificat par le porteur

Domaine	Niveau 1	Niveau 2	Niveau 3
Révocation d'un certificat	❑ Authentification de la demande par vérification d'une ou deux informations de base sur le demandeur (n° de téléphone, adresse…) (2) ❑ Service accessible au moins les jours ouvrés, avec un maximum de 16 h (jours ouvrés) d'indisponibilité par mois ❑ Délai, entre validation de la demande et mise à jour des informations de statuts de moins de 1 jour ouvré	❑ Authentification formelle de la demande (ex : série de quelques questions / réponses (3/4) de levée de doute, utilisation d'un certificat et d'un outil *…) ❑ Service accessible 24h/24, 7j/7, maximum d'indisponibilité 4h par mois ❑ Délai, entre validation de la demande et mise à jour des informations de statuts de moins de 1 jour ouvré	❑ Authentification formelle de la demande (ex : série de quelques questions / réponses (4/5) de levée de doute, utilisation d'un certificat et d'un outil **…) ❑ Service accessible 24h/24, 7j/7, maximum d'indisponibilité 2h par mois ❑ Délai, entre validation de la demande et mise à jour des informations de statuts de moins de 24h, 7j/7
Service d'état des certificats	❑ Au minimum, publication de LCR. Recommandation d'un service en ligne (OCSP) ❑ Service accessible pendant les jours ouvrés, maximum de 32h (ouvrées) d'indisponibilité par mois	❑ Au minimum, publication de LCR. Recommandation de la mise en œuvre de delta CRL et d'un service en ligne (OCSP) ❑ Service accessible 24h/24 et 7j/7, maximum de 8h (ouvrées) d'indisponibilité par mois	❑ Au minimum, publication de LCR. Recommandation de la mise en œuvre de delta CRL et d'un service en ligne (OCSP) ❑ Service accessible 24h/24 et 7j/7, maximum de 4h (ouvrées) d'indisponibilité par mois

Domaine	Niveau 1	Niveau 2	Niveau 3
Protection des clés d'AC (privées/publiques)	❑ Génération et mise en œuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS ❑ Cérémonie des clés par au moins une personne dans un rôle de confiance ❑ Activation des clés privées d'AC par au moins une personne dans un rôle de confiance	❑ Génération et mise en œuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe B2 du RG, certifié à un niveau équivalent à EAL2+ et qualifié à un niveau au moins standard ❑ Cérémonie des clés par au moins deux personne (dans un rôle de confiance) et au moins un témoin externe ❑ Contrôle des clés privées de l'AC par au moins deux personnes dans des rôles de confiance (porteurs de parts de secrets) ❑ Activation des clés privées d'AC par au moins une personne dans un rôle de confiance	❑ Génération et mise en œuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS, certifié à un niveau équivalent à EAL4+ et qualifié à un niveau renforcé de préférence ❑ Cérémonie des clés par au moins deux personne (dans un rôle de confiance) et au moins deux témoins externes (dont un officier public recommandé) ❑ Contrôle des clés privées de l'AC par au moins deux personnes dans des rôles de confiance (porteurs de parts de secrets) ❑ Activation des clés privées d'AC par au moins deux personnes dans des rôles de confiance
Génération des clés privées des porteurs (si elles sont générées par l'AC en dehors du dispositif de création de signature du porteur)	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS (Gestion des clés cryptographiques)	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS, certifié à un niveau équivalent à EAL2+ et qualifié à un niveau au moins standard	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS, certifié à un niveau équivalent à EAL4+ et qualifié à un niveau renforcé de préférence

(1) : Dans le cas de la PAC, l'enregistrement du porteur dans une base de données administrative pré-établie doit être compris au sens de l'enregistrement du porteur dans une des bases de référence d'une des organisations adhérentes à la PAC

(2) Dans le cas d'un certificat d'identité, il faudra tenir compte des contrôles suivants :

Domaine	Niveau 1	Niveau 2	Niveau 3
Dispositif d'authentification	Déclaration de conformité aux exigences	Certification EAL2+ débouchant sur une qualification standard	Certification EAL4+ débouchant sur une qualification de préférence renforcée

Dans le cas d'un certificat de signature, il faudra tenir compte des contrôles suivants :

Domaine	Niveau 1	Niveau 2	Niveau 3
Dispositif de création de signature	Déclaration de conformité aux exigences	Certification EAL2+ débouchant sur une qualification standard	Certification EAL4+ débouchant sur une qualification de préférence renforcée

11. ANNEXE 5 : CARACTERISTIQUES DES CERTIFICATS EN FONCTION DE LEUR NIVEAU DE SECURITE

Le niveau de sécurité d'un certificat est dépendant à la fois du certificat et des processus de création du certificat dépendant de l'IGC.

Critères directement liés aux certificats en faisant référence à la PRIS/RGS.

Domaine	Niveau1	Niveau 2	Niveau 3
Génération des clés privées des porteurs par l'AC en dehors du dispositif du porteur	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS, certifié à un niveau équivalent à EAL2+ et qualifié à un niveau au moins standard	Génération dans un module cryptographique répondant aux exigences de l'annexe B2 du RGS, certifié à un niveau équivalent à EAL4+ et qualifié à un niveau renforcé de préférence
Taille des clés RSA du certificat porteur	❑ RSA : 1024 ou 2048 ❑ DSA : 1024/q=160 ou 2048/q=256	❑ RSA : 2048[5*] ❑ DSA : 1024/q=256 ou 2048/q=256	❑ RSA : 2048 ❑ DSA : 2048/q=256
Dispositif du porteur	❑ Le dispositif peut être logiciel ❑ Déclaration de conformité aux exigences	❑ Dispositif matériel ❑ Certification EAL2+ débouchant sur une qualification standard	❑ Dispositif matériel ❑ Certification EAL4+ débouchant sur une qualification renforcée de préférence

A noter que dans le RGS, Annexe B1 « Mécanismes Cryptographiques », page 15, selon la règle « RégleFact-1 », il est précisé que les clefs doivent voir une longueur minimale de 2048 bits jusqu'en 2020 et 4096 bits au-delà.

[5] L'usage d'une longueur de clef de 1024 est toléré pour les certificats déjà émis jusqu'à leur renouvellement

Critères liés à la qualité des processus de l'IGC

	Niveau 1	Niveau 2	Niveau 3
Validation initiale de l'identité	❑ Envoi d'un dossier papier ❑ Demande d'enregistrement signé par le porteur avec des outils de qualité 2 étoiles ❑ Communication d'un élément propre au futur porteur permettant de l'identifier au sein d'une base de données pré-établie	❑ Face à face physique ❑ Méthode apportant un degré d'assurance équivalent	Idem niveau 2
Identification et validation d'une demande de révocation	Vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer ❑ Une ou deux informations de base	Vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer ❑ Série d'au moins 3 ou 4 questions/réponses sur des informations propres au demandeur ❑ Authentification en ligne à l'aide d'outils qualifiés au moins niveau 1 ❑ Signature électronique à l'aide d'outils qualifiés au moins niveau 1	Idem niveau 2
Délivrance du certificat	Transmission par voie électronique	Remise en face à face si le face à face n'a pu avoir lieu précédemment dans le cycle de vie du certificat	Idem niveau 2
Acceptation du certificat	Acceptation tacite à compter de l'envoi du certificat	Confirmation de l'acceptation du certificat par le porteur, si possible de façon explicite sous la forme d'un accord signé (papier ou électronique)	Idem niveau 2

Par ailleurs, le niveau de qualité du certificat est fonction de :

- La fréquence de publication des LCR
- Les mesures de protection physique (contrôle d'accès aux ressources)
- La sauvegarde hors site
- La répartition des rôles au niveau des acteurs en charge de l'IGC
- Les mesures de sécurité mises en œuvre pour la protection des clés privées et pour les modules cryptographiques
- Les exigences de sécurité du module cryptographique de l'AC.

12. ANNEXE 6 : POSITIONNEMENT RESPECTIF DE LA PAC ET DES REFERENTIELS PRIS ET RGS

La PAC définit, pour le monde bancaire, les exigences techniques, organisationnelles et réglementaires pour répondre au besoin des applications bancaires.

Il a été également choisi de rester compatible, pour ce qui concerne la France avec les référentiels de l'Administration qui sont :

- La PRIS depuis 2004, encore opérationnelle pour les certificats émis jusqu'en mai 2013 avec une validité maximale à mai 2016.
- Le RGS 1.0 depuis mai 2010, qui est reconnu par décret comme le référentiel en vigueur de l'Administration.

Pour les applications existantes de l'Administration, une période transitoire de 3 ans a été définie par l'Administration pour la prise en compte de ces évolutions.

La situation actuelle fait que les applications existantes de l'administration mais également celles des banques peuvent accepter les certificats référencés PRIS.

Depuis mai 2013 , les nouvelles applications bancaires doivent accepter les certificats référencés RGS1.0.

Pour qu'une application puisse être conforme PAC, elle doit accepter tous les certificats PAC du niveau exigé par son analyse de risque.

Actuellement la PAC s'appuie sur les 2 référentiels de l'Administration.

La PAC peut avoir des exigences supplémentaires par rapport à ces 2 référentiels.

Lorsqu'une famille de certificats passe du référentiel PRIS au référentiel RGS, une demande de référencement PAC doit être initiée.

Liste des écarts PAC par rapport au référentiel PRIS

- La PRIS autorise des certificats sur support logiciel et matériel, la PAC exige pour le niveau 2 un support matériel ;
- Une assurance Responsabilité Civile Professionnelle dont le montant minimal de la garantie exigée est précisé dans le dossier de demande de référencement.

Liste des écarts PAC par rapport au référentiel RGS

- Le RGS supporte l'algorithme SHA 256 et SHA 1. Le parc des postes de travail Client est aujourd'hui compatible avec SHA 256, avec une longueur de clef minimale fixée à 2 048 bits;
- Une assurance Responsabilité Civile Professionnelle dont le montant minimal de la garantie exigée est précisé dans le dossier de demande de référencement.

L'utilisation d'un référentiel PRIS ou RGS permet de simplifier le processus de référencement PAC, puisque l'audit de référencement ou de renouvellement PRIS ou RGS est accepté par la PAC. Autrement dit il n'est pas nécessaire de faire un second audit pour la PAC.

Les écarts sont suffisamment réduits pour être constatés et testés, il n'est pas nécessaire de faire un audit complémentaire.

En aucune manière un référentiel n'est imposé. Le référencement PAC peut être réalisé soit avec un autre référentiel, soit sans référentiel préalable.

Les référencements PRIS/RGS et PAC sont indépendants :

- Un référencement PAC n'entraîne pas un référencement PRIS ou RGS
- Un référencement PRIS ou RGS n'entraîne pas un référencement PAC.

Tous les référencements doivent être demandés explicitement par la constitution d'un dossier.

13. ANNEXE 7 : CONTROLES A EFFECTUER SUR LE CERTIFICAT DANS LE CADRE DE LA PAC

La PAC suppose que soient contrôlés :

- Le gabarit du certificat
- Les champs de base
- Les identifications
- Les extensions (présence obligatoire, criticité)
- Les algorithmes
- Les longueurs de clés
- Les listes de révocation / protocoles d'états en ligne des certificats (OCSP)
- Les familles de certificats
- La hiérarchie d'AC à laquelle la famille de certificats est rattachée
- Les Listes de Révocation d'Autorités (ARL)

La PAC ne prend pas en compte les mesures de sécurité suivantes :

- Protection contre les virus, vers, chevaux de Troie, … avec mise à jour régulière
- Contrôle et limitation des échanges entre la machine hôte et d'autres machines dans un réseau ouvert
- Restriction, lorsque cela est possible, de l'accès aux fonctions de la machine aux seuls administrateurs de celles-ci (différentiation compte utilisateur / administrateur)
- Installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de l'administrateur
- Refus par le système d'exploitation de l'ordinateur ou de la borne, d'exécuter des applications téléchargées ne provenant pas de sources sures
- Mise à jour des composants logiciels et systèmes lors de la mise à disposition de mise à jour de sécurité de ceux-ci
- Utilisation d'un lecteur avec PIN/PAD intégré dans le cadre d'une utilisation en signature niveau 3.

14. ANNEXE 8 REFERENTIEL

La PAC, dans sa version actuelle, a été établie sur la base d'une version de la PRIS/RGS que le Comité d'Enregistrement PAC tient à disposition. Pour obtenir tout renseignement sur ces documents, demande doit en être faite auprès du Comité PAC ou Comité d'Enregistrement PAC.

Comme présenté dans le paragraphe 3 de ce document, d'autres référentiels type, notamment ceux en cours dans d'autres pays, pourront être accepté par le comité PAC.

L'acceptation de ces référentiels types, impliquera qu'ils soient l'objet d'audits de référencement indépendants effectués par des cabinets d'audit reconnus par le COFRAC ou un organisme équivalent.

15. ANNEXE -9 : AUTRES DOCUMENTS DE REFERENCE

La PAC s'appuie sur les documents suivants :

- Politique de Référencement Intersectoriel de Sécurité :
  - Préambule
  - Politiques de Certification Types – Profils de certificats / LCR /OCSP
  - Service d'Authentification et de Signature : Politique de Certification Type

- Référentiel Général de Sécurité :
  - Présentation Générale du RGS,
  - Politiques de Certification Types et Variables de temps,
  - Profils de Certificats, CRLs, OCSP et algorithmes cryptographiques,
  - Les versions historisées.

- Politique d'Acceptation du Groupement des Cartes Bancaires 'CB'
  OID : 1.2.250.1.79.8.1

- Propositions des banques sur l'utilisation des champs du certificat X509

Par ailleurs, le Comité PAC met à disposition une Foire Aux Questions (FAQ) publiée sur le site web du CFONB avec notamment des précisions sur les numéros de version des référentiels.