CFONB

Comité Français d'Organisation et de Normalisation Bancaires

FAQ, Foire Aux Questions sur la Politique d'Acceptation Commune PAC

Réf. : Version 1.1 Fr

Sommaire

1 Objet de la PAC

1.1 Quel est l'objectif de la PAC ?

Dans le but de créer un environnement de confiance et favoriser l'utilisation de la signature électronique par les clients, dans les applications bancaires, la Politique d'Acceptation Commune permet :

- à une Autorité de Certification de se conformer à un ensemble de règles pour que ses certificats soient acceptés par les applications de la communauté bancaire ;
- à une application de se déclarer PAC, en fixant le(les) niveau(x) de risques qu'elle accepte d'encourir, validant ainsi l'usage de tous les certificats PAC associés. .

1.2 Quel est le rôle de la PAC ?

La PAC définit, pour la communauté bancaire, des critères communs de qualité et de sécurité pour des familles de certificats susceptibles d'être utilisés par une application bancaire. La PAC propose une classification selon 3 niveaux liés à la gestion du risque supporté par les applications utilisatrices. Les critères sont d'ordres techniques et juridiques et précisent les engagements et responsabilités respectifs des différents acteurs (AC, gestionnaire d'application, utilisateurs, …).

1.3 Combien y-a-t-il de niveaux de sécurité dans la PAC ?

Les niveaux de sécurité vont de 1 à 3. Pour des raisons d'homogénéité avec d'autres travaux, ils sont notamment en correspondance avec les niveaux 1,2 et 3 étoiles définis dans le RGS (Référentiel Général de Sécurité) et jusqu'en mai 2013 dans la PRIS (Politique de Référencement Intersectorielle de Sécurité), édités par l'Administration Française, avec pour cette dernière, des certificats ayant une validité maximale au 19 mai 2016.
Dans la publication, il est rappelé le référentiel sur lequel a été basé le référencement de la famille de certificats.

1.4 Comment intégrer de nouveaux référentiels et les situer par rapport aux 3 niveaux de sécurité de la PAC ?

Chaque niveau, d'un nouveau référentiel est comparé à ceux de la PAC pour une mise en correspondance au niveau immédiatement inférieur ou égal à celui de la PAC. Dans ce contexte, un niveau de référentiel peut être récusé, s'il s'avère moindre que le niveau minimum de la PAC.

2 PAC et Multi-Acceptance

2.1 Qu'est ce que la Multi-Acceptance

La multi-acceptance est la reconnaissance par une application bancaire, de certificats venant de différentes autorités de certification et qui deviennent interopérables avec cette application.
C'est donc la possibilité, et non l'obligation, donnée aux applications bancaires, d'accepter des certificats dont l'interopérabilité est assurée par le respect de critères de la PAC (sécuritaires, techniques, juridiques et responsabilité des acteurs, dont la responsabilité financière).

2.2 Quels sont les avantages de la Multi-Acceptance ?

- Utiliser le même certificat sur plusieurs applications bancaires ayant des exigences sécuritaires compatibles.
- Résoudre la problématique des conflits liés à l'installation de plusieurs supports de certificats sur un même poste de travail.
- Résoudre la problématique du choix du certificat à utiliser par un même porteur équipé de plusieurs certificats.
- Favorise la multi-bancarité des clients en leur proposant un accès aux applications bancaires avec un certificat unique.
- Liberté du choix du client pour un niveau de certificats PAC.

2.3 Quelle est la place de la PAC dans la Multi-Acceptance ?

La PAC est le document de référence pour les critères d'interopérabilité favorisant la Multi-Acceptance pour une application bancaire.

3 Place des référentiels dans la PAC

3.1 Qu'est ce qu'un référentiel ?

Un référentiel de certification est un ensemble de documents types et de règles de bonnes pratiques sécuritaires qui peuvent être proposées par des administrations ou des communautés ou organisations publiques ou privées.
En France, la PRIS puis le RGS sont promus par l'Administration française sous le contrôle de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

3.2 Pourquoi la PAC s'appuie-t-elle sur un référentiel ?

Cela permet d'alléger les procédures de référencement PAC des familles de certificats en s'appuyant sur les qualifications obtenues par les processus déjà en place pour ce référentiel.

3.3 Pourquoi la PAC s'appuie-t-elle sur le référentiel « PRIS/RGS » ?

La PRIS/RGS est un environnement de confiance connu et utilisé par un grand nombre d'Autorités de Certification du marché (compatibilité avec les applications de l'Administration). L'analyse en profondeur de ce référentiel a permis de montrer qu'il convenait également aux applications bancaires (cf. communiqué de presse ….)

3.4 En quoi la PAC est-elle différente de la PRIS/RGS ?

La seule correspondance, au niveau des exigences sécuritaires, sur les référentiels PRIS/RGS de l'Administration française, n'est pas l'unique critère retenu pour assurer la conformité avec la PAC. La PAC peut très bien se rapporter :

- à des familles de certificats conformes à des référentiels autres que PRIS/RGS, français ou non,
- à des familles de certificats dont la Politique de Certification n'est pas basée sur un référentiel, pourvu que le niveau de qualité et de sécurité de ces familles puissent trouver une correspondance avec un niveau défini dans la PAC.

La PAC se base sur des référentiels, et, le cas échéant, ajoute des critères afin de créer l'environnement de confiance recherché. L'utilisation des référentiels existant a pour objectif de faciliter la procédure de référencement PAC.

3.5 Quels sont les référentiels actuellement utilisés par la PAC ?

A date de parution de la FAQ, la PAC a référencé des familles de certificats sur la base des référentiels

- PRIS V1 ;
- V2.3 du RGS 1.0.

3.6 Pourquoi ce double référentiel PRIS/RGS ?

Depuis février 2010, date du décret « RGS », le RGS est devenu la référence de l'Administration. Le maintien de la référence à la PRIS résulte du fait de l'existence de certificats PRIS valides jusqu'au 19 mai 2016.

3.7 La PAC sera-t-elle compatible avec le Règlement eIDAS ?

Une révision de la PAC est prévue lorsque tous les actes d'exécution du règlement eIDAS seront publiés. En tout état de cause, le règlement eIDAS n'entre pas en application avant le 1er juillet 2016.

4 La PAC et les applications bancaires

4.1 Que peut apporter la PAC aux applications bancaires ?

La PAC permet aux applications bancaires de faciliter la gestion de leur environnement de confiance. En effet après avoir effectué leur analyse de risque, elles peuvent choisir le niveau des certificats adapté.

4.2 Quels sont les engagements des applications bancaires vis-à-vis de la PAC ?

Les établissements bancaires ne sont pas tenus de faire référencer leurs applications dans la PAC. Chacun reste donc libre d'utiliser ou non des certificats référencés PAC, dans ses applications.

4.3 Y-a-t-il une obligation, pour les applications, à effectuer une analyse de risque sécuritaire ?

Non, mais cette procédure est recommandée comme bonne pratique pour permettre de choisir le niveau de certificat approprié à l'application.

4.4 Que se passe-t-il si une famille de certificats PAC n'est plus opérationnelle ?

Une famille n'est plus opérationnelle lorsque l'AC cesse son activité suite à une compromission ou par décision commerciale. Avec la PAC, les clients peuvent alors choisir une solution de remplacement dans la liste des familles de niveau équivalent.

4.5 EPC approved CAs et Trusted List

Dans le cadre des services de paiement, (e-mandate, SEPA e-payment) des certificats serveur sont mis en œuvre dans les échanges de messages. Ces certificats répondent à des exigences fixées par l'EPC et sont publiés dans une Trusted List EPC Approved CAs. Le référencement dans cette liste s'effectue sous couvert de l'agrément du Certificate Authority Approval Panel (CAAP).
Le processus développé par l'EPC est similaire à celui proposé par la PAC de la communauté bancaire française mais réservé, pour le moment, uniquement aux certificats serveurs.

4.6 Où trouver les certificats PAC compatibles avec les exigences techniques d'EBICS TS

La liste des certificats compatibles avec les exigences techniques d'EBICS TS (PAC et non PAC) se trouve sur le site du CFONB dans la partie espace documentaire/organisation des échanges/protocoles de communication

4.7 Une famille de certificats PAC doit-elle être aussi PRIS/RGS ?

Non ce n'est pas nécessaire. Les familles de certificats PAC peuvent s'appuyer sur un référentiel différent de la PRIS ou RGS, ou bien n'avoir aucun référentiel désigné.

4.8 Une famille de certificat PRIS/RGS est-elle automatiquement PAC ?

Non, car la PAC n'est pas qu'une exigence technique, et une AC compatible techniquement peut ne pas répondre aux autres critères de la PAC.

4.9 Comment faire un référencement PAC hors contexte PRIS/RGS

La demande de référencement PAC est identique et obligatoire pour toutes les familles de certificats.
Si un référentiel est utilisé, le rapport d'audit vis-à-vis de ce référentiel est utilisable pour la demande de référencement PAC.

4.10 Comment réaliser un audit de référencement PAC lorsque la famille de certificats concernée ne s'appuie sur aucun référentiel existant ?

Dans ce cas la procédure d'audit, obligatoirement effectuée par un organisme accrédité, de type COFRAC en France, doit s'appuyer sur les caractéristiques de la PAC, ainsi que sur les référentiels sur lesquels s'appuie la PAC.

4.11 Peut-il y avoir d'autres référentiels ?

Oui, tous les référentiels compatibles avec les caractéristiques de la PAC peuvent servir de base pour l'audit de familles de certificats s'appuyant sur ces référentiels, quelle que soit leur origine géographique et/ou sectorielle. Aujourd'hui, les référentiels PRIS/RGS sont utilisés en France,.

4.12 Les documents à produire doivent-ils être obligatoirement rédigés en français ?

Non, ils doivent être rédigés ou traduits soit en français soit en anglais.

5 Politique d'Acceptation et Principes communs de validation des certificats et signatures électroniques

5.1 Quelle est la place du guide des principes en matière de validation de certificats ?

Le guide des principes communs de validation des certificats et signatures électroniques est élaboré par la communauté bancaire française pour les applications bancaires.
Il définit les principes de vérification d'une signature électronique et/ou d'un certificat électronique. Lors de la phase de vérification de la signature, une preuve de cette vérification est fabriquée et archivée avec la mise en œuvre d'un horodatage. La vérification est réalisée soit directement par l'application, soit par un serveur dédié et mutualisé pour l'ensemble des applications.
Le guide s'appuie sur la politique de signature de l'application pour effectuer la vérification de la signature.
Le guide s'appuie sur une politique d'acceptation ou sur une ou plusieurs politiques de certification pour la validation des certificats.
De plus, le guide peut faire référence à des politiques d'horodatage et d'archivage.

5.2 Toutes les applications bancaires doivent-elles suivre les préconisations du guide des principes communs de validation.

Non car ce guide n'a pas de caractère obligatoire.

5.3 Est-ce que la PAC exige obligatoirement un guide des principes communs de validation ?

Non, le guide est complémentaire à la PAC. Une application bancaire peut accepter des certificats PAC et appliquer une politique de validation différente du guide des principes communs de validation.

5.4 Est-ce que le guide des principes communs de validation ne s'applique qu'aux certificats PAC ?

Non, le guide des principes communs de validation peut s'appliquer à toute famille de certificats acceptée par une application bancaire.

6 Publication des AC

6.1 Y-a-t-il toutes les familles de certificats compatibles PAC dans la liste.

Pour figurer dans la liste, une famille de certificats doit répondre aux critères de la PAC et avoir fait l'objet d'une demande de référencement auprès du Comité d'Enregistrement PAC par le gestionnaire de l'AC. Donc si une AC ne fait pas cette démarche, une famille de certificats peut être compatible et ne pas être dans la liste.

6.2 Comment trouver les certificats correspondant à l'usage d'une application ?

L'application au travers d'une analyse de risques définit le niveau minimal de certificat qui peut être utilisé par les clients. Il existe une liste de certificats PAC par niveau.

7 Publication des applications

7.1 Y-a-t-il toutes les applications acceptant les certificats PAC dans la liste ?

La procédure de publication des applications étant déclarative, ne sont publiées que les applications ayant effectué cette démarche, elles ne le sont donc pas toutes.

7.2 Y-a-t-il une obligation, pour une application bancaire à être PAC ?

Non, les applications bancaires et les établissements bancaires n'ont aucun engagement vis-à-vis de la PAC. Un établissement bancaire peut décider de son libre choix de ne pas faire référencer ses applications. Une application bancaire déclarée PAC donne une visibilité sur les certificats qui pourront être utilisés.

7.3 Une application bancaire qui utilise des certificats PAC peut-elle utiliser aussi d'autres certificats ?

Bien sûr, les certificats PAC ne sont pas exclusifs. Une application peut décider, selon le niveau de risque associé, d'accepter d'autres certificats, voire d'autres systèmes d'authentification ou de signature.