Politique d'acceptation de certificats

des applications du Groupement des Cartes Bancaires "CB"

VERSION VALIDEE

Mars 2006

© GIE Cartes Bancaires "CB"

Toute diffusion ou copie de ce document, utilisation ou divulgation de son contenu sont interdites sans l'accord préalable du Groupement des Cartes Bancaires "CB"

Gestion du document

Classification

Diffusion restreinte GIE CB		
Transmission	***Télécopie ou Fax***	Sans objet
	Messagerie interne	Pas de règle spécifique.
	Messagerie Internet	Ne doit pas être transmis en clair sur Internet.
	Courrier	Sans objet
Impression		Pas de règle spécifique
Diffusion		Les personnes mentionnées dans la liste de diffusion peuvent, sous leur responsabilité, communiquer le document à d'autres destinataires en le spécifiant clairement sous forme de complément (limité et nominatif) à la liste de diffusion initiale.
Reproduction		Nombre minimal de reproductions pour action
Stockage magnétique		Accès protégé par mot de passe. Informations chiffrées par un logiciel agréé sur poste de travail fixe ou portable.
Stockage papier		Sous la responsabilité du récepteur
Archivage		Destruction / remplacement.

Liste de diffusion restreinte

Membres du Groupement des Cartes Bancaires "CB"

Historique des versions

Date	Version	Objet de la modification	Auteur
jan 06	1.0	Version validée	T.Autret
Mars 06	1.1	Version validée CODIR	T.Autret

Note :

Cette version a été élaborée en collaboration avec les membres du groupe « Politique d'acceptation » du groupe de travail Certification et Signature Electronique (GT CSE) du CFONB.

Table des Matières

1 PRÉAMBULE 7
1.1 Présentation générale 7
1.2 Identification du document 7
1.3 Principes généraux 8
1.3.1 Démarche d'acceptation 8
1.3.2 Couverture des risques 8
1.3.3 Familles de certificats éligibles 9
1.4 Entités intervenant dans l'application 10
1.4.1 Promoteur d'application 10
1.4.2 Correspondant de l'application 10
1.4.3 Porteur de certificat 11
1.4.4 Mandataire d'habilitation (MH) 11
1.4.5 Responsable de l'IGC 12
1.4.6 Autorité d'enregistrement 12
1.4.7 Autres acteurs 12
1.5 Usage des certificats 12
1.6 Gestion de la PA 14
1.6.1 Entité gérant la PA 14
1.6.2 Point de contact 14
1.6.3 Entité déterminant la conformité de cette PA 14
1.7 Définitions et acronymes 14
1.7.1 Acronymes utilisés 14
1.7.2 Objets manipulés 15
1.7.3 Actions 16
2 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES PAR L'AC ÉMETTRICE 17
3 IDENTIFICATION ET AUTHENTIFICATION 18
3.1 Nommage 18
3.2 Validation initiale de l'identité d'un porteur 18
4 EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS 19
4.1 Délivrance des clés et du certificat au porteur 19
4.2 Acceptation du certificat par l'application 19
4.3 Validation d'un certificat par l'application 19
4.4 Utilisation du certificat par l'application 19
4.5 Renouvellement du certificat 20
4.6 Fonction de mise à disposition des LCR 20
4.7 Fréquence d'établissement des LCR 20
4.8 Continuité du service 20
5 MESURES DE SÉCURITÉ NON TECHNIQUES 21

5.1 Changement de clé d'AC 21
5.1.1 Changement en fin de vie des clés d'AC 21
5.1.2 Changement en cas de compromission des clés de l'AC du porteur 21
5.1.3 Changement en cas de compromission des clés d'AC GCB 21
5.2 Reprise suite à compromission et sinistre 22

6 MESURES DE SÉCURITÉ TECHNIQUES 23

6.1 Support des biclés 23
6.2 Transmission de la clé publique de l'AC à l'application GCB 23

7 PROFILS DES CERTIFICATS ET DES LCR 24

8 CONTRÔLE DE CONFORMITÉ DE LA PC À LA PA 25

8.1 Fréquences et / ou circonstances des analyses 25
8.1.1 Processus initial 25
8.1.2 Cas de modifications mineures 25
8.1.3 Cas de modifications majeures 25
8.2 Identités / qualifications des évaluateurs 26
8.3 Relations entre évaluateurs et entités évaluées 26
8.4 Sujets couverts par les évaluations 26
8.5 Démarche de contrôle 26
8.5.1 Famille de certificats référencée PRIS 26
8.5.2 Famille de certificats non référencée PRIS 26
8.6 Actions prises suite aux conclusions des évaluations 27
8.7 Communication des résultats 27
8.8 Déchéance de l'acceptation d'une famille de certificat 27

9 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES 28

9.1 Tarifs 28
9.2 Responsabilité financière 28
9.3 Confidentialité des données professionnelles 28
9.3.1 Périmètre des informations confidentielles 28
9.3.2 Responsabilités en terme de protection des informations confidentielles 28
9.4 Limite de responsabilité 28
9.5 Durée et fin anticipée de validité de la PA 29
9.5.1 Durée de validité 29
9.5.2 Gestion des évolutions de la PA 29
9.6 Notifications individuelles et communications entre les participants 29
9.7 Amendements à la PA 29

10 RÉFÉRENCES 30

11 PROCESSUS D'ACCEPTATION D'UNE FAMILLE DE CERTIFICATS 31

1 PREAMBULE

1.1 Présentation générale

Une politique d'acceptation (PA) est un ensemble de règles portant un nom qui définit notamment les exigences auxquelles une autorité de certification (AC) doit se conformer pour que ses certificats de clé publique soient acceptés par une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.

Une PA est émise par un promoteur d'application ou au nom d'un ensemble de promoteurs lorsque la PA est commune à plusieurs applications utilisant des certificats. En fonction des risques liés à l'utilisation des certificats de clé publique et à leur usage (authentification, signature, confidentialité) dans une application donnée, le promoteur d'application détermine le niveau de certificat correspondant aux exigences de sécurité qu'il juge nécessaire pour couvrir ou réduire ces risques.

Au vu d'une analyse de conformité de la PC d'une AC candidate aux exigences de sa politique d'acceptation, le promoteur d'application décide ou non d'accepter la présentation des certificats de l'AC pour accéder aux services de l'application dont il a la charge.

Les règles de la PA portent principalement sur la sécurité des différentes phases du cycle de vie du certificat et en particulier les modalités d'enregistrement du porteur, le type de support de sa clé privée et les modalités de révocation de son certificat. La politique d'acceptation peut en outre afficher des règles non directement liées à la sécurité mais propres à l'environnement de l'application comme par exemple l'appartenance à une communauté d'intérêts.

Il existe une forte corrélation entre une politique d'acceptation et une politique de certification. La profession bancaire a retenu comme référence la politique de référencement intersectorielle de sécurité PRIS [PRIS] de l'Administration écrite par l'ADAE et la DCSSI, tout en conservant, si besoin, un degré d'adaptabilité, vis-à-vis de la version actuelle et des futures évolutions.

La politique d'acceptation des applications du Groupement des Cartes Bancaires "CB" (ci-après dénommé GIE CB) est complétée pour chaque application d'une procédure d'habilitation des personnes mandatées par leur établissement pour accéder à l'application en question dans le cadre de leur métier.

1.2 Identification du document

Le présent document est la politique d'acceptation de certificats pour l'ensemble des applications du GIE CB mises à disposition de ses membres. Lorsque cela est nécessaire, les chapitres de cette PA indiquent les exigences particulières liées au niveau de sécurité de l'application et des certificats associés.

La présente PA est dénommée « Politique d'acceptation des applications GCB ».

Elle est identifiée par l'Identifiant d'Objet (OID) suivant, déposé par le GIE CB auprès de l'AFNOR :

`1.2.250.1.79.8.1`

{iso(1) member-body(2) france(250) type-org(1) gie-cb(79) pa-paris(8) version(1)}

1.3 Principes généraux

Cette PA s'inspire du modèle de la PRIS[1] [PRIS] afin de faciliter l'analyse de conformité qui conclura à l'acceptation ou non d'une famille de certificats (voir chapitre 8).

Le contexte dans lequel se situe cette démarche d'acceptation est celui d'un établissement bancaire membre du GIE CB qui souhaite utiliser les certificats de clés publique issus d'une AC de son choix pour accéder aux applications du GIE CB. Cette AC peut être un service à part entière de l'établissement, à vocation commerciale ou purement interne, une de ses filiales ou une AC commerciale externe, fournisseur de certificats pour l'établissement.

1.3.1 Démarche d'acceptation

La mise en œuvre d'une politique d'acceptation par les applications nécessite deux étapes :

§ Une analyse des familles de certificats postulant pour accéder à l'application : le promoteur d'application analyse la conformité de la politique de certification de la famille de certificats postulant aux exigences de la politique d'acceptation ;

§ Lorsque cette conformité est avérée le promoteur d'application met à jour les règles d'acceptation programmées dans son application pour accepter les familles de certificats considérées (ex : table d'OID de PC acceptées, table de certificats d'AC acceptés, etc.).

Le processus détaillé est présenté au chapitre 11.

La démarche d'acceptation est formalisée entre l'établissement et le GIE CB par une convention d'utilisation des certificats pour l'accès aux applications du GIE CB.

1.3.2 Couverture des risques

Les certificats utilisés dans le cadre de cette PA contribuent à la couverture des risques potentiels liés aux applications GCB. Suite à une analyse des risques qui est de la responsabilité du promoteur d'application GCB, celui-ci doit indiquer le niveau de certificat (cf. chapitre 1.5) qu'il estime compatible avec le niveau de risque de son application. Selon la nomenclature utilisée dans la Politique de Protection du Patrimoine du GIE CB [PPP] les niveaux de risques sont qualifiés de **faible**, **moyen**, **fort** ou **inadmissible**.

Dans le cadre de la présente politique, aucune application n'est classifiée d'un niveau de risque au delà de fort.

Le processus d'acceptation d'une famille de certificats n'est qu'une première obligation dont le but est de vérifier que la qualité de ces certificats convient pour assurer l'authentification des porteurs se connectant à l'application (éligibilité de la présentation du certificat).

L'acceptation est faite une fois pour toute, puis est complétée par des contrôles de conformité selon une fréquence précisée au chapitre 8.1.

Lors de la connexion d'un porteur, l'application contrôle :

[1] Au moment de la rédaction de ce document la version en vigueur est la V1 qui est équivalente à la PC Type MINEFI version 3.1

§ Que le certificat appartient à une famille acceptée ;

§ Que le certificat est valide (non-périmé, non-révoqué, signature AC correcte, etc.) ;

§ Que le porteur référencé dans le certificat est habilité au vu d'une liste des porteurs habilités à accéder à l'application.

1.3.3 Familles de certificats éligibles

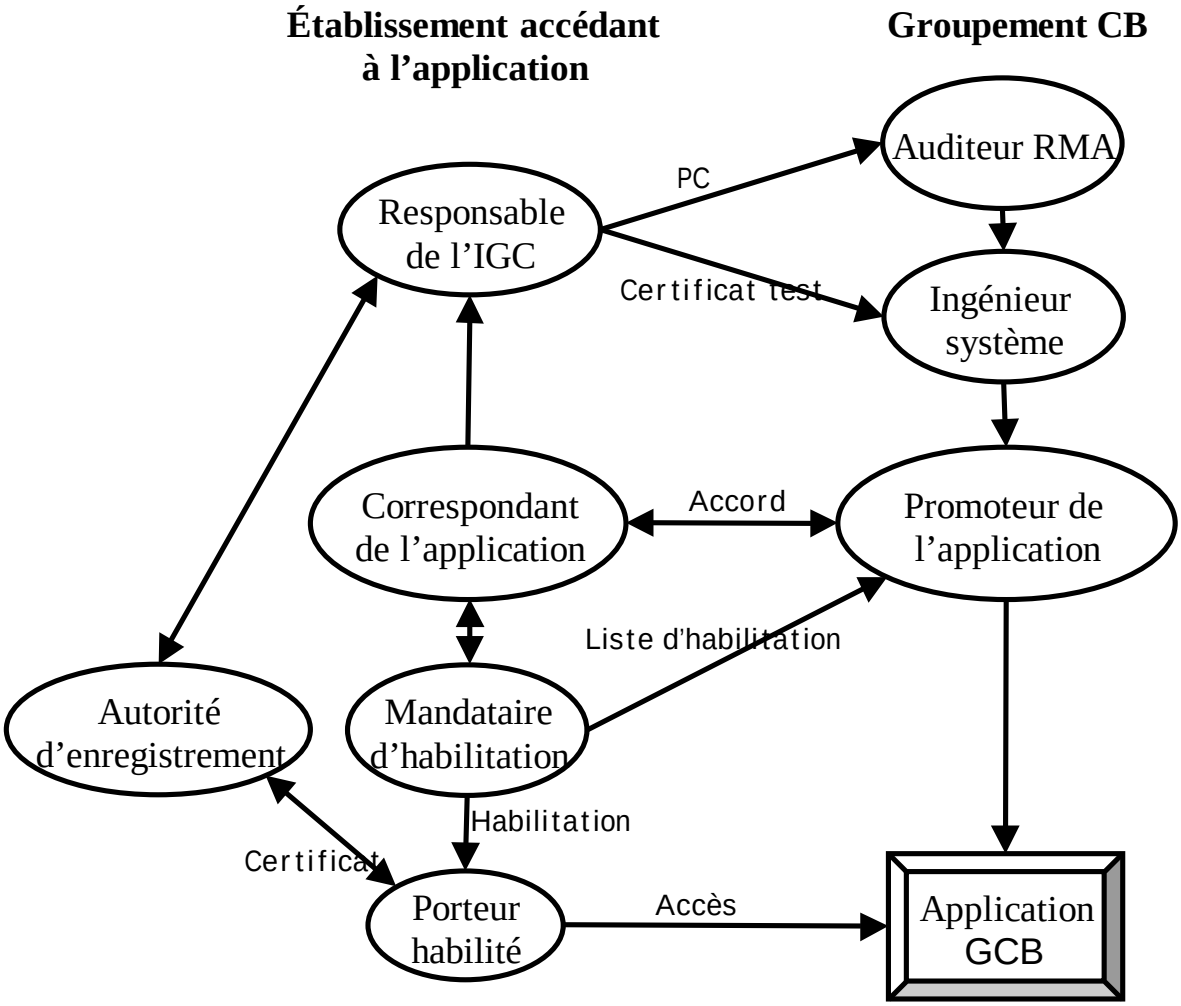
Les familles de certificats éligibles au processus d'acceptation pour la connexion aux applications GCB sont les suivantes :

§ Les certificats émis par des AC publiques référencées PRIS ou pouvant prétendre d'un niveau de sécurité équivalent au référencement PRIS ;

§ Les certificats émis par des AC privées des établissements bancaires membres du GIE CB utilisés pour l'authentification de leurs agents et pouvant prétendre d'un niveau de sécurité équivalent au référencement PRIS ;

§ Les certificats émis par l'AC du GIE CB pour ses personnels habilités pouvant prétendre d'un niveau de sécurité équivalent au référencement PRIS.

1.4 Entités intervenant dans l'application



1.4.1 Promoteur d'application

Le promoteur d'application est un responsable du GIE CB en charge d'une ou plusieurs application(s) du GIE CB utilisatrice(s) de certificats.

Dans le contexte de la présente PA, un utilisateur de certificat est une application dans sa fonction d'authentification et d'établissement d'une connexion sécurisée.

1.4.2 Correspondant de l'application

Le correspondant de l'application métier est le représentant de l'établissement d'appartenance des porteurs qui doivent accéder à une application GCB dans le cadre de leur métier. Ce correspondant est

en liaison directe avec le promoteur de l'application pour toutes les tâches relevant de la mise en œuvre de la présente politique d'acceptation.

Pour cela le correspondant de l'application métier peut s'appuyer sur son correspondant dans l'infrastructure de gestion de clés (IGC) qui lui fournit ses certificats et sur le mandataire d'habilitation pour l'application métier (s'il ne l'est pas lui-même).

Le correspondant de l'application métier doit en outre :

§ S'assurer auprès de son AC qu'elle a correctement effectué et de façon indépendante les contrôles d'identité des porteurs de son entité ;

§ Respecter les parties de la présente PA qui incombent à des collaborateurs de son établissement et en particulier le mandataire d'habilitation ;

§ Veiller à ce que les porteurs de certificat habilités à accéder aux applications du Groupement respectent les exigences qui leur incombent telles que définies dans la PA ;

1.4.3 Porteur de certificat

Dans le cadre de la présente PA, un porteur de certificats ne peut être qu'une personne physique, ayant reçu ce certificat de son établissement, qui utilise sa clé privée et le certificat correspondant dans un cadre professionnel pour l'accès à une application gérée par le GIE CB.

Le porteur respecte les exigences qui lui incombent définies dans la présente PA.

Les porteurs de certificats et des biclés correspondantes peuvent être :

§ Des personnels habilités des établissements membres du GIE CB ;

§ Des collaborateurs habilités du GIE CB.

1.4.4 Mandataire d'habilitation (MH)

L'habilitation des porteurs pour accéder à une application GCB donnée est gérée par le responsable[2] du service métier de son établissement concerné par cette application, selon une procédure établie avec le promoteur de l'application GCB.

Lorsque l'établissement utilise plusieurs applications GCB, il peut être opportun de désigner un mandataire d'habilitation unique qui sera le point de contact vis-à-vis du GCB[3] pour la gestion des habilitations aux diverses applications. Le MH a alors pour rôle de concentrer les droits d'accès donnés par les différents responsables de services métier de son établissement pour accéder aux applications GCB.

Le MH et son suppléant sont désignés par l'établissement d'appartenance des porteurs selon des règles et des procédures qui lui sont propres.

L'établissement doit signaler au promoteur de l'application, si possible préalablement mais au moins sans délai, le départ du MH de ses fonctions et, éventuellement, lui désigner un successeur.

---

[2] Ce responsable est généralement le correspondant de l'application.

[3] Le GCB désignera alors un point d'entrée unique qui sera le correspondant du MH pour l'ensemble des applications.

Dans le cadre des collaborateurs du GIE CB c'est le responsable de l'application qui joue le rôle de MH.

1.4.5 Responsable de l'IGC

Le responsable de l'IGC est le représentant de l'AC choisie par l'établissement dont les porteurs doivent accéder à l'application GCB, qui est en charge de la PC pour l'établissement et de la mise en pratique de la DPC correspondante.

Le responsable de l'IGC peut être amené à avoir des relations avec le promoteur de l'application ou ses représentants pendant le processus d'acceptation de la famille de certificats émis par l'AC pour l'application considérée.

Les prestations d'une AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des biclés et des certificats (génération, diffusion, renouvellement, révocation,...) et s'appuient pour cela sur une infrastructure technique appelée « infrastructure de gestion de clés (IGC) ».

1.4.6 Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat dans le cadre de la PC de son établissement pour la famille de certificats concernée. Ses responsabilités sont décrites dans cette PC et ne sont pas rappelées dans la présente PA.

1.4.7 Autres acteurs

Auditeur : personne désignée par le GIE CB et dont le rôle est de :

§ Valider la recevabilité de la famille de certificats du porteur aux termes de la présente PA ;

§ Procéder de manière régulière à des contrôles de conformité de la mise en œuvre de la politique d'acceptation.

Ingénieur système : il est chargé des tests techniques de recevabilité de la famille de certificats.

1.5 Usage des certificats

Les applications utilisatrices de ces certificats peuvent les utiliser à des fins :

§ D'authentification d'un porteur dans la phase d'authentification de SSL v3 ;

§ D'établissement d'une session chiffrée selon le protocole SSL v3 ;

§ De vérification de signature électronique au sens de la manifestation du consentement selon l'article 1316-4 du code civil ;

Les certificats objets de la présente PA sont utilisés par des applications du GIE CB pour lesquelles les risques de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données, peuvent être **faibles, moyens ou forts** selon le service accédé.

De plus, certaines applications peuvent requérir des preuves d'accès et/ou de demande d'accès à des biens qui puissent être opposables au porteur du certificat par le responsable du contrôle d'accès sur le système informatique qui héberge les biens. La définition de la forme et du fond de la constitution et de la mise en contradiction de ces preuves est du ressort de l'application au travers des conditions d'utilisation de l'application. Ces preuves doivent respecter un cadre réglementaire à l'usage des moyens informatiques mis à la disposition des porteurs. Ces conditions d'utilisation doivent être connues par les porteurs de certificat et le responsable du contrôle d'accès et des biens.

1.6 Gestion de la PA

1.6.1 Entité gérant la PA

Les promoteurs d'applications GCB sont responsables de la définition et de l'évolution de la présente PA.

Le présent document doit être validé par le RSSI du GIE CB et en particulier toute modification majeure des exigences qui y sont contenues doit être soumise à sa validation.

1.6.2 Point de contact

Groupement des Cartes Bancaires
Washington Plaza
75 408 PARIS CEDEX 08
Tél : 01.53.89.34.27
e-mail : mdrgdr@cartes-bancaires.com

1.6.3 Entité déterminant la conformité de cette PA

Les personnes responsables des audits sont issus de la direction :

Risk Management et Audit
Groupement des Cartes Bancaires
Washington Plaza
75 408 PARIS CEDEX 08

1.7 Définitions et acronymes

1.7.1 Acronymes utilisés

AC	Autorité de Certification
ADAE	Agence pour le Développement de l'Administration Electronique
AE	Autorité d'Enregistrement
CGSR	Comité de Gestion Stratégique des Risques
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DN	Distinguished Name
IGC	Infrastructure de Gestion de Clés.
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MH	Mandataire d'habilitation

OC	Opérateur de Certification
OID	Object Identifier
PC	Politique de Certification
RSSI	Responsable de la Sécurité des Systèmes d'Information

1.7.2 Objets manipulés

Biclé : une biclé est un couple de deux clés, une clé privée (devant être conservée secrète) et une clé publique, nécessaire à la mise en œuvre d'une prestation cryptographique basée sur des algorithmes asymétriques.

Certificat : clé publique d'un utilisateur, ainsi que certaines autres informations rendues infalsifiables par chiffrement avec la clé secrète de l'autorité de certification qui l'a délivrée. Le format de certificat utilisé dans le cadre de l'AC GCB est le format X.509 v3 [9594-8].

Un certificat contient des informations telles que :

§ l'identité du porteur de certificat,

§ la clé publique du porteur de certificat,

§ la durée de vie du certificat,

§ l'identité de l'autorité de certification qui l'a émis,

§ la signature de l'AC qui l'a émis,

§ l'usage de la clé.

Chaîne de certification : ensemble des certificats nécessaires pour valider la filiation d'un certificat porteur.

Déclaration des Pratiques de Certification (DPC) : énoncé des pratiques de certification (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Données d'enregistrement d'un utilisateur : ensemble d'informations nécessaires à l'enregistrement.

Dispositif d'authentification : dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée d'authentification.

Paramètres de clés publiques : données publiques relatives à l'algorithme utilisé, pour la mise en œuvre de clés privées, comme par exemple l'exposant, etc.

Politique de certification (PC) : ensemble de règles, identifié 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 à 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 les porteurs et les utilisateurs de certificats.

1.7.3 Actions

Acceptation d'une famille de certificats : l'action visant à contrôler la conformité d'une PC d'une famille de certificats donnée aux exigences d'une PA.

Audit : action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.

Contrôle de conformité à PA : ensemble d'actions consistant à vérifier que les exigences techniques, fonctionnelles et de sécurité de la PC de la famille de certificats proposée pour accéder aux applications GCB correspond aux exigences demandées dans la PA.

Génération d'un certificat : action réalisée par une AC et qui consiste à signer la clé publique et ses données associées, présentées sous la forme d'une requête de certificat éditée par l'AE.

Journalisation : fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant rend possible la traçabilité et l'imputabilité des opérations effectuées.

Révocation de certificat : action initiée par les entités habilitées et dont la conséquence est la fin de validité du certificat émis par l'AC.

Validation intrinsèque d'un certificat : ensemble des actions consistant à vérifier la validité des données de base d'un certificat comme les dates de validité, la vérification cryptographique de la signature de l'autorité, la non présence du certificat dans la LCR, etc.).

Validation d'un certificat par une application : ensemble des actions postérieures à la validation intrinsèque d'un certificat consistant à vérifier l'adéquation du niveau de sécurité du certificat avec la politique d'acceptation de l'application.

Validation d'habilitation : ensemble des actions consistant à vérifier que le porteur désigné dans le certificat préalablement validé dispose des droits pour accéder à une application donnée.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES PAR L'AC EMETTRICE

L'AC retenue par l'établissement doit mettre en œuvre au sein de son IGC une fonction d'information des utilisateurs (applications utilisatrices) pour leur donner accès aux informations devant être publiées conformément aux termes de la PRIS (PC, conditions de services, LCR, etc.).

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

Les exigences concernant le nommage sont celles de la PRIS.

3.2 Validation initiale de l'identité d'un porteur

L'AE ou le MC effectue l'enregistrement des porteurs de l'établissement selon l'organisation définie dans la DPC correspondant à l'AC choisie.

La procédure de validation initiale de l'identité d'un porteur mise en place par l'AE doit lui permettre de s'assurer de l'identité du porteur.

Applications d'un niveau de risque faible ou moyen

L'authentification du porteur peut se faire par une méthode permettant de valider l'identité du porteur sur la base soit de copie de documents officiels portant la mention "copie certifiée conforme à l'original" soit par une pré-connaissance par l'AE du futur porteur au sein d'une communauté, le porteur étant alors identifié de manière unique au sein de cette communauté.

Pour les applications d'un niveau de risque élevé

L'authentification du porteur par l'AE ou le MC est réalisée lors d'un face-à-face physique ou par une méthode apportant un degré d'assurance équivalent.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Les exigences sont celles de la PRIS.

4.1 Délivrance des clés et du certificat au porteur

Les certificats sont remis au porteur selon les exigences liées au niveau de sécurité de la famille de certificats et selon les modalités décrites dans la PC de l'AC.

4.2 Acceptation du certificat par l'application

Les certificats émis par l'AC doivent être techniquement compatibles avec les applications GCB. Des tests d'accroche du certificat à l'application font partie du processus d'acceptation de la famille de certificats.

A l'issue du processus d'acceptation la chaîne de certification de la famille de certificats est intégrée dans le module de validation de certificats.

4.3 Validation d'un certificat par l'application

Les applications GCB sont tenues d'effectuer la validation d'un certificat avant son utilisation. La méthode utilisée est de la responsabilité du promoteur d'application selon les disponibilités et les contraintes liées à son application.

Le principe général de validation consiste en deux étapes : la validation intrinsèque du certificat et la validation du certificat par l'application.

La première étape consiste à vérifier les données de base du certificat qui sont principalement sa période de validité, l'intégrité de la signature calculée sur le gabarit du certificat par l'AC ainsi que celle de la chaîne de certification et l'absence du numéro de certificat de la LCR de l'AC.

La seconde étape consiste à vérifier que la famille de certificat présentée à la validation est du niveau de sécurité requis par l'application. Les contrôles visent principalement à vérifier l'adéquation de la politique sous laquelle a été émise le certificat (niveau du certificat (*, ** ou ***) tel que défini dans la PRIS ou équivalent et support du certificat).

Les moyens mis en œuvre doivent permettre à l'application de récupérer les LCR selon une fréquence cohérente avec leur émission par l'AC et avec les exigences de fraîcheur exigées par l'application.

4.4 Utilisation du certificat par l'application

Chaque promoteur doit s'assurer que son application respecte strictement les usages autorisés des certificats. Dans le cas contraire, la responsabilité du GIE CB pourrait être engagée.

En particulier l'application a la charge d'effectuer le contrôle d'habilitation de l'utilisateur en rapprochant le nom du porteur présent dans le certificat à la liste des personnes ayant été préalablement habilitées pour une application donnée.

4.5 Renouvellement du certificat

Le renouvellement du certificat du porteur doit être transparent pour l'application et pour le porteur vis-à-vis de cette application.

4.6 Fonction de mise à disposition des LCR

Le correspondant de l'application doit s'assurer que, dans le cas d'une impossibilité de l'AC à mettre à disposition ses LCR, il sera prévenu afin d'en informer immédiatement les promoteurs des applications CB. Si cette situation devait durer le correspondant de l'application doit proposer une procédure alternative, par exemple par envoi de la LCR sur CD ROM, sans quoi l'application GCB sera dans l'obligation de ne plus accepter la famille de certificats.

Dans une telle situation, les promoteurs des applications doivent s'assurer que la famille de certificats correspondant est bloquée par les applications dès l'échéance de la LCR en cours.

Dès la remise à disposition du service de publication sur l'état des certificats et après mise à jour de la plus récente LCR le blocage de la famille de certificats est levée.

4.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR doit être de 24h minimum.

4.8 Continuité du service

En cas de dysfonctionnement partiel ou total du service[4], le seul contact du correspondant de l'application est le promoteur de l'application. Celui-ci à la charge de déterminer si l'interruption est induite par un problème lié à l'usage des certificats ou non. Si tel est le cas, après analyse de l'incident et de ses impacts en termes de sécurité, le correspondant de l'application prendra la décision de rétablir ou d'interrompre le service.

En fonction des raisons de l'incident il décidera avec les ingénieurs systèmes du GIE CB des mesures correctrices à donner.

[4] Au sens du service nominal ou au sens de l'accès par certains établissements.

5 MESURES DE SECURITE NON TECHNIQUES

Les exigences sont celles de la PRIS.

5.1 Changement de clé d'AC

5.1.1 Changement en fin de vie des clés d'AC

En cas de changement planifié d'une clé d'AC atteignant sa fin de vie, l'AC doit informer l'auditeur RMA du GCB avec un préavis minimum d'un mois et lui communiquer le nouveau certificat d'AC.

Les applications doivent prendre en compte le nouveau certificat d'AC au plus tard à la date d'entrée en application de la nouvelle clé d'AC.

La nouvelle clé d'AC sera transmise aux promoteurs des applications selon la même procédure que pour le cas initial.

5.1.2 Changement en cas de compromission des clés de l'AC du porteur

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'établissement doit en informer l'auditeur RMA du GCB.

Dès la connaissance de l'information les promoteurs des applications doivent enlever la clé d'AC de la liste des AC acceptées.

Une analyse conjointe entre les promoteurs d'applications, le correspondant métier et le responsable de l'IGC devra éclaircir les conditions ayant conduit à la compromission de la clé d'AC. La nouvelle clé d'AC ne pourra être acceptée au niveau des applications qu'à la condition expresse que les exigences organisationnelles et de sécurité présentes dans la PC avaient été correctement respectées et n'étaient pas la cause directe de la compromission. Dans le cas inverse l'acceptation de la famille de certificats pourra être retirée pour l'accès aux applications CB.

5.1.3 Changement en cas de compromission des clés d'AC GCB

Dans le cas de compromission de la clé de l'AC GCB, celle-ci activera la procédure d'escalade liée à un sinistre majeur [PROC_SM] au sein du GIE CB. Le certificat serveur des applications GCB devra être révoqué. En conséquence l'accès aux applications GCB sera suspendu jusqu'à résolution des raisons de la compromission. Il revient au promoteur d'application d'assurer la communication vers les établissements pour les informer des modalités alternatives inhérentes à cette situation (durée, mesures de contournement, etc.).

La nouvelle clé d'AC et la chaîne de certification permettant de valider le certificat serveur seront mises à disposition des correspondants d'application afin de permettre la remise en production de l'application.

5.2 Reprise suite à compromission et sinistre

Dans le cas où les conditions d'acceptation de la famille de certificats ne sont pas remises en causes la nouvelle clé d'AC sera transmise aux correspondants des applications selon la même procédure que pour le cas initial.

6 MESURES DE SECURITE TECHNIQUES

Les exigences sont celles de la PRIS.

6.1 Support des biclés

Applications d'un niveau de risque faible ou moyen

La clé privée du porteur peut être stockée soit sur le poste de travail du porteur en étant protégée de manière logicielle, soit sur support matériel tel qu'une carte à puce ou une clé USB disposant d'un composant cryptographique ou un autre support disposant du même niveau de sécurité physique et logique.

Pour les applications d'un niveau de risque élevé

La clé privée du porteur doit être protégée à l'aide d'un support matériel tel qu'une carte à puce ou une clé USB disposant d'un composant cryptographique ou un autre support disposant du même niveau de sécurité physique et logique.

6.2 Transmission de la clé publique de l'AC à l'application GCB

La chaîne de vérification de signature de l'AC est diffusée auprès de chaque application GCB par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

7 PROFILS DES CERTIFICATS ET DES LCR

Les exigences sont celles de la PRIS.

8 CONTROLE DE CONFORMITE DE LA PC A LA PA

Ce chapitre décrit le processus de demande d'acceptation initiale d'une famille de certificats pour l'accès aux applications GCB et les contrôles récurrents liés à la gestion des changements de l'AC.

8.1 Fréquences et / ou circonstances des analyses

8.1.1 Processus initial

Le processus initial consiste pour le correspondant de l'application métier à fournir au promoteur de l'application :

§ la PC de la famille de certificats utilisée par les porteurs de son établissement pour accéder à l'application ;

§ les « attestations » éventuellement obtenues d'organismes officiels ou d'auditeurs attestant de la conformité de la famille de certificats à un référentiel d'audit ;

§ les contacts du responsable de l'IGC pour une rencontre sur site dans le cas d'une AC non PRIS.

L'ingénieur système du GCB réalise ensuite des tests avec le correspondant de l'IGC pour qualifier l'accroche de la famille de certificats avec l'application.

8.1.2 Cas de modifications mineures

En cas de modification mineures soit de la PA soit des PC des AC des familles de certificats acceptées une information réciproque des parties sera effectuée au plus tard dans le mois qui suit.

Dans tous les cas, au moins une fois par an un contact entre le correspondant de l'application métier et le promoteur de l'application doit permettre d'établir si les changements intervenus sur l'IGC remettent en question la conformité de la PC à la PA.

8.1.3 Cas de modifications majeures

En cas de modification substantielle des conditions de services[5] de l'AC, celle-ci doit en informer les promoteurs des applications GCB au moins trois mois à l'avance afin d'analyser le maintien ou pas de l'acceptation des familles de certificats émis par cette AC. Le renouvellement du processus d'acceptation peut alors être demandé par le Groupement.

[5] Ces conditions peuvent être d'ordre organisationnel (statuts, actionnariat, filialisation, etc.), technique (changement majeur d'une fonction de l'AC) ou sécuritaire.

8.2 Identités / qualifications des évaluateurs

Le contrôle de conformité d'une PC à la présente PA est réalisé par une équipe d'auditeurs mandatés par le GIE CB. Les auditeurs doivent être compétents en sécurité des systèmes d'information et dans le domaine d'activité des autorités de certification.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC sur laquelle le contrôle de conformité est réalisé, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur l'ensemble des services de l'IGC liés au cycle de vie de la famille de certificats et visent à vérifier l'adéquation des mesures mises en œuvre par l'IGC aux exigences de la présente PA (procédures opérationnelles d'enregistrement, de révocation, ressources mises en œuvre, etc.).

8.5 Démarche de contrôle

Le processus complet est décrit au chapitre 11.

8.5.1 Famille de certificats référencée PRIS

Lorsqu'un établissement demande à utiliser une famille de certificats ayant déjà été référencée PRIS par l'ADAE, le contrôle de conformité de la PC à la PA consiste principalement en une analyse documentaire entre les deux documents et à des tests techniques. Le cas échéant des informations complémentaires peuvent être demandées sur le circuit d'enregistrement des collaborateurs de l'établissement.

8.5.2 Famille de certificats non référencée PRIS

Lorsqu'un établissement demande à utiliser une famille de certificats émise par une AC privée d'établissement bancaire membre du GIE CB mais n'ayant pas été référencée PRIS par l'ADAE, le contrôle de conformité de la PC à la PA consiste en :

§ une analyse documentaire entre la PC et la PA ;

§ si les auditeurs du GCB le jugent nécessaire[6], une visite sur le site de l'AC et de l'IGC. Cette visite consiste à estimer si le niveau de conformité de l'AC nécessite ou non une analyse en profondeur au regard des exigences de la PRIS.

[6] Si un établissement utilise une AC interne directement dérivée d'une AC référencées PRIS ou d'un opérateur de certification référencé PRIS, la visite sur site n'est pas nécessaire.

La démarche de contrôle ne prévoit pas que le Groupement réalise un audit de conformité complet à la PRIS. Si les auditeurs du Groupement estiment que l'AC choisie par l'établissement ne respecte pas les exigences requises, ceci sera signifié à l'établissement qui pourra soit diligenter à ses frais un audit visant à démontrer qu'il respecte bien les exigences de la PRIS, soit changer son choix d'AC.

8.6 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité (initial ou suite à évolutions), l'équipe d'audit rend, au promoteur de l'application, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Le promoteur de l'application restitue au correspondant de l'application les résultats du contrôle sur les points de non conformité. Une démarche de mise en conformité peut être planifiée entre les parties. Celles-ci conviennent d'un planning et du renouvellement du processus de contrôle (cf. chapitre 11).

Si malgré les mesures correctives le résultat du contrôle reste en "échec" ou "à confirmer", le promoteur ou le correspondant de l'application peuvent porter le problème devant le comité ad hoc du Groupement.

8.7 Communication des résultats

Les résultats des contrôles de conformité seront conservés par le GIE CB.

Dans le cas où la mise en conformité ne peut être obtenue, le comité ad hoc[7] du Groupement en est informé et peut décider de l'arrêt de l'acceptation de la famille de certificats.

8.8 Déchéance de l'acceptation d'une famille de certificat

Dans le cas où le promoteur de l'application viendrait à constater que les mesures de sécurité censées être appliquées par une AC émettant une famille de certificats ayant été préalablement acceptée sont défaillantes il serait amené à procéder aux démarches suivantes :

§ Information immédiate du correspondant de l'application des défaillances constatées avec information de l'arrêt du service pour cette famille de certificats si les mesures correctives ne sont pas rapidement entreprises par son AC ;

§ Information du comité ad hoc du Groupement si la défaillance met potentiellement le service en état de risque ;

§ Décision de cesser l'acceptation de la famille de certificats si la situation n'est pas corrigée dans les délais convenus entre les parties.

[7] Actuellement il s'agit du Comité de Gestion Stratégique des Risques (CGSR)

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

L'accès aux LCR publiées toutes les 24h est en accès libre en lecture.

9.2 Responsabilité financière

En cas de problèmes liés au certificat lui-même, la responsabilité de l'AC émettrice dudit certificat pourra être recherchée.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles au vu de l'application sont au moins les suivantes :

§ Les données personnelles sur les porteurs ;

§ Les rapports de contrôle de conformité.

9.3.2 Responsabilités en terme de protection des informations confidentielles

Les applications GCB sont tenues de respecter la législation et la réglementation en vigueur sur le territoire français.

9.4 Limite de responsabilité

Les parties ne peuvent être mises en cause en cas de dommages usuellement qualifiés « d'indirects » tels que les pertes d'exploitation et autres préjudices commerciaux ou moraux (y compris le dommage à la réputation ou à l'image).

9.5 Durée et fin anticipée de validité de la PA

9.5.1 Durée de validité

La présente PA doit rester en application jusqu'à la fin des applications GCB utilisant des certificats.

9.5.2 Gestion des évolutions de la PA

La publication d'une nouvelle version de la présente PA peut être nécessaire en fonction des évolutions apportées aux applications GCB ou en fonction de l'évolution réglementaire concernant la production des certificats de clé publique.

9.6 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC utilisée par l'établissement, le correspondant de l'application métier devra au plus tard un mois avant le début de l'opération, informer les promoteurs des applications afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC vis-à-vis de la présente PA.

Pour plus de précision voir les cas de modification mineure ou majeure évoqués au chapitre 8.1.

9.7 Amendements à la PA

En cas de changement important il est recommandé aux promoteurs des applications de se coordonner avec les correspondants des applications métier pour en contrôler l'impact.

10 RÉFÉRENCES

[9594-8] ISO/IEC 9594-8 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Authentication Framework » (Egalement Recommandation ITU-T X.509 (1997)).

NF ISO/CEI 9594-8 (1996) – « Technologies de l'information – Interconnexions de systèmes ouverts (OSI) – L'annuaire : Cadre d'authentification ».

[PRIS] Politique de Référencement Intersectorielle version 1

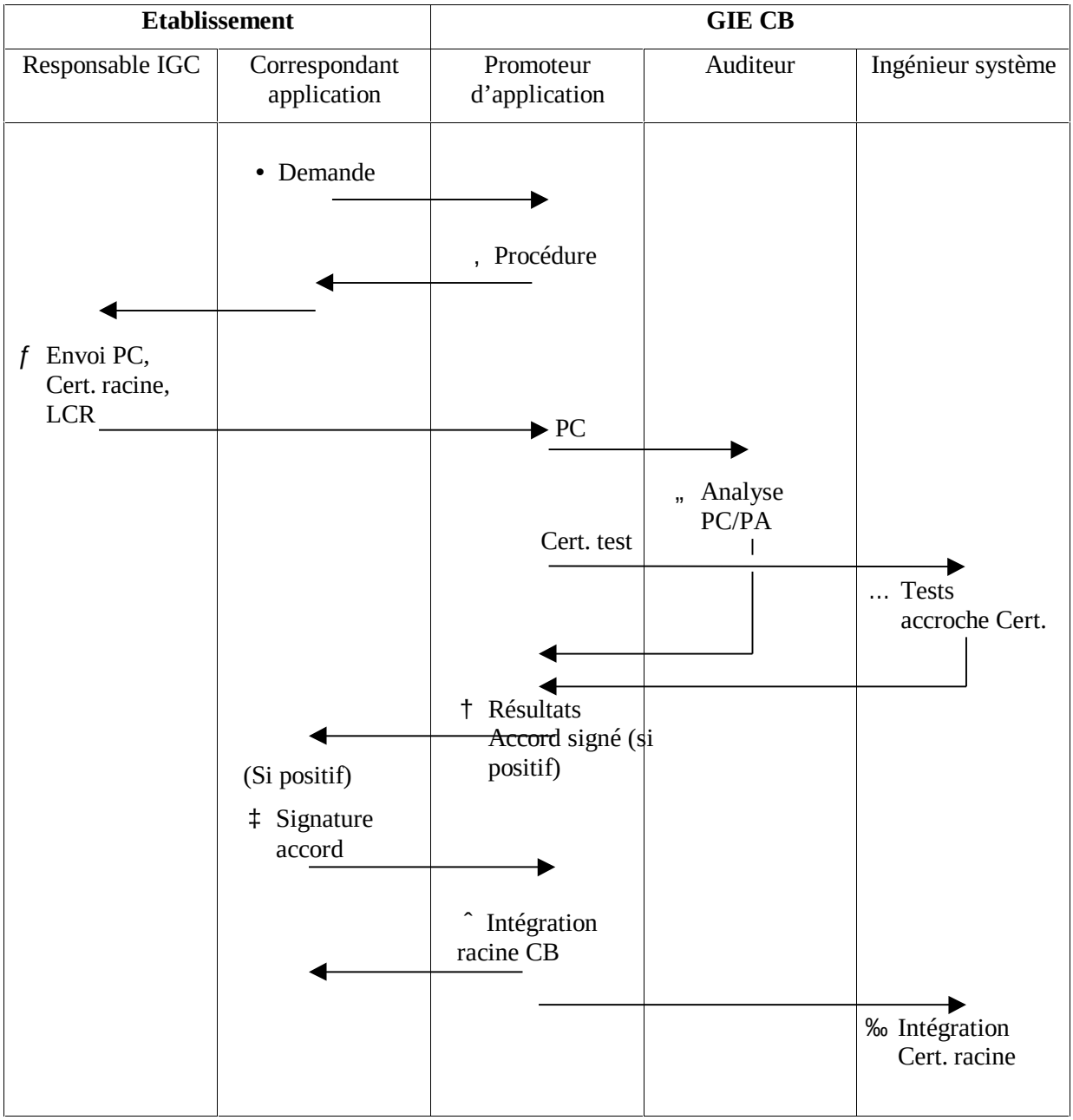
Section A Entreprise ** - Authentification ** - Signature **

[PPP] Politique de Protection du Patrimoine du Groupement des Cartes Bancaires "CB"

[PROC_SM] Procédure sur sinistre majeur au sein du GCB

11 PROCESSUS D'ACCEPTATION D'UNE FAMILLE DE CERTIFICATS

Le processus macroscopique d'acceptation d'une famille de certificats externes au GIE CB pour l'accès aux applications GCB est le suivant :



1. Demande

Le correspondant de l'application demande à faire reconnaître la famille de certificats choisie par son établissement pour accéder aux applications GCB.

2. Envoi de la procédure

Le promoteur de l'application transmet au correspondant de l'application :

§ Le processus de contrôle de conformité de la famille de certificats ;

§ La convention d'acceptation de la famille de certificats qui devra être signée par l'établissement suite à acceptation de la famille de certificats ;

§ La chaîne de certification de l'AC CB.

Dans le cadre de cet échange il demande que lui soit communiquées :

§ La PC de la famille de certificats à référencer ;

§ La chaîne de certification jusqu'à l'AC racine de l'IGC.

3. Envoi des éléments demandés

Le correspondant de l'application contacte le responsable de l'AC (interne ou externe) choisie par son établissement pour lui demander de transmettre[8] au promoteur de l'application les éléments nécessaires aux contrôles d'acceptation de la famille de certificats :

§ La PC de la famille de certificats à référencer ;

§ La chaîne de certification jusqu'à l'AC racine de l'AC

§ Les coordonnées d'un contact technique pour conduire les tests.

A réception, le promoteur de l'application transmet :

§ A l'auditeur : la PC pour analyse la conformité de la PC par rapport aux exigences de la PA ;

§ A l'ingénieur système en charge de l'application : la chaîne de certification et les coordonnées du contact technique.

4. Analyse PC/PA

L'auditeur analyse la PC de la famille de certificats de l'AC choisie par l'établissement et compare les exigences de la PA aux exigences affichées dans la PC.

Après d'éventuels contacts avec le correspondant désigné de l'AC il prépare un rapport d'analyse de conformité.

[8] En cas de téléchargement de la PC depuis le site Web de l'AC le promoteur de l'application demande la confirmation de l'OID de la PC au correspondant de l'application (le cas échéant au responsable de l'IGC).

5. Tests d'accroche des certificats.

L'ingénieur système en charge de l'application teste la vérification du certificat selon un scénario de tests prédéfinis.

Après d'éventuels contacts avec le correspondant désigné de l'AC il prépare un rapport d'analyse de conformité.

6. Résultats

Le promoteur de l'application rédige un rapport d'analyse de conformité sur la base des rapports de l'auditeur et de l'ingénieur système en charge de l'application.

Il transmet les résultats de ce rapport au correspondant de l'application.

§ Si les résultats de l'analyse sont positifs, le promoteur de l'application fait connaître à son correspondant l'accord du Groupement pour l'utilisation de la famille de certificats en lui adressant la convention d'utilisation de la famille de certificats de l'AC signée par un représentant dûment habilité du Groupement et lui demande de la lui retourner signée par un représentant dûment habilité de son établissement.

§ Si les résultats de l'analyse sont négatifs, le promoteur de l'application fait connaître à son correspondant les raisons du rejet de la famille de certificats. En fonction des raisons évoquées l'établissement prendra les dispositions nécessaires soit pour lever les réserves soit pour choisir une autre famille de certificats.

7. Signature convention

Le projet de convention signé par l'établissement est retourné par le correspondant de l'application au promoteur de l'application.

8. Intégration

Le promoteur de l'application prononce l'ouverture du service opérationnel pour la famille de certificats.

9. Intégration de la chaîne de certification de l'AC

Le promoteur de l'application demande à l'ingénieur système en charge de l'application la mise en production de la famille de certificats.