ClubPSCo

Le club des Prestataires de Services de Confiance

GUIDE RÉDACTIONNEL : PRINCIPES DE GESTION DE PREUVES

Version	Date	Description	Auteurs	Organisme
1.0	Septembre 2013	Livrable groupe de travail PGP	Etienne COMBET Jérôme BORDIER	ClubPSco

État du document	Classification
Validé	PUBLIC

SOMMAIRE

PREAMBULE

Ce document a été rédigé par l'association « *Club*PSCo », dans l'objectif d'aider, à travers un ensemble de recommandations, les porteurs d'applications (responsables de téléservices) à définir les principes de gestion de preuves pour leurs applications métier de dématérialisation.

Il est structuré sous la forme d'un guide rédactionnel, présentant, pour chacun des aspects de la gestion de preuve :

- Les éléments attendus, les points à aborder dans les documents que ces responsables devront rédiger ;
- Des exemples de contenu, dans deux cas métier typiques, que les membres de l'association ont considérés représentatif et suffisamment différents pour que le lecteur dispose d'une vue claire du type d'informations que l'on peut trouver dans un exposé des principes.

Le premier exemple métier prend le cas d'un télé-service nécessitant une gestion de preuves, bâti pour un portail de contractualisation B2C en ligne. Les clients d'une banque souscrivent à un contrat en ligne à partir de leur espace personnel privé.

Le second exemple métier est celui de la validation d'un cahier des charges technique par plusieurs parties (contexte B2B). Le cahier des charges est établi et conservé sur un système de gestion électronique de documents (GED) partagé par les différentes parties.

1.1 Qu'entend-on par « principes de gestion de preuve » ?

Les *Principes de Gestion de Preuve* (P.G.P.) décrivent les postulats, le contexte relatif à l'établissement et à la conservation d'« éléments de preuve » dans le cadre de services dématérialisés. Ils explicitent les propriétés de sécurité recherchées (intégrité, authenticité,…) et la façon dont elles sont assurées (signature électronique, horodatage, traces informatiques notamment).

La déclinaison de ces principes est à la charge du responsable du télé-service. Les documents qui seront produits pour décliner ces principes sont avant tout destinés aux successeurs de ce responsable et aux équipes participant à la mise en œuvre du téléservice.

Ces principes ont pour objectif de permettre au responsable du téléservice d'avoir une vision claire de l'argumentaire à fournir, des éléments à restituer et des moyens mis en œuvre à la date du litige, en cas de contestation.

Le document « Politique de gestion de preuve », issu de ces principes, a donc vocation à être maintenu dans le temps, pour faire apparaître les évolutions techniques, juridiques, procédurales du téléservice, et mettre en capacité son responsable de déterminer l'état des moyens mis en œuvre à une date donnée (par nature dans le passé, potentiellement plusieurs années avant).

Ce travail du ClubPSCo, visant à vulgariser ces concepts et à aider les porteurs de projet, fait notamment suite aux travaux historiques de l'AFNOR sur le sujet (standard expérimental Z74-600).

1.2 Contexte juridique : l'écrit à valeur probante

Article 1316-1 *Code civil* :

> *« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »*

Les articles 1316-1 et 1316-4 du *Code civil* constituent la base pour reconnaître la valeur juridique d'un écrit sous forme électronique. La signature électronique est donc essentielle pour les écrits sous forme électronique, parce qu'elle apporte (sous réserve du respect d'un minimum d'exigences) précisément :

- « l'identification de la personne dont il émane »
- l'intégrité de cet écrit, du moins lors de son établissement

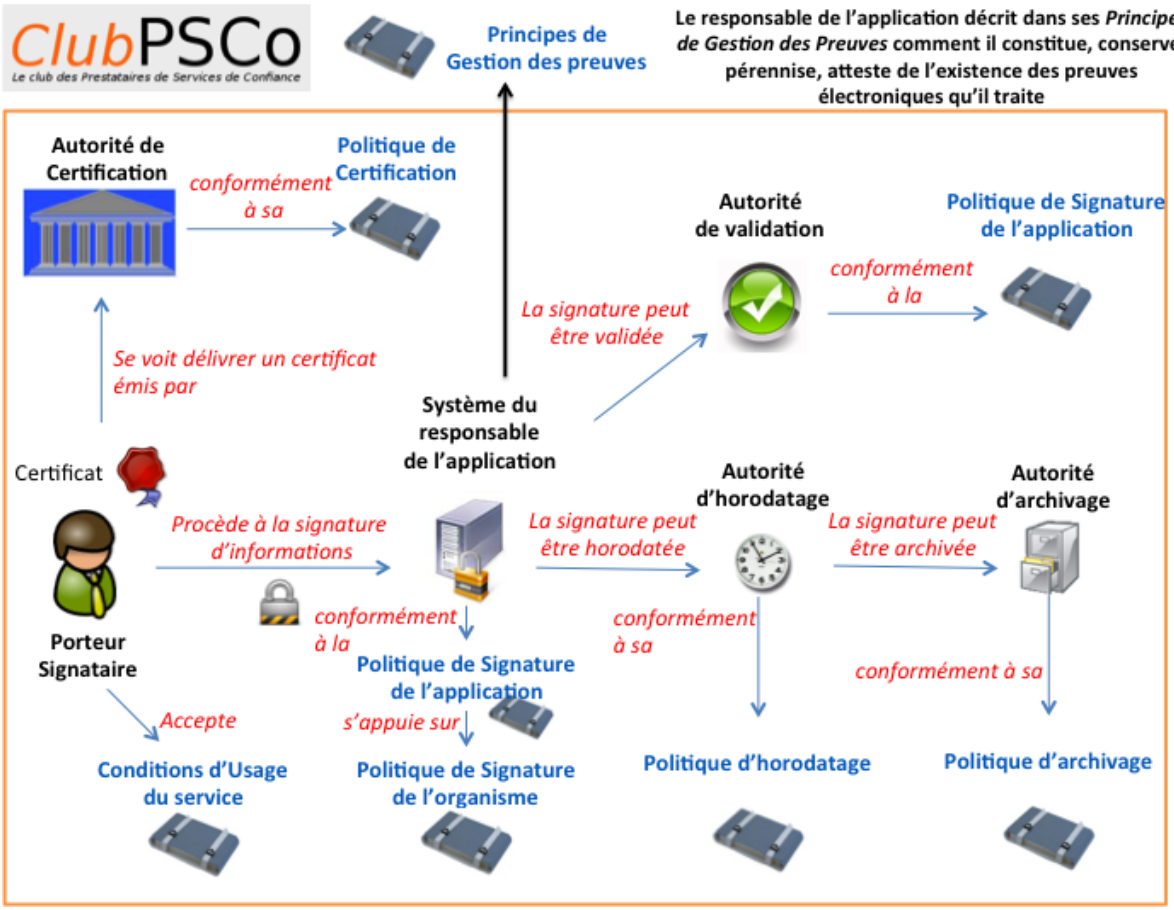
L'intégrité et la conservation de l'écrit dans le temps, relèvent de la signature ou de l'horodatage éventuellement produit sur ces transactions, et, ou de l'*archivage*, c'est pourquoi les P.G.P. s'appuieront sur des Politiques de Signature, d'Horodatage ou *d'archivage*.

1.3 Les politiques voisines

En pratique, la constitution de la preuve s'appuie sur un ou plusieurs services de confiance mis en œuvre dans le cadre du téléservice. Ces services peuvent être opérés par différents acteurs, liés entre eux par différentes conventions, lois ou contrats. Par conséquent, les P.G.P. sont potentiellement adossés aux politiques de ces services :

- Politique de certification (P.C.)
- Politique d'horodatage (P.H.)
- Politique de signature (P.S.)
- Politique d'archivage (P.A.)

Schéma de synthèse du positionnement des P.G.P. par rapport aux Politiques de confiance électronique



2 PRINCIPES DE GESTION DE PREUVE

2.1 Champ d'application des principes

À préciser en fonction du contexte d'application. Cette section est un résumé du chapitre 4.1.

Dans ce résumé, il s'agit de présenter synthétiquement le contexte et les acteurs impliqués dans la production et la conservation des preuves, en précisant le périmètre couvert par les P.G.P.

2.2 Identification des P.G.P

Le document décrivant les P.G.P. doit être identifié au moins par un numéro de version, une date de publication ou de validation, un O.I.D., etc. Cet identifiant doit permettre aux autres documents métier de s'y référer sans ambigüité et, si possible, être mentionné dans les preuves produites.

2.3 Textes juridiques applicables

- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L.013 du 19 janvier 2000, p. 12 et s.)
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968)
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.)
- Ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p.10342)
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du *Code civil* et relatif à la signature électronique (J.O. du 31 mars 2001, p. 5070)

2.4 Définitions et abréviations

A.C. – Autorité de certification

Entité en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation).

Certificat électronique (ou numérique)

Donnée établissant un lien entre une clé publique et une entité (personne morale ou physique, adresse IP ou nom de domaine). Un certificat est établi (et signé électroniquement) par un tiers de confiance (A.C.) qui atteste de ce lien.

Le standard le plus utilisé pour la création des certificats numériques est X.509.

Contremarque de temps

Donnée établissant l'existence d'une donnée informatique à une certaine heure. Une contremarque est établie (et signée électroniquement) par un tiers de confiance (A.H.), qui atteste de : l'existence de la donnée en question à l'heure dite. L'A.H. s'engage aussi sur la précision (fiabilité) de cette heure (en général, à la seconde près).

Élément de preuve

Par opposition à la preuve (notion juridique), on parle d'éléments de preuve pour désigner les données et les documents qui visent à établir la preuve. Il peut notamment s'agir de traces informatiques, de fichiers d'horodatage, de fichiers signés électroniquement ou de tout autre document, fichier, pouvant servir au porteur du téléservice à démontrer l'existence et la validité de la transaction réalisée.

I.G.C. – Infrastructure de gestion de clés

Une infrastructure de gestion de clés (*Public Key Infrastructure (PKI)* en anglais), est un ensemble de composants physiques (ordinateurs, modules cryptographiques, cartes à puces), de procédures humaines et de logiciels assurant la gestion du cycle de vie des certificats électroniques.

Non-répudiation

La non-répudiation est le fait de s'assurer qu'un contrat, notamment un contrat signé via Internet, ne peut être remis en cause par l'une des parties (*Wikipedia*). Le concept s'étend de manière plus générale à tout type d'action, d'échange ou d'accord entre deux ou plusieurs parties, sans forcément que n'intervienne de signature électronique.

Être en mesure de démontrer, prouver qu'un contrat a bien été établi entre les parties concernées consiste précisément à en assurer la non-répudiation. Ce concept rejoint en cela l'écrit à valeur probante du *Code civil* français (cf. 1.2).

OID

Identifiant d'objet *(object identifier)* prenant la forme d'une suite d'entiers séparés par des points. Les OID ont pour but d'assurer l'interopérabilité entre différents logiciels. Ils sont hiérarchisés comme un arbre, certaines branches étant affectées à un organisme ou une entité par l'*Internet Assigned Numbers Authority* (IANA, www.iana.org).

Exemple d'OID : 1.2.840.113549.1.1.5 désigne l'algorithme de signature RSA (PKCS#1, v1.5) en SHA-1. La décomposition de cet OID est la suivante :

1	Branche de l'ISO
2	Sous-branche des membres de l'ISO
840	Membres américains (Etats-Unis)
113549	Société *RSA Security Data Inc.*
1	Standard PKCS
1	Norme PKCS #1
5	Numéro de l'algorithme RSA/SHA-1

OTP-SMS

(one time password) Mot de passe à usage unique reçu par SMS, utilisé comme moyen d'authentification renforcé.

P.A.

Politique d'archivage. Document décrivant l'ensemble des éléments qui vont participer à la mise en œuvre du processus d'archivage propres à assurer qu'un document a été convenablement intégré, contrôlé, conservé, géré et consulté tout au long de son cycle de vie.

P.C.

Politique de certification. Document décrivant les règles, les exigences auxquelles doivent se conformer, s'engager, les entités impliquées dans la délivrance et la gestion des certificats numériques tout au long de leur cycle de vie.

Une P.C. est identifiée par un OID présent dans les certificats émis selon cette politique.

P.G.P. – Principes de gestion de preuve

Voir 1.1.

P.H. – Politique d'horodatage

Document décrivant les règles, les exigences auxquelles doivent se conformer, s'engager, les entités impliquées dans la délivrance de contremarques de temps (ou « jetons d'horodatage »).

Une P.H. est identifiée par un OID présent dans les contremarques émises selon cette politique.

P.S. – Politique de signature

Document décrivant les règles, les exigences auxquelles doivent se conformer, s'engager, les entités impliquées dans la production (signataires) et la validation (destinataires) de signature électroniques.

Preuve

La notion de preuve est à prendre ici au sens juridique (voir p. ex., art. 1315 du Code civil, art. 1317 pour les actes authentiques, art. 1325-26 pour les contrats sous seing privé, etc.). Par conséquent, dans ce document, on préfèrera le terme « d'éléments de preuve » pour désigner les données censées établir la preuve souhaitée.

D'autres définitions sont par ailleurs disponibles sur le site du ClubPSCo : http://clubpsco.fr/glossaire-des-termes-les-plus-utilises/

3 GESTION DES P.G.P

Ce chapitre identifie l'entité responsable du document décrivant les principes : rédaction, suivi, évolutions, diffusion. On distingue en général la gestion des P.G.P. (rédaction, validation) de leur publication (entrée en vigueur, mise à disposition des entités concernées).

D'autres aspects de la gestion des P.G.P. aussi peuvent être abordés :

- Contrôle de l'application des P.G.P.

  Par exemple, à travers des audits, lesquels ont pour objectif de permettre au porteur de l'application de s'assurer et d'assurer à ses utilisateurs la mise en œuvre correcte de mesures et de procédures lui permettant d'atteindre les objectifs énoncés dans les P.G.P.

- Veille règlementaire et juridique

3.1 Entité gérant les P.G.P.

L'entité peut être un organisme, une association, une entreprise, etc. Il s'agit souvent d'un comité ou d'un groupe de travail au sein d'une organisation.

3.2 Point de contact

Point de contact de l'entité (*e-mail*, coordonnées postales, téléphone, etc.).

3.3 Cycle de vie des P.G.P.

Si elle est formalisée, la façon dont sont amendés les principes peut être décrit dans une section spécifique. Parmi les points abordables, citons :

- Calendrier des revues
- Délais de préavis
- Périodes de commentaires
- Traitement des commentaires
- Modifications nécessitant l'adoption de nouveaux principes

Dans tous les cas, il est recommandé de préciser le délai d'entrée en vigueur des nouveaux principes, une fois ceux-ci validés.

3.4 Publication des P.G.P. et autres documents

3.4.1 Informations publiées

Il s'agit d'énumérer ici les données mises à disposition du public ; au minimum, les P.G.P. elles-mêmes.

3.4.2 Points de publication

Identifier ici les modalités d'accès à la P.G.P. et aux autres documents publiés (sur demande, adresse de site Internet, *URL*, etc.).

4 GESTION DU CYCLE DE VIE DE LA TRANSACTION ET DES ELEMENTS DE PREUVE

4.1 Objet de la preuve

Cette section décrit ce que l'on cherche à prouver, quel est le *but* visé par le processus de collecte des éléments de preuve, lesquels ne sont que les *moyens* d'établir un fait. Par exemple, dans le cas d'un écrit électronique, comme il a été rappelé en section 1.2, il y a normalement au moins deux propriétés fondamentales nécessaires pour qu'il soit admis au titre de preuve : son intégrité et l'identité de la personne dont il émane.

Selon les cas, d'autres propriétés (d'un document) peuvent être requises par les textes juridiques. Dans tous les cas, il convient donc de faire valider par une expertise juridique que les éléments de preuve collectés sont admissibles en cas de litige.

4.1.1 Intégrité d'un écrit

L'intégrité d'un document électronique est, plus encore qu'avec le papier, sujette à caution. Les deux principaux moyens pour établir l'intégrité d'un document sont : la signature électronique [1] de ce document et son enregistrement sur un support non réinscriptible (CD-ROM, disque optique, …).

En pratique, le format technique de ce document est important : un document électronique peut être dynamique, c'est-à-dire contenir du code exécutable susceptible d'altérer son contenu ou son apparence, sans que le fichier lui-même ne le soit (images animées, re-calcul de valeurs dans un tableur, etc.).

4.1.2 Identité (d'une personne, d'un serveur…)

Remarque : quand il s'agit d'établir l'identité d'une personne ou d'un serveur, on parle « d'authentification » et non « d'identification ». Il convient en effet de ne pas confondre l'identification d'une personne (établir un lien entre une connexion, une action, et une identité existant dans un annuaire) et le fait de l'authentifier (établir que c'est bien la bonne personne derrière cette identité).

Les trois principales méthodes (ou facteurs) d'authentification sont les suivantes ; on authentifie une personne sur la base de :

- soit quelque chose qu'elle sait (exemple : un mot de passe secret, une question personnelle)
- soit quelque chose qu'elle possède (exemple : une carte bleue, un téléphone portable)
- soit ce qu'elle est (biométrie : empreinte digitale, vocale, ADN, etc.)

La vérification d'identité peut s'appuyer sur un seul ou sur plusieurs de ces facteurs.

L'authentification d'une personne sur Internet est un domaine en plein développement. Le couple (identifiant/mot de passe) à tendance à être remplacé par des systèmes alternatifs (authentification à deux facteurs).

[1] Une signature « technique » (cachet serveur) suffit. Autrement dit, ce n'est pas forcement une signature au sens du *Code civil*.

Dans le cas d'une signature électronique, c'est au certificat électronique qu'incombe la charge d'authentifier le signataire.

4.1.3 Date

La date d'établissement d'un contrat ou celle du dépôt d'une réponse à un appel d'offre peut être requise par les textes (clauses de validité). On recourt pour cela en général à l'horodatage, dès lors que les traces techniques s'avèrent insuffisantes.

4.1.4 Autres exemples de propriétés

- le fait que le signataire d'un document a pu en prendre connaissance (consentement libre et éclairé d'un client)
- le fait que le signataire d'un document est majeur
- le fait qu'il se trouve sur le territoire français

4.2 Transaction et éléments de preuve

4.2.1 Description de la transaction

Cette section décrit le contexte dans lequel les éléments de preuve sont produits. Elle présente les données, les supports et les informations susceptibles d'être des éléments de preuve dans le contexte en question, quels sont les acteurs impliqués dans la création et la gestion de ces éléments.

Pour chaque propriété de sécurité précédemment identifiée, la P.G.P. doit expliquer dans quelle mesure les éléments de preuve ou, le cas échéant, la combinaison d'éléments de preuve, permettent de démontrer la propriété souhaitée.

4.2.2 Éléments de preuve soumis aux P.G.P.

Cette section décrit, techniquement, les éléments de preuve concernés par les présents principes. Elle identifie donc, dans le contexte précédemment présenté, quelles sont les données qui font office de preuve (le cas échéant, pour quel acteur) et qui seront traitées comme telles.

Il peut être pertinent de distinguer entre les éléments dépendant de la transaction et les éléments existant dans l'absolu. Exemple : un jeton d'horodatage concerne une opération donnée (élément transactionnel), tandis que la politique d'horodatage associée concerne un ensemble d'opérations (élément non transactionnel).

4.2.3 Données non concernées par les P.G.P.

Cette section énumère, le cas échéant, les éléments de preuve exclus du périmètre d'application des principes. Cette section peut aussi rappeler les informations ou données qui ne sont pas considérées comme des éléments de preuve en justifiant, à titre informatif, leur exclusion du périmètre.

4.3 Cycle de vie des éléments de preuve

Cette section décrit le processus de constitution des éléments de preuve, étape par étape.

4.3.1 Processus de constitution et de collecte des éléments de preuve

Cette section décrit précisément les canaux de réception des éléments de preuve :

- Quel élément de preuve est fourni par quel acteur ?
- Où, quand, et par qui sont agrégés ces éléments de preuve ?
- Quelles sont les mesures assurant l'intégrité et l'authenticité de ces éléments ?
- Sous quelle forme ces éléments sont-ils enregistrés, collectés ou échangés entre les acteurs ?
- Quelles sont les vérifications effectuées, et par qui, pour s'assurer de la valeur probante de ces éléments ?

4.3.2 Versement, conservation et restitution des éléments de preuve

Cette section décrit :

- les modalités de transmission d'un ou plusieurs éléments de preuve à un service d'archivage, aux utilisateurs ou, de manière générale, aux entités en charge de leur conservation.
- le cas échéant, les modalités de restitution de ces éléments aux acteurs concernés

Elle rappelle les principales caractéristiques de la politique d'archivage appliquée aux preuves ou, à défaut, identifie celle-ci sans ambiguïté. Ces caractéristiques sont :

- la politique d'archivage appliquée
- le cas échéant, les coordonnées du tiers archiveur (ou du service interne)
- la durée de conservation des archives

4.3.3 Consultation des éléments de preuve

Cette section décrit précisément les modalités envisageables pour consulter les éléments de preuve :

- Qui peut les consulter ?
- Dans quelles conditions ?
- En fonction des éléments consultable par les différentes parties, quels sont les propriétés de sécurité qu'elles peuvent vérifier (partie par partie).

4.3.4 Pérennisation des éléments de preuve

Cette section décrit les mesures mises en œuvre pour assurer la conservation à moyen ou long terme des éléments transactionnels de preuve, « dans des conditions de nature à en garantir l'intégrité ». Ces mesures peuvent être décrites dans une politique d'archivage, auquel cas il suffit de s'y référer.

4.3.5 Vérification des éléments de preuve

Cette section décrit précisément les modalités envisageables pour vérifier chacun des éléments de preuve :

- Qui peut le vérifier ?
- Dans quelles conditions, notamment.

4.3.6 Durées de validité des éléments de preuves

Cette section précise deux périodes de temps. D'une part, la période durant laquelle les éléments de preuves peuvent être validés. Par exemple, dans le cas d'un fichier signé électroniquement, on indiquera ici la période de vérification *autonome* de la signature électronique. Si les éléments de preuve font l'objet de signatures complémentaires à intervalles réguliers (format AdES-A), il peut être intéressant de le rappeler ici.

D'autre part, le cas échéant, les données archivées auprès du tiers peuvent constituer une preuve à long terme dans la mesure où leur intégrité, leur lisibilité et leur authenticité peuvent être assurées, indépendamment de la validité cryptographique des signatures qu'elles contiennent (exemple : archivage sur disque non-réinscriptible à date prouvable). Dans ce cas, il importe de le mentionner ici aussi.

4.3.7 Modalités d'acceptation des éléments de preuves

Cette section décrit les modalités de réception et d'acceptation des éléments de preuve par les acteurs concernés et, notamment, si celle-ci est implicite ou explicite.

Cette section mentionne notamment les éventuelles conventions de preuve existant entre les parties, et les éléments de preuve auxquelles elles font référence.

5 OBLIGATIONS ET RESPONSABILITES DANS LE CYCLE DE VIE DES ELEMENTS DE PREUVE

5.1 Obligations des acteurs en matière de gestion des éléments de preuve

Cette section contient généralement une section par acteur. Quelques exemples sont donnés ci-dessous.

5.1.1 Exigences relatives aux A.C. fournissant les certificats

Cette section décrit les contraintes que se fixe le porteur d'application quant aux A.C. fournissant les certificats intervenant dans son service (niveaux de certification, type de certificat, etc.). Une référence à une P.C. ou à une norme est possible.

5.1.2 Exigences relatives à l'archiveur

Cette section décrit les attentes du porteur d'application vis-à-vis de son archiveur ou de ses services d'archivage.

5.1.3 Obligations des utilisateurs du service

Cette section peut reprendre ou citer les *Conditions générales d'utilisation* (C.G.U.) du service, si elles existent et sont accessibles au même titre que la P.G.P.

5.2 Limites de responsabilités du porteur d'application

À compléter selon les besoins.

6 FORMAT DES ELEMENTS DE PREUVE

Le format des différents éléments de preuve est décrit en 4.3.2 mais peut être optionnellement repris ici de façon plus technique (détail sur le codage des données, leur structure ou format technique, etc.). Cette section pouvant contenir des informations confidentielles, il est possible de documenter le format des éléments de preuve traités dans un document annexe, non publié.

Par exemple, si certains éléments sont scellés techniquement par une signature électronique, le ou les formats de signature utilisés pour cela (p. ex., XAdES, en précisant le numéro de version), ainsi que leurs caractéristiques techniques éventuelles (champs présents, champs absents, etc.) peut être rappelé.

Idem. pour le type de signature (RSA, DSA...) et les algorithmes d'empreinte, les certificats de signature ou d'horodatage, etc.

1 ANNEXE : EXEMPLE METIER N^{O} 1

1.1 Principes de gestion de preuve

1.1.1 Champ d'application des principes

Les présents principes concernent la contractualisation en ligne des clients de la banque ALPA BANK. Ils ont pour objet d'assurer la non-répudiation des contrats souscrits par ses clients.

1.1.2 Identification des P.G.P.

Les présents principes sont identifiés par l'OID suivante : …

1.1.3 Textes juridiques applicables

- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L.013 du 19 janvier 2000, p. 12 et s.)
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968)
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.)
- Ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p.10342)
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du *Code civil* et relatif à la signature électronique (J.O. du 31 mars 2001, p. 5070)

1.2 Gestion des P.G.P

1.2.1 Entité gérant les P.G.P.

Le présent document décrivant les P.G.P. est gérée par la DSI de ALPA BANK.

1.2.2 Point de contact

DSI / ALPA ONLINE BK

ALPA BANK GROUP

278 rue des Helvètes

23100 Le Mas-d'Artige

FRANCE

e-mail : dsi-contact@ALPA-bank.fr

1.2.3 Cycle de vie des P.G.P.

Le présent document est revu et validé par le comité projet sur demande du chef de projet ALPA ONLINE. Il est formellement validé avant publication par le directeur de la DSI.

1.2.4 Publication des P.G.P. et autres documents

1.2.4.1 Informations publiées

La version applicable de la P.G.P. est mise à disposition des clients de la banque ALPA sur son site Internet (voir section suivante) par la DSI, suite à l'approbation d'une nouvelle version.

1.2.4.2 Points de publication

La P.G.P. en vigueur est disponible à l'adresse suivante : *http://online.ALPA-bank.fr/legal/documents/pgp-current.pdf*

Les versions précédentes de la P.G.P. sont disponibles à l'adresse suivante : *http://online.ALPA-bank.fr/archive/legal/documents/pgp* ou sur demande auprès du point de contact identifié en section 1.2.2.

1.3 Gestion du cycle de vie de la transaction et des éléments de preuve

1.3.1 Objet de la preuve

L'objet des éléments de preuve est de démontrer qu'un client donné d'ALPA BANK a souscrit un contrat de service donné en ligne (non-répudiation du contrat). Le principal élément de preuve est le contrat lui-même, signé électroniquement par le client : cette signature électronique assure l'identité du client et l'intégrité de l'écrit, conformément aux exigences de l'article 1316-4 du *Code civil*.

1.3.2 Transaction et éléments de preuve

1.3.2.1 Description de la transaction

La contractualisation se déroule comme suit :

a. Le client s'authentifie sur le site de la banque (HTTPS) et accède à son espace personnel. Cette authentification est basée sur un couple numéro de compte/mot de passe établi lors de l'ouverture du compte dans une agence du réseau ALPA BANK.

À cette occasion, une clé USB contenant une biclé et un certificat de signature à son nom lui a été remis en mains propres, conformément à la politique de certification du service SIGN-ON (OID : 1.2.3.4.5.6.7.8.9).

b. Le client sélectionne un contrat de service et coche les options associées.

c. Le client est redirigé sur le service de signature en ligne SIGN-ON.

d. Un récapitulatif (fac-similé de contrat papier, au format PDF) lui est présenté par le site. Le client a la capacité de le télécharger sur son poste.

e. Pour confirmer sa souscription, le client doit cocher une case d'acceptation des conditions générales, lesquelles sont disponibles à travers un lien hypertexte. Ces conditions générales font référence à la présente P.G.P.

g. Ensuite, le client procède à la signature électronique du contrat PDF sur son poste en utilisant son certificat électronique. Le PDF signé est transmis à la plate-forme, laquelle vérifie la signature avant de l'horodater.

h. Ultérieurement, tous les contrats signés sont archivés en même temps que les traces de connexion entre le portail et le poste du client, le portail et la plate-forme SIGN-ON.

1.3.2.2 Éléments de preuve soumis aux P.G.P.

1.3.2.2.1 Éléments transactionnels

Les éléments de preuve produits par le processus précédent sont les suivants :

[P_1] Traces de connexion du client (sur la plate-forme ALPA BANK ONLINE)

[P_2] Traces des requêtes de signature (plate-forme SIGN-ON)

[P_4] Le contrat PDF (produit par la plate-forme ALPA BANK ONLINE)

[P_5] Signature client sur le contrat PDF (conservée sur la plate-forme ALPA BANK ONLINE)

[P_6] Jeton d'horodatage de la signature client (avec [P_5])

[P_7] Réponse OCSP reçu pour s'assurer de la validité du certificat utilisé pour signer

1.3.2.2.2 Éléments de preuve permanents

En complément des éléments précédents, les données suivantes sont des éléments de preuve à part entière :

[PP_1] Politique de signature du service SIGN-ON (OID : 9.8.7.6.5.4.3.2.1)

[PP_2] Politique de certification du service SIGN-ON (OID : 1.2.3.4.5.6.7.8.9)

[PP_3] Politique d'horodatage du service EVERTIME (OID : 1.3.0.2.0.3.1.3.3.1)

[PP_4] Politique d'archivage du service EVERTIME (OID : 3.1.4.1.5.9.2.6.5.3)

1.3.2.3 Données non concernées par les P.G.P.

Les traces de demande des jetons d'horodatage ne sont pas soumises aux présents principes. Le jeton d'horodatage lui-même est considéré comme un élément de preuve suffisant et autonome.

Pareillement, les données d'authentification de l'utilisateur (annuaire de la plate-forme ALPA BANK ONLINE) et son dossier bancaire ne sont pas concernés par les présents principes. La façon dont est établie l'identité du client lors de l'établissement de son compte et la mise à jour de ces informations dans le S.I. de ALPA BANK font l'objet de procédures et de contrôles indépendants du présent contexte. Ces éléments sont considérés comme acquis dans le cadre des présents P.G.P.

Les traces des traitements des requêtes de signature de la plate-forme SIGN-ON sont considérées comme faisant double-usage avec [P_2] et sont couvertes par la politique de signature de SIGN-ON.

1.3.3 Cycle de vie des éléments de preuve

1.3.3.1 Processus de constitution des éléments de preuve

1.3.3.1.1 Traces de connexion du client

Les traces de connexion du client [P_1] rassemblent les traces techniques produites par la plate-forme ALPA ONLINE (traces de connexion SSL : date et heure de connexion, adresse IP du client) et les traces métier de session (identifiant du compte, cookie de session). La déconnexion est aussi tracée.

Ces données sont enregistrées sous forme de fichiers « *syslog* » compressés sur les serveurs de la plate-forme ALPA ONLINE. Ces fichiers sont protégés (intégrité, confidentialité) via les politiques de contrôle d'accès de cette plate-forme.

1.3.3.1.2 Traces des requêtes de signature

Les traces des requêtes de signature [P_2] rassemblent les traces techniques produites par la plate-forme ALPA ONLINE lorsqu'elle transmet un contrat PDF pour signature à la plate-forme SIGN-ON (traces de connexion SSL : date et heure de connexion, adresse IP/FQDN de la plate-forme SIGN-ON) et les traces métier de l'appel Web Service (données d'établissement du certificat éphémère de l'utilisateur, empreinte du contrat PDF). La réponse à cet appel est aussi tracée.

Ces données sont enregistrées sous forme de fichiers « *syslog* » compressés sur les serveurs de la plate-forme ALPA ONLINE. Ces fichiers sont protégés (intégrité, confidentialité) via les politiques de contrôle d'accès de cette plate-forme.

Si le processus de contractualisation est interrompu, ces traces contiennent les causes de l'erreur.

Remarque : ces traces contiennent, entre autre, le numéro de téléphone auquel est envoyé le SMS contenant le code autorisant la requête de signature.

1.3.3.1.3 Contrat PDF

Le contrat (fichier PDF) est constitué par le portail ALPA ONLINE suite aux actions du client en ligne. Une version est ensuite transmise pour signature à la plate-forme SIGN-ON.

Lorsque le fichier signé est renvoyé par celle-ci, il est comparé avec le PDF initial, et la signature est vérifiée. Cela permet à ALPA BANK de s'assurer que, d'une part, le contrat signé par le client n'a pas été altéré avant signature et, d'autre part, que la signature [P_5] est présente et répond aux exigences attendues.

La version signée constitue l'élément [P_4]. Si les vérifications précédentes échouent, cet élément de preuve est inexistant, mais [P_2] contient les traces de cet échec.

1.3.3.1.4 Signature client

Cet élément est contenu dans [P_4] et est autonome : son authenticité et son intégrité sont assurées par les mécanismes cryptographiques de la signature électronique. Cet élément assure aussi l'identité du signataire.

1.3.3.1.5 Jeton d'horodatage

Cet élément est contenu dans [P_4] et est autonome : son authenticité et son intégrité sont assurées par les mécanismes cryptographiques de la signature électronique du jeton. Cet élément porte la date et l'heure de la signature du client. Il est structuré au format défini par la norme RFC3161.

La politique d'horodatage (P.H.) associée est la P.H. du service EVERTIME (OID : 1.3.0.2.0.3.1.3.3.1).

1.3.3.1.6 Établissement des éléments de preuve

Voir 1.3.3.6.

1.3.3.2 Versement, conservation et restitution des éléments de preuve

Les éléments [P_1], [P_2], [P_4], [P_5] et [P_6] sont transmis quotidiennement au service d'archivage ETERNITY selon le protocole défini dans la politique d'archivage [PP_4].

Conformément au contrat de service passé entre la société ETERNITY et ALPA BANK, ces éléments sont conservés durant 10 ans. Les modalités de restitution à ALPA BANK sont décrites dans la P.A. susmentionnée.

Les archives peuvent être demandées par les clients selon les modalités décrites dans les C.G.U. du service : ETERNITY, 17 rue du Lac, 12000 Rodez, France

1.3.3.3 Consultation des éléments de preuve

Les éléments [P_4], [P_5] et [P_6] sont mis à disposition du client sur son espace personnel sous la forme du contrat signé [P_4] ; ce document est librement téléchargeable par le client pendant toute la durée de validité du contrat.

Comme mentionné dans les C.G.U., il appartient au client de conserver un exemplaire au-delà de cette période.

Les éléments [P_1], [P_2] sont utilisés mensuellement dans le cadre de la surveillance des services par ALPA BANK et ses prestataires. Ils sont ensuite supprimés et ne sont accessibles qu'auprès du service d'archivage.

Toute demande concernant les autres éléments de preuve doit être faite par écrit au point de contact indiqué dans la section 1.2.21.3.3.2

Aucune preuve ne sera consultable au-delà du délai de conservation mentionné en 1.3.3.2.

1.3.3.4 Pérennisation des éléments de preuve

La pérennisation des éléments [P_1], [P_2], [P_4], [P_5] et [P_6] est décrite dans la politique d'archivage [PP_4]. Cette pérennisation concerne les éléments archivés par ALPA BANK ; les éléments mis à disposition du client sont sous la responsabilité de ce dernier.

1.3.3.5 Vérification des éléments de preuve

La vérification de la preuve est possible sur demande formulée au responsable identifié au §1.2.2. Les principes suivants s'appliquent :

Il n'y a pas de vérification de [P_1], [P_2] autre que la consultation des éléments archivés.

La vérification de [P_4] et [P_5] (contrat PDF signé) peut être réalisée de façon autonome par un logiciel de vérification de signature électronique durant toute la durée de vie du jeton d'horodatage [P_6]. Au-delà de cette période, ce sont les modalités d'archivage qui précisent la façon de vérifier ces éléments.

Pour la vérification du jeton d'horodatage [P_6], se référer à la politique d'horodatage du service EVERTIME [PP_4].

1.3.3.6 Établissement des éléments de preuve

L'objet de la preuve est de démontrer la réalité d'un contrat établi entre le client et ALPA BANK, aux conditions définies dans celui-ci. L'authenticité de cet écrit et l'identité du signataire sont assurées par la signature électronique ([P_5], [P_6]) du document [P_4].

Les éléments [P_1], [P_2], [P_4], [P_5] et [P_6] sont établis et conservés durant 48 heures sur les serveurs de ALPA BANK. Passé un délai de 24 heures, les L.C.R. suivantes sont examinées :

- L.C.R. de l'autorité de certification du service SIGN-ON [PP_2]
- L.C.R. de l'autorité de certification des unités d'horodatage du service EVERTIME [PP_3].

La plate-forme de ALPA BANK vérifie ainsi que ni le certificat de signature du client ni celui du jeton n'ont été révoqués durant la période de grâce. Les L.C.R. sont jointes aux éléments de preuve.

Le versement de ces éléments au service d'archivage constitue l'établissement de la preuve ; il est décrit dans la politique d'archivage d'ETERNITY [PP_4].

Remarque : au cas où l'un des certificats aurait été révoqué ou aurait expiré préalablement à la signature du contrat, le processus de versement est maintenu. En revanche, ALPA BANK contacte alors le client concerné pour dénoncer le contrat, qui n'est pas considéré comme établi.

1.3.3.7 Durées de validité des éléments de preuves

Le certificat électronique du client, conformément à politique de certification du service SIGN-ON [PP_2] est établi pour une durée de 3 ans. La signature électronique est horodatée par le service EVERTIME selon sa politique d'horodatage [PP_3], lequel produit des jetons dont la durée de validité est de 5 ans.

Les signatures des contrats sont donc vérifiables de manière autonome durant 5 ans. On rappelle à cette occasion que les L.C.R. « du lendemain » sont jointes aux éléments de preuve.

Au-delà de cette période, l'intégrité et l'authenticité des éléments de preuve sont assurées par les mesures d'archivage et de restitution d'ETERNITY.

1.3.3.8 Modalités d'acceptation des éléments de preuves

Le client reconnaît explicitement les éléments de preuve à travers sa signature des C.G.U.

1.4 Obligations des acteurs en matière de gestion des éléments de preuve

1.4.1 Obligations de ALPA BANK ONLINE

ALPA BANK ONLINE est responsable vis-à-vis de ses utilisateurs des opérations relatives à la gestion de la preuve réalisées par les composantes de son infrastructure. Elle garantit le contenu des éléments de preuve et leur intégrité.

ALPA BANK ONLINE veille à ce que l'ensemble des prestataires intervenant dans la gestion de preuve respectent les exigences de la présente politique.

ALPA BANK ONLINE s'engage à documenter les relations contractuelles, les versions des contrats avec ses utilisateurs, les conditions d'utilisation du service et la convention de service.

ALPA BANK ONLINE s'engage à être en mesure de répondre aux contrôles techniques et audits de qualité des procédures qui pourraient lui être demandés dans le cadre des obligations légales et de ses engagements.

ALPA BANK ONLINE doit mettre à jour et préserver l'intégrité des documents qu'elle publie.

ALPA BANK ONLINE doit assurer le contrôle de conformité de ses propres pratiques par rapport aux présents principes.

1.4.2 Exigences relatives aux A.C. fournissant les certificats

1.4.2.1 A.C. des certificats de signature clients

Les certificats utilisés pour produire des signatures client doivent contenir les éléments suivants :

- l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi
- les noms et prénoms du signataire et, le cas échéant, une donnée permettant de résoudre les cas d'homonymie
- l'indication du début et de la fin de la période de validité du certificat
- le numéro de série du certificat

La taille des biclés RSA ne saurait être inférieure à 2048 bits.

L'algorithme d'empreinte utilisé pour signer ces certificats doit être SHA-256.

1.4.2.2 A.C. des certificats de scellement des preuves (archives)

Les certificats doivent être conformes à l'état de l'art en matière de sécurité et de réglementation.

1.4.2.3 Autorité d'horodatage

La précision garantie par les services d'horodatage utilisés pour horodater les signatures clients ou les archives doit être inférieure ou égale à la seconde.

La durée de validité des jetons d'horodatage doit être supérieure ou égale à 3 ans.

1.4.3 Exigences relatives à l'archiveur

Aucune exigence particulière sur l'archiveur.

1.4.4 Obligations des utilisateurs du service

Aucune exigence particulière autre que celles relatives à l'utilisation du certificat et décrites dans la politique de certification.

1 ANNEXE : EXEMPLE METIER N^{O} 2

1.1 Principes de gestion de preuve

1.1.1 Champ d'application des principes

Les présents principes concernent la validation d'un cahier des charges techniques élaboré de façon collaborative par un groupe de travail. La validation consiste à figer le document dans sa version actuelle ; elle intervient lorsque tous les membres du groupe l'ont approuvé.

Lorsque la société Yodasoft élabore un cahier des charges en partenariat avec ses sous-traitants et clients, il est fréquent qu'un espace collaboratif soit utilisé à cette fin dans le système de gestion électronique de document (GED) de la société. Les différents partenaires disposent d'un compte leur permettant de travailler en commun sur le cahier des charges.

L'accès à cet espace de travail n'est ouvert qu'après signature d'une convention de preuve entre les parties.

Le présent document est une annexe de cette convention de preuve.

1.1.2 Identification des P.G.P

Les présents principes sont identifiés par l'OID suivante : …

1.1.3 Textes juridiques applicables

…

1.2 Gestion des P.G.P

1.2.1 Entité gérant les P.G.P.

Le présent document décrivant les P.G.P. est gérée par la DSI de Yodasoft.

1.2.2 Point de contact

Yodasoft / DSI

23 rue des lumières

92320 Châtillon

e-mail : pgp-dsi@yodasoft.com

1.2.3 Cycle de vie des P.G.P.

Le présent document est revu et validé par le groupe « Travail collaboratif » du pôle communication. Il est formellement validé par le chef de pôle.

1.2.4 Publication des P.G.P. et autres documents

1.2.4.1 Informations publiées

La P.G.P. n'est pas publique. Le document est mis transmis aux partenaires de Yodasoft concernés dans le cadre de la convention de preuve établie entre les partenaires.

1.2.4.2 Points de publication

Sans objet.

1.3 Gestion du cycle de vie de la transaction et des éléments de preuve

1.3.1 Objet de la preuve

Le processus de validation du cahier des charges a pour but de prévenir toute contestation future sur son contenu en :

- figeant la version du cahier des charges,
- obtenant l'approbation formelle de chacune des parties sur cette version.

1.3.2 Transaction et éléments de preuve

1.3.2.1 Description de la transaction

Lorsque le groupe de travail a terminé la rédaction du cahier des charges sur le portail, le chef de projet de Yodasoft place les version finales des différents documents constituant le cahier (spécifications fonctionnelles au format PDF, diagrammes de conception et d'architecture au format PNG, etc.) dans un répertoire donné, dit « répertoire d'approbation ». Le contenu du répertoire est compressé (fichier ZIP) et scellé par un cachet serveur horodaté.

Ensuite, chacun des utilisateurs habilités à approuver le cahier se connecte à la GED et procède à l'approbation du répertoire en cliquant sur un bouton « approuver ces documents ». L'approbation n'est effective qu'après la saisie d'un OTP-SMS par l'utilisateur, ce qui assure l'authentification renforcée de ce dernier.

Lorsque tous les approbateurs requis ont approuvé le cahier des charges, un second cachet serveur est apposé sur les traces d'authentification OTP-SMS de chacun des utilisateurs. Ces traces contiennent une heure fournie par l'opérateur de téléphonie et considérée comme suffisamment fiable par les partenaires.

1.3.2.2 Éléments de preuve soumis aux P.G.P.

1.3.2.2.1 Éléments transactionnels

Les éléments de preuve produits par le processus précédent sont les suivants :

[P_1] Répertoire compressé, scellé et horodaté contenant les fichiers constitutifs du cahier des charges

[P_2] Traces des scellées des authentifications OTP-SMS des utilisateurs

1.3.2.2.2 Éléments de preuve permanents

En complément des éléments précédents, les données suivantes sont des éléments de preuve à part entière :

[PP_1] Politique de cachet serveur et d'horodatage (OID : …)

[PP_2] Spécifications fonctionnelles de l'application « répertoire d'approbation » de la GED

[PP_3] Conventions de preuve entre les partenaires de Yodasoft

1.3.2.3 Données non concernées par les P.G.P.

Les traces de connexion des utilisateurs sur la GED ne sont pas considérées comme des éléments de preuve, l'authentification via OTP-SMS répondant à l'exigence d'authentification forte des approbateurs.

1.3.3 Cycle de vie des éléments de preuve

1.3.3.1 Processus de constitution des éléments de preuve

1.3.3.1.1 Cahier des charges

L'élément [P_1] assure l'intégrité et l'authenticité de l'écrit que constitue le cahier des charges.

Cet élément est créé au début du processus d'approbation, par le chef de projet Yodasoft. Le scellement et l'horodatage du cahier assurent la valeur probante de cet écrit.

1.3.3.1.2 Traces d'approbation

L'élément [P_2] assure l'authentification des personnes et leur approbation. Ces traces sont conservées sur la plate-forme Yodasoft et sont scellées lorsque le dernier utilisateur requis valide le cahier des charges. Leur intégrité jusqu'à cette étape est assurée par le contrôle d'accès de la GED.

1.3.3.2 Versement, conservation et restitution des éléments de preuve

Les éléments de preuve sont conservé sur la plate-forme Yodasoft et restent accessible à tous les partenaires durant toute la durée de vie du projet. Il n'y a, par conséquent, aucune procédure de versement ou de restitution spécifique.

Chaque utilisateur/partenaire concerné peut en télécharger une copie.

Chaque partenaire possède une copie de la convention de preuve.

1.3.3.3 Consultation des éléments de preuve

Sans objet (voir ci-dessus).

1.3.3.4 Pérennisation des éléments de preuve

La GED dispose d'un système re-scellant et ré-horodatant à intervalle régulier (tous les trois ans) les cahiers des charges approuvés, avant que les cachets et les jetons d'horodatage n'expirent.

Un cahiers des charges est re-scellé au plus trois fois, ce qui assure une durée de vie de douze ans.

1.3.3.5 Vérification des éléments de preuve

Les sceaux et l'horodatage assurent l'autonomie des éléments de preuves ainsi protégés.

1.3.3.6 Établissement de la preuve

Voir ci-dessus.

1.3.3.7 Durées de validité des preuves

Un cahiers des charges est re-scellé au plus trois fois, ce qui assure une durée de vie de douze ans.

1.3.3.8 Modalités d'acceptation des preuves

Celles-ci sont établies dans les conventions de preuve reconnues par les différentes parties.

1.4 Obligations des acteurs en matière de gestion de la preuve

Ces obligations sont décrites dans les conventions de preuve établies entre les partenaires.

1.5 Format des éléments de preuve

Les formats des fichiers admis dans un cahier des charges sont : PDF/A, JPEG, PNG. Tout document dans un autre format est considéré comme nul et ne faisant pas partie du cahier des charges, quand bien même il serait présent dans le fichier compressé et scellé.

Les traces d'authentification des utilisateurs sont des fichiers « texte » (codage UTF-8) suivant le modèle :

```
Phone number : %0

Hello %1,

Your approbation code for the CDC %2 is : %3

That code is valid until %4
```

Dans ce modèle,

- Le champ `%0` correspond au numéro de téléphone de l'approbateur habilité
- Le champ `%1` est remplacé par le nom et le prénom de l'approbateur habilité
- Le champ `%2` identifie de manière unique le cahier des charges
- Le champ `%3` est le code d'approbation
- Le champ `%4` est la durée de validité de ce code

Ce modèle est la copie du SMS envoyé à l'utilisateur au numéro indiqué. Lorsque celui-ci approuve dans les temps, une seconde trace est produite par la plate-forme :

```
From user : %0

Approbation code %1 received at %2
```

Dans laquelle :

- `%0` correspond à l'identifiant de l'approbateur sur la plate-forme
- `%1` est le code saisi par l'utilisateur sur la plate-forme
- `%2` est l'heure de la plate-forme au moment de l'approbation

2 ANNEXE : EXEMPLE METIER N^{O} 3

2.1 Principes de gestion de preuve

2.1.1 Champ d'application des principes

Les présents principes concernent la souscription dématérialisée d'une assurance par un particulier dans le cadre d'un démarchage ou d'un entretien avec un conseiller commercial.

Afin de faciliter la gestion des souscriptions, la société d'assurance GAMUT a mis en place un portail de souscription en ligne à la disposition de ses conseillers, itinérants comme en agence.

2.1.2 Identification des P.G.P

Les présents principes sont identifiés par l'OID suivante : …

2.1.3 Textes juridiques applicables

…

2.2 Gestion des P.G.P

2.2.1 Entité gérant les P.G.P.

Le présent document décrivant les P.G.P. est gérée par la DSI de GAMUT.

2.2.2 Point de contact

GAMUT / DSI

49 allée Pizarro

94250 Gentilly

e-mail : pgp-dsi@gamut.fr

2.2.3 Cycle de vie des P.G.P.

Le présent document est revu et validé par le groupe « Projet portail » du pôle technique. Il est formellement validé par le chef de pôle.

2.2.4 Publication des P.G.P. et autres documents

2.2.4.1 Informations publiées

La P.G.P. n'est pas publique mais est tenue à disposition des personnes ayant souscrit un contrat d'assurance.

2.2.4.2 Points de publication

Sans objet.

2.3 Gestion du cycle de vie de la transaction et des éléments de preuve

2.3.1 Objet de la preuve

Le contexte est celui de la souscription d'un contrat d'assurance, processus durant lequel un adhérent signe, de façon manuscrite, à l'aide d'un stylet, un dossier de souscription (« dossier » tout court, lorsqu'aucune confusion n'est à craindre), contenant plusieurs documents électroniques.

La constitution de ce dossier (tarification, choix des options de la police d'assurance, numérisation de pièces nécessaires, etc.) et son approbation par l'adhérent sont établies sur des tablettes, en présence d'un représentant de GAMUT. Ce processus permet une dématérialisation complète du dossier et, par conséquent, de la dématérialisation de l'essentiel des éléments attendus pour démontrer :

- L'authenticité et l'intégrité du dossier
- L'identité du souscripteur
- La signature par le souscripteur de la police d'assurance et des conditions financières
- La date citée dans le dossier

2.3.2 Transaction et éléments de preuve

2.3.2.1 Description de la transaction

La constitution du dossier se déroule en deux étapes.

Tout d'abord, le contenu du dossier est constitué en face-à-face avec le souscripteur : le contrat est établit avec le conseiller, puis revu par le souscripteur sur la tablette. La carte nationale d'identité (C.N.I.) du souscripteur est numérisée à cette occasion, et son identité, confirmée dans l'application. L'application produit un dossier au format PDF et demande son approbation au souscripteur.

Lorsque celui-ci la donne (en cliquant sur la tablette), le fichier PDF est transmis aux serveurs de GAMUT, lesquels le signent électroniquement à l'aide d'un certificat émis à la volée au nom du souscripteur, sur la base de l'identité précédemment saisie.

Cette signature est ensuite horodatée et envoyée par e-mail au conseiller et au souscripteur.

2.3.2.2 Éléments de preuve soumis aux P.G.P.

2.3.2.2.1 Éléments transactionnels

Les éléments de preuve produits par le processus précédent sont les suivants :

[P_1] La copie de la C.N.I. du souscripteur

[P_2] Les traces d'authentification de la tablette sur les serveurs GAMUT (chaque tablette est propre à un conseiller et est dotée d'un certificat SSL client)

[P_3] Le dossier signé par le souscripteur, et son certificat

[P_4] Les traces des e-mails envoyés par les serveurs GAMUT

[P_5] L'horodatage par les serveurs GAMUT

2.3.2.2.2Éléments de preuve permanents

En complément des éléments précédents, les données suivantes sont des éléments de preuve à part entière :

[PP_1] Politiques de certification et d'horodatage (OID : …)

[PP_2] Spécifications fonctionnelles de l'application (réf. …)

[PP_3] Politique d'archivage (OID…)

2.3.2.3 Données non concernées par les P.G.P.

Sans objet.

2.3.3 Cycle de vie des éléments de preuve

2.3.3.1 Processus de constitution des éléments de preuve

2.3.3.1.1L'identité du souscripteur

L'identité du souscripteur, matérialisée par la copie de sa C.N.I. [P_1], est établie en présence du conseiller, lequel fait office, à cette occasion, d'autorité d'enregistrement.

2.3.3.1.2Authentification de la tablette

Les traces d'authentification de la tablette sont des traces de connexion SSL sur les portails GAMUT (date et heure de connexion, adresse IP/FQDN de la plate-forme GAMUT et de la tablette).

Ces données sont enregistrées sous forme de fichiers « syslog » compressés sur les serveurs GAMUT. Ces fichiers sont protégés (intégrité, confidentialité) via les politiques de contrôle d'accès de ces serveurs et font l'objet d'un archivage mensuel.

2.3.3.1.3Dossier de souscription

Le dossier (fichier PDF) est constitué par le souscripteur et le conseiller sur la tablette, avant approbation. Une version est ensuite transmise pour signature aux serveurs GAMUT.

La version signée constitue l'élément [P_3], dont la signature et l'horodatage assurent l'intégrité et l'authenticité du document.

La version signée est conservée et archivée par GAMUT.

2.3.3.1.4E-mails

Les traces des e-mails sont enregistrées sous forme de fichiers « syslog » compressés sur les serveurs GAMUT et font l'objet d'un archivage mensuel.

Ces e-mails ont pour but de répondre au besoin, pour chacune des deux parties signataires (la société GAMUT et le souscripteur), de disposer d'un exemplaire du dossier (contrat bilatéral).

2.3.3.1.5Horodatage

Cet élément est contenu dans [P_5] et est autonome : son authenticité et son intégrité sont assurées par les mécanismes cryptographiques de la signature électronique du jeton.

Cet élément porte la date et l'heure de la signature du souscripteur, mais aussi l'identité de la société GAMUT.

La politique d'horodatage (P.H.) associée est identifiée par l'OID …

2.3.3.2 Consultation des éléments de preuve

Les éléments [P_1], [P_3] et [P_5] sont mis à disposition du souscripteur lors de l'établissement du contrat (envoi par e-mail du dossier signé).

Les autres éléments sont disponibles sur demande au point de contact identifié en 2.2.2.

2.3.3.3 Pérennisation des éléments de preuve

La pérennisation des éléments [P_1], [P_2], [P_3], [P_4] et [P_5] est décrite dans la politique d'archivage [PP_3]. Cette pérennisation concerne les éléments archivés par GAMUT ; les éléments mis à disposition du client sont sous la responsabilité de ce dernier.

2.3.3.4 Vérification des éléments de preuve

La vérification de la preuve est possible sur demande formulée au responsable identifié au §2.2.2. Les principes suivants s'appliquent :

Il n'y a pas de vérification de [P_1], [P_2], [P_4] autre que la consultation des éléments archivés.

La vérification de [P_3] (contrat PDF signé) peut être réalisée de façon autonome par un logiciel de vérification de signature électronique durant toute la durée de vie du jeton d'horodatage [P_5]. Au-delà de cette période, ce sont les modalités d'archivage qui précisent la façon de vérifier ces éléments.

Pour la vérification du jeton d'horodatage [P_5], se référer à la politique d'horodatage du service [PP_3].

2.3.3.5 Établissement de la preuve

L'objet de la preuve est de démontrer la réalité d'un contrat établi entre le souscripteur et GAMUT aux conditions définies dans celui-ci. L'authenticité de cet écrit et l'identité des signataires sont assurées par la signature électronique ([P_3]) et l'horodatage du document [P_5].

Les traces des e-mails [P_4] ont pour objet de démontrer qu'une copie du contrat signé a bien été mise à disposition du souscripteur.

2.3.3.6 Durées de validité des preuves

La durée de validité de la signature électronique horodatée selon la politique d'horodatage [PP_3] est de 5 ans. Les signatures des contrats sont donc vérifiables de manière autonome durant cette période.

Au-delà de cette période, l'intégrité et l'authenticité des éléments de preuve sont assurées par les mesures d'archivage.

2.3.3.7 Modalités d'acceptation des preuves

Le client reconnaît explicitement les éléments de preuve à travers sa signature du dossier.

2.4 Obligations des acteurs en matière de gestion de la preuve

Le souscripteur est responsable de la conservation de sa copie.