Politique de Signature des actes dématérialisés en Point de Vente SFR

Politique de signature des actes dématérialisés en point de vente				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.3.1	**Erreur ! Nom de propriété de document inconnu.**1	Mai 2011	Public	1/27

Récapitulatif des éditions

N° Version	Date de version	Description	Nom/Prénom
1.0	20/06/2008	Création	SFR/DISAG/DFSI
1.1	Mai 2011	Modifications mineures	SFR/DISAG/DFSI

Table des matières

1 Définitions

Autorité d'horodatage : Autorité responsable de la gestion d'un service d'horodatage.

Infrastructure de gestion de clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats.

Algorithme de hachage : Fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille variable en un code de taille fixe, en vue de son authentification ou de son stockage.

Autorité de certification (AC) : désigne l'autorité responsable des certificats émis et signés en son nom conformément aux règles définies dans la politique de certification et la déclaration des pratiques de certification associée.

Autorité d'Horodatage : désigne l'autorité responsable de la gestion d'un service d'horodatage.

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

Certificat électronique : Fichier électronique attestant qu'un couple de clé privée/clé publique appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente politique de signature, le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Composante : Plate-forme informatique opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Dispositif de création de signature : Il s'agit du dispositif matériel et/ou logiciel utilisé par l'utilisateur de certificat pour stocker et mettre en œuvre sa clé privée de signature (ex : Terminal).

Entité : Désigne SFR.

OID : Identificateur numérique de document enregistré auprès de l'AFNOR.

Plate-forme de médiation : Ensemble de matériels et de logiciels assurant les relations entre le système d'information de **SFR** et l'Infrastructure de Gestion des Clés.

Politique de certification (PC) : Ensemble de règles, identifié par un nom tel que « Politique de Certification « SFR AC Certificat Client », définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant les conditions d'application 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 utilisateurs de certificats**.**

Politique de signature : Ensemble de règles présidant à la création et la validation d'une signature électronique et vis-à-vis desquelles la signature peut être déterminée comme **valide**.

Point de Vente : Magasin référencé par le distributeur (SFD), agréé par ce dernier et **assurant la** commercialisation des offres SFR.

Racine de confiance : désigne le système de confiance basé sur l'acceptation de l'autorité de certification.

Signataire : Toute personne physique majeure habilitée à signer électroniquement les actes de souscription ou de gestion dématérialisés.

Terminal : Terminal permettant les opérations de collecte par lecture optique des pièces justificatives du Signataire et les opérations de signature des actes dématérialisés.

Vérifieur : Entité technique ou fonctionnelle pouvant vérifier les preuves de signatures.

2 Objet du document

Le présent document a pour objet de décrire les conditions de création et de validation d'une signature électronique dans le cadre des opérations de souscription et de gestion des actes dématérialisés en point de Vente SFR. Il complète les documents décrivant la politique de certification de l'Autorité de Certification « SFR AC Certificat Client » identifiés sous les numéros d'OID suivants : *1.2.250.1.35.25.2.1.2.1.1* et *1.2.250.1.35.25.2.1.2.7.1*.

La signature électronique est appliquée à travers un dispositif de création de signature électronique sur un Terminal et à travers une plate-forme de médiation vers le système d'information et l'Infrastructure de Gestion des Clés (IGC).

3 Politique de signature électronique

3.1 Contexte

Dans la loi n°2000-230 du 13 mars 2000 paru au journal officiel du 14 mars 2000, l'écrit sous forme électronique est admis comme preuve au même titre que l'écrit sur support papier. Deux niveaux de validité juridique sont reconnus dans le décret 2001-272 du 30 mars 2001 permettant de distinguer la signature électronique dite « simple » et la signature électronique « présumée fiable ».

SFR a choisi d'appliquer une signature électronique dite « simple » en mettant en œuvre les meilleurs pratiques s'approchant de la signature électronique «présumée fiable » en s'appuyant sur les éléments suivants :

- L'identification et l'authentification forte du Signataire avec une vérification en face à face de l'identité du Signataire après remise des pièces officiels ;
- L'utilisation d'algorithme de cryptographie conforme aux standards pour assurer l'intégrité des documents ;
- L'utilisation d'une infrastructure sécurisée de gestions des clés.
- La mise en œuvre d'une infrastructure de gestion de preuve pour faire face à toute contestation éventuelle.

3.2 Champ d'application

La présente politique de signature s'applique aux actes de souscription ou de gestion dématérialisés en Point de Vente. Les échanges électroniques sont réalisés par l'intermédiaire d'un Terminal comprenant un dispositif de signature, la carte SIM du client, et une plate-forme de médiation vers le système d'information.

Elle concerne les Signataires d'actes dématérialisés et le dispositif de signature.

Pour créer une signature électronique, le Signataire doit disposer d'un certificat électronique qui l'identifie personnellement. Le certificat électronique est délivrée à travers une procédure sécurisée qui est décrite dans la politique de certification de l'AC « **SFR AC Certificat Client** ».

3.3 Identification de la Politique de Signature

Le présent document politique de signature est identifié par l'O.I.D (Object IDentifier) n° 1.2.250.1.35.25.2.1.2.3.1.

3.4 Processus de mise à jour

La mise à jour de la présente politique de signature peut avoir pour origines, l'évolution du droit, la modification de l'état de l'art, l'apparition de nouveaux risques et de nouvelles mesures de sécurité ou des modifications dans le processus de signature.

La présente politique est réexaminée périodiquement.

3.5 Publication du document

La présente politique est publiée après approbation de SFR sur le site http://www.sfr.fr/signature-electronique/.

4 Rôles

4.1 Acteurs et rôles

Les acteurs concernés par le processus de signature sont les suivants :

- le Signataire,
- le vendeur du Point de Vente,
- l'Autorité Morale (SFR) qui signe électroniquement les contrats.

Le rôle du Signataire est de vérifier que les informations contenues sur le document affiché sur le Terminal sont exactes, puis de signer électroniquement l'ensemble sur le dit Terminal afin de matérialiser son consentement.

Le rôle du vendeur est de contrôler l'identité du signataire et de s'assurer du bon déroulement des opérations de signature électronique en présence du Signataire, ainsi que du bon fonctionnement du dispositif électronique.

4.2 Obligation du Signataire

Le Terminal est un élément sensible dans le processus de signature. Dans la phase de souscription ou de gestion dématérialisés, le Signataire :

- vérifie et accuse réception de son certificat après examen du contenu de celui-ci, tel que présenté par le Terminal ;
- respecte les règles de fonctionnement concernant les étapes de signature ;
- reste à proximité du Terminal jusqu'à la fin du processus de contractualisation.

4.3 Obligations du responsable du Point de Vente

4.3.1 Environnement du Terminal

En raison de la sensibilité des informations contenues dans le Terminal, celle-ci devra :

- Être réservée aux seuls actes de souscription ou de gestion dématérialisés ;
- Être installée dans un environnement permettant de garantir son intégrité ;
- Être utilisée conformément aux recommandations de SFR relatives à la sécurité de l'Information.

4.3.2 Contrôle de l'Activité

Le responsable du Point de Vente est chargé de faire appliquer et de contrôler le bon usage du procédé de signature électronique, ainsi que du respect de l'application de la présente politique de signature et de la politique de certification.

4.3.3 Habilitations des vendeurs

Le responsable du Point de Vente nomme des vendeurs habilités à utiliser le Terminal après les avoir sensibilisés sur le processus de signature électronique.

4.4 Obligations du vendeur en Point de Vente

4.4.1 Contrôle de l'Activité

Le vendeur est chargé d'utiliser le service de signature électronique en respectant la présente politique de signature et la politique de certification.

4.4.2 Reprise en cas d'incident

Suite à un incident de transmission ou sur le Terminal pouvant affecter le processus de signature, le vendeur devra vérifier l'impact de cet incident sur le traitement de l'acte en cours.

4.5 Obligations de SFR

4.5.1 Données de Vérification

Pour effectuer des vérifications, l'application de signature utilise des données publiques telles que les listes de révocation de certificats ou les certificats des autorités de Certification.

4.5.2 Informations transmises en retour

Le dispositif de signature informe le Signataire et le vendeur lorsqu'il détecte un problème nécessitant l'interruption dans le processus de signature. Les messages de notifications sont renvoyés sous forme de code d'erreur.

L'arrêt de la validation et de la signature implique la reprise du processus complet.

4.5.3 Protection

SFR met en œuvre les moyens nécessaires pour assurer la protection du processus de signature électronique. Les mesures prises concernent :

- l'hébergement sécurisé des infrastructures (protection physique, protection logique, alimentation secourue, détection et protection incendie, etc…) ;
- la restriction des accès logiques aux équipements ;
- la protection réseaux en assurant une authentification forte et la confidentialité des échanges d'informations ;
- la sensibilisation et le suivi des procédure dans le processus de signature.

4.5.4 Journalisation

SFR assure une traçabilité et une conservation des traces relatives :

- aux différents échanges sur les réseaux et systèmes d'informations ;
- aux traitement des données échangés.

SFR s'assure que les éléments constituant la signature électronique sont conservés pendant la durée de vie du contrat soit plus de 10 ans de manière sécurisée.

5 Politique de validation de Signature

Lorsque plusieurs tiers (on entend par tiers, toute personne physique ou morale n'étant pas dans la chaîne de traitement des informations de la signature électronique) souhaitent évaluer la validité d'une signature électronique, il est fondamental qu'ils obtiennent le même résultat. Les conditions sur lesquelles s'est engagé le Signataire au moment de signer doivent donc être indiquées au Vérifieur et à tout autre tiers. La politique de signature est le socle commun à toutes ces parties. Les éléments techniques permettant la validation et les revalidations d'une signature électronique seront appelés "politique de validation de signature". La présente section a pour objectif de définir ces éléments.

Tous les couples de paires de clés utilisées par les Autorités de Certification impliquées dans le processus de signature électronique ont été générés en présence d'un huissier de justice.

5.1 Format de signature

Les signatures doivent respecter le format PAdES (ETSI TS 102.778 v1.1.1 ou supérieur).

5.2 Algorithmes autorisés

Les algorithmes de hachage autorisés sont: SHA-1, SHA-256, SHA-384 et SHA-512 définie dans la norme FIPS PUB 180-2.

Les algorithmes de signatures autorisés sont RSA/PKCS#1 et DSS définis dans RFC 3447 et dans le standard FIPS 186-2.

5.3 Racines de confiance pour les signatures

La Racine de Confiance pour les signatures est définie par un nom (*distinguished name*) et une clé publique. Dans le cadre de cette politique, le nom est "C=FR, O=SFR, CN=SFR Public AC Racine" et la clé publique RSA est :

Module (4096 bit):

```
    00:ed:7b:50:5b:76:ba:0e:d2:01:00:fc:5b:c8:b0:
    71:32:f6:92:39:78:c3:e2:c7:61:e1:89:13:74:ff:
    32:68:e6:06:97:2d:d6:bf:6e:be:e9:a7:37:14:da:
    77:b2:64:72:57:98:9b:f6:30:9c:63:78:5d:fd:63:
    ef:fd:12:75:4c:04:4f:39:c8:82:34:9f:69:01:9a:
    16:02:4b:b0:b6:0e:0e:55:68:3a:a2:f7:ea:9a:b7:
    e1:f8:e7:df:7a:68:97:4d:60:ec:d1:36:04:53:7b:
    6b:62:84:78:aa:15:74:86:2c:73:87:28:4c:d7:7c:
    8d:87:96:c5:64:28:a7:c6:83:4a:fc:f1:c6:45:86:
    fa:73:92:69:0a:78:25:67:67:3f:e0:7d:8d:4a:54:
    1f:94:e2:ee:b7:dd:4d:38:06:88:bf:1e:8e:28:80:
    18:f1:6f:17:28:c1:38:48:22:74:28:be:bc:62:f8:
    f3:2c:dc:6c:bc:e7:a8:ca:01:62:f5:a9:f4:68:5e:
    a7:7c:8f:7d:80:d4:af:16:ef:3c:4b:e7:07:e9:48:
    ca:5c:38:96:86:9d:30:23:e2:3c:cd:3b:7f:26:78:
    0a:3f:82:26:02:93:a9:23:2e:5d:19:c8:bd:ac:06:
    3d:6a:5d:c0:9e:41:20:dd:7e:10:3c:25:63:0b:47:
    b1:4d:5c:7d:a2:a9:2b:26:ea:b7:f7:cd:c5:fe:f8:
    81:9f:54:d8:2f:c3:c8:c3:2c:bb:51:29:96:9e:f6:
    9d:f5:ef:4f:a0:ed:9f:3a:3d:77:3e:59:c6:f1:bc:
    55:b1:64:6b:b6:e5:90:75:8c:b5:b3:4f:18:79:e4:
    3e:d6:40:d6:ab:42:00:28:e1:e3:21:2b:e0:67:d1:
    46:1f:0e:d0:79:5a:f9:40:ae:f9:a1:09:ee:a3:20:
    49:cf:f6:b3:3b:ed:db:65:97:ce:0b:ae:e9:61:d9:
    1e:f9:76:89:26:f9:62:4e:ad:65:3a:1d:24:73:55:
```

```
    33:09:0d:fa:e7:cb:74:c1:01:4c:09:58:ac:de:82:
    a3:b0:83:d5:6b:ad:b3:d2:e7:ed:c7:37:67:c1:88:
    33:34:e4:cc:cc:64:c2:2a:b9:06:77:a4:25:ba:82:
    5d:91:70:e1:37:c3:bd:50:e0:2a:37:00:07:f6:d8:
    0f:02:59:c2:42:02:9d:63:1f:76:04:ba:bc:26:2b:
    fa:89:b2:c9:eb:2c:73:a4:dc:a0:0f:90:2f:8a:bb:
    92:45:7f:1f:e5:64:31:a6:67:bd:30:39:1c:fe:94:
    0b:2b:6b:c4:7d:12:83:42:01:ce:7f:8f:e8:dc:35:
    ba:33:e5:54:39:18:95:95:d5:72:bb:f6:0a:c5:f2:
    6a:60:a7

Exposant: 65537
```

5.4 Chemin de certification pour les signatures

Il n'y a pas de contrainte spécifique sur l'établissement et la validation d'un chemin de certification permettant de valider le certificat du Signataire. Il convient simplement de répondre aux contraintes cumulatives suivantes au chemin de certification :

- commençant à la racine de confiance pour les signature ;
- se terminant par un certificat autorisé à réaliser des signatures ;
- incluant des informations complètes de révocation ;
- valide au sens du standard ITU-T X.509 au moment de la validation.

Il est également possible de valider un tel chemin à une date passée à condition de démontrer que l'ensemble des données fournies à l'algorithme de validation existait à cette date.

5.5 Racine de confiance pour l'horodatage

Il est difficile de garantir la non-répudiation d'une signature sans pouvoir la positionner dans le temps d'une manière ou d'une autre. La présente politique autorise l'utilisation de l'horodatage afin de démontrer l'existence de certains éléments à des dates passées. Une politique d'horodatage est en cours de rédaction.

La racine de confiance pour les cachets horodateurs est définie par un nom (DN) et une clé publique. Dans le cadre de cette politique, le nom est "C=FR, O=Cryptolog, OU=AC Racine - Root CA, CN=Cryptolog" et la clé publique RSA est:

Module (4096 bit):

```
    00:c9:ac:3f:0f:f0:7d:7a:61:1b:66:a0:d4:fb:4e:
    64:a0:0c:4b:a1:e0:33:75:16:b4:a1:7d:26:be:10:
    d6:62:83:f8:c9:dd:b1:e0:6e:75:61:39:8f:93:e2:
    50:2e:3d:bd:2a:03:63:6d:84:de:6d:8b:f7:18:f7:
    6e:ca:1f:58:cd:8d:b2:ee:e0:f3:d9:c7:8e:8e:b2:
    51:48:fd:82:d7:55:27:e2:b9:c4:63:dc:f4:14:b8:
    c1:d3:d0:1f:f6:95:73:33:47:15:33:52:12:9d:3a:
    04:53:6e:ca:1e:1e:bf:e3:a3:ec:f0:b6:da:3d:a5:
    97:8a:ce:9d:73:f1:eb:19:c5:3d:12:86:da:46:e0:
    31:db:38:43:d5:45:28:4a:3f:e9:41:4e:40:37:39:
    58:12:27:ea:27:69:cb:67:b6:a6:36:d8:ae:72:2d:
    86:85:bf:53:11:df:95:1e:cb:32:05:8d:ef:eb:14:
    ff:60:b9:01:52:5a:64:1e:b9:d0:57:3f:a8:c4:12:
    4f:29:a9:dd:d7:04:c7:06:07:91:a3:cf:b7:72:24:
    a3:52:ce:bd:12:16:b5:04:08:5e:3f:32:d2:e6:bd:
    5d:25:d5:06:27:f9:d1:81:2a:28:bf:14:ab:38:fc:
    40:e7:d8:89:a3:85:84:ed:03:e3:be:3a:3e:ae:b8:
    2f:16:d4:63:06:1d:33:23:2a:0d:02:c1:e4:dd:6b:
```

```
    48:f8:24:ec:f4:b7:f1:a0:16:2e:99:83:d8:3d:63:
    c2:ab:a5:03:e1:49:bd:10:0f:29:d6:b5:71:8e:97:
    65:d5:d3:4c:10:d0:9c:77:95:2b:eb:af:ea:ae:68:
    ed:70:80:cc:33:7f:05:11:26:5d:0a:53:5b:f1:e4:
    a5:7c:3e:49:95:ff:f1:0d:62:95:54:a2:4e:49:1b:
    7a:32:3f:df:dc:16:b0:18:50:cc:0d:7f:ed:6e:88:
    34:3b:d4:09:fe:f7:2a:c6:a2:39:3a:b1:01:85:43:
    2d:19:46:96:2c:4f:0d:b7:77:c8:b9:57:b0:b5:0a:
    df:eb:bc:f4:e1:9a:49:4b:70:0b:4e:36:5c:0e:2f:
    91:f7:fd:5d:df:13:44:5c:39:58:46:0c:f4:cc:9b:
    46:e1:ac:f3:0b:d3:e8:97:2c:88:5d:09:24:1f:1c:
    ea:76:87:f6:e6:ef:0d:9e:84:35:40:90:8a:80:3a:
    12:42:4a:0d:23:81:59:9f:7a:19:27:fb:00:cd:af:
    7f:c4:e8:ee:10:c7:e1:22:cb:c0:60:0c:d7:6a:59:
    19:74:b9:f1:cc:68:9e:ec:7d:48:1a:80:d2:9a:d9:
    e7:9f:db:35:07:64:9d:4a:ff:de:3c:fb:84:03:02:
    0f:9c:09

Exposant: 65537
```

5.6 Chemin de certification pour l'horodatage

Les règles énoncées pour la validation du chemin de certification du Signataire sont similaires pour celles du chemin de certification des horodatages. Il convient donc de répondre aux contraintes cumulatives suivantes au chemin de certification :

- commençant à la racine de confiance pour l'horodatage ;
- se terminant par un certificat autorisé à produire des cachets d'horodatage ;
- incluant des informations complètes de révocation ;
- valide au sens du standard ITU-T X.509 au moment de la validation.

Il est également possible de valider un tel chemin à une date passée à condition de démontrer que l'ensemble des données fournies à l'algorithme de validation existait à cette date.

5.7 Conditions pour déclarer valide une signature de document

Une signature de document est considérée comme valide s'il est possible à une date donnée de :

- prouver l'existence de tout les éléments techniques (ex : les listes de révocation des certificats, l'horodatage, les clés cryptographiques publiques, etc…) utilisés lors de la validation à cette date ;
- présenter et valider un chemin de certification pour le Signataire comme indiqué ci-dessus ;
- vérifier que l'ensemble des algorithmes cryptographiques utilisées pour cette validation étaient réputés sûrs à cette date ;
- valider la signature cryptographique du document par rapport à la clé publique comprise dans le certificat ;
- démontrer qu'aucune autre paire « clé publique / document signé » vérifiant la même signature ne pouvait exister à la date donnée.

Lorsque des techniques d'horodatage sont utilisées pour prouver l'existence de données dans le passé, le procédé décrit ci-dessus doit s'appliquer pour valider les signatures de l'autorité d'horodatage.

6 Accès au service de signature des actes dématérialisés en Point de Vente

6.1 Pré-requis

L'accès au service de signature électronique est réservé aux clients et futurs clients SFR dans le cadre des actes de souscription ou de gestion dématérialisés dans les Points de Vente de SFR.

6.2 Utilisation du Terminal

La signature électronique utilise un Terminal en Point de Vente permettant les fonctions suivantes :

- la collecte et la saisie des informations d'identité nécessaire à la demande de certificats ;
- la signature électronique du contrat présenté sous format PDF et de l'autorisation de prélèvement.

6.3 Utilisation de la plate-forme de médiation

La plate-forme de médiation assure les fonctions suivantes :

- la transmission des informations d'identité nécessaire à la demande de certificats vers l'autorité de certification;
- la préparation des informations et la transmission du document PDF au Terminal;
- la signature électronique par SFR du contrat PDF signé électroniquement par le client.

6.4 Authentification des accès

Chaque Terminal est authentifié par certificat lors de chacun de ses échanges avec la plate-forme de médiation.

7 Contrôle de conformité

7.1 Objectif du contrôle

Le procédé de signature électronique s'appuie sur un ensemble d'exigences et de règles de sécurité devant favoriser la confiance.

SFR effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement permettant de valider que la signature électronique est conforme aux politiques de signature et de certification.

7.2 Fréquence du contrôle de conformité

SFR procède annuellement à un contrôle de conformité.

7.3 Choix du contrôleur

Le contrôle est effectué à la demande de SFR par une équipe d'auditeurs externes compétents en sécurité des systèmes d'information et indépendante.

7.4 Communication des résultats

Les résultats des audits de conformité contiennent des informations sensibles. Ils sont communiqués à un nombre restreint de personnes dans les entités concernés par l'audit en fonction des résultats.

7.5 Plan d'actions

À l'issue d'un contrôle de conformité, les auditeurs externes rendent un avis et proposent un plan d'actions afin de corriger le cas échéant les non-conformités détectées. Le plan d'actions est communiqué aux seules personnes directement concernées.

8 Confidentialité

Les informations suivantes sont considérées comme confidentielles :

- les clés privées associées aux certificats ;
- le dossier de souscription du Signataire ;
- le dossier d'archivage de tous les élèments électroniques du Signataire;
- les journaux d'évènements de la plate-forme de médiation de signature ;
- les procédures internes ;
- les rapports d'audits ;

9 Dispositions juridiques

9.1 Droit applicable

Le procédé de signature électronique respecte la législation et la réglementation en vigueur.

9.2 Dispositions concernant la résolution de conflits

Tout différend découlant du procédé de signature doit, en premier lieu, et dans toute la mesure du possible, être réglé au moyen de négociations amiables entre les parties.

9.3 Juridictions compétentes

Tout différend né de l'interprétation ou de l'exécution de la politique de signature relèvera de la compétence expresse du **Tribunal de Commerce de Paris,** nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les procédures d'urgence ou les procédures conservatoires, en référé ou par requête.

9.4 Propriété intellectuelle

Tous les droits de propriété intellectuelle détenus par SFR sont protégés par la loi, règlement et autres conventions internationales applicables.

Ni les clients, ni les Points de Vente ne disposent de droit de propriété intellectuelle sur les éléments composant le service de signature.

9.5 Protection des données personnelles

9.5.1 Informations à caractère personnel

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

9.5.2 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel sont réalisés dans le strict respect de la législation et de la réglementation en vigueur, en particulier de la loi dite « Informatique et Libertés » du 6 janvier 1978.