



POLITIQUE DE SIGNATURE ELECTRONIQUE EN LIGNE SEPA

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	1/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Récapitulatif des éditions

Version	Date	Nom du rédacteur	Nature de la modification
1.0	08/08/13	Christian BOUVIER	Version publiée

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	2/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Table des matières

Récapitulatif des éditions	2
1 Politique de signature électronique	4
1.1 Champ d'application	4
1.1 Identification.....	4
1.2 Processus de mise à jour.....	4
1.3 Publication du document	4
1.4 Entrée en vigueur de la nouvelle version et période de validité	5
2 Rôles	6
2.1 Acteurs et rôles.....	6
2.2 Rôles et obligations du Signataire.....	6
2.3 Rôle et Obligations de la plate-forme de signature électronique	6
2.3.1 Données de Vérification.....	6
2.3.2 Informations transmises en retour	6
2.3.3 Protection	6
2.3.4 Journalisation.....	7
3 Signature électronique et vérification	8
3.1 Caractéristiques techniques de l'environnement de signature	8
3.2 Données signées.....	8
3.3 Processus de signature	9
3.4 Caractéristiques des signatures.....	10
3.4.1 Type de signature	10
3.4.2 Norme de la signature	10
3.4.3 Racines de confiance pour les signatures.....	10
3.4.4 Certificats de signature	12
3.4.5 Date et heure de signature	14
3.4.6 Racines de confiance pour l'horodatage	14
3.4.7 Vérification de la signature.....	15
4 Dispositions juridiques	16
4.1 Droit applicable	16
4.2 Dispositions concernant la résolution de conflits.....	16
4.3 Juridictions compétentes	16
4.4 Propriété intellectuelle.....	16
4.5 Protection des données à caractère personnel	16

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	3/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



1 Politique de signature électronique

1.1 Champ d'application

Une politique de signature (P.S) est un document décrivant les conditions de recevabilité d'un document sur lequel sont apposées une ou plusieurs signatures électroniques dans le cadre d'échanges électroniques prédéfinis.

La présente politique de signature s'applique à la signature électronique des mandats SEPA lors de la souscription en ligne sur les services web de SFR des clients SFR. Les échanges électroniques sont réalisés par l'intermédiaire des portails WEB SFR et d'une plate-forme de signature électronique.

Elle concerne les Signataires de documents SEPA dématérialisés et le dispositif de signature électronique. 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 qui est décrite dans la politique de certification de l'AC « **SFR AC Certificat Client – Certificat de Signature en ligne** » portant le numéro O.I.D suivant 1.2.250.1.35.25.2.1.2.10.1 et publiée sur le site Web <http://www.sfr.fr/signature-electronique/>

1.1 Identification

La présente politique de signature est identifiée par l'OID (Object Identifier) 1.2.250.1.35.25.2.1.2.12.1.

1.2 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 lors de toute modification majeure de l'application.

1.3 Publication du document

La présente politique est publiée après approbation sur le site <http://www.sfr.fr/signature-electronique/> avant la mise en production de l'application ou de ses évolutions majeures.

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	4/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



1.4 Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la politique de signature entre en vigueur 15 jours ouvrés après sa mise en ligne (mise à jour des profils de signature applicatifs) et reste valide jusqu'à la publication d'une nouvelle version.

Les anciennes versions sont archivées pendant la durée de vie du service de signature en ligne.

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	5/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



2 Rôles

2.1 Acteurs et rôles

Les acteurs concernés par le processus de création et de vérification de la signature électronique sont les suivants :

- le Signataire ;
- la plate-forme de signature électronique.

2.2 Rôles et obligations du Signataire

Le rôle du Signataire est de vérifier que les informations contenues sur le document à signer sont exactes avant de donner son consentement et de signer électroniquement le document depuis les sites web SFR à l'aide de son certificat personnel de signature.

2.3 Rôle et Obligations de la plate-forme de signature électronique

2.3.1 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.

2.3.2 Informations transmises en retour

Le dispositif de signature informe le Signataire 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 à l'interface des applications web.

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

2.3.3 Protection

SFR s'assure des moyens nécessaires pour assurer la protection du processus de signature électronique. Les mesures prises concernent à la fois :

- 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 ;

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	6/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



- La disponibilité du service
- La surveillance et le maintien en condition du service.

2.3.4 Journalisation

SFR s'assure de la mise en œuvre d'une traçabilité et d'une conservation des traces relatives :

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

SFR s'assure que les éléments constituant la signature électronique sont conservés pendant la durée de vie du contrat + 36 mois après la fin du contrat.

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	7/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



3 Signature électronique et vérification

3.1 Caractéristiques techniques de l'environnement de signature

Le service de signature en ligne de SFR utilise la plate-forme de signature électronique Universign.

Les serveurs hébergeant la plate-forme de signature électronique sont protégés selon les normes de sécurité en vigueur. L'accès physique et technique à ces équipements et aux informations confidentielles qui s'y trouvent sont contrôlés, par exemple : protection par pare-feu, installation des seuls logiciels utilisés pour effectuer les tâches du service, antivirus, mots de passe non partagé, mise à jour systématique des logiciels, ...

3.2 Données signées

Au moment de la signature électronique, le signataire signe électroniquement les informations métiers suivantes :

- Le mandat prélèvement SEPA
- Les propriétés de la signature électronique (détaillées ci-après)

Ces informations sont enregistrées dans un fichier au format PDF généré par la plate-forme de signature électronique.

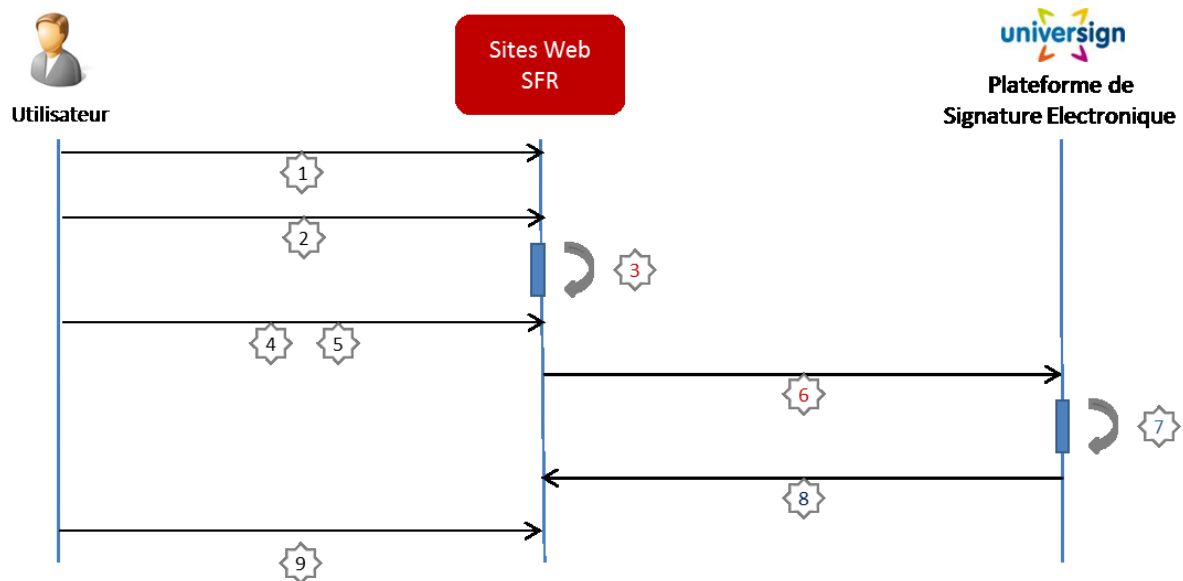
Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	8/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



3.3 Processus de signature

Le parcours de signature électronique du Mandat Sepa concerne le titulaire/payeur client SFR ou prospect SFR. Le processus de signature électronique est détaillé ci-dessous :



- 1 Identification/ authentification de l'utilisateur (client ou prospect)
- 2 Saisie des coordonnées bancaires par l'utilisateur
- 3 Ecran d'affichage des coordonnées + lien de prévisualisation du mandat PDF + case à cocher des C.G.U service de signature
- 4 Acceptation des CGU du service de signature électronique depuis la case à cocher par l'utilisateur
- 5 Appui par l'utilisateur sur le bouton « Signer électroniquement pour autoriser votre prélèvement »
- 6 Envoi automatique de la demande de signature + le PDF à la plate-forme de signature Universign
- 7 Génération du certificat du signataire sur la base des informations saisies sur les sites Web SFR
Signature électronique du PDF avec le certificat porteur du signataire et horodatage sur la plate-forme Universign
Vérification de la signature électronique par la plate-forme Universign
- 8 Envoi du PDF signé par plate-forme de signature Universign
- 9 L'utilisateur peut visualiser le mandat PDF signé

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	9/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



3.4 Caractéristiques des signatures

3.4.1 Type de signature

Les signatures électroniques apposées par les signataires sont enveloppées (PDF).

3.4.2 Norme de la signature

Les signatures électroniques respectent la norme PAdES (ETSI TS 102 778) en version v1.1.1 ou supérieure.

Conformément à la norme PAdES, les propriétés signées contiennent les éléments suivants :

- le certificat du signataire
- la date et l'heure de signature

Le fichier signé est immédiatement validé (voir ci-après), horodaté et complété par l'usage du profil de signature, intégrant la signature électronique et un jeton d'horodatage, permettant de déterminer la date et l'heure de la signature.

3.4.3 Racines de confiance pour les signatures

La Racine de Confiance utilisée pour les signatures électroniques est détaillée dans le profil de certificat ci-dessous :

Champ	Valeur
Version	3 (0x2)
Serial Number	fe:ff:40:98:ab:bd:11:a8:dc:69:d3:01:af:24:e3:47
Signature Algorithm	sha512WithRSAEncryption
Issuer	C=FR, O=SFR, CN=SFR Public AC Racine
Not Before	Mar 17 12:58:00 2008 GMT
Not After	Mar 17 12:58:00 2018 GMT
Subject	C=FR, O=SFR, CN=SFR AC Certificat Client
Public Key Algorithm	rsaEncryption

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	10/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Champ	Valeur
Public-Key	(2048 bit)
Modulus	00:d4:94:56:eb:d2:a9:ac:00:67:5c:c6:35:1f:d5: 15:b3:be:30:ec:24:8c:28:08:5b:ea:1d:7b:a9:f4: 41:67:01:dd:5c:0e:c5:cc:84:d6:bb:8f:21:07:55: 81:09:51:08:19:d3:93:e1:f1:32:9c:47:5f:f0:4f: 02:3e:a7:8e:b1:00:af:e5:68:04:04:0a:ac:cf:32: 24:50:91:a4:72:9e:dd:04:00:b5:40:74:06:58:8e: 5b:e8:17:73:c7:fe:52:46:64:60:07:b8:a0:a2:b7: 28:bf:4c:d8:bb:56:92:2f:36:a9:86:97:4c:89:c7: d2:65:3f:c2:88:13:a4:d6:19:a3:c5:d6:df:37:23: 23:12:96:7a:72:54:58:69:2b:78:34:e6:e8:ae:cd: 9d:bf:3f:1a:55:56:af:b3:74:8a:de:ac:d9:73:6c: 7d:40:ce:c8:03:83:d5:6a:da:59:5a:2a:09:29:a7: ec:d0:61:51:8c:0a:59:8e:a3:c3:f7:cd:f2:0d:69: 0c:bf:a7:aa:d4:4c:cb:a5:27:2c:d5:79:14:3e:93: 84:f2:20:63:4b:ad:95:6f:60:9e:1b:a4:dd:08:9c: fd:44:bc:b1:ff:a3:a6:1c:28:3f:fe:09:42:78:08: f4:db:75:f8:67:23:b3:3a:be:57:50:41:9c:46:2d: 91:2f
Exponent	65537 (0x10001)
X509v3 extensions	
Basic Constraints (critical)	CA:TRUE, pathlen:0
Key Usage (critical)	Certificate Sign, CRL Sign
Subject Key Identifier	0C:7A:2D:C6:C4:ED:F4:2F:A0:A6:69:1E:FC:66:42:75:D5:0B: F8:0C
Authority Key Identifier	keyid:D9:3C:76:06:0F:7C:5D:15:3B:CE:D1:E6:FD:16:22:B0: B9:59:3F:F9
Signature Algorithm	sha512WithRSAEncryption

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	11/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Champ	Valeur
Signature Value	e9:71:7a:b6:d5:19:4a:52:32:0b:af:92:39:71:87:b3:39:6f:8c:35:3a:9f:81:7f:9d:a2:74:8d:14:16:e4:94:fb:f4:6f:db:93:35:b6:96:bb:15:e5:36:6b:8b:92:e2:60:b8:d1:46:66:e6:62:76:ce:61:14:2d:e6:2f:7d:a6:63:b7:ce:24:d4:9a:bd:a2:0e:40:b8:cd:ef:3c:c7:3f:a4:76:55:a1:78:8f:58:56:50:73:52:a9:35:42:e0:d5:e1:6a:14:5c:d2:40:b0:61:7d:bf:b4:28:03:30:f1:94:e6:a9:3e:5c:88:ee:89:60:5a:30:db:be:b6:99:13:94:c3:32:6c:e6:2f:a7:5d:4d:2e:26:c5:54:cc:8e:08:f7:57:99:ac:37:7c:63:e8:34:93:8d:be:1a:98:06:aa:0e:da:5e:fd:56:6b:c8:44:6d:9d:3c:00:30:c7:60:c3:9b:33:7c:a8:31:88:e0:9c:92:7a:49:39:b0:4e:b3:dc:ec:14:b3:56:13:39:2a:87:6d:82:0a:27:f5:f7:19:7f:32:ae:e9:ac:47:9f:09:49:bf:29:ec:33:46:c3:c0:60:25:5f:b5:3b:c1:54:46:54:0f:1b:9b:1e:a4:20:95:00:f6:59:2c:23:84:d8:b2:d2:ac:f2:53:dc:0d:1b:dc:36:6f:f9:79:a7:3b:b8:5c:66:e6:83:3e:4d:b7:1b:38:b0:46:40:8f:aa:8e:bf:12:f2:7a:ba:67:ec:95:4d:4e:b7:9b:22:ed:f6:ba:29:19:9e:a8:e2:8f:22:9e:b3:ef:c9:1c:d7:14:33:91:b9:f0:79:90:6a:4f:9e:02:92:05:32:54:eb:89:4a:a6:e8:a4:72:d0:90:2f:03:10:ab:bd:58:71:ee:bc:b5:8a:0d:d1:11:23:0d:6e:19:26:82:34:45:98:3a:cd:d7:f5:02:79:4f:42:c6:ab:3c:82:b0:1c:f8:ba:b0:ec:9f:31:05:bd:64:37:27:bd:e9:9f:fe:e9:ad:90:4d:48:af:42:bb:88:6b:30:0b:89:a1:09:f6:61:bf:ea:06:12:3c:50:18:86:45:4e:84:7e:0f:5a:f3:27:e2:8d:45:16:66:c6:37:e0:06:6c:62:cf:fc:5c:b9:20:54:2a:9c:7d:fd:f3:28:db:d7:fa:51:55:b8:46:0b:e9:09:ce:e3:b1:90:ab:0e:26:af:18:c2:1f:d6:0c:e3:68:9a:ab:13:2e:4c:c4:63:ae:bd:80:a6:ce:19:42:1e:62:d5:18:1c:9f:29:7b:ee:c6:4a:c5:e8:d1:0f:f9:8a:cc:1a:ab:c1:75:85:07:97:31:c8:63:66:9e:2c:ab:b7:fc:82:c0

3.4.4 Certificats de signature

Les certificats de signature électronique respectent le profil de certificat suivant :

Champ	Valeur/profil	Description
Version	3 (0x2)	
Serial Number	Numéro de série du certificat	Nombre aléatoire de 32 octets
Signature Algorithm	Sha256WithRSAEncryption	
Issuer	C=FR, O=SFR, CN=SFR AC Certificat Client	

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	12/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Champ	Valeur/profil	Description
Not Before	T ₀	Date de début de validité du certificat
Not After	T ₀ +30 minutes	Date de fin de validité du certificat
Subject	CN={Prénom et nom du porteur, séparés par un espace} EMAILADDRESS={adresse e-mail si présente} SERIALNUMBER={numéro de RUM} O=SFR C=FR	
Public Key Algorithm	rsaEncryption	
Public-Key	2048 bit	Clé publique du porteur
Modulus	...	Module de la clé
Exponent	...	Exposant de la clé
X509v3 extensions		
Basic Constraints (critical)	CA:FALSE	
Key Usage (critical)	Non Repudiation	
Subject Key Identifier	...	Identifiant de la clé publique du porteur
CRL Distribution Points	Full Name: URI:http://crl.sfr.fr/sfr_client.crl	
Certificate Policies	Policy:1.2.250.1.35.25.2.1.2.10.1	
Authority Key Identifier	keyid:0C:7A:2D:C6 :C4:ED:F4:2F:A0:A 6:69:1E:FC:66:42: 75:D5:0B:F8:0C	Identifiant de la clé publique de l'A.C. <i>SFR AC Certificat Client</i> (voir 7.1.1 ci-dessus)
Signature Algorithm	Sha256WithRSAEncryption	
Signature Value	...	Valeur de la signature du certificat

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	13/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



3.4.5 Date et heure de signature

La date de la signature est certifiée par une contremarque de temps apposée par la plate-forme Universign sur le document signé, avant transmission aux destinataires.

3.4.6 Racines de confiance pour l'horodatage

La Racine de Confiance utilisée pour l'horodatage est détaillée dans le profil de certificat ci-dessous :

Champ	Valeur
Version	3 (0x2)
Serial Number	00 c3 2e 08 bd f5 97 71 b2 c4 ad 66 63 00 59 57 f4
Signature Algorithm	sha256RSA
Issuer	C=FR, O=Cryptolog International, OU=0002 43912916400026, CN=Universign Primary CA hardware
Not Before	mardi 29 mai 2012 18:58:07
Not After	jeudi 29 mai 2042 18:58:07
Subject	C=FR, O = Cryptolog International OU = 0002 43912916400026 CN = Universign Primary CA hardware
Public Key Algorithm	rsaEncryption
Public-Key	(2048 bit)
Modulus	30 82 01 0a 02 82 01 01 00 d9 9a 74 4d 4d d5 c6 41 70 35 c4 db 6f 4d 5d 71 a7 81 52 60 cb c0 c7 a0 1d ef 55 3d a4 d7 a3 47 1c 8f 40 b7 29 d7 5a 8f b1 b6 26 92 12 2d c8 53 ab a8 4f ce 62 3e ff bc 21 76 fb a5 ce ca c2 ce ee b2 bc 68 4a 44 0a 6a ea 83 d7 42 46 7b 3a 33 c1 4d ba f8 c2 12 f7 a5 d9 9d 6b 71 2e 27 96 ec be e2 6c c9 d1 ca b1 fc 78 24 17 03 55 59 a3 1f d0 5f 9b 4c f9 f0 8b d9 c3 cb 59 bc c3 95 5a 21 f4 a9 20 ec e9 88 30 fb 5e 4d be 86 e6 64 d3 05 4c e8 9f ba 00 94 48 b7 35 1c 69 aa c4 8c 8b 65 cc a9 89 ea a4 fe b0 da 15 ff 63 28 f0 dd cf ab 65 b8 e9 17 2c 42 a4 fc 42 d4 4b ed 91 33 f6 ce 77 ec b3 39 8b c2 0b f0 3b 5c 05 e3 b7 c9 ba 1b 6c e0 58 08 66 64 df 00 e2 ab 54 bc d6 ef 00 b7 25 6e 7c fe 05 10 5e c9 1c d6 2e 75 4e e7 85 f3 b5 ff d8 6e 16 ab 8a d7 9f 3e 43 9f 49 3e 55 bd 02 03 01 00 01

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	14/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



Champ	Valeur
Exponent	65537 (0x10001)
X509v3 extensions	
Basic (critical)	Constraints CA:TRUE, pathlen:0
Key Usage (critical)	KeyCert Sign, CRL Sign
Subject Key Identifier	0C:7A:2D:C6:C4:ED:F4:2F:A0:A6:69:1E:FC:66:42:75:D5:0B:F8:0C
Authority Key Identifier	keyid: 4d d9 fc a8 2d c7 c8 5a a4 ad 5f 49 ae 68 a4 dc 9e 8a 12 22
Signature Algorithm	sha512WithRSAEncryption
Signature Value	

3.4.7 Vérification de la signature par la plate-forme de signature

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature ;
- la vérification du certificat du signataire et de tous les certificats de la chaîne de certification (validité temporelle, statut, signature cryptographique). La vérification du statut des certificats est réalisée en s'appuyant sur les CRL émises par les autorités de certification concernées ;
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;
- la vérification de la signature électronique apposée sur le fichier en utilisant la clé publique du signataire contenue dans le certificat transmis ;
- la vérification de l'identifiant de la politique de signature référencée.

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	15/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable



4 Dispositions juridiques

4.1 Droit applicable

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

4.2 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.

4.3 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.

4.4 Propriété intellectuelle

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

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

4.5 Protection des données 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.

Erreur ! Nom de propriété de document inconnu.				
Identification du document (OID)	Version	Date	Classification	Page
1.2.250.1.35.25.2.1.2.12.1	1.0	Août 13	PUBLIC	16/16

Ce document est la propriété du groupe SFR - il ne peut pas être communiqué à un tiers sans accord préalable