

Conditions d'utilisation service de certification Swisscom (Signatures électroniques qualifiées et avancées)

Conditions d'utilisation relatives au service de certification de Swisscom avec des certificats avancés pour les signatures électroniques avancées (classe de certificat Swisscom « Saphir ») et des certificats qualifiés pour les signatures électroniques qualifiées (classe de certificat Swisscom « Diamant »)

1 Champ d'application des conditions d'utilisation

Les présentes conditions d'utilisation régissent vos relations avec Swisscom (Suisse) SA, Alte Tiefenastrasse 6, Worblaufen, Suisse, numéro d'identification d'entreprise CHE-101.654.423 (ci-après dénommée « Swisscom »), dans le cadre de l'utilisation du service de certification de Swisscom avec certificats qualifiés et avancés pour les signatures électroniques qualifiées et avancées.

2 Prestations de Swisscom

2.1 Service de certification en général

Swisscom est reconnue en Suisse en tant que fournisseur de services de certification selon la loi fédérale suisse sur la signature électronique (SCSE ; RS 943.03) pour vos services de certification avec certificats qualifiés. Elle fait l'objet d'un contrôle et d'une surveillance par l'organisme de reconnaissance SCSE. Pour vos services de certification avec certificats avancés, Swisscom propose des services de certification qui sont exécutés selon les normes techniques reconnues sur le plan international.

De manière générale, le service de certification est fourni selon la politique de certification en vigueur chez Swisscom. Ces directives - directives de certificat (CP/CPS) pour la délivrance de certificats de la classe « Diamant » (qualifiés) et « Saphir » (avancés) - font partie intégrante des présentes conditions d'utilisation. Vous pouvez consulter et télécharger le document sur le site internet

https://www.swisscom.ch/fr/business/enterprise/offre/security/digital_certificate_service.html

(à la rubrique « CH »).

Dans le cadre du service de certification, Swisscom délivre un certificat numérique qui contient entre autres des informations vous concernant. Selon l'application usager, une distinction est faite entre les certificats avec nom en clair et les certificats avec pseudonyme (voir le chiffre 7.3). Swisscom relie ce certificat numérique au fichier que vous signez de manière électronique (p. ex. un document pdf de votre banque). La signature électronique sur le document est ainsi rattachée à votre personne, à l'instar de la signature manuscrite, où la reproduction écrite du nom sur le document est associée à la personne qui signe. Les tiers peuvent ainsi se fier à la signature électronique et aux informations contenues dans le certificat numérique.

En fonction du type de signature proposé par l'application usager (voir le chiffre 3), la signature électronique qui est créée est soit une signature qualifiée selon l'article 2 lettre e de la loi fédérale suisse sur la signature électronique (SCSE ; RC 943.03), soit une signature avancée. Tout autre type d'utilisation du certificat qualifié est interdit dans le cadre de l'utilisation du service de certification selon les présentes conditions d'utilisation (« restriction d'utilisation »).

2.2 Processus d'identification et conservation des informations

Swisscom ou le bureau d'enregistrement mandaté par Swisscom vérifie votre identité lors du processus d'identification. Pour les signatures électroniques qualifiées, ce contrôle s'effectue sur la base de votre passeport, d'une carte d'identité reconnue pour entrer en Suisse ou d'un processus certifié, considéré comme équivalent et permettant de renoncer à une présence physique.

Suivant la configuration concrète du processus d'identification, vous pouvez être invité durant le processus d'identification pour les signatures électroniques avancées à présenter d'autres documents que ceux produits pour la signature électronique qualifiée.

Sur la base de votre processus d'identification pour les signatures électroniques qualifiées, vous pouvez aussi créer des signatures électroniques avancées selon les présentes conditions d'utilisation, pour autant que l'application que vous utilisez propose différents types de signature. En revanche, le processus d'identification pour les signatures électroniques avancées peut ne pas être utilisable pour le niveau de signature plus élevé de la signature électronique qualifiée.

Swisscom enregistre et stocke les informations relatives à votre personne, collectées durant le processus d'identification selon les prescriptions en vigueur. Le traitement de vos données est décrit au chiffre 6 des présentes conditions d'utilisation.

Swisscom exploite en outre un service d'annuaires disponible au grand public, lequel permet de vérifier le statut d'identification d'une personne afin d'éviter qu'une personne déjà identifiée et enregistrée ait à réitérer le processus d'identification. Dans ce cadre, les données suivantes seront vérifiées et affichées sur la base de la saisie du numéro de téléphone portable concerné : identifié pour la signature électronique avancée ou qualifiée, droit de créer des signatures selon le droit Suisse et/ou de l'UE, numéro de téléphone portable confirmé, numéro de série de l'identification interne à Swisscom et mention spécifique si l'autorisation de signature arrive sous peu à échéance (date).

2.3 Délivrance du certificat et des clés, création de la signature

Swisscom crée le certificat avancé ou qualifié ainsi que la paire de clés cryptographiques pour l'opération de signature sur un serveur dédié (Hardware Security

Module, HSM). Le certificat avancé ou qualifié est une attestation qui vous assigne la clé publique d'une paire de clés cryptographiques asymétriques. Vous êtes le(la) seul(e) à disposer des données d'activation, qui vous permettent d'utiliser la clé privée en utilisant une méthode d'authentification associée à votre identité (p.ex. authentification par Mobile ID, par une application autorisée telle que Mobile ID ou par mot de passe/SMS, cf. également les chiffres 3 et 4 des présentes conditions d'utilisation). Dès que vous saisissez les données d'activation après y avoir été invité, Swisscom crée pour vous la signature électronique avancée ou qualifiée basée sur le certificat.

Swisscom crée pour chaque opération de signature un nouveau certificat numérique (d'une durée de validité de 10 minutes) avec une nouvelle paire de clés.

2.4 Vérification de la signature électronique

Le service de certification de Swisscom permet de confirmer la validité de la signature électronique. Les tiers (souvent appelés « relying party ») peuvent également confirmer la validité de votre signature électronique (p. ex. pour les signatures électroniques qualifiées sur la page internet www.validator.ch. S'agissant des effets juridiques des différentes signatures électroniques, il convient de se reporter aux explications figurant au chiffre 5 des présentes conditions d'utilisation.

2.5 Disponibilité

Swisscom s'efforce de mettre le service de certification à disposition sans interruption. Elle n'assume toutefois aucune responsabilité relative à la disponibilité en continu du Signing Service, même en cas de lenteur ou de blocage du système réseau ou de problème en lien avec la disponibilité de services mobiles ou avec la connexion Internet. Elle peut limiter temporairement la disponibilité du service, par exemple lorsque cela est nécessaire compte tenu des limites de capacité, de la sécurité ou de l'intégrité des serveurs ou lorsqu'il faut exécuter des mesures techniques de maintenance ou de remise en état permettant d'assurer une bonne exécution des prestations ou leur amélioration (opérations de maintenance). Swisscom s'efforce à cet égard de tenir compte des intérêts des utilisateurs du service de certification. Vous pouvez consulter l'état actuel de disponibilité du service ici :

<https://trustservices.swisscom.com/fr/etat-du-service/>

3 Conditions requises pour l'utilisation

Vous disposez d'une connaissance appropriée des certificats numériques ainsi que des signatures électroniques qualifiées et avancées.

Vous utilisez un terminal et vous vous connectez via un portail internet ou une application qui permet l'utilisation du service de certification de Swisscom (« application usager »). Il peut s'agir d'un logiciel de comptabilité de votre employeur ou du portail internet de votre banque ou de votre assurance. Des restrictions à l'utilisation du service de certification peuvent résulter des prescriptions de l'application usager. Plus particulièrement, c'est l'application que vous utilisez qui détermine si vous pouvez créer des signatures électroniques avancées ou qualifiées. L'application usager détermine également si vous passez par un processus

d'identification unique pour chaque signature électronique (signature unique) ou si vous pouvez créer plusieurs signatures électroniques pendant une certaine période de temps après le processus d'identification. La connexion de l'application usager au service de certification de Swisscom fait l'objet d'un contrat distinct.

Vous disposez d'un moyen d'authentification autorisé permettant de transmettre votre accord pour la signature électronique (p. ex. un téléphone portable). Il peut s'agir d'une authentification par mot de passe envoyé par SMS, d'une application autorisée telle que Mobile ID ou d'une autre méthode de validation de la signature reconnue. La validation effective de la signature dépend de la connexion de l'application usager que vous utilisez.

Si la signature est validée par Mobile ID, vous devez, pour utiliser le service de certification, disposer d'une Mobile ID fournie par un prestataire suisse de Mobile ID (p. ex. Swisscom) ou utiliser l'application Mobile ID, que vous aurez initialisée auparavant avec votre numéro de téléphone portable.

4 Vos devoirs de collaboration

Dans le cadre du processus d'identification, vous vous engagez à ne fournir que des informations complètes et véridiques à Swisscom ou au bureau d'enregistrement.

Vous vous engagez à ne pas utiliser de données se référant à votre personne (anniversaire et autres) lorsqu'un mot de passe est requis pour la création de la signature électronique). Les éventuelles reproductions du code PIN ou du mot de passe personnel dans le cadre de l'authentification ne doivent pas être divulguées à d'autres personnes, doivent être cryptées ou conservées en lieu sûr et séparément de votre moyen d'authentification (p. ex. téléphone portable) et doivent être protégées contre tout accès de tiers.

Si vous utilisez le processus d'authentification de mot de passe en combinaison avec un mot de passe à usage unique envoyé par SMS transmis par Swisscom, assurez-vous que la saisie des données sollicitées se fait toujours sur les écrans de saisie du système Swisscom. Vous trouverez des précisions à ce sujet dans [ce document](#).

Si p. ex. votre appareil mobile, votre carte SIM ou le mot de passe personnel, que vous devez indiquer lors de la procédure d'authentification par SMS, a été volé ou si vous savez ou supposez qu'une autre personne en a connaissance (facteurs compromis), vous vous engagez à respecter les points suivants :

- renoncer immédiatement à la création de signatures
- modifier le cas échéant les données d'accès (p. ex. sur la page d'enregistrement de Mobile ID, celles de l'application Mobile ID ou le mode de passe) et si nécessaire bloquer la carte SIM

Toute modification d'un appareil utilisé pour l'authentification (par exemple, votre numéro de téléphone portable ou votre carte SIM) ou à vos données d'identité. ou des données d'identité doit être signalée au bureau d'enregistrement ou directement à Swisscom.

Vous vous engagez à utiliser toutes les mesures raisonnables et modernes pour protéger votre terminal et votre téléphone portable utilisé pour l'authentification ou la signature contre des attaques et des logiciels malveillants (« virus », « vers », « cheval de Troie » et autres), en particulier en utilisant toujours des logiciels récents provenant d'une source officielle.

Vous vous engagez à vérifier la signature électronique après sa création conformément au chiffre 2.4 des présentes conditions d'utilisation et à signaler rapidement à Swisscom toute éventuelle irrégularité au niveau du certificat numérique.

5 Effets juridiques de la signature électronique

Le service de certification selon les présentes conditions d'utilisation génère soit une signature électronique qualifiée selon l'article 2 lettre e de la loi fédérale suisse sur la signature électronique (SCSE ; RS 943.03), soit une signature électronique avancée selon les directives de certification de Swisscom.

L'application usager que vous utilisez pour accéder au service de certification (cf. le chiffre 3 des conditions d'utilisation) détermine pour chaque opération de signature le type de signature (signature électronique qualifiée ou avancée). Swisscom n'a aucune influence sur ce choix.

L'application usager que vous utilisez va associer chez Swisscom la signature électronique qualifiée ou avancée à un horodatage qualifié auprès du service de certification. En fonction des paramètres d'accès au service de certification de Swisscom, la signature électronique sera donc générée avec ou sans horodatage qualifié. Lors de la vérification de la signature (cf. le chiffre 2.4 des présentes conditions d'utilisation), vous pouvez contrôler si la signature électronique est associée ou non à un horodatage qualifié.

Seule la signature électronique qualifiée avec horodatage qualifié est assimilée à une signature manuscrite en vertu du droit suisse, les dispositions légales ou conventionnelles contraires demeurant réservées (article 14 du code suisse des obligations). Suivant la situation, certains documents nécessitent une signature manuscrite pour produire les effets juridiques souhaités.

La signature électronique avancée n'est pas réglée dans la loi suisse (à la différence de la signature électronique qualifiée) et ne satisfait pas à l'exigence de forme écrite au sens de l'article 14 du code suisse des obligations ; elle ne déploie donc pas les mêmes effets juridiques qu'une signature manuscrite. L'exigence légale de la signature manuscrite ne peut en principe être valablement remplacée que par la signature électronique qualifiée (en lien avec un horodatage qualifié) jugée équivalente, laquelle ne doit pas être confondue avec la signature électronique avancée basée sur un certificat avancé au sens des présentes conditions d'utilisation.

Dans ce contexte, il vous appartient de clarifier vos exigences ainsi que les effets juridiques de la signature électronique qualifiée ou avancée avant d'utiliser le service de certification.

Vous reconnaissez que les signatures électroniques qualifiées ou avancées créées avec le service de certification suisse de Swisscom peuvent avoir d'autres effets, éventuellement moins étendus, ou ne pas remplir les prescriptions de forme (comme la forme écrite) lorsque le droit d'un pays étranger s'applique.

L'utilisation de certains algorithmes techniques est par ailleurs soumise à des restrictions légales dans certains Etats. Il vous incombe de clarifier au préalable les conditions en la matière.

L'enregistrement d'informations complémentaires sur le certificat numérique (attributs ou qualités spécifiques tels que le droit de représentation de votre employeur) est de nature purement déclarative ; l'existence d'une qualité spécifique et ses effets juridiques sont régis par le droit applicable (droit de représentation, droit de la société, etc.) et ne relèvent ni de la sphère d'influence ni de la responsabilité de Swisscom. Dans ce contexte, Swisscom ne répond que de la vérification de l'existence d'une qualité spécifique au moment de la vérification de l'identité au moyen des justificatifs exigés par Swisscom. Les qualités spécifiques pouvant figurer sur les certificats numériques ne représentent pas toutes les situations prévues par le droit civil (droit de signature collective, droit de signature dans les cas spéciaux, etc.).

6 Durée d'utilisation

Dans les limites des conditions fixées au chiffre 3, vous pouvez utiliser le service de certification régi par les présentes conditions d'utilisation vous pouvez utiliser le service de certification en utilisant une méthode d'authentification déposée au moment de l'enregistrement pendant une durée maximale de cinq ans, cette durée pouvant être raccourcie pour les signatures électroniques qualifiées si la validité des documents d'identification que vous avez présentés est plus courte ou si la procédure d'identification reconnue prévoit de manière générale une durée d'utilisation plus courte.

7 Traitement de vos données

7.1 Généralités, déclaration de confidentialité

Swisscom collecte, stocke et traite uniquement les données nécessaires à l'exécution du service de certification. Le traitement des données est régi par les lois suisses applicables (loi suisse sur la protection des données, loi suisse sur la signature électronique pour les signatures électroniques qualifiées) et par les directives de certificat mentionnées ci-dessus au chiffre 2.1.

Le traitement de vos données est en outre réglé dans [la déclaration de confidentialité](#) relative à l'utilisation du service de certification de Swisscom, que vous pouvez consulter à l'adresse <https://trustservices.swisscom.com/fr/>.

7.2 Documents d'identification

Afin de délivrer le certificat numérique et de préserver la traçabilité du service de certification, Swisscom, ou l'autorité d'enregistrement mandatée par Swisscom, saisit et conserve les données suivantes vous concernant (pour autant que vous les ayez communiquées lors du processus d'identification selon le chiffre 2.2 des présentes conditions d'utilisation) :

Identification personnelle en présence :

- copie des pages pertinentes de la pièce d'identité que vous avez présentée (passeport, carte d'identité, éventuellement d'autres documents selon le chiffre 2.2 lorsque seules des signatures électroniques avancées doivent être créées) avec les informations y figurant (en particulier les prénoms, le nom de famille, le sexe, la date de naissance, la date d'expiration et numéro de série de la pièce d'identité, la nationalité)
- moyen d'authentification personnel utilisé (p. ex. numéro de téléphone portable)

Identification par vidéo ou autovidéo :

- photographie de vous tirée de l'identification vidéo
- photographies des pages pertinentes de la pièce d'identité que vous avez présentée
- enregistrement audio de l'appel vidéo
- données techniques (p. ex. adresse IP) du terminal que vous avez utilisé
- informations résultant du document de légitimation muni d'une photo (en particulier les nom, prénom, sexe, date de naissance, date d'expiration et numéro de série du document d'identification, nationalité)
- moyen d'authentification personnel utilisé (p. ex. numéro de téléphone portable)
- si pris en charge : données lues sur la puce de votre document d'identité (p. ex. nom, prénom, date de naissance, adresse, date d'expiration et numéro de série du document d'identification, nationalité)

Identification par eID :

- moyen d'authentification personnel utilisé (p. ex. numéro de téléphone portable)
- données d'un service eID autorisé auquel il est accédé à distance à l'aide d'un moyen d'authentification (p. ex. nom, prénom, sexe, date de naissance, adresse, date d'expiration et numéro de série du document d'identification, nationalité)

Identification basée sur un compte e-banking :

- vos données personnelles transmises par vos soins ou par l'exploitant de l'application de signature (en particulier les nom, prénom, sexe, date de naissance, lieu de naissance, adresse de domicile, nationalité)
- moyen d'authentification personnel utilisé (p. ex. numéro de téléphone portable)
- votre compte bancaire utilisé pour l'e-banking (IBAN/BIC/nom de la banque)
- le cas échéant, ID de la SchuFa ou ID d'une autre société de renseignement sur la solvabilité
- le cas échéant, données relatives à la transaction de référence
 - titulaire du compte
 - numéro du compte
 - moment du versement de référence
 - procédé de validation de la transaction

Autres données et documents que vous avez transmis dans le cadre de la procédure d'identification, p. ex. également relatifs à votre organisation, tels qu'un extrait du registre du commerce, des procurations, des contrats de société, adresse e-mail ou d'autres justificatifs relatifs à des éléments spécifiques figurant dans le certificat.

7.3 Certificat numérique

Sur la base des données que vous avez fournies et qui ont été recueillies lors du processus d'identification, Swisscom établit, sur requête de l'application usager et avec votre accord, un certificat qualifié ou avancé qui peut contenir les informations suivantes sur vous.

Si l'application usager prévoit l'utilisation de noms en clair :

- prénoms, nom de famille
- nom informel pour une présentation simplifiée (p. ex. prénom usuel)
- code ISO 3166 du pays, à deux caractères

Si l'application usager prévoit l'utilisation de pseudonymes :

- pseudonyme
- description informelle pour une présentation simplifiée (p. ex. mention PSEUDONYME)
- code ISO 3166 du pays, à deux caractères

Les données suivantes peuvent en outre figurer dans le certificat :

- autres données, p. ex. pour garantir le caractère univoque du certificat numérique :
 - désignation de l'entreprise
 - numéro/ID de la pièce d'identité présentée
- numéro de téléphone portable
- texte affiché pour la autorisation de la signature de l'application de signature que vous utilisez (p. ex. « Veuillez confirmer la signature figurant dans le fichier test.pdf dans l'application XYZ »)
- bureau d'enregistrement chargé de l'identification
- date d'établissement du certificat numérique

Au terme de l'opération de signature, le certificat numérique est contenu dans le fichier signé électroniquement. Quiconque est en possession du fichier signé électroniquement peut à tout moment consulter les données du certificat numérique mentionnées ci-dessus. Les tiers peuvent ainsi vérifier les données relatives à votre personne et constater que Swisscom s'est chargée de certifier ces données et l'opération de signature en sa qualité de fournisseur suisse de services de certification.

7.4 Données à l'issue de l'opération de signature

Swisscom ou son bureau d'enregistrement conserve les données décrites au chiffre 7.2 pendant la durée d'utilisation prévue au chiffre 6 des conditions d'utilisation, afin que vous puissiez utiliser le service de certification. Pour les signatures électroniques qualifiées, la loi oblige en outre Swisscom (le cas échéant en recourant à un bureau d'enregistrement) à conserver

certaines données relatives au processus d'identification, au certificat numérique et à l'opération de signature durant 11 ans à compter de la dernière opération de signature. En cas de signatures électroniques avancées, Swisscom conserve certaines données relatives au processus d'identification, au certificat numérique et à l'opération de signature durant 7 ans à compter de la dernière opération de signature, en application de ses directives de certificat. Cela permet de garantir que l'exactitude du document signé électroniquement pourra être retracée dans les années qui suivent sa création. Swisscom enregistre à cet effet toutes les informations pertinentes sur les données qu'elle a émises ou reçues et conserve celles-ci de manière à ce qu'elles soient disponibles, notamment pour fournir des preuves lors de procédures judiciaires ou pour garantir la continuité du service de certification.

Swisscom conserve d'une part les données suivantes :

- fichiers log relatifs à l'opération de signature (comprend en particulier le numéro de partenaire commercial, le numéro de l'opération, les données procédurales)
- valeur de hachage du document signé

Si Swisscom ne conserve pas elle-même les informations au sens du chiffre 7.2 des présentes conditions d'utilisation, le bureau d'enregistrement remet ces données à Swisscom, dans la mesure exigée par la législation pour l'exécution du service de certification. Swisscom tient en outre une banque de données des certificats. Swisscom efface les données décrites au présent chiffre 7.4 après un délai maximum de 17 ans à compter de l'exécution du processus d'identification selon le chiffre 2.2 des conditions d'utilisation. En cas d'identification après une demande portant uniquement sur des signatures électroniques avancées selon le chiffre 2.2, Swisscom efface ces données après un délai maximum de 13 ans à compter de l'exécution du processus d'identification.

8 Recours à des tiers

Swisscom est en droit de faire appel à des tiers pour exécuter ses obligations et fait en particulier appel à Swisscom Trust Services SA, Zurich, Suisse pour la fourniture de technologies et de prestations. Elle peut également charger d'autres tiers (bureaux d'enregistrement) d'exécuter le processus d'identification (y compris la conservation des documents d'identification).

9 Responsabilité et force majeure

Swisscom doit en tout temps respecter les exigences que la loi et les normes techniques imposent aux fournisseurs de services de certification. A cette fin, Swisscom applique des mesures de sécurité appropriées et conformes au niveau technique actuel. Vous prenez acte du fait que malgré

- tous les efforts de Swisscom,
- le recours à une technologie et à des normes de sécurité modernes et
- le contrôle par un organisme indépendant en ce qui concerne le respect des normes techniques et,

- pour les signatures électroniques qualifiées, le contrôle par l'organisme de reconnaissance SCSE en ce qui concerne le respect des dispositions légales,

il n'est pas possible de garantir une sécurité absolue ni l'absence d'erreurs du service de certification.

Swisscom demeure entièrement responsable à votre égard du dommage qui vous a été causé du fait qu'elle n'a pas respecté ses obligations découlant de la loi fédérale suisse sur la signature électronique, à moins qu'elle ne démontre qu'aucune faute ne lui est imputable. Si, avant la création d'une signature, Swisscom vous informe, directement ou par l'intermédiaire de l'exploitant de l'application usager, d'une limite de transaction pour les actes juridiques impliquant le versement d'argent (également en lien avec la création d'une signature électronique avec le service de certification de Swisscom) et que cette limite de transaction est visible pour des tiers, p. ex. lorsqu'elle est indiquée dans le certificat, Swisscom ne répond pas des dommages résultant d'une utilisation des services allant au-delà de cette limite.

Pour les autres violations contractuelles (en particulier celles en lien avec les certificats avancés et les signatures électroniques avancées), Swisscom répond envers vous du dommage prouvé, à moins qu'elle ne démontre qu'aucune faute ne lui est imputable, et ce aux conditions suivantes : La responsabilité pour les préjudices matériels et les dommages pécuniaires dus à une négligence simple est limitée à concurrence de CHF 5'000 pour toute la durée du contrat. La responsabilité de Swisscom est exclue en cas de dommages indirects dus à une négligence simple, de dommages subséquents, de gain manqué, de perte de données, de dommages causés par des téléchargements, de prétentions de tiers et d'atteintes à la réputation. Swisscom demeure entièrement responsable envers vous en cas de dommages corporels. Elle ne répond en revanche pas envers vous du bon fonctionnement des systèmes de tiers, en particulier du matériel informatique et des logiciels que vous avez employés ou de l'application usager que vous avez utilisée pour accéder au service de certification.

La responsabilité de Swisscom à votre égard est exclue lorsque la fourniture de ses prestations est momentanément suspendue, partiellement ou totalement limitée ou rendue impossible en raison d'un cas de force majeure. Par cas de force majeure, on entend notamment les phénomènes naturels d'une intensité particulièrement élevée (avalanches, inondations, glissements de terrain, etc.), les conflits armés, les émeutes, les restrictions imprévisibles imposées par les autorités ainsi que les pandémies et les épidémies. Si Swisscom est dans l'incapacité de remplir ses engagements contractuels, l'exécution du contrat ou le délai d'exécution du contrat est reporté en fonction de l'événement survenu. Swisscom ne répond pas des éventuels dommages causés au client par le report de l'exécution du contrat.

10 Modification des conditions d'utilisation

Swisscom se réserve le droit de modifier les présentes conditions ou de les compléter. En particulier en cas de modification de la loi fédérale sur la signature électronique (SCSE ; RS 943.03) et de ses dispositions d'exécution, de même que sur ordre de l'organisme de

reconnaissance SCSE ou d'un organisme indépendant chargé de la vérification des signatures électroniques avancées, Swisscom peut se voir contrainte d'adapter les directives de certificat mentionnées au chiffre 2.1 des présentes conditions ou les conditions d'utilisation elles-mêmes. Swisscom ou le bureau d'enregistrement mandaté par cette dernière vous informera des et du délai dont vous disposez pour les contester au moins un mois avant leur entrée en vigueur. Cette information peut être donnée par un SMS envoyé au numéro de téléphone portable que vous avez indiqué à condition que vous n'ayez été enregistré que pour une signature unique. Vous pouvez refuser les nouvelles conditions en renonçant à l'utilisation du service de certification régi par les présentes conditions d'utilisation à compter de l'entrée en vigueur. Le fait de continuer à utiliser le service de certification après l'entrée en vigueur des modifications sera considéré comme une acceptation des nouvelles conditions.

11 Droit applicable et for

Tous les rapports juridiques en lien avec les présentes conditions d'utilisation sont soumis au droit suisse.

En cas de différend, nous nous efforçons de régler le litige à l'amiable. Sous réserve des fors impératifs (en particulier les art. 32 et 35 du code suisse de procédure civile en ce qui concerne les consommateurs), le for est Berne, en Suisse.

12 Comment nous joindre

En cas de question concernant la fourniture des prestations selon les présentes conditions d'utilisation, vous pouvez contacter Swisscom via la page internet www.swisscom.com/signing-service.