SAFY TRUST SERVICES

Conditions Générales d'Utilisation
du Service de Création de Signature de SAFY

Version : 1.0
Date d'entrée en vigueur : 28/01/2026
Classification : C0 - Publique

Historique des révisions

Version	Date	Auteur(s)	Commentaires
1.0	22/01/2026	JPA	Version initiale

Table des matières

1 Introduction

Le présent document définit les Conditions Générales d'Utilisation (CGU) applicables au Service de Création de Signature (SCS) fourni par SAFY, qui ont pour but de présenter les conditions d'utilisation du service, les responsabilités des parties impliquées dans le processus de signature électronique, ainsi que les principes applicables aux signatures produites par le SCS.

Il est identifié par son titre et son numéro de version. Les évolutions de version des CGU peuvent intervenir indépendamment de celles de la Politique de Signature et Déclaration des Pratiques de Signature (PS/DPS) du SCS, sous réserve du maintien d'une parfaite cohérence entre ces documents.

Les présentes CGU s'appliquent aux politiques de signature suivantes, chacune identifiée par un OID spécifique :

- **1.3.6.1.4.1.60428.1.3.2.1** : politique de signature relative à la création de signatures électroniques simples conformément à l'article 2 de la loi n°43-20 relative aux services de confiance pour les transactions électroniques ;
- **1.3.6.1.4.1.60428.1.3.2.2** : politique de signature relative à la création de signatures électroniques avancées conformément à l'article 5 de la loi n°43-20, sur la base d'une authentification du signataire au moyen du service d'identité numérique de la DGSN ;
- **1.3.6.1.4.1.60428.1.3.2.3** : politique de signature relative à la création de signatures électroniques avancées conformément à l'article 5 de la loi n°43-20, sur la base d'une vérification de l'identité du signataire réalisée par une Autorité d'Enregistrement Déléguée (AED).

Les politiques de signature couvertes par les présentes CGU sont décrites de manière détaillée dans la PS/DPS, qui précise notamment les exigences techniques, organisationnelles et de sécurité applicables au SCS, ainsi que les processus de création, de validation et de conservation des signatures électroniques. La version en vigueur de la PS/DPS est accessible à l'adresse suivante : https://pki.safy.ma/g2

L'utilisation du SCS implique l'acceptation sans réserve des présentes CGU.

2 Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
DGSN	Direction Générale de la Sûreté Nationale

DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DPC	Déclaration des Pratiques de Certification
DPS	Déclaration des Pratiques de Signature
OID	Object Identifier
OTP	One Time Password
PC	Politique de Certification
PS	Politique de Signature
SCS	Service de Création de Signature
URL	Uniform Resource Location

3 Définitions

Autorité d'Enregistrement (AE)	Autorité chargée de la vérification de l'identité des Signataires et de la conservation des éléments de preuve associés. Dans le cadre des présentes CGU, l'AE est gérée par le SCS.
Autorité d'Enregistrement Déléguée (AED)	Entité légale ayant contractée avec l'AE pour gérer tout ou partie des missions de l'AE.
Autorité de Certification (AC)	Autorité chargée du cycle de vie d'un certificat.
Politique de Certification et Déclaration des Pratiques de Certification (PC/DPC)	Document décrivant les règles et pratiques suivies par une AC pour émettre des certificats. Elle précise les engagements de l'AC, les niveaux de confiance visés, les rôles des parties, et les mesures de sécurité mises en œuvre.
Politique de Signature et Déclaration des Pratiques de Signature (PS/DPS)	Document décrivant les règles et pratiques suivies par le Service de Création de Signature (SCS) pour produire, valider, conserver et mettre à disposition des signatures électroniques. Il précise les engagements du prestataire, les types de signatures proposés, les rôles des parties impliquées, les conditions d'utilisation du service ainsi que les mesures de sécurité mises en œuvre pour garantir l'intégrité des documents, l'identification du signataire et la valeur probatoire des signatures.
Service de Création de Signature (SCS)	Service de confiance gérée par SAFY pour la création de signatures électroniques simples et avancées.

Signataire	Personne physique invitée à signer des documents par le Souscripteur à travers le SCS.
Souscripteur	Entité légale ayant contractée avec SAFY pour utiliser le SCS dans le but de faire signer des documents à des Signataires.
Validateur	Personne physique ou morale qui vérifie et contrôle la validité d'une signature électronique produite par le SCS.

4 Conditions Générales d'Utilisation

Point de contact	SAFY.io TR21A-54, les Portes de Marrakech, 40140 MARRAKECH, MAROC contact-pki@safy.ma
Type de signatures produites	Le Service de Création de Signature (SCS) de SAFY produit les types de signatures électroniques suivants, tels que définis par la loi n°43-20 et identifiés par leur OID dans la PS/DPS : • **Signature électronique simple** (1.3.6.1.4.1.60428.1.3.2.1) : garantit l'identification du Signataire, son consentement et l'intégrité du document signé. Aucune authentification préalable du Signataire n'est obligatoire. • **Signature électronique avancée « eID DGSN »** (1.3.6.1.4.1.60428.1.3.2.2) : le Signataire est authentifié par le service « Identité Numérique » de la DGSN, avec deux facteurs d'authentification distincts (CNIE ou titre de séjour + code PIN ou reconnaissance faciale). • **Signature électronique avancée « AED »** (1.3.6.1.4.1.60428.1.3.2.3) : l'identité du Signataire est vérifiée préalablement par le Souscripteur agissant en qualité d'Autorité d'Enregistrement Déléguée (AED), sur la base d'un document officiel d'identité en cours de validité. Toutes les signatures produites sont au format PAdES-B-LT (ETSI EN 319 142-1), horodatées et accompagnées d'un Dossier de preuve. Le SCS est disponible 24h/24 et 7j/7 selon un taux de disponibilité mensuel de 99,5 %.
Objet du service et des signatures produites	Le SCS permet la signature électronique de documents PDF pour le compte de Signataires, à la demande de Souscripteurs. Les signatures produites garantissent l'intégrité des documents signés, l'identification du Signataire et la traçabilité de son consentement. Elles sont destinées à être vérifiées par des Validateurs à des fins probatoires ou contractuelles.
Processus de signature	**1. Initialisation** Une demande de signature émane de la volonté du Souscripteur de faire signer de façon électronique un ou plusieurs documents

	à un Signataire. Pour cela, le Souscripteur transmet au SCS les informations du Signataire (au minimum son nom et son prénom), les documents à signer, ainsi que les paramètres de la Transaction (type de signature, mode d'invitation, mode d'authentification, etc.). **2. Vérification d'identité** Les preuves de validation de l'identité du Signataire sont conservées dans le Dossier de preuve créé et conservé par le SCS. Pour une signature simple (OID 1.3.6.1.4.1.60428.1.3.2.1) : Le SCS peut, le cas échéant, procéder à une authentification du Signataire via l'envoi d'un OTP par email, SMS ou WhatsApp, ou via une authentification réalisée par un fournisseur d'identité tiers. Pour une signature avancée (OID 1.3.6.1.4.1.60428.1.3.2.2 et .3) : L'identité du Signataire est vérifiée soit par le SCS via le service « Identité Numérique » de la DGSN (avec 2 facteurs d'authentification : CNIE ou titre de séjour + code PIN ou reconnaissance faciale), soit par le Souscripteur agissant en tant qu'AED sur la base d'un document officiel d'identité. **3. Exécution de la Transaction** Le Signataire prend connaissance des documents à signer, approuve les CGU du SCS (obligatoire pour la signature avancée), est authentifié, confirme ses informations d'identification, et clique sur le bouton « Signer ». À tout moment, le Signataire peut refuser de signer en interrompant la Transaction ou en cliquant sur le bouton « Refuser ». **4. Finalisation** Le SCS génère la clé privée du Signataire, émet le certificat via l'Autorité de Certification « Safy Intermediate CA G2 », crée les signatures PAdES-B-LT horodatée, détruit immédiatement la clé privée, puis génère et cachète le Fichier de preuve. L'acceptation de la signature par le Signataire est tacite dès lors qu'il clique sur le bouton « Signer ».

Conservation et archivage	À l'issue de chaque Transaction de signature, le SCS produit et conserve de manière sécurisée un Dossier de preuve pendant une durée minimale de 7 ans. Ce Dossier contient notamment : • Le Fichier de preuve relatif à la transaction de signature (événements du processus, empreintes des documents avant et après signature, etc.). • La version des CGU acceptées par le Signataire (son empreinte de hachage est intégrée au Fichier de preuve). Les documents signés peuvent être conservés par le SCS si le Souscripteur en fait la demande. Le Dossier de preuve est mis à disposition des personnes autorisées (Souscripteur, Validateur, autorités compétentes) sur demande, conformément à la PS/DPS.
Validation des signatures	La validation d'une signature produite par le SCS implique, conformément au chapitre 6 de la PS/DPS : • La vérification cryptographique de la signature PAdES-B-LT (validité de la signature numérique et validité de la chaîne de certification jusqu'à l'AC racine) ; • La validation du cachet électronique du Fichier de preuve ; • Le contrôle de la cohérence du Fichier de preuve (identité du Signataire, OID de la politique de signature, empreinte des CGU acceptées). Ces vérifications peuvent être réalisées avec des outils standards tels qu'Adobe Acrobat Reader, OpenSSL ou BouncyCastle. Le certificat racine Safy Root CA 2 et son empreinte de hachage sont publiés sur : https://pki.safy.ma/g2
Limites d'utilisation	L'utilisation de la clé privée et du certificat associé d'un Signataire est strictement réservée au Service de Création de Signature (SCS) de SAFY dans le cadre de la signature électronique des documents soumis par le Souscripteur. Une clé privée est dédiée à la transaction de signature électronique pour laquelle elle a été spécialement créée et est immédiatement détruite par le SCS après la signature des documents de la transaction.

	Les dossiers d'enregistrement et les journaux associés aux Transactions de signature sont conservés par le SCS pendant une durée d'au moins 7 ans.
Obligations des Signataires	Les Signataires ont pour obligation de : • Vérifier que les informations les concernant, affichées lors de la Transaction de signature, sont exactes et à jour ; • Respecter les conditions d'utilisation de leur clé privée et ne pas l'utiliser pour des usages autres que la signature des documents soumis par le Souscripteur dans le cadre de la Transaction pour laquelle elle est spécifiquement créée ; • Informer le SCS de toute anomalie ou modification concernant les informations les concernant qui seraient contenues dans leur certificat de signature ; • Protéger leurs moyens d'authentification, le cas échéant ; • Consentir à la conservation par le SCS des informations des dossiers d'enregistrement et des Dossiers de preuve, ainsi qu'à leur éventuel transfert à un tiers dans les mêmes conditions de sécurité dans le cas où le SCS mettrait fin à ses services. Dans le cas de signatures avancées, les Signataires doivent également accepter les CGU qui leur sont présentées dans la transaction de signature.
Obligations des Souscripteurs	Les Souscripteurs ont pour obligation de : • Fournir au SCS des informations exactes et à jour lors de la phase d'enregistrement des Signataires, conformément à la PS/DPS ; • Informer le SCS de toute modification des informations concernant les Signataires ; • Lorsqu'ils agissent en qualité d'AED, procéder à la vérification préalable de l'identité du Signataire sur la base d'un document officiel en cours de validité, conformément à la Politique d'Enregistrement Déléguée approuvée par l'AC ; • S'engager à recueillir, au préalable, le consentement des Signataires pour le transfert de leurs données à caractère personnel au SCS, ainsi que pour leur traitement aux fins

	suivantes : la création des signatures électroniques et la conservation des Dossiers de preuve associés.
Obligations de vérification des signatures par les Validateurs	Les Validateurs devraient appliquer le processus complet de validation décrit au chapitre 6 de la PS/DPS (vérification cryptographique, validation du Fichier de preuve, cohérence des informations). Ils devraient en outre s'assurer que le niveau de la signature électronique correspond aux exigences légales ou contractuelles de leur contexte d'usage. En cas de compromission de la clé de l'AC, l'information sera publiée sur : https://pki.safy.ma/g2
Limites de responsabilité	Le SCS ne saurait être tenu responsable de toute utilisation non autorisée, frauduleuse ou non conforme du service, ni des dommages résultant d'une utilisation du SCS par le Souscripteur ou le Signataire contraire aux présentes CGU ou à la PS/DPS. Le SCS décline également toute responsabilité en cas de dommage résultant d'erreurs, d'omissions ou d'inexactitudes dans les informations transmises par le Souscripteur ou le Signataire, notamment concernant l'identité du Signataire ou le contenu des documents soumis à signature. En tout état de cause, et dans la stricte limite permise par la loi applicable, la responsabilité du SCS ne saurait être engagée au titre de dommages directs ou indirects, notamment matériels, immatériels, commerciaux, financiers ou moraux, résultant de l'exécution ou de l'utilisation des présentes.
Références documentaires	La Politique de Signature et Déclaration des Pratiques de Signature (PS/DPS) du SCS et la PC/DPC de l'AC « Safy Intermediate CA G2 » sont accessibles sur : https://pki.safy.ma/g2
Loi applicable et résolution des conflits	Les présentes CGU sont régies par le droit marocain, notamment par les dispositions de la loi n°43-20 relative aux services de confiance pour les transactions électroniques, ainsi que de la loi n°09-08 relative à la protection des données à caractère personnel. En cas de différend relatif à l'utilisation du Service, les parties s'engagent à rechercher, dans la mesure du possible, une solution amiable. À défaut de résolution amiable dans un délai

	raisonnable, tout litige sera porté devant les juridictions compétentes du Royaume du Maroc. Le SCS assure la réception et le traitement des réclamations et signalements via un canal identifié. Le point de contact à utiliser figure en première ligne du présent tableau.
Gestion des données à caractère personnel	Les données à caractère personnel collectées par le SCS (nom, prénom, adresse email, numéro de téléphone portable, adresse IP du Signataire) sont traitées exclusivement pour permettre la création des signatures électroniques et la conservation des Dossiers de preuve associés, dans le respect de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Le Souscripteur agit en tant que responsable de traitement au sens de la loi 09-08 et le SCS agit en qualité de sous-traitant, sur instruction du Souscripteur, afin d'exécuter techniquement la création des signatures électroniques et la conservation des Dossiers de preuve associés.
Audits et références applicables	Le SCS est audité chaque année par un auditeur ayant les compétences et l'impartialité appropriés afin d'attester de sa conformité au référentiel, publié par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) sur son site Internet, relatif aux services de confiance non qualifiés et aux prestataires fournissant ces services, pour la création des signatures simples et avancées. Le SCS est conforme à la norme ETSI EN 319 401.