SAFY TRUST SERVICES

Conditions Générales d'Utilisation des certificats de signature émis par l'AC Safy Intermediate CA G2

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

Ce document définit les Conditions Générales d'Utilisation (CGU) des certificats de signature émis par l'Autorité de Certification « Safy Intermediate CA G2 », appelée ACI dans la suite du document.

Il précise également les engagements et les obligations des différentes parties, ainsi que les modalités de gestion des certificats.

Ce document est référencé par son titre et son numéro de version. Le numéro de version est amené à évoluer de manière indépendante des évolutions de l'OID de la Politique de Certification et de la Déclaration des Pratiques de Certification (PC/DPC) de l'ACI.

Cette version des CGU s'appliquent aux certificats de signature électronique suivants qui sont chacun identifié par un OID spécifique :

- **Certificats signature simple** (1.3.6.1.4.1.60428.1.1.2.1.1) : certificats destinés aux personnes physiques invitées, par les Souscripteurs au Service de Création de Signature (SCS) de SAFY, à signer électroniquement des documents avec des signatures simples[1] ;
- **Certificats signature avancée** (1.3.6.1.4.1.60428.1.1.2.1.2) : certificats destinés aux personnes physiques invitées, par les Souscripteurs du Service de Création de Signature (SCS), à signer électroniquement des documents avec des signatures avancées[2].

2 Acronymes

AC	Autorité de Certification
ACI	Autorité de Certification Intermédiaire
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
CRL	Certificate Revocation List
DGSN	Direction Générale de la Sûreté Nationale
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DPC	Déclaration des Pratiques de Certification
OID	Object Identifier
OTP	One Time Password
PC	Politique de Certification

[1] Voir la définition de la signature électronique simple dans l'article 2 de la [Loi 43-20].
[2] Voir la définition de la signature électronique avancée dans l'article 5 de la [Loi 43-20].

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.
Service de Création de Signature (SCS)	Service de confiance gérée par SAFY pour la création de signatures électroniques simples et avancées. Dans le cadre des présentes CGU, le SCS gère l'AE.
Signataire	Personne physique invitée à signer des documents par le Souscripteur à travers le SCS. Le Signataire est identifiée dans le certificat de signature délivré par l'ACI.
Souscripteur	Entité légale ayant contractée avec SAFY pour utiliser le SCS dans le but de faire signer des documents à des Signataires.
Utilisateur de certificat	Personne physique ou morale qui utilise un certificat, et qui doit, pour pouvoir s'y fier, vérifier la validité du certificat, en contrôlant notamment la validité de sa signature numérique et son statut de révocation.

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 certificats émis	Les 2 types de certificats décrits dans le chapitre 1 sont délivrés par l'ACI à des personnes physiques, appelés Signataires, qui sont invités par des Souscripteurs à signer des documents électroniques. Chaque certificat est valable au maximum 30 minutes et est dédié à la transaction de signature électronique pour laquelle il est spécifiquement créé. L'ACI est émise par l'Autorité de Certification racine « Safy Root CA G2 ». Les certificats de ces AC sont disponibles sur le site de publication https://pki.safy.ma/g2, disponible 24h/24 et 7j/7 selon un taux de disponibilité mensuel de 99.5%.
Objet des Certificats	Les certificats émis par l'ACI sont des certificats de personnes physiques qui sont dédiés à la signature électronique de documents.
Modalités d'obtention	**1. Initialisation** Une demande de certificat émane de la volonté du Souscripteur de faire signer de façon électronique un ou plusieurs documents à un Signataire. Le Souscripteur transmet à l'AE les informations du Signataire (au minima son nom et son prénom). **2. Vérification d'identité** Les preuves de validation de l'identité du Signataire sont conservées dans le dossier de preuve créé et conservé par l'AE. Pour un certificat de signature simple (1.3.6.1.4.1.60428.1.1.2.1.1) :

	L'AE peut, le cas échéant, procéder à une authentification du Signataire, via l'envoi, par exemple, d'un OTP par email ou par SMS, ou via une authentification réalisée par un fournisseur d'identité tiers. <u>Pour un certificat de signature avancée (1.3.6.1.4.1.60428.1.1.2.1.2)</u> : L'identité du Signataire est vérifiée : 1) Soit par l'AE, au cours de la Transaction de signature, via une authentification du Signataire utilisant le service « Identité Numérique » de la DGSN mettant en œuvre 2 facteurs d'authentification différents du Signataire : 1. Avec sa carte nationale d'identité électronique (CNIE) ou son titre de séjour électronique ; et 2. Avec son code PIN ou une reconnaissance faciale. 2) Soit par le Souscripteur lorsqu'il agit en tant qu'AED et qui doit vérifier l'identité du Signataire sur la base d'un document officiel d'identité : passeport, carte nationale d'identité ou titre de séjour. **3. Acceptation du Certificat** L'acception du certificat par le Signataire est tacite dès lors qu'il clique sur le bouton « Signer ». À tout moment, le Signataire peut refuser la création du certificat en interrompant la Transaction de signature ou en cliquant sur le bouton « Refuser ».
Modalités de renouvellement	Les certificats ne sont pas renouvelables.
Modalités de révocation	Les certificats ne sont pas révocables.
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 certificats émis sont conservés par l'ACI pendant une durée de 7 ans.
Obligations des Signataires	Les Signataires ont pour obligation de : • Vérifier que les informations les concernant, fournies par le Souscripteur et 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 autre que la signature des documents soumis par le Souscripteur dans le cadre de la Transaction de signature pour laquelle la clé privée est spécifiquement créée ; • Informer l'ACI de toute modification concernant les informations contenues dans leur certificat ; • Protéger leurs moyens d'authentification, le cas échéant ; • Consentir à la conservation par l'AE, et par l'éventuelle AED, des informations des dossiers d'enregistrement et des certificats, ainsi qu'à leur éventuel transfert à un tiers dans les mêmes conditions que celles exigées par la PC/DPC dans le cas où l'AC mettrait fin à ses services. Dans le cas de certificats de signature avancée, les Signataires doivent également accepter les présentes CGU.
Obligations des Souscripteurs	Les Souscripteurs ont pour obligation de : • Fournir à l'AE des informations exactes et à jour lors de la phase d'enregistrement des Signataires (voir chapitres 3.2.3 et 7.1 de la PC/DPC) ; • Informer l'AE de toute modification des informations contenues dans les certificats ; • Consentir à la conservation par l'AE, et par l'éventuelle AED, des informations des dossiers d'enregistrement et des certificats, ainsi qu'à leur éventuel transfert à un tiers dans les mêmes conditions que celles exigées par la PC/DPC dans le cas où l'AC mettrait fin à ses services ;

	• S'engager à recueillir, au préalable, le consentement des Signataires pour le transfert de leurs données à caractère personnel à l'AE, ainsi que pour le traitement par cette dernière de ces données selon les finalités suivantes :
	  ○ La prestation de délivrance des certificats de signature électronique, conformément aux présentes CGU ;
	  ○ La conservation des éléments de preuve associés.

Obligations de vérification des certificats par les Utilisateurs de certificat	Les Utilisateurs de certificat devraient : • Vérifier et respecter l'usage pour lequel un certificat a été émis ; • Vérifier, pour chaque certificat de la chaîne de certification, la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité et statut de révocation). Ces vérifications peuvent être réalisées de manière automatique avec des outils standards tels que Adobe Acrobat Reader ou avec des bibliothèques Open Source comme OpenSSL ou BouncyCastle. Le statut de révocation du certificat d'ACI peut être vérifié à partir de la liste des autorités de certification révoqués (CARL) téléchargeable à partir de l'URL indiquée dans l'extension `CRL Distribution Point` du certificat de l'ACI. En cas de révocation du certificat de l'ACI, par exemple à la suite d'une compromission de sa clé privée, l'information de révocation sera publiée dans cette CARL. Le certificat de l'AC racine est un certificat auto-signé qui peut être vérifié en comparant son empreinte de hachage avec celle affichée sur le site de publication : https://pki.safy.ma/g2
Limites de responsabilité	L'ACI ne saurait être tenu responsable de toute utilisation non autorisée, frauduleuse ou non conforme des données d'authentification, des certificats, des listes de révocation, ni de tout équipement ou logiciel mis à disposition dans le cadre du service. L'ACI décline également toute responsabilité en cas de dommage résultant d'erreurs, d'omissions ou d'inexactitudes affectant les informations contenues dans les certificats, lorsque celles-ci

	résultent directement des informations erronées fournies par le Souscripteur, le Signataire ou un tiers agissant pour son compte. En tout état de cause, et dans la stricte limite permise par la loi applicable, la responsabilité de l'ACI 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 Certificat et la Déclaration des Pratiques de Certification (PC/DPC) de l'ACI est accessible sur le site de publication de l'AC : 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. L'ACI 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 l'ACI sont traitées exclusivement pour permettre la création du certificat de signature électronique et la conservation des éléments 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 l'ACI agit en qualité de sous-traitant, sur instruction du Souscripteur, afin d'exécuter techniquement la délivrance du certificat et la conservation des éléments de preuve associés.
Audits et références applicables	L'ACI est auditée 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'Informations (DGSSI) sur son site Internet, relatif aux services de confiance non qualifiés et aux prestataires fournissant ces services, pour la création des certificats de signatures simples et avancées. Les certificats de signature avancée (1.3.6.1.4.1.60428.1.1.2.1.2) sont conformes à la norme ETSI EN 319 411-1 pour le niveau LCP.