SAFY TRUST SERVICES

Politique de Signature et Déclaration des Pratiques de Signature du Service de Création de Signature de SAFY

Version : 1.0
Date d'entrée en vigueur : 26/01/2026
Classification : Publique

Historique des révisions

Version	Date	Auteur(s)	Commentaires
1.0	12/01/2026	JPA	Version initiale

Table des matières

1 Introduction

1.1 Présentation générale

SAFY.io, ci-après dénommé « SAFY », est une société marocaine, spécialisée dans le domaine de la confiance numérique, qui est à la fois éditeur de logiciels et Prestataire de Services de Confiance (PSCo).

SAFY, en tant que PSCo, fournit pour ses besoins propres ou pour ceux de ses clients, un ou plusieurs Services de Confiance, conformément à la [Loi 43-20] relative aux services de confiance pour les transactions électroniques et au [Décret n° 2-22-687] pris pour l'application de cette loi.

Le présent document définit la Politique de Signature et la Déclaration des Pratiques de Signature (PS/DPS) du Service de Création de Signature (SCS) de SAFY pour la création de 2 types de signatures électroniques :

- Les signatures électroniques simples[1], appelées **signatures simples** dans la suite du document ;
- Les signatures électroniques avancées[2], appelées **signatures avancées** dans la suite du document.

Chacune de ces signatures électroniques garantie :

- L'intégrité des documents signés (qui pourra être contrôlée à tout moment à travers le processus de vérification et de confirmation de la validité de la signature électronique) ;
- L'identification du Signataire (à travers le certificat électronique qui lui est délivré, qui contient son nom et son prénom et qui est intégré dans la signature électronique) ;
- Le consentement du Signataire à signer les documents qui lui sont présentés.

L'objet de la présente PS/DPS est de préciser le contexte dans lequel les signatures sont créées, conservées et mises à disposition pour vérification, ainsi que les rôles et obligations des différentes entités qui interviennent dans ces processus.

Les signatures sont produites par le SCS, au sein de Transactions de signature, pour le compte de Signataires, à qui sont délivrés des certificats, par l'Autorité de Certification (AC) de SAFY appelée « Safy Intermediate CA G2 », selon les OID suivants :

- **1.3.6.1.4.1.60428.1.1.2.1.1** pour les certificats de **signature simple** ;
- **1.3.6.1.4.1.60428.1.1.2.1.2** pour les certificats de **signature avancée**.

[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].

Le processus de gestion de ces certificats est spécifié dans la Politique de Certification et Déclaration des Pratiques de Certification (PC/DPC) de l'AC, accessible à l'adresse suivante : https://pki.safy.ma/g2

1.2 Identification du document

La présente PS/DPS est identifiée par son nom et son numéro de version.

Le tableau ci-dessous liste les différents OID couverts par la présente PS/DPS.

OID	Description
1.3.6.1.4.1.60428.1.3.2.1	**Signatures simples** créées par le SCS.
1.3.6.1.4.1.60428.1.3.2.2	**Signatures avancées** créées par le SCS à la suite d'une authentification du Signataire avec l'application eID de la DGSN.
1.3.6.1.4.1.60428.1.3.2.3	**Signatures avancées** créées par le SCS à la suite d'une vérification de l'identité du Signataire par une Autorité d'Enregistrement Déléguée (AED).

Tableau 1 - Liste des OID couverts par la présente PS/DPS

1.3 Entités intervenant dans la PS/DPS

Le schéma ci-dessous illustre les différentes entités qui interviennent la présente PS/DPS.

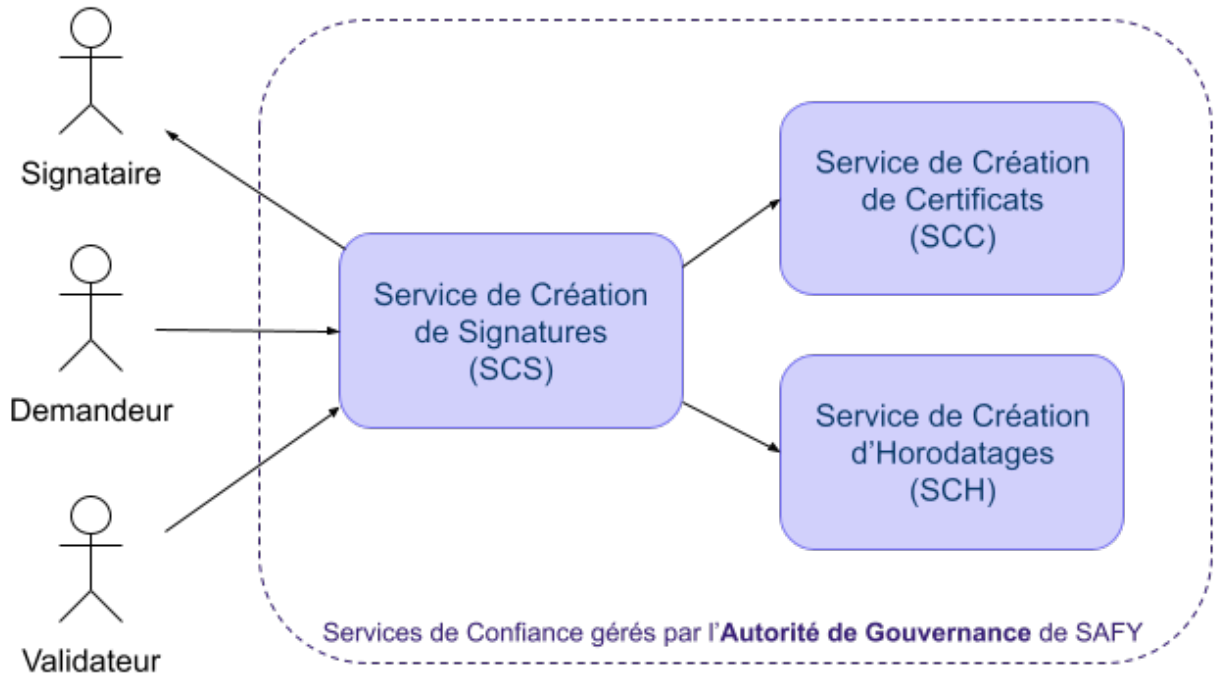

Figure 1 - Entités intervenant dans la PS/DPS

Le Service de Création de Signatures (SCS), le Service de Création de Certificats (SCC) et le Service de Création d'Horodatages (SCH) sont opérés et placés sous le contrôle et la responsabilité de l'Autorité de Gouvernance des Services de Confiance de SAFY. Ces Services s'appuient sur une Infrastructure de Gestion des Clés (IGC) commune qui est conforme aux exigences de la norme [ETSI EN 319 401].

1.3.1 Autorité de Gouvernance (AG)

L'AG est un organe de gouvernance, au sein de SAFY, qui est responsable, avec pouvoir décisionnaire, des Services de Confiance fournit par SAFY dans le cadre de son activité de PSCo.

L'AG définit les politiques des Services de Confiance et vérifie la conformité des pratiques associées. A ce titre, l'AG est responsable du SCS et de la présente PS/DPS.

1.3.1.1 Responsable de l'AG

L'AG est pilotée par le Responsable de l'AG, qui est une personne physique dûment nommée par un représentant légal ou habilité de SAFY.

1.3.1.2 Responsable des Services de Confiance

Le Responsable des Services de Confiance est nommé par le Responsable de l'AG. A noter que le Responsable de l'AG et le Responsable des Services de Confiance peuvent être une seule et même personne physique.

Le Responsable des Services de Confiance est notamment en charge de :

- Rédiger et maintenir les politiques des Services de Confiance ainsi que de les faire approuver par l'AG ;
- Veiller au respect de la conformité des pratiques et des procédures avec les politiques associées ;
- Gérer les certifications et les qualifications des Services de Confiance ;
- Gérer les fournisseurs et sous-traitant intervenant directement, ou indirectement, dans la fourniture des Services de Confiance.

1.3.2 Service de Création de Certificats (SCC)

Le SCC met en œuvre l'Autorité de Certification « Safy Intermediate CA G2 » (AC), rattachée à l'autorité de certification racine « Safy Root CA 2 » et placée sous la responsabilité et le contrôle de l'AG, à travers le Responsable des Services de Confiance.

L'AC est responsable de l'émission des certificats de signature simple et avancée.

L'AC est également responsable de la création, de l'émission, de la révocation et de la publication du statut de révocation des certificats suivants :

- Les certificats de cachet Safy (selon l'OID **1.3.6.1.4.1.60428.1.1.2.1.3**), qui sont utilisés par le SCS, dans le cadre de la présente PS/DPS, pour le cachetage électronique des fichiers de preuve ;
- Les certificats d'horodatage Safy (selon l'OID **1.3.6.1.4.1.60428.1.1.2.1.4**), qui sont utilisés par le SCS, dans le cadre de la présente PS/DPS, pour l'horodatage des signatures et des cachets créés par le SCS.

1.3.3 Service de Création d'Horodatages (SCH)

Le SCH met en œuvre l'Autorité d'Horodatage « Safy Time Stamping Authority G2 » (AH), placée sous la responsabilité et le contrôle de l'AG, à travers le Responsable des Services de Confiance.

L'AH est responsable de l'émission de jetons d'horodatage conformément à l'OID **1.3.6.1.4.1.60428.1.2.2.1** de sa Politique d'Horodatage (PH).

Lorsque le SCS crée une signature ou un cachet électronique, il transmet l'empreinte de hachage de ladite signature ou dudit cachet à l'AH, qui génère un jeton d'horodatage et le retourne au SCS. Ce dernier finalise la création de la signature ou du cachet en ajoutant le jeton d'horodatage dans une propriété non-signée de la signature ou du cachet qu'il vient de créer.

1.3.4 Service de Création de Signatures (SCS)

Le SCS, placé sous la responsabilité et le contrôle de l'AG, à travers le Responsable des Services de Confiance, est chargé de créer les signatures électroniques des Signataires, sur les documents électroniques soumis au SCS par les Demandeurs.

Vis-à-vis de l'AC, le SCS endosse le rôle d'Autorité d'Enregistrement (AE) pour l'émission des certificats de signature, en collectant les informations d'identification des Signataires, en procédant, le cas échant, à leur authentification, et en transmettant ces informations à l'AC pour qu'elle génère leur certificat de signature.

Le SCS, à travers son rôle d'AE, peut déléguer la vérification de l'identité du Signataire à une Autorité d'Enregistrement Déléguée (AED) avec laquelle l'AC aura établi une relation contractuelle.

Les différents types de signature électronique créés par le SCS, ainsi que les OID associés, sont spécifiés dans le tableau du chapitre 1.2.

1.3.5 Demandeur (ou Souscripteur)

Le Demandeur est une personne physique ou morale qui souhaite faire signer un ou plusieurs documents à un Signataire.

Pour cela, le Demandeur utilise le portail web ou l'API du SCS pour initier une Transaction de signature, en spécifiant notamment les documents à signer, les informations du Signataire devant signer ces documents, le mode d'invitation du Signataire et, le cas échéant, le mode d'authentification du Signataire.

Le Demandeur est également appelé Souscripteur, car il doit souscrire au Service de Création de Signature pour pouvoir l'utiliser.

1.3.6 Signataire

Le Signataire est une personne physique à qui le SCS fait signer, au sein d'une Transaction de signature, les documents soumis par le Demandeur.

Le Signataire est identifié dans le certificat de signature qui lui est délivré par l'AC.

1.3.7 Validateur

Le Validateur est une personne physique ou morale qui vérifie et contrôle la validité d'une signature électronique produite par le SCS.

1.4 Gestion de la PS/DPS

1.4.1 Entité gérant la PS/DPS

La présente PS/DPS est élaborée, mise à jour et publiée par l'AG.

1.4.2 Point de contact de la PS/DPS

Toute demande relative à la présente PS/DPS doit se faire, de préférence, via l'envoi d'un email à contact-pki@safy.ma, ou sinon, à l'adresse postale suivante :

A l'attention du Responsable des Services de Confiance SAFY,
LES PORTES DE MARRAKECH, TR21A-54
40140 MARRAKECH - MAROC

1.4.3 Entité déterminant la conformité des pratiques avec la PS/DPS

La conformité des pratiques avec la PS/DPS est déterminée par l'AG.

1.4.4 Procédure d'approbation de la conformité des pratiques avec la PS/DPS

L'AG dispose d'une procédure d'approbation de la conformité des pratiques avec la PS/DPS.

1.5 Définitions et acronymes

1.5.1 Acronymes

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
API	Application Programming Interface
CAdES	CMS Advanced Electronic Signature
CRL	Certificate Revocation List
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DPS	Déclaration des Pratiques de Signature
ETSI	European Telecommunications Standards Institute
OID	Object Identifier
OTP	One Time Password
PAdES	PDF Advanced Electronic Signature

PC	Politique de Certification
PDF	Portable Document Format
PH	Politique d'Horodatage
PS	Politique de Signature
PSCo	Prestataire de Service de Confiance
RSA	Rivest Shamir Adelman
SCC	Service de Création de Certificats
SCH	Service de Création d'Horodatages
SCS	Service de Création de Signatures
UH	Unité d'Horodatage

1.5.2 Définitions

Autorité de Certification (AC)

Au sein d'un PSCo, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCo, l'application d'au moins une Politique de Certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette Politique de Certification.

Dans le cadre de la présente PS, le terme AC sera utilisé pour désigner l'Autorité de Certification « Safy Intermediate CA G2 » qui délivre les certificats de signature.

Autorité d'Enregistrement (AE)

Composante de l'AC chargée de traiter les demandes de création et, le cas échéant, de révocation de certificats en procédant aux vérifications adéquates conformément à la PC de l'AC.

Autorité d'Horodatage (AH)

Au sein d'un PSCo, une Autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSCo, l'application d'au moins une Politique d'Horodatage et est identifiée comme telle, dans les jetons d'horodatage qu'elle délivre au titre de cette Politique d'Horodatage.

Dans le cadre de la présente PS, le terme AH sera utilisé pour désigner l'Autorité d'Horodatage de SAFY (cf. chapitre 1.3.3).

Certificat

Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Dossier de preuve

Un Dossier de preuve est un fichier ZIP associé à un Workflow, créé à la demande par le SCS, et qui contient les Fichiers de preuve relatifs aux Signataires de ce Workflow, ainsi que les documents de politiques et de CGU.

Voir chapitre 5.

Fichier de preuve

Document PDF établi par le SCS à la fin de la Transaction de signature, retraçant le processus de signature des documents par un Signataire et les éléments de traçabilité associés.

Voir chapitre 5.

Infrastructure de Gestions de Clés (IGC)

Infrastructure constituée par l'ensemble de moyens techniques, humains, documentaires et contractuels pour la mise en œuvre de mécanismes de cryptographie asymétrique utilisés par un PSCo pour fournir un ou plusieurs Services de Confiance.

Dans le cadre de la présente PS, le terme IGC sera utilisé pour désigner l'IGC de SAFY sur laquelle s'appuient le SCS, le SCC et le SCH.

Politique de Certification (PC)

Ensemble de règles, identifié par un identifiant unique (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité 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 porteurs et les utilisateurs de certificats.

Politique de Signature (PS)

Ensemble de règles, identifié par un identifiant unique (OID), définissant les exigences auxquelles un PSCo doit se conformer pour la création, la validation et la conservation de signatures électroniques. Ces règles indiquent l'applicabilité de la signature à une communauté particulière et/ou à une catégorie de transactions répondant à des exigences de sécurité communes. Une PS peut également inclure, si nécessaire, les obligations et responsabilités des parties impliquées, notamment les signataires et les entités validatrices.

Prestataire de Services de Confiance (PSCo)

Un PSCo est une personne morale qui fournit un ou plusieurs Services de Confiance.

Service de Confiance

Les services de confiance, tels que définis dans la [Loi 43-20], consistent en :

- La création de signatures électroniques, de cachets électroniques, d'horodatages électroniques ou des services d'envoi recommandé électronique ;
- La création des certificats relatifs aux signatures électroniques, aux cachets électroniques, à l'horodatage électronique ou à l'authentification des sites internet ;
- La validation de signatures électroniques ou de cachets électroniques ;
- La conservation de signatures électroniques, de cachets électroniques ou de certificats relatifs à ces services.

Transaction de signature

Une Transaction de signature est une opération, gérée par le SCS, au cours de laquelle un Signataire doit notamment, prendre connaissance des documents électroniques à signer et marquer son consentement explicite à les signer, afin de déclencher la création par le SCS des signatures électroniques sur les documents.

Workflow

Un Workflow contient un ou plusieurs documents, devant être signés par un ou plusieurs Signataires.

2 Responsabilité concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

L'AG est chargée de la mise à disposition aux parties concernées, ainsi qu'au public, des informations devant être publiées.

2.2 Informations devant être publiées

La dernière version en vigueur de la présente PS/DPS ainsi que les versions antérieures sont accessibles à l'adresse suivante : https://pki.safy.ma/g2

2.3 Délais et fréquences de publication

La PS/DPS est publiée après son approbation par l'AG à la suite de sa mise à jour, pour prendre en compte de nouveaux besoins, des évolutions techniques ou organisationnelles, ou des besoins de mise en conformité avec le cadre juridique et technique.

La PS/DPS est publiée avant la création des signatures électroniques s'appuyant sur cette PS/DPS.

L'AG garantit l'intégrité des informations publiées et leur disponibilité 24h/24 et 7j/7 selon un taux de disponibilité de 99.5% sur un mois.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sont libres d'accès en lecture.

L'accès en modification au système de publication des informations est strictement limité aux fonctions internes habilitées du SCS et requiert une authentification forte.

3 Obligations des acteurs

3.1 SAFY

SAFY, en tant que PSCo, et dans le cadre de cette PS/DPS, a pour obligation, pour chaque Transaction de signature :

- De garantir le principe du WYSIWYS (What You See Is What You Sign), en faisant en sorte que les documents soumis par le Demandeur soient ceux qui seront présentés au Signataire et qui seront signés ;
- De délivrer au Signataire, via l'AC, un certificat de signature électronique simple ou avancé en fonction du type de signature souhaitée par le Demandeur ;
- De créer la clé privée du Signataire après qu'il ait explicitement donné son consentement à signer ;
- De protéger la clé privée du Signataire de telle sorte qu'elle ne puisse être utilisée que pour signer les documents de la Transaction de Signature pour laquelle elle est dédiée et que personne d'autre ne puisse en aucun cas l'utiliser ;
- De détruire la clé privée une fois les documents signés ou dans le cas où la Transaction de signature est interrompue ;
- De créer le Fichier de preuve conformément au chapitre 5.3 ;
- De conserver le Dossier de preuve, et le cas échéant les documents signés, conformément au chapitre 5.4 ;
- De mettre à disposition le Dossier de preuve, et le cas échéant les documents signés, aux personnes autorisées qui en ferait la demande conformément au chapitre 5.5.

SAFY décline toute responsabilité quant au contenu des documents soumis au SCS par le Demandeur, ainsi qu'en cas de mauvaise utilisation du SCS par le Signataire.

3.2 Demandeur

Le Demandeur s'engage à respecter les obligations suivantes :

- Transmettre au SCS l'ensemble des informations requises pour la réalisation d'une Transaction de signature (cf. chapitre 1.3.5), en garantissant leur exactitude, leur complétude et leur licéité ;
- Être seul responsable du contenu des documents transmis au SCS pour signature, ainsi que de sa légitimité à en solliciter la signature par le Signataire ;
- Lorsqu'il agit en qualité d'Autorité d'Enregistrement Déléguée, procéder à la vérification préalable de l'identité du Signataire conformément à la Politique d'Enregistrement Déléguée approuvée par l'AC ;
- Informer sans délai SAFY de tout incident de sécurité, suspicion d'incident ou anomalie susceptible d'affecter l'identité du Signataire, l'intégrité des documents ou le bon déroulement de la Transaction de signature.

3.3 Signataire

Le Signataire a pour obligation, au sein d'une Transaction de signature :

- De prendre connaissance des documents soumis à signature ;
- De fournir des informations exactes et à jour permettant son identification dans le cadre de la Transaction de signature ;
- De respecter les obligations relatives au certificat de signature qui lui est délivré pour ladite Transaction, telles que définies dans la Politique de Certification de l'AC ;
- De préserver la confidentialité des moyens d'authentification et d'accès utilisés dans le cadre de la Transaction de signature.

3.4 Validateur

La Validateur a pour obligation de vérifier et contrôler la validité des signatures produites par le SCS conformément à la présente PS/DPS, en appliquant le processus décrit dans le chapitre 6.

4 Création des signatures

4.1 Processus de signature

Le Processus de signature se déroule de la façon suivante :

1. **Initialisation de la Transaction de signature** : Le Demandeur, qui peut être une personne physique utilisant le portail web du SCS ou une application cliente autorisée appelant l'API du SCS, transmet à ce dernier les informations permettant de constituer une Transaction de signature, à savoir :
    - La liste des documents à faire signer au Signataire ;

- Les informations d'identification du Signataire, dont ses nom, prénom et optionnellement adresse email et / ou numéro de téléphone portable ;
- L'identifiant (OID) du type de signature à créer (cf. tableau du chapitre 1.2) ;
- Le mode d'invitation du Signataire (aucun, email, SMS, WhatsApp, etc.) ;
- Le mode d'authentification du Signataire (aucun, OTP email, OTP SMS, fournisseur d'identité tier, etc.) ;
- L'identifiant de la Politique d'Enregistrement appliquée par l'AED pour vérifier l'identité du Signataire, dans le cas où l'application cliente appartient à une AED ;
- Un paramètre indiquant si le Signataire devra visualiser obligatoirement toutes les pages des documents à signer ;
- Des informations diverses et optionnelles sur le paramétrage de la Transaction de signature.

2. **Connexion à la Transaction de signature** : en fonction du mode d'invitation spécifié par le Demandeur lors de l'initialisation de la Transaction de signature, il y a 2 cas possibles :
   a. Si aucun mode d'invitation n'a été spécifié, alors l'application cliente devra récupérer l'URL sécurisée d'accès à la Transaction de signature via l'API du SCS et devra rediriger le Signataire sur cette URL ;
   b. Sinon, le SCS enverra au Signature, l'URL sécurisée d'accès à la Transaction de signature, selon le mode d'invitation spécifié (email, SMS, WhatsApp, etc.).
3. **Exécution de la Transaction de signature** : une fois connecté à la page web de la Transaction de signature (gérée par SCS), le Signataire doit accomplir les actions suivantes :
   - Prendre connaissance des documents à signer qui lui sont présentés dans un visualiseur web de PDF, mis à disposition par le SCS ; en fonction du paramétrage spécifié par le Demandeur, le Signataire pourra être obligé, ou pas, de visualiser toutes les pages des documents (cette information sera tracée dans le fichier de preuve de la Transaction de signature) ;
   - Approuver les CGU du SCS, le cas échéant ;
   - Être authentifié par le SCS avec le mode d'authentification spécifié par le Demandeur ;
   - Prendre connaissance des informations qui seront insérées dans son certificat et confirmer leur exactitude ;
   - Cliquer sur le bouton « Signer ».
4. **Finalisation de la Transaction de signature** :
   - Le SCS affiche un message demandant au Signataire de patienter pendant le processus de signature ;

- Le SCS génère la clé privée du Signataire de manière sécurisée ;
- Le SCS transmet la clé publique du Signataire à l'AC pour qu'elle émette le certificat du Signataire (cf. chapitre 4.5) ;
- Le SCS calcul l'empreinte de hachage des documents à signer puis l'empreinte de hachage des données à signer (cf. chapitre 4.2) ;
- Le SCS chiffre, avec la clé privée du Signataire, l'empreinte de hachage des données correspondant aux différents documents et produit les signatures électroniques PAdES-B-LT correspondantes (cf. chapitre 4.3) ;
- Le SCS détruit la clé privée du Signataire ;
- Le SCS génère le fichier de preuve, le cachète pour garantir son intégrité et son origine (cf. chapitre 5.3) et le conserve de manière sécurisée (cf. chapitre 5.4) ;
- Si une erreur a lieu pendant ce processus, alors le SCS affiche un message d'erreur au Signataire, sinon il lui indique que la signature s'est déroulée avec succès ;
- Si aucun mode d'invitation n'a été spécifié par l'application cliente, alors le SCS peut rediriger le Signataire vers une URL spécifiée par l'application cliente afin que le Signataire puisse continuer son parcours sur l'application cliente ;
- L'application cliente peut, si elle le souhaite, récupérer les documents signés ;
- Le SCS peut, en fonction du paramétrage, envoyer le lien de téléchargement des documents signés au Signataire.

Dans le cas d'une signature avancée (OID 1.3.6.1.4.1.60428.1.3.2.2 ou 1.3.6.1.4.1.60428.1.3.2.3), les exigences suivantes s'appliquent :

- Le Signataire doit obligatoirement accepter les Conditions Générales d'Utilisation (CGU) du SCS avant de procéder à la signature ;
- Le Signataire doit obligatoirement visualiser l'intégralité des pages de chaque document PDF avant de pouvoir signer.
- Dans le cas d'une signature avancée DGSN (OID 1.3.6.1.4.1.60428.1.3.2.2), l'authentification du Signataire repose obligatoirement sur le service « Identité Numérique » de la DGSN et met en œuvre deux facteurs d'authentification distincts :
  - soit la carte nationale d'identité électronique ou le titre de séjour électronique ;
  - soit le code PIN associé ou un mécanisme de reconnaissance faciale.
- Dans le cas d'une signature avancée avec enregistrement délégué (AED) (OID 1.3.6.1.4.1.60428.1.3.2.3), le Demandeur est responsable de la vérification de l'identité du Signataire sur la base d'un document d'identité officiel en cours de validité (passeport, carte nationale d'identité ou titre de séjour). Le Demandeur transmet ensuite au SCS,

par un canal sécurisé, le rapport de vérification d'identité afin qu'il soit intégré au Fichier de preuve.

- L'OID correspondant au type de signature électronique produite par le SCS est systématiquement inclus dans le Fichier de preuve.

4.2 Données signées

Les données signées par le Signataire, au sein d'une Transaction de signature, sont les documents PDF soumis par le Demandeur.

Ces documents peuvent déjà contenir des signatures électroniques. Ils peuvent aussi être signés ultérieurement par d'autres Signataires.

Techniquement, la signature est le résultat du chiffrement de l'empreinte de hachage des données à signer, par la clé privée du Signataire. Ce chiffrement est réalisé par le SCS en utilisant l'algorithme de signature décrit dans le chapitre 4.4. L'empreinte de hachage des données à signer est quant à elle calculée à partir d'un ensemble de données constitué par l'empreinte de hachage du document PDF à signer et d'un ensemble de propriétés signées dont l'empreinte de hachage du certificat du Signataire (`signing-certificate-v2`) et la date de signature (`signing-time`).

4.3 Type et format de signature

Une signature est créée sur chaque document PDF devant être signé au sein de la Transaction de signature. Les signatures sont des signatures au format PAdES pour le niveau B-LT tel que spécifié dans la norme [ETSI EN 319 142-1].

Techniquement, une fois la signature PAdES-B-B générée par le SCS, ce dernier calcul l'empreinte de hachage de la valeur de la signature et l'envoie au SCH qui lui retourne en réponse un jeton d'horodatage conforme à la norme [RFC 3161]. Le SCS intègre ce jeton d'horodatage dans une propriété non-signée de la signature pour produire une signature PAdES-B-T.

Ensuite, le SCS intègre la dernière version de la CARL (qui prouve que le certificat de l'AC n'était pas révoqué au moment où elle a délivré le certificat au Signataire) dans une propriété non-signée de la signature pour produire la version finale PAdES-B-LT de la signature.

4.4 Algorithme de signature

Les algorithmes de hachage sont SHA256 ou supérieur.

Les algorithmes de signature sont RSASSA-PSS tel que spécifié dans la [RFC 8017] ou ECDSA.

Les clés RSA ont une taille de 3072 bits ou supérieur et les clés ECDSA utilisent l'algorithme P-256 (secp256r1) ou supérieur.

4.5 Certificat de signature

Le certificat de signature contient les informations d'identification du Signataire. Il s'agit d'un certificat de très courte durée (non-révocable), délivré « à la volée » par l'AC selon les OID suivants :

- 1.3.6.1.4.1.60428.1.1.2.1.1 pour les certificats de signature simple ;
- 1.3.6.1.4.1.60428.1.1.2.1.2 pour les certificats de signature avancée.

L'OID est contenu dans l'extension `Certificate Policies` du certificat.

5 Dossier de preuve et documents signés

5.1 Objectif et portée du Dossier de preuve

Le Dossier de preuve a pour objectif de compléter les éléments de preuve intégrés dans les documents signés et dans les signatures électroniques PAdES qu'ils contiennent.

En effet, les signatures électroniques et les documents associés ne permettent pas, à eux seuls, de fournir l'ensemble des informations pouvant être requises par un Validateur afin d'établir la validité d'une signature électronique, notamment dans le cadre d'une vérification ultérieure ou d'un contrôle à des fins probatoires.

Le Dossier de preuve regroupe, conserve et met à disposition les éléments complémentaires nécessaires à l'évaluation de la validité des signatures électroniques, dans les conditions définies par la présente Politique de Signature.

La portée du Dossier de preuve couvre l'ensemble des signatures électroniques générées par le SCS dans le cadre d'un même Workflow. À ce titre, un même Dossier de preuve peut contenir des éléments relatifs à plusieurs signatures, portant sur un même document ou sur un ensemble de documents traités dans une transaction unique.

La figure ci-dessous illustre, à titre d'exemple, le cas de plusieurs documents signés par plusieurs signataires dans le cadre d'un même Workflow, et associés à un Dossier de preuve unique.

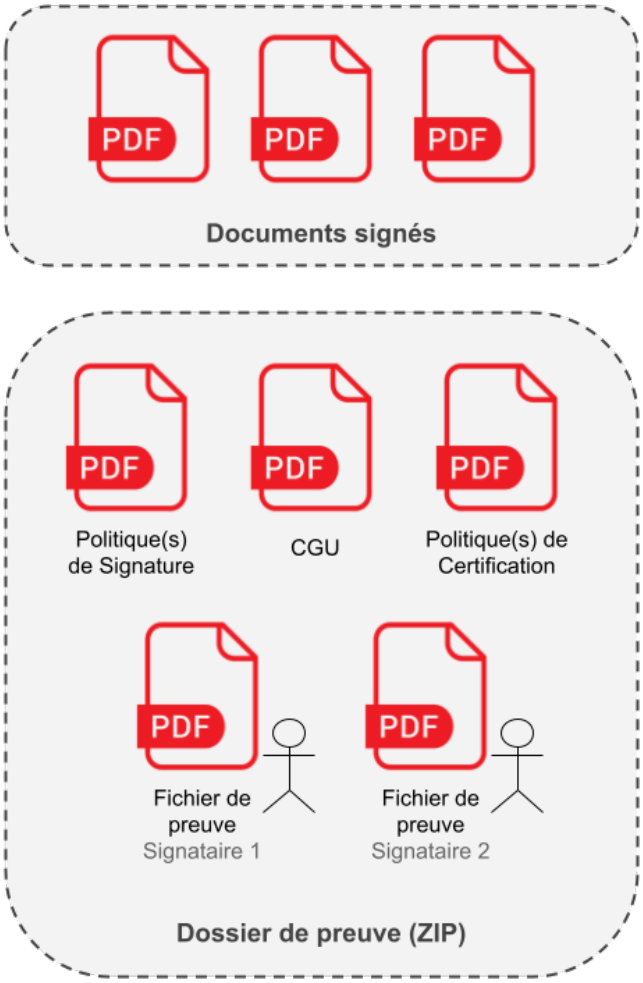

Figure 2 - Exemple de 3 documents signés par 2 Signataires

5.2 Format et contenu d'un Dossier de preuve

Le Dossier de preuve est constitué sous la forme d'une archive au format ZIP, générée à la demande par le SCS. Il regroupe les éléments relatifs à un Workflow donné, nécessaires à l'analyse et à la validation des signatures électroniques qui y sont associées.

Le Dossier de preuve contient notamment les éléments suivants :

- Les fichiers de preuve au format PDF correspondant aux transactions de signature réalisées par les différents Signataires du Workflow ;
- La ou les Politiques de Signature applicables aux transactions de signature concernées ;
- La ou les Politiques de Certification applicables aux certificats utilisés par les Signataires ;

- Les Conditions Générales d'Utilisation approuvées par les Signataires au moment de la signature.

Le SCS garantit que les éléments inclus dans le Dossier de preuve correspondent aux versions en vigueur au moment des transactions de signature concernées.

5.3 Format et contenu d'un Fichier de preuve

Le Fichier de preuve est un document au format PDF, généré par le SCS à l'issue de chaque Transaction de signature finalisée.

Il contient les éléments de traçabilité relatifs à cette Transaction de signature et est cacheté et horodaté électroniquement par le SCS au format PAdES-B-LT, de manière à garantir son intégrité, son origine et date de création.

Le Fichier de preuve contient au minimum les informations suivantes :

Informations relatives à l'environnement et aux composants du SCS

- L'identifiant et le nom de l'organisation (tenant) ;
- L'URL et la version du composant Trusted Service du SCS qui a piloté la Transaction de signature et produit le Fichier de preuve ;
- L'URL et la version du composant Document Service du SCS qui a calculé l'empreinte de hachage des données à signer et intégrer les signatures électroniques produites par le Trusted Service dans les documents PDF ;

Informations relatives au Workflow

- L'identifiant et le nom du Workflow ;
- Lorsque le Demandeur est une personne physique ayant utilisé le portail web du SCS :
    - L'identifiant, le nom et l'adresse électronique du Demandeur, créateur du Workflow ;
- Lorsque le Demandeur est une application cliente ayant utilisé l'API du SCS :
    - L'identifiant et le nom du jeton d'API utilisé pour créer le Workflow ;
- L'identifiant et le nom de l'espace dans lequel se trouvait le Workflow au moment de la création du Fichier de preuve ;
- La date de lancement du Workflow.

Informations relatives au Signataire

- L'identifiant, le nom et le prénom du Signataire ;
- Le mode d'invitation ;
- Le mode d'authentification ;
- Les informations relatives au fournisseur d'identité utilisé (par exemple eID DGSN) et, le cas échéant, le rapport ou l'attestation de vérification produit par celui-ci ;
- L'adresse électronique du Signataire lorsque le mode d'invitation ou d'authentification repose sur l'email ;
- Le numéro de téléphone mobile du Signataire lorsque le mode d'invitation ou d'authentification repose sur le téléphone mobile (ex : OTP SMS) ;
- L'indication précisant si le Signataire a été tenu de visualiser l'ensemble des pages des documents avant signature ;
- La date d'envoi de l'invitation à signer, lorsque le mode d'invitation est applicable ;
- L'adresse IP utilisée par le Signataire ;
- Les informations relatives au navigateur Internet utilisé ;
- La date de finalisation de la signature des documents ;
- L'OID et l'empreinte de hachage de la Politique de Signature utilisée ;
- Dans le cas où une Autorité d'Enregistrement Déléguée (AED) intervient :
    - L'OID et l'empreinte de hachage de la Politique d'Enregistrement Déléguée utilisée ;
    - Le rapport de vérification produit par l'AED et sa date de transmission au SCS ;
    - L'adresse IP de l'AED ayant transmis le rapport ;
- La preuve d'acceptation des Conditions Générales d'Utilisation par le Signataire, incluant notamment l'empreinte de hachage du document correspondant ;
- La date de destruction de la clé privée du Signataire.

Informations relatives aux documents signés

Pour chaque document signé :

- L'identifiant et le nom du document ;
- La taille et la valeur de l'empreinte de hachage du document avant signature ;
- La taille et la valeur de l'empreinte de hachage du document après signature ;
- La valeur hexadécimale de la signature numérique correspondant à la valeur stockée dans l'attribut `signedData.signerInfos[0].signature` de la signature CAdES contenue dans le document PDF, conformément à la norme [ETSI EN 319 142-1] ;

- L'adresse IP du Demandeur ayant déposé le document dans le Workflow.

Note 1 : le champ `subject` du certificat du Signataire contient, dans l'attribut `serialNumber`, une chaîne de caractères constituée de l'identifiant du Workflow, suivi de deux points (:), puis de l'identifiant du Signataire, suivi de deux points (:) et de l'identifiant de la session de signature.

Note 2 : l'identifiant du champ de signature (visible ou invisible) contenant la signature électronique PAdES dans le document PDF signé correspond à l'identifiant du Signataire.

Note 3 : les valeurs des signatures numériques des documents d'un Workflow, contenues dans le Fichier de preuve, peuvent être comparées avec celles présentes dans les documents PDF signés correspondants afin de vérifier leur correspondance (voir chapitre 6.3).

5.4 Conservation

5.4.1 Conservation des documents signés

Les documents signés d'un Workflow peuvent être conservés par le SCS pendant une durée définie contractuellement entre le SCS et le Demandeur ayant soumis les documents à la signature.

Le SCS conserve les documents signés dans des conditions garantissant :

- Leur intégrité ;
- Leur disponibilité ;
- Leur lisibilité dans le temps ;
- Leur confidentialité.

Les mesures mises en œuvre incluent notamment des mécanismes de sauvegarde, de contrôle d'intégrité et de protection contre l'altération ou la suppression non autorisée.

À l'expiration de la durée de conservation, les documents signés sont supprimés ou détruits de manière sécurisée, selon des procédures documentées, sauf obligation légale ou contractuelle imposant une conservation plus longue.

5.4.2 Conservation des Dossiers de preuve

Les éléments constitutifs des Dossiers de preuve sont conservés par le SCS pendant une durée minimale de sept (7) ans à compter de la date de finalisation des transactions de signature concernées. Cette durée peut être étendue lorsque des dispositions contractuelles ou réglementaires l'exigent.

Le SCS conserve les Dossiers de preuve dans des conditions garantissant :

- Leur intégrité ;
- Leur disponibilité ;
- Leur lisibilité dans le temps ;
- Leur confidentialité.

Les Dossiers de preuve font l'objet de mécanismes de protection contre la modification, la suppression non autorisée et la perte de données, incluant notamment des dispositifs d'archivage et de sauvegarde adaptés à leur valeur probatoire.

À l'expiration de la durée de conservation, les Dossiers de preuve sont détruits de manière sécurisée, selon des procédures documentées et traçables.

5.5 Mise à disposition

5.5.1 Mise à disposition des documents signés

Pendant leur période de conservation, les documents signés d'un Workflow peuvent être mis à disposition :

- Du Demandeur ;
- Des personnes explicitement autorisées par le Demandeur, le cas échéant ;
- D'une autorité administrative ou judiciaire dans le cadre d'une procédure légale ou réglementaire.

Le SCS met en œuvre des mécanismes d'authentification et de contrôle d'accès afin de garantir que seuls les utilisateurs autorisés peuvent accéder aux documents signés.

5.5.2 Mise à disposition d'un Dossier de preuve

Pendant leur période de conservation, les Dossiers de preuve d'un Workflow peuvent être mis à disposition :

- Du Demandeur ;
- Des personnes explicitement autorisées par le Demandeur, le cas échéant ;
- D'une autorité administrative ou judiciaire dans le cadre d'une procédure légale ou réglementaire.

Sous réserve de la validation de la demande par le SCS, le Dossier de preuve est fourni dans un délai maximal de deux (2) jours ouvrés.

Le SCS conserve une trace des demandes de mise à disposition et des transmissions effectuées, incluant notamment l'identité du demandeur, la date de la demande et la date de transmission.

6 Validation des signatures

6.1 Processus de validation d'une signature

La validation d'une signature consiste à appliquer le processus de validation d'une signature PAdES décrit dans la norme [ETSI EN 319 102-1], en appliquant le paramétrage suivant dans les règles de validation :

- Le certificat d'AC qui a délivré le certificat du Signataire doit être déclaré comme étant un « trust anchor » ;
- Le certificat du Signataire contenu dans la signature doit contenir dans son extension `Certificate Policies`, l'identifiant (OID) de la PC qui a été utilisée par l'AC pour le délivrer, à savoir 1.3.6.1.4.1.60428.1.1.2.1.1 pour une signature simple, et 1.3.6.1.4.1.60428.1.1.2.1.2 pour une signature avancée ;
- La signature doit être une signature PAdES de niveau B-LT ou B-LTA.

A noter que cette validation peut se faire en utilisant une application de lecture et de présentation de documents PDF qui sait valider les signatures PAdES, comme Adobe Acrobat Reader.

Si la validation réussie, cela indique que le document n'a pas été modifié depuis qu'il a été signé (preuve d'intégrité) et qu'il a été signé par le Signataire identifié dans le champ `subject` du certificat conformément à la présente PS/DPS.

6.2 Processus de validation d'un Dossier de preuve

6.2.1 Validation du cachet d'un Fichier de preuve

La validation du cachet électronique d'un Fichier de preuve consiste à appliquer le processus de validation d'une signature PAdES décrit dans la norme [ETSI EN 319 102-1], en appliquant le paramétrage suivant dans les règles de validation :

- Le certificat d'AC qui a délivré le certificat de cachet doit être déclaré comme étant un « trust anchor » ;
- Le certificat de cachet contenu dans la signature doit :
    - Contenir dans son extension « Certificate Policies », l'identifiant de la Politique de Certification qui a été utilisée par l'AC pour le délivrer, à savoir l'OID 1.3.6.1.4.1.60428.1.1.2.1.3 ;

- Identifier SAFY à travers les attributs `O` et `OI` du champ `subject` du certificat.

- La signature doit être une signature PAdES de niveau B-LT ou B-LTA.

A noter que cette validation peut se faire en utilisant une application d'affichage de PDF qui sait valider les signatures PAdES contenues dans un document PDF.

Si la validation réussie, cela indique que le Fichier de preuve n'a pas été modifié depuis sa création (preuve d'intégrité) et qu'il a été créé par le SCS de SAFY (preuve d'origine).

6.2.2 Validation du contenu d'un Fichier de preuve

Les informations contenues dans un Fichier de preuve doivent être interprétées conformément au chapitre 5.3.

Les contrôles suivants doivent être réalisées :

- Le champ `subject` du certificat du Signataire doit contenir, dans son attribut `serialNumber`, la concaténation de l'identifiant du Workflow tel que spécifié dans le Fichier de preuve, suivi de deux points (:), puis de l'identifiant du Signataire tel que spécifié dans le Fichier de preuve ;
- L'OID de la politique de signature spécifié dans le Fichier de preuve permet d'identifier le type de signature électronique (simple ou avancée).
- L'empreinte de hachage des CGU contenue dans le Dossier de preuve doit être calculée en utilisant le même algorithme que celui contenu dans le Fichier de preuve et doit produire une empreinte similaire à celle spécifiée dans le Fichier de preuve pour les CGU approuvés par le Signataire.

Les contrôles complémentaires suivants peuvent être réalisées pour chaque document signé :

- Vérifier que la valeur de la signature numérique spécifiée dans le Fichier de preuve est identique à celle contenue dans l'attribut `signedData.signerInfos[0].signature` de la signature CAdES du Signataire contenue dans le document signé (conformément à la norme [ETSI EN 319 142-1]) ;
- Recréer le document PDF avant signature, en supprimant la signature et toutes les données qui suivent, puis calculer l'empreinte de hachage du PDF résultant, et comparer cette empreinte avec celle spécifiée dans le Fichier de preuve pour le document avant signature.

6.3 Condition pour déclarer valide les éléments signés

Pour déclarer valide les éléments signés par un Signataire au sein d'une Transaction de signature, les conditions suivantes doivent être respectées :

- Chaque signature électronique de ce Signataire, contenues dans les documents signés de la Transaction de Signature (ou plus généralement du Workflow), doit être validée conformément au chapitre 6.1 ;
- Le Fichier de preuve associé à cette Transaction de signature doit être validé conformément au chapitre 6.2.

7 Autres aspects de la PS/DPS

7.1 Politique de confidentialité

7.1.1 Périmètre des informations confidentielles

Les informations suivantes, considérées comme confidentielles, ne sont accessibles qu'aux personnes habilitées :

- Le corpus documentaire interne du SCS ;
- Les clés privées des Signataires ;
- Les données d'authentification des Signataires ;
- Tous les secrets du SCS ;
- Les journaux d'évènements du SCS ;
- Les documents avant signature et après signature ;
- Les Fichiers de preuve.

7.1.2 Informations hors du périmètre des informations confidentielles

Les informations mises à disposition par le SCS sur son site de publication (cf. chapitre 2.2) sont considérées comme non confidentielles.

7.1.3 Responsabilité en termes de protection des informations confidentielles

Le SCS applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au chapitre 7.1.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. Lors d'échange de ces données, l'intégrité est garantie par un moyen adapté au type d'information.

Le SCS peut mettre à disposition les documents signés et les Fichiers de preuve à des tiers dans le cadre de procédures légales.

7.2 Protection des données à caractère personnel

7.2.1 Politique de protection des données à caractère personnel

La collecte et l'usage de données personnelles par le SCS sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire marocain, en particulier la [Loi 09-08] relative à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel.

7.2.2 Données à caractère personnel

Les informations suivantes sont considérées comme étant des informations à caractère personnel :

- Nom et prénom des Signataires ;
- Adresse email des Signataires ;
- Numéro de téléphone portable des Signataires ;
- Adresse IP des Signataires.

7.2.3 Responsabilité en termes de protection des données à caractère personnel

La présente PS/DPS ne formule pas d'exigence supplémentaire au regard de la législation et de la réglementation en vigueur sur le territoire marocain relatives à la protection des données personnelles qui convient de respecter.

7.2.4 Notification et consentement d'utilisation des données à caractère personnel

Aucune des données personnelles ne peut être collectée et traitée par le SCS, pour une utilisation autre que celle définie dans le cadre de la PS/DPS, sans le consentement exprès et préalable de la personne concernée.

7.2.5 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

La divulgation d'informations personnelles aux autorités judiciaires ou administrative est effectuée conformément à la législation et à la réglementation en vigueur sur le territoire marocain.

7.3 Dispositions juridiques

La validité de la présente PS/DPS et toute autre question ou litiges relatifs à son interprétation seront régis par la législation et de la règlementation en vigueur sur le territoire marocain.

En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution d'un contrat en lien avec la présente PS/DPS et à défaut d'accord amiable entre les parties, la compétence exclusive est attribuée aux tribunaux établis sur le territoire marocain.

8 Références documentaires

8.1 Références réglementaires

[Loi 43-20]
Loi n°43-20 relative aux services de confiance pour les transactions électroniques.
https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-03/loi%2043-20.pdf

[Décret n° 2-22-687]
Décret n° 2-22-687 du 21 rabii II 1444 (16 novembre 2022)
https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-07/Decret%202-22-687%20.pdf

[Loi 09-08]
Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2023-07/loi%2009-08.pdf

8.2 Références techniques

[ETSI EN 319 102-1]
Electronic Signatures and Trust Infrastructures (ESI);
Procedures for Creation and Validation of AdES Digital Signatures;
Part 1: Creation and Validation

[ETSI EN 319 142-1]
Electronic Signatures and Infrastructures (ESI);
PAdES digital signatures;
Part 1: Building blocks and PAdES baseline signatures

[ETSI EN 319 401]
Electronic Signatures and Infrastructures (ESI);
General Policy Requirements for Trust Service Providers

[RFC 3161]
Internet X.509 Public Key Infrastructure
Time-Stamp Protocol (TSP)

[RFC 8017]
PKCS #1: RSA Cryptography Specifications Version 2.2