SAFY TRUST SERVICES

Politique de Certification et Déclaration des Pratiques de Certification des Autorités de Certification Safy G2

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

Historique des révisions

Version	Date	Auteur(s)	Commentaires
1.0	22/01/2026	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 Certification (PC) et la Déclaration des Pratiques de Certification (DPC) des Autorités de Certification G2 de SAFY, composées par l'Autorité de Certification racine « Safy Root CA G2 » et par l'Autorité de Certification intermédiaire « Safy Intermediate CA G2 », appelées respectivement ACR et ACI dans la suite du document.

L'ACR délivre l'ACI et cette dernière délivre les types de certificats suivants :

- **Certificats signature simple** : certificats destinés aux personnes physiques invitées, par les clients du Service de Création de Signature (SCS) de SAFY, à signer électroniquement des documents avec des signatures simples[1] ;
- **Certificats signature avancée** : certificats destinés aux personnes physiques invitées, par les clients du SCS, à signer électroniquement des documents avec des signatures avancées[2] ; ces certificats sont conformes à la norme [ETSI EN 319 411-1] pour le niveau LCP ;
- **Certificats cachet Safy** : certificats de SAFY pour la création de cachets simples[3] ;
- **Certificats horodatage Safy** : certificats de SAFY pour la création d'horodatage simples[4] sur les signatures et cachets électroniques produits par le SCS.

Le schéma ci-dessous illustre la hiérarchie des Autorités de Certification couverte par la présente PC/DPC.

[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].
[3] Voir la définition du cachet électronique simple dans l'article 2 de la [Loi 43-20].
[4] Voir la définition de l'horodatage électronique simple dans l'article 23 de la [Loi 43-20].

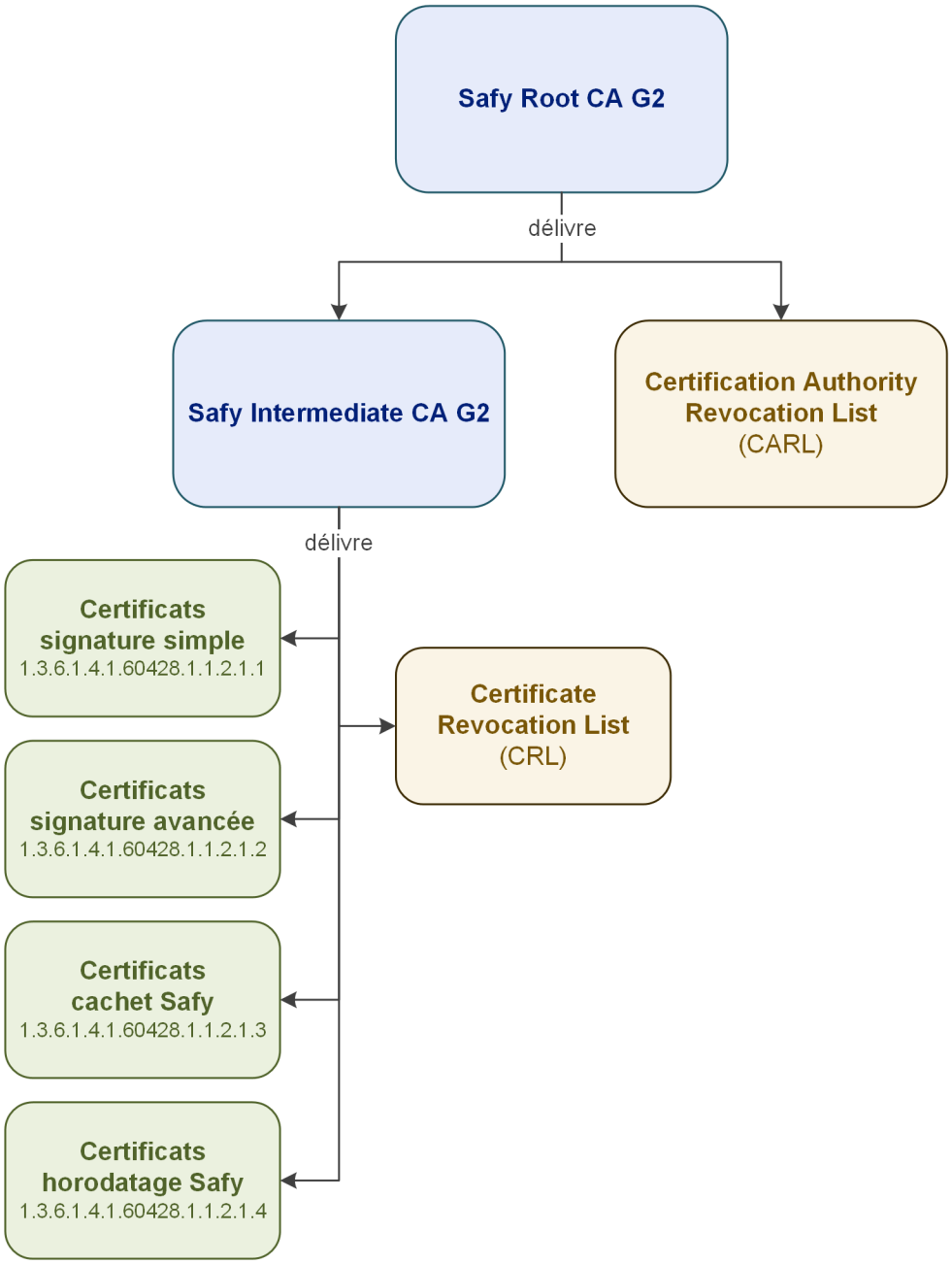

Figure 1 - Hiérarchie des Autorités de Certification couverte par la présente PC/DPC

1.2 Identification du document

La présente PC/DPC et les différents types de certificats sont identifiés par des OID.

Des éléments plus explicites comme le nom, le numéro de version ou encore la date de mise à jour, permettent d'identifier les révisions documentaires de la présente PC/DPC.

Le tableau ci-dessous liste les différents OID couverts par la présente PC/DPC.

OID	Description
1.3.6.1.4.1.60428.1.1.2.0	Safy Root CA G2
1.3.6.1.4.1.60428.1.1.2.1	Safy Intermediate CA G2
1.3.6.1.4.1.60428.1.1.2.1.1	Certificats de signature simple
1.3.6.1.4.1.60428.1.1.2.1.2	Certificats de signature avancée
1.3.6.1.4.1.60428.1.1.2.1.3	Certificats de cachet Safy
1.3.6.1.4.1.60428.1.1.2.1.4	Certificats d'horodatage Safy

Tableau 1 - Liste des OID couverts par la présente PC/DPC

1.3 Entités intervenant dans l'IGC

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 de l'ACR et de l'ACI.

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 en charge :

- De rédiger et maintenir les politiques des Services de Confiance ainsi que de les faire approuver par l'AG ;
- De veiller au respect de la conformité des pratiques et des procédures avec les politiques associées ;
- D'attribuer et de retirer des rôles de confiance à des personnes désignées ;
- De gérer les audits, les certifications et les qualifications des Services de Confiance ;

- De superviser le cycle de vie des Services de Confiance, incluant leur mise en production, leur évolution et leur fin de vie ;
- De veiller à la mise en œuvre et au maintien des dispositifs de continuité et de reprise d'activité applicables aux Services de Confiance ;
- De superviser la gestion des incidents de sécurité affectant les Services de Confiance, y compris la coordination des actions correctives et des notifications réglementaires le cas échéant ;
- De garantir la traçabilité, la conservation et la disponibilité des preuves liées à la fourniture des Services de Confiance, conformément aux exigences applicables ;
- De gérer les fournisseurs et sous-traitant intervenant directement, ou indirectement, dans la fourniture des Services de Confiance ;
- De décider, le cas échéant, de la suspension ou de la limitation d'un Service de Confiance en cas de non-conformité ou de risque majeur identifié.

1.3.2 Autorité de Certification Racine (ACR)

L'ACR, placée sous la responsabilité et le contrôle de l'AG, à travers le Responsable des Services de Confiance, est l'autorité de certification racine, dont le certificat est auto-signé, et qui permet de créer, délivrer, gérer et révoquer les certificats de l'ACI.

1.3.3 Autorité de Certification Intermédiaire (ACI)

L'ACI, placée sous la responsabilité et le contrôle de l'AG, à travers le Responsable des Services de Confiance, est l'autorité de certification intermédiaire rattachée à l'ACR, qui permet de créer, délivrer, gérer et révoquer les certificats finaux (i.e. qui ne sont pas des certificats d'AC).

Le certificat de l'ACI est signé par l'ACR.

Plus précisément, l'ACI assure les fonctions suivantes :

- **Fonction d'enregistrement** : Cette fonction assurée par l'Autorité d'Enregistrement (AE) vérifie et traite les demandes de création des certificats.

- **Fonction de génération des certificats** : Cette fonction génère les certificats à partir des informations que lui transmet l'AE.

- **Fonction d'information sur l'état des certificats** : Cette fonction publie, à l'attention des Utilisateurs de Certificats, un fichier CRL contenant la liste des numéros de série des certificats délivrés par l'ACI qui ont été révoqués, ainsi que la date à laquelle ils ont été révoqués.

- **Fonction de publication** : Cette fonction met à disposition des différentes parties concernées, la présente PC/DPC, les conditions générales de l'ACI, ainsi que le certificat de l'ACI.

- **Fonction de gestion des révocations** : Cette fonction traite les demandes de révocation (notamment l'identification et l'authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la publication des CRL de l'ACI.

1.3.4 Souscripteur

Un Souscripteur est une entité légale qui demande un certificat pour un Sujet.

Certificat signature simple *Certificat signature avancée*
Le Souscripteur est une entité légale ayant contractée avec SAFY pour faire signer des documents à des Signataires via le Service de Création de Signature (SCS). SAFY se réserve le droit d'être un Souscripteur.

Certificat cachet Safy *Certificat horodatage Safy*
Le Souscripteur est SAFY.

1.3.5 Sujet

Un Sujet désigne l'entité identifiée dans le certificat délivré par l'ACI.

Certificat signature simple *Certificat signature avancée*
Le Sujet est le Signataire.

Certificat cachet Safy
Le Sujet est un service applicatif, une unité ou un département de SAFY.

Certificat horodatage Safy
Le Sujet est une unité d'horodatage qui horodate les signatures et cachets électroniques produits par le SCS.

1.3.6 Signataire

Certificat signature simple *Certificat signature avancée*
Le Signataire est une personne physique identifiée dans le certificat de signature délivré par l'ACI et qui est le détenteur de la clé privée correspondante, gérée par le Service de Création de Signature (SCS).

1.3.7 Responsable de Certificat de Cachet (RCC)

Un Responsable de Certificat de Cachet est une personne physique dûment nommée par le Responsable des Services de Confiance pour être responsable du certificat de cachet et de la clé privée associée.

1.3.8 Responsable de Certificat d'Horodatage (RCH)

Un Responsable de Certificat d'Horodatage est une personne physique dûment nommée par le Responsable des Services de Confiance pour être responsable du certificat d'horodatage et de la clé privée associée.

1.3.9 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, s'appuie sur l'IGC de SAFY pour créer les signatures électroniques des Signataires, sur les documents électroniques soumis par les Souscripteurs.

Le SCS publie sa propre Politique de Signature / Déclaration des Pratiques de Signature dans laquelle il définit le cycle de vie des signatures qu'il produit, ainsi que les rôles et obligations des différentes parties prenantes.

Dans le cadre de la présente PC/DPC, **le SCS endosse le rôle d'Autorité d'Enregistrement (AE) de l'ACI** pour la délivrance de certificats de signature, en collectant les informations d'identification du Signataire, en procédant à son authentification et en transmettant ces informations à l'ACI pour qu'elle génère le certificat du Signataire.

L'AE peut déléguer la vérification de l'identité du Signataire à une Autorité d'Enregistrement Déléguée (AED) avec laquelle l'ACI aura établi une relation contractuelle.

1.3.10 Utilisateur de certificat

Un Utilisateur de certificat est une 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.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Clé privée et certificat d'ACR

La clé privée de l'ACR est utilisée pour :

- Signer les certificats d'ACI ;
- Signer la liste des autorités de certification révoquées (CARL).

Le certificat associé permet :

- De vérifier la validité des certificats d'ACI ;
- De vérifier l'origine et l'intégrité des CARL.

1.4.1.2 Clé privée et certificat d'ACI

La clé privée de l'ACI est utilisée pour :

- Signer les certificats qu'elle délivre ;
- Signer la liste des certificats révoqués (CRL)

Le certificat associé permet :

- De vérifier la validité des certificats délivrés par l'ACI ;
- De vérifier l'origine et l'intégrité des CRL.

1.4.1.3 Clés privées et certificats délivrés par l'ACI

Certificat signature simple *Certificat signature avancée*
La clé privée associée à la clé publique contenue dans le certificat est utilisée uniquement par le SCS, sous le contrôle exclusif du Signataire, pour créer des signatures électroniques au sein d'une Transaction de signature. Le certificat associé est utilisé pour vérifier les signatures, l'intégrité des données signées et l'identité du Signataire.

Certificat cachet Safy
La clé privée associée à la clé publique contenue dans le certificat est utilisée par SAFY pour créer des cachets électroniques simples. Le certificat associé est utilisé pour vérifier les cachets, l'intégrité et l'origine des données cachetées.

Certificat horodatage Safy
La clé privée associée à la clé publique contenue dans le certificat est utilisée uniquement pour créer des horodatages électroniques simples sur les signatures et cachets produits par le SCS. Le certificat associé est utilisé pour vérifier les horodatages électroniques.

1.4.2 Domaines d'utilisation interdits

Tout domaine d'utilisation non-prévu dans le chapitre précédent est interdit.

1.5 Gestion de la PC/DPC

1.5.1 Entité gérant la PC/DPC

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

1.5.2 Point de contact de la PC/DPC

Toute demande relative à la présente PC/DPC 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 de SAFY,
TR21A-54, les Portes de Marrakech,
40140 Marrakech - Maroc

1.5.3 Entité déterminant la conformité des pratiques avec la PC/DPC

La conformité des pratiques avec la PC/DPC est déterminée par l'AG.

1.5.4 Procédure d'approbation de la conformité des pratiques avec la PC/DPC

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

1.6 Définitions et acronymes

1.6.1 Acronymes

AC	Autorité de Certification
ACI	Autorité de Certification Intermédiaire
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée

AG	Autorité de Gouvernance des services de confiance de SAFY
CARL	Certification Authority Revocation List
CRL	Certificate Revocation List
DGSN	Direction Générale de la Sûreté Nationale
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion des Clés
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OTP	One Time Password
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
PSCo	Prestataire de Service de Confiance
RCC	Responsable de Certificat de Cachet
RCH	Responsable de Certificat d'Horodatage
RSA	Rivest Shamir Adelman
SCS	Service de Création de Signatures
URL	Uniform Resource Location
UUID	Universally Unique Identifier (identifiant unique)

1.6.2 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 PC/DPC, le terme AC sera utilisé pour désigner à la fois l'ACR et l'ACI.

Autorité d'Enregistrement (AE)
Composante de l'AC chargée de traiter les demandes de certificats en procédant aux vérifications conformément à la PC/DPC de l'AC.
Dans le cadre de la présente PC/DPC, le terme AE sera utilisé pour désigner l'AE de l'ACI.

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 un PSCo. Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Déclaration des Pratiques de Certification (DPC)
Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) qu'une AC applique dans le cadre de la fourniture de ses services de certification électronique en conformité avec la ou les PC qu'elle s'est engagée à respecter.

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 PC/DPC, le terme IGC sera utilisé pour désigner l'IGC de SAFY sur laquelle s'appuient les AC et plus généralement les différents Services de Confiance de SAFY.

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.

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.

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 met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

La fonction de publication est accessible publiquement sur le site de publication suivant : https://pki.safy.ma/g2

La fonction d'information sur l'état des certificats s'appuie sur la publication de listes de certificats révoqués :

- La dernière CARL publiée par l'ACR est disponible aux adresses suivantes :
  - http://c.pki1.safy.ma/safy-root-ca-g2.crl
  - http://c.pki2.safy.ma/safy-root-ca-g2.crl
- La dernière CRL publiée par l'ACI est disponible aux adresses suivantes :
  - http://c.pki1.safy.ma/safy-intermediate-ca-g2.crl
  - http://c.pki2.safy.ma/safy-intermediate-ca-g2.crl

2.2 Informations devant être publiées

Les informations suivantes sont accessibles à travers le site de publication :

- La dernière version en vigueur de la présente PC/DPC ainsi que les versions antérieures (tant que les certificats selon ces versions sont encore en cours de validité) ;
- Les CGU de l'ACI ;
- Le certificat X.509 de l'ACR en cours de validité ainsi que son empreinte de hachage ;
- La dernière CARL publiée par l'ACR ;
- Le certificat X.509 de l'ACI en cours de validité ainsi que son empreinte de hachage ;
- La dernière CRL publiée par l'ACI.

Les différents documents sont publiés en langue française sous forme électronique au format PDF/A.

Le site de publication est disponible 24h/24 et 7j/7 selon un taux de disponibilité mensuel de 99.5%.

2.3 Délais et fréquences de publication

Les informations documentaires de l'IGC sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs des AC.

Les certificats d'AC sont diffusés préalablement à toute délivrance de certificats et/ou de CRL correspondantes.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 4.10.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des 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 de l'IGC au travers d'un contrôle d'accès fort basé sur une authentification au moins à deux facteurs.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés dans les certificats X.509v3 sont conformes aux spécifications de la norme X.500.

Les champs `issuer` et `subject` des certificats contiennent un nom distinctif (DN) conforme à la norme X.501.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les Sujets sont explicites et sont renseignées dans le champ `subject` des certificats.

Voir chapitre 7.1.

3.1.3 Anonymisation et pseudonymisation

L'anonymisation ou l'utilisation des pseudonymes dans les certificats émis n'est pas autorisée.

3.1.4 Règles d'interprétation des différentes formes de nom

Les éléments contenus dans les chapitres 3.1.1, 3.1.2 et 3.1.3 fournissent les explications permettant d'interpréter correctement les différentes formes de nom.

3.1.5 Unicité des noms

L'attribut `serialNumber` contenu dans le champ `subject` des certificats permet de garantir l'unicité de ce champ.

En outre, chaque certificat dispose d'un numéro de série unique qui est non prédictible.

3.1.6 Identification, authentification et rôle des marques déposées

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par des demandeurs de certificats de marques déposées, de marques notoires et de signes distinctifs, ainsi que de noms de domaine.

Si un tel cas se produit, l'AE pourra refuser de délivrer le certificat ou l'AC pourra prendre la décision de révoquer le certificat concerné.

3.2 Validation initiale de l'identité

3.2.1 Méthodes pour prouver la possession de la clé privée

Certificat ACI
L'ACI prouve à l'ACR qu'elle possède bien la clé privée correspondant à la clé publique à certifier en transmettant à l'ACR, au cours d'une cérémonie des clés faisant l'objet d'un procès-verbal, la requête de certificat au format [PKCS#10] qu'elle signe à l'aide de sa clé privée.

Certificat signature simple *Certificat signature avancée*
Les bi-clés des Signataires sont générées par le SCS de manière à ne pouvoir être utilisées que par leur Signataire respectif. Dès qu'une bi-clé est créée, le SCS génère une requête de certificat, contenant notamment la clé publique et le type de certificat à créer, et la transmet à l'ACI via le protocole CMP. L'ACI authentifie le SCS et s'assure qu'il est habilité à demander la création du type de certificat.

Certificat cachet Safy *Certificat horodatage Safy*
Le RCC/RCH transmet à l'AE une requête de certificat au format [PKCS#10] contenant la clé publique à certifier, signée par la clé privée associée.

3.2.2 Validation de l'identité d'une entité

Certificat ACI *Certificat cachet Safy* *Certificat horodatage Safy*
Les certificats sont délivrés exclusivement à SAFY au cours d'une procédure interne documentée.

Certificat signature simple *Certificat signature avancée*
Non applicable. Les certificats de signature sont délivrés exclusivement à des personnes physiques sans association avec des personnes morales.

3.2.3 Validation de l'identité d'un individu

Certificat AC
En tant que responsable des clés privées d'AC, le Responsable des Services de Confiance doit participer à la cérémonie de création des clés. L'identité des différents participants à la cérémonie des clés est vérifiée et tracée dans un procès-verbal archivé par l'AC.

Certificat signature simple
Le Souscripteur transmet au SCS (qui agit en tant qu'AE de l'ACI) les informations du Signataire (au minima son nom et son prénom). Le SCS 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. Les preuves de validation de l'identité du Signataire sont conservées dans le dossier de preuve généré et conservé par le SCS.

Certificat signature avancée

Le Souscripteur transmet au SCS (qui agit en tant qu'AE de l'ACI) les informations du Signataire (nom, prénom, etc.).

L'identité du Signataire est vérifiée :

- Soit par l'AE, au cours de la Transaction de signature, via une authentification du Signataire avec le service « Identité Numérique » de la DGSN ;
- Soit par le Souscripteur lorsqu'il agit en tant qu'AED.

Les preuves de validation de l'identité du Signataire sont conservées dans le dossier de preuve généré et conservé par le SCS.

Validation de l'identité du Signataire via le service « Identité Numérique »

Au cours de la Transaction de signature, après avoir consulté les documents à signer, le Signataire est redirigé par le SCS vers le service « Identité Numérique » de la DGSN qui authentifie le Signataire à travers 2 facteurs d'authentification différents :

1. Soit sa carte nationale d'identité électronique ou son titre de séjour électronique ; et
2. Soit son code PIN ou une reconnaissance faciale.

Validation de l'identité du Signataire par une AED

Lors de l'initialisation de la Transaction de signature, le Souscripteur qui agit en tant qu'AED doit vérifier l'identité du Signataire sur la base d'un document officiel d'identité en cours de validité : passeport, carte nationale d'identité ou titre de séjour.

Une Politique d'Enregistrement Déléguée doit être établie pour décrire le processus de vérification d'identité mis en œuvre. Elle doit également décrire les exigences applicables de la présente PC/DPC qui incombent à l'AED et qu'elle doit s'engager formellement à respecter.

Avant sa mise en œuvre, la Politique d'Enregistrement Déléguée doit être approuvée par l'AC.

Certificat cachet Safy *Certificat horodatage Safy*
L'AE s'assure que le demandeur est bien le RCC/RCH désigné par le Responsable des Services de Confiance et qu'il est toujours en activité.

3.2.4 Informations non vérifiées

L'AE vérifie toutes les informations contenues dans le champ `subject` des certificats, à l'exception de l'attribut `SerialNumber` (qui est généré par l'AE).

3.2.5 Validation de l'autorité du demandeur

Certificat AC *Certificat cachet Safy* *Certificat horodatage Safy*
Cf. chapitre 3.2.3.

Certificat signature simple *Certificat signature avancée*
Aucune vérification n'est effectuée, car les Signataires sont des personnes physiques agissant en leur nom propre.

3.2.6 Critères d'interopérabilité

Sans objet.

3.3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement de la bi-clé d'un certificat entraîne nécessairement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être délivré sans un renouvellement de la bi-clé correspondante.

3.3.1 Identification et validation d'un renouvellement courant

La procédure d'identification et de validation de toute demande de renouvellement est identique à la procédure initiale décrite dans le chapitre 3.2.

3.3.2 Identification et validation pour un renouvellement après révocation

Il n'y a pas de renouvèlement à la suite de la révocation d'un certificat. Il s'agit dans ce cas, d'une nouvelle demande de certificat effectuée conformément à la procédure initiale décrite dans le chapitre 3.2.

3.4 Identification et validation d'une demande de révocation

Certificat signature simple *Certificat signature avancée*
Les certificats de signature sont des certificats dédiées à une Transaction de signature particulière et ont une durée de validité, très courte, largement inférieure à la durée qui serait nécessaire pour traiter leur révocation. Par conséquent, ces certificats ne peuvent pas être révoqués.

Certificat AC *Certificat cachet Safy* *Certificat horodatage Safy*
Pour demander la révocation d'un certificat d'AC, de cachet Safy ou d'horodatage Safy, le demandeur doit se connecter avec son compte nominatif sur le site de support de SAFY qui lui a été communiqué dans le formulaire de demande de certificat et doit renseigner au minima les informations suivantes : • Son numéro de téléphone et sa fonction ; • La valeur de l'attribut CN du champ subject et le numéro de série du certificat à révoquer ; • La raison pour laquelle le certificat doit être révoqué. L'AE s'assure que le demandeur est une personne autorisée à demander la révocation de ce certificat (cf. chapitre 4.9.2). Dans le cas d'une demande de révocation d'un certificat d'AC, l'AE prend directement contact avec le Responsable des Services de Confiance pour s'assurer de la validité de la demande.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Certificat AC
Une demande de certificat d'AC ne peut être effectuée que par le Responsable des Services de Confiance.

Certificat signature simple *Certificat signature avancée*
Une demande de certificat de signature émane de la volonté du Souscripteur de faire signer un ou plusieurs documents à un Signataire au sein d'une Transaction de signature gérée par le SCS.

Certificat cachet Safy *Certificat horodatage Safy*
Une demande de certificat émane du future RCC/RCH ou du Souscripteur.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Certificat AC
Le Responsable des Services de Confiance doit remplir et transmettre à l'ACR le formulaire de demande d'un certificat d'ACI.

Certificat signature simple
Le Souscripteur doit créer la Transaction de signature en passant au SCS, qui endosse le rôle d'AE, les documents à signer et les informations du Signataire (nom, prénom et adresse email). Le certificat sera demandé lors de l'exécution de la Transaction de signature.

Certificat signature avancée
Le Souscripteur doit créer la Transaction de signature en passant au SCS, qui endosse le rôle d'AE, les documents à signer et les informations du Signataire (nom, prénom et adresse email). Les CGU doivent être approuvés par le Signataire avant l'émission du certificat par l'ACI. La preuve de cette approbation doit être conservée par l'AC. Le certificat sera demandé lors de l'exécution de la Transaction de signature.

Certificat cachet Safy *Certificat horodatage Safy*
Le futur RCC/RCH doit remplir et transmettre à l'AE le formulaire de demande de certificat.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

Les processus d'identification et de validation de la demande d'un certificat sont réalisés conformément au chapitre 3.2.

Certificat AC
L'AE traite le formulaire de demande de certificat d'AC en procédant aux contrôles suivants : • L'AE vérifie la complétude du formulaire ; • L'AE vérifie que le formulaire a bien été signé ou approuvé par le Responsable des Services de Confiance ;

- L'AE vérifie que le Responsables des Services de Confiance a bien été nommé par l'AG et est toujours actif.

L'AE s'assure que le champ `CommonName` spécifié dans le formulaire n'est pas déjà réservé ou utilisé par un autre certificat délivré par l'AC.

Certificat signature simple

Lorsque la Transaction de signature s'exécute :

- Le Signataire prend connaissance des documents à signer ;
- Si le Souscripteur a spécifié une méthode d'authentification du Signataire (ex : OTP email, OTP SMS, etc.), alors le SCS authentifie le Signataire avec cette méthode ;
- Le Signataire doit confirmer l'exactitude de ses données d'identification (nom et prénom(s)) qui seront intégrées dans son certificat ;
- Le Signataire doit cliquer sur le bouton « Signer » pour manifester son consentement final à signer les documents ;
- Le SCS procède à la création de la bi-clé dédiée exclusivement au Signataire et à la Transaction de signature ;
- Le SCS transmet la clé publique du Signataire à l'ACI.

Certificat signature avancée

Lorsque la Transaction de signature s'exécute :

- Le Signataire doit prendre connaissance de l'intégralité des documents à signer ;
- Le Signataire doit approuver les CGU ;
- Le SCS doit vérifier l'identité du Signataire, dès lors qu'une authentification préalable n'a pas déjà été réalisée en amont par une AED ;
- Le Signataire doit confirmer l'exactitude de ses données d'identification (nom et prénom(s)) qui seront intégrées dans son certificat ;
- Le Signataire doit cliquer sur le bouton « Signer » pour manifester son consentement final à signer les documents ;
- Le SCS procède à la création de la bi-clé dédiée exclusivement au Signataire et à la Transaction de signature ;
- Le SCS transmet la clé publique du Signataire à l'ACI.

Certificat cachet Safy

Certificat horodatage Safy
La demande de certificat doit être approuvée formellement par le Responsable des Services de Confiance. Elle est ensuite traitée par un Opérateur d'AE de l'ACI selon un processus interne.

4.2.2 Acceptation ou rejet de la demande

En cas d'acceptation de la demande, l'AE transmet à l'ACI la demande de création du certificat.

En cas de rejet de la demande, l'AE informe le demandeur en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

Certificat AC *Certificat cachet Safy* *Certificat horodatage Safy*
Il n'y a aucune restriction concernant la durée maximale ou minimale de traitement entre la demande de certificat et la délivrance de celui-ci par l'ACI. Néanmoins, l'ACI devant délivrer le certificat s'efforce de traiter la demande de certificat dans les meilleurs délais.

Certificat signature simple *Certificat signature avancée*
La durée maximale de traitement entre la demande de certificat et la délivrance de celui-ci par l'ACI est de 1 minute.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

L'AC met en œuvre des mesures contre la falsification de certificat, en particulier en utilisant une cryptographie à l'état de l'art et en s'assurant que l'émission du certificat est lié à l'enregistrement.

L'AC s'assure que la demande émane de l'AE, vérifie la requête de certificat et procède à la création et à la signature du certificat, conformément au profil de certificat approprié qui est spécifié dans le chapitre 7.1.

4.3.2 Notification par l'AC de la délivrance du certificat

Certificat AC

Au cours de la cérémonie des clés, l'ACR remet le certificat d'ACI au Responsable des Services de Confiance.

Certificat signature simple *Certificat signature avancée*
Le Signataire n'est pas notifié de la délivrance de son certificat.

Certificat cachet Safy *Certificat horodatage Safy*
L'AE informe le RCC/RCH de la délivrance de son certificat.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Certificat AC
Au cours de la cérémonie des clés, lorsque l'ACR remet le certificat d'ACI au Responsable des Services de Confiance, ce dernier doit vérifier l'exactitude du certificat pour l'accepter. S'il refuse ou rejette le certificat, il doit demander sans délai la révocation du certificat à l'ACR.

Certificat signature simple *Certificat signature avancée*
L'acception du certificat par le Signataire est tacite dès lors que le Signataire a cliqué 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 ». La preuve d'acception du certificat par le Signataire est conservée par le SCS.

Certificat cachet Safy *Certificat horodatage Safy*
Lorsque l'Opérateur d'Enregistrement remet le certificat au RCC/RCH, ce dernier doit vérifier le certificat. Si le RCC/RCH refuse ou rejette le certificat, il doit demander sans délai la révocation du certificat. Dans le cas contraire, l'acceptation du certificat est implicite.

4.4.2 Publication du certificat

Certificat AC
Les certificats d'AC sont publiés (cf. chapitre 2.2).

Certificat signature simple *Certificat signature avancée*
L'ACI ne publie pas les certificats des Signataires. Les certificats sont intégrés dans les signatures électroniques produites par le SCS.

Certificat cachet Safy *Certificat horodatage Safy*
L'ACI peut publier les certificats.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat

L'utilisation de la clé privée et du certificat associé est décrite au chapitre 1.4, de façon limitative. Les usages décrits doivent être respectés. Dans le cas contraire, la responsabilité du porteur pourrait être engagée, et le certificat associé pourrait être révoqué.

Certificat signature simple *Certificat signature avancée*
Le SCS vérifie, avant toute utilisation de la clé privée du Signataire, la validité du certificat associé. Il garantit en outre que cette clé privée est utilisée exclusivement pour exécuter la Transaction de signature pour laquelle elle a été générée, et uniquement après recueil du consentement explicite du Signataire pour signer les documents concernés.

4.5.2 Utilisation de la clé publique et du certificat par l'Utilisateur de certificat

Les Utilisateurs de Certificats doivent respecter strictement les usages autorisés des certificats tels que décrit au chapitre 1.4. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

Conformément à la [RFC 3647], la notion de « renouvellement de certificat » correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique contenue dans le certificat).

Le renouvellement d'un certificat ainsi entendu n'est pas autorisée dans la présente PC/DPC.

4.7 Délivrance d'un nouveau certificat suite au changement de la bi-clé

Conformément à la [RFC 3647], ce chapitre traite de la délivrance d'un nouveau certificat lié à la génération d'une nouvelle bi-clé.

Le changement de bi-clé entraîne nécessairement le changement de certificat, et la procédure à suivre est identique à la procédure initiale de demande de certificat (cf. chapitre 4.1).

4.8 Modification du certificat

Conformément à la [RFC 3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique et autres qu'uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de certificat ainsi entendu n'est pas autorisée dans la présente PC/DPC.

4.9 Révocation et suspension des certificats

Certificat signature simple *Certificat signature avancée*
Les certificats de signature ne sont pas révocables (cf. chapitre 3.4). Le présent chapitre n'est par conséquent pas applicables à ces types de certificat. En cas de problème avec un certificat de signature, le Signataire ou toute autre personne, peut déposer un signalement sur le point de contact indiqué dans le chapitre 1.5.2. Ce signalement et les échanges qui en découlent, sont archivés et consignés dans les journaux d'audit conformément à la présente PC/DPC. SAFY s'engage à investiguer chaque cas signalé et à garantir la traçabilité des échanges pour assurer leur recevabilité éventuelle devant une juridiction.

4.9.1 Causes possibles d'une révocation

Certificat d'AC *Certificat cachet Safy* *Certificat horodatage Safy*
Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat : • Une personne autorisée demande la révocation du certificat ; • Les informations figurant dans le certificat ne sont plus correctes ; • Les obligations découlant de la PC/DPC ou les modalités applicables d'utilisation du certificat n'ont pas été respectées ;

- Une erreur (intentionnelle ou non) a été détectée dans le dossier de demande de certificat ou dans son traitement ;
- L'obsolescence d'un algorithme cryptographique utilisé par le certificat ;
- La décision faisant suite à une non-conformité révélée lors d'un audit de conformité et imposant de révoquer le certificat ;
- Un certificat d'une AC de la chaîne de certification est révoqué ;
- La clé privée associée au certificat d'une AC de la chaîne de certification est suspectée de compromission, est compromise, est perdue ou est volée (ceci est également valable pour les données d'activation associées à la clé privée) ;
- La cessation d'activité de l'AC.

4.9.2 Origine d'une demande de révocation

Certificat d'AC
Les personnes et entités suivantes sont habilitées à demander la révocation d'un certificat d'AC : • Un représentant légal ou un représentant habilité de SAFY ; • Le Responsable d'AG ; • Le Responsable des Services de Confiance ; • Une autorité judiciaire via une décision de justice.

Certificat cachet Safy *Certificat horodatage Safy*
Les personnes et entités suivantes sont habilitées à demander la révocation d'un certificat : • Un représentant légal ou un représentant habilité de SAFY ; • Le Responsable d'AG ; • Le Responsable des Services de Confiance ; • Le RCC/RCH ; • Une autorité judiciaire via une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

Certificat d'ACI

À la réception d'une demande de révocation, l'AE vérifie l'identité du demandeur et la validité de la demande, selon les exigences décrites au chapitre 3.4.

L'AG notifie la DGSSI de la révocation du certificat d'ACI.

L'ACI doit procéder à la révocation de tous les certificats en cours de validité qu'elle a émis.

Si la demande est recevable, l'ACR organise en urgence une cérémonie des clés au cours de laquelle les étapes suivantes sont réalisées :

- Activation de la clé privée de l'ACR ;
- Signature d'une nouvelle CARL contenant le numéro de série du certificat de l'ACI et sa date de révocation (correspondant à la date courante) ;
- Désactivation de la clé privée de l'ACR ;
- Destruction de la clé privée de l'ACI et de ses éventuelles copies ;
- Publication de la nouvelle CARL.

Certificat cachet Safy
Certificat horodatage Safy

Le traitement d'une demande de révocation d'un certificat se déroule de la façon suivante :

- À la réception d'une demande de révocation, l'AE vérifie l'identité du demandeur et la validité de la demande, selon les exigences décrites au chapitre 3.4 ;
- L'AE demande à l'ACI de procéder à la révocation du Certificat ;
- L'ACI révoque le certificat de manière définitive dans les 24 heures suivants la validation de la demande de révocation ;
- L'AE notifie le RCC/RCH de la révocation du certificat.

Les informations relatives aux demandes de révocation sont archivées.

Les causes de révocation des certificats ne sont pas publiées.

4.9.4 Délai accordé pour formuler la demande de révocation

Dès qu'une personne autorisée (cf. chapitre 4.9.2) a connaissance de la survenance d'une des causes possibles de révocation, de son ressort, elle doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'ACI d'une demande de révocation

Certificat d'AC
La révocation d'un certificat d'AC est effectuée immédiatement, particulièrement dans le cas de la compromission de sa clé privée.

Certificat cachet Safy *Certificat horodatage Safy*
Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24 heures, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des Utilisateurs de Certificat.

4.9.6 Exigences de vérification de la révocation par les Utilisateurs de Certificat

Certificat d'AC *Certificat cachet Safy* *Certificat horodatage Safy*
Les Utilisateurs de Certificat doivent vérifier, avant l'utilisation d'un certificat, l'état de l'ensemble des certificats de la chaîne de certification.

4.9.7 Fréquence d'établissement des CARL et des CRL

Certificat d'AC
Les CARL sont émises à minima tous les 12 mois.

Certificat cachet Safy *Certificat horodatage Safy*
Les CRL sont émises à minima toutes les 24 heures.

4.9.8 Délai maximum de publication d'une CARL et d'une CRL

Certificat d'AC
Les CARL sont publiées au maximum 30 minutes après leur génération.

Certificat cachet Safy *Certificat horodatage Safy*
Les CRL sont publiées au maximum 30 minutes après leur génération.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Les AC ne mettent pas à disposition de service de vérification en ligne du statut des certificats (OCSP).

L'accès aux CARL et CRL est disponible 24h/24 et 7j/7 selon un taux de disponibilité mensuel de 99.5%. En cas de défaillance système, d'interruption de service ou d'un autre facteur indépendant de la volonté de l'AC, celle-ci s'engage à tout mettre en œuvre pour que la CARL ne soit pas indisponible plus de 48 heures consécutives.

4.9.10 Exigences de vérification en ligne du statut de révocation des certificats par les Utilisateurs de Certificat

L'intégrité et l'authenticité du statut des certificats est permise par le fait que les CARL et les CRL sont signées, respectivement, par l'ACR et par l'ACI.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Certificat d'AC
Pour un certificat d'AC, outre les exigences décrites dans le chapitre 4.9.3, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site Internet de l'AC, et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Certificat cachet Safy *Certificat horodatage Safy*
Les personnes et entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délai dès lors qu'ils ont eu connaissance de la compromission de la clé privée. Par ailleurs, en cas de compromission de la clé privée dont il est responsable, ou de connaissance de compromission de la clé privée de l'ACR ou de l'ACI, le RCC/RCH doit cesser, de façon immédiate et définitive, d'utiliser sa clé privée et le certificat associé.

4.9.13 Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée dans la présente PC/DPC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à disposition publiquement un mécanisme de consultation libre des CARL/CRL.

Ces CARL/CRL sont conformes au format [RFC 5280] et sont accessibles via les URL indiquées dans le chapitre 2.2, ainsi que dans l'extension `CRL Distribution Points` des certificats qui contiennent cette extension (cf. chapitre 7).

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 et 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4h et une durée maximale totale d'indisponibilité par mois de 8 heures.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre le porteur d'un certificat et l'AC

Non applicable.

4.12 Séquestre de clé et recouvrement

Les clés privées ne sont pas séquestrées.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Les équipements de l'IGC sont hébergés au sein de datacenters situés sur le territoire marocain.

5.1.2 Accès physique

Un contrôle strict des accès physiques aux équipements de l'IGC est effectué, avec journalisation des accès et vidéo-surveillance. Le périmètre de sécurité défini autour des équipements supportant notamment les fonctions de génération, gestion et révocation des certificats n'est accessible qu'aux personnes disposant d'un rôle de confiance et ne peut être partagé avec d'autres organisations.

Toute personne non autorisée (prestataire, visiteur, etc.) intervenant dans ces zones physiquement sécurisées est accompagnée en permanence par une personne autorisée.

En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion et de mécanismes d'alarme, couvrant les zones sensibles et les accès.

Enfin, des mesures organisationnelles et techniques sont mises en place pour empêcher la sortie non autorisée du site d'équipements, d'informations, de supports ou de logiciels liés aux services de l'IGC.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'infrastructure opérant l'IGC, telles que fixées par leurs fournisseurs, ainsi que les engagements en matière de disponibilité des différentes fonctions des AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Les sites d'hébergement sont équipés d'onduleurs et de groupes électrogènes.

5.1.4 Vulnérabilité aux dégâts des eaux

Les sites d'hébergement sont situés hors zone inondable et des systèmes de détection de fuites d'eau sont en place au sein de ces sites.

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions, notamment celles de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les sites d'hébergement sont soumis à des mesures de prévention et de protection incendie appropriés (système de détection et extinction par système de brouillard d'eau).

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC/DPC en matière de disponibilité de ses fonctions, notamment celles de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Les informations et les actifs support intervenant dans les activités de l'IGC sont identifiés, inventoriés et leurs besoins de sécurité définis en disponibilité, intégrité et confidentialité.

Des mesures sont mises en place pour éviter la compromission et le vol de ces informations.

Les supports correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ces supports sont :

- Manipulés de manière sécurisée afin de les protéger contre les dommages, le vol et les accès non autorisés ;
- Protégés contre l'obsolescence et la détérioration pendant la période durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont détruits de manière sécurisée ou réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

5.1.8 Sauvegardes hors site

Des sauvegardes régulières sont mises en œuvre par l'AC vers un site de secours afin d'assurer une reprise des fonctions de l'AC le plus rapidement possible après incident, conformément aux exigences et aux engagements de la présente PC/DPC.

Le site de secours offre un niveau de sécurité au moins équivalent au site principal et garantit notamment que les informations sauvegardées hors site sont protégées en confidentialité et en intégrité au même niveau que sur le site principal.

Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales. Elles sont, par ailleurs, testées de façon régulière pour s'assurer de leur efficacité dans le cadre du PCA.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance suivants sont définis :

- **Security Officer** : Personne chargée de la mise en œuvre et du contrôle de la politique de sécurité de l'IGC. Elle gère les contrôles d'accès physiques et logiques aux équipements des systèmes de l'IGC ;
- **System Operator** : Personne responsable de la mise en œuvre de la présente PC/DPC au niveau de l'application dont il a la charge. Sa responsabilité couvre l'ensemble des services fournis par cette application et les performances correspondantes.
- **System Administrator** : Personne chargée de l'installation, de la configuration et de la maintenance technique des équipements informatiques de l'IGC. Elle assure l'administration technique des systèmes et des réseaux de l'IGC et est autorisée à réaliser les sauvegardes et les restaurations ;
- **System Auditor** : Personne habilitée à prendre connaissance des archives et est chargée de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. ;
- **Registration Officer** : Personne chargée de vérifier les informations requises pour la délivrance d'un certificat et d'approuver les demandes de certificats envoyés à l'AE ;
- **Revocation Officer** : Personne chargée de vérifier les demandes de révocation de certificats envoyées à l'ACI et de procéder aux révocations.

Les personnes qui ont rôle de confiance doivent être libres de tout conflit d'intérêt incompatibles avec leurs missions.

5.2.2 Nombre de personnes requises par tâche

L'AC détermine les procédures, ainsi que le nombre de personnes et les rôles requis, pour chaque tâche devant être réalisée au sein de l'AC.

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes. Pour certaines tâches sensibles telles que les opérations sur les HSM (par exemple la cérémonie des clés), plusieurs personnes sont requises pour des raisons de sécurité et de « dual control ».

5.2.3 Identification et authentification pour chaque rôle

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de l'AC avant de lui attribuer un rôle de confiance et les droits associés.

Toute personne intervenant dans le fonctionnement de l'AC doit avoir préalablement reçu et acceptée les missions associées à son ou ses rôles de confiance.

Les accès physique et logique sont autorisés aux seules personnes autorisées.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les cumuls des rôles de confiance suivants sont interdits au sein de l'IGC :

- System Administrator / System Operator et Security Officer ;
- System Administrator / System Operator et Registration Officer / Revocation Officer ;
- System Administrator / System Operator et System Auditor.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Les personnels remplissant un rôle de confiance au sein de l'IGC sont nommés par l'AG et sont soumis à une clause de confidentialité. Ils sont également informés de leurs responsabilités et des procédures liées à la sécurité du système et au contrôle du personnel qu'ils doivent respecter. Les missions qui leurs sont demandées sont compatibles avec leurs compétences. Le personnel d'encadrement dispose de l'expertise nécessaire et est familier des procédures de sécurité.

5.3.2 Procédures de vérification des antécédents

Les personnels remplissant un rôle de confiance au sein de l'IGC sont soumis à une procédure de vérification des antécédents avant leur prise de fonction. Ces vérifications sont revues au minima tous les 3 ans.

La procédure de vérification des antécédents est revue au minima tous les 2 ans.

Les vérifications portent sur les points suivants :

- La personne n'a pas commis d'infraction en contradiction avec ses rôles de confiance ;
- Les rôles de confiance de la personne ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de ses tâches.

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter conformément à ses rôles de confiance.

5.3.4 Exigences et fréquence en matière de formation continue

En fonction de la nature des évolutions (liées aux systèmes, aux procédures, à l'organisation, ...), le personnel concerné reçoit une information ou une formation adéquates, préalablement à la mise en œuvre desdites évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

L'AC peut prendre toutes sanctions adéquates (administrative et/ou disciplinaire) envers un personnel en cas d'action non-autorisée soupçonnée ou avérée de sa part. Elle peut notamment lui interdire l'accès à tout ou partie du service.

La nature de ces sanctions sont portées à la connaissance des personnes qui interviennent au sein de l'AC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur des composantes de l'IGC respecte également les exigences du présent chapitre 5.3. Ceci peut se traduire par des clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Le personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre, ainsi que les politiques applicables à la fonction au sein de l'AC (notamment la présente PC/DPC) pour laquelle il est amené à intervenir.

5.4 Procédure de constitution des données d'audit

La journalisation d'événements consiste à enregistrer manuellement ou automatiquement les opérations, sous forme papier ou électronique, afin d'assurer leur traçabilité et leur imputabilité.

5.4.1 Type d'évènements à enregistrer

L'AC journalise, au minimum, les événements tels que décrit ci-dessous sous forme électronique. La journalisation est automatique depuis le démarrage du système et sans interruption jusqu'à son arrêt.

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;

- Traces d'activité (logs) des modules cryptographiques contenant les clés privées ;
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à la défaillance de la fonction de journalisation, pannes logicielles et matérielles ;
- Connexion / déconnexion des personnes ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux qui concernent la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles.

En complément de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions, des évènements spécifiques aux différentes fonctions du service d'émission de certificats sont journalisés, notamment :

- La réception d'une demande de certificat (initiale et renouvellement) ;
- La validation ou le rejet d'une demande de certificat ;
- Les événements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde / restauration, destruction, ...) ;
- La génération des certificats ;
- La génération et la publication des CARL et CRL ;
- La publication et la mise à jour des informations liées aux AC (PC/DPC, certificats d'AC, ...) ;
- La réception d'une demande de révocation ;
- La validation ou le rejet d'une demande de révocation.

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- Le type de l'évènement ;
- Le nom de l'exécutant ou de la référence du système déclenchant l'évènement ;
- La date et heure de l'évènement ;
- Le résultat de l'évènement (échec ou réussite).

L'imputabilité d'une opération revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir le nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes), la cause de l'évènement et toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série ou l'empreinte de hachage de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus, afin de garantir l'exactitude de la date des opérations.

Dans le cas d'un enregistrement manuel d'un événement ou d'une série d'événements (par exemple dans le cas d'une cérémonie des clés), l'écriture de l'opération doit avoir lieu, sauf exception, le même jour ouvré que l'évènement.

5.4.2 Fréquence de traitement des journaux d'évènements

Voir chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins 1 mois et doivent être archivés au plus tard 1 mois après leur génération.

5.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité et leur disponibilité. Ils ne sont accessibles qu'au personnel autorisé à les exploiter.

Les systèmes générant les journaux d'événements sont synchronisés sur une source fiable de temps détaillée au chapitre 6.8.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'évènement sont régulièrement sauvegardés hors du site sur lequel ils ont été générés, afin d'assurer leur disponibilité.

5.4.6 Système de collecte des journaux d'évènements

Les journaux d'événements sont centralisés dans un concentrateur permettant aux personnes et aux applications autorisées, de consulter et analyser les journaux.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

5.4.8 Évaluation des vulnérabilités

L'AC réalise des évaluations régulières des vulnérabilités affectant ses systèmes, notamment au moyen de scans automatisés, de veille sécuritaire et, le cas échéant, de tests d'intrusion.

Les vulnérabilités identifiées sont enregistrées, analysées et traitées conformément aux procédures de gestion des vulnérabilités décrites en section 6.6.

Par ailleurs, les journaux d'évènements sont contrôlés :

- Au moins 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec pouvant révéler des tentatives d'accès non autorisées ;
- 1 fois par semaine dans leur totalité afin d'identifier, d'analyser et d'expliquer les anomalies qui se sont produites, et lorsque cela est possible, de planifier le déploiement d'actions correctives dans le but de remédier à ces anomalies ;
- Dès qu'une anomalie est détectée.

5.5 Archivage des données

5.5.1 Types de données à archiver

Le tableau ci-dessous liste les données archivées et leurs durées de conservation.

Type d'information	Durée
Dossiers de demande et de révocation de certificats	Chaque dossier est conservé pendant une durée d'au moins 7 ans après la date d'expiration du certificat correspondant.
Certificats d'ACR et d'ACI Certificats émis par l'ACI	Chaque certificat est conservé pendant au moins 7 ans après sa date d'expiration.
CARL et CRL	Chaque CARL et CRL est conservée pendant au moins 7 ans après sa date d'expiration.
Journaux d'évènements	Chaque événement est conservé au moins 7 ans après la fin de validité du certificat associé.
Toutes les versions des documents suivants : • PC/DPC • CGU • Politiques d'Enregistrement Déléguée (pour les AED) • Contrats avec les Souscripteurs	Chaque version est archivée pendant au moins sept (7) ans après sa publication. Si l'AC associée est toujours valide à l'issue de ce délai, la version est conservée jusqu'à la date de fin de validité de l'AC.

5.5.2 Période de conservation des archives

Les durées de conservation des archives sont précisées dans le tableau du chapitre précédent.

5.5.3 Protection des archives

Pendant toute leur durée de conservation, les archives et leurs copies de sauvegarde sont :

- Protégées en intégrité et en confidentialité ;
- Accessibles uniquement aux seules personnes autorisées ;
- Lisibles et exploitables.

5.5.4 Procédure de sauvegarde des archives

Les archives sont périodiquement sauvegardées sous forme électronique et exportées sur un autre site d'hébergement, en conservant un niveau de sécurité en matière d'intégrité et de confidentialité au moins équivalent à celui du site principal.

5.5.5 Exigences d'horodatage des données

Voir le chapitre 5.4.4 pour la datation des journaux d'évènements et le chapitre 6.8 pour les exigences en matière de datation et d'horodatage.

5.5.6 Système de collecte des archives

L'archivage est réalisé sur des serveurs d'archivage qui assurent la disponibilité, l'intégrité et la confidentialité des archives.

5.5.7 Procédures de récupération et de vérification des archives

Les archives, qu'elles soient au format papier ou électronique, peuvent être récupérées dans un délai inférieur à 2 jours ouvrés suite à l'acceptation par l'AC de la demande de récupération de l'archive.

L'AC vérifie la restauration et la lisibilité de ses archives par échantillonnage au moins 1 fois par an.

5.6 Changement de clé d'AC

L'AC ne peut pas émettre de certificat dont la date de fin serait postérieure à la date d'expiration de son propre certificat. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC, moins la période de validité des certificats qui ont été émis.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent reste utilisable pour valider les certificats émis sous

cette clé et ce jusqu'à ce que tous les certificats signés avec cette clé aient expiré ou aient été révoqués.

Par ailleurs, l'AC change sa bi-clé et le certificat correspondant dès lors que la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission ou encore le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé…). L'AG doit prévenir directement et sans délai le point de contact identifié sur le site de la DGSSI.

D'une manière générale, toute violation de la sécurité ou perte d'intégrité ayant un impact significatif sur le service de confiance fourni et/ou sur les données à caractère personnel associées fait l'objet d'une notification à la DGSSI dans un délai maximal de 24 heures à compter de l'identification de l'incident.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC devient insuffisant pour son utilisation prévue restante, alors l'AC publiera l'information sur son site Internet et révoquera les certificats concernés.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)

L'AC dispose d'un PCA, testé au moins 1 fois par an, permettant de répondre aux exigences de disponibilité de ses différentes fonctions découlant de la présente PC/DPC, notamment en ce qui concerne les fonctions liées à la publication et / ou à la révocation des certificats.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Dans le cas de compromission d'une clé d'AC, l'AC réalise les actions suivantes :

- Révoquer le certificat correspondant dans les plus bref délais comme précisé au chapitre 4.9 ;
- Arrêter immédiatement l'utilisation de la clé privée compromise ;
- Informer sans délai les parties suivantes :
    - Les clients concernés ;
    - Les Utilisateurs de certificat ;
    - La DGSSI.
- Indiquer sans délai sur son site de publication que les certificats et les informations de statut de révocation, délivrés en utilisant cette clé d'AC compromise, peuvent ne plus être valables ;
- Procéder, le cas échéant, à un dépôt de plainte auprès des autorités compétentes.

5.7.4 Capacités de continuité d'activité suite à un sinistre

L'AC dispose d'un PCA et d'un PRA qui détaillent les mesures à prendre pour rétablir les activités dans les cas d'indisponibilité des locaux, des personnels, des fournisseurs critiques mais aussi dans les cas de cyber-attaques ou d'interruption des services informatiques.

Les opérations de bascule et de restauration décrites dans le PRA sont réalisées par des personnes ayant les rôles de confiance adéquats et sont testées au moins une fois par an.

5.8 Fin de vie

La cessation d'activité de l'AC n'impacte pas les Signataires, dans la mesure où les certificats qui leur sont délivrés sont associés à une transaction de signature spécifique, non-révocables et ont une durée de validité maximale de 30 minutes. Par ailleurs, les signatures, cachets et horodatages produits par le SCS intègrent systématiquement les données de révocation (CARL et CRL) permettant d'attester de la validité des certificats associés au moment où ils furent utilisés pour produire ces signatures, cachets et horodatages.

Les Souscripteurs pourront se fier à la liste publiée par la DGSSI sur les PSCo agréés et non-agréés pour trouver un PSCo de remplacement.

Le processus de cessation est mis en œuvre selon les étapes suivantes, dans le respect des exigences réglementaires, contractuelles et normatives :

1. Notification préalable
2. Arrêt progressif et révocation

3. Archivage et accessibilité post-activité

5.8.1 Notification préalable

- Définition de la date de fin d'activité effective, formellement actée par l'AG.
- Notification formelle à la DGSSI et aux Souscripteurs, dans les meilleurs délais après la décision de cessation, idéalement au moins 60 jours avant la date effective. L'AC informera la DGSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus de cessation d'activité.
- Publication d'un avis de cessation sur le site officiel de SAFY et dans les dépôts publics concernés.

5.8.2 Arrêt progressif et révocation

- Résiliation des contrats actifs avec les prestataires et sous-traitants participant à la gestion des certificats.
- Résiliation des contrats actifs avec les Souscripteurs ;
- Arrêt complet des services de délivrance à la date annoncée ;
- Révocation de tous les certificats en cours de validité qui ont été émis par l'ACI, suivie de la génération d'une CRL finale, avec une date d'expiration positionnée au 31/12/9999 à 23:59:59 ;
- Destruction irréversible de la clé privée de l'ACI, ainsi que de toute copie ;
- Révocation du certificat de l'ACR, suivie de la génération d'une CARL finale, également valide jusqu'au 31/12/9999 à 23:59:59 ;
- Destruction irréversible de la clé privée de l'ACR et de toute copie.

5.8.3 Archivage et accessibilité post-activité

Maintien ou transfert à un tiers de confiance de :

- L'ensemble des archives (fichiers de preuves, certificats, journaux, politiques, etc.) dans des conditions garantissant intégrité, lisibilité et confidentialité pendant la durée définie au chapitre 5.5.
- La mise à disposition publique des certificats d'AC et des dernières CARL et CRL pendant une durée minimale de 12 mois suivant l'arrêt des services.

L'AC a mis en œuvre un mécanisme de garantie destiné à assurer, dans la mesure permise par le droit applicable en matière de faillite, la couverture des coûts requis pour satisfaire à ces exigences, y compris en cas d'insolvabilité ou d'incapacité à les assumer par ses propres moyens.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Toutes les bi-clés sont générées dans des dispositifs sécurisés de protection des clés satisfaisant aux exigences de la section 6.2.11.

Certificat d'ACR
La génération de la bi-clé d'une ACR est effectuée dans des circonstances parfaitement contrôlées, dans le cadre d'une « cérémonies des clés », qui se déroule dans un environnement sécurisé (cf. chapitre 5) avec la participation du Responsable des Services de Confiance, d'au moins un System Administrator, d'au moins un Security Officer, et d'une personne digne de confiance, indépendante de la direction de l'ACR (par exemple, un notaire, un huissier de justice ou un auditeur externe), en tant que témoin attestant que le rapport consigne fidèlement la cérémonie des clés telle qu'elle a été réalisée.

Certificat d'ACI
La génération de la bi-clé d'une ACI est effectuée dans des circonstances parfaitement contrôlées, dans le cadre d'une « cérémonies des clés », qui se déroule dans un environnement sécurisé (cf. chapitre 5) avec la participation d'au moins un System Administrator et d'au moins un Security Officer attestant que le rapport consigne fidèlement la cérémonie des clés telle qu'elle a été réalisée.

Certificat de signature simple *Certificat de signature avancée*
La bi-clé est générée par le SCS, qui met en œuvre des moyens techniques et organisationnels afin d'assurer que la clé privée d'un Signataire ne puisse être utilisée que par lui.

Certificat cachet Safy
La bi-clé est générée par le RCC.

Certificat horodatage Safy
La bi-clé est générée par le RCH.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

Certificat d'AC
La clé publique est transmise dans une requête de certificat au format [PKCS#10], de façon sécurisée sous la supervision des participants de la cérémonie des clés (cf. chapitre 6.1.1).

Certificat de signature simple *Certificat de signature avancée*
Après la génération de la bi-clé, la clé publique est immédiatement transmise à l'AE par le SCS via le protocole [CMP].

Certificat cachet Safy *Certificat horodatage Safy*
La clé publique est transmise par l'AE dans une requête de certificat au format [PKCS#10].

6.1.4 Transmission de la clé publique de l'AC aux Utilisateurs de Certificat

La clé publique de l'AC est publiée sur le site de publication de l'ACI (cf. chapitre 2.2) dans un certificat au format X.509 v3.

6.1.5 Tailles des clés

Les algorithmes et les tailles des clés utilisés doivent respecter la version la plus récente de la norme [ETSI TS 119 312].

Certificat d'AC
A minima RSA 4096 bits pour les bi-clés.

Certificat de signature simple *Certificat de signature avancée* *Certificat cachet Safy* *Certificat horodatage Safy*
A minima RSA 3072 bits.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

Les paramètres utilisés pour la génération des bi-clés doivent respecter la version la plus récente de la norme [ETSI TS 119 312].

Les paramètres et les algorithmes utilisés sont documentés dans le chapitre 7.

6.1.7 Objectifs d'usage de la clé

Les objectifs d'usage des bi-clés sont décrits dans le chapitre 1.4, ainsi que dans le chapitre 7 à travers l'extension « Key Usage » des certificats.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

Des mesures de sécurité et de contrôle sont mises en place pour la gestion des clés cryptographiques et du matériel cryptographique associé au travers de leur cycle de vie.

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés pour la génération et la mise en œuvre des bi-clés des AC sont des dispositifs sécurisés de protection des clés satisfaisant aux exigences définies dans le chapitre 6.2.11.

L'AC met en œuvre des protections physiques et logiques pour empêcher la délivrance non autorisée de certificats.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC est assuré exclusivement selon un mécanisme de dual control, impliquant l'intervention conjointe d'un *Security Officer* et d'un *System Administrator*, conformément à une procédure technique et organisationnelle formalisée et traçable.

6.2.3 Séquestre de la clé privée

Les clés privées ne sont pas séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées d'AC font l'objet de copies de secours dans un dispositif sécurisé de protection des clés satisfaisant aux exigences définies dans le chapitre 6.2.11.

Les opérations de sauvegarde et de restauration des clés privées d'AC sont réalisées exclusivement sous « dual control », impliquant l'intervention conjointe d'un *Security Officer* et d'un *System Administrator*, conformément à une procédure technique et organisationnelle formalisée et traçable.

6.2.5 Archivage de la clé privée

Les clés privées ne sont pas archivées.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Voir chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Voir chapitre 6.2.1.

Certificat d'ACR
La clé privée est stockée dans un dispositif sécurisé de protection des clés satisfaisant aux exigences définies dans la section 6.2.11 de telle sorte qu'elle ne peut être utilisée sans son activation préalable (cf. chapitre 6.2.8).

Certificat d'ACI
La clé privée est stockée dans un dispositif sécurisé de protection des clés satisfaisant aux exigences définies dans la section 6.2.11.

Certificat de signature simple *Certificat de signature avancée*
La clé privée, lorsqu'elle est stockée par le SCS pendant la Transaction de signature, est chiffrée avec une clé secrète générée aléatoirement par le SCS et associée à la Transaction de signature.

Certificat cachet Safy *Certificat horodatage Safy*
La clé privée est stockée sous forme chiffrée par le RCC/RCH de manière à assurer son intégrité et sa confidentialité.

6.2.8 Méthode d'activation de la clé privée

Certificat d'ACR
La clé privée est activée au sein du module cryptographique hors ligne uniquement sous « dual control », via l'intervention conjointe d'un *Security Officer* et d'un *System Administrator*, conformément à une procédure technique et organisationnelle formalisée et traçable.

Certificat d'ACI
La clé privée est activée au sein du module cryptographique uniquement sous « dual control », via l'intervention conjointe d'un *Security Officer* et d'un *System Administrator*, conformément à une procédure technique et organisationnelle formalisée et traçable.

Certificat de signature simple *Certificat de signature avancée*
L'activation de la clé privée est réalisée automatiquement lors de sa création par le SCS dans le cadre de la Transaction de Signature à laquelle elle est spécifiquement liée, de telle sorte que la clé privée reste sous le contrôle exclusif du Signataire et est liée avec le certificat du signataire au travers de la clé publique. Le SCS s'assure de l'intégrité du lien entre la clé et le certificat associé. Le protocole de signature est conçu pour éviter les attaques « man-in-the-middle » et les rejeu, tout en garantissant que la clé privée du Signataire soit utilisée exclusivement pour chiffrer les empreintes de hachage dérivées des documents qui lui ont été présentés par le SCS et qu'il a explicitement consenti à signer électroniquement.

Certificat cachet Safy
L'activation de la clé privée ne peut se faire qu'à la suite d'une authentification du RCC assurant ainsi le contrôle sur la clé.

Certificat horodatage Safy
L'activation de la clé privée ne peut se faire que par l'Unité d'Horodatage dans laquelle le RCH l'a créé.

6.2.9 Méthode de désactivation de la clé privée

Certificat d'ACR
La clé privée est désactivée immédiatement après son utilisation par le rôle de confiance qui l'a activé, afin de la rendre inaccessible. Elle est par ailleurs automatiquement désactivée en cas de redémarrage du module cryptographique et doit être activée conformément au chapitre 6.2.8 pour pouvoir être de nouveau utilisée.

Certificat d'ACI
La clé privée est automatiquement désactivée en cas de détection par le module cryptographique d'une des attaques suivantes : ouverture du dispositif, retrait ou forçage. Elle peut également être désactivée par une personne ayant le rôle de confiance et les droits appropriés.

Certificat de signature simple *Certificat de signature avancée*

La clé privée est éphémère et est automatiquement détruite par le SCS à la fin de la Transaction de signature.

Certificat cachet Safy
La clé privée peut être désactivée à tout moment par le RCC.

Certificat horodatage Safy
La clé privée peut être désactivée à tout moment par le RCH.

6.2.10 Méthode de destruction d'une clé privée

Certificat d'AC
Lors de la fin de vie, normale ou anticipée (révocation), de la clé privée de l'AC, cette clé est systématiquement détruite, ainsi que toutes les copies. Un procès-verbal de destruction de la clé est établi à l'issue de cette procédure.

Certificat de signature simple *Certificat de signature avancée*
La clé privée est éphémère et est automatiquement détruite par le SCS à la fin de la Transaction de signature.

Certificat cachet Safy
La destruction de la clé privée est sous le contrôle et la responsabilité du RCC. Lorsqu'il la détruit, il doit veiller à détruire toutes les éventuelles copies de la clé.

Certificat horodatage Safy
La destruction de la clé privée est sous le contrôle et la responsabilité du RCH. Lorsqu'il la détruit, il doit veiller à détruire toutes les éventuelles copies de la clé.

6.2.11 Niveau de qualification des modules cryptographiques

Certificat d'AC
Les modules cryptographiques utilisées par les AC sont des HSM qui doivent être certifiés selon l'un des 2 schémas de certification suivants : • EAL4+ (ou supérieur) augmentée de AVA_VAN.5 selon le profil de protection [CEN EN 419 221-5] ou équivalent reconnu par la DGSSI ; ou

• FIPS 140-3 level 3 ou supérieur.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées dans le cadre de l'archivage des certificats décrit dans le chapitre 5.5.

6.3.2 Durées de vie des bi-clés et des certificats

La fin de validité d'un certificat d'AC est postérieure à la fin de vie des certificats qu'elle émet.

Certificat d'ACR
Les bi-clés et les certificats associés ont une durée de vie maximale de 20 ans.

Certificat d'ACI
Les bi-clés et les certificats associés ont une durée de vie maximale de 15 ans.

Certificat de signature simple *Certificat de signature avancée*
Les bi-clés et les certificats associés ont une durée de vie maximale de 30 minutes. Les bi-clés sont détruites dès que la Transaction de signature est terminée.

Certificat cachet Safy
Les bi-clés et les certificats associés ont une durée de vie maximale de 3 ans.

Certificat horodatage Safy
Les bi-clés ont une durée de vie maximale de 2 ans. Les certificats ont une durée de vie maximale de 5 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Certificat d'AC
La génération et l'installation des données d'activation du module cryptographique de l'AC s'effectuent lors de la phase d'initialisation et de personnalisation de ce module durant la cérémonie des clés (cf. chapitre 6.1.1).

Certificat de signature simple *Certificat de signature avancée*
Voir chapitre 6.2.8.

Certificat cachet Safy *Certificat horodatage Safy*
Les données d'activation sont créées par le RCC/RCH et doivent rester sous son contrôle.

6.4.2 Protection des données d'activation

Certificat d'AC
Les données d'activation des clés privées d'AC sont remises exclusivement aux personnes exerçant des rôles de confiance lors des cérémonies de clés, selon un principe de séparation des secrets et de « dual control ». Leur utilisation et leur manipulation sont effectuées sous le contrôle d'un *Security Officer* et d'un *System Administrator*, de sorte qu'aucune personne seule ne puisse utiliser les données d'activation nécessaires aux opérations critiques sur les clés privées des AC. Les données d'activation sont conservées dans des conditions garantissant leur confidentialité, leur intégrité et leur disponibilité : elles sont stockées dans un coffre-fort situé en zone physiquement sécurisée, avec accès strictement limité aux personnels autorisés. Elles sont conditionnées dans des enveloppes scellées numérotées, conçues pour permettre la détection de toute tentative d'ouverture ou de substitution. Toute sortie, utilisation, transport éventuel et restitution de ces enveloppes font l'objet d'une traçabilité formelle (journalisation et signatures des personnes impliquées), incluant l'identification de l'enveloppe, des éléments remis, du motif d'utilisation et de la référence d'autorisation.

Certificat de signature simple *Certificat de signature avancée*
Voir chapitre 6.2.8.

Certificat cachet Safy *Certificat horodatage Safy*
Les données d'activation sont protégées par le RCC/RCH de manière à garantir leur confidentialité.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques de l'IGC répondent au minima aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Éventuellement, gestion des reprises sur erreur.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

La configuration des systèmes de l'IGC fait l'objet de vérifications régulières, au minima tous les ans, afin de détecter tout changement qui seraient en contradiction avec les règles de la présente PC/DPC.

6.5.2 Niveau de qualification des systèmes informatiques

Voir chapitre 6.2.1.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 Mesures de sécurités liées au développement des systèmes

La configuration des systèmes mis en œuvre par les différentes composantes de l'IGC, ainsi que toute modification et mise à niveau qui pourraient leur être apportées sont documentées et contrôlées. L'IGC utilise des systèmes et des produits fiables qui sont protégés contre toute modification. Les responsables de ses composantes garantissent que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

Les systèmes de production de l'IGC sont cloisonnées et isolées des systèmes de développement, de test et de préproduction.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative dans le système d'information de l'IGC est réalisée par des personnes ayant les rôles de confiance appropriés et est signalée au responsable de la sécurité de l'IGC pour validation. Elle est documentée et apparaît dans les procédures de fonctionnement interne de l'IGC.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7 Mesures de sécurité réseau

L'interconnexion entre les systèmes informatiques de l'IGC et les réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au bon fonctionnement de l'IGC.

Les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement auditées.

L'IGC met en place des procédures de gestion des accès d'administration de la plate-forme afin de maintenir la sécurité à un niveau élevé. Ces mesures incluent l'authentification forte des administrateurs, la production de traces pour les audits, l'utilisation de canaux sécurisés de type VPN ainsi que la possibilité de modifier à tout instant les droits d'accès.

Les systèmes de production sont séparées des systèmes hors-production (dev, test, staging, préprod, etc.).

Des scans de vulnérabilités sur les adresses IP publiques et privées des services de l'AC sont effectuées régulièrement par du personnel ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires, et donne lieu à un rapport.

Des tests d'intrusion sur les systèmes de l'IGC sont réalisés préalablement à la mise en service d'une application et après toute évolution majeure de l'infrastructure ou des applications. Ce test est effectué par du personnel ou une entité ayant les compétences, les outils, l'éthique et l'indépendance nécessaires, et donne lieu à un rapport.

6.8 Horodatage / Système de datation

Les horloges de l'ensemble des systèmes sont synchronisés avec une source de temps UTC a minima toutes les 24h.

7 Profils des certificats et des CRL

7.1 Profils des certificats

Les certificats sont des certificats X.509 v3 conformes aux exigences de la [RFC 5280] et aux exigences applicables de la norme [ETSI EN 319 412-2].

7.1.1 Profil des certificats d'ACR

7.1.1.1 Champs de base

Champ	Valeur
Version	2
Serial Number	*Générée automatiquement par l'ACR lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Root CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Validity	20 ans
Subject	CN=Safy Root CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Subject Public Key Info	RSA 4096 bits

7.1.1.2 Extensions

Extension	Critique	Valeur

Basic Constraints	Oui	cA=true
Certificate Policies	Non	policyIdentifier=2.5.29.32.0
Key Usage	Oui	keyCertSign(5), cRLSign(6)
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.1.2 Profil des certificats d'ACI

7.1.2.1 Champs de base

Champs	Valeurs
Version	2
Serial Number	*Générée automatiquement par l'ACR lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Root CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Validity	15 ans
Subject	CN=Safy Intermediate CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Subject Public Key Info	RSA 4096 bits

7.1.2.2 Extensions

Extension	Critique	Valeur
Authority Info Access	Non	id-ad-calssuers= http://i.pki1.safy.ma/safy-root-ca-g2.cer http://i.pki2.safy.ma/safy-root-ca-g2.cer
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACR tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
Basic Constraints	Oui	cA=true pathLenConstraint=0
Certificate Policies	Non	policyIdentifier=2.5.29.32.0
CRL Distribution Points	Non	http://c.pki1.safy.ma/safy-root-ca-g2.crl

		http://c.pki2.safy.ma/safy-root-ca-g2.crl
Key Usage	Oui	keyCertSign(5), cRLSign(6)
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.1.3 Profil des certificats de signature simple

7.1.3.1 Champs de base

Champs	Valeurs
Version	2
Serial Number	*Générée automatiquement par l'ACI lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Intermediate CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Validity	30 minutes
Subject	**serialNumber**=*Identifiant de la transaction de signature à laquelle est associé et dédié le certificat.* **commonName**=*Prénom(s) du Signataire indiqué dans l'attribut GivenName, suivi d'un espace, puis suivi du nom du Signataire indiqué dans l'attribut Surname.* **givenName**=*Prénom(s) du Signataire (ce champ est optionnel car il existe des cas où certaines personnes n'ont pas de prénom).* **surname**=*Nom de famille du Signataire.* **countryName**= MA *(code [ISO3166-1] du pays dans lequel est établi l'AC).*
Subject Public Key Info	RSA 3072 bits

7.1.3.2 Extensions

Extension	Critique	Valeur
Authority Info Access	Non	id-ad-caIssuers= http://i.pki1.safy.ma/safy-intermediate-ca-g2.cer

		http://i.pki2.safy.ma/safy-intermediate-ca-g2.cer
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACI tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
Basic Constraints	Oui	cA=false
Certificate Policies	Non	policyIdentifier=1.3.6.1.4.1.60428.1.1.2.1.1 URL=https://pki.safy.ma/g2
ext-etsi-valassured-ST-certs	Non	NULL
Key Usage	Oui	nonRepudiation(1)
No Revocation Availability	Non	NULL
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.1.4 Profil des certificats de signature avancée

7.1.4.1 Champs de base

Champ	Valeur
Version	2
Serial Number	*Générée automatiquement par l'ACI lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Intermediate CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Validity	30 minutes
Subject	**serialNumber**=*Identifiant de la transaction de signature à laquelle est associé et dédié le certificat.* **commonName**=*Prénom(s) du Signataire indiqué dans l'attribut GivenName, suivi d'un espace, puis suivi du nom du Signataire indiqué dans l'attribut Surname.* **givenName**=*Prénom(s) de l'état civil du Signataire tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AE (ce champ est optionnel car il existe des cas où certaines personnes n'ont pas de prénom).*

	surname=*Nom de l'état civil ou nom d'usage du Signataire tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'AE.* **countryName**=MA *(code [ISO3166-1] du pays dans lequel est établi l'AC).*
Subject Public Key Info	RSA 3072 bits

7.1.4.2 Extensions

Extension	Critique	Valeur
Authority Info Access	Non	id-ad-calssuers= http://i.pki1.safy.ma/safy-intermediate-ca-g2.cer http://i.pki2.safy.ma/safy-intermediate-ca-g2.cer
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACI tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
Basic Constraints	Oui	cA=false
Certificate Policies	Non	policyIdentifier=1.3.6.1.4.1.60428.1.1.2.1.2 URL=https://pki.safy.ma/g2
ext-etsi-valassured-ST-certs	Non	NULL
Key Usage	Oui	nonRepudiation(1)
No Revocation Availability	Non	NULL
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.1.5 Profil des certificats de cachet Safy

7.1.5.1 Champs de base

Champ	Valeur
Version	2
Serial Number	*Générée automatiquement par l'ACI lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Intermediate CA G2 O=SAFY.io

	OI=NTRMA-135645 C=MA
Validity	3 ans
Subject	**serialNumber**=*identifiant unique généré aléatoirement par l'AE.* **commonName**=*Nom du service applicatif, une unité ou un département de SAFY.* **organisationName**=SAFY.io **organizationIdentifier**=NTRMA-135645 **countryName**=MA
Subject Public Key Info	RSA 3072 bits

7.1.5.2 Extensions

Extension	Critique	Valeur
Authority Info Access	Non	id-ad-calssuers= http://i.pki1.safy.ma/safy-intermediate-ca-g2.cer http://i.pki2.safy.ma/safy-intermediate-ca-g2.cer
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACI tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
Basic Constraints	Oui	cA=false
Certificate Policies	Non	policyIdentifier=1.3.6.1.4.1.60428.1.1.2.1.3 URL=https://pki.safy.ma/g2
CRL Distribution Points	Non	http://c.pki1.safy.ma/safy-intermediate-ca-g2.crl http://c.pki2.safy.ma/safy-intermediate-ca-g2.crl
Key Usage	Oui	digitalSignature(0)
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.1.6 Profil des certificats d'horodatage Safy

7.1.6.1 Champs de base

Champ	Valeur
Version	2

Serial Number	*Générée automatiquement par l'ACI lors de la génération du certificat*
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Intermediate CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
Validity	5 ans
Subject	**serialNumber**=*identifiant unique généré aléatoirement par l'AE*. **commonName**=*Nom de l'Unité d'Horodatage*. **organisationName**=SAFY.io **organizationIdentifier**=NTRMA-135645 **countryName**=MA
Subject Public Key Info	RSA 3072 bits

7.1.6.2 Extensions

Extension	Critique	Valeur
Authority Info Access	Non	id-ad-caIssuers= http://i.pki1.safy.ma/safy-intermediate-ca-g2.cer http://i.pki2.safy.ma/safy-intermediate-ca-g2.cer
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACI tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
Basic Constraints	Oui	cA=false
Certificate Policies	Non	policyIdentifier=1.3.6.1.4.1.60428.1.1.2.1.4 URL=https://pki.safy.ma/g2
CRL Distribution Points	Non	http://c.pki1.safy.ma/safy-intermediate-ca-g2.crl http://c.pki2.safy.ma/safy-intermediate-ca-g2.crl
Extended Key Usage	Oui	id-kp-timeStamping
Key Usage	Oui	digitalSignature(0)
Private Key Usage Period	Non	2 ans
Subject Key Identifier	Non	*Empreinte SHA-1 de la clé publique tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*

7.2 Profil des CRL

Les CRL sont conformes aux exigences du chapitre 5 de la [RFC 5280].

7.2.1 Profil des CARL d'ACR

7.2.1.1 Champs de base

Champ	Valeur
Version	1
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Root CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
This Update	*Date de création de la CARL*
Next Update	*This Update + 12 mois*

7.2.1.2 Extensions

Extension	Critique	Valeur
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACR tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
CRL Number	Non	*La valeur est incrémentée de 1 à chaque nouvelle CARL*

7.2.2 Profil des CRL d'ACI

7.2.2.1 Champs de base

Champ	Valeur
Version	1
Signature algorithm	SHA512withRSAandMGF1
Issuer	CN=Safy Intermediate CA G2 O=SAFY.io OI=NTRMA-135645 C=MA
This Update	Date de création de la CRL
Next Update	This Update + 7 jours

7.2.2.2 Extensions

Extension	Critique	Valeurs
Authority Key Identifier	Non	*Empreinte SHA-1 de la clé publique de l'ACI tel que spécifié dans la méthode 1 du chapitre 4.2.1.2 de la [RFC 5280].*
CRL Number	Non	*La valeur est incrémentée de 1 à chaque nouvelle CRL*

7.3 Profil des OCSP

Non applicable.

8 Audit de conformité et autres évaluations

8.1 Fréquence et circonstances des évaluations

Avant la première mise en service d'une composante de l'IGC, SAFY fait réaliser un audit de conformité par une personne ou une organisation indépendante de SAFY.

Suite à toute modification significative d'une composante de l'IGC, SAFY procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.

Par ailleurs, SAFY réalise un contrôle interne chaque année pour s'assurer du maintien de la conformité de l'IGC.

8.2 Identité et qualification des évaluateurs

Le contrôle d'une composante est assigné par SAFY à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit est choisie de façon à assurer une indépendance et une impartialité de l'audit.

8.4 Sujets couverts par les évaluations

Les audits couvrent l'ensemble des exigences de la présente PC/DPC.

8.5 Actions prises suite aux conclusions des évaluations

En cas de non-conformités détectées à la suite d'un audit, qu'il soit interne ou externe, un plan de correction est défini et appliqué.

8.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de la DGSSI.

9 Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

La tarification de la fourniture ou du renouvellement des certificats est hors du périmètre de la présente PC/DPC.

9.1.2 Tarifs pour accéder aux certificats

Sans objet.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation de certificats

Les informations d'état et de révocation de certificats sont libres d'accès et gratuit. En revanche, tout abus de sollicitations intensives peut faire l'objet d'une limitation technique pour préserver les ressources.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

Conformément à ses obligations, SAFY prend les dispositions nécessaires pour couvrir, financièrement, ses responsabilités liées à ses opérations et activités.

9.2.1 Couverture par les assurances

SAFY dispose d'une assurance couvrant les risques de responsabilité civile.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

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

- Le corpus documentaire interne de l'AC ;
- Les clés privées des AC, des composantes de l'IGC et des certificats émis ;
- Les données d'activation associées aux clés privées d'AC ;
- Tous les secrets de l'IGC ;
- Les journaux d'évènements des composantes de l'IGC ;
- Les dossiers d'enregistrement ;
- Les procès-verbaux des cérémonies des clés ;
- Les causes de révocation, sauf accord explicite de publication.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilité en termes de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au chapitre 9.3.1, 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 (chiffrement, signature, enveloppe sécurisée…).

L'AC peut mettre à disposition les dossiers d'enregistrement des bénéficiaires à des tiers dans le cadre de procédures légales.

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

La collecte et l'usage de données personnelles par l'AC 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.

9.4.2 Données à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats délivrés par l'ACI ;
- Toutes les données nominatives des personnes physiques enregistrées par l'ACI dans le cadre de la fourniture de ses services, ainsi que celles du personnel ayant des rôles de confiance au sein des AC.

9.4.3 Données à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données à caractère personnel

SAFY s'assure en cas de sous-traitance que le sous-traitant met en place des mesures appropriées pour garantir la confidentialité des données à caractère personnel.

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

Conformément à la législation et réglementation en vigueur sur le territoire marocain, les informations personnelles remises à l'AC ne doivent pas être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

La divulgation des informations personnelles n'est effectuée qu'aux autorités judiciaires ou administratives habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation marocaine.

9.4.7 Autres circonstances de divulgation de données personnelles

Sans objet.

9.5 Droits de propriété intellectuelle et industrielle

La législation et la réglementation en vigueur sur le territoire marocain sont appliquées.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux différentes composantes des AC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC/DPC et les documents qui en découlent ;
- Respecter et appliquer la partie de la PC/DPC qui leur incombent ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC ;
- Respecter les accords ou contrats qui les lient avec ses clients ;
- Documenter leurs procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorité de Certification

L'AC a pour obligation de :

- Faire approuver par l'AG sa PC/DPC et la publier ;
- Garantir et maintenir la cohérence des pratiques mises en œuvre par l'AC avec sa PC/DPC en garantissant notamment la conformité des certificats qu'elle émet avec sa PC/DPC ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Faire, sans délai, une demande de révocation de son certificat, en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation) ;
- Garantir le respect de tous les principes de sécurité par les différentes composantes de l'IGC, et des contrôles afférents.

Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, l'AC est responsable des préjudices causés aux utilisateurs, dans les cas suivants :

- Si les informations contenues dans les certificats qu'elle émet ne correspondent pas aux informations d'enregistrement ;
- Si elle n'a pas fait procéder à l'enregistrement de la révocation d'un certificat ou n'a pas publié cette information conformément à ses engagements.

9.6.2 Service d'enregistrement

Le service d'enregistrement s'engage à conserver et protéger en intégrité et confidentialité, les informations qui lui sont confiées, ainsi qu'à s'assurer que les processus de gestion de demande et de révocation de certificats sont conformes aux exigences applicables de la présente PC/DPC.

9.6.3 Souscripteur

Les obligations du Souscripteur sont les suivantes :

- Respecter les obligations qui lui incombent et qui sont décrites dans les CGU de l'ACI ;
- Fournir des informations correctes à l'AE lors de la phase d'enregistrement ;
- Informer l'AE de toute modification des informations contenues dans le certificat.

9.6.4 Porteur de certificat

Certificat de signature simple
Le Signataire a pour obligation de : • Confirmer, lors de la Transaction de signature, l'exactitude des informations le concernant qui seront intégrées dans son certificat ; • Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ; • Informer l'ACI de toute modification concernant les informations contenues dans son certificat ; • Protéger ses moyens d'authentification, le cas échéant.

Certificat de signature avancée
En complément des obligations qui s'appliquent pour un certificat de signature simple, le Signataire a également l'obligation de : • Approuver les CGU de l'ACI.

Certificat cachet Safy *Certificat d'horodatage Safy*
Le RCC/RCH a le devoir de : • Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ; • Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;

- Informer l'ACI de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

9.6.5 Utilisateurs de Certificat

Les obligations des Utilisateurs de Certificat sont les suivantes :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité et statut de révocation).

9.6.6 Autres participants

La présente PC/DPC ne formule pas d'exigence spécifique sur le sujet.

9.7 Limite de garantie

Sans objet.

9.8 Limite de responsabilités

SAFY ne pourra être tenue responsable de tout dommage consécutif à des erreurs, inexactitudes ou omissions entachant les informations contenues dans les certificats qu'elle émet, dès lors que ces erreurs, inexactitudes ou omissions résultent du caractère erroné des informations communiquées par le demandeur du certificat.

SAFY ne pourra pas être tenue pour responsable d'un fait dommageable qui relève de sa compétence en cas de force majeure. Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux marocains, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

SAFY décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC/DPC.

Enfin, SAFY ne pourra être tenue responsable, dans la limite de la loi marocaine, de perte financière ou de dommage indirect lié à l'utilisation des certificats qu'elle émet.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC/DPC

9.10.1 Durée de validité

La présente PC/DPC reste applicable au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC/DPC.

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 2.1 peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC/DPC correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité. Enfin, la validité de la PC/DPC peut arriver à terme prématurément en cas de cessation d'activité de l'AC.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11 Notifications individuelles et communication entre les participants

En cas de changement majeur de toute nature intervenant dans la composition de l'IGC, l'AC s'engage à :

- A valider en amont ce changement et en identifier les éventuels impacts
- En informer en amont la DGSSI.

9.12 Amendements de la PC/DPC

9.12.1 Procédures d'amendement

Tout amendement de la PC/DPC doit faire l'objet d'une procédure d'approbation et de publication par l'AC.

9.12.2 Mécanisme et période d'information sur les amendements

L'AC communique via son site de publication l'évolution de la PC/DPC au fur et à mesure de ses amendements.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Les OID de la présente PC/DPC étant inscrit dans les certificats finaux qu'elle émet, toute évolution de cette PC/DPC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution des OID correspondants, afin que les Utilisateurs de certificat puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, les OID de la présente PC/DPC évoluent dès lors qu'un changement majeur intervient dans les exigences de la présente PC/DPC s'appliquant à ces OID.

En revanche, lorsque la modification de la PC/DPC est de nature typographique ou lorsque qu'elle n'impacte pas le niveau de qualité et de sécurité des fonctions de l'AC et de l'AE, alors les OID de la PC/DPC ne sont pas modifiés.

9.13 Dispositions concernant la résolution de conflits

SAFY met en place des politiques et procédures permettant le traitement et la résolution des réclamations et des litiges reçus de la part des Souscripteurs ou d'autres parties utilisatrices, concernant la fourniture des services ou toute autre question connexe.

En particulier, toute réclamation peut être soumise au point de contact indiqué dans le chapitre 1.5.2.

9.14 Juridictions compétentes

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente PC/DPC, et à défaut d'accord amiable entre les parties, sera soumis au tribunal de commerce de Marrakech.

9.15 Conformité aux législations et réglementations

La présente PC/DPC est soumise au droit marocain et aux textes législatifs applicables à la présente PC/DPC.

La politique et les pratiques de l'AC sont non-discriminatoires.

9.16 Dispositions diverses

9.16.1 Accord global

Le présent document contient l'intégralité des clauses régissant l'IGC.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

En cas d'une clause non valide, les autres clauses ne sont pas remises en question.

9.16.4 Application et renonciation

Aucune renonciation à se prévaloir de l'un de ses droits ne saurait intervenir tacitement. Pour être opposable à l'AC une renonciation doit avoir été formulée par écrit. Une telle renonciation ne saurait constituer une renonciation pour l'avenir aux dits droits.

9.16.5 Force majeure

L'AC ne pourra être tenue pour responsable de tout retard ou manquement dans l'exécution de l'une quelconque de ses obligations au titre de la présente PC/DPC, si ledit retard ou manquement est dû à la survenance d'un cas de force majeure habituellement reconnu par la jurisprudence des cours et tribunaux marocains.

9.17 Autres dispositions

Sans objet.

10 Références documentaires

10.1 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) pris pour l'application de la loi n°43-20 relative aux services de confiance pour les transactions électroniques
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

10.2 Références normatives

[ETSI EN 319 411-1]
Electronic Signatures and Infrastructures (ESI)
Policy and security requirements for Trust Service Providers issuing certificates;
Part 1: General requirements

[ETSI EN 319 412-2]
Electronic Signatures and Infrastructures (ESI)
Certificate Profiles
Part 2: Certificate profile for certificates issued to natural persons

[ETSI TS 119 312]
Electronic Signatures and Infrastructures (ESI)
Cryptographic Suites

[ISO 3166-1]
Codes for the representation of names of countries and their subdivisions
Part 1: Country code

[PKCS#10]
Certification Request Syntax Specification

[RFC 3647]
Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework

[RFC 5280]
Internet X.509 Public Key Infrastructure
Certificate and Certificate Revocation List (CRL) Profile