POLITIQUE DE CERTIFICATION A LA VOLEE DE BARID MEDIA/BARID ESIGN

Version :	V1.0
Date effective :	22/09/2024
OID :	*1.2.504.1.1.1.1.1.1.2.8.1*
Nom du document :	Barid-Media/BarideSign - PC - AC_Classe_1_Simple
Diffusion :	Publique

CONTROLE DU DOCUMENT

SUIVI DES MODIFICATIONS

Date de mise à jour	Version	Paragraphe	Motif de mise à jour
20/09/2024	1.0		Version initiale

SOMMAIRE

1. INTRODUCTION

La présente Politique de Certification (PC) est un recueil d'engagements et d'exigences portant sur un ensemble de services de confiance et de produits de sécurité et des plateformes qui participent à la création sécurisée des certificats à la volée générés par BARID AL MAGHRIB.

L'objectif de ce document est de définir les engagements minimums que BARID AL MAGHRIB s'engage à respecter dans l'exposition, la délivrance et la gestion de certificats pour la création de signature tout au long de processus.

Ce document concerne les services de confiances non qualifiés suivants :

- ✓ **Délivrance de certificat à la volée pour création de signature électronique simple**;

Ces certificats sont délivrés par l'AC Barid eSign Classe 1 placée sous l'AC Racine Barid eSign eGov. Il s'agit de certificats à la volée supportant la signature électronique simple. Les certificats concernés par ce document peuvent être fournis, soit à des particuliers, soit à des professionnels.

Les certificats à la volée sont fournis via des web services sécurisés avec des mécanismes d'authentification délégués auprès des plateforme des donneurs d'ordre.

Les certificats sont éphémères d'une durée de 2h par défaut ; la durée peut être paramétrée en fonction des besoins des donneurs d'ordre.

Les codes PIN permettant l'usage des clés privées sont communiqués par voie SMS et/ou par émail au signataire.

1.1. Présentation générale

La gestion d'un certificat comprend notamment l'ensemble des phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat, jusqu'à la fin de vie de ce certificat (fin de validité lié à son échéance).

L'objectif de ce document est de définir les engagements minimums que BARID AL MAGHRIB et Barid Media, respectivement en tant que prestataire de services de confiance pour la création de certificats, et opérateur de création de signature électronique s'engagent à respecter dans l'émission, l'exposition et la gestion de certificats à la volée supportant la signature électronique simple

La définition de cette PC fait intervenir des exigences temporelles requises pour le niveau de sécurité escompté. La section 9.2 ci-après permet de quantifier ces valeurs.

Afin de faciliter la lecture de ce document, sa structure suit celle définie dans le [RFC 3647].

1.2. Acronymes et Terminologie

Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
DGSSI	Direction Générale de sécurité des Systèmes d'Information
DO	Donneur d'Ordre
ASN 1	Abstract Syntax Notation One
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards Publications
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés.
OID	Object Identifier (identifiant d'objet)

PC	Politique de Certification
PP	Profil de Protection
PIN	Personal Identification Number (code numérique à 6 chiffres)
PSCO	Prestataire de Services Confiance
RSA	Rivest Shamir Adelman
SP	Service de Publication
RFC	Request For Comments
Classe 1	Dénomination commerciale des certificats simple à la volée de signature
SHA	Secure Hash Algorithm

Terminologie

- **Authentification** – Action de s'assurer de l'identité ou de l'identifiant présumé d'une entité donnée ou de l'origine d'une communication ou d'un fichier.
- **Autorité Administrative** – Autorité responsable d'une IGC et possédant un pouvoir décisionnaire au sein de celle-ci.
- **Autorité d'enregistrement -** Entité en charge de collecter les éléments relatifs à l'identification et authentification d'une personne physique ou morale. Selon le cas d'usage, ce rôle peut être endossé par le Donneur d'ordre, Barid Media ou Barid Al Maghrib.
- **Donneur d'ordre** - Client de Barid Media qui donne aux Visiteurs accès à la Plateforme de signature et permet aux Utilisateurs d'utiliser les Services . Chaque Donneur d'Ordre dispose d'un numéro d'identification individuel au sein de la Plateforme iMDAE.
- **Autorité de Certification (AC)** – Au sein d'un PSCo, une entité 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.
- **Autorité de Certification Racine** – Une Autorité de Certification située au sommet d'une hiérarchie d'ACs.
- **Applications utilisatrices** - Services applicatifs exploitant les certificats émis par l'Autorité de Certification
- **Certificat (numérique)** - Fichier attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans un certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre un identifiant de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une période donnée précisée dans celui-ci.
- **Code OTP** (One time Password) – Code numérique personnel de 6 chiffres Un mot de passe à usage unique (siglé OTP) n'est valable que pour une seule transaction.
- **Composante** - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCo lui-même ou une entité externe liée au PSCo par voie contractuelle, réglementaire ou hiérarchique.
- **Confidentialité** – fonction ou service permettant d'assurer la protection de la sémantique de données stockées ou échangées.
- **Déclaration des pratiques de certification (DPC)** - Ensemble des pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

- **Intégrité** – concerne la détection de modifications de données stockées ou échangées.
- **Infrastructure de gestion de clés (IGC)** - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.
- **Politique de certification (PC)** - Ensemble de règles, identifié par un nom (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.
- **Signataire** : personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat.
- **Prestataire de services de confiance numérique (PSCo)** - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCo peut fournir différentes familles de certificats correspondant à des finalités différentes. Un PSCo comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Un PSCo est identifié dans un certificat dont il a la responsabilité au travers de l'AC ayant émis ce certificat et qui est identifiée dans le champ "issuer" du certificat.
- **Produit de sécurité** - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique avancée, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.
- **Support cryptographique** – Support physique, qui peut être soit une carte à microcircuit avec contacts, soit une clé cryptographique équipée d'un connecteur USB, contenant au moins un certificat et la clé privée associée.
- **Certificat à la volée (éphémère) :** consiste en un envoi d'un certificat électronique à un interlocuteur tiers pour un usage unique, comme par exemple pour signer un contrat client fournisseur, une convention ou un contrat de travail avec un nouveau collaborateur

1.3. Niveau de sécurité

Conformément aux articles 18, 19, 21, 22, 23, 32 et 33 du décret n°2.22.687 pris pour l'application de la loi n°43-20 applicables spécifiquement aux services de confiance autres que qualifiés et/ou aux PSCo qui les fournissent, le tableau suivant décrit le niveau de sécurité du point de vue enjeux considérés :

Domaine	**Niveau de sécurité**
Contextes type d'utilisation	Risques **très forts** de tentative d'usurpation d'identité pour pouvoir signer indûment des données (intérêt pour les usurpateurs, effets de la signature, etc.).

1.4. PSCo et niveau de sécurité

Les processus organisationnels, techniques et sécuritaires adaptés détaillés dans le tableau ci-dessous :

Domaine	Niveau sécurité
Validation initiale de l'identité du signataire	Le Donneur d'ordre assure l'identification et l'authentification du signataire. Ces données sont transmises de façon sécurisée à Barid Media en utilisant des APIs. Barid Media les transmet à son tour, également en mode sécurisé, à la plateforme Barid eSign
Remise / acceptation d'un certificat	Le certificat à la volée est crée par la PKI Barid eSign et communiqué **en temps réel** à la plateforme iMDAE qui l'expose au signataire, Le code PIN est transmis directement de la plateforme Barid eSign au signataire en temps réel par SMS et/ou email. La signature n'est effectuée qu'une fois le code PIN est saisie à travers la fenêtre du consentement du signataire.
Utilisabilité d'un certificat à la volée	Les certificats à la volée ont une durée limitée; ils ne sont utilisables que pendant leur durée d'utilisabilité
Protection des clés de l'AC (privées / publiques)	Génération et mise en œuvre des clés et des certificats de l'AC dans un module cryptographique répondant aux exigences de la PC Type de Barid eSign.

1.5. Certificat électronique

La mise en œuvre d'un procédé de signature électronique simple respectant les exigences définies dans le référentiel relatif aux services de confiance non qualifiés et aux prestataires fournissant ces services.

En effet, les exigences formulées dans la présente PC à l'égard des prestataires de services de certification électronique et des dispositifs de création de signature électronique simple répondent aux exigences de la Loi 43-20 applicables spécifiquement aux services de confiance autres que qualifiés.

1.6. Identification des PCs

L'arc OID de la présente Politique est 1.2.504.1.1.1.1.1.1.2.8

1.7. Fonctionnalités minimales couvertes

L'AC ou Autorité de Certification a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,) et s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC). Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des certificats à la volée

- **Enroulement du signataire (AE)** - la fonction d'enroulement du signataire s'effectue à travers les données communiquées par la plateforme du donneur d'ordre ; ces informations sont communiquées via un processus sécurisé entre la plateforme du donneur d'ordre et la plateforme Barid Media qui transmet automatiquement par voie également sécurisé les informations à la plateforme Barid eSign pour la génération des certificats.
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à la volée à partir des informations transmises par le donneur d'ordre
- **Fonction de génération des éléments secrets des porteurs** - Cette fonction génère les éléments secrets à destination du signataire (PIN transmis par voie SMS et/ou eMail)
- **Fonction de remise du certificat** - Cette fonction envoie en temps réel à la plateforme Barid Media le certificat à la volée en format PKCS#12

- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Durée des certificats à la volée :** les certificats à la volée ont une durée limitée en heure ; ils sont échus automatiquement. Cette fonction traite les demandes de révocation des certificats (notamment identification et authentification des demandeurs) et détermine les actions à mener.

1.8. Interactions avec l'IGC

Un certain nombre d'entités et personnes interagissent avec l'IGC ou au sein de l'IGC. Il s'agit notamment de :

- **Autorité de certification (AC)** - Au sein d'un PSCo, l'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.
- **Entité d'enroulement (EE)** - A pour rôle la communication des données du signataire avec un certificat à la volée
- **Le Signataire**- La personne physique identifiée dans le certificat qui apposera sa signature en utilisant un certificat à la volée.
- **Gateway PKI** : BAM dispose d'un service de Gateway PKI mis à la disposition de ses clients pour la consommation du service de certificats à la volée ou de certificats logiciels. Cette Gateway interagit avec les Systèmes d'Informations opérants internes et externes via une architecture REST API.

1.9. Responsabilités

Les responsabilités de chacun sont reprises au sein de la DPC.

1.10. Usage des certificats

Domaines d'utilisation applicables : Certificat à la volée en PKCS#12

Les certificats de signature simple objet du présent document sont utilisés par des applications clients ; les certificats reçus en PKCS#12 et stockés dans un répertoire dédié et exposés par la suite au signataire via un échange sécurisé entre la plateforme du Donneur d'ordre et la plateforme iMDAE. La manifestation du consentement du signataire quant au contenu de ces données est assurée par la page du consentement. La réception du PIN via SMS et/ou eMail sécurise la signature avec la clé privée du certificat à la volée.

1.11. Gestion de la PC

Entité gérant la PC

BARID AL MAGHRIB est responsable de la gestion des certificats à la volée conformément aux termes de ce document.

Point de contact

CHEF DE DIVISION OPERATIONS

Mme Maria EL MOUSLIH

m.elmouslih@poste.ma

2. IDENTIFICATION ET AUTHENTIFICATION

2.1. Nommage

Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500. Dans chaque certificat X509 V3 de l'IUT-T (voir [X.509]), l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" DN de type X.501.

Nécessité d'utilisation de noms explicites

Le DN du porteur est construit à partir des noms et prénoms et numéros de téléphone, tels que communiqués par la plateforme iMDAE à la plateforme Barid eSign et reçus de la plateforme du donneur d'ordre

Unicité des certificats à la volée

Afin d'assurer une continuité d'une identification unique du signataire au sein du domaine de l'AC dans ses certificats successifs (certificats à la volée) le numéro de série du certificat est propre au certificat en plus des éléments d'identification du signataire

2.2. Validation initiale de l'identité du demandeur de certificat

Pour les certificats à la volée :

Lors du processus d'enregistrement du porteur, BAM émet des certificats de courte durée pour une durée T_PORT_MIN et T_PORT_MAX destinés à un usage éphémère pour la réalisation de signatures électroniques côté serveur.

Ainsi, la génération des certificats de signature électronique repose sur les données du compte nominatif créé pour l'utilisateur dans la plate-forme de service Gateway PKI.

L'identification/authentification du titulaire du certificat est réalisée par le Donneur d'ordre. Le Donneur d'ordre assure l'identification et l'authentification du signataire et transmet ses données de façon sécurisée à Barid Media en utilisant des APIs. Barid Media les transmet à son tour, également en mode sécurisé, à la plateforme Barid eSign.

La demande de certificat est effectuée au moment de l'acte de signature. À ce moment, la fonction d'AE est remplie automatiquement par la Gateway PKI appuyée sur les données reçues du Donneur d'ordre.

3. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

3.1. Demande de certificat

Origine d'une demande de certificat

La demande d'un certificat à la volée prend origine d'un besoin de signature auprès d'une plateforme donneur d'ordre qui envois la requête à la plateforme iMDAE connectée nativement à la plateforme Barid eSign, les éléments d'authentification à l'origine sont communiqués par la plateforme du donneur d'ordre

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

Pour un certificat à la volée du signataire, les informations suivantes doivent au moins faire partie de la demande de certificat:

- Les nom et prénoms signataire
- Un numéro de téléphone et/ou une adresse email pour recevoir le code PIN
- Le numéro d'une pièce d'identité dans certains cas d'usage

.

3.2. Traitement d'une demande de certificat

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

La plateforme iMDAE émet la demande de génération du certificat à BarideSign une fois les informations du certificat sont communiqués par la plateforme du donneur d'ordre ; le certificat à la volée est alors automatiquement généré par Barid eSign et communiqué à iMDAE en temps réel pour une seule session de signature.

Durée d'établissement du certificat

La durée de production unitaire d'un certificat est en quelques secondes.

3.3. Délivrance d'un certificat

Actions de l'AC concernant la délivrance d'un certificat

C'est au niveau de la plateforme du donneur d'ordre que la demande du certificat à la volée prend naissance qui consomme des API de la plateforme iMDAE. Les éléments du certificat sont transmis via canal sécurisé à la plateforme AC pour la génération du certificat à la volée.

L'AC délivre par voie électronique sécurisé le certificat en PKC#12 à la plateforme iMDAE qui l'expose dans le processus de signature comme décrit au-dessus. Le code PIN est communiqué par email et/ou SMS directement au signataire.

Le certificat est créé sous l'AC BarideSign eGOV classe1.

Les conditions de génération des certificats et la génération des bi-clés, ainsi que les mesures de sécurité à respecter sont précisés aux chapitres ci-dessous.

3.4. Acceptation du certificat

Démarche d'acceptation du certificat

Le signataire opère obligatoirement avant signature une action de consentement ; celle-ci lui permet de valider les informations utilisées pour la création du certificat à la volée et qui serviront pour apposer sa signature.

3.5. Usages de la bi-clé et du certificat

Utilisation de la clé privée et du certificat d'un signataire

L'utilisation de la clé privée du signataire et du certificat associé est strictement limitée pour générer des signatures numériques uni-transactionnel visant à signaler que le signataire s'engage à accepter les conditions énoncées dans le texte qu'il signe. Le type précis d'engagement du signataire – "lu et approuvé" , est géré par le processus du consentement.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ». Seul le bit 1 est positionné. Ce bit signifie « non répudiation » selon le RFC 5280 et « acceptation du contenu » (contentCommitment) » selon la recommandation [X.509].

Utilisation des clés publiques et des certificats par les utilisateurs de certificats

L'utilisation de la clé publique contenue dans un certificat de porteur est strictement limitée à la vérification de signatures numériques visant à signaler que le signataire s'engage à accepter les conditions énoncées dans le texte qu'il signe. L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même via l'extension critique « keyUsage ».

Seul le bit 1 est positionné. Ce bit signifie « non répudiation » selon le RFC 5280 et « acceptation du contenu » (contentCommitment) » selon la recommandation [X.509].

Les utilisateurs de certificats doivent respecter strictement l'usage autorisé. Dans le cas contraire, leur responsabilité pourrait être engagée.

Obligations et engagements des demandeurs et utilisateurs des certificats

Le Signataire, et le donneur d'ordre sont responsables :

- des données d'Identité qu'ils ont communiquées via la plateforme du donneur d'ordre . Ils sont responsables de la confidentialité et de l'intégrité des données afférentes à la création de signature qu'il utilise.
- Toute utilisation de celles-ci est réputée, sauf preuve contraire, être leur fait. A cet effet ils s'engagent à fournir toutes informations utiles, exactes et complètes lors de la création des CERTIFICATS A la VOLEE
- de l'authenticité des informations communiquées par voie électronique à Barid MEDIA.
- de la protection du caractère confidentiel des données d'activation des clés.
- utiliser le Certificat conformément aux stipulations de l'article 8 ci-dessous ;
- ne pas divulguer les Données confidentielles relatives au certificat conformément à la loi 09-08 ;
- prendre toutes les mesures nécessaires pour assurer la sécurité et l'intégrité des Données confidentielles ainsi que celles des postes informatiques sur lesquels il utilise les Certificats;

Barid Media et BARID AL MAGHRIB ne pourront en aucun cas voir leur responsabilité engagée en cas de manquement par le Signataire ou au donneur d'ordre aux termes du présent article.

Utilisation des certificats

Les certificats à la volée restent exclusivement stockés et sécurisés sur la plate-forme de signature iMDAE et dans le dossier de preuve remis au Donneur d'Ordre

La plateforme iMDAE s'engage à utiliser les Certificats à la volée et à sécuriser ses plateformes utilisatrices sur des postes informatiques répondant aux spécifications minimales figurant dans la procédure d'installation des certificats. Le Donneur d'ordre reconnaît que ces spécifications minimales pourront être modifiées. Pour chaque intégration un contrat est signé entre Barid Media et le Donneur d'ordre

Obligation de l'AC

L'Autorité de Certification s'engage à mettre en œuvre les moyens nécessaires pour :

- Procéder à la génération et à la délivrance des certificats à la volée à BaridMedia ,
- Les certificats à la volée sont d'une durée éphémère

Barid eSign assure avoir mis en place, tous les moyens matériels et humains lui permettant de respecter les critères règlementaires et législatifs afin de revendiquer la qualité de prestataire des services de confiance.

Etendue des Responsabilités

Un contrat est signé entre Barid Media et BARID AL MAGHRIB qui définit les responsabilités de l'utilisation des certificats à la volée.

4. MESURES DE SECURITE NON TECHNIQUES

Suite à la signature du contrat de prestation entre Barid Media et la Poste Digitale pour la génération des certificats à la volée utilisés par la plateforme iMDAE auprès de la plateforme Barid eSign dans son rôle de fournisseur de PSCo il assure ainsi les mesures et les obligations de la PSCo en matière :

- Les mesures de sécurité physique et procédurales
- Les mesures organisationnelles d'organisation de l'IGC
- La gestion de l'audit et de la traçabilité des journaux d'utilisation des certificats à la volée
- l'Archivage des données utilisés pour la création des certificats à la volée ; Barid Media assure un stockage dans le dossier de preuve pour une période de 7 ans.

A noter que Barid Media a développé des API lui permettant également de se connecter sur d'autres PKI pour la génération des certificats à la volée ceci dans l'esprit d'assurer la pérennité du service iMDAE indépendamment de PSCO ainsi que son interopérabilité entre différents PCSo.

5. MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC s'engage à respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC et des résultats d'une analyse de risque.

L'AC élabore la DPC en fonction d'une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

5.1. Génération et installation de bi-clés

Génération des bi-clés : clés signataires générées par l'AC

La gestion de la bi-clé des signataires se fait au niveau du logiciel Metapki à travers le HSM au niveau de la plateforme Barid eSign.

Les bi-clés des signataires sont générées et envoyés via un système sécurisé à la plateforme iMDAE

Tailles des clés

Les clés de l'AC, des porteurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) définis respectivement dans les paragraphes 9.5, 9.6 et 9.7.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre 9.3).

Objectifs d'usage de la clé

L'utilisation de la clé privée du signataire et du certificat associé est strictement limitée au service de signature électronique.

5.2. Mesures de sécurité liées au développement des systèmes

L'implémentation du système iMDAE et des certificats générés auprès de Barid eSign permettant de mettre en œuvre les composantes d'un système de confiance numérique de bout en bout. Nous respectons une méthodologie de développement et de prise en compte des anomalies remontées. La configuration du système des composantes iMDAE ainsi que toute modification et toute mise à niveau sont documentées et contrôlées.

5.3. Mesures de sécurité réseau

L'interconnexion vers les réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante du système iMDAE.

5.4. Horodatage / système de datation des évènements

De même la plateforme iMDAE utilise le système d'horodatage de Barid eSign L'usage d'une date et d'une heure UTC (Universal Time Coordinated) pour générer les certificats et d'une heure locale pour dater les évènements liés aux activités du donneur d'ordre dans le cas de la génération des certificats à la volée. La date qui prévaut pour la datation de la signature et des événements est la date du service iMDAE.

6. PROFIL DES CERTIFICATS A LA VOLEE

6.1. Profil des certificats

Profil d'un certificat de signature électronique simple

Le gabarit du certificat contient au moins les informations suivantes :

Champs de base : champs de «TBSCertificate»

Champ	Valeur sur plateforme de production	Valeur sur plateforme de pré-production	Remarque
Version	V3		
CertificateSerialNumber	*Variable*		Nombre entier unique
SignatureAlgorithmId	sha256withRSAEncryption		
Issuer	CN=Baridesign AC Classe 1 OU=Baridesign OU=50413 O= Barid Al Maghrib C=MA	CN=TEST Baridesign AC Classe 1 OU=Baridesign OU=50413 O= Barid Al Maghrib C=MA	
Validity	*Suivant date de signature*		Certificat à la volée : Ephémère
Subject	SERIALNUMBER=<serial> UID=<à saisir> CN= *NOM Prénom* OU = Identifiant de l'entreprise OU = identifiant de l'entreprise O = Nom de l'entreprise C=MA		SERIALNUMBER= numéro unique généré par MetaPKI UID=champ optionnel pouvant contenir un numéro de matricule RH ou un numéro de CIN
Public Key Algorithm	rsaEncryption		
SubjectPublicKey	*Valeur de la clé*		Taille de clé : 2048 bits
SignatureValue	*Valeur de la signature*		

Extensions

Champ	Valeur sur plateforme de production	Valeur sur plateforme de pré-production	Criticité	Remarques
basicConstraints : CA	Faux		Non critique	Type d'objet : Entité finale
crlDistributionPoint			Non critique	
AuthorityInformationAccess			Non critique	
certificatePolicies			Non critique	OID de la PC de l'AC
keyUsage	contentCommitment		**Critique**	
SubjectAlternativeName Rfc2822Name	*email*		Non critique	Contient l'adresse email du signataire
AuthorityKeyIdentifier	*Variable*		Non critique	Id de la clé de l'autorité
SubjectKeyIdentifier	*Variable*		Non critique	Identifiant de la clé

7. ANNEXES

7.1. Gestion des données collectées

Les données collectées par Barid Media/Barid eSign, notamment celles à caractère personnel, sont nécessaires à la production, la fourniture et la gestion des certificats électroniques et les services y afférents. Tous les champs sont obligatoires, à défaut Barid eSign ne pourra traiter votre demande du certificat.

Toute collecte de données à caractère personnel dans le cadre de l'activité Barid eSign est réalisée dans le strict respect de la loi N° 09-08

Peuvent seuls, dans les limites de leurs attributions respectives, être destinataires des données collectées précitées : Le personnel chargé de la fourniture du service, L'autorité nationale d'agrément et de surveillance de la certification électronique, les dispositifs de contrôle interne et externe, les donneurs d'ordres pour lesquels le bénéficiaire utilisera son certificat pour exploiter leurs services dématérialisés en cas de besoin et toutes les autorités habilitées conformément à la réglementation en vigueur.

Conformément à la loi n°09-08, vous pouvez accéder aux données à caractère personnel vous concernant, les rectifier ou vous opposer au traitement de vos données à caractère personnel pour des motifs légitimes, par courrier avec accusé de réception à l'adresse suivante : BARID AL-MAGHRIB, Division conformité, Avenue Moulay Ismail, Hassan 10020-RABAT, ou par courrier électronique à l'adresse : donneespersonnelles@poste.ma

Ce traitement a reçu le récépissé d'autorisation de la CNDP sous le numéro : A-I-319/2013

Barid eSign pourra utiliser vos données à caractère personnel pour vous faire profiter d'autres produits et services.

7.2. Exigences de sécurité

Exigences sur les objectifs de sécurité des modules cryptographiques

Les modules cryptographiques, utilisés par l'IGC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques à la volée), répondent aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature durant tout leur cycle de vie;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- lors des opérations de sauvegarde et de restauration des clés privées, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.`

Les modules cryptographiques détectent les tentatives d'altérations physiques et entrent dans un état sûr quand une tentative d'altération est détectée.

Exigences sur les objectifs de sécurité du dispositif de création de signature

Le dispositif de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et générer sa bi-clé, répond aux exigences de sécurité suivantes :

- garantir que la bi-clé générée par le dispositif de création de signature répond aux exigences de robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée ;
- permettre de garantir l'authenticité de la clé publique lors de son export hors du dispositif.

7.3. Documents de référence externe

References	Document
[FIPS 140-2] Level 3	*Federal Information Processing Standards : Security Requirements for Cryptographic Modules*
ETSI EN 319 401	*Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*
ETSI TS 119 312	*Electronic Signatures and Infrastructures (ESI) ; Cryptographic Suites*
[RFC 6960]	X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP
[RFC 3279]	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 5280]	*IETF -Internet X.509 Public Key Infrastructure, Certificate and CRL Profile*, RFC 5280
[X.509]	*ITU - Information Technology – Open Systems Interconnection –* *The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, 6th edition.*

7.4. Algorithmes de signature et taille des clés de l'AC

Pour les clés publiques de l'AC, la taille initiale des clés et le choix initial des algorithmes est le suivant :

Algorithme	Longueur de clé
RSA	2048 bits
Hachage	SHA-256

Les algorithmes et la taille des clés pourront être modifiés, sans remettre en cause cette PC, au profit d'algorithmes offrant des résistances égales ou supérieures.

7.5. Algorithmes de signature et taille des clés des porteurs

Pour les clés publiques des porteurs, la taille initiale des clés et le choix initial des algorithmes est le suivant :

Algorithme	Longueur de clé
RSA	2048 bits

Les algorithmes et la taille des clés pourront être modifiés, sans remettre en cause cette PC, au profit d'algorithmes offrant des résistances égales ou supérieures.

FIN DU DOCUMENT