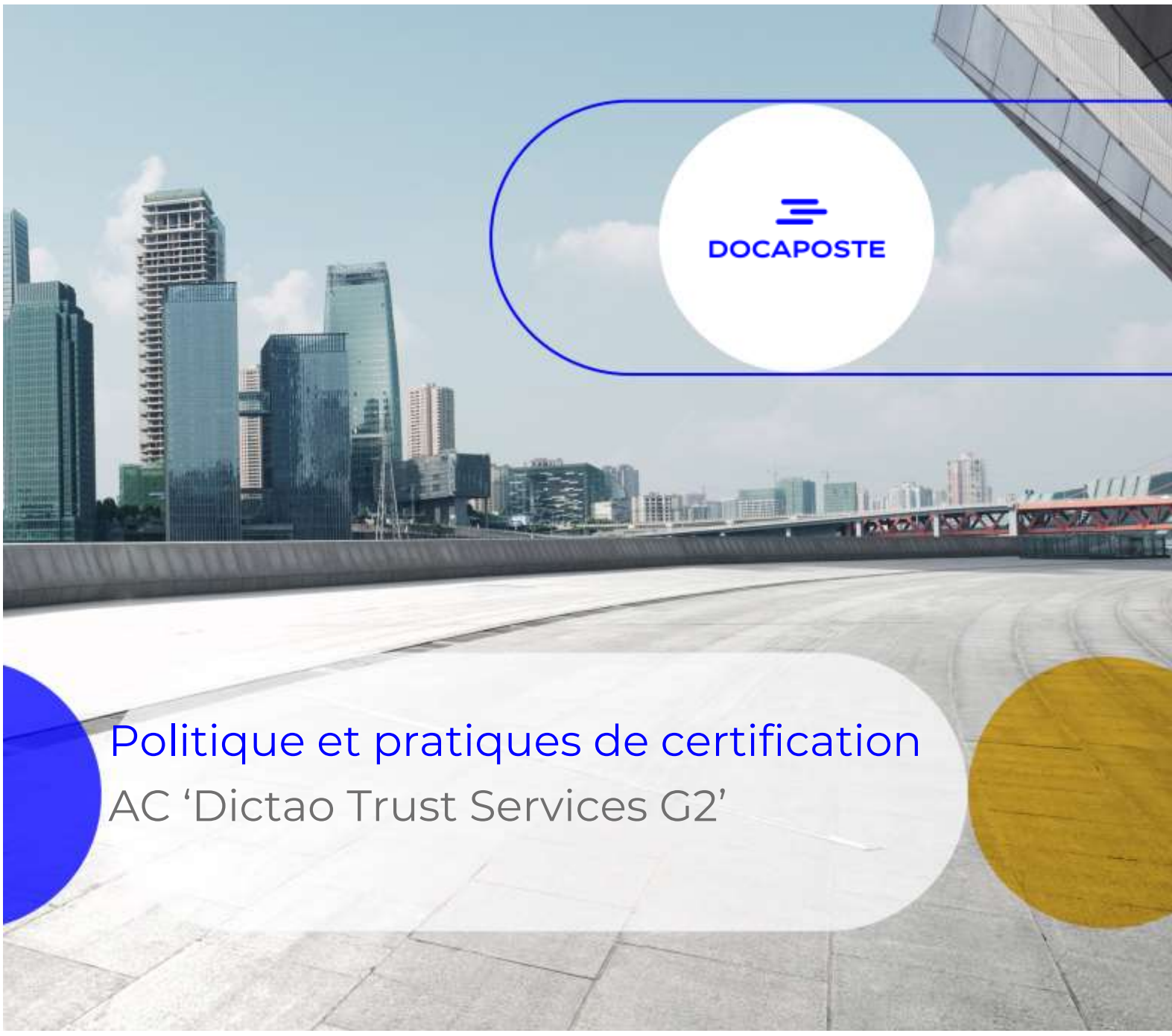
DOCAPOSTE

l'avenir devient plus simple



Politique et pratiques de certification

AC 'Dictao Trust Services G2'

Fichier	dictao-trust-services-cp-g2.pdf
Date	18/11/2021
Référence/version	V1.4
Dossier consultation N°	sans objet

Historique

Version	Auteur	Objet
1.0	IDEMIA I&S	Version initiale du document.
1.1	DOCAPOSTE T&S	Transfert vers DOCAPOSTE T&S Ajout de l'AC Dictao Trust Services User 03 CA G2
1.2	DOCAPOSTE T&S	Remplacement de l'AC Dictao Trust Services User 03 CA G2 par AC Dictao Trust Services User 04 CA G2
1.3	DOCAPOSTE T&S	Ajout des certificats cachet plus et horodatage
1.4	DOCAPOSTE T&S	Révision pour conformité complète aux procédures Docaposte

Acronymes

Acronyme	Définition
API	Application Programming Interface
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished name
DTS	DOCAPOSTE Trust & Sign
IANA	Internet Assigned Numbers Authority
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
PEN	Private Enterprise Number
PEM	Privacy-Enhanced Mail
QSCD	Qualified Signature and Seal Creation Device
RA	Registration authority
SIREN	Système d'identification du répertoire des entreprises
SN	Serial Number
TSU	Time-Stamping Unit
WS	Web Service

Objet

Le présent document décrit les procédures opérationnelles d'enregistrement de l'AC 'Dictao Trust Services G2' (DTS G2) de Docaposte Trust & Sign en vue d'émettre :

- **Des certificats de scellement**
- **Des certificats d'horodatage**
- **Des certificats de signature de personne physique à durée de vie courte**

Elle couvre en particulier toutes les opérations relatives à l'identification

TABLE DES MATIERES

1 INTRODUCTION

Le présent document décrit les procédures opérationnelles d'enregistrement de l'AC 'Dictao Trust Services G2' (DTS G2) de Docaposte Trust & Sign en vue d'émettre :

- Des certificats de scellement
- Des certificats d'horodatage
- Des certificats de signature de personne physique à durée de vie courte

Elle couvre en particulier toutes les opérations relatives à l'identification.

1.1 Préambule

Le 2 Janvier 2015 a été réalisé la dissolution avec transmission universelle de patrimoine de la société Dictao à la société Idemia Identity & Security France, société par actions simplifiées, dont le siège social est domicilié au 2 Place Samuel de Champlain, 92400 Courbevoie, immatriculé au RCS de Nanterre, sous le numéro 440 305 282 .

Suite à cela, l'ensemble des contrats conclus par Dictao avec ses clients et prestataires ont été transmis à Idemia Identity & Security France (société appartenant au groupe IDEMIA et dénommée comme tel par la suite), qui lui a succédé tant aux titres de ses droits que ses obligations, dans le strict respect des conditions contractuelles.

Dictao a été immatriculé au RCS de Paris sous les numéros 429 383 979 et 397 491 184.

Au 31 décembre 2021, les activités de signature électronique de IDEMIA ont été cédées à la société DOCAPOSTE Trust & Sign (société appartenant au groupe DOCAPOSTE), sous le régime juridique des scissions. Les droits et des obligations de Dictao, dans le strict respect des conditions contractuelles ont donc été transférés à Docaposte Trust & Sign.

1.2 Présentation générale

Ce document constitue la Politique de Certification (PC) et la Déclaration des pratiques de certification (*certificate practice statements*, CPS) de l'autorité de certification 'DTS G2' de Docaposte Trust&Sign produisant des certificats électroniques de cachet destinés aux clients de Docaposte Trust&Sign et des certificats de personnes physiques destinés à être utilisés par leur propre clients dans le contexte d'un processus de signature dématérialisé.

Ce document décrit le niveau d'exigence que s'engage à respecter et maintenir l'autorité de certification lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Cette autorité ne vise aucune certification par un auditeur externe.

2 IDENTIFICATION DU DOCUMENT

Le présent document est identifié par l'OID suivant :

1.3.6.1.4.1.54916.1.10.0

Les politiques des profils de certificats décrites dans le présent document sont identifiées par les OID suivante :

Famille	OID
Personne Physique sur l'AC n° 1 (certificat à durée de vie courte)	1.3.6.1.4.1.54916.1.10.1.1
Personne Physique sur l'AC n° 2 (certificat à durée de vie courte)	1.3.6.1.4.1.54916.1.10.2.1
Personne Physique sur l'AC n° 3 (certificat à durée de vie courte)	1.3.6.1.4.1.54916.1.10.4.1
Personne Physique sur l'AC n° 4 (certificat à durée de vie courte)	1.3.6.1.4.1.54916.1.15.4.1
Cachet plus	1.3.6.1.4.1.54916.1.10.3.1
Cachet standard	1.3.6.1.4.1.54916.1.10.5.1
Horodatage	1.3.6.1.4.1.54916.1.10.6.1

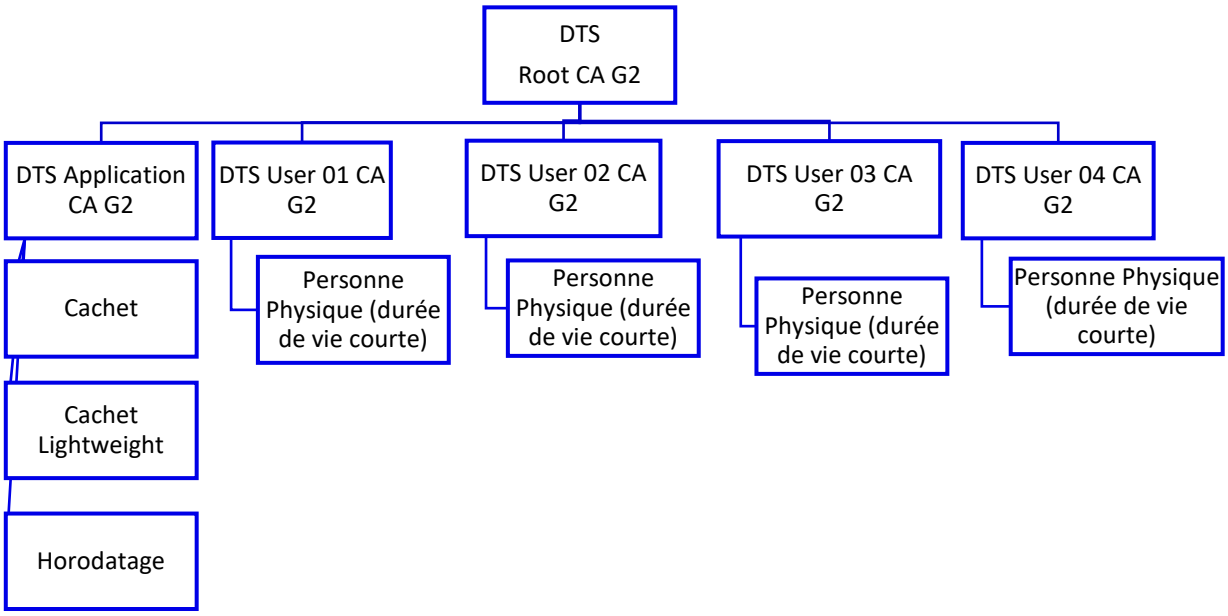
Le numéro d'OID de politique est porté dans les certificats cachet plus et horodatage.

2.1 Entrée en vigueur du document

La présente P.C. s'applique à partir du 23 novembre 2022.

2.2 Entités intervenant dans l'IGC

La hiérarchie d'AC de production est la suivante.

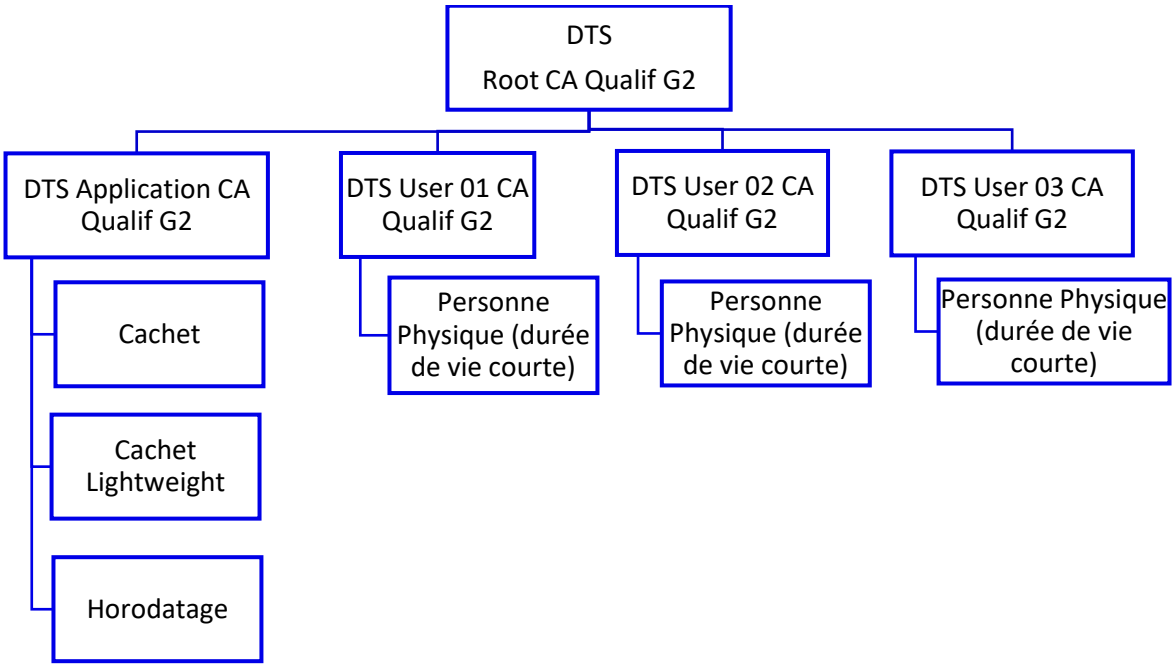


Une hiérarchie d'AC de qualification existe aussi.

La distinction avec l'AC de production se fait à travers la mention Qualif dans le CN de toutes les ac de la hiérarchie.

Aucune des autorités de cette hiérarchie n'est de confiance, elle ne suit aucune procédure spécifique pour le contenu des certificat et l'authentification des personnes Les certificats qu'elle émet doivent donc être utilisés **exclusivement** à des fins de test en interne de Docaposte ou dans les systèmes des clients de Docaposte, sans diffusion au public.

Afin de permettre leur validation à l'identique, ils réutilisent les gabarits et identifiants OID de la hiérarchie de production. La hiérarchie d'AC de qualification est la suivante.



2.2.1 Autorité de Certification

L'autorité de certification 'DTS G2' de Docaposte Trust&Sign est en charge de 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 à clés publiques (IGC).

L'autorité de certification est Docaposte Trust&Sign.

Fonction	Description	Entité responsable
Fonction de génération des certificats	Cette fonction génère (création du format, signature électronique avec la clé privée associée) les certificats en s'appuyant son infrastructure.	Docaposte Trust&Sign
Fonction de remise au porteur	Cette fonction remet au porteur au minimum son certificat ou la chaîne de certification.	Docaposte Trust&Sign
Fonction de publication	Cette fonction met à disposition des différentes parties concernées : les politiques publiées, les certificats d'autorité et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats.	Docaposte Trust&Sign
Fonction de gestion des révocations	Cette fonction traite les demandes de révocation et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.	Docaposte Trust&Sign
Fonction d'information sur l'état des certificats	Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats.	Docaposte Trust&Sign
Fonction d'administration de l'IGC	Cette fonction est associée au rôle qui définit le comportement fonctionnel et le paramétrage technique de l'IGC.	Docaposte Trust&Sign

TABLEAU 1 – DECOMPOSITION FONCTIONNELLE DE L'IGC

Docaposte Trust&Sign pourra opérer directement ou sous-traiter à des tiers chacune des fonctions sous sa responsabilité.

2.2.2 Autorité d'enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du futur porteur de certificat ainsi que des contraintes liées à l'usage du certificat qui lui est délivré, conformément à la politique de certification.

Certificat de cachet plus, cachet standard et d'horodatage
L'AE est portée par Docaposte Trust&Sign

Certificat personne physique
L'AE est opérée par un client de Docaposte Trust&Sign. Dans ce cadre, le client s'engage à réaliser l'authentification et déterminer les informations à porter dans le sujet du certificat de manière conforme aux critères décrits dans le chapitre 4.2.3

2.2.3 Porteurs de certificats

Un porteur de certificat est soit une entité physique qui signe des documents électroniques en son nom, soit une personne morale, représentée par un RC dans le cas des certificats cachet plus et de l'horodatage, qui scelle des documents électroniques en son nom.

Certificat de cachet plus et cachet standard
Il s'agit d'une personne morale, client de Docaposte Trust&Sign

Certificat d'horodatage
Il s'agit de Docaposte Trust&Sign

Certificat personne physique
Il s'agit d'une personne physique.

2.2.4 Responsable de certificat de cachet (RC)

Le RC n'est défini que pour l'émission de certificat de cachet et d'horodatage.

Certificat de cachet plus, cachet standard et d'horodatage
Le RC est la personne physique responsable du certificat de cachet, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat. Cette personne utilise la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité identifiée dans le certificat où cette entité exerce sur elle un lien contractuel d'autorité. Dans le cadre de cette PC, le RC est forcément : ▪ Mandataire social de cette entité ou ▪ Salarié de cette entité ayant reçu délégation de la part du mandataire social Le RC respecte les conditions qui lui incombent telles que définies dans la présente PC. Il est rappelé que le certificat étant attaché au serveur informatique et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc. L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions. L'AC révoque un certificat de cachet pour lequel il n'y a plus de RC explicitement identifié. Les personnels et les clients Docaposte T&S précédemment habilités à servir de RC pour la PKI certifiée Idemia eIDAS dans le périmètre d'une entité donnée sont autorisés à servir de RC au titre de la même entité pour la présente PKI jusqu'à la fin de validité de l'attribution de ce rôle.

2.2.5 Utilisateurs de certificats

Les Utilisateurs sont les personnes physiques et morales destinataires des documents signés, scellés électroniquement ou horodatés, une fois qu'ils ont accepté la réception de ces documents.

2.3 Usage des certificats

2.3.1 Bi-clés et certificats des porteurs

Les restrictions d'utilisation des bi-clés et des certificats sont définies en § 5.5 ci-dessous. L'AC respecte ces restrictions et impose leur respect par ses RC et ses utilisateurs de certificats.

À cette fin, elle publie le présent document qui les contient à destination de tous les signataires, les RC et utilisateurs potentiels.

2.3.2 Bi-clés et certificats d'AC

La clé de l'AC est utilisée pour signer les certificats générés par l'AC et la LCR de l'AC.

2.4 Gestion de la politique de certification

2.4.1 Entité gérant la politique de certification

L'entité en charge de l'administration et de la gestion de la présente politique de certification est Docaposte Trust&Sign (§ 2.2.1). Elle est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

2.4.2 Point de contact

Docaposte Trust&Sign	
Personne à contacter	PKI Information contact DTS G2
Adresse postale	Docaposte Trust&Sign 45-47 Boulevard Paul Vaillant Couturier 94200 Ivry-sur-Seine
Numéro de téléphone	+33 1 56 29 70 01
Adresse email	info@docaposte.fr
Site internet:	http://igc.dictao.com

2.4.3 Procédures d'approbation de la conformité de la PC et de la DPC

Cette PC sera revue a minima à chaque changement majeur.

2.5 Abréviations

Les abréviations utilisées dans la présente P.C. sont les suivantes :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CPS	Certification practice statements (déclaration des pratiques de certification)
CSR	Certificate signing request
CRL	Liste des Certificats Révoqués (Certificate revocation list)
DN	Distinguished Name (nom distinctif)
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
ICD	International Code Designator

IGC	Infrastructure de gestion de clés
LCR	Liste des Certificats Révoqués
OID	Object Identifier (identifiant d'objet)
PC	Politique de Certification
PSCE	Prestataire de Services de Certification Électronique
SIRENE	Système national d'identification et du répertoire des entreprises et de leurs établissements
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator (adresse universelle)

3 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

3.1 Entités chargées de la mise à disposition des informations

Suite à l'approbation des politiques (et, éventuellement, autres informations publiées, cf. ci-dessous) par le comité de suivi de l'AC, le chef de projet fait une demande de publication à l'équipe chargée de la publication des opérations.

3.2 Informations publiées

Le présent document[1]	http://igc.dictao.com/dictao-trust-services-cp-g2.pdf
Les certificats des AC en cours de validité	• User 01 : http://service.dictao.com/dictao-trust-services-user-ca-01-g2.crt • User 02 : http://service.dictao.com/dictao-trust-services-user-ca-02-g2.crt • User 03 : http://service.dictao.com/dictao-trust-services-user-ca-03-g2.crt • User 04 : http://service.dictao.com/dictao-trust-services-user-ca-04-g2.crt • Application : http://igc.dictao.com/dictao-trust-services-application-ca-g2.crt
Le certificat de l'AC racine et son empreinte cryptographique	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt SHA256(dictao-trust-services-root-ca-g2.crt) : bc22a7fec97b5e2c7776e13f4a82acd50e3c885141238074347f011525e20e44
Les certificats des AC de qualification en cours de validité	• User 01 : http://service.dictao.com/dictao-trust-services-user-ca-01-g2-qualif.crt • User 02 : http://service.dictao.com/dictao-trust-services-user-ca-02-g2-qualif.crt • User 03 : http://service.dictao.com/dictao-trust-services-user-ca-03-g2-qualif.crt • User 04 : http://service.dictao.com/dictao-trust-services-user-ca-04-g2-qualif.crt • Application : http://igc.dictao.com/dictao-trust-services-application-ca-g2-qualif.crt
Le certificat de l'AC racine de qualification	http://igc.dictao.com/dictao-trust-services-root-ca-g2-qualif.crt
Les CRL	• User 01 : http://service.dictao.com/dictao-trust-services-user-ca-01-g2.crl • User 02 : http://service.dictao.com/dictao-trust-services-user-ca-02-g2.crl • User 03 : http://service.dictao.com/dictao-trust-services-user-ca-03-g2.crl • User 04 : http://service.dictao.com/dictao-trust-services-user-ca-04-g2.crl • Application : http://igc.dictao.com/dictao-trust-services-application-ca-g2.crl
L'ARL de l'AC racine	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl
Les CRL de qualification	• User 01 : http://service.dictao.com/dictao-trust-services-user-ca-01-g2-qualif.crl • User 02 : http://service.dictao.com/dictao-trust-services-user-ca-02-g2-qualif.crl • User 03 : http://service.dictao.com/dictao-trust-services-user-ca-03-g2-qualif.crl • User 04 : http://service.dictao.com/dictao-trust-services-user-ca-04-g2-qualif.crl
L'ARL de l'AC racine de qualification	http://igc.dictao.com/dictao-trust-services-root-ca-g2-qualif.crl

[1] Version en vigueur et précédentes, le cas échéant

TABLEAU 2 – INFORMATIONS PUBLIEES PAR L'AC

3.3 Délais et fréquences de publication

Les informations liées à la l'autorité de certification d'entités, les systèmes ont une disponibilité de 7 jours sur 7, 24h sur 24. Le SLA assuré sur cette fonction est de 99.8% mensuel.

3.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est en libre accès en lecture. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.

4 IDENTIFICATION ET AUTHENTIFICATION

4.1 Nommage

4.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509 v3 l'autorité émettrice (issuer) et le porteur (subject) sont identifiés par un « Distinguished Name » (DN) de type X.501 structuré comme suit.

Certificat de cachet plus et cachet standard

- CN (Common Name) au format UTF-8. Cette mention est obligatoire. C'est le nom commercial ou public de l'entité morale. Le suffixe « - Test » pourra être ajouté pour émettre un certificat temporaire de démonstration.
- OU (Organizational Unit) au format UTF-8. Il est constitué :
  - Pour les sociétés immatriculées en France, du numéro de SIREN ou de SIRET de l'organisation représentée par le porteur, tel que figurant au Kbis, précédé des caractères « 0002 » (code ICD SIRENE).
  - Pour les autres sociétés Européennes, il est composé :
    - Des caractères « VAT<XX>- » où « <XX> » est remplacé par les deux caractères ISO 3166 du pays d'enregistrement de la société, suivi
    - Du numéro de TVA intra-communautaire de la société
- O (Organization) au format UTF-8. Il est constitué de la raison sociale de l'organisation représentée par le porteur, tel que figurant par exemple au K-Bis.
- C (CountryName) au format PrintableString, contenant le code iso 3166-2 du Pays (FR pour la France)

Certificat d'horodatage

- CN (Common Name) au format UTF-8. Cette mention est obligatoire. C'est le nom de l'unité d'horodatage. Il est de la forme « Docaposte TSUx » avec x un numéro d'ordre incrémental. Optionnellement, le suffixe « - Test » peut être ajouté pour émettre un certificat temporaire de démonstration par exemple.
- OU (Organizational Unit) au format UTF-8. Il est constitué :
  - De la valeur 0002 429383979 identifiant la société Dictao (code ICD SIREN).
- O (Organization) au format UTF-8. Il est constitué de la valeur Dictao, raison sociale de l'organisation représentée par le porteur
- C (CountryName) au format PrintableString, contenant le code iso 3166-2 du Pays (FR pour la France)

Certificat personne physique

Eléments obligatoires :

- CN (Common Name) au format UTF-8 qui est la concaténation du prénom et du nom.
  - Dans le cas du monitoring, la valeur du CN est préfixé par « Monitoring ».

Dans le cas d'usage de test, le suffixe « - Test » sera ajouté au CN initial.

Eléments recommandés :

- C (CountryName) au format PrintableString, contenant le code iso 3166-2 du Pays (FR pour la France)

Eléments optionnels :

- serialNumber : Numéro de série qui permet de garantit l'unicité du nom de l'utilisateur en cas d'homonymie sur le CN.
- emailAddress : Adresse mèl de l'utilisateur

- organizationName : Nom de la société représentée par l'utilisateur. Ne doit être remplit que si l'utilisateur représente cette société au moment où il réalise une signature avec ce certificat personnel. Il est constitué :
    - De la valeur 0002 XXXXXXXXX où XXXXXXXXX identifie la société par son code ICD SIREN.
- organizationalUnitName : Permet de préciser un département de la société dans le cas où l'élément organizationName est utilisé.
- organisationIdentifier : Nom de la société représentée par l'utilisateur au format eIDAS. Il est constitué :
    - De la valeur NTRFR-XXXXXXXXX où XXXXXXXXX identifie la société par son code ICD SIREN.
- givenName : Prénom de l'utilisateur
- surname : Nom de famille de l'utilisateur
-

4.1.2 Nécessité d'utilisation de noms explicites

Les noms des porteurs sont explicites.

4.1.3 Pseudonymisation des porteurs

Les certificats des porteurs ne sont pas pseudonymisés.

4.1.4 Règles d'interprétation des différentes formes de nom

Aucune exigence n'est stipulée en plus des règles spécifiées ci-dessus.

4.1.5 Unicité de Noms

Concernant le sujet d'un certificat,

- Pour un certificat de cachet plus et standard, l'unicité du DN est assurée à l'aide des champs CN et OU.
- Pour un certificat de personne physique,
    - La garantie de l'unicité du DN est sous la responsabilité de l'AE
    - Elle ne sera pas assurée quand l'AE n'inclut que le CN et le C dans le sujet du certificat
    - Elle sera assuré quand l'AE inclut un SerialNumber unique dans le sujet du certificat ou un autre élément qui le garanti comme par exemple emailAddress

4.2 Validation initiale de l'identité

4.2.1 Méthode pour prouver la possession de la clé privée

Pour les certificats cachets, le RC fournit une CSR signée avec la clé privée (format PKCS #10).

Pour les certificats personnels, les clés sont générées par l'application de signature de DOCAPOSTE Trust & Sign qui la transmet de façon sécurisée à l'AC.

4.2.2 Validation de l'identité d'un organisme

Certificat de cachet plus
Elle est vérifiée par l'AC lors de l'enregistrement du RC. Voir ci-dessous.

Certificat de cachet standard
L'organisme est un client établi de Docaposte avec lequel des relations contractuelles sont déjà en place et pour lequel une plateforme de eContracting ou eSeal est déployée. Son identité est vérifiée sur la base des informations déjà connues de Docaposte à ce titre. L'AE vérifie que les informations de l'organisme utilisées sont conformes à celle de l'enregistrement de la société telle que disponible dans les bases officielles en ligne.

Certificat d'horodatage
Les certificats d'horodatage sont destinées exclusivement à l'usage de Docaposte, l'identité est vérifiée lors de l'enregistrement du RC interne.

4.2.3 Validation de l'identité d'un individu

Enregistrement d'un RC

L'enregistrement du futur porteur (personne morale) nécessite l'identification de cette entité et l'identification de la personne physique responsable du certificat (RC), et la preuve du rattachement de la personne physique à l'entité.

S'agissant d'un certificat de cachet, le RC doit de plus être habilité à ce rôle en tant que RC pour le service de création de cachet considéré.

Certificat de cachet plus, cachet standard et d'horodatage
Le dossier d'enregistrement, déposé directement auprès de l'AE, doit au moins comprendre : • Un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le RC auquel le certificat doit être délivré. Ce mandat doit être signé pour acceptation par le RC. • Une demande de certificat écrite, datée de moins de 3 mois, signée par le RC de l'entité et comportant le nom du service de création de cachet concerné par cette demande • Toute pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, …), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ; • Tout document attestant de la qualité du signataire du mandat ; • Une copie d'un document officiel d'identité en cours de validité du RC ou une carte professionnelle délivrée par une autorité administrative, comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ; • Une adresse électronique permettant à l'AC de contacter le RC.

Ces documents sont transmis à l'AC qui les conserve.

L'identité du RC est vérifiée par l'AC en face à face.

Les personnes enregistré précédemment comme RC au titre d'une entité donnée pour la PKI Idemia eIDAS sont autorisées à servir de RC au titre de la même entité pour la présente PKI.

Enregistrement d'une Personne physique

Certificat personne physique
Le dossier d'enregistrement, dématérialisé, comprend : • Une demande de certificat dématérialisée et validée par le porteur

- Optionnellement, une pièce d'identité valide, qui pourra être conservée par l'AE

La vérification de l'identité du porteur est réalisée par l'AE partenaire opérée par le client.
Le client s'assure de la validité de l'identité du ou des signataires, ainsi que de la validité des informations concernant son identité dont il demande l'inclusion dans le sujet du certificat, au travers d'un processus dématérialisé. Il réalise un contrôle de la sécurité de ce processus dématérialisé d'un niveau d'exigence approprié aux risques et des litiges potentiels liés à son cas d'usage.
La demande de certificat dématérialisée est transmise à Docaposte Trust&Sign

4.2.4 Informations non vérifiées du RC

Sans objet.

4.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité du RC pour les politiques certificat de cachet plus..

Pour la politique certificat de cachet standard, l'AE s'assure que le demandeur est l'un des interlocuteurs habituels de Docaposte au sein de l'organisme concerné, ayant un rôle décisionnel dans la plateforme eContracting ou eSeal sur laquelle le certificat va être utilisé.

4.2.6 Certification croisée d'AC

Pas d'exigences en l'état actuel de la PC.

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

Certificat de cachet plus et d'horodatage

Les bi-clés et les certificats de cachet plus sont renouvelés tous les trois ans.
Les bi-clés et les certificats d'horodatage sont renouvelés tous les deux ans.
Le renouvellement de la bi-clé implique la génération d'un nouveau certificat.
Le RC réalise une demande de renouvellement de son certificat selon les modalités d'une demande initiale.
L'AE réalise les vérifications suivantes :

- Existence du certificat à renouveler et vérification de la validité des informations contenues dans la demande de renouvellement certificat (existence de l'entreprise…) à l'identique de la précédente.
- Vérification de l'origine de la demande (identification du RC)

Dans tous les cas, un nouveau certificat ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante.

Certificat de cachet standard

Les bi-clés et les certificats de cachet standard sont renouvelés par défaut tous les trois ans. Leur validité peut être étendue jusqu'à 5 ans.
Le certificat peut éventuellement être régénéré sans modification de la bi-clé si nécessaire pour un besoin client.
Le client réalise une demande de renouvellement de son certificat selon les modalités d'une demande initiale.
L'AE réalise les vérifications suivantes :

- Existence du certificat à renouveler et vérification de la validité des informations contenues dans la demande de renouvellement certificat (existence de l'entreprise…) à l'identique de la précédente.
- Vérification de l'origine de la demande

Certificat personne physique
Non applicable. Les certificats de personne physique étant à durée de vie courte, ils ne font pas l'objet de renouvellement.

4.4 Identification et validation d'une demande de révocation

Certificat de cachet plus et d'horodatage
Le RC et l'AE conviennent, lors de la contractualisation, du moyen à utiliser pour effectuer les demandes de révocation. Ce moyen doit garantir l'authenticité et l'intégrité des demandes. • Lors d'une demande auprès de l'AE, le RC doit s'authentifier. L'opérateur de révocation vérifiera la complétude du dossier conformément aux procédures internes de Docaposte Trust&Sign. • Lors d'une demande par téléphone, l'opérateur de révocation s'assurera de l'identité de son interlocuteur conformément aux procédure interne avant de déclencher la révocation effective du certificat.

Certificat de cachet standard
• La demande de révocation auprès de l'AE peut être réalisée par simple mail du client. L'opérateur de révocation vérifiera l'authenticité de la demande conformément aux procédures internes de Docaposte Trust&Sign. • Lors d'une demande par téléphone, l'opérateur de révocation s'assurera de l'identité de son interlocuteur conformément aux procédure interne avant de déclencher la révocation effective du certificat.

Certificat personne physique
De par sa durée de vie courte, le certificat de personne physique ne fait pas l'objet d'une procédure de révocation.

5 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

5.1 Demande de certificat

5.1.1 Origine d'une demande de certificat

Certificat de cachet plus et d'horodatage
La demande peut être effectuée par le RC, dûment mandaté (cf. § 4.2.3 >).

Certificat de cachet standard
La demande peut être effectuée par le client identifié de la plateforme eContracting ou eSeal où le certificat est déployé.

Certificat personne physique
La demande est réalisée par le porteur au cours d'un processus de signature électronique opéré par Docaposte Trust&Sign à la demande d'un de ses clients.

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

Certificat de cachet plus et d'horodatage
Une fois la demande déposée, le RC et l'AE conviennent d'un rendez-vous pour l'enregistrement du RC.

Certificat de cachet standard
La demande s'effectue à travers l'ouverture d'un ticket sur le portail de service fourni au client par Docaposte.

Certificat personne physique
Le processus est pris en charge par Docaposte Trust&Sign à travers le processus de signature électronique.

5.2 Traitement d'une demande de certificat

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

Certificat de cachet plus et d'horodatage
La demande et l'identification du RC sont validées comme décrit en § 4.2.2 Docaposte Trust&Sign est en charge de la génération des bi-clés de cachet sur les HSM hébergés par Docaposte Trust&Sign et de la demande technique (CSR) associée. Par ailleurs, l'AE au travers des opérateurs d'enregistrement, vérifie les paramètres des bi-clés générés par les administrateurs système (taille et module, dans le cas d'une bi-clé RSA).

Certificat de cachet standard
La demande et l'identification du client sont validées comme décrit en § 4.2.2

Docaposte Trust&Sign est en charge de la génération des bi-clés de cachet sur les HSM hébergés par Docaposte Trust&Sign et de la demande technique (CSR) associée.
Par ailleurs, l'AE au travers des opérateurs d'enregistrement, vérifie les paramètres des bi-clés générés par les administrateurs système (taille et module, dans le cas d'une bi-clé RSA).

Certificat personne physique

Le processus d'identification décrit en § 4.2.3 est réalisé par un opérateur de l'AE.
Docaposte Trust&Sign est en charge de la génération des bi-clés de personne physique en logiciel dans l'application de signature Docaposte Trust&Sign.

5.2.2 Acceptation ou rejet de la demande

Certificat de cachet plus et d'horodatage

La demande est acceptée ou rejetée par l'AE Docaposte Trust&Sign lors de l'échange avec le RC.
En cas de rejet, le RC en est informé directement par l'AE.

Certificat de cachet standard

La demande est acceptée ou rejetée par l'AE Docaposte Trust&Sign lors du traitement du ticket de service.
En cas de rejet, le client en est informé directement par l'AE dans le ticket.

Certificat personne physique

La demande est acceptée ou rejetée par l'AE Partenaire en fonction du processus de vérification auquel elle s'est engagée suivant les critères du paragraphe 4.2.3.

5.2.3 Durée d'établissement du certificat

Certificat de cachet plus, de cachet standard et d'horodatage

Le certificat est produit par l'AC dans un délai maximal de dix jours ouvrés après la validation par l'AE.

Certificat personne physique

Le certificat est établi immédiatement au cours du processus de signature électronique.

5.3 Délivrance du certificat

5.3.1 Actions de l'AC concernant la délivrance du certificat

Certificat de cachet plus et d'horodatage

L'AC génère le certificat au format X509 et le met à disposition du RC.

Certificat de cachet standard

L'AC génère le certificat au format X509 et le met à disposition du client dans le ticket de service

Certificat personne physique

Le certificat est transmis à l'application de signature et inclus dans le document signé remis à l'utilisateur.

5.3.2 Notification par l'AC de la délivrance du certificat au RC

Certificat de cachet plus et d'horodatage
Le RC est informé par courrier électronique de la mise à disposition du certificat, à l'adresse fournie dans la demande.

Certificat de cachet standard
Le client doit consulter le ticket de service pour vérifier la délivrance du certificat.

Certificat personne physique
Le porteur est notifié à travers la réussite du processus de signature.

5.4 Acceptation du certificat

5.4.1 Démarche d'acceptation du certificat

Certificat de cachet plus, de cachet standard et d'horodatage
Le certificat est présenté au client ou au RC afin d'être accepté explicitement. En cas de refus, le certificat fera l'objet d'une demande de révocation.

Certificat personne physique
Le certificat est implicitement accepté lors de son utilisation s'il ne l'a pas été explicitement précédemment.

5.4.2 Publication du certificat

Les certificats des porteurs ne sont pas publiés par l'AC.

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

Sans objet.

5.5 Usages de la bi-clé et du certificat

5.5.1 Utilisation de la clé privée et du certificat par le RC

Les RC doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des clés.

Certificat de cachet plus et standard
L'utilisation de la clé privée et du certificat est strictement limitée à la production de cachets électroniques.

Certificat d'horodatage
L'utilisation de la clé privée et du certificat est strictement limitée à la production de jetons d'horodatage.

Certificat personne physique
L'utilisation de la clé privée est strictement limitée à la création de signatures électroniques dans le cadre d'un processus de signature opéré dans le cadre d'un service Saas de Docaposte Trust&Sign.

5.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

La présente PC ne formule aucune exigence sur ce point.

5.6 Renouvellement d'un certificat

La notion de renouvellement de certificat, au sens RFC 3647, correspondant à la seule modification des dates de validité, n'est pas retenue pour les certificats cachet plus et horodatage. Seule la délivrance d'un nouveau certificat suite à changement de la bi-clé est autorisée.

Le renouvellement des certificats d'AC, ainsi que des certificats cachets standard, pourra être effectué si l'entité responsable de l'autorité de certification détermine que le niveau de sécurité des algorithmes utilisés est toujours conforme au niveau de sécurité nécessaire à la fin de la période de validité initiale.

5.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Certificat de cachet plus, de cachet standard et d'horordatage
La demande et la délivrance d'un nouveau certificat suite à changement de la bi-clé suit la procédure du paragraphe 4.3

Certificat personne physique
Non applicable

5.8 Modification du certificat

Sans objet ; la modification de certificat n'est pas autorisée par la présente PC.

5.9 Révocation et suspension des certificats

5.9.1 Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat électronique :

- Les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement
- Le RC ou son entité n'ont pas respecté leurs obligations découlant de la présente PC
- La clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées)

- L'arrêt définitif du service applicatif ou la cessation d'activité de l'entité de rattachement du service
- Le RC ou une entité autorisée (représentant légal de l'entité) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support)
- L'expiration de la période autorisée d'utilisation d'un des algorithmes cryptographiques mis en œuvre dans le certificat
- La révocation du certificat d'AC

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

5.9.2 Origine d'une demande de révocation

Certificat de cachet plus
Le certificat peut être révoqué par : • Le RC ; • Le responsable légal de l'entité mentionnée dans le certificat ; • L'AE ou l'AC.

Certificat de cachet standard
Le certificat peut être révoqué par : • Le responsable légal de l'entité mentionnée dans le certificat ; • Le contact de Docaposte chez l'entité mentionnée dans le certificat qui est identifié en 5.1.1; • L'AE ou l'AC.

Certificat d'horodatage
Le certificat peut être révoqué par : • Docaposte; • L'AE ou l'AC.

Certificat personne physique
Le signataire ne peut demander à révoquer son certificat.

5.9.3 Procédure de traitement d'une demande de révocation

Certificat de cachet plus
Le RC peut demander la révocation de son certificat en contactant l'AE selon les modalités qui lui auront été précisées.

Certificat de cachet standard
Le client peut demander la révocation de son certificat en contactant l'AE selon les modalités qui lui auront été précisées.

Certificat personne physique
La révocation du certificat n'est pas prise en compte dans le processus de signature, en cas de refus de signature.

5.9.4 Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (ou une personne autorisée) ou l'utilisateur d'un certificat cachet signataire a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

5.9.5 Délai de traitement par l'AC d'une demande de révocation

Certificat de cachet plus ou d'horodatage
Toute demande de révocation est traitée le plus rapidement possible, dans un délai maximum de 72h entre la réception de la demande et son traitement (acceptation ou refus de la demande). Le RC est notifié de la révocation effective du certificat de cachet. Les demandes de révocation sont archivées par l'AC après traitement

Certificat de cachet standard
Toute demande de révocation est traitée le plus rapidement possible entre la réception de la demande et son traitement (acceptation ou refus de la demande). Le client est notifié de la révocation effective du certificat de cachet. Les demandes de révocation sont archivées par l'AC après traitement

Certificat personne physique
Sans objet.

5.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

5.9.7 Fréquence d'établissement des LCR

Les LCR sont publiées toutes les 24 heures.

5.9.8 Délai maximum de publication d'une LCR

Une LCR est publiée au plus 60 minutes après sa génération.

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

Sans objet.

5.9.10 Autres moyens disponibles d'information sur les révocations

Sans objet.

5.9.11 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats cachet, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Quant au porteur, l'AC impose par voie contractuelle qu'en cas de compromission de sa clé privée du porteur ou de connaissance de la compromission de la clé privée de l'AC, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

5.9.12Suspension de certificats

Sans objet ; la suspension des certificats n'est pas autorisée par la présente PC.

5.10 Fonction d'information sur l'état des certificats

5.10.1 Disponibilité de la fonction

Cette fonction à un niveau de disponibilité de 99.8% mensuel.

5.10.2 Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle ou hiérarchique entre l'AC et l'entité de rattachement du certificat avant sa fin de validité, pour une raison ou pour une autre, ce dernier est révoqué.

5.11 Séquestre de clé et recouvrement

Sans objet, il n'est procédé à aucun séquestre ni recouvrement des clés privées des RC.

Il n'est procédé à aucun séquestre ni recouvrement des clés d'AC.

6 MESURES DE SECURITE NON TECHNIQUES

Se référer au document « dictao-trust-cp-measures.pdf »

7 MESURES DE SECURITE TECHNIQUES

Se référer au document « *dictao-trust-cp-measures.pdf* ». Ce chapitre ne décrit que les particularités de la présente PC quant à la gestion des bi-clés et certificats des porteurs.

7.1 Génération des bi-clés et installation

7.1.1 Transmission de la clé privée à son propriétaire

Les clés des certificats des signataires sont directement générées dans un environnement sécurisé opéré par Docaposte Trust&Sign.

7.1.2 Transmission de la clé publique à l'AC

Les modes de transmission de la clé publique des porteurs sont définis dans la procédure de demande de certificat (§ 4.2).

7.1.3 Taille des clés

Les tailles de clés sont les suivantes :

AC	Certificat cachet	Certificat Horodatage	Certificat personne physique
RSA 2048 / 4096	RSA 2048 / 4096	RSA 2048 / 4096	RSA 2048

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

Les clés privées des certificats sont générées dans un environnement sécurisé opéré par Docaposte Trust&Sign qui contrôle ainsi les paramètres utilisés et leur qualité.

7.1.5 Objectifs d'usage de la clé

Pour les certificats des porteurs, voir §2.3.1

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

Certificat de cachet plus, cachet standard et horodatage
Les clés privées sont protégées par les modules cryptographiques conforme à la norme FIPS 140-2 level 2 ou critères communs EAL4+.

L'activation de la clé privée pour déclencher un scellement ne peut être réalisée qu'après l'authentification de l'organisation à l'aide d'un certificat client TLS.

Certificat personne physique
La clé privée est protégée par un environnement sécurisé et est détruite après son utilisation. La clé privée ne peut être activée qu'après une authentification du signataire. La méthode d'authentification mise en œuvre doit être approuvée par Docaposte Trust&Sign.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

Pas d'exigence particulière concernant les clés des porteurs.

7.3.2 Durées de vie des bi-clés et des certificats

Le tableau suivant fournit les durées de vie

Type de certificat	Durée de vie de la bi-clé	Durée de vie du certificat
AC	Jusu'à 16 ans	Idem biclé, jusqu'à 16 ans
Certificat cachet plus et cachet standard	Jusqu'à 5 ans	Idem biclé, jusqu'à 5 ans
Certificat horodatage	2 ans	2 ans
Certificat de personne physique	20 minutes	20 minutes

8 PROFILS

8.1 Profil des certificats

Les certificats émis respectent la norme X.509 v3. Les champs et extensions sont ceux définis dans la RFC 5280.

8.1.1 Autorité de Certification 'DTS Root CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	18:2f:c0:21:88:11:c1:4c:b4:ac:9f:53:2f:23:ea:50:4a:54:d0:de
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	May 21 07:46:22 2010 GMT
Not After	Dec 25 12:00:00 2026 GMT
Subject	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Public Key Algorithm	rsaEncryption
Key length	2048 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE
Subject Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Key Usage	Critical Certificate Sign, CRL Sign

8.1.2 Autorité de Certification 'DTS Application CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	68:00:bd:e6:94:67:80:98:63:ec:59:9e:0f:13:ec:9c:b9:f8:7b:87
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	May 21 07:47:48 2010 GMT
Not After	Dec 25 12:00:00 2026 GMT
Subject	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Application CA G2
Public Key Algorithm	rsaEncryption
Key length	2048 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE Pathlen: 0
Key Usage	Critical Certificate Sign, CRL Sign
Subject Key Identifier	Méthode 1 : E9:99:63:83:CA:61:90:EE:17:E1:16:F5:1D:26:55:5D:FE:56:F5:1B
Authority Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl

8.1.3 Autorité de Certification 'DTS User 01 CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	52:6b:65:80:07:00:c5:bf:f9:40:23:ed:61:00:46:f9:ee:53:9a:99
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	Mar 29 13:10:26 2017 GMT
Not After	Dec 25 12:00:00 2026 GMT
Subject	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 01 CA G2
Public Key Algorithm	rsaEncryption
Key length	4096 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE Pathlen: 0
Key Usage	Critical Certificate Sign, CRL Sign
Subject Key Identifier	Méthode 1 : 96:C9:25:56:C2:79:80:30:69:99:87:A3:CC:98:E0:7F:11:FA:00:5E
Authority Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl

8.1.4 Autorité de Certification 'DTS User 02 CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	5f:84:ab:aa:9a:45:36:82:77:57:23:81:cd:fa:d9:c4:1d:ca:cb:a8
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	Mar 29 13:10:26 2017 GMT
Not After	Dec 25 12:00:00 2026 GMT
Subject	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 02 CA G2
Public Key Algorithm	rsaEncryption
Key length	4096 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE Pathlen: 0
Key Usage	Critical Certificate Sign, CRL Sign
Subject Key Identifier	Méthode 1 : 59:7F:4C:F9:31:23:94:F8:7E:9F:44:C6:E8:B3:C0:B3:05:82:B6:87
Authority Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl

8.1.5 Autorité de Certification 'DTS User 03 CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	36:1a:ff:81:72:ed:01:2f
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	Mai 31 30 12:46:57 2022 GMT
Not After	Jul 14 14:00:00 2025 GMT
Subject	C = FR L = Paris O = Docaposte OU = 0002 429383979 CN = Dictao Trust Services User 04 CA G2
Public Key Algorithm	rsaEncryption
Key length	4096 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE
Key Usage	Critical Digital Signature, Certificate Sign, CRL Sign
Subject Key Identifier	Méthode 1 : 34 :29 :91 :a4 :57 :4e :52 :3b :d3 :ee :df :6a :81 :df :39 :02 :a4 :18 :7f :e6
Authority Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl

8.1.6 Autorité de Certification 'DTS User 04 CA G2'

Attribut	Valeur
Version	3 (0x2)
Serial Number	36:1a:ff:81:72:ed:01:2f
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Not Before	Mai 31 30 12:46:57 2022 GMT
Not After	Jul 14 14:00:00 2025 GMT
Subject	C = FR L = Paris O = Docaposte OU = 0002 429383979 CN = Dictao Trust Services User 04 CA G2
Public Key Algorithm	rsaEncryption
Key length	4096 bit

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:TRUE
Key Usage	Critical Digital Signature, Certificate Sign, CRL Sign
Subject Key Identifier	Méthode 1 : 34 :29 :91 :a4 :57 :4e :52 :3b :d3 :ee :df :6a :81 :df :39 :02 :a4 :18 :7f :e6
Authority Key Identifier	Méthode 1 : AA:4D:CC:BA:C2:64:47:55:A7:1D:EC:72:41:E2:7C:2F:46:45:23:60
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-root-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-root-ca-g2.crl

8.1.7 Certificat Cachet plus

Attribut	Valeur
Version	3 (0x2)
Serial Number	9 ou 19 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Application CA G2
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 5 ansI)
Subject	C=<Pays> O=<Raison sociale> OU=<Semantique ICD> CN=<Nom entreprise / Service>
Public Key Algorithm	rsaEncryption
Key length	2048 bits
Extension X.509 v3	**Valeur**
Basic Constraints	CA:FALSE
Authority Key Identifier	Méthode 1
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-application-ca-g2.crt
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.10.3.1 CPS : http://igc.dictao.com/dictao-trust-services-cp-g2.pdf
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-application-ca-g2.crl
Subject Key Identifier	Méthode 1
Key Usage	Critical Digital Signature

8.1.8 Certificat Cachet standard

Attribut	Valeur
Version	3 (0x2)
Serial Number	9 ou 19 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Application CA G2
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 5 ans)
Subject	C=<Pays> L=<Ville> O=<Raison sociale> OU=<Semantique ICD> CN=<Nom entreprise / Service>
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Basic Constraints	CA:FALSE
Authority Key Identifier	Méthode 1
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-application-ca-g2.crt
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-application-ca-g2.crl
Subject Key Identifier	Méthode 1
Key Usage	Critical Digital Signature

8.1.9 Certificat Horodatage

Attribut	Valeur
Version	3 (0x2)
Serial Number	9 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Application CA G2
Not Before	MM DD HH:MM:SS YYYY GMT
Not After	MM DD HH:MM:SS YYYY GMT (+ 2 ans)
Subject	C= FR L=Paris O=Dictao OU= 0002 429383979 CN=Docaposte TSUx
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Basic Constraints	Critical CA:FALSE
Authority Key Identifier	Méthode 1
Authority Information Access	CA Issuers : http://igc.dictao.com/dictao-trust-services-application-ca-g2.crt
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.10.6.1 CPS : http://igc.dictao.com/dictao-trust-services-cp-g2.pdf
CRL Distribution Points	http://igc.dictao.com/dictao-trust-services-application-ca-g2.crl
Subject Key Identifier	Méthode 1
Key Usage	Critical Digital Signature

Extended Key Usage	Critical Timestamping (1.3.6.1.5.5.7.3.8)

8.1.10 Certificat personne physique (User 01)

Attribut	Valeur
Version	3 (0x2)
Serial Number	19 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 01 CA G2
Not Before	MM DD HH:MM:SS YYYY GMT (T0)
Not After	MM DD HH:MM:SS YYYY GMT (T0 +10mn)
Subject	CN = <Prénom Nom>
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Authority Key Identifier	Méthode 1 : 96:C9:25:56:C2:79:80:30:69:99:87:A3:CC:98:E0:7F:11:FA:00:5E
Authority Information Access	CA Issuers : http://service.dictao.com/dictao-trust-services-user-ca-01-g2.crt
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.10.1.1 CPS : http://igc.dictao.com/dictao-trust-services-cp-g2.pdf
CRL Distribution Points	http://service.dictao.com/dictao-trust-services-user-ca-01-g2.crl
Subject Key Identifier	Méthode 1
Key Usage	Digital Signature, Non Repudiation

8.1.11 Certificat personne physique (User 02)

Attribut	Valeur
Version	3 (0x2)
Serial Number	19 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 02 CA G2
Not Before	MM DD HH:MM:SS YYYY GMT (T0)
Not After	MM DD HH:MM:SS YYYY GMT (T0 +10mn)
Subject	CN = <Prénom Nom>
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Authority Key Identifier	Méthode 1 : 96:C9:25:56:C2:79:80:30:69:99:87:A3:CC:98:E0:7F:11:FA:00:5E
Authority Information Access	CA Issuers : http://service.dictao.com/dictao-trust-services-user-ca-02-g2.crt
Certificate Policies	Policy : 1.3.6.1.4.1.54916.1.10.2.1 CPS : http://igc.dictao.com/dictao-trust-services-cp-g2.pdf
CRL Distribution Points	http://service.dictao.com/dictao-trust-services-user-ca-02-g2.crl
Subject Key Identifier	Méthode 1
Key Usage	Digital Signature, Non Repudiation

8.1.12 Certificat personne physique (User 03)

Attribut	Valeur
Version	3 (0x2)
Serial Number	9 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 03 CA G2
Not Before	MM DD HH:MM:SS YYYY GMT (T0)
Not After	MM DD HH:MM:SS YYYY GMT (T0 +20mn)
Subject	CN = <Prénom Nom> (Obligatoire) givenName = <Prénom Nom> (Optionnel) surname <Prénom Nom> (Optionnel) SN = XXXXXXXXXXXX (Optionnel) emailAddress = <adresse mail> (Optionnel) OU = <Organisation unit if applicable> (Optionnel) O = <Organisation if applicable> (Optionnel) OI = <Organisation if applicable> (Optionnel) C = FR (Recommandé)
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Authority Key Identifier	Key Identifier : Méthode 1 : 34:29:91:a4:57:4e:52:3b:d3:ee:df:6a:81:df:39:02:a4:18:7f:e6 Issuer name and Serial number
Subject Key Identifier	Méthode 1
CRL Distribution Points	http://service.dictao.com/dictao-trust-services-user-ca-03-g2.crl
Key Usage	Digital Signature, Non Repudiation, Encryption
Basic Constraints	CA:FALSE

8.1.13 Certificat personne physique (User 04)

Attribut	Valeur
Version	3 (0x2)
Serial Number	9 octets
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 04 CA G2
Not Before	MM DD HH:MM:SS YYYY GMT (T0)
Not After	MM DD HH:MM:SS YYYY GMT (T0 +20mn)
Subject	CN = <Prénom Nom> (Obligatoire) givenName = <Prénom Nom> (Optionnel) surname <Prénom Nom> (Optionnel) SN = XXXXXXXXXXXX (Optionnel) emailAddress = <adresse mail> (Optionnel) OU = <Organisation unit if applicable> (Optionnel) O = <Organisation if applicable> (Optionnel) OI = <Organisation if applicable> (Optionnel) C = FR (Recommandé)
Public Key Algorithm	rsaEncryption
Key length	2048 bits

Extension X.509 v3	Valeur
Authority Key Identifier	Key Identifier : Méthode 1 : 34:29:91:a4:57:4e:52:3b:d3:ee:df:6a:81:df:39:02:a4:18:7f:e6 Issuer name and Serial number
Subject Key Identifier	Méthode 1
CRL Distribution Points	http://service.dictao.com/dictao-trust-services-user-ca-04-g2.crl
Key Usage	Digital Signature, Non Repudiation, Encryption
Basic Constraints	CA:FALSE

8.2 Profil des CRL

8.2.1 Profil de la CRL 'DTS Root CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Root CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 1 an
Authority Key Identifier	Inclus
Numéro de série	Généré automatiquement par l'AC

8.2.2 Profil de la CRL 'DTS Application CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services Application CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 7 jours
Authority Key Identifier	Inclus
Numéro de série	Généré automatiquement par l'AC

8.2.3 Profil de la CRL 'DTS User 01 CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 01 CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 8 jours
Authority Key Identifier	Inclus
Numéro de série	Généré automatiquement par l'AC
Version de l'autorité	V1.0
Publication de la liste de révocation des certificats suivants (Extension Microsoft)	Date de début de validité + 7 jours

8.2.4 Profil de la CRL 'DTS User 02 CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 397491184 CN = Dictao Trust Services User 02 CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 7 jours
Authority Key Identifier	Inclus
Numéro de série	Généré automatiquement par l'AC
Version de l'autorité	V1.0
Publication de la liste de révocation des certificats suivants (Extension Microsoft)	Date de début de validité + 6 jours

8.2.5 Profil de la CRL 'DTS User 03 CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services User 03 CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 7 jours
Numéro de série	Généré automatiquement par l'AC

8.2.6 Profil de la CRL 'DTS User 04 CA G2'

Champ / Extension	Valeur
Version	2 (0x01)
Algorithme de signature	sha256WithRSAEncryption
Issuer	C = FR L = Paris O = Dictao OU = 0002 429383979 CN = Dictao Trust Services User 04 CA G2
Date de début de validité	Heure de génération
Date de fin de validité (next update)	Date de début de validité + 7 jours
Numéro de série	Généré automatiquement par l'AC

9 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Se référer au document « dictao-trust-cp-measures.pdf ».

10 AUTRES PROBLEMATIQUES METIERS ET LEGALESL

10.1 Tarifs

Sans objet.

10.2 Responsabilité financière

En cas d'inadéquation constatée entre l'utilisation des licences et les droits concédés dans le présent document, les Parties se rapprocheront pour discuter de la bonne foi des conditions financières de régularisation. À défaut d'accord, le CLIENT fera le nécessaire pour revenir aux droits d'utilisation concédés dans les plus brefs délais.

Ces stipulations sont arrêtées sans préjudice de l'indemnisation qui sera due à AC 'DTS G2' en réparation de la violation des conditions d'utilisation des Services par le Client et de l'éventuelle résiliation du Contrat qui pourra intervenir dans les conditions prévues à l'article 20 des présentes.

10.3 Juridictions compétentes

La présente politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique de Certification puissent avoir des effets juridiques en-dehors du territoire de la République française

10.4 Confidentialité des données professionnelles

10.4.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPC correspondant à la présente PC,
- Les clés privées des composantes et des porteurs de certificats de l'IGC de Docaposte Trust&Sign
- Les données d'activation associées aux clés privées des autorités de l'IGC de Docaposte Trust&Sign
- Tous les secrets de l'IGC de Docaposte Trust&Sign
- Les journaux d'événements des composantes des services de confiance de Docaposte Trust&Sign
- Le dossier d'enregistrement des porteurs
- Les causes de révocations, sauf accord explicite de publication ;
- Le procès-verbal de cérémonie de clés.

10.4.2 Informations hors du périmètre des informations confidentielles

Sans objet.

10.4.3 Responsabilités en termes de protection des informations confidentielles

Docaposte Trust&Sign, en tant que fournisseur de services de confiance, est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

10.4.4 Protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'ensemble des services de confiance de Docaposte Trust&Sign sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

10.4.5 Responsabilité en termes de protection des données personnelles

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

10.4.6 Notification et consentement d'utilisation des données personnelles

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

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

Se référer à la législation et à la réglementation en vigueur sur le territoire français.

10.5 Amendements à la PC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente politique de certification.

10.5.1 Procédures d'amendements

L'AC contrôle que tout projet de modification de sa PC reste conforme aux exigences de sécurité nécessaire pour l'opération des services. En cas de changement important, l'AC pourra faire appel à une expertise technique pour en contrôler l'impact.

10.5.2 Mécanisme et période d'information sur les amendements

Le responsable de l'AC informe les bénéficiaires et les tiers utilisateurs lorsque, selon l'évaluation du responsable de la politique, une nouvelle version de la politique qui les impacte est publiée

Le responsable de l'AC donne un préavis aux bénéficiaires et les tiers utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, a un impact sur leurs obligations ou les engagements du service qui leur est rendu. La longueur du préavis est fonction de l'impact et du temps nécessaires pour le prendre en compte pour les bénéficiaires et les tiers utilisateurs.

10.5.3 Circonstances selon lesquelles l'OID doit être changé

Si un changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, des bénéficiaires et/ou de tiers utilisateurs, le responsable de la politique institue une nouvelle politique avec un nouvel identificateur d'objet (OID).

Lorsque le changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur les clients, des bénéficiaires et/ou de tiers utilisateurs d'un des gabarits de certificat de la politique, le responsable de la politique institue un nouvel identifiant de gabarit de certificat avec un nouvel identificateur d'objet (OID).

Lorsqu'un nouveau gabarit de certificat est ajouté à la politique, un nouvel identificateur d'objet (OID) est créé pour le désigner.

10.6 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par Docaposte Trust & Sign sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non-respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet 1998, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par Docaposte Trust & Sign sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr

10.7 Limite de garantie

L'émission de certificats, conformément à la présente Politique de Certification, ne fait pas de l'AC, de l'une des composantes de l'IGC, du responsable de l'AC et du personnel de l'AC et des composantes de l'IGC un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

En conséquence de quoi les Clients et les tiers utilisateurs de certificat sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre. Le contrat ne constitue ni une association, ni une société ou autre groupement, ni un mandat donné par l'une des parties à l'autre.

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients et tiers utilisateurs.

10.8 Limite de responsabilité

L'AC décline absolument toute responsabilité à l'égard de l'usage qui est fait des certificats électroniques qu'elle émet dans des conditions et à des fins autres que celles prévues dans la présente PC, ainsi que dans tout autre document contractuel applicable.

L'AC ne sera en aucun cas tenue responsable des éventuels dommages tant directs qu'indirects, consécutifs ou connexes, ou d'autres réclamations ou obligations quelconques résultant d'un acte délictuel, d'un contrat ou d'une autre cause à l'égard d'un service en relation avec l'émission, l'utilisation ou la fiabilité d'un certificat électronique, offrant un niveau d'assurance selon la classe du certificat ou du bi-clé connexe, au-delà des limites fixées ci-dessous, par l'utilisation, par un bénéficiaire ou un tiers utilisateur. Cette limite de responsabilité s'entend, et de façon non limitative, de tout préjudice financier ou commercial, perte de bénéfices, perte d'exploitation, trouble commercial, manque à gagner, pertes ou actions intentées par un tiers contre le client, trouvant leur origine ou étant la conséquence de la présente déclaration, politiques associées ou autres contrat ou inhérents à l'utilisation ou la fiabilité d'un certificat qu'elle émet.

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'une des parties envers l'autre, les dommages et intérêts et indemnités à sa charge, toutes causes confondues, ne sauraient en aucun cas dépasser les limites de responsabilité mentionnées dans le cadre du contrat conclu entre l'AC et son client.

10.9 Indemnités

Sans objet.

10.10 Conformité aux législations et réglementations

Les pratiques de Docaposte Trust&Sign sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de Docaposte Trust&Sign prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (https://www.w3.org/Translations/WCAG20-fr/).

10.11 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.