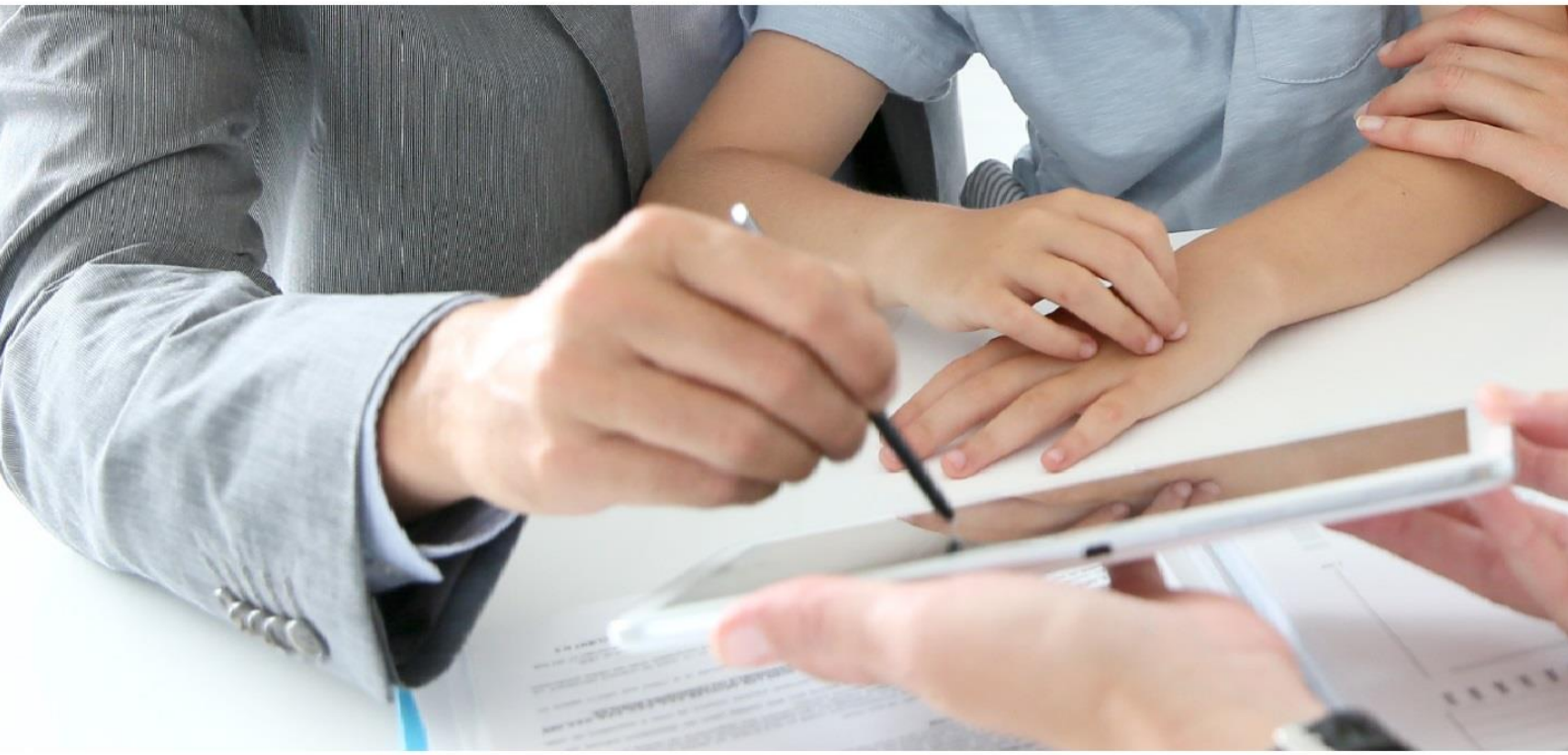
# VIALINK EU STANDARD CA
# Politique et pratiques de certification



**Version : 1.0**
Date de création : 23 Mars 2017
Dernière mise à jour : 24 Mai 2018
État du document : Officiel
Diffusion du document : Public

Vialink
www.vialink.fr
23 Rue Daviel, 75013 Paris

| Liste de diffusion | | |
|---|---|---|
| Personnes | Société | Commentaire |
| Public | / | / |

| Suivi des modifications | | | | |
|---|---|---|---|---|
| Version | Auteur | Contributeur (s) | Modification(s) | Date |
| 1.0 | Comité e-Confiance | Direction Générale | Création du document | 24/05/2018 |

| Documents référencés | | |
|---|---|---|
| Référence | Version | Titre du document |
| [1] | 23/07/2014 | Règlement (UE) No 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit « Règlement eIDAS ». |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# SOMMAIRE





Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'autorisation écrite de Vialink.

# 1 Introduction

**VIALINK** a mis en place une offre de certification pour la sécurisation des transactions sur Internet. Dans ce contexte, **VIALINK** a pour but d'authentifier les participants et de garantir la non-répudiation des transactions. Les certificats, émis par l'AC VIALINK EU STANDARD CA, sont attribués à des personnes physiques, des personnes physiques liées à des entreprises clientes de Vialink, ou des serveurs afin de permettre, l'authentification, la signature ou le cachet électroniques de documents.

## 1.1 Présentation générale

Le présent document constitue la Politique de Certification (PC) et la Déclaration des Pratiques de Certification (DPC) de à l'AC VIALINK EU STANDARD CA. Il décrit les exigences auxquelles l'ICP doit se conformer pour l'enregistrement et la validation des demandes de certificats, et pour la gestion des certificats, ainsi que les moyens publics et pratiques mis en œuvre pour répondre à ces exigences.

| Historique de Politique de Certification | | |
|---|---|---|
| **Version** | **Date** | **Principaux points de modification** |
| 1.0 | 24/05/2018 | Création du document |
| **Date d'entrée en vigueur de Politique de Certification** | | |
| 01 Juin 2018 | | |

## 1.2 Identification du document

Ce document est identifié par le numéro d'OID indiqué ci-dessous pour l'usage considéré :

| Usage du certificat | OID de la PC |
|---|---|
| Certificat de Signature Personne Physique à la volée (5mn) | **1.2.250.1.198.4.1.2.1.0.1** |
| Certificat d'authentification et de Signature Personne Physique 3 ans | **1.2.250.1.198.4.3.2.3.0.1** |
| Certificat de Signature Personne Physique en lien avec une personne morale à la volée (5 mn) | **1.2.250.1.198.4.1.3.1.0.1** |
| Certificat d'authentification et de Signature Personne Physique en lien avec une personne morale 3 ans | **1.2.250.1.198.4.3.3.3.0.1** |
| Certificat de Cachet serveur 3 ans | **1.2.250.1.198.4.4.1.3.0.1** |
| Certificat de Cachet serveur 5 ans | **1.2.250.1.198.4.4.1.4.0.1** |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 1.3 Présentation du service et entités intervenant dans l'IGC

Les échanges d'information entre entreprises requièrent des exigences de confiance propres aux systèmes de communication ouverts : authentification des interlocuteurs, contrôle d'intégrité des informations échangées, non-répudiation des documents conservés, confidentialité des échanges.

Toutes ces fonctions de confiance peuvent être assurées par des outils cryptographiques reposant sur des processus de signature et de chiffrement standard. Ces mécanismes peuvent reposer sur des Infrastructures à Clés Publiques (ci-après appelées ICP, ou PKI pour Public Key Infrastructure) utilisant des certificats numériques comme cartes d'identité numériques.

L'infrastructure à Clés Publiques repose sur les acteurs suivants.

### 1.3.1 Autorité de Certification (AC)

L'Autorité de Certification (AC), définit la Politique de Certification (PC) et la fait appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs.

VIALINK est la société portant l'Autorité de Certification VIALINK EU STANDARD CA.

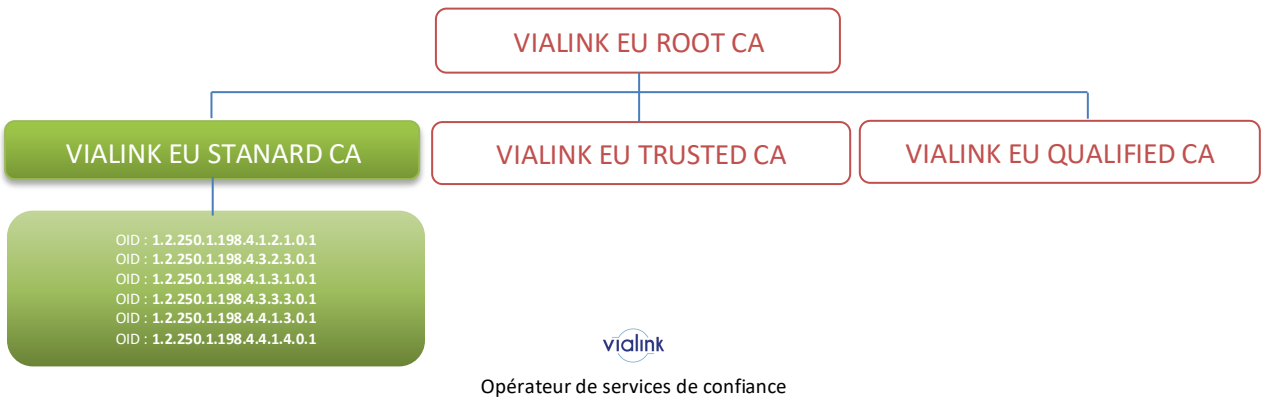
Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de publication des conditions générales d'utilisation, de la PC et des certificats d'AC;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats.

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

Sur le plan technique, l'Autorité de Certification a déployé une hiérarchie de confiance destinée à signer les certificats émis pour l'offre VIALINK EU STANDARD CA.

**Figure 1 – Hiérarchie de confiance**




Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 1.3.2 Autorité d'Enregistrement (AE)

L'Autorité d'Enregistrement a en charge les fonctions suivantes conformément aux règles définies par l'Autorité de Certification :

- L'initiation du dossier de demande ;
- La vérification des informations des demandeurs de certificat, afin de garantir la validité des informations contenues dans le certificat ;
- La constitution du dossier d'enregistrement et de demande suite aux vérifications ci-dessus ;
- L'archivage des dossiers d'enregistrement et de demande de certificat ;
- La vérification des demandes de révocation de certificat.

Les fonctions de vérification des informations du porteur, de constitution puis d'archivage du dossier sont assurées soit directement par Vialink, soit par une entité cliente de Vialink. La vérification des demandes de révocation sont toujours réalisés par Vialink.

La vérification des informations du porteur se fait soit par un face à face, soit de façon automatisée par un portail en ligne sur lequel le porteur fournit ses informations et sa preuve d'identité.

En synthèse, la répartition des fonctions de l'AE est la suivante :

| **Fonction** | **Entité cliente de Vialink** | **Vialink** |
|---|---|---|
| Initiation du dossier de demande | Par une personne habilitée par l'entité cliente | Non |
| Vérification des informations des demandeurs de certificat | En face à face par une personne habilitée par l'entité cliente ou déléguée à l'AE à distance de Vialink | Non |
| Constitution du dossier d'enregistrement et de demande | Suite à toute vérification d'identité réalisée en face à face par l'entité cliente (dossier transmis à Vialink ensuite) | Non |
| Archivage des dossiers | Par l'entité cliente ou par Vialink | Par AC Vialink sur demande de l'entité cliente |
| Vérification des demandes de révocation | Non | Par AC Vialink |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 1.3.3 Opérateur de Certification (OC)

L'Opérateur de Certification (OC) a pour fonction d'assurer la fourniture et la gestion du cycle de vie des certificats. Son rôle consiste à mettre en œuvre une plate-forme opérationnelle, fonctionnelle, sécurisée, dans le respect des exigences énoncées dans la Politique de Certification (PC) et dont les modalités sont détaillées dans la Déclaration des Pratiques de Certification (DPC).

L'opérateur de certification assure les fonctions suivantes :

- Fonction de génération des certificats ;
- Fonction de publication des certificats d'AC ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR).

Les fonctions d'opérateur de certification peuvent être sous-traitées conformément aux exigences de la présente PC.

### 1.3.4 Porteur de certificats

Certificats de personne physique :

Le porteur de certificat est la personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique de ce certificat. Le porteur est titulaire d'un ou plusieurs certificats VIALINK EU STANDARD CA. Le porteur effectue lui-même la demande de certificat pour son compte et à titre personnel ou en lien avec une organisation.

Cette personne utilise la clé privée et le certificat correspondant dans le cadre de ses activités en relation avec l'entité cliente de Vialink lui soumettant le document à signer, et avec laquelle il a un lien contractuel ou réglementaire.

Le porteur respecte les conditions qui lui incombent définies dans cette PC.

Certificats cachet serveur :

Les certificats cachet serveur sont délivrés à des services applicatifs, un certificat cachet serveur doit avoir une personne physique responsable de son utilisation, il s'agit du RCCS : Responsable du Certificat Cachet Serveur).

### 1.3.5 Utilisateurs de certificats

L'utilisateur de certificat est l'entité ou la personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

Les utilisateurs de certificats doivent respecter l'usage des certificats prévu dans cette PC au §1.4, les contraintes d'utilisation détaillées au §4.9.6 et prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document.

## 1.4 Usage des certificats

### 1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des porteurs

Dans le cadre de cette PC, l'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à l'authentification, la signature et le cachet.

Les porteurs doivent respecter strictement ces usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée. Les usages autorisés d'un certificat sont explicitement mentionnés dans celui-ci par le contenu du champ *keyUsage*.

1.4.1.2 Bi-clés et certificats de l'IGC

Plusieurs clés sont utilisées par l'IGC :

- La clé de signature de l'AC VIALINK EU STANDARD CA, utilisée pour :
    - Signer les certificats générés par l'AC ;
    - Signer les informations sur l'état des certificats : Listes de certificats révoqués (LCR);

### 1.4.2 Domaines d'utilisation interdits

VIALINK EU STANDARD CA décline toute responsabilité dans l'usage que ferait un porteur de ses certificats dans le cadre d'une application non mentionnée dans le paragraphe précédent §1.4.1.1. En particulier, VIALINK EU STANDARD CA n'acceptera aucune plainte d'aucune sorte d'usagers ou d'utilisateurs, liée à des litiges sans rapport avec les applications mentionnées dans le présent paragraphe « Usage des certificats ».
Toute utilisation du certificat VIALINK EU STANDARD CA non autorisée dans le paragraphe précédent est interdite.

## 1.5 Gestion de la PC

Cette PC sera revue périodiquement assurer sa conformité aux pratiques en vigueur.
La périodicité de révision de cette PC est fixée à 2 (deux) ans à minima.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 1.5.1 Modification de la PC

L'AC contrôle que tout projet de modification de sa PC reste conforme aux pratiques en vigueur.

Dans un projet de modification, les cas suivants sont envisageables par l'AC VIALINK EU STANDARD CA :

- S'il s'agit de changements typographiques, cela ne donne pas lieu à notification et à modification de l'OID de la PC/DPC ou de l'URL ;
- S'il s'agit de changements quant au niveau de la qualité et de la sécurité des fonctions de l'AC et de l'AE vis-à-vis des certificats référencés, mais sans pour autant perdre la conformité d'un certificat avec la PC qu'il supporte, cela donne lieu à une période de notification d'un mois avant le début des changements sans que soit modifiée l'OID de la PC/DPC ou de l'URL ;
- S'il s'agit de changements entraînant la perte de la conformité d'un certificat avec la PC qu'il supporte, cela implique la modification de l'OID de la PC/DPC. Les spécifications modifiées sont publiées sur le site Internet de l'AC et la notification est effectuée un mois avant de devenir effective. Par ailleurs, l'AC avertit les utilisateurs de certificats, ayant établi des relations contractuelles avec elle, des modifications.
- Si VIALINK estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

### 1.5.2 Coordonnées des entités responsables de la présente PC

#### 1.5.2.1 Organisme responsable

La société VIALINK est responsable de cette PC.

#### 1.5.2.2 Vialink

18 quai de la Rapée
75012 PARIS
France
Service Clients :
Téléphone : +33 (0)1.40.02.91.12
Fax : 01 48.77.78.12
Email : support@vialink.fr


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

#### 1.5.2.3 Personne physique responsable

| |
|---|
| M. Philippe SANCHIS |
| Directeur Général |
| Vialink |
| 18 quai de la Rapée |
| 75012 PARIS |
| France |

### 1.5.3 Contrôle de conformité à la PC

L'Autorité de Certification VIALINK EU STANDARD CA a la responsabilité du bon fonctionnement des composantes de l'IGC, conformément aux dispositions énoncées dans le présent document. L'AC effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement des composantes de cette IGC (cf. chapitre 8).


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

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

## 2.1 Entités chargées de la mise à disposition des informations

L'AC VIALINK EU STANDARD CA diffuse les informations mentionnées au paragraphe suivant via son site Internet www.vialink.fr ou directement sur https://app.vialink.fr/tsp.

## 2.2 Informations publiées

| | |
|---|---|
| La présente politique de certification (PC) | https://app.vialink.fr/tsp |
| Les versions précédentes de la PC | https://app.vialink.fr/tsp |
| Les Listes de Certificats Révoqués (LCR) | http://crl.vialink.fr/vialink/crl-vialink-eu-standard-ca.crl |
| Le certificat d'AC | https://www.vialink.fr/tsp/crt/vialink-eu-standard-ca.crt |
| Les conditions générales du contrat d'utilisation du service | https://app.vialink.fr/tsp |

## 2.3 Fréquence de diffusion

- La Politique de Certification (PC) est mise à jour sur le site après chaque modification. La nouvelle version est communiquée au porteur lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord.
- La fréquence de publication des Listes de Certificats Révoqués (LCR) est précisée au § 4.9.7.
- Le certificat de l'AC est publié initialement et à chaque renouvellement, avant toute émission de certificat porteur.
- La liste de certificats d'AC révoqués (LAR) est publiée initialement et à chaque renouvellement, et en tout état de cause avant sa fin de validité.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 2.4 Contrôle d'accès

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'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.

## 2.5 Dépôt des documents

Les documents mentionnés au paragraphe §2.2 sont publiés via le site Internet de l'AC.
L'ensemble des documents nécessaires au fonctionnement de l'AC est conservé par l'AC, dans leur dernière version, en un lieu centralisé et protégé.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 3 Identification et authentification

## 3.1 Nommage

### 3.1.1 Conventions de noms

Le porteur est identifié dans le champ "Objet" ("*Subject*" en anglais) du certificat émis par VIALINK EU STANDARD CA, par les champs suivants issus de la norme *ETSI EN 319 412* :

Certificat de personne physique :

- E (emailAddress) : contient l'adresse mail de contact du porteur par l'AC et communiquée par le porteur ;
- CN (commonName) : Cette mention est obligatoire. Il est constitué du prénom usuel et du nom patronymique, Ce nom est celui du porteur tel qu'il figure dans ses documents d'identité ;
- SN (surname) : Il est constitué du nom patronymique du porteur tel qu'il figure dans ses documents d'identité ;
- GN (givenName) : Il est constitué du prénom usuel du porteur tel qu'il figure dans ses documents d'identité ;
- O (Organization) : Raison sociale de l'entreprise, uniquement dans le cas où la personne physique est en lien avec une personne morale ;
- OI (organizationIdentifier) : constitué du mot « NTRFR-» suivis du numéro SIREN de l'entreprise, uniquement dans le cas où la personne physique est en lien avec une personne morale ;
- C (countryName) : contenant la chaîne « FR » ou le code du Pays de la pièce d'identité du porteur.

Certificat de cachet serveur :

- E (emailAddress) : contient l'adresse mail de contact du RCCS par l'AC et communiquée par le RCCS ;
- CN (commonName) : Cette mention est obligatoire. Il est constitué du nom du service utilisant le cachet (Exemple : CN = VIALINK SERVICE DE CAUTIONS EN LIGNE) ;
- O (Organization) : Raison sociale de l'entreprise ;
- OI (organizationIdentifier) : constitué du mot « NTRFR-» suivis du numéro SIREN de l'entreprise ;
- C (countryName), contenant la chaîne « FR » ou le code du Pays de la pièce d'identité du porteur.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

Lorsque l'AC VIALINK EU STANDARD CA émet des certificats à des fins de test, ceux-ci sont clairement identifiés par le préfixe « TEST » placé devant le prénom, et donc en début des champs CN et GN pour les certificats de personne physique.

### 3.1.2 Utilisation de noms explicites

Les informations portées dans le champ "Objet" du certificat VIALINK EU STANDARD CA sont explicites ("*Distinguished Name*" en anglais).

### 3.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet. Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes ou pseudonymes.

### 3.1.4 Règles d'interprétation des différentes formes de noms

Aucune interprétation particulière n'est à faire des informations portées dans le champ "Objet" des certificats VIALINK EU STANDARD CA.

Ces informations sont établies par l'AE de VIALINK EU STANDARD CA selon les règles suivantes :

- Tous les caractères sont au format *UTF-8* mis à part les champs *serialNumber* et *CountryName* qui sont en *PrintableString*.

### 3.1.5 Unicité des noms

Le DN du porteur d'un certificat identifie de façon unique ce porteur/RCCS (même par rapport à des homonymes) grâce au champ emailAddress communiqué.

### 3.1.6 Procédure de résolution de litige sur déclaration de nom

L'AC s'engage quant à l'unicité des noms de ses utilisateurs, et quant à la résolution des litiges portant sur la revendication d'utilisation d'un nom conformément aux informations d'unicité précisées ci-dessus.

### 3.1.7 Reconnaissance, authentification et rôle des noms de marques

Sans objet (les noms de marque ne figurent pas au sein des certificats VIALINK EU STANDARD CA).


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 3.2 Validation initiale de l'identité

Dans le cadre de la présente PC, l'AC s'appuiera sur les informations communiquées par l'AE pour délivrer les certificats sur une base déclarative.

### 3.2.1 Méthode pour prouver la possession de la clé privée

Voir § 6.1.

### 3.2.2 Validation de l'identité d'un organisme

Sans objet.

### 3.2.3 Validation de l'identité d'un individu

L'authentification des porteurs est du ressort de l'AE.

Le porteur / RCCS fournit au minimum les informations suivantes à l'AE :

- Son nom et son prénom tels qu'ils apparaissent sur ses documents d'identité ;
- Une adresse courriel à laquelle l'AC peut le joindre ;
- Numéro SIREN de l'organisation à laquelle il appartient ;

L'AC recommande à l'AE de valider l'exactitude de l'identité de la personne (nom, prénom) par l'examen d'une pièce d'identité présentée (ou de sa copie s'il n'y a pas de face à face). Les pièces d'identité recommandée sont les titres authentiques et dans leur période de validité parmi :

- Carte nationale d'identité ;
- Passeport ;
- Carte de séjour ;

L'AC valide par ailleurs que le porteur a bien accès au numéro de téléphone par un challenge envoyé éventuellement par SMS, ce challenge peut être envoyé à l'adresse mail communiquée par le porteur.

### 3.2.4 Validation de l'autorité du demandeur

L'authentification de l'autorité du demandeur est du ressort de l'AE.

L'AC recommande à l'AE de valider l'autorité du demandeur par l'examen de :

- Toute pièce valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements ou inscription au répertoire des métiers, …), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci, ou, à


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat.

- La photocopie d'un document officiel d'identité en cours de validité du demandeur comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour).
- L'existence d'un lien entre l'organisation et le demandeur.

Cette vérification n'est pas obligatoire dans le cas ou le porteur est une personne physique agissant en son nom propre et demandant un certificat pour elle-même.

### 3.2.5 Certification croisée d'AC

Sans objet. L'AC VIALINK EU STANDARD CA n'a aucun accord de reconnaissance avec une autre AC.

## 3.3 Identification et validation d'une demande de renouvellement

Sans objet.

## 3.4 Identification et validation d'une demande de révocation

Lorsque le porteur demande la révocation de son certificat, il saisit son nom, son prénom et l'adresse mail renseignée à la demande du certificat. L'AC l'authentifie par l'envoi d'un lien unique sur cette adresse.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 4 Exigences opérationnelles sur le cycle de vie des certificats

## 4.1 Demande de certificat

### 4.1.1 Origine d'une demande de certificat

La demande et la délivrance du certificat sont effectuées dans le cadre d'une transaction commerciale ou administrative (p. ex., signature de contrat) initiée dans une entité cliente de Vialink.

Un collaborateur de cette entité, dûment authentifié sur le système de signature, saisit au minimum :

- Le nom et le prénom du signataire, qui sera le demandeur du certificat ;
- L'adresse courriel du signataire ;
- Le numéro SIREN de l'organisation ;

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

L'AC s'appuiera sur les informations communiquées par l'AE pour délivrer le certificat sur base déclarative. Dans le cadre de la présente PC, la validation de l'identité est toujours réalisée par le client de Vialink, le client de Vialink est donc une Autorité d'Enregistrement (AE), l'AC recommande l'AE le contrôle de la demande de certificat conformément à la section 3.2, l'opérateur AE est le collaborateur du client de Vialink ayant initié le processus. Ce collaborateur du client de Vialink est responsable de la vérification de l'identité du demandeur et de la constitution du dossier d'enregistrement et l'AC recommande de le faire comme suit :

i. Le demandeur remet à l'AE une copie lisible de sa pièce d'identité ;
ii. L'AE valide l'authenticité et la validité de la pièce et l'exactitude des informations (nom, prénom) saisies au début du processus ;
iii. L'AE ajoute la pièce d'identité du demandeur au dossier d'enregistrement, en certifiant sa validité et son exactitude par rapport à la demande. Selon l'accord existant entre l'entité cliente et l'AC, soit le dossier est transmis intégralement en ligne à l'AC, soit l'entité cliente conserve et archive le dossier et transmet en ligne à l'AC la demande sans la copie de la pièce d'identité ;

Suite à cette validation d'identité, le processus se poursuit avec la délivrance du certificat.

## 4.2 Traitement d'une demande de certificat

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

L'identification et la validation de la demande se font comme indiqué au chapitre 4.1.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 4.2.2 Rejet de la demande de certificat

L'AE peut rejeter une demande de certificat notamment pour l'une des raisons suivantes :

a. En cas d'incohérence entre l'identité du demandeur et les pièces présentées ;
b. Si la pièce d'identité n'est plus valide ;
c. S'il existe un doute sur l'authenticité des pièces.

Dans tous ces cas, la demande n'est pas transmise à l'AC. Un message est affiché au demandeur ou un courriel lui est envoyé pour l'en informer.

L'AC peut rejeter une demande de certificat notamment pour l'une des raisons suivantes :

a. En cas de non acceptation des CGU ;
b. Si le code unique éventuel retourné à l'AC n'est pas identique à celui qui a été envoyé par l'AC.

### 4.2.3 Durée d'établissement du certificat

Le certificat est produit immédiatement après la vérification du code unique éventuel retourné par le porteur à l'AC.

## 4.3 Délivrance du certificat

### 4.3.1 Actions de l'AC concernant la délivrance du certificat

L'AC génère la bi-clé de et le certificat et les transmet à l'AE (service de signature, personnes physiques, …).

### 4.3.2 Notification par l'AC de la délivrance du certificat au porteur

Sans objet.

## 4.4 Acceptation du certificat

### 4.4.1 Démarche d'acceptation du certificat

Le demandeur accepte son certificat.

Si le porteur n'accepte pas le certificat, il doit le signaler auprès de l'AE qui a l'obligation de révoquer le certificat conformément aux procédures décrite dans le présent document.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 4.4.2 Publication du certificat

Les certificats ne font l'objet d'aucune publication par l'AC.

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

Sans objet.

## 4.5 Usages de la bi-clé et du certificat

### 4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux usages définis au §1.4.1.1 et au §1.3.4. En pratique, le porteur ne dispose pas de moyen d'utiliser sa clé pour un autre usage. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

Les utilisateurs de certificats vérifient la signature/cachet des documents grâce au certificat intégré dans le document signé/cacheté. Ils doivent respecter strictement les usages autorisés des certificats définis au §1.4.1.1 et les contraintes du §1.3.5. Dans le cas contraire, leur responsabilité pourrait être engagée.

## 4.6 Renouvellement d'un certificat

Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

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

### 4.7.1 Certificat porteur

Un porteur peut demander un nouveau certificat pour effectuer la signature d'un nouveau document, selon un processus exactement identique au certificat initial.

### 4.7.2 Renouvellement du certificat de l'AC

La période de validité de la clé de l'AC est de dix ans. L'AC ne peut pas émettre de certificat dont la date de fin de validité serait postérieure à la date d'expiration de la bi-clé de l'AC. Par conséquent, la période de validité de la clé de l'AC doit être supérieure à celle des certificats d'utilisateurs.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

L'AC doit donc disposer d'une nouvelle bi-clé trois ans avant l'expiration de son certificat (cette durée correspondant à la plus longue durée de validité parmi tous les certificats émis).

Pendant cette période de trois ans, l'AC disposera alors de deux certificats correspondant à deux bi-clés.

Les certificats d'utilisateurs émis au cours de cette période seront signés par la clé privée de la nouvelle bi-clé de l'AC. La précédente bi-clé n'est alors plus utilisée que pour signer les Listes de Certificats Révoqués concernant les certificats signés par celle-ci et ce jusqu'à la fin de validité du certificat de l'AC correspondant à ce bi-clé.

Ainsi deux Listes de Certificats Révoqués seront maintenues conjointement pendant ces trois années.

## 4.8 Modification du certificat

La modification des certificats émis par l'AC VIALINK EU STANDARD CA n'est pas autorisée.

## 4.9 Révocation et suspension des certificats

### 4.9.1 Causes possibles d'une révocation

#### 4.9.1.1 Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- Les modalités d'utilisation du certificat n'ont pas été respectées ;
- Le porteur n'a pas respecté ses obligations découlant de la PC de l'AC ou des CGU correspondantes ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- La clé privée du porteur est suspectée de compromission, est compromise ou, est perdue (éventuellement les données d'activation associées) ;
- Les données d'authentification du porteur ont été compromises ;
- Le certificat de l'AC VIALINK EU STANDARD CA doit être révoqué, nécessitant de fait la révocation de tous les certificats porteurs qui ont été émis par cette 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.

#### 4.9.1.2 Certificats AC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat AC :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- Décision de changement de composante de l'AC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC,
- Cessation d'activité de l'entité opérant la composante.

### 4.9.2 Origine d'une demande de révocation

Chacune des demandes de révocation implique la saisie d'un motif de révocation qui ne sera pas publié.

4.9.2.1 Certificats de porteurs

La révocation d'un certificat d'un porteur peut être demandée par le porteur lui-même uniquement.

L'AC conserve la faculté de décider de la révocation de tout certificat porteur lorsqu'elle le juge nécessaire pour des raisons de sécurité.

4.9.2.2 Certificats AC

La révocation du certificat de l'AC ne peut émaner que par l'entité responsable de l'Autorité de Certification ou par les autorités judiciaires via une décision de justice ;

La révocation des certificats d'une composante de l'IGC peut émaner de l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

### 4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat porteur

Les exigences d'identification et de validation, effectuée par la fonction de gestion des révocations, sont décrites au §3.4.

Les informations suivantes doivent figurer dans la demande de révocation de certificat :

- Le nom et le prénom du porteur tels qu'ils apparaissent dans le certificat ;
- L'adresse courriel du porteur telle qu'indiquée à son enregistrement.

Si le porteur n'a pas accès à cette adresse de courriel, il contacte l'AC (directement ou par l'intermédiaire de son AE).

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation sera diffusée via une LCR signée.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

Le demandeur de la révocation sera informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

En cas de compromission, le certificat de d'AC sera révoqué.

### 4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

### 4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de porteur

Par nature, une demande de révocation doit être traitée en urgence et dès sa réception.

La fonction de gestion des révocations est disponible 24h/24h 7j/7j.

Toute demande de révocation d'un certificat porteur sera traitée dans un délai inférieur à 24h, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

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

### 4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

### 4.9.7 Fréquence d'établissement des LCR

Les LCR sont produites tous les 5j et à chaque révocation.



Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 4.9.8 Délai maximum de publication d'une LCR

Le délai de publication des LCR est de maximum 4h après leur établissement.

### 4.9.9 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Cf. §4.9.6 ci-dessus.

### 4.9.10 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats d'AC, outre les exigences du §4.9.3.2 ci-dessus, 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.

## 4.10 Fonction d'information sur l'état des certificats

### 4.10.1 Caractéristiques opérationnelles

Les statuts des certificats (LCR/LAR), ainsi que la chaine de certification correspondante sont en accès libre sur le site de publication de l'AC (voir au §2.2).

### 4.10.2 Disponibilité de la fonction

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

Cette fonction est indisponible par interruption au maximum pendant 8h.

## 4.11 Fin de la relation entre le porteur et l'AC

Sans objet.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 5 Mesures de sécurité non techniques

Des analyses de risques sont réalisées par l'AC pour 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 Mesures de sécurité physique

### 5.1.1 Accès physique

Pour les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

### 5.1.2 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

### 5.1.3 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

### 5.1.4 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

### 5.1.5 Conservation des supports

Dans le cadre de l'analyse de risques, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 5.1.6 Mise hors service des supports

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

### 5.1.7 Sauvegardes hors site

Les informations sauvegardées hors site respectent les exigences de la PC de l'AC en matière de protection en confidentialité et en intégrité de ces informations : Ces sauvegardes sont transmises via une liaison spécialisée du site de production vers le site de PCA sur un serveur sécurisé et sont signées numériquement afin d'en assurer l'intégrité.

## 5.2 Mesures de sécurité procédurales

### 5.2.1 Rôles de confiance

Les rôles de confiance suivants ont été identifiés pour chaque composante de l'IGC :

- **Porteur de parts de secrets de l'IGC** : Personne désignée par une autorité compétente et dont le rôle est d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.
- **Responsable de sécurité** : Le responsable de sécurité est chargé de la définition de la politique de sécurité au sein de l'IGC Vialink, et du contrôle de son application. Il gère la liste des habilitations, des contrôles d'accès physiques aux équipements des systèmes de la composante.
- **Ingénieur système** : L'ingénieur système est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante
- **Opérateur Vialink** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
  Les opérateurs de révocation de certificats émis par l'AC VIALINK EU STANDARD CA sont des opérateurs Vialink.
  L'opérateur participe également à la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC.
  L'opérateur peut également avoir des rôles de contrôle niveau 1 des opérations réalisées afin de s'assurer du respect des conditions de sécurité et de la légitimité des opérations réalisées par les autres acteurs disposant d'un rôle de confiance.
- **Opérateur d'Enregistrement Client** : L'opérateur d'enregistrement client est identifié au sein d'une autorité d'enregistrement pour réaliser, dans le cadre de ses attributions, l'enregistrement


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

des porteurs (vérifier l'identité des porteurs et de constituer le dossier d'enregistrement préalable à la demande de certificat).

- **Contrôleur/Auditeur :** Le Contrôleur/Auditeur est désigné afin de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par rapport aux politiques de certification et de sécurité conformément aux déclarations des pratiques de certification de l'IGC.

  Il dispose pour cela d'un accès aux données d'audit du système et aux archives et est chargé de l'analyse régulière de ces données afin de détecter tout incident, anomalie, tentative de compromission, etc.

### 5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Les fonctions liées à la configuration et à la gestion des clés privées des AC sont au moins sous le contrôle de deux personnes ayant des rôles de confiance.

### 5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC vérifie l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants.

### 5.2.4 Rôles exigeant une séparation des attributions

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

Les attributions associées à chaque rôle sont décrites dans la documentation interne de l'AC et sont conformes à la politique de sécurité de la composante concernée.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur ;
- Contrôleur et ingénieur système / opérateur ;
- Ingénieur système et opérateur.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 5.3 Mesures de sécurité vis-à-vis du personnel

### 5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont contractuellement soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante de l'IGC s'assure que les attributions de ses personnels, amenées à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'IGC.

### 5.3.2 Procédures de vérification des antécédents

Des vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement pour vérifier les antécédents et éviter tout conflit d'intérêts préjudiciable à l'impartialité des tâches.

### 5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

### 5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

### 5.3.5 Fréquence et séquence de rotation entre différentes attributions

La rotation entre différentes attributions intervient lors de changements de postes et de fonctions au sein de l'AC.

### 5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions seront prises à l'encontre du personnel en cas d'actions non autorisées.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doivent respecter les exigences du présent chapitre §5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

### 5.3.8 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

## 5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les données sont conservées avec les dates et heures des événements pendant une durée de 10 (dix) ans.

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés.

Elle permet de garantir l'auditabilité, la traçabilité, l'imputabilité ainsi que de s'assurer que la séparation des fonctions est effective. Ce système permet également de collecter des preuves et de détecter des anomalies.

La journalisation des événements est protégée, sauvegardée et fait l'objet de règles strictes d'exploitation.

### 5.4.1 Type d'évènements à enregistrer

La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système, et comprend au minimum les éléments suivants :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

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

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs, ...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- Réception d'une demande de certificat ;
- Validation ou rejet d'une demande de certificat ;
- Evènements liés aux clés et aux certificats d'AC, tels que : génération (en cérémonie des clés), sauvegarde, restauration, révocation, renouvellement, destruction, … ;
- Génération des éléments secrets des porteurs : bi-clés, codes d'activation, ... ;
- Génération des certificats des porteurs ;
- Transmission des clés ou des certificats des porteurs au porteur ou à une autre composante ;
- Activation et désactivation de la clé des porteurs ;
- Destruction des clés des porteurs ;
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- Réception d'une demande de révocation de certificat ;
- Validation ou rejet d'une demande de révocation de certificat ;
- Génération puis publication des LCR ;

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

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements. De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération ;
- Nom du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

### 5.4.2 Fréquence de traitement des journaux d'évènements

Voir §5.4.6 ci-dessous.

### 5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins un mois.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un mois.

### 5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements.

### 5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques de l'AC.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 5.4.6 Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés quotidiennement afin d'identifier des anomalies liées à des tentatives en échec au moyen de scripts de recherche de mots clés.

Les journaux sont analysés dans leur totalité au moins une fois par jour par l'équipe réseaux et système de VIALINK.

Les journaux sont rapprochés au moins une fois par semaine par l'équipe réseaux et système de VIALINK pour détecter toute tentative de modification.

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 3 mois après leur publication. Dans tous les cas, une analyse d'impact est réalisée afin de déterminer l'opportunité de les appliquer ; si un correctif n'est pas appliqué, l'analyse en justifie la décision.

## 5.5 Archivage des données

L'archivage est réalisé par l'AC dans le but d'assurer la continuité de service, l'auditabilité et la non-répudiation des opérations.

Les mesures nécessaires sont mises en place par l'AC afin que ces archives soient disponibles, ré-exploitables, protégées en intégrité et qu'elles fassent l'objet de règles strictes d'exploitation et de protection contre la destruction.

L'AC décrit précisément dans ses procédures internes :

- Les types de données à archiver,
- La période de rétention des archives, dont notamment :
  - Les PC successives sont conservées pendant toute la durée du service de l'AC.
  - Toutes les traces des événements liés au cycle de vie des clés gérées par l'AC sont conservées au minimum 10 ans après l'expiration des clés correspondantes
  - Les certificats, récépissés, notifications, dossiers d'enregistrement et justificatifs d'identité sont conservés au minimum 10 ans après l'expiration des clés.
  - Les LCR sont conservées 10 ans.
- La protection des archives,
- La duplication des archives,
- L'horodatage des enregistrements,


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- La collecte des archives (interne ou externe),
- La récupération et vérification des archives.

### 5.5.1 Types de données à archiver

Les procédures d'archivage permettent d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Elles permettent également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les conditions générales d'utilisation ;
- Les certificats, LCR tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- Les journaux d'évènements des différentes composantes de l'IGC.

### 5.5.2 Période de conservation des archives

**Dossiers de demande de certificat**

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins 10 (10) ans, pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du porteur.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.

Ce dossier doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

**Certificats, LCR émis par l'AC**

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, doivent être archivés pendant au moins sept (7) années après leur expiration.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

**Journaux d'évènements**

Les journaux d'évènements traités au chapitre 5.4 seront archivés pendant 10 (dix) années après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

### 5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

### 5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

### 5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.5.5 pour la datation des journaux d'évènements.

### 5.5.6 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à deux (2) jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

## 5.6 Changement de clé d'AC

La période de validité de la clé de l'AC est définie dans le document qui en décrit les profils.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 5.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC.

### 5.7.2 Procédures de reprise en cas de sinistre

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la PC de l'AC, et des résultats de l'analyse de risques de l'IGC.

Ces plans sont testés au minimum une fois par an.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (cf. § 5.7.2).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

### 5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences du présent document (cf. § 5.7.2).

## 5.8 Fin de vie de l'IGC

L'AC s'engage s'appuiera sur les exigences du Règlement eIDAS quant au transfert, la cessation ou l'arrêt d'activité. Les mesures et procédures relatives à ces sujets sont décrites dans le document *Plan de fin de vie*.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 6 Mesures de sécurité techniques

## 6.1 Génération des bi-clés du porteur et installation

### 6.1.1 Génération des bi-clés

6.1.1.1 Clés de l'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature de l'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du § 6.2.1.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. § 5.2.1), dans le cadre de « cérémonies de clés ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins impartiaux, potentiellement externes à l'AC.

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 Clés de l'IGC

Les clés de l'IGC sont :

- Les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC :
  La génération des clés d'infrastructure est effectuée dans un environnement sécurisé. La génération des certificats SSL pour l'authentification sur les serveurs de l'autorité d'enregistrement est assurée par l'équipes Réseaux et Systèmes.
  La clé pour la signature des archives est générée par l'équipes Réseaux et Systèmes à l'aide de l'outil OpenSSL.
- Les clés de contrôle, assignées au personnel de l'IGC :
  Les clés d'authentification des administrateurs de la solution PKI sont générées sur des dispositifs matériels sécurisés, et sous le contrôle du Responsable de Sécurité de l'IGC.

6.1.1.3 Clés des porteurs

Les bi-clés sont générées par l'AC.

### 6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 6.1.3 Transmission de la clé publique à l'AC

Sans objet.

### 6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de l'AC sont disponibles sur le site Internet de l'AC.

### 6.1.5 Taille des clés

Les clés utilisées ont une taille de 2048 bits et seront mises à niveau au fur et à mesure de l'évolution de la technique et/ou de la législation.

La taille de la clé de l'AC est de 4096 bits.

### 6.1.6 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux services de signature (cf. § 1.4.1.1).

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

### 6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

#### 6.2.1.1 Module cryptographique de l'AC

Le module cryptographique utilisé par l'AC pour la génération et la mise en œuvre de ses clés de signature répond aux exigences du chapitre 10.

### 6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par plusieurs porteurs de part de secret.

### 6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des porteurs ne sont en aucun cas séquestrées.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 6.2.4 Copie de secours de la clé privée

6.2.4.1 Clés des porteurs

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

6.2.4.2 Clé de l'AC

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences de la PC de l'AC, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

6.2.4.3 Clé de l'IGC

Les clés privées de l'IGC ne font l'objet d'aucune copie de secours par l'AC.

### 6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des porteurs ne sont en aucun cas archivées, ni par l'AC, ni par aucune des composantes de l'IGC.

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

Pour les clés privées d'AC, tout transfert est réalisé sous forme chiffrée, conformément aux exigences du § 6.2.4.

### 6.2.7 Méthode d'activation de la clé privée

6.2.7.1 Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique permet de répondre aux exigences définies dans la PC de l'AC.

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (cf. § 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance.

6.2.7.2 Clés privées des porteurs

Les clés privées des porteurs sont actives après la validation du code unique saisi par le porteur du certificat.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 6.2.8 Méthode de désactivation de la clé privée

6.2.8.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès que l'environnement du module évolue.

6.2.8.2 Clés privées des porteurs

Les clés privées des porteurs sont automatiquement désactivées après leur utilisation.

### 6.2.9 Méthode de destruction des clés privées

6.2.9.1 Clés privées d'AC

La méthode de destruction des clés privées d'AC permet de répondre aux exigences définies dans le chapitre 10 pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.9.2 Clés privées des porteurs

Les clés privées des porteurs sont automatiquement détruites après leur utilisation en les supprimant définitivement du serveur.

## 6.3 Autres aspects de la gestion des bi-clés

### 6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

### 6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente ont la même durée de vie.

## 6.4 Données d'activation

### 6.4.1 Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de *l'AC*

La génération et l'installation des données d'activation d'un module cryptographique de l'IGC se font lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

et saisies par les responsables de ces données eux-mêmes, elles leur sont transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. § 5.2.1).

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

La clé privée du porteur est activée après la vérification du code unique retourné par le porteur à l'AC.

### 6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC sont initialisées lors de la cérémonie de clés dans une salle sécurisée, soumise à un contrôle d'entrées et de sorties, au moyen de deux personnes avec authentification forte. Les données d'activation, stockées dans des cartes à puces avec code PIN, sont remises à des porteurs de part de secret responsables d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation sont protégées en intégrité et en confidentialité durant toute leur durée de validité (quelques minutes).

## 6.5 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques que l'AC a menée.

### 6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la PSSI de **ERREUR ! NOM DE PROPRIETE DE DOCUMENT INCONNU.**. Il répond aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès aux systèmes sensibles (authentification à deux facteurs, de nature physique ou logique),
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (non-répudiation et nature des actions effectuées).

## 6.6 Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC a menée.

### 6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation.
La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.

### 6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC est signalée à l'AC pour validation.
L'AC complète la PSSI de **ERREUR ! NOM DE PROPRIETE DE DOCUMENT INCONNU.** avec les règles suivantes :

- L'AC tient à jour un schéma d'architecture précis du système d'information du service de confiance. Ce schéma doit notamment identifier l'ensemble des interconnexions du système d'information du service de confiance ;
- L'AC interdit la connexion d'équipements personnels au système d'information de l'IGC ;
- L'AC met en place des réseaux cloisonnés ;
- L'AC interdit l'accès sans fil au système d'information de l'IGC ;
- L'AC interdit tout accès à Internet depuis les comptes d'administration de l'IGC ;


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- L'IGC dispose d'un réseau d'administration dédié, l'ensemble des opérations d'administration devant être exclusivement réalisées depuis ce réseau ;
- L'AC n'autorise l'accès à distance au réseau d'entreprise, y compris pour l'administration du réseau, que depuis des postes de l'entreprise qui mettent en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes ;
- L'IGC dispose de procédures de gestion des correctifs de sécurité (cf. 5.4.6)

## 6.7 Mesures de sécurité réseau

Le réseau et ses systèmes sont protégés contre les attaques. En particulier,

a) Le SI est segmenté en réseaux ou zones en fonction de l'analyse des risques, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services. Les mêmes contrôles de sécurité sont appliqués à tous les systèmes partageant la même zone.

b) L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du SI du service.

L'AC garantit que les composants du réseau local (routeurs, etc.) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique ; des dispositifs de surveillance (avec alarme automatique) de ces configurations doivent être mis en place.

c) Tous les systèmes critiques sont isolés dans une ou plusieurs zones sécurisées.

d) L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne sont pas utilisés à d'autres fins. Les systèmes de production du service sont séparés des systèmes utilisés pour le développement et les tests.

e) La communication entre des systèmes de confiance distincts n'est établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.

f) Si un niveau élevé de disponibilité au service de confiance est nécessaire, la connexion réseau externe est redondante pour assurer la disponibilité des services.

g) Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par l'AC, est effectuée par une personne ou une entité ayant les compétences, les outils, la


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

compétence, le code de déontologie et l'indépendance nécessaires. Cette analyse doit donner lieu à un rapport.

h) Un test d'intrusion sur les systèmes du service est réalisé lors de la mise en place et après toute évolution de l'infrastructure ou des applications.

## 6.8 Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'évènements liés aux activités de l'IGC (cf. § 5.4).

Pour dater ces évènements, les différentes composantes de l'IGC recourent à l'utilisation de l'heure système de l'IGC en assurant une synchronisation quotidienne des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 7 Profils des certificats et des LCR

## 7.1 Profil des certificats

Voir Annexe 4 : Profil des certificats.

## 7.2 Profil des LCR

Voir Annexe 5 : Format des LCR.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 8 Audit de conformité et autres évaluations

Le présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

## 8.1 Fréquences et / ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante.
L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son IGC au minimum, une fois par an.

## 8.2 Identités / qualifications des évaluateurs

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

## 8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est dûment autorisée à pratiquer les contrôles visés.

## 8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC ou sur l'ensemble de l'architecture de l'IGC et visent à vérifier le respect des engagements et pratiques définies dans cette PC ainsi que des éléments qui en découlent.

## 8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite","échec", "à confirmer".
Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et respecte ses politiques de sécurité internes.

- En cas de résultat "A confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de cette PC et la DPC.

## 8.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de certification en charge de la certification de l'AC.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 9 Autres problématiques métiers et légales

## 9.1 Tarifs

### 9.1.1 Émission ou renouvellement de certificats

Les tarifs correspondants à l'émission ou au renouvellement de certificats sont publiés sur le site Internet de Vialink ou négociés contractuellement avec une entité cliente demandant le service.

### 9.1.2 Validité de certificats

Aucun frais d'accès aux LCR permettant de vérifier la validité des certificats n'est facturé.

### 9.1.3 Politique de remboursement

Toute demande de remboursement devra être adressée à :

| |
|---|
| **Vialink** |
| Service Client |
| 18 quai de la Rapée |
| 75012 PARIS |
| France |

## 9.2 Responsabilité financière

Sans Objet.

## 9.3 Confidentialité des données professionnelles

### 9.3.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les clés privées des entités propriétaires de certificats ;
- Les données d'activation pour les utilisateurs ;
- Les secrets de l'IGC ;
- Les journaux d'événements des composantes de l'AC et de l'AE ;
- Le dossier d'enregistrement du porteur, et notamment les données personnelles (à l'exception des informations à caractère personnel contenues dans les certificats) ;
- Les causes de révocations ;


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- Les rapports d'audit ;
- La partie non publique de la DPC.

### 9.3.2 Divulgation des causes de révocation de certificat

L'AC ne demande pas de justificatif de la demande de révocation. En conséquence, les causes de révocation ne sont pas divulguées.

### 9.3.3 Responsabilité en terme de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles en § 9.2.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

## 9.4 Protection des données personnelles

### 9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

### 9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- Le dossier d'enregistrement du porteur.

### 9.4.3 Notification et consentement d'utilisation des données personnelles

Les informations que tout porteur remet à l'AC sont intégralement protégées contre la divulgation sans le consentement de celui-ci, une décision judiciaire ou autre autorisation légale.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

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

Dans le cadre de procédures légales, l'AC peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers conformément à la législation et la réglementation en vigueur sur le territoire français.

### 9.4.5 Autres circonstances de divulgation d'informations personnelles

Les données à caractère personnel détenues par l'AC ne sont divulguées qu'au porteur, sur demande de ce dernier, et peuvent être consultables et modifiables en conformité avec la loi relative à l'Informatique, aux Fichiers et aux Libertés dite « loi Informatique et Libertés » (Article 32 de la loi n°78-17 du 6 janvier 1978).

## 9.5 Droits de propriété intellectuelle

Lors de l'exécution des prestations de services définies dans le présent document et/ou le Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA, il peut être livré des éléments protégés par la législation sur les droits d'auteur.

Ces éléments, ainsi que les droits d'auteur qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire de ces services aura le droit de reproduire ces éléments pour son usage interne. Mais il ne pourra, sans l'autorisation préalable du détenteur des droits d'auteur, mettre à la disposition de tiers, extraire ou réutiliser en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci, en particulier logiciels ou bases de données.

Sous réserve des dispositions du présent article, aucune licence, implicite ou explicite, n'est concédée par le détenteur des droits sur des inventions, brevets ou demandes de brevets lui appartenant et ayant été réalisés hors du présent document et/ou du Contrat Utilisateur de Certification VIALINK EU STANDARD CA.

## 9.6 Interprétation contractuelles et garanties

Les composantes de l'IGC VIALINK EU STANDARD CA s'engagent à :

- Protéger et garantir l'intégrité et la confidentialité des clés secrètes et/ou privées ;
- N'utiliser les clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés dans les conditions fixées par la Politique de Certification et les documents qui en découlent ;
- Respecter et appliquer leur DPC ;


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC et l'organisme de qualification, en respecter les conclusions et remédier aux non-conformités qu'ils révéleraient ;
- Respecter les accords ou contrats qui les lient aux utilisateurs ;
- Documenter les procédures internes de fonctionnement ;
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent, dans des conditions garantissant qualité et sécurité.

### 9.6.1 Obligations de l'AC

9.6.1.1 S'agissant des fonctions de gestion des certificats

L'AC VIALINK EU STANDARD CA s'engage à :

- Assurer le lien entre l'identité d'un porteur et son certificat ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Assurer la disponibilité de la fonction de révocation et la vérification d'origine des demandes de révocation ;
- Tenir à disposition des utilisateurs et des porteurs de certificats la notification de révocation du certificat d'une composante de l'ICP ou d'un porteur ;
- S'assurer que ses porteurs connaissent leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP. La relation entre un porteur et l'AC est formalisée par un abonnement ou un lien contractuel précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

9.6.1.2 S'agissant de la fonction de gestion des supports et données d'activation

Sans objet.

9.6.1.3 S'agissant de la fonction de publication

L'AC s'engage à diffuser publiquement la politique de certification, les Listes de Certificats Révoqués (LCR) et la liste des certificats auxquels la clé racine de l'ICP est subordonnée.

L'AC s'engage à ce que la Liste de Certificats Révoqués soit :

- Fiables, c'est à dire comportent des informations contrôlées et à jour ;
- Protégés en intégrité ;
- Disponibles 24 heures sur 24 et 7 jours sur 7.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 9.6.2 Obligations de l'AE

L'AE s'engage à vérifier l'authenticité des pièces justificatives et l'exactitude des mentions qui établissent l'identité du porteur ou de l'entreprise selon les procédures décrites dans cette PC.

### 9.6.3 Obligations du porteur

Le porteur a le devoir moral et contractuel de :

- Communiquer des informations exactes et à jour lors de la demande de certificat ou de renouvellement du certificat ;
- Protéger ses données d'activation et les mettre en œuvre ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans son certificat.

La relation entre le porteur et l'AC ou l'AE est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

### 9.6.4 Obligations des utilisateurs de certificats

Les utilisateurs des certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC de l'AC.

## 9.7 Limite de garantie

Sans objet.

## 9.8 Limite de responsabilité

Vialink ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des Certificats, des listes de révocation, ainsi que de tout autre équipement ou logiciel mis à disposition.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

Vialink décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Porteur.
En aucun cas, Vialink ne peut être tenue responsable des préjudices indirects tels que notamment perte financière, perte de données, dommage indirect lié à l'utilisation du certificat.

## 9.9 Indemnités

Les éventuelles indemnités liées au service de certification de l'AC sont négociées contractuellement avec chaque entité cliente.

## 9.10 Durée et fin anticipée de la PC

### 9.10.1 Durée de validité

Cette PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

### 9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la politique LCP de la norme ETSI EN 319 411-1 peut impliquer, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer cette PC.
En fonction de la nature et de l'importance des évolutions apportées, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur. De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

## 9.11 Notifications individuelles et communications entre les participants

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

- Au plus tard un mois avant le début de l'opération, fait valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes.
- Informe si nécessaire l'organe de contrôle national (au sens du Règlement eIDAS) en cas d'impact significatif.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

## 9.12 Permanence de la PC

Le fait que l'une des parties n'ait pas exigé l'application d'une clause quelconque du présent document et/ou du Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA, que ce soit de façon permanente ou temporaire, ne pourra en aucun cas être considéré comme une renonciation aux droits de cette partie découlant de ladite clause dont l'inapplication a été tolérée. Si l'une quelconque des dispositions du présent document et/ou du Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA est non valide, nulle ou sans objet elle sera réputée non écrite et les autres dispositions conserveront toute leur force et leur portée.

Aucune action, quelle qu'en soit la nature, le fondement ou les modalités, née du présent document et/ou du Contrat Utilisateur du Service de Certification, ne peut être intentée par les parties plus de deux ans après la survenance de son fait générateur. Les titres des articles du présent document et/ou du Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA sont insérés dans le seul but d'en faciliter la référence et ne peuvent être utilisés pour donner une interprétation à ces articles ou en affecter la signification. Aussi, en cas de difficulté d'interprétation entre l'un quelconque des titres et l'une quelconque des clauses constituant le document et/ou le Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA, les titres seront déclarés comme inexistants.

## 9.13 Respect et interprétation des dispositions juridiques

Les pratiques du Service de Certification VIALINK EU STANDARD CA sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures du Service de Certification VIALINK EU STANDARD CA 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/).

### 9.13.1 Droit applicable

La Loi française est applicable aux dispositions du présent document (y incluant le Contrat Utilisateur du Service de VIALINK EU STANDARD CA). En cas de traduction seule la version française du présent document fera foi. En cas de difficulté, les parties se conformeront à la procédure de règlement des litiges prévue par le Contrat Utilisateur du Service de Certification VIALINK EU STANDARD CA. A défaut de règlement amiable, le litige sera porté devant les juridictions compétentes.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

### 9.13.2 Règlement des différends

Toute contestation relative aux dispositions du présent document et au Service de Certification sera soumise, préalablement à toute instance judiciaire, à la procédure décrite à l'article règlement des litiges du Contrat Utilisateur du Service de Certification.

### 9.13.3 Dispositions pénales

Le fait d'accéder et de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni deux ans d'emprisonnement et de 30 000 Euros d'amende (article L.323-1, alinéa 1 du Code Pénal).

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 45 000 Euros d'amende (article L.323-1, alinéa 2 du Code Pénal). Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende (article L.323-2 du Code Pénal). Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende (article L.323-3 du Code Pénal).


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 10 Annexe 1 : Exigences de sécurité du module cryptographique de l'AC

## 10.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés permet notamment de :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Etre 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 ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Le module cryptographique détecte les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

## 10.2 Exigences sur la certification

Le module cryptographique utilisé par l'AC a été certifié selon les Critères Communs au niveau EAL4+ selon un profil de protection recommandé par le SOGIS.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 11 Annexe 2 : Liste des sigles et abréviations utilisés

| | |
|---|---|
| AC | Autorité de Certification |
| AE | Autorité d'Enregistrement |
| ANSSI | Agence Nationale de la Sécurité des Systèmes d'Information |
| C | Country (Pays) |
| CN | Common Name |
| DN | Distinguished Name |
| DPC | Déclaration des Pratiques de Certification |
| ICP | Infrastructure à Clés Publiques |
| IGC | Infrastructure de Gestion de Clés |
| LCR | Liste des Certificats Révoqués |
| O | Organisation |
| OC | Opérateur de Certification, ou OSC |
| OID | Object Identifier |
| OSC | Opérateur de Service de Certification |
| OU | Organisation Unit |
| PC | Politique de Certification |
| PS | Politique de Sécurité |
| RSA | Rivest Shamir Adelman |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 12 Annexe 3 : Définitions des termes utilisés dans la PC

*Le symbole (*) signifie que le terme est défini dans le présent paragraphe. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.*

**Autorité de Certification (AC)** : autorité à laquelle les porteurs* font confiance pour émettre et gérer des clés, des certificats et des LCR*. Ce terme désigne l'entité responsable des certificats signés en son nom. L'AC est le maître d'ouvrage de l'ICP. Elle assure les fonctions suivantes :

- Mise en application de la PC*,
- Gestion des certificats*
- Gestion des supports et de leurs données d'activation* si les bi-clés* et les certificats sont fournis aux utilisateurs sur des supports matériels,
- Publication* des certificats valides et des listes de certificats révoqués,
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'ICP

La fonction d'enregistrement des certificats fait partie des fonctions indispensables d'une ICP. L'AC doit s'assurer qu'elle est remplie par une Autorité d'Enregistrement*, avec laquelle elle collabore ou qui lui est rattachée.

**Autorité d'Enregistrement (AE) :** entité en charge de vérifier l'identité des demandeurs de certificat. L'AE s'assure que les demandeurs de certificat sont mandatés par l'Administrateur client, et prennent l'engagement d'utiliser les certificats uniquement dans les conditions définies dans la présente Politique de Certification.

L'AE a également pour tâche :

- De réceptionner et traiter les demandes de révocation de certificats.
- D'archiver les dossiers de demande de certificats ou de révocation.

**Bi-clé** : un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre de services tels que la signature électronique basée sur des algorithmes asymétriques.

**Chaîne de confiance** : ensemble des certificats nécessaires pour valider la filiation d'un certificat porteur.

**Common Name (CN)** : identité réelle ou pseudonyme du porteur* titulaire du certificat (exemple CN = Jean Dupont).

**Composante de l'ICP :** plate-forme jouant un rôle déterminé au sein de l'ICP* dans le cycle de vie du certificat.

**Distinguished Name (DN)** : nom distinctif X.500 du porteur* pour lequel le certificat est émis.

**Données d'activation** : données privées associées à un porteur* permettant de mettre en œuvre sa clé privée.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

**Émission (d'un certificat) :** fait d'exporter un certificat à l'extérieur d'une AC* (pour une remise au porteur, une demande de publication).

**Enregistrement (d'un porteur)** : opération qui consiste pour une Autorité d'Enregistrement* à constituer le profil d'un demandeur de certificat à partir de son dossier de demande de certificat, conformément à la Politique de Certification*.

**Génération (d'un certificat) :** action réalisée par une AC* et qui consiste à signer le gabarit d'un certificat édité par une AE*.

**Identificateur d'objet (OID) :** identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

**Infrastructure à Clé Publique (ICP) :** ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

**Liste de Certificats Révoqués (LCR) :** liste de certificats ayant fait l'objet d'une révocation*.

**Infrastructure de Gestion de Clés (IGC) :** voir ICP.

**Module cryptographique :** un module cryptographique est un dispositif matériel permettant de protéger les éléments secrets tels que les clés privées ou les données d'activation, et de procéder à des calculs cryptographiques mettant en œuvre ces éléments.

**Opérateur de Certification (OC) :** composante de l'ICP disposant d'une plate-forme lui permettant de générer et émettre des certificats pour le compte d'une ou plusieurs Autorités de Certification.

**Opérateur de Services de Certification** (OSC) : voir OC*

**Politique de Certification (PC) :** ensemble de règles, définissant les exigences auxquelles l'AC* se conforme dans la mise en place de prestations adaptées à certains types d'applications. La Politique de Certification doit être identifiée par un OID* défini par l'AC*.

**Porteurs de (certificats) :** personne physique qui obtient des services de l'AC. Dans la phase amont de certification, il est un "demandeur" de certificat, et dans le contexte du certificat X.509V3, il est un "objet".

**Publication (d'un certificat) :** opération consistant à mettre un certificat à disposition d'utilisateurs pour leur permettre de vérifier une signature ou de chiffrer des informations (ex : annuaire X.500).

**Renouvellement (d'un certificat) :** opération effectuée à la demande d'un porteur ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La régénération de certificat après révocation* n'est pas un renouvellement.

**Révocation (d'un certificat) :** opération demandée par le porteur ou par toute autre personne autorisée par l'AC dont le résultat est la suppression de la garantie d'engagement de l'AC* sur un certificat donné, avant la fin de sa période de validité. Par exemple, la compromission d'une clé ou le changement d'informations


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

contenues dans un certificat doivent conduire à la révocation du certificat. L'opération de révocation est considérée terminée lorsque le numéro de certificat à révoquer est publié dans la Liste des Certificats Révoqués (LCR*).

**Utilisateurs (de certificats) :** Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique provenant d'un porteur de certificat.

**Validation (de certificat) :** opération de contrôle du statut d'un certificat ou d'une chaîne de certification*.

**Vérification (de signature) :** opération de contrôle d'une signature numérique.


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 13 Annexe 4 : Profil des certificats

## 13.1 Certificat de Signature Personne Physique à la volée

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 2048 |
| Durée de validité | 5 minutes |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.1.2.1.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |
| Authority Information Access | | FALSE | |
| | id-ad-calssuers | | Voir § 2.2 |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Basic Constraint | | TRUE | |
| | cA | | False |

## 13.2 Certificat d'authentification et de Signature Personne Physique 3 ans

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 2048 |
| Durée de validité | 3 ans |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Digital Signature (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.3.2.3.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Authority Information Access | | FALSE | |
| | id-ad-calssuers | | Voir § 2.2 |
| Basic Constraint | | TRUE | |
| | cA | | False |

## 13.3 Certificat de Signature Personne Physique en lien avec une personne morale à la volée

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 2048 |
| Durée de validité | 5 minutes |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.1.3.1.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |
| Authority Information Access | | FALSE | |
| | id-ad-calssuers | | Voir § 2.2 |
| Basic Constraint | | TRUE | |
| | cA | | False |

## 13.4 Certificat d'authentification et de Signature Personne Physique en lien avec une personne morale 3 ans

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 2048 |
| Durée de validité | 3 ans |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Digital Signature (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.3.3.3.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |
| Authority Information Access | | FALSE | |
| | id-ad-calssuers | | Voir § 2.2 |
| Basic Constraint | | TRUE | |
| | cA | | False |

## 13.5 Certificats de cachet serveur 3 ans

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 4096 |
| Durée de validité | 3 ans |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Digital Signature (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.4.1.3.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |
| Authority Information Access | | FALSE | |
| | id-ad-caIssuers | | Voir § 2.2 |
| Basic Constraint | | TRUE | |
| | cA | | False |

## 13.6 Certificats de cachet serveur 5 ans

| Champ | Valeur |
|---|---|
| Version | 2 (=version 3) |
| Serial number | Défini par l'outil |
| Taille de la clé | 4096 |
| Durée de validité | 5 ans |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI=NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Subject DN | Voir § 3.1.1 |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Parameters | NULL |

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Subject Key Identifier | | FALSE | |
| | Key Identifier | | Key Identifier à générer selon la méthode 1 |
| | Methods of generating key ID | | Méthode 1 |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

| Extension | Champs de l'extension | Critique | Valeur |
|---|---|---|---|
| Key Usage | | TRUE | |
| | Non Repudiation (1) | | Set(1) |
| | Digital Signature (1) | | Set(1) |
| | Autres | | Clear (0) |
| Subject Alternative Name | | FALSE | |
| | RFC822 Name | | Nom RFC822=<Email> |
| CRL Distribution Points | | FALSE | |
| | distributionPoint | | Voir § 2.2 |
| Certificate Policies | | FALSE | |
| | policyIdentifiers | | 1.2.250.1.198.4.4.1.4.0.1 |
| | PolicyQualifiers | | |
| | CPSpointer | | |
| | CPSuri | | Voir § 2.2 |
| Authority Key Identifier | | FALSE | |
| | Key Identifier | | SubjectKeyID du certificat d'AC |
| | Methods of generate key ID | | Methode 1 |
| Authority Information Access | | FALSE | |
| | id-ad-calssuers | | Voir § 2.2 |
| Basic Constraint | | TRUE | |
| | cA | | False |


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.

# 14 Annexe 5 : Format des LCR

| Champ | Valeur |
|---|---|
| Version | 1 (=version 2) |
| Signature Algorithm | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| nextUpdate | 5 jours après la date de génération |
| Périodicité de mise à jour | Toutes les 24 heures |
| Issuer DN | **CN=VIALINK EU STANDARD CA**<br>**OI= NTRFR-428668545**<br>**O=VIALINK**<br>**C=FR** |
| Extension : Numéro de la CRL | Numéro incrémental |
| Extension : Authority Key Identifier | SubjectKeyID du certificat de l'AC VIALINK EU STANDARD CA |
| Liste des certificats révoqués | Numéros de série et date de révocation. Pas de raison de révocation |

➢ FIN DU DOCUMENT ➢


Ce document est la propriété de Vialink, sa diffusion ou sa copie est interdite sans l'audorisation écrite de Vialink.