



Politique de Certification

Universign Trust Network

7, rue du Faubourg Poissonnière, 75009 Paris, France

OID: 1.3.6.1.4.1.15819.5.1.3.(1/3/4/5/6/7)

Table des matières

| | | |
|----------|---|-----------|
| 1 | Introduction | 10 |
| 1.1 | Présentation générale | 10 |
| 1.2 | Identification du document | 12 |
| 1.3 | Entités intervenant dans l'UTN | 12 |
| 1.3.1 | Autorités de Certification | 12 |
| 1.3.2 | Autorité d'Enregistrement | 13 |
| 1.3.3 | Porteurs de Certificats | 13 |
| 1.3.4 | Autorités d'Horodatage | 13 |
| 1.3.5 | Parties Utilisatrices | 13 |
| 1.3.6 | Responsable de Certificat | 13 |
| 1.4 | Usage des Certificats | 14 |
| 1.4.1 | Domaines d'utilisation applicables | 14 |
| 1.4.2 | Domaines d'utilisation interdits | 14 |
| 1.5 | Gestion de la Politique | 15 |
| 1.5.1 | Entité gérant ce document | 15 |
| 1.5.2 | Point de contact | 15 |
| 1.5.3 | Entité déterminant la conformité des pratiques avec la PC | 15 |
| 1.5.4 | Procédures d'approbation de la conformité de la DPC | 15 |
| 1.6 | Définitions et acronymes | 15 |
| 2 | Responsabilités concernant la mise à disposition des informations devant être publiées | 17 |
| 2.1 | Entités chargées de la mise à disposition des informations | 17 |
| 2.2 | Informations publiées | 17 |
| 2.3 | Délais et fréquences de publication | 17 |
| 2.4 | Contrôle d'accès aux informations publiées | 18 |
| 3 | Identification et authentification | 18 |
| 3.1 | Nommage | 18 |
| 3.1.1 | Types de noms | 18 |
| 3.1.2 | Noms explicites | 19 |
| 3.1.3 | Anonymisation ou pseudonymisation des Porteurs | 19 |
| 3.1.4 | Règles d'interprétation des différentes formes de noms | 20 |
| 3.1.5 | Unicité des noms | 20 |
| 3.1.6 | Identification, authentification et rôle des marques déposées | 20 |
| 3.2 | Validation initiale de l'identité | 20 |
| 3.2.1 | Méthode pour prouver la possession de la clé privée | 20 |
| 3.2.2 | Validation de l'identité d'un organisme | 20 |
| 3.2.3 | Validation de l'identité d'un individu | 20 |

| | | |
|----------|---|-----------|
| 3.2.4 | Informations non vérifiées du porteur | 21 |
| 3.2.5 | Validation de l'habilitation du demandeur | 21 |
| 3.2.6 | Critères d'interopérabilité | 21 |
| 3.3 | Identification et validation d'une demande de renouvellement de clés | 21 |
| 3.3.1 | Identification et validation pour un renouvellement courant | 21 |
| 3.3.2 | Identification et validation pour un renouvellement après révocation | 21 |
| 3.4 | Identification et validation d'une demande de révocation | 21 |
| 4 | Exigences opérationnelles sur le cycle de vie des Certificats | 22 |
| 4.1 | Demande de Certificat | 22 |
| 4.1.1 | Origine d'une demande de Certificat | 22 |
| 4.1.2 | Processus et responsabilités pour l'établissement d'une demande de Certificats | 22 |
| 4.2 | Traitement d'une demande de Certificat | 22 |
| 4.2.1 | Exécution des processus d'identification et de validation de la demande | 22 |
| 4.2.2 | Acceptation ou rejet de la demande | 22 |
| 4.2.3 | Durée d'établissement du Certificat | 23 |
| 4.3 | Délivrance du Certificat | 23 |
| 4.3.1 | Actions de l'AC concernant la délivrance du Certificat | 23 |
| 4.3.2 | Notification par l'AC de la délivrance du Certificat | 23 |
| 4.4 | Acceptation du Certificat | 23 |
| 4.4.1 | Démarche d'acceptation du Certificat | 23 |
| 4.4.2 | Publication du Certificat | 23 |
| 4.4.3 | Notification par l'AC aux autres entités de la délivrance du Certificat | 23 |
| 4.5 | Usage de la bi-clé et du Certificat | 23 |
| 4.6 | Renouvellement d'un Certificat | 24 |
| 4.6.1 | Causes possibles de renouvellement d'un Certificat | 24 |
| 4.6.2 | Origine d'une demande de renouvellement | 24 |
| 4.6.3 | Procédure de traitement d'une demande de renouvellement | 24 |
| 4.6.4 | Notification au Porteur de l'établissement du nouveau Certificat | 24 |
| 4.6.5 | Démarche d'acceptation du nouveau Certificat | 24 |
| 4.6.6 | Publication du nouveau Certificat | 24 |
| 4.6.7 | Notification par l'AC aux autres entités de la délivrance du nouveau Certificat | 25 |
| 4.7 | Délivrance d'un nouveau Certificat suite à changement de la bi-clé | 25 |
| 4.7.1 | Causes possibles de changement d'une bi-clé | 25 |

| | | |
|--------|---|----|
| 4.7.2 | Origine d'une demande d'un nouveau Certificat | 25 |
| 4.7.3 | Procédure de traitement d'une demande d'un nouveau Certificat | 25 |
| 4.7.4 | Notification au Porteur de l'établissement du nouveau Certificat | 25 |
| 4.7.5 | Démarche d'acceptation du nouveau Certificat | 25 |
| 4.7.6 | Publication du nouveau Certificat | 25 |
| 4.7.7 | Notification par l'AC aux autres entités de la délivrance du nouveau Certificat | 25 |
| 4.8 | Modification du Certificat | 25 |
| 4.8.1 | Causes possibles de modification d'un Certificat | 26 |
| 4.8.2 | Origine d'une demande de modification d'un Certificat | 26 |
| 4.8.3 | Procédure de traitement d'une demande de modification d'un Certificat | 26 |
| 4.8.4 | Notification au Porteur de l'établissement du Certificat modifié | 26 |
| 4.8.5 | Démarche d'acceptation du Certificat modifié | 26 |
| 4.8.6 | Publication du Certificat modifié | 26 |
| 4.8.7 | Notification par l'AC aux autres entités de la délivrance du Certificat modifié | 26 |
| 4.9 | Révocation et suspension des Certificats | 26 |
| 4.9.1 | Causes possibles d'une révocation | 26 |
| 4.9.2 | Origine d'une demande de révocation | 27 |
| 4.9.3 | Procédure de traitement d'une demande de révocation | 27 |
| 4.9.4 | Délai accordé au Porteur pour formuler la demande de révocation | 27 |
| 4.9.5 | Délai de traitement par l'AC d'une demande de révocation | 27 |
| 4.9.6 | Exigences de vérification de la révocation par les Parties Utilisatrices | 27 |
| 4.9.7 | Fréquence d'établissement des LCR | 28 |
| 4.9.8 | Délai maximum de publication d'une LCR | 28 |
| 4.9.9 | Disponibilité d'un système de vérification en ligne de la révocation et de l'état des Certificats | 28 |
| 4.9.10 | Exigences de vérification en ligne de la révocation des Certificats par les Parties Utilisatrices | 28 |
| 4.9.11 | Autres moyens disponibles d'information sur les révocations | 28 |
| 4.9.12 | Exigences spécifiques en cas de compromission de la clé privée | 28 |
| 4.9.13 | Causes possibles d'une suspension | 28 |
| 4.9.14 | Origine d'une demande de suspension | 29 |
| 4.9.15 | Procédure de traitement d'une demande de suspension | 29 |

| | | |
|----------|--|-----------|
| 4.9.16 | Limites de la période de suspension d'un Certificat | 29 |
| 4.10 | Fonction d'information sur l'état des Certificats | 29 |
| 4.10.1 | Caractéristiques opérationnelles | 29 |
| 4.10.2 | Disponibilité de la fonction | 29 |
| 4.10.3 | Dispositifs optionnels | 29 |
| 4.11 | Fin de la relation entre le Porteur et l'AC | 29 |
| 4.12 | Séquestre de clé et recouvrement | 29 |
| 4.12.1 | Politique et pratiques de recouvrement par séquestre des clés | 30 |
| 4.12.2 | Politique et pratiques de recouvrement par encapsulation des clés de session | 30 |
| 5 | Mesures de sécurité non techniques | 30 |
| 5.1 | Mesures de sécurité physique | 30 |
| 5.1.1 | Situation géographique et construction des sites | 30 |
| 5.1.2 | Accès physiques | 30 |
| 5.1.3 | Alimentation électrique et climatisation | 30 |
| 5.1.4 | Exposition aux dégâts des eaux | 31 |
| 5.1.5 | Prévention et protection incendie | 31 |
| 5.1.6 | Conservation des supports de données | 31 |
| 5.1.7 | Mise hors service des supports | 31 |
| 5.1.8 | Sauvegarde hors site | 31 |
| 5.2 | Mesures de sécurité procédurales | 32 |
| 5.2.1 | Rôles de confiance | 32 |
| 5.2.2 | Nombre de personnes requises par tâches | 32 |
| 5.2.3 | Identification et authentification pour chaque rôle | 33 |
| 5.2.4 | Rôles exigeant une séparation des attributions | 33 |
| 5.2.5 | Analyse de risque | 33 |
| 5.3 | Mesures de sécurité vis à vis du personnel | 33 |
| 5.3.1 | Qualifications, compétences et habilitations requises | 33 |
| 5.3.2 | Procédures de vérification des antécédents | 34 |
| 5.3.3 | Exigences en matière de formation initiale | 34 |
| 5.3.4 | Exigences et fréquence en matière de formation continue | 34 |
| 5.3.5 | Fréquence et séquence de rotation entre différentes attributions | 34 |
| 5.3.6 | Sanctions en cas d'actions non autorisées | 34 |
| 5.3.7 | Exigences vis-à-vis du personnel des prestataires externes | 34 |
| 5.3.8 | Documentation fournie au personnel | 35 |
| 5.4 | Procédures de constitution des données d'audit | 35 |
| 5.4.1 | Type d'événements à enregistrer | 35 |
| 5.4.2 | Fréquence de traitement des journaux d'événements | 35 |

| | | |
|----------|--|-----------|
| 5.4.3 | Période de conservation des journaux d'événements | 35 |
| 5.4.4 | Protection des journaux d'événements | 35 |
| 5.4.5 | Procédure de sauvegarde des journaux d'événements | 36 |
| 5.4.6 | Système de collecte des journaux d'évènements | 36 |
| 5.4.7 | Notification de l'enregistrement d'un événement au responsable de l'événement | 36 |
| 5.4.8 | Evaluation des vulnérabilités | 36 |
| 5.5 | Archivage des données | 36 |
| 5.5.1 | Types de données à archiver | 36 |
| 5.5.2 | Période de conservation des archives | 37 |
| 5.5.3 | Protection des archives | 37 |
| 5.5.4 | Procédure de sauvegarde des archives | 37 |
| 5.5.5 | Exigences d'horodatage des données | 37 |
| 5.5.6 | Système de collecte des archives | 37 |
| 5.5.7 | Procédures de récupération et de vérification des archives | 37 |
| 5.6 | Changement de clés | 38 |
| 5.7 | Reprise suite à compromission et sinistre | 38 |
| 5.7.1 | Procédures de remontée et de traitement des incidents et des compromissions | 38 |
| 5.7.2 | Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) | 38 |
| 5.7.3 | Procédures de reprise en cas de compromission de la clé privée d'une composante | 38 |
| 5.7.4 | Capacités de continuité d'activité suite à un sinistre | 39 |
| 5.8 | Fin de vie de l'AC | 39 |
| 6 | Mesures de sécurité techniques | 39 |
| 6.1 | Génération et installation de bi-clés | 39 |
| 6.1.1 | Génération des bi-clés | 39 |
| 6.1.2 | Transmission de la clé privée au Porteur | 40 |
| 6.1.3 | Transmission de la clé publique à l'AC | 40 |
| 6.1.4 | Transmission de la clé publique de l'AC aux Parties Utilisatrices | 40 |
| 6.1.5 | Tailles des clés | 40 |
| 6.1.6 | Vérification de la génération des paramètres des bi-clés et de leur qualité | 41 |
| 6.1.7 | Objectifs d'usage de la clé | 41 |
| 6.2 | Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques | 41 |
| 6.2.1 | Standards et mesures de sécurité pour les modules cryptographiques | 41 |

| | | |
|----------|--|-----------|
| 6.2.2 | Contrôle de la clé privée par plusieurs personnes | 41 |
| 6.2.3 | Séquestre de la clé privée | 42 |
| 6.2.4 | Copie de secours de la clé privée | 42 |
| 6.2.5 | Archivage de la clé privée | 42 |
| 6.2.6 | Transfert de la clé privée vers / depuis le module cryptographique | 42 |
| 6.2.7 | Stockage de la clé privée dans un module cryptographique | 42 |
| 6.2.8 | Méthode d'activation de la clé privée | 42 |
| 6.2.9 | Méthode de désactivation de la clé privée | 43 |
| 6.2.10 | Méthode de destruction des clés privées | 43 |
| 6.2.11 | Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées | 43 |
| 6.3 | Autres aspects de la gestion des bi-clés | 44 |
| 6.3.1 | Archivage des clés publiques | 44 |
| 6.3.2 | Durées de vie des bi-clés et des Certificats | 44 |
| 6.4 | Données d'activation | 44 |
| 6.4.1 | Génération et installation des données d'activation | 44 |
| 6.4.2 | Protection des données d'activation | 44 |
| 6.4.3 | Autres aspects liés aux données d'activation | 44 |
| 6.5 | Mesures de sécurité des systèmes informatiques | 45 |
| 6.5.1 | Mesures de sécurité technique spécifiques aux systèmes informatiques | 45 |
| 6.5.2 | Niveau de qualification des systèmes informatiques | 45 |
| 6.6 | Mesures de sécurité des systèmes durant leur cycle de vie | 45 |
| 6.6.1 | Mesures de sécurité liées au développement des systèmes | 45 |
| 6.6.2 | Mesures liées à la gestion de la sécurité | 45 |
| 6.6.3 | Niveau d'évaluation sécurité du cycle de vie des systèmes | 46 |
| 6.7 | Mesures de sécurité réseau | 46 |
| 6.8 | Horodatage / Système de datation | 46 |
| 7 | Profil des Certificats, des OCSP et des LCR | 46 |
| 7.1 | Profil des Certificats | 46 |
| 7.1.1 | Certificats | 47 |
| 7.2 | Profil des LCR | 47 |
| 7.3 | Profil des OCSP | 48 |
| 8 | Audit de conformité et autres évaluations | 48 |
| 8.1 | Fréquences et / ou circonstances des évaluations | 48 |
| 8.2 | Identités / qualifications des évaluateurs | 48 |
| 8.3 | Relations entre évaluateurs et entités évaluées | 48 |
| 8.4 | Sujets couverts par les évaluations | 49 |

| | | |
|----------|--|-----------|
| 8.5 | Actions prises suite aux conclusions des évaluations | 49 |
| 8.6 | Communication des résultats | 49 |
| 9 | Autres problématiques commerciales et légales | 49 |
| 9.1 | Tarifs | 49 |
| 9.1.1 | Tarifs pour accéder aux Certificats | 49 |
| 9.1.2 | Tarifs pour accéder aux informations d'état et de révocation des Certificats | 50 |
| 9.1.3 | Tarifs pour d'autres services | 50 |
| 9.1.4 | Politique de remboursement | 50 |
| 9.2 | Responsabilité financière | 50 |
| 9.2.1 | Couverture par les assurances | 50 |
| 9.2.2 | Autres ressources | 50 |
| 9.2.3 | Couverture et garantie concernant les entités utilisatrices | 50 |
| 9.3 | Confidentialité des données professionnelles | 50 |
| 9.3.1 | Périmètre des informations confidentielles | 50 |
| 9.3.2 | Informations hors du périmètre des informations confidentielles | 51 |
| 9.3.3 | Responsabilités en termes de protection des informations confidentielles | 51 |
| 9.4 | Protection des données personnelles | 51 |
| 9.4.1 | Politique de protection des données personnelles | 51 |
| 9.4.2 | Informations à caractère personnel | 51 |
| 9.4.3 | Informations à caractère non personnel | 51 |
| 9.4.4 | Responsabilité en termes de protection des données personnelles | 51 |
| 9.4.5 | Notification et consentement d'utilisation des données personnelles | 51 |
| 9.4.6 | Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives | 51 |
| 9.4.7 | Autres circonstances de divulgation d'informations personnelles | 52 |
| 9.5 | Droits sur la propriété intellectuelle et industrielle | 52 |
| 9.6 | Interprétations contractuelles et garanties | 52 |
| 9.6.1 | Autorité de Certification | 52 |
| 9.6.2 | Service d'enregistrement | 53 |
| 9.6.3 | Porteur | 53 |
| 9.6.4 | Parties Utilisatrices | 53 |
| 9.6.5 | Autres participants | 53 |
| 9.7 | Limite de garantie | 53 |
| 9.8 | Limite de responsabilité | 54 |

| | | |
|--------|--|----|
| 9.9 | Indemnités | 54 |
| 9.10 | Durée et fin anticipée | 54 |
| 9.10.1 | Durée de validité | 54 |
| 9.10.2 | Fin anticipée de validité | 54 |
| 9.10.3 | Effets de la fin de validité et clauses restant applicables | 54 |
| 9.11 | Notifications individuelles et communications entre les participants | 54 |
| 9.12 | Amendements | 55 |
| 9.12.1 | Procédures d'amendements | 55 |
| 9.12.2 | Mécanisme et période d'information sur les amendements | 55 |
| 9.12.3 | Circonstances selon lesquelles l'OID doit être changé | 55 |
| 9.13 | Dispositions concernant la résolution de conflits | 55 |
| 9.14 | Juridictions compétentes | 55 |
| 9.15 | Conformité aux législations et réglementations | 56 |
| 9.16 | Dispositions diverses | 56 |
| 9.16.1 | Accord global | 56 |
| 9.16.2 | Transfert d'activités | 56 |
| 9.16.3 | Conséquences d'une clause non valide | 56 |
| 9.16.4 | Application et renonciation | 56 |
| 9.16.5 | Force majeure | 56 |
| 9.17 | Autres dispositions | 56 |
| 9.17.1 | Impartialité | 56 |
| 9.17.2 | Accessibilité | 57 |

1 Introduction

1.1 Présentation générale

La présente Politique de Certification définit les engagements des membres de l'UTN pour la délivrance et la gestion de Certificats électroniques.

Présentation de l'Universign Trust Network

Le réseau Universign Trust Network (UTN) est un réseau d'Autorités de Certification (AC) et d'Autorités d'Horodatage (AH) gouvernées par des politiques communes définies par la société Cryptolog International¹.

Dans ce document, le terme UTN désigne, selon son contexte d'utilisation, le réseau Universign Trust Network ou la société Cryptolog International en charge de son contrôle et de sa gestion.

L'UTN est notamment composé :

- d'Autorités de Certification Primaires (AC Primaires) ;
- d'Autorités de Certification Intermédiaires (AC Intermédiaires) ;
- d'Autorités de Certification Horodatage (AC Horodatage) ;
- d'Autorités d'Horodatage (AH) ;
- de Porteurs de Certificats finaux ;
- de Parties Utilisatrices.

Organisation de l'Universign Trust Network

Les Autorités de Certification fonctionnent selon une chaîne de confiance structurée hiérarchiquement. Les AC Primaires délivrent des Certificats aux AC Intermédiaires qui, elles-mêmes, délivrent des Certificats à des personnes physiques ou morales (les Porteurs). Les Unités d'Horodatage (UH) des Autorités d'Horodatage reçoivent des Certificats de la part des AC Horodatages et émettent des Contremarques de temps. Les AC Horodatages peuvent recevoir des Certificats de la part des AC Primaires.

Les Parties Utilisatrices se fient aux informations contenues dans les Certificats des Porteurs et les Contremarques de temps.

L'UTN :

- publie la Politique de Certification régissant les AC ;
- publie la Politique d'Horodatage régissant les AH ;

1. Cryptolog International, société par actions simplifiée au capital de 579 504 €, dont le siège social est situé au 7 rue du Faubourg poissonnière, 75009 Paris, immatriculée au Registre du Commerce et des Sociétés de Paris sous le numéro 439 129 164.

— gère les AC Primaires du réseau.

Les membres de l'UTN :

- publient leurs Déclarations des Pratiques ;
- gèrent les AC et les AH associées aux services qu'ils proposent.

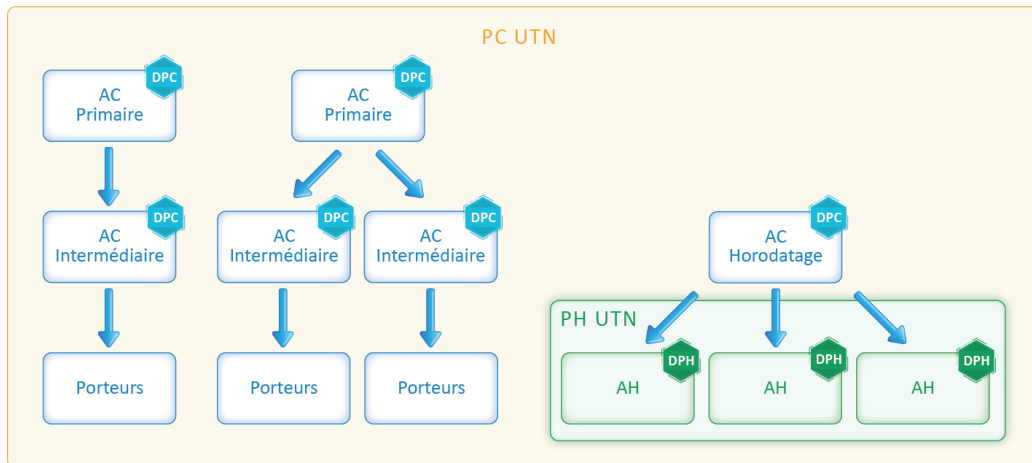


FIGURE 1: Organisation de l'UTN

L'UTN assure la validation, la gestion et la mise en application de la PC et de la PH. L'UTN veille également à la cohérence des référentiels documentaires associés (Accord d'Utilisation, DPC, DPH, ...) à ses Politiques. Chaque autorité membre de l'UTN définit une ou des Déclarations des Pratiques, conformes à la Politique de l'UTN.

Toute demande de rattachement au réseau ou de révocation d'un Certificat d'une AC ou d'une UH du réseau doit être adressée à l'UTN. Les éléments constitutifs du dossier de demande d'un rattachement au réseau ou révocation sont communiqués par l'UTN aux organismes éligibles qui en font la demande.

L'UTN suit les audits et/ou les contrôles de conformité réalisés par les membres du réseau. L'UTN décide des actions à mener et veille à leur mise en application. Il arbitre les litiges entre ses membres.

L'UTN peut auditer ses membres. Les Certificats (AC intermédiaires ou UH) des membres de l'UTN peuvent être révoqués, à tout moment, dans les cas prévus par cette PC.

L'UTN peut déléguer tout ou partie de ses fonctions.

1.2 Identification du document

Ce document est la Politique de Certification de l'UTN.

La présente Politique de Certification (PC) est commune à l'ensemble des Autorités de Certification membres de l'UTN. Elle définit les engagements des AC membres du réseau en termes de sécurité et d'organisation des processus d'émission, de gestion et de révocation des Certificats émis par les AC membres.

Un OID est utilisé pour chacune des familles de Certificats délivrées selon la présente PC. Les Certificats correspondant aux familles 1.3.6.1.4.1.15819.5.1.3.(1/5/6/7) sont reconnus comme qualifiés au sens du règlement eIDAS (EU) No 910/2014.

- des Certificats de personnes physiques, en conformité avec [ETSI 319 411-2] niveau QCP-n, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.1 ;
- des Certificats de personne morale, en conformité avec [ETSI 319 411-2] niveau QCP-l, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.5 ;
- des Certificats de personnes physiques, en conformité avec [ETSI 319 411-2] niveau QCP-n-QSCD, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.6 ;
- des Certificats de personnes physiques, en conformité avec [ETSI 319 411-2] niveau QCP-l-QSealCD, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.7 ;
- des Certificats de personnes physiques, en conformité avec [ETSI 319 411-1] niveau LCP, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.3 ;
- des Certificats de personne morale, en conformité avec [ETSI 319 411-1] niveau LCP, correspondant à l'OID 1.3.6.1.4.1.15819.5.1.3.4.

1.3 Entités intervenant dans l'UTN

1.3.1 Autorités de Certification

Une Autorité de Certification (AC) désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

Chaque membre de l'UTN définit une instance de gouvernance par AC : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :

- définir et approuver des pratiques de certification de l'AC (DPC) conformes à la présente PC ;
- définir le processus de mises à jour de la DPC ;
- informer et mettre à disposition de l'UTN la DPC et ses révisions.

1.3.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement (AE) est une composante de l'AC, responsable de l'identification et de l'authentification des demandeurs de Certificats.

1.3.3 Porteurs de Certificats

Le Porteur de Certificat est la personne physique ou morale détentrice du Certificat. Le Porteur a nécessairement adhéré aux conditions prévues par l'Accord de Souscription.

1.3.4 Autorités d'Horodatage

Une Autorité d'Horodatage (AH) désigne l'autorité chargée de la création et la délivrance des Contremarques de temps au titre de la Politique d'Horodatage.

Chaque membre de l'UTN définit une instance de gouvernance par AH : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :

- définir et approuver des pratiques de certification de l'AH (DPH) conformes à la présente PH ;
- définir le processus de mises à jour de la DPH ;
- informer et mettre à disposition de l'UTN la DPH et ses révisions.

Les Autorités de Certification délivrent des Certificats pour les Unités d'Horodatage des AH. Ces Certificats permettent aux Parties Utilisatrices d'identifier l'AH. Les Certificats des UH sont délivrés par une AC Horodatage de l'UTN.

1.3.5 Parties Utilisatrices

Les Parties Utilisatrices sont les personnes, physiques ou morales, souhaitant, pour leur propre besoin, se baser sur les informations contenues dans un Certificat ou une Contremarque de temps ou vérifier la validité de la Contremarque ou du Certificat. Il appartient aux Parties Utilisatrices de vérifier les informations relatives au statut de révocation du Certificat.

Les Parties Utilisatrices sont soumises aux stipulations de l'Accord d'Utilisation.

1.3.6 Responsable de Certificat

- Un Responsable de Certificat est une personne physique qui :
- accomplit les démarches relatives au cycle de vie d'un Certificat de personne morale (de la demande de Certificat à sa révocation) ;

- contrôle l'utilisation de la clé privée correspondant à ce Certificat.

Le Responsable de Certificat est mandaté par le Porteur du Certificat. Le Responsable de Certificat a un lien contractuel, hiérarchique ou réglementaire avec la personne morale détentrice du Certificat et doit être expressément mandaté par elle. Le Responsable de Certificat est soumis aux conditions prévues par la présente PC, par le mandat qui le lie au Porteur et par l'Accord de Souscription.

Le Responsable de Certificat peut être amené à changer pendant la durée de validité du Certificat (départ du Responsable de Certificat de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.). Le Porteur doit notifier sans délai à l'AC le départ ou la révocation d'un Responsable de Certificat et désigner un nouveau Responsable de Certificat. L'AC doit révoquer un Certificat pour lequel le Responsable de Certificat n'est plus identifié.

1.4 Usage des Certificats

1.4.1 Domaines d'utilisation applicables

Bi-clés et Certificats des AC

Les bi-clés associées aux Certificats des AC peuvent être utilisées pour signer :

- les Certificats des AC Intermédiaires (pour les AC Primaires);
- les Certificats des Porteurs (pour les AC Intermédiaires);
- les LCR et/ou les réponses OCSP de l'AC;
- les Certificats des composantes techniques de son infrastructure.

Bi-clés et Certificats des Porteurs

Les bi-clés associées aux Certificats émis par l'AC sont destinées à être utilisées par les Porteurs pour :

- signer au moyen d'une signature électronique des documents (pour les Certificats de personnes physiques émis par une AC Intermédiaire);
- sceller au moyen d'un cachet électronique des documents (pour les Certificats de personnes morales émis par une AC Intermédiaire);
- émettre des Contremarques de temps (pour les Certificats émis par une AC Horodatage).

1.4.2 Domaines d'utilisation interdits

Tout autre usage que ceux prévus au paragraphe 1.4.1 est interdit.

1.5 Gestion de la Politique

1.5.1 Entité gérant ce document

Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.com

1.5.2 Point de contact

Les questions relatives à ce document sont à adresser à :

Le responsable des Politiques
Universign Trust Network
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France
contact@universign.com

1.5.3 Entité déterminant la conformité des pratiques avec la PC

L'UTN détermine l'adéquation d'une DPC à la PC.

1.5.4 Procédures d'approbation de la conformité de la DPC

L'UTN prononce la conformité des DPC à la PC selon un processus d'approbation qu'il définit librement. Ce processus d'approbation prévoit les audits réalisés par l'UTN.

1.6 Définitions et acronymes

Les termes utilisés dans ce document sont les suivants :

Accord d'Utilisation

Désigne l'accord régissant les relations entre l'UTN et les Parties Utilisatrices.

Accord de Souscription

Désigne l'accord régissant les relations entre l'AC et le Porteur.

Autorité de Certification (AC)

Désigne l'autorité chargée de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.

Autorité d'Enregistrement (AE)

Désigne l'autorité chargée de la mise en œuvre des procédures d'identification et de l'authentification des demandeurs de Certificats ;

Autorité d'Horodatage (AH)

Désigne l'autorité chargée de la création et la délivrance des Contremarques de temps au titre de la Politique d'Horodatage.

Certificat

Désigne le fichier électronique délivré par l'Autorité de Certification comportant les éléments d'identification de son Porteur et une clé cryptographique permettant la vérification de la Signature Électronique ou du Cachet Électronique pour lequel il est utilisé.

Contremarque de temps ou Contremarque

Désigne le fichier électronique délivré par l'Autorité d'Horodatage qui lie la représentation d'une donnée à un temps particulier, établissant ainsi la preuve que la donnée existait à cet instant-là.

Déclaration des Pratiques de Certification (DPC)

Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AC pour la mise en œuvre de son service de certification électronique. Ces pratiques sont conformes à la ou aux PC que l'AC s'est engagée à respecter.

Déclaration des Pratiques d'Horodatage (DPH)

Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AH pour la mise en œuvre de son service d'horodatage. Ces pratiques sont conformes à la ou aux PH que l'AH s'est engagée à respecter.

Liste des Certificats Révoqués (LCR)

Désigne la liste identifiant les Certificats émis par l'Autorité de Certification et révoqués.

Object Identifier (OID)

Désignent les numéros d'identification uniques organisés sous forme hiérarchique permettant notamment de référencer les conditions applicables au service de certification ou d'horodatage, e. g. Politique de Certification, ou d'Horodatage, famille de Certificats, Déclaration de Pratiques de Certification ou d'Horodatage.

Online Certificate Status Protocol (OCSP) Un protocole permettant aux Parties Utilisatrices de vérifier le statut d'un Certificat.

Politique de Certification (PC)

Désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du service de certification.

Politique d'Horodatage (PH)

Désigne l'ensemble des règles auxquelles l'AH se conforme pour la mise en œuvre du service d'horodatage.

Unité d'Horodatage (UH)

Ensemble des matériels et des logiciels utilisés par l'AH pour la création de Contremarques de temps. L'UH est identifiée au moyen d'une clé unique de scellement de Contremarques de temps.

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

2.1 Entités chargées de la mise à disposition des informations

L'AC assure la publication des informations relatives au service qu'elle fournit (cf. 2.2).

L'UTN assure la publication de la PC en cours de validité et de ses versions antérieures ainsi que l'Accord d'Utilisation.

2.2 Informations publiées

L'AC s'engage à porter à la connaissance des Porteurs et des Parties Utilisatrices :

- la PC applicables aux Certificats qu'ils utilisent ;
- les conditions d'utilisation du service de certification ;
- la DPC afférente à la PC applicable ;
- les LCR publiées selon les exigences de la PC applicable aux Certificats ;
- les Certificats de l'AC en cours de validité.

L'UTN met à disposition de l'AC un site de publication accessible à l'adresse <http://docs.universign.eu> pour la mise à disposition des informations publiées.

2.3 Délais et fréquences de publication

Les délais et les fréquences de publication varient selon les informations concernées :

- Les LCR sont publiées toutes les heures pour les AC Intermédiaires et tous les jours pour les AC Racines.
- Les Certificats de l'AC sont diffusés ou mis en ligne avant leur utilisation.
- La PC, la DPC et l'Accord d'Utilisation sont publiés après chaque mise à jour.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sont mises à disposition du public conformément à la section 2.1. Elles sont libres d'accès en lecture.

Les ajouts, suppressions et modifications de ces informations sont limités aux personnes autorisées par l'entité en charge des informations publiées.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

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

L'AC et le Porteur sont identifiés par un nom explicite le "*Distinguished Name*" ("DN " ci-après) de type X.501. Les champs du DN et leurs sémantiques figurent dans le tableau ci-dessous.

Une AC peut utiliser des champs supplémentaires qu'elle définit dans sa DPC.

Certificats de personnes physiques Les Certificats de personnes physiques émis par l'AC comportent les champs suivants dans le DN :

| Champ | Obligatoire | Sémantique du champ | Vérfié par l'AE |
|--------------|-------------|--|------------------|
| C | Oui | Nationalité de l'AC | |
| givenName | Oui | Nom de la personne physique | Oui |
| surname | Oui | Prénom de la personne physique | Oui |
| O | Non | Désignation de la personne morale à laquelle est rattachée la personne physique | Oui |
| OI | Non | Identifiant unique légal de la personne morale à laquelle est rattachée la personne physique, structuré suivant l'ETSI 319 412-1 | Oui |
| SERIALNUMBER | Oui | Le numéro de série attribué par l'AE | Oui ² |
| CN | Oui | Nom et prénom d'usage de la personne physique | Oui |

Certificats de personne morale Les Certificats de personne morale émis par l'AC comportent les champs suivants dans le DN :

| Champ | Obligatoire | Sémantique du champ | Vérfié par l'AE |
|-------|-------------|--|------------------|
| C | Oui | Pays d'établissement du Porteur | Oui |
| ST | Non | Etat/Région du Porteur | Oui |
| L | Non | Ville du Porteur | Oui |
| O | Oui | Nom légal du Porteur | Oui |
| OI | Oui | Identifiant unique légal du Porteur structuré suivant l'ETSI 319 412-1 | Oui |
| CN | Oui | Nom libre désignant l'entité utilisatrice | Oui ³ |

3.1.2 Noms explicites

Les noms choisis pour désigner les Porteurs de Certificats doivent être explicites, ils doivent permettre d'identifier de manière directe ou indirecte le Porteur du Certificat.

3.1.3 Anonymisation ou pseudonymisation des Porteurs

L'anonymisation et la pseudonymisation des Porteurs sont interdites.

2. Il sera uniquement vérifié que ce numéro est unique.
3. Il sera uniquement vérifié que le nom est explicite (voir Sect. 3.1.2)

3.1.4 Règles d'interprétation des différentes formes de noms

Pas d'engagement spécifique.

3.1.5 Unicité des noms

Le même DN ne peut pas être attribué par une AC à des Porteurs distincts.

3.1.6 Identification, authentification et rôle des marques déposées

Les Porteurs déclarent être titulaires des droits de propriété intellectuelle associés aux noms, marques, nom de domaine ou autre signe distinctif contenus dans leur Certificat. L'AC ne procède à aucune vérification de ces droits mais s'autorise toutefois à rejeter une demande de Certificat ou à révoquer un Certificat en cas de litige sur ces signes distinctifs. L'AC dégage toute responsabilité en cas d'utilisation non-autorisée d'éléments protégés par des droits de propriétés intellectuelles.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

S'il génère sa bi-clé, un Porteur doit démontrer par des moyens appropriés à l'AC émettrice du Certificat qu'il possède bien la clé privée correspondant à la clé publique à certifier.

3.2.2 Validation de l'identité d'un organisme

Quel que soit le type de Certificat émis, le futur Porteur de Certificat devra fournir les informations et documents utiles à justifier son identité et les éléments qu'il entend faire figurer dans le Certificat. Seuls les éléments strictement nécessaires à l'établissement du Certificat seront demandés par l'AC. Une copie des documents justificatifs d'identité sera conservée par l'AC de façon sûre dans le dossier d'enregistrement du Porteur. L'AC valide l'identité d'une personne physique lors d'un face-à-face physique ou d'une méthode reconnue comme équivalente pour l'émission de Certificats qualifiés.

L'AC informe le demandeur de Certificat de l'utilisation possible des informations transmises (adresse électronique, numéro de téléphone, ...) comme éléments d'authentification.

3.2.3 Validation de l'identité d'un individu

Voir [3.2.2](#).

3.2.4 Informations non vérifiées du porteur

Les informations dont la vérification par l'AE n'est pas prévue sont mentionnées dans la section [3.1.1](#).

3.2.5 Validation de l'habilitation du demandeur

L'AE vérifie l'habilitation d'une personne physique pour représenter une personne morale au cours de la validation de l'identité du Porteur.

3.2.6 Critères d'interopérabilité

Sans objet.

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

Les clés associées aux Certificats ne sont pas renouvelées.

3.3.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

L'AE authentifie le demandeur de révocation, en se basant notamment sur les informations contenues dans le dossier d'enregistrement dans le cas d'une demande de révocation d'un Certificat à destination d'une personne physique. Elle vérifie également l'habilitation du demandeur conformément à la section [4.9.2](#) dans le cas d'une demande de révocation d'un Certificat à destination d'une personne morale.

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 de Certificat est adressée par le Porteur ou par une personne expressément mandatée par le Porteur (i.e. le consentement préalable du futur Porteur est obligatoire).

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

La demande de Certificat comporte les données d'identification du Porteur. Ces données d'identification sont transmises sous sa seule responsabilité.

Le processus d'enregistrement à l'AC nécessite les étapes suivantes :

- Le demandeur lit et accepte l'Accord de Souscription de l'AC ;
- le demandeur fournit les informations requises lors de la demande d'enregistrement. À ce titre, il est garant de l'exactitude des informations fournies et doit fournir à l'AE l'ensemble des éléments nécessaires du dossier d'enregistrement ;
- l'AE valide les éléments du dossier d'enregistrement (voir Section 3.2.3) et les transmet de façon sécurisée à l'AC ;
- le demandeur génère (ou fait générer) sa bi-clé dans un dispositif cryptographique satisfaisant aux exigences de la Section 6.2.11 ;
- le demandeur transmet (ou fait transmettre) sa clé publique à l'AC ;
- le demandeur démontre à l'AC qu'il possède et/ou contrôle sa clé privée conformément à la section 3.2.1.

4.2 Traitement d'une demande de Certificat

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

L'AE valide les demandes de Certificats des Porteurs. L'AE valide les informations fournies par les Porteurs conformément aux dispositions de la section 3.2.

4.2.2 Acceptation ou rejet de la demande

L'AC traite la requête dès sa réception. En cas de rejet de la demande lors de l'une de ces étapes, le demandeur en est informé dans les meilleurs délais.

4.2.3 Durée d'établissement du Certificat

Une demande de Certificat reste effective tant qu'elle n'est pas rejetée. Il n'y a pas de durée maximum d'établissement du Certificat.

4.3 Délivrance du Certificat

4.3.1 Actions de l'AC concernant la délivrance du Certificat

L'AC crée un Certificat à l'issue du processus de validation de la demande de Certificat défini dans la section 4.2. Le Certificat émis est conforme aux informations contenues dans la demande de Certificat et au profil défini dans la section 7.1.

4.3.2 Notification par l'AC de la délivrance du Certificat

L'AC notifie dans un délai raisonnable le demandeur de l'émission du Certificat et le met à sa disposition de façon appropriée.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

Les Certificats sont considérés acceptés en l'absence d'objection dans un délai de 48h après sa mise à disposition ou à la première utilisation de la clé privée associée.

4.4.2 Publication du Certificat

Les Certificats sont publics.

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

Sans objet.

4.5 Usage de la bi-clé et du Certificat

Le Porteur s'engage à utiliser le Certificat conformément :

- à la PC, en particulier pour les seuls usages prévus en section 1.4;
- à l'Accord de Souscription auquel il consent;
- aux conditions particulières prévues entre l'AC et le Porteur, le cas échéant;
- à l'extension KeyUsage ou tout autre extension contraignant l'utilisation de la clé, définie dans le Certificat émis.

Les Parties Utilisatrices consentent aux conditions de l'Accord d'Utilisation avant toute utilisation des Certificats de l'UTN.

Les Parties Utilisatrices sont tenues de :

- déterminer que l'utilisation du Certificat est conforme aux conditions prévues par la PC (voir section 1.4);
- déterminer que le Certificat est utilisé en conformité avec l'extension KeyUsage définie dans celui-ci;
- vérifier le statut du Certificat.

L'AC exclut toute responsabilité en cas d'utilisation du Certificat non conforme à la PC, à l'Accord de Souscription, à l'Accord d'Utilisation ou à un autre accord particulier conclu entre le Porteur et l'AC.

4.6 Renouvellement d'un Certificat

Aucun renouvellement n'est autorisé.

4.6.1 Causes possibles de renouvellement d'un Certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au Porteur de l'établissement du nouveau Certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.6.6 Publication du nouveau Certificat

Sans objet.

4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau Certificat

Sans objet.

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

Aucune délivrance de nouveau Certificat n'est autorisée.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau Certificat

Sans objet.

4.7.3 Procédure de traitement d'une demande d'un nouveau Certificat

Sans objet.

4.7.4 Notification au Porteur de l'établissement du nouveau Certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.7.6 Publication du nouveau Certificat

Sans objet.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau Certificat

Sans objet.

4.8 Modification du Certificat

Toute modification sans renouvellement de Certificat est interdite.

4.8.1 Causes possibles de modification d'un Certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un Certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un Certificat

Sans objet.

4.8.4 Notification au Porteur de l'établissement du Certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du Certificat modifié

Sans objet.

4.8.6 Publication du Certificat modifié

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du Certificat modifié

Sans objet.

4.9 Révocation et suspension des Certificats

4.9.1 Causes possibles d'une révocation

Le Certificat peut être révoqué en cas :

- de demande du Porteur ;
- de non-respect de l'Accord de Souscription ;
- d'inexactitude ou caducité des informations du Certificat ou encore si ces informations portent atteintes aux droits d'un tiers ;
- de soupçons de compromission, de perte ou vol d'une clé privée (en ce compris l'une des clés privées de l'AC) ;
- d'erreur dans la procédure d'enregistrement ;
- de fin des relations contractuelles entre l'AC et le Porteur ;

- de non-paiement relatif du service de certification, le cas échéant ;
- d'arrêt définitif de l'activité de l'AC ;
- de perte du contrôle de la clé privée associée au Certificat du Porteur (vol ou la perte des données d'activation de la clé privée) ;
- d'utilisation du Certificat qui cause ou est susceptible de causer un préjudice à l'AC.

L'AC ne publie pas les causes de révocation.

4.9.2 Origine d'une demande de révocation

Seuls le Porteur, le Responsable de Certificat et l'AC sont autorisés à adresser une demande de révocation du Certificat.

4.9.3 Procédure de traitement d'une demande de révocation

La validation de la demande par l'AC doit inclure la vérification de l'origine de la demande et de sa recevabilité. L'AC authentifie la demande de révocation conformément aux dispositions de la section 3.4 et révoque le Certificat sans délai. Toutes les opérations sont réalisées de façon à garantir l'intégrité, la confidentialité (si nécessaire) et l'authenticité des données traitées pendant le processus. L'AC informe le demandeur de la révocation et le Porteur (s'il s'agit de personnes distinctes) de la révocation effective du Certificat et du changement de statut. Toute révocation est définitive.

4.9.4 Délai accordé au Porteur pour formuler la demande de révocation

La demande de révocation est adressée à l'AC dès que le Porteur a connaissance d'une des causes possibles de révocation. Elle est formulée sans délai.

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

Les demandes de révocation sont traitées sans délai à partir de l'authentification effective du demandeur et de l'acceptation de la demande et dans un délai maximum de 24 heures.

4.9.6 Exigences de vérification de la révocation par les Parties Utilisatrices

Les Parties Utilisatrices sont tenues de vérifier l'état des Certificats et de la chaîne de confiance correspondante.

4.9.7 Fréquence d'établissement des LCR

Les LCR sont établies a minima toutes les 60 minutes.

4.9.8 Délai maximum de publication d'une LCR

Les LCR sont publiées dans un délai maximum de 30 minutes suivant leur génération.

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

Le service de révocation et les statuts des Certificats sont disponibles sur un site internet de publication. Le service d'information sur l'état des Certificats peut inclure un ou plusieurs répondeurs OCSP (protocole de vérification de Certificat en ligne). L'AC indique dans les Certificats qu'elle émet un lien vers le répondeur OCSP à utiliser pour vérifier le statut du Certificat. Les répondeurs OCSP sont disponibles, en fonctionnement normal, 24h/24 et 7J/7.

4.9.10 Exigences de vérification en ligne de la révocation des Certificats par les Parties Utilisatrices

Une Partie Utilisatrice a l'obligation de vérifier le statut d'un Certificat avant de l'utiliser pour vérifier une signature ou un cachet électronique. La Partie Utilisatrice peut soit consulter la LCR publiée la plus récente, soit effectuer une demande de statut du Certificat auprès du répondeur OCSP.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission ou de soupçon de compromission de sa clé privée, l'AC informe les participants de l'UTN par des moyens appropriés des effets préjudiciables d'un tel incident.

4.9.13 Causes possibles d'une suspension

La suspension de Certificats n'est pas autorisée.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un Certificat

Sans objet.

4.10 Fonction d'information sur l'état des Certificats

4.10.1 Caractéristiques opérationnelles

L'AC doit fournir aux Parties Utilisatrices les informations sur le statut des Certificats leur permettant de les vérifier et les valider préalablement à leur utilisation. L'AC assure l'intégrité et l'authenticité des LCR publiées et des réponses OCSP. Les LCR et les réponses OCSP contiennent les informations sur le statut des Certificats jusqu'à leur expiration. Les informations sur le statut des Certificats qualifiés sont conservées au-delà de leur expiration.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible sur plusieurs serveurs de publication assurant une disponibilité en fonctionnement normal de 24h/24 et 7j/7.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre le Porteur et l'AC

La fin de la relation entre l'AC et un Porteur est prévue contractuellement. Le contrat entre l'AC et le Porteur peut prévoir des obligations se poursuivant après l'expiration ou la révocation du Certificat. En l'absence d'une telle clause, la relation prend fin à l'expiration du Certificat ou à sa révocation.

4.12 Séquestre de clé et recouvrement

Il n'est pas procédé au séquestre de clé.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 Mesures de sécurité non techniques

L'AC définit sa Politique de Sécurité de l'Information (PSI). Elle décrit l'approche et les solutions à mettre en place en termes de gestion de la sécurité.

La PSI est maintenue à jour et approuvée par l'AC.

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'AC héberge ses services dans des locaux sécurisés. Ces sites et locaux disposent de mécanismes de sécurité physique permettant d'assurer une protection forte contre les accès non autorisés.

5.1.2 Accès physiques

L'accès aux zones des services de l'AC est restreint aux seules personnes nommément autorisées.

Les locaux sont composés de plusieurs zones de sécurité physique successives. Chaque zone successive offre un accès plus restreint et de plus grande sécurité physique contre l'accès non autorisé, du fait que chaque zone sécurisée est encapsulée dans la précédente.

5.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne porte pas atteinte aux engagements pris par l'AC en matière de disponibilité.

5.1.4 Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre par l'hébergeur pour parer les risques résiduels.

5.1.5 Prévention et protection incendie

Les zones sécurisées sont soumises à des mesures de prévention et de protection incendie appropriées.

5.1.6 Conservation des supports de données

Les supports sont conservés de façon sécurisée. Les supports de sauvegarde sont stockés de manière sécurisée dans un site géographiquement éloigné du support original. Les zones contenant les supports de données sont protégées contre les risques d'incendie, d'inondation et de détérioration. Les documents papiers sont conservés par l'AC dans des locaux sécurisés fermés à clé et stockés dans un coffre-fort dont les moyens d'ouverture ne sont connus que du responsable de l'AC et des personnels habilités. L'AC prend des mesures pour se protéger contre l'obsolescence et la détérioration des médias durant la période de rétention des enregistrements.

5.1.7 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel d'un niveau de sensibilité identique.

5.1.8 Sauvegarde hors site

Afin de permettre une reprise après incident conforme à ses engagements, l'AC met en place des sauvegardes des informations et fonctions critiques hors site de production. L'AC garantit que les sauvegardes sont réalisées par des personnes ayant des Rôles de Confiance. L'AC garantit que les sauvegardes sont exportées hors du site de production et bénéficient de mesures pour la protection de la confidentialité et de l'intégrité. L'AC garantit que les sauvegardes sont testées de façon régulière pour assurer que les mesures du plan de continuité d'activité sont respectées.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les Rôles de Confiance définis dans le présent chapitre sont applicables à toutes les AC membres de l'UTN.

Les Rôles de Confiance suivants sont définis :

Responsable de sécurité : il possède la responsabilité de tous les aspects de la sécurité du système d'information.

Responsable de l'Administration Système : il est responsable des administrateurs systèmes. Il possède des droits d'authentification sur l'ensemble des composantes de l'AC.

Administrateur Système : il est en charge de l'administration et de la configuration de l'ensemble des composants techniques de l'AC ainsi que des opérations d'exploitation quotidienne de l'AC. Il est autorisé à réaliser des sauvegardes et des restaurations.

Auditeur : il est autorisé à auditer les archives et l'intégralité des données d'audits de l'AC.

Contrôleur : il est en charge de l'analyse récurrente des événements intervenant sur les composantes de l'AC.

Porteur de secrets : il assure la confidentialité, l'intégrité et la disponibilité des parts de secrets qui lui sont confiées.

Opérateur d'enregistrement : il assure l'ensemble des opérations d'enregistrement des futurs Porteurs de Certificats.

Les personnels en Rôle de Confiance doivent être libres de tous conflits d'intérêt incompatibles avec leurs missions.

5.2.2 Nombre de personnes requises par tâches

L'AC détermine les procédures et le nombre de personnes ayant un Rôle de Confiance nécessaires pour chaque opération sur les opérations sensibles.

5.2.3 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont prévues afin de mettre en œuvre la politique de contrôle d'accès et la traçabilité des opérations. Les Rôles de Confiance attribués sont notifiés par écrit aux personnes concernées par l'AC. L'AC s'assure régulièrement que l'ensemble des Rôles de Confiance sont pourvus afin d'assurer une continuité de l'activité.

5.2.4 Rôles exigeant une séparation des attributions

L'AC s'assure que les rôles de Responsable de Sécurité et d'Administrateur Système ne sont pas attribués à la même personne.

L'AC s'assure que les rôles de Contrôleur et d'Administrateur Système ne sont pas attribués à la même personne.

L'AC s'assure que les rôles d'Auditeur et d'Administrateur Système ne sont pas attribués à la même personne.

L'AC s'assure que les opérations de sécurité sont séparées des opérations d'exploitation classiques et qu'elles sont réalisées systématiquement sous le contrôle d'une personne ayant un Rôle de Confiance.

5.2.5 Analyse de risque

L'AC réalise une analyse de risque afin d'identifier les menaces sur les services. Cette analyse de risque est revue périodiquement et lors de changements structurels significatifs. De plus, la méthodologie utilisée pour effectuer l'analyse de risque permet de s'assurer que l'inventaire de l'AC est maintenu à jour.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

L'AC s'assure que les attributions des personnels opérant des Rôles de Confiance correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée et est sensibilisé aux procédures de sécurité. Toute personne intervenant dans des Rôles de Confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel. Les personnels opérant des Rôles de Confiance sont nommés par la direction de l'AC.

5.3.2 Procédures de vérification des antécédents

Avant la nomination d'une personne à un Rôle de Confiance, l'AC procède à la vérification de ses antécédents judiciaires et ses compétences professionnelles, de manière à valider son adéquation au poste à pourvoir. Il est notamment vérifié que :

- la personne n'a pas de conflit d'intérêt préjudiciable à l'impartialité des tâches qui lui sont attribuées ;
- la personne n'a pas commis d'infraction en contradiction avec son Rôle de Confiance.

L'AC sélectionne les personnes remplissant les Rôles de Confiance en tenant compte de leur loyauté, leur sérieux et leur intégrité.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement.

5.3.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte leur travail.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont prévues contractuellement. La nature de ces sanctions sont portées à la connaissance des personnes qui remplissent un Rôle de Confiance.

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

Les exigences vis-à-vis des prestataires externes sont contractualisées. Les contrats conclus avec les prestataires prévoient des engagements en matière de confidentialité et de sécurité ainsi que des mesures relatives à l'utilisation des moyens informatiques.

5.3.8 Documentation fournie au personnel

Les règles et procédures de sécurité documentées sont soumises à l'approbation du Comité d'Approbation de l'AC. Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel au sein de l'AC disposent d'un accès aux procédures correspondantes et sont tenues de les respecter.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

- L'AC prend les mesures nécessaires pour enregistrer les événements suivants :
- l'ensemble des événements liés à l'enregistrement (demande de certificat) ;
 - l'ensemble des événements liés au cycle de vie des clés de l'AC ;
 - l'ensemble des événements liés au cycle de vie des certificats émis par l'AC, y compris les événements liés à la révocation ;
 - l'ensemble des événements des différentes composantes de l'AC (démarrage des serveurs, accès réseau, ...).

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées, en particulier en cas de demande émanant d'une autorité judiciaire ou administrative. L'AC décrit dans ses procédures internes le détail des événements et des données enregistrées. Les procédures de traçabilité mises en place par l'AC sont robustes et permettent l'agrégation des traces issues de différentes sources, la détection d'intrusion et un plan de monitoring.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités systématiquement en cas de remontée d'événement anormal.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservés pendant la durée nécessaire aux besoins de preuve dans le cadre de procédures administratives et judiciaires.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont rendus accessibles uniquement au personnel autorisé. Ils ne sont pas modifiables.

5.4.5 Procédure de sauvegarde des journaux d'événements

Les journaux sont sauvegardés régulièrement sur un système externe.

5.4.6 Système de collecte des journaux d'événements

Les systèmes de collecte des journaux d'événements de l'AC ont pour but de fournir des éléments de preuves dans le cadre de procédures judiciaires et en cas de contrôle administratif. Ils contribuent également à assurer la continuité du service. Les informations collectées sont conservées pendant une période appropriée, y compris après la cessation des activités de l'AC. Elles sont pertinentes et proportionnées au regard de leurs finalités.

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

Il n'y a pas de notification des événements.

5.4.8 Evaluation des vulnérabilités

L'AC met en place des contrôles permettant de détecter :

- les accès non autorisés ;
- les anomalies techniques ;
- les incohérences entre les différents événements de l'AC.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :

- la DPC ;
- les Certificats et LCR publiés ;
- les données d'enregistrement des Porteurs ;
 - la preuve de l'acceptation des conditions générales et particulières d'utilisation et/ou de l'Accord de Souscription (voir Section 4.1.2) ;
 - les demandes d'enregistrement des Porteurs ;
 - une copie des éléments ayant permis de vérifier l'identité d'une personne physique ;
 - le dossier d'enregistrement des Porteurs (voir section 3.2) ;
- les journaux d'événements, contenant notamment :
 - les événements relatifs à un changement significatif de l'environnement de l'AC et le moment précis d'occurrence de l'événement ;

- les événements relatifs aux opérations sur les clés et les Certificats émis par l'AC et le moment précis d'occurrence de l'évènement.

L'AC décrit dans ses procédures internes le détail des données et événements qui sont conservés.

5.5.2 Période de conservation des archives

L'ensemble des archives est conservé en conformité avec la législation en vigueur (voir Sect. 9.4.1) et les obligations inhérentes à l'AC (voir Sect. 5.8).

5.5.3 Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité et ne sont accessibles qu'aux personnes autorisées. Ces archives sont consultables et exploitables pendant toute la durée de leur cycle de vie et sont conservées dans un environnement sécurisé.

5.5.4 Procédure de sauvegarde des archives

Des sauvegardes régulières des archives sous forme électronique sont réalisées par les personnes ayant des Rôles de Confiance. Ces sauvegardes sont exportées hors du site de production et bénéficient de mesures de protection de la confidentialité et de l'intégrité.

5.5.5 Exigences d'horodatage des données

Les enregistrements des événements doivent contenir la date et l'heure de l'évènement. Cependant, il n'y a pas d'exigence d'horodatage cryptographique de ces événements.

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives de l'AC sont internes.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux jours ouvrés. Ces archives sont conservées et traitées par des équipes de l'AC.

5.6 Changement de clés

L'AC n'a pas de procédure automatique de renouvellement de clé, cependant une AC doit générer une nouvelle bi-clé et effectuer une demande de Certificat auprès d'une AC Primaire avant l'expiration du Certificat de l'AC en cours de validité.

L'AC doit appliquer toutes les actions nécessaires pour éviter tout arrêt des opérations de l'AC.

5.7 Reprise suite à compromission et sinistre

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

L'AC met en place des procédures et des moyens de remontée et de traitement des incidents. Ces moyens permettent de minimiser les dommages en cas d'incidents.

L'AC met en place un plan de réponse en cas d'incident majeur, tel qu'une compromission de ses mécanismes de publication ou de son mécanisme d'émission de Certificat.

Un incident majeur, tels qu'une perte, une suspicion de compromission ou un vol de la clé privée de l'AC est immédiatement notifié au Comité d'Approbation, qui, si cela s'avère nécessaire, peut décider de faire une demande de révocation du certificat de l'AC auprès de l'UTN et de mettre fin à l'AC.

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

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'AC. Ce plan est testé régulièrement.

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

Ce point est couvert par les plans de continuité et de reprise d'activité. La compromission d'une clé de l'AC entraîne immédiatement la révocation des Certificats délivrés. Dans ce cas, les différents acteurs et entités concernées seront avertis du caractère non sûr de la LCR signée par la clé compromise de l'AC. Des mesures similaires sont prises si la robustesse de l'algorithme utilisé ou celle des paramètres utilisés par l'AC devient insuffisante pour les usages de l'AC.

5.7.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité suite à un sinistre est traitée par le plan de reprise et le plan de continuité d'activité. Suite à un sinistre, l'AC met en place ce plan afin de restaurer les services touchés. En particulier, l'AC a une architecture redondée pour ses services critiques. De plus, l'AC gère un stock de matériel de rechange afin de palier toute panne matérielle. En cas d'incident majeur, l'AC possède un plan de reprise d'activité lui permettant de mettre en place une nouvelle AC dans une durée raisonnable. Ce plan s'appuie sur une salle d'hébergement secondaire.

A la reprise d'activité, l'AC met en œuvre l'ensemble des mesures nécessaires pour éviter qu'un sinistre similaire se reproduise. Les opérations de restauration sont réalisées par des personnels occupant des Rôles de Confiance.

Le Plan de Reprise d'Activité est testé régulièrement.

5.8 Fin de vie de l'AC

En cas d'arrêt définitif, l'AC met en place un plan de fin de vie. Ce plan de fin de vie traite des aspects suivants :

- la notification de l'arrêt aux Porteurs et aux personnes et organismes concernés par le plan ;
- la notification de l'arrêt à l'UTN ;
- la potentielle révocation de tous les Certificats émis encore en cours de validité au moment de la décision de l'arrêt de l'activité ;
- le sort de la clé privée de l'AC ;
- les dispositions nécessaires pour transférer ses obligations relatives aux dossiers d'enregistrement, aux listes de révocations et aux archives des données d'audit ;
- la mise à disposition des informations pour les Parties Utilisatrices.

Ce plan est vérifié et maintenu à jour régulièrement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Les clés de l'AC sont générées :

- lors d'une cérémonie des clés devant témoins ;

- sous le contrôle d'au moins deux personnes ayant des Rôle de Confiance (voir Sect. 5.2.1);
- dans des locaux sécurisés (voir Sect. 5.1);
- au sein d'un HSM répondant aux exigences définies dans la section 6.2.11.

La génération des clés est réalisée selon une procédure précise et donne lieu à la rédaction d'un procès-verbal en fin de cérémonie.

Les Bi-clé à certifier des Porteurs sont générées conformément aux exigences des sections 6.1.5 et 6.1.6.

Les clés publiques des Porteurs sont transmises à l'AC dans les conditions prévues à la section 6.1.3.

6.1.2 Transmission de la clé privée au Porteur

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique à certifier est transmise à l'AC de façon à garantir l'intégrité et l'origine de cette clé.

6.1.4 Transmission de la clé publique de l'AC aux Parties Utilisatrices

Le Certificat de l'AC est publié sur le Site de Publication.

Le Certificat contient les informations figurant au chapitre 7 de la PC.

6.1.5 Tailles des clés

Les clés de l'AC doivent être conformes (ou être cryptographiquement supérieures ou égales) aux caractéristiques suivantes :

| Certificat | Taille des clés | Format |
|------------|---|------------|
| AC | 2048 4096 (pour les clés générées après le 1er janvier 2019) | RSA RSA |

Les clés des Porteurs doivent être conformes (ou être cryptographiquement supérieures ou égales) aux caractéristiques suivantes :

| Certificat | Taille des clésKey Size | Format |
|------------|-------------------------|--------|
|------------|-------------------------|--------|

| | | |
|---------|---|------------|
| Porteur | 2048 4096 (pour les clés générées après le 1er janvier 2019) | RSA RSA |
|---------|---|------------|

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

L'AC et les Porteurs doivent utiliser du matériel certifié (voir Sect. 6.2.11) et des algorithmes dont les paramètres respectent les normes de sécurité idoines. Les paramètres et les algorithmes utilisés sont documentés dans le chapitre 7.

6.1.7 Objectifs d'usage de la clé

Voir chapitre 7.1.

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

Les modules cryptographiques utilisés par l'AC pour la génération et la mise en œuvre de ses clés de signature sont des modules cryptographiques matériels certifiés répondant aux exigences de la section 6.2.11. L'AC s'assure de la sécurité de ces modules tout au long de leur cycle de vie. En particulier, l'AC met en place les procédures nécessaires pour :

- s'assurer de leur intégrité durant leur transport depuis le fournisseur ;
- s'assurer de leur intégrité durant leur stockage précédant la cérémonie des clés ;
- s'assurer que les opérations d'activation, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des Rôles de Confiance ;
- s'assurer qu'ils sont en bon état de fonctionnement ;
- s'assurer que les clés qu'ils contiennent sont détruites lorsqu'ils sont décommissionnés.

6.2.2 Contrôle de la clé privée par plusieurs personnes

La clé privée de l'AC est contrôlée par des données d'activation stockées sur des cartes à puce remises à des porteurs de secrets lors de la cérémonie des clés. Un partage de secret du HSM est mis en œuvre par l'AC.

6.2.3 Séquestre de la clé privée

Les clés privées ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

Les clés privées de l'AC font l'objet de copies de sauvegarde :

- soit hors d'un module cryptographique mais sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant offre un niveau de sécurité équivalent au stockage au sein du module cryptographique et, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Ces copies de sauvegarde des clés privées de l'AC sont stockées dans un coffre-fort sécurisé et accessible uniquement par des personnes ayant des Rôles de Confiance.
- soit dans un module cryptographique équivalent opéré dans des conditions de sécurité similaires ou supérieures.

Les sauvegardes sont réalisées sous le contrôle de deux personnes ayant des Rôles de Confiance.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées.

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

En dehors des copies de secours, les clés privées de l'AC sont générées dans son module cryptographique et ne sont donc pas transférées. Lors de la génération d'une copie de secours, le transfert opéré met en place un mécanisme de chiffrement permettant de garantir qu'aucune information sensible ne transite de manière non sécurisée.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées de l'AC sont stockées dans un module cryptographique. À des fins de copie de secours, le stockage est effectué en dehors d'un module cryptographique moyennant le respect des mesures de la section [6.2.4](#).

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées est contrôlée par des données spécifiques dites données d'activation. Elle est réalisée au sein d'un module cryptographique ré-

pendant aux exigences de la section 6.2.11 sous le contrôle de deux personnes ayant des Rôles de Confiance.

6.2.9 Méthode de désactivation de la clé privée

La désactivation de la clé privée s'opère lors de l'arrêt du module cryptographique.

6.2.10 Méthode de destruction des clés privées

La destruction de la clé privée de l'AC est effectuée à partir de son module cryptographique. L'AC s'assure que toutes les copies de secours correspondantes sont également détruites.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection de clés privées

Module cryptographique de l'AC : Le module cryptographique utilisé par l'AC satisfait aux exigences de certification suivantes :

- EAL 4+ aux Critères Communs ISO/CEI 15408 (conforme au Profil de Protection CWA 14167-2 ou CWA 14167-3); ou
- FIPS 140-2 level 3
- ou équivalent.

Module cryptographique des Porteurs : L'AC ne remet pas de dispositif de création de signature aux Porteurs. Les dispositifs de création de signature des Porteurs doivent satisfaire au minimum aux certifications suivantes :

- EAL 4+ aux Critères Communs ISO/CEI 15408 (conforme au Profil de Protection CWA 14169 ou certifié conforme au Profil de protection Secure Signature Creation Device (SSCD) par une entité gouvernementale européenne);
- FIPS 140-2 level 3
- QSCD ou QSealCD au sens du règlement eIDAS (EU) No 910/2014.
- ou équivalent.

Pour les Certificats émis conformément à l'OID 1.3.6.1.4.1.15819.5.1.3.6, le dispositif doit être un QSCD.

Pour les Certificats émis conformément à l'OID 1.3.6.1.4.1.15819.5.1.3.7, le dispositif doit être un QSealCD.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

L'AC archive ses clés publiques selon les exigences de la section 5.5.

6.3.2 Durées de vie des bi-clés et des Certificats

La durée de vie maximale des Certificats est de :

- 30 ans pour les Certificats d'AC Racine ;
- 20 ans pour les Certificats d'AC Horodatage ;
- 15 ans pour les Certificats d'AC Intermédiaire ;
- 5 ans pour les Certificats de personne physique et les Certificats de personne morale ;
- 11 ans pour les Certificats de personne morale destinés à l'horodatage.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation de la clé de l'AC sont générées durant la cérémonie des clés. Ces données d'activation sont stockées sur des cartes à puce et remises à des porteurs de secret.

Chaque porteur de secrets prend les mesures nécessaires pour se prémunir contre la perte, le vol, l'utilisation non autorisée ou la destruction non autorisée de sa carte à puce et des données d'activation qu'elle contient.

6.4.2 Protection des données d'activation

Les données d'activation sont stockées sur une carte à puce nominative et personnelle. La responsabilité de cette carte à puce incombe à la personne à qui la carte est remise. La carte est protégée par un mot de passe personnel au porteur de secret. Les cartes à puce sont ensuite stockées dans un coffre-fort sécurisé individuel. Chaque porteur de secret est responsable de sa part de secret d'activation. Il exprime son consentement en signant un formulaire définissant ses responsabilités.

6.4.3 Autres aspects liés aux données d'activation

Transmission des données d'activation : La transmission des cartes à puce contenant des données d'activation d'un porteur de secret vers un nouveau porteur de secret doit être réalisée de façon à protéger les données d'activation contre

la perte, le vol, la modification, la divulgation non autorisée ou l'utilisation non autorisée de ces données.

Destruction des données d'activation : Les données d'activation sont décommissionnées de façon à se prémunir du vol, de la perte, de la modification, de la divulgation non autorisée ou de l'utilisation non autorisée de ces données.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Mesures de sécurité technique spécifiques aux systèmes informatiques

L'AC met en place, en fonction du système à protéger, des mécanismes de contrôle appropriés à la plate-forme à sécuriser (afin de se protéger contre l'exécution de code non autorisé ou potentiellement dangereux sur son système).

L'AC met en place des mécanismes de contrôle d'accès et d'authentification pour tous les rôles permettant la génération de nouveaux certificats. Elle maintient ces systèmes de sécurité en permanence.

Ces mécanismes sont décrits dans la DPC.

6.5.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Tous les composants logiciels de l'AC sont développés dans des conditions et suivant des processus de développement garantissant leur sécurité. L'AC met en œuvre des processus qualité au cours de la conception et du développement de ses logiciels. L'AC s'assure, lors de la mise en production d'un élément logiciel, de son origine et de son intégrité et assure une traçabilité de l'ensemble des modifications apportées sur son système d'information.

Les infrastructures de développement et d'essai sont distinctes des infrastructures de production de l'AC.

6.6.2 Mesures liées à la gestion de la sécurité

L'AC s'assure que la mise à jour des logiciels est réalisée de façon à assurer la sécurité du système. L'AC s'assure que le service met en œuvre une politique de révision des composants techniques à intervalles définis. Les mises à jour sont réalisées par des personnels ayant un Rôle de Confiance de l'AC.

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

Sans objet.

6.7 Mesures de sécurité réseau

Les communications réseaux véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Les règles régissant ces contrôles sont vérifiées régulièrement.

Des mesures de sécurité sont mises en place afin de protéger les composantes locales du système d'information des accès non autorisés, en particulier les données sensibles.

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

L'AC met en place des procédures de contrôle d'accès pour séparer les fonctions d'administration et les fonctions opérationnelles. L'utilisation des applications (publication, génération de certificat, révocation) nécessite une authentification des utilisateurs ou des entités. Une politique de contrôle d'accès est mise en place pour limiter l'accès de ces applications aux seules personnes autorisées.

6.8 Horodatage / Système de datation

L'ensemble des serveurs de l'AC est synchronisé avec la même source de temps (UTC). La synchronisation des serveurs est régulièrement contrôlée.

7 Profil des Certificats, des OCSP et des LCR

7.1 Profil des Certificats

Tous les Certificats émis par l'AC sont conformes aux standards X.509, [ETSI 319 412-2], [ETSI 319 412-3] et [ETSI 319 412-5].

Les tableaux ci-dessous indiquent quels champs doivent être présents et leur sémantique le cas échéant. L'AC précise dans sa DPC la valeur des champs de base, ainsi que la nature et la valeur des extensions utilisées.

7.1.1 Certificats

Champs de base

| Champ | Valeur |
|------------|---|
| Version | v3 |
| Issuer DN | <i>Le DN de l'AC conforme à la section 3.1.1</i> |
| Subject DN | <i>Le DN du Porteur conforme à la section 3.1.1</i> |

Extension des Certificats

| Champ | OID | Crit. | Commentaire |
|--------------------------|-------------------|---------|--|
| Authority Key Identifier | 2.5.29.35 | Non | Doit être présent pour les Certificats d'AC Intermédiaire et de Porteur |
| Subject Key Identifier | 2.5.29.14 | Non | Doit être présent |
| Key Usage | 2.5.29.15 | Oui | Doit être présent |
| Basic Constraint | 2.5.29.19 | Oui/Non | Doit être critique pour les Certificats d'AC Intermédiaire, non critique pour les Certificats de Porteur |
| CRL Distribution Points | 2.5.29.31 | Non | Doit être présent et comporter a minima une URL de téléchargement |
| Authority Info Access | 1.3.6.1.5.5.7.1.1 | Non | Doit être présent pour les Certificats d'AC intermédiaire et de Porteur |
| Certificate Policies | 2.5.29.32 | Non | Doit être présent pour les Certificats de Porteur et comporter un OID défini par la présente PC |
| QC Statements | 1.3.6.1.5.5.7.1.3 | Non | Doit être présent pour les Certificats de Porteurs qualifiés |

7.2 Profil des LCR

Champs de base

| Champ | Valeur |
|-------------|----------------------|
| Version | 1 |
| Issuer DN | <i>Le DN de l'AC</i> |
| Next Update | 7 jours maximum |

Extension de LCR

| Champ | OID | Crit. | Commentaire |
|--------------------------|-----------|-------|-------------------|
| Authority Key Identifier | 2.5.29.35 | Non | Doit être présent |
| CRL Number | 2.5.29.20 | Non | Doit être présent |

7.3 Profil des OCSP

L'AC doit préciser si elle fournit un service de vérification de statut OCSP.

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Des audits sont effectués par l'AC :

- un audit interne réalisé
 - soit par des prestataires externes spécialistes du domaine ;
 - soit par un responsable d'audit interne à l'AC.
- un audit de certification à la norme [ETSI 319 411-1] et [ETSI 319 411-2], réalisé tous les 2 ans par un organisme accrédité.

Un contrôle de conformité à la PC en vigueur est effectué :

- lors de la mise en œuvre opérationnelle du système ;
- au moins une fois par année civile (audit interne) ;
- lors de la surveillance ou du renouvellement des certifications, conformément aux procédures réglementaires en vigueur ;
- lorsqu'une modification significative est effectuée.

8.2 Identités / qualifications des évaluateurs

Les évaluateurs doivent s'assurer que les politiques, déclarations et services sont correctement mis en œuvre par l'AC et détecter les cas de non-conformité qui pourraient compromettre la sécurité du service offert. L'AC s'engage à mandater des évaluateurs dont les compétences sont éprouvées en matière de sécurité des systèmes d'information et spécialisés dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

Sauf accord particulier entre l'AC et l'UTN, l'AC désigne l'évaluateur autorisé à effectuer l'audit. L'AC garantit l'indépendance et l'impartialité de l'évaluateur.

8.4 Sujets couverts par les évaluations

L'évaluateur procède à des contrôles de conformité de la composante auditée, sur toute ou partie de la mise en œuvre :

- de la PC ;
- de la DPC ;
- des composants de l'AC.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AC une liste de composantes et procédures qu'ils souhaiteront vérifier. Ils établiront ainsi le programme détaillé de l'audit.

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'évaluateur et son équipe rendent au Comité d'Approbation de l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Avis "échec" : L'équipe d'audit émet des recommandations à l'AC. Le choix de la mesure à appliquer appartient à l'AC.

Avis "à confirmer", l'équipe d'audit identifie les non conformités, et les hiérarchisent. Il appartient à l'AC de proposer un calendrier de résolution des non conformités. Une vérification permettra de lever les non conformités identifiées.

Avis "réussite", l'AC confirme à la composante contrôlée la conformité aux engagements de la PC et de ses pratiques annoncées.

8.6 Communication des résultats

Les résultats des audits de conformité sont transmis au Comité d'Approbation, à l'UTN et mis à la disposition des autorités en charge de la qualification et de la certification du service.

9 Autres problématiques commerciales et légales

9.1 Tarifs

Les membres de l'UTN fixent les conditions tarifaires de leurs services.

9.1.1 Tarifs pour accéder aux Certificats

Sans objet.

9.1.2 Tarifs pour accéder aux informations d'état et de révocation des Certificats

L'accès au service de publication des LCR, aux répondeurs OCSP et au service de révocation est gratuit.

9.1.3 Tarifs pour d'autres services

Pas d'engagement spécifique.

9.1.4 Politique de remboursement

Les services de l'AC ne font l'objet d'aucun remboursement.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Les membres de l'UTN souscrivent à une assurance responsabilité appropriée permettant de couvrir les risques financiers liés à l'utilisation du service qu'elle fournit et conforme à la réglementation applicable à son activité.

Il appartient à l'AC d'évaluer le risque financier devant être couvert.

9.2.2 Autres ressources

L'AC met en œuvre une politique administrative et financière visant à maintenir pendant toute la durée de son activité les ressources financières nécessaires pour remplir les obligations définies par la PC.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Pas d'engagement spécifique.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- les clés privées de l'AC,
- les données d'activation associées aux clés privées de l'AC,
- les journaux d'événements,
- les pièces justificatives des dossiers d'enregistrement,
- les rapports d'audit,
- les causes de révocation des Certificats,
- les plans de continuité, de reprise et d'arrêt d'activité.

D'autres informations peuvent être considérées comme confidentielles par l'AC.

9.3.2 Informations hors du périmètre des informations confidentielles

Le site de publication de l'AC et son contenu sont considérés comme public.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC s'engage à traiter les informations confidentielles conformément aux obligations qui lui sont applicables.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'AC collecte et traite les données à caractère personnel conformément aux réglementations relatives à la protection des données à caractère personnel qui lui sont applicables.

9.4.2 Informations à caractère personnel

Les données à caractère personnel contenues dans les dossiers d'enregistrement et non publiées dans les certificats ou les LCR sont considérées comme confidentielles.

9.4.3 Informations à caractère non personnel

Des accords entre l'AC et les utilisateurs de ses services peuvent prévoir un traitement particulier des informations à caractère non personnel et non confidentiel au sens de l'article 9.3.1.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AC est responsable du traitement des données à caractère personnel des utilisateurs de son service.

9.4.5 Notification et consentement d'utilisation des données personnelles

L'AC informe les personnes dont elle collecte les données à caractère personnel du traitement de ces données et des finalités de ces traitements.

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

Les informations personnelles peuvent être mises à disposition des autorités judiciaires ou administratives dans les conditions prévues par la réglementation.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Des accords entre l'AC et les utilisateurs de ses services peuvent prévoir la divulgation d'informations personnelles dans les limites prévues par la réglementation française.

9.5 Droits sur la propriété intellectuelle et industrielle

Dans le cadre de son activité, l'AC peut être amenée à délivrer ou permettre l'utilisation d'éléments protégés par la propriété intellectuelle et industrielle.

Ces éléments et les droits d'auteur y afférents resteront la propriété du détenteur de ces droits. Les Parties Utilisatrices et les Porteurs peuvent reproduire ces éléments pour leurs usages internes. Une autorisation préalable du détenteur des droits d'auteur est nécessaire pour la mise à la disposition de tiers, extraction ou réutilisation en tout ou en partie, ces éléments ou des œuvres dérivées ou copies de ceux-ci en dehors des nécessités du service de l'AC.

Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, non autorisées par l'autre partie, à d'autres fins que le fonctionnement du service, est strictement interdite et constitue une contrefaçon qui pourra faire l'objet de poursuites judiciaires.

L'utilisation des informations contenues dans les Certificats ou afférentes à leur statut est autorisée dans le strict respect de l'Accord d'Utilisation.

9.6 Interprétations contractuelles et garanties

Les obligations communes des AC de l'UTN sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés cryptographiques privées ;
- utiliser leurs clés cryptographiques privées uniquement dans les conditions et avec les outils spécifiés dans la PC ;
- appliquer et respecter les exigences de la PC et de la DPC leur incombant ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'UTN ;
- accepter les conséquences de ces contrôles et en particulier, remédier aux non-conformités qui pourraient être révélées ;
- documenter leurs processus internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des opérations dont elle est en charge en garantissant la qualité et la sécurité de ces opérations.

9.6.1 Autorité de Certification

L'AC est responsable :

- de la conformité de la DPC vis-à-vis de la PC ;

- de la conformité des Certificats à la PC ;
- du respect de tous les principes de sécurité par les différentes composantes de l'AC et des contrôles afférents.

L'AC est responsable des préjudices causés aux Parties Utilisatrices si :

- les informations contenues dans le Certificat ne correspondent pas aux informations contenues dans le dossier d'enregistrement ;
- l'AC n'a pas révoqué un Certificat et/ou n'a pas publié cette information dans les conditions prévues par la PC.

9.6.2 Service d'enregistrement

Cf. ci-dessus.

9.6.3 Porteur

Le Porteur :

- communique des informations exactes et à jour lors d'une demande d'établissement d'un Certificat ;
- est responsable de l'accès à sa clé privée et le cas échéant, des moyens d'activation de sa clé ;
- respecte les conditions d'utilisation de sa clé privée ;
- informe l'AC de toute modification des informations contenues dans son Certificat ;
- adresse sans délai une demande de révocation de son Certificat en cas de suspicion de compromission de la clé privée correspondante ou des moyens d'activation de cette clé.

9.6.4 Parties Utilisatrices

Les Parties Utilisatrices s'engagent à respecter les obligations prévues par l'Accord d'Utilisation et à prendre connaissance des termes et conditions de la PC applicable au service qu'elles utilisent en particulier des limites d'utilisations et de garanties associées au service.

9.6.5 Autres participants

Pas d'engagement spécifique.

9.7 Limite de garantie

Les limites de garantie de l'AC sont prévues par les Accords de Souscription et d'Utilisation.

9.8 Limite de responsabilité

L'AC n'est pas responsable d'une utilisation des Certificats non autorisée ou non conforme à la PC, à l'Accord de Souscription ou à l'Accord d'Utilisation.

L'AC ne saurait être tenue responsable des dommages indirects liés à l'utilisation d'un Certificat.

L'AC n'est pas responsable de l'utilisation des clés privées associées aux Certificats ou des données d'activation de ces clés.

L'AC n'est pas responsable de l'utilisation non autorisée ou non conforme à leur documentation des équipements et/ou logiciels mis à la disposition des utilisateurs du service de certification.

L'AC décline toute responsabilité en cas de 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.

9.9 Indemnités

Les conditions d'indemnisation des préjudices causés aux Porteurs et aux Parties Utilisatrices sont prévues contractuellement.

9.10 Durée et fin anticipée

9.10.1 Durée de validité

La PC entre en vigueur à compter de sa publication sur le site de publication de l'UTN.

9.10.2 Fin anticipée de validité

La PC reste en vigueur jusqu'à son remplacement par une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sauf dispositions contraires prévues par la présente PC ou par la PC qui viendrait la remplacer, la fin de validité de la PC entraîne l'extinction de toutes les obligations de l'AC applicables aux Certificats émis conformément aux présentes.

9.11 Notifications individuelles et communications entre les participants

Sauf en cas d'accord entre les parties concernées, toutes les notifications individuelles et les communications prévues par la PC doivent être adressées par des moyens garantissant leur origine et leur réception.

9.12 Amendements

9.12.1 Procédures d'amendements

L'UTN peut amender la PC. Ces amendements prennent la forme de nouvelles versions de la PC. Ils sont publiés sur le site de publication de l'UTN. L'UTN détermine si les modifications à la PC nécessitent un changement des OID pour les Certificats émis.

9.12.2 Mécanisme et période d'information sur les amendements

L'UTN peut effectuer des modifications sans notifications sur la PC en vigueur en cas de changement mineur, comme par exemple des corrections typographiques ou d'URL. L'UTN est la seule entité autorisée à apprécier si une modification est mineure ou non.

L'UTN informe ses membres de son intention de modifier la PC, en précisant les modifications proposées et la période de commentaire. Ces propositions de modifications sont également publiées sur le site de l'UTN. Les membres administrant leur propre site de publication doivent y publier les propositions de modifications dès leur réception.

Période de commentaires Sauf en cas d'indication contraire, la période de commentaire est fixée à un (1) mois à compter de la publication de la proposition de modification non-mineures sur le site de publication de l'UTN. Toutes les entités intervenant dans l'UTN peuvent soumettre des commentaires durant cette période.

Traitement des commentaires À l'issue de la période de commentaires, l'UTN peut décider de publier la nouvelle PC ou de procéder à un nouveau processus d'amendement avec une version modifiée ou de retirer la version proposée.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

En cas de modification substantielle de la PC, le Comité d'Approbation de l'UTN peut décider qu'un changement d'OID est nécessaire.

Un changement d'OID pourra être effectué si la modification de la PC est susceptible d'affecter le niveau d'assurance des Certificats déjà émis.

9.13 Dispositions concernant la résolution de conflits

L'AC met en place une procédure adéquate pour permettre le règlement amiable des différends qui l'opposent aux utilisateurs de ses services.

9.14 Juridictions compétentes

En cas de litige entre l'AC et l'UTN découlant de l'interprétation, l'application et/ou l'exécution de la PC et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée aux juridictions compétentes du ressort de la Cour d'appel de Paris.

9.15 Conformité aux législations et réglementations

Les dispositions de la PC sont conformes aux exigences du droit français applicables.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués en référence de la présente politique.

9.16 Dispositions diverses

9.16.1 Accord global

L'AC pourra préciser des exigences spécifiques dans la DPC.

9.16.2 Transfert d'activités

Pas d'engagement spécifique.

9.16.3 Conséquences d'une clause non valide

Dans le cas où une clause de la PC s'avérerait être nulle ou réputée non-écrite de l'avis de la juridiction compétente, la validité, la légalité et le caractère exécutoire des autres clauses ne serait en aucun cas affectées ou réduites.

9.16.4 Application et renonciation

Les exigences définies dans la PC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

9.16.5 Force majeure

L'AC ne saurait être tenue pour responsable des dommages indirects et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs à leurs utilisateurs.

9.17 Autres dispositions

9.17.1 Impartialité

Pour garantir l'impartialité de ses opérations, l'AC s'assure que les personnes qui occupent des Rôles de Confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs missions en particulier lorsque cette mission consiste à la génération et la révocation des Certificats.

9.17.2 Accessibilité

Dans la mesure du possible, l'AC permet aux personnes handicapées d'accéder aux services qu'elle fournit.

Références

[RFC 3647]

Network Working Group - Request for Comments : 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - November 2003.

[ETSI 319 401]

ETSI EN 319 401 V2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers (2016-02)

[ETSI 319 411-1]

ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 : General requirements (2016-02)

[ETSI 319 411-2]

ETSI EN 319 411-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2 : Requirements for trust service providers issuing EU qualified certificates (2016-02)

[ETSI 319 412-2]

ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2 : Certificate profile for certificates issued to natural persons (2016-02)

[ETSI 319 412-3]

ETSI EN 319 412-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3 : Certificate profile for certificates issued to legal persons (2016-02)

[ETSI 319 412-5]

ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5 : QC Statements (2016-02)

[ETSI 319 421]

ETSI EN 319 421 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps (2016-03)

[Règlement eIDAS (EU) No 910/2014]

Règlement (UE) n 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