Déclaration des Pratiques de Préservation

AP Universign

Universign

7, rue du Faubourg Poissonnière, 75009 Paris, France

OID: 1.3.6.1.4.1.15819.7.4.1

VERSION : 1.1	DIFFUSION : PUBLIQUE	Date d'entrée en vigueur :11/03/2022

Table des matières

1 Introduction

1.1 Présentation générale

La présente Déclaration des Pratiques de Préservation définit la mise en œuvre des engagements pris par Universign, membre de l'UTN, pour la délivrance et la gestion de Signatures électroniques augmentées et le rapport associé par l'AP Universign Preservation Authority.

Présentation de l'Universign Trust Network

Le réseau Universign Trust Network (UTN) est un réseau d'Autorités de Certification (AC), d'Autorités d'Horodatage (AH), d'Autorités de Préservation (AP) et d'Autorités de Validation (AV) gouvernées par des politiques communes définies par la société Cryptolog International [1].

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) ;
— d'Autorités de Préservation (AP) ;
— d'Autorités de Validation (AV) ;
— de Porteurs de Certificats finaux ;
— de Parties Utilisatrices.

Organisation de l'Universign Trust Network

Les Autorités de Certification fonctionnent selon une chaine 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 Autorités de Validation permettent de

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.

confirmer la validité d'une signature ou d'un cachet électronique et d'emmetre un Rapport de Validation. Les Autorités de Préservation protègent en intégrité, unitairement, chaque signature ou cachet électronique, qualifié ou non, par le biais d'une extension régulière de la signature ou du cachet.

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

L'UTN :
— publie la Politique de Certification régissant les AC ;
— publie la Politique d'Horodatage régissant les AH ;
— publie la Politique de Service de Préservation régissant les AP ;
— publie la Politique de Service de Validation régissant les AV ;
— gère les AC Primaires du réseau.

Les membres de l'UTN :
— publient leurs Déclarations des Pratiques ;
— gèrent les AC, AH, AP et les AV associées aux services qu'ils proposent.

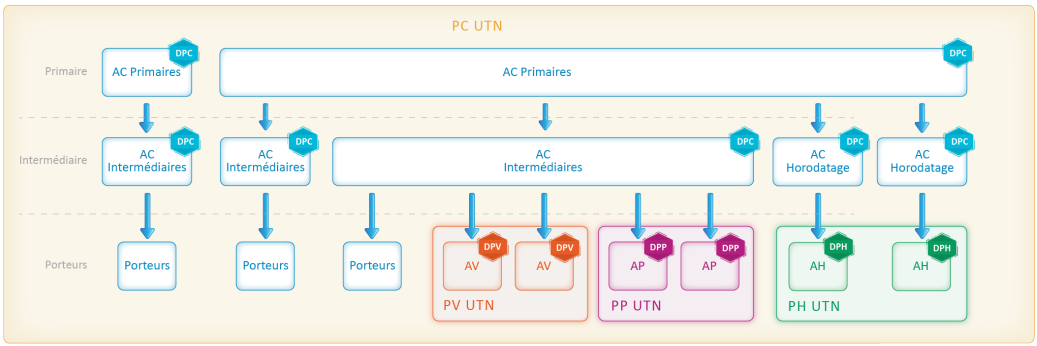


FIGURE 1: Organisation de l'UTN

L'UTN assure la validation, la gestion et la mise en application de la PC, PH, PP et de la PV. L'UTN veille également à la cohérence des référentiels documentaires associés (Accord d'Utilisation, DPC, DPH, DPP, DPV...) 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 la PC.

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

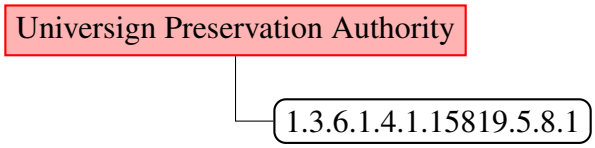
1.2 Identification du document

Ce document est la Déclaration des Pratiques de Préservation de l'AP Universign Preservation Authority, opérée par Universign, membre de l'UTN.

Cette DPP énonce les procédures effectivement mises en œuvre par l'AP pour augmenter des signatures selon les engagements prévus par la PP de l'UTN. Elle est également conforme à la Politique de Service de Préservation de l'ETSI référencée par l'OID 0.4.0.19511.1.2 dans [**ETSI 119 511**]

L'OID attribué à ce document est : 1.3.6.1.4.1.15819.7.4.1

Au sein de la hiérarchie de l'UTN, la présente AP (Universign Preservation Authority) se positionne et émet des Signatures Augmentées à l'OID définis par la PP de l'UTN, tel que résumé comme suit :



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 Autorités de Préservation

Une Autorités de Préservation (AP) désigne l'autorité chargée de l'extension des signatures et cachet électronique avec le but d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique au titre de la Politique de Service de Préservation. L'AP propose une service de conservation des signatures et cachets électronique comme décrit dans le règlement eIDAS (EU) No 910/2014.
NOTE : Dans tout les documents de l'UTN, le terme "préservation" est utilisé pour parler d'une "conservation des signatures ou cachets éléctroniques" comme definit dans le règlement eIDAS (EU) No 910/2014.

Chaque membre de l'UTN définit une instance de gouvernance par AP : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :
— définir et approuver la déclaration de pratique de service de conservation de l'AP (DPP) conformes à la présente PP ;
— définir le processus de mises à jour de la DPP ;
— informer et mettre à disposition de l'UTN la DPP et ses révisions.

1.3.6 Autorités de Validation

Une Autorités de Validation (AV) désigne l'autorité chargée de la création et la délivrance des Rapports de Validation au titre de la Politique de Service de Validation.

Chaque membre de l'UTN définit une instance de gouvernance par AV : le Comité d'Approbation. Il est doté des habilitations nécessaires pour :
— définir et approuver des pratiques de service validation de l'AV (DPV) conformes à la présente PV ;
— définir le processus de mises à jour de la DPV ;
— informer et mettre à disposition de l'UTN la DPV et ses révisions.

1.3.7 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, une Contremarque de temps, une Rapport de Validation ou vérifier la validité de la Contremarque, ou du Certificat, ou de la Signature Augmentée. 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.

1.3.8 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.
- XXX

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
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 Comité d'Approbation
Universign
7, rue du Faubourg Poissonnière, 75009 Paris, France

contact@universign.com

1.5.3 Entité déterminant la conformité des pratiques avec la PP

L'UTN détermine l'adéquation d'une DPP à la PP.

1.5.4 Procédures d'approbation de la conformité de la DPP

L'UTN prononce la conformité des DPP à la PP 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.

Déclaration des Pratiques de service de Préservation (DPP)
Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AP pour la mise en œuvre de son service de préservation. Ces pratiques sont conformes à la ou aux PP que l'AP s'est engagée à respecter.

Déclaration des Pratiques de service de Validation (DPV)
Désigne les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) appliquées par l'AV pour la mise en œuvre de son service de validation. Ces pratiques sont conformes à la ou aux PV que l'AV 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.

Politique de Service de Préservation (PP)
Désigne l'ensemble des règles auxquelles l'AP se conforme pour la mise en œuvre du service de Préservation.

Politique de Service de Validation (PV)
Désigne l'ensemble des règles auxquelles l'AV se conforme pour la mise en œuvre du service de Validation.

Prestataires de Vérification d'Identité à Distance (PVID)
Prestataires de vérification d'identité à distance qualifiés par l'organe de contrôle national, cette qualification lui permettant de proposer un service de validation d'identité équivalent à une vérification d'identité en face-à-face.

Preuve de Préservation
Preuve produite par le service de préservation qui peut être utilisée pour démontrer qu'un ou plusieurs objectifs de préservation sont atteints pour un objet de préservation donné

Rapport de Validation
Désigne le rapport complet de validation de signature fourni par l'application de validation de signature à l'application de signature. Il permet à à toute partie, d'inspecter le détail des actions menées pendant la validation et les causes détaillées de l'indication d'état fournie par l'application de validation de signature.

Signature Augmentée
Signature à laquelle a été ajoutée des données de validation et un jeton d'horodatage pour prolonger la période de validité de cette signature.

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

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

2.2 Informations publiées

L'AP s'engage à porter à la connaissance des Parties Utilisatrices :
— la PP applicables aux Preuves de Préservation qu'ils utilisent ;
— la Politiques de Service de Préservation applicable ;
— le Profil de Préservation applicable qu'ils utilisent ;
— les conditions d'utilisation du service de préservation de signature ;
— la DPP afférente à la PP applicable ;

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

L'AP publie les informations prévues par la section 2.2 sur le site de publication de l'UTN. Elle transmet à l'UTN ces informations dans des délais compatibles avec la section 2.3.

2.3 Délais et fréquences de publication

Les délais et les fréquences de publication varient selon les informations concernées :
— La PP, la DPP 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 Section laissée vide

4 Exigences techniques du service de Préservation

4.1 Protocoles opérationnels et de notification

4.1.1 Protocole de Préservation

Le service est accessible via une confection HTTPS pour garantir la l'identité du service est la confidentialité.

Le Profil de Préservation est accessible via le http://docs.universign.eu.

Il existe un seule Profil de Préservation avec OID 1.3.6.1.4.1.15819.5.8.2 qui est choisi par défaut. Il existe une seule Politique de Preuves de Conservation avec OID 1.3.6.1.4.1.15819.5.8.3 qui est choisie par défaut.

L'appelle est synchrone et retourne dans le cas de succès la Signature Augmentée.

L'utilisateur peux choisir s'il veut réservoir une reçu signé ou pas.

4.1.2 Protocole de Notification

Sans objet.

4.2 Processus de Préservation

4.2.1 Stockage des données et preuves préservées

Sans objet.

4.2.2 Preuves de Préservation

L'AP utilise des Contremarques de temps qualifiés, émis par une AH membre de l'UTN. Les Contremarques sont conforma à [ETSI 319 422]

L'AP cueillit les information de validation correspondant à la Politique de Validation référence dans le Profil de Préservation.

La Signature Augmentée crée par l'AP rajoute les informations de validation et un Contremarque de temps.

Le Contremarque couvre les information de validation et le document et la signature reçu par l'AP.

5 Mesures de sécurité non techniques

L'AP 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'AP.

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'AP 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.

— Le premier datacenter est certifié SSAE16/ISAE3402 SOC-1, ISO 27001, PCI-DSS, FACT, ISO 9001, ISO 50001.
— Le second datacenter est certifié ISO 9001 : 2008, ISO/IEC 27001 : 2005 et ISO 14001.

5.1.2 Accès physiques

L'accès aux zones des services de l'AP 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.

L'accès physique est restreint par la mise en œuvre des mécanismes de contrôle d'accès aux zones hautement sécurisées de l'hébergeur. L'accès à ces salles est renforcé par un contrôle d'accès biométrique. Les profils d'accès à chaque zone sont définis et maintenus par l'AP. Les zones sécurisées des sites et locaux sécurisés de l'AP sont régulièrement inspectés pour vérifier que les systèmes de contrôle d'accès sont toujours opérationnels. Les systèmes de supervision et d'historisation sont mis en œuvre sur tous les sites pour les zones sécurisées. Les contrôles d'accès sont appliqués à toutes les zones sécurisées.

Un cahier de suivi est complété à chaque opération de maintenance réalisée sur les équipements de l'AP. Ce cahier de suivi établit au minimum les informations suivantes :

— la date et l'heure du début d'intervention ;
— le nom et le prénom des intervenants ;
— la description de l'intervention réalisée ;
— la date et l'heure de la fin d'intervention ;
— la signature des intervenants.

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'AP en matière de disponibilité.

Les mesures prises sont :

— Redondance des circuits d'alimentation électrique : N+1
— Redondance de refroidissement : N+1 (pour les refroidisseurs) et N+2 (pour les unités de climatisation en salle)

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.

Les datacenters sont situés hors zone inondable. Des systèmes de détection de fuites d'eau sont en place.

5.1.5 Prévention et protection incendie

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

— Le premier principal comprend une protection incendie : système de détection, extinction par système de brouillard d'eau.
— Le second datacenter comprend un système de sécurité incendie Siemens catégorie A et un système d'extinction incendie automatique par gaz inerte.

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'AP 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'AP et des personnels habilités. L'AP 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'AP met en place des sauvegardes des informations et fonctions critiques hors site de production. L'AP garantit que les sauvegardes sont réalisées par des personnes ayant des Rôles de Confiance. L'AP 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'AP 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 AP 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'AP.

Administrateur Système : il est en charge de l'administration et de la configuration de l'ensemble des composants techniques de l'AP ainsi que des opérations d'exploitation quotidienne de l'AP. 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'AP.

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

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

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'AP 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'AP. L'AP s'assure régulièrement que l'ensemble des Rôles de Confiance sont pourvus afin d'assurer une continuité de l'activité.

Chaque attribution ou révocation d'un Rôle de Confiance fait l'objet d'un formulaire et d'une procédure définie. Un inventaire des Rôles de Confiance est tenu à jour. Les Rôles de Confiance sont revus a minima annuellement.

5.2.4 Rôles exigeant une séparation des attributions

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

L'AP 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.

La tenue d'un inventaire des Rôles de Confiance permet de s'assurer qu'une personne ne dispose pas de plusieurs rôles incompatibles.

5.2.5 Analyse de risque

L'AP 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'AP est maintenu à jour.

L'analyse de risque de l'AP est réalisée suivant la méthode Ebios. Sa pertinence est évaluée a minima tous les deux ans et fait l'objet d'une mise à jour le cas échéant.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

L'AP 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'AP.

5.3.2 Procédures de vérification des antécédents

Avant la nomination d'une personne à un Rôle de Confiance, l'AP 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'AP sélectionne les personnes remplissant les Rôles de Confiance en tenant compte de leur loyauté, leur sérieux et leur intégrité.

Ces vérifications sont menées par l'AP dans le respect de la réglementation en vigueur et préalablement à l'affectation à un Rôle de Confiance. Elles sont revues au minimum tous les 3 ans.

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.

Un plan de formation continue est réalisé. Il est évalué et revu annuellement.

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'AP. 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'AP 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'AP prend les mesures nécessaires pour enregistrer les évènements suivants :
— un empreint du document reçu et de la Signature Augmentée
— le résultat de la préservation (succès, problème de validation, problème d'augmentation

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'AP décrit dans ses procédures internes le détail des évènements et des données enregistrées. Les procédures de traçabilité mises en place par l'AP 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.

Les journaux d'évènements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité dès la détection d'une anomalie et au minimum 1 fois par semaine.

Un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats) est effectué 1 fois par mois

5.4.3 Période de conservation des journaux d'événements

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

Les journaux d'évènements sont conservés sur site pour une durée minimum d'un mois. Les journaux d'évènements sont externalisés tous les mois pour être archivés par l'AP pendant la durée nécessaire aux besoins de fourniture de preuve dans le cadre de procédures judiciaires et administratives conformément à la loi applicable. Les journaux d'évènements sont conservés pendant au moins 7 ans.

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.
La sauvegarde externe des journaux d'événement est quotidienne.

5.4.6 Système de collecte des journaux d'évènements

Les systèmes de collecte des journaux d'évènements de l'AP 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'AP. Elles sont pertinentes et proportionnées au regard de leurs finalités.

Les journaux d'évènement sont conservés 7 ans.
Les fichiers de preuve contenant des données issues des journaux d'évènements sont conservés selon les engagement contractuels applicables et pour une durée maximum de 99 ans.

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

Il n'y a pas de notification des évènements.

5.4.8 Evaluation des vulnérabilités

L'AP met en place des contrôles permettant de détecter :
— les accès non autorisés ;
— les anomalies techniques ;
— les incohérences entre les différents évènements de l'AP.

L'AP met en place les contrôles suivants :
— contrôle quotidien des accès physiques au sein des salles d'exploitation ;
— contrôle quotidien des publications de LCR ;
— analyse quotidienne des évènements et sauvegarde de l'AP. L'ensemble des évènements est ensuite analysé par des personnels occupant des Rôles de Confiance ;
— tests de sécurité (scans de vulnérabilités, tests d'intrusion) et rapports réguliers.

5.5 Archivage des données

5.5.1 Types de données à archiver

Les données archivées sont les suivantes :

L'AP décrit dans ses procédures internes le détail des données et évènements 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'AP (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 évènements doivent contenir la date et l'heure de l'évènement. Cependant, il n'y a pas d'exigence d'horodatage cryptographique de ces évènements.

5.5.6 Système de collecte des archives

Les systèmes de collecte des archives de l'AP 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'AP.

5.6 Changement de clés

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

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

5.7 Reprise suite à compromission et sinistre

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

L'AP 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'AP met en place un plan de réponse en cas d'incident majeur.

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'AP. Ce plan est testé régulièrement.

Ce plan de reprise est testé annuellement.

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'AP entraîne immédiatement la révocation du Certificat de l'AP.

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'AP met en place ce plan afin de restaurer les services touchés. En particulier, l'AP a une architecture redondée pour ses services critiques. De plus, l'AP gère un stock de matériel de rechange afin de palier toute panne matérielle. En cas d'incident majeur, l'AP

possède un plan de reprise d'activité lui permettant de mettre en place une nouvelle AP dans une durée raisonnable. Ce plan s'appuie sur une salle d'hébergement secondaire.

A la reprise d'activité, l'AP 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'AP

En cas d'arrêt définitif, l'AP 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 personnes et organismes concernés par le plan ;
— la notification de l'arrêt à l'UTN ; la révocation du Certificat encore en cours de validité au moment de la décision de l'arrêt de l'activité, utilisé pour signer les rapports de validation 2 mois après l'information des clients ;
— les dispositions nécessaires pour transférer ses obligations relatives 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.
Ce plan est maintenu à jour et revu annuellement.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Les clés de l'AP sont générées par une AC conformément à la PC de l'UTN.

6.1.2 Tailles des clés

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

Certificat	Taille des clés	Format

AC	2048 4096	RSA RSA

6.1.3 Objectifs d'usage de la clé

Voir chapitre des Certificats personnes morales dans la PC de l'UTN

6.1.4 Destruction des bi-clés

Les clés de l'AP sont détruites conformément à la PC de l'UTN.

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

Les clés de de l'AP sont protégé conformément aux Certificats de personnes morales dans la PC de l'UTN.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés de l'AP sont archivé selon les exigences de la PC de l'UTN pour les certificat personnes morales.

6.3.2 Durées de vie des bi-clés et des Certificats

La durée de vie maximale des Certificats de l'AP est 5 ans.

6.4 Mesures de sécurité des systèmes informatiques

6.4.1 Mesures de sécurité technique spécifiques aux systèmes informatiques

L'AP 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'AP 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 DPP.

Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système peut établir l'identité de l'utilisateur qui interagit. Les informations d'authentification sont stockées de façon à ce qu'elles soient uniquement accessibles par les utilisateurs autorisés.

Contrôle d'accès

Les profils et droits d'accès aux équipements de l'AP sont définis et documentés. Ils comprennent également les procédures d'enregistrement et de désenregistrement des utilisateurs. Les systèmes, applications et bases de données sont définis de manière à distinguer et administrer les droits d'accès de chaque utilisateur, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs ou aux deux niveaux. Il est ainsi possible de :

— refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet ;
— limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet ;
— accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

Tout utilisateur non autorisé ne peut accorder ou retirer des droits d'accès à un objet. De même, seuls les utilisateurs autorisés peuvent créer de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée sur les infrastructures de l'AP. Les procédures opérationnelles d'administration et exploitation de l'AP sont documentées, suivies et régulièrement mises à jour. Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les conditions de fin de vie (destruction et mise au rebut) des équipements sont documentées afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.

Les matériels sensibles de l'AP font l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures associées sont documentées. Les personnels concernés par ces procédures sont désignés par la direction de l'AP. Des mesures de contrôles des actions de maintenance sont mises en application.

Intégrité des composantes
Les composantes du réseau local sont maintenues dans un environnement physiquement sécurisé. Des vérifications périodiques de conformité de leur configuration sont effectuées. Les correctifs de vulnérabilités sont appliqués, après qualification, dans un délai raisonnable suivant leur parution.

Sécurité des flux
Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité, le cas échéant, des données échangées entre les différentes composantes.

Journalisation et audit
Un suivi d'activité est possible à partir des journaux d'événements. Il permet notamment d'informer les personnes concernées lorsqu'un incident de sécurité est détecté.

Supervision et contrôle
Une surveillance permanente est mise en place et des systèmes d'alarmes sont installés pour détecter, enregistrer et permettre de réagir rapidement face à toute tentative non autorisée et / ou irrégulière d'accès aux ressources (physique et / ou logique).

Sensibilisation
L'AP met en œuvre des procédures appropriées de sensibilisation des personnels.

6.4.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.5 Mesures de sécurité des systèmes durant leur cycle de vie

6.5.1 Mesures de sécurité liées au développement des systèmes

Tous les composants logiciels de l'AP sont développés dans des conditions et suivant des processus de développement garantissant leur sécurité. L'AP met en œuvre des processus qualité au cours de la conception et du développement de ses logiciels. L'AP 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'AP.

6.5.2 Mesures liées à la gestion de la sécurité

L'AP s'assure que la mise à jour des logiciels est réalisée de façon à assurer la sécurité du système. L'AP 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'AP.

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

Sans objet.

6.6 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'AP 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'AP met également en place un réseau d'administration déconnecté du réseau nominal.

L'AP 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.

6.7 Horodatage / Système de datation

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

7 Section laissée vide

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

Des audits sont effectués par l'AP :
- un audit interne réalisé
  - soit par des prestataires externes spécialistes du domaine ;
  - soit par un responsable d'audit interne à l'AP.
- un audit de certification à la norme [ETSI 119 511], réalisé tous les 2 ans par un organisme accrédité.

Un contrôle de conformité à la PP en vigueur est effectué :
- lors de la mise en œuvre opérationnelle du système ;
- 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'AP et détecter les cas de non-conformité qui pourraient compromettre la sécurité du service offert. L'AP 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'AP et l'UTN, l'AP désigne l'évaluateur autorisé à effectuer l'audit. L'AP 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 PP ;
- de la DPP ;
- des composants de l'AP.

Avant chaque audit, les évaluateurs proposeront au Comité d'Approbation de l'AP 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'AP, un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

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

Avis "réussite", l'AP confirme à la composante contrôlée la conformité aux engagements de la PP 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 conditions tarifaires des services en vigueur sont publiées sur le site internet www.universign.com ou convenues avec l'utilisateur du service dans le cadre d'un contrat commercial.

9.1.1 Tarifs pour d'autres services

Pas d'engagement spécifique.

9.1.2 Politique de remboursement

Les services de l'AP 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'AP d'évaluer le risque financier devant être couvert.

9.2.2 Autres ressources

L'AP 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 PP.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de préjudice subi par un Porteur ou une Partie Utilisatrice du service du fait d'un manquement par l'AP à ses obligations, l'AP pourra être amené à réparer le préjudice dans les limites prévues par ses engagements contractuels.

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'AP,
— les données d'activation associées aux clés privées de l'AP,
— les journaux d'événements,
— les rapports d'audit,
— les documents signés envoyés à l'AP,
— les plans de continuité, de reprise et d'arrêt d'activité.

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

L'AP garantit que seuls les personnels détenant le besoin d'en connaître ont accès et peuvent utiliser aux informations confidentielles. Ces personnels sont tenus par une obligation de confidentialité.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilités en termes de protection des informations confidentielles

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

L'AP met en place des procédures de sécurité pour garantir la confidentialité des informations confidentielles au sens de l'article 9.3.1. L'AP respecte la législation et la réglementation en vigueur sur le territoire français en matière de mis à disposition des informations à des tiers dans le cadre de procédures judiciaires ou administratives.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

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

L'AP s'engage en particulier à se conformer à la réglementation en vigueur sur le territoire français.

En particulier, l'AP informe les personnes dont les données à caractère personnel sont traitées, de leurs droits d'accès, de rectification des données erronées les concernant, et dans les cas et selon les limites prévues par la règlementation, d'opposition, de suppression de certaines de leurs données, d'en faire limiter l'usage ou de solliciter leur portabilité en vue de leur transmission à un tiers.

9.4.2 Informations à caractère personnel

Sans objet. Le traitement des données à caractère personnel est régi par la Politique de Protection des Données personnelles.

9.4.3 Informations à caractère non personnel

Des accords entre l'AP 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'AP 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'AP informe les personnes dont elle collecte les données à caractère personnel du traitement de ces données et des finalités de ces traitements.

L'AP porte à leur connaissance les droits dont elles disposent et leur modalité d'exercice au moyen d'une Politique de Protection des Données Personnelles à laquelle ils consentent expressément.

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'AP 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'AP 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 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'AP.

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 Signatures Augmentées ou Rapports de Validation 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 AP 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 PP ;
— appliquer et respecter les exigences de la PP et de la DPP 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-confirmités 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 Préservation

L'AP est responsable :
— de la conformité de la DPP vis-à-vis de la PP ;
— de la conformité des Signatures Augmentées à la PP ;
— du respect de tous les principes de sécurité par les différentes composantes de l'AP et des contrôles afférents.

L'AP est responsable des préjudices causés aux Parties Utilisatrices si les informations contenues dans la Signature Augmentée ne correspondent pas aux informations contenues dans la signature d'origine ;

9.6.2 Service d'enregistrement

Sans objet.

9.6.3 Porteur

Sans objet.

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 PP 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'AP sont prévues par l'Accord d'Utilisation.

L'AP ne dispose d'aucun pouvoir ni de représentation, ni d'engager l'UTN, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'UTN.

9.8 Limite de responsabilité

L'AP n'est pas responsable d'une utilisation des Signatures Augmentées non autorisée ou non conforme à la PP, ou à l'Accord d'Utilisation.

L'AP ne saurait être tenue responsable des dommages indirects liés à l'utilisation d'un Signatures Augmentées.

L'AP 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 préservation de signature.

La responsabilité de l'AP est limitée selon les termes et les conditions prévus par l'Accord de Souscription et / ou l'Accord d'Utilisation ou tout autre accord particulier conclu entre l'AP et l'utilisateur du service.

9.9 Indemnités

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

9.10 Durée et fin anticipée

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

La DPP 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 PP ou par la PP qui viendrait la remplacer, la fin de validité de la PP entraîne l'extinction de toutes les obligations de l'AP, 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 PP doivent être adressées par des moyens garantissant leur origine et leur réception.

9.12 Amendements

9.12.1 Procédures d'amendements

L'AP peut amender la DPP. Ces amendements prennent la forme de nouvelles versions de la DPP. Ils sont publiés sur le site de publication de l'AC ou de l'UTN.

9.12.2 Mécanisme et période d'information sur les amendements

L'AP informe l'UTN de son intention de modifier la DPP, en précisant les modifications proposées et la période de commentaire. Si l'AC administre son propre site de publication, elle doit y publier les propositions de modifications. Ces propositions de modifications sont également publiées sur le site du l'UTN.

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'AP. 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'AP peut décider de publier la nouvelle DPP 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 DPP, le Comité d'Approbation de l'AP peut décider qu'un changement d'OID est nécessaire.

9.13 Dispositions concernant la résolution de conflits

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

La durée maximale de la procédure de règlement des différends est de 3 mois.

Les modes alternatifs de règlement amiable des litiges sont portés à la connaissance des utilisateurs du service au moyen de l'Accord d'Utilisation ou de tout autre document contractuel.

9.14 Juridictions compétentes

Dans le cas d'un litige entre l'AP et un utilisateur du service découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée aux juridictions du ressort de la Cour d'appel de Paris.

9.15 Conformité aux législations et réglementations

Les dispositions de la DPP sont conformes au droit français.

9.16 Dispositions diverses

9.16.1 Accord global

Pas d'engagement spécifique.

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 DPP 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 DPP doivent être appliquées selon les dispositions de la PP 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'AP 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.

Sont considérés comme des cas de force majeure les événements qualifiés habituellement par le droit et la jurisprudence française.

9.17 Autres dispositions

9.17.1 Impartialité

L'AP met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnes amenées à occuper un Rôle de Confiance. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions. Ces vérifications sont menées préalablement à l'affectation à un Rôle de Confiance et revues régulièrement (au minimum tous les 3 ans).

9.17.2 Accessibilité

Dans la mesure du possible, l'AP 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)

[**ETSI 319 422**]
ETSI EN 319 422 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ; Time-stamping protocol and time-stamp token profiles (2016-03)

[**ETSI 119 441**]
ETSI EN 119 441 V1.1.1 - Electronic Signatures and Infrastructures (ESI) ;

Policy requirements for TSP providing signature validation services (2018-08)

[**ETSI 119 511**]
ETSI EN 119 511 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques (2019-06)