GUIDE DE BONNES PRATIQUES DES PARCOURS DIGITAUX ET DE CONSENTEMENT

fntc

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE

SOMMAIRE

INTRODUCTION :

A. Contexte

Le contexte réglementaire de la signature électronique et plus généralement des services de confiance a évolué ces dernières années, notamment par le déploiement progressif du règlement eIDAS.

Ce dispositif repose sur une politique d'engagement des prestataires de services de confiance sur chacune des activités (certificat, vérification de certificat, cachet, recommandé électronique, horodatage, préservation des signatures) outillant notamment un parcours de consentement « digitalisé ».

La confiance repose sur la **fiabilité des prestataires** de service de confiance, notamment pour les services conformes à eIDAS ou à des réglementations nationales (RGS, ...).

eIDAS harmonise l'identité numérique et les services de confiance entre les Etats membres pour des applications métier selon différents niveaux de garantie ou fiabilité. La sécurité repose essentiellement sur **la garantie des identités numériques**. L'identité numérique « élevée » et la signature électronique « qualifiée » restent cependant peu déployées, notamment en mode BtoC alors que le besoin de dématérialiser les consentements avec la signature électronique a été accentué par l'épidémie de COVID-19.

En conséquence, **le marché se déploie** doucement sur les dispositifs qualifiés et **rapidement sur les dispositifs non qualifiés**, qui répondent à un besoin du marché lorsque le niveau de risque est modéré et que le contexte n'est pas réglementé. Cette tendance pourrait s'inverser avec le déploiement massif de l'identité numérique, des titres d'identité numériques et l'interopérabilité d'outils d'authentification sécurisée souverains.

Les services de confiance, quels que soient leurs niveaux, doivent intégrer un **processus de consentement** qui est lui-même généralement inclus **dans un parcours numérique** complet.
Le consentement est en effet une étape dans un processus métier. Les données collectées en amont et en aval du consentement ont une valeur métier importante et contribuent au **faisceau de preuves** opposable notamment en cas de contentieux.

L'étape finale du parcours digital est la **conservation** des **documents**, **actions** ou affichages produits durant le parcours, ainsi que les **données** et **éléments de preuve**. Ceci a pour conséquence de repositionner la proposition de valeur de l'archivage électronique : cette valeur porte autant sur la préservation du document et sa « vocation probatoire » que sur la **préservation du contexte de production**. Le contexte de production est le faisceau de preuves permettant de démontrer a posteriori que le parcours de consentement était conforme à l'état de l'art au moment du consentement. En ce sens, l'archivage se repositionne sur son origine, la diplomatique, science visant à gérer l'authenticité des documents, porté principalement par **l'intégrité de la forme et l'imputabilité aux consentants.**

L'enjeu actuel n'est pas tant de garantir que chaque composant du parcours de consentement est conforme mais **d'assurer que l'agrégation de l'ensemble des composants dans une chaine de confiance étendue au parcours permettant de fournir les éléments de preuve** nécessaires pour être en mesure de démontrer la cohérence et fiabilité du processus a posteriori.

Cette démonstration nécessite d'assurer une bonne **intelligibilité des éléments de preuve** conservés pour un lecteur humain qui n'est pas nécessairement expert dans les technologies ou traces produites par les machines.

Actuellement, il n'existe pas en France de référentiel permettant d'évaluer la fiabilité d'un parcours de consentement dans son ensemble, ni de standard permettant d'interopérer les éléments de preuve du parcours dans un dispositif d'archivage.

Dans ce contexte, la Fédération des Tiers de Confiance du numérique (FnTC) a trouvé opportun d'investir ce sujet en proposant un **référentiel de bonnes pratiques** aux organisations qui conçoivent, opèrent ou évaluent des parcours de consentement.

B. Objectif du référentiel

Ce document est un référentiel des bonnes pratiques proposées par les membres du groupe de travail « Parcours de consentement ».
Il reprend en partie les travaux des autres groupes (e-finance, blockchain, signature, archivage, ...) du fait de la portée transverse du sujet.

Les objectifs du référentiel sont de :

- **Définir un parcours** de consentement et le processus de consentement;
- **Proposer un cadre documentaire** pour la qualification d'un parcours;
- Aider à la **définition d'une stratégie** de sécurité du parcours, proportionnée aux risques liés au sujet traité;
- Modéliser les principales étapes du parcours et **identifier les bonnes pratiques** sur chaque étape;
- Proposer des bonnes pratiques en matière de **traçabilité**, base de la constitution des **éléments de preuve;**
- Préparer la collecte pour **l'archivage** des documents et données engageants ainsi que les éléments de preuve technique associés.

Ce référentiel est une aide à la conception, évaluation et valorisation de la fiabilité du parcours de bout en bout : de son initialisation à son archivage.

L'enjeu pour les organisations opérant les parcours est d'améliorer la maîtrise du risque juridique et technologique des parcours opérés par leurs soins ou par leurs prestataires.

C. Domaine d'application

Le domaine d'application du référentiel prend en compte **l'ensemble des éléments contextuels d'un parcours** numérique pouvant contenir des informations relatives à la relation client/usager (KYC...), des processus métier (validations internes...), des relations juridiques (acceptations de CGU, informations RGPD...) et le processus final du parcours, qui peut être une signature (identification, production de certificat, signature, vérification de signature...), un paiement, un consentement dans le domaine de la santé.

Exemples :

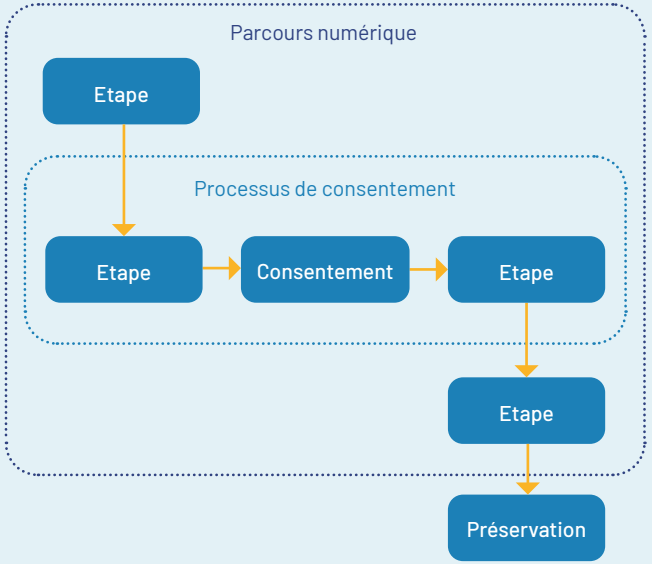
- Pour un parcours de signature, la fiabilité et la conservation ne sont pas limitées aux documents signés durant le parcours, mais également aux données collectées et produites concernant le parcours. Les considérations RGPD sont prises en compte ainsi que les exigences liées aux services de confiance et les exigences particulières liées au métier selon le secteur.
- Pour un parcours d'achat avec paiement en ligne, les données constituant l'identification du client, la commande, l'acceptation des CGV, des données de livraison... peuvent constituer des éléments de preuves.

Les bonnes pratiques sont rédigées avec une **souplesse permettant d'adapter le niveau de sécurité au risque** porté par l'acte consenti et à l'enjeu métier objet du parcours, par exemple à une efficience commerciale liée à la fluidité du parcours. A ce titre le domaine d'application n'est pas limité au niveau qualifié, ni aux technologies de signature électronique mais reste ouvert à tout procédé permettant de formaliser un consentement.

QUALIFICATION D'UN PARCOURS DE CONSENTEMENT

A. Qu'est-ce qu'un parcours de consentement ?

Un parcours de consentement est un processus, généralement intégré dans un parcours numérique, dont l'objectif est de recueillir le consentement d'une ou plusieurs personnes sur un acte.



2

1. Le consentement : définition

Dans un contexte numérique, il est indispensable que les parties manifestent leur consentement lorsqu'elles s'engagent contractuellement par voie électronique, au même titre que lors de la contractualisation sur support papier, dans la mesure où le consentement des parties est l'une des conditions essentielles de la validité d'une convention comme cela est précisé par l'article 1128 du Code civil.

Définition

La manifestation du consentement des parties à l'acte tend à rendre apparente l'intention d'accepter les termes de l'acte et ainsi à rendre opposables aux parties contractantes les obligations qui en découlent. De manière générale, (et sous réserve des actes unilatéraux) le consentement peut se définir comme une rencontre ou un accord d'au moins deux ou plusieurs volontés permettant à la convention de produire des effets de droit.

Méthode de consentement

Sous réserve de l'analyse de la réglementation applicable, la méthode de consentement est a priori libre, l'important étant de pouvoir démontrer a posteriori l'intention, une volonté de contractualiser.

La méthode de consentement ne doit pas être confondue avec la méthode d'identification ou d'authentification d'une personne.

Vice du consentement

Un consentement peut être vicié quel que soit le support de consentement, papier ou numérique.

Il s'agit des vices suivants :

- L'erreur (art. 1132 à 1136 du Code civil). L'erreur de droit ou de fait est une cause de nullité, pourvu qu'elle soit excusable, lorsqu'elle porte « sur les qualités essentielles de la prestation de l'une ou de l'autre partie » (et non plus seulement « sur la substance ») ou sur celles du cocontractant, si le contrat a été conclu en considération de la personne ;
- Le dol (art. 1137 à 1139 du Code civil). Le premier article, au-delà de la définition usuelle du dol, reconnaît expressément le même effet au dol par réticence, défini comme « la dissimulation intentionnelle par l'un des contractants d'une information dont il sait le caractère déterminant pour l'autre partie ». Le second réaffirme que le dol doit émaner du cocontractant ;
- La violence (art. 1140 à 1143 du Code civil). En outre l'article 1143 du Code civil qualifie de violence l'abus de l'état de dépendance du cocontractant en vue d'obtenir un engagement qui n'aurait pas été souscrit en l'absence d'un tel état et dont l'auteur de la violence tire « un avantage manifestement excessif ».

Cas particulier :
le consentement RGPD

Le consentement explicite au traitement de données à caractère personnel (art 6,7 et 8 du RGPD notamment) est un des aspects les plus visibles de la conformité d'une organisation.

Il répond à des enjeux spécifiques qu'on peut situer à 4 niveaux :

Validité du consentement

En tant que base légale sur laquelle s'appuient certains traitements informatiques, un des premiers enjeux est d'assurer la validité des consentements collectés.

Le RGPD, la directive ePrivacy, les Guidelines de l'edpb (European Data Protection Board), entre autres, en fixent les conditions :

- le consentement doit être libre (il doit offrir un choix réel, sans contrainte ni préjudice, ni être lié à l'acceptation d'un contrat ou de CGU) ;

- le consentement doit être spécifique (pour des finalités bien précises et avec une granularité suffisante) ;

- le consentement doit être éclairé (les informations fournies sur les données utilisées et les finalités doivent être claires et exprimées dans un langage accessible) ;

- le consentement doit être univoque (il requiert une action ou une affirmation positive, sans cases pré-cochées) ;

- le consentement doit être révocable (à tout moment et aussi simplement qu'il a été donné).

Auditabilité

La validité du consentement doit pouvoir être démontrée par le responsable de traitement à tout moment. Il s'agit donc de conserver des preuves que les cinq conditions précédentes ont bien été respectées. Elles seront utiles :

- en cas de contrôle par une autorité de contrôle comme la CNIL ;

- en cas de contestation par un utilisateur ou un partenaire.

Une bonne pratique consiste donc à générer des reçus de consentements lisibles par un être humain et par une machine, idéalement horodatés ou cacheté, notamment pour en garantir l'intégrité.

Attention : si un consentement est déclaré non-valide, la conséquence est l'effacement immédiat des données personnelles et l'impossibilité de se prévaloir d'une autre base légale pour les traitements envisagés. Au-delà de l'amende potentielle encourue, le préjudice en termes d'image peut s'avérer être la plus lourde sanction.

Exploitation

La gestion des consentements ne se limite pas à une action ponctuelle de collecte. Il convient d'anticiper notamment la gestion du cycle de vie (révocation, conservation, renouvellement…).

Attention : un consentement RGPD étant une donnée personnelle à part entière, il ne peut pas être conservé ou archivé pour une durée illimitée. Il convient de décider d'une durée de conservation adéquate selon les finalités.

Expérience utilisateur

La gestion des consentements implique des interactions régulières avec les personnes concernées (clients, adhérents, citoyens, patients…) A ce titre, c'est une composante à part entière de la qualité de la relation et de la confiance envers une organisation.

2. Parcours numérique

Un parcours numérique est une série d'étapes dématérialisées que les utilisateurs finaux suivent lorsqu'ils interagissent avec un organisme ou une entreprise, en vue de conclure une transaction. Il peut s'agir de l'inscription à un service, de l'achat d'un produit ou de toute autre interaction numérique avec l'entreprise. Les parcours numériques sont généralement conçus pour aider les utilisateurs finaux à effectuer une action spécifique et pour aider l'entreprise et les utilisateurs finaux à atteindre un objectif précis.

Ces parcours peuvent être en ligne, multi et cross canaux, synchrones ou asynchrones… Ils peuvent également être réalisés physiquement et supporté par une traçabilité numérique du processus.

Ces utilisateurs finaux utilisent ces parcours numériques pour différents objectifs et, en fonction, le parcours sera pensé de manière différente, en particulier au niveau du consentement et de son faisceau de preuves.

3. Processus de consentement

Un processus de consentement peut être défini comme un processus intégré dans un parcours numérique visant à recueillir le consentement d'une personne pour un acte formalisé dans un document numérique ou une transaction et produisant l'ensemble des preuves nécessaires à la démonstration du caractère probant du parcours digital complet.

Les parcours numériques ne peuvent pas être efficaces sans le consentement de l'utilisateur final pour atteindre l'objectif. Le consentement est une partie importante du parcours digital car il permet aux clients de contrôler leur interaction avec l'entreprise. Les entreprises doivent obtenir le consentement des clients pour collecter et utiliser par exemple leurs données personnelles.

Mais, au-delà du consentement sur l'utilisation et ou la validation des données personnelles critiques ou non critiques, s'ajoute le consentement sur les termes d'une commande, d'un contrat et/ou d'un paiement, d'un acte, et d'autres consentements réglementaires peuvent être nécessaires.

1 G29 – Lignes directrices sur le consentement au sens du règlement2016/679– WP259 du 10/04/2018 (p.20), disponible à l'adresse https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf.

2 CNIL - Conformité RGPD : comment recueillir le consentement des personnes ? - 03 août 2018.

Donc durant un parcours numérique plusieurs typologies de consentements sont nécessaires. Trois exemples sont présentés ci-dessous :

a) Parcours commercial numérique

Dans le domaine de l'expérience client, les parcours numériques permettent de fournir une expérience personnalisée et cohérente à travers différents canaux. Les entreprises utilisent des données sur les clients pour personnaliser les parcours numériques, offrir des recommandations et des offres personnalisées, et améliorer la satisfaction des clients. Les parcours numériques permettent également aux clients de prendre des décisions informées sur les produits et services qu'ils achètent. Et surtout la fluidité prévaut, jusqu'à l'acte de validation de la commande et du paiement.

Ces deux consentements sont souvent de la validation :

- Des données personnelles;
- Des éléments constitutif de la commande : biens ou services commandés, lieu de facturation et livraison (le cas échéant);
- Du paiement;

b) Parcours numérique pour les souscripteurs

Les parcours numériques pour les souscripteurs sont utilisés par exemple dans les domaines de l'assurance, des services financiers et de l'abonnement en ligne à des services (telecom, transport, services en ligne, presse…). Les parcours numériques permettent aux souscripteurs de trouver rapidement et facilement les offres qui correspondent le mieux à leurs besoins, tout en bénéficiant d'une expérience client simplifiée et efficace (très proche du parcours commercial).

L'accord sur les termes de la souscription et du paiement éventuels sont également couplés.

c) Parcours numérique social et santé

Dans le cas du social et de la santé, les consentements portent essentiellement sur l'utilisation des données personnelles et leur validation ainsi que l'engagement à fournir des informations justes.

Dans tous ces cas de figure, la traçabilité des consentements est nécessaire pour des raisons réglementaires : RGPD, Code du commerce, Code monétaire et financier, …

Le faisceau de preuves à constituer doit retracer parfois l'ensemble des étapes du parcours numérique, les textes affichés et consentis avec la typologie du consentement : case à cocher, double facteur, …

B. Stratégie

A l'initialisation de la conception d'un parcours digital, il est recommandé de faire **convenir** les différentes parties prenantes du **niveau de contrainte** imposé aux utilisateurs finaux et du **niveau de risque** associé pour l'organisation.

Les parties prenantes de l'organisation sont par exemple :

- Le commerce / marketing dont l'objectif est de disposer du parcours numérique le plus fluide possible pour **optimiser la performance commerciale**;
- Le juridique / conformité / anti-fraude / SSI dont l'objectif est de **protéger l'organisation** du risque induit par le parcours numérique;
- Le métier dont l'objectif est d'appliquer ses bonnes pratiques opérationnelles et **d'optimiser sa charge;**
- L'informatique dont l'objectif est de maintenir les solutions mises en œuvre et **respecter ses budgets.**

Les parties contractantes externes à l'organisation (usagers, prospects, clients, fournisseurs, ...) doivent également être prises en compte pour évaluer le **niveau de contrainte acceptable** par rapport à leurs profils.

La définition d'une stratégie claire est fortement recommandée comme élément d'entrée pour la conception d'un parcours numérique. Cette stratégie servira aux concepteurs et notamment les UX Designer pour élaborer une cinématique d'utilisation adaptée aux types d'utilisateurs et de contractants.

D'un strict point de vue juridique, le point sera également de déterminer sur quels objets numériques porte le Parcours digital. En effet, s'il s'agit de rapporter la preuve d'un acte juridique (ex : un contrat), alors ce sont les règles applicables à la preuve littérale qui trouveront à s'appliquer et il conviendra de disposer d'un écrit signé (qui pourra être contenu dans un dossier de preuve). Par contre, s'il s'agit de traces (ex : données de connexion, date, montant pour un paiement), alors la preuve sera libre. Cela signifie qu'une personne pourra utiliser tout type d'élément licitement collecté pour rapporter la preuve de ce qu'il avance en justice. C'est pourquoi il est important de préciser en amont, avant la conception, quels sont les objets techniques (contrat, traces...) soumis au Parcours digital; le paramétrage sera différent.

Le **processus de consentement** est particulièrement sensible dans le parcours digital car il requiert un niveau de contrainte élevé sur les contractants si l'on souhaite disposer d'un niveau élevé de sécurité. Le choix d'un niveau adapté est donc essentiel pour **disposer du meilleur compromis entre la fluidité** générale du parcours, le **risque induit** et les **coûts associés**.

Les stratégies envisageables pour le processus de consentement peuvent être, par exemple :

- **de limiter la contrainte** sur l'identification des consentants et renforcer les éléments de preuve contextuels (authentification, paiement, justificatifs,...) notamment quand les contractants ne disposent pas d'identité numérique fiable et sur des enjeux modérés de l'acte consenti;
- **d'augmenter la robustesse** sur l'identification des consentants, permettant de diminuer la contrainte sur les preuves contextuelles pour des contractants disposant d'une identité numérique et sur des enjeux importants ou pour respecter des contraintes réglementaires.

Un parcours digital dans son ensemble peut, dans certain cas, être désynchronisé entre l'expérience « client » et les traitements « back office » qui suivront. Une stratégie visant à confirmer l'engagement par l'organisation après l'engagement d'un tiers permet de reporter des charges de contrôle a posteriori et de formaliser l'engagement de l'organisation lorsque son représentant aura signé.

Cette approche permet de concilier un parcours fluide pour capter un engagement client rapide sans engager l'organisation immédiatement.

Nous verrons dans ce document l'importance du dossier de preuves qui permettra de démontrer la conformité du parcours en cas de litige. Les dossiers de preuves des processus de consentement ne sont actuellement pas normés et sont généralement représentés sous une forme technique difficilement intelligible par la sphère juridique.

Les autres données ou éléments de preuve du parcours digital ne pourront également pas être standardisés car ils sont généralement spécifiques aux processus métier de l'organisation. Il est important d'anticiper cette problématique notamment pour les actes consentis pour une durée longue. Il s'agit de clairement d'afficher dans la stratégie l'objectif d'être en mesure d'assurer la charge de la preuve en :

- **Étant intelligible** : produire, par exemple, des attestations sous forme de document textuels compréhensibles par un juriste et conférant à des éléments techniques en cas de besoin d'expertise plus poussée ;
- **Anticipant l'archivage** : anticiper les processus d'archivage des documents consentis ainsi que des contextes de consentement matérialisés par les dossiers de preuve intelligibles.

Le dossier de preuve peut conférer à une documentation du parcours qui évoluera en même temps que ce dernier.

La conformité du parcours devra s'appuyer sur une **documentation maintenue** et notamment une **convention de parcours**, elle-même archivée pour permettre de comprendre le contexte historique du parcours qui a produit les documents consentis et le dossier de preuve associé.

Enfin, une analyse de risque lié au parcours est préconisée pour identifier les risques sur la base du parcours modélisé, les accepter ou planifier la mise en œuvre de mesures complémentaires.

La stratégie peut être formalisée dans :

- Une spécification générale de conception;
- Une politique;
- La convention de parcours.

En résumé la stratégie proposée dans ce référentiel et adaptable aux parcours digitaux consiste à :

- Arbitrer sur les niveaux de contraintes utilisateurs et de risques acceptables par l'organisation;
- Partager les décisions d'acceptation ou non acceptation des risques;
- Anticiper la charge de la preuve dans le temps en cas de litige par :
  - La documentation du parcours;
  - La collecte d'un dossier de preuve intelligible;
  - L'archivage ou préservation sécurisée (en fonction de la durée de conservation.

C. Documentation du parcours numérique

La documentation du parcours numérique formalise un « état de configuration » des moyens mis en œuvre sur la durée d'usage du parcours. Elle permet :

- D'auditer la conformité du parcours en production ;
- De justifier a posteriori de la conformité du parcours au moment du consentement.

A ce titre la documentation doit être versionnée de manière synchronisée avec les versions des outils mis en œuvre pour opérer le parcours.

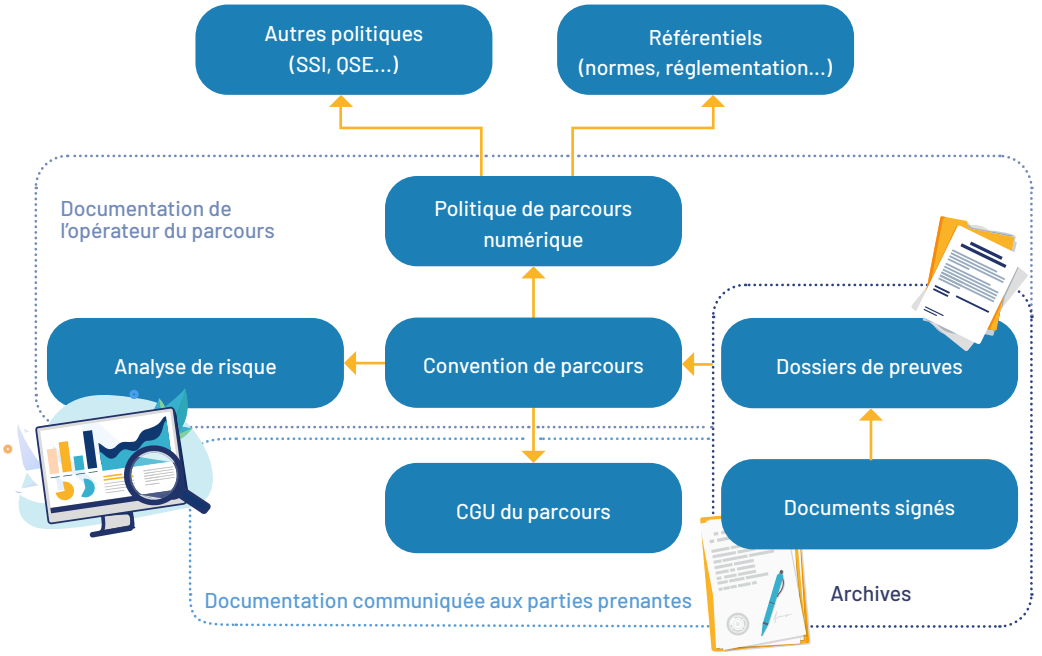
Il convient d'archiver chaque version de la documentation du parcours durant la période de validité des actes consentis et/ou selon les durées légales si elles s'imposent.

L'organisation de la documentation du parcours est libre et dépend de la taille et complexité de l'organisation. Cette organisation documentaire doit être définie dans un des documents présentés dans ce chapitre.
Par exemple :

- Pour une organisation simple, ou pour la qualification d'un seul parcours, d'utiliser une convention de parcours numérique qui contiendra les éléments de politique, stratégie et de modélisation du parcours;
- Pour une organisation complexe qui pilote un ensemble de parcours :
  - Une politique générale à l'ensemble de parcours;
  - Une convention spécifique à chaque parcours.

Le club PSCo propose dans son Guide rédactionne[(1)] le concept de « principes de gestion de preuve » ou PG. Ce principe peut s'appuyer sur des politiques voisines notamment lorsqu'il s'agit d'assembler plusieurs services de confiance disposant de leurs propres politiques de certification, horodatage, signature ou archivage.
La politique de parcours proposée dans le présent document peut servir à matérialiser ce principe de gestion de preuve pour référencer les différentes politiques internes et tierces encadrant la conformité de chaque étape du parcours.

(1) Guide rédactionnel : Principe de gestion de preuves : https://clubpsco.fr/wp-content/uploads/2013/11/Guide-r%C3%A9dactionnel-Principes-de-gestion-de-preuve-v1_signe.pdf



3. Politique de parcours numérique

Une politique de parcours numérique définit le cadre de conformité appliqué par un organisme à un ou plusieurs parcours numériques. Ce cadre dépend du contexte réglementaire et normatif de l'organisme et de ses règles internes.

Il s'agit d'un document pivot entre le système d'organisation général de l'organisme, généralement formalisés dans des systèmes de management (qualité, sécurité, ...), la réglementation et chacun des parcours opérés par l'organisme.

Le contenu type d'une politique est par exemple :

- Le contexte réglementaire et normatif;
- L'organisation documentaire des parcours numériques;
- En référence aux autres politiques internes ou éléments documentés du système de management;
- Une stratégie et des exigences (ou référence aux exigences) applicables à l'ensemble des parcours numériques.

2. Convention de parcours

La convention de parcours spécifie un parcours en particulier dans sa version en production. Son objectif est de démontrer la conformité du parcours au moment du consentement.

Le contenu type d'une convention est par exemple :

- La référence à la politique de parcours de l'organisme;
- L'identification des parties prenantes;
- La stratégie appliquée au parcours;
- Les règles ou exigences spécifiques au parcours et notamment les niveaux de sécurité choisis pour le consentement;
- La modélisation du parcours;
- La composition des livrables du parcours et notamment la composition du dossier de preuve;
- Les règles de gestion du cycle de vie de données et documents produits par le parcours et notamment les modalités d'archivage.

Une approche plus détaillée sur le contenu d'une convention de parcours est disponible dans le Guide rédactionnel : principes de gestion de preuve (PGP) édité par le club PSCo. Le document décrivant les principes de gestion de preuve est similaire à la convention de parcours décrite dans ce document.

Un parcours numérique évolue au même rythme que les outils qui le supportent.

Il est recommandé de versionner la convention de parcours de manière à suivre les versions des outils mis en œuvre.

Pour faciliter les audits, il est recommandé que les références à la convention de parcours dans les productions du parcours (attestations, dossier de preuve, ...) soient également versionnés et que la convention de parcours soit archivée dans les mêmes conditions que ces mêmes productions.

Deux pratiques sont constatées pour gérer les conventions de parcours :

- Une convention unique pour l'ensemble des sessions du parcours : la convention est référencée dans le dossier de preuve;
- Une convention générée pour chaque session du parcours : le contenu de la convention est intégré dans chaque dossier de preuve, par exemple dans les attestations intelligibles.

La première est moins coûteuse et la seconde est autoporteuse.

3. Conditions générales d'utilisation d'un parcours (convention de preuve)

Les conditions générales d'utilisation d'un parcours numérique ont pour objectif de limiter le risque qu'un utilisateur remettre en cause a posteriori la méthode utilisée pour recueillir son consentement.

Il s'agit d'informer les utilisateurs du parcours sur la méthode de recueil du consentement.

Il est recommandé que ces conditions soient acceptées par les utilisateurs au début du parcours de consentement et que cette acceptation soit rappelée dans les actes consentis eux-mêmes.

Ces conditions générales peuvent intégrer d'autres considérations concernant le recueil de données utilisateurs et leur protection, notamment relatives à la protection des données personnelles, de santé ou relative au secret des affaires.

Les conditions générales peuvent conférer à la convention de parcours et/ou à la politique de parcours, auquel cas ces documents devront être accessibles aux utilisateurs. Le cas échéant, certains éléments de la convention de parcours peuvent être repris dans les conditions générales pour préciser les dispositifs mis en œuvre pour recueillir les consentements.

En cas de recours à des prestataires disposant de leurs propres conditions générales d'utilisation, les conditions de l'organisme opérant le parcours peuvent y conférer, s'y ajouter ou être substituées par celles du prestataire. Il convient que le prestataire ou l'opérateur du parcours applique les présentes bonnes pratiques et garantisse la disponibilité de chaque version de ces conditions durant la période d'usage des documents consentis.

4. Analyse de risque

Il est recommandé de formaliser une analyse de risque liée au parcours numérique afin de convenir d'une acceptation des mesures mises en œuvre et des risques résiduels par les différentes parties prenantes.

L'analyse peut être structurée en trois thématiques :

- Le Risque juridique

L'analyse de risque juridique en amont du projet recense l'état des besoins juridiques du client (documents à digitaliser ; cadre juridique applicable ; enjeux financiers ...) et permet d'identifier les exigences techniques et juridiques que devra respecter le parcours numérique en fonction du cadre réglementaire identifié (Ex : Quel niveau de signature électronique ? Quel risque lié à un mauvais archivage ? Quel risque en cas de défaut d'accessibilité à l'original pour telle ou telle administration ?...).

- Le Risque de fraude

Il s'agit d'identifier les motivations que pourrait avoir un utilisateur malveillant pour réaliser une fraude (détournement financier, vol, ...) et les moyens qu'il pourrait mettre en œuvre pour frauder. Les mesures liées au KYC ou la détection de faux sont à évaluer en fonction de l'impact de la fraude et du niveau de ressources nécessaire pour la réaliser : Dans cette analyse du risque de fraude, il convient de dresser un panorama des jurisprudences relatives aux fraudes intervenues quant à la passation d'un document qu'il soit ou non digitalisé. La notion de fraude au sens juridique est en effet protéiforme et renvoie à toutes les façons possibles de remettre en cause l'une des étapes du process (ex : usurpation d'identité, consentement non éclairé, WYSIWYS non respecté...). Ces jurisprudences de plus en plus nombreuses permettront de « calibrer » le Parcours et d'éviter que ce dernier ne soit trop standardisé et à ce titre soumis à des vulnérabilités déjà exploitées par ailleurs.

En effet, certains documents nécessiteront la prise en compte juridique des apports de ces jurisprudences (ex : opposabilité de certains documents précontractuels).

→ Risque technologique

Il s'agit d'identifier les risques sur la sécurité des informations pour une motivation de fraude ou d'attaque sur la disponibilité, l'intégrité et confidentialité des données et documents collectées et conservées. L'analyse de risque technologique peut être réalisée selon la méthode prévue dans le SMSI de l'organisation.

D. Dossier de preuve

1. Définition et objectifs du dossier de preuve

Le dossier de preuve regroupe les données et les éléments de preuve produits sur un parcours de consentement. Les actes consentis peuvent être contenus dans le dossier de preuve ou liés au dossier de preuve.

En cas de contestation légale du parcours, le dossier de preuve a une vocation probatoire. L'audience visée est donc principalement celle des acteurs du monde judiciaire ou règlementaire (audits).

Dans ce contexte, les qualités suivantes sont attendues :

→ Intégrité et authenticité;

→ Intelligibilité;

→ Pérennité;

→ Indépendance / Autonomie.

Intégrité et authenticité

Pour faire l'objet de preuve au sens juridique, l'intégrité et l'authenticité des éléments contenus dans le dossier de preuve, ou du dossier lui-même doivent pouvoir être démontrables.

Par exemple les éléments de preuve ou le dossier de preuve sont généralement protégés au moyen d'un cachet électronique par le service producteur.

Intelligibilité

Il est fortement recommandé que le dossier soit directement compréhensible pour son audience sans nécessiter une expertise technique préalable dans le domaine du parcours. La langue naturelle choisie prend en considération la juridiction compétente.

Interopérabilité

La communication du dossier de preuve doit pouvoir se baser sur des principes concernant la conservation, la réversibilité entre opérateur et la communication vers une autorité.

Pérennité

Le dossier de preuve est adapté à la conservation à long terme.
Par exemple, si le dossier contient des attestations intelligibles au format PDF, le respect de la norme ISO 19005 (PDF/A) est désirable. Ce critère s'applique à chaque composante du dossier de preuves, qu'il s'agisse d'une trace technique ou documentaire, ainsi qu'au choix de la méthode de compression et d'archivage.

Indépendance / Autonomie

Un dossier de preuve est produit sur chaque parcours et contient toutes les données associées à ce parcours qui sont essentielles à sa vocation probatoire (preuves transactionnelles).

Il peut faire référence à des preuves externes, non incluses dans le dossier, si elles font elles-mêmes l'objet d'un référencement versionné et d'un archivage à long terme (cf interopérabilité).

Ces références externes peuvent inclure des preuves infra-structurelles (par exemple les journaux d'une autorité de certification sur un parcours de signature électronique) ou des preuves administratives (politiques de certification, conditions d'utilisation, certifications de conformité) ou des preuves d'un prestataire de paiement ou de KYC/KYB .

2. Contenu type d'un dossier de preuve

La structure et le contenu du dossier de preuve sont spécifiés dans la convention de parcours et notamment la modélisation du parcours. Le dossier de preuve, ses métadonnées ou les attestations peuvent conférer à la référence et la version de la convention de parcours applicable au moment de la réalisation du parcours.

Il est également possible d'intégrer la version applicable de la convention de preuve (ainsi que d'autres éléments de conformité tels que les CGU ou politique) dans le dossier de preuve de manière à le rendre autoporteur.

Un dossier de preuve contient des données techniques et fonctionnelles. Ces données dont la forme est généralement technique, peuvent également être restituées de manière lisible dans des attestations ou annexes aux documents signés.

→ **Les données techniques sont notamment :**

- Les éléments de traçabilité du parcours digital;
- Les logs et attestations de prestataires de confiance (autorités…);
- Les attestations de vérification des certificats;
- Les résultats de vérification des pièces justificatives;
- Les requêtes vers des prestataires de services externes : KYC/KYB, paiement, services de livraison…

→ **Les données fonctionnelles sont :**

- La référence à la convention de parcours et éventuellement aux documents référentiels (politique, CGU);
- Les données saisies par les utilisateurs;
- Les données issues des traitements et contrôles métier.

→ **Les données intelligibles :**

- Les attestations intelligibles;
- La convention de parcours si elle n'est pas référencée dans les attestations ou métadonnées du parcours.

3. Forme du dossier de preuve

Le dossier de preuve est un concept dont l'implémentation est libre. Ce concept peut être matérialisé sous différentes formes par exemple :

- Une enveloppe (zip par exemple) à contenu structuré contenant tous les éléments de preuve, voire les documents signés eux-mêmes;
- Une structure (xml SEDA par exemple) contenant les fichiers de preuve et les métadonnées de chaque fichier contenu ainsi que leur hiérarchie de classement;
- Un ensemble sériel de fichiers de preuves dont les métadonnées les lient ou confèrent à des documents référentiels;
- Des extensions contenues dans les fichiers signés, notament pour les format PDF/PADES.

Le choix de la forme du dossier de preuves dépend de l'usage qui en sera fait, notamment durant l'archivage et selon la forme souhaitée pour la communication qui peut être différente de celle de l'archivage (cf modèle OAIS).

La forme technique du dossier de preuve également peut être différente pour :

- Le processus de transfert vers un autre SI chargé du traitement ou la conservation à l'issue du parcours : forme protocolaire d'échange par exemple SEDA pou un SAE ou CMIS ou une GED;
- Le système de conservation.

Des préconisations d'implémentation pour l'archivage seront proposées dans le chapitre «Conservation» de la troisième partie.

4. Intégrité du dossier de preuve

Il convient d'assurer l'intégrité du dossier de preuve de sa production jusqu'à son sort final.

Selon la forme choisie pour le dossier de preuve, cette intégrité peut être gérée par :

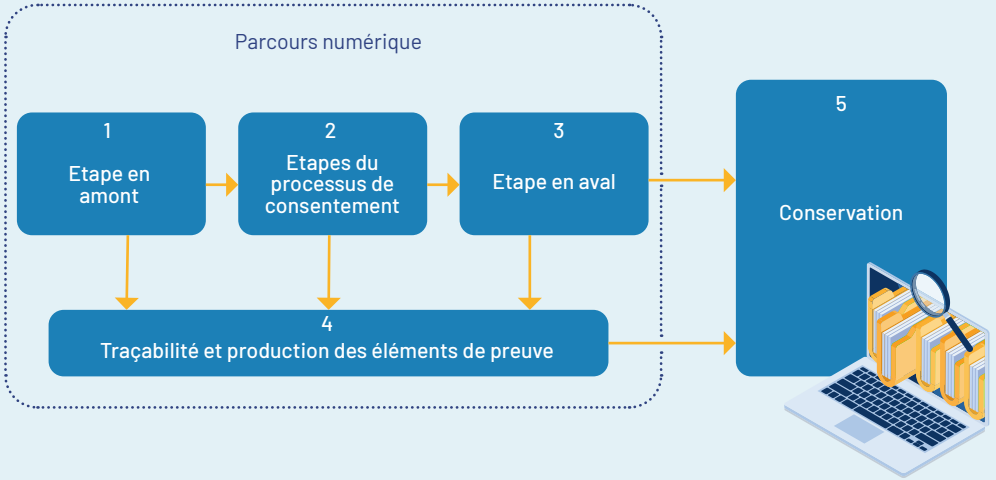
- La signature ou un calcul d'empreinte numérique du dossier lorsque sa forme est un objet autonome;
- Un calcul d'empreinte de chaque fichier technique ou fonctionnel contenu;
- La signature d'une attestation intelligible reprenant les informations de contenu des fichiers techniques.

Dans les cas de contrainte de préservation longue, il est préconisé de préserver les dossiers de preuve dans un CFN ou SAE de manière à gérer l'intégrité des fichiers de preuves (maintenance cryptographique via journalisation chaînée) et la pérennité (maintenance des formats).

MODELISATION D'UN PARCOURS

3

Il convient de modéliser le parcours dans la convention de parcours. Chaque parcours est spécifique aux cas d'usage à traiter. Il n'est pas possible de normaliser cette modélisation. Cependant chaque parcours peut être modélisé selon quatre étapes principales qui structurent ce chapitre :



1. Etapes en amont :

Ces étapes débutent par l'initialisation du parcours, la collecte des données et documents nécessaires à la production des documents à consentir et aux traitements métier. L'aboutissement : la production des documents pour consentement.

2. Etapes du processus de consentement :

Enrôlement de l'identité des personnes qui consentent, production des certificats numériques (s'ils sont nécessaires et s'ils n'existent pas), signature électronique ou toute autre méthode de recueil de consentement, production des fichiers de preuve de conformité du processus de consentement.

3. Etapes en aval :

Traitements métiers post-consentement et composition du dossier de preuve.

4. Traçabilité :

Collecte et production des éléments de preuve.

5. Conservation :

Transmission du dossier de preuve et des documents consentis. Archivage dans sa structure de préservation.

Deux exemples de modélisation de parcours sont présentés dans les annexes 1 et 2 :

- Modélisation d'un parcours d'onboarding et contractualisation en ligne avec usage de la signature électronique;
- Modélisation d'un parcours d'achat et paiement en ligne, sans usage de la signature électronique.

A. Traçabilité

Il convient de mettre en œuvre un dispositif permettant d'assurer la traçabilité du parcours digital de bout en bout, afin d'être en mesure de contrôler le processus et de constituer un dossier de preuve pour consultation.

Il est préconisé de mettre en œuvre un gestionnaire d'événements permettant d'enregistrer, à chaque étape du parcours fonctionnel, un enregistrement des actions réalisées par le SI supportant le parcours et des composants tiers interfacés pour la réalisation de l'étape.

Le gestionnaire d'événement peut être un outil de centralisation des traces ou un moyen permettant de collecter les traces de chaque composant individuellement, notamment pour l'étape de constitution du dossier de preuves et de conservation.

Les données de traçabilité et les éventuels documents collectés durant le parcours doivent être préservés dans des conditions de sécurité adaptées pour prévenir le risque de perte ou corruption de ces informations avant la production du dossier de preuves. Ces conditions de sécurité doivent être spécifiées dans la convention de parcours et l'analyse de risque.

Les conditions de sécurité peuvent être par exemple :

- Des enregistrements en base de données ou des fichiers de log conservés de manière sécurisée. Ce niveau correspond aux mesures mises en œuvre pour prévenir les risques selon l'appréciation de l'organisation qui met en œuvre un système de management de la sécurité de son système d'information;
- Une journalisation basée sur un chainage des blocs d'enregistrement ou l'usage de technologie de type blockchain. Ce niveau permet de démontrer l'absence de perte d'intégrité de la chaine de confiance par l'usage de technologies cryptographiques.

Les données de traçabilité évaluées comme utiles, doivent pouvoir être consultées et agrégées pour une instance du parcours digital dans un objectif de consultation ou de production d'un document intelligible récapitulatif du parcours. Un lien entre les étapes fonctionnelles représentées et les éléments techniques (logs, etc) sources doit pouvoir être établi.

La source « à vocation probatoire » des éléments est généralement portée par des enregistrements sous un format technique, il convient de maintenir une nomenclature des types enregistrement spécifiant comment ceux-ci sont interprétables en cas de besoin d'audit technique en complément des attestations intelligibles qui sont produites.

B. Conservation

Il convient de mettre en œuvre un moyen de conservation pour préserver la disponibilité des documents consentis et des éléments de preuve associés. Cette disponibilité consiste à :

- Permettre de les retrouver : classement, description…
- Garantir l'intégrité des documents et des éléments de preuve;
- S'assurer de la lisibilité des contenus dans le temps;
- Gérer le cycle de vie.

1. Méthodes de préservation

Le parcours digital peut inclure une solution de préservation ou s'interfacer avec une solution d'archivage numérique.

Les critères de choix entre une conservation intégrée ou interfacée sont :

- **La durée de conservation :** si les documents produits ont une durée de conservation supérieure à la durée d'exploitation du système producteur, il est préconisé d'anticiper un versement dans un système d'archivage numérique qui assurera les fonctions de pérennisation sur le long terme;
- **Le coût de mise en œuvre et d'exploitation** des fonctions de préservation dans un parcours digital au regard des coûts d'interfaçage et d'usage d'un système d'archivage numérique;

2. Protocole et format d'échange vers un système d'archivage électronique

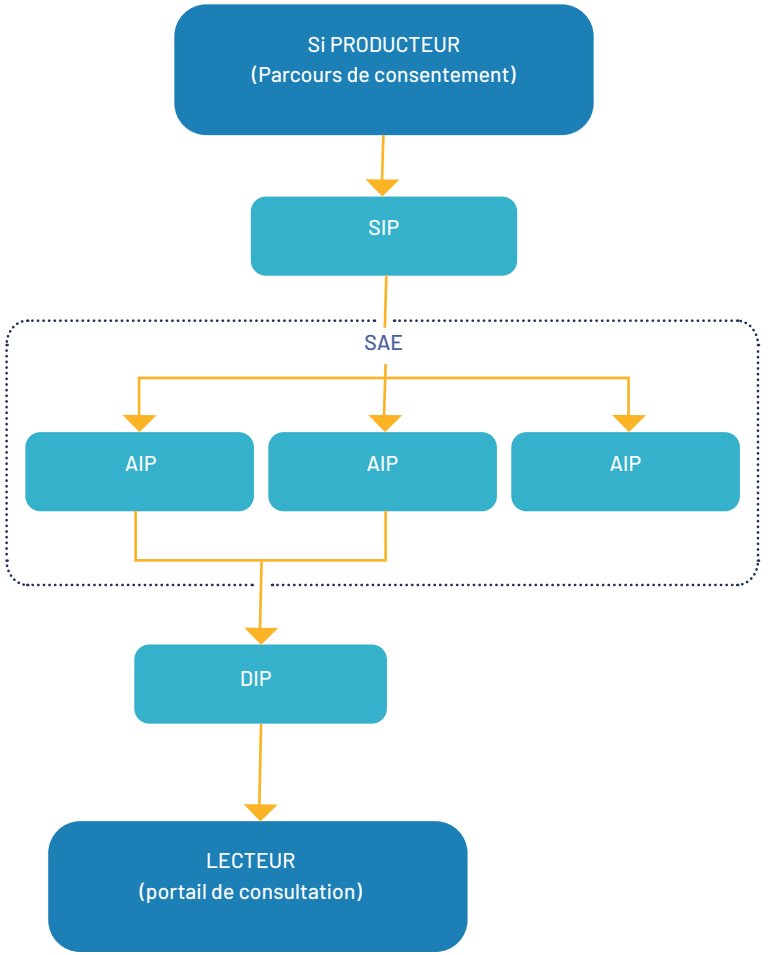
Par convention nous nous appuyons sur la terminologie du référentiel Open Archival Information System (OAIS). Le modèle est normé selon ISO 14721.

La norme identifie les processus d'archivage dans lesquelles transitent des paquets d'archives en entrée, durant la conservation et en sortie du système :

- SIP : paquet d'information à verser;
- AIP : paquet d'information archivé;
- DIP : paquet d'information diffusé.

La granularité (nombre d'archives contenus dans un paquet) peut varier durant le cycle de vie :

- Un SIP est généralement un lot d'archives;
- Les AIP issus des lots d'archives sont généralement conservés de manière unitaire;
- Les DIP pour réversibilité vers un autre système sont généralement des lots d'AIP, pouvant provenir de plusieurs SIP;
- Les DIP pour consultation sont généralement unitaires (consultation sur clic) ou un lot (téléchargement de sélection, etc).



3

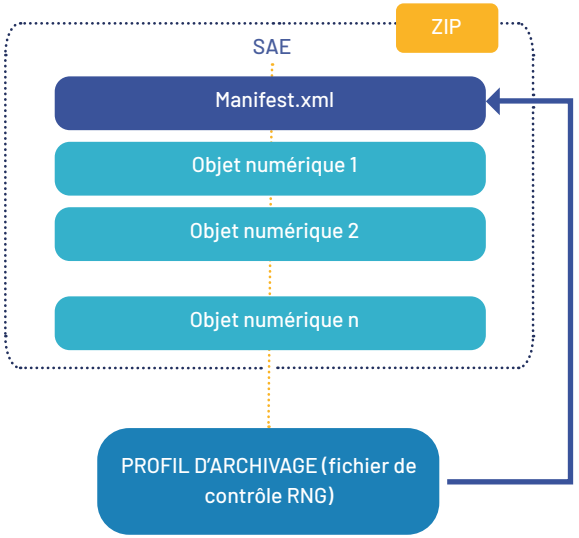
La production de SIP entre le SI du parcours du consentement et le SAE dépendra de la solution d'échange choisie et des protocoles. Les référentiels principaux dans le domaine de l'archivage sont les référentiels FnTC TA et Standard d'Echange des Données d'Archives (SEDA) ou sa version simplifiée normée (DEPIP : ISO 20614)

Un SIP est un ensemble de fichiers contenu dans une enveloppe (zip) durant son transport. Par exemple :

Il contient :

- Un manifeste au format xml avec une structure normée et adaptée aux types d'archives contenus. Le manifeste référence chaque archive, porte la description de chaque archive et la référence vers un ou plusieurs objets numériques et/ou physique ainsi que leur empreinte numérique. Les structures contenues dans les manifestes peuvent être arborescentes (gestion de dossiers).
- Les objets numériques.

Le profil d'archivage est un fichier de contrôle permettant de s'assurer que la structure du manifeste est conforme aux attendus par le système de destination.



3. Organisation et structure d'archivage

Organisation d'archivage

Les archives issues d'un parcours de consentement sont composites.
Il s'agit :

- Des documents consentis;
- Des dossiers de preuve;
- De la documentation du parcours.

L'organisation d'archivage dépendra des usages. Généralement, la structure d'archivage sera conçue pour permettre un accès simplifié aux documents consentis, ce qui correspond aux besoins de la plupart des utilisateurs.

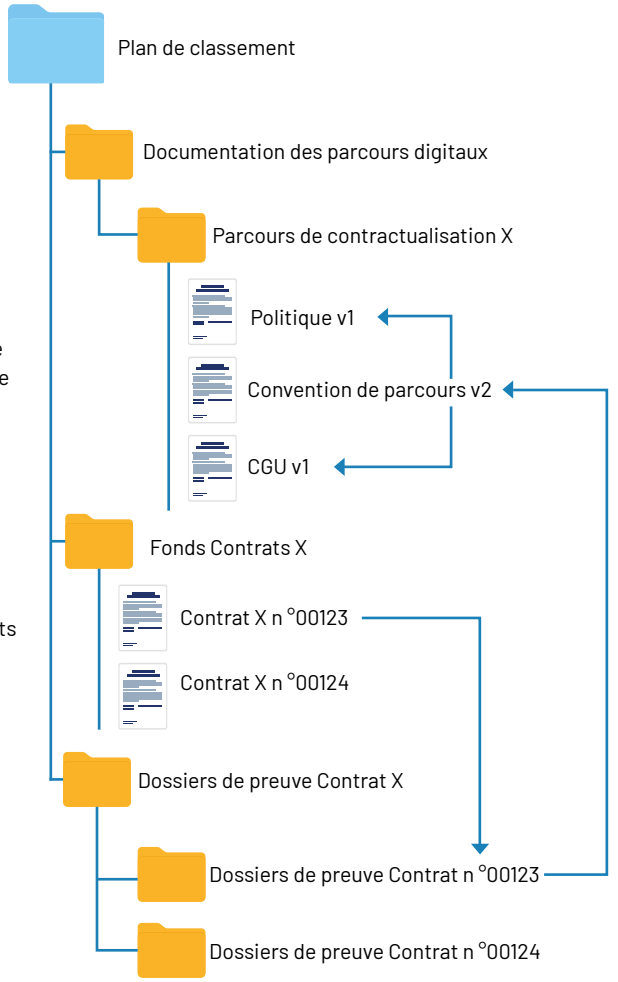
L'accès aux éléments de preuve est généralement plus marginal, en cas d'audit ou de contentieux.

Il est préconisé d'archiver les documents consentis indépendamment des dossiers de preuve et de réaliser un lien de référencement par identifiant (métadonnée ou identifiant externe) permettant l'indexation pour la recherche des documents et éléments de preuve.

Cette structure de classement différentiée permet également de limiter les droits d'accès aux éléments de preuve aux utilisateurs qui ont le besoin d'en connaitre.

Chaque version des éléments référentiels cités dans le dossier de preuve (convention de parcours, politiques, ...) doit également être archivée et référencée de manière à permettre un audit des contextes de production du parcours, rétrospectivement.

Exemple de structure d'archivage :



Dans cet exemple, les éléments contextuels du parcours, les documents signés (contrats) et les dossiers de preuves sont classés séparément de manière à autoriser les accès aux personnes habilitées

La procédure d'audit d'un contrat consiste à :

- Consulter le contrat, contenant une métadonnée d'identification du dossier de preuve;
- Consulter le dossier de preuve contenant une métadonnée d'identification de la version de la convention de parcours applicable au moment du consentement;
- Consulter la version de la convention de parcours, conférant elle-même aux autres éléments contextuels tels que la politique ou les CGU.

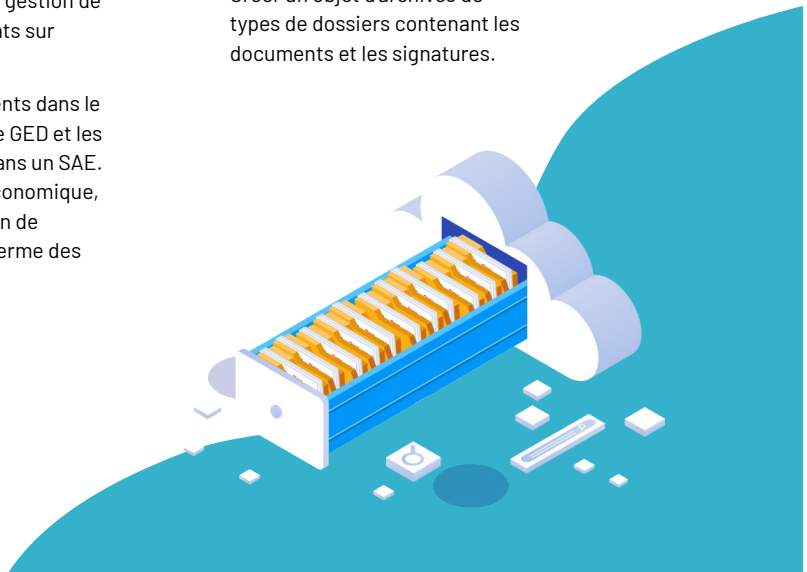
Les exemples de structure d'archivage présentés ci-dessus sont une préconisation. Chaque organisation est libre d'organiser son archivage selon son contexte, par exemple :

- Archiver en « Y » les documents et les éléments de preuves, dans une enveloppe zip. Les copies des documents signés sont conservées dans un système métier pour l'usage courant. Cette solution présente l'avantage de disposer de dossiers autoporteurs en cas de contentieux mais l'inconvénient de gestion de la pérennité des formats sur le long terme;
- Conserver les documents dans le système métier ou une GED et les éléments de preuve dans un SAE. Cette solution, plus économique, n'assure pas la fonction de pérennisation à long terme des documents.

Structures d'archivage des documents signés

Les structure d'archivage dépendront la multiplicité des documents et de la technique de signature, par exemple :

- Document unique contenant la signature : ce cas le plus simple nécessite un archivage sériel du fichier signé et son indexation;
- Document multiples (contrat avec annexes par exemple). Plusieurs solutions sont envisageables :
  - Autant que possible agréger les documents avant signature pour un archivage sériel identique au cas précédent;
  - Créer un objet d'archives de type dossier contenant les documents;
  - Eviter la conservation en enveloppe qui présentera une complexité pour la gestion des formats et de la pérennité.
- Documents simples ou multiples avec signature externe :
  - Créer un objet d'archives de types de dossiers contenant les documents et les signatures.



Structures d'archivage des dossiers de preuves

Les dossiers de preuve généralement produits sont sous format d'enveloppe, celle-ci étant elle-même scellée pour éviter une éventuelle corruption entre sa production et son archivage.

La préservation d'une enveloppe pose des contraintes sur l'archivage, notamment pour gérer la pérennisation (contrôle et migration des documents contenus) lorsque les durées de conservation sont longues.

Pour les durées de conservation longue, il est préconisé de préserver les dossiers de preuve dans une structure d'archivage et de les produire selon une structure de versement normée (par exemple SEDA).

Actuellement il n'existe pas de profil d'archivage de dossiers de preuves normé qui permettrait d'interopérer simplement un parcours digital avec un SAE. Il conviendra donc de définir au cas par cas un profil d'archivage pour chaque typologie de dossier de preuves.

L'approche la plus simple serait :

- Une description au niveau du dossier racine, contenant a minima :
  - L'identifiant métier du dossier de preuves;
  - Sa description (concaténation de métadonnées métier);
  - La référence à la convention de parcours;
  - La version de la convention de parcours;
  - La règle de gestion du dossier, notamment la durée de conservation.
- Une description simplifiée de chaque pièce contenue :
  - Identifiant de la pièce;
  - Description : le nom du fichier;
  - Type de pièce;
  - La règle de gestion héritée de celle du dossier.

Focus sur la validation de signature électronique

Les contrôles réalisés sur une signature électronique sont à deux niveaux :

- Vérifier que le document est resté intègre après signature : comparatif de l'empreinte numérique calculée au moment de la signature et du recalcul de l'empreinte au moment de la vérification. Ce contrôle est réalisé notamment lors de l'affichage des documents par les lecteurs de fichiers PDF;
- Valider que les certificats utilisés au moment de la signature étaient valides (non périmés, ni révoqués). Ceci nécessite de disposer d'une marque de temps fiable (horodatage).

Notons que le fait de disposer d'une marque de temps fiable est indispensable pour réaliser une validation de signature ou une vérification durant l'archivage. Lors de l'utilisation de signatures normalisées, les niveaux LTV (Long Term Validation) ou LTA (Long Term Archive) sont recommandés au moment de la production des documents signés.

La nécessité de réaliser une validation et de produire un rapport de validation dépend du risque porté par le consentement. Il est notamment intéressant de réaliser une validation lorsqu'il s'agit de signatures multiples et que chaque signataire dispose de son propre dispositif technique de signature et de certificat produit par différentes autorités. La validation permet d'interroger chaque autorité productrice de certificat pour limiter le risque qu'un certificat périmé ou révoqué soit utilisé par un signataire.

Lorsque le parcours digital porte la production de certificats avec une autorité unique pour l'ensemble des signataires, le risque est faible et ne nécessite par de réaliser une validation complémentaire à celle réalisée au moment de la signature.

Si une validation est nécessaire, il est préconisé de la réaliser au plus tôt après la signature par le service producteur et que ce dernier produise le rapport de validation dans le dossier de preuves.

Le triptyque de guides FnTC sur la signature, la validation et archivage et la préservation long terme des signatures présente plus en détail les recommandations liées à la validation de signature.

Trilogie de guides sur la signature électronique :

- **Tome 1** : Définitions et cas d'usage
- **Tome 2 :** Validation et archivage
- **Tome 3 :** Conservation à long terme des documents signés
- Archivage de preuves de signature électronique à la volée

Il n'est pas préconisé d'envisager la vérification durant l'archivage car rien ne garantit que les services des autorités ayant produit les certificats soient toujours disponibles. La bonne pratique est donc d'archiver ou d'intégrer dans le document signé les rapports de validation qui permettront, en cas de besoin, de démontrer que les certificats étaient valides au moment de la signature sans dépendance avec les autorités qui les ont produits.

5. Focus sur la préservation des documents signés

Le guide FnTC sur l'archivage et la préservation long terme des signatures présente en détail la problématique de pérennisation, notamment du risque lié à l'obsolescence des robustesses d'empreinte numérique utilisés lors de la signature.

En synthèse, le risque est que si la robustesse d'une empreinte n'est plus suffisante (longueur de l'empreinte et fiabilité de l'algorithme de calcul de l'empreinte), il est possible de créer un faux signé avec la même empreinte numérique que le document d'origine. Ce risque peut s'avérer possible sur les documents à durée de conservation longue car les évolutions technologiques qui rendraient cela possible ne sont pas prévisibles.

Actuellement deux méthodes permettent de gérer cette obsolescence cryptographique :

- L'enrichissement des signatures;
- L'archivage avec une technologie de journalisation chainée maintenue.

L'enrichissement des signatures

L'enrichissement de signature consiste à enrichir le document avec une empreinte dont la robustesse est conforme à l'état de l'art.

Techniquement il s'agit d'ajouter un cachet produit avec le certificat d'une autorité en charge de la maintenance cryptographique des fonds conservés.

Certains opérateurs proposent d'enrichir la signature à chaque péremption de certificat. Cette pratique n'est pas nécessaire d'un point de vue juridique car une signature reste valable quand bien même le certificat utilisé lors de la signature n'est plus valide, au même titre qu'un document papier signé sur présentation d'une pièce d'identité conventionnelle.

L'archivage avec une technologie de journalisation chainée maintenue (SAE)

La journalisation chaînée utilisé dans le SAE conformes à la norme à NFZ 42-013 consiste à :

- Calculer l'empreinte numérique de chaque document versé et produire un enregistrement de cette empreinte lié à la référence unique du document ;
- L'enregistrement est identifié selon un chrono séquentiel. L'ensemble des enregistrements sur une période, sans rupture de séquence constitue un journal;
- Le journal est scellé périodiquement (par exemple chaque jour). Le scellement consiste à calculer l'empreinte du journal et apposer une marque de temps fiable (horodatage).

L'empreinte du journal est le premier enregistrement du journal suivant (chaînage).

La sécurité du dispositif repose sur la difficulté de pouvoir corrompre l'ensemble des journaux. En effet, pour rendre indétectable la modification de l'empreinte d'un document dans un journal, il est nécessaire de reproduire l'ensemble des journaux suivants jusqu'à la date du jour et de corrompre les autorités ayant scellé chaque journal. Ce niveau d'attaque est évalué comme improbable, notamment quand le système est maintenu par des tiers de confiance certifiés ou qualifiés.

Au même titre que les empreintes utilisées pour la signature, les empreintes calculées par le SAE sont réalisées selon des robustesses équivalentes, soumises au risque d'obsolescence cryptographique. A ce titre, le SAE doit intégrer un processus de veille et de recalcul des empreintes selon une robustesse adaptée.

A la différence de l'enrichissement de signature, les documents ne sont pas modifiés car le SAE réalisera des opérations de recalcul en masse sur les fonds concernés et produira un simple événement journalisé avec la nouvelle empreinte.

Un SAE permet donc :

- De factoriser la maintenance cryptographique à moindre coût sans nécessité d'enrichissement;
- De ne pas modifier les documents d'origine et d'éviter la dépendance aux formats de signature, qui peuvent évoluer dans le temps;
- D'éviter de devoir signer chaque élément de preuve pour gérer leur intégrité et de limiter la dépendance avec les autorités de certification ou tiers de signature (disponibilité du service de validation, prestation de préservation via enrichissement);
- De garantir la réversibilité sans rupture de chaine probante.

CONTROLE ET AUDIT

4

A. Surveillance et contrôle

L'opérateur du parcours digital doit mettre en œuvre un dispositif de surveillance permettant de garantir la production de l'exhaustivité des livrables attendus (documents consentis, traces, dossiers de preuve).

B. Audit

Il est recommandé de réaliser des audits périodiques, notamment :

- Simuler l'audit technique d'un dossier de preuves en cas de contentieux;
- Vérifier la mise à jour de la documentation du parcours après chaque modification réalisée;
- Contrôler l'exhaustivité des versements en archivage ou dans le système de préservation choisi.

ANNEXES

5

Annexe 1

Modélisation d'un parcours digital : contractualisation en ligne

La modélisation d'un parcours présentée dans les chapitres suivants est un exemple de contractualisation d'une relation commerciale en BtoC.

Ce cas d'usage présente l'avantage d'illustrer les principales étapes et bonnes pratiques mises en œuvre par une organisation opérant un parcours numérique :

- L'attractivité et la simplicité en permettant à l'utilisateur de s'informer, choisir une offre et simuler un tarif sans enregistrement préalable;
- Un premier enrôlement permettant de sécuriser la saisie d'information utilisateurs;
- L'analyse automatisée des informations et pièces justificatives, associée à un rating KYC;
- La production d'un contrat ainsi qu'un état récapitulatif des informations saisies par l'utilisateur (contenu dans le contrat signé);
- Le scellement des documents à signer par l'opérateur du parcours (personne morale);
- La signature par l'utilisateur avant la validation par l'opérateur du parcours après contrôle back-office et traitements métiers ;
- La production d'un dossier de preuves contenant une attestation intelligible.

Etapes en amont du processus de consentement

	Opérations réalisées	Données collectées
1.1 Orientation prospect Simulateur anonyme	Etape permettant à un internaute de sélectionner une offre et simuler un tarif, sans authentification préalable. - Affichage des offres - Sélection offre - Saisies données de simulation tarifaire - Sélection tarif	- ID token access / ID user - Origine lead - Données de simulation user - Acceptation des limites de responsabilité sur affichage des tarifs - Offre et tarif calculé - Durée de session
1.2 Informations utilisateur	Etape de collecte d'information utilisateur pour création d'un compte identifié : - Nom, prénom - Date de naissance - Email -Téléphone - Autres informations utiles - Coche de l'acceptation des CGU d'utilisation de l'espace client et de la convention de preuve pour le consentement. - Coche d'acceptation des clauses RGPD	- Informations utilisateur - Datation des coches d'acceptation
1.3 Création de compte	Etape de création technique du compte et validation d'existence d'email - Création du compte - Envoi d'un token de validation à l'utilisateur - Saisie mot de passe par utilisateur - Authentification session à l'étape 1.4	- ID technique utilisateur - Datage clic sur token de validation d'email
1.4 Informations contractuelles	Etape de collecte d'informations nécessaires à l'édition du contrat - Saisie formulaire de renseignement selon l'offre choisie	- Informations contractuelles

Etapes du processus de consentement

	Opérations réalisées	Données collectées
2.1 Scellement des documents à signer	Etape de scellement par l'opérateur du parcours permettant de garantir l'intégrité et l'imputabilité du document qui va être signé : - Apposition d'un cachet personne morale sur les documents.	- Log de la transaction de cachet organisation - informations relatives au certificat
2.2 Acceptation du procédé de consentement	Etape d'information sur le processus de consentement : - Affichage des données clés du contrat saisies par l'utilisateur (possibilité de correction et retour à l'étape 1.2 - Affichage du processus de consentement - Acceptation des CGU de l'autorité de certification (notamment pour l'usage des données personnelles nécessaires à la production et utilisation d'un certificat)	- Coche acceptation CGU d'utilisation du processus de consentement
1.2 Lecture des documents	Etape permettant d'assurer que l'utilisateur dispose de moyens de visualisation des documents à signer	
1.3 Signature électronique	Etape technique de signature électronique : - Appel API à l'autorité de certification - Envoi d'un code OTP au signataire - Saisie du code OTP reçu par l'utilisateur - Production d'un certificat d'identité numérique à la volée - Signature électronique du document	- Log transaction API vers l'autorité de certification - Log OTP - Dossier d'enregistrement de l'autorité de certification (conservé par l'AC) - Rapport de preuve du tiers de signature
1.4 Mise à disposition de l'exemplaire signataire	Etape de mise à disposition de l'exemplaire signé par l'utilisateur : - Mise à disposition du document dans l'espace client - Envoi d'un e-mail d'information sur la suite du processus	- Log de versement espace client - (Log de consultation utilisateur.)
Lancement des étapes en aval		

Etapes en aval du processus de consentement

	Opérations réalisées	Données collectées
3.1 Contrôle et opérations métier	Etape de contrôle ou traitements métier nécessaire à la finalisation de la transaction - Vérification de conformité : complétude, résultats de vérifications des justificatifs, rating KYC - Enregistrements métier dans le SI métier pour activer les prestations contractualisées - Demande d'informations ou pièces complémentaires - Appel prospect pour la vérifications d'informations, existence d'une ligne téléphonique valide	- ID opérateur de contrôle back-office - Log des transactions réalisées par le back-office - Résultat de l'étape
3.3 Production du dossier de preuves	Etape technique de production du dossier de preuves - Requête sur la base de traçabilité pour produire un état historique de la transaction - Production d'une attestation intelligible au format PDF (+ cachet éventuellement) - Consolidation des fichiers de logs techniques internes et tiers - Enveloppement et compression zip	- Attestation - Zip dossier de preuves - Fichier de métadonnée du dossier de preuves
Lancement de l'étape de conservation		

Annexe 2

Modélisation d'un parcours digital : achat et paiement en ligne

La modélisation d'un parcours présenté dans les chapitres suivants est un exemple d'achat en ligne avec paiement en plusieurs fois et pour un montant élevé qui représente un risque pour le commerçant. Collecter et conserver des preuves du parcours d'achat et de la transaction de paiement est essentielle pour identifier le type de fraude :

- Usurpation d'identité;
- Utilisation frauduleuse d'un moyen de paiement;
- Auto-répudiation.

Ce parcours présente l'avantage d'illustrer un cas d'usage courant dans le e-commerce qui n'impose pas de signer des documents :

- Validation des données personnelles : prospect avec enrôlement ou client identifié et authentifié;
- Validation du panier au travers de son récapitulatif;
- La mise en œuvre d'un paiement en plusieurs fois par carte, prélèvement ou virement;
- La livraison de la commande.

Etapes en amont au processus de consentement

	Opérations réalisées	Données collectées
1.1 Identification du client	- Enrôlement du prospect ou identification du client (login+mdp, cookies sur matériel connu, appli mobile... - Validation des données personnelles	- Données techniques de connexion : IP, MAC, géolocalisation appel, empreinte du PC/tel - Adresse facturation et livraison
1.2 Vérification et validation de la commande (panier)	- Affichage de la commande	- Commande

Etapes du processus de consentement

Etapes en aval au processus de consentement

	Opérations réalisées	Données collectées
2.1 Acceptation des CGV	- Consentement avec ou sans case à cocher La validation du panier vaut pour acceptation avec un texte explicite.	- Conservation du texte affiché (clic s'il y a lieu)
2.2 Conservation du texte affiché (clic s'il y a lieu)	- Initiation du paiement par un PSP - Paiement OK	- Message d'appel et de réponse au PSP (qui a ses propres traces en cas de litige)
2.3 Livraison	- Livraison effectuée elon le process choisi	- Informations d'une livraison effectuée

Lancement de l'étape de conservation

Comité de rédaction :

- **Pascal Agosti** – Cabinet Caprioli & Associés
- **Marie-Christine Baldy** – Société Générale
- **Odile Bonnet** - SRCI
- **Bruno Claret** - Syrtals
- **François Devoret** – Lex Persona
- **Xavier Lefevre** – LuxTrust
- **Hélène Roizin** - Syrtals et LE6
- **Hervé Streiff** – Xelians

fntc
Fédération des Tiers de Confiance du Numérique

Délégation Générale
5, impasse Gomboust
75001 Paris
infos@fntc-numerique.com
fntc-numerique.com

JUIN 2024