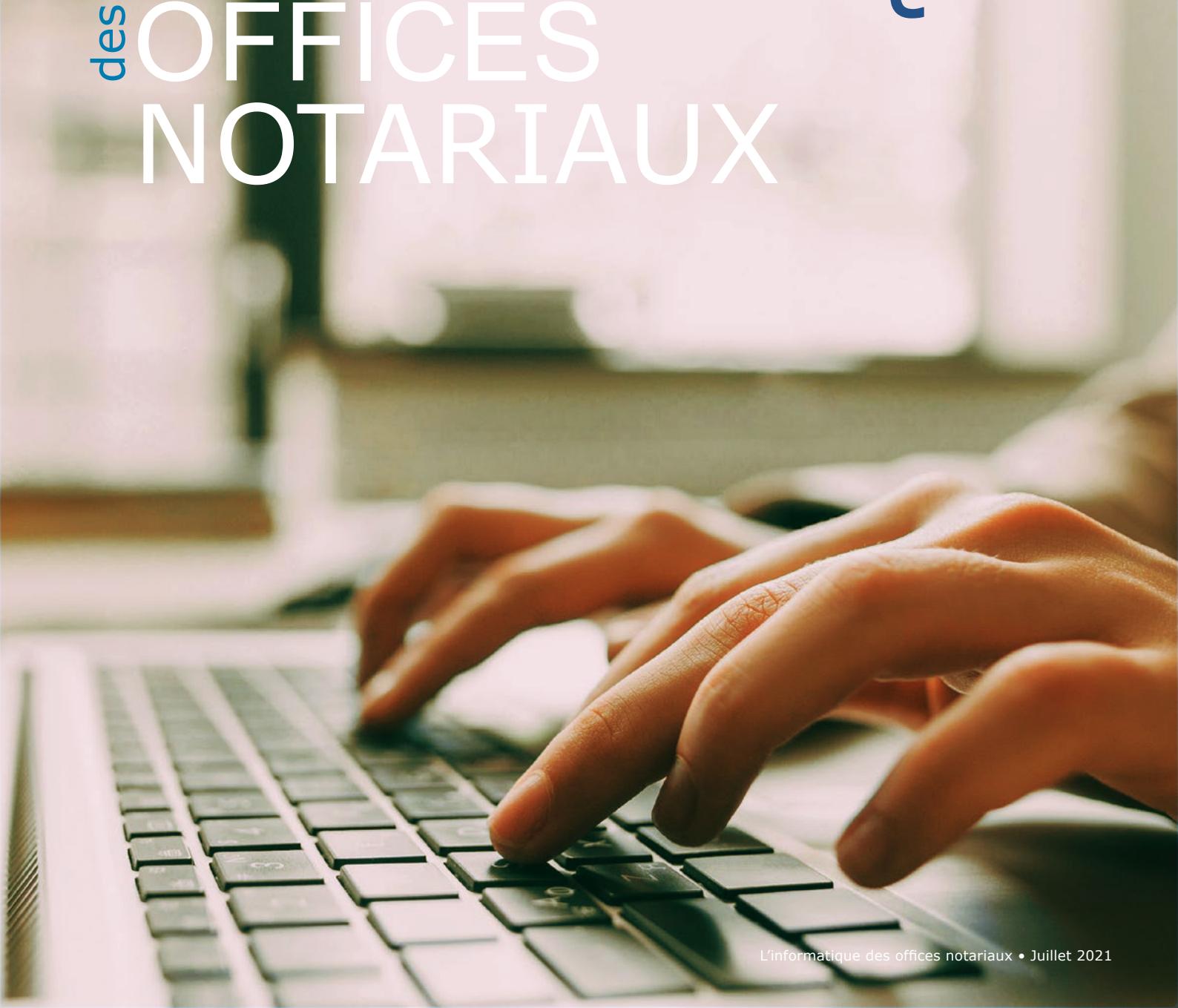




CONSEIL SUPÉRIEUR  
DU NOTARIAT



L'INFORMATIQUE  
des OFFICES  
NOTARIAUX



**David Ambrosiano**

Président  
Conseil supérieur du notariat

En élaborant la Stratégie Digitale 2020 du Conseil Supérieur du Notariat, il nous est apparu nécessaire d'accompagner les notaires et leurs collaborateurs dans la compréhension des notions et solutions informatiques contemporaines. Le but est que nous puissions tous nous sentir plus à l'aise face à la digitalisation croissante de notre environnement de travail, à la complexification des solutions technologiques qui nous sont proposées, et aux discours parfois abscons voire ésotériques de nos fournisseurs.

J'ai voulu une démarche didactique, même si certaines explications pourront paraître évidentes à certains. Ce document, qui se veut un « référentiel » à une date donnée, aborde plusieurs thèmes du quotidien numérique des offices afin d'aider à leur compréhension.

Il n'est bien sûr pas question ici d'une formation à des techniques ou à des outils utilisés par la profession (programmation, intelligence artificielle, paramétrage détaillé...). Ce document n'a pas vocation non plus à remplacer les formations dispensées par les fournisseurs sur leurs produits et les modes opératoires détaillés que l'on peut trouver sur les portails de la profession.

L'objectif est au contraire, pour chaque thème abordé, de chercher à :

- Rappeler les concepts de base,
- Préciser les éléments structurants qui peuvent expliquer des contraintes de mise en œuvre ou orienter des choix,
- Détailler les particularités propres au notariat français,
- Rappeler les bonnes pratiques que beaucoup trop ignorent,
- Présenter les principales solutions du marché à ce jour pour les notaires,
- Indiquer des critères qui peuvent aider les notaires à choisir,
- Clarifier le vocabulaire technique et les nombreuses abréviations, françaises ou anglaises, auxquels nous sommes souvent confrontés.

J'espère que ce document vous permettra de mieux comprendre, comparer et acheter les solutions qui s'offrent à vous et ensuite de mieux utiliser et maîtriser votre environnement technique et numérique.

Bonne lecture.

1. Quelques rappels	P.4
2. Le poste de travail	P.6
3. Le réseau local	P.11
4. Le réseau notarial longue distance	P.16
5. Les accès distants en mobilité	P.25
6. Les serveurs hôtes	P.27
7. La messagerie électronique	P.33
8. La visioconférence	P.39
9. PLANETE	P.44
10. FICEN	P.47
11. ID.Not	P.49
12. Les principales applications du notariat	P.52
13. MICEN	P.55
14. Les espaces collaboratifs	P.59
15. Homologation, agrément et label	P.61
16. La signature électronique	P.65
17. La clé REAL	P.72
18. La sécurité informatique	P.76

Chaque thème est indépendant pour permettre de démarrer la lecture par n'importe quel sujet.

# 1. Quelques rappels

## Représentation informatique

En informatique, il est d'usage de représenter le fonctionnement des ordinateurs ou des logiciels par des couches superposées. En effet, toute l'informatique s'est construite sur le principe d'une couche qui utilise les services normalisés fournis par les couches inférieures, qu'elles soient matérielles ou logicielles.

Par exemple :

- un logiciel utilise les fonctions du système d'exploitation qui lui-même exploite les caractéristiques matérielles de l'ordinateur sur lesquels ils sont installés et les accès réseaux qui sont disponibles.
- une application internet utilise un serveur logiciel de site internet qui lui-même est installé sur un serveur hôte matériel et qui utilise les services d'accès à Internet.
- l'envoi de données entre ordinateurs utilise le protocole de communication TCP/IP qui lui-même est véhiculé sur un réseau local ou un réseau longue distance.



## Octet

Un octet est une unité de mesure de la quantité de données informatiques. Un octet est composé de 8 bits, chacun de valeur 0 ou 1.

Un octet permet de coder un caractère tel qu'une lettre ou un chiffre.

Le symbole de l'octet est « o ». Le symbole du bit est « b » en minuscule. En anglais un octet se dit « Byte » et son symbole est « B », en majuscule pour le distinguer du « b » de bit.

Les multiples supérieurs sont :

- 1 Ko = 1 Kilo octets = 1000 octets
- 1 Mo = 1 Mega octets = 1000 Ko = 1 million octets
- 1 Go = 1 Giga octets = 1000 Mo = 1 Milliard octets
- 1 To = 1 Tera octets = 1000 Go
- 1 Po = 1 Peta octets = 1000 To
- 1 Zo = 1 Zetta octets = 1000 Po

La mesure de la « taille » d'un objet (document, espace disque, mémoire...) s'exprime en général en octets (Ko ou Mo ou Go).

- Un document de taille importante (supérieure à 5 Mo) peut être réduit sans impact sur le rendu, par une opération dite abusivement de « compression », pour retirer les informations inutiles : informations textuelles non visibles, polices de caractères incluses, portions d'images non visibles, résolution d'image supérieure à celle nécessaire pour un affichage à l'écran ou l'impression, etc.

Remarque : historiquement, à cause de son lien avec la notation binaire, les multiples supérieurs de l'octet étaient exprimés en puissance de 2 et non puissance de 10 comme pour les autres unités de mesure usuelles. On avait alors  $1\text{ Ko} = 2^{10} = 1024$  octets. La méthode de calcul a été modifiée en 1998. On trouve encore cette méthode de calcul dans les anciens logiciels qui pouvaient engendrer des différences notables entre la valeur exprimée en octets et la valeur exprimée en Go, par exemple lors de l'affichage de la taille mémoire.

Un document texte sous Word, sans images, d'une centaine de pages fait moins de quelques centaines de Ko.

## Débit

En informatique, le débit est la quantité d'information qui peut être échangée pendant un laps de temps donné. La mesure d'un débit s'exprime généralement en bits par seconde (bit/s ou bps) car historiquement les données étaient envoyées bit par bit sur une ligne télécom constituée de deux fils et l'envoi en série d'un octet nécessite d'ajouter des bits de début et de fin (ou de contrôle de parité) supplémentaires.

Les débits usuels des réseaux d'interconnexion sont exprimés en Mbits/s (ou Mbps) et en Gbits/s (Gbps).

 Pour envoyer un fichier de 20 Mo sur un réseau distant ayant un débit de 20 Mbits/s, il faut environ 10 secondes.

L'envoi au Micen d'un acte de 36 Mo avec un réseau dont le lien montant a un débit moyen de 4 Mb/s prendra au moins 1 minute et 30 secondes.

## 2. Le poste de travail

### 2.1 Les concepts de base

Le poste de travail d'un utilisateur en office est en général constitué d'un ordinateur personnel, avec éventuellement des éléments périphériques tels qu'un deuxième écran externe, un scanner, une imprimante personnelle ou en réseau, une caméra externe.

#### Constitution

Un ordinateur est constitué d'un processeur, de mémoire volatile (RAM), d'un stockage interne (disque dur ou mémoire non volatile), de périphériques (écran, clavier, souris, caméra, haut-parleurs...), de différents ports (USB pour la plupart des périphériques, HDMI pour un écran externe, port RJ45 pour accès au réseau Ethernet...) et accès réseau sans fil (Wifi, BlueTooth).

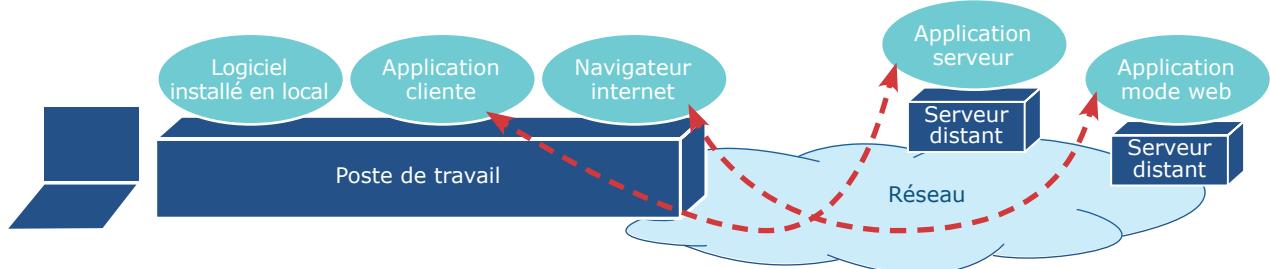
#### Logiciels

Les ordinateurs ont besoin d'un système d'exploitation (« Operating System » ou « OS » en anglais) pour fonctionner avec leurs périphériques et les logiciels. Il y a quatre grandes familles de systèmes d'exploitation :

- Windows de Microsoft (Windows 10),
- Chrome OS de Google pour les ordinateurs ChromeBook,
- MacOS de Apple pour le matériel Apple (macOS 10.11, macOS 11),
- Unix et les différentes déclinaisons de Linux, comme RedHat, Ubuntu ou Debian, pour les utilisateurs aguerris.

Les ordinateurs sont utilisés :

- avec des logiciels installés localement en mode autonome,
- avec une application installée en partie sur l'ordinateur (« client lourd ») et en partie sur un serveur distant (mode client-serveur), avec une communication au travers d'un réseau,
- avec des applications en mode web, installées sur des serveurs distants accessibles au travers du réseau par un navigateur Internet (« client léger » ou « web client »).



Les logiciels standards suivants doivent en général être disponibles sur le poste de travail :

- un antivirus,
- des logiciels techniques spécifiques (ex : pack de sécurité, langage Java),
- un logiciel de compression/décompression de données, comme « 7-Zip »,
- un navigateur pour Internet,
- un traitement de texte comme « Word » de Microsoft,

- un tableur comme « Excel » de Microsoft,
- un logiciel de présentation comme « PowerPoint » de Microsoft,
- un logiciel client de messagerie comme « Outlook » de Microsoft,
- un logiciel de lecture des documents au format PDF comme « Acrobat Reader » d'Adobe,
- un client de visioconférence.

Les principaux navigateurs pour Internet sont : « Chrome » de Google, « Firefox » de Mozilla, « Edge » de Microsoft, « Safari » de Apple.

Les logiciels de Microsoft (Word, Excel, PowerPoint regroupés sous l'appellation « Office ») sont disponibles en version complète destinée à être installée sur le poste de travail et en version allégée en ligne, sous l'appellation « Microsoft 365 », utilisable dans un navigateur Internet.

## Connexion Bureau à distance

Les postes de travail personnels qui n'ont pas de périphériques particuliers peuvent être virtualisés sur un serveur physique adapté à l'aide d'une solution spécifique comme Remote Desktop Services (anciennement Terminal Server Edition) de Microsoft.

En se connectant à distance par l'intermédiaire un logiciel client spécifique installé sur un ordinateur réduit au minimum (Thin PC), on retrouve alors le bureau Windows et l'environnement complet du poste de travail. Les logiciels lancés par l'utilisateur s'exécutent sur le serveur physique comme s'ils étaient installés localement. L'ordinateur local ne gère que la partie affichage et communication.

Plusieurs postes de travail peuvent être virtualisés sur le même serveur. Une application peut alors n'être installée que sur le serveur physique central pour plusieurs utilisateurs.

## 2.2 Les éléments structurants

Un ordinateur personnel peut être fixe ou portable. Pour des besoins bureautiques usuels, la performance d'un ordinateur portable est similaire et suffisante par rapport à celle d'un ordinateur fixe.

La durée de vie d'un ordinateur est d'environ 5 ans. Au-delà, le risque de pannes est plus important et la compatibilité avec les nouveaux périphériques ou les nouvelles versions des applications peut apparaître si les versions de ses logiciels de base ne peuvent pas être mises à jour.

 Le disque dur est l'élément le plus lent d'un ordinateur ; c'est donc celui qui détermine sa performance globale. Plusieurs possibilités permettent d'accélérer le temps de réponse d'un disque : augmenter sa vitesse de rotation, utiliser un raccordement haute vitesse, ajouter de la mémoire cache, remplacer le disque physique constitué de plateaux en rotation par de la mémoire non volatile (SSD).

Les logiciels peuvent être achetés ou, de plus en plus, loués à l'usage et/ou pendant une certaine durée.

Les logiciels évoluent régulièrement pour intégrer de nouvelles fonctions ou pour s'adapter aux nouveaux matériels (nouveaux processeurs, nouveaux périphériques) et aux nouveaux fonctionnements (Cloud, Internet). Ils changent alors de numéro de

version. Il est d'usage de nommer une version majeure, qui apporte un changement notable, par un numéro entier et une version mineure, qui apporte des correctifs, par un numéro décimal. Exemple : Firefox version 90.0.1 .

Derrière le nom unique « Windows 10 » du système d'exploitation de Microsoft se cachent en réalité au moins 12 versions successives différentes nommées selon la date de sortie (format aamm). Par exemple la version 20H2 de Windows 10 est sortie en octobre 2020 (« Half 2 ») et sera supportée jusqu'en mai 2023. La prochaine version majeure de Windows sera Windows 11 qui sera disponible à l'automne 2021.

La mise à jour d'un logiciel de base, comme le système d'exploitation, peut nécessiter la mise à jour des logiciels qui l'utilisent pour assurer la compatibilité.

## 2.3 Les particularités pour les notaires

Les Logiciels de Rédaction d'Actes et les logiciels de la clé REAL fonctionnent avec des postes de travail qui utilisent le système d'exploitation Windows.

Pour différents usages ou sites Internet, il est nécessaire d'installer localement :

- un navigateur Internet,
- les logiciels Java et .Net qui offre des modules de base pour exécuter des programmes écrits avec ces deux langages,
- des logiciels spécialisés, comme AWR pour l'utilisation de la clé REAL.

Le système d'exploitation recommandé pour les postes de travail par les éditeurs de logiciels notariaux est : Windows 10 de Microsoft.

## 2.4 Les bonnes pratiques

Il faut privilégier l'utilisation d'ordinateurs portables avec un écran externe complémentaire car ils permettent de télétravailler facilement.

Pour éviter les vols, les ordinateurs portables, dont le disque interne sera chiffré, doivent systématiquement être attachés avec un câble métallique antivol.

Les postes de travail doivent être paramétrés lors de l'installation pour se verrouiller automatiquement au-delà d'une période d'inactivité de 10 minutes maximum.

La version de chaque logiciel utilisé, et notamment du système d'exploitation, doit être à jour afin de bénéficier :

- des mises à jour ultérieures qui incluent les correctifs de sécurité,
- du support technique de l'éditeur en cas de problème.

Microsoft diffuse le cycle de vie de chacun de ses produits, c'est-à-dire la période pendant laquelle chaque produit bénéficie de mises à jour et d'un support technique (cf le site internet : <https://docs.microsoft.com/fr-fr/lifecycle/>).

La version d'un logiciel est communément visible dans l'écran « À propos de ». Sous Windows, la version courante est visible dans la section « À propos de » de l'onglet « Système » dans les paramètres. Les systèmes doivent être tenus à jour régulièrement.

- Au 01/07/2021, les seules versions de Windows qui devraient être utilisées sur les ordinateurs de bureau sont les versions postérieures ou égales à Windows 10 version 1909 qui bénéficie d'un support jusqu'en 2022.

L'utilisation de Internet Explorer de Microsoft est à éviter car le logiciel n'évolue

plus depuis plusieurs années, son moteur n'est plus compatible avec les derniers standards et il conserve de nombreuses failles de sécurité. Internet Explorer peut être remplacé par Edge de Microsoft qui assure une certaine compatibilité avec les anciennes versions.

- Les espaces de stockage en ligne dans le Cloud, telles que Microsoft OneDrive ou Google Drive ou Dropbox, sont déconseillés pour un usage professionnel parce qu'ils sont liés à un compte personnel, qu'ils induisent une dissémination des documents dans des endroits non contrôlés, que le partage sur les documents est souvent mal maîtrisé et que la confidentialité des données n'est pas assurée.

## 2.5 Les principales solutions du marché

Les ordinateurs peuvent être achetés auprès de distributeurs grand public (FNAC, Darty, LDLC...) ou de fournisseurs orientés vers les professionnels (inmac-wstore, SSII du notariat...).

Toutes les marques peuvent être choisies. Dell, HP et Lenovo constituent des marques usuelles pour un usage professionnel.

## 2.6 Les critères de choix

Pour un ordinateur personnel, la performance de la configuration est déterminée par :

- la performance du processeur : un processeur Intel Core i5 ou AMD Ryzen 5 peut être suffisant,
- la taille de la mémoire centrale : 8 Go minimum,
- le type de disque interne : disque dur classique et/ou disque SSD pour l'installation du système d'exploitation,
- la taille du disque interne : 256 Go minimum,
- la vitesse de lecture/écriture sur la mémoire et sur les disques,
- la taille de l'écran : 15 pouces minimum pour un ordinateur portable et 24 pouces pour un écran externe,
- la qualité de l'écran : respect des couleurs, revêtement anti-reflet.

Pour les logiciels et applications, la location d'une licence est souvent moins intéressante financièrement que son achat car le coût est calculé sur une fréquence d'un renouvellement tous les 3 ans alors que la fréquence de renouvellement réelle est plutôt de 4 ou 5 ans, voire plus, et les deux types d'acquisition bénéficient souvent des mises à jour.

## Le vocabulaire

**ChromeBook** : ordinateur allégé utilisant le système d'exploitation ChromeOS de Google et destiné à être connecté à Internet car principalement réduit à l'exécution du navigateur Internet Chrome ou des applications spécifiques du catalogue d'applications de Google.

**Disque SSD** : dispositif matériel de stockage dont le contenu est composé de mémoire flash qui n'est pas effacée en l'absence d'alimentation électrique et qui se comporte comme un disque dur très rapide.

**Mémoire cache** : espace destiné à stocker temporairement les données, dont celles fréquemment utilisées, afin d'accélérer les traitements. On trouve de la mémoire cache notamment, dans les processeurs et dans les disques, sous forme de mémoire vive spécifique, et dans les navigateurs internet, sous forme d'espace réservé en mémoire vive ou sur le disque dur. Les lectures/écritures de données sollicitent alors d'abord la mémoire cache dont le temps de réponse est plus rapide.

**Mémoire vive ou interne (RAM)** : composant matériel destiné à stocker les données et logiciels en cours d'exécution. Le contenu de la mémoire disparaît en l'absence d'alimentation électrique. La taille de la mémoire est usuellement exprimée en Go.

**Mémoire flash** : composant matériel de mémoire modifiable dont le contenu n'est pas effacé en l'absence d'alimentation électrique. La mémoire flash est utilisée pour remplacer les disques mécaniques dans les disques SSD.

**PC (Personal Computer)** : ordinateur personnel.

**Pouce (Inch)** : unité de mesure anglo-saxonne qui équivaut à 2,54 cm. Un écran de 15 pouces mesure 38 cm de diagonale.

**RPM (Rotation Per Minute)** : vitesse de rotation des plateaux internes d'un disque dur ; les vitesses usuelles sont 5.400, 7.200, 10.000 ou 15.000 tours/minute pour les disques les plus performants.

# 3. Le réseau local

## 3.1 Les concepts de base

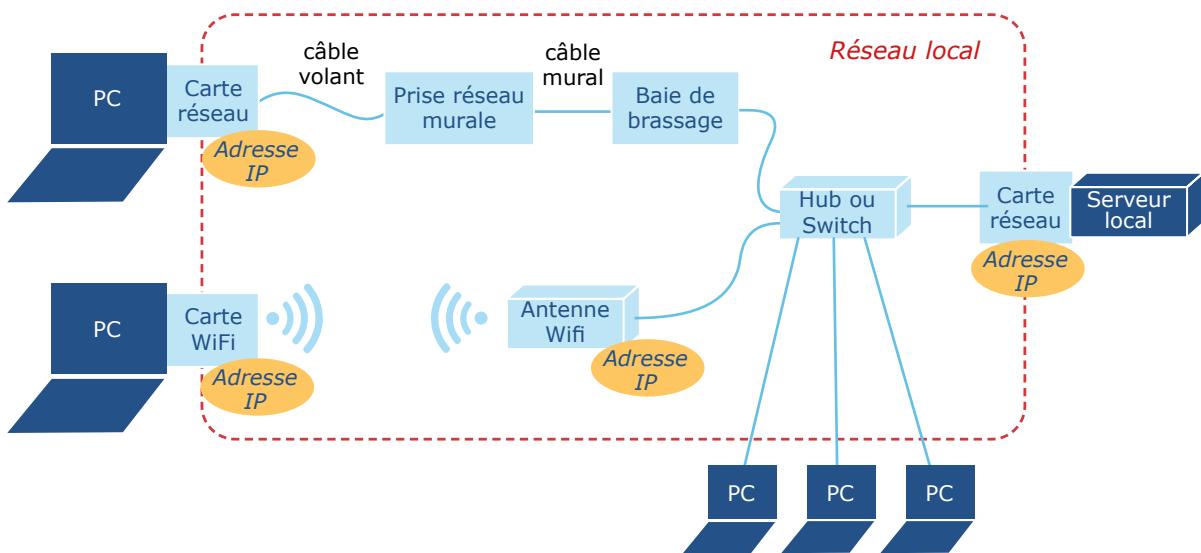
Le réseau local désigne le réseau informatique qui permet de relier les différents matériels informatiques (postes de travail, imprimantes, serveurs...) au sein d'une même entité géographiquement restreinte, souvent un bâtiment, afin qu'ils puissent communiquer entre eux.

### Constitution

Le réseau local est composé des éléments suivants :

- les câbles volants, permettant de relier des matériels informatiques aux prises du réseau installées dans les pièces,
- les câbles installés à demeure, qui permettent de relier les prises réseau à un équipement réseau central,
- un équipement réseau central, qui assure la communication entre tous les équipements : un concentrateur (hub) ou un commutateur (switch) pour un débit plus rapide,
- éventuellement, des bornes ou antennes Wifi pour relier des matériels avec des cartes réseaux sans fil.

Les matériels informatiques sont connectés en étoile sur l'équipement réseau central.



La norme de communication entre équipements techniques sur un réseau local filaire s'appelle Ethernet. Chaque équipement électronique possède une adresse MAC unique attribuée par son fabricant. Cette adresse peut être utilisée pour filtrer techniquement des équipements non autorisés.

La norme de communication par réseau local sans fil s'appelle Wifi. Une borne Wifi possède une antenne qui émet des ondes radioélectriques. Elle diffuse un nom (SSID) pour être reconnaissable par les matériels qui veulent s'y connecter. Les connexions ne sont autorisées qu'après validation d'un mot de passe.

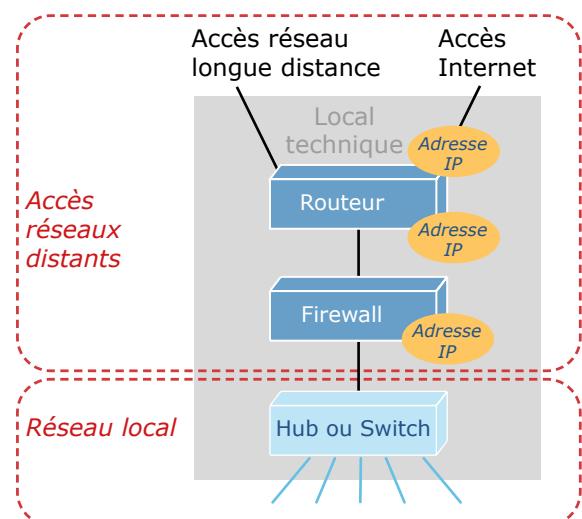
La norme de communication de bout en bout entre logiciels, sur un réseau local ou un réseau longue distance, s'appelle TCP/IP. Une adresse IP est attribuée à chaque matériel informatique raccordé à un réseau afin de pouvoir l'identifier comme émetteur ou destinataire d'un échange.

Différents ports logiciels, numérotés selon une convention publique, permettent à toutes les applications d'un même ordinateur de recevoir les communications qui leur sont destinées (par exemple, le port 80 est réservé aux échanges web HTTP).

## Accès distant

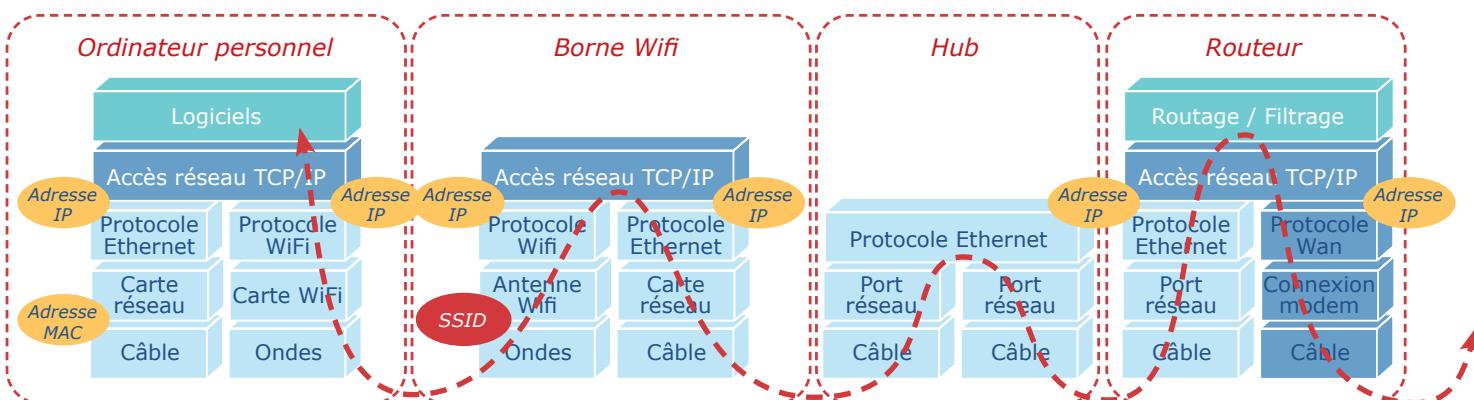
Un réseau local peut être relié à un réseau longue distance par un routeur afin de permettre aux ordinateurs locaux de communiquer avec des ordinateurs distants.

Afin de contrôler les accès entre le réseau longue distance et le réseau local, il est nécessaire d'installer un pare-feu (firewall). Le routeur du site local peut intégrer les fonctions de pare-feu.



## Chemin des échanges

Entre deux logiciels, les communications transitent en utilisant les équipements réseaux reliés les uns aux autres par les différentes technologies.



## 3.2 Les éléments structurants

Un câble réseau Ethernet ne peut pas dépasser 100 mètres.

Un réseau informatique est caractérisé par son débit. Le débit est exprimé en bits/seconde (il faut 8 bits pour coder 1 octet, c'est-à-dire 1 caractère).

Le débit sur un réseau local filaire avec Ethernet est de 10Mb/s ou 100Mb/s ou 1Gb/s voire 10Gb/s ou 100Gb/s pour les cartes réseau des serveurs.

Le Wifi regroupe plusieurs normes utilisées pour les réseaux sans fil. Le débit théorique varie entre 11Mb/s (norme 802.11a) et 450 Mb/s (norme 802.11n). La portée varie entre 20 et 70 mètres.

Conformément aux lois de la physique, plus les ondes ont une fréquence élevée (exprimée en Hertz), moins elles se propagent en distance et dans les matériaux denses. Les fréquences élevées (GHz), utilisées pour obtenir de hauts débits de communication, ont en général une portée plus limitée.

Certains usages, tels que la diffusion de vidéo, la visioconférence, sont très consommateurs de débit réseau : environ 1 Mb/s pour une session.

Les équipements réseaux centraux sont des matériels qui embarquent un logiciel spécifique.

### 3.3 Les particularités pour les notaires

Pour des raisons de sécurité, le réseau local d'un office ne peut pas être raccordé directement à un boîtier d'accès à Internet (box). Un pare-feu (firewall) doit être interposé.

Les routeurs et firewall doivent être installés et configurés par un des opérateurs réseaux agréés par le CSN.

### 3.4 Les bonnes pratiques

#### Débit

Le débit réel d'un réseau local dépend :

- pour un réseau filaire : de la qualité des câbles physiques,
- pour un réseau Wifi : de l'absence de perturbations électroniques, de l'absence d'obstacles physiques (murs épais), du nombre de matériels connectés simultanément et de la distance entre l'ordinateur et la borne Wifi.

Les câbles doivent être au moins de catégorie 5<sup>e</sup> pour accepter un débit de 2,5 Gb/s sur 100 mètres, voire de catégorie 6<sup>e</sup> adaptés à un débit de 10 Gb/s sur 100 mètres. Les câbles sont choisis de préférence blindés (Shielded) pour être moins sensibles aux perturbations électromagnétiques. La qualité des connexions et câbles installés doit être testée prise par prise par un technicien avec du matériel spécialisé après installation.

→ Dans la mesure du possible, pour obtenir le meilleur débit sur le réseau local, il est préférable d'être connecté au réseau local par un câble plutôt qu'en Wifi.

#### Sécurité

Comme tout élément émetteur d'ondes radioélectriques, les bornes Wifi ne doivent pas être installées trop près des utilisateurs.

Les équipements réseaux centraux (hub, switch) étant vitaux pour le bon fonctionnement du réseau, ils doivent être :

- installés dans un local technique, physiquement clos et bien ventilé, a minima une baie électrique fermée à clé voire une salle technique climatisée,
- protégés contre les surtensions électriques par un onduleur,
- protégés par des mots de passe robustes.

Le nom SSID diffusé par la borne Wifi doit être explicite.

L'accès au réseau Wifi doit être protégé par un mot de passe avec la norme WPA 2 ou 3 (« Wi-Fi Protected Access ») crypté selon la méthode AES (« Advanced Encryption Standard »). Le mot de passe doit être suffisamment long et complexe pour ne pas être découvert par une personne du voisinage qui ferait des essais successifs. Il doit être changé tous les 6 mois.

Les éléments réseaux, tels que le routeur ou le firewall, qui font le lien entre le réseau local et le réseau longue distance ou internet doivent être protégés et sécurisés.

→ Les mots de passe par défaut de tous les équipements réseaux doivent être changés avant la mise en service pour éviter à une personne extérieure d'utiliser cet équipement réseau comme cheval de Troie sur le réseau local.

Les versions des logiciels des équipements réseaux centraux doivent être mises à jour, dès qu'une mise à jour est disponible, afin de se prémunir contre les failles de sécurité. Il est donc nécessaire de vérifier régulièrement et au moins une fois par an si des mises à jour doivent être installées.

## 3.5 Les principales solutions du marché

Les câbles RJ45 fixes d'un réseau local peuvent être installés par un électricien équipé du matériel adéquat pour tester que les connexions sont de qualité.  
Les concentrateurs (hubs) et commutateurs (switch) peuvent être achetés chez n'importe quels fournisseurs. Ils sont en général plug-and-play.

## 3.6 Les critères de choix

La proximité avec l'installateur permet de faire évoluer le réseau local et gérer les pannes rapidement.

Le débit standard du réseau local couvre en général les besoins classiques d'un office.

Hormis pour des raisons de sécurité ou pour des entités de grande taille, il n'est pas nécessaire de prévoir des paramétrages spécifiques, tels que la création de sous-réseaux ou la réservation de flux pour certains usages.

## Le vocabulaire

**Adresse IP**: numéro d'identification attribué à un appareil connecté à un réseau et constitué de 4 nombres entre 0 et 255 (ex : 192.6.212.23).

**Bandé passante**: à l'origine un terme électronique, utilisé par abus de langage pour désigner le débit maximum du réseau.

**Bluetooth**: norme de communication radioélectrique (sans fil) de courte portée adaptée pour relier à quelques mètres les équipements électroniques, tels que casques, enceintes audio, à un équipement tel qu'un PC ou un téléphone : portée jusqu'à 10 mètres avec un débit de 2Mb/s.

**CPL (Courant Porteur en Ligne)**: réseau utilisant le réseau électrique pour transporter l'information et permettant de s'affranchir d'un câble réseau spécifique.

**Débit**: quantité d'information qui peut transiter pendant un laps de temps. L'unité de mesure du débit est le nombre de bits par seconde (Kb/s ou Kbps, Mb/s ou Mbps, Gb/s ou Gbps).

**Ethernet**: norme d'accès au réseau local

**Hub (ou concentrateur)**: équipement matériel destiné à renvoyer le trafic réseau reçu sur un port vers tous les autres ports.

**LAN (Local Area Network)**: Réseau informatique local.

**MAC (Media Access Control)**: adresse unique attribuée à une carte réseau par son constructeur et constitué de 6 nombres entre 0 et 255 sous forme hexadécimale (ex : 00:37:6C:E2:EB:62)

**Onduleur**: équipement électrique destiné à stabiliser la tension électrique et éliminer les parasites. Certains onduleurs intègrent des batteries pour laisser le temps au matériel de s'arrêter proprement en cas de coupure électrique.

**PoE (ou Power over Ethernet)**: technologie de réseau local qui permet d'apporter l'alimentation électrique via un câble Ethernet RJ45 pour limiter les câbles vers les petits équipements tels que les téléphones, les caméras IP.

**RJ45**: format des prises pour le réseau comportant 8 fils en cuivre (4 paires torsadées).

**RJ11**: format des prises pour la téléphonie comportant 4 fils en cuivre (2 paires torsadées).

**SSID (Service Set Identifier)**: Nom d'identification donné à un réseau Wifi particulier.

**Switch (ou commutateur)**: équipement matériel destiné à renvoyer le trafic réseau reçu sur un port seulement vers le port auquel il est destiné.

**TCP/IP (Transmission Control Protocol/Internet Protocole)**: ensemble de protocoles qui permettent l'échange de données entre deux logiciels situés sur des ordinateurs différents quels que soient les types de réseaux qui les relient. TCP/IP définit notamment les règles de découpage, d'adressage et de routage pour acheminer les données de manière fiable au bon destinataire.

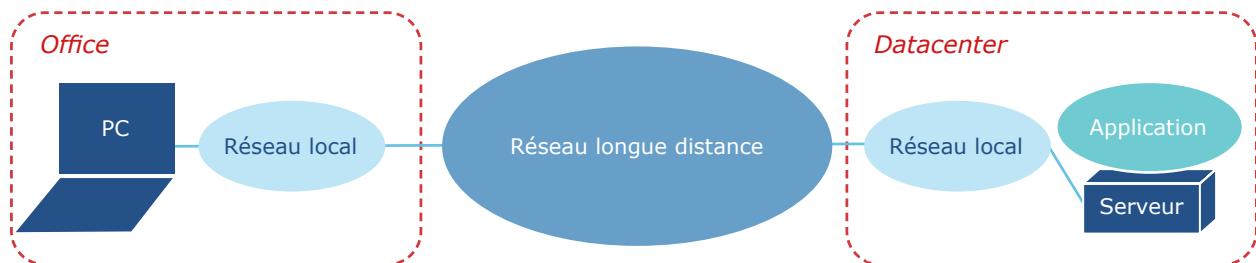
**WAN (Wide Area Network)**: réseau longue distance entre sites, tel que le réseau notarial ou Internet.

**Wifi (Wireless Fidelity)**: norme de communication radioélectrique (sans fil) de moyenne portée adaptée pour la communication entre un matériel réseau et une borne Wifi: portée jusqu'à 70 mètres avec un débit théorique maximum jusqu'à 600Mb/s.

# 4. Le réseau notarial longue distance

## 4.1 Les concepts de base

Un réseau longue distance permet à des ordinateurs connectés à un réseau local d'accéder à des serveurs connectés sur un réseau local distant pour utiliser les applications qui y sont installées.



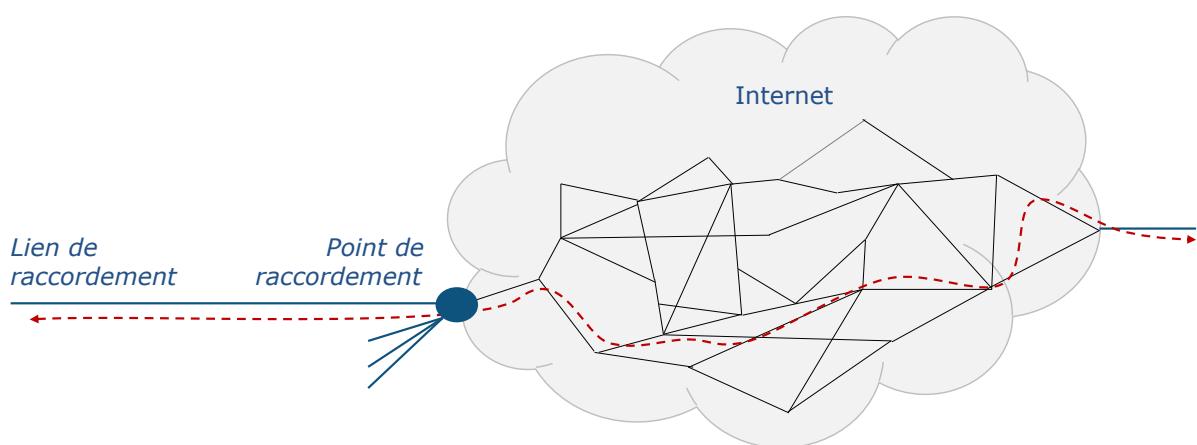
Il existe deux types de réseaux longues distances :

- les réseaux publics, comme Internet, qui autorisent tout le monde à s'y connecter et qui véhiculent tous types d'échanges,
- les réseaux privés auxquels l'accès est contrôlé.

### Internet

Le réseau Internet est un réseau longue distance basé sur des chemins partagés et raccordés les uns aux autres. Ce maillage par construction le rend moins sensible aux pannes sauf sur des tronçons uniques car coûteux (ex : liens intercontinentaux, desserte d'une extrémité reculée).

Le réseau Internet n'assure pas la confidentialité des données qui sont véhiculées car le trafic passe sur des équipements réseaux divers et privés.



Comme les échanges entre utilisateurs différents peuvent emprunter le même chemin ou vouloir accéder au même serveur, le débit n'est pas garanti plus loin qu'entre l'utilisateur et le point de raccordement de son accès Internet chez l'opérateur télécom.

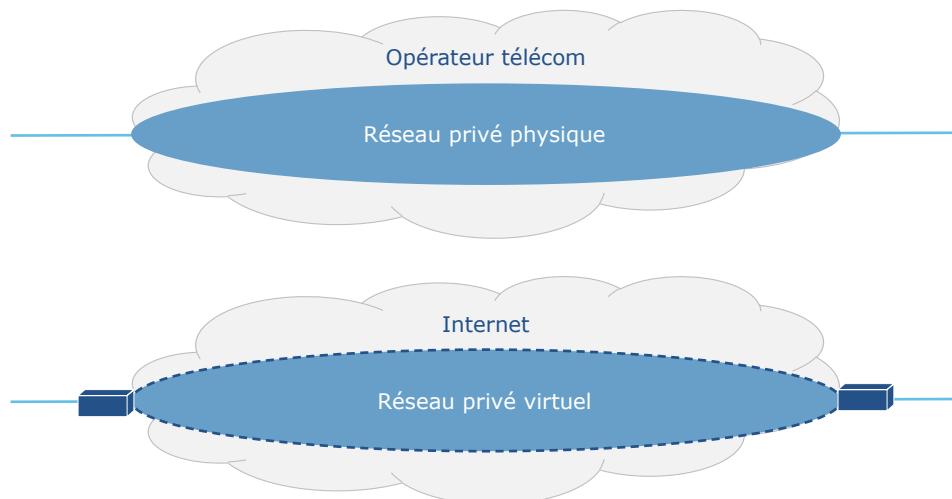
Le routeur est l'équipement réseau qui permet de :

- relier un réseau local d'office à un réseau longue distance pour n'envoyer sur le réseau longue distance que le trafic qui a besoin de sortir du réseau local,
- choisir le meilleur chemin jusqu'à destination en fonction de différents critères, lorsque plusieurs chemins sont possibles.

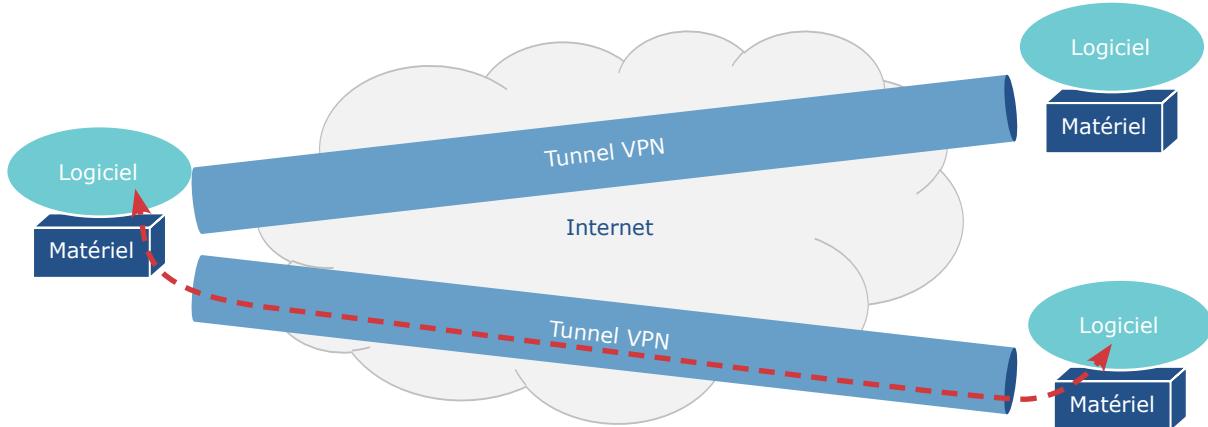
## Réseau privé

Un réseau privé peut être :

- soit physique et constitué de liaisons privées fournies par un opérateur télécom, comme un réseau MPLS d'entreprise ; l'accès au réseau est alors restreint, ce qui assure la confidentialité des échanges ;
- soit virtuel et basé sur un réseau public, tel qu'Internet ; il est alors du ressort des matériels (routeurs) ou des logiciels d'extrémité (applications, navigateur et site internet) d'assurer la confidentialité des échanges de bout en bout.



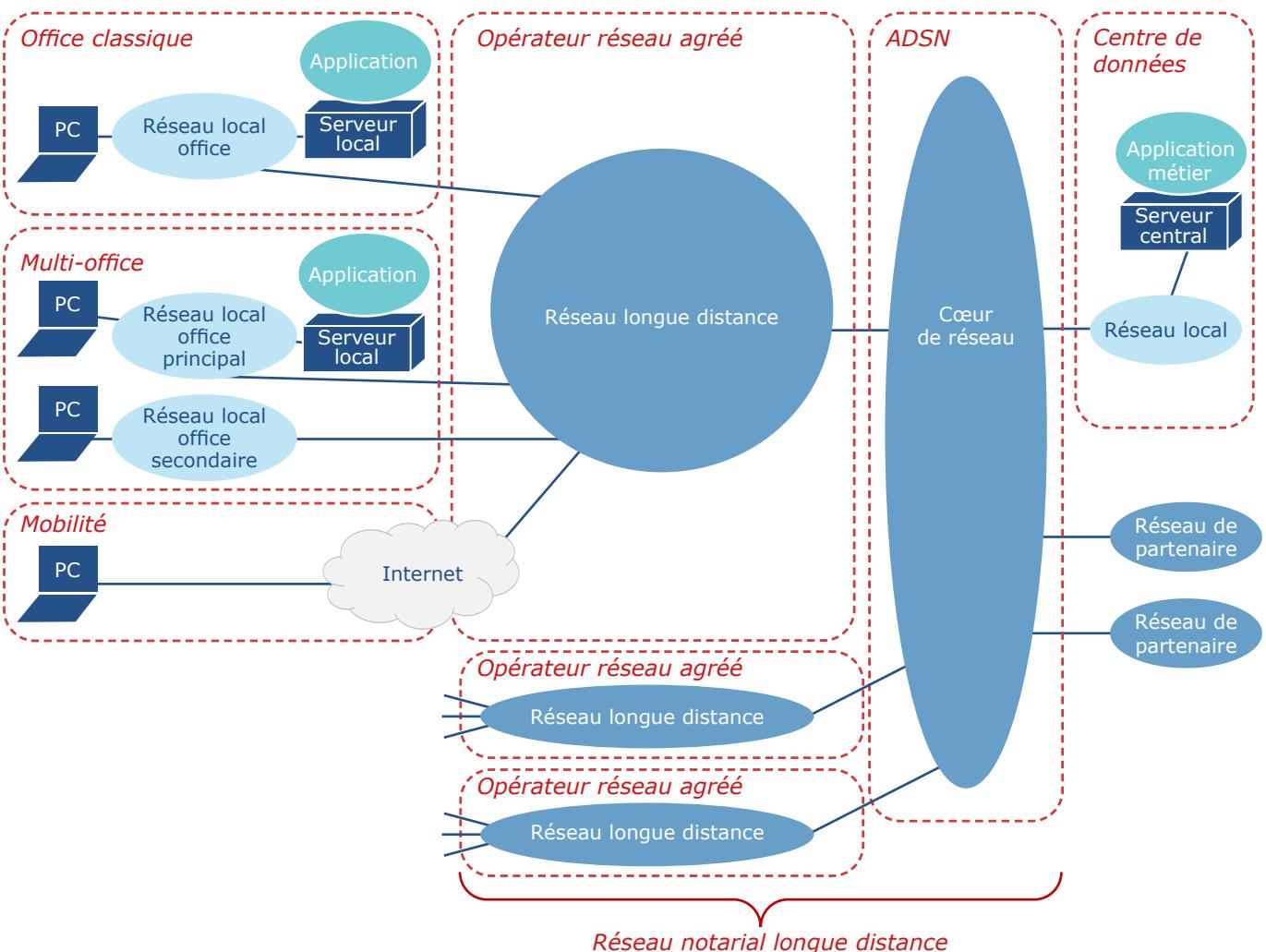
Pour constituer un réseau virtuel sécurisé à partir d'un réseau public, les extrémités peuvent créer un tunnel ou VPN (Virtual Private Network) : tous les flux sont chiffrés à l'origine et déchiffrés à destination afin qu'un tiers qui intercepterait l'échange ne puisse pas en comprendre le contenu.



## Réseau notarial

Le « réseau notarial » est le réseau longue distance qui interconnecte les réseaux locaux de tous les offices avec les réseaux locaux des centres de données (datacenters), qui hébergent les serveurs centraux destinés aux applications métier, et les réseaux des partenaires de la profession tels que la CDC, la DGFiP, la CINP etc.

Le réseau notarial se décompose en deux parties : le réseau longue distance privé propre à chaque opérateur réseau agréé, sur lequel se connectent les offices notariaux, et le « cœur de réseau » qui fédère tous les réseaux.

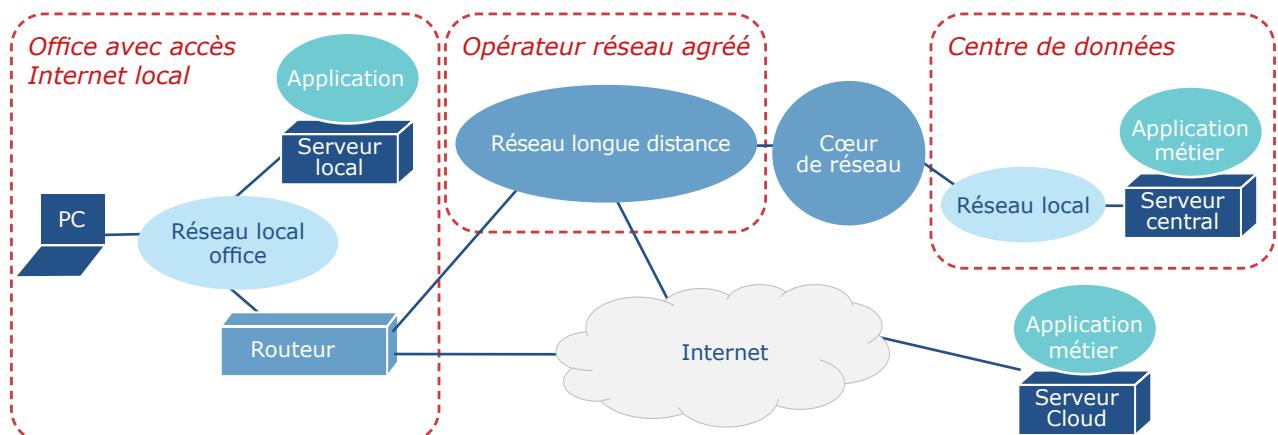


Dans le cas d'une entité répartie sur plusieurs sites (ex : office multisites), afin que les utilisateurs d'un site déporté puissent utiliser les serveurs installés sur le réseau local de l'autre site, les deux réseaux locaux peuvent être reliés soit par une solution de réseau local étendu, soit par le réseau notarial longue distance d'un opérateur réseau agréé.

Les opérateurs réseau agréés offrent des points d'entrée via internet pour des ordinateurs personnels en mobilité qui doivent accéder à des serveurs accessibles seulement par le réseau notarial.

## Raccordement à Internet

De nombreuses applications ne sont accessibles que via le réseau Internet. Il est donc nécessaire pour les offices notariaux d'avoir un accès au réseau Internet. Selon l'opérateur réseau agréé choisi, ce raccordement peut se faire soit localement au niveau de l'office, soit dans le réseau privé de l'opérateur réseau.



## Lien de raccordement

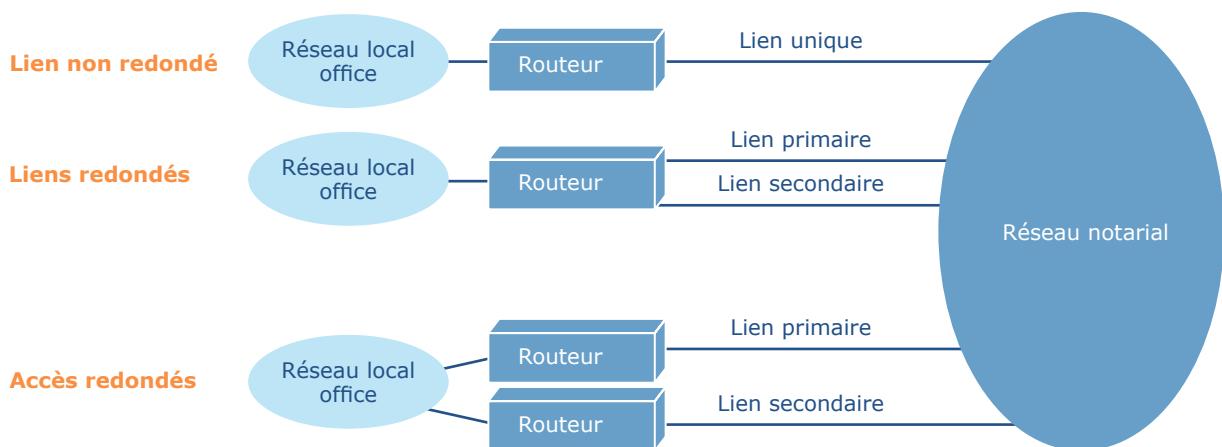
Le raccordement du réseau local d'un office au réseau notarial se fait par un « lien de raccordement » fourni par un opérateur réseau agréé.

Ce lien peut être simple ou doublé pour assurer une redondance. Avec un lien doublé, en cas de panne d'un des liens, les échanges basculent automatiquement sur le second lien sans entraîner de coupure des transmissions.

Les deux liens qui assurent la redondance peuvent être en mode actif/passif, le lien passif est alors dormant jusqu'à la bascule, ou actif/actif, les deux liens sont actifs simultanément et, en théorie, chaque lien doit pouvoir supporter tout le flux de l'autre lien en cas de bascule.

Le routeur de l'office est chargé d'optimiser les flux en fonction de la performance et de la disponibilité de chaque lien.

Pour se protéger contre une éventuelle panne du routeur qui devient le maillon faible de l'accès aux liens, il est possible d'installer deux routeurs en redondance l'un sur l'autre.



Dans ce cas, les deux routeurs peuvent être actifs ensemble et se répartir, hors cas de panne, la charge du trafic en fonction de la destination ou du type de flux. Par exemple, un des routeurs peut se charger des flux vers Internet.

L'utilisation de plusieurs liens permet également d'augmenter le débit disponible vers le réseau notarial. Si un des liens est défaillant, même si les échanges sont assurés, le débit de sortie est néanmoins réduit car tous les flux utilisent alors le seul lien disponible.

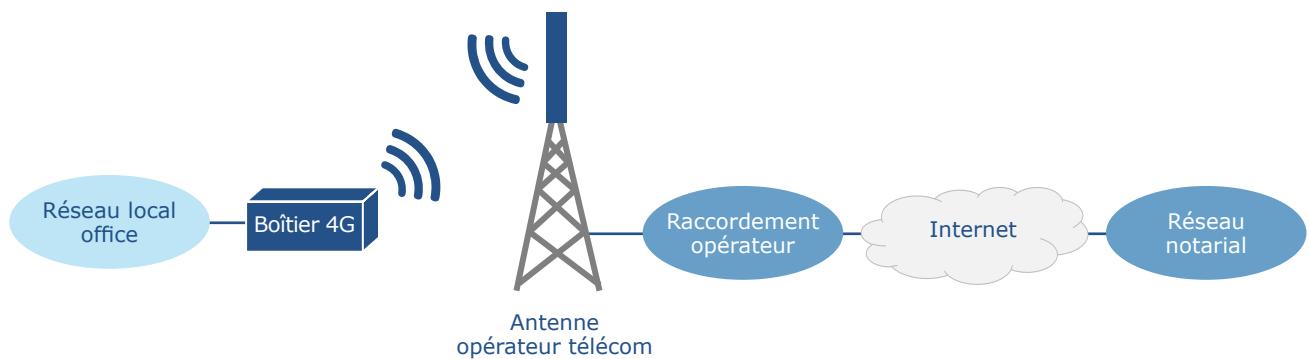
## Support physique

Le support physique utilisé pour le lien de raccordement peut être :

- une ligne téléphonique en cuivre constituée d'au moins 2 fils (torsadés pour réduire la sensibilité aux parasites),
- un câble coaxial en cuivre qui, étant insensible aux perturbations électromagnétiques, permet un meilleur débit,
- un câble réseau spécifique fourni par un opérateur télécom spécialisé (ex : câble Ethernet),
- une fibre optique qui permet un très haut débit, entre 100 Mb/s et 1 Gb/s, sur des longues distances.

Pour un support physique qui permet un débit théorique maximum donné, le débit réellement disponible dépend de l'abonnement souscrit auprès de l'opérateur.

Pour répondre à certains besoins, comme un lien de secours ou l'impossibilité d'avoir un support physique, un lien via le réseau téléphonique 4G ou 5G peut être proposée par l'opérateur télécom.



Le réseau 4G propose, dans de bonnes conditions et suivant le lieu géographique, un débit mutualisé qui peut atteindre en pic jusqu'à 200 Mbit/s en réception et 20 Mbit/s en émission.

Le réseau 5G reprend les fréquences radio de la 4G et peut utiliser également des fréquences radio jusqu'à 20 fois plus élevées. Il débute son déploiement en 2021 en France et propose un débit en pic jusqu'à 2 Gbit/s en réception et des temps de latence très faibles, mais avec une portée géographique moindre (moins de 1 km de l'antenne et moins bonne pénétration dans les bâtiments).

## Technologie

Sur un support physique en cuivre, plusieurs technologies sont proposées par les opérateurs :

- la technologie ADSL (asymétrique) où le débit de réception, de 1 à 15 Mb/s, est supérieur au débit d'émission afin de favoriser les téléchargements à partir de sites web ;
- la technologie VDSL (Very-High-Bit-Rate) où le débit de réception varie de 15 à 70 Mb/s ;
- la technologie SDSL (symétrique) où les débits de réception et d'émission sont identiques et souvent garantis jusqu'à 10 Mb/s afin de faciliter les transmissions dans les deux sens ;
- la technologie EFM (symétrique) où les débits de réception et d'émission, jusqu'à 20 Mb/s, sont identiques et garantis.

### Technologie ADSL



### Technologie SDSL



Seule la technologie ADSL peut cohabiter sur un câble en cuivre avec une ligne téléphonique analogique traditionnelle.

Sur un support physique en fibre optique, plusieurs technologies sont proposées par les opérateurs :

- la technologie FTTH (fibre optique jusqu'à la maison) : le support est partagé entre tous les abonnés raccordés au point de distribution de l'opérateur ; le débit étant mutualisé entre les abonnés, il n'est pas garanti ;
- la technologie FTTO ou FTTB (fibre optique jusqu'au bureau ou bâtiment) ; le support est dédié à un abonné ; le débit minimal est garanti et symétrique.

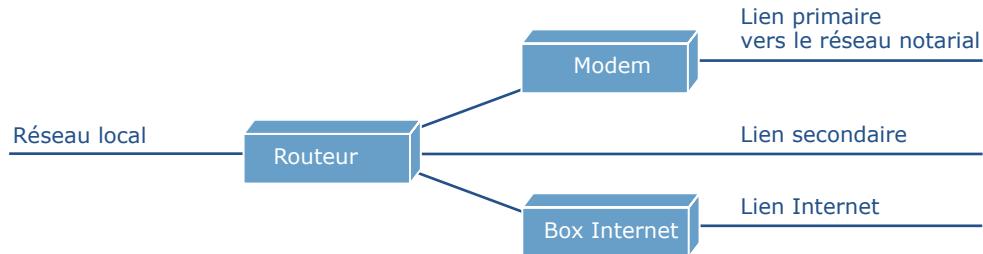
## Terminaison

La technologie est mise en œuvre sur le support physique par un matériel de terminaison.

Ce matériel de terminaison peut être un matériel spécifique, appelé modem, ou directement le routeur avec les interfaces adéquates.

Les box internet font office à la fois de modem et de routeur basique entre le réseau local et le réseau internet.

Le routeur de l'office fourni par l'opérateur réseau agréé doit être raccordé à chaque lien ou au modem quand il existe.



## 4.2 Les éléments structurants

Les différentes technologies se distinguent par le débit maximum supporté en émission et en réception (symétrique ou asymétrique), le débit dédié à un client ou mutualisé entre clients, donc garanti ou non garanti entre le site et le point de raccordement.

Le débit proposé par le lien de raccordement et le nombre de liens actifs influencent la vitesse de transmission des données et donc le confort d'accès aux services et applications distantes. La réactivité perçue d'une application dépend cependant aussi de la capacité du serveur qui la supporte à gérer de nombreuses sollicitations simultanées et de la complexité des traitements réalisés.

Le débit maximum d'un raccordement dépend de la performance du routeur d'accès, du débit maximum supporté par le support physique et du débit souscrit chez l'opérateur.

Le débit réel d'un accès dépend du nombre de clients de l'opérateur connectés sur ce point de raccordement, au-delà du lien, et, dans le cas d'un support en cuivre, de la distance du lien entre l'office et le point de raccordement physique chez l'opérateur (bas de l'immeuble, bout de la rue...).

Dans le cas d'une connexion par liaison 4G ou 5G, le débit réel décroît rapidement lorsque la densité d'utilisateurs augmente (milieu urbain) et lors de l'éloignement par rapport à l'antenne.

Le dimensionnement du lien réseau dépend des usages (web, visioconférence, téléphonie...), du nombre d'utilisateurs qui vont se partager le lien et de la localisation des serveurs utilisés (dans l'office, dans un centre de données distant, sur Internet).

Tous les flux générés par les utilisateurs se partagent le débit du lien de sortie. Sachant qu'un flux de visioconférence utilise environ 1Mb/s par session, il faut veiller à bien dimensionner le lien de raccordement.

La responsabilité de l'opérateur réseau couvre le bon fonctionnement du réseau longue distance jusqu'au matériel de terminaison inclus : box ou modem éventuel pour l'opérateur télécom, routeur pour l'opérateur réseau agréé.

## 4.3 Les particularités pour les notaires

La fourniture d'un lien d'accès au réseau notarial n'est possible que par un opérateur réseau agréé par le CSN.

Le terme « réseau REAL » désigne seulement le réseau longue distance de l'opérateur réseau Adnov.

Toutes les offres d'accès réseau agréées par le CSN permettent l'accès aux applications métier de l'ADSN et supportent l'ensemble des offres de visioconférence agréées par le CSN.

Pour des raisons de sécurité, il est interdit de connecter une box Internet en direct à un réseau local d'office. Cette connexion doit obligatoirement se faire sur le routeur de sortie vers le réseau notarial ou chez l'opérateur réseau.



Les partenaires de la profession (DGFiP, CDC, CINP...) peuvent se raccorder au cœur de réseau notarial selon des modalités spécifiques définies par le CSN et mises en œuvre par l'ADSN.

## 4.4 Les bonnes pratiques

### Accès Internet

De plus en plus, les échanges de données professionnels concernent des serveurs et des applications qui sont connectés à Internet. Il est donc recommandé de disposer d'une sortie vers Internet ayant un bon débit.

La fourniture, par l'opérateur réseau agréé, d'un accès à Internet au niveau de l'office évite de faire transiter le flux Internet (navigation web...) sur tout le réseau longue distance ; ce qui permet de limiter le débit nécessaire au lien de raccordement au réseau notarial longue distance et donc son coût.

- ➔ Les accès à Internet sont banalisés. Un lien d'accès à un Internet peut être substitué par un autre. Un opérateur télécom qui fournit le lien d'accès à Internet peut être remplacé par un autre.

### Débit

Les débits symétriques entre l'émission et la réception, comme le propose la technologie SDSL, sont à privilégier si le réseau local héberge un serveur informatique avec une application ou un site web qui doit être accessible depuis l'extérieur, ainsi que pour la visioconférence.

En cas d'installation de deux liens redondants, il faut s'assurer auprès de l'opérateur télécom que les deux liens n'utilisent ni le même faisceau de câbles physiques, ni les mêmes chemins d'adduction vers l'office. En effet, la panne physique la plus fréquente et la plus longue à réparer est la coupure d'un tronçon de câbles dans la rue par une pelleteuse. Si deux liens redondants passent physiquement au même endroit, la coupure simultanée des deux liens rend la redondance inopérante.

## Sécurité

Les équipements réseaux d'interconnexion (routeur, firewall, serveur de connexions...) étant vitaux pour le bon fonctionnement de l'office, il faut veiller à ce qu'ils soient :

- installés dans un local technique, physiquement clos et bien ventilé, a minima une baie électrique fermée à clé voire une salle technique climatisée,
- protégés contre les surtensions électriques par un onduleur,
- doublés (redondés) dans la mesure du possible,
- protégés par des mots de passe robustes.

## 4.5 Les principales solutions du marché

→ À la date du 01/07/2021, les partenaires agréés par le CSN pour délivrer des accès au réseau notarial sont :

- Adista avec son offre réseau Janua ;
- Adnov avec la gamme RealIT déclinée avec les offres UnIT, AgilIT, AgilIT+ et SerenIT ;
- Comnot avec son offre d'accès au réseau notarial ;
- Navista avec son offre d'accès au réseau notarial.

Cette liste peut évoluer dans le temps et sa version à jour est diffusée sur le portail REAL.

Les fournisseurs des liens locaux de raccordement à Internet peuvent être :

- les opérateurs télécom grand public : Bouygues Telecom, Free, Orange, SFR ;
- les opérateurs télécom dédiés aux entreprises, spécialisés en fibre optique ou dédié à une couverture géographique spécifique : Altitude télécom, Axione, Bretagne Telecom, BT (ex-British Telecom), etc.

## 4.6 Les critères de choix

Les possibilités sont dépendantes de la variété des supports physiques et opérateurs télécoms disponibles à l'emplacement de l'office notarial.

Le choix de la technologie est fonction du débit requis par l'office qui est lui-même dépendant :

- du nombre de collaborateurs dans l'office,
- de la localisation des serveurs physiques qui portent les applications : locale ou Cloud.
- des autres types d'usages : navigation sur Internet, visioconférence, téléphonie IP, sauvegarde à distance...

Le choix d'un opérateur doit prendre en compte :

- le débit maximum proposé,
- le coût d'installation (« Frais d'Accès au Service »),
- les éventuels coûts et délais de génie civil pour amener le support physique choisi jusqu'à l'étude notariale,
- le coût de l'abonnement mensuel,
- la réactivité du support technique en cas de dysfonctionnement définie par la Garantie de Temps de Rétablissement.

→ La Garantie de Temps de Rétablissement d'un lien, souvent de 4h, n'est pas un délai garanti quoi qu'il arrive mais un délai cible de rétablissement par l'opérateur en cas d'incident. À défaut de respect, le client peut demander des pénalités à l'opérateur. Pour assurer la disponibilité d'un raccordement, il est préférable de choisir des liens redondants.

## Le vocabulaire

**4G (4<sup>e</sup> Génération)**: technologie de transfert de données pour téléphonie mobile.

**5G (5<sup>e</sup> Génération)**: technologie de transfert de données haut débit pour téléphonie mobile utilisant des fréquences très élevées mais de portée géographique limitée (1 km autour de l'antenne).

**ADSL (Asymmetric Digital Subscriber Line)**: technologie de réseau où le transfert des données est asymétrique car le débit de réception est environ 15 fois supérieur au débit d'émission.

**EFM (Ethernet in the First Mile, aussi appelé « SDSL Ethernet »)**: lien de raccordement par câble réseau en cuivre utilisant la technologie Ethernet.

**FTTE (Fiber to the Enterprise)**: fibre optique non dédiée dont le débit est garanti et symétrique.

**FTTH / FTTP (Fiber to the Home / Fiber to the Premise)**: fibre optique non dédiée dont le débit est mutualisé et asymétrique.

**FTTO / FTTB (Fiber To The Office / Fiber to the Building)**: fibre optique dédiée dont le débit est garanti et symétrique.

**GTR (Garantie de Temps de Rétablissement)**: délai contractuel, souvent exprimé en heures, dans lequel un service accidentellement interrompu doit être rétabli par l'opérateur.

**Latence réseau**: délai nécessaire pour que des données soient transmises de l'émetteur au destinataire.

**Modem (Modulateur-Démodulateur)**: matériel réseau de terminaison d'un lien d'accès à un réseau longue distance.

**MPLS (MultiProtocol Label Switching)**: réseau longue distance privé fourni par un opérateur télécom, avec des points de raccordements multiples et sécurisés.

**Pare-feu (Firewall)**: logiciel, pouvant reposer sur un matériel réseau dédié, destiné à filtrer les échanges entre un réseau local et un réseau externe par l'application de règles afin d'assurer la sécurité.

**Proxy**: serveur logiciel qui relaie les requêtes entre des systèmes installés sur deux réseaux différents pour accélérer les échanges, tracer les requêtes, anonymiser l'identité des émetteurs et éventuellement bloquer certaines requêtes.

**QoS (Quality of Service)**: méthode de priorisation des flux sur une liaison pour garantir des engagements de débit à certains flux en cas de congestion.

**Réseau REAL** : nom du réseau privé fournit par l'opérateur ADNOV.

**Routeur**: matériel réseau destiné à choisir le meilleur chemin parmi plusieurs liens pour atteindre un équipement distant connecté à un réseau longue distance.

**SD-WAN (Software-Defined Wide Area Network)**: technologie logicielle permettant d'optimiser les flux de communication vers les Datacenters et Internet sur une infrastructure mixant des réseaux privés, sécurisés mais coûteux et de débit limité, avec des accès internet locaux, non sécurisés mais peu chers et proposant un bon débit.

**SDSL (Symmetric Digital Subscriber Line)**: technologie de réseau où le transfert des données est symétrique car le débit de réception est le même que celui d'émission.

**VDSL (Very high-speed rate Digital Subscriber Line)**: technologie de réseau similaire à l'ADSL avec des débits supérieurs.

**WAN (Wide Area Network)**: réseau longue distance permettant de relier plusieurs sites.

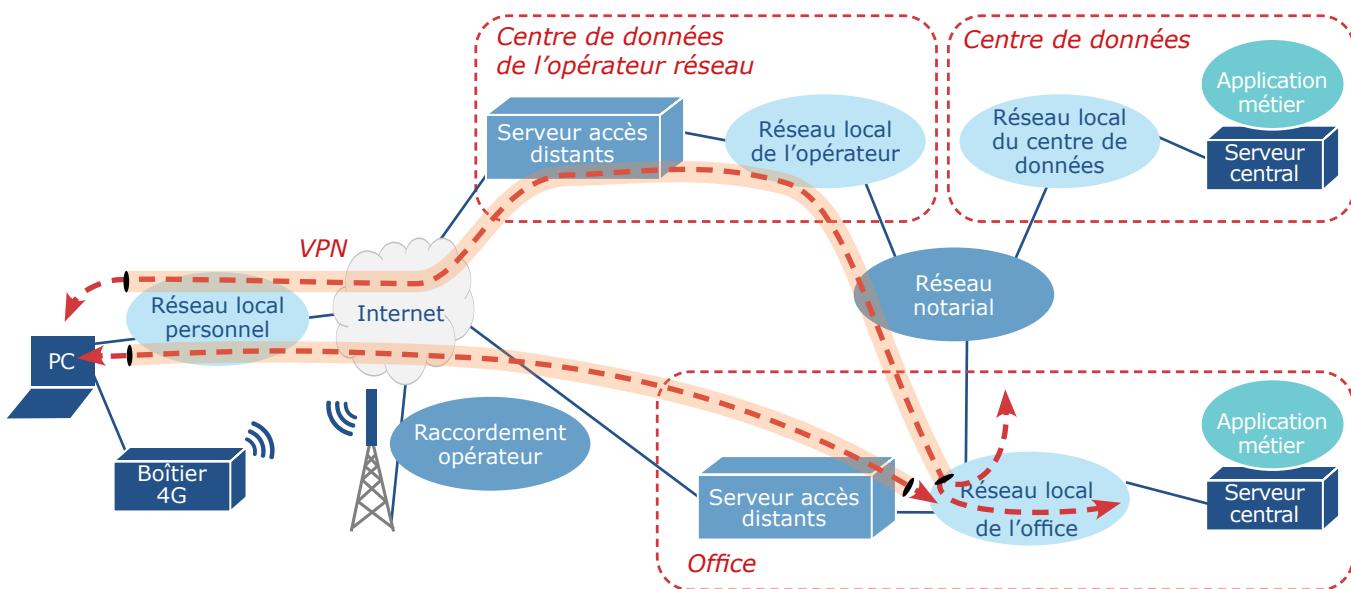
# 5. Les accès distants en mobilité

## 5.1 Les concepts de base

Un accès distant en mobilité permet à un utilisateur d'accéder aux ressources d'un réseau local et à des applications métier centrales quand il est en déplacement (nomadisme) ou en télétravail.

Pour cela, l'utilisateur doit d'abord se connecter à Internet via un accès Internet local ou via le réseau 4G. Ensuite, il doit lancer un logiciel spécifique installé sur son poste de travail qui lui permet de s'authentifier sur le serveur d'accès distants d'un opérateur réseau.

En fonction de l'opérateur réseau, le serveur d'accès distant peut être installé soit dans un centre de données de l'opérateur réseau, soit dans le routeur de l'office lorsque celui-ci dispose d'un accès Internet local.



Une fois que l'utilisateur est reconnu par le serveur d'accès distants, un tunnel VPN est créé de bout en bout, entre l'équipement de l'utilisateur et le réseau de l'office, dans lequel l'ensemble des échanges seront cryptés.

Toutes les transmissions de l'utilisateur vont être relayées vers les applications métier requises comme si cet utilisateur était connecté directement au réseau local de l'office.

Les échanges sur les réseaux intermédiaires, comme Internet, ne pourront pas être lus par une tierce personne.

## 5.2 Les éléments structurants

Chaque utilisateur connecté simultanément utilise une connexion distante et authentifiée sur le serveur d'accès distants.

L'ouverture d'une liaison VPN nécessite au préalable la souscription d'un service spécifique.

Le confort de l'accès aux applications distantes est conditionné par :

- le débit du plus faible réseau intermédiaire,
- la complexité du chemin entre l'utilisateur et l'application utilisée,

- les autres utilisations parallèles qui peuvent saturer les réseaux ou l'accès Internet.

### 5.3 Les particularités pour les notaires

La fourniture d'accès distants pour utilisateur nomade n'est possible que par un opérateur réseau agréé par le CSN.

Le logiciel à lancer sur le poste de travail dépend de l'opérateur réseau agréé.

### 5.4 Les bonnes pratiques

L'équipement qui se connecte via un accès distant doit être protégé comme toute station de travail raccordée au réseau local d'un office (antivirus...).

- En déplacement, il est fortement déconseillé de se connecter à Internet via un accès Wifi public qui peut être une source d'infection ou de surveillance avant l'activation du tunnel VPN. Un accès à Internet via le réseau 4G d'un opérateur télécom est préférable.

### 5.5 Les principales solutions du marché

- À la date du 01/07/2021, les opérateurs réseau agréés par le CSN pour délivrer des accès distants sont :

- Adista avec son offre ADistance liée à l'offre Janua,
- Adnov avec son offre Ballade liée à ses offres RealIT,
- Comnot,
- Navista.

Cette liste peut évoluer dans le temps et sa version à jour est diffusée sur le portail REAL

### 5.6 Les critères de choix

Le critère de choix est principalement le coût récurrent par utilisateur car le débit d'une connexion dépend du débit de l'accès Internet utilisé.

## Le vocabulaire

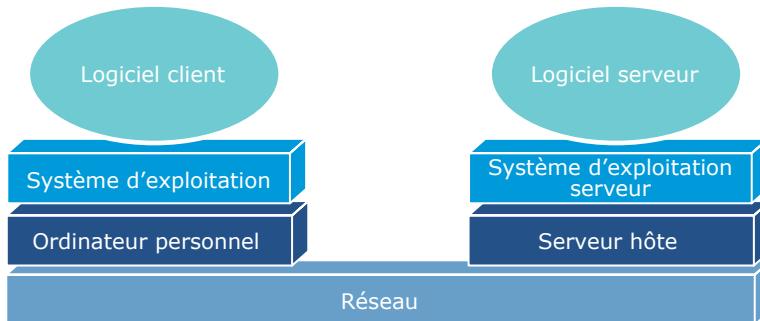
**VPN (Virtual Private Network)** : tunnel chiffré établi entre deux équipements reliés à un réseau et dans lequel passent tous les échanges de données.

# 6. Les serveurs hôtes

## 6.1 Les concepts de base

Un serveur est un dispositif matériel ou logiciel qui offre des services utilisés par des utilisateurs à partir d'autres ordinateurs.

Un serveur hôte (« host » en anglais), ou serveur matériel ou serveur physique, est un ordinateur utilisé pour installer une fonction logicielle (ex: serveur de fichiers partagés, serveur d'imprimantes, serveur web ...) ou une application partagée accessible à distance ; on parle alors d'application utilisée en mode client-serveur.



## Constitution

Un serveur hôte étant une ressource partagée très sollicitée, il se distingue d'un ordinateur personnel classique par :

- un ou plusieurs processeurs puissants,
- plus de mémoire,
- un grand espace de stockage avec des disques rapides et sécurisés contre les pannes (RAID),
- une connexion réseau performante,
- un système d'exploitation avec des fonctions propres de serveur, telles que la capacité à servir de serveur logiciel de fichiers ou d'imprimantes.

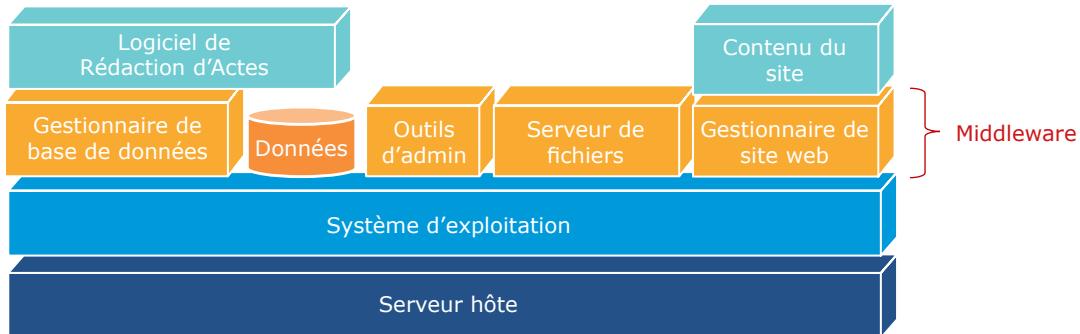
## Logiciels

Il y a deux grandes familles de systèmes d'exploitation destinés aux serveurs hôtes :

- Windows Serveur de Microsoft,
- Unix et les différentes déclinaisons de Linux, comme RedHat, Ubuntu ou Debian.

Un serveur hôte peut supporter :

- des logiciels techniques spécifiques (« middleware ») pour enrichir les fonctionnalités fournies par le système d'exploitation : gestionnaire de base de données, outils d'administration, gestionnaire de sites web, bibliothèques de langages de programmation, fonctions logicielles spécifiques, etc. ;
- des applications métier spécifiques (Logiciel de Rédaction d'Actes, comptabilité, gestion en ligne...) et leurs données.



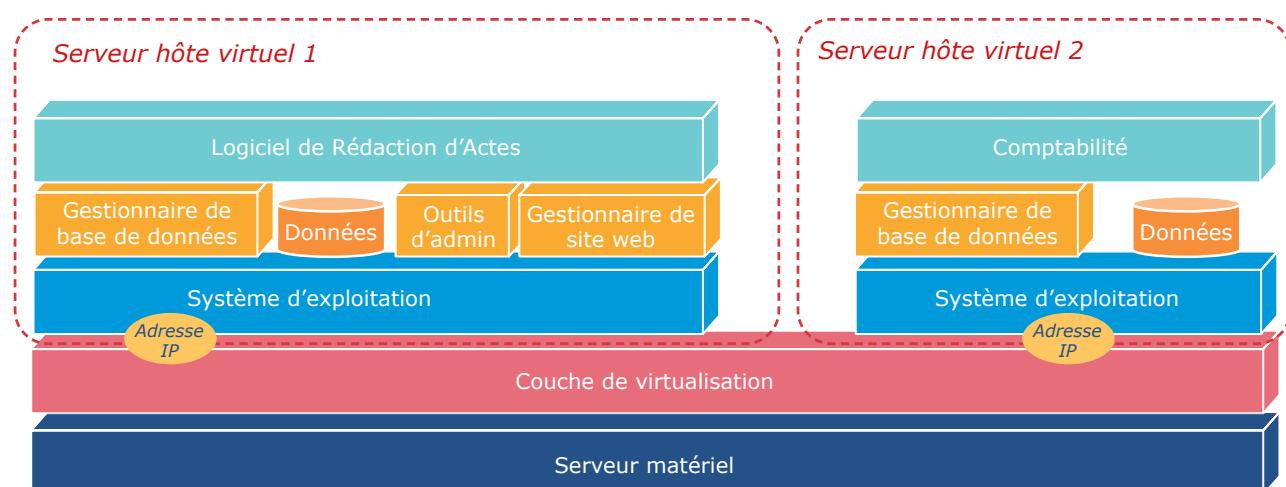
Les principaux logiciels techniques sont :

- gestionnaires de base de données : SQL Server de Microsoft, Oracle Database... ;
- gestionnaires de sites web (ou CMS) : Drupal (portails), WordPress (sites, blog), JaliOS, Joomla! (portails)... ;
- bibliothèques de langages de programmation : Framework .Net de Microsoft, ASP .Net de Microsoft, Visual C++ Runtime de Microsoft, Visual Studio Tools de Microsoft, machine virtuelle Java....
- fonctions logicielles spécifiques : serveur HTTP Apache pour site web, serveur DNS de noms de domaine, serveur LDAP d'annuaire, serveur DHCP d'adresses IP, serveur WSUS de mises à jour Windows...

## Virtualisation

Pour assurer une isolation entre applications ou pour garantir les performances d'une application particulière, chaque application peut demander à être installée sur un serveur hôte distinct. Avec les différents besoins, les serveurs hôtes se multiplient.

Plusieurs serveurs hôtes peuvent être regroupés ou « virtualisés » sur un seul serveur matériel bien dimensionné avec une couche logicielle de virtualisation (ex : VMWare, Hyper-V de Microsoft). Dans ce cas, les différents serveurs virtuels, bien qu'indépendants les uns des autres, se partagent les composants (processeur, mémoire, disques, accès réseau) du serveur matériel.



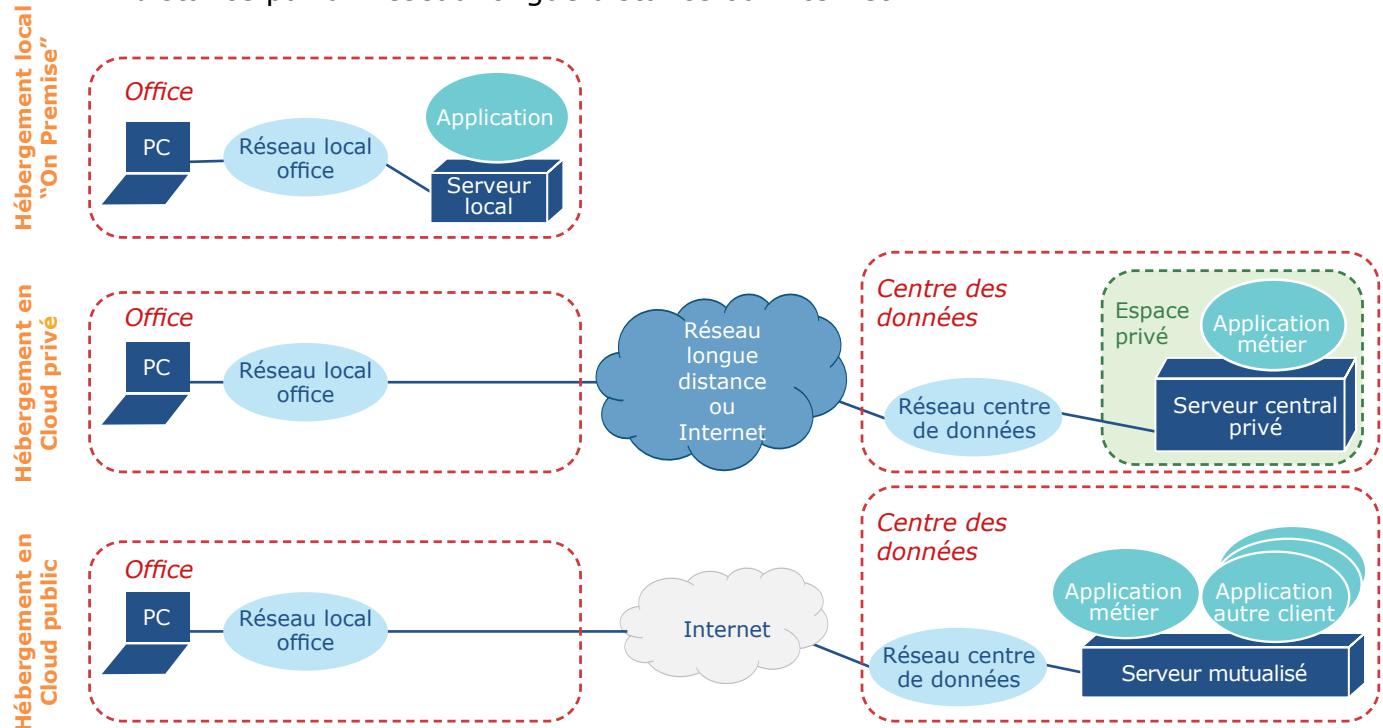
Lorsqu'un serveur hôte n'est pas utilisé, ses ressources processeur et mémoire peuvent être affectées à un autre serveur actif.

Les caractéristiques de chaque serveur hôte peuvent être modulées suivant les besoins. Chaque serveur hôte est accessible à distance séparément par son adresse IP de connexion au réseau.

# Installation

Les serveurs hôtes peuvent être :

- installés en local dans un office notarial (serveur « On Premise »),
- installés dans un espace privé d'un centre de données, appelé aussi « Cloud privé » (ex : Cloud privé de l'ADSN, Cloud d'entreprise, Cloud d'un éditeur de LRA),
- installé sur un serveur mutualisé entre différentes entreprises (« Cloud public »), mis à disposition par un fournisseur dans son centre de données et accessible à distance par un réseau longue distance ou Internet.

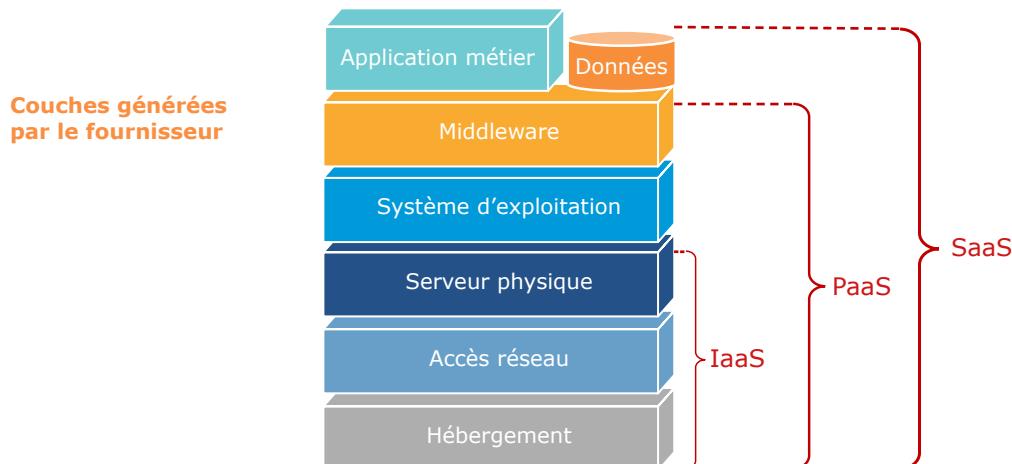


Les principaux fournisseurs internationaux de services Cloud publics sont : Microsoft avec Azure, Amazon avec Amazon Web Services (AWS), Google avec Google Cloud Platform, Oracle Infrastructure Cloud et IBM Public Cloud.

## Modes Cloud

Le terme « Cloud » vient du fait que la ressource utilisée n'est pas directement visible par l'utilisateur mais cachée derrière un nuage, représentation traditionnelle d'un réseau en informatique.

En mode Cloud, le fournisseur peut gérer plus ou moins de niveaux selon le mode choisi (IaaS, PaaS, SaaS). Un site de paramétrage accessible à distance permet au client de configurer l'environnement technique selon ses besoins.



## 6.2 Les éléments structurants

Il existe deux formats matériels pour un serveur matériel :

- le format rack pour être installé dans une baie informatique,
- le format tour pour être posé sur un bureau ou une table.

L'épaisseur des éléments destinés à être mis dans une baie se mesure en U où 1U = 1,44 pouce. La hauteur d'une baie classique est de 42U (Unit). Un serveur extra-plat a une hauteur de 1U.

Les processeurs des serveurs sont soit de la gamme Xeon chez Intel, soit Epyc chez AMD avec un nombre plus ou moins important de cœurs (« Core ») et de mémoire cache intégrée, suivant la performance attendue.

Le dimensionnement d'un serveur hôte dépend de l'usage et du nombre d'utilisateurs auxquels il est destiné.

En mode Cloud public, les ressources sont activables très facilement et la facturation de l'utilisation d'une ressource (serveur, espace disque, base de données, middleware...) est généralement à l'usage et mensuelle. Il faut alors veiller à dimensionner ses ressources en fonction de ses besoins exacts sinon les coûts peuvent rapidement exploser au fil du temps et par l'accumulation de coûts divers.

→ Les différents logiciels installés sur un serveur hôte doivent être mis à jour régulièrement, en particulier pour bénéficier des corrections de dysfonctionnements ou des failles de sécurité. La mise à jour d'un logiciel de base, comme le système d'exploitation, peut nécessiter la mise à jour des logiciels de niveau supérieur qui l'utilisent pour respecter la compatibilité des versions logicielles.

## 6.3 Les particularités pour les notaires

Les serveurs hôtes contenant des données de l'office et des clients, leur sécurisation est très importante (cf. chapitre « La sécurité informatique »).

De plus en plus d'applications métier sont disponibles en mode Cloud. Cette approche apporte différents avantages : bénéficier d'applications immédiatement disponibles avec un faible coût de mise en œuvre, éviter d'avoir à gérer un serveur matériel dans l'office (configuration, sauvegardes, sécurité) et ses mises à jour logicielles.

Les données étant gérées en dehors de l'office, la sécurité de l'application et la confidentialité des données doivent être garanties par le fournisseur au travers d'un contrat et contrôlés régulièrement par des audits.

Quel que soit le mode d'installation d'une application métier sur un serveur (en local, dans le Cloud privé, dans le Cloud en mode Iaas, Paas ou Saas), les données métier « appartiennent » à l'office notarial qui utilise l'application. L'office en est responsable vis-à-vis de ses propres clients. Il faut s'assurer, par contrat, que le prestataire en charge de l'application métier assurera la réversibilité complète des données en fin de contrat afin que l'office puisse récupérer et réutiliser toutes les données métier, actuelles et historiques ; le prestataire ne devant conserver aucune donnée.

## 6.4 Les bonnes pratiques

Les serveurs matériels portant en général des services et applications vitaux pour le bon fonctionnement de l'office, ils doivent être :

- installés dans un local technique, physiquement clos et bien ventilé, a minima une baie électrique fermée à clé et idéalement une salle technique climatisée et protégée contre l'incendie,

- alimentés par une double arrivée électrique,
- protégés contre les surtensions électriques par un onduleur,
- configurés pour s'éteindre automatiquement et proprement en cas de coupure électrique de longue durée,
- sauvegardés tous les jours sur un support externe à l'office pour permettre une restauration même en cas de destruction de l'office et des serveurs par incendie,
- protégés par un antivirus à jour,
- protégés par des mots de passe robustes et changés régulièrement,
- mis à jour régulièrement.

Microsoft diffuse le cycle de vie de chacun de ses produits pour serveurs, c'est-à-dire la période pendant laquelle chaque produit bénéficie de mises à jour et d'un support technique (cf. le site internet : <https://docs.microsoft.com/fr-fr/lifecycle/>).

 Au 01/07/2021, les seules versions de Microsoft Windows Server qui devraient être utilisées sur les serveurs hôtes sont les versions postérieures ou égales à Windows Server 2012 qui bénéficient d'un support étendu jusqu'en 2023. Les versions de Microsoft SQL Server supportées sont celles postérieures ou égales à SQL Server 2012.

La mise à jour des versions des logiciels d'un serveur hôte doit être faite régulièrement.

Cependant, cette opération doit être abordée comme un véritable projet pour anticiper les dépendances de versions et les impacts (besoins de formation des utilisateurs sur les nouvelles fonctionnalités...), garantir une protection des données et permettre un éventuel retour arrière en cas de dysfonctionnement ou de blocage.

## 6.5 Les principales solutions du marché

Les principales marques professionnelles de serveurs matériels sont Dell, HPE et Lenovo.

## 6.6 Les critères de choix

En général, la configuration technique est préconisée dans les prérequis techniques fournis par l'éditeur de l'application à installer.

L'utilisation d'un serveur ou d'une application en mode Cloud permet de s'affranchir de l'installation et de la gestion d'un serveur hôte dans l'office (changement de version majeure, application des correctifs logiciels, sauvegarde des données, opérations de maintenance...).

 Les données hébergées sur des solutions Cloud de sociétés américaines, que ce soit aux USA ou en Europe, sont soumises au « Cloud Act » des USA qui permet à la justice américaine de solliciter la communication des données sans que leur propriétaire en soit informé. Un chiffrement des données est donc à minima requis pour préserver la confidentialité des données et le respect du RGPD.

## Le vocabulaire

**Administration technique**: action de réaliser l'ensemble des tâches techniques de configuration et éventuellement d'exploitation informatique d'un système.

**Base de données (Database)**: collection organisée de données qui est gérée par un Système de Gestion de Base de Données.

**Cloud**: configuration où l'ensemble de serveurs et services peut être utilisé par les utilisateurs à distance depuis n'importe où.

**CMS (Content Management System)**: famille de logiciels qui ont pour buts de créer, gérer et publier facilement des sites internet/intranet (site web, portail, blog, site marchand...) sans programmation.

**Core (Cœur ou noyau)**: microprocesseur autonome au sein d'un processeur. L'assemblage de plusieurs Core permet de paralléliser les traitements pour améliorer la puissance de calcul.

**Datacenter (centre de données ou centre d'hébergement)**: lieu physique protégé, privé ou partagé, où sont installés les équipements informatiques (serveurs physiques, espaces de stockage, équipements réseau...).

**DHCP (Dynamic Host Configuration Protocol)**: fonction logicielle qui distribue les adresses IP sur un réseau local.

**Exploitation informatique**: action de réaliser l'ensemble des tâches techniques et procédures à effectuer régulièrement pour maintenir un système en conditions opérationnelles. Les tâches sont décrites dans la Documentation d'Exploitation.

**Hébergement**: mise à disposition d'espace dans un c, pour installer des serveurs physiques, ou d'un serveur physique pour installer des applications, des sites internet....

**IaaS (Infrastructure as a Service)**: location d'un serveur et d'espace de stockage auprès d'un fournisseur de service Cloud. Les serveurs et les logiciels techniques doivent être entièrement gérés par le client (paramétrage et mises à jour).

**PaaS (Platform as a Service)**: location d'un serveur, d'espace de stockage et de logiciels techniques auprès d'un fournisseur de service Cloud. Les serveurs et les logiciels techniques sont gérés et maintenus par le fournisseur. Le client s'occupe seulement de leur configuration logicielle et de la gestion de l'application métier.

**Patch (correctif logiciel)**: modification circonscrite du code d'un logiciel pour corriger un dysfonctionnement ou une faille de sécurité.

**RAID (Redundant Array of Independent Disks)**: technique de configuration d'un groupe de disques durs pour augmenter la tolérance aux pannes d'un disque. Les principales sont: Raid 1 = Disques en miroir pour des écritures en parallèle / Raid 5 et 6 = Ajout d'une donnée de parité permettant de reconstituer une donnée manquante.

**Réversibilité**: démarche permettant de garantir à une société utilisatrice d'une application ou d'un service de récupérer ses données et leur exploitation à son profit ou celui d'un tiers désigné lors de la fin du contrat d'utilisation, quelle qu'en soit la cause.

**SaaS (Software as a Service)**: location d'un service ou d'une application métier sur un serveur partagé. Les serveurs, les logiciels techniques et l'application métier sont gérés par le fournisseur. L'utilisateur accède seulement à un espace cloisonné sur un environnement mutualisé.

**Serveur**: peut désigner soit un ordinateur quand il s'agit d'un serveur physique, soit une fonction logicielle quand il s'agit d'une application accessible à distance.

**SGBD (Système de Gestion de Base de Données)**: logiciel technique spécifique servant à stocker et manipuler des données dans une base de données à l'aide d'un langage qui masque la complexité des opérations.

**Supervision**: surveillance régulière du bon fonctionnement d'un système afin de détecter des anomalies rapidement.

**VM (Virtual Machine)**: environnement virtuel créé par un logiciel spécifique qui simule le fonctionnement d'un serveur physique isolé. En général, plusieurs VM sont configurées sur un seul serveur physique et se partagent ses ressources matérielles (processeurs, mémoire, disques, réseau). Les VM sont gérées par un hyperviseur.

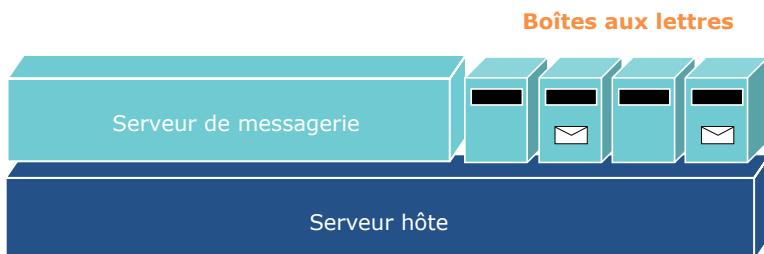
# 7. La messagerie électronique

## 7.1 Les concepts de base

La messagerie est une application qui permet l'envoi, la consultation et la gestion de messages électroniques (« courriels » ou « emails »).

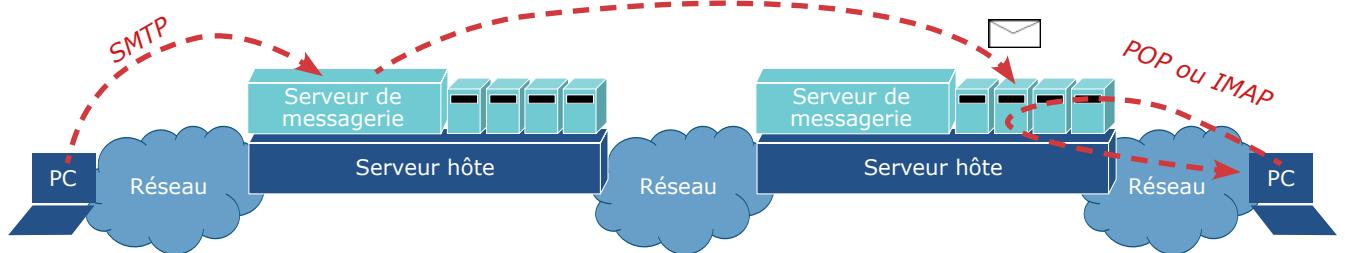
La messagerie est une application qui fonctionne selon un principe client-serveur.

Le serveur de messagerie stocke les messages reçus dans des boîtes aux lettres dans l'attente de leur lecture ou de leur téléchargement sur un poste utilisateur.



La récupération des messages reçus dans une boîte aux lettres se fait par connexion au serveur de messagerie avec l'identifiant et le mot de passe associés à la boîte aux lettres.

Les différents systèmes de messagerie respectent des protocoles d'interconnexion standard et sont interconnectés entre eux.



Un serveur de messagerie fournit en général deux points d'accès :

- un point d'accès au protocole SMTP pour envoyer les messages,
- un point d'accès au protocole POP ou IMAP pour récupérer les messages reçus.

## Logiciels serveurs

Un serveur de messagerie est un logiciel spécifique proposé par différents éditeurs qui peut être installé sur un serveur hôte local ou sur un serveur hôte dans le Cloud.

Chez Microsoft, pour les usages professionnels, le serveur de messagerie est soit le logiciel Exchange pour une installation sur un serveur, soit Microsoft 365 en version Cloud SaaS.

Les messageries gratuites sur Internet telles que Google Gmail, Microsoft Hotmail, Mail Orange, Yahoo mail, etc., sont installées en mode Cloud (SaaS) et proposent un accès via un navigateur Internet.

## **Logiciels clients**

Le client de messagerie peut être soit une page web accessible avec un navigateur Internet (client léger ou « webmail »), soit un logiciel installé sur un ordinateur personnel (client lourd) ou un smartphone.

Les messageries gratuites sur Internet utilisent par défaut un client léger accessible dans un navigateur Internet. Elles peuvent aussi mettre à disposition une application cliente pour consultation sur un smartphone.

Les logiciels de messagerie Microsoft Outlook, Mozilla Thunderbird sont des clients lourds. Ils peuvent être utilisés avec n'importe quelle messagerie en paramétrant le compte de messagerie et les points d'accès POP/IMAP et SMTP du serveur de messagerie.

Lorsque l'utilisateur accède à ses messages avec un client lourd, les messages sont en général téléchargés sur son ordinateur dans une boîte aux lettres locale ; ce qui permet une consultation ultérieure et une préparation des réponses même sans connexion au serveur de messagerie.

## **Adresse de messagerie**

L'adresse d'un correspondant pour lui envoyer un message est de la forme destinataire@domaine. Par exemple : germaine.michu@notaires.fr.

Le format des noms des destinataires est libre. Les majuscules sont traitées comme les minuscules. Les accents, certains caractères spéciaux et les espaces ne sont pas autorisés.

La convention de nommage est en général définie par l'administrateur du domaine de messagerie afin d'éviter les homonymies. Pour une personne dénommée Germaine MICHU qui est externe à une organisation, les usages sont : germaine.michu@domaine, gmichu@domaine, gemichu@domaine, germaine.michu.externe@domaine.

## **Nom de domaine**

Le nom de domaine est un système de nommage, permanent et lisible, des ressources sur Internet basé sur une organisation hiérarchique.

Un nom de domaine est constitué d'une suite de noms, d'au plus 253 caractères, séparés par des points et se décompose de droite à gauche : serveur.sous-domaine.domaine-principal.extension. Exemples : www.notaires.fr, servmess.notaires.fr, micen.real.notaires.fr, www.paris.notaires.fr, test.paris.notaires.fr.

En s'appuyant sur les serveurs de noms de domaine (DNS ou « Domain Name System ») qui tiennent à jour la correspondance entre un nom de domaine et une adresse IP, un mécanisme permet de retrouver, à partir du nom de domaine, l'adresse IP qui indique la localisation d'un serveur.

Le nom de domaine permet de trouver le serveur de messagerie qui gère la boîte aux lettres d'un correspondant. Cette relation est paramétrée dans les serveurs de noms de domaine via un paramètre spécifique appelé MX (« Mail eXchanger »).

## **Courrier indésirable**

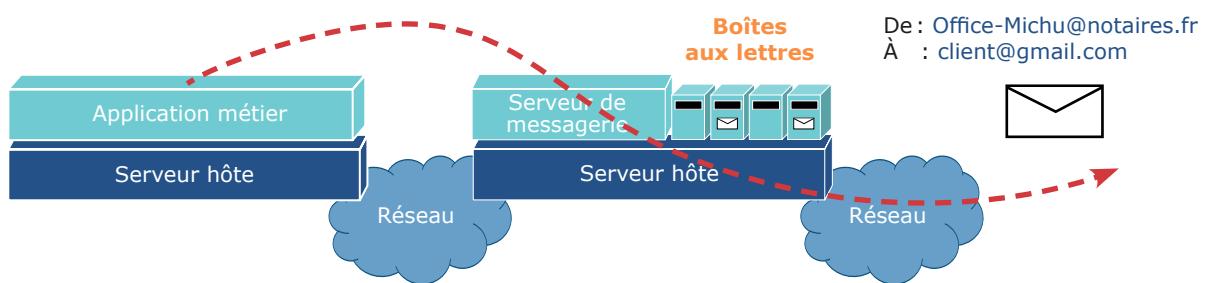
Afin d'éviter de recevoir une multitude de messages indésirables (ou « spam » en anglais), un filtre anti-spam peut être installé en amont ou dans le serveur de

messagerie. Les messages considérés comme indésirables sont alors soit bloqués par le filtre anti-spam, soit classés dans un dossier « Courrier indésirable ».

Lorsqu'un serveur de messagerie émet trop de messages (campagnes marketing d'envoi de messages) ou des messages considérés comme indésirables par une majorité d'utilisateurs, le serveur de messagerie émetteur peut être mis en liste noire (« Black-listé ») par les autres serveurs, notamment les grands serveurs de messagerie comme Gmail, Outlook ou Yahoo. Dans ce cas, tous les messages émis par ce serveur seront refusés par les autres serveurs. Le gestionnaire du serveur doit alors engager une procédure auprès de ces serveurs pour se faire retirer de la liste noire.

## Utilisation par les applications métier

Le point d'accès SMTP permet à des applications métier autorisées d'émettre des messages avec le nom de domaine du serveur. Par exemple, un Logiciel de Rédaction d'Actes va vouloir utiliser le serveur de messagerie des notaires pour émettre automatiquement un message, au nom de l'office, vers des clients.



## 7.2 Les éléments structurants

La taille d'une boîte aux lettres d'un utilisateur est limitée ; par exemple, entre 2 Go et 100 Go avec Microsoft Exchange Online.

- La taille d'un message envoyé, y compris ses pièces jointes, est limitée par le serveur de messagerie ; en général environ 20Mo.

Un message indique par défaut comme émetteur le nom de la boîte aux lettres à partir duquel il a été envoyé. Ceci peut néanmoins être modifié par l'émetteur.

Le courrier reçu sur une boîte aux lettres peut être redirigé automatiquement vers une ou plusieurs autres boîtes aux lettres.

Il ne peut y avoir qu'un serveur de messagerie gestionnaire par domaine de messagerie.

## 7.3 Les particularités pour les notaires

Les messageries sur Internet, telles que Google Gmail, Microsoft Hotmail, Yahoo Mail, ne sont pas compatibles avec la garantie de confidentialité imposée par les pratiques notariales. Leur usage doit être limité à des cas précis. Par exemple, lors de l'installation d'un notaire, pour permettre la création d'un compte ID.Not en attendant la création d'une adresse en « notaires.fr ».

Le principal domaine de messagerie du notariat français est « notaires.fr ». Les notaires et les collaborateurs qui dépendent de la Chambre de Paris sont gérés dans le domaine de messagerie « paris.notaires.fr ».

Les règles à respecter pour le nommage des adresses des notaires, des collaborateurs, des offices et des instances ont été définies par le CSN, conformément à l'article 4.2.2. du Règlement National, dans un document appelé « Plan de nommage du domaine notaires.fr ».

Le serveur de messagerie qui prend en charge environ 70.000 boîtes aux lettres « xxx@notaires.fr » est géré par l'ADSN. Jusqu'à présent, il reposait sur une solution propriétaire fournie par Orange. En 2021, une migration va transférer toutes les boîtes aux lettres sur une solution Exchange Online, la messagerie en mode Cloud (SaaS) de l'offre Microsoft 365.

Le serveur de messagerie du domaine « paris.notaires.fr » est géré par la Chambre des Notaires de Paris. La gestion des adresses de messagerie des collaborateurs et des services de l'office se fait via le portail « Intranotaires ».

Pour installer un serveur de messagerie indépendant des serveurs qui gèrent les messageries des domaines « notaires.fr » et « paris.notaires.fr », il faut créer un sous-domaine, tel que « monoffice.notaires.fr ». La création de ce sous-domaine doit être validée par l'ADSN et doit obtenir l'agrément de la Chambre, conformément au Règlement National.

L'ajout d'applications autorisées à émettre des messages auprès du serveur de messagerie du domaine « notaires.fr » doit être demandé auprès de l'ADSN.

## 7.4 Les bonnes pratiques

### Usages personnels

La messagerie électronique et les boîtes aux lettres professionnelles sont des outils professionnels.

L'utilisation de l'adresse de messagerie professionnelle pour des usages personnels, telles que l'achat sur des sites de vente en ligne ou la communication avec l'école, est fortement déconseillée.

La messagerie professionnelle peut être utilisée pour envoyer ou recevoir des messages personnels, dans la mesure du raisonnable, si les messages sont marqués « PERSONNEL » dans le titre et sont classés dans un répertoire marqué « PERSONNEL ».

- La redirection du courrier reçu dans une boîte aux lettres professionnelle vers une boîte aux lettres grand public est interdite car elle est contraire aux règles de confidentialité et elle peut servir de moyen délictueux pour exfiltrer des informations en préparation d'une attaque informatique ou d'une « fraude au Président ».

### Messagerie nominative

Il est interdit d'envoyer un message avec le compte de messagerie d'une personne physique tierce identifiée comme émetteur. Il s'agirait alors d'usurpation d'identité.

- Une adresse de messagerie attribuée à une personne physique est en général désignée par le nom de cette personne. En cas de départ, de mutation, de décès, etc. de cette personne, tout message envoyé sur l'adresse personnelle doit être retourné automatiquement à l'expéditeur avec un message indiquant l'adresse de messagerie de son successeur dans la fonction. L'adresse de messagerie nominative initiale ne doit plus être utilisable au bout de 1 mois.

Pour des usages partagés entre collaborateurs ou pour assurer la persistance d'une adresse de messagerie malgré le départ des collaborateurs, il est recommandé de créer une adresse de messagerie générique non nominative liée à l'office. Par exemple : comptabilité.62520@notaires.fr

Au cas où plusieurs postes de travail souhaiteraient relever le courrier dans une boîte aux lettres à partir d'un client lourd de messagerie, il est recommandé d'utiliser le protocole IMAP afin que tous les utilisateurs voient l'activité partagée dans la boîte aux lettres.

## Utilisation comme identifiant

L'adresse de messagerie personnelle est souvent utilisée comme identifiant par les applications car :

- c'est un identifiant unique et facile à retenir,
- c'est un identifiant personnel,
- cela permet de vérifier que l'utilisateur est réel par l'envoi d'un lien à cliquer dans un message envoyé à l'adresse de messagerie indiquée.

Les applications qui utilisent l'adresse de messagerie comme identifiant de connexion étant différentes du serveur de messagerie, il faut veiller à ne pas utiliser le même mot de passe pour ces applications que celui utilisé pour accéder à sa boîte aux lettres personnelle.

→ De manière générale, si l'identifiant de connexion peut toujours être l'adresse de messagerie, les mots de passe doivent être différents pour chaque usage. À défaut, cela facilite l'usurpation d'identité en cas de compromission de l'identifiant et du mot de passe sur un des sites.

## Confidentialité

la liste de diffusion, lors de l'envoi du message, il faut mettre la liste de diffusion cible dans le champ « Cci » (« Copie Carbone Invisible ») et le nom de l'émetteur comme destinataire afin de faciliter les réponses.

Les messages stockés dans les boîtes aux lettres du serveur de messagerie sont consultables par les administrateurs de la messagerie. Il faut donc veiller à ne pas envoyer d'information confidentielle en clair dans un message.

Les messages confidentiels doivent être envoyés dans des documents Microsoft Office protégés par un mot de passe et le mot de passe doit être communiqué séparément. Ces messages peuvent également être envoyés via la plateforme d'échange de la CINP.

## Fausse identité

→ L'envoi de messages trafiqués ou l'utilisation d'un nom de domaine d'émetteur proche d'un nom connu sont des techniques utilisées dans le Phishing pour récupérer des données personnelles confidentielles ou les « fraudes au Président » qui utilisent l'ingénierie sociale pour demander des virements indus sur un compte à l'étranger. Par exemple : michu@paris-notaires.fr au lieu de michu@paris.notaires.fr.  
Il faut donc se méfier des demandes inhabituelles faites par message électronique.

Certains serveurs de messagerie acceptent de recevoir des messages à émettre, via le protocole SMTP, à partir d'applications non connues. L'émetteur du message est alors vu comme faisant partie du domaine du serveur ; ce qui lui apporte à tort de la crédibilité. Le nom du domaine n'est donc pas une garantie totale sur l'identité de l'émetteur.

## 7.5 Les principales solutions du marché

Suivant qu'ils dépendent de la Chambre des Notaires de Paris ou non, les notaires devront s'adresser à l'ADSN ou à la Paris Notaires Services ou des fournisseurs spécialisés.

Des services complémentaires liés à la messagerie électronique peuvent également être proposés : agenda partagé, archivage des messages électroniques (cf. NotmailArchives de Paris Notaires Services), etc.

## 7.6 Les critères de choix

La messagerie un des fondements de la communication et de la visibilité d'un office.

- ➡ Le choix de format des adresses de messagerie doit se faire en accord avec le « Plan de nommage du domaine notaires.fr » pour éviter les confusions.

### Le vocabulaire

**Adresse de messagerie**: adresse de la forme nom@domaine et attribuée à une boîte aux lettres d'un système de messagerie.

**Boîte aux lettres (Mailbox)**: espace de stockage des messages reçus par une adresse de messagerie particulière.

**DNS (Domain Name System)** : Service distribué sur Internet pour traduire un nom de domaine en une adresse IP qui localise physiquement un serveur.

**Email (Electronic Mail)** : message électronique ou courriel.

**Hameçonnage (ou Phishing)**: technique basée sur l'usurpation d'identité de l'émetteur ou d'un site Internet pour soutirer des renseignements personnels ou cliquer sur un lien corrompu.

**IMAP (Internet Message Access Protocol)**: protocole de récupération des messages sur un serveur avec lequel les messages sont simplement synchronisés entre le client et le serveur.

**Liste de diffusion**: liste qui contient plusieurs adresses de messagerie permettant l'envoi simultané du même message à plusieurs correspondants.

**Nom de domaine**: système de nommage des ressources sur Internet basé sur une organisation hiérarchique.

**POP (Post Office Protocol)**: protocole de récupération des messages sur un serveur avec lequel les messages sont par défaut effacés du serveur après récupération.

**SMTP (Simple Mail Transfer Protocol)**: protocole pour l'envoi de messages sur un serveur de messagerie.

**Spam**: courrier électronique indésirable telle qu'une publicité envoyée en masse.

# 8. La visioconférence

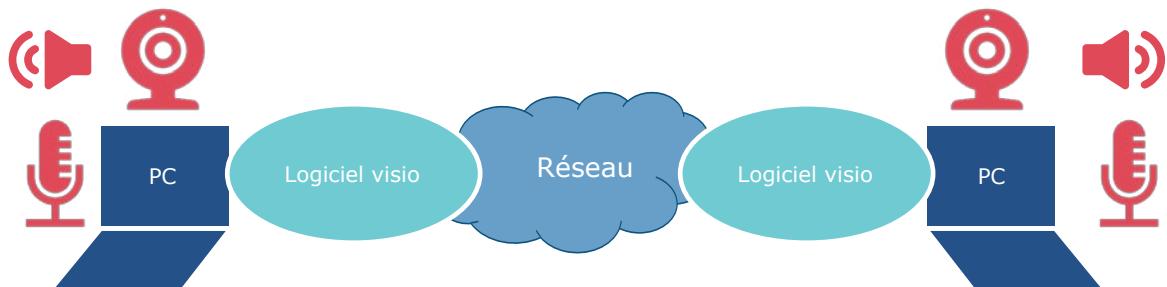
## 8.1 Les concepts de base

La visioconférence (ou vidéo-conférence) est un service qui permet de dialoguer, de se voir en direct et de partager des documents entre deux ou plusieurs interlocuteurs.

### Équipement nécessaire

La visioconférence nécessite pour chaque interlocuteur : un équipement informatique, tel qu'un ordinateur personnel ou un matériel spécifique, doté de :

- une caméra vidéo (« webcam »),
- un microphone,
- des haut-parleurs,
- une connexion réseau,
- d'un logiciel de visioconférence.



Il est nécessaire que tous les participants disposent du même logiciel de visioconférence, sauf si les logiciels sont compatibles entre eux.

Sur un ordinateur personnel, le logiciel de visioconférence est en général une application (client lourd) installée localement.

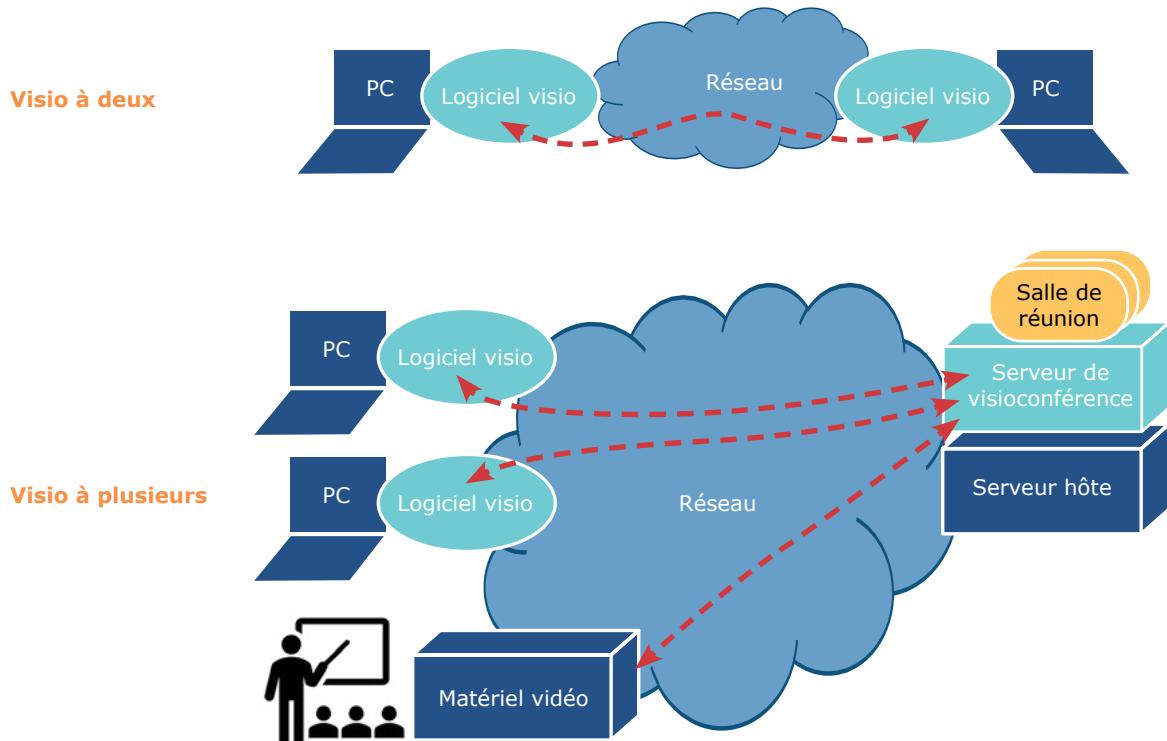
Pour réaliser une visioconférence ponctuellement avec un interlocuteur uniquement équipé d'un ordinateur personnel, comme un client ou un prestataire, à défaut d'utiliser une solution grand public, il faut lui envoyer une invitation avec un lien vers le logiciel de visioconférence à installer ou à lancer localement.

Il est possible d'équiper une salle de réunion avec un équipement spécifique à demeure : caméra pilotable à distance avec champ de vision large et détection de l'intervenant, pieuvre audio haute sensibilité à disposer au milieu de la salle.

### Fonctionnement

À deux participants, il est possible de faire une visioconférence de poste à poste. Pour se retrouver, un participant appelle l'autre avec son adresse dans le système de visioconférence (identifiant spécifique, numéro de téléphone...).

S'il y a plus de deux participants, il est nécessaire que tous les participants se connectent sur un serveur central qui va relayer les échanges aux autres participants.



Pour se retrouver, un participant réserve une salle de réunion virtuelle sur le serveur puis partage son code et un éventuel mot de passe avec les autres participants. à la date convenue, tous les participants se connectent sur le serveur de visioconférence en indiquant le code de la salle de réunion virtuelle.

## Logiciels

Il existe de multiples solutions de visioconférence :

- Zoom, Apple FaceTime, Google Duo, WhatsApp, Signal, Microsoft Skype qui sont logicielles et plutôt orientées grand public, voire seulement disponibles sur smartphone,
- LifeSize, Microsoft Teams, Google Hangouts, Tixeo, Cisco Webex, Polycom qui sont logicielles ou matérielles et plutôt orientées monde professionnel.

La plupart des solutions proposent une application à installer sur smartphone.

## Codec

La vidéo est un media lourd. De plus, le son et l'image doivent être transmis simultanément et le son doit être transmis rapidement afin que les échanges soient confortables.

Pour réduire le flux vidéo et optimiser la qualité des échanges, il est nécessaire de le compresser à la source et de le décompresser à destination. C'est le rôle d'un codec.

Ce codec est intégré dans le logiciel installé sur un ordinateur. Il est matériel ou logiciel dans les équipements de visioconférence des salles de réunion.

## Confidentialité

Comme tout flux de données qui est véhiculé sur un réseau, le flux des échanges vidéo peut être intercepté par un tiers qui aurait accès au flux.

Pour éviter cela, le flux vidéo est souvent chiffré par un codec spécifique.

## Autres fonctionnalités

Les solutions de visioconférence intègrent en général les fonctions suivantes :

- le partage d'écran à partir d'un ordinateur personnel,
- l'envoi de messages textes (« Chat » en anglais) à partir d'un ordinateur personnel.

Le partage d'écran permet de choisir une fenêtre particulière ou la totalité de l'écran.

## 8.2 Les éléments structurants

La qualité de la vidéo captée dépend de l'éclairage des participants, du débit du réseau et des caractéristiques de la caméra :

- sa résolution, c'est-à-dire la taille de l'image générée, doit être d'au moins 720 pixels/pouce,
- sa fréquence de capture des images, doit être d'au moins 25 images/secondes.

Le débit du réseau entre les participants est déterminant pour la qualité des échanges.

 Plus la qualité de la vidéo captée est importante, plus le flux vidéo est lourd et plus le débit du réseau doit être important.

Le nombre maximum de participants à une même réunion dépend de la solution logicielle :

- 1000 participants annoncés par Zoom,
- 300 participants, voire bientôt 1000, annoncés pour Microsoft Teams,
- 100 participants garantis en visioconférence avec la solution LifeSize, si la salle de réunion virtuelle a été ouverte par un notaire client de Adnov,
- 50 participants garantis avec la solution LifeSize, si la salle de réunion virtuelle a été ouverte par un notaire client de Comnot,
- 20 garantis pour la solution sécurisée Tixeo.

## 8.3 Les particularités pour les notaires

Toutes les offres d'accès réseau agréées par le CSN supportent l'ensemble des offres de visioconférence agréées par le CSN. Les unes sont indépendantes des autres.

Pour réaliser des Actes Authentiques Electroniques à Distance (AAED) et bénéficier du partage d'émolument entre notaires, ou pour réaliser des Procurations Authentiques avec Comparution à Distance, il est impératif d'utiliser une solution de visioconférence qui est agréée par le CSN et qui assure la confidentialité des échanges, notamment par :

- un chiffrement des flux vidéo de bout en bout, qui va coder les données afin de les rendre inutilisables par des tiers,
- une absence d'enregistrement des échanges (vidéo ou autres).

Le Logiciel de Rédaction d'Actes et l'application de visioconférence sont indépendants et n'ont besoin d'aucun lien technique. Les tablettes de signature électronique des actes ne sont pas liées à la visioconférence.

Dans le cadre d'un AAED, tous les participants peuvent lire le projet d'acte sur leur écran avec la fonctionnalité de partage d'écran fournie par défaut par la visioconférence. Pour cela, le notaire instrumentaire doit seulement ouvrir l'acte avec le Logiciel de Rédaction d'Actes sur son poste puis partager son écran avec la fonctionnalité de partage d'écran de la visioconférence, comme il peut le faire avec n'importe quel autre logiciel lancé sur son ordinateur. La signature d'un AAED utilise les fonctions du portail collaboratif SignActe du MICEN.

L'usage de Microsoft Teams et des autres solutions de visioconférence grand public doit être réservé à des usages professionnels, hors AAED et Procurations Authentique avec

Comparution à Distance, en gardant à l'esprit que la confidentialité des échanges n'est pas assurée.

Attention à la solution Teams de Microsoft qui est un portail, qui regroupe environ 40 outils de Microsoft dont la visioconférence, le Chat, le partage de documents, les sondages, les tableaux blancs, la transcription écrite en direct des échanges oraux, etc., et qui garde la trace des échanges une fois la session terminée, contrairement aux exigences de confidentialité du notariat.

## 8.4 Les bonnes pratiques

Pour les salles de réunion, les avantages du matériel de visioconférence dédié par rapport à un ordinateur sont les suivants: le matériel n'est pas sensible aux montées de version régulières de Windows ou aux déconfigurations régulières par les utilisateurs, le traitement du son est de meilleure qualité, la caméra vidéo peut être adaptée à la taille de la salle et peut suivre automatiquement la personne qui parle.

Si plusieurs salles de réunion de l'office sont équipées avec un équipement dédié, chaque session peut consommer jusqu'à 1Mb/s. Il faut donc veiller à ce que l'accès réseau de l'office fournisse un débit important ; au risque sinon, qu'une session de visioconférence ne nuise à la qualité de l'autre.

## 8.5 Les principales solutions du marché

→ À la date du 01/07/2021, les partenaires agréés par le CSN pour délivrer une solution de visioconférence sont :

- Adnov avec son offre VisioAct basée sur la solution LifeSize,
- Comnot avec son offre VisioNot basée sur la solution LifeSize.

Cette liste peut évoluer dans le temps et sa version à jour est diffusée sur le portail REAL.

## 8.6 Les critères de choix

→ Pour la réalisation d'Actes Authentiques Electroniques à Distance et de Procurations Authentiques avec Comparution à Distance, le choix d'une visioconférence agréée par le CSN est un impératif.

Les solutions de visioconférence non agréées peuvent répondre aux besoins professionnels usuels.

L'installation d'un équipement dédié dans au moins une salle de réunion de l'office permet de réaliser des AAED dans de bonnes conditions pour tous les participants.

L'utilisation d'un écran haute définition n'a de sens que si les caméras qui captent les flux vidéos sont également en haute résolution de part et d'autre.

La taille de l'écran dédié doit être choisie en fonction de la taille de la salle équipée. La distance idéale pour regarder un écran avec une définition Full HD est d'environ 2,6 fois la taille de sa diagonale (1,3 fois pour un écran Ultra HD 4K car les pixels sont plus petits).

L'installation et la mise en service du matériel dédié peuvent être réalisées par le prestataire.

Le support à distance (Helpdesk) et la maintenance technique doivent être proposés par le prestataire.

## Le vocabulaire

**Chat (« tchat » en français)** : outil de messagerie instantanée permettant l'échange de messages ou de documents en temps réel dans un groupe (bavardage).

**Codec (ou Codeur-Décodeur)** : dispositif matériel ou logiciel pour optimiser la transmission d'un flux de données numériques en appliquant de la compression ou du chiffrement des données.

**Définition d'une image** : nombre de pixels dans l'image.

**Full HD** : définition d'écran de 1080 lignes et 1920 pixels par ligne.

**HD** : définition d'écran de 720 lignes et 1280 pixels par ligne.

**Pixel (de « Picture Element » en anglais)** : plus petit élément d'une image électronique.

**Pouce (« Inch » en anglais)** : unité de mesure anglo-saxonne qui équivaut à 2,54 cm. Un écran de 65 pouces mesure 165 cm de diagonale (hors contour).

**Résolution** : nombre de pixels par pouce (ppp ou « ppi » / « pixel per inch » pour un écran ou « dpi » / « dot per inch » pour une impression). Pour une surface donnée, plus la résolution est élevée, plus l'image est précise car plus les pixels sont petits et plus il est possible de zoomer dans l'image.

**Ultra HD 4K** : définition d'écran de 2160 lignes et 4096 pixels par ligne.

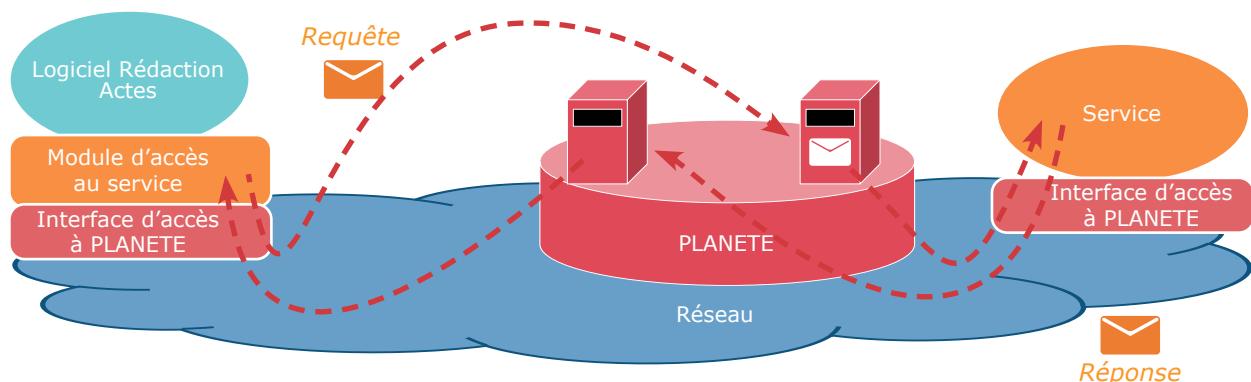
# 9. PLANETE

## 9.1 Les concepts de base

PLANETE (« PLAtorme Notariale d'Echanges par TElétransmission ») est une solution informatique propre au notariat français qui sert à véhiculer des messages selon un principe standardisé entre différentes applications.

La solution PLANETE a un rôle de « poste restante centrale » : par des interfaces (API) mises à sa disposition, une application peut déposer des messages pour un destinataire identifié et elle vient régulièrement récupérer les messages qui ont été déposés à son intention.

Les messages véhiculés contiennent soit des requêtes, soit les réponses aux requêtes. Ces requêtes sont mises à disposition par PLANETE auprès de l'application ou du service adéquat qui se charge d'apporter une réponse.



### Émetteurs – Destinataires

La grande majorité des messages de requête est émise par les Logiciels de Rédaction d'Actes et les logiciels de comptabilité des notaires. Des applications centrales du notariat ou de partenaires accrédités peuvent aussi émettre des requêtes.

Ces messages de requête permettent de réaliser les formalités préalables, telles que des interrogations ou déclarations, et les formalités postérieures à l'acte, telles que la télépublication.

Les destinataires des requêtes qui renvoient les réponses sont :

- les services de l'État :
  - le service Téléactes de la Publicité Foncière de la DGFIP pour la réquisition des états hypothécaires (téléréquisition) et la publication des actes assujettis à publicité foncière (télépublication),
  - le service ANF (Accès des Notaires au Fichier immobilier) pour l'accès direct à la base immobilière et aux données hypothécaires de la DGFIP,
  - les Tiers De TElétransmission (TDT) de la DGFIP,
  - le service du Casier Judiciaire pour l'interrogation du bulletin n°2,
  - le service central de l'État Civil pour récupérer des données d'état civil pour un acte de naissance, de mariage ou de décès à l'étranger ;
  - l'Agence Nationale des Titres Sécurisés (ANTS) pour communiquer avec les communes sur l'état civil des personnes physiques pour un acte de naissance, de mariage ou de décès en France ;
  - les Sociétés d'Aménagement Foncier et d'Établissement Rural (SAFER) pour les Déclarations d'Intention d'Aliéner des biens ruraux ;

- les applications du notariat :
  - le FICEN-ECO pour la remontée des Déclarations d'Activité Professionnelle issues des comptabilités notariales,
  - la Base de Références Immobilières (BRI), pour le dépôt des avant-contrats et actes de vente immobilière à des fins statistiques.

## Contenu des messages

À chaque type de requête ou de réponse contenu dans un message, un format de données associées est défini.

Les types de requête acceptés, leur signification, les réponses possibles et le format des données associées sont définis par le service destinataire.

Par exemple, pour le service Télé@ctes de la Publicité Foncière, les requêtes peuvent être de type : publication, acte de vente, réquisition, régularisation, radiation, demande de document, etc. Les réponses peuvent être : acceptation, refus, etc.

Pour accéder à un service particulier, une application doit posséder un module informatique spécifique qui met en œuvre les règles définies par le service distant : respect des types de requêtes et réponses supportés, mise en forme spécifique des données dans chaque message...

Les données transmises dans les messages sont codées avec le langage XML. Planete réalise différents contrôles (syntaxe du message, cohérence des données...) sur les messages échangés afin de réduire les erreurs de traitement.

## 9.2 Les éléments structurants

L'accès à un service particulier se fait via un logiciel qui possède une interface technique conforme aux spécifications de Planete et un module informatique de gestion des messages conforme aux règles définies par le service distant : respect des types de requêtes supportés, du format des données dans les messages...

- La plupart des services accessibles sont facturés à l'usage. Pour les utiliser, il est nécessaire de souscrire au préalable un abonnement et de se conformer aux Conditions Générales d'Utilisation (CGU).

## 9.3 Les particularités pour les notaires

Les Logiciels de Rédaction d'Actes disposent d'une interface technique d'accès à Planete et, pour la plupart, des différents modules qui leur permettent d'interagir avec les services distants.

L'ADSN vérifie la conformité technique des Logiciels de Rédaction d'Actes à ces services distants et délivre une homologation technique à ceux qui sont conformes aux règles définies.

À travers le service ANF, la DGFiP donne accès à l'application FIDJI (Fichier Informatisé des Données Juridiques Immobilières) des services de publicité foncière, qui contient les anciennes fiches hypothécaires sur papier qui ont été scannées (« Stock ») et les fiches dématérialisées nativement (« Flux »), ainsi qu'aux actes publiés depuis 1956 (« Actes »).

L'accès au service ANF est payant par virement à la CDC pour chaque demande.

La Base de Références Immobilières, gérée par l'ADSN, alimente la base Perval, gérée par Adnov, pour les statistiques immobilières de la province et la base Bien, gérée par Paris Notaires Services, pour celles d'Île-de-France.

L'accès aux services suivants, via un Logiciel de Rédaction d'Actes, nécessite au préalable la souscription d'un abonnement payant auprès de l'ADSN et la signature de CGU spécifiques :

- Télé@ctes pour les Services de la Publicité Foncière,
- Casier Judiciaire National,
- État Civil,
- Safer-DIA.

La majorité des services requiert l'utilisation d'une clé REAL.

## 9.4 Les bonnes pratiques

Le Casier Judiciaire National et le Service Central de l'État Civil sont accessibles par le Logiciel de Rédaction d'Actes via Planete ou directement par un site spécifique : <http://casierjudiciaire.real.notaires.fr> et <http://etatcivil.real.notaires.fr/etat-civil>.

## 9.5 Les principales solutions du marché

Au 01/07/2021, les Logiciels de Rédaction d'Actes sont homologués techniquelement pour les accès aux services :

Editeur du logiciel	Logiciel	Télé@ctes v4	État civil	Casier Judiciaire National
Fichorga	Authen.tic	Oui	Oui	Oui
Fiducial Informatique	Fiducial Notaires Actes	Oui	Oui	Oui
	Signature	Oui	Oui	Oui
	Winnot Expert	Oui	Oui	Oui
Genapi	Inot Actes	Oui	Oui	Oui

## 9.6 Les critères de choix

L'utilisation des services distants via les Logiciels de Rédaction d'Actes permet un gain de temps dans les formalités ainsi qu'une précision et cohérence des données transmises.

### Le vocabulaire

**API (Application Programming Interface ou Interface de programmation applicative)** : porte d'accès à une fonctionnalité offerte par une application pour d'autres logiciels et définie par des règles.

**XML (eXtensible Markup Language ou Langage de balisage extensible)** : langage informatique de description des données en mode texte, basé sur des balises ouvrantes et fermantes, qui permet de vérifier facilement le respect de la syntaxe convenue. Le langage HTML utilisé pour décrire les pages web est une utilisation du XML.

# 10. FICEN

## 10.1 Les concepts de base

Le FICEN (« Fichier Interactif Centralisé du Notariat ») est l'annuaire de référence du notariat français géré par le CSN. Il regroupe les informations officielles sur les notaires, les offices, les collaborateurs, les instances et les organismes.

Il est mis à jour principalement par le CSN et les Chambres lors des nominations officielles de notaires et lors les évènements qui touchent chaque notaire, collaborateur ou instance (changement de statut, changement d'office...).

Certaines informations issues d'autres bases de données sont également centralisées, manuellement ou automatiquement, dans le FICEN : adresses de messagerie des offices, liste des sites web des offices, affiliations à la CRPCEN...

Certaines informations du FICEN servent à alimenter des référentiels spécifiques, tels que l'annuaire des notaires et des offices du site internet [www.notaires.fr](http://www.notaires.fr), les comptes ID.Not, la liste des offices et instances de Sacre, la liste des offices des applications Radar et Baromètre, l'annuaire des notaires français de la plateforme de collaboration européenne EUFides, etc.

Les informations du FICEN servent ponctuellement à éditer des listes de notaires pour des organismes, telle que l'Association du Congrès des Notaires.

### API Annuaire

Des applications destinées au notariat peuvent accéder automatiquement à certaines données du FICEN au travers d'une interface informatique spécifique appelée « API Annuaire ».

Ce mode d'interrogation des données du FICEN est réservé à des applications et des usages validés par le CSN.

### FICEN-ECO

FICEN-ECO est une application satellite du FICEN qui centralise, via Planete, les données économiques relatives aux offices et qui permet d'éditer les bordereaux de cotisations CSN.

Il est alimenté par les Déclarations d'Activité Professionnelle.

FICEN-ECO alimente l'application Oscar.

## 10.2 Les éléments structurants

- ➡ La mise à jour des données dans le FICEN est primordiale pour assurer la pertinence des données dans les autres référentiels.

## 10.3 Les particularités pour les notaires

- Les modifications des informations de base dans le FICEN sont réservées au CSN et aux Chambres qui en assurent leur véracité.

## 10.4 Les bonnes pratiques

- Au cas où un notaire ou un collaborateur détecterait une information erronée le concernant, il doit s'adresser en priorité à sa Chambre (cas d'un changement d'activité ou d'office) ou au support technique de l'ADSN.

## 10.5 Les principales solutions du marché

Le FICEN est unique et géré par le CSN.

## 10.6 Les critères de choix

Le FICEN répond aux obligations du CSN de gestion du référentiel des notaires.

### Le vocabulaire

**DAP (Déclaration d'Activité Professionnelle)**: édition informatisée reprenant une synthèse des états comptables produite par les comptabilités des offices au 31 décembre et à chaque clôture de période comptable.

# 11. ID.Not

## 11.1 Les concepts de base

L'utilisation d'une ressource informatique, telle d'une application, nécessite d'être authentifié afin de pouvoir limiter les accès aux utilisateurs autorisés et de contrôler les droits attribués à chaque utilisateur.

L'authentification d'un utilisateur est en général basée sur un identifiant de compte, qui peut être une suite de caractères quelconque ou une adresse de messagerie, et un mot de passe confidentiel associé à cet identifiant.

### Fonctionnement sans authentification centralisée

Chaque application peut mettre en place son propre contrôle d'accès. Cette méthode induit les inconvénients suivants :

- un utilisateur doit être déclaré dans chaque application,
- l'activation ou l'invalidation d'un compte doit se faire dans chaque application,
- un utilisateur possède autant de couple identifiant de compte-mot de passe que d'applications auxquelles il accède,
- l'utilisateur doit saisir un identifiant de compte et un mot de passe spécifique lorsqu'il se connecte à chaque application,
- avec une politique de sécurité un peu stricte qui oblige à changer de mot de passe tous les mois, la gestion des nombreux mots de passe devient vite infernale.

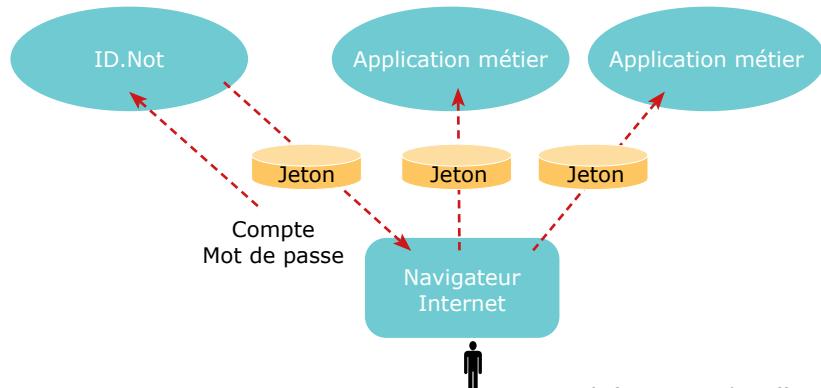
### Fonctionnement avec authentification centralisée

Sur un principe similaire à celui de FranceConnect proposé par l'État au grand public, le CSN a mis en place un système d'authentification unique et centralisé appelé ID.Not pour faciliter la vie des professionnels du notariat :

- l'utilisateur est déclaré dans un seul système de contrôle des droits,
- l'utilisateur a un seul identifiant de compte et mot de passe utilisable pour toutes les applications du notariat en relation avec ID.Not,
- l'utilisateur s'authentifie une fois auprès sur la mire de connexion du site internet ID.Not,
- il est ensuite reconnu par toutes les applications qui sont associées à ID.Not.

Le système ID.Not permet, par paramétrage, une authentification à « double facteur » ; c'est-à-dire l'utilisation du mot de passe personnel et d'un dispositif physique détenu par l'utilisateur, comme un smartphone.

Techniquement, lorsque l'utilisateur s'authentifie auprès d'ID.Not avec son navigateur Internet, ID.Not délivre un jeton d'authentification (« token ») à son navigateur Internet que celui-ci va présenter automatiquement aux autres applications web auxquelles il veut ensuite accéder. Le jeton d'identification est valide pendant une durée de 10 heures.



## Applications liées

À la date du 01/07/2021, les applications utilisables avec ID.Not sont listées dans le chapitre « Les principales applications du notariat ».

### 11.2 Les éléments structurants

ID.Not est un système d'authentification spécifique au notariat français.  
L'utilisation d'ID.Not est réservée à des applications et des usages validés par le CSN.

- Tous les notaires et leurs collaborateurs peuvent avoir gratuitement un compte ID.Not.

Les collaborateurs multi-office et les notaires qui exercent un mandant en instance ne peuvent avoir qu'un seul compte. Ils peuvent choisir l'office auquel ils sont rattachés.

Pour créer un compte ID.Not, un utilisateur doit à minima indiquer sa date de naissance et une adresse email personnelle.

La possibilité d'utiliser ID.Not avec une application suppose que :

- l'application soit accessible avec un navigateur Internet,
- l'éditeur de l'application ait adhéré au système ID.Not auprès du CSN,
- l'éditeur de l'application ait mis en œuvre le protocole d'authentification défini par ID.Not dans son application.

### 11.3 Les particularités pour les notaires

Seules les applications en relation avec la profession notariale sont habilitées à utiliser ID.Not.

La procédure d'activation d'un compte ID.Not est différente pour :

- les notaires (titulaires, associés et salariés) et les secrétaires généraux d'instance ;
- les collaborateurs car ils doivent être rattachés à une entité par leur employeur.

À terme, ID.Not devrait supplanter la clé REAL pour la fonction d'authentification.

### 11.4 Les bonnes pratiques

Un seul identifiant et mot de passe donnant accès à toutes les applications, il faut veiller à :

- utiliser un mot de passe complexe,
- changer régulièrement son mot de passe,
- ne pas partager son identifiant et mot de passe.

- Les responsables d'office ou d'instance doivent mettre à jour régulièrement la liste des collaborateurs qui leur sont attachés.

L'utilisation d'un identifiant personnel appartenant à un tiers relève de l'usurpation d'identité.

### 11.5 Les principales solutions du marché

Le CSN est responsable de la gestion du système ID.Not. Il accompagne les éditeurs pour la mise en place dans leur application.

### 11.6 Les critères de choix

ID.Not est un des fondements de l'accès aux ressources techniques de la profession notariale.

## Le vocabulaire

**Authentification**: procédure visant à demander des preuves d'identité pour déterminer si une personne ou une machine est effectivement la personne ou la machine qu'elle est censée être.

**Authentification à double facteur**: méthode de reconnaissance d'une personne basée sur deux preuves d'identité distinctes, telle que la connaissance d'un mot de passe et la détention d'un dispositif physique.

**Autorisation**: droit d'accès à une ressource.

**Fédération d'identité**: groupement d'acteurs qui partagent leurs systèmes de gestion d'identité et un système d'authentification.

**FranceConnect**: Fédération d'identité basée sur des fournisseurs d'identité publics (DGFiP, Assurance Maladie...) et privés (La Poste...) qui est proposée par l'État aux particuliers pour faciliter l'authentification et l'accès aux services en ligne.

**Identification**: procédure pour établir l'identité d'une personne. L'identification est un prérequis à l'authentification.

**Identifiant**: toute suite de caractères alphabétiques ou numériques qui permet de repérer une personne précise.

**OpenIDConnect**: un des deux protocoles techniques utilisés pour la délivrance des jetons d'authentification.

**Preuve**: élément justificatif qui peut être une information que l'on connaît (mot de passe, code PIN...), un dispositif physique que l'on possède (carte d'identité, acte de naissance, smartphone, clé Real...), une information qui décrit ce que l'on est (photo, données biométriques...), un geste que l'on sait faire (signature manuscrite, reproduction d'un motif sur un smartphone...).

**SAML**: un des deux protocoles techniques utilisés pour la délivrance des jetons d'authentification.

**Token (jeton)**: certificat temporaire délivré par le système central d'authentification.

# 12. Les principales applications du notariat

## 12.1 Les concepts de base

Les principales applications du notariat peuvent :

- proposer des services essentiels à la mission du notaire (Micen, FCDDV, gestion des clés REAL...),
- permettre de réaliser numériquement des formalités (consultation État Civil et Casier Judiciaire...),
- faciliter la relation client de l'office (enquête de satisfaction...),
- aider le notaire pour le pilotage de l'office (analyse de rentabilité...),
- contribuer au développement des collaborateurs (formation, emploi...).

Le site internet Notaccess, réservé aux notaires ayant un compte ID.Not, est un portail qui recense toutes les applications disponibles.

Les Chambres et Paris Notaires Services proposent également des sites d'information ou des applications particulières, gratuites ou payantes, accessibles à tous les offices, telles que le Dépôt Electronique Notarial.

Des acteurs concurrentiels peuvent proposer des applications complémentaires, telles que la gestion de site internet pour l'office ou l'envoi de recommandé électronique.

## Applications de base

Application	Description	Type	Accès via LRA	Adresse site Internet	Gestionnaire	Sécurisé par ID.Not	Cle REAL nécessaire
CRPCEN	Caisse de prévoyance et de retraite des notaires	Site internet	Non		CPRCEN	Oui	
Extranet ADSN	Portail de gestion des relations avec ADSN	Site internet	Non	extranet-adsn.notaires.fr	ADSN	Oui	
Ficen	Annuaire de la profession notariale	Application	Non	ficen.notaires.fr	CSN	Oui	Non
ID.Not	Site d'administration des identités numériques des notaires	Site internet	Non	https://compte.idnot.fr/	CSN	Oui	Non
Notaccess	Magasin des applications téléchargeables sur smartphone ou tablette	Site internet	Non	notaccess.notaires.fr/	CSN	Oui	
Portail des consentements	Gestion de la diffusion des données bancaires auprès de la CDC	Site internet	Non	prc.real.notaires.fr/prc	ADSN	Non	Oui
Sacre	Site d'administration des clés REAL	Site internet	Non	https://sacre.real.notaires.fr	ADSN	Non	Oui

## Applications essentielles

Application	Description	Type	Accès via LRA	Adresse site Internet	Gestionnaire	Sécurisé par ID.Not	Cle REAL nécessaire
CDC-Net	Banque en ligne de la Caisse des Dépôts	Site internet	Non	http://real.cdc-net.com	CDC	Non	Oui
FCDDV	Fichier Central des Dispositions de Dernières Volontés	Application	Oui	fcddv.real.notaires.fr	ADSN	Non	Oui
MICEN	Minutier Central Electronique des Notaires de France	Application	Oui	micen-portail.real.notaires.fr	ADSN	Non	Oui
PACSen	Fichier d'enregistrement des PACS notariés	Site internet	Non	pacsen.real.notaires.fr	ADSN	Non	Oui
Téléactes	Publicité foncière	Application	Oui		DGFIP	Non	Oui

## Applications de production

Application	Description	Type	Accès via LRA	Adresse site Internet	Gestionnaire	Sécurisé par ID.Not	Cle REAL nécessaire
ANF	Accès des Notaires au Fichier immobilier	Application	Oui		DGFIP	Non	Oui
Cadastre	Consultation du plan cadastral	Site internet	Non	http://spdc.dgfip.finances.gouv.fr/index.asp	DGFIP	Non	Non
Casier judiciaire	Interrogation du Casier Judiciaire sur les condamnations opposables	Application	Oui	casierjudiciaire.real.notaires.fr	ADSN	Non	Oui
DIA-Safer	Déclarations d'intention d'alléger dématérialisées	Application	Oui		ADSN	Non	Oui
Etat civil	Interrogation des services d'Etat Civil	Application	Oui	etatcivil.real.notaires.fr	ADSN	Non	Oui
EUFides	Plateforme de partage de documents entre notaires européens.	Site internet	Non	www.eufides.eu/	CEE	Non	Non
Ficoba	Fichier des comptes bancaires et assimilés ouverts en France	Site internet	Non	https://applications.dgfip.finances.gouv.fr	DGFIP	Non	Non
Ficovie	Fichier des contrats d'assurance-vie et de capitalisation ouverts en France	Site internet	Non	https://applications.dgfip.finances.gouv.fr	DGFIP	Non	Non
Perval	Consultation des références immobilières pour comparaison	Site internet	Non	https://www.perval.fr/	ADSN	Oui	Non
Tracfin	Portail Tracfin	Site internet	Non	https://tracfin.finances.gouv.fr	DGFIP	Non	Oui

## Applications d'aide à la production

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
ARERT	Gestion des testaments européens	Site internet	Non	www.arert.eu	CEE	Non	
Cridon	Portail d'accès aux sites des 5 CRIDON	Site internet	Non	cridon.notaires.fr	Cridon	Non	Oui
Hectaur	Outil de calcul des usufruits économiques, des rentes viagères, des prêts et des refinancement de prêts	Site internet	Non	hectaur.notaires.fr	CSN	Oui	Non
Immobilier	Annonces immobilières	Site internet	Non	immobilier.notaires.fr	CSN	Oui	
Notaires et Territoires	Gestion des plans d'actions des instances accompagnées par la CDC	Site internet	Non	https://www.notaires-et-territoires.fr/	CDC	Oui	Non
Vigilance	Plateforme notariale de prévention du risque client	Site internet	Non	https://intra.notaires.fr/csn/jcms/t1_680331/questionnaire-de-vigilance-lab/ft	CSN + Dow Jones	Oui	

## Applications de relation client

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
Baromètre satisfaction clients	Mesure de la satisfaction des clients	Site internet	Non	https://barometre.satisfaction.notaires.fr/	CSN	Oui	
Notadirect	Mise en relation des internautes et des notaires	Site internet	Non	https://notadirect.notaires.fr/	CSN	Oui	

## Application de développement personnel

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
Bourse d'emplois	Bourse d'emplois réservée à la profession	Site internet	Non	https://bourse-emplois.notaires.fr/		Oui	
Formacen	Suivi de la formation continue des notaires	Site internet	Non	formacen.notaires.fr	CSN	Oui	
Gisele	Gestion des parcours de labellisation des notaires et des collaborateurs postulants	Site internet	Non	https://www.gisele.notaires.fr	CSN	Oui	

## Application de diagnostic de l'office

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
Ma structure	Aide à la décision pour déterminer les structures juridiques adaptées à son activité	Site internet	Non	https://mastructure.notaires.fr	CSN	Oui	
Odeon	Outil d'analyse des difficultés d'un office et des pistes d'amélioration	Site internet	Non	odeon.notaires.fr	CSN	Oui	
Oscar	Outil de comptabilité analytique et de réflexion stratégique	Site internet	Non	https://oscar.notaires.fr/	CSN	Oui	
Radar	Outil d'analyse, de comparaison et de prévision de l'activité des offices	Site internet	Non	https://radar.notaires.fr/	CSN	Oui	

## Application de support à l'office

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
Extranet du Conseil Régional de Bordeaux	Base documentaire, formation et communication	Site internet	Non		CR Bordeaux	Oui	
Institut du développement	Portail de l'Institut du développement	Site internet	Non			Oui	
Management	Bonnes pratiques de management	Site internet	Non	management.notaires.fr		Oui	
Projet d'entreprise	Outil pour accompagner l'office dans son projet entrepreneurial et son développement	Site internet	Non			Oui	
Zéro papier	Accompagnement dans une démarche « Zéro Papier »	Site internet	Non		CSN	Oui	

## Applications diverses

Application	Description	Type	Accès via LRA	Adresse site internet	Gestionnaire	Sécurisé par ID.Not	Clé REAL nécessaire
Cahier pratique NVP	Fiches pratiques NVP	Site internet	Non				
Congrès des notaires	Inscription au Congrès des Notaires de France	Site internet	Non	http://www.congresdesnotaires.fr/fr/	Congrès des Notaires	Oui	

## 12.2 Les éléments structurants

La plupart des applications sont mises à disposition sous forme de site Internet accessible à distance via un navigateur Internet (client léger).

Les applications suivantes sont accessibles via le Logiciel de Rédaction d'Actes connecté à PLANETE :

- Casier Judiciaire National,
- État Civil,
- Safer-DIA,
- Télé@ctes pour les Services de la Publicité Foncière.

L'adresse de l'application distante ou « URL » précise le protocole à utiliser, le nom du serveur, le nom de domaine, le chemin d'accès hiérarchique et le nom de la page.

- Les formes usuelles sont : protocole://serveur.sousdomaine.domaineprincipal/répertoire/page ou protocole://serveur.sousdomaine.domaineprincipal/requête?paramètres. Par exemple : <http://micen.real.notaires.fr/>, <https://www.google.com/search?client=firefox-b-d&q=marecherche>,

Chaque protocole est associé à un port logiciel différent (ex : 80 par défaut pour le protocole http, 443 pour le protocole HTTPS) sur un serveur hôte localisé à une adresse IP.

Les applications sécurisées utilisent le protocole HTTPS qui chiffre les communications entre le client et le serveur.

### 12.3 Les particularités pour les notaires

L'accès aux applications notariales est contrôlé par ID.Not ou par la clé REAL.

Les applications de la DGFIP, telles que Ficoba, Ficovie, peuvent nécessiter un identifiant qui leur est propre.

Pour installer une application accessible à l'adresse « monserveur.monsousdomaine.notaires.fr », il est nécessaire de créer le sous-domaine « monsousdomaine.notaires.fr ». Ce sous-domaine du domaine « notaires.fr » doit être conforme au plan de nommage défini par le CSN et doit obtenir l'agrément de la Chambre, conformément au Règlement National.

### 12.4 Les bonnes pratiques

- Les applications distantes accessibles par les URL <http://serveur.domaine/> et <https://serveur.domaine/> sont deux applications distinctes situées à la même adresse IP mais associées à des ports logiciels différents, sauf si une adresse renvoie vers l'autre. Il faut donc veiller à spécifier le bon protocole.

La création d'un compte ID.Not est un prérequis pour accéder aux applications.

### 12.5 Les principales solutions du marché

La liste des applications notariales disponibles est actualisée dans Notaccess.

Les applications et services proposés par Paris Notaires Services sont présentés sur le site <http://paris-notaires-services.fr/>.

### 12.6 Les critères de choix

Chaque application répond à un besoin spécifique.

## Le vocabulaire

**Application** : Ensemble de logiciels destiné à une finalité donnée.

**HTTP (HyperText Transfer Protocol)** : protocole de communication client-serveur développé pour le World Wide Web et utilisé pour les sites internet.

**HTTPS (HyperText Transfer Protocol Secure)** : variante sécurisée du protocole http utilisant des certificats électroniques.

**Portail** : site Internet qui donne accès à des ressources.

**URL (Uniform Resource Locator)** : adresse d'une ressource, telle qu'un site web, sur Internet.

# 13. MICEN

## 13.1 Les concepts de base

Le MICEN (« Minutier Central Electronique des Notaires de France ») est l'archive centrale électronique du notariat français. Il recueille et conserve de manière sécurisée tous les actes authentiques réalisés sous forme électronique depuis 2008.

Les actes déposés au MICEN sont des documents signés électroniquement par le notaire à l'aide de la clé REAL ; ce qui garantit leur authenticité. Cf. chapitre « la clé REAL ».

Le MICEN garantit leur conservation, leur consultation, leur intégrité et leur confidentialité.

L'ajout d'un acte authentique électronique, ou d'une mention, au MICEN se fait en deux phases :

- la création à l'aide d'un Logiciel de Rédaction d'Actes,
- la signature et l'envoi au MICEN à l'aide du logiciel SignActe et de la clé REAL du notaire instrumentaire.

### Fonctionnement de SignActe

Le logiciel SignActe a été développé par l'ADSN. Il est constitué d'un client lourd qui doit être installé sur le poste de travail du notaire et d'un tableau bord accessible en mode web.

SignActe a pour rôles :

- la vérification de l'acte transmis pour signature par le Logiciel de Rédaction d'Actes,
- l'affichage de l'acte,
- le recueil de la signature électronique du notaire instrumentaire,
- le dépôt au MICEN.

Le logiciel SignActe tient à jour, dans 3 répertoires du poste de travail du notaire, le statut des actes, mentions, notes et recueils déposés au MICEN.

### Alimentation du MICEN

Le processus métier d'alimentation du MICEN est le suivant :

1. Le notaire rédige le projet d'acte sur son Logiciel de Rédaction d'Actes, y attache les éventuelles annexes, obtenues depuis des documents papier scannés ou nativement numériques, puis indique les parties signataires et, pour chacune, leur lieu de signature ;
2. À partir de son Logiciel de Rédaction d'Actes, le notaire instrumentaire procède à la conversion de l'acte et de ses annexes au format d'archivage PDF/A-1b et demande sa validation ;  
Si l'acte est réalisé à distance entre deux offices, le notaire instrumentaire crée, à partir de son Logiciel de Rédaction d'Actes et via l'outil SignActe, une session de signature avec un identifiant unique sur l'espace collaboratif du MICEN ;
3. Le notaire instrumentaire procède à la lecture de l'acte sur un écran devant les parties ;  
Si l'acte est à distance, il utilise un logiciel de visioconférence agréé par le CSN pour partager l'acte affiché sur son écran avec les parties distantes et le notaire en participation ;

- 4.** Le notaire instrumentaire recueille, via une tablette tactile homologuée, les signatures manuscrites des parties ;  
Si l'acte est réalisé à distance entre deux offices, le notaire participant accède à la session de signature avec l'identifiant unique qui lui a été communiqué par le notaire instrumentaire puis il collecte sur un « formulaire de recueil des consentements », via une tablette tactile, les signatures manuscrites attestant le consentement des clients présents en son office puis il signe lui-même électroniquement ce formulaire à l'aide de sa clé REAL. Le notaire instrumentaire agrège ensuite sur l'acte le « formulaire de recueil des consentements » contenant l'ensemble des signatures. Afin de permettre aux parties distantes de suivre cette cérémonie de signature, les parties signataires peuvent tour à tour partager leur écran avec le logiciel de visioconférence ;
- 5.** Le recueil de l'ensemble des signatures des parties terminé, le notaire instrumentaire scelle l'acte, ses annexes et les signatures des parties en apposant une signature électronique grâce au certificat électronique contenu dans sa clé REAL et au logiciel SignActe ;
- 6.** L'acte authentique électronique ainsi obtenu est transmis au MICEN par SignActe, via le réseau notarial sécurisé, pour être classé dans un espace d'archivage privé à l'office. Une preuve de dépôt est renvoyée par le MICEN au Logiciel de Rédaction d'Actes.

## Consultation

Un office notarial peut consulter tous ses actes électroniques transmis au MICEN sur le tableau de bord de SignActe appelé « Portail de visualisation des actes ».

Il peut également demander des copies simples ou des copies authentiques électroniques de l'AAE, soit en fin de signature, soit à partir du tableau de bord.

### 13.2 Les éléments structurants

3,65 millions de nouveaux Actes Authentiques Electroniques (AAE) ont été déposés au MICEN en 2020, pour un total de 16,3 millions d'actes depuis 2008.

Un acte notarié établi sous forme électronique, avec un dispositif de signature de niveau « qualifié », comme la clé REAL, à la même valeur qu'un acte authentique papier : date certaine, force probante et force exécutoire.

Les actes et leurs copies n'ont pas de notion de pages sous forme électronique. Les références à un nombre de pages sont donc supprimées dans un acte authentique électronique.

L'image et la signature de l'acte ne doivent pas être altérées dans le temps. Pour cela, les documents sont stockés au MICEN en format PDF/A-1b qui inclut tous les éléments strictement nécessaires au rendu visuel.

- La taille des documents déposés (acte, signatures et annexes) est limitée à 36 Mo. Une marge est prévue jusqu'à 40 Mo pour permettre le dépôt ultérieur de mentions postérieures.

Le MICEN assure la conservation des Actes Authentiques Electroniques pendant 75 ans minimum. Au-delà de cette durée, les actes électroniques seront versés, comme les actes au format papier, aux services des Archives Départementales ou Nationales.

### 13.3 Les particularités pour les notaires

L'utilisation du MICEN nécessite d'une part l'utilisation d'équipements homologués ou agréés par le CSN (Logiciel de Rédaction d'Actes, tablette tactile de recueil des signatures, logiciel SignActe, réseau notarial) et, d'autre part, de l'adhésion préalable, auprès de l'ADSN, à des Conditions Générales d'Utilisation spécifiques.

Le MICEN propose un environnement de formation permettant de faire des tests sans impacter l'environnement de production officiel.

Lors d'une séance de signature à distance entre deux offices, l'identification de l'ensemble des parties et témoins à l'acte, ainsi que leur signature manuscrite, sont recueillies dans un « formulaire de recueil des consentements ». Ce formulaire est ajouté au pied de l'acte, avant les annexes.

L'accès aux actes déposés dans le MICEN est exclusivement réservé aux notaires de l'office qui les a déposés.

Un notaire peut, via son Logiciel de Rédaction d'Actes, octroyer des droits de consultation d'actes aux collaborateurs de son office. Ces derniers devront cependant être équipés d'une clé REAL qui sécurise l'accès au MICEN.

### 13.4 Les bonnes pratiques

Au 01/07/2021, la version majeure la plus récente du logiciel SignActe est la v4.

- Il faut veiller au poids des documents annexés à l'acte.

Quand quelques pages d'un document original papier sont scannées à l'aide d'une imprimante de bureau paramétrée avec une résolution élevée (supérieure à 300 ppp) et en couleur, le document PDF obtenu peut rapidement dépasser 1 Mo. Diviser la résolution du scanner par 2 permet de réduire par 4 le poids d'une page scannée.

- Les documents papier doivent être scannés avec une résolution basse et de préférence en noir/blanc ; par exemple 150 ppp pour les documents qui ne contiennent que du texte ou 200 ppp en général.

Avant d'annexer des documents aux actes (PDF, images), il est nécessaire de les compresser. Attention à certains formats d'images, tels que PNG ou TIFF, qui se compriment plus difficilement que le format JPEG.

Au cas où l'acte et tous ses composants auraient une taille supérieure à 36 Mo, il est possible, soit d'établir un acte sous forme papier, soit d'établir plusieurs Actes Authentiques Electroniques dans lesquels les annexes se répartissent. Avec cette seconde méthode, l'acte doit mentionner qu'il a été établi ainsi.

Seuls les Actes Authentiques Electroniques conservés au MICEN ont le statut de « minutes ». Les AAE conservés dans une application de Gestion Electronique de Documents (GED) ne sont que des copies simples.

### 13.5 Les principales solutions du marché

Le MICEN est unique et placé par décret sous le contrôle du Conseil Supérieur du Notariat.

### 13.6 Les critères de choix

Le MICEN est un des systèmes principaux du notariat français.

## Le vocabulaire

**Minute** : Original d'un acte authentique

**Minutier** : lieu où chaque notaire conserve l'ensemble des minutes au sein de l'office notarial

**PDF/A-1b (Portable Document Format for Archive – ISO 19005-1 Basic)** : format PDF adapté à l'archivage long-terme de documents statiques, assurant notamment la reproduction fiable de l'apparence visuelle, par l'incorporation de tous les éléments de rendu visuel tels que les polices de caractères, et dont la pérennité est garantie. La combinaison de PDF/A et des signatures électroniques assure que le document ne puisse pas subir de manipulations ultérieures.

**Résolution** : nombre de pixels par unité de mesure exprimée en pouce (ppp ou « ppi » / « pixel par pouce » ou « pixel per inch » pour un écran ou « dpi » / « dot per inch » pour une impression). Plus la résolution d'un document est élevée, plus il est précis et net à l'affichage mais lourd car il contient des pixels plus nombreux offrant la possibilité de zoomer dans l'image du document.

**SignActe** : logiciel développé par l'ADSN pour signer électroniquement l'acte et le déposer au MICEN.

# 14. Les espaces collaboratifs

## 14.1 Les concepts de base

Un espace collaboratif, ou espace client, est un site internet, avec des accès sécurisés, qui assure le partage d'informations entre différents groupes de personnes pour améliorer la collaboration.

Les utilisateurs peuvent être un agent immobilier, un promoteur immobilier, un notaire, un vendeur, un acquéreur, un diagnostiqueur immobilier, une banque.

L'espace collaboratif permet de dématérialiser les processus en amont du notaire pour constituer un dossier :

- saisie en ligne des informations relatives aux clients au bien immobilier : identité, coordonnées, situation matrimoniale, etc.,
- téléchargement des pièces numérisées : pièces d'identité, diagnostics, certificats, documents de copropriété...
- suivi en temps réel de l'état du dossier et relance automatique.

D'autres fonctionnalités peuvent être proposées comme :

- la prise de rendez-vous,
- une visioconférence intégrée,
- la réalisation de formalités préalables ne nécessitant pas la clé REAL (rapport Géorisques, plan cadastral, note de renseignement d'urbanisme...),
- des simulateurs de calculs,
- le suivi de la commercialisation d'un programme de VEFA,
- la signature électronique de contrats de réservation.

## 14.2 Les éléments structurants

→ Le dossier dans l'espace collaboratif est créé par un des intervenants en amont dans le processus de vente ou par le notaire pour les autres actes.

Le créateur du dossier peut inviter d'autres personnes en saisissant leur adresse de messagerie.

La plupart de LegalTechs ciblent les acteurs du marché immobilier en amont de la vente chez le notaire.

Lorsque les espaces collaboratifs seront techniquement interopérables avec les Logiciels de Rédaction d'Actes, le flux des messages électroniques avec des pièces jointes associées qui sont à traiter manuellement sera notablement réduit.

## 14.3 Les particularités pour les notaires

Un notaire peut être utilisateur de plusieurs espaces collaboratifs différents car les dossiers peuvent avoir été créés au début du processus de vente immobilière par un promoteur ou différents agents immobiliers, avant le choix du notaire.

Suivant la solution choisie, le notaire peut suivre dans l'espace collaboratif les formalités à réaliser selon le type d'acte.

## 14.4 Les bonnes pratiques

Les droits des utilisateurs qui ont accès à un dossier doivent être gérés avec précision.

- Comme tout système qui gère des données personnelles, l'espace collaboratif est soumis au RGPD et au « droit à l'oubli ». Les dossiers contenant des données personnelles doivent être supprimés après un délai justifié.

## 14.5 Les principales solutions du marché

Les espaces collaboratifs disponibles pour les notaires sont :

- les solutions des éditeurs de Logiciels de Rédaction d'Actes : « Izinot » de Fichorga, « Signature Relation Client » de Fiducial, « Espace Client » de Genapi,
- les solutions des LegalTechs spécialisées : Dooxi, FoxNot, My Notary, « NotaRoom » de NotaSolutions, Notiplus, Quai des Notaires,
- les solutions de la profession : « Espace notarial » et « Espace notarial promoteurs » de Paris Notaires Services.

## 14.6 Les critères de choix

L'utilisation d'un espace collaboratif permet de :

- communiquer avec son client au travers d'un outil moderne,
- reporter sur le client la saisie des éléments d'un dossier,
- faire vérifier par le client les éléments d'un dossier au cours de sa constitution.

La sécurité des données, et notamment la confidentialité, est primordiale. Il faut veiller à la localisation des données et à l'expertise du prestataire en charge de l'hébergement de la solution.

## Le vocabulaire

**Extranet**: extension du système d'information d'une organisation accessible à des membres extérieurs à cette organisation. Les espaces collaboratifs peuvent être vus comme une forme

# 15. Homologation, agrément et label

## 15.1 Les concepts de base

À la base de toute homologation, agrément ou label, il existe un cahier des charges ou « référentiel » qui fixe des objectifs, des critères et des règles à respecter, que ce soit d'un point de vue technique, juridique, opérationnel ou organisationnel.

Ce cahier des charges peut s'appliquer à tout système : un produit technique et/ou un service délivré et/ou le fonctionnement d'une organisation.

Le cahier des charges peut être public pour un usage large (ex : norme de management de la qualité ISO 9001 v2015, normes de sécurité ISO 270xx,) ou privé pour un usage spécifique (ex : médical, armée, CSN).

Une homologation va certifier qu'un système respecte un cahier des charges. Dans de nombreux contextes où la sécurité est primordiale (ex : aérien, automobile, médical, alimentaire...), une homologation technique est souvent un prérequis à l'utilisation ou la commercialisation d'un système.

Un agrément, délivré par une autorité administrative compétente, va officialiser une autorisation à utiliser un système. Cet agrément, préalable à l'utilisation, est le plus souvent basé sur une ou plusieurs homologations.

Un label est une reconnaissance destinée à valoriser auprès du grand public l'engagement d'une entité par rapport à un cahier des charges non obligatoire.

## 15.2 Les éléments structurants

Une homologation technique est délivrée par une entité technique à la suite d'une procédure de certification qui peut comprendre une batterie de tests techniques.

→ Seule une autorité administrative compétente peut délivrer un agrément. Le CSN est habilité par différents décrets à délivrer les agréments des systèmes du notariat français.

Sans agrément, un système soumis à agrément préalable ne doit juridiquement pas être utilisé.

Le respect des critères d'un label résulte d'une démarche volontaire de l'adhérent.

Les agréments et labels sont en général délivrés pour une durée limitée.

→ Les différents agréments et labels concernent des périmètres ou services spécifiques. Ils sont donc indépendants les uns des autres. L'attribution d'un agrément spécifique pour un système ne vaut pas agrément pour un autre système.

## 15.3 Les particularités pour les notaires

### Homologations

Les comptabilités notariales font l'objet d'une homologation technico-fonctionnelle par rapport aux conditions définies par l'arrêté du 27 janvier 2006 modifié.

Les homologations techniques concernent notamment :

- les interfaces des Logiciels Rédaction d'Actes avec les systèmes du notariat : interface Planète, utilisation de Télé@actes, accès au MICEN, accès au Casier Judiciaire National, accès au service d'État Civil et alimentation de la Base de Références Immobilières,
- les tablettes tactiles de signature des AAE,
- l'accès à l'API Annuaire du FICEN,
- l'utilisation de ID.Not.

La plupart des homologations techniques sont délivrées par la Direction Informatique du CSN ou, par délégation, par l'entité ADSN.

Les homologations sont valables tant que le cahier des charges n'évolue pas.

## Agréments

Les systèmes informatiques du notariat français soumis à agrément sont :

- les accès au réseau notarial, y compris les accès en mobilité,
- les solutions de visioconférence qui permettent de faire des Actes Authentiques Electroniques à Distance et des Procurations Authentiques avec Comparution à Distance.

Les agréments des systèmes informatiques du notariat français sont délivrés exclusivement par le Conseil Supérieur du Notariat et pour une durée de 3 ans.

Les différents systèmes informatiques agréés dans une catégorie se doivent d'être interchangeables, car répondant aux mêmes exigences, et interopérables entre eux afin que l'utilisation d'un système avec un autre soit transparente.

## Labels

Les labels du notariat, tels que le label « ETIK », ne concernent pas spécifiquement les systèmes informatiques mais les personnes et les organisations afin de mettre en valeur la qualité de leur expérience et de leurs pratiques.

## 15.4 Les bonnes pratiques

→ Tout office notarial se doit d'être équipé d'au moins un système homologué conforme ou agréé par catégorie.

D'autres systèmes, tels que des systèmes de visioconférence grand public, peuvent être utilisés pour des usages complémentaires. Il faut néanmoins garder à l'esprit que la confidentialité des échanges n'est pas assurée.

## 15.5 Les principales solutions du marché

À la date du 01/07/2021, les logiciels de comptabilité notariale déclarés conformes par le CSN à l'arrêté du 27 janvier 2006 modifié sont :

ÉDITEUR DE LOGICIEL	LOGICIEL
Fichorga	Juris Compta
	Juris Web
Fiducial Informatique	Fiducial Notaires Comptabilité
Genapi	Inot Comptabilité
	Wincompt

À la date du 01/07/2021, les Logiciels de Rédaction d'Acte déclarés conformes aux différents cahiers des charges technique de l'ADSN, issus notamment de la Convention entre le CSN et la DGFiP, sont :

ÉDITEUR DE LOGICIEL	LOGICIEL
Fichorga	Authen.tic
Fiducial Informatique	Fiducial Notaires Actes
	Signature
	Winnot Expert
Genapi	Inot Actes

À la date du 01/07/2021, les opérateurs agréés par le CSN pour l'accès au réseau notarial sont :

OPÉRATEUR RÉSEAU	OFFRE COMMERCIALE
Adista	Janua
Adnov	UnIT
Adnov	AgilIT
Adnov	AgilIT+
Adnov	SerenIT
Comnot	<i>sans nom particulier</i>
Navista	<i>sans nom particulier</i>

À la date du 01/07/2021, les solutions de mobilité proposées par les opérateurs agréés pour se connecter au réseau notarial sont :

OPÉRATEUR RÉSEAU	OFFRE COMMERCIALE
Adista	ADistance
Adnov	Ballade
Comnot	<i>sans nom particulier</i>
Navista	<i>sans nom particulier</i>

À la date du 01/07/2021, les solutions de visioconférence agréées par le CSN pour les Actes Authentiques Electroniques à Distance et les Procurations Authentiques avec Comparution à Distance sont :

PARTENAIRE	OFFRE COMMERCIALE	SOLUTION TECHNIQUE
Adnov	VisioAct	LifeSize
Comnot	VisioNot	LifeSize

Ces listes peuvent évoluer dans le temps et leur version à jour est diffusée sur le portail REAL.

## 15.6 Les critères de choix

L'homologation d'un système et l'obtention d'un agrément ou d'un label par un fournisseur sont des critères de qualité car il démontre la capacité à se soumettre à un cahier des charges multicritères exigeant.

Le choix d'un système homologué conforme est une garantie de bon fonctionnement et d'interopérabilité avec d'autres systèmes.

Le choix d'un système agréé est obligatoire.

Le choix d'un partenaire labellisé est un gage de qualité.

Hormis pour la solution de mobilité qui est liée à l'opérateur réseau choisi, le choix d'un fournisseur dans une catégorie de solutions n'impose pas le choix du même fournisseur dans une autre catégorie. Par exemple, un logiciel de comptabilité notariale peut être choisi indépendamment du Logiciel de Rédaction d'Actes.

## Le vocabulaire

**Audit**: contrôle, effectué par une entité experte, de la conformité du fonctionnement réel d'un système par rapport à un fonctionnement attendu et aboutissant à un rapport formel.

**Certification**: procédure qui consiste à faire valider, par un organisme agréé indépendant, la conformité d'un système par rapport à un cahier des charges.

# 16. La signature électronique

## 16.1 Les concepts de base

La signature électronique est la transposition de la signature manuscrite dans le monde numérique qui a des contraintes propres, notamment la facilité à modifier l'information.

La signature électronique est un mécanisme informatique qui a pour objectifs d'identifier le signataire d'un objet numérique et de garantir que l'objet numérique n'est pas modifié après signature.

La signature électronique n'est pas la simple apposition d'une image d'une signature manuscrite sur un objet numérique. Elle met en œuvre des procédés cryptographiques pour faire le lien avec l'identité du signataire et pour détecter l'altération ultérieure de l'objet numérique.

Par rapport à la signature manuscrite, la signature électronique permet de vérifier avec certitude l'identité exacte du signataire, l'intégrité du document signé et la date de signature.

La signature électronique repose sur une « infrastructure à clé publique » (PKI) combinant des moyens techniques utilisant la cryptographie et une organisation de confiance qui permettent d'assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation.

Elle met en œuvre une cryptographie dite « asymétrique » basée sur l'utilisation d'une clé privée pour la signature du document et d'une clé publique pour sa vérification. Les deux clés sont liées, mais la clé privée ne peut pas être déduite de la clé publique dans un délai raisonnable.



La clé publique étant partagée entre les parties, l'identification du propriétaire, la clé publique et l'intégrité de ces données sont protégées au sein d'un certificat électronique.

Pour contrecarrer l'adage « Sur Internet, personne ne sait que tu es un chien », le certificat électronique va attester de l'identité de la personne physique propriétaire de la clé publique. Pour cela le certificat doit être délivré en respectant une méthode rigoureuse de vérification de l'identité.

Plus la méthode sera rigoureuse basée sur des preuves physiques, plus la signature sera de niveau sécurisé.

## Certificat électronique

Un certificat électronique est un support de l'identité numérique et un moyen technique permettant de diffuser une clé publique en toute sécurité. C'est une sorte de conteneur qui contient notamment :

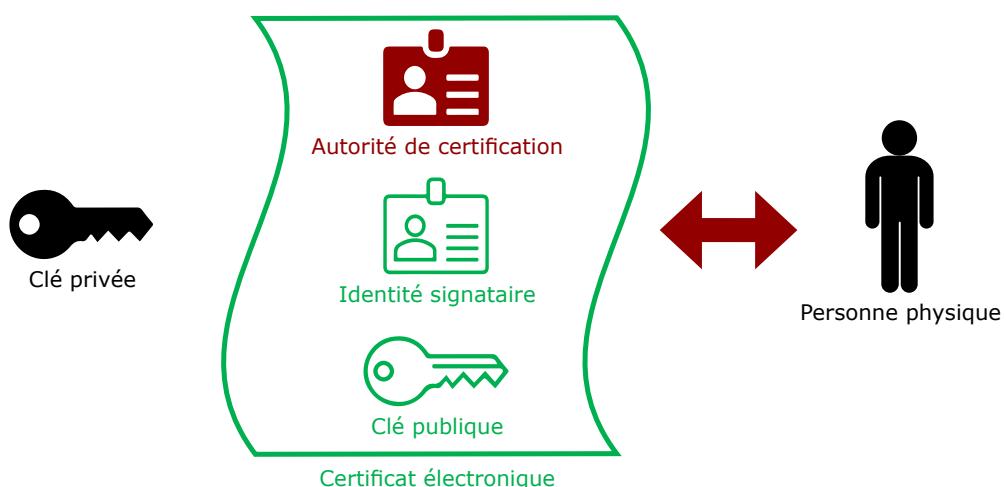
- le code d'identification du certificat,
- le nom de l'Autorité de Certification qui a créé le certificat,
- la signature électronique de l'Autorité de Certification.
- l'identité du porteur du certificat,
- la clé publique du porteur,
- les dates de début et fin de validité du certificat.

Il est matérialisé sous forme d'une suite de caractères alphanumériques :

```
9E55DH9794BDFS99RSC132WX1C5Z3EZR41CQ3R6ER5  
8ER4EZR445140UP5HN4D4215QRGR5487EYH5GGE5T  
5H4HET4HS8F7ET4VRT43AZ4+9QSD3FD42F2DF2F58Z  
EZR5454S6F9QSDUP5HN4D4215QRGR5487EY5H4HET
```

Un certificat électronique est nominatif et délivré par une Autorité de Certification à l'issue d'une procédure de vérification d'identité réalisée par une Autorité d'Enregistrement. L'Autorité de Certification atteste du lien entre l'identité de la personne physique et le certificat électronique qui la représente.

En général, au moment de la délivrance du certificat électronique, l'Autorité de Certification remet au porteur une clé privée et un code PIN qui servira à protéger l'utilisation de la clé privée.



Un certificat électronique est lisible mais infalsifiable et certifié, car lui-même signé au moyen de la clé privée de l'Autorité de Certification.

Un certificat électronique a trois grandes finalités :

- identifier une personne ou un serveur ou un service,
- réaliser une opération cryptographique sur des données avec une paire de clés,
- signer des informations.

Ces finalités se retrouvent dans plusieurs usages pratiques :

- l'authentification de personnes physiques ou de serveurs,
- la signature électronique par des personnes physiques,
- l'apposition de cachets électroniques pour la signature par des services numériques ou des personnes morales,
- le chiffrement des données pour assurer la confidentialité,
- l'apposition de sceaux électroniques pour la certification et l'horodatage,
- l'envoi de recommandé électronique.

Par exemple, les certificats électroniques SSL/TLS garantissent l'identification du serveur et la sécurité des données échangées entre un site web et un navigateur Internet dans une session chiffrée du protocole sécurisé HTTPS.

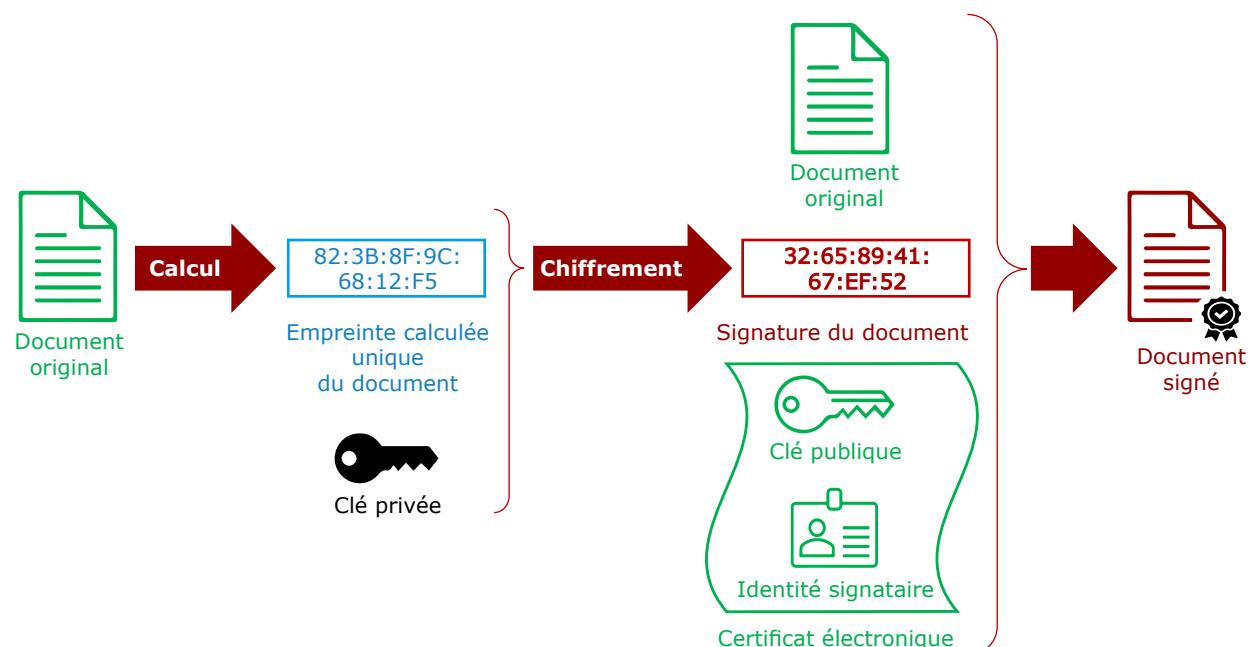
Dans le cas où un certificat ne doit plus être utilisé au cours de sa durée de vie, il est nécessaire de procéder à la révocation du certificat auprès de l'Autorité de Certification émettrice. Cela peut être le cas si le porteur a quitté l'entreprise au titre de laquelle le certificat avait été émis ou si le support du certificat a été perdu ou si la confidentialité de la clé privée est compromise.

Pour assurer la confiance dans les certificats électroniques, l'Autorité de Certification tient à jour la liste des certificats révoqués.

## Signature électronique d'un document

La signature électronique d'un document nécessite un certificat électronique contenant l'identité électronique du signataire et un logiciel de création de signature électronique.

Le processus de signature d'un document est le suivant :



L'empreinte digitale (ou Hash en anglais) est une courte chaîne de caractères hexadécimaux (par exemple, 64 caractères) calculée en appliquant un algorithme de « hachage », dit à sens unique sur le document. Deux documents qui diffèrent ne seraient-ce que d'un caractère auront deux empreintes complètement différentes.

La clé privée, associée au certificat électronique, est utilisée pour chiffrer l'empreinte, qui devient la signature du document d'origine. L'utilisation de la clé privée du signataire est protégée par un code PIN.

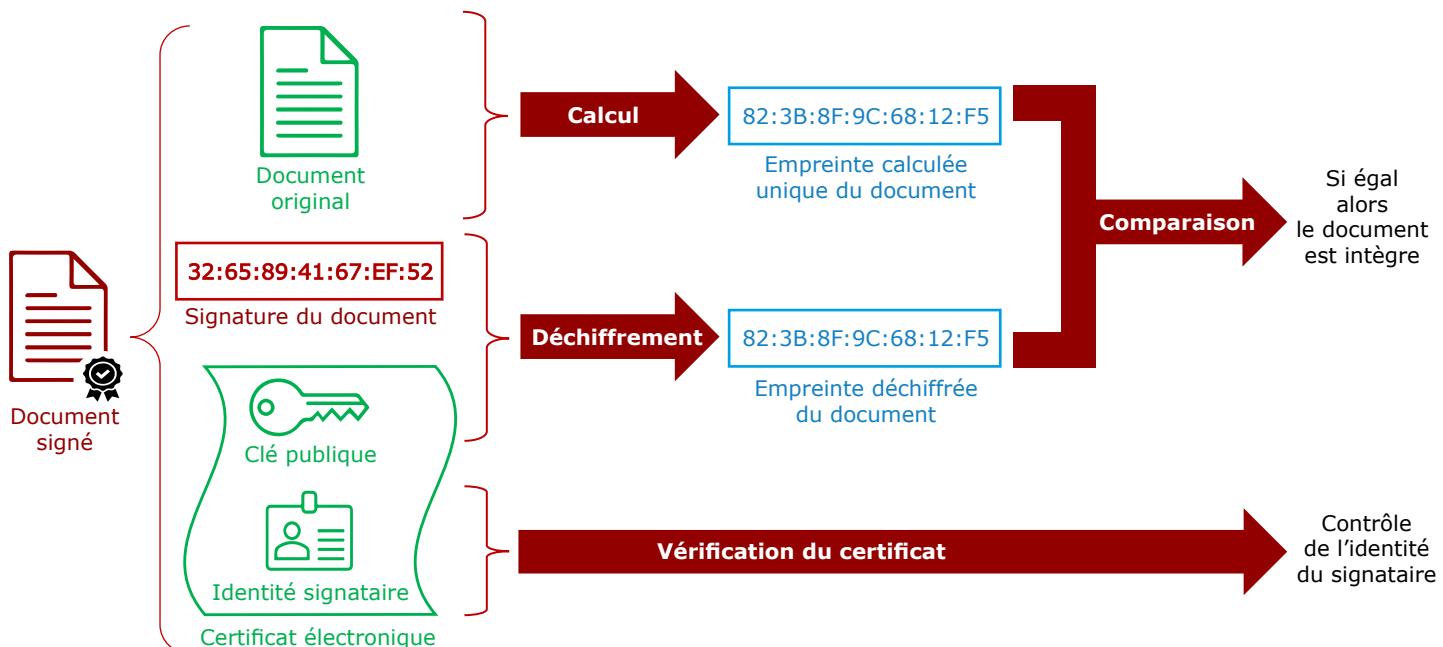
Au moment de la signature, un jeton d'horodatage avec l'heure et la date est ajouté afin que la date de signature ne puisse pas être contestée et de pouvoir vérifier ultérieurement que le certificat électronique n'était pas révoqué au moment de la signature.

Le document signé peut être dans un des trois formats suivants : PDF, XML ou binaire (CMS). Suivant le format choisi, la signature électronique peut être liée ou détachée du document.

# Vérification d'un document signé électroniquement

La lecture d'un document signé se fait dans un logiciel qui dispose des fonctions de lecture des certificats tel que : Adobe Acrobat Reader, Microsoft Office, les navigateurs Internet ou un client de messagerie électronique.

Le processus de vérification d'un document signé est le suivant :



La signature du document signé est « déchiffrée » par la clé publique du certificat électronique qui l'accompagne. La comparaison de l'empreinte recalculée du document et de cette signature « déchiffrée » permet de vérifier que le document n'a pas été modifié depuis sa signature.

La lecture du certificat électronique associé au document signé permet de contrôler l'identité du signataire.

## Niveaux de signature

La réglementation européenne sur l'identification électronique et les services de confiance pour les transactions électroniques favorise le développement d'un espace de confiance propice aux échanges et au commerce. Elle définit, dans le « règlement eIDAS », trois niveaux de signature électronique :

- la signature simple,
- la signature avancée,
- la signature qualifiée.

Ces niveaux de signature se distinguent par la sécurité de la démarche de vérification de l'identité du signataire et donc à la confiance que l'on peut accorder à la signature qui en résulte pour prouver l'identité de la personne qui a signé.

Le niveau « simple » est le niveau le plus courant dans lequel aucune garantie particulière n'est prise pour vérifier l'identité réelle du signataire. La signature manuscrite sur le terminal d'un livreur de colis, l'image numérisée de la signature manuscrite apposée dans un document ou la case à cocher utilisée pour accepter des conditions générales sont des exemples de signature simple.

Le niveau « avancé » est le niveau intermédiaire dans lequel :

- la signature est liée à son signataire de manière unique et claire,

- la signature permet d'identifier formellement le signataire, par exemple par la fourniture complémentaire d'une pièce d'identité,
- la signature est créée par des moyens sous le contrôle exclusif du signataire, tels qu'un smartphone, qui apportent une preuve supplémentaire de son consentement,
- la signature doit garantir que l'objet numérique signé ne pourra pas être modifié ultérieurement.

Pour réaliser une signature électronique de niveau « qualifié », il est nécessaire d'utiliser un certificat électronique de niveau « qualifié » qui est émis :

- par une Autorité de Certification qualifiée, faisant partie de la liste de confiance contrôlée par l'ANSSI dans le cas de la France,
- lorsque l'identité du signataire et sa preuve d'identité ont été vérifiées en face-à-face dans des conditions précises, que ce soit par une rencontre physique ou à distance par visioconférence.

Une signature électronique de niveau « qualifié » doit être créée à partir du certificat électronique qualifié par un dispositif sécurisé (QSCD) protégeant la clé privée et géré par un Prestataire de Service de Confiance qualifié.

## 16.2 Les éléments structurants

Le vocable « signature électronique » ne concerne que des personnes physiques. Pour la signature par des personnes morales ou de systèmes informatiques, il faut parler d'apposition de « cachets électroniques ».

 Un certificat électronique de signature électronique est lié à une personne physique désignée. Pour une société morale, le porteur est soit un représentant légal, soit une personne qui a reçu une délégation de pouvoir.

Une personne peut disposer de plusieurs certificats électroniques pour différents usages.

En cas de signature électronique de niveau simple ou avancé, la charge de la preuve de la fiabilité de la signature repose sur celui qui s'en prévaut.

Une signature de niveau simple peut facilement être répudiée par le signataire.

 L'effet juridique d'une signature électronique de niveau qualifié est équivalent à celui d'une signature manuscrite sur support papier dans tous les Etats membres de l'UE (Article 25 – 2 du règlement eIDAS).

La durée de validité du certificat électronique étant en général de 3 ans, il doit être renouvelé régulièrement. Les anciens documents signés restant sécurisés, sous réserve de maintien dans le temps des éléments de vérification de la signature électronique.

La force d'un chiffrement est liée à la taille de la clé : plus la clé est grande, plus le chiffrement est fort. Les nouveaux certificats ont des clés d'une longueur supérieure à 2048 bits.

## 16.3 Les particularités pour les notaires

La signature électronique de niveau « avancé » (niveau intermédiaire) est suffisante pour les compromis de vente immobilière, l'ouverture de services bancaires et les crédits.

La signature électronique de niveau « qualifié » est requise pour les Actes Authentiques Electroniques, les Actes Authentiques Electroniques à Distance et les Procurations Authentiques avec Comparution à Distance.

La clé REAL est un dispositif QSCD de niveau « qualifié » contenant plusieurs certificats électroniques (cf. chapitre « La clé REAL ») qui permettent de signer des documents et d'authentifier le notaire qui signe.

Dans le cas d'une Procuration Authentique avec Comparution à Distance, l'acte doit être signé électroniquement par le client puis par le notaire. La clé REAL permettant seulement la signature électronique du notaire, il est nécessaire de recourir, pour le client, à une solution externe qui propose une signature électronique de niveau « qualifié ».

## 16.4 Les bonnes pratiques

La clé privée associée à un certificat électronique et le code PIN qui la protège ne doivent pas être divulgués. Si tel est le cas, le certificat doit être révoqué.

- Pour vérifier une signature, il faut vérifier que les certificats n'étaient pas révoqués à la date de signature et que l'autorité qui a émis le certificat est légitime.

## 16.5 Les principales solutions du marché

Tous les Logiciels de Rédaction d'Actes agréés permettent de réaliser des Actes Authentiques Electroniques et des Actes Authentiques Electroniques à Distance entre deux offices en apposant la signature électronique du notaire instrumentaire grâce à sa clé REAL.

- Au 01/07/2021, pour les Procurations Authentiques avec Comparution à Distance des clients, la société DocuSign France est la seule à proposer une solution certifiée par l'ANSSI pour délivrer un logiciel QSCD permettant la signature électronique de niveau « qualifié » à distance par le client. L'Autorité d'Enregistrement associée est la société IDNow.

Cette liste de solutions peut évoluer dans le temps et sa version à jour est diffusée sur le portail REAL.

La solution DocuSign est accessible de manière intégrée à travers le LRA de la société Genapi ou au travers de la solution de la société Quai des Notaires, elle-même partenaire notamment de Fiducial.

## 16.6 Les critères de choix

Pour la signature d'un client dans une Procuration Authentique réalisée avec Comparution à Distance, il est recommandé de choisir la solution partenaire de son Logiciel de Rédaction d'Actes.

L'utilisation d'une solution comme DocuSign est payante.

## Le vocabulaire

**ANSSI (Agence Nationale de Sécurité des Systèmes d'Information)**: entité rattachée au Service du Premier Ministre et chargée d'une part de proposer les règles à appliquer pour la protection des systèmes d'information de l'État puis de vérifier l'application des mesures adoptées, et, d'autre part, et sensibiliser aux bonnes pratiques de sécurité information et de réagir aux attaques informatiques majeures en apportant son expertise technique.

**Autorité d'Enregistrement**: entité chargée de vérifier l'identité et la qualité des demandeurs de certificats électroniques. Ces informations seront inscrites dans le certificat électronique.

**Autorité de Certification**: tiers de confiance contrôlé par l'ANSSI qui délivre des certificats, gère leur cycle de vie (expiration, révocation...) et fournit les moyens de vérifier les certificats qu'il a délivrés. L'Autorité de Certification signe tout certificat qu'elle délivre avec sa clé privée pour garantir l'intégrité du certificat et la véracité des informations qu'il contient.

**Certificat électronique**: conteneur d'informations constitué d'une chaîne de caractères qui contient l'identité d'une personne physique, sa clé publique et les usages possibles du certificat. Un certificat est nominatif, infalsifiable, certifié par l'autorité qui le délivre et valable pour une durée maximale donnée.

**Chiffrage**: évaluation de la valeur de quelque chose. N'a donc aucun rapport avec la sécurité informatique.

**Chiffrement (« encryption » en anglais)**: opération de codage des données avec une clé numérique afin de les rendre incompréhensibles aux personnes qui n'ont pas la clé

**Clé**: nombre, en général codé sur 128 à 4096 bits, utilisé dans une opération cryptographique. Plus la longueur en bits de la clé est grande, plus les usages de la clé sont sécurisés contre le décryptage qui utiliserait une grande puissance de calcul (attaque par force brute).

**Crypter / Encrypter**: termes impropre (anglicisme) pour dire chiffrer.

**Cryptographie symétrique**: chiffrement basé sur le partage d'une clé secrète et utilisé dans des algorithmes, tels que AES, pour protéger la confidentialité des données ou des communications sur un réseau.

**Décrypter**: action de décodage d'un message sans posséder la clé de chiffrement eIDAS (Electronic Identification and Authentication Services): règlement de l'Union Européenne n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour accroître la confiance dans les transactions électroniques au sein du marché intérieur. Le règlement eIDAS définit une reconnaissance mutuelle des moyens d'identification électronique entre Etats membres et couvre l'authentification, les sceaux de signature, les services d'envoi en recommandé électronique et l'horodatage.

**PKI (Public Key Infrastructure ou Infrastructure à clés publiques)**: système à la fois technique et administratif de gestion de clés publiques pour signer et chiffrer des données et ainsi assurer la confidentialité, l'authentification, l'intégrité et la non-répudiation.

**PSCO (Prestataire de Services de Confiance)**: entité délivrant des services de confiance, tels que des signatures électroniques ou des cachets électroniques. L'entité peut être qualifiée au sens du règlement eIDAS et c'est alors un PSCQ (« Prestataire de Services de Confiance Qualifié ») pouvant délivrer des signatures électroniques de niveau qualifié.

**RGS (Référentiel Général de Sécurité)**: cadre réglementaire français révisé en 2014 pour la sécurité des services électroniques de l'Etat.

**SHA-2 (Secure Hash Algorithm 2)**: algorithme destiné à produire l'empreinte numérique d'un objet numérique. Il existe plusieurs versions (SHA-224, SHA-256, SHA-384, SHA-512) qui se distinguent par la longueur de l'empreinte produite pour rendre la signature plus résistante aux usurpations d'empreinte.

**QSCD (Qualified Signature Creation Device)**: dispositif qualifié de création de signature électronique qui assure la confidentialité des données et la sécurité de la procédure.

# 17. La clé REAL

## 17.1 Les concepts de base

La clé REAL est un dispositif matériel d'identité numérique de niveau « élevé » propre au notariat français qui ressemble à une clé USB.

Elle est constituée d'une puce, de type SIM téléphonique, et d'un support au format USB destiné à recevoir et lire la puce.

La clé REAL peut être utilisée sur tout ordinateur personnel sous Microsoft Windows qui dispose d'un port USB standard et des applications de la profession prévues pour l'utiliser.

La puce contient différents certificats électroniques (cf. chapitre « La signature électronique ») et les clés privées associées qui sont utilisés pour :

- s'authentifier lors de l'utilisation de certaines applications telles que MICEN, FCDDV, etc.,
- signer officiellement et électroniquement tout type de document, avec un niveau de sécurité « qualifié »,
- signer et chiffrer des Actes Authentiques Electroniques ou des copies authentiques, dans le cas du notaire, avec un niveau de sécurité « qualifié ».

La puce d'une clé REAL d'un notaire contient également une image de sa signature manuscrite et de son Sceau afin de les apposer sur les documents signés.

Chaque certificat, représenté par une chaîne de caractères spécifique, est infalsifiable car signé pour indiquer toute modification, nominatif car délivré à une seule personne, certifié par l'autorité qui le délivre, en l'occurrence le CSN, et valable pour une durée maximale donnée.

L'utilisation des données de la puce est sécurisée par un code PIN, personnel et confidentiel, composé à minima de 4 chiffres. Le code PIN est demandé par les applications de la profession à chaque utilisation de la clé REAL.

## Délivrance

Afin de répondre aux exigences de l'identité numérique, la clé REAL est délivrée personnellement par un mandataire de certification habilité lors d'un rendez-vous physique qui atteste l'identité du porteur.

Un mandataire de certification est :

- soit un notaire d'instance qui a reçu une délégation de certification du Président du CSN,
- soit un notaire d'office qui a reçu délégation de certification par un mandataire d'instance.

## Affectation

Chaque notaire et collaborateur doit avoir sa clé REAL personnelle liée à l'office dans lequel il exerce.

Les mandataires de certification disposent d'une clé REAL spécifique qui est liée à une instance.

Dans une société multi-offices :

- seul le notaire associé peut avoir une clé REAL pour valider les opérations relatives aux comptes de gestion de l'office,
- un collaborateur comptable ou clerc peut détenir plusieurs clés sous condition de pouvoir justifier d'un contrat de travail ou avenir l'autorisant à travailler dans chacun des offices.

## Utilisation

Pour être utilisée sur un poste de travail, la clé REAL a besoin des logiciels AWR et DXS qui doivent être installés localement.

Le logiciel AWR, inclus dans le pack de sécurité REAL, a pour rôle de sécuriser les échanges avec les applications distantes à l'aide des certificats de la clé REAL. Ainsi, lors de l'accès un service authentifié par la clé REAL, le logiciel AWR va demander la saisie du code PIN.

Le logiciel DXS permet de générer et valider des signatures électroniques.

## Applications liées

À la date du 01/07/2021, les applications suivantes ne sont utilisables qu'avec la clé REAL :

- ANF
- Casier Judiciaire
- Déclaration d'Activités Professionnelles (via la comptabilité de l'office)
- État Civil
- FCDDV
- Micen (via le Logiciel de Rédaction d'Actes)
- PACSen
- Portail banque en ligne de la CDC (ex : CDC Net)
- Portail des consentements
- Portail des CRIDON
- Safer
- Téléactes

## 17.2 Les éléments structurants

La clé REAL est un dispositif QSCD propre au notariat français qui permet des signatures électroniques de niveau « qualifié » par le notaire (cf. chapitre « La signature électronique »).

Une signature électronique de niveau « qualifié » sur un document électronique a la même force légale qu'une signature manuscrite sur un document papier.

Au 01/07/2021, la clé REAL d'un notaire contient 4 certificats visibles avec l'application AWP. Seuls 3 certificats sont utilisés. Le quatrième était prévu pour du chiffrement mais n'est plus utilisé.

La gestion des clés REAL (supports et puces) se fait via l'application Sacre accessible sur le site internet <https://sacre.real.notaires.fr>.

→ La puce de la clé REAL doit être renouvelée tous les 3 ans car les certificats qu'elle contient ont eux-mêmes une durée de vie de 3 ans.

## 17.3 Les particularités pour les notaires

Le support USB est acquis via Sacre indépendamment de la puce (cf. documentation de Sacre). La puce est délivrée gratuitement par courrier mais seulement après le face-à-face avec le mandataire pour respecter les conditions propres aux dispositifs de niveau « qualifié ».

Avant toute utilisation, la puce de la clé REAL doit être initialisée avec un code d'activation reçu en main propre lors d'un face-à-face.

La clé REAL peut se connecter sur n'importe quel port USB d'ordinateur personnel qui dispose des applications prévues pour l'utiliser.

La clé REAL du mandataire n'est pas utilisable pour accéder aux applications de l'office. Elle est réservée aux validations et révocations des autres clés.

La validation d'un Acte Authentique Electronique ne requiert que la signature électronique de niveau « qualifiée » du notaire à l'aide de sa clé REAL.

Dans le cas d'une Procuration Authentique réalisée avec Comparution à Distance, l'acte doit être signé électroniquement par le client puis par le notaire. La clé REAL permettant seulement la signature électronique du notaire, il est nécessaire pour le client de recourir à une solution externe qui propose une signature électronique de niveau « qualifié ».

## 17.4 Les bonnes pratiques

La clé REAL contient des certificats qui indiquent le propriétaire. L'utilisation de la clé REAL engage la responsabilité de son propriétaire.

→ La clé et son code PIN sont strictement personnels et confidentiels. Ils ne doivent être ni prêtés, ni divulgués à quiconque.

L'utilisation d'une clé REAL personnelle appartenant à un tiers relève de l'usurpation d'identité.

→ La clé REAL doit immédiatement être révoquée sur le site Internet Sacre dans les cas suivants :

- perte ou vol,
- blocage consécutif à trois saisies erronées successives du code PIN,
- changement de statut du titulaire,
- changement d'office, cessation d'activité, suspension, décès du titulaire.

## 17.5 Les principales solutions du marché

Seul le CSN, Autorité de Certification agréée par l'ANSSI, est habilité à délivrer des puces de clé REAL.

## 17.6 Les critères de choix

La clé REAL est un des fondements de l'utilisation des applications métier de la profession notariale.

La puce de la clé Real est gratuite. Seul le support USB est payant.

## Le vocabulaire

**AAED (Acte Authentique Electronique à Distance)** : Acte authentique électronique réalisé en visioconférence, avec un système agréé par le CSN entre plusieurs notaires officiant à distant depuis les offices respectifs, et établi en une seule séance.

**AWP (Authentic Web Pack)** : logiciel de gestion des certificats d'une clé REAL.

**AWR (Authentification Web REAL)** : logiciel inclus dans le Pack de sécurité REAL en remplacement de WebPass, installé sur le poste de travail pour servir de proxy et chiffrer avec la clé REAL les échanges entre les logiciels installés localement et les serveurs distants.

**Certificat électronique** : conteneur d'informations constitué d'une chaîne de caractères qui contient l'identité d'une personne physique et sa clé publique. Un certificat est nominatif, infalsifiable, certifié par l'autorité qui le délivre et valable pour une durée maximale donnée.

**Mandataire de certification** : personne ayant pouvoir par délégation du Président du CSN d'autoriser une demande de certificat en identifiant le demandeur.

**PIN (Personal Identification Number)** : code confidentiel de sécurité à 4 chiffres destiné à authentifier le porteur et assurer la confidentialité des clés privées.

**Procuration Authentique avec Comparution à Distance** : Procuration notariée sous forme électronique réalisée en visioconférence, avec un système agréé par le CSN, entre un notaire et une ou plusieurs parties à distance dont l'identité est vérifiée, et validée à l'aide d'un procédé de signature électronique « qualifié ».

**WebPass** : ancien logiciel de sécurisation des flux vers les serveurs métier et remplacé par AWR.

# 18. La sécurité informatique

## 18.1 Les concepts de base

La sécurité informatique a pour objectifs d'assurer :

- la confidentialité des données gérées dans les applications,
- l'intégrité des données, c'est-à-dire l'impossibilité de modifier les données sans autorisation,
- la disponibilité des données et des systèmes (matériels ou applications) qui les gèrent,

face à un risque d'accident, de défaillance technique, d'erreur humaine ou de malveillance.

Comme toute démarche de sécurité, la sécurité informatique est contraignante mais vitale pour la pérennité des activités.

« *La sécurité est toujours considérée comme excessive, jusqu'au jour où elle ne suffit pas* »  
(W.H. Webster, ex-Directeur du FBI).

Pour atteindre ces objectifs, la sécurité s'appuie pour plusieurs approches complémentaires :

- des bonnes pratiques, telles que le règlement RGPD pour les données des personnes, les normes ISO 2700x pour la sécurité générale, le règlement eIDAS pour la signature électronique, la norme PCI DSS pour les cartes bancaires,
- l'authentification, qui va demander à un utilisateur ou un système d'apporter des preuves de son identité avant tout accès,
- la traçabilité, qui va maintenir des traces des différentes manipulations sur les données afin de pouvoir les retrouver, les imputer voire prouver leur existence (non-répudiation) ou les annuler,
- le chiffrement, qui va coder les données afin de les rendre inutilisables par des tiers qui n'auraient pas la clé de lecture,
- la sauvegarde des données, qui va assurer qu'il existe une copie saine et récente des données pour les reconstituer en cas d'altération,
- les tests de sécurité et de continuité, qui visent à éprouver si les mesures prises pour la sécurité sont efficaces et si la continuité de fonctionnement est bien assurée.

## Analyse des risques

Toute organisation, petite ou grande, connue ou discrète, est exposée à des risques pour son système d'information.

Une démarche de sécurisation du système d'information, telle que décrite dans la norme ISO 27005, consiste à évaluer l'ensemble des menaces sur chacun des éléments (matériel, logiciel, humain...) dans son contexte (matériel, logiciel, humain, environnement...) puis apporter des mesures de protection préventive pour réduire l'exposition aux risques.

L'analyse doit tout d'abord identifier les activités indispensables au fonctionnement et les données « sensibles » : données dont la perte ou la divulgation pourraient causer un préjudice élevé.

Les risques les plus importants sont ensuite déterminés par la règle suivante : menace (notée de 1 à 5) avec probabilité forte de survenir X impact (noté de 1 à 5) fort en cas de survenue.

En commençant par les éléments les plus vitaux ou sensibles et les risques forts, les mesures de sécurité informatique doivent réduire la menace ou réduire son impact.

## Stratégie de sécurisation

En lien avec l'analyse des risques, la stratégie de sécurisation peut viser à empêcher toute interruption de l'activité, notamment pour les activités sensibles ou vitales, et/ou à réduire le temps d'indisponibilité des systèmes en cas de sinistre.

La principale méthode pour assurer la disponibilité des systèmes informatiques, donc la continuité des activités métier, est de doubler les systèmes (redondance matérielle et logicielle, double site), voire les humains. Cela entraîne bien sûr un coût élevé.

La principale méthode pour assurer la reprise en cas de sinistre est la sauvegarde informatique.

## Principal facteur de risque

Il est habituel d'entendre que « le facteur de risque n°1 est entre la chaise et le clavier », c'est-à-dire l'humain : méconnaissance de la technique par les utilisateurs, comportements à risque, erreur d'inattention, maladresse, laxisme dans l'application des règles, malveillance interne, piratage, manipulation extérieure par « ingénierie sociale », etc.

Pour assurer la sécurité informatique, différentes mesures techniques de sécurité peuvent être mises en œuvre de manière préventive. Cependant l'attention à l'humain est capitale et permet d'améliorer significativement le niveau de sécurité : explication des règles, a minima dans la charte informatique, sensibilisation aux bonnes et aux mauvaises pratiques, définition de procédures avec double contrôle, séparation des comptes d'accès et des droits, blocage des pratiques interdites, contrôle régulier de l'application des règles, tests en conditions réelles et audits.

## Prévention

Les mesures de sécurité doivent être mises en œuvre de manière préventive :

- dès la conception d'un système (« security by design ») : développement d'une application avec contrôle des accès par mot de passe, chiffrement des échanges de données, séparation de deux fonctions essentielles, création d'un journal des modifications...
- lors de l'installation : mise en place d'un matériel doublé pour assurer la redondance, choix de câbles réseaux distincts, installation d'une sauvegarde...
- lors de la configuration : création de groupes d'utilisateurs avec des droits différents, interdiction de certains types d'accès, définition de mots de passe forts...
- à l'utilisation : changement régulier de mot de passe, protection des sauvegardes de données, limitation de l'utilisation des droits d'accès à privilège (administrateurs), contrôle régulier du respect des règles de sécurité définies, mise à jour régulière des applications...

## Menaces classiques

MENACE	RISQUE	EXEMPLE DE MESURES DE PRÉVENTION
Incendie, inondation	Destruction complète du système d'information	<ul style="list-style-type: none"><li>• Préparation d'un plan de continuité d'activité</li><li>• Répartition des serveurs sur plusieurs sites</li><li>• Sauvegarde informatique quotidienne hors des locaux avec capacité de restaurer la sauvegarde</li><li>• Analyse régulière des risques</li></ul>

Panne matérielle	Equipement indisponible	<ul style="list-style-type: none"> <li>Supervision régulière du matériel</li> <li>Installation du matériel dans une zone protégée</li> <li>Matériel en réserve pour redondance passive</li> <li>Matériel doublé avec redondance active</li> <li>Souscription de contrat de maintenance matérielle</li> </ul>
Vol ou perte de matériel	Perte des données	<ul style="list-style-type: none"> <li>Sauvegarde régulière des données</li> <li>Contrôle des accès par mot de passe fort</li> <li>Chiffrement des disques durs</li> <li>Chiffrement des clés USB avec un mot de passe</li> <li>Outil d'effacement à distance</li> </ul>
Vol de données	Fuite de données confidentielles	<ul style="list-style-type: none"> <li>Filtrage des accès réseaux</li> <li>Journalisation des accès</li> <li>Changement régulier des mots de passe</li> <li>Suppression des données avant mise au rebut du matériel</li> <li>Restriction des extractions de données</li> <li>Sensibilisation des collaborateurs</li> </ul>
Virus, faille logicielle	Atteinte aux données	<ul style="list-style-type: none"> <li>Antivirus à jour sur les serveurs et postes de travail</li> <li>Mise à jour des versions logicielles</li> <li>Sensibilisation des collaborateurs aux événements suspects</li> </ul>
Modification des matériels ou logiciels	Atteinte aux applications	<ul style="list-style-type: none"> <li>Restriction des accès physiques aux matériels</li> <li>Blocage des accès d'administration depuis Internet</li> <li>Contrôle des accès logiques aux logiciels</li> <li>Suppression des droits d'administration sur les postes de travail pour les utilisateurs</li> <li>Attribution de droits d'accès limités</li> <li>Changement régulier des mots de passe</li> </ul>
Consultation ou modification de données sensibles	Atteinte aux données	<ul style="list-style-type: none"> <li>Inventaire des données sensibles</li> <li>Séparation des tâches et des droits d'accès</li> <li>Vérification régulière des droits accordés</li> </ul>
Personne clé indisponible	Processus indisponible	<ul style="list-style-type: none"> <li>Doublement des personnes affectées à un rôle</li> <li>Conservation sous enveloppe scellée au coffre-fort des mots de passe d'administrateur</li> </ul>
Erreur de manipulation	Altération des données	<ul style="list-style-type: none"> <li>Sauvegarde quotidienne des données sur un média rapide d'accès</li> <li>Rappel de formation aux utilisateurs</li> </ul>

## Sauvegardes

La sauvegarde informatique est la base de la remise en état du système d'information après un sinistre.

Une sauvegarde contient, sur un média spécifique, une copie des logiciels, des applications installées et des données.

Pour être utilisables, les sauvegardes doivent être complètes, récentes, accessibles, identifiables, lisibles et rapides à restaurer. Il faut donc y porter une grande attention.

## 18.2 Les éléments structurants

Un matériel ou un logiciel non maîtrisé peut faire office de cheval de Troie pour faire entrer des logiciels malveillants ou pour accéder de manière illégitime à des ressources accessibles sur un réseau local.

Lorsque les smartphones permettent l'accès au système d'information, ils doivent être sécurisés comme des postes de travail.

La protection de la plupart des systèmes contre les accès indésirables est basée sur une authentification par identifiant et mot de passe.

- Un mot de passe est propre à un système/usage et un identifiant.
- Les comptes d'administration sont les comptes racines qui permettent de gérer un système et de créer d'autres comptes d'utilisateurs. La perte d'un mot de passe d'administration peut entraîner la perte du système.

Sur un serveur hôte, chaque composant logiciel (système d'exploitation, base de données, application...) est en général doté d'un compte d'administration spécifique.

Chaque personne qui utilise un système doit avoir un identifiant propre afin que son action soit traçable et imputable.

Les correctifs de sécurité sont en général intégrés dans les mises à jour de logiciel.

- Les serveurs physiques et les postes de travail, les applications et les données critiquent doivent être sauvegardés quotidiennement et automatiquement selon les procédures opérationnelles communiquées par le fournisseur des applications dans la documentation d'exploitation.

Les sauvegardes sont en général effectuées la nuit afin de ne pas perturber les utilisateurs, de ne pas avoir de modifications en cours pendant la sauvegarde et d'avoir une « photographie » des données à un moment connu. En cas de perte de données pendant la journée, la situation pourra être restaurée à la veille au soir, entraînant la perte des activités enregistrées pendant cette journée.

## 18.3 Les particularités pour les notaires

Les offices notariaux gérant des données sensibles et des fonds financiers importants, ils sont des cibles exposées aux risques et aux attaques.

Tous les matériels et applications métiers utilisés dans un office doivent être sécurisés préventivement et sauvegardés régulièrement : serveur physique, routeur, serveur de fichiers partagé, comptabilité notariale, Logiciel de Rédaction d'Actes, CRM, GED, messagerie...

L'ensemble des notaires et collaborateurs doit être sensibilisé régulièrement à la sécurité.

Les notaires doivent surveiller le maintien des mesures de sécurité.

Il faut veiller à garder en lieu sûr les clés REAL qui participent à l'authentification des notaires.

Les clés REAL, comme les mots de passe, ne se prêtent pas.

## 18.4 Les bonnes pratiques

### Réduction des risques

- Une analyse rapide de la tolérance aux pannes et des risques affectant la continuité d'activité peut être menée en se posant deux questions pour chaque élément (matériel, logiciel, réseau, humain) : « que se passe-t-il si cet élément est complètement indisponible quelle que soit la cause ? » puis « combien de temps faut-il pour remplacer l'élément indisponible ? ».

Seuls les matériels connus et sécurisés doivent être connectés au réseau local, que ce soit par un câble Ethernet ou par une connexion Wifi ou par une connexion nomade.

Pour limiter les menaces basées sur du Phishing (cf. chapitre « La messagerie électronique »), il ne faut pas ouvrir une pièce jointe ou cliquer sur un lien web dans un message électronique provenant d'un émetteur inconnu ou qui semble bizarre. « Dans le doute, abstiens-toi ».

Une technique classique d'infiltration dans un ordinateur est de laisser traîner une clé USB infectée. En cas de découverte d'une clé USB perdue, il ne faut surtout pas la connecter à un poste de travail pour « voir ce qu'il y a dessus ».

Sachant que 20% des attaques informatiques se font par l'intermédiaire des prestataires, il faut veiller à appliquer des règles de sécurité strictes et des contrôles vis-à-vis des prestataires et des moyens techniques qu'ils utilisent : interconnexions, modes d'interventions, traçabilité, données partagées, mots de passe, contrats, procédures d'audit, etc.

Les droits d'accès accordés à une personne doivent être cohérents avec son rôle et non son statut.

### Mot de passe

Lorsqu'une session est inutilisée pendant 5 minutes, elle doit se mettre en veille automatiquement et demander un mot de passe pour être réouverte.

Les mots de passe utilisés doivent être complexes (minimum 8 caractères majuscules, minuscules, chiffres et caractères spéciaux), changés régulièrement et différents pour chaque usage.

- Les mots de passe configurés par défaut par les fournisseurs doivent être modifiés.

Les mots de passe doivent être différents entre les systèmes, même si l'identifiant est identique.

- Les mots de passe d'administrateur des systèmes appartiennent à l'organisation et non à une personne. Ils doivent tous être sauvegardés régulièrement sous enveloppe scellée dans un coffre-fort hors de locaux pour permettre la mise en œuvre d'un plan de reprise en cas de sinistre.

Si quelqu'un demande la communication d'un mot de passe pour intervenir, il faut refuser par défaut, sauf si c'est vraiment nécessaire, auquel cas il faut changer le mot de passe avant et après l'avoir communiqué.

Les navigateurs internet proposent souvent par défaut d'enregistrer les mots de passe saisis. Cette pratique est déconseillée car cela revient à supprimer le contrôle d'accès.

Pour créer un mot de passe complexe facile à retenir, il suffit de créer une longue phrase et de saisir la première lettre de chaque mot. Par exemple « Je suis un bon notaire depuis 15 ans spécialisé en droit immobilier » donnera le mot de passe fort « Jsubnd15asedi », qui est facile à mémoriser par la phrase associée mais difficile à capter par quelqu'un qui le verrait saisi en direct sur un clavier et difficile à attaquer par la méthode du dictionnaire.

Face à la multiplication des mots de passe à gérer, il est possible de se simplifier la vie en utilisant un gestionnaire de mot de passe, comme « KeePass Password Safe ».

## Journal

Quand elle est possible, la journalisation des connexions aux applications doit être activée.

Les fichiers de journalisation doivent être purgés régulièrement parce qu'ils grossissent vite et qu'ils contiennent souvent des données personnelles soumises au RGPD. Cette action doit être décrite dans la documentation d'exploitation d'un système fournie par son concepteur.

## Mises à jour

→ Les versions des logiciels et applications doivent être mises à jour régulièrement afin de bénéficier des correctifs de sécurité.

Les postes de travail et les serveurs physiques doivent être équipés d'un antivirus à jour (logiciel et fichier des signatures de virus).

## Sauvegardes

Les sauvegardes peuvent être de plusieurs types à la fois pour répondre à plusieurs usages : sur disque proche du système sauvegardé pour une restauration rapide, sur un système spécifique pour une restauration complète et l'externalisation du média, en ligne pour une bonne accessibilité, déconnectée pour éviter leur effacement ou leur cryptage lors d'une cyber-attaque...

→ Au moins une sauvegarde doit être identifiée clairement et conservée, déconnectée, hors du site où est situé le système sauvegardé et non dans un coffre-fort, même ignifugé, dans les locaux ; en effet, en cas d'incendie, la sauvegarde serait au mieux inaccessible dans les décombres ou, au pire, fondue.

Les sauvegardes contiennent toutes les données du serveur. Elles sont soumises au RGPD. Il faut veiller à leur confidentialité, par des procédures de manipulation adaptées, des mesures de chiffrement, des contrats de confidentialité avec les sous-traitants qui les manipulent...

La capacité à restaurer les sauvegardes doit être testée régulièrement : identification aisée du média de sauvegarde à une date donnée, relecture du média, non saturation du média, exhaustivité des informations nécessaires à la restauration, restauration complète ou partielle possible, ancienneté des données, temps de restauration raisonnable...

De plus en plus, des solutions de sauvegardes sont disponibles dans le Cloud, comme OneDrive de Microsoft, Google Drive, Dropbox. Ces solutions doivent être utilisées avec précaution car la localisation et la confidentialité des données ne sont pas garanties. De plus, le périmètre sauvegardé avec ces solutions est souvent incomplet.

## 18.5 Les principales solutions du marché

Il existe plusieurs catégories de logiciels de sécurité informatique pour ordinateurs, telles que : les antivirus, les logiciels de détection de portes dérobées (« anti-rootkits »), les logiciels de détections de logiciels malveillants (« anti-malware »), les logiciels de recherche de vulnérabilités (services mal configurés, mots de passe faibles...).

Les solutions gratuites sont souvent des déclinaisons, aussi efficaces mais limitées aux fonctionnalités antivirus, des suites de sécurité payantes des mêmes éditeurs.

Pour les réseaux, il existe deux grandes catégories de solutions de sécurité pour les usages classiques : classiques :

- les firewalls (pare-feu) qui bloquent certains accès entre un réseau externe et un réseau interne,
- les proxys qui relaient les requêtes entre deux ordinateurs situés sur des réseaux différents pour tracer, anonymiser et contrôler les requêtes.

Les méthodes de sauvegardes des applications notariales sont proposées par les éditeurs de ces applications.

## 18.6 Les critères de choix

Les investissements dans les mesures de sécurité sont déterminés par :

- le coût financier direct lié à un sinistre : perte d'exploitation consécutive à l'indisponibilité des systèmes, achat de nouveau matériel, recours à des experts, pénalité du RGPD consécutive à une atteinte aux données personnelles,
- les conséquences indirectes : temps passé à rétablir le fonctionnement nominal, suivi juridique, perte d'image et de réputation, perte de clientèle.

→ La durée maximale d'interruption admissible pour une activité doit être évaluée afin de définir la stratégie de sécurisation des systèmes utilisés par cette activité.

Pour accélérer la restauration des sauvegardes, notamment en cas de perte de données par erreur de manipulation, une sauvegarde de premier niveau sur média rapide, comme un disque, est à privilégier. Une sauvegarde complète et délocalisable reste cependant nécessaire.

## Le vocabulaire

**Cheval de Troie** : logiciel en apparence légitime mais qui contient une fonctionnalité malveillante qui permet des actions à distance.

**Cybersécurité** : néologisme tendance pour désigner la sécurité des systèmes de toute sorte à base de technologies informatiques ou électroniques : systèmes d'information, objets connectés, robotique, réseaux, etc.

**Documentation d'exploitation** : document fourni par le fournisseur d'un système et qui décrit l'ensemble des tâches techniques et procédures à réaliser régulièrement pour maintenir ce système en conditions opérationnelles.

**Journal (ou « Log file » en anglais)** : fichier contenant les enregistrements horodatés des évènements relatifs à un système.

**Plan de continuité** : document stratégique, formalisé, régulièrement mis à jour et testé, de planification de la réaction à un sinistre grave afin d'assurer le fonctionnement sans interruption, éventuellement en mode dégradé, d'une organisation. Le Plan de Continuité d'Activité (PCA) traite de l'activité dans son ensemble. Le Plan de Continuité Informatique (PCI) traite de la continuité du Système d'Information.

**Plan de reprise**: ensemble des procédures documentées, régulièrement mises à jour et testées, permettant à une organisation de reprendre ses activités après une interruption consécutive à un sinistre grave. Le Plan de Reprise d'Activité (PRA) traite de la reprise de l'activité dans son ensemble. Le Plan de Reprise Informatique (PRI) traite de la reprise du Système d'Information.

**Porte dérobée (ou Backdoor)**: fonctionnalité inconnue de l'utilisateur d'un logiciel légitime ou d'un matériel, qui donne un accès distant et secret à son logiciel. Le logiciel peut alors être utilisé par un tiers pour accéder aux données locales ou pour des usages malveillants.

**PSSI (Politique de Sécurité des Systèmes d'Information)**: document qui regroupe l'ensemble des règles de sécurité à adopter pour maintenir la sécurité de l'information d'une organisation

**SMSI (Système de Management de la Sécurité de l'information)**: ensemble de politiques concernant la gestion de la sécurité de l'information. La norme ISO 27001 est un SMSI.

**Système d'information**: ensemble des ressources (matériel, communication, logiciel, humain) qui permettent de collecter, stocker, traiter et distribuer l'information dans une organisation.

**Virus**: programme conçu pour se propager dans les logiciels légitimes d'un ordinateur à l'insu de son utilisateur. Un virus est activé soit lors de l'exécution locale, par un utilisateur, d'un programme dans un objet contaminé (logiciel téléchargé, fichier comportant des macros, email piégé, clé USB avec exécution automatique à la connexion, code exécutable contenu dans une page d'un site internet), soit par l'exploitation de failles de sécurité. Le virus peut affecter le système d'exploitation, un logiciel, un navigateur internet, un site internet, etc. dans le but d'espionner, récupérer des données, nuire à l'ordinateur ou bloquer pour extorquer de l'argent (« ransomware »).



Conseil Supérieur du Notariat  
60 boulevard de la Tour-Maubourg  
75007 Paris  
01 44 90 30 00

Direction du Numérique et  
des Systèmes d'Information