NATHAN HATTAB
CONSULTANT EN SYSTEMES D'INFORMATION
EXPERT EN INFORMATIQUE PRES LA COUR D'APPEL DE PARIS
ET LES COURS ADMINISTRATIVES D'APPEL DE PARIS ET DE VERSAILLES
54 RUE JULIETTE SAVAR
94000 CRETEIL

AUDIT DU RESEAU PRIVE VIRTUEL AVOCATS (RPVA)

09/06/2010

Rapport d'audit

réalisé à la demande de Monsieur A.J.M. POUCHELON,

Président de la Conférence des Bâtonniers

TELEPHONE : 01.49.80.34.06. - TELECOPIE : 01.49.80.34.07. - E-MAIL : Nathan.Hattab@Wanadoo.fr"

SOMMAIRE

1 LA MISSION D'AUDIT, LES ACTEURS ET LE CONTEXTE

1.1 CONTEXTE ET OBJECTIFS

1.1.1 METTRE EN ŒUVRE LA CONVENTION ENTRE LE MINISTERE DE LA JUSTICE ET LE CNB

Le Ministère de la Justice et le Conseil National des Barreaux (CNB) ont signé une convention le 4 mai 2005 puis le 28 septembre 2007. Elle porte sur « *le système de communication entre les Juridictions et les cabinets d'avocats pour la consultation du dossier informatique et l'échange sous format électronique des données utiles à la gestion des procédures civiles et pénales* ». « *L'ensemble des fonctionnalités des systèmes est conforme au droit positif* » et « *les systèmes de communication instaurés sont conçus pour s'adapter aux évolutions procédurales* ».

Elle désigne le CNB comme responsable de l'opération du « réseau privé virtuel avocats» raccordant les avocats aux juridictions. Ce réseau est désigné par la suite comme « RPVA ».

1.1.2 CNB EXPLOITE, MAINTIENT, FAIT EVOLUER E-BARREAU ET SECURISE SON ACCES

Conformément aux dispositions de la convention avec la Chancellerie, le CNB a organisé un point d'accès unique aux greffes des tribunaux de grande instance et des cours d'appel de France, qui résulte d'une suite d'analyses et de décisions.

Les 19 et 20 mars 2004, le Conseil National des Barreaux a examiné un rapport sur la messagerie et l'accès Internet sécurisé pour les avocats.

Son paragraphe introductif était le suivant :

« L'informatique et l'Internet sont parties intégrantes de la vie quotidienne des avocats et les professionnels que nous sommes ne peuvent, à titre individuel, qu'être tous impliqués à terme dans ces nouvelles technologies.

La mission de nos instances représentatives, au premier rang desquelles se place le Conseil National des Barreaux, est de promouvoir l'accès d'un maximum, sinon de la totalité de nos confrères, aux nouvelle technologies, et ce en raison de la nécessité d'éviter en ce domaine une sorte de fracture sociale qui serait une fracture technologique.

La nature de nos activités, la confidentialité des éléments qui nous sont confiés par les clients, nos principes déontologiques devraient cependant appeler à une vigilance extrême.

Le Conseil National des Barreaux entend insister pour que les avocats obtiennent de leurs prestataires des assurances techniques afin de protéger efficacement le flux d'informations sensibles que véhiculent leurs messageries électroniques.

Il réfléchit, par ailleurs, avec tous les acteurs de la profession, aux solutions utiles à notre communauté professionnelle ».

Dans le droit fil de cette première délibération, le Conseil National des Barreaux a décidé, à l'occasion de son assemblée générale des 10 et 11 décembre 2004, de doter la profession d'un véritable intranet, de façon à pouvoir répondre collectivement à l'ensemble des besoins (connus ou susceptibles de se révéler) liés à l'exercice de la profession,

Les conséquences techniques de ces choix politiques ont également été prises en considération, comme le montre l'extrait du procès-verbal :

- «*Option 1 : Un accès sécurisé aux données disponibles sur le serveur Web du Conseil National [extranet cnb.fr en https + certificats]. Cette solution répond de manière restreinte (accès Web uniquement) au cahier des charges de la Chancellerie. Les autres types d'échanges électroniques relevant de chaque avocat*
- *Option 2 : Un internet professionnel et sécurisé [réseau RPVA + extranet cnb.fr + certificats]. Cette solution repose sur une infrastructure de sécurité collective et globale pour tous les échanges Internet professionnels (emails, Web, accès nomades, échanges inter-applications).*

L'assemblée générale du Conseil a adopté à la majorité des voix l'architecture technique du RPVA option 2.»

Les engagements contractuels pris par le Conseil National des Barreaux vis à vis du Ministère de la Justice pour l'interconnexion avec le RPVJ, imposent de respecter un haut niveau de sécurité et un interlocuteur unique garant/responsable de l'ensemble des accès "avocat".

C'est en fonction des orientations rappelés ci-dessus et en adéquation avec les différents besoins de services exprimés par la profession que le Conseil National des Barreaux a élaboré la solution proposée aux avocats.

Cette solution est matérialisée dans une plateforme e-Barreau qui permet à un avocat de consulter l'état de ses dossiers, et de réaliser des actes de procédure de façon électronique.

Pour sécuriser l'authentification de l'avocat aux services d'e-Barreau, le CNB a mis en place une authentification forte assurée par un certificat protégé par un code Pin et stocké sur un cryptoprocesseur.

Le transport est sécurisé par un cryptage point à point via Https authentifié par le certificat. Un deuxième niveau de sécurité est mis en œuvre puisque le flux Https est encapsulé dans des tunnels VPN reliant le réseau local du cabinet d'avocat au frontal d'e-Barreau.

Pour la mise en œuvre de ces tunnels VPN, le CNB a pris l'option de déployer des boitiers « firewall-VPN » mis au point par la société NAVISTA.

1.1.3 3 SOLUTIONS MISES EN AVANT POUR LA SECURISATION DE L'ACCES

Remarquant que la solution du CNB induit un coût pour la collectivité des avocats de plusieurs millions d'Euros, le Barreau de Paris a proposé une architecture plus légère, maintenant un niveau de sécurité élevé, mais répondant principalement à la fonction accès au service e-Barreau.

L'utilisation du VPN comme surcouche de sécurité n'a donc pas été adoptée par le Barreau de Paris.

Le Barreau de Marseille a adopté une démarche comparable à celle du CNB, tout en s'appuyant sur la mutualisation du boitier « firewall-VPN » NAVISTA.

CNB.COM – DEPLOYER LE RESEAU NAVISTA DANS TOUS LES CABINETS

CNB a pris l'option de déployer un réseau privé virtuel au sein de tous les cabinets d'avocats. Le réseau est réalisé par des boitiers NAVISTA. Outre le chiffrement, les boitiers ont aussi vocation à assurer la sécurisation des réseaux locaux des cabinets et ouvrir l'accès à des télé-services adaptés aux exigences de sécurité des avocats.

PARIS – LA CONVENTION N'IMPOSE QUE LE HTTPS ET LE CERTIFICAT

Le Barreau de Paris estime que la sécurisation par HTTPS et authentifié par un dispositif à cryptoprocesseur est largement suffisante. C'est le dispositif historique qui est exploité au sein du Barreau avec le greffe du TGI de Paris.

Le Barreau de Paris a obtenu un accès spécifique à e-Barreau pour les avocats parisiens, qu'il a intégré à son bouquet de services.

MARSEILLE – UNE ALTERNATIVE ECONOMIQUE A LA SECURISATION PAR NAVISTA

Le Barreau de Marseille a pointé en 2009 le coût important de l'option prise par le CNB et ses limitations en termes de mobilité. Elle a développé une plateforme d'accès à e-Barreau sécurisant l'accès par des technologies Cisco. Le principe même de l'accès permet l'accès nomade.

Compte tenu des exigences du CNB en matière de connexion à e-Barreau, Marseille a connecté son concentrateur CISCO au RPVA en passant par un boitier RSA qu'elle a ainsi mutualisé.

1.2 AUDIT TECHNIQUE ET ECONOMIQUE POUR ECLAIRER LA CONFERENCE DES BATONNIERS

1.2.1 MISSION D'AUDIT

Le Président de la Conférence des Bâtonniers a désigné un expert pour :

- Auditer techniquement et économiquement la solution du CNB
- Auditer techniquement et économiquement la solution du Barreau de Marseille
- Recueillir les informations techniques et économiques de la solution du Barreau de Paris

Le Président a demandé à l'auditeur de prendre en compte dans ses questionnaires, les éléments qu'il estime utile de retenir de la grille d'évaluation technique du CNB.

Cette grille porte notamment sur :

- Les pré-requis techniques et la politique de licence.
- La sécurité de la liaison,

- L'accès sécurisé à des télé-services,
- La sécurité du réseau local du cabinet et des accès internet.

1.2.2 DEMARCHE D'AUDIT

Elle a consisté à :

- Comprendre le contexte, les acteurs, les enjeux
- Positionner le débat, les arguments de chacun et leurs fondements
- Présenter les éléments de fait collectés et des premières conclusions aux principaux acteurs interviewés
- Élaborer le rapport d'audit avec les points forts, les points faibles et les recommandations
- Traduire les objectifs de l'audit en points d'audit
- Identifier les sites à visiter, les acteurs à interviewer et collecter la documentation
- Comprendre le contexte général du milieu professionnel
- Visiter des cabinets d'avocats dotés du boitier NAVISTA et conduite des interviews
- Rencontrer les promoteurs de chacune des trois solutions et conduire les interviews
- Présenter pour validation les éléments de fait collectés
- Élaborer un rapport d'audit intermédiaire
- Elaborer le rapport définitif après recueil des observations du mandant

1.2.3 EQUIPE D'AUDIT

Directeur de mission : Nathan Hattab, Consultant en systèmes d'information, Expert près la Cour d'Appel de Paris et les Cours Administratives d'Appel de Paris et de Versailles.

Consultant : Philippe Aymar, Consultant en systèmes d'information, Expert près la Cour d'Appel de Paris et les Cours Administratives d'Appel de Paris et de Versailles.

1.2.4 ORIENTATIONS

L'audit s'est déroulé en s'appuyant sur les thèmes d'analyse et de réflexion suivants :

- Les acteurs
  - Le CNB, CNB.COM et NAVISTA
  - Le Barreau de Paris
  - Le Barreau de Marseille
- L'analyse
  - Les positions respectives sur l'accès sécurisé aux services d'e-Barreau, concepts et fondements,
  - La sécurité de liaison et de l'authentification,
  - La sécurité des échanges électroniques
  - La sécurité des cabinets et des travailleurs nomades
  - Le développement de nouveaux services sécurisés
  - La dépendance à NAVISTA
- Comparatif et analyse critique

- Aspects économiques
- Sécurité informatique
- Intégration dans les cabinets, prise en compte par les prestataires informatiques
- Maitrise contractuelle

- Conclusions

1.3 LES ACTEURS

1.3.1 CNB, CNB.COM ET NAVISTA

CNB.COM

Le CNB – Conseil National des Barreaux représente la profession des avocats auprès de la Chancellerie.

Il a signé en 2005 puis en 2007 une convention avec la Chancellerie qui permet aux avocats la consultation du dossier informatique et l'échange, sous format électronique, d'informations utiles à la gestion des procédures civiles et pénales.

Le CNB a pris l'engagement de mettre en œuvre l'infrastructure et les mesures pour garantir la fiabilité de l'identification des avocats parties à la communication électronique, l'intégrité des documents adressés, la sécurité et la confidentialité des échanges ainsi que l'établissement avec certitude de la date d'envoi et celle de réception des éléments échangés.

Le CNB a opté dans un premier temps pour un accès Internet haut débit (ADSL) comme le montre l'extrait du PV d'AG des 27 et 28 avril 2007 :

« *Techniquement la solution qui a été retenue propose aux avocats un accès Internet haut débit (ADSL), une messagerie électronique sécurisée consacrant l'identification « avocat-conseil », une certification forte avec authentification de la qualité d'avocat et un outil de signature électronique spécifique de la profession.*

Elle a entrainé la signature par le Conseil National des Barreaux d'un contrat avec France Télécom pour une durée de trois ans (mai 2005 à mai 2008) et dont les coûts fixes, de l'ordre de 300 k€ par an, sont seuls pris en charge par le Conseil (…)

Le déploiement de l'offre RPVA, lancée à l'occasion de la convention de Marseille, s'est avérée complexe compte tenu d'un certain nombre de contraintes techniques (unicité et changement du FAI impliquant des coupures d'accès sauf à disposer de deux lignes distinctes, etc..) qui ont considérablement compliqué la mise en place du réseau dans les cabinets. »

Les difficultés rencontrées avec l'accès Internet haut débit (ADSL) ont conduit le CNB à opter pour une autre solution comme le montre l'extrait du PV de l'AG des 14 et 15 septembre 2007 :

« Le dossier a connu ces derniers temps une importante accélération en raison du changement d'opérateur par le Conseil National et de la pros en charge du chantier par la Caisse des dépôts qui met à la disposition du ministère de la justice des moyens financier, techniques et humains.

L'objectif annoncé par la Chancellerie est 'équipement de tous les TGI au 1er janvier 2008 au rythme de trois juridictions par jour à compter du 1er octobre prochain.

(…)

Il s'agit donc d'un challenge monumental pour la profession qui dispose de trois mois pour finaliser ce projet et équiper les barreaux.

Le Conseil National a travaillé pour se faire sur une modification de l'offre technique d'e-barreau. Il a ainsi fait choix de la société NAVISTA qui propose un boitier électronique sans obligation pour le cabinet de changer d'opérateur et de nom de domaine. Cette solution technique qui se greffe sur le réseau informatique du cabinet, avec le même niveau de sécurité, permet de connecter autant de poste que l'on veut et n'impose aucun changement d'adresse de messagerie. »

Le CNB a alors confié à l'association à vocation nationale, CNB.COM, la charge de

- Maintenir la plateforme technique e-Barreau,
- Déployer l'architecture NAVISTA (frontal à Rennes et boitiers RSA dans les cabinets d'avocats) pour l'accès au service e-Barreau,
- Assurer le support utilisateur pour les clés e-Barreau et les boitiers RSA (niveau 0 seulement),

CNB.COM a opté pour une fiscalité qui permette aux avocats de se faire rembourser la TVA sur les prestations refacturées par CNB.COM, et notamment celles de NAVISTA et de CertEurope.

CNB.COM a signé en 2007 avec la société NAVISTA une convention qui définit un modèle économique bâti sur

- la location mensuelle des boîtiers RSA par NAVISTA à CNB.COM, organisme national,
- le support et la maintenance des boitiers déployés chez les avocats,
- l'attribution à NAVISTA de la garantie du monopole des accès à e-Barreau assortie de la garantie d'une quantité minimum de boitiers. Le monopole est formé par « *l'exclusivité de la fourniture des services de liaison sécurisée de type TCP/IP – XDSL à l'exclusion de celles transportant le protocole IP en mode MPLS aux services RPVA* » des échanges entre les cabinets d'avocats et le serveur e-Barreau.

Un accord a été trouvé en 2009 pour autoriser la sortie du Barreau de Paris du dispositif et revoir les engagements prix-volumes pour la location à NAVISTA des boitiers RSA.

NAVISTA

NAVISTA est une société d'une dizaine de personnes implantée à PERPIGNAN. Elle conçoit, déploie et administre des solutions réseaux sécurisées. Elle est certifiée ISO 9001 depuis mars 2006 et elle est composée de :

- un service de recherche et développement qui définit les boitiers, développe les logiciels embarqués dans les boitiers et les solutions de contrôle centralisé (NCC),

- un service support avec trois niveaux, le premier niveau règle les questions simples, le second permet de répondre aux questions techniques en particulier des installateurs de boitiers, le troisième prend en charge les corrections d'applicatif et est porté par le service recherche et développement,
- un service de montage, de paramétrage, de tests et vérification, et d'expédition des boîtiers RSA vers les cabinets d'avocats
- une salle de serveurs comportant les serveurs de tests et de développement ainsi que le serveur qui héberge l'application de contrôle centralisé des boitiers.

Outre le Réseau Privé Virtuel des Avocats, NAVISTA a deux autres références dans le monde de la Justice, les cabinets de notaires d'Ile de France pour lesquels elle déploie un réseau privé virtuel, et l'administration pénitentiaire à laquelle elle propose des terminaux « client léger » à destination des détenus en fin de peine.

NAVISTA est consciente de l'impact potentiel de son organisation sur la sécurité du RPVA et des cabinets d'avocats qui y sont connectés, à la fois par la qualité de ses développements et par la capacité que lui donne son centre de contrôle NCC. Elle envisage d'engager une certification ISO 27001. Son site est d'ailleurs en voie de sécurisation renforcée puisque outre le site de badge de contrôle d'accès, elle fait clôturer le périmètre immédiat de son immeuble dont elle est la seule occupante.

LA VISION CNB, CNB.COM ET NAVISTA POUR LE RPVA

Le CNB voit le RPVA comme un réseau privé qui sanctuarise les cabinets d'avocats évoluant au sein d'Internet. D'abord conçu pour assurer la communication sécurisée avec le serveur d'e-Barreau, le RPVA est vu comme le canal de communication sécurisé des avocats avec leurs confrères et leurs partenaires.
La sécurité est assurée par des communications chiffrées, par le déploiement de routeurs-firewall-chiffreurs qui en contrôle les accès à Internet des cabinets, par la contractualisation de services adaptés aux exigences de sécurité des avocats et par le contrôle centralisé des boitiers par CNB.COM, acteur issu de la profession et au service de la profession.
Les points clés de cette organisation sont :

- Une liaison sécurisée entre le cabinet d'avocats et les greffes des juridictions,
- L'utilisation d'une messagerie sécurisée pour les échanges des avocats avec les tiers,
- La sécurisation du réseau local du cabinet et des travailleurs nomades
- L'ouverture de services numériques sécurisés tels que Visio-conférence, télé-sauvegarde, filtre de contenu,…
- Un partenariat avec un prestataire de qualité, NAVISTA, reconnu dans le monde de la justice

1.3.2 LE BARREAU DE PARIS

LE PRECEDENT E-GREFFE

Le Barreau de Paris représente le 1er Barreau de France avec 40% des avocats de France et 80% du CA des avocats de France,

Il avait déjà mis en place en 2003 un accès aux serveurs du TGI de Paris, appelé e-Greffe et reposant sur l'utilisation d'un certificat sur clé USB intégrant un cryptoprocesseur. Le Barreau de Paris passe par l'autorité de certification CertEurope pour la gestion et la fourniture de ces clés.

Le service e-Barreau du CNB a repris les principales fonctionnalités du service e-Greffe qui a été abandonné, et remplacé par le nouveau service.

Relevant à la fois les contraintes apportées par le RPVA et la performance sécuritaire de l'infrastructure déjà en place à Paris, le Barreau de Paris a négocié un accord avec le CNB et NAVISTA, pour connecter sa plateforme dédiée aux avocats parisiens au serveur e-Barreau. Ainsi, les avocats parisiens peuvent se connecter à e-Barreau grâce à leur seul certificat sur clé USB et n'ont pas besoin de s'équiper du boitier NAVISTA.

Ainsi, le Barreau de Paris propose donc un accès au service e-Barreau et n'estime pas nécessaire que l'ensemble des avocats appartiennent à un même réseau privé virtuel, il a créé un précédent montrant que l'accès sécurisé à e-Barreau était possible sans passer par l'architecture à base de boitiers NAVISTA.

LA VISION DE PARIS

L'organisation mise en place par le Barreau de Paris repose sur une plateforme d'accès aux différents services du Barreau de Paris. La sécurité de cette plateforme est assurée par :

- Une authentification par certificat support physique,
- Un chiffrement par HTTPS,
- Un dispositif de supervision de la plateforme d'interconnexion,
- La validation de la plateforme d'interconnexion par des tests d'intrusions effectués par un acteur indépendant.

La plateforme a été adaptée pour intégrer e-Barreau à la gamme de services offerts.

e-Barreau a été adapté pour que la plateforme parisienne puisse relayer l'authentification initiale de l'avocat par sa clé et qu'e-Barreau puisse reconnaitre cette authentification qui émane d'une autorité de certification différente de celle utilisée par le CNB.

Pour fonctionner, cette organisation ne nécessite que l'installation d'un pilote logiciel pour que la clé 'Paris' soit reconnue sur le poste de travail.

Pour le reste, elle ne nécessite pas d'autre adaptation, ni de l'ordinateur, ni du réseau local. HTTPS et les certificats étant pris en charge par l'ensemble des navigateurs du marché.

Le Barreau de Paris n'envisage pas d'autres dispositions. Il considère que pour la messagerie relative aux échanges des avocats avec les tiers, le niveau de sécurisation des services internet grand public est suffisant. Si nécessaire, des offres d'hébergement dédiées de type « Exchange » ou autre foisonnent.
S'agissant de la sécurisation du réseau local des cabinets et des travailleurs nomades :

- Les « gros » cabinets d'avocats ont déjà sécurisé leur réseau local avec des couches de pare-feu et savent se procurer des services de filtrage s'ils l'estiment nécessaires
- La sécurité des petits cabinets par les « box Internet » est suffisante.

Quant à l'ouverture de services sécurisés, le Barreau de Paris rappelle que le marché est très dynamique et propose déjà des télé-services avec un niveau de sécurité suffisant pour les avocats. Il estime que la définition d'une offre dédiée aux avocats par le CNB n'aura pour effet que de créer des monopoles, donc de réduire le rapport qualité/prix offert à l'utilisateur. Si ces services peuvent avoir un intérêt parce qu'ils facilitent leur appropriation pour l'avocat, ils ne doivent pas être imposés.

1.3.3 LE BARREAU DE MARSEILLE

LE BARREAU DE MARSEILLE

Le Barreau de Marseille représente le 3ème Barreau de France, avec 5% des avocats de France.

Il a conçu et mis en place une solution à base de matériels et de logiciels CISCO permettant un accès distant et sécurisé (VPN) au boitier RSA du Barreau de Marseille. Cette solution a été hébergée par un infogérant à Vénissieux.

A un moment où la solution NAVISTA était critiquée pour son coût (55€ HT/mois) et l'impératif d'être au cabinet pour se connecter, la solution CISCO qu'il a mis au point, permet l'accès des avocats à e-Barreau pour au plus 2€ par mois et depuis n'importe quel point connecté à Internet.

Compte tenu des réticences du CNB à ouvrir de nouveaux accès au centre de Rennes, le Barreau de Marseille a connecté sa plateforme CISCO au RPVA en passant par un boitier RSA NAVISTA mutualisé.

En avril 2010, NAVISTA a décidé d'arrêter le fonctionnement de la solution du Barreau de Marseille, en bloquant les adresses IP utilisées par l'infogérant à Vénissieux.

LA VISION DE MARSEILLE

L'organisation mise en place par le Barreau de Marseille est basée sur les règles suivantes :

La liaison sécurisée avec les greffes repose sur le protocole HTTPS avec authentification par certificat support physique. Le flux HTTPS est lui-même crypté au sein d'un tunnel VPN établi depuis le poste de l'avocat jusqu'au serveur frontal CISCO.

La sécurité est assurée par :

- Une première authentification par la clé USB délivrée par le CNB sur le frontal CISCO,
- Un cryptage du flux passant par Internet au sein d'un tunnel VPN Cisco puis d'un tunnel VPN NAVISTA,
- Une deuxième authentification sur le serveur e-Barreau par la clé USB du CNB.

Marseille rappelle que les accès ADSL grand public sont fournis par les FAI (Fournisseurs d'Accès Internet) avec des routeurs-firewall intégrés et que les postes de travail depuis Windows XP SP2 (2004) sont maintenant sécurisés par des firewalls locaux.

L'avocat n'est donc pas dépendant du bon fonctionnement de son boitier RSA et de son accès internet cabinet, lorsqu'il est en mobilité.

Rappelant que la sécurité est avant tout une affaire de dispositions organisationnelles et compte tenu du niveau élevé de sécurisation déjà apporté au grand public, elle estime ainsi que la sécurisation du réseau local apportée par le RSA est superflue, sinon redondante avec les dispositifs déjà en place au sein de quelques groupements.

Quant à l'ouverture de services sécurisés, le marché propose des solutions sécurisées sur des architectures plus légères que celle de CNB NAVISTA

2 L'ANALYSE

2.1 LA SECURITE DE LA LIAISON ET DE L'AUTHENTIFICATION

Les analyses respectives développées se présentent succinctement comme suit :

2.1.1 CNB

Le protocole HTTPS avec certificat support physique n'est pas suffisant, pour assurer la sécurité optimale des échanges sur Internet.

Le protocole VPN NAVISTA introduit un niveau de chiffrement supplémentaire pour se protéger contre les attaques visant à décrypter le flux. Il permet aussi de restreindre l'exposition du frontal NAVISTA de Rennes qui se limite aux seuls accès de type NTS (NAVISTA Transport System).

Le principe du VPN plutôt qu'HTTPS a été retenu dès novembre 2004 par le CNB par un vote de son assemblée générale.

2.1.2 PARIS

Le protocole HTTPS avec certificat physique représente l'état de l'art sur les services sensibles des professionnels dans l'économie de l'Internet, et il est suffisant. Le chiffrement autorisé est de 256bits et de 128 bits pour HTTPS, en fonction des navigateurs des postes des avocats.

L'introduction d'un niveau de chiffrement supplémentaire du VPN, n'apporte pas de valeur ajoutée significative parce que l'ensemble des correspondances avec les partenaires du cabinet est relayé en clair sur internet et que le Conseil constitutionnel n'impose pas plus de sécurité. Le code de procédure pénale mentionne aussi les communications par courriels sans signaler de procédure de chiffrement.

2.1.3 MARSEILLE

Le protocole HTTPS avec certificat physique représente l'état de l'art sur les services sensibles dans l'économie de l'Internet, et il est suffisant.

Puisque selon le CNB, il est indispensable d'introduire un niveau de chiffrement supplémentaire du flux par VPN, Marseille encapsule aussi le flux Https dans un flux VPN. Elle maintient aussi que les solutions VPN du marché sont préférables économiquement à des solutions VPN propriétaires, pour une sécurité équivalente.

2.1.4 ECLAIRAGE DES AUDITEURS

En premier lieu, l'architecture des solutions examinées est décrite dans l'annexe 1 du présent rapport.

LE CHIFFREMENT A 128 BITS EST SUFFISANT

Le niveau de chiffrement n'est pas critique dans la protection des échanges numériques. Le chiffrement de base de HTTPS est à 128 bits, et l'ANSSI[1] estime que ce niveau résistera aux attaques en forces brutes jusqu'en 2020 minimum. Pour une utilisation au-delà de 2020, la taille minimale des blocs des mécanismes de chiffrement par bloc est de 128 bits.

Les nouveaux algorithmes AES permettent de mettre en œuvre des chiffrements à 256 bits sans pénaliser les performances logicielles. Ce niveau de chiffrement devrait se généraliser dans les années à venir.

LE CERTIFICAT EST LA CLE DE LA SECURITE D'HTTPS

La limite reconnue des communications HTTPS est leur exposition aux attaques de type « Men in the middle », dans lesquelles un attaquant arrive à s'intercaler dans la communication pour fonctionner comme répéteur et ainsi accéder à l'ensemble des flux.

L'utilisation de l'authentification par certificat permet de se protéger contre cette attaque et complique la tâche de l'attaquant qui doit aussi s'insérer dans la liaison avec l'autorité de certification.

Aussi, si l'autorité de certification surveille correctement ses logs, elle est capable de détecter des intrusions et de réagir pour renouveler les clés concernées et alerter la vigilance des administrateurs concernés.

LE VPN APPORTE UNE SECURITE SUPPLEMENTAIRE PARCE QU'IL INTRODUIT UN DEUXIEME NIVEAU D'AUTHENTIFICATION

Le VPN apporte une deuxième façon de mettre en place la séquence de chiffrement et un deuxième dispositif de supervision de la liaison.

Dans ce contexte, le VPN apporte effectivement un plus en sécurité, parce qu'il donne une deuxième opportunité de déjouer ou détecter une attaque.

Le VPN mis en place par Marseille n'a qu'un intérêt réduit parce qu'il utilise la même authentification que le HTTPS et que l'algorithme de chiffrement (SSL) est similaire.

---

[1] ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information publie notamment « Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques »

L'utilisation des clés NAVISTA, si elles sont bien gérées, renforcent effectivement la sécurité, puisqu'elle impose au pirate de tromper un système qui est bien indépendant.

L'UTILISATION D'UN PROTOCOLE PROPRIETAIRE N'EST PAS GARANTIE DE SECURITE

L'ANSSI rappelle dans ses « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques », version 1.20 du 20/01/2010 (RGS_B_1), les règles qu'un processus de chiffrement doit respecter. Elles n'ont rien de trivial et un certain nombre d'algorithmes ne les respectent pas.

Ces règles concernent toutes les étapes, de la génération des clés jusqu'aux algorithmes de chiffrement.

Des protocoles réputés sécurisés tels que « OpenVPN », n'ont progressé que par leur exposition aux regards de tous.

Le protocole NTS de NAVISTA a fait l'objet d'une déclaration mais n'a pas encore été soumis à la certification. Tant que cette certification n'a pas été obtenue, son intégrité doit être abordée avec précaution.

CASSER UNE LIAISON HTTPS AVEC UN CERTIFICAT REPRESENTE UN GROS EFFORT ET LAISSE DES TRACES

Même si le protocole HTTPS avec certificat encapsulé dans un VPN authentifié par un mécanisme indépendant représente le « must de la sécurité », il ne faut pas considérer pour autant que HTTPS avec certificat est une solution faible.

1) Une attaque laisse des traces, au minimum sur les serveurs de l'autorité de certification.

2) Une attaque nécessite plusieurs jours de préparation pour tromper le routeur du client ou le serveur DNS auquel il répond. Son exécution nécessite un niveau d'expertise élevé.

3) Prolonger la session après la désactivation du certificat est encore plus difficile, aussi l'attaque cesse lorsque le certificat est débranché.

A ce niveau de technicité, un pirate peut être tenté d'attaquer le serveur ou le poste client plutôt que d'attaquer la liaison. Ce point sera abordé dans la partie relative à la sécurité du poste de travail et du réseau local.

2.2 LA SECURITE GLOBALE DES ECHANGES ELECTRONIQUES

2.2.1 CNB

Le CNB considère que l'obligation des avocats de protéger la confidentialité des dossiers confiés par leurs clients devrait les conduire à disposer :

- de flux chiffrés avec les serveurs de mails,
- des mails stockés sur des serveurs sécurisés, soit en interne, soit chez un prestataire de confiance.

Le serveur « avocat-conseil.fr » répond à ces deux préoccupations, même si cette adresse courriel n'est pas imposée. L'accès à partir du cabinet se fait par le VPN NAVISTA et les mails sont conservés sur un serveur qui est contrôlé par la profession. En cas d'injonction à communiquer des documents, le Bâtonnier concerné sera informé.

2.2.2 PARIS

80% des échanges de mails des avocats sont faits avec les clients et les confrères, et ne sont pas couverts par la messagerie « avocat-conseil.fr »

La messagerie « avocat-conseil .fr » court-circuite les noms de domaine des cabinets d'avocats qui en ont un (80% du chiffre d'affaires de la profession).

Les accès depuis des PDA à la messagerie « avocat-conseil.fr » restent non chiffrés.

Le Barreau de Paris considère aussi que les solutions gratuites comme Gmail et les Google Apps offrent des niveaux de sécurité suffisants :

- Flux cryptés SSL
- Historique des accès sur le site
- Obligation de conformité à la loi américaine et sanction du marché, sont plus efficaces qu'un monopole

La question de savoir si les sociétés françaises doivent ou non utiliser des services fournis par des sociétés américaines n'est pas d'actualité pour le Barreau de Paris.

Finalement, quelque soit l'hébergeur, la protection des correspondances d'avocats s'applique.

2.2.3 MARSEILLE

Pour la sécurité des échanges électroniques par un cabinet d'Avocat, le Barreau de Marseille estime que la sécurité de sa liaison et l'authentification de l'avocat par la clé USB délivrée par le CNB sont conformes aux textes en vigueur.

S'agissant de la sensibilisation des Avocats pour une meilleure réflexion sur ce que devrait être la sécurité globale d'un cabinet informatisé, le Barreau de Marseille estime que l'action doit être

nationale et pédagogique et l'imposition du boitier NAVISTA ne constitue en rien la sécurisation générale et souhaitable d'un cabinet, outre qu'elle n'est pas pédagogique.

Le Barreau de Marseille propose de sensibiliser les avocats de son Barreau par des cycles de formation si aucune action nationale n'est entreprise.

2.2.4 ECLAIRAGES DES AUDITEURS

LA SECURISATION DES COURRIERS ELECTRONIQUES DE LA PROFESSION PAR L'ADRESSE (PRENOM).(NOM)@AVOCAT-CONSEIL.FR EST CONFRONTEE A DE NOMBREUX OBSTACLES

La sécurisation des courriers électroniques nécessite que l'ensemble des correspondants soit pris en charge par le dispositif de communication.

Le serveur avocat-conseil.fr accédé via le RPVA ne prend en charge qu'une partie des correspondants :

- Les politiques de marque des cabinets, les font communiquer par des adresses attachées aux cabinets, et le serveur avocat-conseil.fr ne prend en compte qu'une partie des mails,
- Les courriers des avocats concernent un ou plusieurs acteurs qui sont en dehors du RPVA et en dehors du domaine avocat-conseil.fr,
- Les accès par PDA et Smartphone se généralisent et ne sont pas pris en charge par le RPVA (pas de client NAVISTA sur les iPhones, Blackberry, et autres) et sont contraints de passer par des protocoles non sécurisés,
- Les cabinets d'avocats parisiens n'ont pas adoptés les boitiers NAVISTA,

Compte tenu de la diversité des acteurs concernés et de leur parc informatique, seul un standard de marché semble réaliste et, pour les échanges de courriels sécurisés, il n'y en a pas qui se dégage.

LES CABINETS D'AVOCATS PEUVENT DEJA DISPOSER DEJA D'UNE SECURITE EQUIVALENTE A AVOCAT-CONSEIL.FR

L'analyse des niveaux de sécurité qui s'imposent aux courriers des avocats n'a pas été faite au préalable par la profession.

A minima, un cabinet doit s'assurer que les mails qu'il stocke sont conservés dans de bonnes conditions de sécurisation. Cette sécurité passe par des dispositions organisationnelles et pour la partie technique par :

- L'hébergement chez un tiers de confiance,
- L'échange crypté avec le serveur.

Les cabinets qui sont suivis par un prestataire informatique ont pour la plupart des serveurs de mails hébergés au cabinet ou sur une plateforme contrôlée par leur prestataire. Les autres passent par des services grand-publics, affichés sous leur nom de domaine, ou sous la marque du prestataire.

Les hébergeurs publics (wanadoo, free.fr, gmail, hotmail, yahoo, etc.) ou mutualisés (OVH, etc.) proposent tous des accès chiffrés. Ils intègrent des services d'antivirus et d'antispam plus ou moins performants, et assurent une surveillance étroite de la sécurité de leurs installations. De plus ces services ayant une grande audience, les anomalies sont vite remontées et prises en compte (ex. débat récent sur les procédures de récupérations de mot de passe).

Ces services ont des niveaux de sécurité équivalents à ce que propose le CNB. Ils ne sont pas tous hébergés en Europe et peuvent soulever des difficultés relevant de l'intelligence économique et de la protection des données personnelles. Les avocats qui s'estiment concernés par cette problématique devront la prendre en compte dans le choix de leur hébergement.

Compte tenu des observations précédemment faites sur les accès à avocat-conseil.fr, il convient de souligner que cette messagerie est en marge de l'architecture RPVA puisqu'elle est également accessible depuis Internet. Il s'agit d'une solution Sun iplanet hébergée par Orange BS.

LES PLATES-FORMES COLLABORATIVES OFFRENT LA POSSIBILITE DE CREER DES ESPACES D'ECHANGES POUR DES EQUIPES PROJET

Des solutions peuvent toutefois être adoptées au cas par cas et selon la criticité des dossiers. Elles peuvent passer par des plateformes collaboratives dédiées, éventuellement sécurisées par l'utilisation de clés de chiffrement, l'utilisation d'un deuxième facteur d'authentification (SMS, clé USB, cryptoprocesseur, « calculatrice » générateur de code,…).

Ce type de plate-forme se généralise (ex. Google Apps, Soho, BaseCamp, etc.) Elles utilisent pour la plupart des niveaux de sécurité de type Https simple. Elles posent aussi la problématique du stockage hors Europe lorsque des considérations d'intelligence économique ou de protection des données personnelles s'appliquent.

Certains prestataires proposent des plateformes collaboratives hébergées sur leurs serveurs ou sur des serveurs mutualisés, et construites à partir de suites propriétaires (SharePoint) ou libres (Zimbra).

Les conditions de sécurité de ces plateformes auraient intérêt à être évaluées en attendant la mise en place d'une plateforme dédiée aux avocats par le CNB.

2.3 LA SECURISATION DU RESEAU LOCAL DU CABINET ET DU TRAVAILLEUR NOMADE

2.3.1 CNB

La convention entre le Ministère de la Justice et le Conseil National du Barreau de 2007, et les négociations en cours pour sa refonte, font apparaître des obligations en la matière pour la profession des avocats.

Compte tenu du nombre des avocats individuels et des difficultés qu'ils rencontrent pour régler cette question, le CNB a visé une solution RPVA basée sur un boitier RSA qui apporte une offre accessible à tous pour un haut niveau de sécurité.

D'autre part, le CNB responsable de la sécurité des accès à e-Barreau, considère qu'elle doit passer par des dispositifs de chiffrement pour les échanges et la sécurisation des points d'accès au RPVA. A ce titre, il est indispensable que ces points d'accès au RPVA soient situés derrière des firewalls.

Le déploiement de boitiers RSA au sein de chaque cabinet est la seule façon qu'à le CNB de s'assurer que les points d'accès sont bien sécurisés.

2.3.2 PARIS

La question de la sécurité des cabinets d'avocats doit être abordée globalement en termes d'organisation et de déontologie, et non pas seulement en matière d'outil et de technique.

2.3.3 MARSEILLE

Le Barreau de Marseille considère que les systèmes grand public (Freebox, Livebox, etc.) intègrent déjà un firewall et que, si un niveau supplémentaire devait être imposé, les prestataires infogérants des cabinets d'avocats savent mettre en place des solutions incluant pare-feu et VPN avec des équipements du commerce (Fortinet, Netasq ; Harpoon, Cisco,…) dont le coût est sans comparaison avec celui du boitier NAVISTA.

De plus, depuis Windows XP, toutes les versions de Windows intègrent un firewall et rappellent la nécessité d'un antivirus.

2.3.4 ECLAIRAGE DES AUDITEURS

LE FIREWALL PROTEGE DES ATTAQUES FRONTALES, L'UTILISATION DU VPN RENFORCE LA SECURITE APPORTEE PAR LE FIREWALL

Le firewall limite l'exposition du réseau local à Internet. Il n'expose aux requêtes provenant d'Internet que les machines qui ont été prévues à cette fin (serveur mail, serveur collaboratif, serveur Citrix, serveur TSE par exemple). Il est nécessaire que la sécurité des machines exposées à Internet soit adaptée et tenue à jour.

Lorsque les accès passent par un VPN, le firewall introduit une étape d'authentification préalable à l'accès au réseau local et ajoute une couche de protection à ces services. Le paramétrage de ce mode d'accès doit s'accompagner d'un ajustement de la gestion des droits sur le réseau local. C'est une opération délicate qui nécessite l'intervention d'un professionnel.

LE VPN CONTRIBUE A SECURISER LES ACCES NOMADES

L'avocat qui se connecte par un accès Wifi grand public n'est pas assuré d'être sur un réseau local amical. Le principe de reconnecter l'avocat à un réseau local sécurisé (son cabinet) par un tunnel VPN apporte dans ce cas précis un gain de sécurité appréciable une fois que le VPN est activé. Les risques ne sont pas pour autant évacués (phase préalable à l'activation du VPN par exemple). Il faudra compléter ce dispositif technique par des consignes aux utilisateurs nomades pour :

- Les stratégies de choix des points d'accès grand public,
- L'activation des paramètres de sécurité renforcée du poste de travail dans les lieux publics (disposition activées par défaut sur Windows à partir de la version Vista)

L'utilisation de clé 3G est une alternative pour l'accès sécurisé. L'isolation faite par l'opérateur assure à l'utilisateur d'être dans un environnement amical.

LA SECURITE PAR LE FIREWALL EST LIMITEE

La sécurité est une préoccupation importante qui est largement prise en compte par les acteurs du marché qui déploient des solutions de sécurisation à tous les niveaux.

La conséquence est double :

- les gains apportés par la technique seule sont déjà mis en œuvre par les technologies grand public et les gains résiduels sont à rechercher dans l'éducation des acteurs et l'application de règles organisationnelles,
- les pirates développent des techniques qui court-circuitent les dispositifs de contrôle par firewall et antivirus.

Les techniques actuelles d'attaque passent par l'intégration de contenu malveillant dans les documents (en ce moment, 50% des attaques relayées par document le sont par les PDF) et l'intégration de contenu malveillant dans des sites internet malveillants ou parfois même dans des sites «bienveillants » mais faiblement sécurisés.

Les contenus malveillants intègrent des mécanismes de diffusion et sont complétés par des campagnes d'appâtage (phishing, scams, etc.).

Le firewall NAVISTA offre, dans sa configuration actuelle, une protection limitée contre ces attaques, qui exploitent l'utilisateur comme moyen d'accès aux failles. Lorsque le filtrage de contenu sera mis en place, il aura la possibilité d'agir sur ce risque. Ces fonctions et leur tarification ne sont pas encore connues et ne peuvent pas être évaluées.

LA SECURITE EST UNE PREOCCUPATION ORGANISATIONNELLE

Ainsi le cabinet qui souhaiterait optimiser sa sécurité aurait à mettre en place des règles organisationnelles sur l'accès aux mails, sur l'importation de contenu provenant d'internet et sur une surveillance de ses installations. Il aurait intérêt à se rapprocher d'un prestataire informatique qui

l'assisterait dans la définition de ces règles organisationnelles et leur implémentation dans l'organisation informatique du cabinet.

Les composants techniques qui entrent en jeu sont la gestion des droits d'accès sur les ressources du réseau local et leur gestion centralisée par un contrôleur de domaine.

Cette opération nécessite l'intervention d'un prestataire informatique.

COMPTE TENU DU MODE D'ADOPTION DU FIREWALL NAVISTA PAR LES PRESTATAIRES INFORMATIQUES, TOUTE DEMARCHE DE SECURISATION DE L'ORGANISATION COURT-CIRCUITE LES FONCTIONS DE SECURITE DU BOITIER NAVISTA

Nous avons vu ici que le dispositif Firewall-VPN mis en œuvre par NAVISTA est limité s'il n'est pas complété par l'intervention d'un prestataire informatique.

Nous avons observé que les prestataires informatiques court-circuitent fréquemment les fonctions de sécurité du firewall NAVISTA pour leur préférer un équipement de sécurité standard sur lequel ils ont la totale maitrise et ils ont développé une expertise.

La position des prestataires informatiques s'explique en partie par le fait que le firewall NAVISTA n'a pas encore reçu de certification émanant d'une autorité indépendante, même si la carte utilisée dans le boîtier NAVISTA est certifiée. D'autre part, il n'est pas anormal que sans directive précise, ils préfèrent des équipements notoires ou des équipements avec une certification internationale de type Critères Communs, ITSEC ou française comme celle de l'ANSSI (CSPN – Certificat de sécurité de premier niveau).

De plus, un firewall est un équipement complexe à régler. Il n'est pas anormal que les prestataires se spécialisent sur un ou deux équipements, et que leur choix se porte sur des appareils du marché qu'ils maîtrisent.

LE FIREWALL NAVISTA A UN INTERET POUR LES PETITES STRUCTURES

Dans ce contexte, le boitier NAVISTA présente un intérêt pour les petits cabinets d'avocats qui souhaitent disposer d'un accès distant et sécurisé à leur serveur de fichier.

Compte tenu du morcellement de la profession, les petits cabinets représentent de l'ordre de 70% des déploiements.

Du fait des offres de stockage distant disponibles actuellement sur le marché (voire télé-sauvegarde), il est probable que seule une partie de ces cabinets seront concernés.

Nous ne disposons pas d'évaluation de la sécurité des box Internet, aussi il est difficile de prendre position sur ce sujet. La situation mériterait d'être précisée, en commandant un comparatif à un prestataire spécialisé.

En ce qui concerne les boitiers routeurs du commerce, ils offrent des fonctions de sécurité satisfaisantes, mais nécessitent d'être maintenus (1 ou 2 patchs par an) par un prestataire. Les petits

cabinets ne disposent pas de compétence pour réaliser ces opérations. S'ils adoptaient une telle solution, il faudrait prévoir un budget de 200€ par an ou l'achat d'un boitier avec une solution de mise à jour automatique.

2.4 LE DEVELOPPEMENT DE NOUVEAUX SERVICES SECURISES

2.4.1 CNB

Le CNB envisage d'utiliser les boitiers RSA pour donner aux avocats l'accès à un certain nombre de télé-services avec lesquels elle aurait des partenariats. Les partenariats auraient pour objectifs d'adapter les télé-services aux exigences de la profession, voire d'organiser un point de facturation unique centralisé par CNB.COM

Les services envisagés sont :
- Coffre-fort électronique,
- Télé-sauvegarde,
- Contrôle des accès internet et du contenu,
- Espace collaborative.

En parallèle, le CNB insiste sur la possibilité d'accéder au cabinet à distance grâce aux capacités VPN du RSA. Elle appelle cette possibilité « télétravail » dont le mode d'accès est décrit en annexe 1 du présent rapport. Le collaborateur du cabinet peut ainsi travailler depuis chez lui en prenant la main sur son poste resté connecté dans le cabinet. Cette solution peut aussi être utilisée par les connexions nomades de type clef 3G depuis n'importe où, tout en garantissant un niveau de sécurité général. Ce système permet aussi établir une session sur e-Barreau depuis son ordinateur personnel tout en gardant un niveau de sécurité élevé de bout en bout, à condition de disposer de la clé d'authentification.

2.4.2 PARIS

Ces télé-services ne font pas partie de la convention que la profession a passée avec la chancellerie.

Le terme « Télétravail » n'est pas la bonne appellation parce qu'elle suppose un cadre légal (travail à distance) et organisationnel (contrôle des horaires), ce qui n'est pas le cas. Il s'agit plutôt d'accès à distance.

L'accès à distance sécurisé est déjà mis en œuvre par les gros cabinets (80% du CA de la profession) et se fait très bien avec des solutions simples sur étagère. La sécurisation des accès à distance nécessite aussi la sécurisation du réseau local qui n'est pas couverte par NAVISTA.

La télé sauvegarde sécurisée existe sur le marché avec des accès sécurisés. La couche VPN de NAVISTA n'apporte rien de plus. Le service télé-sauvegarde «CNB.COM » n'existe pas encore.

2.4.3 MARSEILLE

Le Barreau de Marseille constate que la convention avec la Chancellerie ne porte pas sur les services annexes proposés (et pas encore développés) par NAVISTA. Le CNB ne peut pas imposer aujourd'hui de futurs services à des avocats qui n'en auront pas l'utilité.

2.4.4 ECLAIRAGE DES AUDITEURS

LE TUNNEL SECURISE VERS UN PRESTATAIRE SELECTIONNE EST SEDUISANT DANS SON PRINCIPE

Le CNB envisage pour fournir ces nouveaux services, de contracter avec des tiers fournisseurs de ces services à distance. La valeur ajoutée selon le CNB résiderait dans :

- La mise en place d'un tunnel VPN dédié avec le prestataire du télé-service,
- L'adaptation du télé-service aux spécificités des avocats,
- La prise en charge du paramétrage du télé-service par la gestion centralisée des boitiers.

Il est difficile de se prononcer sur des dispositifs qui ne sont pas encore connus, et dont les modalités techniques et économiques de déploiement restent à définir.

LES INFOGERANTS OFFRENT DEJA CE TYPE DE SERVICES

Il faut noter que les services identifiés (coffre fort, sauvegarde, contrôle de contenu, …) existent déjà sous forme de télé-services sur le marché et ont été conçus pour s'intégrer facilement aux réseaux des cabinets et aux postes de travail.

Ces services sont assurés par les prestataires infogérants des cabinets d'avocats et par des opérateurs grand public.

Par exemple pour la télé-sauvegarde, plusieurs acteurs sont déjà présents :

- Les infogérants sur leurs serveurs ou via des télé-services en OEM (Oodrive, OVH,…)
- Les éditeurs de logiciel de gestion de cabinet intègrent des dispositifs de télé-sauvegarde à leur offre commerciale

Tous ne mettent pas en œuvre des tunnels VPN mais certains sécurisent la connexion par Https.

DES OFFRES DE TELESAUVEGARDE EXISTENT AUSSI

Le marché Internet propose plusieurs solutions de télé-sauvegarde accessibles par SSL et, pour certaines assurant le cryptage avant envoi des données sauvegardées.

Par exemple, Dropbox, box.net, Live.com, Me.com, OVH.com en grand public, et avec des stockages hors Europe.

Certaines solutions logicielles permettent d'utiliser un répertoire FTP distant comme support de backup chiffré.

QUELLES SOLUTIONS POUR QUELLES DONNEES

Différents cadres réglementaires s'appliquent aux données traitées par les cabinets d'avocats. Ces cadres peuvent être très restrictifs et contraignants et en particulier en matière pénale où le secret professionnel est opposable. D'autre part, l'avocat qui traite de la préservation des données personnelles ou celui qui est confronté à de l'intelligence économique ont probablement des exigences différentes.

Une revue des cadres et des niveaux de sécurité qui en découlent devrait être effectuée pour apprécier les différents cas de figure qui s'appliquent aux données des cabinets d'avocat. A chacun de ces cas de figure, les dispositions organisationnelles et techniques associées seraient identifiées, de façon à apprécier le cadre d'emploi des différents services du marché.

2.5 LA DÉPENDANCE À NAVISTA

2.5.1 CNB

Le CNB met en avant les avantages du choix du prestataire NAVISTA par :

- Son intégration verticale, il couvre à la fois les développements, la distribution, le paramétrage initial, le support des utilisateurs, le support aux prestataires.
- Sa compétence et son professionnalisme – qualification ISO 9001-2000, intention de qualification ISO 27001, intention de certification ANSSI du protocole NTS.
- Sa connaissance des métiers du droit, et son agrément au chiffrement par DCSSI.
- Son coût attractif, et la maitrise contractuelle par CNB.COM.

Le CNB rappelle les conditions qui ont conduit au choix de ce prestataire.

- Au lancement du RPVA, le Conseil National des Barreaux a contracté avec France Telecom (ORANGE).
- Le Service Equant IP VPN retenu est un service d'interconnexion de Sites et d'Utilisateurs à travers un réseau privé virtuel sécurisé ou Virtual Private Network appelé « VPN » transportant le protocole IP en mode MPLS : Multi-Protocol Label Switching RFC2547 (VPN/MPLS). Ce service permet aux avocats d'échanger des flux de données entre les différents sites équipés d'Accès IP VPN et appartenant à son réseau VPN. L'étanchéité des flux est garantie au sein d'un VPN sécurisé. Le CNB a une souplesse de gestion de topologie au travers de la gestion des tables VRF (Virtual Routing Forwarding Table) permettant le routage et la commutation de labels.

- Dans toutes les configurations validées, les flux issus des sites ou utilisateurs équipés d'accès IP VPN ADSL monoposte et light sont dirigés vers un site désigné appelé aussi site de concentration, à savoir la plateforme RPVA.

- Les offres proposés à l'époque s'articulaient autour des débits et technologies suivants : ADSL 512Ko, ADSL 8 Mo et SDSL 1 Mo (pour un coût minimal de 70 €HT/mois.

Le CNB rassure sur les risques associés à un partenaire unique par :

- Son intention d'organiser un plan de reprise et de réversibilité en cas de défaillance de NAVISTA.

- L'hébergement prochain des services NCC sur les plateformes du CNB à Rennes.

- Son intention de prendre en charge le support via NCC.

En parallèle, NAVISTA rassure aussi sur ses changements de statuts en les justifiant par une économie sur les coûts de structure.

2.5.2 MARSEILLE

Le choix d'un partenaire unique expose de façon déraisonnée la profession à une petite structure juridique à faible capital social.

La technologie propriétaire (par boîtier individuel) est injustifiée alors que des protocoles équivalents (logiciels, sans boitier individuel) existent avec des implémentations standards, supportées par des grands fournisseurs et des grands comptes, et avec un haut niveau de portabilité (cas CISCO et VPN over SSL).

Le système NCC permet à quelques acteurs, dont NAVISTA, de contrôler l'ensemble des boitiers de la profession et de s'introduire dans les réseaux locaux de tous les cabinets d'avocats.

Que devient le RPVA, et la sécurité des cabinets d'avocats si une prise de contrôle « hostile » de NAVISTA se produit ?

Le service de base rendu par la formule de NAVISTA à savoir « le transport de données entre les cabinets d'avocats et les greffes des juridictions » peut parfaitement être rendu avec des technologies standards pour un coût bien moindre. Les services à valeur ajoutée ne sont pas couverts par le prix actuel, jugé déjà élevé, et les prix à venir ne sont pas arrêtés et donc inconnus.

2.5.3 ECLAIRAGE DES AUDITEURS

LA MAITRISE CONTRACTUELLE EST A AMELIORER

La capacité du CNB à gérer la reprise et la réversibilité du RPVA, en cas de défaillance de NAVISTA, n'est pas démontrée avec les moyens techniques et humains aujourd'hui en place. Ce point est développé dans la partie du rapport relative à la maitrise contractuelle du CNB.

LE RISQUE D'INTRUSION PAR NAVISTA PEUT-ETRE MAITRISE

NAVISTA a certes la capacité de s'introduire dans les cabinets d'avocats mais elle peut être encadrée si le cabinet adapte ses dispositions pour la sécurité (isolation du boitier NAVISTA, restriction des droits des utilisateurs anonymes sur le réseau et les dossiers partagés, etc.).

Cette capacité d'introduction est bien moindre que celle des prestataires informatiques qui eux ont un accès de télémaintenance complet au serveur, aux sauvegardes, aux postes de travail.

Certes les prestataires ont une capacité d'accès limité en largeur (100 cabinets max pour les gros prestataires), mais elle est sans commune mesure si on l'évalue en profondeur.

Il nous apparait que globalement, le risque pris est de même niveau que celui déjà pris avec les prestataires informatiques.

Avec NAVISTA, il est possible d'encadrer sa responsabilité contractuelle et de mettre en place des moyens de contrôle de son utilisation des moyens qu'elle développe. Si le CNB et NAVISTA ont une politique volontaire sur ce point, le risque peut être maitrisé.

3 COMPARATIFS ET ANALYSE CRITIQUE

3.1 ASPECTS ÉCONOMIQUES DES TROIS SYSTEMES

3.1.1 DONNEES DE REFERENCE SUR LES AVOCATS ET COUTS DE REFERENCE

Les données et les définitions qui suivent sont extraites d'une publication en date d'octobre 2008, de l'Observatoire du Conseil National du Barreau : « Avocats - faits et chiffres », disponible sur le site www.cnb.avocat.fr

Cette étude recense en 2007, 47.765 avocats France entière, se décomposant en :

- 15484 avocats individuels[2]
- 14019 avocats associés[3]
- 15093 avocats collaborateurs[4]
- 3169 avocats salariés non associés[5]

Parmi ces 47.765 avocats, le Barreau de Paris en compte 19.250, soit 40,3%. La région PACA en compte 4462 avocats, soit 9,3%.

Le Barreau de Marseille compte en avril 2010, 1675 avocats actifs.

Pour l'année 2006, le revenu moyen des avocats est de 72.352 € et le revenu médian à 42.536 €. L'Ile-de-France détient avec 90.440 €, le revenu moyen le plus élevé.

Pour les cabinets d'avocats, les coûts induits par le RVPA se répartissent en :

- Coût d'installation initiale
- Coût de location
- Coût de maintenance

3.1.2 DONNEES ÉCONOMIQUES CNB

Le nombre de boitiers recensés par NAVISTA en avril 2010 est de 2722.

Selon son dirigeant, NAVISTA compte installer 4000 boitiers d'ici le 31 décembre 2010 et vise un parc de l'ordre de 7.000 boitiers à terme.

2 L'avocat individuel exerce sa profession de façon totalement indépendante. Il est imposé au régime de l'IR et est responsable indéfiniment sur ses biens propres.

3 L'avocat associé est une personne physique détenant des parts dans une société d'avocats, ses revenus se composant d'honoraires et de dividendes.

4 L'avocat collaborateur travaille de façon autonome sur les dossiers qui lui sont confiés. Sa rémunération s'effectue sous forme de rétrocession d'honoraires.

5 L'avocat salarié est une personne travaillant sous contrat de travail avec son employeur moyennant le versement régulier d'un salaire. Il n'a pas de clientèle personnelle.

Le prix payé par le CNB à NAVISTA pour la location des boitiers dépend du nombre de boitiers déjà déployés, par exemple les 4000 premiers boitiers ont un prix, les 1000 suivants un autre, etc.

D'autre part, pour stimuler le projet de déploiement des RSA au sein des cabinets, le CNB a réduit le prix payé par le cabinet d'avocat, à la fois en :

- Subventionnant une part du prix du boitier, pour que l'avocat n'ait à payer que 25 € HT,
- Engageant la profession sur un nombre de boitiers minimum, et selon le CNB, pour que le prix de location soit lui aussi réduit.

En complément des prix mensuels, le cabinet doit aussi régler un forfait de prise en charge par NAVISTA de 39 € HT, dans l'accompagnement du cabinet ou de son prestataire, pour le paramétrage du RSA au sein du réseau local.

NAVISTA propose aussi une prise en charge de l'installation pour 169€ HT, qui correspond à ce qu'un prestataire informatique facturerait pour intégrer le RSA dans le réseau local du cabinet.

Il faut ainsi ajouter de l'ordre de 200€ HT par installation du RSA dans les cabinets.

Pour la location / maintenance des boîtiers RSA, la première mensualité versée à CNB.COM, par les cabinets d'avocats s'est élevée au départ à 55 € HT, dont 5 € pour la clé d'authentification et 2€ l'adresse de messagerie. Elle est passée à 25 € HT à partir d'avril 2010.

Depuis avril 2010, un nouvel accord a permis de réduire le montant payé par CNB.COM à NAVISTA. La redevance mensuelle du boitier RSA est ainsi passée de 45 à 35 € HT et passera à 30 € HT à partir du janvier 2011. La différence entre le montant payé à NAVISTA et celui payé par le cabinet d'avocats est pris en charge par le CNB. Les 7€ HT pour la clé et l'adresse mail s'appliquent encore.

Ainsi sur la base de ces nouveaux tarifs, le coût annuel à payer par les cabinets d'avocats s'évalue :

- Pour 2.010, le changement de tarif en avril 2010 et le passage de 2700 à 4000 cabinets conduit à un montant de l'ordre de 1.000.000 € HT
- Pour 4.000 boitiers à 25 € par mois en 2011, le montant sera au moins de 1.200.000 € HT
- Pour 5.000 boitiers à 25 € par mois en 2012, le montant sera de 1.650.000 € HT
- Pour 7.000 boitiers à 25 € par mois, le montant passera à 2.100.000 € HT.

De son coté, le CNB complète le financement :

- Pour 4.000 boitiers en 2011, il aura à débourser de 240.000 € HT.
- Pour 5.000 boitiers en 2012, il aura à débourser de 240.000 € HT.
- Pour 7000 boitiers en 2013, il sera de 300.000 € HT.

Le CNB ayant concédé à NAVISTA le monopole des accès XDSL pour la France hors Paris, jusqu'en 2014, le coût global de l'équipement des cabinets d'avocats en boîtiers RSA de 2010 à 2014 est supérieur à 9,3 M€.

Nous faisons la simulation suivante pour déterminer les ordres de grandeur :

	2008	2009	2010	2011	2012	2013	2014	Total
Nb cabinets	NC	NC	2 700	4 000	5 000	7 000	7 000	
Coût cabinet (€)	45	45	45/25	25	25	25	25	
Coûts cabinets (M€)	NC	NC	1,00	1,2	1,5	2,1	2,1	7,90
Coût CNB (M€)	0	0	0,3	0,24	0,28	0,3	0,3	1,42
Nb d'avocats	NC	NC	7000	11000	16000	22000	22000	
Coût avocat/mois	0	0	14	9	8	8	8	

NC = Non Connu

Ce montant couvre la seule part de l'accès à e-Barreau. Le coût des clés et du support assuré en direct par le CNB n'est pas pris en compte.

En toute rigueur, il faudrait aussi ajouter les 200 € par cabinet pour l'installation du boîtier RSA, ce qui s'élève à 1,4 M€ pour 7 000 cabinets.

Ainsi sur la période 2010 à 2014, le déploiement du RPVA avec la solution NAVISTA aura coûté de l'ordre 10,7 M€, dont 1,42 M€ pris en charge par le CNB.

Par avocat et par mois, le coût moyen est de 14 € en 2010 et de 8 € à partir de 2012.

3.1.3 DONNEES ECONOMIQUES PARIS

A Paris, les avocats reçoivent les clés d'authentification, gratuitement pour l'instant et ne payent aucune redevance pour accéder à e-Barreau.

Il n'y a pas de coût d'installation ni de coût de maintenance pour les avocats.

Le Barreau de Paris utilise sa plateforme d'accès aux services e-Carpa et anciennement e-Greffe qu'il a fait évoluer pour qu'elle puisse relayer l'authentification faite par Paris sur le serveur d'e-Barreau.

La migration e-greffe vers e-barreau, a nécessité l'adaptation de la plateforme d'authentification afin de rediriger les flux des avocats authentifiés vers le RPVA, ainsi que l'adaptation de la plateforme e-barreau afin que celle ci soit en mesure de gérer les flux en provenance du réseau parisien. Cette évolution a couté 24 000 € HT.

Le Barreau de Paris a aussi mis en place une liaison sécurisée et redondée pour accéder à e-Barreau :

- Il a acheté et mis en place en 2008 des équipements réseaux pour un montant de 66.000 € (dont les 24.000 € d'adaptation des plates-formes) à amortir sur 5 ans, soit 13.200 € par an.

Il s'agit de deux clusters de deux « Fortinet Fortigate 200A » possédant les fonctions de pare-feu et de réseaux privés virtuels associés à un moteur IPS (Intrusion Prevention System). Un analyseur « Fortinet Fortianalyser 800B » a été installé par CertEurope pour concentrer et traiter les logs et les alertes de sécurité.

- Il s'est doté d'une ligne privée haut débit Orange business à 10 Mb/s, secourue par un lien privé SDSL à 4 Mb/s pour un montant annuel de 57.328 €. Il finance la maintenance du Firewall pour 7176 € par an ainsi qu'une surveillance et une exploitation pour 12.228 € par an.

Le budget annuel pour assurer la fonction « transport jusqu'à e-Barreau » est de 89.932 € par an.

Le prix de revient par avocat et par an, sera fonction du nombre d'avocats utilisant la liaison :

- Pour 4.000 avocats, il revient à 1,87 € par avocat et par mois, soit 22,48 € par an
- Pour 5.000 avocats, il revient à 1,5 € par avocat et par mois, soit 18 € par an
- Pour 20.000 avocats, il serait de 0,38 € par avocat et par mois, soit 4,50 € par an

	2008	2009	2010	2011	2012	2013	2014	Total
Nb cabinets			2 700	9360	9360	9360	9360	
Coût cabinet			0	0	0	0	0	
Coûts cabinets (M€)			0	0	0	0	0	0,00
Coût Barreau Paris (M€)		0,09	0,09	0,1	0,1	0,1	0,1	0,58

Le support consiste essentiellement au support du certificat sur clé. Nous ne l'avons pas pris en compte comme nous ne l'avons pas pris en compte pour le CNB et pour Marseille.

Au global, le coût de la solution parisienne est de l'ordre de 0,6 M€ dont 0,5 M€ de liaison avec la plateforme e-Barreau.

A titre de comparaison, le Barreau de Paris a recensé en 2008, le nombre de sites qui auraient nécessité un boîtier NAVISTA. Il a recensé 9360 sites. Au moment du choix par Paris de sa solution, pour une redevance mensuelle de 55 € par mois (dont 48€ pour le boîtier NAVISTA) et par avocat, le coût induit par NAVISTA aurait été de 4 492 800 € HT/an.

Cette analyse mériterait d'être affinée parce que le CNB estime que la couverture nationale hors Paris est de l'ordre de 7300 boitiers, alors que le nombre de cabinets couverts est supérieur au nombre de cabinets d'avocats parisiens (1/3 de plus d'avocats en province qu'à Paris et des cabinets plus petits en province qu'à Paris).

En projection sur 2011, avec les nouveaux tarifs à 25 € par boitier et par mois, la redevance annuelle avocat et hors subvention CNB pour les 9.360 boîtiers serait passée pour les avocats parisiens à 2.808.000 € HT/an.

3.1.4 DONNEES ECONOMIQUES MARSEILLE

La solution du Barreau de Marseille a été mise en place à VENISSIEUX par un infogérant ICT-Flowline. Elle a nécessité l'acquisition d'équipements réseaux et implique des coûts de fonctionnement annuels et récurrents.

L'acquisition porte sur un frontal CISCO ASA 5550 doté d'un firewall de 100 licences Premium pour un montant de 23.000 € HT. Un Routeur 3845 et un Switch 2960 pour gérer si nécessaire plusieurs boîtiers RSA NAVISTA mutualisés pour 17.000 € HT, et 1950 € HT pour les installations successives. Le montant des acquisitions initiales est de 47.800 € HT, à amortir sur 5 ans, soit 9.560 € HT par an.

Si le nombre d'utilisateurs simultanés devait dépasser les 100, le Barreau de Marseille envisage d'acheter un pack de licences Cisco supplémentaires qui coûterait de l'ordre de quelques milliers d'euros.

Les coûts récurrents concernent 4 boîtiers RSA, une liaison de bande passante de 1 Mo/s, et un hébergement, pour 770 € HT par mois, soit 5.875 € HT par an.

Le coût annuel de la solution du Barreau de Marseille est dès lors de 15.435 € HT.

Il faut remarquer ici que si la solution « Marseille » devait être validée par le CNB comme un mode d'accès autorisé à e-Barreau, le concentrateur Cisco ASA devrait être localisé dans le centre d'exploitation du CNB. Le transport et les 4 boitiers RSA seraient évités et la liaison serait fiabilisée.

L'avocat dispose d'une documentation qui lui explique la démarche à suivre pour installer sur son ordinateur les logiciels à télécharger et les paramètres à initialiser. Un support est assuré par un technicien du Barreau de Marseille. L'installation de ce logiciel est concomitante à celle des pilotes de la clé Gemalto, aussi il n'est pas pris en compte.

Dimensionnée pour 1000 avocats dotés de la clé e-Barreau, la solution revient à 1,29 € HT par avocat et par mois.

	2008	2009	2010	2011	2012	2013	2014	Total
Nb avocats			1000	1200	1200	1200	1200	
Coût avocat (€)			0					
Coûts avocats (M€)			0	0	0	0	0	0,00
Coût Marseille (M€)			0,015	0,015	0,015	0,015	0,015	0,08

Au global, le coût de la solution du Barreau de Marseille est de 80 k€, dont 60€ de transport jusqu'à e-Barreau.

3.1.5 COMPARATIF DES SERVICES RENDUS PAR LES TROIS SOLUTIONS

Pour la communauté des avocats, la solution CNB est plus chère de plusieurs ordres de grandeurs que les solutions marseillaise et parisienne.

Elle ne peut évidemment pas être réduite au transport sécurisé qu'assurent les deux autres solutions, et nécessite d'être mise dans la perspective des services complémentaires qu'elle apporte aux cabinets d'avocats en terme de sécurité et de nouvelles fonctionnalités.

Il faut retenir ici que compte tenu du système complexe au sein duquel elle se place et des évolutions du marché récentes pour l'amélioration globale d'internet et la diffusion de télé-services, la justification du service rendu par le déploiement du RSA est délicate à apprécier.

Effectivement, le boitier permet de sécuriser l'accès au réseau internet et d'accéder à des télé-services sécurisés.

Mais les cabinets moyens et gros qui font appel à des prestataires informatiques pour gérer leurs postes de travail et leur réseau local, disposent déjà des solutions de sécurité et de télé-services. Le boitier vient en doublon pour les fonctions de sécurisation.

Les petits cabinets ont aujourd'hui la possibilité d'utiliser les solutions grand public pour sécuriser leur accès internet et accéder à des télé-services. Ces services sont performants (une box internet intègre un routeur firewall mis à jour automatiquement par le Fournisseur d'Accès Internet (FAI) et un service comme Dropbox assure le transport chiffré des données de télé-sauvegarde qui sont elles-mêmes conservées chiffrées sur les serveurs de Dropbox.

Si la sécurité et la qualité de ces service n'étaient pas adaptées à ce que l'on imagine du niveau de qualité qui s'impose à l'avocat, l'analyse n'a pas été faite et menée par le CNB qui impose le RSA.

3.1.6 SYNTHESE ECONOMIQUE

L'architecture NAVISTA impose un coût à la profession de quelques millions d'Euros par an, et un coût global, sur la période couverte par le contrat NAVISTA, de l'ordre de 12 M€.

Le CNB justifie ce surcoût par un service rendu sur les points suivants :

- la sécurisation renforcée de la liaison,
- la sécurisation du réseau local du cabinet,
- la sécurisation du poste de travail de l'avocat,
- l'accès sécurisé aux boites aux lettres avocat-conseil.fr
- l'extension à de nouveaux services,

- la simplicité d'installation sur les postes de travail du cabinet,
- la maintenance centralisée d'un firewall-VPN.

L'architecture NAVISTA présente effectivement toutes ces propriétés, mais compte tenu de la diversité des situations rencontrées sur le terrain, il est difficile de se prononcer sur leur intérêt effectif pour les cabinets d'avocats. En effet :

- La liaison est déjà fortement sécurisée avec un chiffrement HTTPS et une authentification par cryptoprocesseur sur clé USB. En cas d'intrusion, les logs serveurs permettent d'apprécier la pertinence d'une contestation. Le transport au sein d'un VPN éprouvé apporte une sécurité supplémentaire sur la liaison. Il n'y a pas d'évaluation qui justifie le gain apporté ;
- La sécurité du poste de travail de l'avocat et du cabinet d'avocat dépend pour l'essentiel des facteurs organisationnels et des dispositions techniques relevant du réseau local du cabinet. Ces dispositions ne sont pas couvertes par le RSA qui se limite à mettre en place un (bon) firewall contrôlant les accès Internet ;
- La sécurisation des échanges de mails entre avocats par l'adresse avocat-conseil.fr, accédée à travers le VPN NAVISTA, est confrontée à de multiples obstacles : cabinet utilisant leur propre nom de domaine, avocats préférant la richesse fonctionnelle des webmails commerciaux (Gmail,Hotmail,…), inexistence de client VPN NAVISTA pour les terminaux mobiles (PDA, Smartphone), non prise en compte des tiers (clients, magistrats sur adresses personnelles) ;
- L'extension à de nouveaux services passera par l'accès sécurisé par VPN à des télé-services. La sécurisation par VPN est un plus par rapport à la sécurisation HTTPS sans certificat des offres grand public. Cependant, les services retenus par le CNB ne sont pas encore connus et ainsi n'ont pas pu être évalués. Ils ne seront pas gratuits (20% de plus à la location du RSA pour le transport jusqu'au nouveau service, plus coût du service lui même) et leur intérêt technique et économique devra être démontré ;
- Pour la simplicité de l'accès à e-Barreau, le boitier RSA n'évacue pas la nécessité d'installer les pilotes Gemalto sur les postes de travail qui s'impose aussi aux deux autres solutions. La solution du Barreau de Marseille impose d'installer un autre logiciel à l'occasion de l'installation des pilotes. Cette tâche supplémentaire est bien assistée et reste du même niveau de complexité que la création d'un compte d'accès distant sur le RSA ;
- La maintenance centralisée par NAVISTA du firewall-VPN est un réel service apporté par la solution du CNB. Elle permet au cabinet d'avocat d'avoir son matériel suivi par une hotline spécialisée et mis à jour des derniers correctifs de sécurité. Il intéresse les petits cabinets qui souhaitent accéder à distance à leur cabinet et qui souhaitent économiser le suivi par un prestataire informatique. La maintenance NAVISTA lui assure les dernières mises à jour et le service support lui reparamètre le routeur si sa configuration était amenée à évoluer.

Même si c'est le critère de la sécurité des échanges avec e-Barreau qui a été mis en avant par le CNB pour prescrire le boîtier RSA, c'est l'angle du service pour les petits cabinets qui émerge comme la véritable valeur ajoutée potentielle du RSA.

- La gestion du routeur et de ses mises à jour par une administration centrale,
- La possibilité de se brancher par un lien hautement sécurité (VPN) à des services sélectionnés par e-Barreau et compatibles avec le protocole NTS (Navista Tunneling System).

Cette valeur ajoutée, qui pouvait faire sens au démarrage du projet en 2007, est aussi remise en question par la nouvelle configuration de marché qui voit des acteurs très dynamiques se positionner en offrant mobilité, souplesse d'accès et sécurité.

3.2 SÉCURITÉ INFORMATIQUE

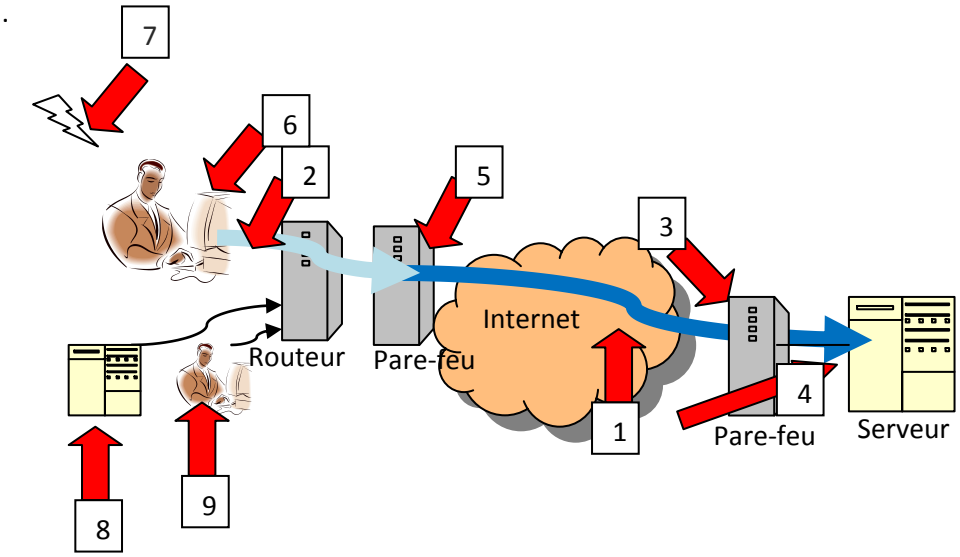
Il ne nous a pas été communiqué d'analyse de sécurité ni de référentiel de sécurité pour les cabinets d'avocats, ni par le CNB ni par aucun des autres acteurs de l'audit.

Nous présentons ici les principes de base qui ont guidé notre analyse sécuritaire.

3.2.1 LES DIFFERENTES ATTAQUES

Pour récupérer la copie des données accédées par un internaute sur un serveur internet, différentes attaques sont possibles :

.



- La liaison internet
    - 1 - Interception du flux, soit en s'interposant entre (Man in the Middle) le serveur et le poste de l'utilisateur grâce à une attaque du routeur et/ou des DNS de référence du cabinet,

- 2 - En interceptant la liaison depuis le réseau local (quand on y a accès), soit parce qu'elle est en clair, soit parce qu'elle est en HTPPS qui est plus « facile » à intercepter sur le réseau local,

- Le serveur
  - 3 - Le firewall pour avoir un accès au serveur,
  - 4 - Le serveur à travers les accès qu'il offre à travers le pare-feu ou firewall,
- Le réseau local
  - 5 - En attaquant le firewall pour avoir accès au réseau local,
  - 6 - En attaquant le serveur s'il est exposé directement à Internet (cas des serveurs TSE branchés en direct) et avoir accès soit aux documents stockés, soit par rebond aux autres machines du réseau local,
  - 7 – En attaquant le réseau Wifi si on est à proximité,
- L'organisation
  - 8 - En attaquant l'utilisateur concerné ou un autre utilisateur du réseau en incitant son utilisateur à activer une charge offensive (pièce jointe, site web exploitant des failles navigateur) ,
  - 9 - En manipulant une personne ayant accès au réseau pour qu'il/elle crée une brèche de sécurité dans le réseau (divulgation de mot de passe par exemple, envoi de document, activation d'une procédure de récupération, etc.)

Cette diversité d'attaques rappelle que la sécurité est une affaire globale et impliquent de multiples mises à niveau. Elle nécessite une approche méthodique au sein d'un projet à la fois technique et organisationnel.

3.3 INTEGRATION DANS LES CABINETS, PRISE EN COMPTE PAR LES PRESTATAIRES INFORMATIQUES

3.3.1 AUJOURD'HUI, LES CABINETS CONFIENT LEUR INFORMATIQUE GLOBALEMENT A DES SOCIETES SPECIALISEES

LES DIFFERENTS NIVEAUX DE SERVICE

Les cabinets d'avocats font appel fréquemment à des prestataires de services en informatique pour

- Installer leur matériel (poste de travail, serveur, équipement réseau)
- Mettre au point notamment la configuration logicielle des postes de travail
- Configurer le domaine informatique et/ou le serveur de fichiers
- Configurer le système de courrier électronique accessible à distance
- Configurer les accès à internet, notamment les liaisons intersites, les accès distants

DANS CE CONTEXTE LE PRESTATAIRE INFORMATIQUE UTILISE LES SERVICES QU'IL MAITRISE VOIRE QU'IL PRODUIT LUI-MEME OU QU'UN DE SES PARTENAIRES PRODUIT

Le prestataire installera des équipements qu'il maîtrise et qu'il a déjà installés chez d'autres clients. Ces équipements sont parfois déjà en place et fonctionnent en donnant toute satisfaction, lorsqu'on lui demande d'installer un boîtier NAVISTA. C'est le cas avec les routeurs VPN (Fortinet, Cisco, Arkoon,…) dont les fonctions sont proches de celles du RSA.

Le prestataire gère aussi le serveur de mails du cabinet et peut assurer le suivi des sauvegardes en interne (cassettes, disque de backup), ou sur ses serveurs, voire sur ceux d'un autre prestataire de services.

CNB.COM S'INSERE DANS CE DISPOSITIF AVEC LE BOITIER RSA

Le boitier RSA NAVISTA est un matériel imposé au prestataire qui doit l'intégrer dans le réseau informatique du cabinet.

Le matériel et l'organisation Internet associée, viennent s'insérer ou se substituer à des dispositifs du cabinet.

Les prestataires procèdent à cette opération pour un prix souvent forfaitaire pour un petit cabinet ou un cabinet moyen pour un coût de l'ordre de 200 € HT.

3.3.2 PRISE EN COMPTE DU BOITIER PAR LES PRESTATAIRES INFORMATIQUES DES CABINETS

Les quelques visites effectuées dans des cabinets de l'Ile de France et de la Région PACA ont montré que le boîtier RSA dans une grande partie des cas, est utilisé comme « décodeur RPVA » et le reste des fonctions est ignoré.

Le boîtier RSA vient en doublon à des dispositifs déjà existants, pour lesquels le prestataire est capable de garantir les performances et d'optimiser le paramétrage.

Son installation est contraignante, nécessite de passer par l'assistance en ligne de NAVISTA pour obtenir un mot de passe qui donne accès aux paramètres élémentaires ou de solliciter l'intervention distante de NAVISTA pour les opérations fines de paramétrage.

Il a aussi été constaté que dans la gamme de télé-services envisagés par CNB.COM, certains sont déjà assurés par les prestataires. C'est le cas de la télé-sauvegarde.

3.3.3 LA POSITION DE CNB ET CNB.COM

L'organisme CNB.COM s'impose comme un partenaire incontournable des cabinets d'avocats. Il s'appuie sur les prestataires informatiques pour déployer son dispositif mais ne leur donne pas toujours les directives et les moyens de valoriser ce service.

Il développe en parallèle une offre qui peut apparaître aux prestataires des cabinets d'avocats comme concurrentielle. Le boitier est perçu comme le vecteur de cette concurrence à venir.

Le boiter NAVISTA est en plus surdimensionné par rapport à sa fonction initiale qui est le cryptage des communications, il ne prendra sa valeur que lorsque les télé-services seront utilisés.

3.3.4 CNB.COM PEUT-ELLE ETRE LE PRESTATAIRE UNIQUE DES CABINETS D'AVOCATS ?

La technologie NAVISTA est-elle la meilleure offre possible pour cette technologie unique? S'il avait le choix, quelle alternative peut adopter un cabinet d'avocats ?

Le niveau de sécurité supplémentaire apporté par le RSA justifie-t-il la dépense imposée aux avocats?

Le choix imposé par le CNB crée-t-il des distorsions de concurrence avec les prestataires de services informatiques ?

Les cabinets d'avocats peuvent-ils être laissés libres de configurer leur sécurité pour atteindre le niveau de sécurité visé par le CNB?

Est-il possible d'évaluer cette sécurité? Pour l'avocat concerné? Pour le Barreau?

Aujourd'hui les fonctions de filtrage sécuritaire ne sont pas adoptées par les cabinets d'avocats qui utilisent le RSA comme décodeur e-Barreau. Il en est de même des cabinets d'avocats parisiens qui ont obtenu la dérogation.

Est-il possible de leur imposer d'utiliser du RSA comme frontal internet des cabinets ?

Pour les grands cabinets tels que FIDAL, la réponse est déjà donnée. Le CNB a admis que ces cabinets n'utiliseront le RPVA que pour sa fonction « transport e-Barreau ».

A ce jour, seuls les petits cabinets pourraient rentrer complètement dans le schéma CNB.

3.4 MAITRISE CONTRACTUELLE

3.4.1 LES ENGAGEMENT MUTUELS

CNB.COM et NAVISTA ont signé le 10 octobre 2007 une convention qui attribue pendant 5 ans, à NAVISTA un monopole des échanges entre les cabinets d'avocats et le serveur e-Barreau.

CNB.COM s'est engagé à :

- Maintenir la plateforme technique e-Barreau,
- Déployer l'architecture NAVISTA (frontal à Rennes et boitiers RSA dans les cabinets d'avocats) pour l'accès au service e-Barreau,
- Assurer le support utilisateur pour les clés e-Barreau et les boitiers RSA (niveau 0 seulement)

NAVISTA loue à CNB.COM des boîtiers RSA qui équiperont les cabinets d'avocats et en assure la maintenance et la télé-administration.

NAVISTA s'engage dans cette convention à assurer l'administration et la maintenance du service de liaison sécurisé. Elle s'engage à réaliser un télédiagnostic dans un délai indicatif de 4 heures et à adresser à l'abonné un équipement de remplacement dans un délai de 48 heures après l'expiration du délai de télédiagnostic.

A l'article 10 de la convention du 10 septembre 2010, intitulé « Propriété Industrielle – Conséquences de la défaillance de la société NAVISTA », il est précisé que :

> « *En cas de défaillance de la société NAVISTA, dans la fourniture du service de liaison sécurisée supérieur à SOIXANTE DOUZE HEURES (72), l'Association CNB.COM peut lui substituer un tiers SEPT (7) JOURS après la réception d'une mise en demeure restée sans effet faite par lettre recommandée avec avis de réception* »

Dans ce même article, ile est précisé que :

> « *La société NAVISTA s'oblige à déposer les sources des logiciels d'accès, leurs mises à jour ainsi que leur documentation auprès de l'Agence Pour la Protection des Programmes (APP)*»

En octobre 2009, un nouvel accord a été trouvé avec NAVISTA, pour autoriser le Barreau de Paris à sortir du dispositif. A cette occasion, les prix ont été revus à la baisse, et des engagements sur des quantités de boîtiers RSA à installer au 31 décembre 2010 ont été pris par CNB.COM.

3.4.2 LA REPRISE DE MAIN

Actuellement NAVISTA assure la télé administration sans partage ni contrôle.

Pour éviter un risque humain, il convient que des contrôles périodiques de cette administration soient réalisés par un tiers.

3.4.3 LA REVERSIBILITE

En cas de défaillance, la convention prévoit en son article 10, la substitution d'un tiers en cas de défaillance grave de NAVISTA, qui dans ce cas s'est engagée à transférer le savoir faire et les sources nécessaires à la poursuite de la prestation.

Le périmètre de la reprise (données, NCC, OS des boitiers, NTS) et ses modalités sont imprécises dans le contrat.

Nous relevons aussi que le CNB ne s'est pas encore organisé pour avoir à assurer cette reprise.

En premier lieu, aucun tiers n'a été identifié pour l'instant pour prendre en charge cette reprise de l'activité, en cas de défaillance de NAVISTA.

En deuxième lieu, le dépôt de sources qui protège le CNB d'une défaillance globale de NAVISTA n'a pas été validé, ni sur son contenu, ni sur son utilisabilité par un tiers.

En particulier, les codes sources déposés n'ont pas été validés en termes de contenu et d'utilisabilité. Rien ne garantit que le CNB dispose de la dernière version des sources, que les outils et les directives de compilation, sont fournis et qu'ils permettent bien d'obtenir la version en production.

Il conviendrait aussi d'en valider de contenu pour s'assurer qu'une documentation technique est fournie ou que la description des outils de développement et de tests est disponible.

3.4.4 L'ENCADREMENT DE L'EVOLUTION FONCTIONNELLE DU RSA

Nous n'avons pas vu de contrat dans lequel NAVISTA précise les fonctionnalités qu'elle allait développer pour le CNB.

Nous observons que les options prises par NAVISTA sont utiles et constructives :

- Développement d'une suite « Accès distant » (paramétrage depuis e-Barreau, client VPN téléchargeable, etc.),
- NCC gérant les tickets et les configurations,
- Renforcement de la fiabilité des boitiers par un test avant montage des cartes et une meilleure gestion de la mémoire flash,

Aussi, les nouvelles évolutions annoncées par NAVISTA sont prometteuses :

- Filtre de contenu à intégrer au routeur,

- Paramétrage par l'interface NCC mis à disposition des prestataires,

Dans l'ensemble NAVISTA apparait comme un partenaire proactif du CNB. Il est intéressé au succès de son offre auprès des avocats et met en œuvre un effort global.

En revanche, il est préoccupant que l'ensemble de ce bon fonctionnement ne soit pas encadré par un contrat précis entre le CNB et NAVISTA et ne repose que sur l'intérêt commun perçu par les deux parties.

Nous relevons au passage que la sélection de NAVISTA n'a pas résulté d'un appel d'offre.

Le CNB explique cette situation par le contexte historique du RPVA et les difficultés rencontrées avec la première solution retenue et toujours disponible, à base d'un accès Internet haut débit.

4 CONCLUSION

4.1 ANALYSE DE LA SITUATION GENERALE

Le déploiement du RPVA soulève de nombreuses questions parmi lesquelles nous relevons les thématiques suivantes :

- Quel est le niveau de sécurisation à atteindre sur les échanges avec les juridictions et contre quels scénarios protège-t-il ?
- Quel est, au-delà de la mise en œuvre d'une solution de chiffrement, le périmètre à sécuriser pour assurer la sécurité de liaison ?
- Au-delà de la liaison, quel est le niveau d'exigences de sécurité auquel doivent se soumettre les cabinets d'avocats ?
- Quel est le niveau de services d'informatisation que devront mettre en œuvre les cabinets d'avocats ?

Face à ces questions, nous n'avons pas trouvé de réflexion globale, ni d'analyse détaillée sur le plan organisationnel, mais une réponse construite autour de l'adoption de moyens techniques.

Ce manque est d'autant plus frappant que le projet engage la profession jusqu'en 2014 dans un financement évalué à près de 10,7 M€ HT.

Nous retenons que l'engagement de la profession vis-à-vis de la chancellerie est d'organiser une communication et une authentification sécurisée avec les services du greffe.

Ce contrat minimum est assuré par l'utilisation de certificats sur cryptoprocesseurs, qui garantissent l'authentification sur les services du greffe et sécurisent la mise en place du canal sécurisé avec la plateforme relais qu'est e-Barreau.

Ce dispositif fait consensus et les trois solutions, dans les grandes lignes satisfaisantes, en assurent la prise en charge.

Le CNB va plus loin en imposant une architecture qui a pour objectif d'améliorer :

- La sécurisation de la liaison
- La sécurité des données échangées avec les greffes
- L'adoption par la profession d'outils de productivité sécurisée

Nous passons en revue les gains attendus et l'adéquation des moyens mis en œuvre.

4.1.1 LA SECURISATION DE LA LIAISON ET DE L'AUTHENTIFICATION

Ce dispositif HTTPS plus Certificat d'authentification n'est pas inviolable. Des attaques sont possibles, elles nécessitent des moyens importants (plusieurs jours d'expert). Elles laissent aussi des traces sur les serveurs si les moyens de surveillance adéquats ont été mis en place et sont exploités. Ces traces permettent de valider ou d'invalider une éventuelle contestation de l'authentification.

L'amélioration mise en place par le CNB consiste à encapsuler le canal HTTPS au sein d'un tunnel VPN. Si le VPN est bien constitué, cette amélioration rend la communication quasiment « inviolable ». Elle introduit aussi une séparation des clés : la clé RSA du VPN sert à sécuriser le transport, la clé du certificat sert à sécuriser l'authentification.

Cette amélioration, si elle est en première approche bienvenue, conduit un attaquant, expert, à reporter ses efforts sur des cibles plus faciles que sont le « réseau » du cabinet ou le serveur.

Ainsi vouloir améliorer la sécurité du dispositif Https+Certificat, c'est s'engager dans une course à la sécurité qui va engager tout l'écosystème dans lequel s'inscrit cette liaison :

- Les clés d'authentification, le processus de délivrance de ces clés, leur utilisation au sein du cabinet,
- Le routeur, les clés de chiffrement des VPN ouverts par le routeur,
- L'organisation qui gère la maintenance des routeurs et les clés de chiffrement,
- Le poste de travail qui se connecte, mais aussi tous les postes du réseau local sur lequel il se trouve, et tous les serveurs qui sont ouverts à Internet,
- L'organisation qui gère ces équipements, qui les approvisionne, qui les maintient, ainsi que les comportements de ceux qui utilisent ces équipements.

C'est la mise à niveau simultanée de ces dispositifs qui permet d'améliorer la sécurité du dispositif « Https avec certificat » du point de vue de l'authentification et de l'accès au serveur e-Barreau pour le faire passer de fortement sécurisé à « inviolable ».

Une telle démarche nécessite de coordonner tous les acteurs qui interviennent autour d'objectifs concrets.

Nous observons un certain nombre de lacunes dans ce dispositif :

- Le partage des clés dans les cabinets
- Le manque de contrôle sur les routeurs utilisés par les cabinets d'avocats (entre 30 et 50% court-circuitent le routeur de référence du CNB),
- L'inexistence de certification du routeur RSA de référence du CNB, des protocoles utilisés, de l'organisation qui les gère,
- L'absence de visibilité organisationnelle relayée par le RPVA sur le niveau de sécurité de postes de travail et plus généralement du réseau local du cabinet,

- L'inexistence d'un accord avec les prestataires informatiques des cabinets

- L'absence de politique centrale sur la manière dont les cabinets devraient aborder la sécurité au quotidien.

Sans une coordination globale de ces différents éléments du dispositif, il nous semble que le déploiement des boitiers RSA ne suffira pas à améliorer la sécurité générale de l'accès et de l'authentification.

4.1.2 LA SECURITE DES DONNEES ECHANGEES AVEC LES GREFFES AU SEIN DES CABINETS

Ce point n'est pas explicitement couvert par la convention avec le Ministère de la Justice, mais il peut résulter des engagements de confidentialité de la profession, auquel cas il faudrait l'étendre à l'ensemble des documents gérés par le cabinet.

- Quels sont les documents sensibles ? Quel est le niveau de protection qu'il faut leur assurer ? Quels sont les scénarios critiques ? Quelles sont les conséquences d'une défaillance ?
- Comment les documents sont référencés ? repérés ? stockés ? Comment leur accès est-il contrôlé ? Quels sont les outils de stockage et de diffusion de données ? Quels sont les usages associés ?
- Quels sont les moyens mis en œuvre pour sécuriser ces documents ? Quels sont les règles organisationnelles associées ? Quelles sont les métriques ?
- A qui les documents sont-ils communiqués ? Par quels moyens ? Quels engagements de sécurité prend le correspondant ?

C'est ainsi une politique complète de sécurité qui se décline.

Il est probable qu'elle se formule en termes simples mettant en jeu quelques principes de ségrégation dans le stockage des documents et les points d'accès Internet, et que ces principes soient complétés par des bonnes pratiques au niveau de la gestion informatique au sein des cabinets et de l'utilisation d'Internet et des services Internet.

Cette formulation nécessite au préalable une concertation au niveau de la profession pour définir le niveau de sécurité à adopter selon les grandes familles de documents (éléments de procédures, pièces communiquées, éléments clients, etc.), un positionnement sur les moyens disponibles sur le marché et des bonnes pratiques à diffuser au sein de tous les cabinets.

Aujourd'hui, le CNB propose des adresses mails, associées à un serveur de courrier qu'il héberge et des moyens sécurisés d'accès à cette adresse. Ce dispositif se heurte à un certain nombre de limitations liées pour l'essentiel à la non adoption de ces adresses par les avocats qui ont une politique de marque sur Internet ou qui préfèrent la convivialité de services éprouvés par le grand public.

4.1.3 L'ADOPTION DE NOUVEAUX SERVICES SECURISES

La bonne utilisation des outils documentaires peut permettre de gagner en sécurité et en productivité. Elle permettrait à la profession d'avocats de rester compétitive par rapport aux évolutions du paysage juridique français et européen.

Des solutions techniques sont envisagées par le CNB pour couvrir certaines des préoccupations de la sécurité des données, il s'agit pour l'essentiel de l'utilisation de télé-services accédés par des tunnels VPN ouverts depuis le boitier NAVISTA.

Les télé-services envisagés sont :

- Télé-sauvegarde des données sur une plate-forme sécurisée et localisée en France,
- Plate-forme collaborative pour permettre aux avocats de créer des espaces collaboratifs avec leurs clients,
- Coffre-fort électronique pour archiver des documents auprès d'un tiers de confiance,

Nous ne doutons pas de l'intérêt potentiel de ces services.

Nous n'avons cependant pas eu de description précise de ces télé-services, de leur coût, de leur calendrier, de leur positionnement par rapport aux offres du marché existantes aujourd'hui et à court terme, et de la liberté de choix des cabinets vis-à-vis de ces télé-services. Il nous est donc difficile de nous positionner sur leur intérêt ou leur adéquation au besoin de la profession.

4.2 POINTS PARTICULIERS ET RECOMMANDATIONS

4.2.1 INTERET ECONOMIQUE DE LA SOLUTION NAVISTA POUR UN CABINET

Indépendamment du monopole qu'impose le CNB, la solution NAVISTA offre-t-elle un intérêt économique pour un cabinet ?

Le prix de 900 € sur 3 ans que coûtera la solution NAVISTA pour un cabinet, est du même ordre de grandeur qu'un routeur[6] haut de gamme qui intègre des filtres de contenu mis à jour quotidiennement et avec une maintenance 24/7.

Le boîtier RSA NAVISTA a l'ambition d'offrir un niveau de service analogue.

Il offre l'intérêt d'être géré par les avocats, d'être déjà déployé au sein de la profession et d'avoir une offre de services associée qui peut dispenser le cabinet d'avoir un prestataire informatique, si le cabinet est à même de gérer ses postes de travail et son réseau et qu'il souhaite déléguer la gestion de l'accès sécurisé à Internet avec une fonction d'accès distant.

[6] Nous intégrons dans cette comparaison en ordre de grandeur une installation initiale simplifiée réalisée par un installateur agréé.

Aux recommandations près qui suivent sur la qualification de l'offre NAVISTA et du projet RPVA, le boitier NAVISTA peut représenter une solution viable pour les cabinets qui souhaiteraient améliorer leur sécurité, en utilisant un tiers pour la gestion du routeur, et tout en gérant eux-mêmes la sécurité de leur réseau local.

Le profil du cabinet intéressé est ainsi un petit cabinet, possédant quelques postes avec un serveur de fichier, connectés à Internet par la « box » livrée par le Fournisseur d'Accès Internet. Il aurait déjà mis sous contrôle sa sécurité informatique, avec des principes organisationnels, la gestion des documents électroniques, la gestion des installations de supports et de logiciels, la gestion des profils, la gestion des mots de passe, la gestion des mises à jour, le paramétrage de la « box », l'utilisation de télé-services (dont télé-sauvegarde et courrier électronique) de qualité, etc.

Pour améliorer sa sécurité, il prendrait l'option de ne pas transformer son réseau local parce que son informatique locale ne change par significativement et qu'il passe de plus en plus par de télé-services. Ainsi, il pourrait se dispenser de passer par un prestataire informatique pour le réseau local et mettrait l'accent de l'amélioration de la sécurité sur le niveau de sa connexion Internet et des télé-services qu'il utilise.

Dans ce scénario, le choix de passer par le routeur NAVISTA et les télé-services qu'envisage de développer CNB.COM peut avoir une justification technique et économique. La proximité de CNB.COM avec la profession faciliterait la démarche et réduirait le coût de transaction pour le cabinet.

L'intérêt pour les cabinets plus consistants est moindre parce que ces cabinets doivent passer par un prestataire informatique. Cet intérêt dépendra aussi de la capacité du RSA NAVISTA à être adopté par les prestataires informatiques qui devront utiliser alors le routeur NAVISTA à plein potentiel et non plus en marge de solutions de sécurité reconnues par le marché et qu'ils maitrisent.

Si la profession choisit d'engager une politique volontariste sur la mise à niveau de la sécurité des cabinets d'avocats, il nous semble que d'ici à deux ans le scénario que nous avons décrit ci-dessus pourrait concerner l'ensemble des cabinets de 1 à 4 personnes (soit 1 ou 2 avocats).

RECOMMANDATIONS :

Le CNB devrait s'assurer d'un certain nombre de mises à niveau :

- Validation de la sécurité effective apportée par le boitier par un tiers indépendant, par exemple via un certificat de sécurité de premier niveau (CSPN) de l'ANSSI.
- Validation par un tiers que l'organisation que NAVISTA et CNB.COM développent autour du boitier est aux bonnes pratiques de sécurité,
- Contour fonctionnel et économique des services qui seront attachés au boitier,
- Intégration d'une technologie standard et sécurisée comme IPSEC dans les services offerts par le boitier, au minimum pour la prise en charge des terminaux mobiles, au mieux pour garantir l'ouverture de la solution adoptée par le cabinet,
- Politique d'agrément des prestataires informatiques, validant que les prestataires maitrisent les différentes options techniques du boitier et disposent des moyens d'accéder au paramétrage du boitier en conformité avec les bonnes pratiques de sécurité.

4.2.2 INTERET ECONOMIQUE DE RPVA A BASE DE BOITIER NAVISTA POUR LA PROFESSION

Pour la profession, le projet NAVISTA dans la logique du monopole imposé par le CNB représente un investissement de l'ordre de 10,7 M€ seulement pour la partie NAVISTA, boitiers et frontal associé.

Nous remarquons que :

- Pour une bonne part, ces boitiers sont en doublons des routeurs-NAT déjà en place et sont utilisés à minima pour le seul accès à e-Barreau par le VPN propriétaire de NAVISTA,
- Le montant est justifié pour le renforcement de la sécurité de routeurs en place, alors que leurs insuffisances éventuelles n'ont été ni explicitées ni démontrées, et pour ouvrir la possibilité d'intégrer des solutions de sécurité et de télé-services dont le contour et le prix ne sont pas connus,
- La solution NAVISTA est une solution qui est en constante amélioration depuis 2007 et ses évolutions se font en dehors de tout cahier des charges formalisé par le CNB, et au sein d'un dispositif contractuel peu maitrisé.

Les plus sécuritaires apportés par l'utilisation de tunnels VPN et de pare-feu pour protéger les points d'accès à ce VPN, pour être effectifs, nécessitent que la sécurité de ces VPN et pare-feu soit attestée. Ils impliquent aussi une série de mises à niveau concomitantes, portant sur la sécurité des réseaux locaux, des serveurs, des postes de travail et de l'organisation en général, qui ne sont pas prises en compte par le projet technique de déploiement des boitiers RSA.

Dans ces conditions de double emploi, de valeur ajoutée sécuritaire conditionnée à des mises à niveau des cabinets hors du périmètre du projet RPVA et d'absence de maitrise contractuelle, la justification économique du réseau virtuel à base de boitiers RSA dans tous les cabinets nous semble problématique.

RECOMMANDATIONS :

Il nous parait important

- de mettre en place une conduite du projet RPVA qui précise les objectifs visés, en termes fonctionnels, techniques, économiques et de déploiement engageant les partenaires au sein d'un calendrier.
- de procéder à la formalisation de la reprise en main et de la réversibilité en cas de défaillance de NAVISTA,
- d'organiser conjointement la mise à niveau des points d'accès Internet et la mise à niveau de la sécurité au sein des cabinets. Une approche globale type ISO 27001 aborderait l'ensemble de ces points. Compte tenu de l'aspect service public de la profession dans sa dimension judiciaire, il nous paraitrait judicieux d'adopter les préconisations de l'ANSSI et son approche de l'ISO 27001 par la méthodologie eBIOS.

4.2.3 LA SOLUTION DE MARSEILLE A-T-ELLE UN INTERET COMPTE TENU DES DEUX SOLUTIONS DEJA EN SERVICE, PARIS ET CNB

La solution Marseillaise est une façon astucieuse de permettre l'accès au RPVA dans des conditions de sécurité acceptable et sans avoir à passer par le déploiement des boitiers RSA dans les cabinets marseillais.

Le sur chiffrement VPN SSL par certificat n'apporte pas de sécurité supplémentaire parce qu'il utilise le même certificat que le HTTPS et il impose une opération, minime, supplémentaire sur les postes des avocats.

D'autre part, si la solution Marseillaise devait être officialisée, le routeur Cisco ASA qui la constitue devrait être géré par le CNB. D'une part, cela simplifierait l'architecture actuelle qui impose de monter des boitiers RSA en batterie, et permettrait au CNB d'intégrer ce nouveau point d'accès à e-Barreau dans sa gestion de la sécurité. Ce ne serait donc plus la solution Marseillaise, mais une solution inspirée par Marseille.

La solution parisienne est déjà éprouvée et a fait l'objet d'une procédure d'intégration technique par le CNB. Elle dispose aussi de liens de haute capacité et redondés.

Dans ces conditions, si le principe dérogatoire qui offre la possibilité de ne pas passer par les boitiers RSA des cabinets était étendu, il nous semble que la solution du Barreau de Marseille ne démontre pas d'intérêt par rapport à la solution du Barreau de Paris.

D'autre part, si le principe dérogatoire devait être étendu, il nous semble que l'organisation de l'accès Https + Certificat, devrait être prise en charge depuis la plate-forme du CNB avec un dispositif qu'elle gérerait et dont elle maitriserait la sécurité.

Si la mise en œuvre technique par les prestataires du CNB devait être retardée par des considérations, contractuelles, techniques ou organisationnelles, alors la solution mise en œuvre par Paris ou une solution inspirée par l'architecture de Marseille pourrait constituer une solution temporaire acceptable.

Aussi, une des raisons qui nous conduit à dire que les solutions « Marseille » et « Paris » sont satisfaisantes pour la sécurité du transport des données, c'est qu'actuellement le facteur qui limite la sécurité n'est pas le chiffrement de la liaison, mais l'organisation des cabinets en terme de sécurité, sur laquelle nous n'avons pas de visibilité et qui est, aujourd'hui, hors du champ de contrôle du CNB.

Si le principe dérogatoire devait être étendu, il devrait être accompagné par un renforcement de la politique de sécurité au sein des cabinets. Des principes simples pourraient être rapidement mis en œuvre.

Aussi, les cabinets qui ont déjà intégré la sécurité dans leurs préoccupations et leurs pratiques, ne doivent pas être pénalisés et pouvoir continuer à utiliser des tunnels VPN pour se connecter à e-Barreau.

RECOMMANDATIONS :

Si la solution « Marseillaise » devait servir de base à la généralisation d'un accès dérogatoire, elle serait à réexaminer par le CNB qui pourrait s'en inspirer pour permettre l'accès hors boitier NAVISTA.

Si les délais de mise en œuvre au sein de la plateforme du CNB devaient être trop longs, et ainsi nécessiter une solution transitoire, alors la solution « Paris » ou en deuxième intention une solution inspirée de la solution Marseillaise pourraient être utilisées.

La baisse de sécurité induite par les accès dérogatoires, doit être compensée par une mise à niveau de la sécurité des ordinateurs, des réseaux, des pratiques des organisations utilisant ce mode d'accès. Le CNB pourrait formuler les principes élémentaires qu'auraient à respecter les cabinets d'avocats candidats à ces accès dérogatoires.

4.3 SYNTHESE

En terme de sécurité du transport, Paris et Marseille mettent en place des solutions théoriquement plus faibles que le celle du CNB qui n'apporte un gain effectif que pour les cabinets qui ont intégré la sécurité informatique aux pratiques de leurs cabinets.

Si la sécurité informatique des cabinets est une préoccupation pour l'ensemble des acteurs que nous avons rencontrés, nous n'avons relevé aucune démarche au niveau de la profession pour clarifier ce que seraient des objectifs et des pratiques de sécurité au niveau des cabinets.

Le boitier NAVISTA peut contribuer à cette sécurité au même titre que toute la gamme des services de sécurité offerts par le marché. Il offre l'avantage de venir dans un package combinant la plateforme technique, une organisation de support et la caution de la profession. Il peut avoir du sens pour les petits cabinets (1 ou 2 avocats) qui seraient autonomes sur la gestion de leurs ordinateurs et auraient ainsi un prestataire pour l'accès réseau.

A ce jour, NAVISTA n'a présenté aucun élément de certification, tant sur le protocole que sur l'intégration des composants informatiques ou l'organisation de gestion des boitiers qu'elle met en place. Cela nous semble plus une affaire de priorité dans l'agenda de NAVISTA qu'une faille structurelle de NAVISTA.

Le CNB s'est engagé à se doter des moyens nécessaires à la maitrise du RPVA, notamment en cas de défaillance de son fournisseur, avec un plan de reprise de main et des dispositions de réversibilité.

Sur ces deux points, certification « NAVISTA » et maitrise du fournisseur, NAVISTA et le CNB annoncent réévaluer leurs priorités.

Le principe du boitier déployé et télé-administré par le CNB.COM dans tous les cabinets, offre la possibilité de déployer rapidement des télé-services auprès des cabinets d'avocats. Le principe est séduisant, notamment dans la perspective de l'acte d'avocat qui imposera de déployer une fonction de coffre-fort électronique auprès des cabinets. Cependant, nous n'avons vu aucun plan projet décrivant ce que seraient ces déploiements, aussi bien sur les plans fonctionnels, techniques, économiques et calendaires.

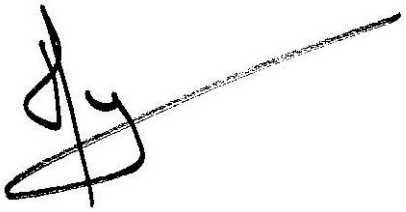
La question de la possibilité pour les barreaux de province d'utiliser d'autres solutions que celle du CNB, est à l'origine de cet audit.

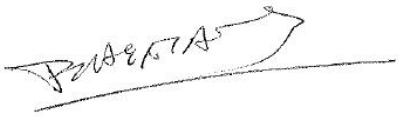
Nous ne pouvons pas faire de préconisations, dans la mesure où les enjeux dépassent largement la question technique.

Sur un plan purement technique, et si les objectifs politiques devaient évoluer, il nous semble que les solutions parisiennes et marseillaises ne montrent pas de carences qui les empêcheraient d'être ouvertes plus largement.

La solution marseillaise est plus à voir comme une « démonstration de capacité » et si elle était étendue, doit être reprise à sa charge par le CNB.

Finalement, l'état du système tant sur le plan de la sécurité que sur celui de la conduite du projet RPVA, nous semble justifier que dans le cadre d'une remise à plat, soient développés les aspects sécurité, organisation et lien avec les prestataires informatiques.





Nathan HATTAB

Philippe AYMAR

5 ANNEXES

5.1 ANNEXE 1 – L'ARCHITECTURE DES TROIS SOLUTIONS

5.1.1 L'ARCHITECTURE CNB MISE EN PLACE POUR L'ACCES A E-BARREAU

ARCHITECTURE GENERALE

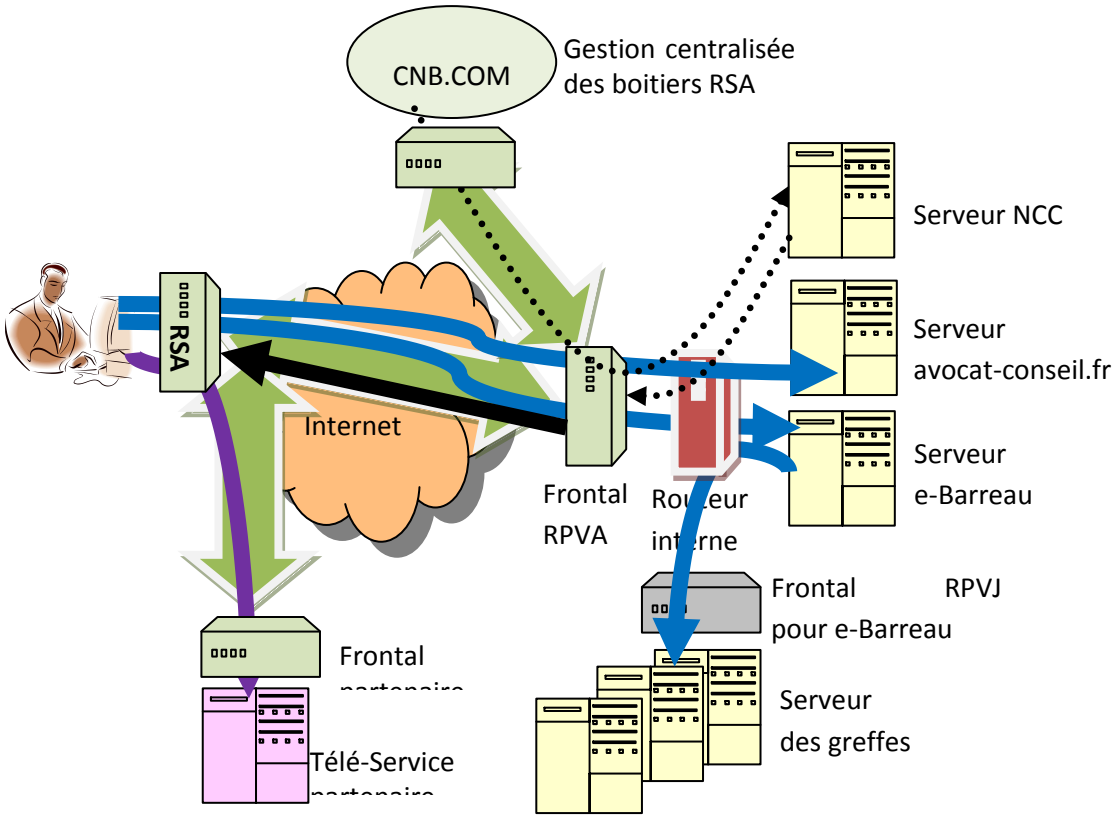
Le RPVA mis en place par le CNB s'appuie sur une architecture à base de boîtiers routeurs firewall-VPN NAVISTA pour connecter les différents services à Internet. La fonction VPN assure le chiffrement des communications et la fonction firewall, la sécurisation des installations vis-à-vis d'internet.

Les boitiers sont installés à l'accès Internet de chaque cabinet et de chaque ressource exploitée par le RPVA. Les boitiers sont contrôlés depuis le centre de gestion centralisée des boitiers RSA qui est coopéré par CNB.COM et NAVISTA.

L'avocat accède ainsi à sa boite (prenom).(nom)@avocat-conseil.fr par un canal sécurisé par VPN.

Il accède à e-Barreau par un canal sécurisé par VPN et HTTPS, l'authentification étant assurée par un certificat sur support physique.

Le centre de contrôle qui supervise l'ensemble des boitiers opère aussi via un canal sécurisé par VPN. Le serveur de contrôle sera à terme hébergé par CNB. L'administrateur transmet ses consignes au serveur NCC, qui les relaie au frontal. Le frontal les relaie aux boitiers RSA qui lui sont connectés.



LE RSA - BOITIER NAVISTA DEPLOYE DANS LES CABINETS

Le boitier qui est déployé au sein de chaque cabinet est en fait un ordinateur complet, compact et sans ventilateur (« fanless ») qui embarque une configuration de Linux orientée routeur-firewall-VPN-proxy.
Le même boitier équipé d'une configuration différente de Linux est déployé avec écran, clavier, souris, pour fonctionner comme terminal « client léger » dans les prisons.

Dans le cas du RPVA, il intègre :

- Un firewall Iptable, permettant le contrôle et le routage des flux,
- Un serveur DHCP d'adresses locales
- Un proxy de contrôle d'accès à Internet Squid,
- Un client et serveur VPN au protocole propriétaire NAVISTA « NTS »,
- Un client du logiciel NCC permettant le contrôle distant depuis le NCC pour le paramétrage et les mises à jour,
- L'accès des webservices pour des extensions de fonctionnalités,
- La capacité à prendre en charge deux connexions à Internet, l'une pour les flux prioritaires, l'autre pour les flux courants, et en cas d'incident, le report de l'ensemble des communications sur la ligne restante.

La carte « ordinateur » est fournie par Axiomtek et intégrée dans un boitier aluminium par NAVISTA. Selon NAVISTA, la carte choisie fournit une capacité suffisante pour chiffrer 70Mb/s, ce qui suffit aux besoins d'un cabinet. (à titre de comparaison, la plateforme parisienne observe un débit moyen de 0,5 Mb/s pour l'ensemble des avocats parisiens connectés sur e-Barreau en mars 2010).

LE NCC – CENTRE DE CONTROLE DES BOITIERS RSA

La supervision des boîtiers est réalisée à l'aide du NCC (NAVISTA Control Center) qui est la plateforme de supervision de NAVISTA. Elle intègre différentes fonctions :

- Un annuaire ou base de gestion administrative des boitiers RSA qui recense les boitiers, leurs paramètres en cours, l'abonné détenteur ainsi qu'une base de données des événements (tickets) associés aux boîtiers (problèmes rencontrés, demandes de support des prestataires, …
- Un outil de contrôle des boitiers permettant le paramétrage et la mise à jour des boitiers RSA connectés.
- Un outil de gestion d'accès aux différentes fonctions du NCC,
- Il existe aussi un outil de production et de déploiement des matériels d'accès, qui recense les boîtiers en production et qui n'ont pas encore été affectés.

NCC permet notamment de visualiser l'état d'un boitier RSA, de gérer ses mises à jour, de configurer ses services, notamment firewall et VPN.

Il permet de déléguer à un tiers de confiance (CNB.COM voire les infogérants des cabinets), la possibilité d'accéder de façon temporaire ou permanente au paramétrage d'un ou plusieurs boitiers.

Les fonctions qui peuvent être contrôlées à distance sont notamment :

- l'activation/désactivation de l'accès du boitier au RPVA,
- la mise à jour des logiciels des boitiers à chaque nouvelle version,
- la configuration du logiciel de contrôle de contenu lorsqu'il existera,
- la création de compte d'accès distant au réseau local, fonction dite de télétravail,
- l'interconnexion par VPN des réseaux de deux filiales, voire de deux cabinets,
- l'établissement d'une connexion spécialisée (exemple visioconférence) entre deux boitiers,
- la configuration de routes au sein du cabinet,
- l'autorisation ou l'inhibition de l'accès à certains services du cabinet depuis l'extérieur.

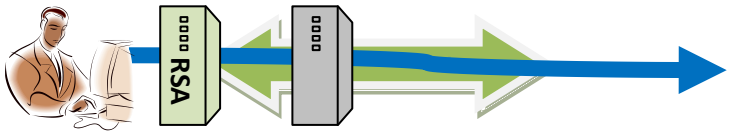
DIFFERENTES FORMES D'INSTALLATION DANS LES CABINETS

Les installations combinent plusieurs paramètres :

LE MONTAGE PHYSIQUE – EN CASCADE OU EN ETOILE

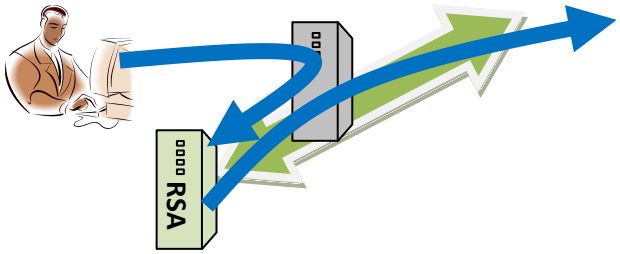
Dans le montage en cascade, le boitier RSA a deux câbles réseaux, l'un provient de la connexion internet (modem ou box ADSL), l'autre est branché sur le réseau local.

Tout le trafic réseau du cabinet traverse le boitier RSA, notamment celui à destination d'e-Barreau qui est automatiquement dirigé dans le tunnel VPN du RPVA.



Montage en cascade

Dans le montage en étoile, le boitier RSA ne reçoit qu'un câble réseau, qui est branché sur le réseau du cabinet.



Montage en étoile

Le réseau du cabinet est paramétré pour rediriger tout ou partie de ses flux vers le boîtier RSA qui fonctionne en passerelle.

Ce montage permet aux administrateurs de conserver le réseau en état de marche si le boitier RSA venait à tomber en panne.

Il n'est disponible que depuis peu.

L'ACTIVATION DU FIREWALL DU BOITIER NAVISTA (DHCP, DU ROUTAGE NAT)

Dans la plupart des réseaux informatiques, il y a plusieurs composants qui sont capables d'assurer la sécurité du réseau. La « box Internet », le routeur NAT du cabinet s'il en avait déjà un, le contrôleur de domaine si le cabinet a organisé son réseau.

Le boîtier RSA peut être paramétré pour assurer ces fonctions de sécurité ou laisser un autre composant les réaliser.

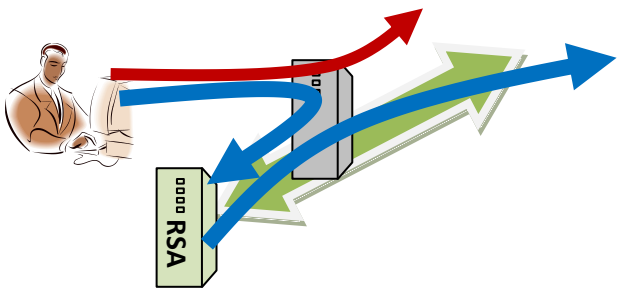
LA CONFIGURATION DU RSA COMME PASSERELLE

Il est impératif que le RSA soit configuré en passerelle sur les flux à destination d'e-Barreau pour que la fonction de cryptage soit activée et ainsi accéder au le RPVA. Cette passerelle peut être configurée :

- pour tous les postes (paramétrage global réseau) ou pour seul les postes concernées par e-Barreau (paramétrage au niveau des postes),
- pour tous les flux ou seulement pour les flux RPVA

Toutes les combinaisons sont possibles.

Par exemple dans l'illustration ci-dessous, les flux RPVA sont routés sur le RSA puis dans le VPN, les autres sont routés sur les infrastructures habituelles du réseau.



BILAN

Le boitier RSA est ainsi polyvalent et peut s'adapter à toutes les configurations réseau rencontrées par les installateurs.

Actuellement, les configurations « types » sont :

- Petit cabinet avec une « box ADSL » installant le RSA lui-même, sans passer par un installateur.

  Le boitier est monté en cascade et configuré comme firewall et passerelle.

- Petit cabinet avec une « box ADSL » passant par un installateur,

  Le boitier est monté en étoile, le réseau est configuré pour utiliser le RSA comme firewall et comme passerelle,

- Moyen cabinet avec une box ADSL, un firewall et un infogérant,

  Le boitier est monté en étoile, le réseau est configuré pour utiliser le firewall du cabinet et utiliser le RSA en passerelle, pour tout ou partie des postes,

- Gros cabinet

  Le boitier est monté en étoile, le RSA est cloisonné, et n'est utilisé comme passerelle que pour les flux RPVA,

En cascade	Flux seuls	65%
	Avec DHCP et routage NAT	
En étoile	Flux seuls	35%
	Avec DHCP et routage NAT	

NAVISTA n'a pas apporté plus de précision sur les statistiques de l'activation DHCP. Toutefois on a relevé que parmi les cabinets d'avocats visités, ceux qui avaient un prestataire infogérant n'ont pas activé les fonctions DHCP/NAT du boîtier RSA. Le prestataire a préféré utiliser les couches de sécurité sur lesquelles il avait la pleine maitrise.

L'AUTHENTIFICATION DES CONNEXIONS

La connexion à e-Barreau est sécurisée par le protocole HTTPS avec certificat sur support physique. Ce protocole utilise des mécanismes disponibles sur tous les navigateurs Internet.

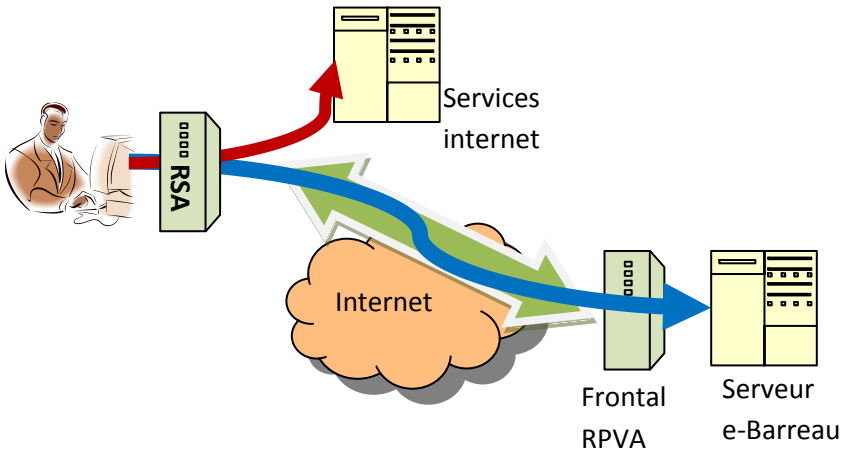
En cas d'accès hors du bureau, le travailleur nomade qui souhaite se connecter à e-Barreau, doit se connecter au routeur NAVISTA du cabinet. C'est possible par la solution de télétravail déployée par NAVISTA qui lui permet de se connecter par VPN à son cabinet.

La connexion au cabinet est sécurisée par un identifiant/mot de passe propre au travailleur nomade.

La gestion des accès nomades reste uniquement accessible par l'utilisation de la clé USB cryptographique.

L'ACCES DEPUIS LE BUREAU SELON LE CNB EN MODE TRAVERSANT

Dans ce mode tous les flux passent par le boitier RSA NAVISTA, que ce soit pour accéder à e-Barreau ou à d'autres services Internet.

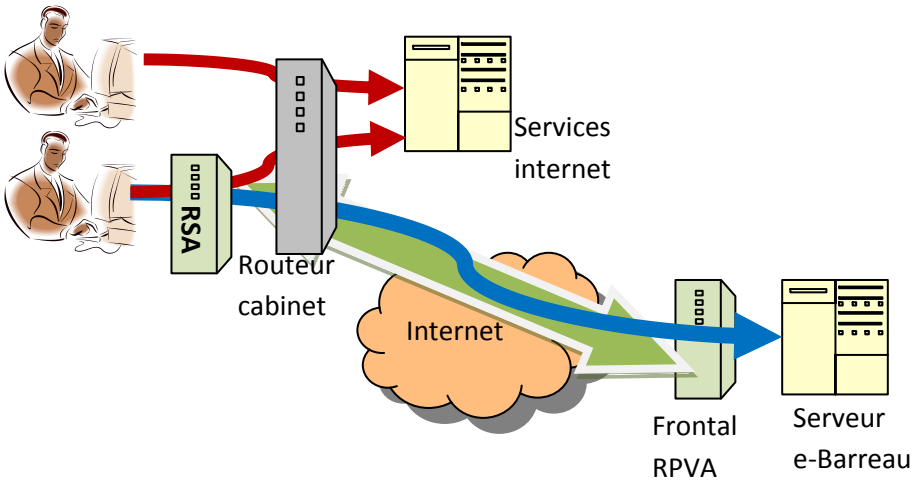


La flèche en vert désigne le tunnel VPN. Le flux en bleu est en HTPPS. Le flux en rouge n'est pas forcément en HTPPS.

Le modem routeur du bureau n'est pas représenté sur le schéma ci-dessus (entre le RSA et Internet) pour alléger la présentation.

L'ACCES DEPUIS LE BUREAU EN MODE PASSERELLE

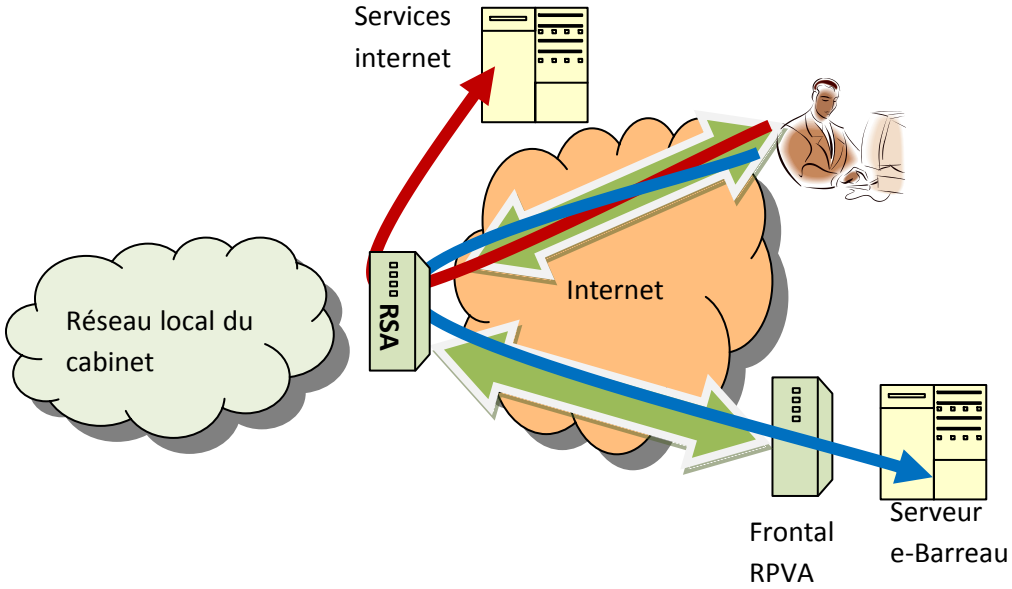
Dans ce mode les échanges avec e-Barreau passent par le boitier RSA et à l'intérieur du tunnel VPN mais d'autres échanges ne passent pas par le boitier RSA. Par contre tous les flux sont filtrés par un routeur du cabinet déjà en place.



Une partie du flux ne bénéficie pas des fonctions de routage et de sécurité du RSA.

L'ACCES HORS DU BUREAU SELON LE CNB

Ce mode permet à un avocat associé ou à un collaborateur après autorisation préalable d'accéder à distance au boitier RSA. L'établissement du tunnel VPN permet ensuite à cet utilisateur l'accès au service e-Barreau, s'il dispose de la clé d'authentification. Il peut aussi accéder aux serveurs du réseau local du cabinet, sous réserve qu'il dispose des identifiants et des mots de passe nécessaires.



Il faut remarquer que dans ce mode d'accès au service e-Barreau, le réseau local du cabinet n'est pas nécessaire. Pour fonctionner, l'accès distant n'a besoin d'avoir que le boitier RSA et le modem en état de fonctionnement. Il n'est pas nécessaire que le poste de l'avocat au bureau soit allumé pour accéder à e-Barreau.

5.1.2 L'ACCES PAR LA PLATEFORME DU BARREAU DE PARIS

LA PLATEFORME RELAIS PARISIENNE

La plateforme de connexion à e-Barreau proposée par Paris est un serveur relais localisé dans le centre d'exploitation de CertEurope. Le serveur est redondé et protégé derrière deux firewalls indépendants.

La connexion à la plateforme relais n'est possible que si l'avocat dispose d'une clé « Paris » et de son code Pin. La connexion est cryptée par SSL 128bits.

La clé « Paris » sert ainsi une fois, pour authentifier l'utilisateur sur la plateforme relais.

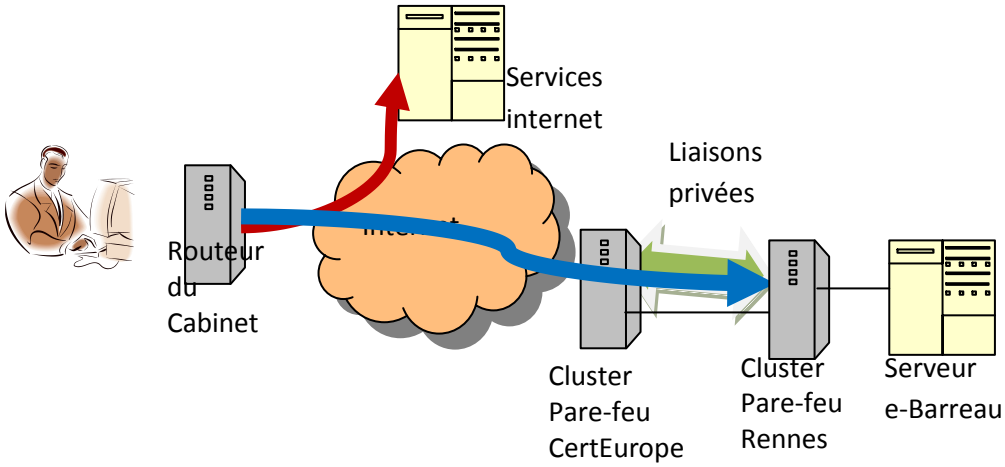
La plateforme parisienne relaie l'authentification sur e-Barreau (qui a été adapté à cette fin), aussi l'avocat qui se connecte à e-Barreau depuis la plateforme parisienne n'a à saisir son code pin qu'une seule fois.

Les autres services internet sont routés par les infrastructures habituelles du cabinet

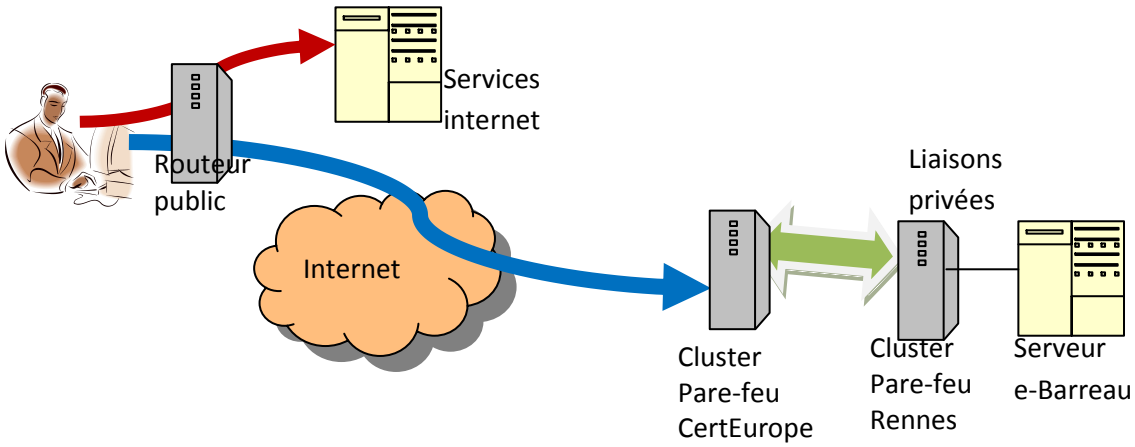
En cas d'accès hors du bureau, la configuration ne change pas. L'accès est permis grâce à la clé e-Barreau et les autres services internet (mail et Google par exemple) sont accédés par l'infrastructure locale.

L'ACCES DEPUIS LE BUREAU SELON PARIS

Les échanges vers e-Barreau peuvent se faire à partir du cabinet de l'avocat. Les systèmes de routage et de sécurité en place ou la simple « Box Internet » font office de pare-feu et de routeur.



L'ACCES HORS DU BUREAU SELON PARIS



5.1.3 L'ACCES PAR LE CONCENTRATEUR CISCO DU BARREAU DE MARSEILLE

L'ARCHITECTURE CISCO MISE EN PLACE PAR MARSEILLE

La plateforme de connexion à e-Barreau proposée par Marseille est un frontal Cisco ASA auquel l'avocat se connecte par VPN.

La connexion au VPN n'est possible que si l'avocat dispose d'une clé USB délivrée par le CNB. Le protocole utilisé est de type SSL à un niveau de chiffrement AES 256, c'est un protocole de niveau comparable au protocole propriétaire utilisé par NAVISTA pour son VPN.

La clé USB délivrée par le CNB, sert ainsi deux fois :

- La première fois pour authentifier l'utilisateur sur le frontal Cisco de Marseille,

- La deuxième fois pour authentifier l'utilisateur sur le serveur e-Barreau.

Le routeur CISCO ne relaie pas l'authentification sur e-Barreau, aussi l'avocat qui passe par la solution marseillaise saisira deux fois son code pin.

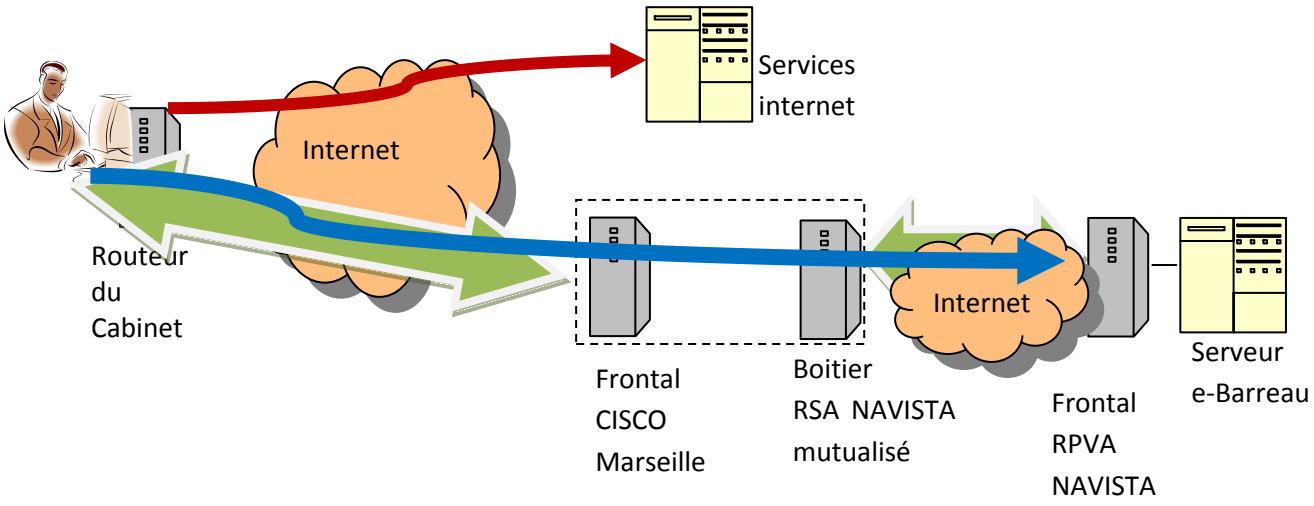
Les autres services internet sont routés par les infrastructures habituelles du cabinet

En cas d'accès hors du bureau, la configuration ne change pas. Le travailleur nomade établit directement un VPN sécurisé avec le frontal de Marseille depuis tout ordinateur connecté à Intenet. Les autres services internet sont accédés par l'infrastructure locale.

L'ACCES DEPUIS LE BUREAU SELON MARSEILLE

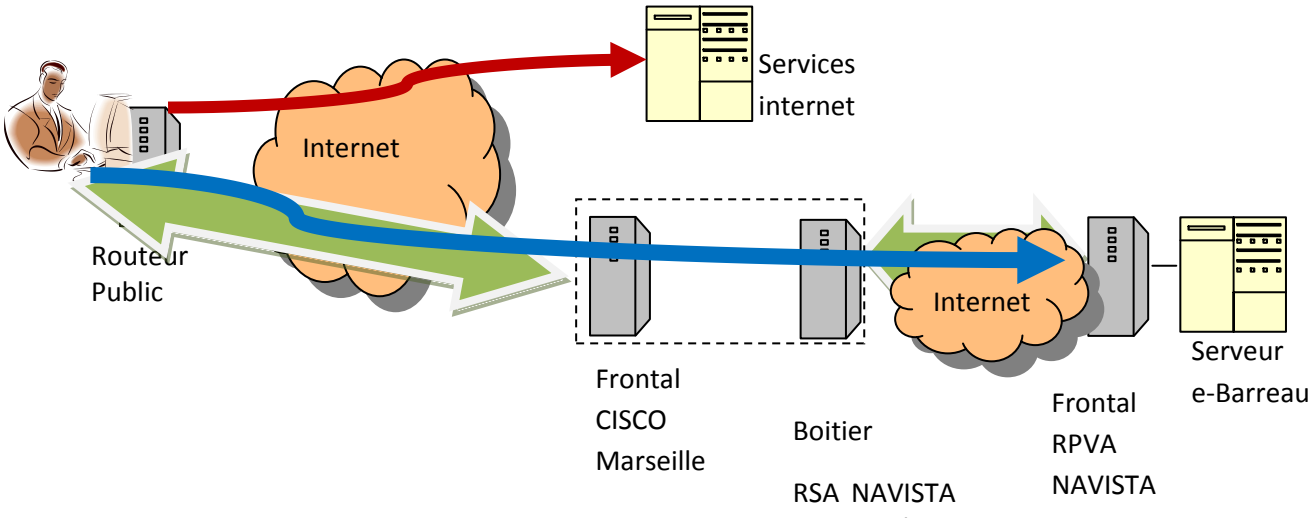
Les échanges vers e-Barreau peuvent se faire à partir au cabinet de l'avocat. Les systèmes de routage et de sécurité en place ou la simple « Box Internet » font office de pare-feu et de routeur.

Les flux passeront ensuite à travers le frontal CISCO de Marseille, le boitier RSA et le frontal RPVA NAVISTA avant d'être présenté au serveur e-Barreau



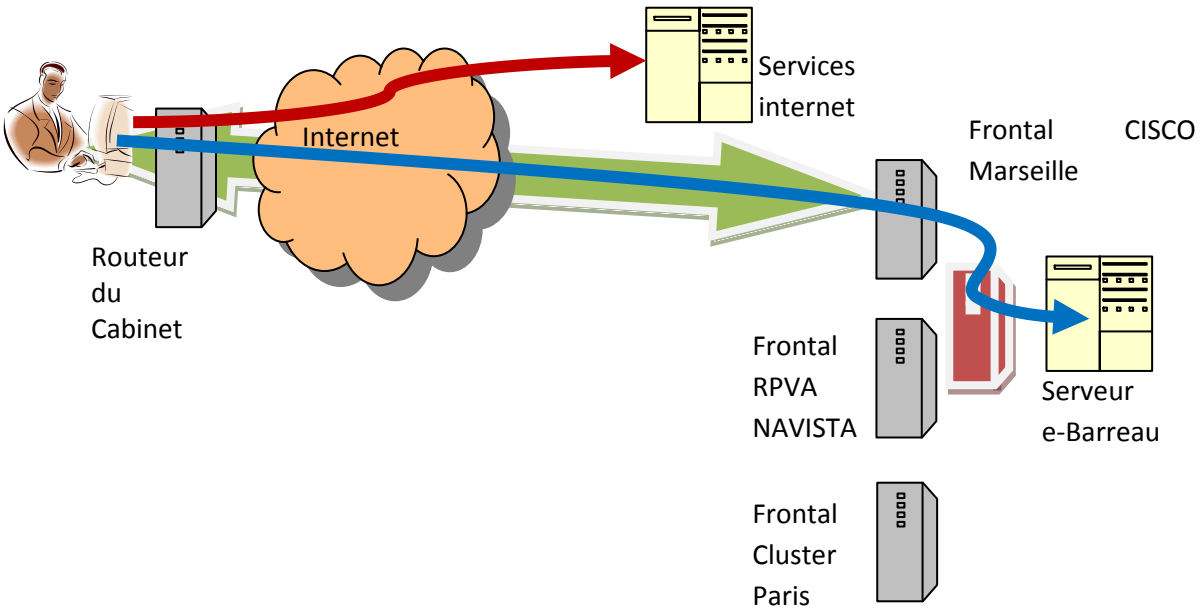
L'ACCES HORS DU BUREAU SELON MARSEILLE

Hors du cabinet l'avocat suit la même procédure de connexion



LA CONFIGURATION CIBLE POUR MARSEILLE

Marseille estime que l'utilisation de boitiers RSA mutualisés n'est que la résultante d'une contrainte anormale imposée par le CNB, et que le concentrateur CISCO devrait être comme pour Paris directement connecté au firewall du CNB à Rennes, soit en lien direct sur place, soit via une liaison spécialisée. L'ergonomie générale ainsi que le coût par avocat en serait encore amélioré.



5.2 ANNEXE 2 – LE BOITIER NAVISTA, QUALITE, PERFORMANCE ET SECURITE

La société NAVISTA a communiqué différents éléments relatifs à son boitier RSA et notamment à :

- la sécurité du firewall

  Il s'agit de la certification CSPN de la technologie, « Netfilter sur un noyau Linux v2.6.27 – Iptables v1.4.2 » que NAVISTA utilise dans son firewall. Navista ne justifie pas que son intégration respecte les conditions d'utilisation de ce noyau,

- le protocole propriétaire « Navista Tunneling system »

  Il s'agit de l'autorisation de chiffrer accordée par la DCSSI. Elle assure que les services de l'Etat sauraient déchiffrer les communications NTS en tant que de besoin. Elle n'apporte aucune démonstration sur le protocole utilisé et sa mise en œuvre.

- un cahier de test qui porte sur
  - La capacité des concentrateurs à supporter la montée en charge
  - La capacité des boitiers VPN à gérer de multiples accès
  - La capacité des boitiers VPN à gérer de la QoS
  - La capacité des solutions techniques retenues à basculer d'un Datacenter vers un autre en cas de problème

Nous relevons ici que :

Il n'y aucune étude d'adéquation réalisée par le CNB ou NAVISTA, pour justifier du dimensionnement des boitiers par rapport au besoin du RPVA :

- flux induits par le trafic avec les greffes
- prise en charge du trafic complet des cabinets,
- mise en œuvre du télétravail,
- services supplémentaires (filtrage de contenu, télé-sauvegarde,….)

Il n'y a aucun élément établi par un tiers indépendant qui justifie de la qualité du boitier, notamment sur ses performances en termes de sécurité.

- Sécurité du boitier – tests d'intrusion, tests de non régression,
- Sécurité du frontal - – tests d'intrusion, tests de non régression,
- Sécurité du tunnel « NTS » - agrément, certification

Il conviendrait au minimum que NAVISTA présente un Certificat de sécurité de premier niveau (CSPN) sur ces éléments. Le respect des certifications « Critères Commun » serait souhaitable.

Les choix d'architecture pris par NAVISTA sont classiques. La démonstration de sécurité semble être une affaire de priorité plutôt qu'une carence structurelle. Elle est néanmoins indispensable parce que la solution est propriétaire, déployée en petite série au sein de communautés restreintes et ouvertes sur internet. Ainsi, elle ne dispose pas d'un grand retour d'expérience qui permettrait d'apprécier et d'améliorer sa sécurité.

5.3 ANNEXE 3 –LES ENTRETIENS ET LES VISITES EFFECTUEES

31/03/2010 : M. S. SACCOCIO : Service Informatique du CNB – L'architecture du RPVA.

01/04/2010 : M. le Président de la Conférence des Bâtonniers : M. A.J.M. POUCHELON – Lettre à l'ensemble des Bâtonniers

01/04/2010 : Commission Nouvelle Technologie du CNB (Président Me GUERRINI, Vice Président Me PERRAULT, Me FAUGÈRES).

07/04/2010 : Ordre des Avocats de Marseille – M. le Bâtonnier D. MATTEÏ et Me J. JANSOLIN.

15/04/2010 : Cabinet BKP à VERSAILLES – Présentation du télétravail – (Me PERRAULT - M. SACCOCIO).

19/04/2010 : Site FlowLine ICT à VENISSIEUX – M. S. SCOTTO DI PERROTOLO – Présentation de l'infrastructure du RPVA Marseille.

20/04/2010 : Société NAVISTA – PERPIGNAN – M. J VINEGLA – M. LECLERCQ – Organisation et architecture technique RPVA à base de la solution NAVISTA.

21/04/2010 : Cabinet FIDAL – NEUILLY-SUR-SEINE – M. D. BEAULIEU – M. A. LEMOINE – M. S. SACCOCIO – Architecture technique d'un grand cabinet ayant intégré la solution NAVISTA.

21/04/2010 : Ordre des avocats de LILLE – M. le Bâtonnier R. DESPIEGHELAERE – Me TITRAN – M. S. SACCOCIO – La situation du Barreau de LILLE et les actions menées en faveur de la mise en place du RPVA à base du boîtier NAVISTA.

21/04/2010 : Cabinet comportant un avocat et un stagiaire avocat– LILLE –– Me TITRAN - M. S. SACCOCIO – L'intégration d'un boitier NAVISTA dans un petit cabinet.

23/04/2010 : Ordre des avocats de PARIS – M. le Bâtonnier J. CASTELAIN – Me X – Me A. BENSOUSSAN – M. T. BERTE – La solution du Barreau de PARIS hors des boitiers NAVISTA.

27/04/2010 : Me A. BENSOUSSAN - La solution du Barreau de Paris et les nouveaux services

03/05/2010 : Ordre des Avocats de Marseille - M. le Bâtonnier D. MATTEÏ, Me J. JANSOLIN et M. S. SCOTTO DI PERROTOLO. La solution du Barreau de Marseille

03/05/2010 : Visite de trois cabinets d'avocats de Marseille disposant d'un boîtier RSA Me GALLO, Me GUIDI, Me STALLA –Me J. JANSOLIN et M. S. SCOTTO DI PERROTOLO

07/05/2010 : Direction Informatique de l'Ordre des Avocats de PARIS – M. T BERTE – L'architecture technique de solution du Barreau de PARIS.

5.4 ANNEXE 4 - GLOSSAIRE

Adresse IP : Les ordinateurs connectés au réseau Internet, possèdent tous une adresse IP numérique. Dans la version actuelle IPv4, ces adresses prennent la forme xxx.yyy.zzz.aaa, où xxx, yyy, zzz et aaa sont quatre nombres variant entre 0 et 255. Aujourd'hui, l'adressage IPv4 est saturé. Dans la version IPv6, les adresses sont de la forme aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh, où a, b, c, d, e, f, g et h sont des caractères au format hexadécimal.

Pour faciliter l'accès à un serveur Internet, on a substitué à son adresse IP un nom plus simple à retenir, appelé **nom de domaine**.

Assistant numérique personnel est un appareil numérique portable, souvent appelé par son sigle anglais **PDA (Personal Digital Assistant***)* (Exemple : Iphone, Balckberry, …)

Certificat d'authentification a pour objet d'identifier une entité physique ou non-physique. Il fait le lien entre l'entité physique et une entité numérique. Il est attribué par une autorité de certification qui atteste de ce lien entre l'identité physique et l'entité numérique.

Un certificat d'authentification est un bloc de données comportant différentes informations dont un numéro de série, l'identification de l'algorithme de signature, la désignation de l'autorité de certification émettrice du certificat, la période de validité au-delà de laquelle il sera suspendu ou révoqué, le nom du titulaire de la clé publique, l'identification de l'algorithme de chiffrement et la valeur de la clé publique constitués d'une paire de clés asymétriques , … Lorsque le certificat est placé sur une clé USB, il est dit de classe 3+.

CNB.COM : Association loi 1901 mandatée par le Conseil Nationale du Barreau pour la mise en œuvre auprès des cabinets d'avocats du déploiement de l'accès réseau, notamment pour la centralisation des commandes d'abonnement des avocats au service RPVA.

DHCP (**Dynamic Host Configuration Protocol)** : A la fois protocole et serveur, dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station. Il associe à l'adresse physique MAC de la station une adresse IP dynamique. Dès lors, seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage et toute modification des paramètres du réseau est répercutée sur les stations lors du redémarrage.

DNS (**Domain Name System)** (ou système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

HHTP (**HyperText Transfer Protocol**) est le protocole inventé par l'organisme WWW (World Wide Web) pour assurer les échanges sur l'Internet entre des clients et des serveurs.

Les clients HHTP les plus courants sont les navigateurs tels qu'Internet Explorer, ou Mozilla FireFox. Ils permettent notamment à un utilisateur d'accéder à un serveur Web distant.

HHTPS (HyperText Transfer Protocol Secured) est la version sécurisée du protocole HTTP. Il s'agit de la simple combinaison de HTTP avec une couche de chiffrement telle que SSL. HTTPS permet au visiteur de vérifier l'identité du site auquel il accède grâce à un **certificat d'authentification**. Il garantit la confidentialité et l'intégrité des données envoyées par l'utilisateur et reçues du serveur.
Il est généralement utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc.

IPsec (Internet Protocol Security) est un cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques. Il se différencie des standards de sécurité antérieurs en n'étant pas limité à une seule méthode d'authentification ou d'algorithme.

Routeur est un élément intermédiaire dans un réseau informatique qui assure le routage des paquets de données binaires d'une interface réseau vers une autre, selon un ensemble de règles.

Routeur NAT (**Network Adress Translation**) ou Routeur (Traducteur d'adresse réseau) a pour rôle de traduire des adresses internes au réseau local en adresses externes, et vis-versa. Ce mécanisme permet de pallier la carence d'adressage de l'IPv4 d'Internet en faisant correspondre une seule adresse externe publique visible sur Internet à plusieurs adresses internes à un réseau privé. Le NAT dynamique utilise un numéro du port source de la machine interne pour l'identifier.

RPVA (Réseau Privé Virtuel des Avocats) : Réseau indépendant à usage privé de communications électroniques réservées aux avocats inscrit à un tableau de l'Ordre d'un Barreau français.

RSA (**Routeur Sécurisé Avocat**) est le nom du boitier NAVISTA spécialement mis au point pour le réseau RPVA.

Pare-feu (*firewall* en anglais), dans le contexte d'un réseau informatique, désigne un logiciel et/ou un matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, en autorisant ou en interdisant certains types de communication.

Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent, et notamment celles qui proviennent d'Internet.

Le filtrage se fait selon divers critères, dont les plus courants sont l'origine ou la destination des paquets (adresse IP, ports, etc.), les données elles-mêmes (taille, correspondance à un motif, etc.), les utilisateurs, ...

Proxy (**ou serveur mandataire)** est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs proxy sont notamment utilisés pour assurer les fonctions de journalisation des requêtes (« logging »), de sécurité du réseau local ou de filtrage.

SaaS (**Software as a Service**) est un concept consistant à proposer un abonnement à un logiciel plutôt que l'achat d'une licence. De plus en plus d'offres **SaaS** se font au travers du Web. Il n'y a alors plus besoin d'installer une application de bureau ou un logiciel client.

Serveur informatique est un ensemble composé de logiciels et de l'ordinateur qui les héberge. Son rôle est de répondre de manière automatique par des services à des requêtes ou demandes envoyées par des clients.

SNMP (Simple Network Management Protocol) est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux, matériels à distance.

SMTP (Simple Mail Transfer Protocol) est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

SSL (Secure Socket Layer) : ancien nom du protocole **Transport Layer Security** (**TLS**). Il s'agit d'un protocole de sécurisation des échanges sur Internet, développé à l'origine par Netscape et dans lequel l'utilisateur authentifie le serveur sur lequel il se connecte.

Cette authentification est réalisée par l'utilisation d'un certificat numérique délivré par une autorité de certification.

Le certificat de l'utilisateur peut être stocké au format numérique sur le poste client ou sur un support matériel (carte à puce, token USB).