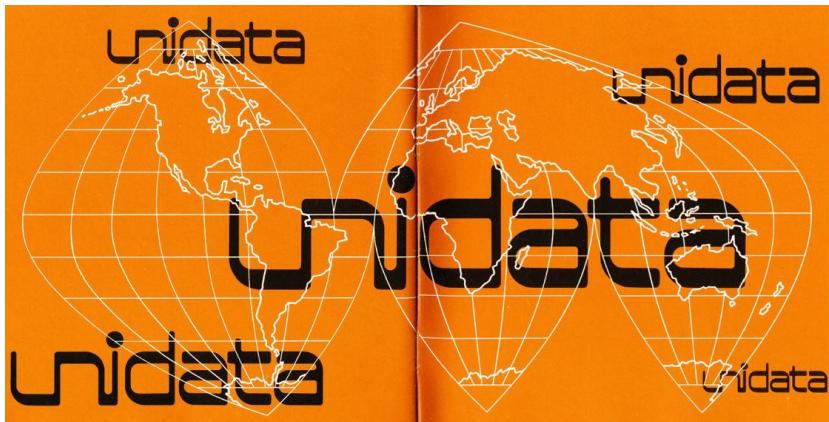


Vers une informatique européenne souveraine
1975 La stratégie **unidata** 2025

- Une histoire
- Une vision
- Des récits

Témoignage de Guy Maréchal



1975 : Le sabordage de l'informatique européenne

2025 : L'émergence d'une souveraineté informatique européenne

**Marie d'Udekem-Gevers
Guy-Noël Maréchal
Roger Roberts**

Avec des contributions de :



Adrien Brysse
Bernard Durieux
Claude Fosseprez
Yves Genin
Georges Goeman

Jean-Marie Pétronio
Jean-Jacques Quisquater
Steny Solitude
Jean Voisin
Ferdinand de Wasseige

Partie III : Témoignages

Dans cette partie, notre intention est de donner la parole à des témoins qui présenteront transversalement la vie industrielle et industrieuse de l'époque. Ces fragments devraient mieux montrer le contexte, la vie de l'intérieur de la période qui a suivi Unidata jusqu'à nos jours.

Ces fragments montrent aussi l'influence tout à fait significative et de longue durée que le projet de la Machine mathématique IRSIA-FNRS et l'aventure Unidata 7.720 ont eu, au travers des destins de ceux qui y ont collaboré, mais aussi du dynamisme et des opportunités qu'offrait un grand groupe, comme l'était Philips dans les années 60, et de grands hommes qui dirigeaient des équipes et des projets ambitieux et éclectiques. Ces témoignages illustrent aussi le passage de l'analogique au numérique tant sur le plan technique que sociétal.

Nous tenons à remercier le professeur Jacques Neirynck, qui nous a chaudement encouragés de nous exprimer de manière « vécue » via ces témoignages !

Les pistes pour la souveraineté informatique européenne présentées au chapitre 5 découlent directement des expériences, visions, réalisations de ces témoins.

En pratique, chaque témoignage sera introduit sommairement. Le lecteurs désireux de découvrir les témoignages complets pourront le faire en y accédant via un QR Code.

Chapitre 7 : Témoignages de et sur Claude Fosseprez

Chapitre 8 : Témoignage de Guy Maréchal

Chapitre 9 : Témoignage de Jean Voisin

Chapitre 10 : Témoignage de Georges Goeman

Chapitre 11 : Témoignage de Ferdinand de Wasseige

Chapitre 12: Témoignage de Jean-Jacques Quisquater

Chapitre 13 : Témoignage de Bernard Durieux

Chapitre 14 : Témoignage de Roger Roberts

Chapitre 15 : Témoignage de Steny Solitude

Témoignage de Guy Maréchal

Au cours de cette vie professionnelle j'ai eu la chance de participer à des activités, des projets très variés. Avec le recul je suis heureux d'avoir contribué à ce que je considère des avancées majeures ; mais je suis aussi déçu d'être passé à côté de potentialités que ce soit par manque d'ambition ou suite à des obstructions managériales, politiques ou économiques. Mais, il ne faut pas se méprendre, l'essentiel est le fait de la collaboration efficace d'équipes enthousiastes !



Je suis particulièrement fier d'avoir contribué à l'émergence des amplificateurs paramétriques qui furent le fondement du système de sécurité des réacteurs nucléaires de première génération ; d'avoir contribué à l'émergence de la carte d'identité belge ; d'avoir contribué à l'adoption internationale d'une méthode de mesure de la qualité des fibres de laine, fondement du commerce de la laine et d'avoir largement fait la promotion de la représentation sémantique des informations.

Je suis particulièrement déçu que je ne sois pas parvenu à convaincre les pouvoirs publics de la nécessité de refonder le droit au moment de l'éclosion de l'informatique pour le grand public et la généralisation de son usage dans les entreprises et organisations ; de même, pour n'avoir pas su convaincre les représentants de la Commission Européenne de garder le contrôle du Web en collaboration avec l'INRIA ; de même d'avoir été si près de la mise en place de services publics informatiques en collaboration avec Belgacom et La Poste belge.

Je réalise aujourd'hui que, dans les années 90, les réseaux de télécommunication auraient pu être organisés pour exploiter la complémentarité d'Internet et de l'ATM et que bien que nous ayons réussi un sans-fautes dans le démonstrateur des potentialités de l'ATM, nous n'avons plus pas tenté de rebondir, de convaincre d'entreprendre ...

Mon témoignage se termine au basculement du siècle. Mais, j'ai continué à être actif dans le domaine jusqu'aujourd'hui, notamment dans le cadre de projets européens, pour l'UNESCO et pour diverses associations sans buts lucratifs, en particulier TITAN.

Mon témoignage est disponible en PDF via le QR Code ci-joint. En 82 pages j'ai tenté de raconter ma vie professionnelle dans toute sa variété. Elle est balisée en six phases que je caractérise par les noms des personnes clés impliquées dans ces périodes :



1.1 UNIVERSITÉ de LIÈGE :

Professeurs Marcel Linsman et Charles Massonnet

1.2 Mon entrée à MBLE :

Jacques Vorobitchik, Vitold Belevitch et Raymond Schayes

1.3 Bureau d'Études Ordinateurs :

Claude Fosseprez

1.4 Projets MBLE pendant la période « NatLab »

Gaston Bastiaens

1.5 Philips Research Centrum

Jakob Vlietstra

1.6 Philips Professional Systems

Jacques Berleur, Jacques van Haren, Dirk Frimout et Melchior Wathelet

1.1 Université de Liège

Professeur Marcel Linsman et Charles Massonnet

En mi-1957 j'ai mon diplôme de « Candidat Ingénieur Civil » et je dois choisir quel type d'ingénieur je souhaite devenir. Avec la terminologie d'aujourd'hui, l'on dirait que j'ai mon baccalauréat [à l'époque, les candidatures duraient deux ans] et que je dois choisir quel Master [à cette époque le Master durait trois ans] je souhaite suivre.

À cette époque je bricole beaucoup en électronique, notamment pour construire des chaînes audio en haute-fidélité. J'envisage de devenir Ingénieur acousticien, d'autant plus qu'il y a une section forte de ce type à l'Institut Universitaire Montefiore, une des sections de l'Université de Liège.

Finalement, je choisis de devenir Ingénieur Électronicien et de prendre deux compléments :

- Le Master complémentaire **d'Ingénieur Architecte**. En effet, à cette époque, il était possible de cumuler ces deux masters. Ce cours visait à donner la formation nécessaire au calcul de la résistance des matériaux et de la stabilité des ponts, des grues, des locaux industriels ... et marginalement des maisons à appartement avec ascenseurs. Ce cours était donné par le Professeur Charles Massonnet. Pour avoir le droit de signer des plans, il fallait faire un stage dans un bureau d'architecte accrédité pour les études de stabilités (ce que je n'ai pas fait). J'étais aussi évidemment attiré par l'acoustique des bâtiments.
- Comme cours à option, je choisis un tout nouveau cycle de trois années intitulé « **Traitements des informations par les machines** ». Aujourd'hui, l'on désignerait ce cycle de cours comme « **Formation à l'Informatique** » ; mais cela serait réducteur, car, à cette époque, le cours couvrait non seulement les « **Machines numériques** », mais aussi les « **Machines analogiques** ». Quatre élèves se sont inscrits pour suivre ce cycle. Il était donné par le Professeur Marcel Linsman qui partageait son temps entre l'enseignement à l'Université de Liège (comme assistant du professeur Bureau et du professeur Dacos) et une collaboration avec la Machine mathématique IRSIA-FNRS à Anvers. Le programme était comme suit :

A. Introduction générale :

Essentiellement une introduction aux trois mots clés de la définition du cours [Machine / Information / Traitements]. Il va mettre l'accent sur trois types de machines et montrer comment chacune traite de l'information :

1. Les machines numériques mécaniques

La machine aux **quatre opérations** ODHNER en est l'une des plus belles.



Figure 1: La ODHNER de légende !

Les bouliers compteurs: le professeur Linsman nous a expliqué comment additionner, soustraire, multiplier et diviser avec les bouliers compteurs chinois à deux registres et double report. L'on peut aussi les utiliser en base 16 [Hexadécimal].

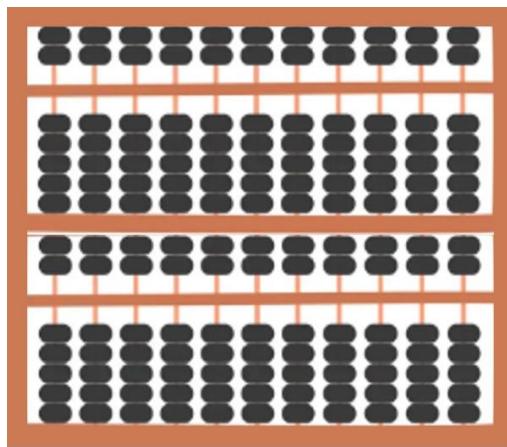
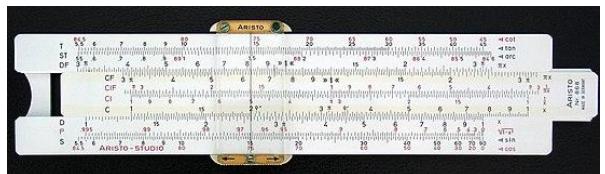


Figure 2 : Boulier à deux registres

2. Les machines analogiques

Nous savions déjà tous comment se servir des règles à calcul basées sur les logarithmes. Elle est capable d'effectuer des multiplications et des divisions ; le calcul des logarithmes, des fonctions trigonométriques et exponentielles.



Je possède encore ma règle à calcul de cette époque : elle avait sa place dans une poche spéciale de mes vestons jusqu'aux années 80.

Les machines de **calcul opérationnel** qui réalisent les quatre opérations, les dérivées et les intégrales par une approche analogique grâce à des ‘amplificateurs opérationnels’.

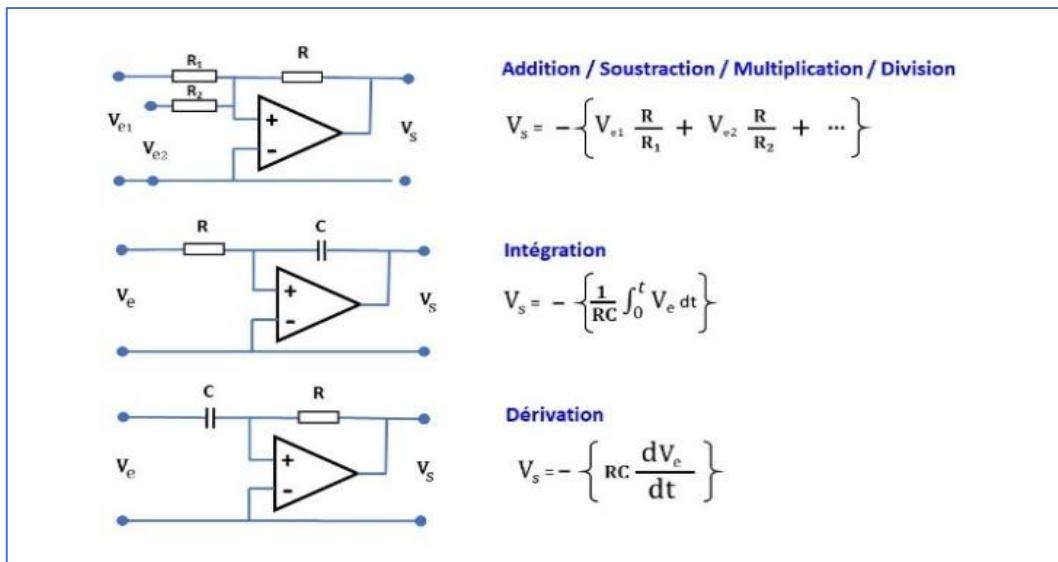


Figure 3: Les machines de calcul opérationnel

L'Université de Liège possédait une telle machine dans le département du professeur Dacos, en charge de la chaire d'électronique et physique théorique. Ces machines, comme le montre la figure, sont capables de réaliser les quatre opérations, la dérivée et l'intégration de fonctions temporelles. Il s'agissait probablement d'un OME P2, à tubes électroniques, de la firme SEA (Paris). Le professeur Dacos me donna comme travail de fin d'études [TFE] l'étude des possibilités d'améliorer la précision et la stabilité de cette machine. Elle disposait de plus d'une douzaine d'amplificateurs opérationnels ; d'une batterie de résistances et de condensateurs ; d'un '*patch panel*' permettant de définir l'équation que l'on voulait simuler. Ce type de machine est par définition instable pour l'intégration, car elle supporte le coutant continu : l'initialisation à zéro devait se faire périodiquement ou juste avant de longs calculs. J'ai mis au point une procédure et une technique facile à mettre en œuvre pour augmenter la précision et la stabilité de cette initialisation. L'élément essentiel étant d'utiliser le patch panel pour l'initialisation, de le câbler avec des câbles coaxiaux isolés au téflon et de définir une méthode et protocole d'initialisation du système et des calculs. Ce qui a conduit à une amélioration très significative de la précision et de la stabilité.

3. Les machines numériques programmables : les traitements

Enfin et surtout, évidemment, le calcul booléen et les machines de traitement numérique électroniques. Le professeur Linsman nous a essentiellement introduit la structure dite « Von Neumann »²

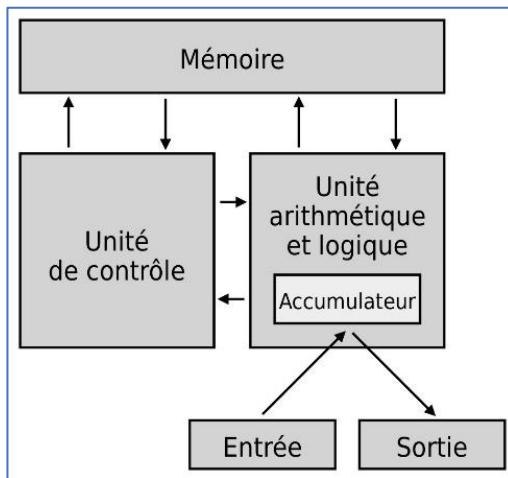


Figure 4: L'architecture dite architecture de von Neumann

L'architecture dite **architecture de von Neumann** est un modèle pour un ordinateur qui utilise une structure de stockage unique pour conserver à la fois les instructions et les données demandées ou produites par le calcul. De telles machines sont aussi connues sous le nom d'ordinateur à programme enregistré. La séparation entre le stockage et le processeur est implicite dans ce modèle.

Pour ce qui touche aux traitements, trois aspects étaient enseignés :

- A **L'algèbre de Boole**, ou calcul booléen, est la partie des mathématiques qui s'intéresse à une approche algébrique de la logique, vue en termes de variables, d'opérateurs et de fonctions sur les variables logiques, ce qui permet d'utiliser des techniques algébriques pour traiter les expressions à deux valeurs du calcul des propositions. Elle fut lancée en 1854 par le mathématicien irlandais, George Boole. L'algèbre de Boole trouve de nombreuses applications en informatique et dans la conception des circuits électroniques.³

B La programmation : Essentiellement l'étude du FORTRAN et quelques algorithmes optimisés pour les classements, le tri et autres calculs de base. Plus tard, à partir des années 1970, Donald Knuth rassemblera ces « best practices » dans un ensemble de livres qui seront au chevet des programmeurs durant de nombreuses années : « *The Art of Computer Programming* ».

C La modélisation : Essentiellement l'approche des Machines à États-finis

Le professeur Linsman s'est ici révélé grand pédagogue. En introduction il nous a demandé de tenter de réaliser le circuit électrique d'un ascenseur destiné à un immeuble de trois étages et cave. Nous pouvions utiliser autant de relais et de contacts sur ces relais que nous voulions. Aucun d'entre nous n'y est parvenu. Puis il nous a expliqué l'approche des modèles à états finis et, pas-à-pas, il nous a guidés pour réaliser le câblage des commandes de l'ascenseur. Enfin, il nous a expliqué que l'on pourra un jour commander des ascenseurs par des machines Von Neumann style et, plus généralement, modéliser des processus via des « Machines à États finis ».

L'Expo-58 et l'ordinateur IBM-650 du pavillon des USA

L'Expo-58 est un choc pour moi. J'y vais trois fois ! Je suis particulièrement fasciné par la première horloge atomique (au pavillon de la Suisse), par les bâtiments à l'architecture inventive (la flèche du génie civil ; le pavillon Philips ; le pseudo-tube de MBLE ; le pavillon américain ...), par les ordinateurs exposés dans de nombreux pavillons, en particulier dans le pavillon des USA et dans celui d'IBM (tout proche de celui de la MBLE).

En fin 1958, le professeur Linsman annonce qu'il a conclu un accord avec la délégation américaine auprès de l'Expo-58 pour que le système d'ordinateurs IBM-650 qui y était exposé soit mis en dépôt à l'Université de Liège sous sa direction plutôt que d'être rapatrié aux USA. Cet ordinateur est basé sur des tubes à vide, un codage des nombres en biquinaire et des périphériques basés sur les cartes perforées. Il consommait plus de 15 kW ! IBM venait de sortir sa nouvelle gamme d'ordinateurs basés sur l'État Solide (transistors plutôt que tubes à vide). La fiabilité de l'IBM 650 était très faible : elle tombait en panne plusieurs fois par jour. Il fallait identifier puis remplacer le tube à vide défectueux et, après initialisation, elle repartait.

Le code biquinaire est un système de codage des valeurs 0 à 10 au moyen de 7 bits, c'est-à-dire 128 valeurs.

Le premier bit représente la valeur « 0 » par « 0 » et la valeur « 5 » par « 1 ».

Les cinq bits suivants couvrent les chiffres de 0 à 5 : représentent la valeur « 0 » par « 0 » et la valeur « 1 » par « 1 ».

Le chiffre représenté est la somme des valeurs attribuées aux bits.

Exemple : la chaîne de bits suivante 1 0 0 0 1 0 0 signifie « 5 + 3 » soit « 8 ».

En sus d'être redondant (ce qui permet d'identifier la plupart des pannes), ce système permet de représenter la dizaine de deux façons, ce qui permet de résoudre élégamment le calcul des reports.

La console de la IBM-650 visualisait directement le biquinaire : deux lampes horizontales et cinq verticales en dessous !



Figure 5 : Console de commande de l'IBM-650 ! 4

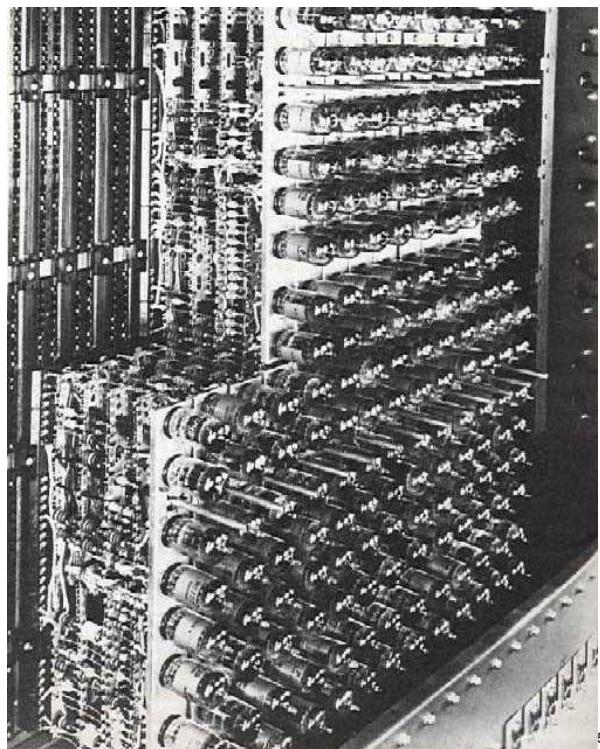
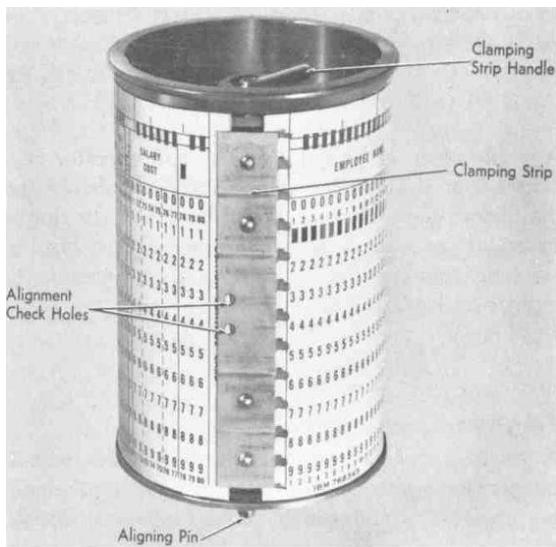


Figure 6: Mémoire vive de l'IBM-650



de cartes perforées (cela s'exprimait en mètres d'épaisseur). Programmer les perforatrices pour que l'on puisse imprimer le contenu des cartes perforées de manière lisible⁷: en particulier le FORTRAN. Cette programmation se faisait en utilisant une carte perforée spéciale montée sur un cylindre qui structurait la perforation et l'impression du programme. Vérifier des programmes écrits en FORTRAN.

Nous disposions aussi de tas de cartes perforées correspondant à des routines directement exécutables qu'il fallait assembler, car IBM ne nous avait pas donné l'assembleur SOAP [*Symbolic Optimal Assembly Program*] qu'il venait de développer.

Donald Knuth raconte qu'en 1957, jeune étudiant, il a découvert l'informatique sur une IBM 650 et que ses premiers pas en programmation consistèrent à développer un assembleur et des programmes de calcul et de jeux. Pour rappel, c'est Donald Knuth qui est l'auteur de la série monumentale de référence TAOCP [*The Art Of Computer Programming*] ! Il y affirme que programmer est un art, l'art d'expliquer des choses à un ordinateur.

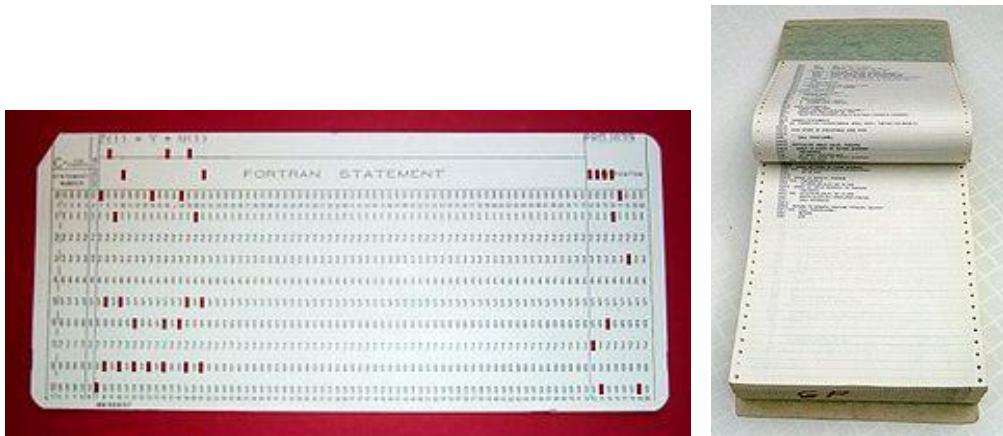


Figure 7: Carte perforée servant à formater la perforatrice et les impressions

Comme cet accord n'avait pas été programmé dans les budgets de l'Université, le professeur Linsman ne pouvait mobiliser que peu de ressources. Il a reçu un assistant à temps plein et un budget d'opération minime. Il a alors largement demandé si des élèves ne seraient pas disposés à devenir « élèves – assistants » argumentant que ceux qui accepteraient y gagneraient beaucoup en savoirs, mais peu en francs. Gérard Thibaut et moi avons accepté.

Le professeur Linsman nous confiait des tâches de base : Traduire en français la notice de la perforatrice IBM-026 // Organiser les étagères où l'on plaçait les programmes exprimés sur des tas

Nous avions aussi des tâches d'opérateur. Une tâche particulière nous était confiée en cours d'exécution : les programmes écrits en FORTRAN étaient d'abord compilés vers un langage appelé FORTRAN-IT. Le résultat était mémorisé sur des cartes perforées par le lecteur / perforateur de l'IBM-650. Lors de l'exécution des programmes, il y avait des étapes programmées pour générer un « dump » [copie de l'état de la machine] de la situation à cette étape. Comme il fallait souvent plusieurs heures pour qu'un programme donne ses résultats et, comme l'ordinateur tombait souvent en panne, l'on s'assurait par cette approche d'aboutir à obtenir plusieurs résultats de programme par jour. Si l'ordinateur tombait en panne, l'on recommençait le calcul en cours au dernier « dump » avant la panne.

Le professeur Linsman avait pris un accord avec le professeur Massonnet pour se servir de l'IBM-650 afin de calculer des structures hyperstatiques.

Jusqu'alors, usuellement, les calculs ne couvraient que des structures statiques en réseaux de poutres reliées par des nœuds considérés comme mobiles axiaux.

Cas de charge	Moment de flexion	Effort tranchant	Divers
① Charge uniformément répartie	$M_x = \frac{qL^2}{2}$ pour $x_0 = \frac{L}{2}$ $M(x) = \frac{qx^2}{2} (L-x)$	$V_A = \frac{qL}{2}$ $V_B = \frac{qL}{2}$ $V(x) = \frac{qL}{2} - qx$	Fleche (f) $f = -\frac{5}{48} \frac{qL^4}{EJ}$ pour $x = \frac{L}{2}$
② Charge concentrée P	$M_x = \frac{P(x-a)}{L}$ pour $x_0 \approx a$	$V_A = R_A$ $V_B = -R_A$ $V_{22} = R_A$ $V_{12} = -R_A$ V_{21} signifie V entre A et C	$S = a + b + \frac{L}{2}$ $R_A = \frac{P}{2}$ $M_A = \frac{P^2}{4} \cdot \frac{L}{2}$ $f = -\frac{PL^3}{48 EI}$
③ Charge répétée (symétrique)	$R_A = \frac{qL}{2}$ $R_B = R_A$	$V_A = R_A$ $V_B = -R_A$	Avec $P = \frac{qL}{2}$ $R_A = \frac{P}{2} + R_S$ $M_A = \frac{PL}{4}$ $V = 0$ pour $x = \frac{L}{2}$
④ Charge à répartition variable	$R_A = \frac{qL}{6}$ $R_B = \frac{qL}{3}$	$V_A = R_A$ $V_B = -R_A$ $V = 0$ pour $x = \frac{L}{\sqrt{3}}$	Avec $P = \frac{qL}{2}$ $R_A = \frac{P}{2} + R_S$ $M_A = \frac{PL}{4}$ $V = 0$ pour $x = \frac{L}{2}$
⑤ Charge uniformément répartie	$M_1 = 0$ $M_2 = -0.125qL^2$ $M_3 = 0$ $M_4 = -0.125qL^2$	$M_1 = 0$ $M_2 = -0.125qL^2$ $M_3 = 0$ $M_4 = -0.125qL^2$	Pour $a = b = L/2$: $M_1 = \frac{qL^2}{24}$ $M_2 = \frac{qL^2}{24}$ $R_A = \frac{2}{3} R_S$ $M_A = \frac{2PL}{9\sqrt{3}}$ Fleche = $\frac{qL^4}{3456 EI}$
			Moments en travée $M_{1,2} = 0.075qL^2$ $M_{3,4} = 0.075qL^2$
			Cas de deux travées $R_1 = 0.375qL$ $R_2 = 1.25qL$ $R_3 = 0.375qL$
			← Actions des appuis

Exemple de formules de calcul des treillis



Figure 8: Exemple de pont treillis⁸

Le professeur Massonnet avait piloté une équipe qui avait péniblement réalisé le calcul très long et très difficile d'une structure hyperstatique en caissons. Il avait démontré que l'on pouvait alléger la quantité d'acier par rapport aux approches traditionnelles (constructions en acier avec rivets) en réalisant des modules hyperstatiques et en laissant des degrés de liberté pour les dilatations thermiques.

Il avait en particulier largement contribué à calculer le pont de Commerce de Liège⁹(devenu Pont Albert I) qui était en cours de construction en remplacement du pont détruit pendant la guerre. Le pont provisoire était tout à fait insuffisant.



Figure 9: Le pont Albert I en cours de construction en 1956¹⁰



Figure 10: Le pont Albert I termine en 1960¹¹

Cette approche hyperstatique est radicalement différente des ponts usuels de l'époque et donne une élégance incomparable ! Pour renforcer cette finesse, cette légèreté, l'éclairage du pont est (et est encore maintenant) réalisé dans les mains courantes des balustrades bordant les deux trottoirs.

Les calculs sur l'IBM-650 avaient pour but de refaire les calculs qui avaient été effectués précédemment (à la main) et à comparer les prédictions avec la réalité lorsque le pont a été construit et a été mis en charge avec de nombreux gros camions pour tester la stabilité. Des capteurs (appelés « *strain gauges* ») mesuraient avec précision les déformations dues aux charges des poids de ces camions, ce qui permettait d'induire la capacité de résistance des divers éléments du pont et vérifier si les calculs avaient bien prédit cette mise en tension.

En 1959, le professeur Massonnet a créé une des premières ‘Spin-off’ de l’Université et initialisé une tradition de compétence de l’Université de Liège pour le calcul de structures architecturales

innovantes. Aujourd’hui, le bureau Greisch de Liège est dans cette continuité. Il est un des bureaux d’ingénierie et d’architecture les plus pointus d’Europe, sinon du monde ! Depuis sa création, il a conçu ou participé à plus de 5.000 projets dans plus de 20 pays, dont le calcul du fameux ‘Viaduc de Millau’ au centre de la France.

Il est aussi remarquable que dans le pont Albert I^{er}, l’usage du béton armé y est vraiment très limité et toujours pour des structures accessibles des supports sur les berges. L’ossature du pont est réellement un enchaînement de caissons soudés réalisés en acier passivé.

L’IBM-650 était toujours en service lorsque, fin 1961, j’ai quitté l’université pour faire mon service militaire.

Marcel Linsman et l’Intelligence Artificielle en 1961

À cette époque, à Trooz où je suis né, un groupe de jeunes, dont j’étais, avait créé une association culturelle qui organisait des conférences sur de nombreux sujets. Pour ces soirées, une mécène, Evelyne Servaye, mettait les salons de son château à la disposition de notre association. Le professeur Marcel Linsman a accepté mon invitation d’y donner une conférence. Il nous a présenté sa vision de la place de l’informatique dans la société. C’est à cette conférence que j’ai entendu pour la première fois le mot « épistémologie » ! Quel titre prémonitoire : « Les Machines à Penser (Utopie & Réalité) ». Il pensait déjà à l’Intelligence Artificielle !

Voici copie de la page du livre d’or où il a signé :

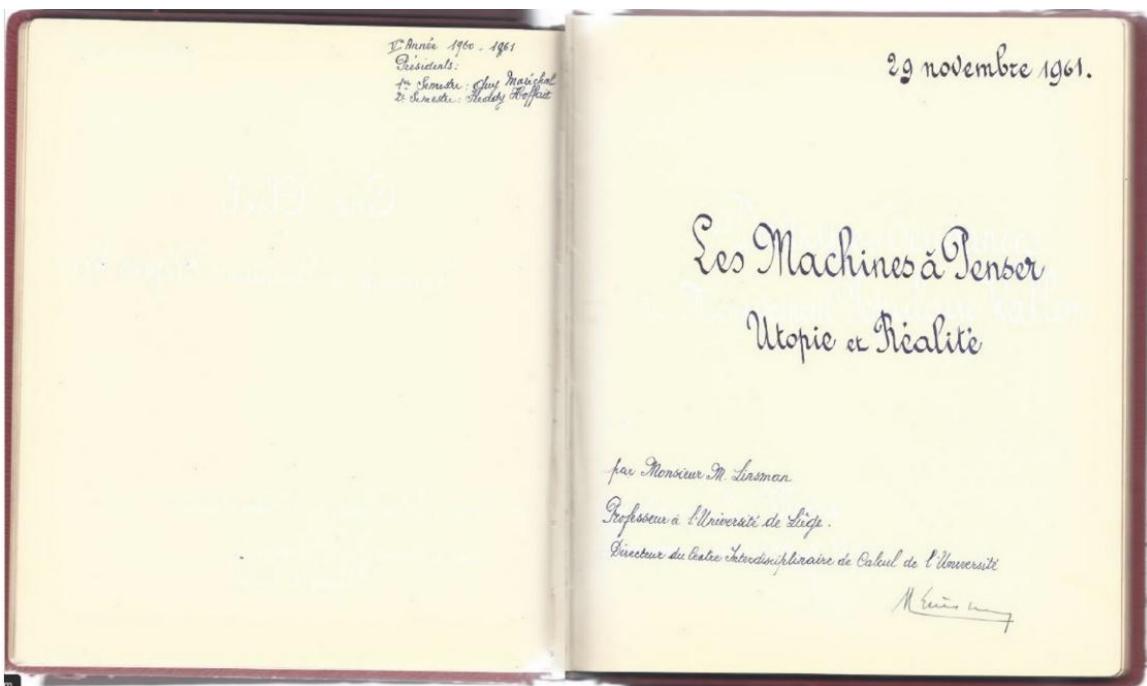


Figure 11: Les Machines à Penser (Utopie & Réalité)

1.2 Mon entrée à MBLE (1963 – 1971) :

Jacques Vorobeitchik & Vitold Belevitch & Raymond Schayes

Mes champs de recherche :

Textile / Nucléaire / Bases de données EARE « Entity Attribute Relationship Event »

En décembre 1962 je passe un entretien de candidature (corsé par le challenge d'imaginer un schéma électronique pour un filtre à haut facteur « Q » à état solide) pour être engagé aux « Bureaux d'Études » de la MBLE. Je suis interviewé par Stéphane de Vleminck, chef de l'un des départements des Bureaux d'Études, celui de la téléphonie et des télécommunications [BETT], accompagné par Yves Lebon, son adjoint. Ce département utilise de nombreux filtres de spectre suivant des techniques analogiques. Dans son livre « Essai de 'Réminiscience' », Pierre-Jacques Courtois montre à quel point les travaux de Vitold Belevitch sont essentiels pour le calcul de tels filtres. Dès 1947, mais surtout en 1955 (page 87 du livre), les besoins en filtre deviennent de plus en plus complexes : l'approche par « Matrice de Répartition » révolutionne le calcul des filtres analogiques !

Cet entretien a lieu rue Bara, là où sont les locaux du département BETT. Vu l'avis positif, je reçois immédiatement un avant-projet de contrat d'engagement. Dans les jours qui suivent, je l'accepte.

Lorsque, ayant terminé mon service militaire comme « Officier de Réserve », je me présente, en début mars 1963, au Service du Personnel (oui, à cette époque, le département des « Ressources Humaines » s'appelait comme cela) l'on m'annonce que je ne travaillerai pas au BETT, mais dans un autre département, car une restructuration était en cours. L'on m'explique que les Bureaux d'Études Techniques de la MBLE sont dirigés par Yvan Hecq et qu'il a un adjoint, Jacques Vorobeitchik, qui le conseille, qui accueille les nouveaux ingénieurs et qui coordonne la partie scientifique, théorique et de publication des études et projets. J'apprends que ma réorientation était la conséquence de la démission inopinée d'un ingénieur du Bureau d'Études de l'Instrumentation Scientifique [BEIS], département dont le chef était Raymond Schayes. L'ingénieur démissionnaire (dont je ne me rappelle plus le nom) m'invite à son « pot d'adieu », le soir même, et m'encourage à démissionner aussi : il m'explique qu'il avait reçu un « pont d'or » pour aller travailler dans la nouvelle usine de Texas-Instruments, sur les hauteurs de Cannes dans le parc scientifique « Sophia Antipolis » en création et qu'ils recrutent encore ! Il y fera une brillante carrière.

Le lendemain, lors de ma première rencontre avec Jacques Vorobeitchik, il me dit s'appeler en fait Ladislas, mais que, en pratique, il avait adopté le prénom de Jacques ! Il me présente deux autres jeunes ingénieurs, qui sont eux aussi en tutorat chez lui. Je me souviens de leurs noms : Jean-Claude Decroly et Marc Dieudonné. J'apprends que la décision est prise : je suis membre du BEIS, affecté (à 1/5^{ème} du temps) dans l'équipe de Jacques Vorobeitchik ; affecté (à 4/5^{ème} du temps) au projet ALMETER de BEIS. Marc Dieudonné, de même, est détaché (à 1/5^{ème} du temps) chez Jacques Vorobeitchik tout en étant membre du Département « Bureau d'Études Astronautique et Militaire » [BEAM], dont le chef est Marcel Vigneron. Jean-Claude Decroly, de même, est détaché (à 1/5^{ème} du temps) chez Jacques Vorobeitchik tout en étant membre du Bureau d'Études Téléphonie et Télécommunications [BETT] de Stéphane de Vleminck.

Le lendemain, je me présente au BEIS. Raymond me dit que :

Un expert externe, Joseph Grignet (Président de la Fédération Lainière Internationale), dont les bureaux sont à Verviers, va m'introduire la problématique à résoudre par un appareil, en cours de développement au BEIS, l'« ALMETER ». Il s'agit de mesurer les caractéristiques d'échantillons de laine ou de coton afin d'établir une base d'estimation de la valeur de lots de matière brute textile : quel type de fil peut-on filer avec cette matière ? quelle qualité (solidité, souplesse, finesse ...) pourrait-on obtenir avec ce type de matériau brut ?

Jacques Vorobeitchik m'introduira à la méthodologie de mesure prévue. L'adjoint au démissionnaire, Thierry le Fevere, m'introduira aux plans et au développement en cours.

Le département commercial en charge des activités textiles (dont l'ALMETER est l'un des produits prévus d'être commercialisé) a comme chef (Henri-)Jacques Randaxhe.

En résumé, il m'introduit l'organigramme de la MBLE de 1963 présenté dans la Partie I (Figure XXX).

La finalisation du développement de l'ALMETER va prendre toute l'année 1963. Les principes étaient bons, mais de nombreux détails laissaient à désirer et la précision restait tout à fait insuffisante. Heureusement, rapidement j'identifie les problématiques, les erreurs de conception et trouve une solution de correction ou de contournement. Les premiers tests sur le prototype finalisé ont lieu à l'automne 63. En début 1964 la commercialisation de l'ALMETER commence.

Le département BEIS a d'autres développements que le textile. Il y a notamment le développement de dosimètres pour le contrôle des radiations reçues par des personnes travaillant avec des substances radioactives : la dosimétrie par double électroluminescence. C'est cette technologie qui a été montrée au Roi Baudouin en 1961 (voir le chapitre 1)

En 1964 je continue à perfectionner l'ALMETER et je développe son complément, le DB-Computer. C'est à cette occasion que j'exploiterai ma compétence en calcul opérationnel : le DB-Computer comporte six amplificateurs opérationnels. En 1967, Jacques Randaxhe et moi publions un long article dans la « revue mble » sur l'instrumentation textile.

Ce Volume X N°3 de la revue fera date, car il rassemble trois articles particulièrement pertinents :

- La collaboration entre l'Industrie et l'Université en matière de recherches (par Jacques Neirynck)
- La structure et le fonctionnement des calculatrices digitales (par Claude Fosseperez [Chef de groupe au Laboratoire de recherches de la MBLE (Groupe « Calculatrices digitales)])¹²
- Un nouvel appareil pour l'Industrie textile le DB-Computer (par G. Maréchal et H.J. Randaxhe).

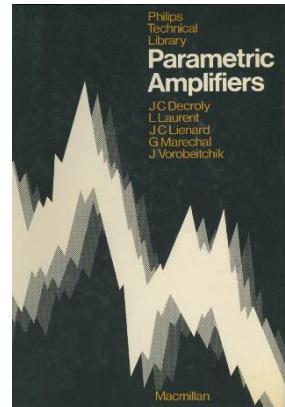
En 1967, je suis envoyé à Boston au MIT pour contrôler la laine qui servira à faire les fils prévus pour réaliser les habits des astronautes d'Apollo 11. En 1969 je suis invité par le ministère du commerce américain pendant 3 semaines à New York : expliquer les avantages de la méthode de mesure, détailler la justification théorique et mettre au point un protocole expérimental visant à évaluer la précision de la méthode et valider sa répétabilité.

En 1973, la méthodologie et les principes des trois équipements de mesure exposés dans cet article seront adoptés comme référence pour le commerce de la laine. Cette adoption semble toujours valable, car en 2016 j'ai encore eu une demande de validation d'un nouvel équipement conçu pour respecter cette méthodologie et ses principes de réalisation.

En fin 1963 ou début 1964, Philips Eindhoven commande à MBLE le développement du triple système et de la triple chaîne de contrôle de la future centrale nucléaire expérimentale qui doit être installée à Den Haag par Westinghouse, en collaboration avec Philips. Les validations doivent se faire au centre d'étude nucléaire belge de Mol. L'approche était d'avoir une chaîne de mesure linéaire qui mesurait l'activité du réacteur ; d'avoir une chaîne logarithmique qui mesurait essentiellement les fluctuations d'activité du réacteur, en vue de surveiller sa stabilité ; et une chaîne différentielle qui suivait les montées et descentes en puissance du réacteur. Chacune de ces chaînes était réalisée en trois exemplaires, chacun contrôlant si les deux autres mesuraient la même chose via un système de vote ultra-fiable (un risque ultra-faible de panne pendant une période ultra-longue). Je suis impliqué dans ce projet car Jean-Claude Decroly et moi imaginons les « Amplificateurs paramétriques à phase cohérente dégénérés » complètement à état solide. Cette innovation a été induite par le système de mesure des fibres textiles et a été mise en œuvre de manière simple grâce à un choix technologique astucieux de Jean Van Praet. C'est cet équipement qui sera fondement pour les trois chaînes de contrôle de la sécurité des réacteurs nucléaires de première génération de Westinghouse. À cette époque Westinghouse n'avait pas de solution à état solide. En 1965 Philips prend un brevet sur ce type d'amplificateur et le vend à Westinghouse. En septembre 1966, je donne, à Bâle, une conférence¹³ à la « Foire Internationale de Industries

Nucléaires » [nuclex-66] sur les possibilités et avantages déterminants d'appliquer ce type d'amplificateur dans les systèmes de mesure et de sécurité des réacteurs nucléaires.

En 1968 (version 2 en 1973) [je ne retrouve pas mon exemplaire]), je rédige l'un des chapitres du livre « *Parametric Amplifiers* » (un gros livre qui sera publié chez MacMillan Press Ltd) dont la rédaction est coordonnée par Jacques Vorobeitchik, lequel d'ailleurs en a écrit les principaux chapitres théoriques. La base conceptuelle de ces amplificateurs a été donnée en 1956 dans un article remarquable de MANLEY (J. M.) et ROWE, (H. E.) : *Some general properties of non-linear-elements*. L'essentiel du livre s'appuie sur les systèmes non-dissipatifs non-linéaires. D'une part, le cas des hautes fréquences y est traité, en particulier pour les applications dans les communications avec les satellites. Ma contribution s'adresse aux basses fréquences, jusqu'au continu. Cette approche s'avère radicalement nouvelle ! C'est à l'occasion de l'écriture de ce livre que je rencontre Jean-Claude Liénard et Louis Laurent.



En 1965, Jacques Vorobeitchik m'implique dans un programme de recherche, financé par la FNRS belge, exécuté en collaboration avec ITT [Anvers], SAIT [Bruxelles] et le ACEC [Charleroi]. C'est à cette époque, avec ces subsides FNRS, que je finalise la mise au point des « Amplificateurs paramétriques à phase cohérente dégénérés ».

Comme dit précédemment, l'essentiel du livre sur les amplificateurs paramétriques se rapporte aux hyperfréquences. En effet, à cette époque c'est la seule façon d'assurer la communication hertzienne à haute sensibilité requise pour les liaisons entre le sol et les satellites. Le besoin est crucial pour la MBLE à qui la Belgique a confié sa partie du programme ELDO. ELDO est l'acronyme de *European Launcher Development Organisation*.

Ce programme vise à doter l'Europe d'un lanceur de satellites. La base de lancement étant au nord de l'Australie. La Belgique, sous la coordination de la MBLE, y fut en charge de la guidance des deux derniers lancements. En effet, comme aucun des 10 lancements qui ont été réalisés (depuis le 5 juin 1964) n'ont jamais pu mettre un satellite en orbite, la décision fut prise d'arrêter ELDO.

À l'occasion de l'écriture du livre, je me lie d'amitié avec plusieurs des 'co-writers' du livre, en particulier Jean-Claude Liénard (responsable du développement hardware).

Par affinité culturelle, je tisse des liens avec Claude Vigneron (le chef du département BEAM), Michel Lorthioir (le Directeur Commercial), Christian Derouck¹⁴ (Chef du projet ELDO) et Marc Dieudonné. Ces trois dernières personnes étaient intéressées par énormément de secteurs culturels : musique, littérature, artisanat ethnique, dessin

Marc Dieudonné était l'ingénieur qui fut le responsable de la station de guidage radio installée au nord de l'Australie dans la péninsule de Gove ; la station de lancement était à Woomera au sud de l'Australie). La station de Gove fut pleinement opérationnelle en 1968. Le premier des lancements qui aurait dû être guidé par la station terrestre installée par la MBLE fut la « tentative F8 » : ce fut un lamentable fiasco, l'échec fut tel que la station de guidage n'a pas pu être validée. Le second des lancements qui a été le dernier des lancements « tentative F9 » (en début 1970) fut de nouveau un échec, car il ne permit pas de satelliser le satellite expérimental de l'Italie. Quelques années plus tard, l'on identifiera que l'échec avait été dû à un mauvais fonctionnement d'un boulon explosif de la coiffe. La qualité du fonctionnement de la station de guidance fut elle démontrée (un sans-faute).

À une date que je n'ai pas reconstituée (1970 ?), Jacques Vorobeitchik décède d'un cancer. Yvan Hecq ferme alors le « Bureau de Recherches Scientifiques », mais organise que ce soit Vitold Belevitch qui continue le tutorat scientifique que Jacques Vorobeitchik assurait. Il reprend aussi le rôle de coordinateur FNRS. Vitold Belevitch n'est pas très enclin à de telles coordinations : il n'en organisera pas dans le cadre de la recherche fondamentale telle que pratiquée à PRLB. Mais, il prend ce rôle très au sérieux ! Je me souviens que, lors d'une réunion FNRS à Anvers, Vitold Belevitch a

effectué une critique virulente d'une contribution d'un des membres des ACEC qui avait plagié des travaux japonais.

Il faut remarquer que, lorsqu'il est devenu le directeur de PRLB, Vitold Belevitch était connu comme l'inventeur d'une méthode de calcul de filtres de signaux analogiques (voir le livre de J.-P. Courtois) et un des théoricien des caractéristiques respectives des langages naturels (humain) et artificiels (informatique). C'est lui qui m'a suggéré une méthode de filtres mixtes (analogique et échantillonnage numérique) pour l'industrie textile.

Indépendamment de la collaboration FNRS, il me confie de collaborer à un programme de recherche du PRLB (Boitsfort), coordonné par Marc Davio, concernant les bases de données en EARE [*Entity Attribute Relationship Events*]. La puissance de modélisation de cette approche est exceptionnelle ! C'est une généralisation de la modélisation par des 'Machines à États Finis' que le Professeur Marcel Linsman m'avait enseignée. Mais il apparaît rapidement que les technologies de l'informatique des années 1960-80 sont incapables de réaliser des produits logiciels utilisables basés sur ce niveau conceptuel. Ce sera bien après, en 2012 je crois, que j'ai assisté pour la première fois à la démonstration de la puissance et de la simplicité de l'approche : Franck Casado, travaillait à l'époque pour Memnon Archiving Services. Il avait développé une base de données sémantiques ayant les concepts de « Vecteur d'État » et de « Processus sémantiques » : l'intention était de modéliser les processus de numérisation des archives « audio » de la British Library : une merveille !

Dans les années 1990, en collaboration avec l'INRIA [France], je reprendrai l'approche EARE dans le cadre du projet CIM-OSA dont je fus le coordinateur scientifique (voir plus loin). Là encore, cette approche de modélisation sémantique des données ne sera pas commercialisée dans SAP, mais ici pour de mauvaises raisons.

Cette approche sera retenue pour les langages de contrôle de processus exigeant des garanties de qualité en « temps réel » conduisant à des langages de type CHILL et ADA. Cette approche sera aussi déterminante, plus tard, dans l'élaboration du Web-Sémantique.

En 1969-70, de nombreux bouleversements vont secouer les Bureaux d'Études de MBLE :

Philips décide de vendre (pour un pont d'or¹⁵) à Westinghouse la technologie, les brevets¹⁶ et les plans des triples trois chaînes de contrôle des réacteurs nucléaires. Complètement à l'état solide et présentant une sensibilité et une sécurité inégalée, ces amplificateurs dépassent largement les performances des équipements de Westinghouse de l'époque encore basés sur des tubes à vide, bien moins fiables et difficiles à réparer.

Philips décide de vendre (à bon prix) à Zellweger (la firme Suisse de référence dans les équipements textile) toutes ses activités 'laine et coton'.

Philips décide d'arrêter les développements dans le domaine spatial. En effet, le programme européen ELDO a été arrêté suite au double échec de derniers lancements des satellites. Sous la direction de Claude Vigneron, l'équipe de développement [Jean-Claude Lienard] et l'équipe opérationnelle [Marc Dieudonné] sont mis en attente.

Le financement du développement de la seconde génération d'avions sans pilote [drones] développée pour les applications militaires est mis en attente par l'armée belge.

Un nouveau bureau d'études est créé : le « Bureau d'Études des Ordinateurs » [le BEO].

Ces bouleversements seront à la fois essentiels pour la réussite de la création du BEO ainsi que traumatisants :

Toutes ces terminaisons d'activités vont libérer du personnel pour constituer les équipes nécessaires au BEO. Ce personnel est formé et a travaillé sur des projets avancés exigeant un haut niveau de compétence et de qualité : le spatial ; le nucléaire ; le militaire.

Certaines personnes s'intégreront rapidement dans le BEO et rapidement l'activité de développement commencera : c'est le cas notamment d'équipes issues de PRLB, en particulier,

Luc Crousel et Bernard Martin ; et la force de développement du BEAM conduite par Jean-Claude Liénard.

Certaines personnes n'y trouveront pas leur place, en particulier Claude Vigneron ! Il décide de quitter la MBLÉ pour devenir le directeur technique de SAIT ; il essaye d'emmener avec lui certains de ses collaborateurs et de ceux de Raymond Schayes.

À ce moment je fus très déçu de l'arrêt des deux activités où je travaillais et où j'avais pu faire mes preuves. Claude Vigneron me propose de le rejoindre à SAIT comme chef du développement Hardware et responsable de la « Qualité ». J'envisage sérieusement de quitter la MBLÉ.

Au même moment, une proposition constructive m'est faite par Claude Fosseperez que j'accepte rapidement. En début 1971 je rejoins le BEO.

Le département « Radio & Applications Électronique », n'ayant plus les applications ciblées (textile, nucléaire, dosimétrie ...), change de nom pour devenir le BERA [Bureau d'Études Radio] dont Raymond Schayes reste le chef. Malgré mon transfert au BEO, je reste malgré tout proche de Raymond. C'était un ingénieur imaginatif, un peu brouillon dans les mises en œuvre, mais brillant dans des fulgurances. Parfois il était d'une distraction légendaire tellement concentré sur la résolution des problèmes. Un jour où j'étais allé à PTI Hilversum avec lui dans sa petite Renault Juvaquatre, nous avions convenu de nous retrouver à 16h00 au parking près de sa voiture. Ne le voyant pas arriver, je m'enquiers auprès de son contact : il me dit que la réunion avait été courte et que Raymond Schayes avait repris son train en début d'après-midi. J'attrape le dernier train pour rentrer à Bruxelles. Le lendemain, ne le voyant pas dans son bureau, je demande à sa secrétaire ; elle me dit qu'il est à la police pour déclarer que l'on lui avait volé sa voiture !

Il me plaît de profiter de cette occasion pour signaler que c'est au BERA que sera mis au point, pour les besoins des militaires, le premier système de transmission radio réellement confidentielle et résilient parce qu'auto-reconfigurable. L'approche consistait en une modulation à bande latérale unique, contrôle de phase et sauts de fréquence basés sur des générateurs pseudo-aléatoires synchronisés [Raymond Schayes et Roger Gourlet en étaient les pionniers]. Cette approche implique une précision et une stabilité très haute du générateur d'onde. Ils adopteront la configuration de la vibration d'un cristal asservissant le générateur d'onde via une boucle de rétroaction synchronisée en phase. Ces approches combinées serviront d'inspiration aux modulations en FSK [*Frequency Shift Keying*], en QPSK [*Quadrature Phase-Shift Keying*] adoptées, 20 ans plus tard, par la télévision numérique.

1.3 Bureau d'Études Ordinateurs (1971 – 1982)

Claude Fosseperez

Mes champs de recherche : Computer Aided Design / Configuration Management / Unidata

- Je suis accueilli chaleureusement au BEO par Claude Fosseperez qui confie à Marc Dieudonné ma formation initiale. Lui aussi avait été sollicité par Marcel Vigneron pour le rejoindre chez SAIT. Il y a beaucoup d'animation, beaucoup de nouveaux ... mais cela fonctionne. Les pré-études sont en cours et des réalisations partielles de prototypes ont déjà été faites. Marc me donne à étudier de nombreux documents techniques liés aux technologies choisies (TTL essentiellement ; pour des raisons de performance, une petite partie sera en ECL) ; les choix de représentation des divers types de données (purement binaire avec des mots de 32 bits) ; la technologie des circuits intégrés multicouches avec trous métallisés

Mais ce qui est essentiel pour le futur concerne le développement d'un système informatique destiné à assister les développeurs hardware dans le transfert des schémas fonctionnels et réalisation sous forme de composants soudés sur ces circuits imprimés. Ce logiciel est appelé MIDAS [Minimum Design Automation System]. Il est développé essentiellement par une équipe de PRLB. C'est Jean Desmet qui est mon contact. L'interaction avec ce programme est vraiment artisanale : une partie est faite via des cartes perforées : il y avait 4 perforatrices IBM 026 au

premier étage ; une autre partie est faite via des rubans perforés. Je me souviens d'avoir vu Jean Desmet repérer une erreur de programme en le lisant directement sur les trous de la bande perforée. Chaque type de carte était modélisé. Le résultat du programme MIDAS était d'une part une représentation du plan de chaque couche du futur circuit imprimé multicouche et d'autre part le positionnement des futurs trous.

- La première représentation était envoyée dans un laboratoire photographique situé à Bruxelles qui faisait un masque dans une plaque qui, à son tour, servait à impressionner un film photographique. Ce film négatif était transformé en film positif de telle sorte que les futurs conducteurs soient représentés par des traces opaques.

Le centre international de Philips pour la production de circuits imprimés multicouches à trous métallisés avait été établi dans l'usine MBLE de l'avenue Herbette à Anderlecht. Le processus de production des multicouches se réalisait comme suit :

Le matériau de base était des plaques de circuits imprimés avec les faces complètement cuivrées et enduites à l'extérieur d'un film photosensible résistant aux acides. L'acide va enlever le cuivre dans les zones non protégées lors du développement photographique ; seules les traces des conducteurs vont subsister de la surface initialement complètement cuivrée. Certains circuits imprimés étaient simplement bifaces. Dans la plupart des cartes du BEO il s'agissait de quatre couches : dans ce cas les bifaces étaient collés pour obtenir un sandwich.

- La seconde représentation pilotait le forage des trous. La métallisation des trous intervenait ensuite à Herbette via un processus de bains de galvanoplastie.

Dans certains cas simples, ou en urgence, les circuits imprimés étaient fabriqués au BEO artisanalement par une technique mixte au scalpel et par une photogravure bricolée.

- Le bâtiment de la place Fontainas n'était pas idéal pour héberger des bureaux d'étude. Le rez-de-chaussée est en cours d'aménagement pour devenir le centre d'intégration des systèmes. Le bureau de Claude Fosseperez est au dernier étage (9^{ème}, si je me souviens) dans les meubles du directeur général de Philips Belgique qui vient de déménager dans le prestigieux « Philips Building » de la Place de Brouckère. Depuis le bureau de Claude la vue y était époustouflante ; la salle de réunion en imposait ; il y avait même une terrasse à ciel ouvert.
- Assez rapidement, Claude Fosseperez me demande de coordonner ce passage des plans fonctionnels à la réalisation des circuits imprimés prototypes. Cette activité implique de coordonner les développements de MIDAS et d'envisager un processus plus rapide et fiable pour assurer ce passage et gérer les documents qui y sont associés. La coordination concernait aussi les outils spécifiques au développement des microprogrammes : cela était d'autant plus important que le système de diagnostic¹⁷ en cas de panne et de validation en cours de fabrication était basé sur le lancement d'un microprogramme et la récolte synchrone des états des interfaces des cartes.
- L'embryon de ce qui deviendra le département « Factory Engineering » se crée implicitement. Comme la disponibilité des plans et de rapports des tests sont des marqueurs de l'avancement des travaux de développement, je collabore beaucoup avec Jean-Pierre Van Wayenberg (la personne en charge du contrôle du planning [PLO]). De même, je collabore beaucoup avec Claudine Trullemans¹⁸ (la secrétaire de Claude Fosseperez) pour rédiger les parties techniques des rapports que le BEO doit envoyer périodiquement à la direction générale d'Apeldoorn et pour servir d'interface avec le département de propriété intellectuelle de Philips à Apeldoorn.
- En 1972 la direction générale de Philips Data Systems¹⁹ (Apeldoorn) et la direction générale de Philips (Eindhoven) organisent au BEO une réunion essentielle pour vérifier que le complexe industriel mis en place à MBLE était capable de mener à bien le développement, la qualification et la production de l'*« Entrée de gamme » P1100* des ordinateurs de Philips Data Systems. J'ai le

souvenir d'une belle journée colorée (ce qui me fait penser à l'automne). Pour cette réunion, Claude Fosseperez m'avait confié d'être présent comme secrétaire technique ; Claudine Trullemans y assurait le secrétariat administratif et l'organisation de l'événement.. Les divers responsables firent leurs présentations avec peu de réactions ou questions de la part des 'big boss' de Philips. Le docteur Teer et le docteur Pannenborg y furent particulièrement avenants, mais silencieux. Ils posaient peu de questions. De nombreuses fois Claude Fosseperez s'inquiétait. En fin de journée, c'est le docteur Pannenborg qui a nous a remercié sur un ton assez neutre et il y avait du bruit dans le voisinage de la salle de réunion.

Après le départ de nos visiteurs, Mme Trullemans avait réservé une salle de réunion au premier étage d'une brasserie de l'avenue Louise « *La Danish Tavern* ». Nous y étions une douzaine à nous poser la question : « Finalement, le docteur Pannenborg et le docteur Teer ont-ils validé le plan d'action et le budget que Claude Fosseperez avait préparé ? ». Heureusement, j'avais tout enregistré sur un petit enregistreur personnel (pas un Nagra, mais pas mauvais du tout) et nous avons pu réécouter la conclusion : « **GO ON !** » et pousser un « hourra ! » retentissant :

- L'« Entrée de gamme » de l'offre de *Philips Data Systems* était attribuée au BEO à Bruxelles !
- Nous étions en charge de réaliser le prototype « BS » [Basic System] de cette future P1100.
- Le développement d'ordinateurs ne serait pas possible sans une discipline rigoureuse dans la gestion. Cela était d'autant plus important et nécessaire qu'il s'agissait d'une collaboration entre groupes industriels, entre de nombreuses entreprises du groupe Philips et qu'il fallait aussi organiser la manière par laquelle l'on allait gérer des systèmes composés de matériels et de logiciels ; organiser le déploiement en clientèle ; assurer la maintenance préventive et corrective ; assurer les mises à jour ; organiser le « End of Life »

À cette époque Philips n'avait pas de méthodologie générale applicable à ce type de situations. Electrologica / Philips Data Systems a imposé un système de gestion dénommé « **SYSTEMS MANAGEMENT** ».

Au BEO je fus en charge de la facette « Configuration Management » de cette méthodologie qui coordonnait, conjointement avec le « Test Management » les autres facettes. Il y avait beaucoup de similitudes entre les exigences applicables aux applications nucléaires et celles applicables aux ordinateurs.

Tous les membres du BEO ont reçu un aide-mémoire, format d'une carte de visite, des éléments essentiels, structurants de ce « Systems Management » :

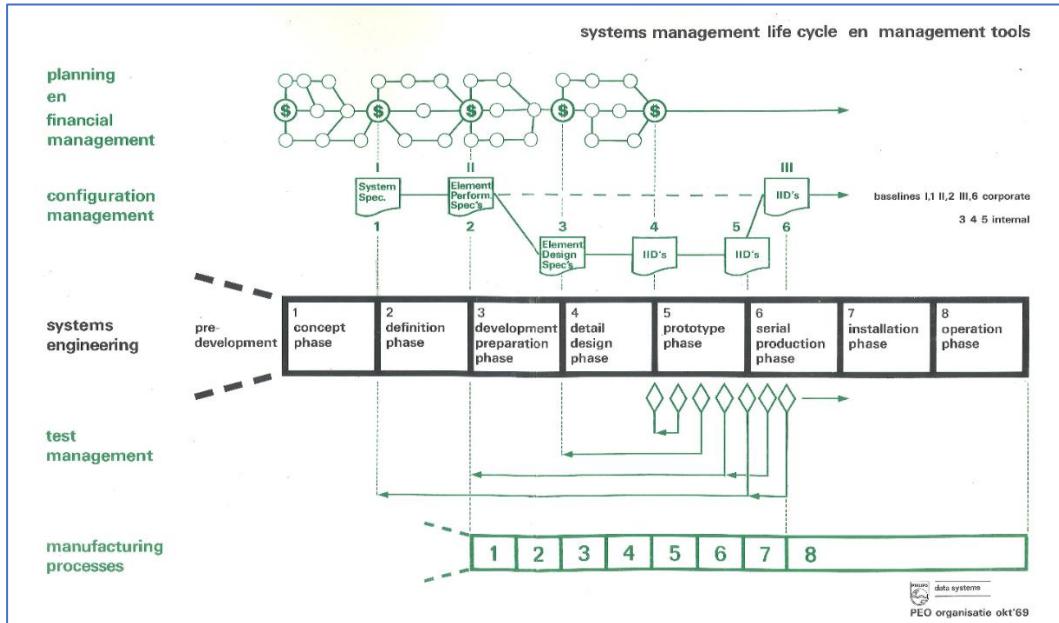


Figure 12 : Le système de gestion du cycle de vie – les outils de gestion

Adopter une méthodologie était en soi essentiel. Le document de base de référence date de septembre 1969. Il était globalement porteur, mais avait de nombreuses lacunes, surtout pour couvrir les développements software. Dans Unidata, le groupe de SIEMENS utilisait une méthodologie plus complète et plus naturelle où le contrôle des processus était dans l'essence de la méthode : cette particularité faisait que les développements des logiciels s'y intégraient sans difficulté.

Quoi qu'il en soit, pour Apeldoorn, imposer cette méthodologie au BEO était aussi une méthode de s'assurer d'avoir le moyen de contrôler notre bonne exécution des projets, une communication plus claire, via une terminologie unifiée, et le suivi du planning rigoureuses, sans échappatoires.

Cette méthodologie est décrite plus en détail dans la première Partie. Les livres détaillés sont aux archives.

Tous les aspects étaient bien couverts, mais, dans le détail, la méthodologie avait des faiblesses. Ce qui était important est qu'une méthodologie a été suivie. Je me souviens que Claude Fosseprez nous avait réuni dans la grande salle de conférence de l'immeuble de la Place Fontainas avec un conférencier expert de la mise en œuvre de cette méthode. Il avait commencé sa conférence par citer Oscar O. Paine, le chef du projet APOLLO de la NASA, après le succès de APOLLO 16 qui avait assuré les premiers pas de l'homme sur la Lune : « ***The power of management*** » ; ce qui peut se traduire par « ***La puissance de la méthode*** » !

Plus tard, une méthodologie similaire plus détaillée, plus correcte et plus pragmatique a été choisie et imposée, appelée **PRODOSTA**. Le planning détaillé qui a été expliqué au chapitre 2 est l'un des documents essentiels de gestion prévu tant par le « Systems Management » que par « PRODOSTA ». PRODOSTA signifie « PROject control and DOcumentation STAndard ». Il correspond à l'adaptation du « Systems Management » aux normes internes de Philips [CSD => « Concern Standardisation Department » et de ISA « Information Systems & Applications ». PRODOSTA est plus détaillé que « Systems Management » : il incorpore des consignes précises

dans certains secteurs, comme le formalisme à suivre pour l'identification des produits et documents.

- Pour mettre en place cette méthodologie, en début 1973, Claude Fosseperez retoucha l'organisation du BEO.

L'organigramme qui a été reconstruit par Jean-Marie Pétronio est présenté au chapitre 1 :
Mon groupe y est responsable

- Des développements de « *Computer Aided Design* » CAD ; cet acronyme a ma préférence sur DAS « *Design Automation System* » [terminologie utilisée dans « *Systems management* »], car il exprime mieux la réalité : il s'agit d'une assistance au « *design* » !
- De la gestion des normes ['standards' en anglais] et la vérification de 'compliance', c'est-à-dire le contrôle que les équipements sont conformes aux spécifications et aux normes applicables. C'est dans cette facette que l'on couvre aussi le « Configuration Management »
- Les objets essentiels gérés par le « Configuration management » sont les documents : documents définissant les produits et les processus de production et d'usage ; documents de gestion. Cette facette impliquait une collaboration étroite avec le groupe PLO.

Mais rapidement on s'est rendu compte que les outils de CAD devaient avoir une compréhension importante avec ce qui se passait pendant le cycle de vie complet des produits et de leurs composants. En effet, dans le Hardware, il était essentiel que la partie assurant que le test automatique et les diagnostics soient mis en place de manière globale et intégrée à la gestion du service après-vente. Cette vision intégrée a été appelée « **Factory Engineering** ». Rapidement Claude Fosseperez a été séduit par cette approche et, après quelques tâtonnements, il m'a confié le soin de réfléchir à la création d'une telle entité d'intégration de la gestion du Hardware, du Software, des Supports et de la Documentation.

Cette méthodologie et terminologie existait. Il s'agit d'une extension du concept de « *Manufacturing Engineering* ». L'approche « *Systems Management* » lui a donné du corps en articulant le concept de « Configuration Management » avec le concept de « *Manufacturing Engineering* ». Plus tard, PRLB a aussi travaillé à la définition et aux outils du « Configuration Management ». À titre d'exemple, tout ce qui touche à la gestion des changements, des choix et de la gestion des documents de projets et de produits est du « Configuration Management »

Dans le « Factoring Engineering » on incluait essentiellement quatre grands domaines :

- La **gestion de configuration**, c'est-à-dire tout ce qui touche à la gestion des identifications des documents, identification des produits, de documentation des produits, documentation de self-control, de l'évaluation des documents, et du bon fonctionnement des produits ...
- Assez rapidement aussi et c'est une première pièce que j'ai renforcée plus tard avec Siemens c'est non seulement de faire la **documentation produit**, ce qui est de la spécialité Philips, mais aussi
- Une **documentation de processus** ce qui était très nouveau et même très controversé chez Philips ! J'ai eu énormément de difficultés plus tard à faire, à expliquer à la direction Philips à Eindhoven que la documentation du logiciel et des processus lorsqu'on exécutait les logiciels, pouvaient être documenté de manière formelle, de la même façon que le hardware, mais en documentation de processus (en intention, en exécution, en contrôle et en documentation d'états) ! Les fondations conceptuelles que j'avais reçues du Professeur Linsman trouvaient ici toutes leurs applications ! Il y avait mille et une raisons pour dire que le software c'était autre chose que le Hardware et qu'il ne fallait pas le documenter, que le code source suffisait comme documentation ! Ici aussi, le travail que j'avais effectué pour l'étude du modèle EARE trouvait toute sa place.
- La gestion de la **qualité** confiée à une équipe indépendante était aussi une nouveauté.

- Je n'ai pas été informé que des pourparlers avaient lieu entre Philips et CII / Siemens. Avec le recul, il est clair que Claude Fosseperez y a vendu l'idée que l'« Entrée de gamme » de la ligne Philips pouvait devenir l'« Entrée de gamme » de la ligne **Unidata**. Le prototype **BS** de la « **Philips P1100** » devenait le prototype de la « **Unidata 7-720** ». Ce prototype fut nommé **X-0** !

Le fait que la BS était organisée suivant la structure de type « Von Neumann » à deux niveaux (les fonctionnalités du noyau étaient programmées via ce que l'on appelle les microprogrammes) a fait que pour changer d'operating system il suffisait de changer les microprogrammes lors du « boot ». Cela a fait que le passage aisément de BS à X-0 était crédible. D'ailleurs cela aussi facilitait les tests, ce qui nous a permis de faire la présentation, partiellement en supercherie, au SICOB (nous en avons parlé en deuxième partie). C'est aussi l'une des deux raisons pour laquelle, dans le planning, le développement et le test des microprogrammes est à ce point important ! L'autre raison était que les microprogrammes servaient aussi à valider le bon fonctionnement du hardware et la localisation de la carte à remplacer en cas de panne (ce qui avait fait l'objet d'un brevet).

En fait, en début 1973 nous étions prêts pour cette aventure.

- L'aventure **Unidata** formellement durera de mi-1973 à mi 1975 ! Au moment de la décision de la fin de la collaboration **Unidata**, la production de 120 exemplaires de l'**Unidata 7.720** avait été lancée et le commercial en avait déjà vendu 105 exemplaires. La direction de Philips Data Systems décide de livrer les machines commandées et d'assurer leur maintenance et service pendant 5 ans ; et décide rapidement de fermer les développements au BEO. Pour assurer la gestion de parc de machines, PDS décide de ne garder qu'une petite équipe de maintenance technique. Claude Fosseperez me choisit pour la gérer. Il est nommé à Eindhoven. Plus tard il deviendra le directeur général des activités de Télécommunication chez Philips et en charge des relations avec AT&T qui a repris l'usine de Philips Télécommunication Industries [PTI] à Hilversum.

Ce suivi Unidata pour Philips a été organisé comme un duumvirat, Piet Wagemans en charge du suivi commercial et moi en charge du suivi technique.

La coordination technique entre Philips – CII – Siemens était assurée par un triumvirat composé de Michel Ugon (CII) ; Ulrich Palme (Siemens) et moi [Philips]. Au début nous nous réunissions tous les trois mois, tantôt à Munich, à Paris et à Bruxelles.

- Siemens possédait un important bâtiment au cœur de Munich, à proximité de Marienplatz, réservé aux réunions internes de Siemens ou internationales. Nous étions reçus dans des salons sans fenêtres où nous pouvions travailler ; des repas de haute qualité y étaient servis sans que nous ayons besoin de changer de local.
Ulrich Palme avait une connaissance de gestion remarquable, mais ne connaissait pas bien les logiciels de Siemens, en particulier lorsqu'il y avait des problèmes dans l'operating system BS1000/BS2000. C'est lui qui m'a introduit au système de gestion documentaire des produits (tant hardware que software) organisé autour des « **Sachnummers** ». La caractéristique de cette approche est qu'elle donne une place à la documentation non seulement des produits, mais aussi des processus et de gestion administrative, ce que l'approche de Philips des 12NC ne permettait pas !
- Les réunions chez CII se tenaient en fait près de Versailles, à Louveciennes / Le Chesnay-Rocquencourt, dans les anciens bâtiments du SHAPE où CII avait l'un de ses centres de recherche et développement. Il s'agissait souvent de baraquements sans confort. Michel Ugon était brillant scientifiquement, mais il avait une connaissance insuffisante de l'anglais et quasi nulle de l'allemand. Souvent nous utilisions le français, puis je traduisais en anglais pour Ulrich Palme et vice-versa.

- Les réunions chez Philips se tenaient à Bruxelles [MBLE].

Dès 1977, une réunion par an suffisait. La dernière eu lieu à Munich lors de l'***Oktoberfest*** de 1979.

En fin 80 ou début 81 (je ne me souviens plus de la date exacte) les partenaires signent le « *end of life order* ». Par cette convention, les firmes commandaient les pièces détachées et les accessoires qu'elles voulaient avoir pour assurer la maintenance des quelques machines qui restaient en service ; la cannibalisation des machines arrêtées était aussi planifiée. La signature du « *end of life order* » s'est faite à Versailles, sous le regard amusé de Jan Berghuis (qui à l'époque était l'un des vice-présidents de Philips). En fait Jan Berghuis voulait que cela se passe à Versailles parce qu'il était furieux qu'Unidata ait été arrêté et il disait « *Je dois considérer que Philips a fait sa part dans le consortium en menant bien la barque de la 7-720 qui a fonctionné magnifiquement, la maintenance a été faite correctement. Siemens et CII (l'Allemagne et la France) vous devez le reconnaître. Ce n'est pas notre fait ou faute qu'Unidata s'est arrêté* ». Il est arrivé avec une arrogance ! Il avait choisi Versailles parce qu'il disait que c'est là qu'avait été signé le traité de Versailles et avec lui les Français et les Allemands qui étaient représentés ... enfin bon c'était un personnage à la fois génial et odieux, c'est comme ça ... on doit vivre avec des gens comme cela ! Jan Berghuis était très fier d'être grand (210 cm) et membre d'un club suprémaciste des grands !

La maintenance des configurations de la 7-720 a été assurée par nos équipes jusqu'en 1982.

Rapidement la direction de Philips à Apeldoorn et à Eindhoven décide de fermer le BEO et ne garder qu'une petite équipe raccordée administrativement aux Bureaux d'Études Télécommunications de la MBLE, dirigés par Stéphane de Vleminck. En effet, à la nomination d'Yvan Hecq comme Directeur Général Technique de la MBLE, Stéphane de Vleminck l'a remplacé comme Directeur des Bureaux d'Études Télécommunications.

- La direction convient que je dirigerai cette équipe en tant que Chef du Factory Engineering.
- Mon groupe de maintenance et finalisation est d'une douzaine de personnes. Au début l'essentiel du travail consistait en assister les installateurs en finalisant et validant en fin d'installation. La finalisation consistait à installer les dernières versions des microprogrammes (il y avait des corrections qui n'étaient pas transmises à la fabrication) et à personnaliser les systèmes pour chaque client. La validation consistait à passer tous les programmes de diagnostic et de test de conformité. Les rapports de finalisation et validation étaient transmis au Commercial pour activer la « Réception » de la configuration. La gestion de la cohérence et compatibilité des modifications s'est effectuée via un registre de « *Configuration Controlled Entities* ». Cette innovation en gestion a été reprise comme norme dans Philips.
- La **maintenance** des configurations était organisée à trois niveaux :
 - **Maintenance client** : l'entretien usuel était assuré par le client lui-même. Si une panne survenait, le client avait un protocole de diagnostic de base qui, souvent, conduisait à l'identification de l'endroit de la panne. En effet, la plupart des pannes survenaient dans les chips hardware et les microprogrammes de diagnostic identifiaient la carte qu'il fallait remplacer. Soit cette carte était en stock chez le client (les cartes de mémoire vive, surtout) ; soit la carte était envoyée par express.
Le client était aussi capable de remplacer des cartes si des corrections étaient décidées et capable de mettre à jour les microprogrammes.
 - **Maintenance téléphonique** : lorsque le protocole de diagnostic de base échouait à identifier la carte concernée ou conduisait à une panne autre que le remplacement d'une carte, le client contactait par téléphone l'un des membres de mon équipe qui tentaient ensemble de résoudre le problème.

- **Maintenance sur site** : lorsque les deux niveaux précédents n'aboutissaient pas, l'un des membres de mon équipe était envoyé sur site. Cela ne s'est passé qu'un très petit nombre de fois et surtout au début.
- **Gestion courante** : Le protocole de diagnostic étant très fiable et le nombre de systèmes diminuant rapidement, il a suffi de garder quatre personnes pour assurer cette maintenance technique des 7.720 en clientèle. Je veux ici rendre hommage à Daniel Maghue qui a superbement assuré cette gestion technique.
Il faut ici rendre hommage à Philippe Nyssens, à Jean-Claude Emond et à Ferdinand de Wasseige qui ont imaginé la testabilité de la 7.720 avec un autodiagnostic remarquable qui a été breveté pour la qualité ! IBM a racheté des droits d'adaptation de ce système ... je ne pourrais pas dire plus simple ! C'était tellement simple que la plupart des pannes étaient réparables, identifiables, diagnosticables par le client lui-même dans le hardware et qu'on avait fait un manuel extrêmement simple grâce à ce coup de génie !

Il faut aussi ici signaler que la **cohérence technologique** était gérée essentiellement dans le *Factory Engineering* et cela a montré des fruits ... au point même qu'il y a eu des tensions importantes certains moments avec la production qui n'acceptait pas de se trouver en quelque sorte sous, non pas les ordres, mais bien des protocoles qui avaient organisé à l'intérieur même du développement !

1.4 Projets MBLE pendant la période « NatLab » (1976 – 1986)

Gaston Bastiaens

Mes champs de recherche :

Archivage optique / Fax / Technologie intégrée CAD

La section suivante concerne la période où, pendant plusieurs années, j'ai travaillé des mardis aux jeudis à Eindhoven, puis à Hilversum, sous la direction de Jakob Vlietstra. Les lundis et vendredis je travaillais à Bruxelles en tant que chef du *Factory Engineering*. Je vais d'abord évoquer quelques projets et développements auxquels mon département a été impliqué de manière significative pendant cette période. La section suivante reprendra les projets effectués sous la direction de Jakob Vlietstra.

1.4.1 Des grands disques numériques au CD-Audio et CD-ROM

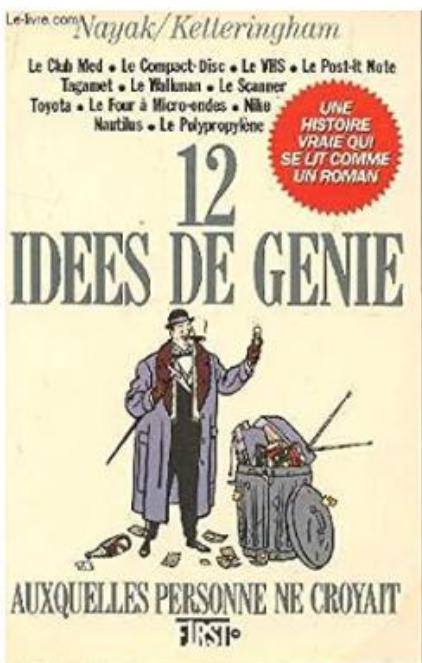
En mi des années 1970, trois formats d'enregistrement / lecture **sur bande** sont mis sur le marché en concurrence : le format VHS de JVC, qui arrive peu de temps après son concurrent direct, le Betamax créé par l'entreprise japonaise Sony. C'est le VHS qui devint le format le plus populaire. Un troisième concurrent tente de rivaliser avec les deux premiers sans succès, le V2000 de Philips et Grundig. Dans les trois systèmes, le codage est analogique.

En fin des années 70, Philips développe le LaserDisc destiné à commercialiser des films vidéo : il a un diamètre de 30 cm ; il permet de visualiser 30 minutes par face en haute qualité et 60 minutes par face en qualité standard. Il ne permet pas d'enregistrer. Le catalogue des films disponibles n'est pas très grand et il n'y a pas de 'porno' (tandis qu'il y en a en VHS). Le codage est réalisé en analogique en modulation de phase et de fréquence. Malgré la qualité supérieure, le LaserDisc n'aura pas de succès.

À cette époque, Gaston Bastiaens est le directeur technique de l'usine Philips à Hasselt, centre qui a en charge la production de certains des titres du catalogue du LaserDisc. Ils sont capables de graver des masters et de réaliser des copies en petites séries. L'équipe de Hasselt imagine d'utiliser la technologie du LaserDisc comme support pour des jeux. Ils utilisent la faculté d'adresser des fragments vidéo et le système des métadonnées comme support des scènes et des programmes :

ils appellent cela de Vidéodisque interactif. L'idée de Gaston est de se servir de ce format pour commercialiser des jeux interactifs.

Philips Belgique avait organisé que chaque année les divers centres de recherche appliquée présentent leurs travaux et provoquent des recherches de synergies ou l'éclosion de suggestions. Gaston nous présente ses travaux et très fier nous montre comment il a organisé de tester les jeux en faisant venir des personnes de Hasselt : il y avait cinq ou six alcôves de test. Il s'agissait souvent d'enfants ou d'épouse de travailleurs de l'usine. Cette initiative de Gaston Bastiaens sera arrêtée par Philips sous prétexte qu'il n'y a pas d'avenir dans les consoles de jeux ! Je suggère d'utiliser cette technologie pour l'archivage et de codage en format FAX.



Par ailleurs, à cette époque, diverses personnes au NatLab travaillaient à mettre au point le Compact-Disc numérique pour les applications audio.

Gaston Bastiaens revient à la charge et collabore avec François Dierckx pour la définition de la future norme et la réalisation des prototypes de lecteur et de graveur. En complicité avec le NatLab et largement en opposition de nombreux cadres de la « Product Division Média » un projet de recherche fondamentale est lancé au NatLab pour spécifier le CD-Audio, puis le CD-Rom. Philips approcha Sony, qui travaillait sur un projet similaire. Ayant été évincés pour les bandes par le VHS de JVC, Philips et Sony vont s'unir pour gagner la bataille du numérique audio puis vidéo. Un résumé intéressant de cette aventure est présenté dans le livre « 12 idées de génie auxquelles nul ne croyait » par Nayak et Ketteringham.

Au début de la commercialisation, les lecteurs de Philips étaient assez gros et très coûteux ; tandis que ceux de Sony

étaient plus petits et moins chers. C'est Gaston Bastiaens qui, en 1983, donnera l'impulsion et imposera des méthodes de développement et d'innovation radicales (c'est-à-dire hérétiques, suivant les règles internes de Philips). Je me souviens qu'il me montra tous les trucs que son équipe avait imaginés pour réduire le nombre de moteurs et de composants : la plus brillante de ses innovations fut d'assurer le positionnement de la lentille de lecture des encoches photographiques représentant la numérisation, en fixant un compound par un flash ultraviolet (suivant une technique mise au point ultérieurement pour les dentistes).

1.4.2 Le Facsimile (Fax)

Claude Fosseprez sera chargé d'établir un nouveau segment de produits : les « Facsimile ». Pour ce, Philips choisi de collaborer avec MBLE pour le développement et la fabrication et le centre de décision est installé à Eindhoven sous sa direction. Le responsable technique à Bruxelles fut Pol Gustin. L'approche choisie est une imprimante laser sur papier ordinaire chargé en rouleaux et un système de coupe à lame tangentielle : c'est-à-dire très fiable et très rapide.

Un cadre supérieur de XEROX (Rochester) est débauché par Philips comme responsable du Marketing pour ce programme Fax. Il parviendra à convaincre la direction générale de Philips qu'il n'y a pas d'avenir pour les Facsimilés haut de gamme. L'activité s'arrêtera au moment où une présérie d'une dizaine d'exemplaires aura été produite. Pendant plus de dix ans, notre exemplaire du secrétariat a fonctionné sans panne ni malfaçons.

Pendant ce temps, ce transfuge reprenait sa place comme du responsable du marketing chez Xerox, qui, quelques mois plus tard, inondait le marché avec des Facsimile bon marché, sur papier électrostatique !

1.4.3 Les archives du SHAPE

C'est en échangeant avec Gaston Bastiaens sur la technologie du CD-I que Hasselt avait développé et sur les Fax que j'ai eu l'idée de réaliser une station d'archivage de documents basée sur des scanners/imprimantes de Fax et un juke-box de Vidéodisques Interactifs où les pages sont codées en numérique, suivant le mode « jeux » et les pages représentées suivant le format de représentation des Fax. En effet, j'avais été confronté indirectement à la problématique dans mes contacts pour Unidata. Quand le SHAPE a quitté Louveciennes pour s'installer à Casteau en Belgique, c'est CII qui s'est installé dans les baraquements du SCHAPE. Nombreux d'anciens collaborateurs du SCHAPE avaient rejoint CII et quelques-uns étaient restés sur place, en particulier l'équipe chargée des archives. Je les rencontre lors de mes visites à CII pour Unidata. C'est sur ces bases que je propose de réaliser l'archivage des documents du SHAPE en se servant de leur programme de gestion lié à leurs archives sur microfilms. L'avantage était de pouvoir accéder directement aux contenus, à pour imprimer en bonne qualité et assurer une traçabilité de tous les accès. En collaboration avec le SHAPE je rédige les spécifications techniques du système. Pour pouvoir bien comprendre les besoins et accéder à des documents témoins, je reçois une accréditation « Tempest 5 » qui est la plus haute accréditation qu'un civil peut atteindre.

La réalisation du système a été confiée à Paul Gustin et Gustave Pouillon qui imaginent un Juke-Box à trois colonnes de Vidéodisques Interactifs de 30 cm de diamètre. Le projet porte le nom de Megadoc ! Je n'ai pas été impliqué dans la mise en service.

1.4.4 Les centraux téléphoniques analogiques à commutation spatiale

Philips Télécommunication Industries [PTI] adopte notre technologie de circuits imprimés à trous métallisés, gérée via ARCADE. Nous contribuons directement au développement de leur central téléphonique pour entreprises privées (maximum de 256 postes) dont le dimensionnement a été réalisé par le PRLB (Marc Davio). Ce domaine industriel sera à la base de mission au Portugal au nom de l'OTAN.

La commutation est assurée par des relais commandant des contacts plaqués or placés dans des tubes de verre. La fiabilité et l'absence de craquements en assurent une belle pénétration dans les banques, les hôpitaux et les administrations.

Le prix de cette solution laisse donc un marché de niche. La demande de solutions plus compactes et moins chères va conduire à la solution à commutation temporelle, d'abord hybride, puis complètement numérique.

1.5 Philips Research Centrum [NatLab] (1976 – 1994)

Jakob Vlietstra

Mes champs de recherche :

Factory Engineering / Computer Integrated Manufacturing / Secure Information Systems

1.5.1 Coordination CAD :

Claude Fosseprez a fait une présentation au NatLab de l'approche technologique hardware mise au point pour le BEO et, en particulier, le fait que nous avions mis au point une chaîne complète de prototypage rapide et fiable basé sur le développement assisté par ordinateur. Le NatLab est le nom du centre de recherches fondamentales de Philips à Eindhoven. Le PRLB agissait comme centre décentralisé du NatLab. La direction du NatLab m'a mis en rapport avec le patron d'une organisation satellite du NatLab dirigée par Jakob Vlietstra, dénommée PC-CAD [Philips-Corporate Computer Aided Design]. Cette organisation visait à donner assistance transversale aux divers groupes de recherche, en particulier au début pour faciliter la réalisation de prototypes hardware.

Cette organisation dépendait directement du docteur Pannenborg qui, à cette époque, était vice-président de Philips et un des piliers de la fondation du « Club de Rome » qui, en 1972, venait de publier le rapport « *The Limits to Growth* » ou encore connu sous le nom de « Rapport Meadows ». Dès cette époque j'ai été très sensibilisé sur ces aspects et, aujourd'hui encore, je suis membre du Club de Rome (section EU).

À cette époque, Jakob Vlietstra avait déjà un curriculum d'exception : il avait été lieutenant de vaisseau dans la marine industrielle au long cours ; puis coordinateur de projets de recherche pour Philips. Rapidement nous avons sympathisé ! Puis nous sommes devenus amis ; d'ailleurs, encore maintenant, nous continuons à être en contact. Il vit à Willits en Californie. Une biographie détaillée de Jakob Vlietstra dans sa période Philips est disponible sur Internet²⁰.



Jakob Vlietstra joined the Research Laboratories of the N.V. Philips' Gloeilampenfabrieken in 1960 after a nine year career as Deck Officer in the Merchant Navy. During the period 1960-1965, he studied Numerical Analysis, Programming, and Process Analysis at the Technical Universities of Eindhoven and Delft, and at the Amsterdam Mathematical Centre. In addition, from 1961-1969, the author was responsible for software development for numerically controlled machine tools at Philips, and was a member of a small research team that realized a project wherein the design and manufacture of television tubes were carried out with the aid of computerized processes. From 1969-1973, Jakob Vlietstra investigated the fundamentals of Computer Aided Design. In 1973 he became System Architect and Concern Coordinator for Computer Aided Design in Electronic Engineering applications. He was appointed Assistant to the Director of the Product and Factory Engineering Department of Philips Telecommunication Industry in 1981 and, recently he joined the newly created company: AT&T and Philips Telecommunications in which he manages the CAD and CAM departments. Jakob Vlietstra chaired IFIP's Technical Committee on Computer Applications in Technology from 1977-1983 and he received the IFIP Silver Core Award in 1977.

21

Figure 13 : Courte biographie de Jakob Vlietstra

Dès les premiers contacts, Jakob Vlietstra s'est intéressé à la suite logicielle, matérielle et technologique que nous avions mise au point pour la X-0 et qui avait été adoptée pour l'Unidata 7.720. En effet, notre approche avec Midas et la technologie des circuits imprimés à trous métallisés permettaient de réaliser des prototypes de qualité « production » en 10 jours, ce qui, à l'époque, apparaissait comme une prouesse.

Il a rapidement été convenu que je collaborerais avec ce groupe deux ou trois jours par semaine : l'idée ayant la faveur de Jakob Vlietstra était que je reste le chef du « Factory Engineering » à Bruxelles et que je contribue, à temps partiel, à son unité de recherche fondamentale et appliquée en CAD. Cette approche avait l'avantage de me laisser connecté aux problématiques concrètes pour être capable d'en inférer les orientations de la recherche et de son application ; vice-versa, pouvoir essayer en concret les solutions dégagées ; disposer de l'expertise de l'équipe ayant développé MIDAS, en particulier Jean Desmet.

Au bout de quelques mois, Philips a organisé que je resterais à Bruxelles les lundi et vendredi et que je serais à Eindhoven les mardi, mercredi et jeudi. J'ai d'abord été logé dans l'hôtel de prestige que Philips possédait à Eindhoven, le « Cocagne » (tout un programme dans un tel nom) puis Philips m'a réservé un pied-à-terre sympathique. Pour la petite histoire, c'est dans cet hôtel que Philips logeait ses invités de prestiges, conférenciers, hommes d'affaires et hauts gradés de sociétés en recherche de partenariat.

J'y ai eu la chance et le bonheur d'y assurer l'accompagnement d'un jour de Nicholas Negroponte (le chef du département du MIT en charge de l'interaction humaine – machine, qui a été à source du concept de « bureau virtuel » et de ses « fenêtres » [qui allait donner le nom 'Windows']). J'en ai un souvenir ému d'avoir échangé avec lui une soirée entière sur le sujet ! À l'époque de cette rencontre, je venais d'être cofondateur d'Eurographics, une initiative du professeur José Encarnaçao²² de l'université de Darmstadt. Je venais aussi d'être l'organisateur du Congrès associé à l'exposition Eurographics 87 et éditeur des '*Proceedings*' [550 pages] de ce Congrès publiées chez Elsevier.

Le professeur Negroponte était avide de collaborer avec nous, en particulier sur les aspects de normalisation et des approches 'backwards' et 'ray-tracing' que nous avions mises au point pour résoudre les vus et cachés dans les présentations multiples et rendre réalisés les modèles 3D.

C'est Philips qui a réalisé le premier chip visant à retourner le processus impliqué associé à chaque pixel d'un écran d'interaction. José et moi avons été invités à donner des cours d'été de CAD et de représentation graphique à l'Université de Tokyo. De même, quelques années plus tard, pour présenter les résultats du projet CIMOSA. Ces deux fois trois jours de cours et le programme de visites au Japon me laissent des souvenirs profonds.

Jakob Vlietstra a pris aussi alors un accord de collaboration avec le centre de Recherche & Développement de la division de produits « Sounds & Visions » qui avait aussi un équivalent du « Factory Engineering ». Jan Takke, un ingénieur brillant et visionnaire, pilotait ce FE.

Entretemps, à Bruxelles, nous avions pris des accords avec l'Institut Géographique National qui disposait de matériel pour impressionner des films au départ de données informatiques sur un « photoplotter ». Il s'agissait d'une imprimante de grande taille (largeur 130 cm) dont l'« encre » était un spot lumineux. Ce photoplotter était un développement d'une petite firme anglaise dont le patron avait donné son nom Benson à la firme. Rapidement il a investi ses profits dans des initiatives de promotion de la paix !

C'est alors que se sont stabilisés les concepts du projet et de la suite de logiciels et technologies que nous avons appelés ARCADE. Dans les grandes lignes, il s'agissait de généraliser et rendre modulaire l'approche MIDAS. Comme son acronyme l'indique (*ARchitecture for Computer Aided Design for Electronics*) au départ, ARCADE visait à spécifier l'architecture, les données et les interfaces d'interopérabilité. Rapidement, la demande a été de développer un système modulaire très flexible et adaptable aux besoins spécifiques locaux : divers modules applicatifs ont été développés ; une base de données ; une interface dénommée POLI [*Problem Oriented Logical Interface*] ; un langage de définition SAIL [*Service Application Interface Language*]. Cette approche

était totalement novatrice ! Nous avions même incorporé un noyau de « Configuration Management » puis des profils applicatifs ; les spécifications de détail étaient exprimées sous forme de « data model » et de protocole d'enchainement conditionnel de processus.

Pour les applications, nous avons d'abord étendu MIDAS. Nous avons aussi intégré d'autres types de circuits imprimés multicouches, jusqu'au fameux 6 couches à impédance contrôlée et à garantie de crosstalk qui permettait des applications jusqu'à 4 Ghz d'horloge. Vers 1979 nous avons aussi intégré des applications développées aux USA : la plus importante fut SCI-Cards. Cette application avait été développée dans un spin-off de l'université de Boulder. Nous avons aussi contribué au développement de ce qui allait devenir AutoCAD : nous étions en charge de l'extension 3D.

Au début des années 1970, Philips avait créé une organisation transversale [‘corporate’ et ‘décentralisée’] pour la définition de la politique en informatisation et ayant un monopole d'exploitation de l'informatique, tant pour les applications de gestion que pour la recherche : cette organisation portait le nom de « ISA » [Information Systems & Applications²³]. Cette organisation avait de fait un pouvoir exorbitant : l'on disait « un État dans l'État ». En particulier, ISA imposait l'usage exclusif d'ordinateurs IBM et imposait que les échanges informatiques soient régis par une norme intitulée IFO [Input, Filing & Output] qui avait été ciblée sur l'administration et la gestion et qui, par ce fait, était inadaptée aux besoins de Recherche & Développement techniques multilingues. À titre d'exemple : seuls les caractères ASCII étaient autorisés ; seul ISA avait le droit de créer les bases de données sur spécification des besoins (c'est-à-dire sans avoir le droit de l'exprimer sous forme de schémas de données).

Pour le développement d'ARCADE, nous étions donc confrontés aux dictats d'ISA. Les premiers développements d'ARCADE se sont effectués dans ce contexte. Mais, SCI-Cards avait été développé dans le milieu universitaire. Ils avaient choisi les ordinateurs de « Digital Equipment Corporation », en l'occurrence des PDP-11 et des VAX11-780 (dotées d'un Operating System efficace pour les applications scientifiques), et un photoplotter d'une firme de Hartford au Connecticut. Jakob Vlietstra, Jan Takke et moi avons d'abord tenté de convaincre ISA de la nécessité de changer leurs règles dans le cadre de la recherche. Peine perdue, ISA imposait son choix d'ordinateurs et nous disait de développer l'équivalent de SCI-Cards nous-mêmes sur leurs ordinateurs IBM. Nous avons alors contourné l'obstacle : en 1979, conjointement, Jakob, Jan et Guy ont introduit une demande d'investissement d'une configuration applicative (SCI-Cards) et de son photoplotter associé un Gerber [Petite société à Hartford Connecticut fondée par David Gerber]. Par cette approche, administrativement, la VAX11-780 et les deux PDP11 n'étaient pas des ordinateurs, mais des accessoires d'une application et d'un photoplotter ! La direction du NATLAB avait été tenue au courant de la manœuvre et, ayant vu toutes les possibilités des VAX11-780, s'en est rapidement dotée de nombreux exemplaires. La tempête dans ISA a été d'abord grande, puis apparemment calmée ; mais, par la suite Jakob Vlietstra, Jan Takke et moi avons eu à souffrir de rancœurs ridicules.

Une petite anecdote : rentrant d'une visite à Gerber, je suis arrivé à New York au moment de la grande panne d'électricité. Vers 6 pm le premier décrochage se manifestait par le fait que, dans ma chambre d'hôtel, les clignotements des tubes aux néon de ma chambre n'étaient plus synchrones avec le retour d'image de la télévision, ce qui induisait des barres traversant l'écran. Un à un les quartiers de New York sont passés dans le noir. J'avais une petite radio (que l'on appelait un transistor) fonctionnant sur piles. Une des chaînes émettait des nouvelles : les autorités annonçaient que la panne serait longue, qu'il y avait des pillages et qu'il était interdit d'entrer dans New York sans autorisation. Tard le soir, je suis descendu de ma chambre (12^e étage) sans m'éloigner. J'ai vu des rats sortant des bouches de métro ; des restaurateurs ayant mis leur frigo dehors avec un écriteau « *Help yourself* ». Le lendemain, dimanche matin, la panne était toujours là ! Il y avait grand soleil et le dynamisme avait fait que les journaux étaient quand même disponibles malgré l'absence d'électricité.

Dans ce mode de collaboration partiellement au NatLab à Eindhoven et partiellement aux bureaux d'études de MBLE j'ai collaboré à d'autres projets et recherches que le projet ARCADE.

Philips a été l'une des entreprises multinationales ayant contribué à établir le « Programme de Recherches » cohérent ESPRIT [European Strategic Programme for Research & Development in Information Technologies] 1984 à 1994. Il s'agit de constituer des Consortium précompétitifs répondant à des appels d'offres. La Commission Européenne finançant une large partie des coûts.

Philips a participé à plusieurs des projets qui ont été retenus par la Commission Européenne. Ceux auxquels j'ai participé sont :

1.5.2 CIM-OSA: Computer Integrated Manufacture Open System Architecture [1990]

Ce projet ESPRIT N°688 a défini une architecture modulaire destinée à représenter et gérer des industries indépendamment de leur spécificité et une méthodologie de personnalisation pour obtenir des modules opérationnels spécifiques.

The logo features the acronym 'CIM' in a large, bold, white font on a yellow background, and 'OSA' in a green font below it.

Industry	Sub-contractor	Address
AEG	GEC Electrical Projects Ltd	AEG AKTIENGESELLSCHAFT Goldsteinstrasse 235 D-6000 FRANKFURT 71
AEROSPATIALE	IBM	AEROSPATIALE 37, Bd Monterency F-75016 PARIS
ALATEL (CGE)	ICL	ALATEL (CGE) 33, Rue Eureau F-75725 PARIS 15
APT	ITALSIEL	APT EN PHILIPS TELECOMMUNICATIE BEDRIJVEN B.V. J.v.d. Heyendaalweg 41 - P.O. 1168 NL - 1200 BD HILVERSUM
BULL	PHILIPS AND NELLE ASSOCIATED	BULL S.A. 121, Avenue Molokhoff F-75116 PARIS
CAP GEMINI INNOVATION *	SELENIA AUTOMOTIVE	CAP GEMINI INNOVATION * 129, Rue de l'Université F-75007 PARIS
CRI	SIEMENS	CRI COMPUTER RESOURCES INTERNATIONAL A/S Vesterbrogade 1A DK 6162 COOPENHAGEN V
DIGITAL	VOLKSWAGEN AG	DIGITAL EQUIPMENT INTERNATIONAL G.m.b.H. Sudetenstrasse 5 D 61950 KAUFBEUREN
DORNIER	WZL AACHEN UNIVERSITY – Labs. of Machine Tools / Steinbachstrasse 53B	DORNIER G.m.b.H. Postfach 1420 D-7990 FRIEDRICHSHAFEN 1

*PRIME CONTRACTOR.

Central consortium facilities The consortium, also known as AMICE, has central facilities for the central team, project management and general information, at the following address and accessses:

Phone : + 32-2-647 31 75
 Fax (q2/3) : + 32-2-648 99 49
 Telex : + 046 63 370 (AMICE)
 DCS25 : 2210134 (9600 bps)

CIM-OSA/AMICE, 489 Avenue Louise, B 14 - B-1050 Brussels, Belgium

Figure 14 : Les 21 principales industries européennes et 80 sous-traitants ont collaboré à ce projet

Les 21 principales industries européennes et 80 sous-traitants ont collaboré à ce projet. Cap Gemini [Bernard Lorimy] était le 'Prime' Contractor et Philips [Jakob Vlietstra] 'Executive' Contractor. J'y ai assuré la coordination scientifique et technique.

Le groupe noyau de développement de CIMOSA travaillait à Bruxelles au N°489 de l'avenue Louise où nous avions loué tout un plateau pour l'équipe.

L'architecture qui a résulté du projet a été représentée par un cube couvrant quatre vues : les « Fonctions », les « Informations », les « Ressources » et les « Organisations ».

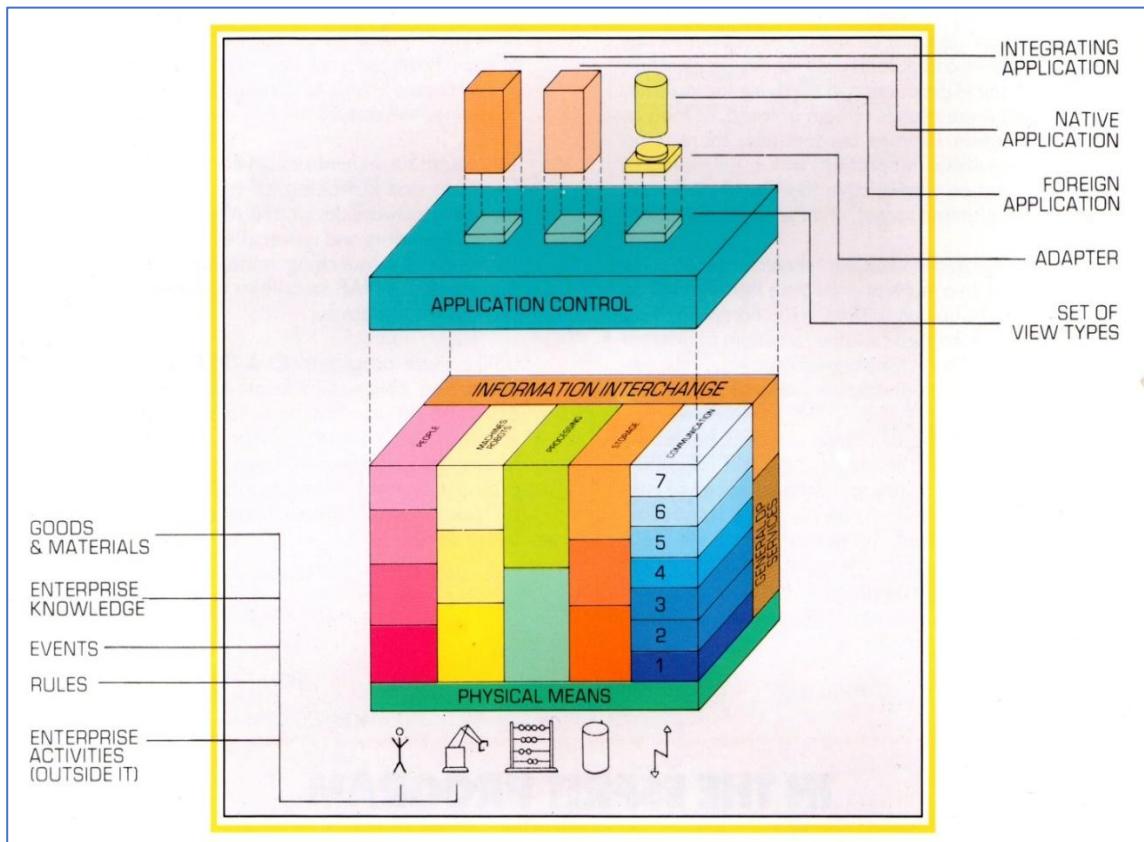


Figure 15: Le cube de CIM-OSA

C'est Philips [Jean-Claude Emond] et IBM [Kurt Kosanke] qui ont le plus contribué à élaborer ce modèle fonctionnel.

Mais, à mon sens, la plus remarquable contribution a été l'établissement du **modèle d'information** sous la coordination de François Vernadat [INRIA France]. L'équipe a adopté l'approche sémantique proche du modèle EARE « *Entity Attribute Relationship Event* » que j'avais étudié au PRLB, mais en y scindant la partie « Event » du modèle de la partie EAR ce qui apportait la possibilité de performance qui manquait.

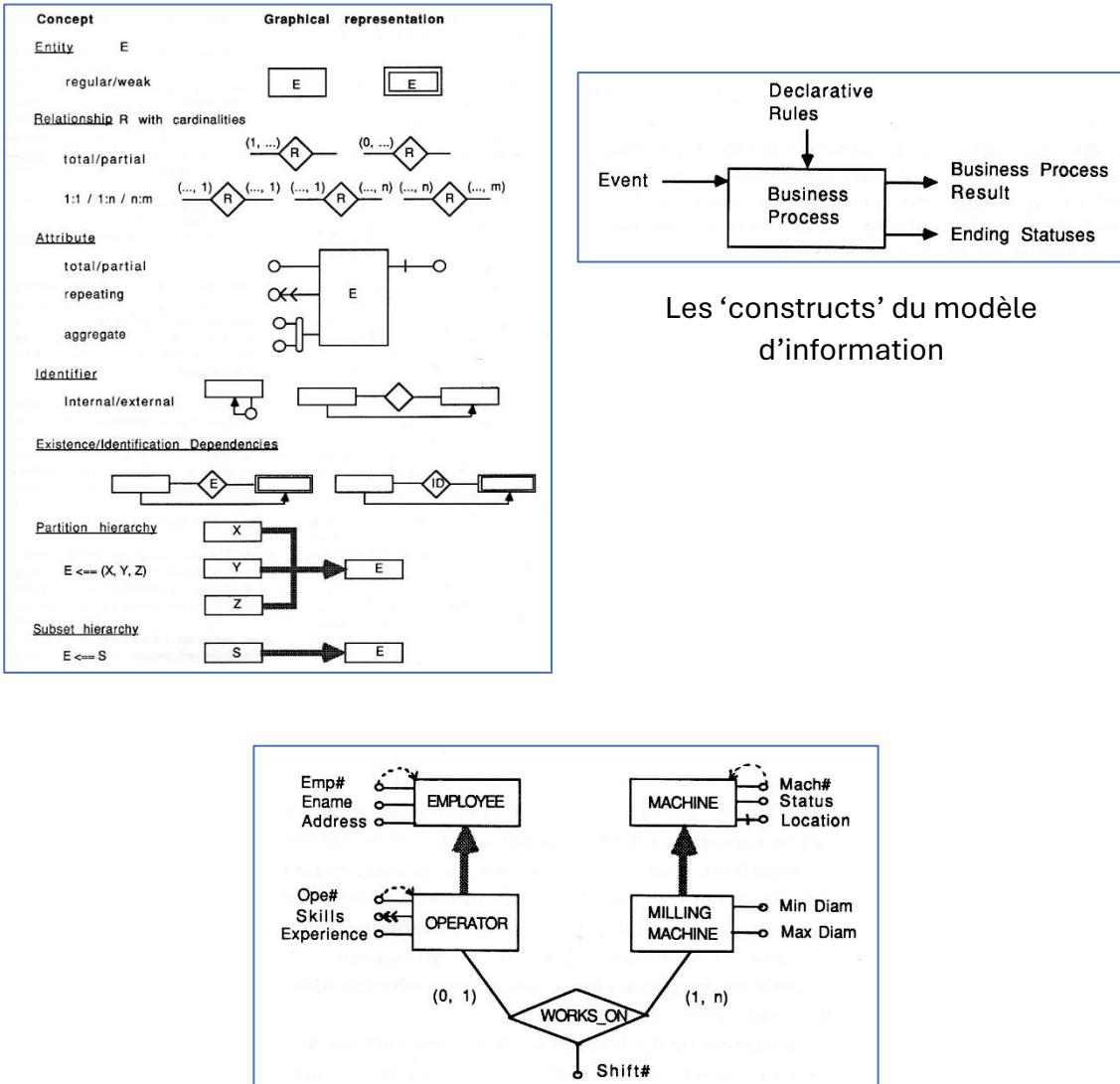


Figure 16 : Simple exemple d'instanciation du modèle (1)

Cette approche sera adoptée pour la définition du Semantic Web. Le langage OWL [Ontology Web Language] est très proche du système de modélisation de l'information développé par CIM-OSA.

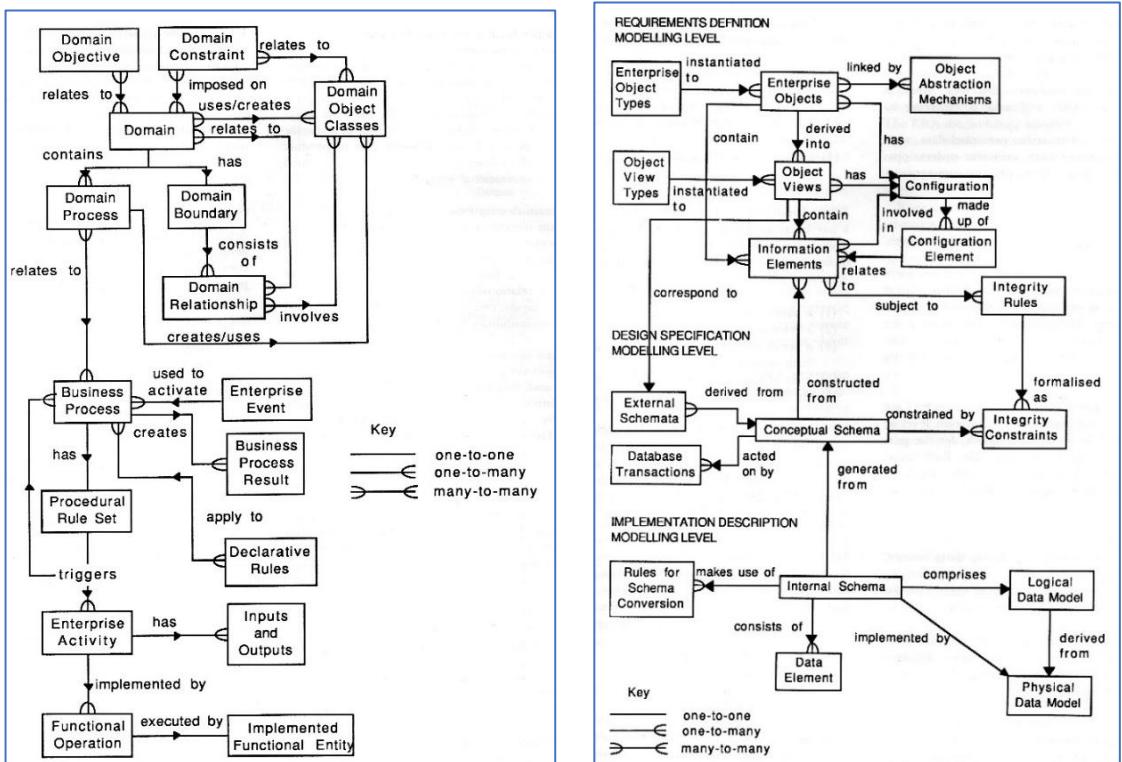


Figure 17 : Simple exemple d'instanciation du modèle (2)

Le représentant d'IBM, Kurt Kosanke, a coordonné la diffusion et promotion des résultats du projet. Il a été responsable de l'organisation d'un congrès de diffusion des projets principaux du programme ESPRIT. Il a été l'éditeur de la “*Special Issue of the International Journal of Computer Integrated Manufacturing on the ESPRIT Programme*” [Taylor & Francis Vol 3 Numbers 3 and 4 May-August 1990].

C'est Kurt Kosanke qui créera SAP sur base des résultats de CIM-OSA. Malheureusement Kurt n'utilisera que peu le modèle d'Information et bridera très fort le mécanisme de généricité. Le résultat est que SAP est peu convivial et complexe à mettre en œuvre.

Personnellement, j'ai collaboré avec l'ISO à la normalisation des archives des documents industriels et des documents représentés par l'informatique. Ces travaux aboutiront à la norme ISO OAIS [ISO-14721] dont une copie est disponible à <https://public.ccsds.org/pubs/650x0m2.pdf>.

À cette époque, la société américaine AT&T signe un accord de partenariat avec Philips pour prendre le contrôle de PIT [Philips Télécommunication Industries] à Hilversum. Pendant plusieurs années, le *Factory Engineering* de Bruxelles collabore avec le *Factory Engineering* d'Hilversum. Puis, le top staff d'Hilversum (Herman Bosman, Piet Hoving et Edward Ekas) tente d'évincer Jakob Vlietstra, de le mettre sur une voie de garage et refuse de lancer un projet de modernisation dans la ligne de CIM-OSA. C'est un transfuge du programme de Philips Data Systems (Apeldoorn) Piet Stam qui sera le fossoyeur de ce projet et de la collaboration de Philips avec AT&T. C'est aussi Piet Stam qui s'opposera aux extensions d'ARCADE (voir ci-après). En 1992, Jakob Vlietstra donne sa démission et refuse une fête de départ. À la place, il rédige un document de recommandations sur les orientations qu'il préconise pour Philips, document qu'il diffuse largement à ses frais. Quelques années plus tard, le docteur Pannenborg obtient que Jakob soit nommé « Ingénieur en Chef » [*Hoofd Ingenieur*] à titre rétroactif.

Avec le recul l'on se rend compte que la programmation orientée objet largement étudiée et exploitée à PRLB, les travaux de modélisation orientée objet de CIMOSA correspondaient aux bases nécessaires à définir le Web sémantique, ce que fera le W3C (projet de 2004 à 2008) avec les formats

de définition des ontologies **OWL**, des bases de données sémantiques basées sur **RDF** et le langage des requêtes **SPARQL**.

1.5.3 La commercialisation des résultats de la recherche

Dans un premier temps, ARCADE a été développé pour usage exclusivement en interne de Philips. Sous l'impulsion de Jakob Vlietstra, Philips a décidé de tenter une commercialisation d'ARCADE et du système technologique (en particulier les circuits imprimés multicouches à trou métallisés) et de gestion qui lui étaient associés. Cette commercialisation a été effectivement faite, mais fut vite arrêtée pour les raisons qui seront explicitées ci-après. Jakob Vlietstra avait préparé une exploitation plus large sur base de CIM-OSA qui a été rejetée pour ces mêmes raisons.²⁴ Jakob Vlietstra prendra sa retraite de Philips en fin 1992.

Une dynamique similaire s'était développée sur base d'une collaboration du centre de recherche de Philips à Briarcliff Manor avec les équipes de développement du centre de Montréal. L'intention était de commercialiser une suite de bureautique (les équivalents de Word, Excel et PowerPoint) développée en collaboration par ces deux centres de recherche.

L'architecture était superbe : adoptant déjà la séparation du physique et du logique et exprimant les résultats en XML, avec des feuilles de style exprimées dans un langage très proche de SGML.

La direction de Philips Corporate a ordonné l'arrêt de tous les programmes de ces types, sous prétexte que ces développements ne faisaient pas monter l'action de Philips (voir ci-après). Charles Dumortier à Montréal et Richard L. Wexelblat à Briarcliff Manor ont exprimé leurs critiques et recommandations constructives lors de leurs départs ou démissions²⁵.

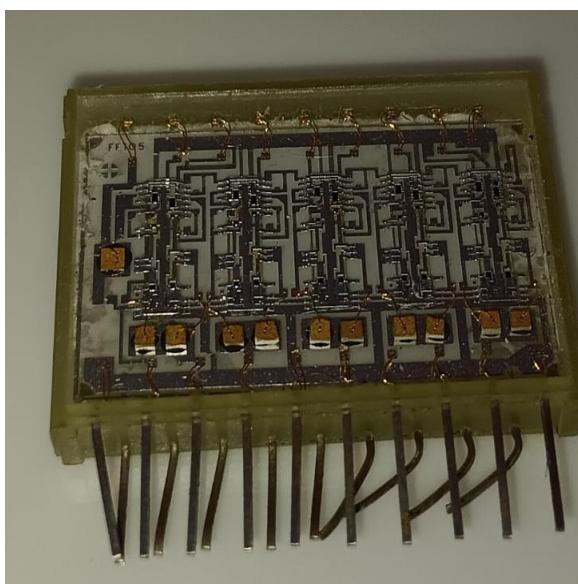
1.5.4 La commercialisation d'ARCADE et de son environnement

Essentiellement, ARCADE couvre tout le processus de développement des circuits imprimés multicouches (y compris à trous métallisés) et fournit les documents et fichiers nécessaires à leur production, leur documentation et instruction de montage des composants. Cette approche permet de faire très rapidement (quelques heures ou jours) des prototypes de développement (capacité d'être légèrement modifiés), des préséries (de qualité garantie) et de série de production.

ARCADE a prévu un format d'échange ouvert permettant de se lier à divers modules applicatifs dont les principaux sont le « *Layouter* » [le plus utilisé était Sci-Cards développé par une spin-off de l'Université de Boulder], le « *photoplotter* » [à l'époque, nous avions le choix de trois *photoplotters* : Benson / Geber / Fortex] et les centres de production des circuits imprimés [le centre d'Herbette pour les circuits imprimés multicouches à trous métallisés / le centre RPU du NatLab / et quelques autres].

Nous avions reçu une demande de l'IMEC (Leuven) pour collaborer avec eux pour étendre ARCADE en vue de couvrir le développement des ASICs [*Application Specific Integrated Circuits*] dans leur centre de production spin-off de la KUL. Stéphane de Vleminck, en fin de carrière et Moi avons visité ce centre et étions convaincu du sérieux et de la rentabilité de cet investissement. Nous avons alors tenté de convaincre '*Philips Corporate*' d'entrer en collaboration avec l'IMEC. La réponse fut un refus radical, sous le prétexte que ce centre allait faire concurrence avec le centre de Circuits Intégrés que Philips établissait dans son usine de Caen. Plus tard, lorsque l'usine de Caen a brûlé, Philips a arrêté de réaliser leurs circuits intégrés et d'arrêter leurs développements de Téléphone Portables GSM (les ancêtres des Smartphones). IMEC existe toujours et est un des fleurons de la Belgique dans le secteur. Plus tard, Philips reconnaîtra son erreur de l'époque et sauvera ASML [*Advanced Semiconductor Materials Lithography*] de la faillite pour l'amener à être un des leaders mondiaux des machines à produire des chips. Mais, la capacité de développement de ces chips reste dans les mains des leaders mondiaux, en particulier Nvidia pour les chips de l'Intelligence Artificielle.

Le centre de développement de circuits hybrides à couches minces de MBLE Agrafe nous avait aussi demandé d'étendre notre interface pour couvrir les beam-leads²⁶ et leur soudure sur des circuits imprimés et des couches minces. Le besoin avait été exprimé par l'un de leurs clients, le centre de développement spatial du Sart-Tilman (un spin-off de l'Université de Liège] sur les hauteurs de Liège.



Stéphane de Vleminck, en fin de carrière, et moi avons visité ce centre et étions convaincu du sérieux et de la rentabilité de cet investissement. Nous avons alors tenté de convaincre 'Philips Corporate' d'entrer en collaboration avec ce centre. La réponse fut un refus radical, sous le prétexte que les beam-leads n'avaient pas d'avenir. Effectivement, l'ordre d'abandonner ces technologies (beam-leads et couches minces) n'a pas tardé.

Figure 18 : Les beam-leads

Ces technologies font toujours merveille dans les équipements professionnels et dans les satellites. Les dépôts sous vide d'aluminium et la soudure par ultrason conduisaient à une parfaite conductivité, à des soudures ultrasolides et à la précision des formes (au nanomètre) permettant d'imprimer des antennes et des cavités en hyperfréquences.

Une des usines du *Philips Concern* située près de Krefeld (à la frontière entre la Hollande et l'Allemagne) s'occupait de fine mécanique à destination militaire et professionnelle. Ils avaient développé de noyau de ce qui allait devenir AutoCAD. Ils avaient repéré de nombreux éléments d'ARCADE qui manquaient dans leur application. De plus, ils cherchaient à étendre leur système pour couvrir la simulation et le contrôle des mouvements de systèmes mécaniques articulés. Ils avaient appris que le Centre de Recherches de Philips à Bruxelles PRLB avait une expérience et une compétence dans des langages informatiques capables de représenter et d'activer en temps réel (à performance assurée) des automates. Effectivement les langages CHILL et ADA avaient les caractéristiques voulues et il y avait une connaissance suffisante en « Machines à États Finis ». L'ordre est rapidement tombé de ne pas engager une telle collaboration. En effet, la décision d'arrêter les développements d'outils de bureautique (les équivalents de Word, PowerPoint, Excel et AutoCAD) avait déjà été prise.

1.6 OASIS : Open Architecture for Secure Information Systems [1992 – 1994]

Ce projet a déjà été évoqué au point 6.9.3. se rapportant aux aspects juridiques et au droit applicable au monde de l'informatique, des réseaux et des services.

Ce projet faisait partie d'un programme de l'Union européenne, distinct d'ESPRIT se concentrant sur la sécurisation du fonctionnement des systèmes d'informatique.

J'ai été amené à travailler sur la classification et la définition de la sécurité comme une des facettes de la Qualité et de la gestion des risques. La Commission a édicté des normes européennes relatives à la force des processus et des architectures mises en place pour « assurer » des systèmes. Cette norme était connue sous le nom de « Livre Vert » ou plus complètement sous :

« ***Green Paper on the Security of Information Systems (European Commission DG XIII April, 1994)*** ».

Dans la foulée, j'ai collaboré aux avant-projets de normes ISO sur la qualité qui seront les bases pour la série de normes ISO-9000 couvrant la gestion de la qualité et des normes ISO-31 000 couvrant la gestion des risques. La combinaison des deux aspects couvre la « qualité de service » qui joue un rôle essentiel dans les technologies de télécommunication.

OASIS a défini une architecture modulaire destinée à représenter et gérer tous les aspects de l'assurance des systèmes d'information, des données et les agents impliqués.

Sur base de documents préparatoires à la dynamique FideServices et CryptoWorks dont il sera question ci-après, j'ai reconstitué ces cinq caractéristiques essentielles dégagées par le projet OASIS. Elles ont été détaillées ci-dessous au point 6.9.3.

Les sept caractéristiques essentielles de cette architecture sont :

1. L'adoption d'une approche légale où les lois existantes deviennent des cas particuliers de lois plus générales.
2. L'adoption d'une combinaison d'approches cryptographiques : Symétrique / Asymétrique et, plus tard, à apport de connaissances nul ZK.
3. L'adoption de technologies d'identification des choses et rôles sujets de droits avec assurance basée sur des Certificats.
4. L'approche à couches pour les communications : en particulier, qu'un même message pourrait être transmis suivant plusieurs modes de transport.
5. La disjonction entre la chose (logique) et son incorporation [*spatiotemporal embodiment*]. Disjonction des supports et de leurs usages.
6. La résolution de l'accès aux Artefacts
7. La qualification de la qualité systémique des systèmes

La mise en place de cette approche implique la disponibilité de quelques Services Universels.

Pour diverses raisons qui seront expliquées ci-après, les pouvoirs publics rejettent le premier et le 3^{ème} points ; mais l'approche du 2^{ème} point sera adoptée, tandis que les derniers points ne le seront que partiellement.

Pour ce projet, nous avons pu collaborer avec Marieke de Soete qui, déçue, quittera SOC pour travailler au centre de développement de « MasterCard » à Waterloo.

Dans ce projet et aussi pour le projet envisagé avec le centre de recherches et développement de Montréal. Il faut aussi citer Jan Matthys spécialiste de l'interface homme-machine et des éléments graphiques. Sa déception sera grande, car il a fait une thèse de doctorat et avait suivi la formation pour me succéder lorsque j'aurais pris ma retraite.

De même, il faut saluer une des plus fines intelligences que j'ai eu la chance de rencontrer en la personne de Guy van Hooveld. C'est lui qui a assuré la commercialisation des développements de SOC, puis la gestion de SOC lorsque j'ai lancé la « Business Opportunity Platform » [qui sera décrite ci-après]. C'est lui aussi qui tenta de convaincre M. Devoldere (le CEO de Philips Belgique en 1995) de miser sur le business des jeux bien avant l'explosion des offres de Sony, Microsoft ou Nintendo !

1.7 Centraux téléphoniques numériques à commutation temporelle

Le dernier projet d'envergure que MBLE effectua en collaboration avec Philips Télécommunication Industries [PTI] & AT&T à Hilversum est la collaboration dans le développement d'un nouveau central téléphonique pour entreprises privées (256 postes) qui n'ait plus de pièces mobiles (sans contacts).

- La commutation est assurée par un découpage temporel. Le signal audio reste analogique, mais il n'y a plus de relais.
- Le dimensionnement des commutateurs du noyau est réalisé par le PRLB (Marc Davio).
- La réalisation s'effectue sur des circuits imprimés à trous métallisés à haute densité (8 couches) et impédance contrôlée ; la mise en œuvre reste basée sur ARCADE.

J'ai trois souvenirs liés à ce projet :

1. Je reçois un coup de téléphone de l'Ambassade d'Irak à Bruxelles me demandant si je suis bien le Guy Maréchal qui avait été invité d'État d'Irak en janvier 1979. Je confirme. Le secrétaire m'informe que l'Ambassadeur souhaite me rencontrer. Comme j'étais sur le départ vers Baltimore (voir point 2) je dis que je ne pourrai le rencontrer qu'à mon retour. Il me passe alors l'Ambassadeur qui me demande d'excuser son pays et ses dirigeants de la façon indigne avec laquelle l'Irak a traité ses invités d'État, dont j'étais, lors de cette visite. En effet, avec l'accord des instances européennes compétentes pour les produits à double usage (c'est-à-dire à applications civiles et potentiellement militaires). Philips m'avait envoyé à Bagdad avec un délégué commercial afin de :

- a. Présenter le drone (avion sans pilote) de supervision de terrain de bataille développé par la MBLE, en collaboration avec la Défense belge, et commercialisé sous le nom d'Épervier²⁷.
- b. La technologie des circuits à quatre et six couches avec trous métallisés et ARCADE.

Nous sommes reçus en grande pompe et nous sommes logés dans un des plus beaux anciens hôtels anglais de Bagdad. Nous y resterons enfermés dans notre chambre, avec vue sur le Tigre, pendant 7 jours sans que personne ne nous reçoive. Il semble que la visite d'un dirigeant de l'URSS avait attiré ceux qui devaient nous recevoir et qu'ils nous avaient oubliés.

L'Ambassadeur me dit que l'offense qui nous a été faite a été lavée, car les trois personnes qui auraient dû nous recevoir ont été passées par les armes ce matin-là ! Il termine en disant que, si nous avions été reçus, l'Irak aurait adopté notre drone (ce qui aurait épargné beaucoup de morts dans la guerre Iran - Irak) et aurait conduit à une industrialisation des développements électroniques de qualité. Stupéfait, je ne puis que me retrancher sur mon voyage aux USA pour écourter la conversation.

2. Je suis en effet amené à faire un voyage éclair à Baltimore pour signer le contrat par lequel une entreprise pour applications militaires (Raytheon) acquiert les droits non exclusifs sur la technologie, les outils de développement et l'usage d'ARCADE avec SciCards ; la production des circuits imprimés multicouches se faisant chez MBLE (boulevard Maurice Herbette). Il s'agissait de la version la plus avancée, la plus fiable et garantissant des délais ultra-courts.



3. Je me vois confié par l'OTAN une mission assez spéciale. Il s'agit d'accompagner la création au Portugal d'une usine de développement et production de petits centraux téléphoniques : une version simple de la collaboration MBLE : PTI / AT&T.

La chose pourrait paraître étrange que ce soit l'OTAN qui commande et finance ce projet. Mais, cela est peu connu, les statuts de l'OTAN ont des points qui organisent le fonctionnement et les objectifs en temps de guerre ; mais aussi en temps de paix. En quelque sorte, encourager la paix, lui donner ses chances avant que la folie des hommes pense qu'il existe des causes qui ne peuvent être prises en compte que par la violence.

En l'occurrence, l'idée était d'aider le Portugal à se développer afin qu'il puisse entrer rapidement dans l'Union européenne.

À cette fin je suis amené à me rendre cinq fois au Portugal et progressivement constater que l'usine s'installe ; que la qualité technique est atteinte ; que la capacité de gestion est réelle ; que le personnel est recruté et formé ; que les plans sont bien gérés ; que le réseau commercial est établi ... Au bout de 18 mois, le premier central validé sort et est installé dans une des annexes du ministère du Commerce.

Lors de ma dernière visite, je suis reçu par le chef de cabinet du ministre de l'Industrie avec dégustation d'un Porto datant de 1890.

Le directeur technique de cette usine sera élu député européen. J'aurai l'occasion de le rencontrer à Bruxelles.

1.8 Philips dans la tourmente

1.8.1 Développement et commercialisation de la recherche bloqués par Philips

Dans le courant du début des années 90, le « *Raad van Bestuur* » [Conseil d'Administration] de Philips a mis en place une orientation de gestion radicalement nouvelle.

Dans les années 80, Jan Timmer, comme CEO de Philips, avait été amené à redresser PolyGram, l'une des 11 « Divisions de Produits » de Philips en charge des médias (audio et vidéo). Notamment en misant sur le CD-Audio, puis sur le DVD, au début des années 90, il avait conduit à ce que PolyGram avait pris une valeur de l'ordre de grandeur de la capitalisation boursière de tout Philips ! La crainte d'une OPA s'imposait ! En 1996, Cor Boonstra succède à Jan Timmer à la tête de Philips : il doit annoncer de lourdes pertes, mais aussi un ensemble de mesures destinées à faire monter l'action : ces mesures étaient à ce point radicales que l'ordre était de supprimer toute activité qui ne donnait pas à Philips d'être dans le top 10 mondial du secteur et de refuser tout investissement qui ne faisait pas monter l'action. Ces mesures feront merveille pour les actionnaires, mais conduiront au démantèlement progressif de Philips. Seule « Royal Philips », focalisée sur les activités médicales et « Lightning » (Éclairage) vont subsister comme « Divisions de Produit » significatives. Le reste sera vendu avec option de branding (c'est-à-dire de payer une fee à Philips pour utiliser son logo !

1.8.2 Les 5 valeurs de Philips

Il est étrange de voir comment de superbes directives générales de gestion éthique, émises par Philips en 1993, vont être distordues en 1996. En effet, sous le titre « *The Philips Way* » [L'Esprit Philips], en 1993, un code de conduite était édicté. Il était organisé autour de « Cinq valeurs » et de « Quatre idéaux de gouvernance ».

Les 5 valeurs étaient :

1. Satisfaire pleinement nos **clients** [Delight customers]
2. Considérer nos **collaborateurs** comme notre ressource principale [Value people as our greatest resource]
3. Introduire **Qualité** et Excellence dans toutes nos actions [Deliver quality and excellence in all actions]
4. Tirer le meilleur parti de notre capital investi [Achieve premium return on equity]
5. Encourager l'esprit d'**entreprise** à tous les niveaux [Encourage entrepreneurial behaviour at all levels]

Les 4 idéaux de gouvernance étaient :

1. Gérer efficacement les **compétences noyaux** [Manage our core competences effectively]
2. Développer les **coopérations** inter-organisation [Develop cross-organisational co-operations]
3. Élimination de pratiques managériales **contreproductives** [Eliminate counter-productive management practices]
4. **Déploiement immédiat** de pratiques managériales nouvelles et meilleures [Implement new and better management practices immediately]

Sous l'impulsion de Cor Boonstra, la valeur N°4 et les idéaux N°1 et N°4 vont être hypertrophiés et l'idéal N°2 va être interdit (car il rend difficile la valorisation et la vente d'organisations par parties).

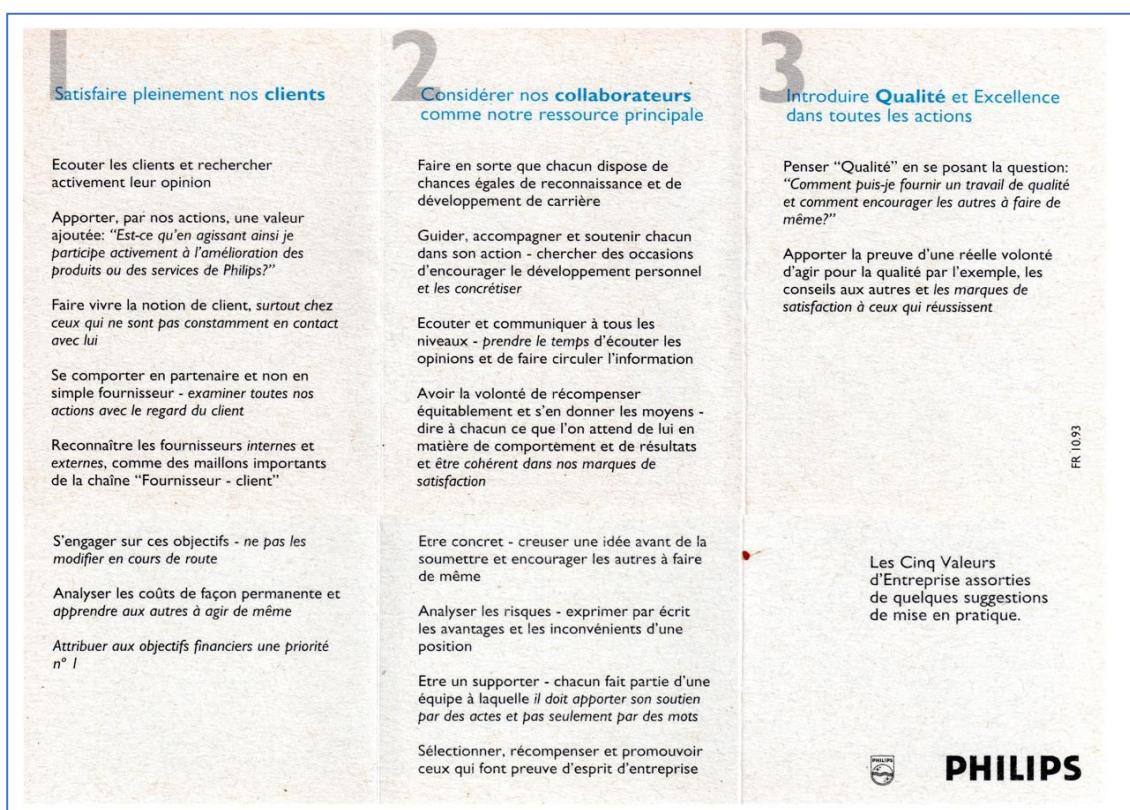


Figure 19 : « the Philips Way » (1 – 3)

<h2>4</h2> <p>Tirer le meilleur parti de notre capital investi</p> <p>Etablir des objectifs financiers clairs et s'assurer que tous les partenaires internes comprennent et sachent comment les atteindre</p> <p>S'engager sur ces objectifs - ne pas les modifier en cours de route</p> <p>Analyser les coûts de façon permanente et apprendre aux autres à agir de même</p> <p>Attribuer aux objectifs financiers une priorité n° 1</p>	<h2>5</h2> <p>Encourager l'esprit d'entreprise à tous les niveaux</p> <p>Stimuler la liberté des idées, dans un cadre clairement défini - entraîner ses collègues à comprendre comment une idée devient une suggestion vraiment pratique</p> <p>Etre concret - creuser une idée avant de la soumettre et encourager les autres à faire de même</p> <p>Analyser les risques - exprimer par écrit les avantages et les inconvénients d'une position</p> <p>Etre un supporter - chacun fait partie d'une équipe à laquelle il doit apporter son soutien par des actes et pas seulement par des mots</p> <p>Sélectionner, récompenser et promouvoir ceux qui font preuve d'esprit d'entreprise</p>	<p>The Philips Way "L'Esprit Philips"</p> <ul style="list-style-type: none"> • Nos Valeurs <p>Les Cinq Valeurs d'Entreprise assorties de quelques suggestions de mise en pratique.</p>  <p>PHILIPS</p>
--	---	---

Figure 20 : « the Philips Way » (4 – 5)

En fait ces cinq ‘valeurs’ correspondent assez à ce qui était espéré par les collaborateurs de Philips et de MBLÉ.

En pratique, elles étaient effectivement vécue de manière assez disparates.

La valeur N°1 ‘Satisfaire nos clients’ avait peu de sens dans les Bureaux d’études. Néanmoins, si l’on voyait ‘Philips’ comme notre donneur d’ordre, il était aussi en quelque sorte notre client.

La valeur N°2 ‘Nos collaborateurs sont notre ressource principale’ était vécu de manière effective, au-delà même de ce que Philips imaginait. Deux biais profonds marquaient la culture d’entreprise de la direction de Philips.

D’une part Philips avait organisé une ségrégation des personnes en fonction de leur niveau hiérarchique ! Il faut imaginer qu’à Eindhoven et à Hilversum un promotion impliquait de déménager vers une maison ou une villa de plus haut standing !

D’autre part, il y avait une ségrégation au niveau du sexe : les femmes étaient engagées pour des fonctions dites ‘subalternes’. L’idée même qu’une femme puisse être engagée comme ingénieur semblait farfelue ! Pire encore, lorsque j’avais proposé Andrée Lenoir comme ‘Chef de Projet’, le comité de direction m’avait clairement dit « *Vous n'y pensez pas ! C'est une femme et jeune encore ! Elle aura des enfants et le projet ira à vau-l'eau !* ». J’ai tenu bon et le projet c’est déroulé sans accroc. Elle a d’ailleurs fait une brillante carrière en dehors de Philips. Je pourrais raconter des anecdotes similaires pour Marieke de Soete, Véronique Baudrenghien, Sabine Spronck et Michèle Struvay.

The Philips Way

Group Management Committee 1993

 **PHILIPS**

Introduction

This booklet aims to set out the guiding principles by which all managers can judge their actions and achievements. It is not simply our corporate philosophy; not just an ideal towards which we strive for the future.

It is a code of conduct for today.

We are all agreed that what is needed within our organisation is action, not just words. And the only way we can expect others to act is to start setting an example ourselves.

As with any guidelines of this type, these cannot hope to cover every aspect of every individual's role within Philips. But we believe our corporate intentions are now clearly defined - how each individual carries them out will be a measure of their own skill and commitment.

Figure 21 : « the Philips Way » Introduction

Our Purpose

As a company our Purpose is clear:

- To improve our customers' lives at home and at work by providing innovative, attractive and easy-to-use products, software and services
- To increase our shareholders' value by meeting or exceeding our profit and investment goals
- To make working at Philips an enjoyable, stimulating and challenging experience
- To make the Philips company name one which inspires pride and confidence
- To conduct our business ethically and with respect for our customers, employees, shareholders, suppliers and the communities in which we operate

Our Beliefs

To achieve our Purpose we must not only be aware of our corporate objectives but also develop a set of Beliefs that underpin our everyday actions. Performance can only be improved if people *believe* in what they are doing and, as managers, it is our role to demonstrate these Beliefs to others.

As a company we believe:

- our people want to do a good job
- each of our employees has a key role and knows how to fulfil it better than anyone else
- high performance is the result of a personal sense of responsibility
- our people must be given trust, co-operation and respect if they are to develop a personal sense of responsibility
- our people are motivated by open, two-way communication

which means that, as managers, we believe:

“We must encourage our employees to feel responsible for their own performance by showing respect for their contribution and by giving them the opportunity to participate in the arrangement and direction of their own work.”

“We must encourage teamwork amongst all of our employees.”

“We must keep our employees informed *and* listen to their views.”

“We are accountable for recognising and developing the skills and talents of our staff.”

“We must encourage our employees to use their initiative by providing the direction, the freedom *and* the support to work creatively.”

“We must ensure our employees are given work that stretches their capabilities and that they are inspired to seek out new challenges for themselves.”

“Every employee should have equal opportunities for recognition and career development, so we must monitor and recognise performance consistently and reward fairly.”

Figure 22 : « the Philips Way » Notre objectif

<p>Our Values</p> <p>In addition to our commonly held Beliefs, it is important for us to share a set of values that clearly state how we aim to achieve our Purpose. Through internal and external research we have arrived at a list of Five Corporate Values which we believe will be the cornerstone of our future development and success.</p> <p>These values are listed below together with some practical ideas on how to put them into everyday practice.</p> <p>1 Delight customers</p> <ul style="list-style-type: none"> • Listen to customers and actively seek their opinion • Add value through all your actions - ask yourself '<i>Am I actively improving Philips products or services through this action?</i>' • Make the customer visible, especially to those not in day-to-day contact with customers • Be a business partner not simply a supplier - look at all your actions from the customer's point of view • Treat both internal and external suppliers as a valued part of the customer's supply chain <p>2 Value people as our greatest resource</p> <ul style="list-style-type: none"> • Ensure every employee has equal opportunity for recognition and career development • Monitor, coach and support people - look for opportunities to encourage personal development, and act on them • Listen and communicate to all levels - make time to hear views and give out information • Be willing and able to reward fairly - define how we expect others to behave and what we want them to achieve and make sure we are consistent in our rewards 	<p>3 Deliver quality and excellence in all actions</p> <ul style="list-style-type: none"> • Understand quality, ask yourself '<i>How can I deliver quality in my own role and encourage others to do the same?</i>' • Demonstrate commitment to quality - let others see us delivering quality, show them how to follow suit and reward achievements <p>4 Achieve premium return on equity</p> <ul style="list-style-type: none"> • Set clear financial targets and make sure your colleagues understand them and know how to achieve them • Commit to these targets - do not move the goalposts • Maintain continuous cost evaluation - and educate others to do the same • Make our financial targets your number one priority <p>5 Encourage entrepreneurial behaviour at all levels</p> <ul style="list-style-type: none"> • Encourage freedom of ideas within clearly defined borders - educate your colleagues to understand what makes an idea a truly practical suggestion • Use realistic reporting - work on an idea before submitting it and encourage others to do the same • Agree risk assessment - look at the risks and present the pros and cons formally, in writing • Be a supporter - you are part of the team, so support with actions not just words • Select, reward and promote people who demonstrate entrepreneurial behaviour
--	--

Figure 23 : « the Philips Way » Nos valeurs

<p>Our Governance Ideals</p> <p>In order to achieve a common acceptance of our Beliefs and implementation of our Values we must adopt a clearly defined approach to Corporate Governance. To achieve this we must commit ourselves to the following courses of action:</p> <ul style="list-style-type: none"> • To manage our core competences effectively • To develop cross-organisational co-operation • To eliminate counter-productive management practices • To implement new and better management practices immediately <p>The following is a list of practical ways in which we can fulfil these new commitments:</p> <p>1 Manage our core competences effectively</p> <p>The core competences will be identified and defined by the Board. It is essential for our Company's future profitability that a consistent approach to their management is achieved throughout the organisation. We can achieve this by:</p> <ul style="list-style-type: none"> • <i>Understanding the importance</i> of managing the Company's core competences effectively • <i>Giving our full support</i> to the departments which are responsible for managing these competences • <i>Implementing the practices</i> which are developed to support these competences <i>without delay</i> 	<p>2 Develop cross-organisational co-operation</p> <p>We agreed that altering the Company structure will not by itself achieve our objectives. Instead we must also change how we behave within that structure - and that will require <i>constant and whole-hearted co-operation</i> across different product areas, functions and national boundaries. We can achieve this by:</p> <ul style="list-style-type: none"> • Understanding and believing in the set of common Beliefs and Values defined previously in this document • Giving managers <i>clear guidelines</i> for cross-organisational co-operation • Suggesting methods of cross-organisational learning • <i>Looking out for</i> and indicating opportunities for cross-organisational co-operation through our existing review procedures <p>3 Eliminate counter-productive management practices</p> <p>Before we can cope with the challenges of profitable growth we must eliminate certain characteristics of our organisation that currently work against our ideals of co-operation and commonly held Beliefs and Values. These counter-productive characteristics include:</p> <ul style="list-style-type: none"> • Working for personal, rather than corporate gain • Territorial behaviour and lack of co-operation • Slow learning • Limited active support and coaching of subordinates • Acceptance of mediocre performance
--	--

Figure 24 : « the Philips Way » Nos idéaux de gouvernance

4 Implement new and better management practices immediately

Our objectives can only be achieved through *truly* empowering individuals to take the initiative themselves and make their own informed decisions. This can be achieved by:

- Establishing best practices and *setting an example* in their implementation
- Defining certain management processes as a guide for others
- Encouraging each Business Unit to define how its management process and levels '*add value*' to the business as a whole
- Supporting and encouraging subordinates through direct coaching and by example
- *Taking and sharing responsibility*
- Challenging people's performance by setting targets and *monitoring change*
- Using the existing review process and establishing new procedures for rewarding positive changes in behaviour

Overall, our management objective is to create an attitude of collective responsibility towards achieving our shared business ambitions. This means that, as managers, our personal credo must be:

"I understand and believe in the Company's Purpose and I am personally responsible for helping to achieve it through my commitment to our Beliefs, Values and Governance Ideals."

GB 11.83
Printed on T2N-recycled paper



PHILIPS

Figure 25 : « the Philips Way » mettre en œuvre subito une gestion nouvelle et meilleure

1.8.3 L'ordre d'arrêter tout ce qui ne fait pas monter l'action de Philips

Cette dynamique (dynamite !) managériale de faire monter l'action de Philips à tout prix va conduire notamment à l'arrêt de la commercialisation d'ARCADE, à l'arrêt des développements de l'ATM, à l'arrêt des activités de la « Business Opportunity Platform », à l'arrêt des activités de sécurité et de cryptographie, à l'arrêt des applications [tel le FideFax qui sera décrit ci-après] basées sur les codes de représentation des données en évidence et perception [par des codes à barres ou bidimensionnels (comme les QR codes) ou tridimensionnels (comme les PDF-417 en couleurs)]. Pour être certain que personne ne puisse prendre de brevets généraux, le 15 septembre 2000, avec l'accord de Philips, j'ai fait sur ce sujet une conférence à Vienne à la tribune d'InterGraph (l'organisation regroupant les organisations impliquées dans la conception et la fabrication de Cartes d'Identité, de Billets de Banque et de Passeports). Philips considérait que ces technologies et applications n'avaient aucun avenir chez Philips.

Bien des autres secteurs seront ainsi supprimés ou vendus : les recommandations de Richard L. Wexelblat du Research Laboratory de Philips à Briarcliff Manor ; de Jean Dumortier du Research Laboratory de Philips à Montréal ; de Jakob Vlietstra de PTI // AT&T à Hilversum ; et d'autres éminents collaborateurs de Philips ... vont être totalement ignorées.

À cette époque, PRLB restait concentré sur de la recherche fondamentale et peu sur la recherche appliquée. Il faut cependant noter que Pierre Wodon, Jean-Marie Goethals et Claude Fosseperez ont tenté d'infléchir cette tendance plus conceptuelle vers une vision plus réaliste. Mais il était trop tard.

Néanmoins, une avancée majeure, brillante, a encore eu lieu à ce moment [1989] : l'invention du protocole ZK [Zero Knowledge] en cryptographie par Jean-Jacques Quisquater [PRLB] et Louis

Guillou [France Télécom] ! En 2012, un gros livre (500 pages) hommage à Jean-Jacques Quisquater a été publié par Springer-Verlag sous le titre « *Cryptography and Security: From Theory to Applications* ». Il contient 33 contributions d'experts en cryptographie coordonnés par David Naccache. L'article « *The Challenges Raised by the Privacy-Preserving Identity Card* » (Yves Deswarte et Sébastien Gams) montre que l'utilisation conjointe de solutions à clé publique (comme RSA) et de protocoles à apports nuls de connaissance (ZK) sont parfaitement capables de relever le challenge !

Il faut aussi signaler que SWIFT est devenu le centre mondial de la consolidation des échanges entre banques au niveau mondial, en partie grâce au support de PRLB [essentiellement Jean-Jacques Quisquater] et, marginalement, de SOC. En effet, le codage pour applications militaires appelé « DES » ne pouvait être fourni qu'à des militaires après agrément des pouvoirs politiques belges et internationaux. Nous sommes parvenus en Belgique à faire passer le DES comme un produit à double usage (civil et militaire) et nous avons donc pu légalement livrer à SWIFT les codeurs et décodeurs DES. De même, nous avons équipé les camions et les sièges de sociétés internationales de transport et logistiques (avions et camions) de systèmes de communication protégés par une cryptographie basée sur DES.

Dans cette ligne, les activités militaires seront toutes vendues, en particulier celles de PPS [Philips Professional Systems Belgique] qui seront transférées à Thomson (Tubize).

1.9 Philips Professional Systems : 1987 - 1997

Jacques van Haren & Jacques Berleur & Dirk Frimout & Melchior Watheler

Mes champs de recherche :

Réseaux de télécommunication / Sécurisation des Operations et des Communications / Informatique et Droit

Le départ à la retraite de Jakob Vlietstra à Hilversum ; les décisions de rationalisation et la prise de pension imminente de Stéphane de Vleminck ... conduisent à ce que je cesse de travailler en part-time à Hilversum. Adieu à ce pied-à-terre de Loosdrecht, aux voiliers, au restaurant 'Het Kompas', au promenades dans ce mini 'Key West'...

Un peu avant, Claude Fosseperez quitte aussi Loosdrecht pour être nommé à Eindhoven, puis comme directeur de PRLB.

En 1992, Jacques van Haren est nommé directeur de Philips Belgique en remplacement d'Urbain Devoldere. Ce qui reste de MBLE devient « Philips Professional Systems » [PPS]. À sa prise en pension, je succède à Stéphane de Vleminck comme directeur technique de PPS.

Parmi les diverses activités que je dirige, je n'en évoquerai que trois d'entre-elles :

- Le projet et démonstrateur ATM de la BBA
- Secure Operations & Communications
- « Business Opportunity Platform ».

La création de l'Association Sans Buts Lucratifs TITAN où Philips a joué un grand rôle sera présentée ci-après.

1.9.1 La situation au début des années 1990

Le besoin d'organiser les transports de données et d'organiser les liens avec les applications a émergé dans les années 1980. Rapidement il a été reconnu que le besoin était les noeuds des réseaux et les liaisons entre les noeuds devaient être organisées pour que de nouvelles liaisons ou de nouveaux noeuds puissent être ajoutés ; mais aussi que leurs caractéristiques puissent changer ; mais aussi puissent tomber en panne. C'est un peu les caractéristiques auxquelles les militaires sont confrontés.

Pour répondre à ces 'challenges' il fallait découper les messages en blocs de données et organiser le choix du chemin envoyant chaque bloc de l'émetteur au destinataire. Trois approches vont être suivies caractérisées par la manière par laquelle les blocs seront routés et que finalement le message soit reconstitué.

1. Les PTT (Poste – Téléphone – Télégramme) mondiaux adoptent l'approche de la numérisation de leur 'core business' et l'utilisation compatible de leurs infrastructures et de leur quasi-monopole dans ces secteurs : le réseau à couche qui en résultera est de transmission de données à commutation de paquets suivant la norme **X25**. En France, il s'agira du réseau « **Transpac** » et d'applications telles que le Minitel, précurseur des services Web. Le routage y est prédictible. Les enjeux industriels de la CGE [Compagnie générale d'Électricité] le fournisseur essentiel des PPT français conduisent à promouvoir cette approche ciblée aux dépens de solutions porteuses d'avenir. Le porteur industriel et politique de cette dynamique était Ambroise Roux, le président de la CGE. En fait, il s'agissait de réaliser des réseaux privés a priori non interconnectés
2. Une autre approche laisse les paquets trouver leur routage adaptatif à chaque noeud. Il s'agit en fait d'une approche établissant une approche fédérant des réseaux : en quelque sorte un « réseau de réseaux ». Deux mises en œuvre vont faire leurs preuves de cette approche : d'abord le réseau français de **Cyclades** [basé sur le Datagramme de Louis Pouzin, développé à l'IRIA (qui

deviendra l'INRIA)] et plus tard, via une adaptation du réseau **Arpanet** qui deviendra **Internet**. Cette approche intrinsèquement, par principe et par construction n'offre aucune garantie de qualité de service autre que « *best efforts* » : pas de garantie que le message pourra être reconstitué ou arriver en ‘temps utile’ (reportages audio / vidéo, téléphonie ...) ni donner priorité à certains types de trafic (hôpitaux, pompiers ...). Le World Wide Web a choisi Internet comme réseau malgré que les Cyclades lui était nettement supérieur. CII faisait la promotion de l'approche des Cyclades, mais les PTT ont combattu l'approche du Datagramme pour promouvoir l'ATM en combinaison avec Transpac. La France du président Giscard d'Estaing a arrêté Unidata en 1975 et a bridé CYCLADES en 1976 et l'a arrêté définitivement en 1978. Ces décisions étaient officiellement basées sur des visions ultralibéralistes, où VGE exploitait ses pouvoirs et sa position en vue de favoriser des intérêts français (mais sans vision à long terme).

Les tribulations de ces luttes d'influence ont fait l'objet de nombreux articles économiques, scientifique et surtout politiques ; mais ont aussi inspiré des romans à succès, dont le plus connu est « *Comédies françaises* » d'Éric Reinhardt (Gallimard). Je ne résiste pas à citer une phrase de ce livre (page 382 de l'édition originale de 2020) :

« C'est à croire qu'Ambroise Roux, quand il avait arraché à Valéry Giscard d'Estaing, à peine élu, la décision de disloquer le consortium européen Unidata, de clore le Plan calcul, de liquider la Délégation générale à l'informatique et, par voie de conséquence, de passer par pertes et profits le datagramme élaboré par Louis Pouzin dans son laboratoire de l'IRIA à Rocquencourt, avait identifié au plus profond du subconscient du nouveau président de la République un putain gros désir refoulé [...] de réorientation de la politique française dans le domaine des télécoms ».

Il y a probablement un peu de vrai dans cette phrase issue d'un livre orienté, prêtant à Amboise Roux et à Valery Giscard d'Estaing une compréhension technique du domaine et une vision sur les personnes que, de toute évidence, ils n'avaient pas.

3. L'approche de l'**ATM** est une variante ouverte de la première approche. Elle organise le routage des paquets sur base des besoins de service. C'est ce que l'on appelle l'approche à « qualité de service » paramétrée. Le routage des paquets est organisé de bout en bout suivant les besoins exprimés et les ressources sont réservées avant d'envoyer : il y a connexion logique et physique tout en optimisant l'utilisation des ressources. En cas de problème, il faut réinitialiser. Au début des années 1990, sous la coordination des Pouvoirs Publics (à savoir le CCITT) un consortium mondial a défini un avant-projet de norme de transport de données entre des pointes d'accès qui soit universelle (tous types de données représentant voix, vidéo, images ...) et à qualité de service garantie : l'**ATM** [*Asynchronous Transfer Mode*]. En Belgique, sous la coordination de la RTT [Régie des Télégraphes et Téléphones] (au moment où elle devient Belgacom) un consortium va être établi pour réaliser un démonstrateur ATM complet qui fait l'objet ci-après, du témoignage de Jean Voisin, l'un des acteurs phares de ce projet.

L'ATM organise la qualité de service de manière très souple et bien adaptée aux spécificités des couches applicatives et des types de données (documents ; streaming ; interaction ...) représentant l'Information.

Dans un premier temps, en pratique, l'Internet, dopé par le Web, a complètement supplanté toutes les autres techniques, y compris l'ATM, malgré ses qualités indiscutables.

Mais, aujourd'hui Internet a montré ses limites malgré l'abondance de ressources mises à disposition pour pallier ses limitations intrinsèques. De nombreuses mises en œuvre d'Internet se font maintenant en adoptant des techniques mixtes : l'accès à Internet se fait via les protocoles Internet normalisés [essentiellement, les **protocoles “TCP”** (Transmission Control Protocol) et “IP” (Internet Protocol)] ; mais les routages et la transmission ultérieurs se

font via d'autres technologies de communication, à qualité de service assurée, afin de réaliser les réseaux centraux. L'ATM est l'une de ces technologies qui revient en force.

1.9.2 Collaboration pour l'ATM : le projet BBA

Ce projet pilote et cette collaboration sont décrits dans la contribution de Jean Voisin dans l'ouvrage associé à ce livre. Jean Voisin l'évoque ci-après.

Il m'a semblé pertinent d'introduire le contexte tant technique que politique de ce projet et de l'ATM.

La collaboration de Philips avec AT&T à Hilversum battant de l'aile, il a été décidé que le groupe des télécommunications de PPS ne serait plus connecté avec Hilversum, mais avec PKI, le centre de production et de recherches de Philips à Nürnberg sur les télécommunications [*Philips Kommunikation Industrie*].

En 1987, alors que la normalisation de cette technique au niveau international n'en était qu'à ses prémices, Belgacom lança en Belgique un projet de recherche très ambitieux dans le domaine de l'ATM. Il en confia l'exécution à un consortium dénommé « *Belgian Broadband Association* » (BBA). Ce consortium regroupait les principaux fabricants belges de matériel de télécommunication (Alcatel Bell, ATEA/Siemens, Alcatel Bell-SDT et Philips).

Le porteur de cette vision à Belgacom fut Marcel Fastrez : je l'ai rencontré aux deux réunions de coordination auxquelles j'ai assisté et lors des démonstrations et tests de validation (à Uccle, près de l'observatoire, au 49 avenue Lancaster). Il maîtrisait parfaitement ses dossiers. De plus, humainement, c'était quelqu'un de très agréable avec qui on pouvait collaborer dans une ambiance sereine. Jean Voisin qui l'a côtoyé bien plus que moi, confirme complètement cette vision positive de Marcel Fastrez.

Une anecdote :

Tant pour le projet BBA que pour les Set-Top-Boxes du DVB, j'ai été amené à aller de nombreuses fois à l'usine et bureaux de Philips à Suresnes. En mi-1993, lorsque l'Union européenne a organisé de ne plus avoir de contrôles systématiques des douanes aux frontières des États, je me suis trouvé dans une situation particulière. Arrivant à la Gare du Nord à Paris, je suis arrêté par les agents du « Services des douanes » pour contrôler ma valise. Ils y découvrent 10 cartes de commutateurs de paquets X25 et je leur montre que j'ai bien avec moi l'autorisation de mouvement estampillée sur le nouveau formulaire signalant que Philips avait préalablement déclaré que j'allais livrer ce matériel à notre usine de Suresnes à la date du jour. Les agents ne veulent rien entendre ; ils me déclarent que j'ai tenté de passer frauduleusement du matériel électronique ; que rien ne prouve que ce matériel ne tombe pas sous le coup d'un embargo ; que c'est peut-être du matériel 'militaire sensible' ; que je n'ai droit qu'à un seul coup de téléphone. J'appelle donc le directeur technique de Suresnes ; en m'entendant, il se met à rire et me dit qu'il arrive avec le conseiller juridique de Philips France. En les attendant, je suis mis dans la prison de la gare du Nord. Deux heures plus tard, le conseiller juridique me fait libérer. Nous quittons la gare (avec les cartes X25) dans la voiture du directeur technique de RTC Suresnes, qui m'explique que les agents des douanes françaises sont opposés à ce nouveau protocole de libéralisation des frontières et que les Services décentralisés n'ont jamais officiellement reçu les instructions du ministère annonçant les nouvelles procédures ! Ces instructions, comme par hasard, ont été perdues par La Poste partout en France !

En février 1993, au nom de PPS [*Philips Professional Systems*], je signe un « *Memorandum of Understanding* » spécifique à l'ATM avec la « *Business Unit NetWork Systems* » PKI [*Philips Kommunikation Industrie*] par laquelle toutes les retombées du projet BBA pourront être exploitées par PKI avec PPS en support ; le financement de la partie non subsidiée du projet BBA étant à charge de PKI. En fin 1996 (ou début 1997) Philips PKI sera forcé d'abandonner toute recherche et projet de production de systèmes ATM.

Une autre convention avait été signée avec PKI pour les contributions de PPS à la mise sur le marché du premier système de guidage par satellite GPS. Philips ordonnera aussi à PKI de cesser ces activités sur le GPS.

1.9.3 Secure Operations & Communication [SOC]

Son objectif : la sécurité et la qualité de l'informatique à usage civil

En 1994, le gouvernement des Pays-Bas suggère (?) à *Philips Corporate* de prendre le contrôle de la société CryptoAG²⁸ et d'assurer l'assurance de qualité de leurs produits. Cette petite société est exclusivement dédiée aux applications de la cryptographie pour l'armée. Philips va renommer cette société « Philips Crypto », puis PHILIPS-USFA.

En France, à Fontenay-aux-Roses, Philips a créé le centre de développement et de production des cartes à puce cryptographique : le TRT-CTI.

Dans les années 1980, PRLB (l'équipe coordonnée par Jean-Jacques Quisquater) avait fait des merveilles pour planter le calcul du DES dans l'espace mémoire libre (ridicullement petit) des cartes de première génération.

Au début des années 90, je propose alors à Urbain Devoldere (le CEO de Philips Belgique) et Jacques Van Haren (CEO de Philips Professional Systems) de créer un département de PPS dédié à la sécurité et à la qualité de l'informatique à usage civil qui serait un complément de Philips-Crypto (restant focalisé sur les applications militaires) : SOC !

La direction de Philips à Eindhoven accepte cette création. Lorsque Philips prend le contrôle de CryptoAG, il impose que SOC soit sous son contrôle et qu'un département commercial spécifique à SOC soit créé au sein de PPS.

Les incompréhensions entre CryptoAG / Philips Crypto et SOC seront nombreuses, car les règles et pratiques des applications militaires ne conviennent pas aux besoins des applications civiles. Rapidement, dès 1991, la coordination *corporate* est transférée en France sous la forme d'une collaboration avec TRT-CTI [M. Selezneff] et en synergie avec la BU-TT, la Business-Unit « Terminaux de Télévision à péage » [M. Jacques Lefèvre (CEO) & M. Allan de Suza (Directeur Commercial)] à Suresnes. La volonté de cette BU-TT était de disposer d'une offre complète de « Set-Top-Boxes » et de plug-in de contrôle d'accès (via le Common Interface PCMCIA) des téléviseurs et système de diffusion de programmes conformes à la norme ETSI émergente du projet DVB [*Digital Video Broadcasting*].

L'élaboration et la mise en œuvre du système de contrôle d'accès DVB de Philips est confié à SOC et une mise en œuvre pilote de 2 000 terminaux est décidée d'être faite en Belgique en collaboration avec Canal+ Belgique, le contrôle d'accès étant réalisé via CryptoWorks. BU-TT nous garantit 500 terminaux en octobre 1996 et 1 500 en novembre 1996.

Bernard Durieux et Jean Desmet coordonnent ce pilote pour CryptoWorks et l'EPG [*Electronic Program Guide*]. En parallèle nous développons un système de Fax sécurisé en collaboration avec la firme suédoise qui a inventé les « Mister Cash » et autres terminaux bancaires accessibles au public.

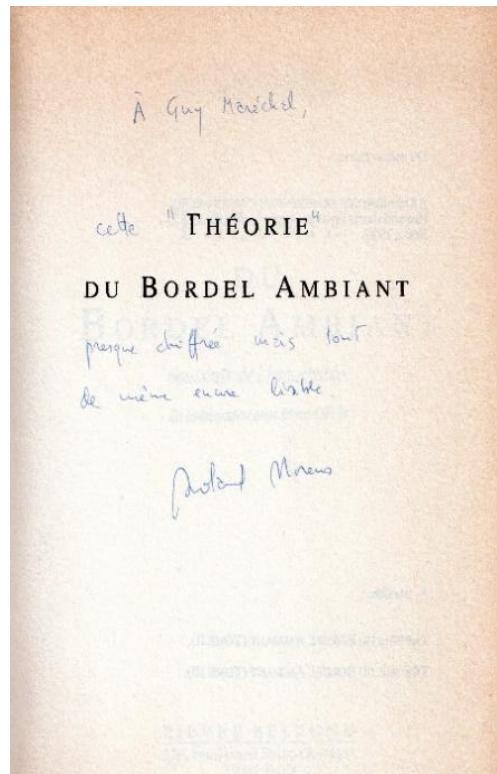
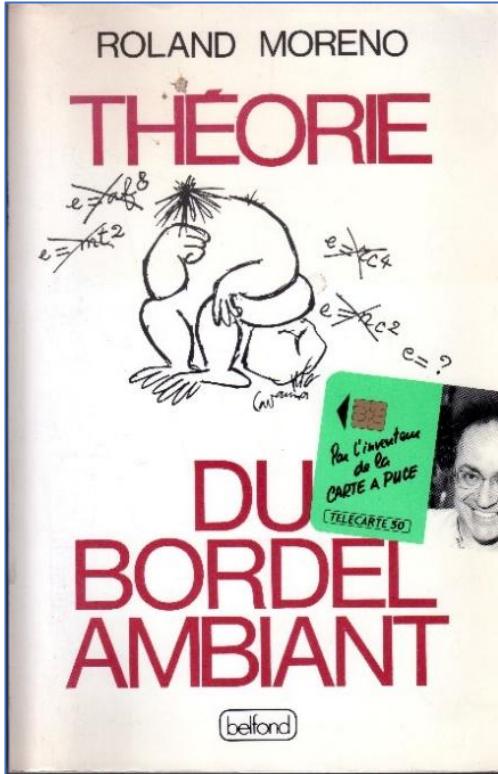


Figure 26 : Roland Moreno : la théorie du bordel ambiant

À ces occasions, je rencontre l'inventeur de la carte à puce, Roland Moreno qui me dédicace un exemplaire de son livre phare « Théorie du bordel ambiant : souvenir de l'irréversible ». Rencontre inoubliable tant il s'auto caricature !

1.9.3.1 ISO-9000 & OAIS & « Green Book »

La collaboration de SOC avec la Commission européenne a aussi pris via la participation à un projet de rédaction du « Livre Vert » de la sécurité informatique. Le 29 avril 1995, la Commission européenne approuvera ce document sous le nom : « **Green paper on the Security of Information Systems** ». Il sera usuellement connu sous le nom de « Green Book ». La Commission voulait pouvoir incorporer la sécurité informatique dans les normes de « Qualité » qui étaient en préparation. Une classification des approches et des forces respectives des diverses approches a été réalisée.

Ma copie de ce document a été confiée à M. Edouard Van Heule (Belgacom) qui est décédé sans me l'avoir rendu ; mais des copies devraient pouvoir être retrouvées dans les archives des travaux de la Commission visant à contribuer à l'élaboration de l'ISO-9000 pour la partie de sécurisation de l'information

SOC a collaboré à donner des cours pour former des évaluateurs qui seraient chargés de contrôler des logiciels applicatifs sensibles, et ce préalablement à leur mise en service dans le cadre de la norme **ISO-9000** couvrant la « qualité » !

Dans le cadre de ce même programme, SOC a contribué à l'élaboration de la partie du « *Conceptual data model* » de la norme d'archivage **OAIS** [*Open Archival Information Systems*] et en a assuré des formations.

Une version gratuite de la norme est distribuée par les agences spatiales : <https://public.ccsds.org/Pubs/650x0m2%28F%29.pdf>. La version officielle est identifiée ISO 14721 : <http://www.oais.info/>

1.9.3.2 CryptoWorks : la plateforme technique et son application pour le DVB / BUTT.

La plateforme cryptographique

La collaboration de SOC avec la BU-TT avait été organisée. Le logiciel d'exploitation était développé par BU-TT et le logiciel de gestion par SOC.

En pratique, BU-TT se chargeait, du côté des abonnés, de l'interaction, via la télécommande des terminaux ou du téléviseur, essentiellement en interaction avec l'EPG [*Electronic Program Guide*] ; du côté des fournisseurs il se chargeait de fournir les données nécessaires à la facturation.

SOC était chargé du logiciel de gestion des abonnés et des services auxquels ils ont accès ; des fournisseurs de contenu ; des canaux de diffusion ; des pouvoirs publics compétents et du contrôle du « *rating* » [sexe / violence / éthique] des programmes.

Les trois éléments techniques fondamentaux étaient les CAP [Cartes à puce (pour les terminaux ou pour les modules des Common Interfaces)], les Protocoles d'authentification et les TRD [*Tamper Résistant Devices*].³⁰

Pour les CAP, le groupe cryptographique de PRLB, en particulier Jean-Jacques Quisquater, a collaboré avec les experts français, en particulier Louis Guillou, pour convaincre TRT-CTI de développer un nouveau type de CAP [carte à puce] basée sur RSA et DES : avancée significative pour pouvoir développer des applications civiles. Nous avons collaboré avec TRT-CTI pour que ces CAPs soient caractérisées par les éléments suivants :

- Chaque CAP est typée, identifiée et il lui est attaché un couple ‘Clé Publique / Clé Secrète’ et les certificats associés. Ces données sont verrouillées lors de la production.
- Dans chaque CAP, il y a un couple CP / CS destiné à prendre la main en cas de suspicion d'attaque. Ces données sont verrouillées lors de la production.
- Dans chaque CAP il y a des tiroirs de service qui peuvent être ajoutés en production sous les contrôles des deux facilités initiales. Pour chaque tiroir : type de service, paramètres de service, identification, couple CP / CS.

Ces caractéristiques donnaient à ces CAP la possibilité d'être initialisés pour n'importe quel type d'application, en particulier pour le contrôle de la télévision suivant le DVB ; mais aussi que l'usager puisse accéder à plusieurs usages (comme carte d'identité, en même temps que carte sociale et de carte de banque) avec une seule carte dans sa poche. L'approche pouvait être étendue aux cartes SIM des téléphones portables dont le déploiement commençait.

Il fallait aussi assurer que, localement ou à distance, via les réseaux, des applications puissent agir en s'étant préalablement assurées de l'existence et de l'identité des Agents impliqués, vérifier qu'ils étaient bien ceux attendus / autorisés. Ces **authentifications** devaient pouvoir s'effectuer suivant divers protocoles combinant diverses approches :

- Ce que l'on est : pour des humains, les empreintes digitales, l'iris de l'œil ; pour une carte à puce, un filigrane personnalisé et une paire de clés cryptographique ...
- Ce que l'on possède : pour les humains, la possession d'une carte à puce ...
- Ce que l'on connaît : pour les humains, le mot de passe de la carte à puce que l'on possède ...
- Ce que l'on est capable de faire : pour les humains : reconnaître des types d'objets sur une photo ; signer valablement en temps réel ; résoudre un jeu complexe ; jouer « Pour Élise » au piano ; retirer un Euro du compte en banque d'une Organisation ...
- Suivant le témoignage d'un tiers fiable : l'agent de la population d'une administration communale ; le gynécologue certifiant la naissance d'un bébé dont il a été témoin et assistant ...
- Suivant l'endroit et le moment : pour un humain, être présent dans son domicile, dans sa voiture ...
- ...

Les **TRD** sont caractérisés par le fait que, lorsqu'ils sont fermés, ils ne peuvent exécuter que les programmes qui y ont été installés ! Ces programmes ont été préalablement validés comme capables d'effectuer le service prévu, rien que ce service et rien d'autre que ce service. Parmi les services prévus, il faut citer la génération des paires de clés, la génération de nombres aléatoires forts, la signature de documents, la vérification des signatures digitales et des certificats, la personnalisation de CAP (Agent / Rôle / Liens / paramètres), le chiffrement et déchiffrement de messages.

Il faut citer les noms de Bernard Durieux et Vlatko Bencic qui ont imaginé les deux astuces brevetables essentielles à la crédibilité radicale de notre TRD ; l'idée de développer un TRD comme une « *Trusted Third Party* » incorruptible, agnostique venait de moi, mais les ‘trucs’ pour une mise en œuvre concrète opérationnelle vient d'eux.

Bernard Durieux raconte cet épisode dans son témoignage en notant que c'est en buvant une « *Moinette* », la bière emblématique de la brasserie Dupont, que les choses ont pris forme. Nous avions même prévu le cas extrême où la prise de contrôle par les pouvoirs publics pouvait se faire, mais avec autorisation préalable et traces indélébiles. Bien plus tard, lors d'une réunion des anciens, Guy Van Hooveld me fit la remarque qu'il eut suffi de peu pour que nous réalisions des blockchains par l'enchaînement d'une collection potentiellement mondiale de TRD.



Figure 27 : le TRD de l'association des banques belges [1994]

Les choix et combinaisons d'approches permettent d'assurer au niveau de force de confiance recherché. Les applicatifs ou les services seront construits en combinant ces trois groupes de la plateforme cryptographique CryptoWorks. D'une certaine façon, la plateforme développée par SOC pouvait convenir à une très large gamme d'applications pouvant travailler en mode off-line ou on-line. Pragmatiquement ces applications ont pris le nom de CryptoWorks pour la télévision (car la plateforme de base avait été développée et financée pour le BU-TT) tandis que les autres applications ont porté le nom générique de FideServices.

Nous avons reçu beaucoup de pression pour incorporer des backdoors dans nos systèmes. Je n'imagine pas que l'on ait pu le faire dans SOC et j'ai toujours eu l'assurance qu'il n'y en avait pas dans les Cartes à Puces. Un article intéressant, abordant aussi ces backdoors, est celui de Cees Jansen : <https://www.ceesjansen.nl/en/cryptography/>.

CryptoWorks DVB

La première de ces applications fut donc la télévision numérique DVB à péage pour BU-TT.

Pour ce cas, la protection exigée est extrêmement forte, car, par définition, la télévision en diffusion (câble / satellite / terrestre) n'a usuellement pas de canal de retour, malgré le fait que le DVB avait prévu le protocole mixte : débit extrême en flux descendant et canal limité en flux montant ! Mais seuls quelques rares réseaux à câble coaxial supportaient ce canal de retour. Il fallait donc que la sécurité soit assurée par construction et via les protocoles sans rétroaction informatique. Ce n'est qu'à quelques moments très contrôlés que des initialisations se font (par la présence de personnes ; par un retour téléphonique ; par l'usage d'un TRD ...) et que le contrôle opérationnel se fasse en respectant la vie privée, sauf dans les cas prévus par la loi (anonymat démocratique).

Le déploiement pilote avait été préparé en Belgique via Canal+ Belgique (à l'époque une succursale de Canal+ France qui, à cette époque, avait un quasi-monopole sur la télévision à péage, mais pour de la télévision diffusée en analogique).

L'objectif était de faire un déploiement pilote en Belgique avec 2000 terminaux.

Le CEO de Canal+ Belgique, Daniel Weeckers, le directeur opérationnel, Alain Deneef, et le directeur technique, Francis Bodson, avaient organisé ce déploiement en étroite collaboration avec Philips [Jacques Van Haren (CEO de Philips Belgique), André De Smedt (CEO de Philips Professional Systems) et SOC technique et commercial (Kris Gielis)] et Jacques de Wergifosse [le CEO de RTD – Brutélé (le câblodistributeur couvrant Bruxelles)].

Dictat de Canal+ France

Stupéfaction !!! Canal+ France donne l'ordre à Canal+ Belgique de cesser la collaboration pour le déploiement pilote en Belgique. Malgré une tentative de médiation, le projet pilote avec Canal+ Belgique est arrêté.

Paradoxalement, quelque temps plus tard, Canal+ France achètera la licence CryptoWorks DVB et équipera sa succursale Roumaine des terminaux de la BU-TT avec CryptoWorks DVB.

Pour illustrer la puissance politique, culturelle et commerciale, il faut évoquer que Canal+ est parvenu à faire supprimer à la dernière minute, dans la norme ETSI du DVB, le champ d'identification des émissions diffusées. Son objectif était de rendre impossible de repérer les publicités. Le résultat est que la programmation de l'enregistrement d'une émission doit se faire sur base des heures prévues au programme. En pratique l'on démarre l'enregistrement 20 minutes avant et l'on le termine 20 minutes après et ainsi les publicités sont aussi enregistrées et l'on ne peut pas les zapper. Quelle gabegie et quel inconfort !

Démonstrateur Titan

Pour assurer la crédibilité des tests du projet pilote et impliquer indirectement les Pouvoirs Publics (à savoir le CSA [Conseil Supérieur de l'Audiovisuel] ; la CFB [Communauté française de Belgique] et l'IBPT [Institut belge des Postes et des Télécommunications], une ASBL [Association Sans Buts Lucratif] appelée TITAN avait été impliquée dans le projet dès le début. Philips, la CFB, Canal+ Belgique et RTD-Brutélé étaient membres fondateurs de cette ASBL. Le nom « TITAN » d'ailleurs se rapporte à ce projet créé comme « Terminal interactif de Télévision Analogique et Numérique ». Le président-fondateur de TITAN est Roger Roberts, un ancien cadre supérieur de la direction de la production de la RTBF [Radio-Télévision Belge Francophone] organisme lui aussi membre de TITAN.

De plus, les Facultés Notre-Dame de la Paix de Namur étaient aussi membre fondateur de TITAN, son représentant étant Yves Poulet, le fondateur du CRID ! Les aspects légaux étaient donc aussi couverts par ce projet pilote !

La première phase de ce projet pilote avait consisté en des essais grandeur nature de déploiement de la transmission numérique sur câble, en étroite collaboration avec Pierre de Wergifosse, le CEO

de Brutélé. Les essais concernaient le choix de la technique QPSK ou QAM, et le niveau de modulation. Sur base de ces tests, pour la Belgique, c'est le **QAM-64** qui a émergé.

Un autre type de test avait été organisé pour démontrer la qualité du codage en MPEG-2. TITAN a acquis au laboratoire de recherches de Philips France l'un des rares codeurs prototypes. Là aussi les techniciens et le grand public validèrent les paramètres **MPEG-2** recommandés par TITAN. Ce codeur sera bientôt visible au musée **NAM-IP** !

Le Conseil d'Administration de TITAN a poursuivi le projet pilote jusqu'à son terme, mais en ne le déployant que sur un seul terminal de BU-TT et avec CryptoWorks comme système de contrôle. Le démonstrateur a porté le nom d'**OSCAR** [Ouvert et Sûr Contrôle d'Accès pour Réseaux]. Les démonstrations et les validations ont toutes été faites avec un « sans faute » !

Certains des membres de TITAN n'ont jamais été mis au courant du dictat de Canal+ France.

Un des tous premiers déploiements complets du DVB a donc été effectué en Belgique ! Il a notamment servi lors de la constitution du dossier qui a abouti aux normes ETSI liées au déploiement du DVB, en particulier à la norme relative à l'agrément des équipements comme conformes aux normes et du niveau de qualité requis pour les exploitations.

Quelque temps plus tard, Philips ordonnera la fermeture de SOC et exploitera le CryptoWorks-DVB en partenariat avec son associé suédois.

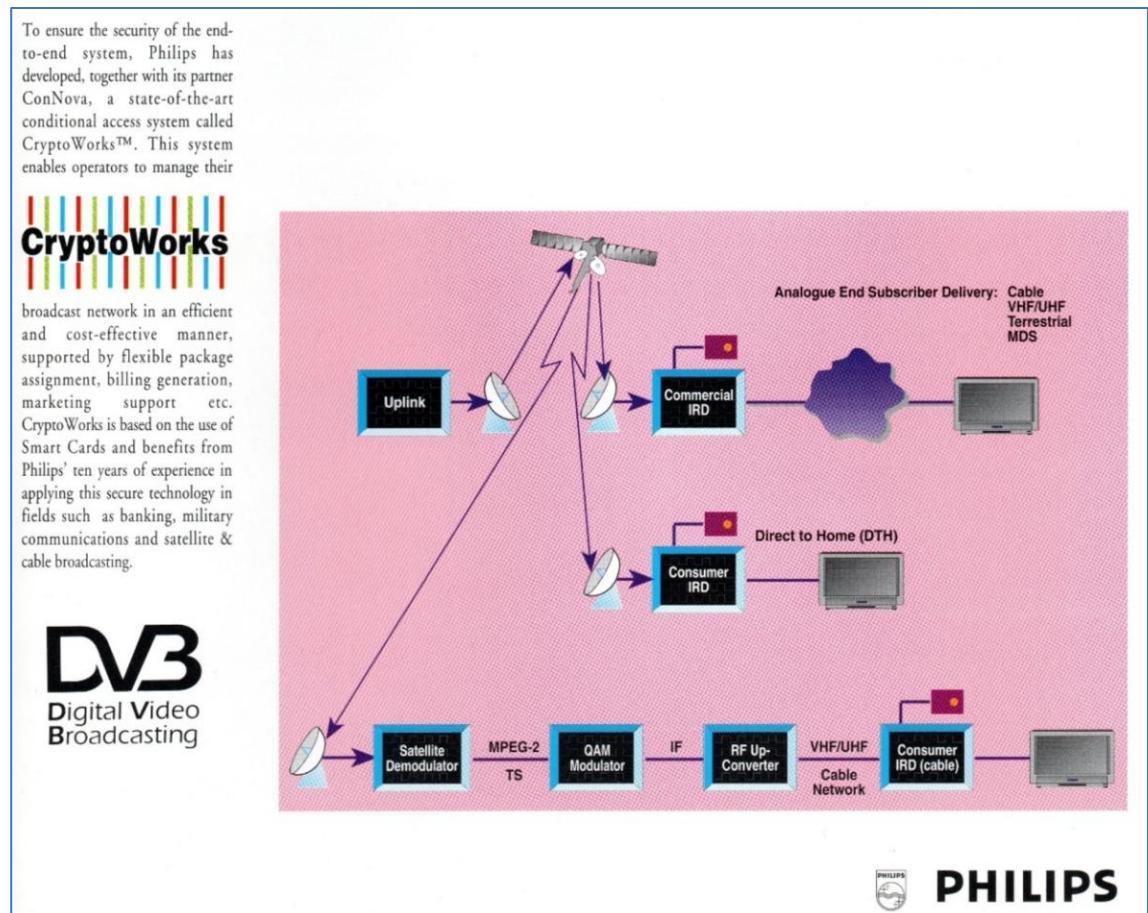


Figure 28 : Déploiement par Philips professionnel du DVB par câble et satellite

FideServices : les mises en œuvre particulières de la plateforme :

La collaboration avec Belgacom et La Poste :

Dirk Frimout, Alain Deneef, Édouard Van Heule, Olivier Delos

Le 22 décembre 1992, Philips SA [la maison mère de Philips en Belgique, représentée par Jacques Van Haren (Administrateur délégué], conjointement Philips Professional Systems [représentée par André De Smet (Administrateur délégué], signe le contrat de développement « Pudicis » avec Belgacom SA [représentée par Dirk Frimout³¹(Technology Scan Director)]. L'intention était d'offrir une gamme de « Services Universels » modernes dans la ligne des recommandations de l'UNESCO. L'annexe N°2 précise les intentions.

Il s'agit d'un contrat de développement de services informatiques à déployer sur des réseaux ; de préparation à une mise en service ; de préparation à une telle mise en service via Belgacom en collaboration avec Philips. Ces services concernaient initialement :

- Les documents authentiques et la signature numérique (Fax / Courriel / actes). Il s'agit tant les formes dites « dématérialisées » que les formes « incorporées » [expéditions matérialisées avec cachet hyperlien signé] apportées par les facteurs.
- Les services universels, en particulier la boîte aux lettres informatique personnelle sécurisée inaliénable. Il s'agissait d'un renversement de rôle ! Ce n'était plus le citoyen qui devait aller chercher les documents (diplômes / factures / extraits bancaires / certificats ...) sur les sites des Entreprises ou des Pouvoirs publics, mais c'était à eux de spontanément déposer les documents dans la boîte aux lettres du citoyen ! Plus d'attitudes léonines ! Cette boîte aux lettres pouvant aussi servir de dépôt fiable persistant pour les documents importants des citoyens. Cette boîte informatique est, en quelque sorte, sur la porte de la résidence permanente d'une personne physique ou d'une personne morale.

D'une certaine façon, ces services étaient des services universels de service public. Une large part du financement du projet Pudicis était assuré par Belgacom. De son côté, Belgacom préparait les mises en service.

Dirk Frimout avait été engagé par Belgacom après son séjour de neuf jours dans l'espace (du 23 mars au 1^{er} avril 1992) pour assurer la veille technologique et proposer à Belgacom des nouveaux produits et services. C'est dans ce contexte que je lui ai donné un cycle de formation à la sûreté de l'information (principes et mises en œuvre).

En fin 1993 la recherche et la recherche appliquée du projet Pudicis ont déjà mis au point les éléments novateurs nécessaires à des mises en place des produits et services. En particulier, les cinq modules essentiels :

1. Jean Desmet imagine un système de codage de longs textes, imprimable en évidence, compatible avec le codage Fax, redondant avec code détecteur et correcteur d'erreurs et lisible numériquement. Ce code REDA [*Reliable in Evidence Digital Array*] est mis au point près de six mois avant que Masahiro Hara développe pour Toyota ce qui allait devenir le QR code et plusieurs années avant que le QR code ne devienne public. Cette approche permettait notamment de transmettre, via les protocoles fax, des documents numériques (fichiers) et, en particulier, des hyperliens signés numériquement. Les blocs pouvaient être enchaînés en vue de pouvoir représenter de gros fichiers.



Figure 29 : “REDA” [Reliable in Evidence Digital Array]

2. Le centre de Philips TRT à Fontenay-aux-Roses achève l'appropriation pour CryptoWorks de la carte à puces pour laquelle Jean-Jacques Quisquater de PRLB avait collaboré.
3. Les TRD sont développés à Bruxelles par SOC.
4. Nous avons établi un accord de collaboration avec une société suédoise afin d'adapter leur « SealFax » aux besoins de Pudicis et des services à mettre en place.
5. Le Monitoring System est complètement développé par les équipes de SOC.

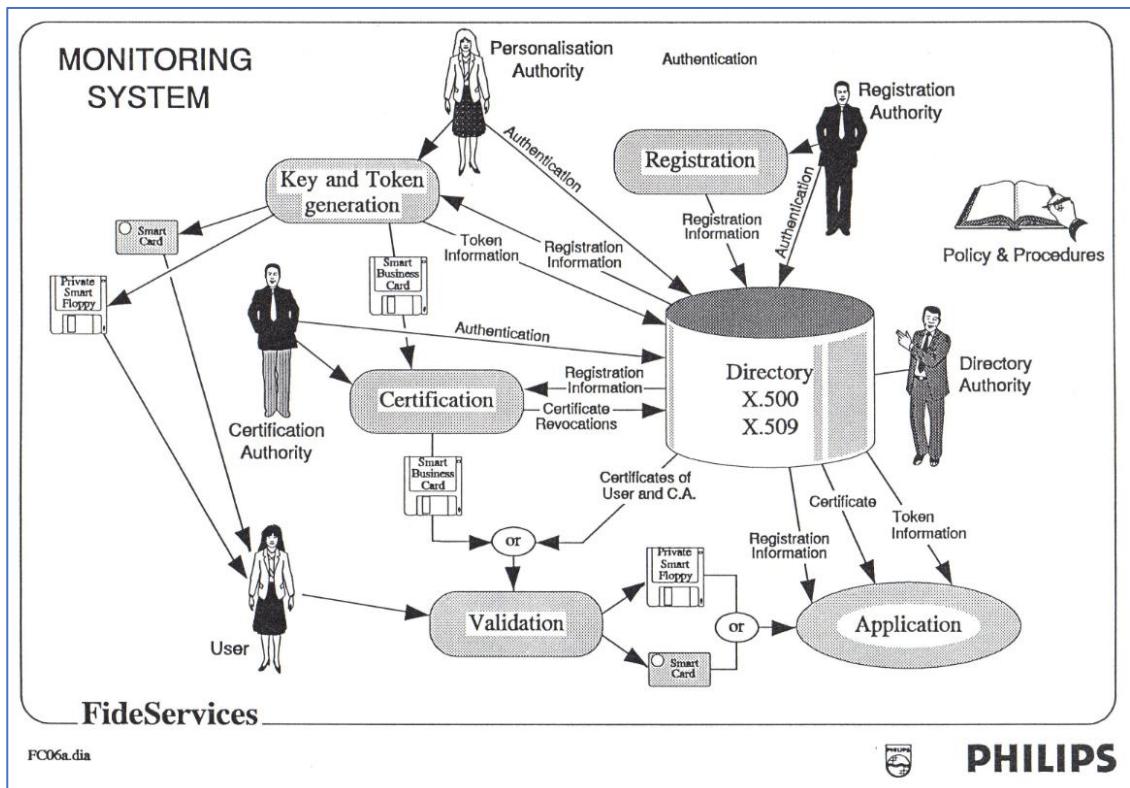


Figure 30 : FideServices : monitoring system

Il faut remarquer qu'à cette époque, les sticks USB n'existent pas et ce sont des *Floppy Disks* qui font office de mémoire modulaire portable. La sécurisation de ces porteurs s'effectue par des procédures faisant usage de clés secrètes à usage unique, actives après initialisation RSA.

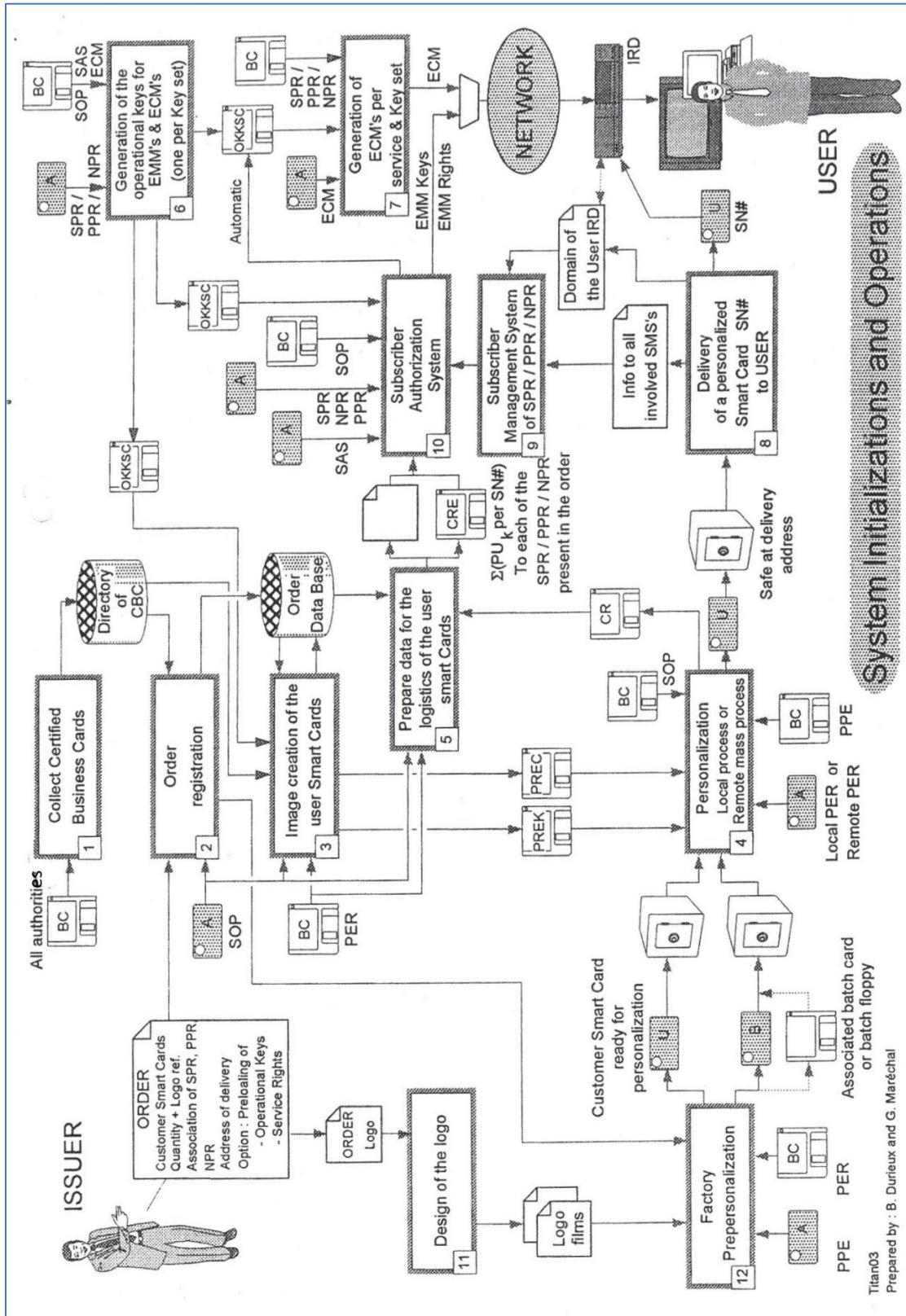


Figure 31 : FideServices : System initialization and operations

La structure générale des initialisations et des opérations est reprise ci-dessus.

Tout était prêt pour engager des plans de commercialisation :

- Pour la direction des nouveaux services, Belgacom avait engagé Alain Deneef comme directeur. Il avait quitté la direction de Canal+ Belgique.
- Comme chef de projet, Belgacom [Dirk Frimout] avait nommé un jeune ingénieur brillant et constructif, Olivier Delos, qui nous avais promis son témoignage, qui, malheureusement, n'est jamais venu (malgré plusieurs rappels. Sollicité, Dirk Frimout a lui aussi renoncé à témoigner).
- Pour le commercial, Belgacom avait nommé Édouard Van Heule [†]. Il était responsable de la mise en service de ces services dans Belgacom et des contacts de coordination avec La Poste.

Rapidement la direction de Belgacom a donné la priorité au service de fax, de courriels sécurisés [les services EDI], mais avec l'exigence d'impliquer La Poste, car elle seule avait explicitement le monopole de la lettre recommandée. La direction de La Poste avait l'intention de lancer un service de fax recommandés, mais sans garantie de contenu. Pour développer ce service, elle avait choisi de collaborer avec la firme liégeoise Gillam. Lorsque nous leur avons proposé ce service avec certification de contenu, la direction de La Poste a demandé que Philips collabore avec Gillam, ce que nous avons fait en nous partageant les rôles dans la collaboration et le consortium à créer. À cette époque la direction de La Poste était partagée entre investir pour de nouveaux services ou simplement faire le minimum en se bornant des miettes des créneaux porteurs pris par Belgacom. Souvent, les réunions de travail à La Poste étaient plus l'occasion de boire du champagne que de réellement préparer des exploitations. À l'intérieur de Belgacom aussi, il y avait des luttes d'influence entre les anciens dirigeants de la RTT [Jean-Pierre Lambotte en mars 1994] et la nouvelle vague de Belgacom [Bessel Kok (ex-patron de Swift) puis John Goossens].

En janvier 1996, les PTT-Post & PTT-Telecom et La Poste française envisagent un consortium avec La Poste belge en vue d'un service pilote pour les services d'envoi recommandé à contenu certifié via notre solution. Cette solution impliquait une imprimante mettant automatiquement les pages imprimées dans une enveloppe scellée indéchirable en mylar, qui avait une fenêtre permettant de visualiser notamment l'adresse du destinataire d'un envoi. Cette imprimante avait été développée par une firme suédoise et commercialisée sous le nom de SealFax.

Des réunions de concertation ont lieu avec eux et nous, en présence d'Édouard Van Heule (Belgacom) et de Jean-Michel Adam (Gillam).

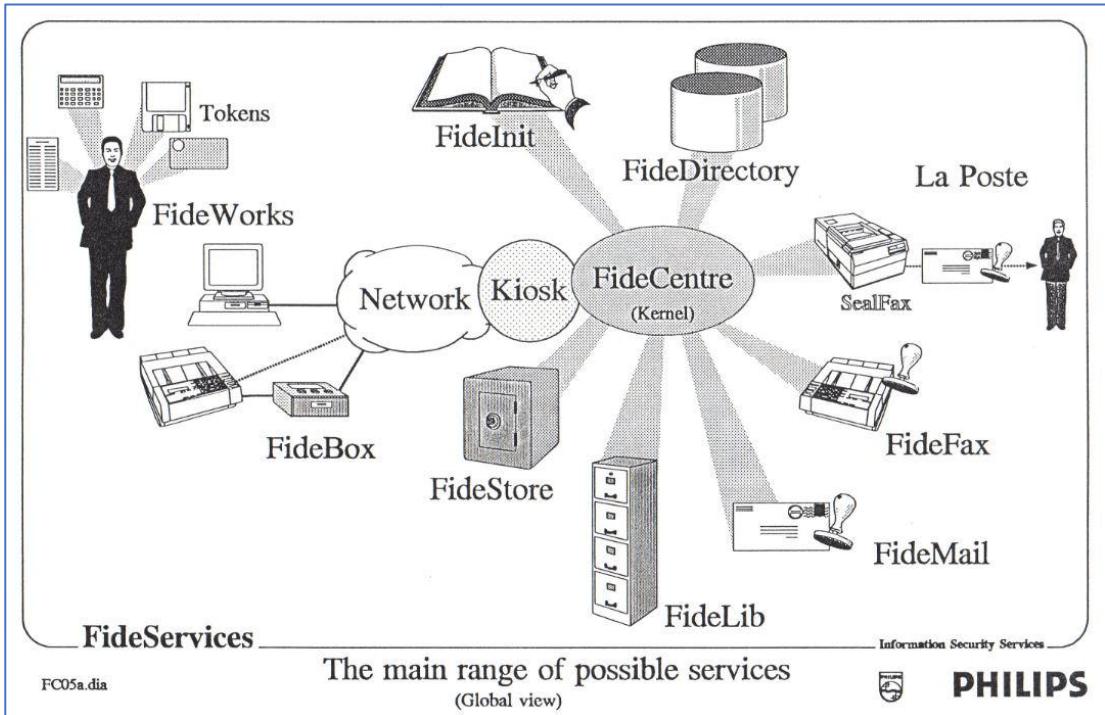


Figure 32 : Extrait de la présentation à PTT-Post & PTT-Telecom et La Poste française

Un service pilote est défini pour l'envoi recommandé à contenu certifié au moyen des Fax et des PC. Il ne couvre pas toutes les fonctions envisagées, mais a l'avantage d'être très simple à mettre en place : à l'un des guichets de La Poste, les clients Fax achètent des formulaires d'envoi comme s'ils achetaient des timbres ; les clients PC achètent un '*floppy disks*' et un bloc de codes cachés (grattage). Le service pilote est opérationnel à l'automne 1996 ainsi que les modalités d'exploitation et du Consortium à créer.



FideFax

Brussels Centre

Receipt of deposit of a registered mail

Addressee

Mr. Guy Maréchal
Philip
80 rue des deux gares
B-1070 Bruxelles

Sender

Date

Aug/09/1995 17h45
(1995 08 09 15h45 UT)

Reference

75 993 025

Control

265 078

Your reference

11050095195

Storage: 3 months

The document was
composed of 2 page(s)

Sender Fax number: 010/438 609

This receipt has been electronically signed by the Brussels FideFax Centre.

For any information : tel 0900 123 45

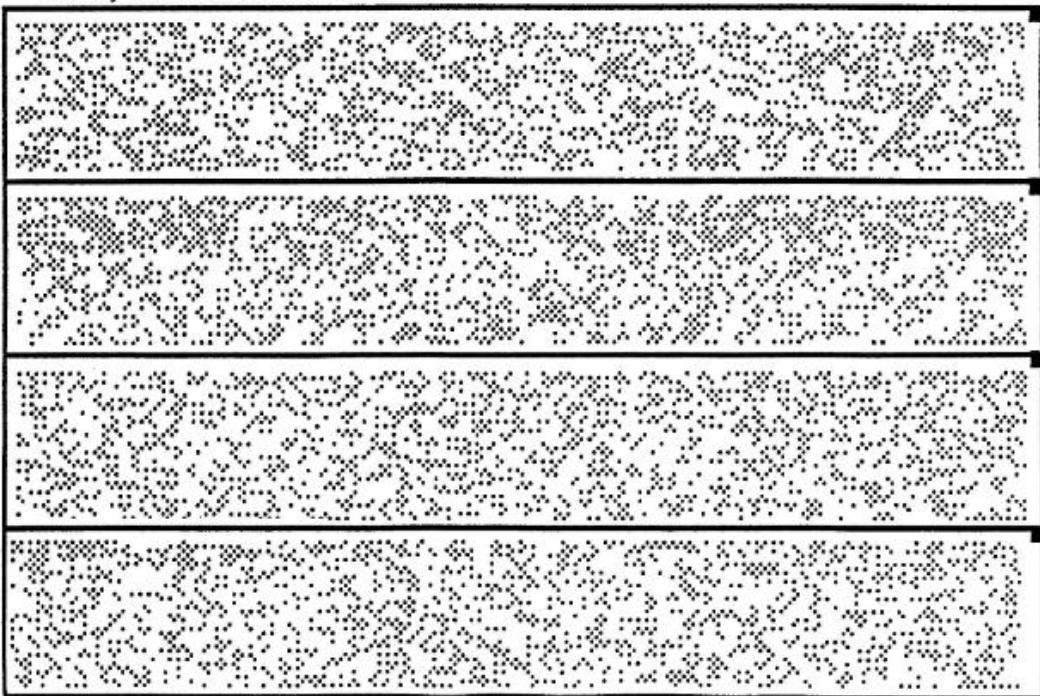


Figure 33 : FideFax : reçu d'un dépôt d'un mail enregistré

La collaboration avec Belgacom est assez chaotique malgré les contrats qui avaient été signés : en particulier les projets PUDICIS, FAXA, Testfit et Cedifact. Belgacom imposait des restrictions

étranges, notamment sur la cryptographie et rejetant l'extension des services EDI (*Electronic Data Interchange*)

En juin 1997, Édouard Van Heule nous informe que Belgacom renonce à mettre en place des services universels et se concentre exclusivement sur le déploiement du GSM et du réseau Internet pour les sites Web et les emails. Il ajoute que cette décision implique que Dirk Frimout, Alain Deneef et lui-même quitteront Belgacom rapidement ; ce qui aura lieu en 1998. La Poste débraye aussi, évidemment ! Pour éclaircir les motivations de Belgacom nous avons demandé leur témoignage. Malgré plusieurs rappels, nous n'avons pas reçu d'éclaircissement des personnes impliquées.

CryptoWorks-DVB étant en léthargie, le contrat PUDICIS se terminant et cet arrêt des possibilités de collaboration avec Belgacom et la Poste ont sonné la fin programmée de SOC.

Quelques autres projets porteurs ont aussi été abordés par SOC :

La carte d'identité du citoyen

Sur base de la carte à puce destinée à CryptoWorks-DVB, nous imaginons une carte à puce du citoyen qui sera décrite ci-après. Elle était prévue pour donner accès immédiat à sa boîte aux lettres informatique inaliénable et pérenne, ainsi qu'à la fonction de carte de sécurité sociale, de signature numérique de documents informatiques et de générateur de logo code graphique (l'équivalent du sceau incrusté dans la cire authentifiant les parchemins. Elle aurait pu contenir des informations facilitant la vie de tous les jours, comme le numéro de plaque de son véhicule et les éléments médicaux et pharmaceutiques.

Cela sera réalisé largement via les équipes du SOC, après la fermeture.

Le vote électronique

En 1996, l'État avait lancé un appel d'offres pour 'moderniser' la manière de voter via le vote électronique. Nous décidons d'y répondre. Bernard Durieux et Jean-Claude Emond imaginent une solution élégante où voter est convivial et fiable, mais, qu'en plus, l'expression du vote est reprise comme un bar-code redondant et anonyme, ce qui permet de recompter s'il y avait doute ou panne informatique. L'appel d'offres ne prévoyait pas cette faculté de recompter, ce qui a signifié que nous étions légèrement plus chers qu'un autre soumissionnaire.

Aujourd'hui, je constate que le système de vote électronique adopté en Flandres est très proche de ce que nous avions imaginé alors.

Les serveurs bancaires et entiercements

Paradoxalement, c'est dans le domaine bancaire que les TRD vont avoir un déploiement important. En effet, notre TRD avait été conçu pour pouvoir être mis comme des 'Plug-Ins' sur un des réseaux des banques. Toutes les opérations sensibles se passaient exclusivement à l'intérieur des TRD sans qu'il puisse y avoir de fuite ni via les agents de la banque (ayant accès aux équipements) où aux agents extérieurs qui tenteraient de s'introduire via les réseaux. La vente en série de nos TRD a continué largement après la fermeture du SOC : en effet, Vlatko Bencic avait reconstitué chez lui un atelier de fine mécanique et, en collaboration avec Bernard Durieux.

1.9.3.3 La mission pour le ministre de la Justice

Contrat de mission du 2 septembre 1994

En début juillet 1994, je suis contacté par Jérôme Glorie, à l'époque il était chef de cabinet du ministre de la Justice, Melchior Wathelet. Il m'annonce que le ministère souhaite recevoir des conseils pour la mise en œuvre et la modification de la loi sur la protection de la vie privée, ce

vu les développements nouveaux de l'informatique et des communications : en particulier et par ordre de priorité, le GSM ; les applications des réseaux numériques³² (en particulier l'ATM [*Asynchronous Transfer Mode*], une norme développée en tant que service public de normalisation du CCITT) comme le courrier électronique et la télévision numérique (en cours de développement via le projet DVB [Digital-Vidéo-Broadcasting] 1993).

Il me dit savoir que j'ai organisé l'archivage des documents du SHAPE peu après son installation à Casteau-Maisières et qu'à cette occasion j'ai été classifié « Tempest 5 » [le plus haut niveau de secret militaire que des civils peuvent recevoir] ; que j'ai personnellement donné des cours à Dirk Frimout sur les bases de la cryptographie pour applications civiles ; que les équipes que je dirige [le département SOC] collaborent avec le CRID de l'Université de Namur et avec le groupe de cryptographie du Centre de Recherches de Philips à Boitsfort.

Il me demande s'il serait possible que je donne à brève échéance des conseils au gouvernement dans ce domaine. Je réponds que je ne vois pas pourquoi Philips n'accepterait pas une telle mission si elle n'implique pas trop de jours. Le département juridique de Philips prépare un avant-projet de Contrat – Convention que deux administrateurs de « Philips Professional Systems », Messieurs Joseph van Vliet et Pierre Bresseel signent et envoient au ministère. Celui-ci fait savoir à Philips que cette mission s'adresse à Guy Maréchal en tant qu'expert et non en tant que membre de Philips. La mission s'exécute de mi-juillet à mi-septembre 1994. Le contrat ne sera finalement signé que le 2 septembre 1994.

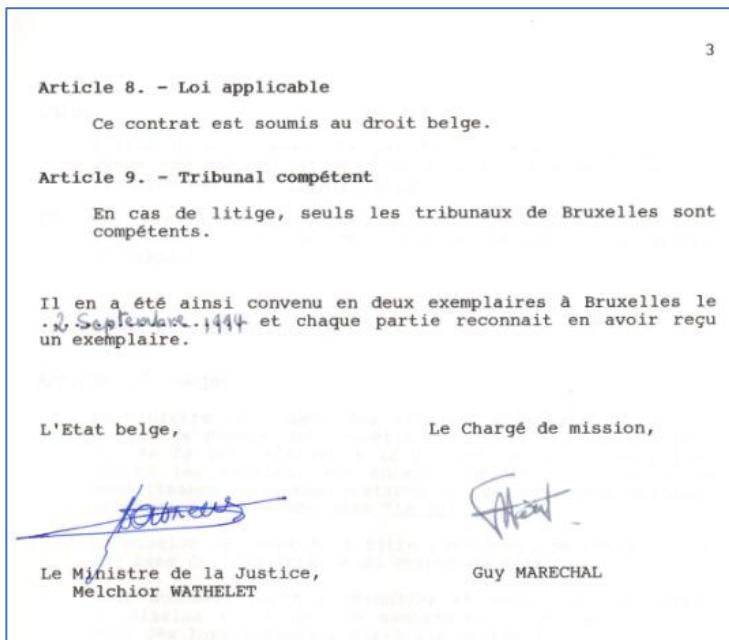


Figure 34 : « Convention du 2 septembre 1994 »

Rapport de Mission

Le ministre et son équipe étaient confrontés à des besoins nouveaux liés notamment à la mise en place du **GSM**, des **réseaux**, du **courrier électronique** et de la **télévision numérique** (en mode câble, hertzien et satellite). Il fallait s'assurer de l'écoutabilité de ces moyens de communication et des moyens de remonter à l'identité des malfrats tout en protégeant la vie privée. De plus, organiser l'écoutabilité et effectuer les écoutes implique des moyens matériels et humains que les lois existantes ne prévoyaient pas au niveau voulu. Il fallait aussi créer des organismes et des services nouveaux, en particulier des « Services Universels ».

Le rapport de mon contrat de mission (18 pages) couvre le concept d'écoutabilité en général ; il donne aussi des recommandations en vue d'aboutir à une législation générale à long terme (avec des modalités transitoires) ; il introduit les mécanismes liés à l'identité des Agents et au contrôle via une approche de « *Fair Escrow Systems* » impliquant des représentants des parties (mandataires et/ou juges) et l'usage de TRD et cartes à puce. Certains aspects des techniques de mise – en – œuvre restent confidentiels, aujourd’hui encore ! Les recommandations de mon rapport furent directement des applications des principes dégagés par le projet OASIS ! Ci-dessous quelques extraits de ce rapport :

La Loi Belge en principe protège la **confidentialité** des communications privées mais autorise ou impose l'écoute dans certaines circonstances et suivant certaines modalités. La Loi Belge ne réglemente en rien l'usage de la cryptographie (si ce n'est pour l'exportation ou l'importation (dans certains cas) suivant les règles COCOM). En conséquence, forts du principe de protection, des industriels, *Network Providers*, *Service Providers*, malfrats... pourraient être tentés d'empêcher l'Etat d'écouter dans les situations d'exception. **Le corollaire inéluctable à la loi sur "la protection..." est qu'il faut organiser le secteur des techniques de confidentialité et de preuve d'identité.**

Figure 35 : Extrait du rapport (1)

L'organisme à qui la Loi donne le contrôle des éléments clefs est l'IBPT: agrément des terminaux (contrairement à la définition de l'Union Européenne la Loi Belge ne prévoit pas la connexion indirecte sur le réseau); création ou agrément (dans certains cas passif) de cahiers de charges de services à valeur ajoutée...Cependant la gestion de la distinction entre Utilisateur et *Access System* n'est pas de leur ressort: cette distinction devient de plus en plus importante dans les techniques de mobilité, GSM par exemple (la puce personnalisée est indépendante du radiotéléphone: usage typique en location de voiture équipée du GSM, routage et facturation automatiques au locataire, où qu'il aille). Cet élément est aussi essentiel dans des domaines connexes d'intérêt commercial stratégique (signature digitale et preuves pour des documents "dématérialisés", par exemple).

Figure 36 : Extrait du rapport (2)

Aux USA la solution du Clipper-Chip n'est pas bonne et des règles de *Fair Escrow Systems* sont en train d'émerger avec une phase transitoire. De même dans l'expérience Tintan1 en Belgique il est prévu deux *Fair Escrow Systems* mais le cadre institutionnel est à créer. De même le Ministère des Finances a préparé un projet de Loi ou Arrêté Royal cessant le régime des dispenses et organisant la signature digitale (Factures et Déclaration TVA).

Figure 37 : Extrait du rapport (3)

Lors de la retouche de l'administration Clinton, dont question ci-avant, diverses exceptions ont été acceptées: en particulier INTERNET a été considéré comme d'usage scientifique et dispensé de l'écoutabilité: le lendemain, le processus de dégager PGP (Pretty Good Privacy) des contraintes de la sûreté de l'Etat Américain étaient déjà entamé. Avant fin 94 la cryptographie à applications professionnelles sera disponible en licences indépendantes des USA. L'administration Clinton prépare donc un retour à une plus grande orthodoxie.

Figure 38 : Extrait du rapport (4)

Lors de réunions de travail avec les collaborateurs du Ministre Wathelet, en particulier Jérôme Glorie, j'ai l'occasion d'évoquer que la problématique dépasse largement les aspects d'écoutabilité et qu'il faut les placer dans une approche générale. J'évoque alors les conclusions du projet OASIS (techniques et impact sur le droit). L'écoute est faible, car c'est l'urgence qui prime. Jérôme Glorie pense que cette approche conceptuelle globale serait pertinente dans le cadre de travaux en cours à la Commission européenne. Il m'annonce que je vais recevoir une demande de la Commission pour participer en octobre 1994 à une « *hearing* » à titre d'expert.

Quelques jours plus tard, je reçois cette invitation avec une courte description des développements de services s'appuyant sur le réseau Internet, en particulier le « World Wide Web ». À cette époque, je ne suis que peu informé de ce qui est en cours au CERN. Nous bénéficions des réseaux pour communiquer et pour consulter des documents : en particulier, Philips a un accord avec le centre de Frascati (dans le nord de l'Italie) pour pouvoir consulter un grand nombre de revues scientifiques.

1.9.3.4 Le « *hearing* » à la Commission européenne (octobre 1994)

Le *hearing*

Je suis invité en milieu d'après-midi. La salle de réunion est assez petite. Le représentant de la Commission est un homme élégant d'une quarantaine d'années. Il introduit la réunion en annonçant qu'à cette session il y aurait trois présentations d'experts : en quelques mots il m'introduit ainsi que les deux autres experts, puis il invite l'un des autres experts à faire sa présentation. Nous faisons remarquer que nous aimerais savoir qui sont les autres personnes présentes et si elles sont compétentes et accréditées pour connaître des informations sensibles, en particulier en cryptographie. Le représentant de la Commission nous présente en quelques mots les autres participants en précisant que nous pouvons parler librement : un autre membre de la Commission (une personne de la cinquantaine, plus petite, avec un fort accent lorsqu'il parle anglais ; il ne dira quasi rien (avec le recul je me demande s'il ne s'agissait pas de George Metakides ?) ; un délégué de l'INRIA (il ne connaît pas François Vernadat de l'INRIA avec qui j'ai travaillé au projet CIMOSA) ; un délégué américain (présenté comme lié à la sûreté de l'État : CIA) et une autre personne (présentée aussi comme américaine, sans précision de compétence).

J'écoute à peine les présentations des deux autres experts. Elles concernent certains aspects spécifiques au « World Wide Web ».

Je fais ma présentation en commençant par plaider pour que les solutions techniques soient choisies pour être indépendantes du type de réseau impliqué dans le transport des données (pas exclusivité à Arpanet/Internet). Je présente alors la solution souple que je recommande, basée sur la certification et l'authentification par les pouvoirs publics des identifiants des agents, tiers fiables, et des sites, tout en assurant l'**anonymat démocratique**, sur le caractère de « **publication** » des sites Web et sur la garantie de protection de la vie privée, y compris la confidentialité tout en assurant l'écoutabilité (avec traçabilité) dans les cas prévus par la loi lorsqu'il s'agit de « **communications privées** ». Pour illustrer la faisabilité, j'explique les deux technologies capables de réaliser aisément des systèmes conformes : l'approche RSA à clés publiques certifiées et l'entierrement (escrow) des clés dans des TRD. Dans le cadre des limites prévues par la loi, il faut toujours pouvoir remonter vers les auteurs d'actes ou propos délictueux !

Pas de questions, pas de commentaires, ni pour mon exposé ni pour celui des deux autres « experts ».

Le rapport du « hearing »

Quelques semaines plus tard, je reprends contact avec le représentant de la Commission m'étonnant de n'avoir pas reçu le rapport de cette réunion et lui demandant s'il s'attendait à recevoir un texte reprenant l'essentiel de ma présentation. Comme réponse, il m'invite à le rencontrer.

Il m'explique que la décision a été prise de ne pas mentionner mon nom dans le rapport. Il précise que, si l'on adoptait l'approche que je préconisais, alors il ne serait pas possible aux services secrets d'espionner à grande échelle sans laisser de traces ; ni d'effectuer des impersonnalisation sans laisser de traces. Il ajoute que c'est de toute façon trop tard ; que les changements techniques ne peuvent pas imposer des changements des lois ni imposer des lois identiques dans les différents pays. Je fais remarquer que les lois générales sur la protection de la vie privée existent ainsi que les lois relatives à la responsabilité de publier. Ce sont uniquement les modalités, les décrets d'applications qui doivent être exprimés pour tenir compte des spécificités des moyens de l'informatique et des communications.

Je lui rappelle que, pour les normes techniques du GSM et pour celles en préparation pour le DVB [la télévision numérique (câble, satellite et terrestre) européenne], l'usage de la cryptographie a été organisé indépendamment des lois malgré les craintes (presque hysteriques) des services secrets américains de voir des hors-la-loi se servir des réseaux de télédistribution. Je ne lui dévoile évidemment pas quelles solutions techniques ont été choisies.

Il me dit que c'est inutile d'insister et m'encourage à tenter de convaincre les pouvoirs publics de mon pays.

La direction générale de Philips et les services du ministère de la Justice décident de ne pas faire de vagues.

Mon équipe SOC et moi-même nous concentrons alors sur les actions vis-à-vis de la Belgique : tenter de convaincre de notre vision et de ses conséquences pratiques techniques et légales. Comme expliqué par ailleurs, nous ne réussirons que pour la Carte d'Identité et, marginalement, pour la signature numérique et pour le protocole <https://...>. En fin 1994, ce protocole sécurisé était déjà actif sur Netscape ! À cette époque, il aurait dû être imposé pour tous les sites Web et sous contrôle des États ! De même pour son équivalent d'assurance de l'identité des internautes. Mais ce ne fut évidemment pas le cas et nous en payons aujourd'hui les graves conséquences.

Alexandria

En 2019, à sa sortie, je lis le livre de Quentin Jardon « Alexandria »³³. Quentin est journaliste. Ce livre suit l'enquête de Quentin sur les débuts du Web et, en particulier, il y tente d'éclaircir la place de Robert Cailliau et de son hypothétique rapport « Alexandria ». Il est indiscutable que c'est Tim Bernes-Lee qui a conçu au CERN le système d'informations partagées mondialement sur les réseaux, système qui deviendra le World Wide Web. Mais, c'est la collaboration de Robert Cailliau avec Tim qui fondera le Web : en quelque sorte, comme le dit Quentin Jardon, ils sont les co-fondateurs du Web. Quentin y rapporte les résultats de ses enquêtes et ne peut que constater qu'il subsiste des parts d'ombre. Le rapport « Alexandria » a-t-il vraiment existé ? Comment est-il possible que la Commission européenne ait pu laisser s'échapper la gestion exclusive du Web vers les USA ; n'ait exigé aucune contrainte ; aucun droit de regard ou même de veto au profit de l'INRIA ... ; n'ait pas exigé que les protocoles soient modifiés pour que l'on puisse utiliser d'autres réseaux de transport qu'Internet, comme l'ATM ; comment l'INRIA n'a-t-elle pas revendiqué que le réseau des « Cyclades » puisse aussi être utilisé ? Pourquoi le CERN a-t-il dû rétrocéder des sommes importantes au MIT ?

Quentin identifie que ce basculement incompréhensible a lieu à l'automne 1994. Je ne puis m'empêcher de faire le rapprochement et d'imaginer que, sans m'en rendre compte, lors de mon *hearing*, j'avais perturbé les plans suspectés de Michael Dertouzos et de George Metakides. Il ne fallait pas que l'on sache qu'il était encore temps et aisément d'adopter des technologies, des protocoles et leur mise en place, capables de donner toute liberté aux Agents respectueux des lois, tout en donnant aux pouvoirs publics la capacité de remonter aux personnes suspectées d'enfreindre les lois et de tracer les infractions !

1.9.3.5 L'impact sur le Droit

À cette époque nous avions initialisé des contacts avec le **CRID**. Remarquablement créé en 1979 par Jacques Berleur et Yves Pouillet³⁴, le CRID [Centre de Recherches Informatique et Droit³⁵] des Facultés universitaires Notre-Dame de la Paix à Namur (Belgique) a pour objectif de susciter une réflexion universitaire et pluridisciplinaire sur le droit et l'économie des Technologies de l'information et de la communication. Ultérieurement, pour rendre compte de l'extension de son champ de recherche, le CRID a modifié sa dénomination en CRIDS [Centre de Recherches Information, Droit et Société]. À cette époque, mon équipe SOC avait d'ailleurs commandé au CRID plusieurs recherches ciblées.

Il est devenu clair que les lois en cours ne donnaient aucun statut aux documents informatiques, ni aux services rendus par l'informatique, ni aux sites Web (bien qu'il s'agisse de publications). Il était évident que la création d'une organisation telle que CRID s'imposait !

Après ma mission auprès du ministre de la Justice et mon *hearing* à la Commission européenne, je me suis dit qu'il fallait cesser de modifier les lois **en réaction** aux problèmes. Mais qu'il était fondamental d'être **proactif** : il fallait élaborer un ensemble de lois cadres organisant la place de l'informatique dans la société et donner statut légal aux formes informatiques et aux Agents informatiques équivalents aux formes physiques et aux Agents actuels ! La direction de Philips Belgique, surtout Jacques Van Haren (CEO de Philips Belgique) et André De Smedt (CEO de Philips Professional Systems) ont appuyé la suggestion portée par mon équipe de tenter de mettre en place un projet à la fois juridique, technique et politique, de préférence au niveau européen, ou à portée limitée à la Belgique (avec subsides de l'IRSIA et du FNRS) qui établisse un avant-projet de cadre juridique et un projet pilote de réalisation précompétitive des éléments techniques essentiels (cartes à puce d'identité d'Agents // services universels // ...) de mise en œuvre opérationnelle d'une société de l'information et des médias. Un contact a alors été établi avec le cabinet du Premier Ministre. Nous y avons retrouvé Jérôme Glorie, qui venait du cabinet du ministre de la Justice. Il nous a encouragés de prendre l'initiative de contacter des partenaires clés pour lancer ce projet de recherche ; nous étions déjà en contact avec Belgacom, La Poste et Isabel. Nous nous sommes alors adressés à Jacques Berleur (alors Recteur de l'Université de Namur) pour obtenir son soutien et celui du CRID dans la défense et la mise en œuvre de cette recherche proactive. Paradoxalement Jacques Berleur s'est radicalement opposé à cette approche, plaidant pour une approche progressive, réactive en fonction des besoins et sans implication technique qui pourrait favoriser un fournisseur particulier et qui en imposerait au juridique sous prétexte de cohérence technique. Il a même ajouté que c'était dangereux de vouloir représenter les lois par des produits, services et modèles informatiques, car l'on risquait de mettre en évidence des incohérences et de déstabiliser le droit ou, pire encore, donner des contraintes aux changements des lois. C'est aux Assemblées représentatives, au 'politique' et non au 'technique' d'élaborer les lois !

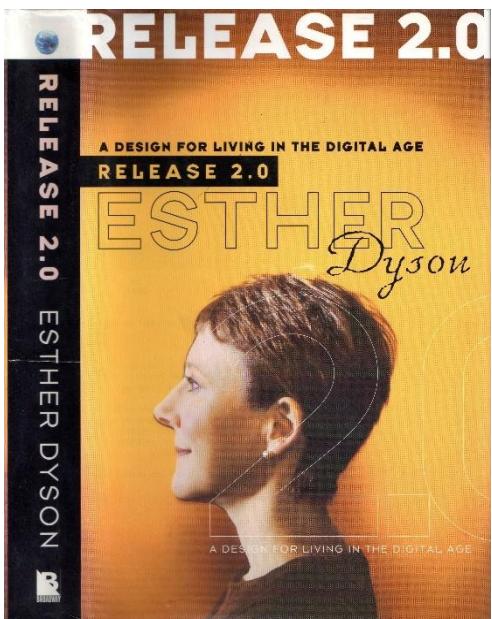
En fait notre projet était une utopie : nombreux étaient ceux qui voulaient la plus grande liberté sur les réseaux ; le problème aurait dû être réglé au niveau mondial par l'ONU et les politiques n'en voulaient pas (surtout pas les USA qui n'avaient quasi pas de lois pour la protection de la vie privée des gens et qui, aujourd'hui encore, refusent la notion de « Carte d'Identité »).

En début 1996, le « Conseil de l'Europe » organise une audition relative à l'impact des nouvelles technologies de la communication sur les « Droits de l'homme et les valeurs démocratiques ». Sur

base de l'analyse précitée et avec l'appui de l'ASBL TITAN, je prépare une contribution qui est retenue par le « Conseil de l'Europe » et je la présente en début mai 1996. Cette contribution de 13 pages, complétée par des annexes, est encore pertinente aujourd'hui. L'annexe rédigée par Philippe GÉRARD du CRID (datée du 1^{er} mars 1996) montre à suffisance que la lasagne institutionnelle belge rend quasi impossible de résoudre correctement la problématique et que le pays n'est pas prêt pour un cadre réglementaire cohérent. Cet aspect a dû jouer un rôle dans la froideur de Jacques Berleur pour l'approche que nous y défendions. Ces 13 pages du rapport sont présentées en Annexe 1.

En 1997, Esther Dyson, qui était alors une des conseillers du président Bill Clinton, a publié un livre qui a fait date : « **Release 2.0** » (*A design for living in the digital age*). Avec un arrogance décomplexée, elle y plaide pour que, pour ce qui concerne les réseaux informatiques, le monde entier adopte les lois américaines qu'elle présente comme convenant au monde entier.

Si les internautes acceptaient de se conformer aux lois américaines, les États devraient les accepter ! Elle enfonce le clou en faisant remarquer que ce ne serait que normal puisque « *Après tout, les États-Unis gèrent encore plus de la moitié du trafic Internet mondial, prennent en charge plus de la moitié de ses serveurs et hébergent plus de la moitié de ses utilisateurs.* ».



[Page 104] « How the Net should be governed? »

« As the old structures lose sway, how should cyberspace be governed, not only from within but between Net communities? [...] Of course, the popular assumption is that the solution to these problems lies in more government: some sort of central world government, which would manage all these issues nearly and fairly [...] »

« Well! That didn't happen in the terrestrial world and there's no reason it needs to happen on the Net. An alternative route – let's call it a path of least resistance – would be for everyone on the Net to agree to comply with U.S. laws.

After all, the United States still handles more than half the world's Internet traffic, supports more than half its servers, and is the home of more than half its users. »

Figure 39 : How the Net should be governed by Esther Dyson

La voie avait été préparée dès 1994 aux USA lorsqu'Al Gore a établi le NIAC [le « Conseil consultatif national sur les infrastructures critiques » (*The President's National Infrastructure Advisory Council*)]. Ce Conseil comprend des dirigeants du secteur privé et des gouvernements étatiques et locaux qui conseillent la Maison Blanche sur la manière de réduire les risques physiques et cybernétiques et d'améliorer la sécurité et la résilience des secteurs d'infrastructures critiques du pays. Esther Dyson y était l'un des membres très écoutée. Le NIAC a notamment recommandé de contribuer au financement des travaux du W3C et ceux de Nicolas Negroponte au MIT qui, en 1995, publierà « **being digital** », dont le sous-titre est « *The road map for survival on the information superhighway* ».

La version française de ce livre porte le nom de « L'homme numérique ». Elle incorpore le schéma populaire de l'Internet (voir la figure) que n'a pas la version originale anglaise.

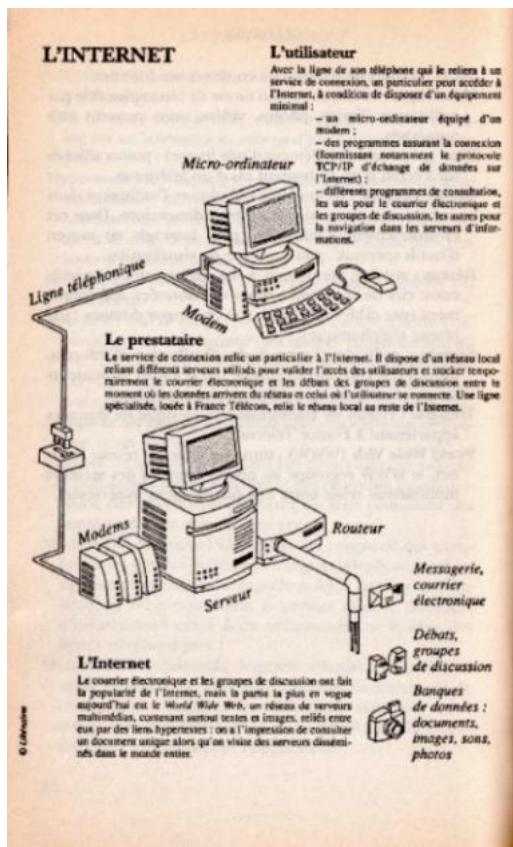
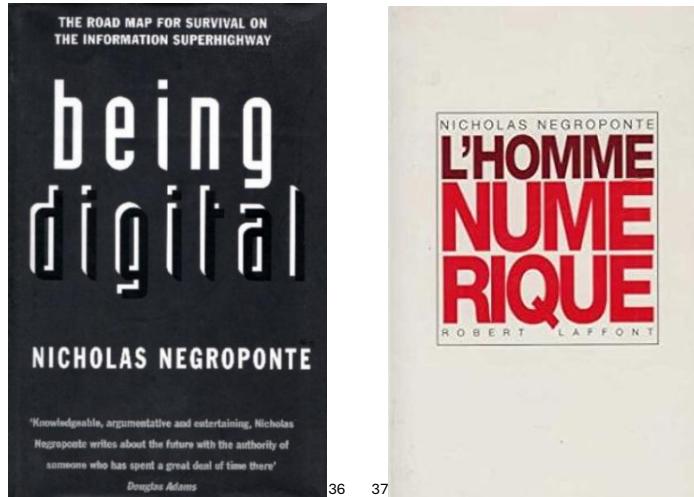


Figure 40 “Being digital by Nicholas Negroponte

Esther Dyson ne s'était pas trompée : l'Europe n'a plus son mot à dire ! C'est le W3C [basé au MIT, à Boston] qui, statutairement, fixe les aspects techniques du Web et, de facto, ce sont les lois américaines qui ont servi de base au monde entier pour réglementer le Web jusqu'aujourd'hui et ce de manière extrêmement laxiste ! Il faudra attendre le milieu de la décennie 2010 pour que l'Union européenne ait un sursaut avec le RGPD [Règlement Général sur la Protection des Données] qui s'imposera progressivement au monde entier. Mais ce règlement est loin d'être suffisant pour couvrir la vision des pays européens.

En Belgique, la « Carte d’Identité sociale » [dite « Carte SIS »] a été créée en 1995, dans un cadre juridique spécifique, comme porteur de données, mais sans signature digitale. Puis il a fallu attendre mai 1997 pour qu’une « Note au Conseil des Ministres » tente de couvrir la problématique dans son ensemble. Cette Note a été approuvée et, pendant de nombreuses années, a servi de base aux retouches du cadre juridique.

Cette note ne couvre que la signature digitale, mais c'est une avancée majeure pour la Belgique.

Le texte complet de cette note est disponible en Annexe 2.

Le Ministre de la Justice [Stefaan De Clerck à l'époque] tente de reporter sur d'autres la charge de régler les problèmes et se limite à un simple plaidoyer pour reconnaître la signature numérique de documents, reconnaître des « Autorités de Certification » et autres retouches ancillaires et emplâtres. Les deux questions finales (pages 15 et suivantes) sont les bonnes ; mais les réponses y sont incohérentes par rapport aux arguments exprimés : ne pas faire de vagues !

Il faut comparer ce texte à celui présenté un an plus tôt par TITAN lors de sa contribution au Conseil de l'Europe qui a été détaillé ci-devant (Section 9.3) et aussi disponible via QR-Code ! La Note au Conseil des Ministres évite soigneusement de rappeler que :

- C'est aux Pouvoirs Publics qu'incombe le SP [**Service Public**] d'AC [**Autorité de Certification**] primaire, clé de voûte des AC de rôle public ou de rôle privé !
- C'est aux Pouvoirs Publics qu'incombe la responsabilité d'enregistrer l'existence de PP [**Personnes Physiques**] et de leur donner les moyens de prouver qui ils sont ! Pour ce, la solution évidente passe par l'ajout, dès que possible économiquement et techniquement, d'une puce sur la carte d'identité, puce qui porterait la paire de clés cryptographiques et les certificats émis par l'AC de Pouvoir Public concerné (ministère de l'Intérieur ...) ;
- C'est aux Pouvoirs Publics qu'incombe la responsabilité d'enregistrer l'existence de PM [**Personnes Morales**] impliquant des responsabilités vis-vis de Tiers, et de leur donner aux PP [Personnes Physiques] les moyens d'être impliquées dans ces PM [Personnes morales] dans le cadre de rôles, droits, pouvoirs et devoirs. Pour garantir cette implication, la solution évidente passe par l'ajout dans la puce de leur carte d'identité, dès que possible économiquement et techniquement, des paramètres exprimant ces rôles, droits, pouvoirs et devoirs ; la puce porterait aussi la paire de clés associée aux PM concernées par cette PP et les certificats émis par les AC [Autorités de Certifications] des Pouvoirs Publics (ou les AC mandatées par les Pouvoirs Publics) y relatifs. Il s'agit d'assurer la preuve d'identité des PM concernées ;
- Cette approche permet à des Personnes physiques de **signer** des Documents au « nom de » ou en « vue de » PMs dans le cadre de leurs rôles, droits, pouvoirs, devoirs. Ce n'est pas la PM qui signe, c'est la PP qui signe avec contexte. Le document signé est autoprobant, car il incorpore les preuves de :
 - L'identité de la (des) PP signataires ;
 - L'identité de la (des) PM impliquées ;
 - L'identité du (ou des) SP impliqués ;
 - Des rôles/droits/pouvoirs/devoirs activés liant la (ou les) PP signataires avec les PM et les SP impliqués
 - L'identité des Autorités de Certification intervenues.
- Qu'il y a d'autres Agents que les Personnes Physique ou les Personnes Morales : les artefacts performatifs ; les personnages ; les avatars ...

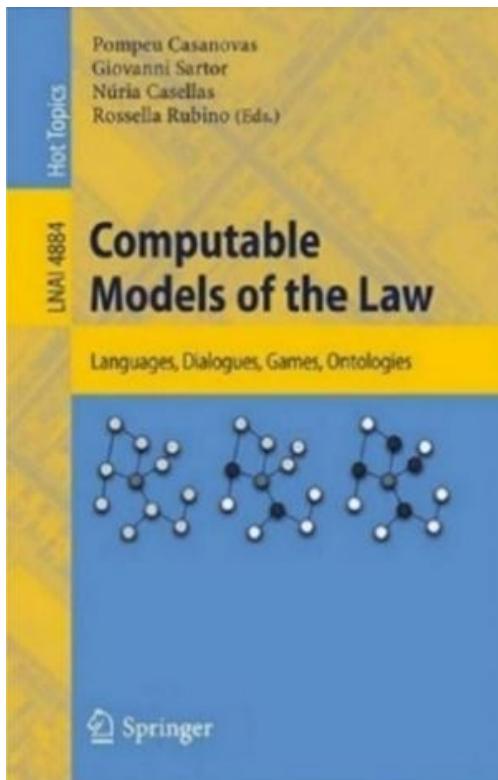
Sans doute, aujourd’hui, nous sommes mieux à même d’interpréter les timidités et les errements du passé ; sans doute aussi notre équipe n’a-t-elle pas été assez persuasive et/ou claire ! Cette « Note », c’était mieux que rien, mais quel gâchis et que de temps perdu !

Il faut noter que, dès 1995, de nombreuses Universités sont allées beaucoup plus loin ! Elles ont effectué des recherches sur la représentation du Droit et l’exercice de la Justice par l’informatique, essentiellement via l’approche sémantique. Il faut citer en particulier l’Université de Bologne [les professeurs Rossella Rubino³⁸ puis Fabio Vitali³⁹] dans le département CIRSFID. Ces travaux continuent actuellement via les normes du Web sémantique.

Cette représentation du droit par l’informatique représenterait une avancée significative dans l’application des lois [*Nul n’est censé ignorer la Loi*] ; mais aussi à leur activation [*quelle loi s’applique dans le cas présent ? Quelle était la loi applicable au moment des faits concernés ?*]. De plus, il faut remarquer que les lois sont souvent très procédurales, imposant des protocoles très stricts : en quelque sorte, bien des domaines du droit s’expriment suivant des protocoles à machines à états finis que l’on peut programmer simplement comme un enchaînement de formulaires. L’approche sémantique implique la cohérence des lois et ouvre la porte à la guidance dans l’exécution correcte des procédures et l’émission de rappels automatiques.

Le CRID va rester très actif dans le domaine, essentiellement dans l’analyse des lois et peu dans la recherche de pistes conceptuelles pour gérer le monde de l’informatique et des réseaux. Ces analyses fouillées vont culminer avec le congrès des 15 et 16 juin 2001, dont les annales ont fait l’objet d’une synthèse dans le Cahier N°22⁴⁰ du CRID.

Figure 41 : Computable Models of the Law



GOUVERNANCE DE LA SOCIÉTÉ DE L'INFORMATION

J. Berleur
E. Brousseau
M. Coipel
R. Delmas
T. Dedeurwaerdere
T. Ewbank de Wespain
I. Falque-Pierrotin
L. Hennuy
C. Lazaro
M. Maesschalck
Y. Poulet
R. Queck



BRUYLANT

PRESSES
UNIVERSITAIRES
DE NAMUR

Rassemblant des membres des Facultés de Droit, des Sciences Économiques et Sociales et de l'Institut d'Informatique, le Centre de Recherches Informatique et Droit des Facultés Universitaires Notre-Dame de la Paix à Namur constitue une expérience originale et unique en Belgique de recherche interdisciplinaire Droit - Informatique - Economie.

Le C.R.I.D. se donne pour objectif de faire progresser la réflexion dans deux domaines :

1. "Le droit de l'informatique" (au sens large), d'une part, ou, de façon plus précise, l'ensemble des questions juridiques et institutionnelles suscitées par les nouveaux moyens de traitement et de transport de l'information (informatique, télématique, réseaux) ;
2. "L'information juridique", d'autre part, entendant par là les problèmes liés au traitement automatique de l'information juridique.

Dans les deux domaines, le C.R.I.D. est attentif à la dimension politique, économique, sociale voire culturelle des choix législatifs ou réglementaires opérés.

Déjà parus dans la collection "Les cahiers du C.R.I.D." :

- n° 10 Vers une société de l'information
- n° 11 Le droit d'auteur, du logiciel au multimédia
- n° 12 Internet face au droit
- n° 13 Vie privée / données
- n° 14 La sécurité informatique, entre technique et droit
- n° 15 Service universel, concurrence et télécommunications
- n° 16 Droit des technologies de l'information
- n° 17 Commerce électronique
- n° 18 Le droit d'auteur / copyright
- n° 19 Le commerce électronique européen sur les rails ?
- n° 20 Variations sur le droit de la société de l'information
- n° 21 Le règlement extrajudiciaire des litiges relatifs aux noms de domaine



www.bruylant.be

Conception graphique : Agence de communication

Figure 42 : Gouvernance de la société de l'information

Dans cette publication, Jacques Berleur, Christophe Lazaro et Robert Queck reflètent bien les préoccupations de l'époque, les pistes pour placer l'autorégulation et la corégulation dans la régulation. Le besoin de services publics est mentionné, mais sans lui en donner de contenu. Une belle analyse du droit et des challenges ! Peu de solutions à promouvoir. Il faut aussi noter qu'il n'y avait aucun industriel dans la liste des congressistes !

La problématique de l'assurance de l'identité et de l'accès à l'identité des Agents n'est même pas mentionnée !

Philips a alors renoncé à tenter de réunir les organisations belges ou internationales à impliquer dans un tel projet proactif. Philips s'est alors concentré sur CryptoWorks et sur la collaboration de FideServices avec Isabel, Belgacom et La Poste (voir les projets pilotes signalés dans la Note).

Aujourd'hui

Aujourd'hui les Pouvoirs Publics en Belgique, en Europe et, dans une moindre mesure, dans le monde, ont pris conscience qu'il fallait assurer que, conceptuellement, les lois gouvernent les choses mutatis mutandis de la même façon via les réseaux et en évidence.

En Belgique, l'avancée de la « Carte d'Identité » est l'une des meilleures au monde. Elle couvre correctement ce qui est lié à l'identité de la Personne Physique concernée et aux droits que cette PP a vis-à-vis de ses relations avec les services rendus ou garantis par les pouvoirs publics, tel que pour les soins de santé et l'accès aux documents administratifs légaux ou liés à des services publics (l'eau, par exemple). Indirectement la carte d'identité belge a conduit à une évolution majeure du statut légal et économique des smartphones. En effet, en Belgique, maintenant, il est obligatoire d'associer sa carte d'identité avec la carte SIM de son smartphone et il n'y a donc plus de smartphones anonymes ! Indirectement, cela a rendu possible que les applications bancaires et certaines transactions économiques puissent être exécutées via le smartphone sans besoin de carte de banque ou carte de crédit. Sur les réseaux il existe des authentifications d'identité à deux passes qui assurent qu'une personne physique est bien la titulaire d'une adresse de courriel ou d'un

compte auprès d'un service ; puis qui assurent que ce titulaire est bien légalement la personne physique connue par les services publics belges. Pour Google je puis assurer que non seulement je suis bien le titulaire de guy.noel.marechal@gmail.com utilisable tant comme identifiant pour les services de Google et comme adresse de courriel sur les services de Gmail ; mais aussi, via une seconde passe, comme la personne physique bien connue sous le nom de Guy-Noël Maréchal, domiciliée à Ixelles et née le 25 décembre 1937. C'est en quelque sorte la puce de la carte SIM qui a reçu accréditation au départ de la carte d'identité.

Il y a même des projets en cours visant à étudier la possibilité qu'à l'avenir les smartphones puissent faire office de carte d'identité avec la puissance de calcul embarquée capable de faire des services performants, comme des vérifications biométriques d'identité.

Malheureusement, à ce jour, rien n'a été fait pour mettre en œuvre des solutions liées aux Personnes Morales et aux Services Publics. Cette incurie dépasse à tel point l'imagination qu'il vaut mieux se taire. Le bricolage actuel des lois et des mises en œuvre est à ce point mauvais qu'il eut mieux valu ne rien faire ! Mais, comme il y avait obligation de faire, les solutions adoptées ont été celles dénoncées en 1995 : des solutions ponctuelles **réactives** souvent redondantes et incohérentes entre elles.

Jean
Smeesters
(Signature)

Signature numérique
de Jean Smeesters
(Signature)
Date : 2023.09.15
12:09:58 +02'00'

Néanmoins, malgré l'incurie du cadre légal belge sur les PP et les SP, la carte d'identité belge a été intégrée dans les protocoles aptes à effectuer la signature de documents représentés en PDF. C'est une solution hybride, pragmatique, sans explicitation des rôles et PM impliquées.

Mise en œuvre pour les Cartes d'Identité et Passeports

La qualité et la beauté de la solution belge actuelle méritent d'être décrites et expliquées.

Actuellement [2023], en Belgique, c'est la date de naissance qui sert de codage de l'identification ultime d'une personne physique ; et c'est la Carte d'Identité de cette personne qui sert d'artefact fiable porteur de la clé privée de cette personne et le certificat de l'autorité assurant la fiabilité de sa clé publique. La Carte d'Identité belge est la clé de voûte de l'assurance d'identité (au civil, mais aussi pour le GSM, les Smartphones, les laptops, les cartes bancaires ; et l'application ItsMe ...) et des services publics (la sécurité sociale, les prescriptions pharmaceutiques ...).

En Belgique, le numéro d'identité nationale est basé la date de naissance déclarée, complétée par la référence au Registre de l'État Civil concerné. Cela donne 39.08.14-322.85 pour quelqu'un né le 14 août 1939 et repris sur le registre N°322.

La puce cryptographique utilise l'approche asymétrique et les certificats émis par les pouvoirs publics.

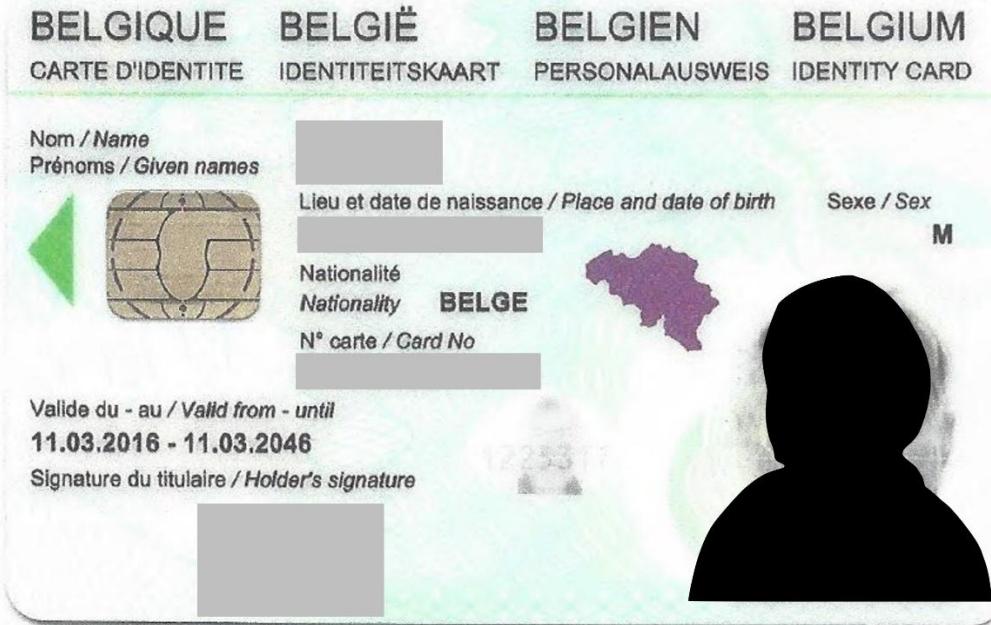


Figure 43 : Mise en œuvre pour les Cartes d'Identité

Il faut remarquer que, actuellement, les deux clés sont générées par les Pouvoirs Publics. Il est néanmoins probable (et souhaitable) que cette mise en œuvre actuelle se fasse de telle sorte que les Pouvoirs Publics n'aient aucun accès au processus de génération des paires de clés (en les générant dans la carte à puce faisant office de TRD). Mais, si le processus permettait au Pouvoir Public de connaître les deux clés, dans ce cas, ils pourraient faire de l'impersonnalisation [faire semblant d'être moi] ou accéder à mes secrets. Le protocole auquel le citoyen est confronté ne lève pas le soupçon !

1.9.4 La « Business Opportunity Platform » [BOP]

Jacques van Haren, puis, à son décès prématuré, Jean Van Lierde, le remplaçant comme Président de Philips Belgique, étudient les façons de redynamiser Philips dans les organisations locales.

Trois journées de réflexion sont organisées dans un hôtel près de l'aéroport de Zaventem. Il en sort que les Organisations décentralisées de Philips devraient créer des Cellules de gestion de projets pluridisciplinaires dans les domaines où Philips est compétent :

Télévision / Téléphonie / Médical / Informatique dédiée / Réseaux câblés / ...

En Belgique, cette initiative prend le nom de « Business Opportunity Platform ». À cette fin, trois quatre personnes sont détachées à temps partiel. Personnellement, j'y suis à temps plein ! En effet, ayant été malade, c'est Guy van Hooveld qui est devenu le chef du SOC. Il aura d'ailleurs la charge de le fermer ! Il parviendra à négocier avec plusieurs organisations la reprise du personnel (avec leur ancienneté) et de l'expertise : notamment Isabel, ATOS et l'association belge des Banques.

L'objectif est triple :

- Repérer des Appels d'Offres pluridisciplinaires et d'y répondre, seul ou en partenariat avec d'autres Entreprises expertes dans les domaines où Philips ne peut faire seul.
- Entrer ou créer des partenariats ou des consortiums pour couvrir des secteurs porteurs potentiels, en particulier l'aménagement des villes connectées et servantes.
- Apporter des contributions scientifiques liées à la mise en œuvre de percées techniques. Au début des années 1990, l'Académie des Sciences envisageait de créer la Classe « Technologie et

Société ». À cette fin, elle est entrée en contact avec des responsables d'universités, d'entreprises et d'organisations actives dans les techniques de pointe industrielles et techniques. Dans ce contexte, Jacques Van Haren fut approché, à la fois comme président de la FABI [F.A.B.I. (Féd. Royale d'Associations Belges d'Ingénieurs Civils et d'Ingénieurs Agronomes)] et comme président de Philips Belgique. Grâce à lui, je deviens membre du CAPAS [Comité de l'Académie pour l'Application des Sciences] et liaison avec le CAWET [Comité van de Academie voor Wetenschappen en Techniek]. Conjointement ces deux Comités ont pour nom « BACAS » [Belgian Academy Council of Applied Science]. Dans ce contexte de l'Académie, j'ai été impliqué activement dans trois groupes de travail : « La déontologie de la profession de l'ingénieur civil et de l'ingénieur agronome », « La Société de l'Information » et le « Technology Assessment Observatory ». Les travaux du premier groupe se termineront par une conférence, journée d'étude. Les travaux du premier groupe se termineront par un colloque tenu le 27 novembre 1997 (dont Philips sera sponsor de la plaquette des Actes du Colloque) ; les travaux du second groupe se termineront par une conférence, journée d'étude (le 17 février 2000) dont j'ai assuré l'introduction générale, la section sur la « Sécurité de l'information » et la publication d'un CD-Rom reprenant les interventions et les conclusions. Pour les travaux du troisième groupe, sur le « Technology Assessment », j'ai été le rédacteur de la Charte de la « TAO » avec référence et nuance détaillée au « Principe de Précaution ». Malheureusement, le successeur du Professeur Nicolas Dehouze à la tête du CAPAS, Pierre Klees, est entré en conflit violent avec Hervé Hasquin, le nouveau Secrétaire Perpétuel des Académies. Dégoûté par l'attitude de Pierre Klees, j'ai remis ma démission du CAPAS.

À cette initiative, il faut attacher les projets des InfoCities, d'Hôpitaux, d'UniMédia, d'Archives. La plus importante initiative fut la collaboration avec l'ALE à Liège, qui prit la forme d'un Consortium : Philips se retira rapidement de ce Consortium. Quelques détails sur cette collaboration sont présents dans la contribution de TITAN.

Très rapidement, Philips *Corporate* donnera l'ordre d'arrêter tous ces types d'activités comme freinant les possibilités de valorisation indépendante de chaque secteur de Philips.

Sur proposition de Philips, j'accepte de prendre ma retraite anticipée au début de 1998 .

1.9.5 Préservation des archives de Philips et de MBLE.

Le 16 novembre 2004, une convention a été signée entre Philips, l'association « Le Club des Anciens de la M.B.L.E. » et les services d'Archives industrielles du Royaume pour assurer l'archivage de documents essentiels à l'histoire de Philips et MBLE en Belgique. Jusqu'à son décès, Jacques Van Haren, en tant que CEO de Philips Belgique et ex-CEO de Philips Professional Systems, sera volontariste à ce sujet.

Mais, Marcel Foulon qui venait d'être nommé CEO de Philips Professional Systems (l'usine de Philips-Wavre, dont il était le patron, venait d'être vendue) avec mission de fermer PPS le plus rapidement possible, avait estimé que le mieux était de détruire toutes les archives de la MBLE. Pour ce faire, il avait demandé à Max Fourez, responsable de la logistique de Philips Belgique, de faire déposer de grandes caisses et de les envoyer à la destruction comme des documents confidentiels.

Max me prévient et nous organisons l'exfiltration de ces documents à l'insu de Marcel Foulon. Discrètement et progressivement un groupe de volontaires fiables a manœuvré pour assurer que ces archives et celles de Philips Belgique soient déposées aux Archives du Royaume :

- Pour Philips Belgique : Kris Vangilbergen ; Julien Michiels et Adrien Brysse.
- Pour le « Club des Anciens de la M.B.L.E » : Urbain Roozen ; André Junqué et Guy Maréchal
- Les représentants des Archives du Royaume furent : Herman Coppens et Caroline Six

Pour les détails, voir l'annexe N°3

Dès que, officiellement, Philips ait accepté ce don aux Archives Générales du Royaume, Adrien Brysse et moi avons organisé une exposition dans la grande salle du rez-de-chaussée du siège social de Philips Belgique, qui avait été transféré depuis la Place de Brouckère vers le site de MBLE [Rue des Deux Gares, 180 à Bruxelles (Anderlecht). Pour ce, nous avons choisi une ou deux centaines de documents, photos ou artefacts illustrant quelques moments ou objets clés de l'histoire de MBLE.

Malheureusement, lors du démontage de cette exposition, il semble qu'une ou deux des caisses ont été perdues. Malade, je n'avais pas pu être présent. Cela fait que certains documents et photos et une large partie de ma collection personnelle d'artefacts ont été perdus. Néanmoins, l'essentiel des boîtes a bien été déposé soit aux Archives Générales du Royaume (les documents et les photos) ; soit, pour les artefacts, à la « Fonderie » : Rue Ransfort 27, 1080 Molenbeek-Saint-Jean <https://www.lafonderie.be/>.

Heureusement, Adrien Brysse avait fait des scans de nombreuses photos et nous a transmis des documents sous forme PDF ou DOC. Nous en avons donc des copies, mais ce n'est qu'indirectement que nous avons formellement l'autorisation de les publier. Nous allons déposer ces copies aux Archive Générales du Royaume en complément des dépôts existants.

C'est, en mon nom, que ma collection personnelle d'artefacts et de documents informatiques a été physiquement déposée par le « Club des Anciens de MBLE ».

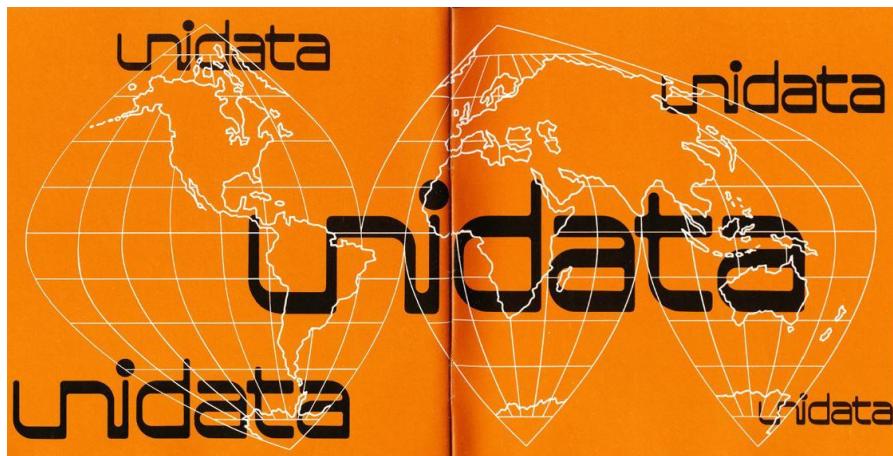
Note : Les inventaires de « La Fonderie » sont incomplets ; j'y ai vu certains de mes artefacts qui ne sont pas inventoriés.

ANNEXES

Au témoignage de Guy Maréchal

Vers une informatique européenne souveraine
1975 La stratégie **unidata** 2025

- Une histoire
- Une vision
- Des récits



1975 : Le sabordage de l'informatique européenne

2025 : L'émergence d'une souveraineté informatique européenne

Marie d'Udekem-Gevers
Guy-Noël Maréchal
Pierre Mounier-Kuhn

Avec des contributions de :

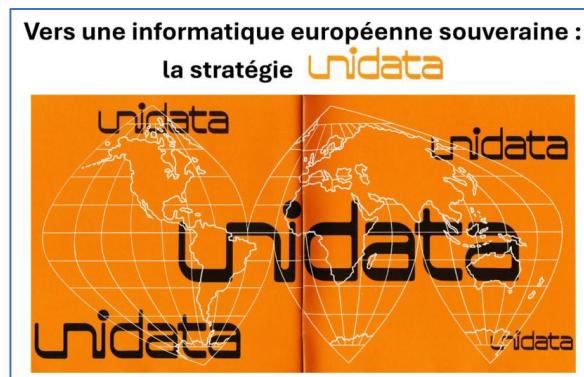


Gérard Alberts
Jean-Louis Blanchart
Francis Bodson
Adrien Brysse
Roland Bullman
Bernard Durieux
Claude Fosseprez
Yves Genin

Georges Goeman
Jean-Marie Pétronio
Michel Pirlot
Jean-Jacques Quisquater
Roger Roberts
Guy Vanden Bemden
Jean Voisin
Ferdinand de Wasseige

Documents associés au livre

Annexe 1 au témoignage de Guy Maréchal



**Contribution à l'audition du Conseil de l'Europe relative à l'
Impact des nouvelles technologies de la communication sur les
Droits de l'homme et les valeurs démocratiques**

03 mai 1996



**Contribution
à l'audition du Conseil de l'Europe
relative à l'**

**Impact des nouvelles technologies de la communication
sur les
Droits de l'homme et les valeurs démocratiques**

Préparé par Guy MARECHAL

Pour certains point, avec inclusion de contributions de Messieurs
Jean-Louis Blanchart et
Roland Bullman

Privé Avenue Emile de Béco,46
 B-1050 Bruxelles
Tel et Fax +32 2 6489828

Bureau Philips Professional Systems
 R&D Manager
 Rue des deux gares 80,
 B-1070 Bruxelles
Tel +32 2 525 6356
Fax +32 2 525 6600

Note: Ce texte n'engage ni
Philips ni l'Asbl Titan.

1.- Introduction

Cette contribution est le fruit de réflexions qui ont mûri dans le cadre de l'Association Sans Buts Lucratifs Titan. Cette ASBL a pour objet la promotion du Multimédia numérique sous tous ses aspects, non seulement techniques et commerciaux mais aussi culturels, sociaux et éthiques. En particulier, l'annexe relative à l'ossature d'un cadre réglementaire a été élaborée dans le cadre de Titan.

Cette contribution ne couvre pas tous les aspects qui seront abordés lors de l'audition. Elle couvre cependant un sous-ensemble cohérent de principes et de recommandations de modalités de mise en place qui devraient pouvoir servir de base à tout l'édifice de promotion et protection des droits et devoirs de l'homme dans le contexte des nouvelles techniques de télécommunication. Cette contribution est volontairement compacte; les développements devraient faire l'objet d'une rédaction en collaboration.

Plusieurs des propositions et analyses présentées pourraient sembler s'éloigner du corps du sujet. Néanmoins, c'est l'avis de l'auteur que précisément, via la mise en place de ces propositions, une base solide pourrait être donnée aux solutions des défis et opportunités qu'offrent ces nouvelles technologies. **L'idée clef est que il faut trouver un cadre de droit opérant sur les réseaux de télécommunications qui présente les mêmes fonctions que celles actuellement disponibles pour les actions et interactions humaines locales et non dématérialisées! Les techniques à maturité sont maintenant disponibles.**

Notes: Le mot "service" couvre tous les types de services et programmes multimédia quelque soit leur support: CD-Rom, ... (En temps différé), Satellite, Câble, Fibre, Hertzien terrestre, ... (En temps réel).

Par formats l'on entend les éléments sémiotiques, syntaxiques et sémantiques des documents ou messages ainsi que de l'interaction des acteurs entre eux assurée au travers ces documents ou messages télécommuniqués. Il s'agit en particulier des techniques de codages, du ou des langages utilisés et des protocoles aux interfaces des diverses couches du modèle réglementaire qui sera proposé ci-après. En particulier, l'analyse des signifiés d'un message et l'écoute légale pourront se faire sur base de ces formats.

Les définitions des concepts fondamentaux relatifs à la sécurisation de l'information sont présentées à l'annexe 1.

2.- Principes

2.1 L'action de l'homme à distance

La société devrait s'organiser pour que les hommes puissent effectuer tous les actes qui sont possibles via les réseaux de télécommunications, avec la même valeur sociale que s'ils avaient été effectués par une action directe localement.

Cela signifie que l'action devient possible en indépendance

**du moment
du lieu
des formats**

Ce principe implique en particulier:

2.1.1 Que l'authenticité de l'identité des interagissants doit pouvoir être garantie à distance au moins aussi bien que via des cartes d'identité émises sous l'autorité publique et vérifiées localement.

2.1.2 Que les informations dématérialisées doivent pouvoir être rematérialisées de manière irréfutable pour servir de preuve (au tribunal, arbitrage privé ou autre). Cette opération a pour but de reconstituer ce que le droit anglo-saxon appelle *proof of evidence* sur base d'*autoconclusive documents*.

2.1.3 Que les informations de lieu, moments ou formats devront devenir explicites quand elles sont pertinentes.

2.1.4 Que des réglementations spécifiques peuvent être d'application pour les transactions qui ne peuvent pas être effectuées via les réseaux de télécommunication, c'est-à-dire qui, par nature, ne peuvent pas ou que l'homme ne veut pas dématérialiser. Le droit intellectuel (toutes les copies sont porteur de l'information) n'est pas le même que le droit des choses matérielles (objets uniques).

Par exemples:

le courrier postal consiste au transport physique d'un objet, qui peut être des feuilles de papier sur lesquelles peut se trouver du texte et avoir été parfumées; par l'envoi postal l'expéditeur se dessaisi de son original.

le billet de banque ne peut être, par nature, transmis à distance par dématérialisation et rematérialisation d'une copie à distance.

par opposition, un ordre de paiement peut être transmis par télécommunication; l'exécution unique de l'ordre peut être assurée par procédure.

Dans les autres cas, les réglementations devraient être homogènes s'il y a ou non dématérialisation dans le transfert de l'information.

2.1.5 Que lorsque l'information n'est pas seulement objet de savoir mais est aussi source pour l'action (tel la source d'un produit logiciel), le cadre réglementaire s'applique non seulement aux droits intellectuels mais aussi aux droits du produit.

2.2 Le contexte de l'action de l'homme à distance

La société devrait s'organiser pour que le cadre réglementaire ne soit pas plus contraignant que nécessaire et suffisamment ouvert que pour que les valeurs, droits et devoirs de chacun puissent être respectés et promus.

Ce principe implique en particulier:

2.2.1 Que les pouvoirs publics doivent disposer d'un cadre de droit où l'action des citoyens puisse s'exprimer.

2.2.2 Que l'expression de l'action puisse être garantie dans deux contextes mutuellement exclusifs, à savoir la communication publique et la communication privée.

Dans le premier cas, une partie prend l'initiative de proposer l'établissement une relation publique avec qui le souhaite. La relation publique a lieu avec chaque correspondant qui accepte cette proposition; le corollaire est que quiconque, y inclus l'état, peut décider d'établir la relation. Cette relation peut être unidirectionnelle ou bidirectionnelle.

Dans le second cas les relations s'établissent entre un nombre limité de membres d'un "club privé" qui ne veulent pas que d'autres puissent connaître ni l'existence ni le contenu des relations établies. Une communication téléphonique est d'habitude de ce type. A priori, l'état doit considérer que le régime normal est celui de garantir la confidentialité de la relation.

2.2.3 Que les pouvoirs publics doivent pouvoir mettre en place, ou organiser que des opérateurs assurent, des services ou programmes publics ou privés d'intérêt public. Pour certains il s'agira de services universels. A titre d'exemples, une Radio ou Télévision publique; des cours privés à destination de chômeurs (cours privés d'intérêt public).

2.2.4 Que les pouvoirs publics ont le droit, et parfois le devoir, de réglementer tous les services quand leur exploitation ou usage a un caractère sociétaire ou d'intérêt collectif.

2.2.5 Que l'accès aux divers rôles associés aux télécommunications soient suffisamment garantis. Que dans tous les cas, par technique ou par contrat, l'accès soit assuré contre un prix raisonnable, équitable et non discriminatoire, en particulier lorsque les ressources sont "rares".

2.2.6 Que les personnes qui effectuent ces actions bénéficient des droits mais aussi des devoirs qui y sont associés. En particulier, les titulaires de droits intellectuels ne doivent pas se borner à assurer la protection de ces droits mais aussi assurer les responsabilités afférentes aux caractéristiques sociales des œuvres ou produits. L'organisation d'un service, en particulier la diffusion d'une œuvre, à destination d'un pays implique de respecter les lois de ce pays. Le titulaire des droits doit donc assumer les implications de confier son œuvre à un fournisseur de services.

2.2.7 Que les acteurs jouant des rôles puissent être:

Des personnes physiques

Des personnes morales, représentées par des personnes morales

Des équipements mandatés par et sous la surveillance de personnes (physiques ou morales) pour jouer en leur nom un rôle précis: à titre d'exemples, un service d'horodatage fiable de document; un service de personnalisation de cartes à puce. Lorsque le mandat est relatif à une personne physique des provisions doivent être prises pour régler la succession en cas de décès ou incapacité.

3.- Recommandations pratiques pour la mise en oeuvre

3.1 Le cadre réglementaire

L' Union Européenne doit mettre en place un cadre réglementaire adapté. Je recommande, avec l'appui de l'ASBL Titan (voir texte en annexe 2), d'adopter un cadre basé sur une réglementation en couches, axées sur les rôles remplis par les acteurs, et où le règlement serait homogène par couche. Dans chaque couche le caractère privé ou public du rôle ainsi que l'impact collectif doivent permettre de moduler la réglementation. Une introduction progressive de ce cadre est possible.

3.1.1 Les couches

Les couches seraient organisées comme suit:

Contenu:

Couche 5 **Les informations de la relation**, représentées suivant un format adapté aux acteurs de la couche 5 et à son interface avec la couche 4.
Exemples: les mots prononcés ou écoutés lors d'une communication téléphonique; la vidéo, son et données constituant un film.

Couche 4 **Les services rendus et les données d'accès au service.**
Les fournisseurs de programmes, ou de services tels Canal+ ou l'un des services du Minitel ou l'un des services du téléphone en GSM. Les données d'accès au services incluent, par exemple le numéro de téléphone, l'adresse Internet, les données de la carte à puce donnant accès à un service de télévision à péage.

Conduit:

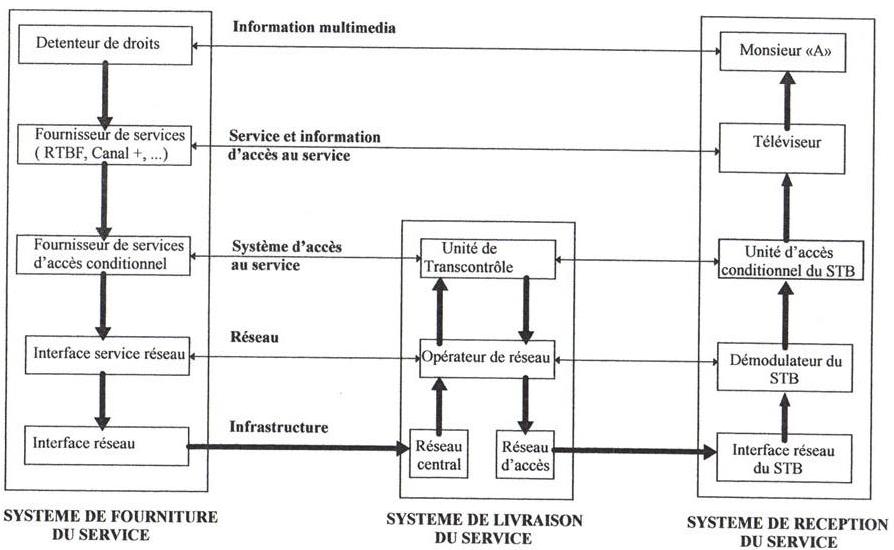
Couche 3 **Le système d'accès aux services.**
Le système des numéros de téléphone, le système d'adresse Internet, le système de contrôle d'accès (*Integrated Receiver Decoder with Smart-Card System*).

Couche 2 **Le réseau**, en tant que gestionnaire du routage et du transport du message (et/ou du document qui y est inclus).

Couche 1 **L'infrastructure physique de communication** assurant le transport de l'information.
Exemples: le câble, le satellite, le canal hertzien terrestre, le disque CD-ROM ou DVD.

ARCHITECTURE DU SYSTEME

→ : Flux réel d'information
 ↔ : Flux fonctionnel



Illustrations du modèle:

Le modèle est prévu pour être applicable non seulement au télécommunications mais aussi à la poste et au livre. L'application à ces secteurs peut être éclairante:

Le courrier postal (établissement d'une relation privée):

- Couche 5 L'expéditeur rédige une lettre privée sur une feuille de papier;
- Couche 4 L'expéditeur place la lettre dans une enveloppe, écrit l'adresse du destinataire, met un timbre, dépose cette lettre dans une des boîtes postales (local; pays; international);
Note: le système d'enveloppes, adresses, timbre, boîte postale avec sa fente et sa porte fermée à clef, le bureau de poste avec ses guichets... est dans la couche 3; le fait de mettre un lettre dans la fente de la boîte postale est dans la couche 4;
- Couche 3 Le facteur relève les lettres dans les boîtes postales;
- Couche 2 Le facteur récolte en fonction des divers centres de tri;
- Couche 1 Le facteur apporte le courrier au centre de tri avec sa camionnette;
- Couche 2 Le service postal trie les lettres en fonction de la destination, vérifie et oblitére le timbre, gère les rebuts et problèmes;
- Couche 1 Les lettres à destination des internationales sont conduites à l'aéroport en camion;
- Couche 2 Le service postal trie les lettres en fonction de la destination;
- Couche 1 Les lettres à destination des USA sont transportées par avion;
- Couche 2 Le *Post Office* trie les lettres en fonction de la destination;
- Couche 1 La lettre est transmise par train au bureau de poste desservant le destinataire;
- Couche 2 Le bureau trie par tournée;
- Couche 3 Le facteur dépose la lettre dans la boîte privée du destinataire;
- Couche 4 Le destinataire relève son courrier et ouvre les enveloppes;
- Couche 5 Le destinataire lit la lettre.

L'on remarquera que le caractère privé du contenu de la correspondance (couche 5) implique que les techniques et le protocole du service postal assurent la *privacy* sur toutes les couches du "conduit". Le service postal assure le transfert fiable de la chose confiée par l'expéditeur jusqu'au destinataire.

Dans le cas du recommandé la couche 4 est différente: le dépôt et la remise procèdent d'un protocole plus complexe, qui implique notamment l'authentication du destinataire.

Le livre (établissement d'une relation publique):

- Couche 5 Un écrivain écrit un roman; il en rédige un tapuscrit;
- Couche 4 Un éditeur publie ce roman en 20 000 exemplaires et prépare affiches, interviews et autres éléments de promotion;
- Couche 3 Le diffuseur collecte 12 000 exemplaire pour diffusion et met en stock 8 000 exemplaires;
- Couche 2 Le diffuseur attribue les exemplaires à diffuser immédiatement aux 2000 librairies et autres points de vente de son réseau de France, Belgique, Canada et Suisse;
- Couche 1 Les trains, camions, avions,... assurent le transport;
- Couche 2 Le diffuseur local remet à chaque point de vente le nombre de livres qui lui sont destinés;

Couche 3	Le libraire met le livre à l'étagage, en rayon, ...; il colle les affiches;
Couche 4	Le client est séduit; il achète le livre;
Couche 5	Le client lit le roman.

L'on remarquera que le caractère public du contenu et de la diffusion du livre (couches 5 et 4); ce qui ne dispense pas l'auteur et l'éditeur de respecter la loi .

Un service de Télévision à péage (établissement d'une relation publique):	
Couche 5	Le film "Basic Instinct"
Couche 4	Un opérateur de service de télévision à péage décide de mettre le film "Basic Instinct au programme de tels jours et telles heures, en mode "pay per event"; il ajoute le niveau de "code parental"; il génère les clefs de chiffrement du transport diffusé par câble et des droits destinés aux cartes à puces des abonnés qui commandent l' <i>event</i> ;
Couche 3	Le système de contrôle d'accès diffuse les droits destinés aux cartes à puces des abonnés;
Couche 2	Le câblodistributeur organise les liaisons vers les divers têtes de réseau;
Couche 1	Les câbles transmettent vers les abonnés;
Couche 2	Le <i>tuner</i> sélectionne le service de télévision à péage;
Couche 3	L'utilisateur a mis sa carte à puce dans le décodeur;
Couche 4	Le terminal-décodeur dé-embrouille le signal au moyen des clefs et la carte à puce acte la consommation; le client élève le code parental;
Couche 5	Le client regarde le film.

L'on remarquera que, bien que l'offre est publique, la relation publique n'a lieu qu'avec les clients qui regardent.

3.1.2 La modulation

Dans chaque couche le caractère privé ou public du rôle ainsi que l'impact collectif doivent permettre de moduler la réglementation. En particulier, les éléments collectifs comme la protection des droits de l'homme et des valeurs démocratiques.

3.1.3 L'introduction progressive

La plupart des législations et cadres réglementaires existant sont organisés **verticalement**, c'est-à-dire que l'infrastructure physique de communication dicte les règles applicables aux couches successives.

Le modèle par couches suppose une organisation **horizontale**, homogène dans la couche. Les particularités ne peuvent dépendre que du caractère spécifique des diverses réalisations de la couche: le CD-ROM et le Satellite sont dans la même couche (l'un offre un support intemporel tandis que l'autre est en temps réel. Le premier s'adresse à chacun, l'autre à tous).

La recommandation est que les pouvoirs publics segmentent d'abord leur législation actuelle suivant les couches proposées: le règlement reste le même, mais les autorités gèrent leurs compétences en segmentant leurs analyses. Ensuite, les diverses autorités coordonnent leurs actions entre elles couches par couches. Enfin, un cadre homogène est introduit.

De plus, il est suggéré que le régime actuel, presque exclusivement basé sur les autorisations préalables, soit remplacé par un régime mixte où, dans le contexte d'un cadre réglementaire cohérent et d'un ensemble de modalités d'applications spécifiques, le régime normal, pour la plupart des contextes, soit le régime de liberté, tel le cas du livre actuellement: le contrôle se ferait alors *a posteriori*. Pour d'autres contextes, notamment quand les arrêtés d'applications ou les formats ne sont pas disponibles dans le cadre réglementaire, un régime de déclaration serait nécessaire; avec autorisation implicite après un certain délai. Enfin, dans certains cas, clairement définis [en particulier quand le concept de service universel est d'application ou applicable], une autorisation serait nécessaire préalablement; par exemple, pour l'ouverture de trottoirs pour y placer des fibres optiques (couche 1).

Note La commission a mis en route la rédaction d'un cadre général applicable à chaque pays de l'Union pour couvrir ce domaine, ainsi qu'une extension de l'ONE. Il y aurait lieu de vérifier s'il couvre correctement les principes et modalités préénoncées ici.

3.2 Les Trusted Third Parties

La Commission de l'Union Européenne a approuvé le livre Vert sur la sécurisation des systèmes d'information 1995 avril 29 [*Green Paper on the Security of Information Systems*]. Il y est montré que cette sécurisation implique la présence de tiers fiables (TTPs).

La recommandation est que l'Union Européenne organise conjointement avec les Etats un réseau de TTPs.

3.2.1 Assurance d'identité et de *privacy*

Les Etats assurent eux-mêmes (en le faisant ou en le faisant faire sous leur contrôle) que divers niveaux de pouvoir doivent mettre en place un système de délivrance de "cartes d'identité électroniques" respectant la *privacy* de chacun, système en particulier non obligatoire et non réquisitionnable. Les techniques nécessaires existent. De la sorte, les actes posé à distance pourront être attribués indubitablement et leur auteur devra assumer les devoirs et profitera des droits y associés. Un Etat qui a reconnu un autre état doit mettre en place un système de certifications croisées.

Sans assurance de l'identité il n'y a pas de moyen d'assurer le respect des droits et devoirs: par exemple, il y a obligation de mentionner l'éditeur responsable d'une publication et, dans certains pays, obligation de dépôt légal pour vérifier la véracité des informations.

Notes: Le protocole pourrait être:
 que le TTP personnalise un jeton (une carte à puce);
 que ce jeton soit attribué à une personne physique qui définirait elle-même un secret qu'il lui soit propre (par exemple la clef secrète de RSA);
 que la clef publique associée à ce secret ainsi que le ou les rôles seraient certifiés par le TTP sur vérification de la paire clef de jeton, clef publique; ultérieurement confortée par des critères biométriques;
 que la clef secrète de confidentialité serait générée par une technique de *Fair Escrow* dans un TRD, de telle sorte que seules les clefs partielles dispersées sortiront du TRD chiffrée avec la clef publique de l'autorité concernée (voir usage par la suite);
 que le jeton soit validé par son titulaire comme premier usage.

3.2.2 Accréditation de TTPs

Les divers niveaux de pouvoir doivent mettre en place un système d'accréditation et de contrôle de TTPs en charge d'autres tâches que celle d'assurance d'identité et de privacy. Certains de ces services de TTP doivent exister obligatoirement, notamment:

- l'archivage fiable;
- la dématérialisation fiable (autoconclusive document);
- la rematérialisation fiable;
- la certification de contenu;
- le marquage fiable du moment, de l'endroit ou des formats;
- la non répudiation vis-à-vis de tiers;
- enregistrement fiable des formats.

3.3 La normalisation des formats

La normalisation ou le dépôt des formats sont nécessaires dans de nombreuses situations. Elle implique que le signifié d'une transaction est rendu aussi non-ambigu que nécessaire.

L'analyse des signifiés d'un message est nécessaire pour que les droits des parties communicantes et des tiers lésés ou concernés puissent être garantis. L'écoute légale suppose comprendre ce qui s'échange.

Dans beaucoup de cas, la définition d'un format sera quasi implicite: le codage téléphonique; un tapuscrit en français codé en MS-Word ou en Wordperfect.

Dans d'autres cas, cette définition est formalisée dans des normes détaillées, telle EDIFact, où chaque élément de donnée est défini, y inclus la sémantique fine, au point que des ordinateurs puissent analyser un message et en dériver les opérations de logistique et de facturation d'une commande.

3.4 La qualification des contenus

La responsabilité du titulaire des droits intellectuels est d'assurer:

1. l'identification de (des) titulaires de droits intellectuels (couche 5);
2. la responsabilité de la qualification de chaque œuvre ou produit d'usage public ou même privé dans certains cas, lorsqu'elle présente des caractéristiques sociétaires particulières, de telle sorte que leur usage puisse être fait en connaissance de cause. Cela impliquerait de signaler le caractère violent, fanatique, pornographique, révisionniste, dangereux,...

Ces deux types d'information seraient exploitable directement par les fournisseurs de services et autres intervenants pour en tirer les conséquences sur l'opportunité et modalités de diffusion dans un pays donné. Ils pourraient alors ajouter leur identification et l'éventuel code parental applicable lors de la mise en œuvre du service.

Il faut rapprocher cette recommandation des règles existantes qui définissent la responsabilité du fait du produit et des règles valables pour l'édition.

3.5 L'écoute légale du contenu de relations privées

Comme dit précédemment l'usage de la cryptographie pour tous usages devrait être libéralisé, sauf dans le cas d'usage pour la confidentialité qui serait assuré comme régime normal mais levé dans les cas où la loi le permet ou l'impose. Cela signifie que tous les usages courants de la cryptographie sont libéralisés tels en contrôle d'accès, en transfert bancaire, en signature digitale, en certification de moment, places ou formats, et autres cas où la cryptographie assure l'information et l'accès autorisé ou non refusé à des ressources.

L'écoutabilité des archives privées est un domaine du droit qui est distinct.

La mise en oeuvre de la capacité d'écouter (écoutabilité) aura lieu pratiquement dans le "conduit". Mais la responsabilité de l'écoutabilité est en fait transmise depuis le titulaire du contenu (couche 5), au titulaire du service (couche 4) puis au titulaire du système d'accès au service, lequel le transmet au titulaire du réseau (couche 2) et enfin au transporteur (couche 1). A chaque transfert le contrat doit prévoir explicitement (tant que la loi n'existe pas le rendre implicite) que les messages (et documents qui peuvent y être inclus) sont exprimés dans des formats et par des moyens de mise en oeuvre de ces formats qui sont écoutables. Pour des raisons pratiques et d'efficacité, les Etats vont s'adresser d'abord au fournisseur de service qu'ils supposent s'être assuré de l'écoutabilité du contenu et qui a pu utiliser des clefs cryptographiques pour embrouiller le signal quand il est diffusé par câble, satellite ou autres.

Le concept d'écoutabilité:

Tout responsable de conduit, solidaire avec le fournisseur du service de télécommunication doit assurer les moyens permettant l'écoute, à l'insu des écoutés (et idéalement à leur propre insu), quand le prévoit (autorise ou l'impose) la loi. Cette obligation de solidarité s'entend pour les responsables du conduit afin de donner accès au message quand la séparation entre le réseau et le codage de représentation (de contenu ou de service) sont disjoints. Cette même obligation s'entend aussi pour l'utilisateur final qui, au-delà du codage de représentation ajouterait un codage de confidentialité; ce faisant il réalisera une partie de la couche 4.

En principe, l'écoutabilité (le fait de rendre possible l'écoute dans les conditions prévues par la loi) est à charge des organisations responsables du service mais doit être mise en oeuvre par l'infrastructure et à l'endroit le plus approprié du "conduit" concerné. Cependant, cette charge doit pouvoir être couverte de manière raisonnable.

Divers éléments jouent dans cette situation:

Concertation sur le moyen d'assurer l'écoutabilité: l'écoutabilité peut être réalisée de plusieurs manières pouvant avoir un impact financier très différent (Module hardware ou co-routage par voie de logiciel, par exemple)

Concertation sur le nombre d'écoutes simultanées: les équipements à prévoir sont en partie dépendants des paramètres quantitatifs; ceci pourrait entrer en conflit avec les prérogatives très larges des Juges d'Instruction.

Concertation sur le modèle statistique: dans certains cas, les lois autorisent de fixer une limite à la probabilité de ne pas pouvoir acheminer une communication surveillée vers les centres d'enregistrement: ce paramètre a un impact direct sur l'architecture

et les coûts d'infrastructure d'acheminement.

Concertation sur les modalités transitoires: les personnes concernées doivent avoir un calendrier d'échelonnement de la mise en place de l'écoutabilité.

Mise en place d'une organisation de la liaison Ecoute-Ecoutabilité: les interfaces et protocoles doivent être définis.

L'écoutabilité démocratique se doit de mettre en place les moyens et les modes opératoires de l'écoute de telle sorte que l'écoute ne soit possible que pendant la période décidée par l'autorité compétente dans les limites de la loi et pour la (les) personnes ciblées uniquement.

En principe, l'écoute (s'est à dire exploiter l'écoutabilité) serait à charge des services de l'Etat préposés à cette écoute.

Plusieurs formules peuvent être adoptées: la plus simple est de refléter les coûts de l'écoutabilité liés à chaque utilisateur sur l'utilisateur (amortissement repris dans le tarif d'abonnement); de refléter les coûts relatifs à l'écoutabilité liés au système d'écoute dans les tarifs de l'exploitation de l'écoute. C'est cette approche qui avait été adoptée par l'administration du président Bush. Sous la pression de puissants lobbies, argumentant qu'historiquement les organisations de télécommunication n'ont aucune responsabilité de service public qui n'aït été financée par l'Etat, cette organisation a été retouchée par l'administration Clinton.

Le corollaire inéluctable aux lois de protection de la vie privée est qu'il faut organiser le secteur des techniques de confidentialité et de preuve d'identité.

De nombreuses techniques permettent d'assurer l'écoutabilité. Plusieurs sont du ressort de la protection du territoire et sont secrets.

Cependant dans des pays démocratiques, une des approches acceptable est celle du *Fair Escrow* qui offre des garanties de protection de la vie privée en régime normal et autorise l'écoute comme une exception dans des cas précis, après décision motivée de la justice, pour un temps limité, et ce sans que cette autorisation ne compromette ultérieurement la clef privée de confidentialité. La dispersion des éléments de clef et le placement des fragments en lieux non connectés au réseaux devrait assurer une protection sérieuse contre les usages abusifs. Une présomption de culpabilité de l'utilisateur serait d'application en cas d'usage non autorisé (par exemple sur base d'un format non déposé ou autorisé) ou hors du cadre, avec à la clef de lourdes peines.

Aux USA la solution du Clipper-Chip n'est pas bonne car elle ne respecte pas les règles de *Fair Escrow* ce qui, à juste titre a provoqué une colère des forces démocratiques.

3.6 Les services universels

Le financement de la charge supplémentaire relative aux services universels devraient être assurés par les services non soumis au service universel.

Note La commission a mis en route la rédaction d'un cadre général applicable à chaque pays de l'Union pour couvrir ce domaine. Il y aurait lieu de vérifier s'il couvre correctement les principes et modalités préénoncées ici.

3.7 Les règles de protection contre la piraterie

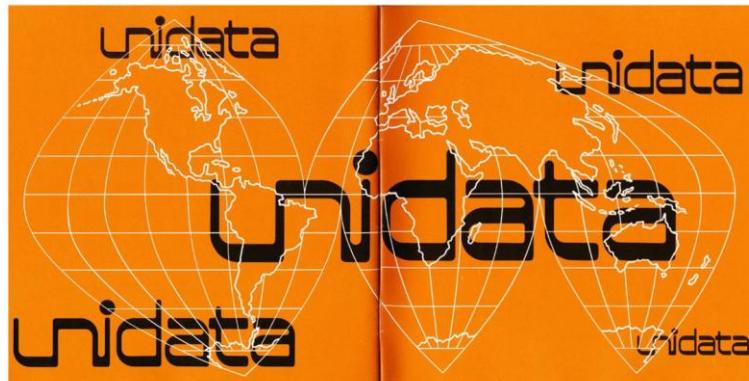
Note La commission a mis en route la rédaction d'un cadre général applicable à chaque pays de l'Union pour couvrir ce domaine. Il y aurait lieu de vérifier s'il couvre correctement les principes et modalités préénoncées ici.

Annexes: **1. Les réseaux ouverts, les risques de sécurité et les droits fondamentaux**
 2. Ossature d'un cadre Réglementaire (ASBL Titan)

Documents associés au livre

Annexe 2 au témoignage de Guy Maréchal

**Vers une informatique européenne souveraine :
la stratégie unidata**



Note au Conseil des Ministres sur la signature digitale

27 mai 1997



BRUXELLES le 27-05-1997

- 1 -

MARECHAL G.

Note au Conseil des Ministres

Vers une réglementation juridique en matière de signature digitale

1. Introduction

Dans notre pays également, de plus en plus d'actes juridiques sont accomplis par voie électronique. De nouvelles technologies informatiques et de communication créent, tant dans le secteur privé que dans le secteur public, des possibilités permettant de travailler plus vite et de manière plus efficace. Voici quelques exemples :



CABINET JUSTICE
115 BOULEVARD DE WATERLOO
1000 BRUXELLES
TEL. 02-542 79 11
FAX 02-538 07 67

Isabel

En Belgique, dans le secteur privé, c'est surtout le secteur bancaire qui connaît une explosion d'initiatives. Le réseau Isabel (Interbank Standards Association Belgium) en est un exemple. Ce réseau permet à des entreprises et à des particuliers de communiquer de manière uniforme avec les banques par voie électronique. A l'aide d'un seul programme, un client peut dès lors traiter des extraits de compte de toutes les grandes banques belges, envoyer des ordres de virement à toutes les banques, etc. Les communications, telles que, par exemple, des ordres de virement, sont, dans le cadre d'Isabel, signées électroniquement au moyen d'un signature digitale. En outre, le réseau offre un certain nombre de services supplémentaires, tels que le courrier électronique, la consultation de bases de données, le commerce électronique et une liaison avec Internet. De par sa possibilité d'effectuer, de manière peu onéreuse et simple, des opérations bancaires électroniques avec toutes les grandes banques belges, on s'attend à ce qu'Isabel devienne très rapidement un des plus grands réseaux électroniques de notre pays.

Internet

Internet est également de plus en plus souvent utilisé à des fins commerciales. En effet, ce seront surtout les entreprises et les indépendants qui feront appel au réseau Isabel dont il est question ci-dessus, car ce sont eux qui ont le plus besoin d'une communication électronique harmonisée avec les banques. En revanche, le grand public exploitera principalement les possibilités d'Internet.

De nombreuses entreprises proposent déjà leurs produits et services par le biais d'Internet. Des "marchés" électroniques apparaissent également en Belgique, tels que Intermart de la société Innet, qu'utilisent actuellement environ 265 sociétés pour proposer leurs produits et services. "Belgium on Net" d'Interpac, etc. Parmi les "websites" les plus fréquentés figurent notamment les cinémas et les théâtres (pour la réservation de billets), les agences de voyage (pour la sélection et la réservation de voyages), les librairies, les magasins de cd, etc. Les banques et les compagnies d'assurances proposent également plus en plus leurs produits aux particuliers par le biais d'Internet. C'est surtout pour ces derniers secteurs que l'utilisation de la signature digitale dans le cadre d'opérations bancaires électroniques ou pour l'échange d'une proposition de police d'assurance, est d'une importance capitale.

Carte d'identité sociale

Dans le secteur public, tous les regards se tournent actuellement vers la carte d'identité sociale parce qu'elle constitue la base d'une première circulation de données entre le citoyen et le secteur public qui soit électronique, opérationnelle et de pointe, et qui, dans le secteur public, fait également appel à la technique de la signature digitale. La carte d'identité sociale sera utilisée afin de mettre de manière électronique des données relatives au statut d'une personne en matière de sécurité sociale à la disposition, notamment, des pharmaciens et des hôpitaux, dans le cadre de l'application du système du tiers payant lorsque des soins sont prodigués. La carte sert également de moyen d'identification à l'aide duquel les employeurs peuvent, de manière fiable et efficace, fournir des données concernant leurs employés à la sécurité sociale. Enfin, l'assuré social pourra également accéder à certaines données concernant l'état de ses dossiers grâce à la carte d'identité sociale. Les données confidentielles - par exemple, à quelle mutuelle l'intéressé est-il affilié ? - figurent sur la carte d'identité sociale de manière codée et ne sont accessibles qu'aux seuls prestataires de soins qui disposent d'une clé de décodage. Ces derniers reçoivent cette clé de l'INAMI sous la forme d'une carte à puce qui leur permet de lire et éventuellement d'adapter les données contenues sur la carte. Il faudra utiliser des *signatures digitales* dans les transactions entre, d'une part les employeurs et les prestataires de soins et, d'autre part, les organismes de sécurité sociale.

2. Problématique

L'absence de réglementation juridique en matière de signature électronique constitue un obstacle au développement des applications précitées. Une communication de la Commission européenne souligne l'absence de pareille réglementation au sein des Etats membres de l'Union européenne (COM (97)157 : Vers une initiative européenne en matière de commerce électronique,

Communication au Parlement européen, le Conseil, le Comité économique et social et le Comité des Régions, 15 avril 1997, § 36).

Au cours des dernières années, la majorité des états des Etats-Unis ont édicté une législation concernant la valeur juridique et l'usage des signatures digitales. Une initiative fédérale est actuellement élaborée. En Allemagne, le gouvernement fédéral a approuvé fin 1996 un projet de loi qui contient une réglementation en matière de signature électronique (Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste, Bundesrat, Drucksache 966/96, Artikel 3, Gesetz zur digitalen Signatur). Le gouvernement danois a également élaboré un projet de loi similaire. En mars 1997, le gouvernement britannique a publié un "consultation paper" à ce sujet (Licensing of Trusted Third Parties for the Provision of Encryption Services. Public Consultation Paper on Detailed Proposals for Legislation).

Toutes ces initiatives ont pour objectif d'éliminer l'insécurité liée au statut juridique des signatures digitales, afin de promouvoir l'accomplissement d'actes juridiques par voie électronique dans les secteurs privé et public. Notre pays ne peut évidemment se laisser distancer dans ce domaine.

3. Qu'est une signature digitale ?

Une signature digitale est un fichier informatique de petite taille et codé que l'expéditeur envoie en même temps qu'un message de télécommunication. Ce petit fichier codé (une série de lettres et de chiffres) possède les caractéristiques suivantes :

- il est produit à l'aide d'une clé cryptographique qui n'est connue que de l'expéditeur et de personne d'autre;
- à l'aide de cette clé est effectuée une opération mathématique sur le message qui doit être envoyé et le résultat de cette opération est fixé dans le petit fichier informatique codé qui, lors de l'envoi, accompagne le message;
- le petit fichier informatique codé qui constitue la signature digitale peut uniquement être décodé à l'aide de la clé publique de l'expéditeur et cette clé publique peut être demandée par tout un chacun;
- de ce fait, le destinataire du message a une double garantie : 1) il s'agit d'un message authentique 'signé' par l'expéditeur et 2) depuis le moment de la 'signature' absolument rien n'a été modifié dans le message (sinon le résultat de l'opération mathématique ne serait plus exact).

Les questions suivantes sont fréquemment posées concernant cette technique :

D'où provient la clé privée à l'aide de laquelle l'expéditeur produit sa signature ?

Cette clé est généralement (en même temps qu'une clé dite "publique", voir plus loin) générée par l'intéressé lui-même à l'aide d'un programme informatique approprié. Cette facilité est intégrée aux versions récentes des programmes informatiques les plus répandus pour l'usage d'Internet (Netscape Communicator, Microsoft Internet Explorer).

Parfois, la clé privée est initialement attribuée à l'intéressé (par exemple, par une banque à ses clients ou par une entreprise aux membres de son personnel). Dans ce cas, l'intéressé a cependant très souvent la possibilité de modifier lui-même la clé (comparez la possibilité de modifier le code secret de cartes bancaires électroniques telles que Bancontact ou Mister Cash).

Où l'expéditeur conserve-t-il sa clé privée ?

Actuellement, il conservera souvent la clé privée dans un fichier sur le disque de son PC et protègera l'accès à ce fichier par un mot ou une phrase de passe. Le désavantage de cette méthode est que l'intéressé n'emporte pas son code partout et que, par conséquent, il a toujours besoin de son ordinateur pour apposer une signature. C'est pourquoi la clé est de plus en plus souvent placée sur une carte à puce (voir, par exemple, la carte à puce donnée aux prestataires de soins dans le cadre de la carte d'identité sociale).

Comment le destinataire peut-il savoir que la signature digitale appartient à l'expéditeur ?

Dans le cas d'une signature digitale, le contrôle est effectué à l'aide d'une "clé publique". Cette clé publique constitue le complément de la clé privée de l'expéditeur. Lors de la création de la clé privée, la clé publique est générée simultanément. Seule une clé publique déterminée correspond à une clé privée précise. Tout comme la clé privée, la clé publique est une série (assez longue) de chiffres et de lettres. Dans les programmes de communication les plus utilisés a été intégré un software qui avertit l'utilisateur lorsqu'aucune clé publique ne peut être trouvée pour une signature digitale ou lorsque la clé publique ne correspond pas à la clé privée à l'aide de laquelle la signature a été générée.

Où le destinataire trouve-t-il la clé publique de l'expéditeur ?

Afin de prévenir les fraudes, l'expéditeur fera "certifier" sa clé publique. Pour ce faire, il doit s'adresser à une "autorité de certification". Cette dernière contrôlera si la clé publique appartient effectivement à l'expéditeur et si elle correspond à sa clé privée. A cet effet, l'expéditeur doit idéalement, après avoir produit la clé privée et la clé publique correspondante, se présenter personnellement auprès de l'autorité de certification afin de prouver son identité. L'autorité de certification lui délivrera alors un certificat confirmant l'authenticité de la clé publique. Le certificat porte la signature digitale de l'autorité de certification de sorte qu'il ne peut plus être falsifié. Dorénavant, l'expéditeur enverra son certificat contenant la clé publique en même temps que chaque communication signée. Si un doute subsistait néanmoins concernant la validité du certificat, le destinataire peut toujours s'adresser à l'autorité de certification même. Par le biais du réseau, cette dernière devra notamment mettre à disposition une base de données incluant une liste des certificats retirés.

Par quelle instance les certificats digitaux sont-ils délivrés ?

Afin de délivrer ces certificats digitaux, une instance doit disposer d'un know-how de pointe et d'un environnement informatique très bien protégé. Dans le contexte Internet, le leader actuel du marché dans ce domaine est la société américaine Verisign. La société anonyme BelSign, créée par la Fédération des Chambres de Commerce et d'Industrie en collaboration avec la société Netvision de Louvain, est depuis peu active en Belgique. BelSign entend jouer un rôle d'autorité de certification en Belgique et au Luxembourg. Toutefois, de nombreuses autres autorités de certification sont déjà actives à l'étranger. On s'attend à ce que, dans notre pays, en plus de BelSign, d'autres comme Isabel, Belgacom, la Poste, le notariat, etc. se lanceront également sur ce marché et délivreront des certificats au public. Ce qui soulève automatiquement la question de savoir si la délivrance de certificats digitaux n'est pas une tâche qui incombe plutôt aux autorités.

La clé privée de l'expéditeur ne peut-elle être volée ?

Dès qu'une personne a créé ou reçu ses clefs privée et publique, il est très important qu'elle soit la seule à avoir accès à la clé privée. En effet, si quelqu'un d'autre obtient l'accès à la clé privée, la signature digitale peut être 'contrefaite'. Si la clé privée est conservée dans la mémoire d'un ordinateur, l'accès sera généralement protégé par un mot ou une phrase de passe. Lorsque la clé privée est placée sur une carte à puce, l'accès à la clé privée est généralement protégé par un code secret (comme pour Bancontact ou Mister Cash), qui peut être modifié par l'intéressé lui-même. A l'avenir, le code secret sera probablement remplacé pour certaines applications par des techniques biométriques (par exemple, une empreinte digitale), mais les applications

basées sur ces techniques restent provisoirement très chères. Néanmoins, l'identification biométrique par reconnaissance d'empreintes digitales pour accéder à la clé privée est déjà appliquée par les organismes de sécurité sociale espagnols. Tout comme pour une simple signature manuscrite, chaque personne individuellement veillera à ne pas donner sa clé privée à un tiers (par exemple, à un adjoint, à un ou une secrétaire, etc.) et à la protéger contre le vol et l'usage illicite.

Comment peut-on apposer une signature digitale à l'aide d'une carte à puce ?

Un lecteur de carte est requis afin de lire la clé privée figurant sur la carte à puce. Pareils lecteurs de carte sont actuellement déjà utilisés dans le réseau Isabel. Un autre exemple est le lecteur de carte à puce utilisé pour la carte Proton de Banksys. Lorsque l'on souhaite signer un document rédigé à l'aide d'un traitement de texte ou reçu par courrier électronique (par exemple, un projet de contrat), la clé privée (après l'encodage d'un code secret) sera enregistrée par un programme informatique et ensuite utilisée pour l'opération mathématique qui conduit à la signature digitale. Dans certains cas, l'opération qui mène à la signature digitale est même entièrement exécutée par un processeur incorporé dans la carte à puce.

Une même personne peut-elle posséder différents certificats et clés privées ?

Une même personne peut effectivement générer ou recevoir différentes clés privées et faire chaque fois certifier la clé publique correspondante par l'autorité de certification. A titre d'exemple, une personne peut recevoir une clé privée de son employeur, une autre de son organisme bancaire, et générer en outre elle-même une clé privée pour pouvoir apposer des signatures digitales lors de commandes personnelles sur Internet. Il est également possible de faire certifier une même clé publique par différentes autorités de certification. Dans la pratique, on travaillera toujours pour une application déterminée (par exemple, Internet) avec la même clé privée. Il va de soi qu'il faut viser le plus possible à ce qu'une même personne utilise le plus possible, pour toutes les applications, une même clé privée (une seule carte à puce, un seul code secret à mémoriser, etc.). Naturellement, cela n'empêche pas que la clé doit régulièrement être remplacée pour des raisons de sécurité.

Qu'en est-il de la signature digitale des personnes morales ?

Une clé privée - et la clé publique correspondante - peut être attribuée à une personne morale. Il est également possible d'obtenir un certificat pour une clé publique, qui garantit que la clé publique appartient, par exemple, à la société ABC. Du point de vue technique, une personne morale peut dès lors apposer une "signature digitale". Du point de vue juridique, cela ne peut toutefois pas être considéré comme une signature parce que seules les personnes physiques

peuvent apposer une signature. Si une personne morale conclut un accord, l'acte est signé par une ou plusieurs personnes physiques au nom de la personne morale. Dans ce contexte, nous souhaitons dès lors réserver le terme "signature digitale" à la signature digitale au sens juridique (personnes physiques uniquement).

La technique de la signature digitale est-elle déjà suffisamment mûre pour faire l'objet d'une législation ?

Quelles que soient les critiques que l'on puisse émettre à l'égard de la technique de la signature digitale en tant que telle, il est un fait que cette technique constitue à l'heure actuelle, non seulement à l'étranger, mais en Belgique également, l'instrument par excellence pour incorporer un certain degré de sécurité au niveau de documents envoyés par voie électronique. En négligeant de légiférer en cette matière et de veiller ainsi à plus de sécurité juridique, on occasionne un important retard pour les entreprises privées, les administrations publiques et pour les particuliers qui, dans notre pays, veulent investir dans l'introduction de la télématique dans leurs activités.

Les clés utilisées pour la signature digitale peuvent-elles également servir à coder un message et le rendre illisible pour des tiers ?

Pour coder des messages, on utilise en règle générale les mêmes clés que celles avec lesquelles on appose une signature digitale. Cela entraîne notamment des conséquences au niveau de la discussion sur l'accès aux messages codés dans le cadre de l'application de la législation sur les écoutes.

4. Nécessité d'un cadre juridique

Il est nécessaire pour diverses raisons que soit créé à court terme en Belgique un cadre juridique pour l'emploi de signatures digitales. Les raisons les plus importantes sont les suivantes :

- l'absence de cadre juridique constitue un frein important au développement de services électroniques dans notre pays;
- un cadre juridique est également nécessaire pour assurer une meilleure protection du consommateur qui est de plus en plus en contact avec les nouvelles technologies en matière d'information et de communication;
- l'introduction de la télématique dans le secteur public est ralentie par l'incertitude relative au statut de la signature digitale dans les procédures administratives;

- des initiatives divergentes sont prises tant dans le secteur privé que dans le secteur public en vue de permettre l'emploi d'une signature digitale dans des applications limitées (carte d'identité sociale, autorités de certification, etc.); l'absence de réglementation mènera à court terme à une prolifération incontrôlée et à des incompatibilités.

Que faut-il réglementer ?

Afin de permettre l'emploi de signatures digitales dans notre pays, il convient d'élaborer des réglementations sur quatre plans :

1. adaptation des règles en matière de preuve dans le Code civil (voir la note du Ministre de la Justice "Uitdagingen van de informatiemaatschappij en opdrachten voor het justtiebeleid, deel II : Bewijsrecht op de informatiesnelweg") : voir ci-après au point 4.1;
2. adaptations ponctuelles d'un grand nombre de lois et d'arrêtés où il est expressément renvoyé à des documents sur papier, portant des signatures manuscrites, des lettres recommandées à la poste, etc. (voir notamment la note "Juridische vragen bij de automatisering van griffies en parketten", janvier 1997); ces adaptations doivent être apportées de manière progressive et après avoir soigneusement pesé le pour et le contre; l'échange électronique de messages et la signature digitale ne sont pas opportuns dans tous les cas : voir ci-après au point 4.2;
3. réglementation de l'activité des autorités de certification par le biais d'un système de licences accordées par l'autorité : voir ci-après au point 4.3;
4. réglementation de l'emploi de signatures digitales dans le secteur public, non seulement pour les titulaires d'un emploi public, mais également pour les citoyens dans le perspective de leurs relations avec les autorités (carte d'identité digitale) : voir ci-après au point 4.4.

4.1 Adaptation des règles du Code civil en matière de preuve

Il s'avère que l'actuelle réglementation en matière de preuve contenue dans les articles 1316 et suivants du Code civil crée une insécurité juridique et gêne de ce fait l'accomplissement d'actes juridiques électroniques ainsi que la conservation électronique de données juridiquement pertinentes. Plusieurs raisons expliquent cette insécurité juridique :

- aucune disposition légale ne prévoit explicitement que des moyens de preuve électroniques peuvent en principe être utilisés;

- en outre, on doit recourir à l'application ou l'interprétation par analogie d'anciens articles de loi pour donner malgré tout une force probante aux moyens de preuve électroniques (art. 1347-1348). Toutefois, le juge appréciera dans chaque cas la force probante de sorte que l'on ne saura jamais à l'avance si les moyens seront acceptés comme preuve;
- on peut toutefois déroger aux règles du Code civil en matière de preuve en concluant des conventions en matière de preuve, mais cette solution n'est possible que si les parties se sont préalablement contactées;
- les juges ne sont pas familiarisés avec les moyens de preuve électroniques et ils attacheront moins de valeur aux données électroniques dans l'évaluation de ces moyens.

Dès 1981, le Conseil de l'Europe a indiqué la nécessité d'autoriser les moyens de preuve électroniques dans sa Recommandation concernant l'harmonisation des législations sur le plan des conditions requises en matière d'écrits et sur le plan des reproductions de documents et de fichiers informatiques.

A l'heure actuelle, la plupart des pays européens autorisent déjà expressément les moyens de preuve électroniques ou sont le cadre de travaux en vue de l'établissement d'un système de preuve qui corresponde aux nouvelles exigences.

Il est possible d'admettre les données électroniques comme moyen de preuve moyennant quelques modifications minimes de la législation actuelle.

En premier lieu, l'article 1316 du Code civil peut être adapté de sorte que les données électroniques soient expressément admises comme moyen de preuve. De cette manière, il n'est plus nécessaire de considérer les moyens de preuve apportés électroniquement comme présomption, ni d'essayer d'interpréter des articles de loi existants d'une façon extensive telle qu'ils engloberaient également les moyens de preuve électroniques.

En deuxième lieu, il conviendrait de faire figurer au Code civil une définition des notions d'"écrits" et de "signature" qui serait fonctionnelle et ne tiendrait pas compte de critères technologiques afin qu'un écrit ne soit pas seulement un document sur papier et qu'une signature ne soit pas uniquement une signature apposée manuellement sur un document. En insérant une définition large et indépendante de la technologie de ces deux notions, l'interprétation très restrictive de la jurisprudence de la Cour de Cassation, surtout en ce qui concerne la notion de "signature", pourra être modifiée.

Conclusion : le Ministre de la Justice présentera au Conseil des Ministres, en concertation avec son collègue des Affaires économiques et des Télécommunications, un projet de loi adaptant les règles du Code civil en matière de preuve aux technologies de l'informatique et des télécommunications.

4.2 Adaptation de diverses lois en vue de l'introduction de la télématiche

Dans des sous-domaines spécifiques du droit, le législateur a déjà prévu la possibilité de produire des copies électroniques de documents ayant la même force probante que leurs originaux. Dans certains cas, la force probante est même octroyée explicitement aux informations transmises électroniquement. L'élargissement du droit en matière de preuve se limite le plus souvent à certaines instances publiques qui sont autorisées à remplacer les documents en papier par des fichiers électroniques.

Quelques exemples :

- Article 19 de la loi sur le chèque postal (loi du 02/05/56) : "Les copies photographiques, microphotographiques, magnétiques, électroniques ou optiques des documents détenus par LA POSTE font foi comme les originaux, dont elles sont présumées, sauf preuve contraire, être des copies fidèles lorsqu'elles ont été établies par LA POSTE. (article remplacé par la loi du 21/03/91)"
- Article 196 de la loi portant organisation du secteur public du crédit : "Les copies photographiques, microphotographiques, magnétiques, électroniques ou optiques des documents détenus par les établissements publics de crédit (...), par les établissements privés de crédit (...) ou par les entreprises d'assurances (...) font foi comme les originaux, dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été établies par une de ces sociétés ou sous son contrôle. Le Roi peut fixer les conditions et les modalités de l'établissement de ces copies.
Les reproductions qui en sont délivrées doivent être certifiées conformes par un agent délégué à cette fin et revêtues du sceau de la société."
- Article 103bis de la loi relative aux opérations financières et aux marchés financiers (loi du 04/12/90) : "Les copies photographiques, microphotographiques, magnétiques, électroniques ou optiques des documents détenus par les [sociétés de bourse belges, les établissements boursiers étrangers, les sociétés de la bourse de valeurs mobilières, ...] font foi comme les originaux, dont elles sont présumées, sauf preuve contraire, être une copie fidèle lorsqu'elles ont été établies par un intermédiaire, une société de la bourse de valeurs mobilières, la Caisse d'intervention ou un des organismes précités ou sous leur contrôle. Le Roi peut fixer les conditions et les modalités de l'établissement de ces copies.

Les reproductions qui en sont délivrées doivent être certifiées conformes par un agent délégué à cette fin et revêtues du sceau de l'intermédiaire, de la société de la bourse de valeurs mobilières, de la Caisse d'intervention ou de l'organisme susvisé. (...) (article inséré par la loi du 28/07/92 et complété par la loi du 06/08/93)

- Article 18bis de la loi relative aux allocations aux handicapés (loi du 27/02/87) : "Les copies photographiques, microphotographiques ou par moyen électronique des documents détenus par le Service des allocations aux handicapés font foi comme les originaux, si elles ont été établies par ce service ou sous son contrôle." (article inséré par la loi du 22/12/89).
- Article 173ter de l'arrêté royal relatif aux allocations familiales (A.R. du 19/12/39) : "Les copies photographiques, microphotographiques ou par moyen électronique des documents détenus par les organismes d'allocations familiales et par le Service allocations familiales du Ministère de la Prévoyance sociale font foi comme les originaux, si elles ont été établies par ces organismes ou sous leur contrôle." (article inséré par la loi du 29/12/90)
- Article 8 de l'arrêté royal du 22 mars 1993 relatif à la valeur probante, en matière de sécurité sociale, des informations enregistrées, conservées et reproduites par des institutions de sécurité sociale : "Lorsque le Ministre agrée les procédures que les institutions lui ont soumises (...), les informations enregistrées, conservées ou reproduites conformément aux procédures ainsi agréées, de même que leur représentation sur un support lisible, ont valeur probante pour l'application de la sécurité sociale, jusqu'à preuve du contraire."

Dans tous ces textes de loi, on a opté en matière de force probante pour l'assimilation des copies électroniques aux documents originaux. Ce ne sont toutefois que des solutions très fragmentaires dans des secteurs bien spécifiques.

Dans chaque département, il convient néanmoins d'examiner quels articles doivent être modifiés de manière à ne pas empêcher le recours à la télématique en général et aux signatures digitales en particulier.

Conclusion : chaque membre du Conseil des Ministres, pour les matières qui ressortissent à son département, fait procéder à l'examen des dispositions légales qui compliquent l'emploi de la télématique en général et des signatures digitales en particulier, et déterminer là où des adaptations sont souhaitables.

4.3 Réglementation des activités des autorités de certification (ci-après dénommées AC)

Comme dit plus haut, une autorité de certification (AC) veille à ce que le lien entre une clé publique et une personne soit contrôlé et confirmé dans un "certificat digital";

Les activités des autorités compétentes en matière de certification doivent-elles faire l'objet d'une réglementation juridique ? Sans doute pas, tant que ces activités se limitent à la délivrance de certificats digitaux à un groupe fermé d'utilisateurs. Une banque, par exemple, peut délivrer des certificats digitaux à ses clients, si bien que ces derniers peuvent en toute sécurité échanger du courrier électronique avec elle, par exemple sur Internet. Les banques peuvent également confier ce rôle à une AC commune qui délivre les certificats aux clients de toutes les banques affiliées.

De même, une entreprise peut délivrer des certificats à son personnel ou à ses agents. Il n'est sans doute pas nécessaire de réglementer ces formes de certification à l'usage de groupes d'utilisateurs fermés. Dans ce cas, la plupart du temps on certifie en premier lieu l'appartenance d'une personne au groupe en question et le fait qu'elle dispose dans ce cadre de certaines compétences : une banque certifie que monsieur X est titulaire du compte 123 et peut, au moyen de sa signature digitale, effectuer des opérations sur ce compte; une entreprise certifie que madame Y remplit la fonction 456 et que par sa signature digitale elle peut engager l'entreprise pour un montant de 100.000 francs, etc. Si dans ce contexte la validité d'une signature digitale donne matière à contestation, on pourra toujours se fonder sur ce qui a été convenu entre les parties à cet égard.

En revanche, si des certificats sont délivrés au public en général, on se trouve confronté à un autre cas de figure. Ici, on certifie en premier lieu que monsieur Z, au moyen d'une clé publique qui lui est attribuée ou qu'il a lui-même produite, est véritablement monsieur Z et que monsieur Z existe effectivement. En d'autres termes, dans ce contexte, le certificat a pour but de permettre, en garantissant un degré de sécurité élevé, que des personnes qui n'ont jamais eu de contact puissent néanmoins faire des transactions sur la base de leurs signatures digitales respectives. C'est typiquement le cas en ce qui concerne les commandes de biens ou de services sur Internet. En l'absence de certification, on ne peut jamais exclure que la signature électronique qui figure au bas du bon de commande n'appartient pas à une personne existant réellement..

Comment une AC peut-elle être certaine que monsieur Z existe et qu'il n'est pas une personne fictive ? On peut, par exemple, le vérifier en cherchant dans l'annuaire téléphonique les coordonnées de monsieur Z. Ce procédé n'offre toutefois pas de garantie suffisante parce que monsieur Z a peut-être un numéro privé ou n'a pas le téléphone. Il est préférable de demander à monsieur Z de se présenter en personne muni des pièces d'identité nécessaires et de

contrôler s'il détient la clé privée qui correspond à la clé publique produite. L'AC américaine Verisign applique une procédure de comparution personnelle de ce type en collaboration avec l'U.S. Postal Service. Les clients de Verisign peuvent se rendre dans les bureaux de poste munis de leur clé publique afin de faire certifier leur identité. A cet effet, la société belge BelSign veut recourir aux chambres de commerce et d'industrie locales.

Il convient de se demander si de telles procédures de certification privées offrent des garanties suffisantes pour les autorités. En effet, si la validité d'une signature digitale est contestée, un juge devra, le cas échéant, se prononcer sur la valeur du certificat.

La réponse à cette question est généralement la suivante : l'autorité (le juge) peut admettre pareille signature digitale certifiée mais uniquement si la certification émane d'une autorité de certification "agrée". Une AC agréée est dans cette hypothèse une AC à qui les autorités, après un audit minutieux, ont octroyé une licence.

Afin de pouvoir délivrer des licences à des organisations qui agissent en tant qu'AC vis-à-vis du public, il convient d'élaborer un projet de loi réglant notamment les points suivants :

- définition des notions : "signature digitale", "autorité de certification", etc.;
- signature digitale uniquement pour les personnes physiques; aucune reconnaissance des certificats délivrés à des personnes morales;
- formulation du principe selon lequel une AC agréée doit obtenir une licence des autorités;
- effets de la licence quant à la force probante sur le plan juridique de la signature digitale certifiée;
- quelle administration est chargée de délivrer les licences;
- comment la signature digitale de l'AC elle-même est-elle certifiée (par la hiérarchie ou par une certification mutuelle ?);
- à quelles normes de sécurité une AC doit-elle satisfaire afin d'obtenir une licence et comment et par qui ces normes doivent-elles être contrôlées;

- formulation du principe selon lequel, dans le cadre de la reconnaissance, l'AC fait certifier la conformité des techniques de sécurité qu'elle emploie et le produit final qu'elle a généré par une tierce partie indépendante, c'est-à-dire un organisme de certification accrédité;
- quel paquet de tâches minimum une AC doit-elle offrir afin d'obtenir une licence; conditions relatives à la permanence et à la continuité du service;
- contenu (minimum) des certificats délivrés : quelles sont les mentions qui peuvent ou doivent y figurer;
- obligation de l'AC d'informer les demandeurs en ce qui concerne les mesures à prendre en rapport avec l'obsolescence des signatures digitales;
- responsabilité de l'AC et assurance professionnelle obligatoire éventuelle;
- protection de la vie privée lors du traitement de données à caractère personnel par l'AC;
- accès éventuel d'une AC agréée au Registre national afin de contrôler l'identité;
- où le demandeur d'un certificat doit-il se présenter pour faire vérifier son identité (par ex. à l'administration communale du lieu de son domicile ?);
- statut des certificats délivrés par une AC étrangère (conditions d'équivalence);

Conclusion : le Ministre des Affaires économiques et des Télécommunications présentera au Conseil des Ministres, en concertation avec son collègue de la Justice, un projet de loi contenant les principes énoncés ci-dessus.

4.4 Réglementation de l'utilisation des signatures digitales dans le secteur public

Pour les administrations publiques se posent deux questions importantes quant à l'utilisation de la signature digitale.

- quelles règles régiront la signature digitale utilisée par les citoyens dans leurs relations avec les services publics : commune, contributions, sécurité sociale, etc.

- sous quelles conditions des agents des services publics pourront-ils utiliser dans l'exercice de leurs fonctions une signature digitale en lieu et place d'une signature autographe ou de l'apposition d'un cachet.

Ces deux problématiques font dès à présent l'objet du projet pilote "AGORA" dans le cadre du programme pluriannuel de soutien scientifique pour la diffusion des télécommunications géré par les Services fédéraux des Affaires scientifiques, techniques et culturelles (SSTC). Le projet pilote en question est appliqué dans le domaine des déclarations en matière de TVA.

Question 1 : les autorités doivent-elles elles-mêmes délivrer des certificats digitaux ?

Des organisations privées telles que la société anonyme BelSign seront d'ici quelques mois en mesure d'offrir au public des cartes d'identité digitales (dénommées certificats). Les particuliers pourront alors utiliser ces certificats pour des transactions sur Internet ou sur d'autres réseaux. On prévoit que dans les prochains mois d'autres entreprises, notamment Isabel, La Poste et Belgacom, offriront des certificats de ce type. De plus, dans notre pays, les particuliers pourront également obtenir des certificats auprès d'autorités de certification étrangères. Des dizaines d'entreprises offrent déjà ce service sur Internet. Il a été proposé au point 4.3 que les organisations qui veulent délivrer des certificats au public en Belgique aient obtenu une licence des autorités.

Les autorités vont-elles accepter dans leurs relations avec le citoyen (contributions, sécurité sociale, justice, commune, etc.) que celui-ci ait recours à une signature digitale certifiée par une AC agréée ? Ou bien les autorités vont-elles dans le cadre de ces relations exiger une signature digitale certifiée par elles ou par des organismes qu'elles auront chargés de pareille certification ?

Dans la plupart des pays, on semble opter pour la première possibilité. Dans l'hypothèse où, dans le cadre de communications électroniques avec les citoyens, les autorités exigeraient de ceux-ci une signature digitale obligatoirement certifiée par elles ou à leur demande, la libre concurrence entre les autorités de certification privées se trouverait sérieusement perturbée. En effet, dans ce cas peu de citoyens marqueront encore de l'intérêt pour un certificat qu'ils ne pourront pas utiliser également dans leurs relations avec les autorités.

C'est pourquoi il a été proposé de ne pas créer de certificat distinct pour les rapports entre les autorités et les citoyens mais d'utiliser les certificats des autorités de certification agréées par les autorités.

Relation avec la carte d'identité sociale

Actuellement, la carte d'identité sociale est un support électronique qui contient des données d'identification, à savoir les données essentielles pour les rapports que les citoyens entretiennent avec les organismes de la sécurité sociale. Un espace est laissé libre pour ajouter sur la même carte d'autres données, notamment à des fins fiscales. Certaines données sont codées, d'autres par contre ne le sont pas.

On peut se demander si l'on ne pourrait pas faire figurer sur la carte d'identité sociale la clé privée et le certificat délivré par une AC agréée de sorte que cette carte pourrait également être utilisée par le citoyen pour conserver la clé privée. Pour l'instant, la création d'une signature digitale nécessite encore un processeur supplémentaire. A plus long terme, la carte d'identité sociale pourrait être remplacée par une carte à puce à part entière qui permettrait la génération d'une signature digitale.

Question 2 : Certification interne pour les administrations publiques ?

L'introduction de la télématique dans les administrations publiques requiert que les fonctionnaires puissent dans l'exercice de leurs fonctions faire usage de la signature digitale. Un chef de service devra, par exemple, apposer sa propre signature digitale sur les documents administratifs établis par son service. Qui certifiera cette signature ? En principe, comme pour les autres citoyens, c'est une autorité de certification agréée qui procédera à cette certification. Ce certificat ne garantit que le lien entre l'identité personnelle du fonctionnaire et sa clé publique. Un certificat ne donne donc aucune indication quant à la compétence d'un fonctionnaire dans l'exercice de ses fonctions.

Toutefois, certains documents nécessiteront peut-être une délégation expresse confirmant la compétence spécifique du fonctionnaire, par exemple pour signer un document déterminé. Cette délégation est parfois nécessaire pour conférer au document une validité juridique. Il convient toutefois de noter immédiatement que pareilles délégations expresses sont plutôt rares dans le secteur public à l'heure actuelle.

Dans ces circonstances exceptionnelles, le fonctionnaire devra donc ajouter une délégation au document qu'il signe. Cette délégation définira succinctement sa compétence au sein de l'administration publique à laquelle il appartient et portera éventuellement la signature digitale de la personne qui gère cette administration publique : le secrétaire général du département, l'administrateur général du parastatal, etc.

Mode d'octroi des délégations internes dans les administrations publiques

La technique qui vient d'être esquissée nécessite qu'une administration publique mette sur pied le cas échéant une base de données interne avec délégations. Il est probable que cette banque de données peut être créée par une entreprise spécialisée pour l'administration. Chaque membre du personnel qui a besoin d'une délégation interne dans le cadre de sa fonction doit bénéficier d'une clé publique personnelle mentionnant sa fonction et/ou sa compétence. Sur cette délégation est alors apposée la signature digitale de la personne qui gère ladite administration.

La distinction ainsi établie entre la certification interne dans les administrations publiques et la certification de la signature digitale personnelle des fonctionnaires mêmes permet à une personne d'utiliser sa propre clé privée pour signer un document au nom de l'administration. C'est donc avec cette même clé privée que cette personne appose une signature digitale en tant que personne privée, par exemple, pour réserver sur Internet un ticket pour un match de football.

Toutes les personnes physiques désireuses de recourir à la signature digitale, que ce soit à des fins privées ou dans l'exercice d'une fonction publique, doivent donc demander la certification de leur clé publique à une AC agréée. Si ces personnes font partie d'une administration publique, cette clé publique sera liée à une définition de leur fonction. Ainsi, il sera établi un certificat interne sur lequel sera apposé la signature digitale de la personne qui gère ladite administration. Il est à noter que cette solution s'applique également dans n'importe quelle société privée.

Conclusion : étant donné que la technique de la délégation interne dans les administrations publiques qui vient d'être esquissée doit d'abord être sérieusement expérimentée, il convient, outre le projet AGORA, de mettre sur pied quelques projets pilotes dans une ou plusieurs administrations publiques. Ce principe doit être envisagé dans le cadre des initiatives prises par les autorités fédérales à ce niveau, sur la proposition du Ministre de la Politique scientifique.

Conclusion générale

Il est demandé au Conseil des Ministres d'approuver les principes contenus dans la présente note.

Stefaan De Clerck

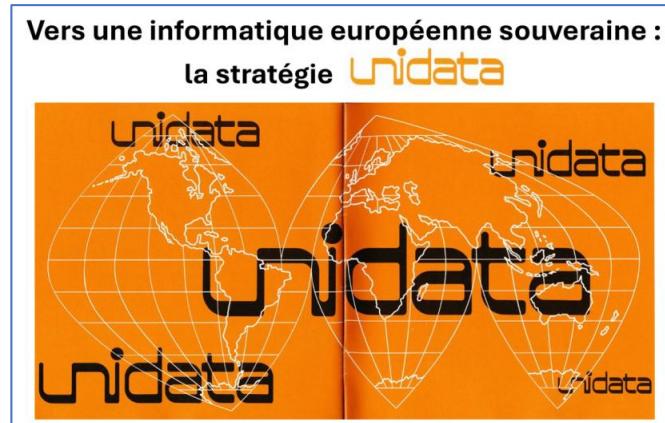
Ministre de la Justice

Elio Di Rupo

Vice-premier Ministre
et Ministre des Affaires
économiques et des
Télécommunications

Documents associés au livre

Annexe 3 au témoignage de Guy Maréchal



Les archives de MBLE & PHILIPS

16 novembre 2004



APPEL à CONTRIBUTION

pour un UN DÉPÔT « M.B.L.E. » AUX ARCHIVES D'ÉTAT ?

Par Guy-Noël Maréchal

Résumé :

Ce qui suit est un appel à contribution pour la constitution d'un fonds sur l'aventure industrielle de M.B.L.E. et pour son dépôt à la section « Archives d'entreprises » aux « Archives générales du Royaume » dénommées maintenant officiellement « Archives d'État ». Jacques Van Haren avait souhaité ce projet en s'appuyant sur les fonds constitués par d'anciens collaborateurs et sur la mémoire de ceux qui ont vécu cette épopée ; la maladie, puis la mort l'ont empêché de le réaliser. Il devrait être possible de faire quelque chose, certainement pas aussi ambitieux, mais réaliste. Nous avons donc pensé que cela valait la peine de vous lancer un appel à contribution ! Le 'Club des anciens de M.B.L.E' a relayé cet appel dans sa revue et Philips Belgique donne son soutien à notre initiative. Ceux qui voudraient déposer des contributions pourront le faire, par exemple, via Adrien Brysse (Philips) ou André Junqué (Le Club).

LE RÊVE

Le projet initial :

À la fin de son mandat comme Administrateur délégué de Philips Belgique, Monsieur Jacques Van Haren, sur suggestion de quelques anciens de MBL (ce qu'il était lui aussi), avait imaginé de demander à un journaliste (ou autre personne à la plume habile) de recueillir des **témoignages** de collaborateurs voulant contribuer par leur mémoire, leur expérience, ... et de rassembler des **témoins** (*documents, plans, produits innovateurs, réalisations ayant fait date, technologies, des photos, des enregistrements sonores de moments d'exception, ou autres*) et sur ces bases de rédiger un texte racontant l'histoire, les prouesses, les joies, les échecs, les réalisations, ... de cette entreprise dont sont fiers tous ceux qui y ont vécu. Une des originalités du projet était que ce texte serait illustré par ces photos, par des photos des témoins technologiques, des documents et enregistrements sonores ; le tout aurait été gravé sur un CD-rom attaché à la couverture d'une petite plaquette de quelques pages présentant le contenu du CD de manière évocative et illustrée. Les émoluments du journaliste et les frais induits lors de cette phase du projet auraient été à charge d'un fonds de mécénat financé par Philips.

Cette plaquette aurait alors été reproduite aux frais des souscripteurs. Enfin, le tout (c'est-à-dire le CD-rom, les témoins technologiques et les originaux des photos et enregistrements) aurait été déposé dans une organisation publique, telle la Bibliothèque royale dans sa section « Archives d'entreprises ».

La table des matières qui avait été envisagée :

À titre d'orientation envisagée pour cibler le travail du journaliste, en quelques minutes, un avant-projet de table des matières avait été rédigé en vrac. Toute suggestion est évidemment bienvenue pour son amélioration.

- **Introduction**

1. Histoire générale et dates clefs

2. Quelques hommes

Marcel Hublou, Jacques Lagrange, Claude Fosseprez, Yvan Hecq, Ladizlas Vorbeitchick, Vitold Bélévitch, ...

3. Quelques projets et produits

Eldo, Textile, Lampes à incandescence, Lampes à vide, Instrumentation nucléaire, spectrométrie de masse, Thermoluminescence, Couches minces, Circuits imprimés,

Ordinateur FNRS - I.R.S.I.A., Assurance de qualité, unidata, ARCADE, Drônes, Radios militaires, Kits, EREA, ...

4. Quelques témoins

Revue MBLE, Allo MBLE, Techniques nouvelles, Horizon, Collection de mémoires mortes, Collection de mémoires vives, Technologies d'UNIDATA, d'ARCADE, CIM-OSA, des couches minces, des circuits imprimés, des amplificateurs paramétriques (et le livre théorique associé), de la gestion de configuration, ainsi que « quelques brevets significatifs » tel celui de la cryptographie à apport nul de connaissances ...

5. Quelques signes

Le livre MBLE progrès, le pavillon de MBLE à l'exposition 58, L'évolution du Logo et du sigle ...

LA RÉALITÉ

Le projet minimum :

Au printemps 2004, Urbain Roosen, André Junqué et Guy Maréchal se sont réunis. Rapidement Adrien Brysse a relayé cette initiative dans Philips. Ils ont évoqué ce projet et ont conclu que le minimum serait de simplement de demander à chacun voulant contribuer de constituer un **fonds** propre constitué de **témoins** (voir plus haut) accompagnés d'un **commentaire écrit** (c'est-à-dire remettant ce témoin dans son contexte et en exprimant sa signifiance) et de **témoignages** (textes rédigés par d'ancien collaborateurs de M.B.L.E.). Puis, les responsables de la section des « Archives d'entreprise » des « Archives d'État » recueilleraient ces fonds. Guy Maréchal se chargera des contacts avec les services des « Archives ». Il a, en effet, recueilli un fonds important au cours de sa longue carrière à M.B.L.E.

Le projet ambitieux :

Il se pourrait que parmi vous quelqu'un (ou une petite équipe rassemblée autour d'un coordinateur) se sente capable de prendre en charge, avec l'appui d'experts des « Archives », la constitution d'un texte de synthèse des divers fonds. Le dépôt aux « Archives » se ferait alors de manière bien plus porteuse d'avenir.

L'appel :

Nous suggérons que chacun d'entre vous se pose sérieusement la question : « *vais-je contribuer ?* ».

Si vous pensez que vous avez de tels témoins (auxquels vous pouvez associer un commentaire écrit) et / ou que vous êtes prêts à rédiger un témoignage écrit, alors prenez contact avec l'une des personnes reprises ci-dessous.

Si vous envisagez de collaborer à une éventuelle cellule de « synthèse », faites-le savoir de même.

Conclusion :

Cet appel est une occasion de ressouder les liens, de vider vos greniers, d'alimenter d'éventuels chercheurs qui voudraient comprendre ce qui a fait notre fierté. De plus, notre appel donne, en quelque sorte, une vie posthume à ce qui a fait une superbe partie de notre vie.

- Adrien Brysse
Philips, Département Juridique, Rue des deux Gares, 80 à B-1070 Bruxelles 02 525 80 22
- Urbain Roosen, Varenberg, 7 à B-3360 Lovenjoel 016 46 14 01
- André Junqué, Rue des Brebis, 25 à B-1170 Bruxelles (Watermael-Boitsfort) 02 672 14 72
- Guy Maréchal, Avenue de Béco, 46 à B-1050 Bruxelles (Ixelles) 02 648 98 28

CONVENTION DE DON D'ARCHIVES

D'une part,

La société anonyme **PHILIPS BELGIUM**, filiale de **ROYAL PHILIPS ELECTRONICS**,

Ayant son siège social 80 rue des Deux-Gares à 1070 Bruxelles,
(en abrégé, Philips)

Représentée par les sous-signés, Messieurs

Julien MICHELS, Chief Officer Corporate Communication & Public Affairs et
Kris VANGILBERGEN, Administrateur,
ADRIEN BRYSSE, Contact pour les archives MBLE

D'autre part,

Les **ARCHIVES GÉNÉRALES DU ROYAUME ET ARCHIVES DE L'ÉTAT DANS LES PROVINCES**

(en abrégé, les Archives de l'État),
représentées par Monsieur Herman COPPENS, Archiviste général du Royaume f.f.,

Attendu :

- Que le **CLUB DES ANCIENS DE MBLE**, ayant son siège social Varenberg 7, à B-3360 Lovenjoel, (en abrégé le Club) a réuni des archives relatives aux activités déployées par la Manufacture belge de Lampes et de Matériel Électronique s.a. (en abrégé, MBLE) ;
- Que la société anonyme **PHILIPS BELGIUM**, filiale de **ROYAL PHILIPS ELECTRONICS**, ayant son siège social rue des Deux-Gares, 80 à 1070 Bruxelles (en abrégé Philips) est aussi dépositaire d'archives de la MBLE ;
- Que le Club et Philips souhaitent verser conjointement ces archives aux Archives de l'État pour constituer un fonds unique sous la dénomination : « **Archives de la Manufacture belge de Lampes et de Matériel électronique s.a.** ». Ces archives concernent la période 1912 à 2004 et totalisent environ 7 mètres linéaires de documents et petits témoins technologiques commentés ;
- Que le Club et Philips se déclarent ouverts à rassembler d'autres documents et témoignages relatifs à MBLE qui leur serait confié, en vue de les intégrer au fonds en début 2005 ;

Ont convenu :

1. Philips déclare par la présente faire don, à titre irrévocable et définitif et transmettre la propriété quitte et libre des archives, visées ci-dessus, aux « Archives de l'État » qui acceptent ;
2. Ce fonds d'archive sera conservé aux Archives générales du Royaume, rue de Ruysbroeck, 2 à 1000 Bruxelles, sous la dénomination : « **Archives de la Manufacture belge de Lampes et de Matériel électronique et de ses prédecesseurs en droit, 1912-2004** ».
3. Les archives visées ci-dessus pourront être données en communication, selon les règles en vigueur aux Archives de l'État, et ce pendant 20 ans après l'année de la signature de la présente déclaration, soit à partir du 1^{er} janvier 2005 jusqu'au premier janvier 2025 ; au-delà de cette date, les « Archives de l'État » disposeront du fonds suivant leur volonté. Les éventuelles enveloppes scellées marquées « CONFIDENTIEL » ne pourront être ouvertes avant la date du 1^{er} janvier 2010, sauf par autorisation écrite de Philips. Les demandes éventuelles sont à adresser. Les demandes éventuelles sont à adresser au responsable du service juridique.
4. Le Club et Philips ont le droit de mandater des représentants autorisés à consulter sur place toutes les archives du fonds unique visé ci-dessus ou d'emprunter celles-ci par lots raisonnables, à leurs propres frais et à leurs risques, à leurs domiciles (pourvu que ces derniers soient situés en Belgique) pour un délai limité à quatre semaines et contre remise d'un récépissé ; le mandat est exprimé par une autorisation écrite préalable et expresse de l'un des donateurs aux personnes qu'il désignera ;

Fait à Bruxelles, le 16 novembre 2004, en quatre exemplaires originaux : deux aux Archives de l'État, un au donateur et un pour information, au Club.

Pour Philips

Kris VANGILBERGEN & Julien MICHELS & ADRIEN BRYSSE

Pour les Archives du Royaume

Herman COPPENS

CONVENTION DE DON D'ARCHIVES

D'une part,

Le **CLUB DES ANCIENS DE MBLE**, ayant son siège social Varenberg 7, à B-3360 Lovenjoel,
(en abrégé, le Club)
représenté par les soussignés Messieurs
URBAIN ROOSEN (Président) et
GUY MARECHAL (Membre)
ANDRE JUNQUE (Membre)

D'autre part,

Les **ARCHIVES GÉNÉRALES DU ROYAUME ET ARCHIVES DE L'ÉTAT DANS LES PROVINCES**
(en abrégé, les Archives de l'État),
représentées par Monsieur Herman COPPENS, Archiviste général du Royaume f.f.,

Attendu :

- Que le Club a réuni des archives relatives aux activités déployées par la Manufacture belge de Lampes et de Matériel Électronique s.a. (en abrégé MBLE) ;
- Que la société anonyme **PHILIPS BELGIUM**, filiale de **ROYAL PHILIPS ELECTRONICS**, ayant son siège social rue des Deux-Gares, 80 à 1070 Bruxelles (en abrégé, Philips) est aussi dépositaire d'archives de la MBLE ;
- Que le Club et Philips souhaitent déposer conjointement ces archives aux Archives de l'État pour constituer un fonds unique sous la dénomination : « **Archives de la Manufacture belge de Lampes et de Matériel électronique s.a.** ». Ces archives concernent la période 1912 à 2004 et totalisent environ 7 mètres linéaires de documents et petits témoins technologiques commentés ;
- Que le Club et Philips se déclarent ouverts à rassembler d'autres documents et témoignages relatifs à MBLE qui leur serait confié, en vue de les intégrer au fonds en début 2005.

Ont convenu :

1. Le Club déclare par la présente faire don, à titre irrévocable et définitif et transmettre la propriété quitte et libre des archives, visées ci-dessus, aux 'Archives de l'État' qui acceptent ;
2. Ce fonds d'archive sera conservé aux Archives générales du Royaume, rue de Ruysbroeck, 2 à 1000 Bruxelles, sous la dénomination :
« Archives de la Manufacture belge de Lampes et de Matériel électronique et de ses prédecesseurs en droit, 1912-2004 ».
5. Les archives visées ci-dessus pourront être données en communication, selon les règles en vigueur aux Archives de l'État, et ce pendant 20 ans après l'année de la signature de la présente déclaration, soit à partir du 1^{er} janvier 2005 jusqu'au premier janvier 2025 ; au-delà de cette date, les 'Archives de l'État' disposeront du fonds suivant leur volonté. Les éventuelles enveloppes scellées marquées « CONFIDENTIEL » ne pourront être ouvertes avant la date du 1^{er} janvier 2010, sauf par autorisation écrite de Philips. Les demandes éventuelles sont à adresser au responsable du service juridique.
6. Le Club et Philips ont le droit de mandater des représentants autorisés à consulter sur place toutes les archives du fonds unique visé ci-dessus ou d'emprunter celles-ci par lots raisonnables, à leurs propres frais et à leurs risques, à leurs domiciles (pourvu que ces derniers soient situés en Belgique) pour un délai limité à quatre semaines et contre remise d'un récépissé ; le mandat est exprimé par une autorisation écrite préalable et expresse du donneur, donnant un droit de consulter sur place les archives visées ci-dessus aux personnes qu'il désignera.

Fait à Bruxelles, le 16 novembre 2004, en quatre exemplaires originaux : deux aux Archives de l'État, un au donneur et un, pour information, à Philips.

Pour le Club
Urbain Roosen & Guy Maréchal & André Junqué

Pour les Archives du Royaume
Herman COPPENS

- ¹ Photo de l’ODHNER de ma collection ! Elle fonctionne toujours parfaitement !
- ² https://fr.wikipedia.org/wiki/Architecture_de_von_Neumann
- ³ Wikipédia : [https://fr.wikipedia.org/wiki/Alg%C3%A8bre_de_Boole_\(logique\)](https://fr.wikipedia.org/wiki/Alg%C3%A8bre_de_Boole_(logique))
- ⁴ <https://upload.wikimedia.org/wikipedia/commons/f/f0/IBM650.jpg>
- ⁵ https://www.ibm.com/ibm/history/exhibits/650/650_intro.html
- ⁶ https://www.ibm.com/ibm/history/exhibits/650/650_intro.html
- ⁷ https://fr.wikipedia.org/wiki/Code_source
- ⁸ <http://aubertrain.com/ponts-m%C3%A9talliques.html> https://fr.wikipedia.org/wiki/Pont_m%C3%A9tallique
- ⁹ <https://histoiresdeliege.wordpress.com/2020/03/30/le-pont-albert-ier/>
- ¹⁰ <https://histoiresdeliege.wordpress.com/2020/03/30/le-pont-albert-ier/>
- ¹¹ <https://histoiresdeliege.wordpress.com/2020/03/30/le-pont-albert-ier/>
- ¹² Implicitement, ceci signifie qu'en 1967 le BEO n'est pas encore créé, mais que Claude Fosseprez s'active à sa création.
- ¹³ G. N. Maréchal, Proceedings of the « NUCLEX-66 », ST N°7b / 21
- ¹⁴ Christian Derouck était un brillant ingénieur qui fera une carrière remarquable dans MBLE. En particulier c'est lui qui fera de l'usine d'Herbette l'un des centres mondiaux des circuits imprimés multicouches à trous métallisés. Lors de la vente à Thomson des activités militaires de mble, il en deviendra le directeur. Christian était un merveilleux pianiste amateur. Il avait la chance d'avoir pu acquérir un Bossendorfer, le piano idéal pour jouer Brahms ou Schumann.
- ¹⁵ À cette époque les contrats d'engagement des ingénieurs précisait que les éventuels revenus des innovations revenaient exclusivement à l'employeur ! Souvent même le nom des « inventeurs » n'étaient pas cités dans le dépôt de brevet. Dans le cas Westinghouse, l'équipe 'innovante' fut de quatre personnes : J-C. Decroly, J. Vorobeitchik, J-P. Wertz et moi.
- ¹⁶ En particulier le brevet de l'« Amplificateur paramétrique à phase cohérente dégénéré à état solide ».
- ¹⁷ Cette approche de validation et diagnostic fit l'objet d'un brevet qui fut vendu à IBM.
- ¹⁸ Claudine Trullemans m'a toujours impressionné par sa compétence, sa gentillesse, son dévouement, sa fermeté et sa volonté que les textes dont elle était responsable soient exprimés en une langue bien faite (que ce soit en français, anglais ou autre). Je ne fus absolument pas surpris (et je fus très heureux pour eux) quand j'ai appris qu'elle était devenue l'épouse de Chaude Fosseprez !
- ¹⁹ Plusieurs documents continuent à nommer « Electrologica » l'organisation d'Apeldoorn ; d'autres nomment « Philips Data Systems » la 'Product Division' de Philips en charge du segment de marché des ordinateurs.
- ²⁰ <https://hagenbeuk.nl/wp-content/uploads/2021/03/Philips.pdf>
- ²¹ Extrait de « ARCADE » : Computer in Industry 5 (1984) 3 – 20 Elsevier Science Publishers B.V. (North-Holland)
- ²² https://en.wikipedia.org/wiki/Jos%C3%A9_Luis_Encarna%C3%A7%C3%A7%C3%A3o
- ²³ À vérifier
- ²⁴ Information Plan of AT&T NETWORK SYSTEMS NEDERLAND BV (JNL 975-R92-1213) 1992-03-13
- ²⁵ *Innovative Systems Development in Philips : An Entrepreneurial Approach* (R. L Wexelblat April 1989)
- ²⁶ La technologie Beam-Lead est une méthode de fabrication d'un dispositif de raccordement des puces en semi-conducteur. Son application initiale concernait les transistors de commutation au silicium à haute fréquence et les circuits intégrés à grande vitesse.
- ²⁷ Épervier : Revue MBLE Volume 10 N°2 pg 98
- ²⁸ Ne pas confondre avec Crypto AG <https://crypto.ch/en> une firme fondée en Suède 1952 et clôturée en Suisse en 2018. Elle a été en Belgique au centre du scandale MAXIMATOR magnifiquement disséqué par Jean-Jacques Quisquater dans : <https://www.regional-it.be/detached/cruel-paradoxe-de-la-cryptographie-belge-quand-la-biere-maximator-coule-la-belgique-a-grands-flots/>. L'article source est <https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538>
- ²⁹ Théorie du bordel ambiant Roland Moreno Editions Belfond ISBN 2-7144-2483-X
- ³⁰ En fait, les Cartes à puces sont aussi des Tamper Resistant Devices à performances et fonctionnalités limitées !
- ³¹ Le Vicomte Dirk Frimout, né le 21 mars 1941 à Poperinge en Belgique, est le premier astronaute Belge à avoir été dans l'espace.
Il appartient à la génération qui a vu partir les premiers engins spatiaux, tels que le Spoutnik. Passionné de technique depuis son plus jeune âge, il s'est rendu dans le Colorado en tant que chercheur post-doctorant

-
- dans un laboratoire de physique atmosphérique et spatiale en 1972 après avoir obtenu son diplôme d'ingénieur en électronique (1963) et son doctorat en physique appliquée (1970) à l'Université de Gand. Il effectue son vol dans l'espace du 24 mars au 2 avril 1992.
- ³² À cette époque le réseau Internet émergeait et celui des Cyclades était peu connu.
- ³³ ALEXANDRIA par Quentin JARDON Éditions Gallimard ISBN : 978-2-07-285287-9/
- ³⁴ https://fr.wikipedia.org/wiki/Yves_Poulet
- ³⁵ https://fr.wikipedia.org/wiki/Centre_de_recherches_informatique_et_droit
- ³⁶ **ISBN-13** : 978-0679762904
- ³⁷ **ISBN-13** : 978-2221080627
- ³⁸ ISBN-10 3-540-85568-8 Springer Berlin Heidelberg NewYork
- ³⁹ <https://www.unibo.it/sitoweb/fabio.vitali/en>
- ⁴⁰ GOUVERNANCE DE LA SOCIÉTÉ de l'INFORMATION Bruxelles // Presses Universitaires de Namur ISBN 2-8027-1688-3