



# ADELI

La LETTRE n° 46

Janvier 2002

*2001 a vu s'achever les derniers préparatifs du passage à l'euro. Nos systèmes d'information semblent avoir assez bien résisté à ces nouvelles transformations. Deux de nos muses préférées « Gestion du changement » et « Analyse des risques » ne peuvent que s'en féliciter.*

*Vous découvrirez dans le compte rendu de l'Assemblée Générale l'ensemble de nos projets 2002 ; Claire Lassudrie vous invite à participer à l'actualisation du PÉRILoscope publié en 1997. Vous trouverez également dans ce numéro un article de fond sur les notions de base de la signature cryptographique, du numérique à l'électronique, et des réflexions sur le thème de l'innovation, collectées à l'occasion du dernier congrès de l'AFITEP.*

*Bonne année à tous !..▲*

La Lettre est une publication périodique d'**ADELI**, dont la coordination est assurée par **Gilles Trouessin et Martine Otter**.

Pour toute information au sujet d'ADELI :  
**info@adeli.com** ou **01.45.89.02.01**

Pour tout contact au sujet de La Lettre :  
**lalettre@adeli.com**

*ADELI*

*87 rue Bobillot - 75013 Paris - [www.adeli.com](http://www.adeli.com)*

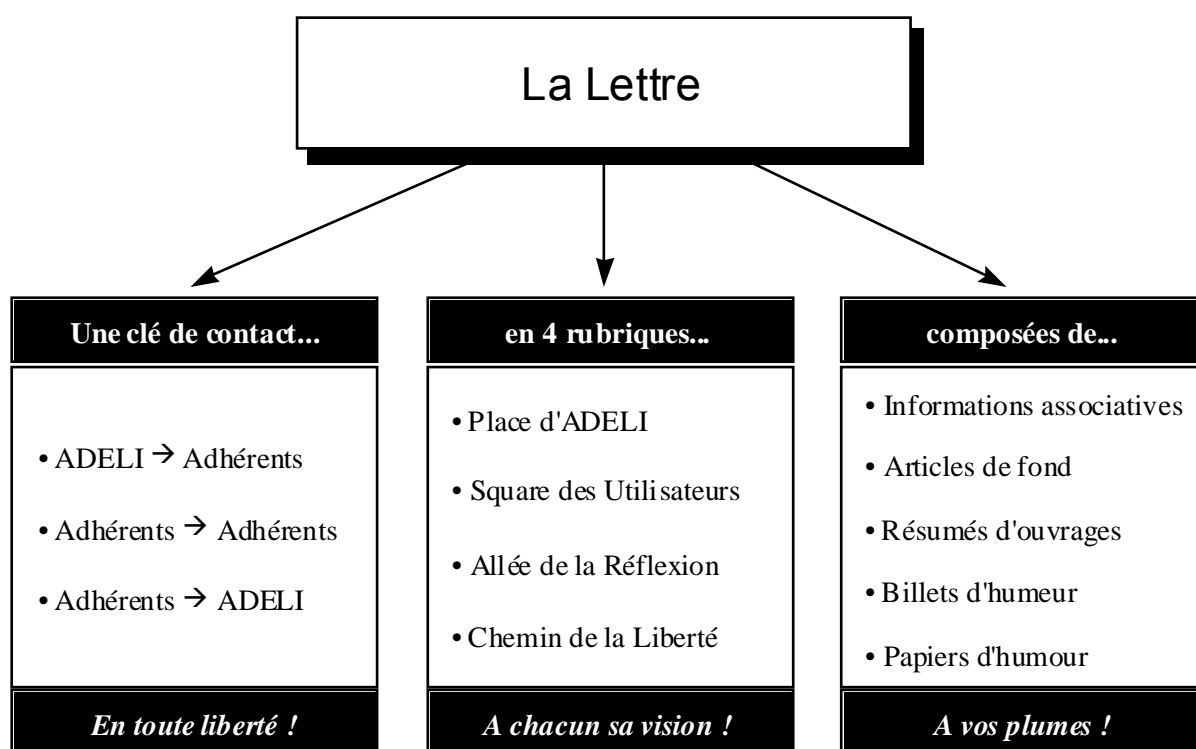
ISSN 1147-5902 © Les Éditions d'ADELI

*Martine Otter*

ADELI est une association qui œuvre pour la maîtrise des systèmes d'information. Elle a été créée en 1978 et compte, à ce jour, 200 adhérents représentant d'entreprises, de SSII, d'éditeurs de logiciels ou consultants indépendants, étudiants, particuliers.

ADELI, régie par la loi de 1901, est rigoureusement indépendante de toute influence commerciale et idéologique. Ses adhérents sont des acteurs impliqués dans les systèmes d'information et concernés par les méthodes et les outils de génie logiciel. L'indépendance des travaux d'ADELI, le charisme et le professionnalisme de ses membres en font un arbitre et une référence dans le domaine des systèmes d'information. ADELI offre les conditions idéales d'une veille technologique efficace et sérieuse, qui en fait le partenaire reconnu du SYNTEC Informatique, de l'AFNOR, du CMSL et de l'AILF.

Lien entre tous les adhérents, La Lettre propose un parcours périodique dans le monde des systèmes d'information.



# Sommaire



*Le mot de la Présidente* \_\_\_\_\_ 4

*Les statuts d'ADELI : texte intégral  
incluant les modifications de décembre 2001* \_\_\_\_\_ 6

*Compte rendu de notre Assemblée Générale  
du vendredi 14 décembre 2001* \_\_\_\_\_ 9

*PERILoscope Le retour ! Appel à (re) création de  
la commission « Management des risques... »* \_\_\_\_\_ 21



*Signature cryptographique,  
du numérique à l'électronique* \_\_\_\_\_ 23

*Management de projet et Innovation  
Quelques pistes de réflexion* \_\_\_\_\_ 29



# Le mot de la Présidente

*Les dernières nouvelles d'ADELI*

## Le nouveau Comité

Le Comité, issu de l'Assemblée Générale qui s'est tenue le 14 décembre 2001, s'est réuni sans plus attendre, le 19 décembre pour élire un nouveau Bureau.

Le Bureau 2002 est composé de la manière suivante :

- Martine Otter, Présidente ;
- Gina Gullà-Menez, Vice-Présidente ;
- Gilles Trouessin, Vice-Président ;
- Michel Demonfaucon, Vice-Président ;
- Alain Coulon, Secrétaire-trésorier.

Le Comité reste constitué de 9 membres. Gérard Saccone et Nguyen Manh Hung rejoignent Bernard Decourbe, et Laurent Hanaud.

Le nouveau Comité s'est réparti l'ensemble des rôles et tâches qui concourent au bon fonctionnement de l'association, de la manière suivante :

- La lettre trimestrielle restera coordonnée par Martine Otter, avec la collaboration de Gilles Trouessin pour la mise en page et d'Alain Coulon pour la logistique et la diffusion ;
- Les commissions seront représentées par leur animateur, la fonction de coordination des commissions revenant de façon collégiale à l'ensemble du Comité ;
- La gestion et la mise à jour du site Web seront assurées par Martine Otter et Alain Coulon ;
- Les tâches de communication avec les associations, la presse et les universités sont réparties entre les membres du Comité ;
- La liaison avec les correspondants étrangers et plus spécialement pour la francophonie sera assurée conjointement par Alain Coulon et Nguyen Manh Hung ;
- Enfin notre secrétaire-trésorier, Alain Coulon, continuera à assurer avec efficacité les tâches administratives et logistiques.

## 2002, année productive

### **Le NORMAscope**

2001 a vu la naissance du MÉTROscope ; 2002 verra celle du NORMAscope.  
Mais peut-être l'avez-vous déjà reçu !

Cet ouvrage, rédigé par Jacqueline Sidi, présidente de la commission de normalisation des technologies de l'information « Ingénierie et Qualité du logiciel et des systèmes » de l'AFNOR et nouvelle adhérente d'ADELI, présente un panorama des normes utilisables dans le cadre d'une approche processus appliquée au développement de logiciels et de systèmes.

## **Les commissions**

Les commissions actives :

- Processus ;
- Qualité ;
- Gestion de configuration
- et Sécurité

poursuivront leurs travaux par la publication de retours d'expériences et d'articles dans La Lettre.

La commission Maîtrise des risques, réactivée, nous promet une nouvelle version du PÉRILoscope.

Un nouveau thème de réflexion, « incidence de la culture dans les différentes étapes des projets Systèmes d'Information », sera exploré par Nguyen Manh Hung et débouchera peut-être sur la création d'une nouvelle commission.

## **L'évolution du site Web**

Notre base de données d'articles de La Lettre, consultables en ligne, nous a déjà amenés quelques nouveaux adhérents et nous a permis d'accroître notre notoriété.

La partie réservée aux adhérents du site Web devrait s'enrichir pour devenir un véritable espace de communication via les forums et la mise en ligne des comptes rendus et documents de travail de nos commissions. L'expérience de création de forums n'est pas actuellement très concluante, faute de participants actifs. Pour améliorer les conditions de leur consultation, nous envisageons de changer d'hébergeur.

## **Les assises d'ADELI ?**

Nous vous présenterons bientôt ce grand projet qui devrait réunir en décembre 2002 adhérents et non-adhérents autour des thèmes processus et systèmes d'informations.

## **Bonne et Européenne année !**

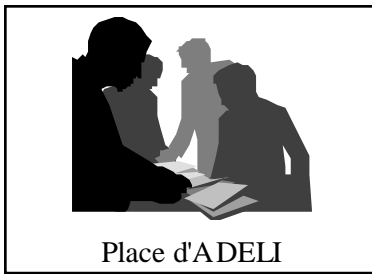
Les nouveaux euros sont encore tous frais dans nos poches et nous n'avons pas encore eu le temps de faire le bilan de nos projets de migration. Il faut dire qu'après le flop tout relatif du passage à l'an 2000, aucun informaticien n'avait plus le courage d'inquiéter ses proches en énumérant les difficultés du passage à l'euro.

J'espère que tout s'est bien passé pour vous, y compris la conversion de vos richesses et de vos désirs.

J'adresse à chacun d'entre vous mes meilleurs vœux personnels et professionnels.

Et, au nom de notre association, j'émetts le vœu que la maîtrise des systèmes d'information fasse encore quelques progrès !

*Martine Otter*  
*Présidente d'ADELI*



# Les statuts d'ADELI

*Texte intégral incluant les modifications de décembre 2001*

*L'Assemblée générale du 14 décembre a approuvé, à l'unanimité, la modification des statuts, en remplaçant la référence au génie logiciel par la référence à la maîtrise des systèmes d'information. À cette occasion, nous vous rappelons ci-dessous l'intégralité des statuts actuels.*

## Titre I - Objet de l'Association

### **Article 1<sup>er</sup>**

Sous la dénomination ADELI, il est fondé, entre les adhérents aux présents statuts, une Association pour la maîtrise des systèmes d'information, à but non lucratif, régie par la loi du 1er juillet 1901 et par le décret du 16 août 1901. La durée de l'Association est illimitée.

### **Article 2 - Objet**

Cette Association a pour objet :

- de faciliter les échanges d'informations entre professionnels et universitaires, autour des méthodes et outils qui contribuent à la maîtrise des systèmes d'information ;
- d'organiser des rencontres, de proposer des sujets d'études et d'échange d'expériences ;
- d'en diffuser les conclusions.

### **Article 3 - Siège**

Le siège de l'Association est situé au **87, rue BOBILLOT, 75013 PARIS**. Il pourra être transféré, en tout autre endroit du territoire français, sur décision du Comité, sous réserve de ratification par l'Assemblée Générale.

## Titre II - Conditions d'admission

### **Article 4 - Membres**

L'Association se compose de membres actifs et de membres honoraires.

Un membre actif est une personne physique ou une personne morale. Une personne morale (entreprise ou service d'une entreprise) est représentée par une personne physique nommément désignée.

Un membre honoraire est une personne physique qui a contribué de façon significative au développement de l'Association.

### **Article 5 - Admission**

L'admission d'un membre actif (personne physique ou morale) est soumise à l'agrément du Comité (qui n'est pas tenu de justifier sa décision) et au versement d'une cotisation annuelle dont le montant est fixé par l'Assemblée Générale.

L'admission d'un membre honoraire est décidée par l'Assemblée Générale, sur proposition du Comité. Un membre honoraire est dispensé de cotisation.

### **Article 6 - Radiation**

La qualité de membre de l'Association se perd par :

- signature d'une lettre de démission ;
- défaut de paiement d'une cotisation annuelle ; la défaillance est constatée par le Comité un mois

- après l'envoi d'un avertissement (lettre recommandée avec avis de réception) resté sans effet ;
- exclusion pour motif grave ; l'exclusion est prononcée par le Comité (à la majorité des deux tiers des présents et représentés) ; la personne concernée ayant été préalablement invitée (par lettre recommandée avec avis de réception) à présenter ses arguments devant le Comité.

## **Titre III - Administration**

### **Article 7 - Comité**

L'Association est administrée par un Comité de 9 à 15 membres actifs, élus pour un an par l'Assemblée Générale, au scrutin secret, lorsqu'un membre en fait la demande. En cas de vacance, le Comité peut pourvoir au remplacement d'un de ses membres par cooptation. Les membres sortants sont rééligibles.

### **Article 8 - Réunions du Comité**

Le Comité se réunit :

- périodiquement, au minimum une fois par trimestre, sur convocation du Bureau ;
- sur demande du quart de ses membres.

La présence ou la représentation du tiers de ses membres est nécessaire pour la validité des délibérations relatives à l'ordre du jour communiqué une semaine à l'avance. Le Comité peut convier à ses réunions toute personne dont la présence lui paraît utile. Tout membre de l'Association peut demander à participer à une réunion, avec voix consultative.

### **Article 9 - Bureau**

Lors de sa première réunion, le Comité élit pour un an, parmi ses membres ayant au moins un an d'ancienneté, un Bureau responsable composé :

- du Président ;
- du Secrétaire ;
- du (ou des) Vice-Président(s) ;
- du Trésorier ;
- des membres responsables d'une mission permanente nécessitant un suivi régulier.

Le **Président** est le premier représentant de l'Association. Il établit le rapport moral annuel soumis à l'approbation de l'Assemblée Générale. Un Vice-Président remplace le Président, en cas d'absence ou d'empêchement.

Le **Secrétaire** est responsable de la gestion administrative de l'Association. Il suit la correspondance et conserve les archives de l'Association. Il tient à jour la liste des adhérents. Il transmet les convocations et les ordres du jour des réunions (Comité, Bureau, Assemblés Générale) ; il en rédige et diffuse les comptes rendus.

Le **Trésorier** est responsable de la gestion financière de l'Association. Il recouvre les recettes et effectue les paiements. Il établit le rapport financier, soumis à l'approbation de l'Assemblée Générale.

Tout autre membre du Bureau est **responsable d'une mission permanente** précise dont il rend compte au Bureau.

### **Article 10 - Réunions du Bureau**

Le Bureau se réunit sur convocation du Président ou à la demande de l'un de ses membres. La présence ou la représentation du tiers de ses membres est nécessaire pour la validité des délibérations relatives à l'ordre du jour communiqué une semaine à l'avance. Le Bureau peut convier à ses réunions toute personne dont la présence lui paraît utile. Les membres du Comité sont invités à participer, avec voix consultative, aux réunions du Bureau.

### **Article 11 - Démission du Bureau**

Au cours de son mandat, le Bureau peut présenter sa démission. Il doit démissionner si la majorité du Comité lui refuse sa confiance lors d'un vote demandé par plus d'un quart de ses membres. Le Comité procède à l'élection d'un nouveau Bureau. Chaque membre du Bureau sortant est rééligible.

### **Article 12 - Assemblée Générale**

L'Assemblée Générale ordinaire comprend tous les membres à jour de leur cotisation à la date de la



convocation. Elle se réunit une fois par an. Elle est convoquée par le Comité qui en fixe la date, le lieu et l'ordre du jour. Elle est appelée :

- à apprécier les rapports (moral et financier) de l'exercice écoulé ;
- à définir les orientations de l'exercice suivant : objectifs, budget prévisionnel, fixation du montant des cotisations, élection des membres du Comité.

Une Assemblée Générale extraordinaire peut, en outre, se réunir :

- sur convocation du Comité ;
- à la demande du quart, au moins de ses membres.

Les Assemblées délibèrent quel que soit le nombre des présents et représentés. Le nombre de pouvoirs détenus par un membre présent est limité à 5. Les délibérations sont prises à la majorité des voix des membres présents et représentés. Le Secrétaire établit un compte rendu validé par le Président.

### **Article 13 - Ressources**

Les ressources de l'Association se composent :

- du montant des cotisations ;
- de dons, de legs et de subventions ;
- de toute autre ressource licite qu'elle pourrait se procurer, dans le cadre de son objet.

L'Association dispose de comptes bancaires réservés à ses propres opérations. En aucun cas, les fonds ne pourront être déposés sur les comptes personnels des membres de l'Association.

Le patrimoine de l'Association sert seul à répondre des engagements contractés sans qu'aucun membre ne puisse être tenu personnellement responsable.

### **Article 14 - Représentation en justice**

L'Association est représentée en justice et dans tous les actes de la vie civile par le Président ou par un membre du Comité spécialement mandaté à cet effet.

## **Titre IV - Modification des statuts et dissolution**

### **Article 15 - Modification des statuts**

Les statuts ne peuvent être modifiés qu'au cours d'une Assemblée Générale dont l'ordre du jour prévoit expressément les nouvelles dispositions des statuts dont la modification est envisagée. La modification ne peut être votée qu'à la majorité des deux tiers de ses membres, présents et représentés.

### **Article 16 - Dissolution**

L'Assemblée Générale appelée à se prononcer sur la dissolution de l'Association est convoquée spécialement à cet effet, par lettre recommandée avec avis de réception. La dissolution ne peut être votée qu'à la majorité des deux tiers des membres, présents et représentés. En cas de dissolution prononcée par l'Assemblée Générale, un ou plusieurs liquidateurs sont nommés. L'actif, s'il y a lieu, est dévolu conformément à l'article 9 de la loi du 1er juillet 1901 et au décret du 16 août 1901.

## **Formalités administratives**

### **Article 17**

Le Président, ou un délégué du Comité, doit effectuer à la Préfecture de Paris, les déclarations prévues à l'article 3 du décret du 16 août 1901 portant règlement d'administration publique pour l'application de la loi du 1er juillet 1901. Ces déclarations concernent notamment : les modifications apportées aux statuts, le changement de titre de l'Association, le transfert de siège social, les changements survenus au sein du Bureau.

*Le Comité d'ADELI*



# Compte rendu de notre Assemblée du vendredi 14 décembre 2001

Notre Association s'est réunie, le vendredi 14 décembre 2001, dans le salon de la Flèche d'or du NOVOTEL de Paris Gare de Lyon. L'Assemblée générale s'est tenue de 15 h. 30 à 17 h. selon l'ordre du jour traditionnel des associations régies par la loi de 1901. Après une pause, la réunion s'est poursuivie, sous forme d'une conférence-débat animée par Gérard Saccone « Processus et maîtrise du système d'information ? Enjeux – outils- pratiques » dont vous trouverez l'essentiel dans une prochaine LETTRE.

## Première partie : l'Assemblée générale annuelle

### 1. Les adhérents présents et représentés

1.1 Les adhérents présents		1.2 Les adhérents représentés	
Nom	Entreprise	Nom	Entreprise
Joseph BARBOU	des COURIÈRES	Gilbert ABOUHAIR	
Lionel BECQUEREAU	Ponthieu Particip.	Edmond BRINDOU	
Jean-Luc BLARY	EPHITEQ	Gérald CROCE	AFPA Lorraine
Dominique BRIOLAT	ESSEC	Claude DASSAS	SYSTÉMIQUE CED
Joseph CENTAURE	2AI	Nicolas DUFFOUR	Conseil sup. Pêche
Antoine CLAVE		Patrick FRANÇOIS	SAPRR
Yves CONSTANTINIDIS		Frédéric GALLEYN	
Alain COULON		Prasong Cuong KHAM	
Bernard DECOURBE		Francis LEY	
Michel DEMONFAUCON	AHIMSA	Gérard MASSI	Crédit Agricole Alsace
Pierre FISCHOF		Alain MUSELET	GFI Informatique
Gina GULLÀ-MENEZ		Vinh Tuong NGUYEN	
Laurent HANAUD		Odile THIÉRY	
Jean JOSKOWICZ	AFISI	Philippe TOUBERT	Software AG
Noé LAVALLÉE		Christophe TOURNIER	
Annie MARCHEIX	AILF	Daniel SAULNIER	
NGUYEN Manh Hung		Alain VAILLY	Fac. Sciences Nantes
Martine OTTER	EXPERIAN	Alain VERNOTTE	
Claude SARRAZIN			
Gérard SACCONNE			
Yann SCOLAN	Mutuelles de Provence		
Nicolas TRÈVES	RDT CONSULTING		
Gilles TROUOSSIN			
Jacky VATHONNE			

À l'occasion de cette manifestation, nous avons reçu des messages sympathiques de plusieurs adhérents : Philippe BASTARD, Geneviève COULLAULT (A Posteriori), Gérard CRAPLET (Groupe Carrefour), Éric HUET (Hôpitaux de Paris), Claude LE BERRE (CCF), Patrice LOLIVIER, Kémal MADDI, Dominique MOLLARD, qui n'ont pu prendre part à cette Assemblée.

## 2. Rapport moral

Après le traditionnel tour de table des participants, Martine OTTER, présidente d'ADELI, présente, à l'aide de visuels vidéo-projetés, le rapport des activités de la période écoulée, depuis notre précédente assemblée du 8 décembre 2000.

### 2.1 Composition du Comité 2001, élu le 8 décembre 2000

Gilbert ABOUHAIR	Alain COULON	Bernard DECOURBE
Michel DEMONFAUCON	Gina GULLÀ-MENEZ	Laurent HANAUD
Martine OTTER	Pascal THYS	Gilles TROUÉSSIN

Patrice LOLIVIER a été coopté le 24 janvier 2001.

Lors de sa réunion du 20 décembre, le Comité avait constitué son Bureau :

Martine OTTER	Présidente
Gina GULLÀ-MENEZ	Vice-Présidente, chargée des commissions
Gilles TROUÉSSIN	Vice-Président, chargé des activités nouvelles
Pascal THYS	Vice-Président, chargé des commissions
Alain COULON	Secrétaire-Trésorier

Le Comité s'est réuni 11 fois, dans les salons du Méridien Montpamasse ou dans les locaux de France Télécom à Issy les Moulineaux, avec une moyenne de 6,5 présents par séance.

### 2.2 La LETTRE

La LETTRE a respecté sa cadence trimestrielle. Quatre numéros ont été diffusés : du n° 42 en janvier 2001 au n° 45 en octobre 2001.

Nos colonnes ont privilégié les thèmes suivants :

- processus (7 articles) ;
- systèmes d'information (6 articles) ;
- sécurité (3 articles) ;
- gestion de configuration (3 articles) ;
- estimation des charges (2 articles).

Le Comité de lecture, animé par Martine OTTER, recueille les projets de communication, sélectionne les articles et suggère des améliorations.

Il est rappelé que les colonnes de La LETTRE sont ouvertes à tous.  
N'hésitez pas à nous proposer vos projets d'articles.

### 2.3 Le site [www.adeli.com](http://www.adeli.com)

Les articles de la LETTRE sont accessibles par un outil de recherche sur mot-clé. Les articles parus depuis plus d'un an, soit plus de 110 articles, sont téléchargeables au format PDF.

Un espace réservé aux adhérents, accessible avec un mot de passe, permet l'accès :

- à l'annuaire détaillé des adhérents ;
- à certains comptes rendus de commissions ;
- à des forums, associés à l'animation des commissions, le premier lancé autour des commissions processus et qualité.

Par suite de l'évolution de l'entreprise qui nous héberge, nous regrettons de ne pouvoir produire, cette année, les statistiques d'accès à notre site.

## **2.4 Les commissions suspendues**

Ces commissions provisoirement fermées, peuvent être de nouveau activées si certains membres souhaitent reprendre les travaux.

### **2.4.1 RSU (Réseau Sémantique Universel) – animation : Jean-Luc BLARY**

Cette commission a été close après publication d'un ensemble de 8 articles, dont « Merise 2000<sup>®</sup> » dans La LETTRE n° 43.

### **2.4.2 Estimation des charges – animation : Alain COULON**

Cette commission a été close après publication d'un ensemble d'articles dressant un panorama de l'état de l'art des méthodes d'estimation de charges et de délais :

- LETTRE n° 35 – avril 1999 – Que sont les estimations devenues ? – Alain COULON
- LETTRE n° 39 – avril 2000 – Estimations de charges : orientations de la commission – Alain COULON
- LETTRE n° 41 – octobre 2000 – Estimations de projets informatiques – Kathleen PETERS
- LETTRE n° 42 – janvier 2001 – Calibrage et étalonnage – Jean JOSKOWICZ
- LETTRE n° 45 – octobre 2001 - Science ou magie ? - Le point sur les estimations des projets logiciels - Nicolas TRÈVES et Alain COULON

### **2.4.3 Administration du système projet – animation : Gilbert ABOUHAR**

Cette commission, annoncée dans la LETTRE N° 43, n'a pas démarré, faute de participants.

## **2.5 Les commissions actives**

### **2.5.1 Outils de gestion de configuration – animation : Michel DEMONFAUCON**

**Participants :**

Bernard DECOURBE, Sylvie FABRY, Chantal TAULEIGNE.

Cette commission se propose de recenser les outils de gestion de configuration, afin de publier un ouvrage dans la lignée de l'AGLoscope et du RÉALiscope.

Un article de réflexion générale sur la gestion de configuration a été publié dans la LETTRE n° 44.

Un guide méthodologique, en deux parties, a été publié, dans les LETTRES n° 44 et 45.

### **2.5.2 Qualité et maîtrise des systèmes d'information – animation Laurent HANAUD**

**Participants :**

Martine OTTER, José RELAND, Jacky VATHONNE

Dans la mouvance de la sortie des nouvelles normes ISO 9000 : 2000, cette commission se propose d'actualiser notre interprétation de l'ISO 9001, pour l'étendre, cette fois, à la globalité du système d'information, incluant l'ensemble des phases, de la conception à la production.

Dans un premier temps, les travaux de la commission Qualité sont communs avec ceux de la commission Processus, afin de répondre à la question :

« Quel modèle de processus adopter pour mettre en œuvre l'ISO 9001 ? »

Les différentes normes et les standards de fait en matière de processus seront examinés sous l'angle de leur adaptation à cet objectif et de leur facilité d'utilisation.

## **2.6 Les commissions nouvelles**

### **2.6.1 Maîtrise des processus – animation Gina GULLÀ-MENEZ**

**Participants :**

Alain COULON, Antoine CLAVE, Bernard DECOURBE, Philippe DELEPLANCQUE, Gérard SACCONI.

Les résultats des travaux de cette commission s'exprimeront dans un ouvrage constitué des chapitres suivants :

- un glossaire ;
- l'état de l'art ;
- un panorama des approches des entreprises, pour la gestion de leurs processus : chaque intervenant témoignera des méthodes et techniques utilisées dans son entreprise ;
- une analyse des retours d'expérience ;
- un état des techniques et des outils.

### **2.6.2 Sécurité(s) et sûreté(s) – Animation Gilles TROUËSSIN**

Cette commission se propose d'approfondir une réflexion sur les thèmes connexes de la sécurité et de la sûreté, trop souvent traités de façon uniquement technique.

Plusieurs articles ont été publiés.

- LETTRE N°42 - Sécurité(s) et sûreté(s) : article introductif présentant les thèmes de réflexion.
- LETTRE N°44 - Sécurité(s) et intimité des données à caractère personnel  
Notions sémantiques et terminologiques relatives à la sécurité (disponibilité, intégrité, confidentialité et auditabilité) et à l'intimité (occultation, anonymisation, pseudonymisation, segmentation) des données à caractère personnel, en général, et de santé, en particulier (dont médicales hospitalières ou ambulatoires).
- LETTRE N°45 - Appel à participations sous diverses formes à la réflexion « sécurité(s) et sûreté(s) ».
- LETTRE N°46 - (à paraître) Notion juridico-technique de « signature électronique ».

### **2.6.3 Risques – Animation Claire LASSUDRIE**

En complément au PÉRILoscope, cette commission projette de constituer un panorama actualisé des approches de management des projets informatiques des entreprises, analyser les retours d'expérience et donner des conseils d'application, fondés sur la démarche proposée par le PÉRILoscope et les pratiques recueillies.

Une grille d'enquête, conçue par la commission, téléchargeable sur le site web, avait été diffusée avec la LETTRE n°40. Une nouvelle diffusion est prévue pour enrichir les retours d'expérience.

Un appel à participation sera publié dans la LETTRE n°46.

## **2.7 Publication du MÉTROscope**

Le MÉTROscope, élaboré sous la direction de Gina GULLÀ-MENEZ, paru en mars 2001, présente :

- l'ensemble des grilles d'analyse ;
- une démarche réactualisée de construction d'indicateurs et tableaux de bord ;
- un panorama des normes existantes dans ce domaine.

Le MÉTROscope publie les travaux restés inédits issus d'un projet européen ESPITI, conduit en 1996-97, par un groupe d'experts, rassemblant une vingtaine de témoignages d'entreprises sur les indicateurs utilisés lors de développements de logiciels.

## 2.8 Activités nouvelles

La veille technologique et la réflexion du Comité se sont développées autour du thème de la **gestion des connaissances**.

Un dîner-débat, organisé par Michel DEMONFAUCON, a réuni autour du thème « **modélisation et connaissance** » une quinzaine d'adhérents et d'invités le 20 juin 2001, lançant ainsi les prémices d'une future commission.

## 3. Rapport financier

Alain COULON, Secrétaire Trésorier d'ADELI, commente les éléments quantitatifs du rapport.

### 3.1 Adhésions

#### 3.1.1 Nombre d'adhérents

Évolution des adhésions, selon notre répartition en trois collèges.

Année	Particuliers	Professionnels	Entreprises	Total	Variation
1996	62	11	118	191	
1997	66	12	112	190	- 0,5 %
1998	53	14	95	162	- 15 %
1999	47	12	88	147	- 10 %
2000	44	10	76	130	- 12 %
<b>2001</b>	<b>48</b>	<b>11</b>	<b>74</b>	<b>133</b>	<b>+ 2 %</b>

Après trois années consécutives d'érosion, nous observons, avec satisfaction, une modeste, mais très encourageante, reprise de la croissance du nombre d'adhérents.

#### 3.1.2 Taux de fidélité

*Pourcentage d'adhérents de l'année n qui renouvellent leur adhésion l'année n+1.*

	97/96	98/97	99/98	2000/1999	<b>2001/00</b>
Entreprises	83 %	79 %	80 %	77 %	<b>92 %</b>
Professionnels	91 %	100 %	100 %	75 %	<b>90 %</b>
Particuliers	89 %	80 %	79 %	89 %	<b>100 %</b>

19 adhérents sur 20 renouvellent leur adhésion l'année suivante. Ce taux de 95 % reste très satisfaisant, pour une association.

#### 3.1.3 Évolution des adhésions 2001 par rapport à celles de 2000

##### 3.1.3.1 Collège des Particuliers : 48 adhérents + 4 par rapport à 2000

Nous comptons 44 adhérents particuliers en 2000.

**42 sur 44 ont renouvelé leur adhésion dans le même collège**

**+ 4 nouveaux particuliers rejoignent ce collège**

Fouad RWAYANE                      Mean CHHOA                      Gilles TROUESSIN  
Kémal MADDI

**+ 1 professionnel rejoint ce collège**

Joseph BARBOU des COURIÈRES

**+ 1 entreprise rejoint ce collège**

IDEAWARE → Pascal THYS

**- 2 particuliers changent de collège**

Laurent KERO                      → Entreprise - Crédit Mutuel de Bretagne  
Geneviève COULLAUT → Professionnel - A posteriori

**3.1.3.2 Collège des Professionnels : 11 adhérents +1 par rapport à 2000**

Nous comptons 10 adhérents professionnels en 2000.

**8 sur 10 ont renouvelé leur adhésion dans le même collège**

**+ 1 particulier rejoint ce collège**

Geneviève COULLAULT

**+ 2 entreprises rejoignent ce collège**

Jean-Luc BLARY - EPHITEQ

Michel DEMONFAUCON – AHIMSA

**- 1 professionnel change de collège**

Joseph BARBOU des COURIÈRES → Particulier

**- 1 professionnel exclu**

Mireille RENNERT – TROIZAIRE

**3.1.3.3 Collège des Entreprises : 74 adhérents – 2 par rapport à 2000**

Nous comptons 76 entreprises adhérentes en 2000.

**67 sur 76 ont renouvelé leur adhésion dans le même collège**

**+ 6 nouvelles entreprises nous rejoignent**

Mutuelle de Provence      Conseil supérieur de la pêche      GEMPLUS

BMCE BANK (Maroc)      ERNST & YOUNG      CUIOP

**+ 1 entreprise rejoint ce collège**

Laurent KERO → Crédit Mutuel de Bretagne

**- 4 entreprises nous quittent**

OPAC      GIE SESAM VITALE      APTITUDE

ORACLE

**- 3 entreprises changent de collège**

IDEAWARE      → Pascal THYS (particulier)

EPHITEQ      → Jean-Luc BLARY (professionnel)

AHIMSA      → Michel DEMONFAUCON (professionnel)

**- 2 entreprises sont exclues**

CEMAGREF      TURBOMECA

**3.1.4 Conclusion**

Les chiffres 2001 semblent satisfaisants. Mais, faute de prosélytisme et de promotion autour d'actions spectaculaires, l'accueil de nouveaux membres reste trop faible pour assurer une véritable croissance de l'association.

**3.2 Résultats comptables (en francs français) :**  
**exercice du 1<sup>er</sup> octobre 2000 au 30 septembre 2001**

CHARGES (dépenses)		Budget en kFRF
Impression des publications	50 214,06	95
Fournitures de papeterie	1 711,00	5
Téléphone (+ poste Sillage)	3 747,26	1
Abonnements	2 735,32	4
Réception	8 967,00	5
AG 2000 (solde)	7 803,17	7
AG 2001 (provision)	3 195,00	3
Site Internet	3 076,38	5
Timbres	15 821,80	20
Taxes	108,90	
Divers	594,89	15
<b>Dépenses</b>	<b>97 974,78</b>	<b>160</b>
<b>Remboursement TVA</b>	<b>9 000,00</b>	<b>20</b>
<b>Total des dépenses</b>	<b>88 974,78</b>	<b>140</b>
<b>Marge</b>	<b>13 268,79</b>	<b>0</b>

PRODUITS (recettes)		Budget en kFRF
Cotisations entreprises 2001	69 243,43	70
Cotisations profession. 2001	5 699,97	5
Cotisations particul. 2001	11 500,02	15
Cotisations entreprises 2000	2 400,00	
Cotisations profession. 2000		
Cotisations particul. 2000	350,00	
Vente ouvrages	2 862,00	0
Droits d'auteur AFNOR	754,40	2
<b>Revenus des activités</b>	<b>92 809,82</b>	<b>92</b>
Intérêts CNEP	3 939,98	3
SICA V Association (+ value)	3 624,29	3
SICA V Latitude (+ value)	1 869,48	2
<b>Revenus financiers</b>	<b>9 433,75</b>	<b>8</b>
<b>Total des recettes</b>	<b>102 243,57</b>	<b>100</b>
Provision METROscope	40 000,00	40

ACTIF en FRF	
38 SICA V Associations à ~ 2 709,17 au 30.09.2001	102 948,38
300 SICA V Latitude à ~ 167,79 au 30.09.2001	50 338,14
CNE (épargne) au 30.09.2001	179 654,29
CCP au 30.09.2001	6 090,25
<b>Report au 30.09.2001</b>	<b>339 031,06</b>

PASSIF en FRF	
38 SICA V Associations à ~ 2 613,79 au 30.09.2000	99 324,09
300 SICA V Latitude à ~ 161,56 au 30.09.2000	48 468,66
CNE (épargne) au 30.09.00	171 714,31
CCP au 30.09.2000	6 255,21
<b>Report au 30.09.2000</b>	<b>325 762,27</b>
<b>Marge de l'exercice</b>	<b>13 268,79</b>

Nous avons basculé notre comptabilité en euros au 1<sup>er</sup> octobre 2001

ACTIF en EUROS au 1 <sup>er</sup> octobre 2001	
38 SICA V Associations à 413,01 €	15 694,38
300 SICA V Latitude à 25,58 €	7 674,00
CNE (épargne)	27 388,12
CCP	928,46
<b>Report au 1.10.2001</b>	<b>51 684,96</b>



## 4. Actualisation des statuts

La dernière refonte des statuts remonte à décembre 1996. Depuis, les activités de l'association ont débordé du cadre du génie logiciel pour aborder les aspects de la maîtrise des systèmes d'information. Nous profitons de cette Assemblée pour mettre à jour nos statuts, en remplaçant la référence au génie logiciel par la référence à la maîtrise des systèmes d'information ; cette modification ne touche que les deux premiers articles.

### Article 1<sup>er</sup>

Sous la dénomination **ADELI**, il est fondé, entre les adhérents aux présents statuts, une **Association (française de génie logiciel) pour la maîtrise des systèmes d'information** à but non lucratif, régie par la loi du 1er juillet 1901 et par le décret du 16 août 1901. La durée de l'Association est illimitée.

### Article 2 - Objet

Cette Association a pour objet :

- de faciliter les échanges d'informations entre professionnels et universitaires, autour des méthodes et outils (~~de génie logiciel~~) qui contribuent à la maîtrise des systèmes d'information ;
- d'organiser des rencontres, de proposer des sujets d'études et d'échange d'expériences ;
- d'en diffuser les conclusions.

## 5. Votes

Le rapport moral et le rapport financier sont adoptés à l'unanimité des membres présents et représentés.

La modification des statuts est approuvée à l'unanimité des membres présents et représentés.

## 6. Perspectives 2002

Les activités que nous engagerons en 2002 contribueront à l'affirmation de nos valeurs :

- Partager le plaisir à apprendre et à connaître ;
- Démythifier les apports des nouvelles technologies ;
- Maîtriser la mise en œuvre de leurs applications :
  - -en diffusant des retours d'expériences,
  - -en élaborant des synthèses,
  - -en indiquant des points de repère.

### 6.1 Publication du NORMAScope

#### Mettre en œuvre l'ISO 9000 :2000 et ses processus Application à l'ingénierie du logiciel et des systèmes

Cet ouvrage, rédigé par Jacqueline SIDI, paraîtra sous quelques semaines.

Le NORMAScope présente un panorama complet des normes actuelles et en cours de rédaction, dans le domaine de l'ingénierie du logiciel et des systèmes. Il tente, plus précisément, de répondre aux questions :

- quelles normes pour quelles exigences de l'ISO 9001 ?
- quelles normes pour quels processus ?

### 6.2 Les commissions

Les commissions actives en 2001 s'organisent pour produire leurs premiers résultats concrets au cours de l'année 2002 :

- Qualité ;
- Processus ;
- Gestion de configuration.

Les commissions lancées en 2001 commenceront leurs travaux :

- Risques ;
- Sécurité.

Les publications 2002 continueront à refléter les travaux des commissions :

- soit au travers d'articles de LA LETTRE ;
- soit par des ouvrages de synthèse marquant une étape dans la réflexion des dites commissions.

### **6.3 Les nouveaux projets**

#### **6.3.1 Organisation de dîners-débats**

En accompagnement de la vie des commissions ou sur des thèmes exploratoires ou innovants, comme celui de la gestion des connaissances.

#### **6.3.2 Organisation des assises d'ADELI**

Nous envisageons d'organiser un congrès ADELI, centré sur le thème « Système d'information et processus » au cours du mois de décembre 2002.

Ces assises se dérouleraient sur 2 jours.

#### **6.3.3 Un glossaire**

ADELI envisage de constituer un glossaire pour aider à la compréhension et à la démythification des concepts utilisés dans les milieux informatiques.

### **6.4 Les activités traditionnelles**

#### **6.4.1 La LETTRE trimestrielle**

Ce support de communication, qui semble particulièrement apprécié de ses lecteurs (beaucoup plus nombreux que nos adhérents) continuera à vous informer chaque trimestre :

- en relatant les événements qui marquent la vie de l'association ;
- en jalonnant l'avancement des commissions ;
- en publiant des articles sélectionnés par le Comité de lecture ;
- en vous donnant la parole et en publiant vos écrits ;
- en y glissant une dose d'humour.

#### **6.4.2 Le développement du site web**

Notre vitrine sur le monde internet continuera à s'enrichir. Elle offrira à nos visiteurs de nouveaux éclairages sur les différents aspects de la maîtrise des systèmes d'information, pour les inciter à nous rejoindre.

Ce site évoluera vers plus d'interactivité :

- via l'ouverture de nouveaux forums associés aux commissions ;
- par la publication plus systématique des comptes rendus et résultats intermédiaires de travaux.

## 6.5 Proposition de budget prévisionnel : 1<sup>er</sup> octobre 2001 - 30 septembre 2002

Dépenses prévisionnelles	en k€	Recettes prévisionnelles	en k€
Impressions	10	Cotisations "entreprises"	10
Abonnements	1	Cotisations "professionnels"	1
Timbres	3	Cotisations "particuliers"	2
Salons et Réception	3	Ventes d'ouvrages	1
Téléphone	1	Droits d'auteur AFNOR	1
Internet	1	<b>Revenus des activités</b>	<b>15</b>
Divers	5	Produits financiers	2
<b>Total des Dépenses TTC</b>	<b>24</b>		
Remboursement TVA	- 3		
<b>Total des Charges</b>	<b>21</b>	<b>Total des Produits</b>	<b>17</b>
		<b>Déficit</b>	<b>4</b>

## 7. Élection du comité

Trois membres sortants ne représentent pas leur candidature :

Gilbert ABOUHAIR                      Patrice LOLIVIER                      Pascal THYS

Sept membres sortants renouvellent leur candidature :

Alain COULON                      Bernard DECOURBE                      Michel DEMONFAUCON  
Gina GULLÀ-MENEZ                      Laurent HANAUD                      Martine OTTER  
Gilles TROUÉSSIN

La candidature des adhérents présents à l'assemblée est sollicitée et deux d'entre eux se joignent à la liste initiale :

Gérard SACCONÉ                      NGUYEN Manh Hung

Cette liste de 9 membres est élue à l'unanimité des membres présents et représentés.

Ce nouveau Comité, se réunira le mercredi 19 décembre 2001, chez France Télécom à Issy les Moulineaux.

Au cours de sa première réunion, le Comité élira son Bureau pour l'année 2001.

## 8. Proposition de cotisations 2002

Le montant des cotisations 2002 sera, naturellement, exprimé en euros.

Le Comité poursuit sa politique de stabilité des cotisations depuis 5 ans (la dernière révision remonte à l'exercice 1997).

De plus, les arrondis se feront à la dizaine d'euros, inférieure au résultat de la conversion. Le Comité propose les tarifs suivants pour 2002 :

- Particuliers                      50 €                      45 €(avant le 31/03/02)
- Professionnels                      90 €                      75 €(avant le 31/03/02)
- Établissements d'enseignement                      120 €
- Entreprises                      180 €

Les montants des cotisations sont approuvés à l'unanimité des présents et représentés.

## Deuxième partie, la conférence-débat

De 17 heures à 17 heures 30, les participants ont levé leur flûte de champagne, au succès de notre association, en dégustant quelques petits canapés.

Cet intermède convivial a constitué la chaudière de la réunion. Ceux qui nous ont quittés ont croisé les personnes venues participer à la conférence-débat : Geneviève COULLAULT, Sylvie LAFARGUE, Jacqueline SIDI.

Puis, de 17 heures 30 à 19 heures 45, la conférence, présentée par Gérard SACCONI et animée par Michel DEMONFAUCON s'est tenue dans une ambiance attentive et passionnée qui a canalisé de nombreux échanges constructifs entre le conférencier et la salle.



### ***Processus d'affaire et maîtrise du système d'information : enjeux, outils pratiques***

Le titre de la conférence pourrait constituer, à lui seul, le programme d'un enseignement universitaire de plusieurs années. L'exposé était fort dense et nous en retiendrons quelques lignes directrices :

- La notion de « processus d'affaires » autorise enfin le rapprochement entre le domaine des systèmes informatiques et celui des domaines organisationnels, jusqu'ici peu communicants. Informaticiens et organisateurs pourraient-ils arriver à se comprendre ? Le débat était lancé.
- La modélisation des traitements restait réductrice, car elle ne traduisait pas suffisamment l'aspect dynamique des processus et en masquait la finalité. De même, la modélisation des données, orientée vers la conception des bases de données, masquait la notion plus naturelle de document. Le couple **documents-processus** vient remplacer le modèle **données-traitements**, de façon plus souple et mieux adaptée à la description du fonctionnement de l'entreprise.
- La **notion de processus** « suite semi-ordonnée d'activités concourant à l'obtention d'un bien ou service » a été éclairée par de nombreuses définitions et mise en regard de celle de modèle, qui en apporte une représentation simplifiée (on ne confondra pas le processus lui-même, dans sa complexité, et le modèle qui en fournit une description).

- La **modélisation**, véritable couteau suisse de l' « informaticien-organisateur-qualiticien-systémicien », a été présentée dans ses différentes fonctions d'outil d'étude, d'analyse, de simulation, de description, d'amélioration, de standardisation, de paramétrage, de support de workflow. Différents types de modèles utilisables dans différentes situations ont été (trop) rapidement présentés.
- La question du choix du modèle amenant tout naturellement à poser celle du choix du méta-modèle, nous atteignîmes un niveau réellement méta-physique lorsque fut évoquée la notion de méta-méta-modèle.
- Un ensemble de conseils pratiques nous ramena à nos questions de départ sur le choix des outils (simples logiciels de dessin ? graphes ? modeleurs dérivés des AGLs ? voire méta-modeleurs ?).

Les questions posées étaient pragmatiques : Un modèle peut-il tenir sur une page A4 ? Les utilisateurs peuvent-ils apprendre à lire les modèles ? Un modèle se valide-t-il ? Par quelle méthode ?  
Toutes les réponses ne furent pas apportées. Cet exposé magistral s'acheva sur une invitation que nous ne pouvons que reprendre à notre compte :

### **Rejoignez la commission processus !**

Vous pouvez dès maintenant consulter la présentation de Gérard Saccone sur notre site Web.

## **Troisième partie : le dîner de clôture**

Les conversations, professionnelles et amicales, se sont poursuivies, autour des deux tables qui ont accueilli les convives, invités à partager un dîner.

### **1ère table**

Michel DEMONFAUCON	Martine OTTER	Joseph BARBOU des COURIÈRES
Antoine CLAVE	Lionel BECQUEREAU	Gilles TROUessin
Jacqueline SIDI	Annie MARCHEIX	Alain COULON

### **2<sup>ème</sup> table**

Laurent HANAUD	Noé LAVALLÉE	Gina GULLÀ-MENEZ
Lionel MENEZ	Jean-Luc BLARY	Yves CONSTANTINIDIS
Gérard SACCONNE	Yann SCOLAN	Jean JOSKOWICZ
Guy LAVALLÉE		

*Alain Coulon*  
*Secrétaire d'ADELI*



Square des Utilisateurs

# Signature cryptographique : du numérique à l'électronique

*Après l'article paru dans La Lettre d'ADELI n°42 de janvier 2001, présentant les généralités concernant la sécurité (au sens « security »), la sûreté (au sens « safety ») et la sûreté de fonctionnement (au sens « dependability ») des systèmes d'information, puis l'article paru dans La Lettre d'ADELI n°44 de juillet 2001 évoquant les problématiques de sécurité, sûreté et sûreté de fonctionnement relatives à l'intimité (au sens « privacy ») des données à caractère personnel, ce troisième article se focalise sur un premier niveau de généralités autour des concepts et propriétés de la signature électronique.*

- *Qu'entend-on par signature... cryptographique : signature numérique ? signature électronique ?*
- *Que peut-on faire à l'aide de signature : s'authentifier ? authentifier ? certifier ? accréditer ?*
- *Quelles responsabilités peuvent être supportées : techniques ? organisationnelles ? juridiques ?*

*Cet article présente les quelques fondements historiques et technologiques de la signature avec une vision sur ses retombées envisageables à moyen et long termes. Le lien est fait avec la propriété d'auditabilité, évoquée dans les précédents articles de la commission « Sécurité(s) & Sûreté(s) », comme étant un des piliers de la sécurité des systèmes d'information et donc de la confiance en ceux-ci et de leur maîtrise.*

*L'article qui suit est constitué d'extraits d'un ouvrage à paraître en janvier 2002 aux éditions Eyrolles qui s'intitule « Sécuriser ses échanges avec une PKI : Solutions techniques et aspects juridiques ». Les auteurs sont Thierry Autret d'Ernst & Young, Laurent Bellefin de Solucom et Marie-Laure Oble-Laffaire du cabinet d'avocats HSD Ernst & Young.*

*Nous ne traiterons pas dans cet article des aspects propres à la cryptographie et nous n'introduirons que les bases élémentaires pour comprendre le développement de l'article.*

## Préambule

Un premier article, paru dans la lettre n°42, décrivait comment « Sécurité(s) et Sûreté(s) » participent à la qualité des données, des programmes et des systèmes tout au long du cycle de vie du logiciel.

Après un rappel des concepts et de la terminologie en sûreté de fonctionnement dont la sécurité informatique et la sûreté-innocuité font partie, cet article ouvrait une première réflexion adélienne en la matière. C'était une mise en appétit, riche de termes consacrés et de sigles afin de lancer des appels aux adhérents pour les inviter à : rédiger des articles, proposer des thèmes de réflexions, etc.

Un deuxième article, paru dans la lettre n°44, abordait très précisément la problématique « Sécurité(s) et Intimité... des données à caractère personnel ».

Il replaçait ce sujet dans le cadre générique de la sûreté de fonctionnement, puis dans le contexte général de la sécurité informatique (disponibilité, intégrité, confidentialité et auditabilité) et y ajoutait une réflexion spécifique relative au respect de la vie privée et à la garantie d'intimité électronique, si tant est que cela puisse se résumer ainsi.

Ce nouvel article propose une déclinaison de la propriété d'auditabilité des systèmes d'information par le biais des technologies de signature électronique (originellement appelée signature numérique) à laquelle est désormais attribuée la valeur juridique de force probante depuis l'adaptation, puis son adoption en loi française, de la directive européenne sur la signature électronique.

Une tendance actuelle de la sécurité des systèmes d'information et de communication, notamment dans des domaines d'une sensibilité toute particulière comme ceux de la santé, du social, du bancaire et de la communication électronique en général, consiste à prendre en compte au plus tôt du cycle de

vie du système un autre axe de besoins et d'exigence, pour construire la confiance dans le système.

Cet axe de besoins ou d'exigence correspond à ce que l'on appelait non-répudiation (des échanges), ou encore « contrôle et preuve » : il s'agit de *l'auditabilité* du système. L'auditabilité du système d'information, tant lors de son élaboration, sa construction, sa validation ou son utilisation, consiste à faire en sorte que les décisions prises et les actions entreprises, pour élaborer, construire, valider ou utiliser, soient de confiance au sens de prouvables, tant techniquement que juridiquement.

Lorsqu'il n'y avait que le niveau technique de la preuve (numérique), l'auditabilité était restreinte à de la *traçabilité* (capacité à garder la trace des décisions prises et des actions entreprise), voire à de *l'imputabilité* (capacité à attribuer à un auteur une décision ou à un exécutant une action). En aucun cas il n'y avait certitude sur l'engagement de responsabilité concernant ces décisions et actions, ni donc sur la possible reconnaissance juridique de cette responsabilité.

Depuis que l'on dispose également d'un niveau juridique de la preuve (électronique), l'auditabilité peut être vue comme une propriété englobant l'*opposabilité* (possibilité de présenter une décision ou une action comme étant opposable à son auteur ou son exécutant devant un juge), et aussi l'*irréfutabilité* (possibilité de devenir irréfutable après la prise d'une décision de justice) : au terme « *irréfutable* », un juriste préférerait très certainement le terme « *irréfragable* ».

Cet article présente un tout premier niveau de détail de ce qu'est une signature cryptographique en liaison avec cette progression que nous venons de décrire concernant la propriété d'auditabilité : progression depuis sa restriction (technique) à de la traçabilité et de l'imputabilité, jusqu'à son évolution (juridique) vers de l'opposabilité et de l'irréfutabilité ; d'où notre titre : « *Signature cryptographique : du numérique à l'électronique* ».

## Introduction

La signature électronique est une application très concrète de la cryptographie asymétrique qui fut inventée dans le milieu des années 70. Elle va permettre à tout un chacun de signer un acte électronique avec une valeur juridique identique à celle que l'on accorde actuellement à la version papier de cet acte. Alors que beaucoup d'autres technologies cryptographiques sont utilisées à l'insu même de l'utilisateur, et pour sa plus grande satisfaction, comme le chiffrement pour la confidentialité ou le scellement pour garantir l'intégrité, la signature électronique doit garder une marque de la volonté de s'engager sur ce que l'on signe. A ce titre cet outil va prendre une place importante dans la vie quotidienne des responsables d'entreprises et à terme des citoyens.

« *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose.* » dit le législateur français dans la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Pour le spécialiste de la sécurité ceci permet d'assurer la traçabilité des actes effectués et l'auditabilité des actions. Pour le spécialiste des questions relatives à la vie privée ceci peut également devenir une menace si la signature électronique est utilisée comme un moyen de surveillance des individus par pistage de leurs actions.

Mais ne mélangeons pas tout. La signature électronique n'a pas d'autre finalité que celle de la traditionnelle signature manuscrite, à savoir identifier le signataire d'un acte et manifester son consentement aux obligations qui découlent de cet acte. Le reste est l'application des techniques cryptographiques à d'autres besoins de sécurité.

Après un bref rappel de la cryptographie asymétrique nous citerons les différents mécanismes de sécurité auxquels elle peut s'appliquer. Ensuite nous expliquerons la différence qui existe entre la signature numérique et la signature électronique, puis nous introduirons le certificat de clé publique et décrirons brièvement les infrastructures qui permettent d'assurer la gestion des clés cryptographiques qui y sont liées.

## De la cryptographie à la sécurité

La cryptographie, du grec *kryptos* (κρυπτος), caché, et *graphein* (γραφειν), écrire, est la science des

écritures secrètes. Les cryptographes, qui sont aujourd'hui des mathématiciens, étudient l'ensemble des techniques qui permettent de concevoir des systèmes cryptographiques, en même temps que les moyens de les casser dans le but d'en tester la résistance. La cryptographie est donc indissociable de la cryptanalyse. Les utilisateurs autorisés, c'est-à-dire ceux qui possèdent les secrets, font du chiffrement ou du déchiffrement, alors que les cryptanalystes, ou agresseurs (car ils ne possèdent pas les secrets ni les autorisations pour les détenir), font du décryptage afin de retrouver l'information en clair sans se servir des clés cryptographiques. La logique étymologique voudrait donc que l'on n'emploie jamais le terme de « *cryptage* »<sup>1</sup> et encore moins le néologisme angliciste de « *encryptage* » (mauvaise traduction du terme anglais « *encryption* »), ni même « *enchiffrer* » (très mauvaise traduction de « *to encipher* »).

## **Symétrique et asymétrique**

La cryptographie utilise des données spécifiques qui sont appelées des clés et qui ne sont ni plus ni moins que des suites de caractères traités au niveau le plus élémentaire à savoir le bit. Ces clés sont utilisées dans des algorithmes qui sont des suites organisées d'opérations mathématiques, précisément définies, portant sur des données externes, comme le texte d'un message électronique.

Les systèmes cryptographiques symétriques sont sans doute les plus connus car ils ont été utilisés depuis la nuit des temps pour assurer la confidentialité des messages. La caractéristique principale d'un système symétrique est que l'émetteur et le récepteur utilisent la même valeur de clé. Cette classe d'algorithmes est également appelée « *systèmes à clé secrète partagée* ». Les systèmes bancaires utilisent largement ces techniques aujourd'hui.

Les systèmes asymétriques sont également appelés systèmes à clé publique parce qu'ils sont fondés sur l'existence de deux ensembles de valeurs distinctes : les valeurs qui sont conservées privées par leur propriétaire et celles qui sont rendues publiques. Pour ne pas créer de confusion avec les systèmes symétriques décrits ci-dessus où l'on parle de clé secrète, ici les valeurs qui ne doivent pas être divulguées sont appelées les clés privées.

## **Application à la sécurité**

Les techniques cryptographiques symétriques s'appliquent aux différents besoins de sécurité pour les échanges de données informatisées :

- L'authentification : par challenge cryptographique (défi-réponse), c'est à dire transformation, avec l'aide d'une valeur secrète, d'une valeur (le défi) pour donner une valeur attendue par le vérificateur (la réponse).
- L'intégrité : par calcul d'une empreinte numérique du texte à protéger avec un algorithme résistant aux collisions (risque que deux textes différents donnent la même empreinte).
- La confidentialité : par transformation cryptographique, avec l'aide d'une clé secrète, du texte à protéger.
- La non-répudiation : par calcul d'une valeur propre à l'acteur qui a fait telle ou telle action.

## **Signature et non-répudiation**

Les trois premiers services de sécurité énoncés ci-dessus peuvent être réalisés à l'aide de mécanismes cryptographiques symétriques ou asymétriques. Nous n'entrerons pas dans les détails qui font que tel ou tel algorithme est plus approprié qu'un autre pour chacun des services, mais nous dirons que les techniques asymétriques trouvent une pleine application de leurs propriétés intrinsèques pour garantir la non-répudiation.

Le service de non-répudiation est complexe à présenter. En une approche volontairement simple mais peu rigoriste, nous dirons qu'il s'agit d'apporter à l'un des participants d'un échange des protections dans le cas où l'autre participant viendrait à soulever un litige quant à l'aboutissement de la transaction. Par exemple, un client nie avoir commandé des marchandises car il a changé d'avis, ou un

---

<sup>1</sup> « *cryptage* » est un terme en lui seul contradictoire puisqu'il signifierait : "protéger cryptographiquement (i.e. donc avec l'aide d'une clé cryptographique) sans l'aide d'une quelconque clé cryptographique", par analogie avec « *décryptage* » dont le sens est bien : "déprotéger cryptographiquement par des techniques d'attaques en cryptanalyse, c'est-à-dire sans l'aide d'une quelconque clé cryptographique".



commerçant nie avoir reçu un paiement pour tenter de se faire payer deux fois. Notons au demeurant que la non-répudiation n'est pas un service juridique car tout acte est "*contestable*" devant une cour de justice, au sens où il n'est pas juridiquement recevable, ni donc opposable à son auteur, bien que techniquement fidèle à la réalité et techniquement authentique (i.e., non-répudiable).

En signant numériquement un message avec sa clé privée, le signataire prouve qu'il a participé à ce message et ne peut pas le nier *a posteriori*.

## De la signature numérique à la signature électronique

### Signature numérique

Le principe des systèmes asymétriques est fondé sur la complexité de résolution de certains problèmes mathématiques. Les problèmes complexes auxquels nous faisons référence sont la factorisation d'un nombre entier formé de grands facteurs premiers (RSA, RW), la résolution d'un logarithme discret sur un corps fini (DH, El Gamal, DSA), ou encore la résolution d'un logarithme discret sur une courbe elliptique (ECDSA). Le principe général de tous ces systèmes est que chaque partenaire souhaitant communiquer dispose d'un couple de clés complémentaires, nommées respectivement la clé publique et la clé privée. Les deux éléments du couple sont liés par des caractéristiques mathématiques très précises qui rendent les deux clés complémentaires, et l'ensemble unique pour un partenaire donné.

La particularité principale des systèmes asymétriques est leur capacité à réaliser le mécanisme de signature numérique. La signature est réalisée en utilisant la clé privée du signataire, tous ses partenaires pouvant alors vérifier sa signature en utilisant sa clé publique. Dans tous les protocoles opérationnels, c'est en fait une empreinte numérique, et non pas l'ensemble du document, qui est signée, ce pour des raisons de performance, les algorithmes asymétriques étant très consommateurs de ressources.

Jusqu'ici, nous n'avons évoqué que la signature numérique, mais les débats autour d'Internet et du commerce électronique évoquent plutôt la notion de signature électronique. Est-ce la même chose ?

Pour bien comprendre la nuance entre les deux notions, il convient de rappeler quelques définitions. Voici, selon la norme ISO 7498-2 relative à l'architecture de sécurité pour les systèmes ouverts, la définition de la signature numérique : « *Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon par le destinataire par exemple* »

### Signature électronique

Le 16 avril 1997, la Commission européenne a présenté au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions une communication sur une initiative européenne dans le domaine du commerce électronique. Dans ce texte, tout en mentionnant très clairement le mécanisme de signature numérique qui s'appuie sur la cryptographie asymétrique, le rédacteur fait référence en une seule occasion à la signature électronique en relevant : « *Propre à chaque expéditeur et à chaque message envoyé, la signature électronique est vérifiable et doit être honorée* ». C'est en fait cette appellation qui sera reprise, le 13 décembre 1999, par le Parlement européen et le Conseil de l'union européenne qui fait paraître la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques.

Cette directive ne mentionne plus que la notion de signature électronique qui est définie comme : « *Une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification.* »

Cette définition ne vise qu'à remplir les besoins de l'authentification et, à ce titre, plusieurs technologies pourraient la satisfaire. Il s'agit de l'authentification reposant sur le principe du partage de secret, du calcul d'une donnée biométrique ou encore de la signature numérique. Le texte de cette directive européenne, qui se devait d'être neutre d'un point de vue technologique, ne parle donc pas directement de signature numérique ni même de cryptographie asymétrique, mais il mentionne néanmoins les notions de certificat et de données qu'un tel certificat doit contenir : on parle alors de certificat de clé publique.

Mais le texte introduit en outre la notion de signature électronique « *avancée* » (ou signature électronique « *sécurisée* », dans la transposition française), qui doit satisfaire aux exigences suivantes :

- a) être liée uniquement au signataire ;
- b) permettre d'identifier le signataire ;
- c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et
- d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Pour répondre à ces besoins, qui sont ceux de la non-répudiation, les seules techniques qui puissent être aujourd'hui mises en œuvre sont celles de la signature numérique utilisant la cryptographie asymétrique et les certificats de clé publique.

En résumé, nous pouvons conclure en disant que la signature numérique est une technique informatique alors que la signature électronique est une solution technico-organisationnelle qui répond à un besoin juridique.

## Le certificat de clé publique

Pour pouvoir utiliser une clé publique avec sécurité, il faut donc que le récepteur puisse répondre au moins aux deux questions suivantes : « *à qui appartient cette clé publique ?* » et « *à quoi sert cette clé publique ?* ».

Pour cela, il faut que la clé publique soit accompagnée d'informations descriptives de son propriétaire et de son usage. Cela pourrait alors ressembler à une carte de visite électronique du propriétaire de la clé, sur laquelle le récepteur trouverait le nom, la valeur de la clé publique et son usage.

Mais, de plus, il faut que cette carte de visite soit rendue infalsifiable, sinon une personne malveillante pourrait constituer une fausse carte de visite électronique. En fait, un certificat ressemble en bien des points à une pièce d'identité, carte d'identité ou passeport, dont il constitue une sorte d'équivalent électronique. Dans le monde électronique cette pièce d'identité électronique s'appelle un « certificat de clé publique », plus simplement appelé « certificat ». Un certificat est délivré par une Autorité de Certification (AC).

Le format de certificats aujourd'hui le plus utilisé est le format normalisé par le standard X.509 dans sa version 3. Ce dernier permet l'utilisation des protocoles normalisés ou des applications telles que SSL, IPSec, S/MIME ou SET.

Un certificat X.509 v3 contient les données suivantes :

Version du certificat ( <i>certificate format version</i> )
Numéro de série du certificat ( <i>certificate serial number</i> )
Description de l'algorithme de signature de l'AC ( <i>signature algorithm identifier for CA</i> )
Nom de l'AC qui a généré le certificat ( <i>issuer X.509 name</i> )
Période de validité ( <i>validity period</i> )
Nom de l'utilisateur auquel appartient le certificat ( <i>subject X.509 name</i> )
Clé publique ( <i>subject public key</i> )
Description de l'algorithme à utiliser avec la clé publique ( <i>subject public key information</i> )
Identification possible de l'AC (optionnel) ( <i>issuer unique identifier</i> )
Identification possible de l'utilisateur (optionnel) ( <i>subject unique identifier</i> )
Extensions (optionnel)
Signature de l'AC ( <i>CA signature</i> )

## Infrastructure à clé publique

Comme son nom l'indique, une infrastructure à clé publique (ICP) , ou "*Public Key Infrastructure*"

(PKI) en anglais, est un ensemble de moyens matériels, de logiciels, de composants cryptographiques, mis en œuvre par des personnes, combinés par des politiques, des pratiques et des procédures requises, qui permettent de créer, gérer, conserver, distribuer et révoquer des certificats basés sur la cryptographie asymétrique.

Cette définition empruntée à l'IETF (normalisation de l'Internet) montre qu'une ICP est bien plus qu'un système technique. Les politiques, pratiques et procédures décrivent le cadre de mise en œuvre des moyens dédiés à l'ICP de façon sûre, et qui correspondent à l'attente, en termes de confiance, de ses utilisateurs.

Le guide de l'IETF, *PKI Roadmap*, et certains documents du NIST américain, présentent une ICP comme un ensemble constitué des cinq types de composants suivants :

- Les autorités de certification (AC) qui émettent et révoquent les certificats.
- Les autorités d'enregistrement (AE) organisationnelles qui se portent garantes du lien entre une clé publique, l'identité du porteur du certificat et d'autres attributs.
- Les porteurs de certificats auxquels sont attribués des certificats et qui peuvent signer et/ou déchiffrer des documents.
- Les utilisateurs qui vérifient les signatures numériques ou chiffrent des données, et valident les chemins de certification des certificats à partir d'une AC digne de confiance.
- Le service de publication, qui comprend les répertoires qui contiennent et rendent disponibles les certificats de clés publiques et les listes de certificats révoqués.

## Conclusions

Après les deux articles publiés dans les Lettres d'ADELI n°42 et n°44, cet article est le troisième maillon proposé dans le cadre de notre réflexion adélienne sur la sécurité des systèmes d'information et de communication.

Ce n'est qu'un premier pas vers une meilleure compréhension de l'actualité florissante autour des concepts d'IGC (PKI) et autres notions liées à la signature numérique, désormais devenue signature électronique. Il contribue à la réflexion adélienne dans son ensemble.

D'autres pas de compréhension et de réflexion autour de la signature électronique seront proposés à l'avenir ; ils feront partie de la vie de la commission « Sécurité(s) et Sûreté(s) » pour laquelle les contributions, avis et retours d'expériences et autres interventions des adhérents de l'ADELI sont comme toujours souhaitables et souhaités.

*Avis :*     par courriel :     *thierry\_autret@ernst-young.fr*                     *gilles\_trouessin@ernst-young.fr*  
          par la toile :        [www.ey.com](http://www.ey.com)                             [www.adeli.com](http://www.adeli.com)  
          par téléphone :     +33 (0) 1 4693.8266                     +33 (0) 6 8255.7406  
          par télécopie :    +33 (0) 1 5847.4318                     +33 (0) 1 5847.1033  
          par courrier :     Ernst & Young Audit (France) – Tour Egée – 92037 PARIS La Défense Cedex

***Thierry Autret***  
***Directeur au sein de Ernst & Young Audit***

***Gilles Trouessin***  
***Directeur de Mission au sein de Ernst & Young Audit***  
*Vice-président d’ADELI “en charge de l’innovation”*  
*Responsable de la commission “Sécurité(s) & Sûreté(s)”*

*Quelques noms d’algorithmes de signature :*

RSA (Rivest – Shamir – Adleman) : algorithme cryptographique asymétrique, du nom de ses auteurs.  
RW (Rabin – Williams) : algorithme cryptographique asymétrique, du nom de ses auteurs.  
DH (Diffie – Hellman) : algorithme à l’origine de la cryptographie asymétrique, du nom de ses auteurs.  
El Gamal : algorithme de signature à base de logarithmes discrets, du nom de son auteur.  
DSA (Digital Signature Algorithm) : nom d’un algorithme mondial standardisé de signature numérique.  
ECDSA (Elliptic Curve DSA) : version du DSA reposant sur les courbes elliptiques.



Square des Utilisateurs

# Management de projet et Innovation

## *Quelques pistes de réflexion*

*Le congrès francophone du management de projet, organisé à Paris par l'AFITEP<sup>1</sup>, conjointement avec l'AFAV<sup>2</sup>, s'articulait cette année autour du thème de l'innovation. Je m'étais inscrite au congrès dans l'idée que, peut-être, l'innovation était un moyen de redonner un peu d'attrait au domaine aride des méthodes et de l'assurance qualité. Le programme proposait plusieurs conférences simultanées parmi lesquelles j'ai dû faire un choix, en fonction de mes centres d'intérêt personnel. Ce texte ne se veut pas une synthèse fidèle de l'intégralité des contributions multiples qui ont été formulées au cours du congrès. Il reflète plutôt ma compréhension personnelle du thème de l'innovation, forgée à l'écoute de quelques conférences, et en fonction de ma sensibilité personnelle à certains des champs de réflexion proposés.*

## L'innovation dans l'entreprise

### **Qu'est-ce que l'innovation ?**

L'innovation est synonyme de création et de nouveautés :

- création d'entreprises ;
- création d'emplois ;
- création de valeur.

À coup sûr l'innovation, associée naturellement à l'idée de créativité, fait partie des valeurs positives de notre monde moderne. On en parle souvent comme d'un objectif à atteindre, sans même prendre la peine de la définir, ce qui amène quelques confusions, entre invention et innovation, entre Recherche & Développement et innovation, ou encore entre marketing et innovation.

Il faut par exemple distinguer l'innovation perçue de l'amélioration technique réelle : on citera tel nouveau modèle d'automobile, perçue par le public comme innovante, alors qu'elle était techniquement ringarde et que l'innovation ne résidait que dans l'originalité de la carrosserie.

Le mot innovation vient du bas latin « innovatio » qui signifie « renouvellement ». Le dictionnaire de l'Académie Française définit l'action d'innover comme le fait d'« introduire quelque chose de nouveau dans une pratique, dans un domaine particulier ».

L'idée d'innovation suppose aussi celle d'amélioration. L'innovation serait un type d'amélioration obtenue par changement radical, plutôt que par un processus progressif de changement.

**« Innover c'est introduire dans une organisation quelque chose de nouveau et d'inconnu dans son domaine d'activité lui procurant un avantage concurrentiel. »**

---

<sup>1</sup> Association Francophone de Management de Projet – 17, rue de Turbigo – 75002 Paris – [www.afitep.fr](http://www.afitep.fr)

L'AFITEP rassemble des professionnels issus de multiples secteurs d'activité (banque, assurance, industrie, ingénierie, conseil, informatique, production, recherche, université ...) concernés par le management de projet. L'AFITEP organise depuis 15 ans une grande manifestation : le Congrès annuel du Management de Projet (la [17e édition](#) s'est déroulée à Paris les 6 et 7 Novembre 2001 sur le thème " Innovations et Projets ").

<sup>2</sup> Association Française d'Analyse de la Valeur - 17, rue de Turbigo – 75002 Paris – [www.afav.asso.fr](http://www.afav.asso.fr)

Dans l'entreprise l'innovation s'appliquera effectivement suivant le cas :

- à la création ou au perfectionnement d'un procédé, dans une stratégie de domination par les coûts ;
- ou à celle d'un nouveau produit ou service, dans une démarche de différenciation réactive ou proactive vis-à-vis du client.

L'introduction d'un nouveau procédé n'est pas visible du client, elle permet d'améliorer des facteurs internes tels que le rendement ou la rentabilité. La mise sur le marché d'un nouveau produit est une innovation perçue par le client, à condition qu'elle réponde à un besoin réel de ce dernier.

Le tableau suivant synthétise une typologie des projets innovants, présentée par deux professeurs de l'école Polytechnique de Wrocław<sup>3</sup>, suivant l'orientation de la relation entre produit, marché et processus :

	Produit	Marché	Processus
<b>Logique tirée</b>			
Le marché impose un produit	←		
Le produit nouveau exige un processus nouveau ou modifié			→
Le marché demande un processus nouveau <sup>4</sup>			→
<b>Logique poussée</b>			
Le nouveau produit entraîne la création d'un nouveau processus ou la modification du processus existant			→
Un nouveau produit crée un débouché nouveau		→	
Un nouveau processus s'adresse au marché		←	

<sup>3</sup> Politechnika Wroclawska - Wybrzeże Wyspiańskiego 27 - 50-370 Wrocław – Poland - e-mail: [Sekrpwr@ac.pwr.wroc.pl](mailto:Sekrpwr@ac.pwr.wroc.pl) - [www.pwr.wroc.pl](http://www.pwr.wroc.pl).

*Si vous ne souhaitez pas vous promener trop longtemps sur les pages en langue polonaise, vous pouvez consulter la page « école française » à <http://www.pwr.wroc.pl/sf/>.*

<sup>4</sup> *Ce serait le cas des demandes liées au respect de l'environnement ou au respect de l'éthique : pas de test sur les animaux, pas de travail des enfants...*

## Pourquoi innover ?

Les réponses à cette question sont nombreuses :

- L'innovation liée à des changements technologiques dans les procédés améliore la rentabilité de l'entreprise, de façon plus rapide que par la recherche des dysfonctionnements dans les procédés en usage ou par une meilleure formation du personnel. Elle permet alors de réduire les coûts sans réduire la valeur.
- L'innovation par création de produits facilite le développement de l'entreprise en créant de nouveaux marchés, plutôt qu'en disputant des parts de marché existantes à la concurrence.
- La nouveauté est une qualité en tant que telle, elle répond à un besoin de changement en s'opposant à la routine et à des valeurs démodées de tradition : à prix et qualité égale, le client curieux ou snob essaiera la dernière lessive, la dernière crème anti-ride, la dernière version d'un logiciel<sup>5</sup>.
- Le lancement de produits toujours plus sophistiqués « tirerait l'entreprise vers le haut » et, de fait, l'innovation attire les investisseurs.
- Une image innovante et dynamique permet à l'entreprise d'attirer et de retenir des chercheurs compétents.

## Pourquoi est-ce si difficile d'innover ?

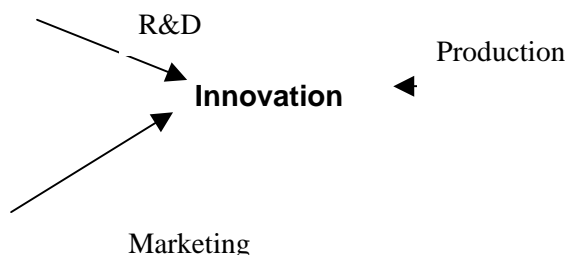
Est-ce si difficile d'innover que le gouvernement français ait cru bon de créer une agence spécialisée, l'ANVAR<sup>6</sup>, pour aider les entreprises à se poser les bonnes questions et à obtenir des financements ?

L'inventeur est souvent incapable de tirer profit de son invention et de la transformer en produit industriel. Il lui faut évaluer la capacité de son invention à répondre aux besoins et aux attentes du marché, repérer les problèmes potentiels liés au fonctionnement technique et à la fabrication, estimer les chances de succès de son invention. Il lui faut aussi trouver les fonds nécessaires aux investissements, contacter des banquiers, en un mot se transformer en chef d'entreprise.

L'invention n'est qu'une invention. L'innovation associe l'idée créative et sa mise en œuvre. La difficulté de l'innovation ne réside pas tant dans la chasse aux bonnes idées que dans le processus de leur transformation en produits et services, et surtout dans la difficile articulation entre la Recherche & Développement et le processus de production.

L'innovation se situe en effet au carrefour de trois processus qu'elle tend à intégrer :

- le processus de recherche et développement ;
- le marketing ;
- la production.



Il convient de distinguer invention et innovation : l'invention ne devient innovation que par la transformation en produit ou service utilisable et utilisé par les usagers. Cela suppose à la fois la mise

<sup>5</sup> Le retour même aux valeurs traditionnelles pourra être présenté comme une innovation, par un habile réhabillage marketing.

<sup>6</sup> ANVAR : L'agence française de l'innovation, est un établissement public à caractère industriel et commercial, placé sous la tutelle des ministères chargés de l'Industrie, des PME et de la Recherche. Elle dispose d'un budget d'intervention annuel d'environ 200 millions d'euros (1,4 milliard de francs) pour apporter financements et conseils aux PME, laboratoires et créateurs qui relèvent le défi technique, commercial, financier et humain de l'innovation.

sur le marché et l'acceptation de la nouveauté par les utilisateurs.

Dans le modèle classique, l'innovation est poussée par la recherche :

- le chercheur ou l'équipe de recherche fait une découverte ;
- un brevet est déposé ;
- l'industrie lui trouve une application.

Dans le modèle de la « nouvelle économie », celui des « start-up », c'est la demande qui tire l'innovation, par l'écoute des clients :

- le marché exprime, de façon explicite ou implicite, des besoins ;
- et l'entreprise se met alors en quête des moyens permettant de répondre à ces besoins : « vous l'avez rêvé, nous l'avons fait ! ».

Innover, c'est créer de la valeur, à partir des bonnes idées, celles des inventeurs mais aussi celles des consommateurs en quête de produits ou services nouveaux.

### **Comment détecter la bonne idée ?**

Y-a-t-il une méthodologie de sélection de la bonne idée ? celle qui est transformable en produit attendu ou au moins acceptable par les clients ?

Pour une entreprise l'innovation n'est bonne qu'au regard de sa stratégie. Le premier critère est celui du délai, le fameux « time to market<sup>7</sup> ». La première question à se poser est celle de la faisabilité : Le produit existe-t-il vraiment ? Y-a-t-il un procédé pour le fabriquer ? Dans des conditions de qualité, coût et délai compatibles avec le marché ?

Il convient de ne lancer en développement que des projets qualifiés, à la fois sur le plan de la faisabilité technique et de l'existence d'un marché demandeur. Cette vérification est quelquefois qualifiée de « double démonstration ».

### **L'innovation suppose une prise de risque**

L'innovation s'accompagne nécessairement d'incertitude. Le lancement d'un nouveau produit constitue une prise de risque nécessaire pour le développement de l'entreprise, à apprécier à sa juste valeur sans le faire supporter par le client. Le risque majeur serait celui de l'innovation zéro, il n'y aurait en effet aucune sécurité à ne rien changer. L'entreprise est obligée d'innover pour survivre.

Il faut rappeler en France que la notion de risque n'est pas forcément négative. On parle en français de capital-risque, alors que l'anglais utilise le terme capital-venture. La distance entre risque et aventure traduit une différence de conception entre les deux cultures du risque. L'Anglo-saxon sécurise son parcours alors que le Français s'inquiète des embûches possibles. Tout un programme !

Quelques chiffres issus du capital-risque : sur 100 idées, 10 seront explorées, une seule étudiée. Sur 3 projets financés, un seul sera rentable.

Le processus d'élimination est nécessaire. Les critères de choix doivent être discriminants.

Une autre spécialité française serait la transformation des succès technologiques en échec commercial, ce qui s'est malheureusement révélé vrai dans l'histoire de l'informatique française. Certains expliquent ce phénomène par l'opposition typiquement française entre les écoles d'ingénieur et les écoles de commerce. Le niveau d'innovation d'une société serait directement lié à son niveau de communication.

Dans le cas du lancement d'un service, la réalisation d'un prototype est rarement possible. Il faut alors construire des plans de secours, en recherchant les solutions standard de remplacement.

---

<sup>7</sup> Temps de mise sur le marché, expression anglo-saxonne passée dans le langage courant du marketing.



## ***L'innovation suppose des interactions entre savoirs***

Le passage de la phase de conception à la phase de production suppose des processus de plus en plus collectifs, des interactions entre les deux types d'ingénierie que sont l'ingénierie de définition (ou conception) du produit, et l'ingénierie de la réalisation (ou production) du produit.

Il s'agit de faire participer le concepteur à la mise en œuvre, et inversement l'homme de production à la conception. Architectes et entreprises de travaux publics gagnent à coopérer, de même que bureaux d'études et fournisseurs de composants.

- Quelles sont les motivations de l'interaction ?
- Quel est le bon moment pour cette coopération ?
- Quels outils utiliser ?

On notera que l'interaction est fortement nécessaire lorsque l'interface entre les deux phases (conception et production) n'est pas réglementée par une norme, ce qui est souvent le cas dans les projets d'innovation, lorsque le savoir n'est pas suffisamment stabilisé. Dans ces cas il est nécessaire de créer une équipe multi compétente, d'effectuer des recrutements croisés. Chacun des deux métiers est validé par l'autre métier, suffisamment tôt, avant que le projet ne soit complètement verrouillé.

## ***Proposition de cycle de vie pour l'innovation***

### **Phase 1 : de la recherche à l'invention**

On distingue classiquement la recherche fondamentale qui vise à une meilleure compréhension des mécanismes de base du monde qui nous entoure, de la recherche appliquée qui aurait pour objectif la production de brevets. L'université serait plutôt spécialiste de la première et l'entreprise de la seconde. Selon le cas les questions de recherche sont ouvertes ou imposées.

La recherche ne produit pas forcément l'invention. Dans un premier temps, elle produit de la connaissance, sur les objets, leurs propriétés, leurs comportements et mécanismes d'inter réaction. On notera que l'entreprise a aujourd'hui pris conscience de la valeur de la connaissance dans ses processus de conception et de production.

La gestion de la recherche consiste à maîtriser cette production de connaissance par l'entreprise, en l'orientant vers la réponse aux besoins exprimés par les autres acteurs du processus d'innovation.

### **Phase 2 : filtrage des idées : de l'invention à l'innovation**

À de multiples reprises, dans le discours des intervenants, nous avons pu noter que parler de Recherche et Développement (R&D) et les réunir dans une même fonction était une aberration. Ces deux activités appartiennent à des mondes de culture et de formation différentes. L'articulation entre la phase de recherche et celle de développement passe par un processus de médiation qui est celui même de l'innovation.

Le processus d'innovation recouvre des activités multiples de mise en relation entre l'offre et la demande que constituent le processus amont de recherche et le processus aval de développement :

- Demandes adressées aux chercheurs, internes ou externes ;
- Production d'idées de produits, prêts à être développés ou à des stades moins avancés de spécification ;
- Diffusion de nouvelles connaissances, traduction des jargons employés par les deux types d'acteurs ;
- Création de nouvelles compétences.

D'un côté la technologie génère des idées (mode push) et de l'autre côté le marketing sélectionne des concepts (mode pull).

Le passage de la phase d'innovation à la phase de développement passe par la qualification des projets, en fonction de la grille de critères retenus.

La décision finale de lancement est conditionnée par l'évaluation des moyens et ressources nécessaires au développement.

### **Phase 3 : Le développement en environnement incertain**

Les projets d'offre innovante posent des problèmes stratégiques : les résultats sont difficiles à appréhender. Les objectifs sont mouvants et viennent se heurter à la résistance au changement et à l'évolution continuelle des exigences. L'incertitude sur les résultats reste forte en phase de développement.

Le processus de développement d'un produit nouveau doit cependant se plier aux contraintes générales du management de projet, notamment le meilleur équilibre possible entre les trois objectifs, quelquefois contradictoires, de qualité, coût et délai. Le profil du manager de projet de développement est orienté méthode, se différenciant de celui de l'animateur du processus d'innovation, orienté créativité.

Il a été rappelé à plusieurs reprises que les outils de planification (Gantt, PERT, WBS) ne sont pas des outils d'aide au management de projet et n'indiquent pas au chef de projet la liste des tâches à exécuter.

Le manager du projet de développement doit structurer méthodologiquement une réalité à venir, et, pour faire face à l'incertain, viser simultanément plusieurs cibles concurrentes. Il peut être ainsi amené à construire une planification en scénario. En l'absence de jalons classiques, il devra se créer des urgences ex-nihilo, qui prendront la forme de revues de projet et seront l'occasion de réévaluer les objectifs. La définition des exigences pourra ainsi s'effectuer de façon progressive. Il importe alors de veiller à la traçabilité de l'évolution des exigences. L'on notera que, dans ce type de projet, les comités de pilotage doivent être, sans doute, plus fréquents que dans des projets classiques et que l'une de leurs fonctions essentielles est le recensement des décisions.

### Proportions relatives des trois phases

Les proportions couramment admises seraient les suivantes :

Recherche	Innovation	Développement
2%	8%	90%

Contrairement à une idée reçue, si l'on veut réduire le coût complet du cycle Recherche/Innovation/Développement, par exemple de 25%, il ne faut pas réduire dans la même proportion le coût de chaque phase, mais bien dépenser plus en amont pour obtenir une baisse des coûts en aval.

Recherche	Innovation	Développement	Total
2	8	90	100
+50%	+50%	-30%	-25%
3	12	60	75

### Peut-on mesurer l'innovation ?

Nous l'avons déjà évoqué, la perception de l'innovation est assez subjective, puisqu'elle dépend de la façon dont un nouveau produit est accepté par le client. L'évaluation de la performance et de la productivité des chercheurs est un sujet délicat.

On peut cependant apprécier la plus ou moins grande atteinte des objectifs fixés par la mesure du portefeuille de projets.

## Innovation et méthode

Innovation et méthode sont dans un rapport antinomique :

- Organiser, c'est réduire l'incertitude ;
- Innover c'est tirer parti de l'incertitude (à ne pas confondre avec inventer, qui consiste à trouver quelque chose de nouveau), mettre en œuvre les inventions en transgressant les règles établies.

La méthode la plus appropriée dans un tel contexte incertain est celle du management par les risques. Il s'agit d'apprendre à gérer l'incertitude, à réagir rapidement à l'imprévu. Il faut un cadre à tout projet, mais le cadre, ici, doit être flexible.

Le cabinet Algoe<sup>8</sup> propose d'élaborer un Master Plan<sup>9</sup> constitué de livrables plutôt qu'un planning de tâches et d'assurer le pilotage des projets d'innovation par l'analyse des risques plutôt que par l'analyse de l'avancement. En matière d'analyse de risques on pourra utiliser différentes approches, telles que l'AMDEC<sup>10</sup>, largement répandue dans les milieux militaires et ceux de l'automobile, ou encore la méthode « futur passé » qui permet d'analyser en se projetant dans le futur les facteurs de succès ou d'échec qui ont conduit à une situation finale d'échec ou de succès.

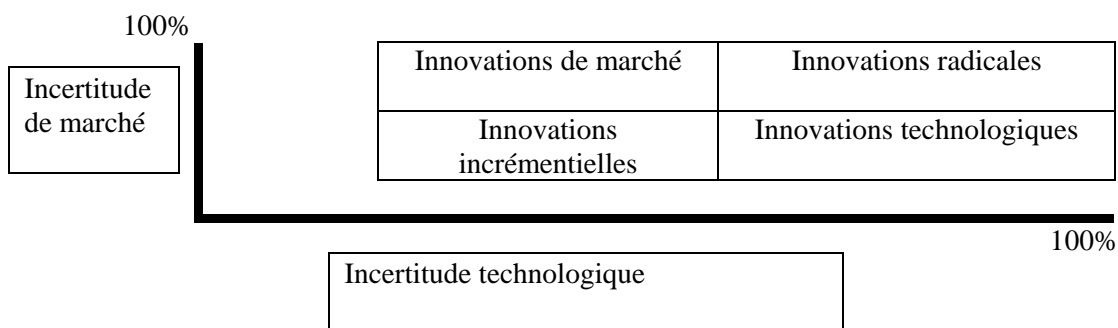
Nous citerons encore les travaux de l'École Polytechnique de Wroclaw sur ce thème de l'évaluation du risque :

L'évaluation du risque d'un projet d'innovation peut s'analyser suivant deux axes :

- L'incertitude de marché (le marché va-t-il accepter le nouveau produit ou le nouveau procédé ?)
- L'incertitude technologique (allons-nous arriver à produire le produit annoncé ?).

On distinguera les innovations où l'incertitude de marché est prépondérante et celle où l'incertitude technologique est majeure. Les innovations radicales combinent ces deux facteurs de risques, alors que les innovations « incrémentielles » ne font que peu bouger ces deux facteurs.

L'intérêt de cette typologie est d'adapter plus finement les critères d'évaluation du risque à la nature du projet.



<sup>8</sup> [www.algoe.com](http://www.algoe.com)

<sup>9</sup> Master Plan pourrait être traduit par « Plan Directeur » ou « Plan Cadre ».

<sup>10</sup> Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités : L'armée américaine a développé l'AMDEC sous la référence Militaire MIL-P-1629, datée du 9 novembre 1949. L'AMDEC est intégré dans le QS 9000, équivalent de l'ISO 9000 pour l'automobile.

## Innovation et système d'information

### ***En informatique, tous les projets sont innovants***

Le sigle NTIC11 traduit bien cette réalité. La technologie et les besoins du marché évoluent si vite que tout projet informatique est quasiment un projet d'innovation. Ce qui se traduit par beaucoup d'échecs, beaucoup de difficultés dans le management des projets, en particulier dans l'estimation des charges et des délais.

Ce caractère innovant serait la principale explication de la « crise » actuelle des méthodes et de la qualité dans nos métiers. L'innovation se poursuit au détriment de la fiabilité, en construisant des systèmes toujours plus complexes et plus fragiles.

La puissance des outils actuels donne aux développeurs une illusion de facilité. On ne perçoit plus toujours la nécessité de concevoir un modèle de données avant de construire une base de données et on se retrouve seulement confronté à des problèmes d'optimisation en phase de montée en charge de l'application.

### ***À propos de la brevetabilité du logiciel***

Il faudrait ici aborder le thème, très conflictuel, de la brevetabilité du logiciel.

Les brevets sont présentés comme un moteur essentiel de l'innovation<sup>12</sup>, en particulier grâce aux NTIC qui en permettent la diffusion et l'exploitation pratique. D'un autre côté, l'utilisation des brevets dans le domaine des NTIC se heurte à de multiples difficultés. Un logiciel ne peut avoir le statut d'invention,<sup>13</sup> et n'est brevetable que s'il est intégré, dans le cadre d'une fonction globale, à un produit lui-même brevetable comme dans le cas des logiciels embarqués<sup>14</sup>.

Les brevets actuellement délivrés aux États-Unis dans le domaine du logiciel servent en réalité plus la protection juridique de quelques grands éditeurs qui verrouillent le marché que le processus d'innovation lui-même.

On pourra lire à ce propos la contribution de l'Isoc-France<sup>15</sup>. Nous aurons probablement l'occasion de revenir sur ce thème dans une prochaine lettre d'ADELI.

---

<sup>11</sup> *Nouvelles Technologies de l'Information et de la Communication*

<sup>12</sup> *Innover grâce au brevet Yann Kermadec – Insep – Vie pratique*

<sup>13</sup> *Article 52 de la convention de Munich de 1973 sur les logiciels*

<sup>14</sup> *On pourra également, sur ce thème, relire les réflexions sur les logiciels libres dans l'article de la Lettre 41 : BSA ou GNU ? Protection et liberté des logiciels, par Michel Demonfaucon, Alain Coulon et Noé Lavallée.*

<sup>15</sup> [www.isoc.asso.fr/PRESSE/ce-brvt.htm](http://www.isoc.asso.fr/PRESSE/ce-brvt.htm)

*L'Internet Society (Isoc - <http://www.isoc.org>) est une association de droit américain à vocation internationale créée en janvier 1992 par les pionniers de l'Internet pour promouvoir et coordonner le développement des réseaux informatiques dans le monde. Elle est aujourd'hui l'autorité morale et technique la plus influente dans l'univers du World-Wide Web.*

*Le Chapitre français de l'Internet Society (Isoc-France), Association régie par la loi de 1901, s'inscrit dans la réalité française et européenne. « Il propose l'organisation d'une initiative fédératrice en France pour que les décideurs et les utilisateurs professionnels, les associations diverses, les organisations et les groupes qui interviennent dans l'Internet, puissent se rencontrer, échanger et faire émerger les contours du Net de demain. »*

## Innovation et qualité

Me voici ramenée à mon point de départ : en quoi l'innovation peut-elle aider l'entreprise dans sa démarche qualité ?

### **Faut-il choisir entre les deux termes : Innovation ou qualité ?**

Si on définit la qualité comme la conformité aux exigences du client, on peut obtenir une meilleure satisfaction en déplaçant le besoin du client vers un produit ou service nouveau, plus facile à produire.

Dans le secteur des logiciels dits « bureautique », nous savons tous que l'innovation n'a pas toujours été, loin s'en faut, synonyme de qualité. Le besoin des clients devrait orienter les éditeurs vers plus de fiabilité et une meilleure ergonomie. L'objectif de certains éditeurs est bien souvent prioritairement la mise sur le marché de nouvelles versions dans des délais n'autorisant pas toujours l'élimination suffisante des bugs. Il est par ailleurs très difficile à l'utilisateur de résister à de telles pratiques : l'achat d'un PC neuf est forcément accompagné de celui des nouvelles versions de logiciel, l'échange de fichiers avec d'autres utilisateurs amène forcément un jour ou l'autre à évoluer vers la version supérieure, afin de ne pas se couper du reste du monde.

Un premier défi consiste donc, de notre point de vue, à maintenir l'exigence de qualité dans les projets innovants.

Mais le véritable défi est bien celui de la mise de l'innovation au service de la qualité, celui du partage des connaissances, de l'évolution des méthodes et processus.

Affaire à suivre, donc.▲

*Martine Otter*  
*Présidente d'ADELI*

### **Bibliographie :**

**L'innovation à tous les étages - Comment associer les salariés à une démarche d'innovation**

de F.Pons M.Ramecourt - Éditions d'Organisation, août 2001

**Innovation et management des connaissances**

de D.Amidon - Éditions d'Organisation, juillet 2001

**Innover dans les services - De l'évident à l'impensable**

de A.Dumont - Village Mondial, avril 2001

**L'entreprise créative**

de A.Robinson S.Stern - Éditions d'Organisation, octobre 2000

**Projet et innovation - méthode Hybrid pour les projets innovants**

de Poulain - Hermès - mars 2000

**Économie des nouvelles technologies – Internet, Télécommunications, Informatique ?**

**Audiovisuel, Transport aérien**

de Michel Volle – Éditions Economica