DÉCISION DU CONSEIL

du 31 mars 1992

en matière de sécurité des systèmes d'information

(92/242/CEE)

LE CONSEIL DES COMMUNAUTÉS EUROPÉENNES,

vu le traité instituant la Communauté économique européenne, et notamment son article 235,

vu la proposition de la Commission (1),

vu l'avis du Parlement européen (2),

vu l'avis du Comité économique et social (3),

considérant que la Communauté a pour mission, par l'établissement d'un marché commun et par le rapprochement progressif des politiques économiques des États membres, de promouvoir un développement harmonieux des activités économiques dans l'ensemble de la Communauté, une expansion continue et équilibrée, une stabilité accrue, un relèvement accéléré du niveau de vie et des relations plus étroites entre les États membres ;

considérant que l'information conservée, traitée et transmise à l'aide de moyens électroniques prend une importance de plus en plus grande dans l'activité économique et sociale ;

considérant que l'introduction de communications globales efficaces et de l'utilisation diffusante du traitement électronique de l'information a mis davantage l'accent sur la nécessité de fournir une protection adéquate ;

considérant que, dans ses débats et résolutions, le Parlement européen a mis l'accent à plusieurs reprises sur l'importance de la sécurité des systèmes d'information ;

considérant que le Comité économique et social a souligné le besoin de traiter des questions relatives à la sécurité des systèmes d'information dans les actions de la Communauté, particulièrement en vue de l'impact de la réalisation du marché intérieur ;

considérant que des actions aux niveaux national, international et communautaire fournissent une bonne base ;

considérant qu'il y a une relation étroite entre les télécommunications, les technologies de l'information, la normalisation, le marché de l'information et les politiques de recherche et développement technologique (R&DT), ainsi que les travaux déjà entrepris dans ces domaines par la Communauté ;

considérant qu'il convient de concerter les efforts en s'appuyant sur les travaux existants aux niveaux national et international et en promouvant la coopération entre les principales parties concernées ; qu'il est dès lors opportun d'y procéder dans le cadre d'un plan d'action cohérent ;

considérant que la complexité de la sécurité des systèmes d'information requiert la mise au point de stratégies permettant à l'information de circuler librement à l'intérieur du marché unique, tout en assurant la sécurité de l'utilisation des systèmes d'information dans l'ensemble de la Communauté ;

considérant qu'il appartient à chaque État membre de tenir compte des contraintes imposées par la sécurité et l'ordre public ;

considérant que les responsabilités des États membres dans ce domaine supposent une approche concertée fondée sur une étroite collaboration avec des hauts fonctionnaires des États membres ;

considérant qu'il y a lieu de prévoir une action comprenant un plan d'action pour une période initiale de vingt-quatre mois et la création d'un comité de hauts fonctionnaires dotés d'un mandat à long terme, en vue de conseiller la Commission sur les actions dans le domaine de la sécurité des systèmes d'information ;

considérant qu'un montant de 12 millions d'écus est estimé nécessaire pour la mise en œuvre de l'action pour une période initiale de vingt-quatre mois ; que, pour 1992, dans le cadre des perspectives financières actuelles, le montant estimé nécessaire est de 2 millions d'écus ;

considérant que les montants à engager en vue du financement du programme pour la période postérieure à l'année budgétaire 1992 devront s'inscrire dans le cadre financier communautaire en vigueur,

DÉCIDE :

Article premier

Une action dans le domaine de la sécurité des systèmes d'information est adoptée par la présente décision. Elle comprend :

— le développement de stratégies globales afin d'assurer la sécurité des systèmes d'information (plan d'action) pour une période initiale de vingt-quatre mois

et

— la création d'un groupe de hauts fonctionnaires dotés d'un mandat à long terme, ci-après dénommé « comité », en vue de conseiller la Commission sur les actions à mener dans le domaine de la sécurité des systèmes d'information.

(1) JO n° C 277 du 5. 11. 1990, p. 18.
(2) JO n° C 94 du 13. 3. 1992.
(3) JO n° C 159 du 17. 6. 1991, p. 38.

Article 2

1. La Commission consulte systématiquement le comité sur les questions ayant trait à la sécurité des systèmes d'information des différentes activités menées par la Communauté, notamment sur la définition de stratégies et de programmes de travail.

2. Comme indiqué à l'annexe, le plan d'action comprend des travaux préparatoires relatifs aux thèmes suivants :

I. développement d'un cadre stratégique pour la sécurité des systèmes d'information ;

II. identification des besoins des utilisateurs et des prestataires de services en matière de sécurité des systèmes d'information ;

III. élaboration de solutions pour certains besoins à court et moyen termes des utilisateurs, des fournisseurs et des prestataires de services ;

IV. élaboration de spécifications, normalisation, évaluation et certification en ce qui concerne la sécurité des systèmes d'information ;

V. développements technologiques et opérationnels en matière de sécurité des systèmes d'information ;

VI. mise en œuvre de la sécurité des systèmes d'information.

Article 3

1. Le montant estimé nécessaire des moyens financiers communautaires pour la mise en œuvre de l'action pour la période initiale est de 12 millions d'écus dont 2 millions d'écus pour 1992 dans le cadre des perspectives financières 1988-1992.

Pour la période d'application ultérieure du programme, le montant devra s'inscrire dans le cadre financier communautaire en vigueur.

2. L'autorité budgétaire détermine les crédits disponibles pour chaque exercice, en prenant en compte les principes de bonne gestion visés à l'article 2 du règlement financier applicable au budget général des Communautés européennes.

Article 4

Un groupe d'experts indépendants procède, pour la Commission, à une évaluation des progrès réalisés au cours de la période initiale. Le rapport de ce groupe, assorti d'éventuelles observations de la Commission, est soumis au Parlement européen et au Conseil.

Article 5

1. La Commission est responsable de la mise en œuvre de l'action. Elle est assistée par un comité consultatif composé de représentants des États membres et présidé par le représentant de la Commission.

2. Le plan d'action est mis en œuvre conformément aux objectifs définis à l'article 2 et il est mis à jour en tant que de besoin. Il expose les objectifs détaillés et les types d'actions à entreprendre, ainsi que les arrangements financiers y afférents. La Commission lance des appels de propositions sur la base du plan d'action.

3. Le plan d'action est mis en œuvre en étroite collaboration avec les acteurs du secteur. Il prend en compte, promeut et complète les activités de normalisation en cours aux niveaux européen et international dans ce domaine.

Article 6

1. La procédure prévue à l'article 7 s'applique aux mesures ayant trait à la politique communautaire dans le domaine de la sécurité des systèmes d'information.

2. La procédure prévue à l'article 8 s'applique :

— à l'élaboration et à la mise à jour du plan d'action visé à l'article 5,

— au contenu des appels de propositions, à l'évaluation des propositions et au montant estimé de la contribution communautaire aux mesures lorsqu'il dépasse 200 000 écus,

— à la coopération d'organisations non communautaires à toute activité au titre de la présente décision,

— aux modalités de diffusion, de protection et de valorisation des résultats des mesures,

— aux mesures à prendre pour évaluer l'action.

3. Lorsque le montant de la contribution communautaire aux mesures est inférieur ou égal à 200 000 écus, la Commission consulte le comité sur les mesures à prendre et l'informe du résultat de son évaluation.

Article 7

Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet dans un délai que le président peut fixer en fonction de l'urgence de la question en cause, le cas échéant en procédant à un vote.

L'avis est inscrit au procès-verbal ; en outre, chaque État membre a le droit de demander que sa position figure à ce procès-verbal.

La Commission tient le plus grand compte de l'avis émis par le comité. Elle informe le comité de la façon dont elle a tenu compte de cet avis.

Article 8

Le représentant de la Commission soumet au comité un projet des mesures à prendre. Le comité émet son avis sur ce projet dans un délai que le président peut fixer en fonction de l'urgence de la question en cause. L'avis est émis à la majorité prévue à l'article 148 paragraphe 2 du

traité pour l'adoption des décisions que le Conseil est appelé à prendre sur proposition de la Commission. Lors des votes au sein du comité, les voix des représentants des États membres sont affectées de la pondération définie à l'article précité. Le président ne prend pas part au vote.

La Commission arrête les mesures envisagées lorsqu'elles sont conformes à l'avis du comité.

Lorsque les mesures envisagées ne sont pas conformes à l'avis du comité, ou en l'absence d'avis, la Commission soumet sans tarder au Conseil une proposition relative aux mesures à prendre. Le Conseil statue à la majorité qualifiée.

Si, à l'expiration d'un délai de trois mois à compter de la saisine du Conseil, celui-ci n'a pas statué, les mesures proposées sont arrêtées par la Commission, sauf dans le cas où le Conseil s'est prononcé à la majorité simple contre lesdites mesures.

Fait à Bruxelles, le 31 mars 1992.

Par le Conseil

Le président

Vitor MARTINS

ANNEXE

Résumé des lignes d'action

ORIENTATIONS POUR UN PLAN D'ACTION DANS LE DOMAINE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

INTRODUCTION

Le plan d'action a pour objectif de développer des stratégies globales visant à fournir aux utilisateurs et aux producteurs d'informations conservées, traitées ou transmises sous forme électronique une protection adéquate des systèmes d'information contre les menaces accidentelles ou volontaires.

Le plan d'action prend en compte et complète les activités de normalisation en cours au niveau mondial dans ce domaine.

Il comprend les lignes d'action suivantes :

— le développement d'un cadre stratégique pour la sécurité des systèmes d'information,

— l'identification des besoins des utilisateurs et des prestataires de services en matière de sécurité des systèmes d'information,

— l'élaboration de solutions pour certains besoins à court et moyen termes des utilisateurs, des fournisseurs et des prestataires de service,

— l'élaboration de spécifications, la normalisation, l'évaluation et la certification en ce qui concerne la sécurité des systèmes d'information,

— des développements technologiques et opérationnels en matière de sécurité des systèmes d'information,

— la mise en œuvre de la sécurité des systèmes d'information.

Le plan d'action est mis en œuvre par la Commission, en association étroite avec les actions connexes dans les États membres et en conjonction avec les actions communautaires de recherche et de développement en la matière.

1. Ligne d'action I : développement d'un cadre stratégique pour la sécurité des systèmes d'information

1.1. *Problème*

La sécurité des systèmes d'information est reconnue comme une qualité partout nécessaire dans une société moderne. Les services d'information électronique requièrent des infrastructures de télécommunications sûres, des matériels et des logiciels sécurisés, ainsi que des conditions d'utilisation et de gestion sûres. Il faut établir une stratégie globale, prenant en compte tous les aspects de la sécurité des systèmes d'information, en évitant toute approche fragmentaire. Toute stratégie pour la sécurité de l'information traitée électroniquement doit tenir compte du désir qu'a chaque société d'agir efficacement, tout en se protégeant, dans un monde en mutation rapide.

1.2. *Objectif*

Un cadre stratégique doit être mis sur pied pour accorder les objectifs sociaux, économiques et politiques avec les choix techniques, opérationnels et juridiques de la Communauté dans un contexte international. C'est aux acteurs du secteur œuvrant ensemble au développement d'une perception commune et d'un cadre stratégique convenu qu'il appartient de trouver l'équilibre délicat entre les divers préoccupations, objectifs et contraintes. Il s'agit d'un préalable pour concilier les intérêts et les besoins tant en matière de conduite d'une politique que de développement industriel.

1.3. *Situation et tendances*

La situation est caractérisée par une prise de conscience croissante du besoin d'agir. Cependant, en l'absence d'une initiative pour coordonner les efforts, il est très probable que des efforts dispersés dans des secteurs variés créeraient une situation *de facto* contradictoire, posant progressivement encore plus de problèmes juridiques, sociaux et économiques.

1.4. *Besoins, options et priorités*

Un tel cadre devrait traiter et examiner l'analyse et la gestion du risque en matière de vulnérabilité des systèmes d'information et services assimilés, l'harmonisation des dispositions législatives et réglementaires relatives à l'usage abusif et le mauvais usage de l'informatique et des télécommunications, les infrastructures administratives, y compris les politiques de sécurité et comment celles-ci peuvent être effectivement mises en œuvre par différentes industries et disciplines, les préoccupations sociales et de protection de la vie privée (par exemple l'application des systèmes d'identification, d'authentification, de non-répudiation et, éventuellement, d'autorisation dans un environnement démocratique).

Des orientations claires doivent être fournies afin d'élaborer des architectures physiques et logiques pour des services d'information distribués sûrs, des normes, des lignes directrices et des définitions pour des produits et services de sécurité garantis, des projets pilotes et prototypes, afin d'assurer la viabilité des diverses structures administratives, ainsi que des architectures et normes relatives aux besoins de secteurs spécifiques.

Il faut encourager une prise de conscience des problèmes de sécurité de façon à inciter les utilisateurs à manifester un souci accru de sécurité en matière de technologies de l'information (TI).

2. Ligne d'action II : identification des besoins des utilisateurs et des prestataires de services en matière de sécurité des systèmes d'information

2.1. *Problème*

La sécurité des systèmes d'information est la condition intrinsèque de l'intégrité et de la crédibilité des applications commerciales, de la propriété intellectuelle et de la confidentialité. Cela pose le problème de l'équilibre délicat — et parfois des choix — entre, d'une part, le soutien à la liberté des échanges et, d'autre part, la protection de la vie privée et de la propriété intellectuelle. Choix et compromis doivent se faire sur la base de l'appréciation globale des besoins et de l'impact des options adoptées en matière de sécurité des systèmes d'information pour satisfaire ces besoins.

Les utilisateurs ont besoin de fonctions de sécurité des systèmes d'information liées aux aspects technologiques, opérationnels et réglementaires. Un travail de recherche systématique sur les besoins en sécurité des systèmes d'information est, par conséquent, essentiel pour l'élaboration de mesures adéquates et efficaces.

2.2. *Objectif*

Il convient d'établir la nature et les caractéristiques des besoins des utilisateurs et des prestataires de services et leurs relations avec des mesures en matière de sécurité des systèmes d'information.

2.3. *Situation et tendances*

Jusqu'à présent, aucun effort concerté n'a été entrepris pour identifier les besoins en évolution rapide des principaux acteurs en matière de sécurité des systèmes d'information. Certains États membres de la Communauté ont identifié les besoins d'harmonisation des activités nationales (spécialement des « critères d'évaluation de la sécurité des TI »). Des critères et des règles d'évaluation uniformes pour la reconnaissance mutuelle des certifications d'évaluation sont de la plus grande importance.

2.4. *Besoins, options et priorités*

Pour traiter des besoins justifiés des acteurs du secteur de manière cohérente et transparente, il apparaît nécessaire d'établir une classification agréée des besoins des utilisateurs et de leurs relations avec la mise en œuvre de la sécurité des systèmes d'information.

Il importe également d'identifier les besoins en matière de législation, réglementation et codes de conduite à la lumière d'une évaluation des tendances en ce qui concerne les caractéristiques et la technologie des services, de définir d'autres stratégies permettant d'atteindre les objectifs au moyen de dispositions administratives, de service, opérationnelles et techniques, et d'évaluer l'efficacité, la convivialité et les coûts des options et des stratégies de rechange en matière de sécurité des systèmes d'information pour les utilisateurs, les prestataires de services et les opérateurs.

3. Ligne d'action III : élaboration de solutions pour certains besoins à court et moyen termes des utilisateurs, des fournisseurs et des prestataires de services

3.1. *Problème*

Il est aujourd'hui possible d'empêcher efficacement l'accès non autorisé aux ordinateurs depuis l'extérieur par le biais de mesures « d'isolement », c'est-à-dire de mesures traditionnelles sur les plans organisationnel et physique. Il en est de même pour les communications électroniques au sein d'un groupe fermé d'utilisateurs opérant sur un réseau dédié. La situation est tout autre lorsque l'information est partagée entre différents groupes d'utilisateurs ou échangée via un réseau public ou d'accès général. La technologie, les terminaux et les services, d'une part, les normes et procédures associées, d'autre part, ne sont généralement pas en mesure, dans ces cas, d'assurer une sécurité des systèmes d'information d'un niveau comparable.

3.2. *Objectif*

L'objectif doit être de fournir, à brève échéance, des solutions qui peuvent répondre aux besoins les plus immédiats des utilisateurs, des prestataires de services et des constructeurs. Cela implique l'utilisation de critères communs d'évaluation de la sécurité des TI. Ces critères doivent être conçus de façon ouverte aux besoins et solutions futurs.

3.3. *Situation et tendances*

Certains groupes d'utilisateurs ont mis au point, pour leur propre usage, des techniques et procédures répondant en particulier aux besoins d'authentification, d'intégrité et de non-répudiation. En général, des cartes magnétiques ou à mémoire sont utilisées. Certains emploient des techniques plus ou moins sophistiquées de cryptographie. Cela implique souvent la définition d'« autorités » spécifiques des groupes d'utilisateurs. Cependant, il est difficile de généraliser ces techniques et méthodes pour répondre aux besoins dans un environnement ouvert.

L'ISO travaille sur une sécurité des systèmes d'information OSI (ISO DIS 7498-2), ainsi que le CCITT dans le contexte du X 400. On peut aussi insérer des segments de sécurité dans les messages. L'authentification, l'intégrité et la non-répudiation sont traitées comme parties des messages (EDIFACT) et de X 400 MHS.

À l'heure actuelle, le cadre juridique de l'EDI (Electronic Data Interchange) en est encore au stade conceptuel. La Chambre de commerce internationale a publié des règles de conduite uniformes pour les échanges de données commerciales via les réseaux de télécommunications.

Plusieurs pays (par exemple l'Allemagne, la France, le Royaume-Uni et les États-Unis d'Amérique) ont mis au point ou élaborent des critères pour évaluer la crédibilité des produits et systèmes de TI et les procédures correspondantes pour procéder à des évaluations. Ces critères ont été coordonnés avec les fabricants nationaux et ils donneront naissance à une gamme élargie de produits et systèmes fiables, à commencer par les produits simples. La création d'organisations nationales chargées de conduire les évaluations et d'octroyer des certifications viendra conforter cette tendance.

La plupart des utilisateurs considèrent que les dispositions en matière de confidentialité sont de moindre importance. Il est toutefois probable que cela changera à l'avenir du fait de la très large diffusion des services de communications avancées et en particulier des services mobiles.

3.4. *Besoins, options et priorités*

Il est essentiel de développer dès que possible les procédures, les normes, les produits et les outils aptes à assurer la sécurité des systèmes d'information en tant que tels (ordinateurs, périphériques) et des réseaux publics de communication. Priorité devrait être donnée à l'authentification, l'intégrité et la non-répudiation. Des projets pilotes devraient être mis en œuvre pour établir la validité des solutions proposées. Les solutions à certains besoins prioritaires dans le domaine de l'EDI sont recherchées dans le cadre du programme *Tedis* et coordonnées dans le cadre plus vaste du présent plan d'action.

4. Ligne d'action IV : élaboration de spécifications, normalisation, évaluation et certification en ce qui concerne la sécurité des systèmes d'information

4.1. *Problème*

Les besoins en matière de sécurité des systèmes d'information se font sentir partout et c'est pourquoi l'existence de spécifications et de normes communes est cruciale. L'absence de normes et spécifications agréées pour la sécurité des TI pourrait constituer un obstacle majeur au progrès des procédés et des services basés sur l'information dans l'ensemble de l'économie et la société. Il faut également prendre des mesures pour accélérer l'élaboration et l'utilisation d'une technologie et de normes dans plusieurs domaines connexes des communications et des réseaux informatisés d'importance capitale pour les utilisateurs, l'industrie et les administrations.

4.2. *Objectif*

Des efforts sont nécessaires pour soutenir et réaliser des fonctions de sécurité spécifiques dans les domaines généraux de l'OSI, de l'ONP, du RNIS/IBC et de la gestion des réseaux. Les techniques et approches en matière de vérification, y compris la certification débouchant sur une reconnaissance mutuelle, sont intrinsèquement liées à la normalisation et à la spécification. Chaque fois que possible, il convient d'appuyer des solutions adoptées au niveau international. Il faudrait également encourager la mise au point et l'utilisation de systèmes informatiques dotés de fonctions de sécurité.

4.3. *Situation et tendances*

Les États-Unis d'Amérique, en particulier, ont lancé d'importantes initiatives pour traiter la question de la sécurité des systèmes d'information. En Europe, ce sujet est traité dans le contexte de la normalisation des TIT dans le cadre de l'ETSI et du CEN/Cenélec, en préparation du travail du CCITT et de l'ISO dans ce domaine.

En raison des préoccupations croissantes, le travail aux États-Unis d'Amérique s'intensifie rapidement et tant les vendeurs que les prestataires de services accroissent leurs efforts dans ce domaine. En Europe, la France, l'Allemagne et le Royaume-Uni se sont lancés, chacun de leur côté, dans des activités similaires, mais un effort commun correspondant à celui des États-Unis d'Amérique ne se développe que lentement.

4.4. *Besoins, options et priorités*

Dans le domaine de la sécurité des systèmes d'information, les aspects réglementaires, opérationnels, administratifs et techniques sont, par essence, très étroitement liés. Les normes doivent refléter les réglementations et on doit pouvoir démontrer que les dispositions en matière de sécurité des systèmes d'information se conforment aux normes et réglementations. Sous plusieurs aspects, les réglementations doivent comporter des spécifications allant au-delà de l'objectif traditionnel de la normalisation, c'est-à-dire incluant des codes de conduite. Des exigences en matière de normes et codes de conduite existent dans tous les secteurs de la sécurité des systèmes d'information et il faut distinguer les exigences de protection correspondant aux objectifs en matière de sécurité et certaines des exigences techniques qui peuvent être confiées aux organismes européens de normalisation compétents (CEN/Cenélec/ETSI).

Les spécifications et normes doivent couvrir les domaines des services de sécurité des systèmes d'information (authentification des personnes et des entreprises, protocoles de non-répudiation, preuve électronique juridiquement valable, contrôle d'autorisation), leurs services de communication (respect de la vie privée au regard de la communication de l'image, de la voix et des données, protection des banques d'images et de données, sécurité des services intégrés), leur gestion de la communication et de la sécurité (systèmes de clés publiques/privées pour le fonctionnement des réseaux ouverts, de la protection de la gestion des réseaux, la protection des prestataires de services) et leur certification (critères et niveaux d'assurance, procédures d'assurance de la sécurité des systèmes d'information).

5. Ligne d'action V : développement technologique et opérationnel en matière de sécurité des systèmes d'information

5.1. *Problème*

Un travail de recherche et de développement technologique systématique permettant de trouver des réponses économiquement viables et opérationnellement satisfaisantes à une série de besoins présents et futurs en matière de sécurité des systèmes d'information est une condition nécessaire au développement du marché des services et à la compétitivité de l'économie européenne dans son ensemble.

Tout développement technologique en matière de sécurité des systèmes d'information devra porter à la fois sur la sécurité informatique et sur la sécurité des communications, dans la mesure où la plupart des systèmes actuels sont des systèmes distribués auxquels on accède par des services de communication.

5.2. *Objectif*

Un travail de recherche et de développement technologique systématique permettant de trouver des réponses économiquement viables et opérationnellement satisfaisantes à une série de besoins présents et futurs en matière de sécurité des systèmes d'information.

5.3. *Besoins, options et priorités*

Les travaux en matière de sécurité des systèmes d'information devraient porter sur les stratégies de développement et de mise en œuvre, les technologies, ainsi que l'intégration et la vérification.

Le travail stratégique de R&DT devrait comporter l'étude de modèles conceptuels de systèmes sûrs (sûrs au regard des modifications non autorisées et de l'interdiction de service), de modèles d'exigences fonctionnelles, de modèles de risque et d'architectures pour la sécurité.

Le travail de R&DT devrait inclure l'authentification de l'utilisateur et du message (par exemple grâce à l'analyse de la voix ou aux signatures électroniques), les interfaces techniques et les protocoles de chiffrement, les mécanismes de contrôle d'accès et des méthodes de mise en œuvre pour obtenir des systèmes garantis sûrs.

La vérification et la validation de la sécurité du système technique et son applicabilité seraient étudiées au moyen de projets d'intégration et de vérification.

Outre la consolidation et le développement de la technologie de la sécurité, un certain nombre de mesures d'accompagnement sont nécessaires en matière de création, mise à jour et application cohérente des normes, ainsi que de validation et certification de produits des TIT en ce qui concerne leurs propriétés en matière de sécurité, y compris la validation et certification des méthodes de conception et de mise en œuvre des systèmes.

Le troisième programme-cadre communautaire de R&DT pourrait être utilisé pour promouvoir des projets de coopération aux niveaux préconcurrentiel et prénormatif.

6. Ligne d'action VI : mise en œuvre de la sécurité des systèmes d'information

6.1. *Problème*

Selon la nature exacte des éléments de sécurité des systèmes d'information, il faudra intégrer les fonctions requises à différents points des systèmes d'information allant des terminaux, des services, de la gestion des réseaux aux dispositifs cryptographiques, aux cartes à mémoire, aux clés publiques et privées, etc. Certaines de ces fonctions seront probablement incorporées dans le matériel ou les logiciels fournis par les vendeurs tandis que d'autres pourront soit faire partie des systèmes distribués (par exemple gestion de réseaux), soit être en possession des utilisateurs individuels (par exemple cartes à mémoire), soit encore être fournies par un organisme spécialisé (par exemple clés publiques et privées).

La plupart des produits et services de sécurité seront probablement fournis par des vendeurs, des prestataires de services ou des opérateurs. Pour certaines fonctions spécifiques, comme par exemple la fourniture de clés publiques et privées et l'autorisation de contrôle, il pourra être nécessaire d'identifier et de mandater des organismes appropriés.

Il en est de même pour la certification des produits, l'évaluation et la vérification de la qualité du service, toutes fonctions qui doivent être confiées à des organismes indépendants des intérêts des vendeurs, prestataires de services ou opérateurs. De tels organismes pourraient être soit privés, soit publics, soit mandatés par l'État pour remplir ces fonctions.

6.2. *Objectif*

De façon à faciliter la mise en œuvre harmonieuse de la sécurité des systèmes d'information dans la Communauté dans un souci de protection du public et des intérêts commerciaux, il sera nécessaire d'adopter une attitude cohérente en matière de mise en œuvre de la sécurité des systèmes d'information. Lorsque des organismes indépendants seront mandatés, leurs fonctions et les conditions de fonctionnement devront être définies et acceptées et, si nécessaire, inscrites dans le cadre réglementaire. L'objectif serait de parvenir, comme préalable à la reconnaissance mutuelle, à un partage des responsabilités clairement défini et convenu entre les divers acteurs au niveau communautaire.

6.3. *Situation et tendances*

À l'heure actuelle, la mise en œuvre de la sécurité des systèmes d'information n'est bien organisée que pour des domaines particuliers et ne répond qu'à leurs besoins spécifiques. L'organisation au niveau européen est le plus souvent informelle et la reconnaissance mutuelle de la vérification et de la certification n'a pas lieu en dehors de certains groupes fermés. Du fait de l'importance croissante de la sécurité des systèmes d'information, il devient urgent de définir une approche cohérente dans ce domaine en Europe et au niveau international.

6.4. *Besoins, options et priorités*

En raison du nombre des acteurs concernés et des liens étroits avec les questions réglementaires et législatives, il est particulièrement important de dégager un consensus sur les principes qui devraient régir la mise en œuvre de la sécurité des systèmes d'information.

Lors de la définition d'une attitude cohérente en la matière, on devra traiter les aspects d'identification et de spécification de fonctions impliquant, par leur nature même, l'intervention d'organismes indépendants (ou d'organismes travaillant conjointement). Cela pourrait couvrir des fonctions telles que l'administration d'un système de clés publiques/privées.

En outre, il convient d'identifier et de préciser rapidement les fonctions qui doivent, dans l'intérêt du public, être confiées à des organismes indépendants (ou à des organismes travaillant conjointement). Ces fonctions pourraient par exemple comprendre le contrôle, la garantie de qualité, la vérification, la certification et des fonctions similaires.