Proposal for a Council Decision in the field of information security

COM(90) 314 final

(Submitted by the Commission on 27 July 1990)

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Article 235 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament,

Having regard to the opinion of the Economic and Social Committee,

Whereas the Community has as its task, by establishing a common market and progressively approximating the economic policies of the Member States, to promote throughout the Community a harmonious development of economic activity, a continued and balanced expansion, increased stability, accelerated raising of the standard of living, and closer relations of the States belonging to it;

Whereas the information stored, processed and transmitted electronically plays an increasingly important role in social and economic activities;

Whereas the advent of efficient global communication and the pervasive use of electronic handling of information emphasizes the need for adequate protection;

Whereas the European Parliament has repeatedly stressed the importance of information security in its deliberations and decisions;

Whereas the Economic and Social Committee has emphasized the need to address information security related issues in Community actions, particularly in view of the impact of the completion of the internal market;

Whereas it is necessary to develop a global strategy for information security in order to ensure the security of the user on the Community level and avoid the creation of new technical obstacles to communication;

Whereas the inherent complexity of information security issues calls for subsidiarity, the active involvement of several sectors and the concerted use of several policies;

Whereas actions on national, international and Community level provide a good basis;

Whereas there is a close link between telecommunications, standardization, information market and RD&T policies and the work already undertaken in these domains by the European Community;

Whereas it is appropriate to assure the concerted efforts, by building on existing national and international work and by promoting the cooperation of the principal protagonists concerned; whereas it is therefore appropriate to proceed within the framework of a coherent action plan;

Whereas the responsibility of the Member States in this domain implies a concerted approach based on a close collaboration with senior officials of the Member States;

HAS DECIDED AS FOLLOWS:

Article 1

1. An action plan in the field of information security (Infosec) is adopted for a period of 24 months starting on [...].

2. The action plan is designed to develop a global strategy providing the users of electronically stored, processed or transmitted information with protection of information systems against accidental or deliberate threats.

3. The action will take into account and support the evolving European and world-wide standardization activities in the field.

Article 2

The action plan, the details of which are set out in the Annex hereto, shall comprise the following lines of action:

I. Development of an information security strategy framework.

II. Analysis of information security requirements.

III. Solutions for immediate and interim needs.

IV. Specifications, standardization and verification of information security.

V. Integration of technological and operational developments for information security within a general strategy.

VI. Integration of certain security functions in information systems.
Article 3
The action plan shall be implemented by the Commission in collaboration with the organizations and enterprises concerned and in close association with the Member States.

Article 4
The amount attributed to this action shall be determined in the course of the annual budgetary procedure.

Article 5
The Commission shall send to the European Parliament and the Council a report on the results of the action within three months of its completion.

Article 6
For the implementation of the action plan, the Commission shall consult, as necessary, a Senior Officials Group on Information Security (Sogis). This group shall consist of two representatives of each Member State and of the Commission. A Commission representative shall be in the chair.

The members of the group may be assisted by experts or advisers depending on the nature of the issues under consideration.

The proceedings of the group shall be confidential. The group shall adopt its own rules of procedure. The secretariat shall be provided by the Commission.

ANNEX
SUMMARY OF ACTION LINES

1. Action line 1 — Development of an information security strategy framework

1.1. Issue

1.1.1. Information security is recognized as a pervasive quality necessary in modern society. Electronic information services need a secure telecommunication infrastructure, secure terminals (including processors and data bases) as well as secure usage. An overall strategy, considering all aspects of information security, needs to be established, avoiding a fragmented approach. Any strategy for the security of information processed in an electronic form must reflect the wish of any society to operate effectively yet protect itself in a rapidly changing world.

1.2. Objective

1.2.2. A strategically oriented framework has to be established to reconcile social, economic and political objectives with technical, operational and legislative options. The sensitive balance between different concerns, objectives and constraints has to be found by sector actors working together in the development of a common perception and agreed strategy. These are the prerequisites for reconciling interests and needs both in policy making and in industrial developments.

1.3. Status and trends

1.3.3. The situation is characterized by growing awareness of the need to act. However, in the absence of an initiative to concert the efforts it seems very likely that dispersed efforts in various sectors will be taken which create de facto a situation which will be contradictory, creating progressively more serious legal, social and economic problems.

1.4. Requirements, options and priorities

1.4.4. Such a shared framework would need to address and situate risk analysis and risk management concerning the vulnerabilities of information and related services, the alignment of laws and regulations associated with computer telecommunications abuse and misuse, administrative infrastructures including security policies and how these may be effectively implemented by various
industries/disciplines, and social and privacy concerns (e.g. the application of identification, authentication and possibly authorization schemes in a democratic environment).

1.4.5. Clear guidance is to be provided for the development of physical and logical architectures for secure distributed information services, standards, guidelines and definitions for assured security products and services, pilots and prototypes to establish the viability of various administrative structures, architectures and standards related to the needs of specific sectors.

1.4.6. Security awareness must be created in order to influence the attitude of the users towards an increased concern about security in IT and telecommunication systems.

2. Action line II - Information security requirements

2.1. Issue

2.1.7. Information security is the inherent prerequisite for the protection of privacy, intellectual property, commercial confidentiality and national security. This leads inevitably to a difficult balance and sometimes choices, between a commitment to free trade and a commitment to securing privacy and intellectual property. These choices and compromises need to be based on a full appreciation of requirements and the impact of possible information security options to respond to them.

2.1.8. User requirements imply information security functionalities interdependent with technological, operational and regulatory aspects. Therefore, a systematic investigation of information security requirements forms an essential part of the development of appropriate and effective measures.

2.2. Objective

2.2.9. Establishing the nature and characteristics of user requirements and their relation to information security measures.

2.3. Status and trends

2.3.10. Up to now, no concerted effort has been undertaken to identify the rapidly evolving and changing requirements of the major actors for information security. Community Member States have identified the requirements for harmonization of national activities (especially of the 'IT security criteria'). Uniform evaluation criteria and rules for mutual recognition of evaluation results/certificates are of major importance.

2.4. Requirements, options and priorities

2.4.11. As a basis for a consistent and transparent treatment of the justified needs of the sector actors it is considered necessary to develop an agreed classification of user requirements and its relation to information security provision.

2.4.12. It is also considered important to identify requirements for legislation, regulations and codes of practice in the light of an assessment of trends in service characteristics and technology, to identify alternative strategies for meeting the objectives by administrative, service, operational and technical provisions, and to assess the effectiveness, user-friendliness and costs of alternative information security option and strategies for users, service providers and operators.

3. Action line III - Solutions for immediate and interim needs

3.1. Issue

3.1.13. At present it is possible to protect adequately computers from unauthorized access from the outside world by 'isolation' i.e. by applying conventional organizational and physical measures. This applies also to electronic communications within a closed user group operating on a dedicated network. The
situation is very different if the information is shared between user groups or exchanged via a public, or generally accessible, network. Neither the technology, terminals and services nor the related standards and procedures are generally available to provide comparable information security in these cases.

3.2. Objective

3.2.14. The objective has to be to provide, at short notice, solutions which can respond to the most urgent needs of users. These should be conceived as open towards future requirements and solutions.

3.3. Status and trends

3.3.15. Some user groups have developed techniques and procedures for their specific use responding, in particular, to the need for authentication, integrity, and non-repudiation. In general magnetic cards or smart cards are being used. Some are using more or less sophisticated cryptographic techniques. Often this implied the definition of user-group specific 'authorities'. However, it is difficult to generalize these techniques and methods to meet the needs of an open environment.

3.3.16. ISO is working on OSI information security (ISO DIS 7498-2) and CCITT in the context of X400. It is also possible to insert information security segments into the messages. Authentication, integrity and non-repudiation are being addressed as part of the messages (Edifact) as well as part of the X400 MHS.

3.3.17. Presently, the EDI legal framework is still at the stage of conception. The International Chamber of Commerce has published uniform rules of conduct for the exchange of commercial data via telecommunications networks.

3.3.18. Several countries (e.g. Germany, France, the United Kingdom and the USA) have developed or are developing criteria to evaluate the trustworthiness of IT and telecommunication products and systems and the corresponding procedures for conducting evaluations. These criteria have been coordinated with the national manufacturers and will lead to an increasing number of trusted products and systems starting with simple products. The establishment of national organizations who will conduct evaluations and offer certificates will support this trend.

3.3.19. Confidentiality provision is considered by most users as less immediately important. In the future, however, this situation is likely to change as advanced communication services and in particular mobile services will have become all pervasive.

3.4. Requirements, options and priorities

3.4.20. It is essential to develop as soon as possible the procedures, standards, products, and tools suited to assure information security on public communications networks. A high priority should be given to authentication, integrity and non-repudiation. Pilot projects should be carried out to establish the validity of the proposed solutions. Solutions to priority needs on EDI are looked at in the Tedis programme within the more general content of this action plan.

4. Action line IV — Specification, standardization and verification for information security

4.1. Issue

4.1.21. Information security requirements are pervasive and as such common specifications and standards are crucial. The absence of agreed standards and specifications may present a major barrier to the advance of information-based processes and services throughout the economy and society. Actions are required to accelerate the development and use of technology and standards in several related communication and computer network areas that are of critical importance to users, industry and administrations.
4.2. Objective

4.2.22. Efforts are required to provide a means of supporting and performing specific functions in the general areas of OSI, ONP, ISDN/BC, network management and network security for unclassified, but sensitive, information. Inherently related to standardization and specification are the techniques and approaches required for verification.

4.3. Status and trends

4.3.23. The USA, in particular, have taken major initiatives to address information security in the non-defence domain. In Europe the subject is treated in the context of IT and telecommunications standardization in the context of ETSI and CEN/Cenelec in preparation of CCITT and ISO work in the domain.

4.3.24. In view of growing concern, the work in the USA is rapidly intensifying and both vendors and service provider are increasing their efforts in this domain. In Europe, France, Germany and the United Kingdom have independently started similar activities but a common effort corresponding to the USA is only evolving slowly.

4.4. Requirements, options and priorities

4.4.25. In information security there is inherently a very close relationship between regulatory, operational, administrative and technical aspects. Regulations need to be reflected in standards and information security provisions need to comply in a verifiable manner to the standards and regulations. In several aspects regulations require specifications which go beyond the conventional scope of standardization, i.e. include codes of practice. Requirements for standards and codes of practice are present in all areas of information security, and a distinction has to be made between the protection requirements which correspond to the security objectives and some of the technical requirements which can be entrusted to the competent European standard bodies (CEN/Cenelec/ETSI).

4.4.26. Specifications and standards must cover the subjects of information security services (personal and enterprise authentication, non-repudiation protocols, legally acceptable electronic proof, authorization control), communication services (image communication privacy, mobile communications voice and data privacy, data and image data-base protection, integrated services security), communication and security management (public/private key system for open network operation, network management protection, service provider protection) and certification (information security assurance criteria and levels, security assurance procedures).

5. Action line V — Technological and operational developments for information security

5.1. Issue

5.1.27. Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future information security requirements is a prerequisite to the development of the services market and the competitiveness of the European economy as a whole.

5.1.28. Any technological developments in information systems security will have to include both the aspects of computer security and security of communications as most present-day systems are distributed systems, and access to such systems is through communications services.

5.2. Objective

5.2.29. Systematic investigation and development of the technology to permit economically viable and operationally satisfactory solutions to a range of present and future information security requirements.

5.3. Requirements, options and priorities

5.3.30. Work on information security would need to address development and implementation strategies, technologies, and integration and verification.
5.3.31. The strategic R & D work would have to cover conceptual models for secure systems (secure against compromise), functional requirements models, risk models, and architectures for security.

5.3.32. The technology orientated R & D work would have to include user and message authentication (e.g. through voice analysis and electronic signatures), technical interfaces and protocols for encryption, access control mechanisms, and implementation methods for provable secure systems.

5.3.33. Verification and validation of technical system security and its applicability would be investigated through integration and verification projects.

5.3.34. In addition to consolidation and development of security technology, a number of accompanying measures are required concerned with the creation, maintenance and consistent application of standards, and the validation and certification of IT and telecommunication products with respect to their security properties, including validation and certification of methods to design and implement systems.

5.3.35. The third RDT Community framework programme might be used to foster cooperative projects at pre-competitive and pre-normative levels.

6. Action line VI — Information security provisions

6.1. Issue

6.1.36. Depending on the exact nature of the information security features required functions will need to be incorporated at different parts of the communication systems including terminals/computers, services, network management to cryptographic devices, smart cards, public and private keys, etc. Some of these can be expected to be embedded in the hardware or software provided by vendors while others may be part of distributed systems (e.g. network management), in the possession of the individual user (e.g. smart cards) or provided from a specialized organization (e.g. public/private keys).

6.1.37. Most of the information security products and services can be expected to be provided by vendors, service providers or operators. For specific functions, e.g. the provision of public/private keys, auditing, authorization, there may be the need to identify and mandate appropriate organizations.

6.1.38. The same applies for certification, evaluation and verification of quality of service which are functions which need to be addressed by organizations independent of the interests of vendors, services providers or operators. These organizations could be private, governmental, or licensed by government to perform delegated functions.

6.2. Objective

6.2.39. In order to facilitate a harmonious development of the provision of information security in the Community for the protection of the public and of business interests it will be necessary to develop a consistent approach as to the provision of information security. Where independent organizations will have to be mandated, their functions and conditions will need to be defined and agreed and where required embedded into the regulatory framework. The objective would be to come to a clearly defined and agreed sharing of responsibilities between the different actors on a Community level as a prerequisite for mutual recognition.

6.3. Status and trends

6.3.40. At present information security provision is well organized only for specific areas and limited to addressing the specific needs. The organization on a European level is mostly informal and mutual recognition of verification and certification is not yet established outside closed groups. With the growing importance of information security the need for defining a consistent approach to information security provision in Europe and internationally is becoming urgent.
6.4. Requirements, options and priorities

6.4.41. Because of the number of different actors concerned and the close relations to regulatory and legislative questions it is particularly important to pre-agree on the principles which should govern the provision of information security.

In developing a consistent approach to this question one will need to address the aspects of identification and specification of functions requiring, by their very nature, the availability of some independent organization (or interworking organizations). This could include functions such as the administration of a public/private key system.

In addition, it is required to identify and specify, at an early stage, the functions which in the public interest need to be entrusted to independent organization (or interworking organizations). This could, for example include auditing, quality assurance, verification, certification and similar functions.

Proposal for a Council Decision on the conclusion by the European Economic Community of an Agreement on trade and commercial and economic cooperation between the European Economic Community and the European Atomic Energy Community and Romania

SEC(90) 1872 final

(Submitted by the Commission to the Council on 8 October 1990)

(90/C 277/06)

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European Economic Community, and in particular Articles 113 and 235 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament,

Whereas the conclusion by the European Economic Community of the Agreement on trade and commercial and economic cooperation between the European Economic Community and the European Atomic Energy Community and Romania is necessary to achieve the Community's external relations objectives;

It seems that some of the economic cooperation measures envisaged in the Agreement exceed the powers of action provided for in the field of common economic policy,

HAS DECIDED AS FOLLOWS:

Article 1

The Agreement on trade and commercial and economic cooperation between the European Economic Community and the European Atomic Energy Community and Romania is hereby approved on behalf of the European Economic Community.

The text of the Agreement is annexed to this Decision.

Article 2

The President of the Council shall give on behalf of the European Economic Community the notification provided for in Article 25 of the Agreement (1).

Article 3

The Commission, assisted by representatives of the Member States, shall represent the Community in the Joint Committee set up under Article 22 of the Agreement.

(1) The General Secretariat of the Council will publish the date of entry into force of the Agreement in the Official Journal of the European Communities.