ETSI TECHNICAL REPORT

ETR 330

November 1996

Source: ETSI TC-STAG

Reference: DTR/NA-002801

ICS: 33.020

Key words: Security

Security Techniques Advisory Group (STAG); A guide to the legislative and regulatory environment

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Security Techniques Advisory Group (STAG) and is part of the overall security standards policy being developed by STAG. It provides general information on the regulatory aspects of telecommunications security and shall be used as reference by ETSI TCs and STCs in preparing their security requirements and security specifications.

The use of telecommunications has grown in importance in all sectors of the society, and of the economy to the point where most organizations are totally dependent upon their networks. Telecommunications technology continues to develop; new environments are emerging providing the user with, amongst other features, increased mobility. Further, largely as a result of increased liberalisation of the telecommunications market, there is a trend for services to be supplied by more than one network operator.

Telecommunications security requirements are changing for four main reasons:

- liberalisation of telecommunications (infrastructures, services and terminal equipment);

- changes in technology and services;

- increasing dependence upon, and expectations from telecommunications services (especially quality of service) by society;

- the furthering of national and international requirements with regard to legal interception of telecommunications, for purposes of national security and the fighting of organized crime.

The security of telecommunications is therefore affected by many factors, some technical or operational, some legal. Existing laws have been based upon traditional concepts of harm and, in particular, of fraud, theft and invasion of privacy, and have not been framed by reference to that which becomes possible within the new and emerging telecommunications environments. In addition, there are legislative disparities between States.

Blank page

1 Scope

This ETSI Technical Report (ETR) forms a part of the documentation on the security standards policy from the Security Techniques Advisory Group (STAG). This aspect of the security standards policy is concerned with legislation, guidelines or recommendations which could (possibly) influence decisions concerning the inclusion or nature of security features in ETSI standards. Technical and operational factors are outside the scope of this ETR.

The ETR is solely descriptive; the information provided is of a general nature. STAG intends to provide supplementary documentation on how to address specific issues mentioned in the ETR.

2 References

For the purposes of this ETR, the following references apply:

[1] ETR 232: "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology".

[2] 88/301/EEC: "Commission Directive on Competition in the Market for Terminal Equipment" (OJ L 131 (27.05.88)).

[3] 90/388/EEC: "Commission Directive on Competition in the Market for Telecommunications Services" (OJ L 192 (24.07.90)).

[4] 90/387/EEC: "Council Directive on the establishment of the Internal Market for Telecommunications Services through the Implementation of Open Network Provision" (OJ L 192 (24.07.90)).

[5] 9529/95 ENFOPOL 90: "Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications" (Brussels, 28 August 1995).

[6] CM(95)101: "Council of Europe Recommendation on Problems of Criminal Procedural Law connected with Information Technology" (Strasbourg, 31 July 1995 (adopted 7-8 September 1995)).

[7] Department of Trade and Industry: "A Code of Practice for Information Security Management" (British Standards Institution, September 1993 (ISBN 0 580 22536 4)).

[8] 94/942/GBVB: "Council Decision on the Joint Action adopted by the Council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods" (19 December 1994, OJ L 367 (31.12.94)).

[9] 3381/94: "Council Regulation, setting up a Community regime for the control of exports of dual-use goods" (19 December 1994), OJ L 367 (31.12.94)). and 837/95: "Amendment to Council Regulation 3381/94" (10 April 1995, OJ L 90 (21.4.95)).

NOTE: Amendment 837/95 concerns date coming into force 01.07.95.

[10] C(80)58 (Final): "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (23 September 1980).

[11] OCDE/GD(92)190: "Recommendation of the Council concerning Guidelines for the Security of Information Systems" (26 November 1992).

[12] Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Strasbourg, 28 January 1981).

[13] R(95)4: "Council of Europe Recommendation on the Protection of Personal Data in the area of Telecommunications Services, with particular reference to Telephone Services" (adopted 7 February 1995).

[14] 95/46/EEC: "Council Directive on the Protection of Individuals in relation of the processing of Personal Data and on the free Movement of such Data" (OJ L 281 (23.11.95)).

[15] COM(94)128 final-COD 288: "Amended Proposal for a European Parliament and Council Directive concerning the Protection of Personal Data and Privacy in the context of Digital Telecommunications Networks, in particular the Integrated Services Digital Network (ISDN) and Digital Mobile Networks" (OJ C 200 (22.07.94)).

3 Definitions, symbols and abbreviations

3.1 Definitions

The definitions of security terminology in this ETR conform to ETR 232 [1].

For the purposes of this ETR, the following additional definitions apply:

law enforcement agency: A service authorized by law to carry out telecommunications interceptions.

lawful authorization: Permission granted to a law enforcement agency under certain conditions to intercept specified telecommunications. Typically this refers to an order or warrant issued by a legally authorized body.

legal interception: The statutory-based action of providing access and delivery of a subject's telecommunications and call associated data to law enforcement agencies.

subject: Person(s) identified in the lawful authorization and whose incoming and outgoing telecommunications are to be intercepted and monitored.

3.2 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

COCOM	Co-ordinating Committee on the Export Control of Strategic Goods
EEC	European Economic Communities
GSM	Global System for Mobile communications
ITU	International Telecommunication Union
MoU	Memorandum of Understanding
OJ	Official Journal of the European Communities
STAG	Security Techniques Advisory Group

4 Sources of law and regulation

The laws and regulations affecting telecommunications (standards) security derive from a number of sources. The principal sources include:

- the national constitutions;
- the Treaties of Rome and Maastricht, and Directives or other measures based upon those treaties;
- the Constitution and Conventions of the International Telecommunication Union (ITU);
- other international conventions;
- national laws, such as specific telecommunications laws, other relevant specific laws (e.g. on the protection of personal data, encryption and copyright) and other general national laws (e.g. civil and criminal codes);
- telecommunications rules, licences and contracts issued by the relevant minister or regulator; and
- codes of practice, which may be voluntary or required by national legislation.

4.1 National constitutions

Telecommunications are used for carrying messages and data, some being personal, some containing valuable business secrets. To a greater or lesser extent, parties expect the confidentiality of the contents of their communications and of any personal details or statistics held by the operators or service providers to be respected. In most European countries, the legal basis for the protection of personal and other data is founded in the principles of the Constitution, aimed at guaranteeing the secrecy of correspondence, the right of privacy, the right of personal liberty, freedom of expression or of personality. Some countries make express reference to telephone communications, others do not. In addition, many national Constitutions also provide for exceptions to the constitutional rights, like breaches of secrecy by judicial order. The prohibition of listening-in to telecommunications, and therefore the right to privacy, is a qualified right, with legal interception being accepted as an exception, even though precise circumstances and proceedings to be adopted do vary (see clause 6 for further information).

4.2 The Treaties of Rome and Maastricht

The powers of the European Union are laid down in the Treaties of Rome and Maastricht. The Union shall respect Fundamental Rights, as guaranteed by the European Convention for the protection of Human Rights, and Fundamental Freedoms, and as they result from the constitutional traditions common to the Member States, as general principles of Community law. The Union is served by a single institutional framework which has to ensure the consistency and continuity of all its activities. New under Maastricht is the development of close co-operation on justice and home affairs, including on fraud, civil and criminal matters and police co-operation (the so-called Third Pillar; next to the traditional First Pillar and the also new Second Pillar on the co-operation on defence and foreign affairs).

4.2.1 The First Pillar

Under the provisions of the First Pillar, as a rule, the Commission takes the initiative for measures to be adopted by the Council or by the Council and the European Parliament. These measures can be considered as the building bricks for the overall European telecommunications policy.

There are a number of **legal instruments** which can be applied:

- the Regulation. A regulation has a general application and is binding in its entirety. It is directly applicable in every Member State;

- the Directive. A directive is binding for the Member State(s) to which it is addressed with respect to the result to be achieved. It is up to the Member State(s) to choose forms and methods;

- the Decision. A decision is binding in all its parts for those to whom it is directed;

- the Recommendation. Recommendations and opinions are not binding.

Next to these instruments, the Council Resolution is used as a Declaration of Intent. Its legal force is addressed by the Treaty. It has to be determined by its wordings: usually it is not legally binding but merely a declaration of opinion or intent.

The Council of Ministers and the Commission have already adopted a number of important measures in the area of telecommunications. The are published regularly in the Official Journal of the European Communities. Some major ones include:

- Commission Directive on Competition in the Market for Terminal Equipment, 88/301/EEC [2];

- Commission Directive on Competition in the Market for Telecommunications Services, 90/388/EEC [3];

- Council Directive on the establishment of the Internal Market for Telecommunications Services through the Implementation of Open Network Provision, 90/387/EEC [4] (a so-called Council framework Directive, with subsequent specific Directives on e.g. Voice and Leased Lines and Recommendations on Packet Switched Data and ISDN).

A common theme identified in these directives refers to the so-called "essential requirements", which need to be satisfied in all cases. Narrowly, they include the safety of the network, the integrity of the network, the inter-operability of services, where justified, and the protection of data, where this is appropriate.

Preparatory work in the area of the security of information systems, including telecommunications, is carried out by SOG-IS (the Senior Officials Groups on the security of Information Systems, an advisory body to the Commission).

In addition, the European Union, through the Council, may conclude treaties with third countries or other international organizations. These treaties are binding for the European Union and its Member States.

4.2.2 The Third Pillar

The Third Pillar contains provisions concerning the co-operation between the Member States in the fields of Justice and Home Affairs in the Union. Before Maastricht, this co-operation was based on intergovernmental agreements between States, outside the scope and framework of the European Community. Within the Union’s structure, a number of working groups are now involved in several dedicated topics. The Technical and Forensic Police Working Party deals with Interception of telecommunications and works at establishing harmonized measures and procedures in this area. Here, the Commission, although fully involved, has no right of initiative: this remains with Member States.

The Council of Ministers takes all the decisions. There are three types of instruments:

- the Joint Position. Member States can adopt Joint Positions with the purpose of voicing these in international organizations and on international conferences. It has a certain political sense. On account of its nature, the Joint position is not a legally binding instrument. However the conditions and provisions, laid down in the Joint Position itself, may imply a legally binding status;

- the Joint Action. This decision will be applied if the envisaged outcome will be achieved more effectively through a common action rather than through action by Member States separately. It also has a certain political implication. On account of its nature, the Joint Action, too, is not a legally binding instrument but the conditions and provisions themselves, as agreed, may imply a legally binding nature;

- the Convention. The Council may draw up Conventions which it shall recommend to its Member State for adoption in accordance with their constitutional provisions. A Convention may contain legally binding provisions.

Next to these instruments, the Council Resolution is used as a Declaration of Intent. But this modality, together with the Council Recommendation, is not specified under the new treaty.

An example of a **Council Resolution** is the Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, 9529/95 ENFOPOL 90 [5], adopted in January 1995.

4.2.3 The European Union bodies

The European Union has a number of institutions. The most important are the European Commission, the Council of the European Union (Council of Ministers), the European Parliament and the European Council (Summit). In short, their respective roles can be regarded as follows.

The European Commission, which consists of 20 members or commissioners, is responsible for initiating European legislation. The Commission is the only body entitled to issue proposals for legislation. Proposals need to be approved or adopted by the Council of the European Union (Council of Ministers) to become effective. The Commission also acts as the executive body of the Union and takes care that tasks, laid down in treaties and Council Decisions, are carried out. It is responsible to the European Parliament.

Member States are directly represented in the Council of the European Union (Council of Ministers). It is the body of the Union that takes the decisions. Pending on the agenda, the Council meets in different compositions. If decisions of a general political nature are to be taken, it is formed by the Ministers of Foreign Affairs.

The European Parliament is actively involved in the European legislation process. Pending on the subject, it may advice on, amend or veto a proposal by the European Commission. The European Parliament has to approve the Union's budget. The Parliament may take political initiatives e.g. by pressing for the development of new policy or legislation. In addition, the European Parliament, following a vote of censure supported by a two third majority, may dismiss the European Commission.

The European Council (Summit), consisting of the Heads of State and Government, meets at least twice a year. The European Council discusses major political European questions. These Summits often lead to important decisions by the Union. As arranged under the Treaty of Maastricht, the European Council gives general guidance for the common Foreign and Security policy of the Union.

4.3 The constitution and conventions of the ITU

The ITU is a specialized body of the United Nations, responsible for virtually all international regulation in the field of telecommunications. The Constitution, Convention and, in addition, Administrative Regulations of the ITU provide members with important sources of principles, rules and regulations concerning operational and administrative procedures in relation to different telecommunications services. States are parties to the Constitution of the ITU, which contains provisions which would affect members in relation to the security of telecommunications. Members are required to, for example, agree to take all possible measures with a view to ensuring the secrecy of international correspondence; however, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of national laws or the execution of international conventions to which they are parties. In addition, members are required to recognize the right of the public to correspond by international means, but they are also given the right to stop transmission or cut off telecommunications which may appear dangerous to the security of the State or contrary to its laws, public order or decency. Members are to take the necessary steps to ensure the establishment, under the best technical conditions, of the channels and installations necessary for the rapid and uninterrupted exchange of international telecommunications. These channels and installations are to be safeguarded within their jurisdiction.

4.4 Other International Conventions

There are a number of other International Conventions which contain certain obligations having (some) relevance to the security of telecommunications. For example, the European Convention on Human Rights, stipulates that everyone has the right to respect for his private and family life, his home and his correspondence, and that there will be no interference by a public authority except in specified cases, such as in the interest of national security and for the prevention of crime.

Other conventions and documentation directly or indirectly relevant to the security of telecommunications include:

- the Charter of the United Nations, the Universal Declaration of Human Rights, and the Covenants issued under it;

- the Berne Convention for the Protection of Literary and Artistic Works, and its revisions (amongst other things, this Convention contains some provisions for the publication of literary works, etc. through e.g. radio-emission or by wire);

- the Universal Copyright Convention, and its revisions.

4.5 National Laws

Network operators and service providers are governed by national telecommunications laws of the countries in which they are operating. These laws vary in scope and content but may include the principles of international Conventions or Constitutions such as of the ITU. The laws set rules (to include general conditions and provisions) concerning the operation of telecommunications networks, the supply of telecommunications services, competition, access to the networks, etc. European Union Member States organize their national regulatory frameworks implementing or taking into account the directives and other measures adopted in Brussels.

Security in telecommunications is considered to be an important aspect in the provision of infrastructures and services and is regulated in general terms by law.

Next to telecommunications laws, there exist other laws which have a specific impact on telecommunications and telecommunications security. These include legislation on data protection, privacy, copyright, computer misuse and on the other hand on the legal interception of telecommunications. Legislation on data protection and on privacy in Europe has been harmonized to a great extent by the Council of Europe. The Organization for Economical Co-operation and Development undertakes similar activities on a more global level (see clause 7 for further information). The Council of Europe is also carrying out substantial work to achieve further harmonization on computer crime legislation (Recommendation on Problems of Criminal Procedural Law connected with Information Technology, CM(95)101 [6]). Other general laws which may affect telecommunications are criminal or civil codes, for example on theft, malicious damage and, as mentioned before, the interception of telecommunications.

4.6 Rules issued by the Regulator

Under the telecommunications laws, States may issue subordinate rules or regulations. These may take the form of decrees, contracts, licenses or concessions and determine in more detail the conditions under which telecommunications operators and service providers need to carry on their business. As a rule, this is the responsibility of the national regulatory authority, which is provided for in the telecommunications laws.

Security of telecommunications, of course, is of great importance to the operators and service providers themselves. Research has indicated there may be a need for more self-regulation (like e.g. Codes of Practice) rather than (too much) detailed regulation by government.

4.7 Codes of Practice

Especially with regard to telecommunications security, network operators and service providers share common risks and may therefore require co-operation. A means to achieve a harmonized approach to those risks is the Code of Practice. Codes of Practice are agreed policies, or ways of acting, and provide a common basis for telecommunications companies and organizations to develop, implement and measure effective security management practices. They also provide confidence in inter-company trading. Codes of Practice may be developed by companies, or by the regulatory authority with the assistance of companies. An example is the Code of Practice for Information Security Management [7], developed by the UK Department of Trade and Industry with the assistance of a group of leading UK companies and organizations.

Although not a Code of Practice in its own right, regulatory authorities, network operators and service providers may bind themselves through a Memorandum of Understanding (MoU) to develop, exploit and maintain a dedicated telecommunications system under the provisions and with the features as agreed by the MoU. An example of such an MoU is the MoU on Global System for Mobile communications (GSM). The MoU structure may comprise of topic-related subgroups, like on security or on data protection. The membership to an MoU group may be required by law.

5 Cryptography

Cryptography or, in this context, encryption, is an instrument to, amongst others, protect privacy and confidentiality in telecommunications. As such, it provides protection against disclosure to unauthorized individuals, entities or processes. It has become an important, if not essential, "tool" in telecommunications. It can be discussed whether cryptography should be regarded as a legal principle, or not. There are considerable arguments to favour such an approach.

5.1 Export requirements

In many countries, cryptography is considered of "strategic" importance and is consequently subject to an export licence. Although export of goods is a national responsibility, an overall co-ordination on export control was pursued by the so-called COCOM (the Co-ordinating Committee on the Export Control of Strategic Goods), a group of several important Western trade nations who set rules for the export of strategic goods. During the Cold War and its immediate aftermath, COCOM played an important role with regard to the export of cryptography but acted only from a defence and national security point of view. As a result of international developments, COCOM needed to be reshaped. It abandoned itself as an organization but talks continued to prevent unwanted proliferation of strategic goods. A new organization, called New Forum, was set up for that purpose. The European Union, under the framework of the Second Pillar which contains provisions with regard to a Common Foreign and Security Policy, adopted a Council Decision on a Joint Action concerning the control of exports of "dual-use" goods, 94/942/GBVB [8] (which can be used for both civil and military purposes) and consequently a Council Regulation, setting up a regime for the control of exports of such goods, 3381/94 [9].

Also as a result of international developments, interests other than defence and national security emerged. They include economical, telecommunications, privacy, data protection and judicial interests. It may be evident that the world-wide introduction of telecommunications (networks, services and terminal equipment) is depending on its exportability. Cryptography, both hardware and software, is subject to export licence conditions in a considerable number of States.

5.2 Business requirements

International business are demanding seamless webs of telecommunications networks whereby information can flow in a free and secure manner. Encryption is currently the most appropriate means to ensure this security. Encryption is particularly important for telecommerce, which requires absolute guarantees in areas such as the integrity of signatures and text, irrevocable time and date stamping and international legal recognition. In this respect, the need for Trusted Services is growing. Many countries, however, have a variety of restrictions which inhibit business from using secure telecommunications. These restrictions include export and import control laws, usage restrictions, restrictive licensing arrangements, etc. These measures may create an international environment which does not permit business to acquire, use, store or sell cryptographic methods uniformly to secure their world-wide telecommunications. In addition, they hinder the competitiveness of companies.

Several business associations in Europe and beyond have indicated the urgent need for an international harmonized approach in the field of commercially available security products, in particular cryptography. In their view, a global encryption policy, taking into account all needs, would be a major step forward with respect to the fulfilment of the business requirements.

5.3 Government requirements

It is the responsibility of governments to remove unnecessary trade barriers and to face business needs such as for Trusted Services. On the other hand, it is recognized that governments have also a judicial and national security responsibility. Government may therefore need powers to override encryption for the purposes of fighting against crime and protecting national security. National attempts to bring commercial cryptography under some sort of control have so far not been really successful. Indeed, an answer given at a national level to this, and to the hacking issue, will inevitably prove to be insufficient because telecommunications reach beyond national frontiers. Also from the governments' point of view a harmonized and balanced approach on an international scale might therefore be the best solution.

6 Legal Interception of Telecommunications

6.1 Legal basis

The interception of telecommunications is a subject that falls under the right to respect for private life as is guaranteed by article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. An exception is provided for under the strict conditions mentioned in paragraph 2 of this article, as further elaborated by the case law of the European Court of Human Rights. Within the limits of international law, many States have national legislation specifying the conditions under which the interception of telecommunications is allowed and carried out in the interests of national security or the prevention of crime. National legislative bases are found in Criminal Codes, Criminal Procedure Acts, Telecommunications Acts and other laws or regulations. Some States, however, have no specific legislation concerning this subject.

6.2 New technologies

Recent years have seen an expansion in the use of telecommunications. This has been supported by rapid technological developments, leading to a wider variety of sophisticated products, and by the liberalisation of the telecommunications markets, breaking down the monopolies formerly held by state owned or sponsored organizations. New companies, more or less independent of direct governmental control, entered the market place. In addition, growing privacy awareness led to an increased need by governments and business to strengthen information security.

All these developments have positive effects as to economic growth and human freedom but organized crime is also to benefit. These organizations will be among the first to use these new technologies that may safeguard them from public surveillance. High costs may be for them less an impediment than for others.

The era of the "plain old telephone set" with relatively easy techniques and, hence, easy and low-cost interception techniques is over. The new telecommunications technologies, therefore, threaten to impede the exercise of the governmental powers to intercept telecommunications for the protection of national interests (notably the investigation of serious and organized crime and national security) within the aforementioned limits of the law.

6.3 Meeting the challenge

In order to meet this challenge, Ministers in Europe and beyond, responsible for Justice, Police and National Security, have taken and continue to take appropriate steps, while pursuing contact with the Ministers responsible for Telecommunications and/or Encryption on the matter. Within the European Union, the co-operation in the area of interception now takes place within the framework of Title VI of the Treaty of Maastricht. It is the view of law enforcement Ministers that if their needs with regard to interception are not taken into account and incorporated into networks at an early stage (i.e. before and during the standardization process, and during the further stages of their development), they may be achieved later only at considerable cost, if at all. New European instruments regulating the telecommunications markets might have implications for the way in which national authorities can ensure that interception is provided for.

At the same time, the relationships established between governments and telecommunications organizations to ensure that interception could be achieved may not be sufficient in a rapidly diversifying and expanding market in which there are a large number of operators and service providers.

Moreover, systems which enable services to be provided across national boundaries may require international collaboration if interception of those systems is to be possible. As this is increasingly the case, international co-operation has become essential.

With the endorsement of international interception requirements, through its Council Resolution on the Lawful Interception of Telecommunications of January 1995, 9529/95 ENFOPOL 90 [5], the European Union has taken a first but major step in meeting the challenge. The Resolution contains detailed requirements with regard to the legal interception of telecommunications. Some of the major requirements described in the resolution are for call content, call associated data and target location. There are specific provisions for confidentiality, integrity and auditing in the interception process.

Implementation of these requirements is at hand. In addition, several nations outside Europe also intend to adopt the same requirements, or have already done so. Worth mentioning are also the activities of the Council of Europe, and in particular of its Committee of Experts on Criminal Procedural Law problems connected with Information Technology, who also addressed the problem of legal interception and issued recommendations regarding this aspect, CM(95)101 [6].

It may be possible that these developments lead to a subsequent discussion on a common approach to cryptography.

7 Protection of privacy and personal data

Privacy is usually defined in two ways: the right to be left alone, free from intrusion or interruption, and the right to exercise control over one's personal information. (personal) data protection is an aspect of privacy protection that involves control over the collection, storage, accuracy, use and dissemination of personal information.

There is general agreement that, given the increasingly significant role of telecommunications and information systems and growing dependence on them in economic, social, cultural and political life, appropriate safeguards need to be established to eliminate the risks arising from available means of unauthorized access, use, misappropriation, alteration and destruction of data. The security of telecommunications and information systems has therefore become essential. The objective of security of information systems, in this context, may be regarded as the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality and integrity.

7.1 Legal basis

The right to respect for privacy is fundamental. It is well anchored within international conventions, such as the Convention for the Protection of Human Rights and Fundamental Freedoms and the European Convention on Human Rights, and national constitutions. In many cases, this is further elaborated in national laws and regulation.

On a global level, the Organization for Economical Co-operation and Development has undertaken several activities with respect to privacy protection and the security of information systems. The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58 [10] and the Recommendation of the Council concerning Guidelines for the Security of Information Systems, OCDE/GD(92)190 [11] have indicated, amongst other things, that international co-ordination and co-operation are necessary in these particular areas.

In Europe, legislation on privacy and data protection has been harmonized to a great extent by the Council of Europe Convention on the Automatic Processing of Personal Data [12] and Recommendation on the Protection of Personal Data in the area of Telecommunications Services, with particular reference to Telephone Services, R(95)4 [13].

Important measures by the European Union with reference to the protection of personal data are the Council Directive on the Protection of Individuals in relation of the processing of Personal Data and on the free Movement of such Data, 95/46/EEC [14], and the Amended Proposal for a European Parliament and Council Directive concerning the Protection of Personal Data and Privacy in the context of Digital Telecommunications Networks, in particular the Integrated Services Digital Network (ISDN) and Digital Mobile Networks, COM(94)128 [15]. Further harmonization will indeed be achieved if this proposal is adopted.

Despite all the international initiatives taken so far, disparities may still occur between national legislations on the protection of privacy and personal data.

7.2 New technologies

The demand for the protection of privacy will increase as the potential of the new technologies to secure, even across national frontiers, and to manipulate detailed personal information from various telecommunications sources is realized. The ongoing development of the Information Infrastructures highlights the growing importance of free data flow in today's and tomorrow's society. The need to process and disseminate data at unprecedented quantities and unprecedented speeds, now becoming possible through the technological advances, may raise additional privacy concerns. Privacy expectations may therefore change over time. It will be a challenge to preserve the right balance between privacy requirements and the use of new, trans-frontier telecommunications services.

8 Conclusions

When preparing their security requirements and security specifications, ETSI TCs and STCs find themselves in a spider's web with respect to prevailing national and international regulations in the area of telecommunications and telecommunications security. It is realized that network operators and service providers rather than ETSI TCs and STCs should anticipate the conditions on which they may operate in specific countries but system designers and developers may need advance knowledge.

One should also be aware that regulating, in general, is an on-going process that may change in time. The information given in this ETR is merely a synopsis and a snapshot. If further information is required, STAG should be contacted.

In the area of commercial security, political discussions with regard to exportability, usage and proliferation of cryptography are going on, but as long as a clear, common approach has not been reached, national conditions prevail despite the needs expressed by various sources.

Fulfilling the business needs for Trusted Services in balance with the governmental needs will prove to be a challenge.

It is anticipated that the legal interception of telecommunications will become (or rather remain) an essential governmental requirement: an early awareness of the requirements (in accordance with national legislation) to be incorporated in the design and standardization phase of new systems, should avoid work and costs afterwards. The European Union has drawn up harmonized requirements which are being translated into national legislations.

The demand for the protection of privacy may change over time as new technologies, even across national frontiers, are becoming available as a result of the ongoing development of the Information Infrastructures.

History

Document history	
November 1996	First Edition

ISBN 2-7437-1142-6
Dépôt légal : Novembre 1996