International Standardisation of IT Security

Klaus Vedder

Giesecke & Devrient GmbH
Prinzregentenstr. 159, D-81677 München, Germany
klaus.vedder@gdm.de

Abstract. This paper discusses the standards and activities of the ISO/IEC committee SC 27 "Information technology - Security techniques", which develops general security mechanisms, guidelines and criteria for IT security, and of the European Telecommunications Standards Institute, which specifies security services as part of the standardisation of telecommunication systems.

1 Introduction

Until well into the seventies, research in the field of cryptography, and consequently the use of cryptographic techniques for information security, was largely restricted to government institutes. The increasing influence of information technology, its spread to everyday life and its need for security products inevitably resulted in a surge of activity in this field that affected both the IT industry and academic institutions. The need for protecting (open) systems also produced a response from international standardisation bodies. A prominent role was played by the Consultative Committee on International Telegraphy and Telephony (CCITT) which published its Recommendation X.509, *The Directory - Authentication Framework* in 1988.

The first International Standards were published in the mid-eighties by the Technical Committee TC 68 "Banking, securities and other financial services" of the International Organization for Standardization (ISO). They were based on the Data Encryption Standard (DES) and its modes of operation [10,11] of the US National Bureau of Standards (NBS) for the protection of unclassified government information. These standards had also been adopted by the American National Standards Institute (ANSI) as American national standards.

This period also saw the establishment of an international group to work exclusively on the standardisation of cryptographic techniques. The first meeting of Working Party 1 (WP1) on data encryption of the ISO Technical Committee TC 97 "Information processing" took place in January 1981. In 1984 WP1 was transformed into the subcommittee SC 20 "Data cryptographic techniques". The scope was the standardisation of cryptographic techniques for use within information processing

B. Preneel, V. Rijmen (Eds.): COSIC'97 Course, LNCS 1528, pp. 353-365, 1998.

systems. SC 20 had three WGs dealing with "Secret key algorithms and applications" (WG 1), "Public key crypto-systems and modes of use" (WG 2) and "Use of encipherment techniques in communication architectures" (WG 3). The programme of work included the standardisation of encryption algorithms such as the DES. In 1986, after several years of preparatory work, ISO 8227 "DEA1 (Data Encryption Algorithm 1)" was ready for publication. In early 1986 the USA had however proposed to TC 97 to change the scope of SC 20 so that it would not develop standards for encryption algorithms. TC 97 recognised at its Plenary meeting in May 1986 that the standardisation of encryption algorithms was a politically sensitive area of activity in several member countries and referred the issue to the ISO council. The council decided not to publish ISO 8227. Furthermore, all other work on the standardisation of cryptographic algorithms had to be discontinued shortly afterwards. Due to this change in its programme of work and the complexity of its topics SC 20 only completed two standards until it was dissolved in 1989. For more information on the early days of the security standardisation within TC 97 see [20].

The discussion on the need to standardise cryptographic algorithms did however continue. While TC 68 still standardises such algorithms for use in banking, the scope of SC 27, the committee which succeeded SC 20, explicitly excludes their standardisation for Information Technology. A new initiative was taken at the October 1996 plenary meeting of SC 27 where consensus was reached to ask the parent body JTC 1 to lift this restriction. The JTC 1 plenary meeting in December 1996 unanimously agreed to have the revised scope of SC 27 balloted by its national member bodies.

Cryptographic algorithms constitute only one component of the security package required for the (cryptographic) protection of information systems. Message authentication to detect manipulations, authentication of network nodes, computers and users to prevent unauthorised access, management of the (secret) keys used for the algorithms, criteria for the evaluation of systems and management guidelines are only a few examples of standardisation projects in the field of IT security carried out by standardisation bodies and industry organisations throughout the world.

2 International Standardisation

Besides the International Organization for Standardization (ISO) there are two organisations which are involved in standardisation issues on a global level. These are the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU), the Telecommunication Standardization Sector (ITU-TS) of which took over the work of the CCITT. Apart from these organisations there are regional bodies such as CEN, CENELEC and ETSI in Europe and industry interest groups such as IEEE, the Institute of Electrical and Electronic Engineers, and ECMA, the European Computer Manufacturer's Association, which are heavily involved in the standardisation of security techniques. Such groups have, due to their

close link with applications and their implementations, the necessary resources in manpower and time. They can create (regional) de-facto standards which may in the medium term compete with the International Standards from ISO, IEC and ITU. Those are usually not application specific, more on a generic level and take, due to the multitude of interests of the supporting organisations, companies, and delegates as well as quite often a lack of resources, much longer to complete.

In the remaining part of this chapter we will restrict the discussion to the work of ISO and IEC. For information on the general terms and their definitions concerning standardisation and related activities of ISO and IEC see the ISO/IEC Guide 2 [14] which is published in the three official languages English, French and Russian.

2.1 JTC 1

In 1987 ISO and IEC founded the Joint Technical Committee 1 (JTC 1) "Information technology" to harmonise their standardisation efforts in this field. JTC 1 took over the work of TC 97 and, in particular, the standardisation of security techniques. The "Banking Committee" TC 68 continued to develop, as an independent ISO committee, its own security standards. JTC 1 has currently 20 subcommittees covering the various aspects of the standardisation of Information Technology. These range from "Vocabulary" (SC 1), which plays an important part in ensuring the compatibility of standards, via "Programming languages, their environments and systems software interfaces" (SC 22) to "Open-edi" (SC 30), which is producing generic IT standards for open electronic data interchange, and to "Automatic data capture", on which the newest committee, SC 31, is working. It should be noted that the number of a subcommittee which has been dissolved is not re-used. For up-to-date information not only on JTC 1 but on all ISO committees the reader is referred to the "ISO Bulletin" [12] which is published monthly and contains the meeting calendars of the TCs and SCs, a listing of all documents having been sent for ballot and standards having been published, confirmed or withdrawn.

Standards for products and aspects of IT security are developed in particular by SC 17 "Identification cards and related devices", SC 21 "Open systems interconnection, data management and open distributed processing" and SC 27 "Information technology - Security techniques". Whereas the security related activities of SC 17 concentrate mainly on smart cards, i.e. integrated circuit cards with microcomputers, SC 21 develops general security frameworks (e.g. for authentication) as part of its scope covering the various aspects of OSI. The work of SC 27, which a "pure" security committee, will be discussed in detail later.

Members of JTC 1 and its subcommittees are national standards institutes, whereby each country may be represented by one institute only. As of March 1996, 29 countries participate in the work of JTC 1 as so-called P(articipating)-members with the right to vote, while 27 countries have the status of an Observing Member (O-member). It should be noted that a P-member of an SC is not necessarily a P-

member of JTC 1 and vice versa. Voting takes place on a "one body, one vote" basis. Details on the structure of JTC 1 and its operational procedures can be found in the "Directives" [15].

2.2 The Security Committee

SC 27 which was established by JTC 1 in 1989 as the successor to SC 20 had its first Plenary meeting in Stockholm in April 1990. SC 27 took over most of the work items of SC 20 with the exception of those of SC 20/WG 3 which were assigned to SC 6 "Telecommunications and information exchange between systems" and the already mentioned committee SC 21. The scope of SC 27 is the standardisation of generic methods and processes for IT security. Important aspects of the work beyond the purely cryptographic part of IT security include terminology, guidelines for IT security management and criteria for the evaluation of IT security. Explicitly excluded are the standardisation of cryptographic algorithms and the incorporation of the security mechanisms into applications. A synopsis of each project of SC 27 is contained in the "Standing Document" *SD7: Catalogue of SC 27 Work Items and Standards*. A listing of the current documents of the projects, the names of the Project Editors and the target dates is contained in SD4, the *SC 27 Programme of Work*. Both documents are updated after every meeting of the three Working Groups of SC 27 and are available on the Web [17,18].

The day-to-day work of the subcommittee is handled by the Secretariat, which is currently held by DIN (the German institute for standardisation), and the SC 27 Chairman. He chairs the annual Plenary meeting of SC 27 and is supported in this by the Secretariat. The Plenary is responsible for the technical and administrative "guidance" of the WGs. It appoints the Conveners (i.e., the chairpersons of the Working Groups), approves at a WG's suggestion the promotion of a project to the next higher level (see below), is responsible for setting up new projects, has to endorse the appointment of Project Editors and Liaison Officers proposed by a WG (or relieves them of their duties) and deals with general questions relating to its field of work. As of October 1996 SC 27 had 21 P-members and 11 O-members.

2.3 The Working Groups of SC 27

As in most of the subcommittees the detailed technical work on the projects is done in Working Groups (WGs). The three WGs of SC 27 meet twice a year. The meetings are held at the same time in the same location to stimulate the exchange of ideas, to improve the flow of information and to achieve the necessary alignment of the projects assigned to the groups.

2.3.1 SC 27/WG 1: Requirements, Security Services, and Guidelines

The work of WG 1 comprises, as its title suggests, the following activities:

- Identification of application and system requirement components.
- Development of models for services the mechanisms of which are specified by WG 2.
- Development of supporting interpretative documents such as security and management guidelines, glossaries and risk analyses.

The first standard completed by WG 1 was the *Register of Cryptographic Algorithms* (ISO/IEC 9979: 1991). This register had been developed to help users to overcome the problems inflicted by the decision that there was no standardisation of cryptographic algorithms by SC 27 as stated in its Scope and Area of Work. The information on an algorithm contained in the register depends on its provider. A listing of the algorithms registered is contained in SD7 [18]. Other standards developed by WG 1 include the general part for the multi-part standards on entity authentication (ISO/IEC 9798: 1991) and key management (ISO/IEC 11770: 1997).

Due to the nature of the topics most other projects within WG 1 will be published as so-called Technical Reports. Of particular interest are the "Guidelines for the Management of IT Security (GMITS)" and the "Trusted Third Party Services". The first part of the five part report on GMITS discusses concepts and models for IT Security and is due to be published as ISO/IEC TR 13335-1. Parts 2 and 3 which deal with the management and planning and the techniques for the management of IT security, respectively, are in an advanced state. Work on the baseline approach and aspects on the application of services and mechanisms has only just started. For more information on these and the other projects of WG 1 the reader is referred to [18]. Also quite recent is the work on Trusted Third Party Services which are needed for the introduction of public-key cryptography on a large scale in an open environment and for non-repudiation services as well as the "consequential" arbitration required for such systems.

WG 1 is also the main liaison body of SC 27 to the outside world both within and outside of JTC 1 and the realms of ISO and IEC. This and the fact that standards are (supposed to be) made for users are reflected in WG 1's Terms of Reference: "WG 1 recognises that it is user oriented and must satisfy the needs of a diverse community. This community ranges from security technicians to standards developers, all with varying concerns and needs (e.g., regulatory, financial, business, technical). The areas of need are also taken to include the systems and/or applications of the open systems environment. SC 27/WG 1 must maintain an awareness of other security-related activities outside of JTC 1".

2.3.2 SC 27/WG 2: Security Techniques and Mechanisms

WG 2 has essentially taken over the work of the two WGs of SC 20 dealing with secret key algorithms and public key crypto-systems. The merging of these fields of cryptography proved advantageous for the standardisation process. Work and status of WG 2 can probably best be summarised by quoting from its Terms of Reference:

"WG 2 provides a centre of expertise for the standardisation of IT Security techniques and mechanisms within JTC 1."

One of the first (international) standards for a digital signature concept was published in 1991 as ISO/IEC 9797 *Digital signature scheme giving message recovery*. Due to the nature of the algorithm, which could - as often is the case in such a scheme - also be used for enciphering data by reversing the roles of the entities involved, the actual process is described in an informative annex. This standard was used in the drafting of Part 1 of the *Digital Signature Standard (DSS)* (ANSI X9.31). To cover the case of messages which need to be compressed prior to being signed, SC 27 is developing a second part of ISO/IEC 9796 under the title "Mechanisms using a hash-function" as well as parts dealing with check-functions and the discrete logarithm. An overview on standards for the authentication of entities and messages is contained in [6].

The work of WG 2 covers the whole range of cryptographic topics on security mechanisms. Scope and Terms of Reference state that the "Areas of work include, for example, mechanisms relating to authentication, access control, confidentiality, key management, non-repudiation and data integrity. Techniques may be cryptographic or non-cryptographic". Though the scope explicitly mentions non-cryptographic techniques there are currently no such projects discussed within WG 2 due to lack of contributions and experts in this field.

The following is a list of topics contained in the Programme of Work of WG 2. It should be noted that the projects usually deal with both symmetric and asymmetric techniques though these may be in a different state of completion. Some projects also include a part dealing with zero-knowledge techniques. For details on the projects and the degree of completion the reader is referred to [17,18].

- Modes of operation (2 International Standards);
- Entity authentication (5 parts, four have been published as an IS);
- Data integrity mechanism (message authentication codes) (1 IS);
- Non repudiation (3 parts);
- Digital signature schemes (2 parts, one has been published as an IS);
- Digital signature with appendix (3 parts);
- Hash - functions (4 parts, two have been published as an IS);
- Key management (3 parts, one has been published as an IS).

2.3.3 SC 27/WG 3: Security Evaluation Criteria

When forming SC 27 it was recognised that the scope of the former SC 20 was too limited as it only covered techniques (apart from the projects of WG 3 on communication architectures) but not issues such as management guidelines and criteria for the evaluation of IT security. WG 3 was set up to develop a three-part standard on the latter based on the "Provisional Harmonised Criteria" for France, Germany, the Netherlands and the UK (ITSEC [2]). Details on this topic can be found in the report of a CEN project team [3] which also contains a proposal for a European solution. This paper has, however, been shelved due to the activities of Germany,

France, Canada, the USA and the UK, which have set up a working group, the Common Criteria Editorial Board (CCEB), to harmonise the "Provisional Harmonised Criteria" (ITSEC) with those of the USA and Canada and to develop the "Common Criteria". It was recognised that the work of the CCEB had of course some influence on the progress and work of WG 3 and a formal liaison was established between the two groups in October 1993. This proved beneficial to both parties as, in particular, several delegates and Project Editors of WG 3 were also members of the CCEB which ensured the flow of information. In April 1996 it was decided to replace the Working Drafts developed by WG 3 by the respective documents of the CCEB. They were then circulated as a CD.

The Terms of Reference of WG 3 also include administrative procedures for evaluation, certification, and accreditation schemes as well as assessment and testing methods. A new work item on the registration procedures for protection profiles has been agreed within JTC 1 and a study period on testing and assessment methods was initiated by SC 27 at its Plenary meeting in Seoul in November 1995.

3 Standards

Standardisation bodies produce standards. What is a standard and what are the rules governing the development, the voting process and the maintenance of a standard? There is no standard definition of what comprises a standard as the interests of the various committees are too diverse.

The ISO Memento [13] which is published annually in English and French by the ISO Central Secretariat provides the following information on ISO: "ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies, at present comprising 118 members, one in each country. The object of ISO is to promote the development of standardization and related activities in the world with a view to facilitating international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity. The results of ISO technical work are published as *International Standards*."

How does one get from a first idea to an International Standard? As a rule, an International Standard and a Technical Report will pass through the following stages in the course of its life.

Study Period: This period allows a committee to (informally) study a subject which is considered to require standardisation. The outcome of a study period should be a documentation showing that the topic should either be dropped or subjected to an NP ballot.

New work item Proposal (NP): A proposal put forward by the JTC 1 Secretariat to the national member bodies of JTC 1 (in response to an application from an SC or a national body) that a subject should be adopted by an SC as a new work item.

Working Draft (WD): Internal document of the WG or SC dealing with the project.

Committee Draft (CD), Preliminary Draft Technical Report (PDTR): If a WD is considered sufficiently stable, it is registered by the SC as a CD (formerly: Draft Proposal) with the Information Technology Task Force (ITTF) of ISO/IEC in Geneva. It is then circulated for a three months letter ballot by the SC to the national member bodies of the SC for their comments. In the case of a PDTR the document is distributed by JTC 1.

Draft International Standard (DIS), Draft Technical Report (DTR): If a CD has received the necessary support, and no more technical modifications are to be expected, the SC requests the ITTF to ballot the document as a DIS. The ballot is at JTC 1 level and lasts for four months. If the DIS receives the necessary support (see [15]) then there is, generally speaking, no further obstacle to it being published as an International Standard. DTRs are as PDTRs distributed by JTC 1.

International Standard (IS), Technical Report (TR): Following publication as an International Standard or Technical Report, any technical errors discovered can be pointed out by means of a "Defect Report". On the basis of this report, submitted by a national member body, the SC decides whether the standard is to be revised or, possibly, withdrawn.

Review: Every standard/report is reviewed by JTC 1 at five-year intervals. At this point it may be confirmed for another five years, withdrawn or revised. Prior to the formal decision by JTC 1 the SC responsible for the project analysis the standard and issues a recommendation to JTC 1.

Looking at the times needed to process a document at the various stages, whereby circulation for comments at WD level and letter ballots at CD level are usually carried out more than once, and bearing in mind that the WGs meet only twice a year, it becomes clear that the anticipated time of three years from conception to publication of a standard is achievable only under optimum circumstances. It is in fact the exception rather than the rule. In the field of Information Technology, such lengthy gestation periods do not always keep up with the demands of the market. To speed up the work JTC 1 has established some new procedures such as the shortening of the DIS letter ballot from six to four months, the "Fast Track Procedure" by means of which an existing national standard can go straight to DIS level and the possibility to have "parallel" voting on a new project as both an NP and a CD. Details on the phases in the life of a standard and the rules for its development are given in [15,16].

4 European Standardisation

In an age of globally operating companies and a (more or less) open international marketplace, the existence of regional standardisation bodies at first seems anachronistic, and not necessarily conducive to general technical and economic progress. However, standards also reflect common interests, which can be translated much more quickly into standards on a regional level and, as a result, into market share on a wider level. The importance of European standards was underlined by the EC Commission in its Green Book of October 1990 on the development of European standardisation [19].

4.1 The European Bodies

The bodies corresponding at European level to the three international standardisation organisations ISO, IEC and ITU are the "Comité Européen de Normalisation" (CEN), the "Comité Européen de Normalisation Electrotechnique (CENELEC) and the "European Telecommunications Standards Institute" (ETSI). The Bulletin of the European Standards Organizations [5], a monthly report published jointly by the three institutes, contains a list of adopted and draft standards, as well as information on important decisions and mandates of the three organisations. Information on the European standardisation requirements for information systems security can be found in a joint document of the three bodies [4]. The impact of the Commission's Green Book about the security of information systems [1] on the work of CEN and CENELEC remains to be seen.

To prevent duplication of effort, agreements between the three European bodies CEN, CENELEC and ETSI on one side and ISO, IEC and JTC 1 on the other side have been or are about to be signed. Both the "Vienna Agreement" between ISO and CEN as well as the "Lugano Agreement" between CENELEC and IEC were signed in 1991. The agreement between ETSI and JTC 1 has been concluded in November 1996 and is subject only to ratification.

Membership of CEN and CENELEC is along the same lines as membership of ISO and IEC, i.e., through the national standards institutes of the EU and EFTA countries. Each organisation has currently 18 members as well as affiliates from central and eastern Europe. Different is the use of a weighted voting system. While all members of ISO and IEC have formally the same rights, the weight of a member of the European organisations ranges from 1 to 10 depending on the size of the country.

4.2 ETSI

The European Telecommunications Standards Institute which is based in Sophia Antipolis, France, was established in 1988 with the aim of accelerating technical harmonisation in all areas of telecommunication in view of the development of a

common market. Membership is open to all companies and organisations with an interest in the creation of European telecommunications standards and the companies themselves nominate their delegates to the committees. The national standards bodies simply co-ordinate the voting.

The standards developed by ETSI are dedicated to a specific application or technology and quite often form at the same time the basis for implementation by industry. The definition of an ETSI standard thus differs substantially from those quoted above: "A standard is a document that contains technical specifications laying down the characteristics required of a product, such as levels of quality, performance, safety or dimensions. It includes the requirements applicable to the product, as regards terminology, symbols, testing and test methods, packaging, marking or labelling."

The standards which have been developed for GSM, the Global System for Mobile communications, and DECT, the Digital Enhanced Cordless Telecommunications system, include security models and risk analysis as well as the parameters and routines necessary for the implementation of the security functions. The European Telecommunications Standard ETS 300 175-7 [7] contains a risk analysis of DECT as well as authentication mechanisms and key management procedures.

The specification of GSM as a digital, cellular mobile telecommunications network and its security functions started in 1983 within CEPT and is now handled by ETSI. Security functions in this context are, in particular, the cryptographic authentication of the user (using a chip card with non-volatile memory and microprocessor), the use of temporary identities to prevent a users' whereabouts being traced, and the enciphering of user data and user-related signalling information on the air interface. The cryptographic algorithms used for these purposes are handled on a need-to-know basis. To achieve interoperability and the possibility to roam across boarders and networks without any loss of security, the functions and features as well as the parameters had to be standardised [8,9]. The Technical Committee responsible for GSM has now established its own SubTechnical Committee to look after the security aspects of GSM and UMTS, the future Universal Mobile Telecommunications Systems. For an overview of the security functions and aspects of GSM the reader is referred to [21].

ETSI has also established two groups which solely deal with security aspects. The Security Techniques Advisory Group (STAG) was founded in 1992 to co-ordinate the security activities of the various committees and to advise them on security matters. It is also responsible for guidelines on the introduction of security services and for drafting design specifications for algorithms. The development of these algorithms and the protocols is the responsibility of the Security Algorithm Group of Experts (SAGE).

5 Outlook

Standardisation in the field of IT security is currently at a decisive stage. The work of SC 27 is gaining momentum which is manifested in an increasing number of important standards having been published or close to being completed. They are, however, competing with an even more increasing number of national and industry standards as well as other International Standards not only in the "key-cryptography" area of WG 2 but also in the field of management and general concepts of IT Security. Whether SC 27 is going to be a key player will depend not only on the acceptance (marketing) of its work but also whether it can improve its time to market ability, its standards become more "applicable" by including cryptographic algorithms and thus form the basis from which to derive application specific standards. Two important steps have been taken with respect to the last two issues, the already mentioned initiative to standardise cryptographic algorithms and the discussions with TC 68 about a close co-operation. The latter was agreed upon at a joint meeting of the two committees in early October 1996 and was endorsed later that month by the SC 27 Plenary. As a first step it is envisaged to set up a co-ordination group consisting of the SC 27 WG conveners and the TC 68 subcommittee chairmen to achieve a close liaison not only with respect to general matters of common interest and new projects but also to harmonise existing standards when they come up for review.

There are several other aspects which influence the status and the success of SC 27. The readiness to make funds available for "general" standardisation work has noticeably diminished. Furthermore, the sole existence of the various committees, a certain amount of sometimes unavoidable parallel development, or simply the lack of the basic standards, can result in International (or de-facto) Standards which, in spite of dealing with the same topics and having the same objectives, are not compatible with each other and lead to incompatible products. Efficiency and resources could doubtless be improved by better co-ordination between the committees through improved liaison (instead of working in parallel), the clearer definition of competencies, and, as contradictory as it may sound, shorter intervals between meetings. At least within ISO and IEC this should be achieved by having only one committee under whose roof all general as well as all application specific security standardisation should be united. Structures and procedures that have developed over many years are, however, very difficult to change.

Glossary

CCITT	Comité Consultatif International Télégraphique et Téléphonique
CD	Committee Draft
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Electrotechnique
DIS	Draft International Standard
DTR	Draft Technical Report
ETSI	European Telecommunications Standards Institute

FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
IS	International Standard
ISO	International Organization for Standardization
ITU	International Telecommunications Union
PDTR	Preliminary Draft Technical Report
SC	Subcommittee
TC	Technical Committee
TR	Technical Report
WD	Working Draft
WG	Working Group

References

[1] CEC, *Green Book on the Security of Information Systems*, Draft 3.6, July 1993.

[2] CEC, *Information Technology Security Evaluation Criteria (ITSEC)*, Office for Official Publications of the European Communities, Brussels, Luxembourg, 1991.

[3] CEN, *European Standardization of the IT Security Evaluation Criteria*, CEN Project Team PT05, issue 1.1, March 1993.

[4] CEN/CENELEC/ETSI, *Taxonomy and Directory of European Standardisation Requirements for Information Systems Security*, M-IT-06.

[5] CEN/CENELEC/ETSI, *The Bulletin of the European Standards Organizations*. Published 11 times a year by CEN, CENELEC, ETSI, subscriptions c/o CEN Infodesk, 36, rue de Stassart, B-1050 Bruxelles, Belgium.

[6] M. De Soete and K. Vedder, *Authentication Standards*, in: W. Wolfowicz (ed.): *State and Progress of Research in Cryptography*, Fondazione Ugo Bordoni, Rome 1993, 207-218.

[7] ETS 300 175-7, *Digital Enhanced Cordless Telecommunications (DECT), Common interface, Part 7: Security Features*, 1996 (2nd edition).

[8] ETS 300 506 (GSM 02.09), *Digital cellular telecommunications system (Phase 2); Security aspects.*

[9] ETS 300 534 (GSM 03.20), *Digital cellular telecommunications system (Phase 2); Security related network functions.*

[10] FIPS 46: 1977, Federal Information Processing Standards Publication, *Data Encryption Standard*, National Bureau of Standards.

[11] FIPS 81: 1980, Federal Information Processing Standards Publication, *DES Modes of Operation*, National Bureau of Standards.

[12] *ISO Bulletin*. Published monthly by ISO Central Secretariat, 1, rue de Varembé, CH-1211 Geneva 20.

[13] *ISO Memento*, ISO Central Secretariat, Geneva, 1996.

[14] *ISO/IEC Guide 2:1991, General Terms and Their Definitions Concerning Standardization and Related Activities*, ISO and IEC, Geneva, 1991 (6th edition).

[15] ISO/IEC, *Directives, Procedures for the technical work of ISO/IEC JTC 1 on Information Technology*, Geneva, 1995 (3rd edition).

[16] ISO/IEC, *Directives Part 3, Drafting and presentation of International Standards*, Geneva 1989 (2nd edition).

[17] ISO/IEC JTC 1/SC 27, *Standing Document 4: Programme of Work*, http://www.iso.ch:8080/ISOWeb.html.

[18] ISO/IEC JTC 1/SC 27, *Standing Document 7: Catalogue of SC 27 Work Items and Standards*, http://www.iso.ch:8080/ISOWeb.html.

[19] Kommission der Europäischen Gemeinschaften, *Grünbuch der EG-Kommission zur Entwicklung der europäischen Normung: Maßnahmen für eine schnellere technologische Integration in Europa*, KOM(90) 456, Brüssel 1990.

[20] L. Krause, *Data Encryption in ISO, the International Organization for Standardization*, Computers & Standards 3 (1984), 195-198.

[21] K. Vedder, *GSM: Security, Services and the SIM*, this volume, pp. 227-243.

The author joined JTC 1/SC 20 in 1988 as a delegate of the German national member body. He was Project Editor for the International Standards ISO/IEC 9798-3: 1993, *Entity authentication mechanisms - Part 3: Entity authentication using a public key algorithm* and ISO/IEC 9797: 1994 (2nd edition), *Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm*. From 1992 until 1996 he was chairman of the security committee ISO/IEC JTC 1/SC 27 "Information technology - Security techniques".