ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 038

August 1995

Source: ETSI TC-NA/STAG

Reference: DTR/NA-002401

ICS: 33.020

Key words: Security standards policy

Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy

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

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI). It was given the classification of TCR-TR by the 20th TC Chairmens' Co-ordination (TCC) meeting and approval by the 22nd Technical Assembly (TA).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilized by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

This TCR-TR is a guide to a series of technical reports being prepared by STAG and known collectively as the ETSI security standards policy. All ETSI technical committees with an interest in including security features in their specifications or reports are invited to make use of this report as a guide to the ETSI security standards policy and the way in which they should use it.

Blank page

1 Scope

The ETSI security standards policy is being produced by STAG in order to foster a consistent approach to the inclusion of security features in ETSI telecommunications standards and technical reports. The policy is being produced as a set of TCR-TRs which will provide guidelines to ETSI technical committees on the inclusion of security features in their technical specifications or reports. The scope of this TCR-TR is to provide an introduction to the policy by outlining the purpose and scope of the reports which make up the policy, the relationships between them, and the way in which they should be used by a technical committee in consultation with STAG.

2 Normative references

For the purposes of this TCR-TR, the following reference applies:

ISO/IEC 9797:1989 (E): "Data cryptographic techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm".

3 Abbreviations

For the purposes of this TCR-TR, the following abbreviations apply:

ISO	International Standards Organisation
SAGE	ETSI Security Algorithms Group of Experts
STAG	ETSI Security Techniques Advisory Group

4 Introduction

The material presented in the rest of this TCR-TR is organized as follows.

Clause 5 is concerned with the objectives of the ETSI security standards policy. It explains the need for the policy, and defines the scope and structure of the policy. Clause 6 consists of a description of the way in which those ETSI technical committees who need to include security features in their standards or reports should use the policy. The description is given in terms of a two part process for determining what security features should be included in a specification and how they should be included, a process that should usually be carried out by the technical committee in consultation with STAG.

A complete list of the technical reports which together form the ETSI security standards policy is given in annex A.

5 Objectives of the ETSI security standards policy

5.1 Need for the policy

The need for organizations to ensure the confidentiality, integrity, authenticity, availability and accountability of the information they process and transmit electronically, in an economical way and to an assured standard, is leading to an increased demand for technical standards with integrated security features. This demand has led to the ETSI Technical Assembly recognizing the need for an ETSI security standards policy to address the provision of security features in ETSI technical specifications and reports.

5.2 Scope of the policy

The ETSI security standards policy consists of guidelines and recommendations that are designed to ensure a consistent approach to the provision of security features in ETSI technical specifications.

The topics addressed by the policy are: security requirements capture, security mechanisms (in particular standardized security mechanisms), security evaluation and the potential impact on the security standardization process of the legal and regulatory environments in which systems conforming to ETSI specifications may be deployed.

The set of documents that make up the ETSI security standards policy is not intended to replace the advice on security matters which a technical committee may obtain by consulting STAG directly. Instead it is intended that the documents should supplement and complement such advice, and help foster an understanding of the scope of the advice that STAG is able to provide. Therefore, the documents do not treat the subjects which they address in any great depth, but rather serve as a means of alerting their readers to the issues which need to be considered when designing security features into a technical specification.

5.3 Structure of the policy

The ETSI security standards policy is presented as a set of TCR-TRs, which is divided into four series, each series dealing with one of the topics addressed by the policy.

- The DTR/NA-0025xy series of TCR-TRs provides a framework for identifying, analysing and documenting requirements for security features. The series includes a glossary of security terminology and a directory of security features in ETSI specifications. Use of this series of reports will help ensure a comprehensive and consistent approach to identifying requirements for security features in ETSI technical specifications.

- The DTR/NA-0026xy series of TCR-TRs provides catalogues of security mechanisms and security management techniques, guidelines on how to integrate security mechanisms into technical specifications, and guidelines on specifying requirements for cryptographic algorithms. The series should be used to help define the security mechanisms that will be included in a technical specification. Use of this series of reports will help ensure a consistent approach to the type and level of integration of security features in ETSI technical specifications.

- The DTR/NA-0027xy series of TCR-TRs provides guidelines to standards and recommendations which should be used if some or all of the security features in a system which conforms to an ETSI technical specification are expected to meet and be evaluated against internationally recognized security criteria. Use of this series of reports will help ensure that ETSI technical specifications are compatible with international standards for security evaluation.

- The DTR/NA-0028xy series of TCR-TRs provides guidelines to European and other legislation, recommendations or guidelines which could influence decisions about the inclusion or nature of security features in an ETSI technical specification. Use of the series should help to ensure that the security features in ETSI technical specifications are compatible with the legal and regulatory environments in which systems conforming to the specifications may be used.

6 Using the ETSI security standards policy

6.1 Overview of the process

It is recommended that security features for inclusion in an ETSI standard are determined by means of a two stage process. The first stage of the process, the security requirements capture stage, identifies the security features that need to be included in the standard. The second stage of the process identifies the features themselves. Because the provision of security features in a system may itself generate new security requirements, it may be necessary to iterate the process.

6.2 Consultation with STAG

At any stage in the process of defining the security features for inclusion in a specification, the technical committee undertaking the work is encouraged to consult STAG.

Consultation with STAG is particularly advisable during periods when some of the reports that make up the ETSI security standards policy are still being prepared or are being revised, or for questions relating to aspects of the policy which are susceptible to change. This includes, for example, questions about regulatory aspects of security provision such as lawful interception and export control of cryptographic products, where the situation can be very changeable and internationally variable. Similarly, when considering security evaluation, the technical committee should consult STAG directly because of the current uncertainty with regard to the potential impact of security evaluation on standardization. Assistance from STAG should also be requested if cryptographic algorithms are required. Any requirements specification for a cryptographic algorithm must be submitted to STAG for review.

6.3 Security requirements capture

The set of security features which need to be specified in an ETSI standard is identified by first setting objectives for the security of systems conforming to the standard. Security requirements for such a system are captured by considering, within the context of the security objectives, the threats to the system, the security expectations of users of the system and the legal and regulatory environments in which the system may be deployed. Once the security requirements have been identified, a list of security features to address them is prescribed. The list may then be filtered to exclude features which are not considered appropriate for standardization. This process results in a decision to include in the standard a particular set of security features.

A number of the reports which form the ETSI security standards policy should be used in the process outlined in the paragraph above in the following way:

- when considering the security objectives for a telecommunications system and the threats to the security of that system, DTR/NA-002501 [6] should be consulted. That report outlines a methodology for conducting a threat analysis and for formulating security requirements based on such an analysis;

- two of the reports in the policy should be consulted when considering security expectations of users. These are TCR-TR 029 [2] and DTR/NA-002701 [10]. The first of these reports provides an overview of the security features that have already been incorporated in ETSI standards, and which may therefore be considered as indicative of user expectations. The second report provides a summary of the situation regarding security evaluation and an assessment of the potential impact of security evaluation on standardizing security features. That report need only be used if it is expected that systems which conform to the standard are required to be submitted to a formal security evaluation;

- legal and regulatory considerations are the subject of DTR/NA-002801 [11]. This TCR-TR should be used to ensure that the process of identifying the security requirements pays due attention to legal or regulatory issues, such as lawful interception and controls on export of cryptographic equipment;

- TCR-TR 028 [1] should be used to help ensure an unambiguous definition of the security features which are to be included in the standard, as well as to help ensure consistency in the use of security terminology within ETSI.

The process for identifying those security features which need to be included in a standard, as outlined in this subclause, is illustrated in figure 1.

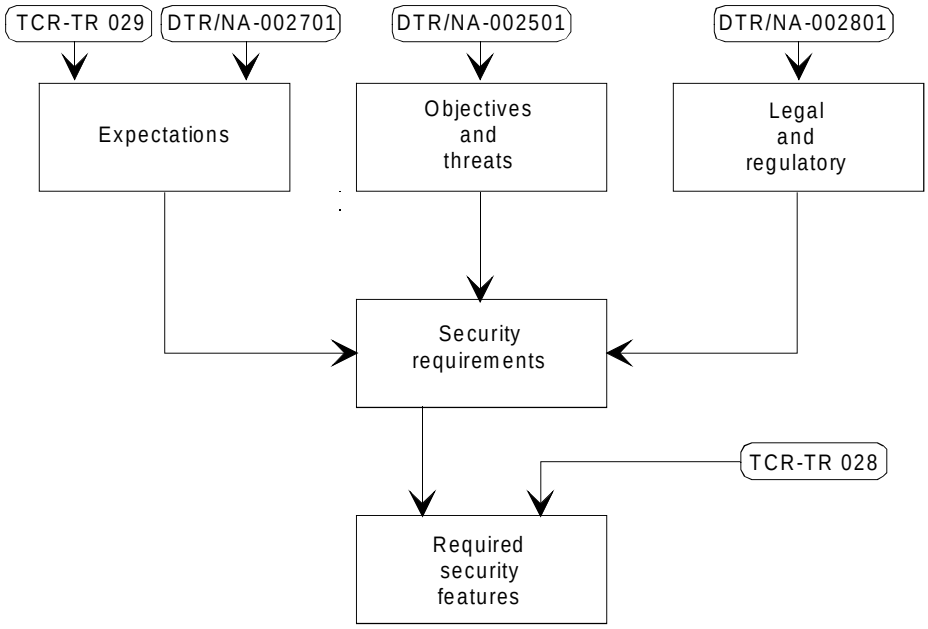

Figure 1: Capturing requirements for security features

6.4 Specification of security features

This stage of the process begins with a list of security features, and is concerned with their specification to a level of detail appropriate for inclusion in the standard. There are four principal steps in the process. The first step is to select suitable mechanisms, often cryptographic mechanisms, for providing the required security features. The second step is to specify any (security) mechanisms that may be needed to manage the security features, and which also need to be included in the standard. The third step is to integrate the various security mechanisms and their associated management mechanisms into the standard. The final step is to specify the requirements for any cryptographic algorithms that are needed by the security mechanisms.

A number of the reports that make up the ETSI security standards policy should be used in the process outlined in the paragraph above in the following way:

- TCR-TR 042 [5] provides a list of security mechanisms, together with guidelines on how to select a mechanism to provide a particular security service or feature. Many of the mechanisms described in that report are ISO standards, mechanisms being considered for standardization by ISO, or mechanisms that have already been used in ETSI standards When selecting security mechanisms, this is the first document which should be consulted. For each mechanism it provides information on what it can be used for, what type of cryptographic algorithm it needs and what its management requirements are. It also gives some indication of the limitations of particular mechanisms, as well implementation information. When selecting security mechanisms, use may also be made of TCR-TR 029 [2], especially if a mechanism is required for a security feature which is the same as, or similar to, one which is known to have been included in another ETSI standard. During the mechanism selection step it is advisable to try to minimize the number of distinct mechanisms that are needed by considering whether some mechanisms can be used to provide a number of different security features;

- when considering management of the security features, in addition to the information given in TCR-TR 042 [5], use may be made of the more general information on how to approach security management given in DTR/NA-002602 [8]. As with the security mechanisms themselves, it may be advisable to look for management mechanisms that can be used to manage a number of the security features;

- integration of security mechanisms into ETSI standards is the subject of DTR/NA-002603 [9]. That report provides guidance on how to integrate security protocols into a telecommunications standard;

- security mechanisms which use cryptographic techniques invariably need cryptographic algorithms for their implementation. Moreover, it is generally the case that published, or standardized, security mechanisms do not include cryptographic algorithms. Typically the mechanism is defined as requiring a particular type of algorithm, but the algorithm itself is left unspecified (for example see the ISO standard for a data integrity mechanism [1]). ETSI has decided that all cryptographic algorithms that need to be standardized for use with ETSI standards should be provided by ETSI TC SAGE. The technical report TCR-TR 030 [3] should be used as a guide to the procedure that needs to be followed in order to prepare and submit to SAGE a requirements specification for a cryptographic algorithm. In order to minimize the number of cryptographic algorithms that may be required for a particular standard, it is advisable to consider whether a single algorithm could be used in a number of different mechanisms. Also careful consideration needs to be given as to whether there is really a need for a standard cryptographic algorithm - if the choice can be left to manufacturers or operators this may be preferable.

During the various steps outlined in the sequence of bullet points given above, it may be necessary to consult DTR/NA-002701 [10] or DTR/NA-002801 [11]. For example, the first of these reports may be consulted during the mechanism selection step because certain mechanisms may be preferred if a particular level of security evaluation is to be achieved. The second report may be useful when preparing a requirements specification for a cryptographic algorithm, for instance as a guide to export restrictions.

The process for specifying security features for inclusion in a standard, as outlined in this subclause, is illustrated in figure 2.

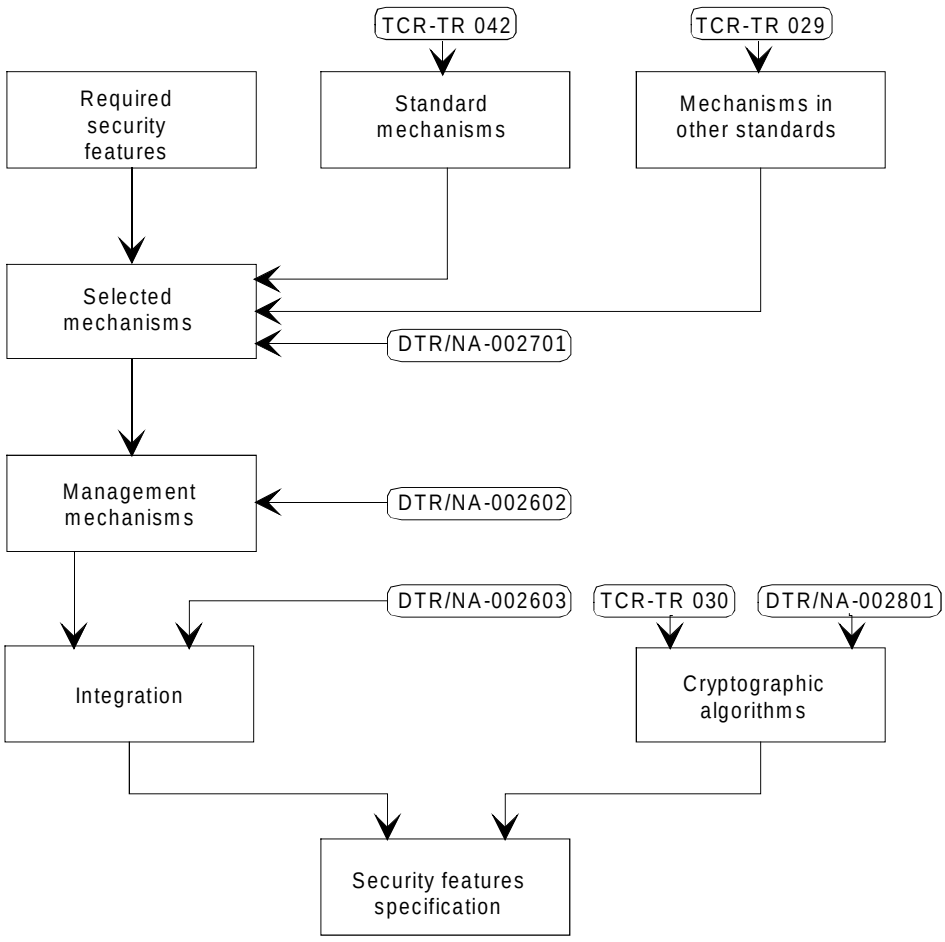

Figure 2: Specification of security features

Annex A: TCR-TRs forming the ETSI security standards policy

[1] TCR-TR 028: "Network Aspects (NA); Security Techniques Advisory Group (STAG); Glossary of security terminology" (DTR/NA-002503).

[2] TCR-TR 029: "Security Techniques Advisory Group (STAG); A directory of security features in ETSI standards" (DTR/NA-002504).

[3] TCR-TR 030: "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms" (DTR/NA-002604).

[4] TCR-TR 038: "Security Techniques Advisory Group (STAG); A guide to the ETSI security standards policy" (DTR/NA-002401).

[5] TCR-TR 042: "Security Technical Advisory Group (STAG); Baseline security standards; Features and mechanisms" (DTR/NA-002601).

[6] DTR/NA-002501: "Security Techniques Advisory Group (STAG); Guidelines and methods for identifying, analysing and documenting security requirements for telecommunication systems and services".

[7] DTR/NA-002502: Unallocated.

[8] DTR/NA-002602: "Security Technical Advisory Group (STAG); Guidelines for security management techniques".

[9] DTR/NA-002603: "Security Technical Advisory Group (STAG); Guidelines for integrating security mechanisms into ETSI standards".

[10] DTR/NA-002701: "Security Techniques Advisory Group (STAG); The relevance of security evaluation to ETSI standards".

[11] DTR/NA-002801: "Security Techniques Advisory Group (STAG); A guide to legislation, recommendations and guidelines governing the provision of security features".

History

Document history			
March 1995	Draft for endorsement by	TCC 20	1995-05-29 to 1995-05-31
June 1995	Final draft for approval by	TA 22	1995-06-19 to 1995-06-20
August 1995	First Edition		
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)		