ETSI ES 202 382 V1.1.1 (2005-04)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);
Security Design Guide;
Method and proforma for defining Protection Profiles

Reference

DES/TISPAN-07009-Tech

Keywords

IP, methodology, profile, protection, security,
VoIP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

Introduction

The present document has been prepared with the sponsorship of the eEurope programme as part of the ETSI support to the eEurope action line for a secure information infrastructure (item 3: Society).

A major part of any security specification, and of a security product, is the measure of assurance it provides with respect to the security it offers.

Information security evaluation contributes to the users' trust and confidence in communications products and services. The use of common criteria for evaluation (as defined in ISO/IEC 15408 [7]) has facilitated mutual recognition of results in many European countries and these countries have also entered into an arrangement with the US and Canada for further mutual recognition of IT security certificates.

The present document is part of a set of standards and guidelines which show how the Common Criteria as identified in ISO/IEC 15408 [7] can be used effectively within the ETSI standardization process. The documents in this set are:

- EG 202 387 [1]: Method for application of Common Criteria to ETSI deliverables;
- ES 202 382: Method and proforma for defining Protection Profiles;
- ES 202 383 [2]: Method and proforma for defining Security Targets.

Between them, these documents identify how standards fit to the Common Criteria and how developers of standards should prepare their standards with a view to support submission for evaluation of product conforming to the standards.

Adoption of Common Criteria objectives in standardization of security countermeasures is also consistent with achieving the objectives and recommendations of the NIS report.

1 Scope

The present document provides guidance on the preparation of Protection Profiles (PP) based upon ETSI communication standards. A PP defines an implementation-independent set of security requirements for a category of communications equipment which is subject to evaluation under the Common Criteria (CC) scheme described in the multipart ISO/IEC 15408 [7].The detailed contents of a PP are specified in ISO/IEC 15408-1 [4].

The use and applicability of the CC to the ETSI standardization process is described in EG 202 387 [1] and further guidance on the implementation of security-related standards in telecommunications equipment is specified in ES 202 383 [2].

Throughout the present document, a worked example of a Protection Profile (PP) for TETRA Direct Mode Operation (DMO) security is used as an illustration. A partially complete PP for TETRA DMO security can be found in annex B.

NOTE: TETRA DMO was chosen as the example in the present document as, although the security analysis results, objectives and requirements are not necessarily collected together in one document, most of this information exists either explicitly or implicitly and it was, therefore, possible to construct a realistic and representative example PP.

Conformance to the present document is established by successful evaluation to the requirements of ISO/IEC 15408-3 [6].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[2] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[3] ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

[4] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[5] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[6] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[7] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [1] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CC	Common Criteria
DMO	Direct Mode Operation
EAL	Evaluation Assurance Level
IT	Information Technology
MT	Mobile Terminal
PP	Protection Profile
TETRA	TErrestrial Trunked RAdio
TOE	Target Of Evaluation

4 Overview

4.1 Common Criteria concepts

The evaluation criteria for IT security, generally referred to as the "Common Criteria (CC)", are defined in the multipart standard, ISO/IEC 15408 [7] and are used as the basis for evaluation of security properties of IT products and systems.

CC evaluation involves the preparation of a Protection Profile (PP) which is considered to be an implementation-independent set of IT security requirements for a category of equipment intended to meet common consumer needs for IT security. Communications standards are independent of any implementation and, thus, those specifying security requirements can be considered to be PPs. Once published, such a PP could be used without modification to specify the security requirements of a specific product or service. Alternatively, it could be extended to include additional requirements where necessary.

ISO/IEC 15408-3 [6] makes provision for a PP to be evaluated under the requirements of the common criteria and it is for this purpose that the PP proforma in the present document has been specified.

4.2 Relationship between a standard and a PP

The information and the requirements expressed in a security-related standard are very similar to those that are expected to be found in a PP. However, because a standard is intended to be the basis for implementation whereas the intended purpose of a PP is to be the basis for evaluation, the presentation and emphasis of the contents is necessarily different in each. The PP proforma for communications standards (annex A), therefore, summarizes the content of the standard in a form that is acceptable as a PP and provides references to clauses where more detailed information can be found.

It is essential that the references to clauses in the base security standard and the Vulnerability Analysis are accurately maintained. To simplify this maintenance, both the PP proforma and the Vulnerability Analysis should be included either as annexes to the base security standard or, where the present document is extensive, as distinct parts of a multi-part document set.

5 PP development

5.1 Elements of a Protection Profile

Figure 1 shows in graphic form the content of a PP required by ISO/IEC 15408-1 [4].

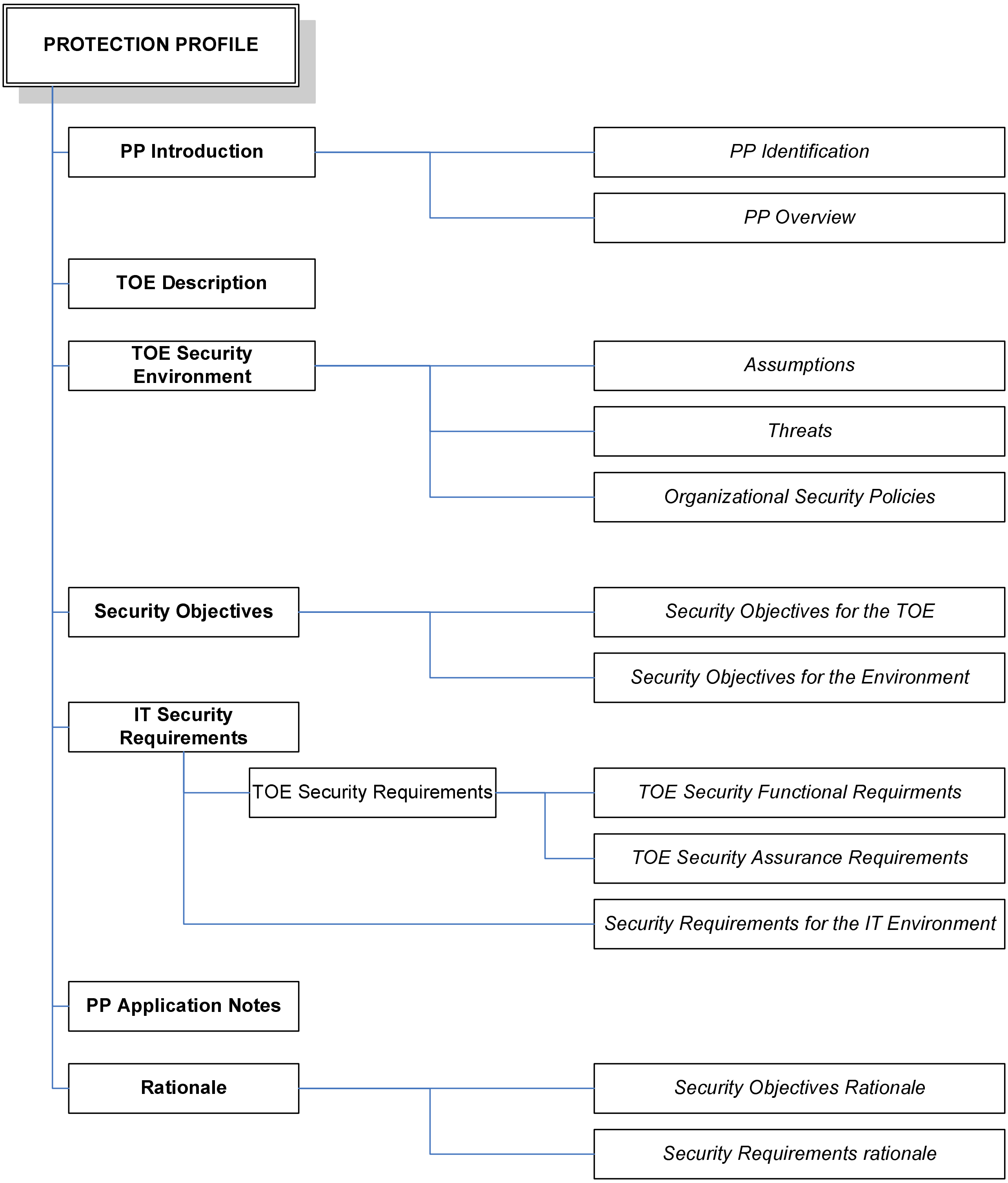
PROTECTION PROFILE
PP Introduction
PP Identification
PP Overview
TOE Description
TOE Security Environment
Assumptions
Threats
Organizational Security Policies
Security Objectives
Security Objectives for the TOE
Security Objectives for the Environment
IT Security Requirements
TOE Security Requirements
TOE Security Functional Requirments
TOE Security Assurance Requirements
Security Requirements for the IT Environment
PP Application Notes
Rationale
Security Objectives Rationale
Security Requirements rationale

Figure 1: Protection Profile content

5.1.1 PP Introduction

5.1.1.1 PP identification

A PP is required to provide enough labelling and descriptive information to enable it to be identified, catalogued, registered and cross referenced. The document number, version, date and full title of an ETSI standard are sufficient for this purpose and should be used.

EXAMPLE:

Introduction					
Doc No.	EN 300 396-6	Version	V1.2.1	Date	2004-05

Full Title	Terrestrial Trunked Radio (TETRA);
	Direct Mode Operation (DMO);
	Part 6: Security				

5.1.1.2 PP overview

A PP should include a narrative summary as part of the Introduction [4]. The purpose of this is to provide enough information that a potential user can make an informed decision on whether the PP is likely to be of interest. A fully specified Scope clause from an ETSI standard meets this requirement and should be used.

EXAMPLE:

Introduction					
Doc No.	EN 300 396-6	Version	V1.2.1	Date	2004-05

Full Title	Terrestrial Trunked Radio (TETRA);
	Direct Mode Operation (DMO);
	Part 6: Security				

Overview	The present document defines the Terrestrial Trunked Radio system (TETRA) Direct Mode of operation. It specifies the basic Air Interface (AI), the interworking between Direct Mode Groups via Repeaters and interworking with the TETRA Trunked system via Gateways. It also specifies the security aspects in TETRA Direct Mode and the intrinsic services that are supported in addition to the basic bearer and teleservices. The present document describes the security mechanisms in TETRA Direct Mode. It provides mechanisms for confidentiality of control signalling and user speech and data at the AI. It also provided some implicit authentication as a member of a group by knowledge of a shared secret encryption key. The use of AI encryption gives both confidentiality protection against eavesdropping, and some implicit authentication.				

5.1.2 Target Of Evaluation description

NOTE 1: Throughout the present document, the term "Target Of Evaluation (TOE)" is used to identify any product which implements the technical requirements of the standard(s) associated with a particular PP.

ISO/IEC 15408-1 [4] requires that a brief but clear description of the Target Of Evaluation (TOE) should be included in a PP. While not expressing the security requirements in detail, this should make the security aspects of the standard clear. If the standard includes a short clause entitled "General Description" (or something similar) early in the document, it is likely that this text will be adequate as the TOE description. In the event that such a clause does not exist it will need to be written for the PP and should include the following:

- identification of the type of product that is likely to implement the standard;

NOTE 2: In the context of the present document, the term "product" should be interpreted in its widest sense to include all types of communications equipment as well as services.

- general summary of the communications features specified in the standard or set of standards;
- brief overview of the security aspects specified in the standard.

EXAMPLE:

TOE Description

TETRA Direct Mode Operation (DMO) offers 4 security classes as follows:

DM-1

No encryption applied.

DM-2-A

The DM-SDU and any related traffic is Air Interface (AI) encrypted. Addresses are not encrypted:

The purpose of security class DM-2-A is to provide confidentiality of user traffic and signalling in applications where it is not necessary to hide the addressing information. It allows calls to be made through a repeater where the repeater is not provided with the capability to encrypt or decrypt messages by maintaining the layer 2 (MAC) elements of any signalling in clear.

DM-2-B

The destination address (SSI), DM-SDU and any related traffic are AI encrypted:

The purpose of security class DM-2-B is to provide confidentiality of user traffic and signalling. It extends the confidentiality applied to signalling over that provided in class DM-2-A to encrypt parts of the MAC header. The encryption allows repeater operation to be made without requiring the repeater to be able to encrypt and decrypt transmissions unless it wishes to check the validity of the destination address. Because the source address is in clear, a pre-emptor can identify the pre-emption slots and hence the call can be pre-empted even if the pre-emptor does not have the encryption key being used by the call master.

DM-2-C

Significant elements of the DMAC-SYNC PDU and the DMAC-DATA PDU are encrypted. Any related traffic is AI encrypted.

The purpose of security class DM-2-C is to provide confidentiality of user traffic and signalling including all identities other than those of repeaters and gateways. The bulk of the MAC header elements are encrypted. Where repeaters are used, the repeater requires the ability to encrypt and decrypt all transmissions. Calls can only be pre-empted by an MS which has the SCK in use by the call master.

5.1.3 TOE security environment

The TOE security environment should describe the security aspects of the environment in which the TOE is intended to be used [4]. It is expected to include:

- security assumptions:
  - security aspects of the environment in which an implementation of a standard will be used;
  - the intended use of the implementation;
  - the physical, user and connection aspects of the environment in which an implementation will operate;
- threats:
  - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
- organizational security policies:
  - any security policies or rules with which an implementation of a standard must comply.

The TOE security environment summarizes the results of a threat analysis of the communications system specified in the base standard. Threat analyses should be prepared following the process described in ETR 332 [3].

EXAMPLE:

TOE		
a.1 Assumptions		
a.1.1	Each security service is totally independent of any other.	DTR/TETRA-06139 clause 9.1.2
a.1.2	Quality of Service (QoS) is not adversely affected by the implementation of security measures	DTR/TETRA-06139 clause 9.1.2
..	..	..
a.2 Assets		
a.2.1	TETRA Mobile Terminal (MT)	DTR/TETRA-06139 clause 9.4
a.2.2	Key management information	DTR/TETRA-06139 clause 9.2
..	..	..
a.3 Threat agents		
a.3.1	Unauthorized user agents	DTR/TETRA-06139 clause 8.2
a.3.2	Authorized user agents	DTR/TETRA-06139 clause 8.2
..	..	..
a.4 Threats		
a.4.2	Interception at the radio interface	DTR/TETRA-06139 clause 8.3.1.1
a.4.3	Use of resources beyond the authorized limits	DTR/TETRA-06139 clause 8.5.2.2
..	..	..
a.5 Security policies (OPTIONAL)		
a.5.1	To protect the TETRA network operator's information and the users' information and interests	DTR/TETRA-06139 clause 9.2
a.5.2	To provide a set of security services which allow TETRA operators to build their own security policy based on the security services.	DTR/TETRA-06139 clause 9.2

5.1.4 Security objectives

A PP should contain a definition of the security objectives of both the TOE and its environment [4]. These objectives are expected to cover the assumptions, threats and policies described in the TOE security environment (see clause 5.1.3). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- security objectives for the TOE:
  - it should be clear which aspects of the identified threats and policies are addressed by each objective;
  - if the base security standard specifies a protocol, it is likely that the TOE security objectives will be specified in the Stage 1 (or equivalent) specification.
- security objectives for the environment:
  - it should be clear which aspects of the identified threats and policies are expected to be addressed by the environment because they are not covered (either wholly or in part) by the TOE security objectives;
  - communications standards rarely specify requirements for the environment so it is unlikely that the security objectives for the environment will be stated explicitly in the base security standard or any associated document. If this is the case, the objectives should be expressed in full in the PP.

EXAMPLE:

b Security Objectives		
b.1 Security objectives for the TOE		
b.1.1	A TETRA system shall be able to provide a high level of confidentiality in private systems used by public safety organizations	ETR 086-3 clause 6.2.3
b.1.2	A TETRA system must be able to prove the true identity of any entity communicating with it	ETR 086-3 clause 6.2.2
..	..	..
b.2 Security objectives for the environment		
	TETRA is specified as a closed system and, as such, it has no security objectives expressed for the environment	

5.1.5 IT security requirements

5.1.5.1 The relationship between security objectives and security requirements

The distinction between security objectives and security requirements is an important one to make. An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. As an example, the following statement is a security objective for a TOE:

> The TOE must identify and authenticate all users before granting access to the system.

One of the security requirements associated with this objective could be:

> A user shall be successfully identified and authenticated to the TOE by means of a user name and password before all other interactions between the TOE and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

5.1.5.2 TOE Security requirements

Security requirements should be identified for both the TOE and, where applicable, its environment [4]. The TOE security requirements should be classified into the following groups:

- TOE security functional requirements:
  - an identification of each of the security-related functional requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found;
  - where possible, in indication of which of the functional components defined in ISO/IEC 15408-2 [5] the requirement represents.
- TOE security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) [6] that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g., EAL3 - EAL5);
  - where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [6] which will apply to an implementation;
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [6].

The specification of security requirements for the environment is optional and should only be included in the PP if security objectives for the environment are identified earlier in the PP (see clause 5.1.4). If requirements for the environment are included, they should be presented in the same way as functional requirements for the TOE.

EXAMPLE:

c IT Security Requirements c.1 TOE security requirements			
c.1.1 TOE security functional requirements			
c.1.1.1	User authentication key generation using the TA11 and TA12 algorithms	FIA_UAU.3	EN 300 392-7 clause 4.1.2
c.1.1.2	Challenge/response user authentication mechanism	FIA_UAU.4	EN 300 392-7 clause 4.1.2
..	..	..	..
c.1.2 TOE security assurance requirements			
c.1.2.1	A TETRA Class 3 implementation can be evaluated at CC EAL4 or above		ISO/IEC 15408-3 [6]
..	..		..
c.2 Environment security requirements (OPTIONAL)			
c.2.1	TETRA is specified as a closed system and, as such, it has no security requirements expressed for the environment		

5.1.6 Application notes (OPTIONAL)

ISO/IEC 15408-1 [4] provides for optional application notes to be included in a PP. It is intended that this should include any additional information that might be considered useful to either or both of the implementor and the evaluator. This clause should be unnecessary if the base security standard has been fully and carefully specified.

EXAMPLE:

d Application notes (OPTIONAL)

Each TETRA security class has associated features that are mandatory or optional and are summarized in the following table.

Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable	End-to-end
	Clause 4	Clause 4	Clause 6	Clause 5	Clause 7
1	O	-	-	M	O
2	O	O	M	M	O
3	M	M	M	M	O

NOTE: M = Mandatory;
O = Optional;
- = Does not apply.					

A Mobile Station may support one, several, or all security classes and each TETRA cell may support one of the following options at any one time:

- class 1 only;
- class 2 only;
- class 2 and class 1;
- class 3 only; or
- class 3 and class 1.

5.1.7 Rationale

ISO/IEC 15408-1 [4] requires that a PP provides a rationale, subdivided into security objectives rationale and security requirements rationale to explain in detail how the security objectives and the security requirements, respectively, address the threats identified in the TOE security environment. This rationale should be included in the Vulnerability Analysis.

EXAMPLE:

e Rationale

The relationship between identified threats, security objectives and security requirements is described in DTR/TETRA-06139.

Annex A (normative): Protection Profile definition proforma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the Protection Profile definition proforma in this annex so that it can be used for its intended purposes and may further publish the completed Protection Profile definition.

Protection Profile					
Introduction					
Doc No.		Version		Date	
Full Title					
Overview					
TOE Description					
a TOE Security Environment					
a.1 Assumptions					
a.1.1					
a.1.2					
a.2 Assets					
a.2.1					
a.2.2					
a.3 Threat agents					
a.3.1					
a.3.2					
a.4 Threats					
a.4.1					
a.4.2					
a.5 Security policies (OPTIONAL)					
a.5.1					
a.5.2					
b Security Objectives					
b.1 Security objectives for the TOE					
b.1.1					
b.1.2					
b.2 Security objectives for the environment					
b.2.1					
b.2.2					
c IT Security Requirements c.1 TOE security requirements					
c.1.1 TOE security functional requirements					
c.1.1.1					
c.1.1.2					
c.1.2 TOE security assurance requirements					
c.1.2.1					
c.1.2.2					
c.2 Environment security requirements (OPTIONAL)					
c.2.1					
c.2.2					
d Application notes (OPTIONAL)					
e Rationale					

Annex B (informative): Example Protection Profile

The following incomplete PP consolidates all of the partial examples used in clause 5 of the present document into a single PP proforma. It is shown here as a guide to completing a PP based on an ETSI standard and is not intended to be a complete and true summary of TETRA DMO security. It makes reference to the following ETSI publications:

- EN 300 396-6
- EN 300 392-7
- ETR 086-3
- DTR/TETRA-06139

  unpublished draft DTR/TETRA-06139.

Protection Profile
TETRA Direct Mode Operation (DMO)

Introduction

Doc No.	EN 300 396-6	Version	V1.2.1	Date	2004-05

Full Title	Terrestrial Trunked Radio (TETRA);
	Direct Mode Operation (DMO);
	Part 6: Security				

Overview	The present document defines the Terrestrial Trunked Radio system (TETRA) Direct Mode of operation. It specifies the basic Air Interface (AI), the interworking between Direct Mode Groups via Repeaters and interworking with the TETRA Trunked system via Gateways. It also specifies the security aspects in TETRA Direct Mode and the intrinsic services that are supported in addition to the basic bearer and teleservices. The present document describes the security mechanisms in TETRA Direct Mode. It provides mechanisms for confidentiality of control signalling and user speech and data at the AI. It also provided some implicit authentication as a member of a group by knowledge of a shared secret encryption key. The use of AI encryption gives both confidentiality protection against eavesdropping, and some implicit authentication.					

TOE Description

TETRA Direct Mode Operation (DMO) offers 4 security classes as follows:

DM-1

No encryption applied.

DM-2-A

The DM-SDU and any related traffic is Air Interface (AI) encrypted. Addresses are not encrypted:

The purpose of security class DM-2-A is to provide confidentiality of user traffic and signalling in applications where it is not necessary to hide the addressing information. It allows calls to be made through a repeater where the repeater is not provided with the capability to encrypt or decrypt messages by maintaining the layer 2 (MAC) elements of any signalling in clear.

DM-2-B

The destination address (SSI), DM-SDU and any related traffic are AI encrypted:

The purpose of security class DM-2-B is to provide confidentiality of user traffic and signalling. It extends the confidentiality applied to signalling over that provided in class DM-2-A to encrypt parts of the MAC header. The encryption allows repeater operation to be made without requiring the repeater to be able to encrypt and decrypt transmissions unless it wishes to check the validity of the destination address. Because the source address is in clear, a pre-emptor can identify the pre-emption slots and hence the call can be pre-empted even if the pre-emptor does not have the encryption key being used by the call master.

DM-2-C

Significant elements of the DMAC-SYNC PDU and the DMAC-DATA PDU are encrypted. Any related traffic is AI encrypted.

The purpose of security class DM-2-C is to provide confidentiality of user traffic and signalling including all identities other than those of repeaters and gateways. The bulk of the MAC header elements are encrypted. Where repeaters are used, the repeater requires the ability to encrypt and decrypt all transmissions. Calls can only be pre-empted by an MS which has the SCK in use by the call master.

Protection Profile **TETRA Direct Mode Operation (DMO)**			
a TOE Security Environment			
a.1 Assumptions			
a.1.1	Each security service is totally independent of any other.		DTR/TETRA-06139 clause 9.1.2
a.1.2	Quality of Service (QoS) is not adversely affected by the implementation of security measures		DTR/TETRA-06139 clause 9.1.2
..	..		..
a.2 Assets			
a.2.1	TETRA Mobile Terminal (MT)		DTR/TETRA-06139 clause 9.4
a.2.2	Key management information		DTR/TETRA-06139 clause 9.2
..	..		..
a.3 Threat agents			
a.3.1	Unauthorized user agents		DTR/TETRA-06139 clause 8.2
a.3.2	Authorized user agents		DTR/TETRA-06139 clause 8.2
..	..		..
a.4 Threats			
a.4.2	Interception at the radio interface		DTR/TETRA-06139 clause 8.3.1.1
a.4.3	Use of resources beyond the authorized limits		DTR/TETRA-06139 clause 8.5.2.2
..	..		..
a.5 Security policies (OPTIONAL)			
a.5.1	To protect the TETRA network operator's information and the users' information and interests		DTR/TETRA-06139 clause 9.2
a.5.2	To provide a set of security services which allow TETRA operators to build their own security policy based on the security services.		DTR/TETRA-06139 9.2
..	..		..
b.1 Security objectives for the TOE			
b.1.1	A TETRA system shall be able to provide a high level of confidentiality in private systems used by public safety organizations		ETR 086-3 clause 6.2.3
b.1.2	A TETRA system must be able to prove the true identity of any entity communicating with it		ETR 086-3 clause 6.2.2
..	..		..
b.2 Security objectives for the environment			
	TETRA is specified as a closed system and, as such, it has no security objectives expressed for the environment		
c IT Security Requirements c.1 TOE security requirements			
c.1.1 TOE security functional requirements			
c.1.1.1	User authentication key generation using the TA11 and TA12 algorithms	FIA_UAU.3	EN 300 392-7 clause 4.1.2
c.1.1.2	Challenge/response user authentication mechanism	FIA_UAU.4	EN 300 392-7 clause 4.1.2
..	..	..	..
c.1.2 TOE security assurance requirements			
c.1.2.1	A TETRA Class 3 implementation can be evaluated at CC EAL4 or above		ISO/IEC 15408-3 [6]
..	..		..
c.2 Environment security requirements (OPTIONAL)			
c.2.1	TETRA is specified as a closed system and, as such, it has no security requirements expressed for the environment		

Protection Profile
TETRA Direct Mode Operation (DMO)

d Application notes (OPTIONAL)

Each TETRA security class has associated features that are mandatory or optional and are summarized in the following table.

Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable	End-to-end
	clause 4	clause 4	clause 6	clause 5	clause 7
1	O	-	-	M	O
2	O	O	M	M	O
3	M	M	M	M	O

NOTE: M = Mandatory;
O = Optional;
- = Does not apply					

A Mobile Station may support one, several, or all security classes and each TETRA cell may support one of the following options at any one time:

- class 1 only;
- class 2 only;
- class 2 and class 1;
- class 3 only; or
- class 3 and class 1.

e Rationale

The relationship between identified threats, security objectives and security requirements is described in DTR/TETRA-06139.

Annex C (informative):
Bibliography

ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

DTR/TETRA-06139: "Terrestrial Trunked Radio (TETRA); Security; Security requirements analysis for TETRA-2".

History

Document history		
V1.1.1	February 2005	Membership Approval Procedure MV 20050401: 2005-02-01 to 2005-04-01
V1.1.1	April 2005	Publication