EESTI STANDARD EVS-ISO/IEC 18028-2:2007

INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 2: Võrguturbe arhitektuur

Information technology
Security techniques
IT network security
Part 2: Network security architecture

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
Käesolev Eesti standard EVS-ISO/IEC 18028-2:2007 “Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 2: Võrguturbe arhitektuur” sisaldab rahvusvahelise standardi ISO/IEC 18028-2:2006 “Information technology — Security techniques — IT network security — Part 2: Network security architecture” identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 18028-2:2007 consists of the identical English text of the International Standard ISO/IEC 18028-2:2006 “Information technology — Security techniques — IT network security — Part 2: Network security architecture”.
Standardi avaldamise korraldas Eesti Standardikeskus.	Estonian standard is published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 18028-2:2007 on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teataja 2008. aasta jaanuarikuu numbris.	This standard is ratified with the order of Estonian Centre for Standardisation dated 07.12.2007 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 18028 see osa määratleb võrguturbe arhitektuuri, millega tagada võrgu turvalisus otspunktist otspunktini. Seda arhitektuuri saab rakendada mitmesugust tüüpi võrkudes, kus probleemiks on turvalisus otspunktist otspunktini, ja sõltumatult võrgu aluseks olevast tehnoloogiast. ISO/IEC 18028 selle osa eesmärk on olla aluseks üksikasjalike soovituste väljatöötamisel otspunktide vahelise turbe kohta.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviations 2

5 Reference Architecture for network security 3

6 Security Dimensions 3
6.1 Access Control Security Dimension 4
6.2 Authentication Security Dimension 4
6.3 Non-repudiation Security Dimension 4
6.4 Data Confidentiality Security Dimension 4
6.5 Communication Flow Security Dimension 4
6.6 Data Integrity Security Dimension 4
6.7 Availability Security Dimension 4
6.8 Privacy Security Dimension 5

7 Security Layers 5
7.1 The Infrastructure Security Layer 6
7.2 The Services Security Layer 6
7.3 The Applications Security Layer 6

8 Security Planes 6
8.1 The Management Security Plane 7
8.2 The Control Security Plane 7
8.3 The End-User Security Plane 7

9 Security threats 8

10 Description of the objectives achieved by application of Security Dimensions to Security Layers 9
10.1 Infrastructure Security Layer 11
10.2 Services Security Layer 14
10.3 Applications Security Layer 17

Bibliography 21

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*, in collaboration with ITU-T. This part of ISO/IEC 18028 is technically aligned with ITU Rec. X.805 but is not published as identical text.

ISO/IEC 18028 consists of the following parts, under the general title *Information technology — Security techniques – IT network security*:

— *Part 1: Network security management*

— *Part 2: Network security architecture*

— *Part 3: Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

— *Part 5: Securing communications across networks using Virtual Private Networks*

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. Thus, the purpose of ISO/IEC 18028 is to provide detailed guidance on the security aspects of the management, operation and use of IT networks, and their inter-connections. Those individuals within an organization that are responsible for IT security in general, and IT network security in particular, should be able to adapt the material in ISO/IEC 18028 to meet their specific requirements. Its main objectives are as follows:

- in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security – including on how to identify and analyse the communications related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);
- in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;
- in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;
- in ISO/IEC 18028-4, to define techniques for securing remote access;
- in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPN).

ISO/IEC 18028-1 is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for Information Security (IS) and/or network security, network operation, or who are responsible for an organization's overall security programme and security policy development.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example IT network managers, administrators, engineers and IT network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example IT network managers, administrators, engineers, and IT network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example IT network managers, administrators, engineers, and IT network security officers).

Information technology — Security techniques — IT network security —

Part 2: Network security architecture

1 Scope

This part of ISO/IEC 18028 defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where end-to-end security is a concern and independently of the network's underlying technology. The objective of this part of ISO/IEC 18028 is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

CCITT Recommendation X.800 (1991), *Security architecture for Open Systems — Interconnection for CCITT applications*

3 Terms and definitions

For the purposes of this document, the following terms defined in ISO 7498-2:1989 | CCIT Rec. X.800 apply.

3.1
access control
prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

3.2
data origin authentication
corroboration that the source of data received is as claimed

3.3
peer-entity authentication
corroboration that a peer entity in an association is the one claimed

3.4
availability
property of being accessible and useable upon demand by an authorized entity