

INFOTEHNOLOOGIA

Turbemeetodid

Infotehnoloogiavõrkude turve

Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil

Information technology

Security techniques

IT network security

Part 5: Securing communications across networks using
virtual private networks

EESTI STANDARDI EESSÕNA**NATIONAL FOREWORD**

Käesolev Eesti standard EVS-ISO/IEC 18028-5:2007 "Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil" sisaldab rahvusvahelise standardi ISO/IEC 18028-5:2006 "Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks" identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 18028-5:2007 consists of the identical English text of the International Standard ISO/IEC 18028-5:2006 "Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks".
Standardi avaldamise korraldas Eesti Standardikeskus.	Estonian standard is published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 18028-5:2007 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 annab detailseid juhiseid turvaaspektide kohta VPN-ühenduste kasutamisel võrkude kokkuühendamiseks või kaugkasutajate ühendamiseks võrkudega. Ta on rajatud võrguhalduse juhistele, mida annab ISO/IEC 18028-1.

Ta on suunatud neile, kes vastutavad selliste tehniliste meetmete valimise ja teostamise eest, mis on vajalikud võrguturbe tagamiseks VPN-ühenduste kasutamisel, ja VPNi turbe sellele järgneva võrguseire eest.

ISO/IEC 18028 see osa annab ülevaate virtuaalsetest privaatvõrkudest, esitab VPNi turvaeesmärgid ja teeb kokkuvõtte VPNi turvanõuetest. Ta annab juhiseid turvaliste VPNide valimise ja rakendamise kohta ning VPNi turbe võrguseire kohta. Ta annab ka teavet tüüpiliste VPNides kasutatavate tehnoloogiate ja protokollide kohta.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine**Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele**

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse poolt antud kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, palun võtke ühendust Eesti Standardikeskusega:
Aru 10 Tallinn 10317 Eesti; www.evs.ee; Telefon: 605 5050; E-post: info@evs.ee

Right to reproduce and distribute belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without permission in writing from Estonian Centre for Standardisation.

If you have any questions about standards copyright, please contact Estonian Centre for Standardisation:
Aru str 10 Tallinn 10317 Estonia; www.evs.ee; Phone: 605 5050; E-mail: info@evs.ee

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
3.1 Terms defined in other International Standards	2
3.2 Terms defined in this part of ISO/IEC 18028	2
4 Abbreviated terms	3
5 Overview of VPNs	3
5.1 Introduction	3
5.2 Types of VPN	4
5.3 VPN techniques	5
5.4 Security aspects	6
6 VPN security objectives	7
7 VPN security requirements	7
7.1 Confidentiality	8
7.2 Integrity	8
7.3 Authentication	8
7.4 Authorization	8
7.5 Availability	8
7.6 Tunnel Endpoints	8
8 Guidelines for the selection of secure VPNs	9
8.1 Regulatory and legislative aspects	9
8.2 VPN management aspects	9
8.3 VPN architectural aspects	9
9 Guidelines for the implementation of secure VPNs	12
9.1 VPN management considerations	12
9.2 VPN technical considerations	12
Annex A (informative) Technologies and protocols used to implement VPNs	15
A.1 Introduction	15
A.2 Layer 2 VPNs	15
A.3 Layer 3 VPNs	17
A.4 Higher Layer VPNs	17
A.5 Comparison of typical VPN protocol security features	19
Bibliography	20

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 should not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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 information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and 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 analyze 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 (VPNs).

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 and/or network security, network operation, or who are responsible for an organization's overall security program 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers and 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 network managers, administrators, engineers, and 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 network managers, administrators, engineers, and network security officers).

Information technology — Security techniques — IT network security —

Part 5:

Securing communications across networks using virtual private networks

1 Scope

This part of ISO/IEC 18028 provides detailed direction with respect to the security aspects of using Virtual Private Network (VPN) connections to inter-connect networks, and also to connect remote users to networks. It builds upon the network management direction provided in ISO/IEC 18028-1.

It is aimed at those individuals responsible for the selection and implementation of the technical controls necessary to provide network security when using VPN connections, and for the subsequent network monitoring of VPN security thereafter.

This part of ISO/IEC 18028 provides an overview of VPNs, presents VPN security objectives, and summarizes VPN security requirements. It gives guidance on the selection of secure VPNs, on the implementation of secure VPNs, and on the network monitoring of VPN security. It also provides information on typical technologies and protocols used by VPNs.

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/IEC 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18028-1:2006, *Information technology — Security techniques — IT network security — Part 1: Network security management*

ISO/IEC 18028-2:2006, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

3 Terms and definitions

3.1 Terms defined in other International Standards

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts) and ISO/IEC 18028-1 apply, as do the following terms defined in ISO/IEC 13335-1: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, security policy, non-repudiation, reliability, risk, risk analysis, risk management, safeguard, threat, and vulnerability.

3.2 Terms defined in this part of ISO/IEC 18028

For the purposes of this document, the following terms and definitions apply.

3.2.1

layer 2 switching

technology that uses internal switching mechanisms to establish and control connections between devices using layer 2 protocols

NOTE It is typically used to simulate a LAN environment to upper layer protocols.

3.2.2

layer 2 VPN

virtual private network used to provide a simulated LAN environment over a network infrastructure

NOTE Sites linked by a layer 2 VPN can operate as though they are on the same LAN.

3.2.3

layer 3 switching

technology that uses internal switching mechanisms in combination with standard routing mechanisms, or which employs MPLS techniques, in order to establish and control connections between networks

3.2.4

layer 3 VPN

virtual private network used to provide a simulated WAN environment over a network infrastructure

NOTE Sites linked by a layer 3 VPN can operate as though they are on a private WAN.

3.2.5

private

restricted to members of an authorized group: in the context of VPNs, it refers to the traffic flowing in a VPN connection

3.2.6

private network

network that is subject to access controls which are intended to restrict use to members of an authorized group

3.2.7

protocol encapsulation

enveloping one data flow inside another by transporting protocol data units wrapped inside another protocol

NOTE This is one method which can be used to establish tunnels in VPN technology.