INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkudega (VPN)

Information technology
Security techniques
Network security
Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
(ISO/IEC 27033-5:2013)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard EVS-ISO/IEC 27033-5:2014 „Infotehnoloogia. Turbemeetodid. Võrguturve. Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkudega (VPN)“ sisaldab rahvusvahelise standardi ISO/IEC 27033-5:2013 „Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“ identset ingliskeelset teksti.

Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.

Standard EVS-ISO/IEC 27033-5:2014 on jõustunud sellekohase teate avaldamisega EVS Teataja 2014. aasta oktoobrikuu numbris.

Standard on kättesaadav Eesti Standardikeskusest.

NATIONAL FOREWORD

This Estonian Standard EVS-ISO/IEC 27033-5:2014 consists of the identical English text of the International Standard ISO/IEC 27033-5:2013 „Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“.

Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.

This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.

The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 27033 see osa annab juhiseid võrguturbe tagamiseks vajalike tehniliste turvameetmete valimise, rakendamise ja seire kohta VPN-ühenduste kasutamisel võrkude kokkuühendamiseks või kaugkasutajate ühendamiseks võrkudega.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040

Contents

Page

Foreword ... **iv**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviations ... **2**

5 Document structure ... **2**

6 Overview ... **2**
6.1 Introduction ... 2
6.2 Types of VPNs ... 3

7 Security Threats ... **4**

8 Security Requirements ... **5**
8.1 Overview ... 5
8.2 Confidentiality ... 5
8.3 Integrity ... 6
8.4 Authenticity ... 6
8.5 Authorization ... 6
8.6 Availability ... 6
8.7 Tunnel Endpoint Security ... 6

9 Security Controls ... **6**
9.1 Security aspects ... 6
9.2 Virtual circuits ... 7

10 Design Techniques ... **7**
10.1 Overview ... 7
10.2 Regulatory and legislative aspects ... 8
10.3 VPN management aspects ... 8
10.4 VPN architectural aspects ... 8
10.5 VPN technical considerations ... 11

11 Guidelines for Product Selection ... **12**
11.1 Carrier protocol selection ... 12
11.2 VPN appliances ... 12

Bibliography ... **14**

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 27033 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*.

This first edition cancels and replaces ISO/IEC 18028-5:2006, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios — Threats, design techniques and control issues*

— *Part 4: Securing communications between networks using security gateways*

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

— *Part 6: Securing wireless IP network access*

(Note that there may be other parts. Examples of possible topics to be covered by parts include local area networks, wide area networks, broadband networks, web hosting, Internet email, and routed access to third-party organizations. The main clauses of all such parts should be Risks, Design Techniques, and Control Issues.)

Information technology — Security techniques — Network security —

Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

1 Scope

This part of ISO/IEC 27033 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.

2 Normative references

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

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27033-1:2009, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27033-1 apply.