SLOVENSKI STANDARD
SIST-TS CEN/TS 16080:2014

01-februar-2014

Programska oprema in storitve za filtriranje internetne vsebine in internetnih komunikacij

Internet Content and communications filtering software and services

Software und Dienste für Filterung von Internetskommunikation und Internestsinhalt

Logiciel et services de filtrage de contenus et communications d'internet

Ta slovenski standard je istoveten z: CEN/TS 16080:2013

<u>ICS:</u>

35.080	Dokumentiranje razvoja programske opreme in sistemov (sistemska dokumentacija)	Software development and system documentation

SIST-TS CEN/TS 16080:2014   **en**

iTeh STANDARD PREVIEW

(standards.iteh.ai)

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 16080

November 2013

ICS 35.080; 35.240.99

English Version

Internet Content and communications filtering software and services

Logiciel et services de filtrage de contenus et
communications d'internet

Software und Dienste für Filterung von
Internetskommunikation und Internestsinhalt

This Technical Specification (CEN/TS) was approved by CEN on 7 January 2013 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 16080:2013: E

CEN/TS 16080:2013 (E)

Contents   Page

iTeh STANDARD PREVIEW

(standards.iteh.ai)

CEN/TS 16080:2013 (E)

Foreword

This document (CEN/TS 16080:2013) has been prepared by Technical Committee CEN/TC 365 "Internet Filtering", the secretariat of which is held by AENOR.

In view of the increasing use of Internet communication technologies and the impact that these technologies necessarily have on the general public, in January 2004, the European Commission adopted a Communication to combat SPAM which served as a basis for the March 2004 Council Conclusions highlighting the essential role of technical solutions and consumers empowerment.

In addition, the European Parliament and the Council agreed to a multi-annual programme, proposed by the Commission, to promote safer use of the Internet and new online technologies.

The 4-year programme, Safer Internet Plus (2005-2008) aims at combating illegal and harmful content online. The programme has several actions such as awareness campaigns, hot lines, interoperability issues relevant for Internet filtering and benchmarking (SIP-BENCH project).

In view of the increasing awareness and use of filtering software and services, and worried about the lack of objective testing and scarcity of comparatives, ANEC, the association representing consumers in standardization and certification, commissioned a study on "The standards requirements for Internet filtering tools" at the end of 2005. The purpose of this ANEC project was to investigate to what extent unsolicited commercial communications (SPAM) and Internet content filters should be testable and comparable in order to help consumer choice. Performance standards for Internet filtering products and services were identified as helpful in both ensuring product transparency and aiding choice. The protection of consumers (and especially children) was intended to be the main aim of the ANEC work.

CEN BT WG 194 on Internet filtering tools was set up in February 2007, upon request by ANEC, to consult stakeholders on this issue. Participants range from European Commission representatives from DG Information Society and Justice and Home Affairs (JAI) to national standards bodies (BSI, DIN, AFNOR and NEN).

The CEN BT WG 194 met on 14 March 2007; no other meeting was planned.

The Report was finalized after this meeting and endorsed electronically in June 2007. As a way forward, BT/WG 194 proposed the creation of a CEN Task Force (TF) leading to this Technical Specification with the restricted scope of Web filters.

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

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Nearly three quarters of the population of the European Union is now using the Internet. A very large proportion of them use the Internet for the purpose of education, work, communication and commerce. However, even though the Internet is becoming part of everyday life, potentially harmful or illegal material exists on the Internet.

To protect their children and themselves, Internet users are turning towards filtering product and services besides education. However, there is no easy way for Internet users to discover which of these products and services is best suited to their needs or, indeed, whether a filter is effective.

A Technical Specification can help Internet users to make informed choices when selecting filter tools. They shall be able to expect a filter that complies with the standard to perform to a certain level.

The Technical Specification covers issues such as ease of use and installation, as well as filtering performance. This can lead to an increase of confidence of the user in the filter. The users can also be ensured, that they shall be able to install, configure and maintain (update/upgrade) the filter themselves.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

CEN/TS 16080:2013 (E)

1 Scope

The objective of this Technical Specification is to define a set of criteria on how Web filters shall perform and that shall give Internet users more confidence in choosing a suitable product or service in order to help protecting children online.

NOTE   A product is a software system that is installed by its administrator or its provider. A service is provided without specific installation by the administrator, but by direct provision of the customer by the provider. An example of a product is a software system installed on a personal computer, and an example of a service is an Internet connection filter provided by an Internet Service Provider and added on the Internet access service.

By using a Web filter that complies with the requirements set out in this Technical Specification, a user can be confident that the product or service:

a)   has been specifically designed to meet the needs of parents and carers (administrators of the filter) to protect children from potentially harmful URLs on the Internet;

b)   has been specifically targeted to minors, and is also suited for individuals looking to protect themselves from potentially harmful URLs on the Internet;

c)   delivers a minimum set of features and efficacy that are sufficient to provide the required level of protection;

d)   comes with clear and comprehensive documentation, installation and implementation instructions and available support;

e)   is reasonably secure, i.e. adopts proven measures to prevent bypassing or removal of the filter itself.

This Technical Specification does not cover the following technologies:

f)   any kind of email filtering, including: antispam filtering, antivirus analysis of emails and attachments, anthiphishing filtering;

g)   other Web filtering for the purpose of enterprise or adult Web usage, including: antivirus analysis of Web content, antiphishing filtering;

h)   the analysis and/or filtering of any other application traffic delivered over HTTP/HTTPS/FTP including for instance: instant messaging, peer to peer file (P2P) sharing, VoIP;

i)   the analysis and/or filtering of any other application traffic delivered over non HTTP/HTTPS/FTP protocols including for instance: newsgroups, instant messaging, peer to peer file (P2P) sharing, VoIP and social networking applications.

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.

EN ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1
administrator
person who is responsible for the implementation, configuration and administration of the Web filter

Note 1 to entry: For the purpose of this Technical Specification, the administrator could be the parents, an educator, or the responsible adult.

3.1.2
blacklist
list of URLs that are always blocked by a Web filter

3.1.3
block page
informative web page that is shown to the end user of the filtering service when trying to access blocked URL

3.1.4
blocking
prevention to access URL in its entirety

EXAMPLE   Blocking all or some of the images on a web page or access to parts of a web page is not considered blocking.

3.1.5

certification body
a third-party body contracted to provide certification to a customer

3.1.6
chat
communication between two or more end users over the Internet in the form of real time short messages exchanged in virtual meeting places or chat rooms

3.1.7
content
any material, such as text, images, sound, animation or video, which can be accessed or received using the Internet

3.1.8
default settings
the settings of the Web filter once the installation is finished assuming that installation has been performed with no voluntary modification by the administrator

3.1.9
domain
sequence of letters and numbers separated by dots that conform the root part of a valid URL, excluding the protocol part and the path part

EXAMPLE   The domain of the URL http://www.example.com/path/to/file.html is the sequence www.example.com.

3.1.10
education material
material intended for use by both administrators and those for whom they are responsible that explains the purpose, function and limitations of Internet filters

3.1.11
efficacy
rate of URLs blocked among those belonging to a particular harmful URL category in a reference database

3.1.12
e-mail
system of sending messages (which may include text, images, sound, animation or video) over the Internet for immediate or later retrieval

3.1.13
end user
person who is protected from potentially harmful or dangerous URLs when accessing material on the Internet by any of the methods under the scope of this Technical Specification

3.1.14
filtering
selective blocking of URLs (e.g. web pages) against specified criteria

3.1.15
instant message
system that allows exchange of short messages and sharing of files in real time over the Internet (see also chat), usually one-to-one

3.1.16
Internet
global interconnected network of networked computers, providing an infrastructure through which applications such as web browsing, email, chat and instant messaging operate

3.1.17
Internet Service Provider (ISP)
provider of Internet services such as Internet connectivity and web site hosting

3.1.18
manufacturer
organization or corporation developing the product or service

3.1.19
newsgroup
area where end users can post or read comments about specific subjects

3.1.20
overblocking
prevention of access to acceptable URLs wrongly classified as belonging to any of the categories of potentially harmful URLs described in Annex A

3.1.21
overblocking rate
rate of URLs blocked among those not belonging to a particular harmful URL category in a reference database

3.1.22
personnel list
feature that allows the administrator of a Web filter to prevent a site not blocked by the Web filter or to authorize a site blocked by the Web filter, regardless of the filtering mode selected

3.1.23
personnal identification number
sequence of numbers that act as a password for a protected data asset or for accessing configuration option in a computer system

3.1.24
phishing
malicious sites designed to steal personal data from end users, such as credit card numbers, passwords, etc, by masquerading as an authentic and trustworthy site or entity

3.1.25
potentially harmful URL
a URL whose content is considered not appropriate for fruition by the end user of a Web filter because potentially harmful, even if it is not illegal in the country where the recipient of the service lives or resides

Note 1 to entry: Annex A specifies harmful URL categories.

3.1.26
product description
information describing a product or service, designed to help potential consumers evaluate a product before purchasing or adopting it

3.1.27
product packaging
physical wrapping of a software product, point of download for software products downloaded from the Internet, or point of activation for services available through the Internet

3.1.28
SPAM
unsolicited or undesired electronic messages usually sent in bulk

3.1.29
reference database
a list of URLs belonging to a particular harmful URL category, together with a list of URLs that do not belong to such category

Note 1 to entry: Annex A specifies harmful URL categories. Annex C provides with the procedure to build a reference database for a category.

3.1.30
social networking service
a social networking service is an online site that focuses on building and reflecting of social networks or social relations among end users, who, for example, share interests and/or activities

Note 1 to entry: Annex B provides more details of social networking services.

3.1.31
step by step instructions
instructions that are presented in a manner that details each end user or administrator action as a separate command thus making carrying out the operation less error prone

Note 1 to entry: On their own Step by Step instructions may not necessarily explain how the product or service actually works or what it does.

3.1.32
software product
set of computer programs, procedures, and possibly associated documentation and data

CEN/TS 16080:2013 (E)

3.1.33
support provider
organization that provides technical support to consumers and administrators of the Web filter

3.1.34
user documentation
set of documents, available in print or electronic form, that provides information on the installation, configuration, use and maintenance of the Web filter

3.1.35
Web filter
software product or service designed to protect end users from potentially harmful or dangerous URLs when accessing material on the Internet

3.1.36
Web filter support
the provision of information to the administrator in order to solve specific technical problems or clarifications to doubts on Web filter use

3.1.37
whitelist
list of URLs that are never blocked by a Web filter

3.2   Abbreviations

E-mail	Electronic mail
FAQs	Frequently Asked Questions
HTTP	Hyper Text Transfer Protocol
ISP	Internet Service Provider
P2P	Peer to Peer
PIN	Personal Identification Number
URL	Universal Resource Locator
VoIP	Voice over Internet Protocol

4   Web filter requirements

4.1   General

In order to comply with this Technical Specification, manufacturers or providers of Web filters shall fulfil the requirements described on this clause.

4.2   Requirements

4.2.1   Level of protection

The Web filter shall block access to potentially harmful URLs by default with an efficacy equals or over 0,95 for all potentially harmful URLs categories and their corresponding reference databases.

Compliance is checked using reference databases built according to C.3.

The Web filter shall not overblock access to acceptable URLs by default with an overblocking rate equals or below 0,05 for all potentially harmful URLs categories and their corresponding reference databases.