ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2010**

Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ČSN ISO/IEC 15408-3
36 9789

Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components

Technologies de l,information – Techniques de sécurité – Criteres d,évaluation pour la sécurité TI – Partie 3: Composants d,assurance de sécurité

Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 3: Anforderungen an die Vertrauenswürdigkeit

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-3:2008. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15408-3:2008. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 15408-3 (36 9789) z listopadu 2002.

Národní předmluva

Změny proti předchozím normám

Tato norma představuje technickou revizi předchozí normy ČSN ISO/IEC 15408-3 z roku 2002. Vydání ISO/IEC 15408:2005 nebylo do soustavy českých norem zavedeno.

Informace o citovaných normativních dokumentech

ISO/IEC 15408-1 dosud nezavedena

ISO/IEC 15408-2 zavedena v ČSN ISO/IEC 15408-2 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční požadavky

Národní poznámka

Malé písmeno „s“ u anglické zkratky vyjadřuje její množné číslo, například: SFRs, TSFs, apod.

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 15408-3
Kritéria pro hodnocení bezpečnosti IT – Třetí vydání
Část 3: Komponenty bezpečnostních záruk 2008-08

ICS 35.040

Obsah

Strana

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících národních orgánů.

Pozornost je nutno věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech takových patentových práv.

ISO/IEC 15408-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC27, *Bezpečnostní techniky IT*. Identický text ISO/IEC 15408-3 je zveřejněn organizacemi sponzorujícími projekt „Common Criteria“ pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. Veřejný XML zdroj obou publikací lze nalézt na http://www.oc.ccn.cni.es/xml.

Třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 15408-3:2005), které prošlo technickou revizí.

ISO/IEC 15408 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT:*

– *Část 1: Úvod a všeobecný model*

– *Část 2: Bezpečnostní funkční komponenty*

– *Část 3: Komponenty bezpečnostních záruk*

Právní poznámka

Dále uvedené vládní organizace přispěly k vyvinutí této verze Společných kritérií pro hodnocení bezpečnosti informačních technologií. Jako společní držitelé autorských práv k dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, verze 3.1, části 1 až 3 (nazývané CC 3.1), tímto poskytují nevýhradní oprávnění pro ISO/IEC k používání CC 3.1 při pokračujícím vývoji/údržbě mezinárodní normy ISO/IEC 15408. Tyto vládní organizace si však ponechávají právo používat, kopírovat, šířit, překládat nebo pozměňovat CC 3.1 jak uznají za vhodné.

Austrálie/Nový Zéland The Defence Signals Directorate and the

Government Communications Security Bureau respectively;

Kanada Communications Security Establishment;

Francie Direction Centrale de la Sécurité des Systemes d,Information;

Německo Bundesamt für Sicherheit in der Informationstechnik;

Japonsko Information Technology Promotion Agency;

Nizozemsko Netherlands National Communications Security Agency;

Španělsko Ministerio de Administraciones Públicas and Centro Criptológico Nacionál;

Spojené království Communications-Electronic Security Group;

USA The National Security Agency and the National Institute of Standards and Technology.

Úvod

Komponenty bezpečnostních záruk, jak jsou definovány v této části ISO/IEC 15408, jsou základem pro požadavky na bezpečnostní záruky vyjádřené v profilu ochrany (Protection Profile, PP) nebo v bezpečnostním cíli (Security Target, ST).

Tyto požadavky ustanovují standardní způsob vyjádření požadavků záruky pro předměty hodnocení (Target of evaluation, TOE). Tato část ISO/IEC 15408 katalogizuje sadu součástí záruky, rodin záruky a tříd záruky. Tato část ISO/IEC 15408 rovněž definuje kritéria hodnocení pro PP a ST a představuje úrovně záruk hodnocení, které vymezují předem definovanou stupnici ISO/IEC 15408 hodnocení záruk pro TOE, která se nazývá úrovně hodnocení záruky (Evaluation Assurance Levels, EAL).

Uživateli této části ISO/IEC 15408 jsou spotřebitelé, vývojoví pracovníci a hodnotitelé bezpečných IT produktů. ISO/IEC 15408-1 poskytuje dodatečné informace týkající se cílových uživatelů ISO/IEC 15408 a používání ISO/IEC 15408 skupinami, které zahrnují cílové uživatele. Tyto skupiny mohou používat tuto část ISO/IEC 15408 následovně:

a. Zákazníci, kteří používají tuto část ISO/IEC 15408 při výběru komponent pro vyjádření požadavků záruky, které splní bezpečnostní cíle vyjádřené v PP nebo ST, stanovujících požadované úrovně bezpečnostních záruk TOE.

b. Vývojoví pracovníci, kteří reagují na aktuální nebo vnímané požadavky zákazníků na bezpečnost při vytváření TOE, se odkazují na tuto část ISO/IEC 15408 při interpretaci specifikací požadavků záruky a při určování přístupů k zárukám TOE.

c. Hodnotitelé, kteří používají požadavky záruky definované v této části ISO/IEC 15408 jako závazný výrok kritérií pro hodnocení při určování záruky TOE a při hodnocení PP a ST.

1 Předmět normy

Tato část ISO/IEC 15408 definuje požadavky normy na záruku. Obsahuje úrovně hodnocení záruky (Evaluation Assurance Levels, EALs), které definují měřítko pro posouzení záruky TOE komponenty, sestavené balíky záruk (composed assurance packages, CAPs), které definují měřítko pro posouzení záruky sestavených TOE, jednotlivé komponenty záruky, z kterých se skládají úrovně záruky a balíky, a kritéria pro hodnocení PP a ST.