ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2016**

Informační technologie – Bezpečnostní techniky – Verifikace kryptografických protokolů

ČSN
ISO/IEC 29128
36 9707

Information technology – Security techniques – Verification of cryptographic protocols

Technologies de l'information – Techniques de sécurité – Vérification des protocoles cryptographiques

Tato norma je českou verzí mezinárodní normy ISO/IEC 29128:2011. 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 29128:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN ISO/IEC 15408-1:2013 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ČSN ISO/IEC 15408-2:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původním tvaru, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu: nonce, man-in-the-middle.

Anglický termín „seed“ je přeložen jako „náhodná počáteční hodnota“.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 29128
Verifikace kryptografických protokolů První vydání
2011-12-15

ICS 35.040

Obsah

Strana

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 29128 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Bezpečnost digitální komunikace závisí na mnoha aspektech, kdy kryptografické mechanismy hrají stále důležitější roli. Jsou-li takové mechanismy používány, existuje mnoho bezpečnostních záležitostí, jako jsou síla kryptografických algoritmů, přesnost a správnost implementace, správná činnost a použití kryptografických systémů, a bezpečnost nasazených kryptografických protokolů.

Normy pro specifikaci kryptografických algoritmů a pro implementaci a testování kryptografických zařízení a modulů již existují. Neexistují však žádné normy nebo obecněji akceptované postupy pro posuzování specifikace protokolů použitých v takové komunikaci. Cílem této mezinárodní normy je ustavit prostředky pro verifikaci specifikací kryptografických protokolů a poskytnout tak definované úrovně důvěry týkající se bezpečnosti specifikace kryptografických protokolů.

1 Předmět normy

Tato mezinárodní norma stanoví technický základ pro bezpečnostní důkaz specifikace kryptografických protokolů. Tato mezinárodní norma specifikuje kritéria hodnocení návrhu pro tyto protokoly, stejně jako metody, určené k použití v procesu verifikace takových protokolů. Tato mezinárodní norma také poskytuje definice různých úrovní záruky protokolů odpovídajících komponentám záruky hodnocení v ISO/IEC 15408.