ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Březen 2025**

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Ověřování kryptografických protokolů – Část 1: Rámec	ČSN ISO/IEC 29128-1 36 9707

Information security, cybersecurity and privacy protection – Verification of cryptographic protocols – Part 1: Framework

Tato norma je českou verzí mezinárodní normy ISO/IEC 29128-1:2023. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29128-1:2023. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN EN ISO/IEC 15408 (soubor) (36 9789) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT

ČSN EN ISO/IEC 19790:2020 (36 9879) Informační technologie – Bezpečnostní techniky – Bezpečnostní poža-
davky na kryptografické moduly

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Pro účely této normy byl použit následující anglický termín v původní podobě, vzhledem k rozšíření tohoto termínu v odborné komunitě a absenci českého ekvivalentu:

nonce.

Vypracování normy

Zpracovatel odborného překladu: RNDr. David VARNER, Ph.D., IČO 60586087

Technická normalizační komise: TNK 20 Informační technologie

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Ověřování kryptografických protokolů – Část 1: Rámec

ISO/IEC 29128-1
Druhé vydání
2023-03

ICS 35.030

Obsah

Strana

Předmluva..... 5
Úvod..... 6
1..... Předmět normy..... 7
2..... Citované dokumenty..... 7
3..... Termíny a definice..... 7
4..... Formální ověřování kryptografických protokolů..... 8
4.1..... Metody modelování kryptografických protokolů..... 8
4.2..... Požadavky na ověřování..... 8
4.2.1... Metody ověřování..... 8
4.2.2... Nástroje ověřování..... 9
4.2.3... Vázané vs. nevázané ověřování..... 9

4.3..... Model kryptografického protokolu..... 9

4.3.1... Popis modelu..... 9

4.3.2... Formální specifikace..... 9

4.3.3... Model protivníka..... 10

4.3.4... Předložení modelu..... 11

4.3.5... Bezpečnostní vlastnosti..... 11

4.3.6... Sebehodnotící důkaz..... 11

5..... Proces ověřování..... 11

5.1..... Obecně..... 11

5.2..... Povinnosti předkladatele..... 11

5.3..... Povinnosti hodnotitele..... 11

5.3.1... Hlavní povinnosti..... 11

5.3.2... Hodnocení testeru..... 11

5.3.3... Hodnocení

modelu..... 12

5.3.4... Hodnocení důkazu..... 12

5.3.5... Příklad hodnocení..... 12

Příloha A (informativní) Protokol veřejného klíče Needham-Shroeder-Lowe..... 13

Příloha B (informativní) Vzorové podání..... 14

Příloha C (informativní) Příklad hodnocení..... 15

Příloha D (informativní) Model Dolev-Yao..... 16

Příloha E (informativní) Bezpečnostní vlastnosti..... 17

Bibliografie..... 18

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů
(členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives nebo www.iso.iec.ch/members_experts/refdocs).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržených IEC (viz patents.iec.ch).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 29128:2011), které bylo technicky zrevidováno.

Hlavní změny jsou:

- odstranění neformálních zkoušek a zkoušek na papíře;
- vyřazení úrovní PAL;
- zjednodušení technických požadavků a vysvětlení;
- drobné redakční změny s cílem uvést dokument do souladu se směrnicemi ISO/IEC, část 2, 2021.

Seznam všech částí souboru ISO/IEC 29128 lze nalézt na webových stránkách ISO a IEC.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html

a www.iec.ch/national-committees.

Úvod

Mnoho kryptografických protokolů nedosáhlo svých stanovených bezpečnostních cílů kvůli své složitosti a obtížnému návrhu při dosažení požadovaných funkčních a bezpečnostních požadavků. Podstatou této obtížnosti je, že protokoly je nutné pečlivě analyzovat za účelem nalezení chyb v jejich návrhu. Cílem tohoto dokumentu je standardizovat metodu pro analyzování protokolů navrhováním jasně definovaného rámce ověřování založeného na podložených vědeckých metodách.

Tento dokument navrhuje postup standardizace obdobný tomu, který již pro kryptografické algoritmy existuje. Národní a mezinárodní orgány používají procesy hodnocení, které vzbuzují vysoký stupeň důvěry, že standardizovaný kryptografický algoritmus splňuje konkrétní bezpečnostní požadavky, pro které byl navržen. Podobný proces pro kryptografické protokoly by poskytl důvěru, že ověřený protokol splňuje jeho stanovené bezpečnostní vlastnosti a je možné jej použít v systémech, které jsou z hlediska bezpečnosti kritické.

Navržený proces ověřování je založen na nejmodernějších technikách modelování protokolů a využívá přísnou logiku, matematiku a počítačovou vědu. Je navržen tak, aby poskytl objektivní důkaz, že protokol splňuje jeho stanovené bezpečnostní cíle. Ověření není zárukou bezpečnosti; stejně jako u každého modelování jsou výsledky omezeny rozsahem a kvalitou modelu a použitými nástroji.

1 Předmět normy

Tento dokument ustanovuje rámec specifikací pro ověřování kryptografických protokolů podle nejlepších akademických a oborových postupů.