ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2015**

Informační technologie – Bezpečnostní techniky – Signcryption

ČSN
ISO/IEC 29150
36 9704

Information technology – Security techniques – Signcryption

Technologies de l,information – Techniques de sécurité – Signcryptage

Tato norma je českou verzí mezinárodní normy ISO/IEC 29150:2011 včetně opravy ISO/IEC 29150:2011/Cor.1:2014-03. 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 29150:2011 including its Corrigendum ISO/IEC 29150:2011/Cor.1:2014-03. It was translated by the Czech Office for Standards, Metrology and Testing.
It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 9796-2:2010 zavedena v ČSN ISO/IEC 9796-2:2013 (36 9780) Informační technologie – Bezpečnostní techniky – Schémata digitálních podpisů umožňující obnovu zprávy – Část 2: Mechanismy založené na faktorizaci celých čísel

ISO/IEC 9796-3:2006 zavedena v ČSN ISO/IEC 9796-3:2013 (36 9780) Informační technologie – Bezpečnostní techniky – Schémata digitálních podpisů umožňující obnovu zprávy – Část 3: Mechanismy založené na diskrétních logaritmech

ISO/IEC 14888-1:2008 dosud nezavedena

ISO/IEC 14888-2:2008 dosud nezavedena

ISO/IEC 14888-3:2006 dosud nezavedena

ISO/IEC 18033-1:2005 dosud nezavedena

ISO/IEC 18033-2:2006 dosud nezavedena

Souvisící ČSN

ČSN ISO/IEC 8825-1:2012 (36 9635) Informační technologie – Kódovací pravidla pro ASN.1: Specifikace základ-
ních kódovacích pravidel (BER), kanonických kódovacích pravidel (CER) a zvláštních kódovacích pravidel (DER)

ČSN ISO/IEC 9797-1:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9798-1:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit –
Část 1: Všeobecně

ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce –
Část 1: Všeobecně

ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce –
Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 15946-5:2012 (36 9794) Informační technologie – Bezpečnostní techniky – Kryptografické techniky založené na eliptických křivkách – Část 5: Generování eliptických křivek

Vysvětlivky k textu převzaté normy

U anglických termínů „signcryption“ a „unsigncryption“ byly ponechány jako český ekvivalent dva termíny „signcryption“ i „signkrypce“ a „unsigncryption“ i „unsignkrypce“. Na prvním místě byl ponechán anglický termín nezměněn vzhledem k jeho používání v odborné literatuře v tomto tvaru.

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.

Upozornění na národní poznámky

Do této normy byla doplněna národní poznámka, která opravuje text A.1 podle opravy ISO/IEC 29150:2011/Cor.1:2014-03.

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 – Signcryption ISO/IEC 29150
První vydání
2011-12-15

Obsah

Strana

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Citované dokumenty 8

3 Termíny a definice 9

4 Symboly a způsoby zápisu 13

5 Konečná pole a eliptické křivky 15

5.1 Konečná pole 15

5.2 Eliptické křivky 16

6 Konverzní funkce 16

6.1 Bity a řetězce 16

6.2 Konverze mezi řetězci bitů a celými čísly 17

6.3 Konverze mezi prvky konečných polí a řetězci celých čísel/bitů 17

6.4 Konverze mezi body na eliptických křivkách a řetězci bitů 17

7 Kryptografické transformace 18

7.1 Úvod 18

7.2 Kryptografické hašovací funkce 18

7.2.1 Standardní kryptografické hašovací funkce 18

7.2.2 Kryptografické hašovací funkce úplné domény 18

7.3 Funkce odvození klíče 19

8 Obecný model pro signcryption 19

9 Mechanismus signcryption založený na diskrétních logaritmech (DLSC) 20

9.1 Úvod 20

9.2 Specifické požadavky 21

9.3 Parametry platné v celém systému 21

9.4 Algoritmus generování klíčů 21

9.5 Algoritmus signcryption 21

9.6 Algoritmus unsigncryption 23

10 Mechanismus signcryption založený na eliptických křivkách (ECDLSC) 23

10.1 Úvod 23

10.2 Specifické požadavky 23

10.3 Parametry platné v celém systému 23

10.4 Algoritmus generování klíčů 24

10.5 Algoritmus signcryption 24

10.6 Algoritmus unsigncryption 25

Strana

11 Mechanismus signcryption založený na faktorizaci celých čísel (IFSC) 26

11.1 Úvod 26

11.2 Specifické požadavky 26

11.3 Parametry platné v celém systému 27

11.4 Algoritmus generování klíčů 27

11.5 Algoritmus signcryption 27

11.6 Algoritmus unsigncryption 28

12 Mechanismus typu „zašifrování a pak podepsání“ (EtS) 30

12.1 Úvod 30

12.2 Specifické požadavky 30

12.3 Algoritmus generování klíčů 30

12.4 Algoritmus signcryption 31

12.5 Algoritmus unsigncryption 31

Příloha A (normativní) Identifikátory objektu 32

Příloha B (informativní) Bezpečnostní úvahy 34

Příloha C (informativní) Návod k použití mechanismů 39

Příloha D (informativní) Příklady 42

Bibliografie 53

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 vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC1.

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

Hlavním úkolem společné technické komise je příprava 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 29150 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie,* subkomise SC 27
IT Bezpečnostní techniky.

Úvod

Při posílání dat z jednoho místa na druhé je často nezbytné je při jejich přepravě určitým způsobem chránit, například před odposlechem nebo neoprávněnou modifikací. Podobně je důležité data chránit před neoprávněným přístupem, jsou-li data uložena v prostředí, ke kterému mohou mít přístup neautorizované strany.

Jestliže je nutné chránit důvěrnost dat například před odposlechem, pak je jedním řešením použít šifrování s veřejným klíčem dle specifikace v ISO/IEC 18033. Obdobně, jestliže je nutné chránit data před neoprávněnou modifikací nebo paděláním, mohou být použity digitální podpisy dle specifikace

v ISO/IEC 9796 a ISO/IEC 14888. Je-li požadována důvěrnost i nepadělatelnost, jednou z možností je použít šifrování s veřejným klíčem i digitální podpis. Zatímco tyto operace mohou být kombinovány mnoha způsoby, ne všechny kombinace takových mechanismů poskytují stejné bezpečnostní záruky. Proto je žádoucí podrobně a přesně vymezit, jak by měly být mechanismy důvěrnosti a nepadělatelnosti kombinovány, aby poskytly optimální úroveň bezpečnosti. Kromě toho je možné získat v některých případech významně vyšší účinnost přesným vymezením jediné metody zpracování dat s cílem zajistit jak důvěrnost, tak nepadělatelnost.

V této mezinárodní normě jsou definovány *mechanismy signcryption*. Jsou to metody pro zpracování dat k zajiš-
tění jak důvěrnosti, tak nepadělatelnosti. Tyto metody zpracování dat obvykle zahrnují buď použití schématu asymetrického šifrování a schématu digitálního podpisu kombinovaného specifickým způsobem, nebo použití speciálně vyvinutého algoritmu, který vykonává současně obě funkce.

Metody specifikované v této mezinárodní normě byly navrženy s cílem maximalizovat úroveň bezpečnosti a poskytnout účinné zpracování dat. Všechny mechanismy zde definované mají matematické „důkazy bezpečnosti“, tj. rigorózní argumenty podporující jejich nároky na bezpečnost.

1 Předmět normy

Tato mezinárodní norma specifikuje čtyři mechanismy pro signcryption, které využívají kryptografické techniky s veřejným klíčem, vyžadující, aby jak původce, tak příjemce chráněných dat měli svoji vlastní dvojici veřejného a soukromého klíče.

Tato mezinárodní norma není použitelná pro infrastruktury pro správu veřejných klíčů, které jsou definovány v ISO/IEC 11770-1 a ISO/IEC 9594.

POZNÁMKA 1 Mechanismy signcryption jsou přesně vymezené způsoby zpracování řetězce dat s dále uvedenými bezpečnostními cíli:

- **důvěrnost dat**, tj. ochrana před neoprávněným odhalením dat;
- **integrita dat**, tj. ochrana umožňující příjemci dat ověřit, že data nebyla změněna;
- **autentizace původu dat**, tj. ochrana umožňující příjemci dat ověřit identitu původce dat;
- **nepadělatelnost dat**, tj. ochrana před neoprávněnou modifikací dat, dokonce i příjemcem dat.

Tyto čtyři bezpečnostní cíle se nutně vzájemně nevylučují. Čtvrtý cíl, nepadělatelnost dat, je především výraznější představou o bezpečnosti, zahrnující v sobě jak integritu dat, tak autentizaci původu dat.

POZNÁMKA 2 Dva mechanismy, specifikované v této mezinárodní normě, a to mechanismy DLSC a ECDLSC, vyžadují použít v celém systému platné parametry veřejných klíčů odesílatelem i příjemcem dat. V systému, kde existuje více dvojic odesílatelů a příjemců, všichni tito uživatelé by měli použít stejné parametry platné v celém systému. Dva zbývající specifikované mechanismy, IFSC a EtS, nevyžadují použití takových parametrů veřejných klíčů v celém systému.

POZNÁMKA 3 Při výběru čtyř signcryption mechanismů z velkého počtu publikovaných a používaných technik pro zařazení do této mezinárodní normy bylo dodrženo stejných sedm kritérií, jako jsou kritéria uvedená v ISO/IEC 18033-1:2005, Příloha A. Z vyloučení konkrétních metod nevyplývá, že tyto metody nejsou bezpečné.

POZNÁMKA 4 Tato mezinárodní norma vnáší koncepční podobnost do ISO/IEC 19772[14], která specifikuje několik mechanismů pro autentizované šifrování, tj. současné dosažení integrity a důvěrnosti zprávy. Hlavní rozdíly mezi ISO/IEC 19772 a touto mezinárodní normou jsou tyto: (1) mechanismy specifikované v ISO/IEC 19772 spadají do kategorie symetrických kryptografických technik, kdežto mechanismy specifikované v této mezinárodní normě představují asymetrické

kryptografické techniky; (2) i když všechny mechanismy specifikované v ISO/IEC 19772 a v této mezinárodní normě nabízejí integritu dat a autentizaci původu dat, mechanismy specifikované v této mezinárodní normě nabízejí navíc ještě nepadělatelnost dat, a to dokonce i příjemcem dat.