ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červenec**
2001

	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí	ČSN ISO/IEC 9798-5 36 9743

Information technology - Security techniques - Entity authentication - Part 5: Mechanisms using zero knowledge techniques

Technologies de l’information - Techniques de sécurité - Authentification d´entité - Partie 5: Mécanismes utilisant les techniques de connaissance du zéro

Informationstechnik - Sicherheitsverfahren - Mechanismen zur Authentifikation von Instanzen - Teil 5: Mechanismen auf Basis von Zero-Knowledge-Techniken

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-5:1999. Mezinárodní norma ISO/IEC 9798-5:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9798-5:1999. The International
Standard ISO/IEC 9798-5:1999 has the status of a Czech Standard.

61395

Národní předmluva

Citované normy

ISO/IEC 9796 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie. Bezpečnostní techniky. Schéma digitálního podpisu umožňující obnovu zprávy, nahrazena ISO/IEC 9796-2:1997 a ISO/IEC 9796-3:2000

ISO/IEC 9798-1 zavedena v ČSN ISO/IEC 9798-1:1998 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanizmy autentizace míst - Část 1: Všeobecně

ISO/IEC 10118-1 zavedena v ČSN ISO/IEC 10118-1:1996 (36 9930) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 1: Všeobecně, nahrazena ISO/IEC 10118-1:2000

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí

ISO/IEC 9798-5
První vydání
1999-03-15

ICS 35.040

Obsah

Strana

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 dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% hlasujících členů.

Mezinárodní norma ISO/IEC 9798-5 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 9798 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Autentizace entit:*

– *Část 1: Všeobecně*

– *Část 2: Mechanismy používající symetrické šifrovací algoritmy*

– *Část 3: Mechanismy používající techniky digitálního podpisu*

– *Část 4: Mechanismy používající kryptografickou kontrolní funkci*

– *Část 5: Mechanismy používající techniky nulových znalostí:*

Přílohy A, B, C, D, E a F této části ISO/IEC 9798 jsou pouze informativní.

ISO a IEC upozorňují na skutečnost, že existují prohlášení, že na shodu s touto částí ISO/IEC 9798 může mít vliv použití patentů uvedených v příloze E.

ISO a IEC nezaujímají žádné stanovisko k důkazům, platnosti a rozsahu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni vyjednávat o licencích s uživateli po celém světě při zachování rozumných a nediskriminačních termínů a podmínek. V tomto smyslu jsou výroky držitelů těchto patentových práv organizacemi ISO a IEC zaprotokolovány. Informace je možné získat na adresách uvedených v příloze E.

Je třeba upozornit, že některé prvky této části ISO/IEC 9798 mohou být předmětem dalších patentových práv, která nejsou uvedena v příloze E. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

---

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje tři mechanismy autentizace entit používajících techniku nulových znalostí. Všechny mechanismy specifikované v této části ISO/IEC 9798 poskytují unilaterální autentizaci. Tyto mechanismy jsou sestaveny s použitím principů nulových znalostí, nebudou však odpovídat přísné definici načrtnuté v příloze A pro všechny volby parametrů.

První mechanismus je založený na identitách. Důvěryhodná akreditační autorita poskytuje každé nárokující straně soukromou akreditační informaci, vypočtenou jako funkce identifikačních dat nárokující strany a soukromého klíče akreditační autority.

Druhý mechanismus je založený na certifikátech, používající diskrétní logaritmy. Každá nárokující strana vlastní pro použití v tomto mechanismu dvojici veřejný klíč, soukromý klíč. Každý ověřovatel identity nárokující strany musí vlastnit důvěryhodnou kopii veřejného ověřovacího klíče nárokující strany; prostředky, kterými je toho dosaženo, jsou mimo rozsah této normy, může toho být však dosaženo distribucí certifikátů podepsaných důvěryhodnou třetí stranou.

Třetí mechanismus je založený na certifikátech, používající asymetrický šifrovací systém. Každá nárokující strana vlastní pro asymetrický šifrovací systém dvojici veřejný klíč, soukromý klíč. Každý ověřovatel identity nárokující strany musí vlastnit důvěryhodnou kopii veřejného klíče nárokující strany; prostředky, kterými je toho dosaženo, jsou mimo rozsah této normy, může toho být však

dosaženo distribucí certifikátů podepsaných důvěryhodnou třetí stranou.

-- Vynechaný text --