ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Měsíc Rok**

|  |  |
| --- | --- |
| Identifikační karty – Karty s integrovanými obvody s kontakty –Část 8: Mezioborové příkazy pro zabezpečení | ČSNISO/IEC 7816-836 9205 |

Identification cards – Integrated circuit(s) cards with contacts –
Part 8: Security related interindustry commands

Cartes d’identification – Cartes à circuit(s) intégré(s) à contacts –
Partie 8: Commandes intersectorielles de sécurité

Tato norma přejímá anglickou verzi mezinárodní normy ISO/IEC 7816-8:2004. Má stejný status jako oficiální verze.

This standard implements the English version of the International Standard ISO/IEC 7816-8:2004. It has the same status as the official version.

Anotace obsahu

Soubor norem ISO/IEC 7816 se společným názvem *Identifikační karty – Karty s integrovanými obvody* popisuje parametry identifikačních karet, které jsou vymezeny v ISO/IEC 7810 a použití těchto karet pro mezinárodní
výměnu.

Osmá část ISO/IEC 7816 specifikuje:

* bezpečnostní protokoly pro používání v kartách;
* rozšíření zabezpečené výměny zpráv;
* mapování mechanismů zabezpečování na bezpečnostní funkce/služby karet, včetně popisu zabezpečovacích mechanismů v kartě;
* datové prvky pro podporu zabezpečení;
* použití algoritmů implementovaných na kartě (avšak vlastní algoritmy nejsou popsány podrobně);
* použití certifikátů;
* příkazy vztahující se na zabezpečení.

Tato část ISO/IEC 7816 nepokrývá implementaci uvnitř karty a/nebo ve vnějším světě.

Výběr a podmínky používání kryptografických mechanismů mohou ovlivnit exportovatelnost karet. Vyhodnocení vhodnosti algoritmů a protokolů přesahuje předmět této části ISO/IEC 7816.

Není závazné, aby karty splňující tuto část ISO/IEC 7816 podporovaly všechny popsané příkazy nebo všechny možné volby podporovaných příkazů.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 7816-3:1997 zavedena v ČSN ISO/IEC 7816-3:2004 (36 9205) Informační technologie – Identifikační karty – Karty s integrovanými obvody s kontakty – Část 3: Elektronické signály a protokoly přenosu

ISO/IEC 7816-4:1995 zavedena v ČSN EN ISO/IEC 7816-4:1997 (36 9205) Informační technologie – Identifikační karty – Karty s integrovanými obvody a s kontakty – Část 4: Mezioborové příkazy pro výměnu

ISO/IEC 7816-6:1996 zavedena v ČSN EN ISO/IEC 7816-6:1998 (36 9734) Identifikační karty – Karty s inte-grovanými obvody a s kontakty – Část 6: Mezioborové datové prvky

ISO/IEC 9796:1991 nezavedena[[1]](#footnote-1)1)

ISO/IEC 9798-2:1994 nezavedena[[2]](#footnote-2)2)

ISO/IEC 9798-3:1993 nezavedena[[3]](#footnote-3)3)

ISO/IEC 9979:1991 nezavedena[[4]](#footnote-4)4)

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, obsahující překlad kapitoly Termíny a definice přejímané mezinárodní normy.

Vypracování normy

Zpracovatel: Anna Juráková, Praha, IČO 61278386, Dr. Karel Jurák

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Radek Dvořák

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.

# Národní příloha NA (informativní)

Termíny a definice

V této části ISO/IEC 7816 jsou uvedeny dále uvedené termíny a definice:

**3.1
certifikační autorita** *(Certification Authority)***CA** důvěryhodná třetí strana, která zajišťuje spojení veřejného klíče a dalších relevantních informací s jeho vlastníkem

**3.2
kryptografický mechanismus** *(cryptographic mechanisms)*funkce poskytované kartou jako výsledek implementace kryptografických algoritmů do karty se specifickou sadou operačních parametrů, např. režim činnosti a velikost dat nebo klíčů

**3.3
zabezpečená výměna zpráv** *(secure messaging)*výměna zpráv poskytující prostředky pro kryptografickou ochranu dat vyměňovaných v průběhu příkazu (jak je popsáno v ISO/IEC 7816-4) kódovaných podle pravidel BER-TLV (viz tabulka A.1)

**NÁSLEDUJE TEXT PŘEJÍMANÉHO ORIGINÁLU**

1. 1) ČSN ISO/IEC 9796:1996, která přejímala ISO/IEC 9796:1991, byla zrušena z důvodu nahrazení mezinárodní normy
novějším vydáním a je dostupná v zákaznickém centru ČAS. [↑](#footnote-ref-1)
2. 2) ČSN ISO/IEC 9798-2:1998, která přejímala ISO/IEC 9798-2:1994, byla zrušena z důvodu nahrazení mezinárodní normy novějším vydáním a je dostupná v zákaznickém centru ČAS. [↑](#footnote-ref-2)
3. 3) ČSN ISO/IEC 9798-3:1997, která přejímala ISO/IEC 9798-2:1993, byla zrušena z důvodu nahrazení mezinárodní normy novějším vydáním a je dostupná v zákaznickém centru ČAS. [↑](#footnote-ref-3)
4. 4) ČSN ISO/IEC 9979:1996, která přejímala ISO/IEC 9979:1991, byla zrušena z důvodu nahrazení mezinárodní normy
novějším vydáním a je dostupná v zákaznickém centru ČAS. [↑](#footnote-ref-4)