PŘEDBĚŽNÁ ČESKÁ TECHNICKÁ NORMA

ICS 03.220.01; 35.240.60

**Leden 2018**

# Inteligentní dopravní systémy – Dopravní a cestovní informace (TTI) v dopravním protokolu expertní skupiny, druhá generace (TPEG2) – Část 24: Jednoduché šifrování (TPEG2-LTE)

ČSN P ISO/TS 21219-24

01 8259

Intelligent transport systems – Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) –
Part 24: Light encryption (TPEG2-LTE)

Systemes intelligents de transport – Informations sur le trafic et le tourisme via le groupe expert du protocole de transport, génération 2 (TPEG2) –
Partie 24: Cryptage léger (TPEG2-LTE)

Tato předběžná norma přejímá anglickou verzi technické specifikace ISO/TS 21219-24:2017. Má stejný status jako oficiální verze.

This prestandard implements the English version of the Technical Specification ISO/TS 21219-24:2017. It has
the same status as the official version.

Anotace obsahu

Tato technická specifikace definuje šifrovací mechanismy LTE pro datové rámce služby TPEG. Navrhuje šifrování symetrickým sdíleným klíčem, který je podle pravidel daných touto normou pozměňován, aby nebylo příliš snadné zprávu rozšifrovat. Specifikace byla navržena pro použití v business modelu B2B.

Národní předmluva

Upozornění na používání této normy

Tato předběžná česká technická norma přejímá technickou specifikaci ISO/TS 21219-24:2017 vydanou v souladu se směrnicemi ISO/IEC, část 1 a je určena k ověření. Případné připomínky k obsahu normy přijímá Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, odbor technické normalizace.

Převzetí TS nevyžaduje zrušení konfliktních národních norem platných pro stejný předmět normalizace.

Informace o citovaných dokumentech

ISO/TS 21219-1 dosud nezavedena

ISO/TS 21219-2 dosud nezavedena

ISO/TS 21219-3 dosud nezavedena

ISO/TS 21219-4 dosud nezavedena

ISO/TS 21219-5 dosud nezavedena

ISO/TS 21219-9 dosud nezavedena

Federal Information Processing Standards Publication 197 – Specifikace pro standard pokročilého šifrování (AES), 26. listopad, 2001 nezavedeno

NIST Special Publication 800-38A:2001 Doporučení pro režim blokové šifry: Metody a techniky nezavedeno

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Informace o citovaných dokumentech“ 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).

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje překlad kapitoly 3 a 4 technické specifikace.

Vypracování normy

Zpracovatel: SILMOS s.r.o. – CTN, IČ 45276293, ve spolupráci s ČVUT v Praze, Ing. Petr Bureš, Ph.D.

Technická normalizační komise: TNK 136 Dopravní telematika

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jan Křivka