

# ISO 24100 - Privacy - Basic principles for probe personal data protection

**Application Area:** [Communications](#), [Data and information transfer security](#)

**Publication Year, Number of Pages:** Published 2010, 29 pages

**Zavedení normy do ČSN:** nezavedena

**Extract Creation Year:** 2009

**Standard Topic Group:** CALM

**Standard Topic:** CALM plovoucí vozidlo

**Topic Description:** CALM - základní přístupy k ochraně osobních informací u plovoucích vozidel

<b>Introduction, Explanation of Starting Points</b>
CALM - základní přístupy k ochraně osobních informací u plovoucích vozidel
<b>Description of Architecture, Hierarchies, Roles, and Object Relationships</b>
<b>Description of Process / Function / Method of Use</b>
<b>Description of Interfaces / APIs / System Structure</b>
<b>Protocol / Algorithm / Computation Definition</b>
<b>Definition of Data Representation / Physical Meaning</b>
<b>Definition of Constants / Ranges / Restrictions</b>

## Introduction

Tato mezinárodní norma je součástí skupiny norem, které standardizují rozhraní [CALM \(komunikační infrastruktura pro pozemní mobilní zařízení\)](#). Rozhraní [CALM](#) vytváří univerzální komunikační model zajišťující jednoduchou a pružnou výměnu dat mezi vozidly a silniční infrastrukturou. Využití rozhraní [CALM](#) ve vozidlových jednotkách a na silniční infrastruktuře umožňuje snadnou realizaci nových telematických služeb jako je například automatický přenos informace o nehodě z havarovaného vozidla, inteligentní dopravní značení s přímou vazbou na projíždějící vozidlo, online sběr dopravních dat z plovoucích vozidel, internet a interaktivní multimediální zábava ve vozidlech. Kromě toho že [CALM](#) využívá stávající komunikační infrastrukturu, do budoucna zůstává otevřen i pro nové budoucí systémy komunikace. [CALM](#) nahrazuje různé jednoúčelové komunikační protokoly navržené výrobcí vozidel a zavádí pro všechny jednotnou komunikační platformu.

Tato norma je zpracována v rámci ISO TC204, pracovní skupiny WG16. Norma je ze skupiny norem zaměřených na senzorové systémy ve vozidlech, monitorování stavu vozidla a komunikace vozidel s centrem.

Mezi centrem a vozidly je realizována datová cesta, zejména ve směru vozidlo-centrum může v některých případech probíhat přenos osobních informací vztažených ke konkrétnímu vozidlu. S ohledem na zachování utajení datových informací na přenosové trase je nezbytné definovat základní přístupy k jejich ochraně.

Ochrana osobních dat vyplývá ze základních principů definovaných v rámci OECD v roce 1980.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

## Application

Současné systémy ve vozidlech využívají mnoha senzorových systémů monitorování stavu a zařízení ve vozidlech. Tyto informace jsou dále předávány bezdrátovými technologiemi do řídicích center. Struktura přenášených senzorových dat musí být unifikována; stejně tak musí být unifikovány systémy správy těchto dat (PDRM). Vzhledem k tomu, že je v některých případech nezbytné přiřazení informace konkrétnímu vozidlu či osobě, je nezbytné zajištění ochrany těchto osobních dat při přenosu z vozidla do centra.

Tato norma definuje základní přístupy k ochraně osobních dat zejména poskytovatelům služeb pro monitorovací vozidlové systémy.

**Pro poskytovatele služeb**

Sjednocení stejné úrovně zabezpečení přenosových tras pro osobní data vozidlo-centrum.

**Pro uživatele (řidiče) vozidel**

Definováním jednotných přístupů dojde ke zvýšení transparentnosti sběru dat z vozidel a tím ke zvýšení věrohodnosti senzorových systémů z pohledu uživatelů systému.

**Související normy**

K zajištění shody s touto normou je nezbytné, aby všechny protokoly technických řešení podle IEEE 802.16e byly ve shodě s platnými národními předpisy a splňovaly požadavky následujících norem:

- [ISO 21217](#) architektura [CALM](#);
- [ISO 21210](#) síťové protokoly [CALM](#);
- [ISO 21218](#) přístupové body [CALM](#).

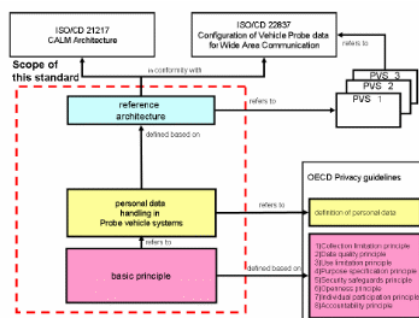
Tato norma je úzce vázána na další související normy ([ISO 24102](#), [ISO 25111](#), předpis IEEE 802.16e a IEEE802.16g).

**1. Scope**

Norma je zaměřena na následující tři oblasti:

- Definuje referenční architekturu systémů sledování sond ve vozidlech, architektura se vztahuje k požadavkům normy ISO CD [22837](#);
- Definuje význam osobních dat dle ustanovení závěrů OECD z roku 1980 a datové toky systémů sledování sond ve vozidlech;
- Definuje základní přístupy k ochraně osobních dat zasílaných vozidlovými sondami do centra.

Následující schéma zobrazuje předmět této normy:



**Obrázek 1 - Předmět normy**

Norma dále navazuje na tyto normy:

- ISO/IEC 13335-1 Informační technologie – Bezpečnostní [procesy](#) – Část 1: Koncepty a modely pro Bezpečnostní systémy managementu informačních a komunikačních technologií
- ISO CD [22837](#) Inteligentní dopravní systémy – Konfigurace dat vozidlové sondy pro dálkové komunikace

## 2. Terms and Definitions

**autentizace** (*authentication*) identifikace správného ID prvku či zdroje

**autentizační data** (*authentication data*) data v [procesu](#) identifikace

**kontextová data** (*contextual data*) kontextová data obsahující informaci o informacích

**kryptografie** (*cryptography*) vědní obor, který zahrnuje principy, prostředky a metody pro transformaci dat za účelem skrytí jejich informačního obsahu, zabránění jejich neautorizovanému použití, ověření jejich pravosti, zabránění jejich neodhalenému pozměnění a/nebo zabránění jejich odmítnutí (repudiation)

**zdroj dat** (*data source*) odesílatel sensorových dat z vozidla do „sběrače“ těchto dat v systému vozidlových sond

**datový subjekt** (*data subject*) osoba, od které jsou shromažďována / pomocí které jsou odhalována a používána osobní data ve sběrači sensorových dat

**dešifrování** (*decryption*) inverzní funkce k [šifrování](#)

**šifrování** (*encryption*) funkce transformující data prostřednictvím kryptografie tak, aby byla nedešifrovatelná kýmkoliv jiným než oprávněným odesílatelem a příjemcem

**šifrovací data** (*encryption data*) data určená k zašifrování

**integrita** (*integrity*) kompletnost a harmonizace metod a dat

**osobní data** (*personal data*) data náležící konkrétnímu jedinci a zároveň jej identifikující, přenášená ze systému vozidlové sondy definovaného v ISO CD [22837](#) do centra, při sběru [dat sondy](#) z vozidla a jejich přenosu

**sběr dat ze sond** (*probe collection*) aplikace přijímající zprávy z vozidel a dekomponování jejího obsahu

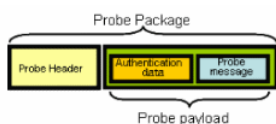
**data sondy** (*probe data*) obsahují datové prvky a [zprávy sondy](#); [data sondy](#) je informace ze sensorů vozidla, která je zpracována, formátována a přenesena do [základnové stanice](#) s [cílem](#) určit aktuální stav vozidla a prostředí, ve kterém se pohybuje

**kolektor dat sond** (*probe data collector*) [proces](#) příjmu sensorových dat z vozidel a jejich dekompozice na místě určení

**hlavička zprávy** (*probe header*) datový obsah odpovídající struktuře požadované konkrétním přenosovým médiem

**zpráva sondy** (*probe message*) výsledek transformace a formátování jednoho nebo více [datových prvků sondy](#) do jedné formy vhodné pro dodání do palubního komunikačního zařízení pro další přenos do [základnové stanice](#)

**datový paket sondy** (*probe package*) datový paket s informacemi z vozidla přenesený do centra



**užitná data sondy** (*probe payload*) data přenášená v aplikační vrstvě z vozidla do [kolektorů dat sondy](#)

**zpracování dat sondy** (*probe processing*) [proces](#) zpracování dat obdržených z vozidel v centru bez identifikace vozidla nebo řidiče

**systém sledování sond vozidel** (*probe vehicle system*) systém obsahující 1) vozidla se sondami zasílajícími data ke zpracování a 2) [základnové stanice](#) zpracovávající sensorová data; [zpracováním dat sondy](#) se vytvoří přesná představa o celkové situaci na PK a podmínkách řidiče sloučením a analýzou dat z více vozidel a dat z jiných zdrojů; takto



Příklady	Registrační informace o odesílateli Databáze osob a jejich hesel	Mapy s POI Knihovny adres Žluté stránky WHOIS databáze Databáze zón konkrétní domény ser
----------	---	--

Rovněž mezi osobní data patří systémy, které přenášejí informace s časovou známkou a lokalizací, které mají vazbu na osobní informaci.

### Šifrovaná data, označovaná jako osobní data

Jedná se o data šifrovaná dle daného klíče, která jsou u [cíle](#) dešifrována a stávají se osobními informacemi.

Následující tabulka č.2 znázorňuje případy šifrovaných dat.

**Tabulka 2 - Případy šifrovaných dat**

	<b>Šifrovaná data s možností vzniku osobních d</b>
Definice	V případech, kdy je osoba identifikována během šifrovacích <ul style="list-style-type: none"> <li>• Šifrovaná data, která mohou identifikovat konkrétní osobu</li> <li>• Šifrovaná data používaná osobou disponující databází dat s tím, že data nemohou přímo identifikovat konkrétní osobu</li> </ul>
Konkrétní případy užití	Šifrovaná data použitá v šifrovacím <a href="#">procesu</a> osobou disponující databází těchto dat v případech, kdy je v <a href="#">procesu šifrování</a> šifrovací klíč pro konkrétní sondu vozidla

### Data užívaná k identifikaci, označená v některých případech jako osobní

Data používaná k [autentizaci](#) doručené zprávy, zda je ta, za kterou je považována, jsou rovněž nosičem osobních informací vztahených k osobě či vozidlu.

Následující tabulka č.3 znázorňuje případy dat pro identifikaci označovaná také jako osobní data.

**Tabulka 3 - Případy dat pro identifikaci**

	<b>Autentizační data, která mohou být daty osobními</b>
Definice	<ol style="list-style-type: none"> <li>1. <a href="#">Autentizační data</a>, která mohou přímo identifikovat osobu</li> <li>2. <a href="#">Autentizační data</a> získaná osobou oprávněnou disponovat s těmito daty s tím, že tato data nemohou přímo identifikovat osobu</li> </ol>
Příklady	<p>Příklad k bodu 1:</p> <p>Data použitá s veřejným šifrovacím klíčem, obsahující veřejné klíče odesílatelů sond z vozidel</p> <p>Příklad k bodu 2:</p> <p>Data použitá v <a href="#">procesu</a> <a href="#">autentizace</a> a získaná osobou oprávněnou disponovat auter databází</p>

## **6 Základní přístupy**

Základní přístupy definují způsoby ochrany osobních dat při odesílání z vozidel.

Základní přístupy jsou vyvinuty a zkoušeny na základě rizikové analýzy, viz příloha A.

Základní rámec je převzat z nařízení OECD z roku 1980.

## **7 Omezení sběru dat**

Kapitola obsahuje sadu požadavků omezujících sběr dat ze sensorického vozidlového systému.

## **8 Požadavky na kvalitu dat**

Kapitola definuje požadavek na přesnost a aktuálnost dat, která mají být v centru přijímána.

## **9 Specifikace případů užití**

Kapitola obsahuje požadavky na centrum sběru dat z hlediska definování jejich způsobů užití.

## **10 Přístup k omezení užití dat**

Kapitola definuje požadavky na ověření oprávnění k užití sbíraných osobních dat z vozidel.

## **11 Přístup k ochraně dat**

Kapitola definuje požadavky na kontrolu přístupu k datům a jejich ochranu přes neoprávněným přístupem třetích stran.

## **12 Princip otevřenosti**

Kapitola definuje požadavek, za kterého lze data poskytnout např. Policii, částečně pro vývoj, apod.

## **13 Požadavky na individuální přístup**

Kapitola definuje požadavky na ošetření přístupu k datům ze strany individuálních přístupů

## **14 Princip protokolování**

System musí umožnit zaznamenání jednotlivých přístupů a operací s osobními daty ke kontrole přístupů k datům

## **Příloha A (informativní) Rizika a hrozby zneužití osobních dat**

Příloha s analýzou možných rizik je zaměřena zejména na dvě skupiny rizik:

- Rizika zaměřená speciálně na data ze systémů sond ve vozidle;
- Rizika spojená s riziky v telekomunikační síti obecně, bez ohledu na typ přenášených dat.

Tabulka č.4 popisuje příklady rizik pro data ze systémů sond.

**Tabulka 4 - Příklady rizik pro data ze systémů vozidlových sond**

Číslo	Hrozba, riziko	Umístění v architektuře systému	Popis rizika, hrozby	Vazba na princip ochrany dat dle O
T-4	Užití ID informace a obsahu datové zprávy k jiným účelům, než je určena	Příjem <u>datových paketů sondy</u>	<u>Proces</u> , který ohrožuje zájmy odesílatele <u>dat sondy</u> v případě, že ID zprávy obsahuje osobní data	(2) princip kvality dat (3) princip specifikace <u>cíle</u> (4) princip omezení využití

Tabulka č.5 představuje možná rizika z hlediska napadení v telekomunikační síti obecně.

**Tabulka 5 - Rizika napadení v telekomunikační síti**

Číslo	Hrozba, riziko	Umístění v architektuře systému	Popis rizika, hrozby	Vazba na princip ochrany dat dle O
T-1	Útok na vnitřní vozidlový systém	Odesílatel <u>dat sondy</u>	<u>Proces</u> pokusu o neautorizovaný přístup k datům uloženým ve vozidle	(5) princip zajištění bezpečnosti

Tabulka č.6 znázorňuje detailní rizika a hrozby pro data ze systémů sond ve vozidlech

**Tabulka 6 - Detailní rizika a hrozby pro data ze systémů sond ve vozidlech**

Číslo	Hrozba, riziko	Principy OECD k zajištění bezpečnosti osobních dat				
		Princip omezení sběru dat	Princip kvality dat	Princip specifikace <u>cíle</u>	Princip omezení přístupu	Princip zajištění bezpečnosti
T-4	Užití ID informace a obsahu datové zprávy k jiným účelům, než je určena		Riziko zneužití ID datových zpráv předchozího majitele prodaného vozidla	a) Riziko zneužití ID datových zpráv, kdy není specifikován <u>cíl</u> využití b) Riziko zneužití ID datových zpráv, kdy je <u>cíl</u> užití změněn	a) Riziko zneužití ID datových zpráv, k jiným účelům, než jsou definovány b) Riziko zneužití ID datových zpráv třetí osobu při jejich přenosu ze zdroje k <u>cíli</u> c) Riziko zneužití ID datových zpráv třetí osobou, aniž by jí byla přiřazena práva v souladu s legislativou	

#### Associated Terms

- [data source](#)
- [probe data sender](#)
- [probe payload](#)
- [encryption](#)
- [cryptography](#)
- [contextual data](#)
- [probe data collector](#)
- [probe header](#)
- [decryption](#)
- [data subject](#)
- [probe package](#)
- [probe processing](#)