

ISO/TS 24534-5 - Automatic vehicle and equipment identification - Electronic Registration Identification (ERI) for vehicles - Part 5: Secure communications using symmetrical techniques

EXTRACT NOT UPDATED TO THE LATEST VERSION OF THE STANDARD

Application Area: [Automatic Vehicle and Equipment Identification \(AVI/AEI\)](#)

Publication Year, Number of Pages: Published 2008, 38 pages

Extract Creation Year: 2010

Standard Topic Group: Automatická identifikace vozidel, zařízení a nákladů

Standard Topic: Identifikace elektronické registrace (ERI) vozidel

Topic Description: Zabezpečení aplikační vrstvy použitím symetrického šifrování

Introduction, Explanation of Starting Points
Specifikace podporuje různé úrovně bezpečnosti s maximální kompatibilitou
Description of Architecture, Hierarchies, Roles, and Object Relationships
Definice šifrování, zabezpečený přístup k datům a jejich editace
Description of Process / Function / Method of Use
Description of Interfaces / APIs / System Structure
Protocol / Algorithm / Computation Definition
Definition of Data Representation / Physical Meaning
Definition of Constants / Ranges / Restrictions

Introduction

Tato technická specifikace je součástí norem zaměřených na [automatickou identifikaci vozidla](#), [nákladu](#) či položky zařízení – elektronickou [identifikaci](#). Čtyřmi předcházejícími částmi jsou architektura, provozní požadavky, data o vozidle a asymetrické šifrování pro zabezpečenou komunikaci. Tato část specifikace popisuje aplikační vrstvu rozhraní mezi zařízeními ve vozidle obsahujícím elektronickou [identifikaci vozidla \(ERT\)](#) a čtecím nebo zápisovým zařízením vně nebo uvnitř vozidla. Symetrické šifrování je založeno na tajném kódu sdíleném určitou skupinou [uživatelů](#). Asymetrické šifrování je popsáno v části 4.

Poznámka: Extrakt uvádí [vybrané](#) kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

Application

Specifikace se zabývá rozhraním mezi zařízením obsahujícím identifikační informace ([ERT](#)) a palubním čtecím nebo zápisovacím zařízením, mezi tímto palubním zařízením a čtecím nebo zápisovacím zařízením na dopravní komunikaci a v neposlední řadě se zabývá [bezpečností](#) těchto komunikací.

1. Scope

Popisovaný dokument stanovuje požadavky na elektronickou [identifikaci](#) registrace vozidla ([ERI](#)) s využitím symetrického šifrování, založenou na [identifikátoru](#) přiděleném vozidlu. [ERI](#) slouží k [identifikaci](#) tuzemských i

zahraničních vozidel [úřady](#), ke správě [životního](#) cyklu vozidla, k úpravě dat vozidla (např. při prodeji do zahraničí), k bezpečnostním účelům, k potírání kriminality a pro komerční služby při dodržení ochrany [soukromí](#) a osobních údajů.

Popisovaný dokument stanovuje rozhraní pro zabezpečenou výměnu dat mezi elektronickým registračním tagem ([ERT](#)), tj. palubním zařízením obsahujícím data [ERI](#), a čtečkou nebo zapisovačem [ERI](#) ve vozidle nebo mimo něj:

- rozhraní mezi [ERT](#) a palubní čtečkou nebo zapisovačem [ERI](#),
- rozhraní mezi palubním zařízením [ERI](#) a (silničním) čtecím a zapisovacím zařízením,
- [zabezpečení](#) komunikace s [ERT](#).

Symetrické šifrování je založeno na [tajných klíčích](#) sdílených uzavřenou skupinou [uživatelů](#). [Identifikátory](#) vozidla a související údaje o vozidle stanovuje [ISO 24534-3](#).

2. Related Documents (Selection)

Popisovaný dokument uvádí 4 normativní odkazy: ISO/IEC 8825-2 (pravidla kódování PER), [ISO 14816](#) (číslování a datové struktury [AVI/AEI](#)), [ISO 15628](#) a EN 12834 (aplikační vrstva [DSRC](#)). Specifikace podporuje [automatickou identifikaci vozidel](#) popsanou v normách [ISO 14814](#) a [ISO 14816](#).

3. Terms and Definitions

Kapitola stanovuje termíny z [oblasti](#) elektronické [identifikace](#) a [zabezpečení komunikace](#), z nichž klíčové jsou:

elektronická [identifikace](#) registrace (*electronic registration identification*) [842] – úkon [identifikace vozidla](#) elektronickými prostředky pro účely uvedené v [předmětu](#) popisovaného [dokumentu](#)

elektronický registrační [tag](#) (*electronic registration tag*) [2714] – [palubní zařízení ERI](#), které obsahuje [data ERI](#) včetně implementovaných bezpečnostních [opatření](#) a jedno nebo více rozhraní pro [přístup](#) k těmto [datům](#)

[čtečka ERI](#) (*ERI reader*) – zařízení pro čtení [dat ERI](#) přímo nebo nepřímo z [ERT](#) pomocí [transakcí ERI](#)

[zapisovač ERI](#) (*ERI writer*) – zařízení pro [zápis dat ERI](#) přímo nebo nepřímo do [ERT](#) pomocí [transakcí ERI](#)

[provozovatel systému ERI](#) (*ERI system operator*) – [organizace odpovědná](#) za provoz [systému ERI](#), která je [bezpečnostní autoritou](#) bezpečnostní [domény ERI](#)

[tajný klíč](#) (*secret key*) – [klíč](#) používaný se symetrickým kryptografickým algoritmem

[vzájemná autentizace](#) (*mutual authentication*) – autentizace [entit](#), která oběma [entitám](#) poskytuje jistotu o [identitě](#) té druhé

[seznam řízení přístupu](#) (*access control list*) – seznam [entit](#) spolu s jejich přístupovými právy, které jsou oprávněny k [přístupu](#) ke [zdroji](#)

Další termíny a zkratky z oboru [ITS](#) jsou obsaženy ve slovníku [ITS](#) terminology.

4. Abbreviations

Kapitola uvádí zkratky, mimo jiné:

[ERI](#) elektronická [identifikace](#) registrace (*Electronic Registration Identification*)

[ERR](#) elektronická registrační [čtečka](#), zařízení pro čtení nebo [zápis dat ERI](#) (*Electronic Registration Reader*)

[ERT](#) elektronický registrační [tag](#) (*Electronic Registration Tag*)

[OBE](#) [palubní zařízení](#) (*Onboard Equipment*)

[PICS](#) [prohlášení o shodě implementace protokolu](#) (*Protocol Implementation Conformance Statement*)

[SAM](#) bezpečnostní aplikační [modul](#) (*Secure Application Module*)

[VIN](#) identifikační číslo [vozidla](#) (*Vehicle Identification Number*)

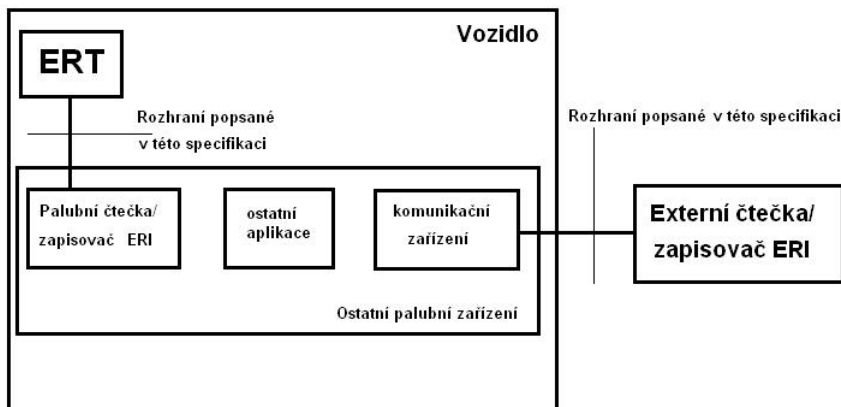
Další termíny a zkratky z oboru [ITS](#) jsou obsaženy ve slovníku [ITS terminology](#) (www.ITSterminology.org).

5 Koncept komunikace systému

Kapitola je informativního charakteru pro lepší pochopení celého konceptu elektronické [identifikace](#). Normativní požadavky na rozhraní stanovuje kapitola 6 a příloha A.

Článek 5.1 vymezuje kontext: rozhraní se symetrickým šifrováním pro uzavřenou skupinu [uživatelů](#) v jurisdikci jednoho [provozovatele systému ERI](#), který odpovídá za správu [klíčů](#) a působí jako registrační autorita. Obecnější rozhraní s asymetrickým šifrováním pro spolupráci více autorit stanovuje [ISO 24534-4](#).

Článek 5.2 popisuje [identifikaci vozidla](#) ([identifikátor](#) vozidla, přednostně VIN, spolu s jedinečným číslem [ERT](#)), koncepci systému a podporovaná rozhraní (obrázek 1), zúčastněné role, kontext čtení a zápisu dat [ERT](#) a podporované [úrovně služeb](#).



Obrázek 1 - Koncepce systému a podporovaná rozhraní (obr. 1 popisovaného dokumentu)

Článek 5.3 stanovuje bezpečnostní služby: předpoklady (odolnost [ERT](#) proti aktivním i [pasivním hrozbám](#), použitelnost čtení jako důkazu, ochrana [soukromí](#), ochrana vozidla před útokem přes [ERI](#)), autentizaci entit a [důvěrnost](#) při čtení dat [ERI](#), [klíče](#) pro autentizaci a [důvěrnost](#) a [řízení přístupu](#) k datům [ERI](#). Článek 5.4 popisuje architekturu komunikace pro [identifikaci vozidla](#), pro vzdálený přístup a palubní komunikaci, článek 5.5 vzdušné rozhraní krátkého dosahu a palubní rozhraní s [ERT](#).

6 Požadavky rozhraní

Kapitola stanovuje rozhraní pro přístup k datům [ERI](#) v [ERT](#): článek 6.2 abstraktní definice transakcí, článek 6.3 palubní rozhraní s [ERT](#), článek 6.4 vzdušné rozhraní krátkého dosahu mezi palubním zařízením [ERI](#) a vnější čtečkou nebo zapisovačem a článek 6.5 rozhraní pro vzdálený přístup.

Komunikace s [ERT](#) probíhá v relacích. Relace se skládá ze tří po sobě jdoucích fází (čl. 6.2.2):

1. Vzájemná [autorizace](#) – jedná se o vzájemnou [autorizaci](#) mezi [ERT](#) a [ERI](#) čtečkou nebo zapisovačem, pokud je [ERT](#) v pověřeném stavu. Pokud [ERT](#) není v tomto stavu, je tato fáze přeskočena.
2. Fáze výměny dat – v této fázi probíhá výměna dat [ERI](#) nebo bezpečnostních dat, a to v jakémkoliv pořadí.
3. Ukončovací fáze.

Popisovaný dokument stanovuje 9 transakcí, jejich přehled je v tabulce 1. Většina transakcí probíhá ve fázi výměny dat, kromě vzájemné [autorizace](#), která probíhá v autorizační fázi. Transakce jsou v popisovaném dokumentu popsány s jednotlivými možnostmi, které mohou nastat, a definovány ve formátu [ASN.1](#), příklady jsou ve výpisech 1 až 3.

Tabulka 1 - Povinné a volitelné transakce (tab. 1 popisovaného dokumentu)

Článek	Transakce	Povinnost	Popis
6.2.4	mutualAuthentication1	R	vzájemná autentizace , 1. krok
6.2.5	mutualAuthentication2	R	vzájemná autentizace , 2. krok
6.2.6	getSecretKeyEriData	R	čtení dat ERI úřady nebo provozovatelem systému
6.2.7	setSecretKeyEriData	R	přizpůsobení ERT a aktualizace dalších dat ERI provozovatelem systému
6.2.8	commissionSecretKeyErt	A, C	nahrání symetrických klíčů provozovatele systému do ERT
6.2.9	decommissionSecretKeyErt	O	odstranění klíčů provozovatele systému
6.2.10	updateAccessControlList	A, C	přidání nebo odebrání úřadů v seznamu řízení přístupu ERT
6.2.11	getCiphertextAccessControlListEntry	O	čtení položek seznamu řízení přístupu v zašifrované podobě
6.2.12	endOfSession	R	ukončení relace ERI

Povinnost: R – vždy povinná, C – povinná pro [důvěrnost](#), A – povinná pro autentizaci, O – volitelná.

Vzájemná autorizace 1 – funkce probíhá jako první v první fázi. Vyvolává ji čtečka/zapisovač [ERI](#) a odpovídá na ni [ERT](#). Transakce je ve výpisu 1.

```
mutualAuthentication1 TRANSACTION ::= {
  ARGUMENT  OCTET STRING
  RESULT    OCTET STRING
  CODE      1
}
```

Výpis 1 – Transakce mutualAuthentication1 (čl. 6.2.4 popisovaného dokumentu)

Získání dat [ERI](#) – funkce slouží pro získání dat [ERI](#) z [ERT](#), vykonává ji pouze [ERT](#), pouze pokud je v přizpůsobeném a pověřeném stavu (viz výpis 2).

```
getSecretKeyEriData TRANSACTION ::= {
  ARGUMENT  OCTET STRING
  RESULT    OCTET STRING
  CODE      3
}
```

Výpis 2 – Transakce getSecretKeyEriData (čl. 6.2.6 popisovaného dokumentu)

Aktualizace přístupového seznamu – přístupový seznam obsahuje unikátní [klíče](#) jednotlivých [uživatelů](#), kteří vstupovali do [ERT](#). Lze ji provést pouze v [ERT](#) v pověřeném stavu. Transakce je ve výpisu 3.

```
updateAccessControlList TRANSACTION ::= {
  ARGUMENT  OCTET STRING
  RESULT    OCTET STRING
  CODE      7
}
```

Výpis 3 – Transakce updateAccessControlList (čl. 6.2.10 popisovaného dokumentu)

Rozhraní (čl. 6.3 až 6.5)

Data [ERI](#) a zabezpečená data [ERI](#) a [ERT](#) samotné mohou být přístupná pouze podle této specifikace. Výměna dat na aplikační vrstvě [ERT](#) je v protokolu SecretKeyEriPdu, který je možné dekodovat podle normy ISO 8825-2. Protokoly na nižších vrstvách jsou stanoveny mezinárodními normami.

V případě, že komunikace mezi [ERT](#) a čtečkou [ERI](#) je založena na ISO 14443, se [ERT](#) chová jako PICC typu A nebo B a palubní čtečka/zapisovač [ERI](#) jako PCD podporující oba typy (A i B). Jednotka protokolu [ERI](#) může být přímo převedena

použitím pole INF. Nesmí být zabalena podle ISO 7816-4.

Pokud použijeme pro aplikační vrstvu [ERI DSRC](#), musí být použita norma [ISO 15628](#). To umožní [ERI DSRC](#) být kompatibilní s ostatními aplikacemi [DSRC](#).

Vzdálený přístup musí využívat pro dekódování pravidla PER podle ISO 8825-2. Nižší vrstvy opět podle mezinárodních norem.

Příloha A (normativní) Moduly [ASN.1](#)

Příloha stanovuje normativní modul [ASN.1](#) EriSecretKeyTransactionsModule s definicemi transakcí a jednotek protokolu (SecretKeyEriPdu) a informativní modul AviEriDSRCData pro použití s aplikační vrstvou [DSRC](#). Při rozporu s ostatním textem popisovaného dokumentu mají přednost definice v této příloze.

Příloha B (informativní) Provozní scénáře

Příloha popisuje tři scénáře, které se mohou stát při komunikaci mezi čtečkou/zapisovačem [ERI](#) a [ERT](#). Popisuje scénáře [identifikace vozidla](#) (B.2), relace čtení a zápisu dat [ERI](#) (B.3) a relace zápisu a zprovoznění [ERT](#) (B.4).

Příloha C (normativní) Formulář PICS

Příloha obsahuje nevyplněné prohlášení o shodě implementace protokolu PICS (Protocol Implementation Conformance Statements) k použití pro [ERT](#) a čtečky a zapisovače [ERI](#).

Related Documents (Selection)

- [CEN ISO/TS 24534-1 - Automatic vehicle and equipment identification – Electronic Registration Identification \(ERI\) for vehicles – Part 1: Architecture](#)
- [EN ISO 24534-2 - Automatic vehicle and equipment identification – Electronic Registration Identification \(ERI\) for vehicles – Part 2: Operational requirements](#)
- [EN ISO 24534-3 - Automatic vehicle and equipment identification – Electronic Registration Identification \(ERI\) for vehicles – Part 3: Vehicle data](#)
- [EN ISO 24534-4 - Automatic vehicle and equipment identification – Electronic Registration Identification \(ERI\) for vehicles – Part 4: Secure communications using asymmetrical techniques](#)
- [ISO 24535 - Automatic vehicle and equipment identification – Electronic Registration Identification \(ERI\) for vehicles – Part 2: Operational requirements](#)

Associated Terms

- [security authority](#)
- [system operator](#)
- [ERI system operator](#)
- [secret key](#)
- [mutual authentication](#)