EN ISO 24534-4 - **Dopravní telematika – Automatická identifikace vozidel, zařízení a nákladů – Identifikace elektronické registrace (ERI) vozidel – Část 4: Zabezpečení aplikační vrstvy použitím asymetrického šifrování**

Aplikační oblast: Automatická identifikace vozidel, zařízení a nákladů (AVI/AEI)

Rok vydání normy a počet stran: Vydána 2010, 102 stran

Rok zpracování extraktu: 2010

Skupina témat: Automatická identifikace vozidel, zařízení a nákladů

Téma normy: Identifikace elektronické registrace (ERI) vozidel

Charakteristika tématu: Zabezpečení aplikační vrstvy použitím asymetrického šifrování

Úvod, vysvětlení východisek
Koncept komunikace systému

Popis architektury, hierarchie, rolí a vztahů objektů
Zabezpečení asymetrickým šifrováním

Popis procesu / funkce / způsobu použití

Popis rozhraní / API / struktury systému

Definice protokolu / algoritmu / výpočtu

Definice reprezentace dat / fyzikálního významu

Definice konstant / rozsahů / omezení

Úvod

Tato technická specifikace je součástí norem zaměřených na automatickou identifikaci vozidla, nákladu či položky zařízení – elektronickou identifikaci. Tři předcházející částmi jsou architektura, provozní požadavky a data o vozidle. Tato část specifikace popisuje aplikační vrstvu rozhraní mezi zařízením ve vozidle obsahujícím elektronickou identifikaci vozidla (ERT) a čtecím nebo zápisovým zařízením vně nebo uvnitř vozidla. Data vyměněná mezi těmito dvěma zařízeními zabezpečená asymetrickým šifrováním jasně určují dané vozidlo a obsahují často informace z technického průkazu vozidla. Další (5.) norma tohoto souboru se také týká zabezpečení aplikační vrstvy, ale pomocí symetrického šifrování.

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

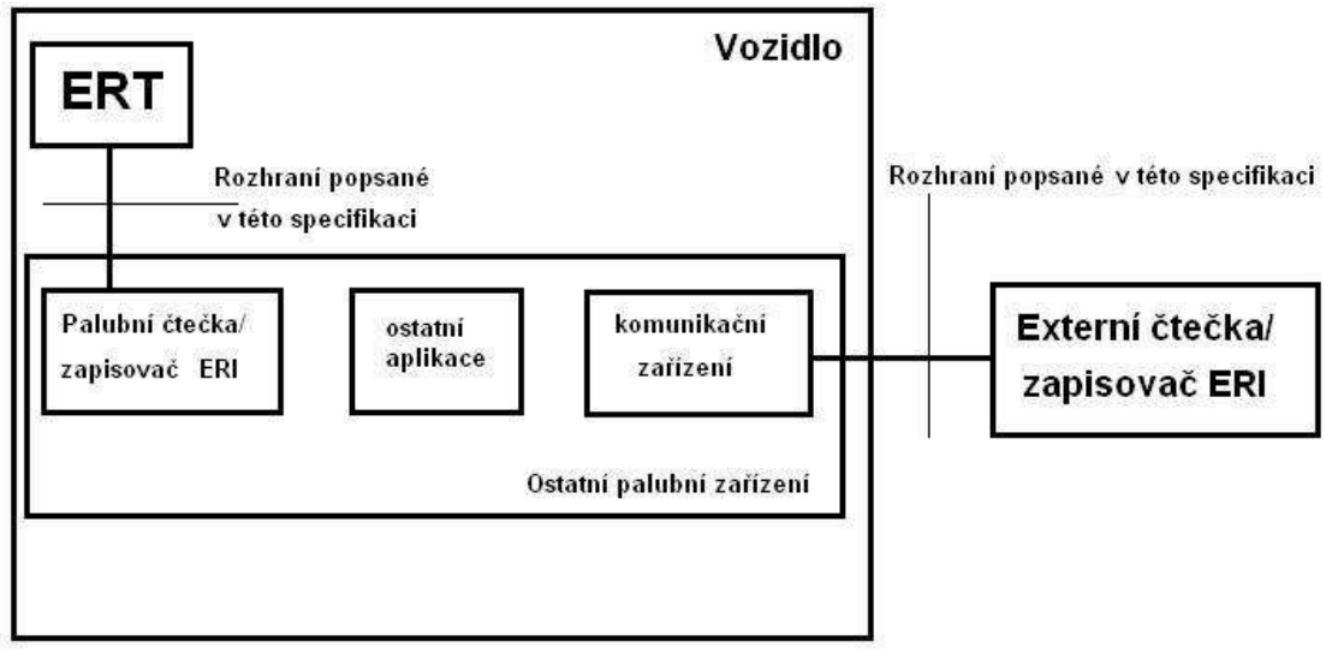
Užití

Specifikace podporuje různé úrovně bezpečnosti s maximální kompatibilitou, velký důraz klade na interoperabilitu mezi zařízením obsahujícím identifikaci vozidla a čtecím zařízením. Podporuje zařízení různého rozsahu od jednoduchého zařízení read-only až po zařízení obsahující historii zápisů na toto zařízení. Elektronická identifikace vozidel může být použita pro identifikaci orgány státní správ y, výrobcem vozidel, při mezinárodním prodeji vozidel, pro bezpečnostní účely, redukci kriminality. Specifikace se zabývá rozhraním mezi za řízením nesoucím informace o vozidle a čtecím zařízením a současně zabezpečením této komunikace.

1. Předmět normy

Koncept komunikace systému

Na obrázku 1 je znázorněno, co přesně specifikuje tato část specifikace.



Obrázek 1 – Koncept elektronické identifikace (obr. 1 popisovaného dokumentu)

2. Souvisící normy

Specifikace podporuje automatickou identifikaci vozidel popsanou v normách ISO 14814 a ISO 14816. Mezi související normy lze zahrnout také normy zabývajícími se informačními technologiemi.

3. Termíny a definice

ERI – samotný děj elektronické identifikace vozidla

ERT – zařízení ve vozidle obsahující identifikační informace

Čtečka ERI – zařízení schopné přečíst informace z ERT

Zapisovač ERI – zařízení schopné zapisovat informace v ERT

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

5 Požadavky rozhraní

Definice prováděných funkcí

Kapitola obsahuje definici funkcí ERI používajících ASN.1. Základními funkcemi jsou zápis dat na ERT a pozdější získání informací z ERT. Ve specifikaci je popsán různý rozsah podle toho, pro koho jsou dané funkce určené (státní správa, vlastník ERT, výrobce). Je zde několik volitelných funkcí (viz níže). Také je možno vytvořit seznam povolených přístupů a editovat ho, vytvořit různé bezpečnostní úrovně (např. pro různé orgány státní správy). Je vhodné nastavit práva přístupu k určitým funkcím podle „profilu“ jednotlivých uživatelů. Specifikace popisuje jednotlivé případy v programovacím jazyce a konkrétně vypisuje jednotlivé případy, co se při jakém případu stane.

Získání dat ERI – Tato funkce je použita při čtení čtečkou dat ERI. Pro státní správu je ve výpisu 1.

```
getEriData TRANSACTION ::= {
   ARGUMENT    GetEriDataArgument
   RESULT      GetEriDataResult
   ERRORS      {notCustomized}
   CODE        1
   }
```

Výpis 1 – Transakce getEriData (čl. 6.2.3 popisovaného dokumentu)

Pro vlastníka ERT je ve výpisu 2.

```
getAuthenticatedEriData TRANSACTION ::= {
   ARGUMENT    GetAuthenticatedEriDataArgument
   RESULT      GetAuthenticatedEriDataResult
   ERRORS      {notCustomized}
   CODE        2
   }
```

Výpis 2 – Transakce getAuthenticatedEriData (čl. 6.2.4 popisovaného dokumentu)

Nastavení dat ERI – Funkce slouží pro zápis prvních dat nebo editování již zapsaných dat. Argument funkce je ve výpisu 3.

```
SetEriDataArgument ::= CHOICE {
   clearTextArgument    ClearTextSetEriDataArgument,
   encryptedArgument    ENCRYPTED {ClearTextSetEriDataArgument}
   }
```

Výpis 3 – Argument transakce setEriData (čl. 6.2.5 popisovaného dokumentu)

Získání informací o předchozím nastavení – tato funkce může poskytnout informace v čistém textu nebo jako zašifrovaný argument. Pro zašifrovaný argument je definována ve výpisu 4.

```
getCiphertextHistoricEriData TRANSACTION ::= {
   ARGUMENT    GetCiphertextHistoricEriDataArgument
   RESULT      SECURED {HistoricEriData}
   ERRORS      {notCustomized}
   CODE        4
   }
```

Výpis 4 – Transakce getCiphertextHistoricEriData (čl. 6.2.6 popisovaného dokumentu)

Pro čistý text je definována ve výpisu 5.

```
getCleartextHistoricEriData TRANSACTION ::= {
   ARGUMENT    GetCleartextHistoricEriDataArgument
   RESULT      CLEAR-SECURED {HistoricEriData}
   ERRORS      {notCustomized}
   CODE        5
   }
```

Výpis 5 – Transakce getCleartextHistoricEriData (čl. 6.2.7 popisovaného dokumentu)

Získání ověřovacího klíče veřejného certifikátu– použití pro ověření kódu nejvyšší úrovně certifikátu (viz výpis 6).

```
getPublicCertificateVerificationKeyId TRANSACTION ::= {
   ARGUMENT    NULL
   RESULT      KeyId
   CODE        6
   }
```

Výpis 6 – Transakce getPublicCertificateVerificationKeyId (čl. 6.2.8 popisovaného dokumentu)

Získání veřejného kódovacího klíče ERT – tento klíč je nutný k dekódování získaných dat (viz výpis 7).

```
getPublicEnciphermentKeyErt TRANSACTION ::= {
   ARGUMENT    BOE-AUTHENTICATED {vehicleId}
   RESULT      PublicEnciphermentKey
   ERRORS      {GetPublicEnciphermentKeyErrors}
   CODE        6
   }
```

Výpis 7 – Transakce getPublicEnciphermentKeyErt (čl. 6.2.9 popisovaného dokumentu)

Pověření ERT – funkce pro státní správu pro vytvoření nebo přetvoření bezpečnostních parametrů (viz výpis 8).

```
commissionErt TRANSACTION ::= {
   ARGUMENT    CommissionErtArgument
   RESULT      NULL
   ERRORS      { CommissionErtErrors }
   CODE        7
   }
```

Výpis 8 – Transakce commissionErt (čl. 6.2.10 popisovaného dokumentu)

Další funkce – konec pověření, získání zašifrovaného argumentu nebo čistý text historie pověřování ERT.

Aktualizace přístupového seznamu

Transakce je ve výpisu 9.

```
updateAccessControlList TRANSACTION ::= {
   ARGUMENT    UpdateAccessControlListArgument
   RESULT      NULL
   ERRORS      {UpdateAccessControlListErrors}
   CODE        11
   }
```

Výpis 9 – Transakce updateAccessControlList (čl. 6.2.14 popisovaného dokumentu)

Další funkce – získání zašifrovaného seznamu nebo v čistém textu.

Získání výpisu schopností ERT

Transakce je ve výpisu 10.

```
getErtCapabilities TRANSACTION ::= {
   ARGUMENT    NULL
   RESULT      ErtCapabilities
   CODE        15
   }
```

Výpis 10 – Transakce getErtCapabilities (čl. 6.2.17 popisovaného dokumentu)

Rozhraní elektronické identifikace

Data ERI a zabezpečená data ERI a ERT samotné mohou být přístupné pouze podle této specifikace. Výměna dat na aplikační vrstvě ERT je v protokolu EriPdu, který je možné dekódovat 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, chová se ERT 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 EN 12834. To umožní ERI DSRC být kompatibilní s ostatními aplikacemi DSRC.

Příloha A (normativní) Moduly ASN.1

Příloha popisuje výměnný modul ASN.1, který lze najít v ISO 24534-3.

Příloha B (informativní) Provozní scénáře

Příloha popisuje jednotlivé scénáře, které mohou při zápisu nebo čtení z ERT nastat. Popisuje jednotlivé bezpečnostní úrovně, kdy mohou nastat, kdo je hlavním účastníkem, jaké je potřeba zařízení pro dodržování pravidel a zabránění nabourání systému.

Příloha C (normativní) Předběžný protokol PICS

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

Souvisící normy

- CEN ISO/TS 24534-1 - Dopravní telematika – Automatická identifikace vozidel, zařízení a nákladů – Identifikace elektronické registrace (ERI) vozidel – Část 1: Architektura
- EN ISO 24534-2 - Dopravní telematika – Automatická identifikace vozidel, zařízení a nákladů – Identifikace elektronické registrace (ERI) vozidel – Část 2: Provozní požadavky
- EN ISO 24534-3 - Dopravní telematika – Automatická identifikace vozidel, zařízení a nákladů – Identifikace elektronické registrace (ERI) vozidel – Část 3: Data o vozidle
- ISO/TS 24534-5 - Automatická identifikace vozidel, zařízení a nákladů – elektronická identifikace vozidel – Část 5: Symetrické šifrování pro zabezpečenou komunikaci
- ISO 24535 - Inteligentní dopravní systémy – Automatická identifikace vozidel, zařízení a nákladů – Základní identifikace elektronické registrace (ERI)

Souvisící termíny

- žadatel
- soukromý klíč
- soukromý dešifrovací klíč
- pověření
- pořadové číslo
- pasivní hrozba
- palubní čtečka ERI
- ověřovatel
- nešifrovaný text
- soukromý podpisový klíč
- transakce ERI
- úřad
- zašifrovaný text
- výzva

- veřejný šifrovací klíč
- veřejný ověřovací klíč
- veřejný klíč
- útok opakováním odposlechnuté zprávy
- náhodné číslo
- maskování
- digitální podpis
- dešifrování
- čtečka ERI
- číslo tagu elektronické registrace
- certifikát veřejného klíče
- certifikační úřad střední úrovně
- certifikační úřad nejvyšší úrovně
- autorizace
- koncové šifrování
- jednostranná autentizace
- identifikace
- hrozba
- hlavní subjekt
- heslo
- hašovací kód
- hašovací funkce
- aktivní hrozba

© Silmos, s.r.o. 2018 - 2026. *Pomůžeme Vám se zorientovat v oboru Dopravní telematiky a najít správnou normu.*