ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 13.3.2019 г.
C(2019) 1789 final

ANNEX 4

ПРИЛОЖЕНИЕ

към

Делегиран регламент на Комисията

за допълване на Директива 2010/40/ЕС на Европейския парламент и на Съвета по отношение на внедряването и експлоатацията на съвместни интелигентни транспортни системи

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

СЪДЪРЖАНИЕ

ПРИЛОЖЕНИЕ IV

1. ПОЛИТИКА ЗА СИГУРНОСТ НА СИТС

1.1. Определения и съкращения

EU CCMS (СУПС на ЕС)	European Union C-ITS security credential management system (система на Европейския съюз за управление на пълномощията за сигурност в СИТС)
CAM	cooperative awareness message (съобщение за съвместно оповестяване)
CP (ППУ)	certificate policy (политика за предоставяне на удостоверения)
DENM	decentralised environmental notification message (съобщение за децентрализирано уведомление за средата)
ISMS	information security management system (система за управление на сигурността на информацията)
IVIM	infrastructure-to-vehicle information message (съобщение за информация между инфраструктура и превозно средство)
SPATEM	signal phase and timing extended message (разширено съобщение за фаза и синхронизация на сигнала)
SREM	signal request extended message (разширено съобщение за заявка за сигнал)
SSEM	signal request status extended message (разширено съобщение за състояние на заявка за сигнал)

1.2. Определения

достъпност	да бъде достъпен и използваем при поискване от упълномощен субект (ISO 27000) [2]
инфраструктура на СИТС	система от съоръжения, оборудване и приложения, необходими за функционирането на организация, която предоставя услуги на СИТС, свързани с фиксирани станции на СИТС.
заинтересовани лица в СИТС	лице, група или организация с функции и отговорности в мрежата на СИТС
поверителна информация	информация, която не трябва да се предоставя или разкрива на неупълномощени лица, субекти или процеси (ISO 27000) [2]
сигурност на информацията	запазване на поверителността, целостта и достъпността на информацията (ISO 27000) [2]

инцидент, свързан със сигурността на информацията	нежелано или неочаквано събитие, свързано със сигурността на информацията, или поредица от събития, които има голяма вероятност да компрометират служебни операции и да застрашат сигурността на информацията
цялост	свойство на прецизност и пълнота (ISO 27000) [2]
местна динамична карта (LDM)	динамично актуализиращо се хранилище на данни за местните условия на движение на станция на СИТС, намираща се в превозно средство; в него се съдържа информация, получавана от бордови датчици и от съобщения CAM и DENM (ETSI TR 102 893) [5]
контрол на протокола	Активите за контрол на протокола избират подходящ протокол за предаване на съобщения при подадена заявка за изходящо съобщение и изпращат съобщението до по-долните слоеве в стека на протокола във формат, който може да бъде обработен от тях. Входящите съобщения се преобразуват във формат, който може да бъде обработен в станцията на СИТС, и се предават на съответния функционален актив за по-нататъшно обработване (ETSI TR 102 893) [5]

1.3. Стратегия за сигурност на информацията

1.3.1. Система за управление на сигурността на информацията (ISMS)

1) Всеки оператор на станция на СИТС работи със система за управление на сигурността на информацията в съответствие с ISO/IEC 27001 при спазване на ограниченията и на допълнителните изисквания, посочени в този раздел.

2) Всеки оператор на станция на СИТС определя външни и вътрешни въпроси, свързани със СИТС, включително:

- COM(2016) 766 final [10];
- GDPR (ОРЗД) [6].

3) Всеки оператор на станция на СИТС определя страните, които имат отношение към системата за управление на сигурността на информацията, и техните изисквания, включително всички заинтересовани страни в СИТС.

4) Обхватът на системата за управление на сигурността на информацията включва всички станции на СИТС в експлоатация и всички други системи за обработване на информация, които преобразуват данните на СИТС в съобщения, отговарящи на следните стандарти:

- CAM [7]
- DENM [8]
- IVIM [9]
- SPATEM [9]
- MAPEM [9]
- SSEM [9]
- SREM [9]

5) Всеки оператор на станция на СИТС гарантира, че неговата политика за сигурност на информацията е в съответствие с настоящата политика.

6) Всеки оператор на станция на СИТС гарантира, че неговите цели в областта на сигурността на информацията обхващат и съответстват на целите за сигурност и на високите изисквания, определени в настоящата политика.

7) Операторите на станции на СИТС класифицират информацията, упомената в раздел 1.4.

8) Операторите на станции на СИТС прилагат процедура за оценка на риска за сигурността на информацията, както е посочено в раздел 1.5, на планирани интервали от време или когато се предлагат или възникват значителни промени.

9) Операторите и/или производителите на станции на СИТС определят изискванията за смекчаване на рисковете за сигурността, набелязани при оценката на риска за сигурността на информацията, в съответствие с раздел 1.6.

10) Производителите на станции на СИТС проектират, разработват и оценяват станциите на СИТС и други системи за обработване на информация, така че да осигурят тяхното съответствие с приложимите изисквания.

11) Операторите на станции на СИТС експлоатират станциите на СИТС и всички други системи за обработване на информация, които прилагат подходящи контролни механизми за управление на рискове за сигурността на информацията, в съответствие с раздел 1.6.

1.4. Класификация на информацията

В този раздел са описани минималните изискванията относно класифицирането на информацията. Това не пречи на заинтересованите страни в СИТС да прилагат по-строги изисквания.

12) Операторите на станции на СИТС класифицират информацията, с която боравят, при което категорията за сигурност може да бъде изразена по следния начин:

Категория за сигурност на информацията = {(поверителност, въздействие), (цялост, въздействие), (достъпност, въздействие)};

13) Заинтересованите страни СИТС класифицират информацията, която управляват, при което категорията за сигурност на системата може да бъде изразена по следния начин:

Категория за сигурност на информационната система = {(поверителност, въздействие), (цялост, въздействие), (достъпност, въздействие)};

14) Допустимите стойности за потенциално въздействие са „ниско“, „умерено“ и „високо“, както е обобщено в таблица **1**.

Таблица 1 Определяне на потенциалното въздействие за всяка цел в областта на сигурността, свързана с поверителност, цялост и достъпност

	Потенциално въздействие		
Цел, свързана със сигурността	**НИСКО**	**УМЕРЕНО**	**ВИСОКО**
Поверителност Поддържане на официално въведени ограничения за достъп до информация и за разкриване на информация, включително средства за защита на личната неприкосновеност и търговската информация	Може да се очаква неразрешеното разкриване на информация да доведе до **ограничени** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква неразрешеното разкриване на информация да доведе до **сериозни** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква неразрешеното разкриване на информация да доведе до **тежки или катастрофални** неблагоприятни последици за операции и активи на организации или за физически лица.
Цялост Защита срещу неправомерно модифициране или унищожаване на информация; това включва гаранции за неопровержимост и достоверност на информацията	Може да се очаква неразрешеното модифициране или унищожаване на информация да доведе до **ограничени** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква неразрешеното модифициране или унищожаване на информация да доведе до **сериозни** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква неразрешеното модифициране или унищожаване на информация да доведе до **тежки или катастрофални** неблагоприятни последици за операции и активи на организации или за физически лица.
Достъпност Осигуряване на навременен и надежден достъп до информация и на навременно и надеждно използване на информация	Може да се очаква прекъсването на достъпа до информация или до информационна система или временното преустановяване на ползването на информация или на информационна система да доведе до **ограничени** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква прекъсването на достъпа до информация или до информационна система или временното преустановяване на ползването на информация или на информационна система да доведе до **сериозни** неблагоприятни последици за операции и активи на организации или за физически лица.	Може да се очаква прекъсването на достъпа до информация или до информационна система или временното преустановяване на ползването на информация или на информационна система да доведе до **тежки или катастрофални** неблагоприятни последици за операции и активи на организации или за физически лица.

15) В зависимост от размера на щетите или на разходите, понесени от услуги на СИТС или от заинтересовани страни в СИТС вследствие на инцидент, свързан със сигурността на информацията, въздействието може да бъде класифицирано в следните категории:

- пътна безопасност — въздействие, което излага участниците в движението на непосредствен риск от нараняване;

- безопасност — въздействие, което излага заинтересована страна в СИТС на непосредствен риск от нараняване;
- оперативни въздействия — въздействие със значителни отрицателни последици за ефикасността на движението по пътищата, или друго обществено значимо въздействие, свързано например с екологичния отпечатък и с организираната престъпност;
- правно въздействие — въздействие, което налага предприемане на значителни действия от една или повече заинтересовани страни в СИТС за спазване на законовите разпоредби и/или на регулаторните изисквания;
- финансово въздействие — въздействие, което води до преки или непреки парични разходи за една или повече заинтересовани страни в СИТС;
- неприкосновеност — правно и финансово въздействие на GDPR (ОРЗД);
- репутация — въздействие, което уврежда репутацията на една или повече заинтересовани страни в СИТС и/или на мрежата на СИТС, напр. неблагоприятни публикации в пресата и/или значителен политически натиск на национално или на международно равнище.

16) Заинтересованите страни в СИТС се придържат към следните минимални стойности на въздействие по отношение на информацията, с която боравят:

Таблица 2: Въздействия

	Информация изпратена от фиксирани станции на СИТС	**Информация изпратена от мобилни станции на СИТС**
Поверителност	CAM: ниско DENM: ниско IVIM: ниско MAPEM: ниско SPATEM: ниско SSEM: ниско	CAM: ниско DENM: ниско SREM: ниско лични данни, съдържащи се в някое от трите съобщения: умерено
Цялост	CAM: умерено DENM: умерено IVIM: умерено MAPEM: умерено SPATEM: умерено SSEM: умерено	CAM: умерено DENM: умерено SREM: умерено
Достъпност	CAM: ниско DENM: ниско IVIM: ниско	CAM: ниско DENM: ниско SREM: умерено

	Информация изпратена от фиксирани станции на СИТС	Информация изпратена от мобилни станции на СИТС
	MAPEM: ниско SPATEM: ниско SSEM: умерено	

1.5. Определяне на риска

1.5.1. Общи положения

17) Оценка на риска се прави периодично в съответствие с ISO/IEC 27005. В нея се взема под внимание подходяща документация за:

- обхвата на оценката на риска, т.е. оценяваната система, нейните цели и предназначение, както и информацията, с която се борави;
- критериите за рискове, свързани със сигурността;
- определяне на риска, включително установяване, анализ и оценка.

1.5.2. Критерии за рискове, свързани със сигурността

18) Критериите за оценка на риска се определят, като се отчитат следните аспекти:

- стратегическата стойност на услугата и на мрежата на СИТС за всички заинтересовани страни в СИТС;
- стратегическата стойност на услугата и на мрежата на СИТС за оператора на станцията на СИТС, предоставяща услугата;
- последиците за репутацията на мрежата на СИТС;
- законови и регулаторни изисквания и договорни задължения.

19) Критериите за въздействие на риска се определят въз основа на класификацията на видовете въздействие върху информацията, посочена в раздел 1.4.

20) Критериите за приемливост на риска включват определяне на нивата на риск, които са неприемливи за услугите на СИТС и за заинтересованите страни в СИТС, по вид въздействие.

1.5.2.1. Установяване на риск

21) Рискът се установява в съответствие с ISO/IEC 27005. Прилагат се следните минимални изисквания:

- основните активи, които трябва да бъдат защитени, са съобщенията на СИТС, посочени в раздел 1.3.1;
- трябва да бъдат набелязани и спомагателни активи, включително:
  - информация, ползвана в съобщенията на СИТС (напр. местна динамична карта, време, контрол на протокола и т.н.);
  - станции на СИТС заедно с техния софтуер, конфигурационни данни и свързаните с тях канали за комуникация;
  - централни активи на СИТС за контрол;

- всички субекти в СУПС на ЕС;

- определят се заплахите за тези активи и техните източници;

- определят се съществуващите и планираните механизми за контрол;

- установяват се уязвимости, от които източниците на заплаха могат да се възползват, за да нанесат вреда на активи или на заинтересовани страни в СИТС; уязвимостите се описват в сценарии в случай на инцидент;

- възможните последици за активите от инциденти, свързани със сигурността, се определят въз основа на класификацията на информацията.

1.5.2.2. Анализ на риска

22) По отношение на анализа на риска се прилагат следните минимални изисквания:

- въздействието на установените инциденти, свързани със сигурността на информацията, върху услуги и заинтересовани страни в СИТС се оценяват въз основа на категориите за сигурност на информацията и на информационните системи, като се прилагат най-малко трите нива, посочени в раздел 1.4;

- определя се нивото на въздействие върху:

  - цялата съществуваща мрежа и всички съществуващи услуги на СИТС; и

  - отделна заинтересована страна/организационен субект в СИТС;

- за общото въздействие се прилага най-високото ниво;

- вероятността на определените сценарии в случай на инцидент се оценява, като се прилагат най-малко следните три нива:

  - малко вероятен (стойност 1) — сценарият за инцидента е малко вероятно/трудно да се осъществи или мотивацията на нападателя би била много ниска;

  - възможен (стойност 2) — сценарият за инцидента е възможно/постижимо да се осъществи или мотивацията на нападателя би била оправдана;

  - вероятен (стойност 3) — сценарият за инцидента е вероятно/лесно да се осъществи и мотивацията на нападателя би била висока;

- нива на риск се определят за всички сценарии в случай на инцидент въз основа на сбора от въздействието и вероятността, като се прилагат най-малко следните три нива: ниско (стойности 1, 2), умерено (стойности 3, 4) и високо (стойности 6, 9), определени, както следва:

Таблица 3: Ниво на риск

Ниво на риск, определено въз основа на сбора от въздействието и вероятността		**Вероятност**		
		малко вероятен (1)	**възможен (2)**	**вероятен (3)**
Въздействие	**ниско (1)**	ниско (1)	ниско (2)	умерено (3)
	умерено (2)	ниско (2)	умерено (4)	високо (6)
	високо (3)	умерено (3)	високо (6)	високо (9)

1.5.2.3. Оценка на риска

23) Нивата на риск се сравняват с критериите за оценка на риска и с критериите за приемливост на риска, за да се определи кои рискове подлежат на третиране. Третират се най-малко рисковете със средно или високо ниво, отнасящи се до услугите и мрежата на СИТС, както е посочено в раздел 1.6.

1.6. Третиране на риска

1.6.1. Общи положения

24) Рисковете се третират по един от следните начини:

- модифициране на риска чрез използване на механизмите за контрол, упоменати в раздел 1.6.2 или в раздел 1.6.3, така че при повторна оценка остатъчният риск да е приемлив;
- приемане на риска (в случай че нивото на риск отговаря на критериите за приемливост на риска);
- избягване на риска.

25) Не се допуска споделянето или прехвърлянето на рискове, които засягат мрежата на СИТС.

26) Третирането на риска се документира, включително посредством:

- декларация за приложимост в съответствие с ISO 27001, в която се описват необходимите механизми за контрол и се определят:
  - остатъчната вероятност от възникване на риска;
  - остатъчната тежест на въздействието;
  - остатъчното ниво на риск;
- основанията за приемане или избягване на риска.

1.6.2. Механизми за контрол за станции на СИТС

1.6.2.1. Общи механизми за контрол

27) Станциите на СИТС прилагат подходящи ответни мерки за модифициране на риска в съответствие с раздел 1.6.1. Тези ответни мерки включват общи механизми за контрол съгласно ISO/IEC 27001 и ISO/IEC 27002.

1.6.2.2. Механизми за контрол на комуникацията между станции на СИТС

28) Внедряват се поне следните минимални задължителни механизми за контрол от страна на изпращача:

Таблица 4: Механизми за контрол от страна на изпращача

	Информация изпратена от фиксирани станции на СИТС	**Информация изпратена от мобилни станции на СИТС**
Поверителност	—	Личните данни, които се съдържат в съобщенията, се защитават чрез подходяща процедура за смяна на талона за разрешение — AT (TP), за да се гарантира ниво на сигурност, съответстващо на риска от повторно установяване на самоличността на водачите въз основа на излъчваните от тях данни. За тази цел станциите на СИТС променят AT (TP) по подходящ начин при изпращане на съобщения и не използват повторно AT (TP) след промяна, освен при поведение, отклоняващо се от това на средностатистическия водач[1].
Цялост	Всички съобщения се подписват в съответствие с TS 103 097 [14].	Всички съобщения се подписват в съответствие с TS 103 097 [14].
Достъпност	—	—

29) Внедряват се поне следните минимални задължителни механизми за контрол от страна на получателя:

Таблица 5: Механизми за контрол от страна на получателя

	Информация изпратена от фиксирани станции на СИТС	**Информация изпратена от мобилни станции на СИТС**
Поверителност		Получените лични данни следва да се съхраняват за възможно най-кратък период от време за служебни цели, с **максимален срок на съхранение пет минути** за сурови и разпознаваеми елементи от данни. Получени CAM или SRM не се препращат/излъчват. Получени DENM могат да бъдат препращани/излъчвани само в ограничена географска област.
Цялост	Целостта на всички съобщения, ползвани от приложенията на ИТС, се валидира в съответствие с TS 103 097 [14].	Целостта на всички съобщения, ползвани от приложенията на ИТС, се валидира в съответствие с TS 103 097 [14].

[1] Поведението на средностатистическия водач се определя въз основа на подходящ статистически анализ на поведението при шофиране в Европейския съюз, напр. по данни на германския авиокосмически център (DLR).

Достъпност	—	Получено SRM се обработва и на неговия подател се изпраща SSM.

30) В подкрепа на изискванията за сигурност, свързани с поверителността, целостта и достъпността, посочени в таблиците по-горе, всички станции на СИТС (мобилни станции (включително станции в превозни средства) и фиксирани станции) се оценяват и сертифицират въз основа на критериите за оценка на сигурността, посочени в „общите критерии“/ISO 15408[2]. Поради различните характеристики на различните видове станции на СИТС и различните изисквания за поверителност на местоположението, могат да бъдат определени различни защитни профили.

31) Всички защитни профили и свързаните с тях документи, приложими за удостоверяването на сигурността на станциите на СИТС, се оценяват, заверяват и сертифицират в съответствие с ISO 15408, като се прилага *Споразумението за взаимно признаване на удостоверенията за оценка на сигурността на информационните технологии* на групата на висшите служители по информационната сигурност (SOG-IS)[3] или равностойна европейска схема за удостоверяване на киберсигурността съгласно съответната европейска рамка в областта на киберсигурността. При разработването на такива защитни профили, обхватът на удостоверяването на сигурността на станция на СИТС може да бъде определен от производителя след оценка и одобрение от СРА (ОПУ) и от орган за оценяване на съответствието на SOG-IS, или най-малкото от равностоен орган, както е описано в следващия параграф.

32) Предвид важността на поддържането на възможно най-високо ниво на сигурност удостоверенията за сигурност на станции на СИТС се издават съгласно схемата за удостоверяване (ISO 15408), основана на общи критерии, от орган за оценяване на съответствието, признат от управителния комитет в рамките на споразумението на SOG-IS, или се издават от орган за оценяване на съответствието, акредитиран национален удостоверяващ орган в областта на киберсигурността на държава членка. Този орган за оценяване на съответствието осигурява условия за оценяване на сигурността, които са поне равностойни на предвидените в споразумението за взаимно признаване (СВП) на Групата на висшите служители по сигурността на информационните системи (SOG-IS).

1.6.2.3. Механизми за контрол за станции на СИТС, действащи като краен субект

33) Станциите на СИТС прилагат политиката за предоставяне на удостоверения [1] в зависимост от функциите си като крайни субекти в СУПС на ЕС.

[2] Портал ‘Common criteria’ („Общи критерии“) http://www.commoncriteriaportal.org/cc/

[3] В сектора на автомобилния транспорт SOG-IS вече е участвала в удостоверяването на сигурността на интелигентния тахограф например. Понастоящем споразумението на SOG-IS е единственият механизъм в Европа, който може да подкрепи хармонизирането на удостоверяването на сигурността на електронни продукти. На този етап SOG-IS поддържа само процеса, свързан с „общите критерии“, така че станциите на СИТС трябва да бъдат оценявани и удостоверявани в съответствие с „общите критерии“; вж. https://www.sogis.org/

1.6.3. Механизми за контрол за участници в СУПС на ЕС

34) Участниците в СУПС на ЕС прилагат политиката за предоставяне на удостоверения [1] в зависимост от функциите си в СУПС на ЕС.

1.7. Съответствие с настоящата политика за сигурност

35) Операторите на станции на СИТС изискват периодично да бъде установено тяхното съответствие с настоящата политика, като се спазват насоките за одит съгласно ISO 27001, дадени в [12].

36) Одитиращият орган следва да бъде акредитиран и сертифициран от член на „Европейска акредитация“ (European Accreditation). Той трябва да отговаря на изискванията на [11].

37) За да бъдат удостоверени, операторите на станции на СИТС създават и поддържат документация съгласно изискванията за документиране на информацията, определени в клауза 7.5 на [3]. По-конкретно операторите на станции на СИТС създават и поддържат следните документи, свързани с ISMS:

- обхват на ISMS (раздел 1.3.1 и [3], клауза 4.3);
- политика и цели по отношение на сигурността на информацията (раздел 1.3.1, и [3], клаузи 5.2 и 6.2);
- подробности относно методологията за оценка и третиране на риска (раздел 1.5 и [3], клауза 6.1.2);
- доклад за оценка на риска (раздел 1.5 и [3], клауза 8.2);
- декларация за приложимост (раздел 1.6 и [3], клауза 6.1.3d);
- план за третиране на риска (раздел 1.6 и [3], клаузи 6.1.3e и 8.3);
- документи, необходими за прилагането на определени механизми за контрол (раздел 1.6 и [3], Приложение A).

38) В допълнение операторите на станции на СИТС създават и поддържат следните архиви с доказателства за постигнатите резултати:

- документи за обучение, умения, опит и квалификация ([3], клауза 7.2);
- резултати от наблюдения и измервания ([3], клауза 9.1);
- програма за вътрешен одит ([3], клауза 9.2);
- резултати от вътрешни одити ([3], клауза 9.2);
- резултати от прегледа от страна на ръководството ([3], клауза 9.3);
- резултати от коригиращи действия ([3], клауза 10.1).

2. ПРЕПРАТКИ

В настоящото приложение се правят препратки към следните документи:

[1] Приложение III към настоящия регламент

[2] ISO/IEC 27000 (2016): Информационни технологии. Методи за

сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник

[3] ISO/IEC 27001 (2015): Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания

[4] ISO/IEC 27005 (2011): Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията.

[5] ETSI TR 102 893 V1.2.1, Интелигентни транспортни системи (ИТС). Сигурност. Анализ на заплахите, уязвимостта и риска (TVRA)

[6] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

[7] ETSI TR 302 637-2 V1.4.0, Интелигентни транспортни системи (ИТС). Връзки с автомобили. Основен комплект приложения. Част 2: Спецификация на основна услуга за съвместно оповестяване

[8] ETSI TR 302 637-3 V1.3.0, Интелигентни транспортни системи (ИТС). Връзки с автомобили. Основен комплект приложения. Част 3: Спецификации на основна услуга за децентрализирано уведомяване за пътна обстановка

[9] ETSI TS 103 301 V1.2.1. Интелигентни транспортни системи (ИТС). Връзки с автомобили. Основен комплект приложения. Протоколи за обслужващ слой и комуникационни изисквания за инфраструктурни услуги

[10] Европейската стратегия за съвместни интелигентни транспортни системи — крайъгълен камък по пътя към съвместната, свързана и автоматизирана мобилност (COM(2016) 766, 30 ноември 2016 г.)

[11] ISO/IEC 27006:2015 Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията

[12] ISO/IEC 27007:2011 Информационни технологии. Методи за сигурност. Насоки за одита на системи за управление на сигурността на информацията

[13] ETSI EN 302 665 V1.1.1 Интелигентни транспортни системи (ИТС). Архитектура на връзките

[14] ETSI TS 103 097 V1.3.1. Интелигентни транспортни системи (ИТС). Сигурност, формати на заглавен ред и удостоверения за сигурност