

התקן תדלוק אוטומטי כללי: דרישות תפקוד

General automatic vehicle refueling device: Functional requirements

לעיון ולמתן הערות

אסמך זה הוא הצעה בלבד

מכון התקנים הישראלי
The Standards Institution of Israel



תקן זה הוכן על ידי ועדת המומחים 87002 - הַתְקָן תדלוק אוטומטי כללי - דרישות תפקוד, בהרכב זה: ארי אנושי, בני הסר, בוריס קוגן (יו"ר), חיים רחמיאל, אבנר שדמי.

שמואל טיש, גיא ליפשיץ וזיוה שלו ריכזו את עבודת הכנת התקן.

טיוטה

מילות מפתח:

כלי רכב, תחנות תדלוק, אמצעי תדלוק, התקנים מופעלי חשמל, אוטומטי.

Descriptors:

road vehicles, filling stations, filling devices, electrically-operated devices, automatic.

עדכניות התקן

התקנים הישראליים עומדים לבדיקה מזמן לזמן, ולפחות אחת לחמש שנים, כדי להתאימם להתפתחות המדע והטכנולוגיה. המשתמשים בתקנים יוודאו שבידיהם המהדורה המעודכנת של התקן על גיליונות התיקון שלו. מסמך המתפרסם ברשומות כגיליון תיקון, יכול להיות גיליון תיקון נפרד או תיקון המשולב בתקן.

תוקף התקן

תקן ישראלי על עדכוניו נכנס לתוקף החל ממועד פרסומו ברשומות. יש לבדוק אם התקן רשמי או אם חלקים ממנו רשמיים. תקן רשמי או גיליון תיקון רשמי (במלואם או בחלקם) נכנסים לתוקף 60 יום מפרסום ההודעה ברשומות, אלא אם בהודעה נקבע מועד מאוחר יותר לכניסה לתוקף.

סימון בתו תקן

כל המייצר מוצר, המתאים לדרישות התקנים הישראליים החלים עליו, רשאי, לפי היתר ממכון התקנים הישראלי, לסמנו בתו תקן:



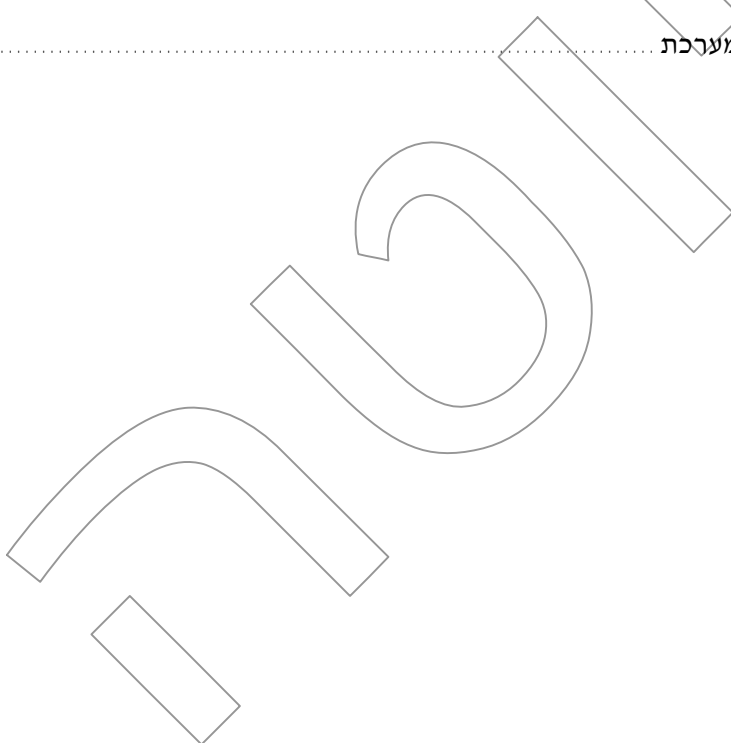
זכויות יוצרים

© אין לצלם, להעתיק או לפרסם, בכל אמצעי שהוא, תקן זה או קטעים ממנו, ללא רשות מראש ובכתב ממכון התקנים הישראלי.

תוכן העניינים

1	הקדמה
1	מבוא
2	פרק א – עניינים כלליים
2	1.1 חלות התקן
2	1.2 אזכורים נורמטיביים
3	1.3 מונחים והגדרות
4	1.4 כללי
5	פרק ב – יחידות כלליות המותקנות בכלי רכב
5	2.1 הִתְקַן זיהוי
7	2.2 משדר רכב
7	פרק ג – יחידות כלליות המותקנות בתחנת תדלוק
7	3.1 קורא
8	פרק ד – תקשורת
8	4.1 תקשורת בין הִתְקַן זיהוי לקורא
8	4.2 תקשורת בין משדר רכב לבקר תחנה
9	פרק ה – אבטחה
9	5.1 כללי
9	5.2 אבטחה פיזית
9	5.3 אבטחת מידע
10	5.4 מרחקי תקשורת בין הִתְקַן זיהוי וקורא
10	פרק ו – בדיקות
10	6.1 מידע והצהרות היצרן
11	6.2 ציוד בדיקה
13	6.3 בדיקות במעבדה
16	נספח א – מבנה הנתונים של הִתְקַן זיהוי על גבי תג HITAG S 2048
16	א-1 כללי
16	א-2 מיפוי הזיכרון
16	א-3 מבנה האוגרים (רגיסטרים)
17	א-4 מפתח הזדהות (Challenge-Response)

19	נספח ב – מבנה הנתונים של הֶתְקָן זיהוי על גבי תג ATmel ATA5580
19	ב-1. כללי
19	ב-2. מיפוי הזיכרון
21	ב-3. מבנה האוגרים (רגיסטרים)
22	ב-4. מפתח הזדהות (Challenge-Response)
22	ב-5. הגנת הנתונים
23	נספח ג – ממשק התקשורת בין משדר רכב לבקר תחנה בתחנת התדלוק
23	ג-1. מאפייני תקשורת אלחוטית
23	ג-2. מצבי עבודה של משדר הרכב
23	ג-3. הודעות ממשק אלחוטי
27	נספח ד – דרישות מומלצות למערכת
27	ד-1. כללי
27	ד-2. מבנה ותפקוד הקורא
27	ד-3. דיווח אירועים במערכת



הקדמה

תקן זה הוא חלק מסדרת תקנים הדנים בהתקן תדלוק אוטומטי כללי.

חלקי הסדרה הם אלה:

- ת"י 6200 חלק 1 - התקן תדלוק אוטומטי כללי: דרישות תפקוד
 - ת"י 6200 חלק 2 - התקן תדלוק אוטומטי כללי: דרישות כלליות, דרישות לעמידות בתנאי סביבה ודרישות חשמל
 - ת"י 6200 חלק 3 - התקן תדלוק אוטומטי כללי: דרישות התקנה
- בתקן ישראלי זה יש לעיין יחד עם התקן הישראלי ת"י 6200 חלק 2.

מבוא

סדרת התקנים הישראליים ת"י 6200 דנה ביחידות הכלליות של התקן תדלוק אוטומטי כללי (להלן "מערכת"), שמטרתן להבטיח את האפשרות לרכוש דלק באמצעות התקן תדלוק מכל חברת דלק, בין שהתקן התדלוק שייך לחברת דלק כלשהי או הותקן על ידיה ובין שהוא שייך לחברת דלק אחרת או הותקן על ידיה.

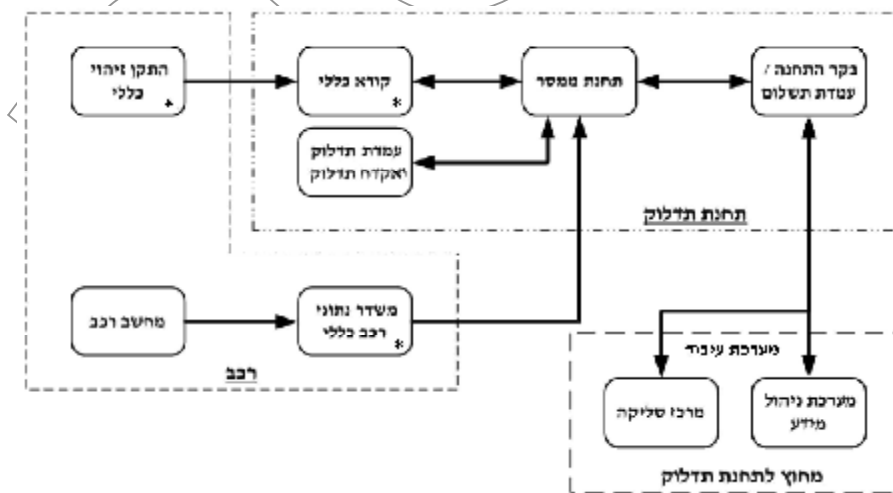
יחידת "התקן זיהוי כללי"⁽¹⁾ המותקנת בכלי רכב ומכילה מידע מזהה ייחודי של כלי הרכב, הנקרא באמצעות צימוד מגנטי על ידי יחידת "קורא כללי"⁽¹⁾ המעבירה את הנתונים לבדיקה, עיבוד ואישור ביצוע התדלוק.

יחידת "משדר נתוני רכב כללי"⁽¹⁾ (המותקנת בכלי הרכב לפי דרישה) מעבירה בשידור אלחוטי את נתוני הנסועה (קילומטרו') של כלי הרכב אל תחנת הדלק וממנה אל מערכת ניהול המידע.

מטרת חלק זה של סדרת התקנים היא להגדיר דרישות תפקוד שעל היחידות הכלליות של המערכת לעמוד בהן, ובכלל זה דרישות חומרה, תוכנה ותקשורת, וכן להגדיר תהליכי הצפנה ופענוח ולפרט את הבדיקות לשל התאמת המערכת לדרישות אלה.

תרשים לוגי של המערכת מתואר בציור 1.

סדרת התקנים דנה ביחידות הכלליות המצוינות בסימן * ובקשרי התקשורת המצוינים ב-a ו-b בציור 1 שלהלן.



ציור 1 – תרשים לוגי של התקן תדלוק אוטומטי כללי

(1) ראו את הסימן (*) בציור 1.

פרק א – עניינים כלליים

1.1. חלות התקן

תקן זה חל על היחידות הכלליות: "התקן זיהוי כללי", "קורא כללי" ו"משדר נתוני רכב כללי" (יחידה אופציונלית המותקנת לפי דרישה) של התקן תדלוק אוטומטי כללי (להלן "מערכת"), המיועדות להתקנה בכלי רכב מהסוגים M, N ו-T1 (כמוגדר בסעיף 1.3.10) ובתחנות תדלוק. תקן זה מפרט דרישות תפקוד ובדיקות ליחידות הכלליות שלעיל. כמו כן דן תקן זה במבנה הנתונים של התקן זיהוי על גבי תג גלי רדיו (RFID) ובמשק תקשורת של משדר הרכב של המערכת (ראו נספחים א-ג).

1.2. אזכורים נורמטיביים

תקנים ומסמכים המוזכרים בתקן זה (תקנים ומסמכים לא מתוארכים – מהדורתם האחרונה היא הקובעת).

תקנים ישראליים

- ת"י 6200 חלק 2 - התקן תדלוק אוטומטי כללי: דרישות כלליות, דרישות לעמידות בתנאי סביבה ודרישות חשמל
- ת"י 6200 חלק 3 - התקן תדלוק אוטומטי כללי: דרישות התקנה
- ת"י 60079 חלק 0 - אטמוספרות נפיצות: ציוד – דרישות כלליות
- ת"י 60079 חלק 11 - אטמוספרות נפיצות: הגנה על ציוד באמצעות בטיחות עצמותית "i"
- ת"י 60079 חלק 32 - אטמוספרות נפיצות: סיכוני חשמל סטטי

חוקים, תקנות ומסמכים ישראליים

תקנות התעבורה, התשכ"א-1961, על עדכוניהן

תקנים בין-לאומיים

- IEC 61000-4-2 - Testing and measurement techniques - electrostatic discharge immunity test
- ISO/IEC 7816-4 - Identification cards - Integrated circuit cards: Organization, security and commands for interchange
- ISO/IEC 15963 - Automatic identification - radio frequency identification for item management - unique identification for RF tags.
- ISO/IEC 18000-2:2004 - Information technology - radio frequency identification for item management Part 2: Parameters for air interface communications below 135 kHz

תקנים אירופיים

- ETSI EN 300 330-1 - Electromagnetic compatibility and radio spectrum matters (ERM). Short range devices (SRD). Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz. Part 1: Technical characteristics and test methods

תקנים לאומיים

- IEEE 802.15.4 - IEEE standard for local and metropolitan area networks Part 15.4: Low-rate wireless personal area networks (LR-WPANs)
- SAE J1939-71 - Vehicle Application Layer

1.3. מונחים והגדרות

מונחים והגדרות אלה כוחם יפה בתקן זה.

1.3.1. דלק

דלק נוזלי המיועד להנעת כלי רכב מנועי.

1.3.2. חברת דלק

מי שעוסק במכירה או באספקה של דלק לתחנות תדלוק, במישרין או באמצעות תאגיד קשור.

1.3.3. תחנת תדלוק

מבנה המיועד למכירת דלק באמצעות משאבות תדלוק הכוללות אקדח תדלוק.

1.3.4. הִתְקַן תדלוק אוטומטי

הִתְקַן המאפשר תדלוק כלי רכב תוך כדי זיהויו ורישומו במאגר מידע אלקטרוני לצורך חיוב כספי ממוחשב.

1.3.5. הִתְקַן תדלוק אוטומטי כללי (להלן "מערכת")

הִתְקַן תדלוק אוטומטי המאפשר לרכוש דלק מכל חברת דלק, בין שהִתְקַן התדלוק שייך לחברת דלק כלשהי או הותקן על ידיה ובין שהוא שייך לחברת דלק אחרת או הותקן על ידיה.

1.3.6. הִתְקַן זיהוי כללי (להלן "הִתְקַן זיהוי")

יחידה במערכת המותקנת בכלי רכב וכוללת מידע ייחודי של הצרכן ושל כלי הרכב.

1.3.7. קורא כללי (להלן "קורא")

יחידה במערכת המותקנת על אקדח התדלוק בתחנת תדלוק, הקוראת את המידע הייחודי שבהִתְקַן הזיהוי ומעבירה אותו למערכת ניהול המידע לבדיקה ולקבלת אישור לביצוע תדלוק.

1.3.8. משדר נתוני רכב כללי (להלן "משדר רכב")

יחידה המותקנת בכלי רכב (לפי דרישה) ומעבירה את נתוני הנסוּעָה ממחשב כלי הרכב למערכת ניהול המידע.

1.3.9. יחידה כללית (אוניברסלית) (להלן "יחידה")

הִתְקַן זיהוי או קורא או משדר רכב המהווים חלק מהמערכת.

1.3.10. כלי רכב מהסוגים M, N ו-T1 (להלן: "כלי רכב")

כל סוגי כלי רכב למעט, טרקטור משא, כמוגדר בתקנות התעבורה, התשכ"א-1961, בתיקון בנושא רישום סוג הרכב, תק' התשס"ה-2005 (מס' 4), תק' התשס"ח-2008 (מס' 12).

1.3.11. מידע

זיהוי הצרכן, זיהוי כלי הרכב, סוג הדלק שנרכש, כמות הדלק הנרכש, מקום הרכישה ומועד הרכישה.

1.3.12. מידע ייחודי

מידע הנשמר בהִתְקַן הזיהוי המשמש לזיהוי חד-ערכי של כלי הרכב וכולל מזהה של יצרן הִתְקַן הזיהוי, מזהה תג ייחודי (UTI) מוצפן ומידע תפעולי לשימוש יצרן הִתְקַן הזיהוי.

1.3.13. מפתח הצפנה אוניברסלי

מפתח הצפנה באורך של 128 סיביות (16 בתים) המשמש להצפנת מזהה תג ייחודי (UTI). ערך המפתח נקבע על ידי הרגולטור⁽²⁾.

(2) הרגולטור – מנהל הדלק והגז במשרד האנרגיה והמים.

- 1.3.14. **מפתח הצפנה משני**
מפתח הצפנה אוניברסלי המשמש כחלופה.
- 1.3.15. **מערכת עיבוד (Back Office)**
מערכת ניהול מידע וניתוח מידע המשמשת לניהול התקני תדלוק אוטומטי וסליקה כספית.
- 1.3.16. **פרוטוקול**
מבנה נתונים ודרך התקשרות אלקטרונית, המשמשים להעברת מידע בין הֶתֶקֶן זיהוי לקורא ובין משדר רכב לתחנת ממסר או/וגם לבקר תחנה של המערכת.
- 1.3.17. **צרכן**
מי שבכלי הרכב שלו מותקן הֶתֶקֶן זיהוי.
- 1.3.18. **אירוע**
תרחיש המתקיים בזמן תדלוק וגורם לדיווח עליו ולרישום במערכת.
- 1.3.19. **בקר תחנה**
יחידה המותקנת בתחנת התדלוק, האחראית לניהול תהליך התדלוק והנמצאת בקשר עם הקורא ומשדר הרכב, ישירות או דרך תחנת ממסר, ועם מערכות מחוץ לתחנת התדלוק כגון מערכת ניהול צי רכב, מרכז סליקה.
- 1.3.20. **תחנת ממסר**
יחידה המותקנת בתחנת התדלוק (לפי דרישה) שמטרתה לאפשר את הקשר בין הקורא ומשדר הרכב לבקר התחנה ולשפרו.
- 1.3.21. **טווח פעולה**
טווח ממרחק אפס (צמוד) ועד למרחק המרבי שבו מתאפשרת תקשורת והעברת מידע מהֶתֶקֶן הזיהוי בכלי הרכב לקורא באופן רציף ללא הפסקה, הפרעה או שיבוש.
- 1.3.22. **טווח אי-פעולה**
טווח הגדול מטווח הפעולה שלעיל שבו לא תתקיים תקשורת ולא תהיה העברת מידע מהֶתֶקֶן הזיהוי בכלי הרכב לקורא.
- 1.3.23. **זמן העברת מידע מהֶתֶקֶן הזיהוי לקורא**
משך הזמן הנדרש להעברת המידע מהֶתֶקֶן הזיהוי לקורא כאשר נחיר אקדח התדלוק נמצא במלואו בתוך פיית התדלוק בכלי הרכב.
- 1.4. **כללי**
- 1.4.1. **תקשורת בין יחידות כלליות במערכת**
- 1.4.1.1. התקשורת בין הֶתֶקֶן זיהוי וקורא ובין משדר רכב תהיה בצימוד מגנטי.
התקשורת בין משדר הרכב ובקר תחנה בתחנת התדלוק תהיה בשידור אלחוטי כמוגדר בתקן זה.
- 1.4.1.2. התקשורת בין משדר הרכב בקר תחנה תהיה באישור משרד התקשורת.
- 1.4.2. הסבולת של מידות, של נתונים ושל זמנים תהיה $\pm 10\%$ אלא אם הוגדר אחרת.

פרק ב – יחידות כלליות המותקנות בכלי רכב

2.1. הֶתְקָן זִיּהוּי

2.1.1. מבנה

- 2.1.1.1. הֶתְקָן הזִיּהוּי יעמוד בדרישות התקן הישראלי ת"י 6200 חלק 2.
- 2.1.1.2. הֶתְקָן הזִיּהוּי יהיה פסיבי ללא חיבור למקור זינה או לסוללה.
- 2.1.1.3. הֶתְקָן הזִיּהוּי יהיה מבוסס על אחד התגים המפורטים להלן, בטכנולוגיית תיוג אלקטרוני באמצעות גלי רדיו (RFID) בתדר המוגדר בפרק ד – תקשורת, סעיף 4.1:
 - 2.1.1.3.1. Phillips Semiconductors HITAG S 2048 (ראו נספח א) ;
 - 2.1.1.3.2. Atmel ATA 5580 (ראו נספח ב).
- 2.1.1.4. הֶתְקָן הזִיּהוּי יכלול מידע ספציפי וייחודי לזיהוי חד-ערכי של כלי הרכב, כמוגדר בטבלה 1 שלהלן.
- 2.1.1.5. מידע ייחודי לתג גלי רדיו (RFID) בהֶתְקָן הזִיּהוּי ואופן יישום המידע הייחודי באמצעות התג מוגדרים בנספחים א ו-ב.

טבלה 1 – מידע ייחודי בהֶתְקָן הזִיּהוּי

שדה נתונים		פירוט
SID	שם	מזהה יצרן הֶתְקָן זִיּהוּי
	פורמט	8 ספרות, 4 הראשונות – עבור זיהוי היצרן (יוקצה על ידי הרגולטור), 4 נוספות – לשימוש היצרן לסימון דגמים, סדרות ייצור וכדומה
	אורך	4 בתים
OP	שם	ערכים תפעוליים (שמור לשימוש היצרן)
	פורמט	ערכים מותרים: כל ערך
	אורך	4 בתים
TDS	שם	מזהה תג ייחודי (UTI) מוצפן
	פורמט	חתימה קריפטוגרפית המשמשת לזיהוי התג (מוגדר בסעיף 2.1.1.6.2.1.1.6 להלן)
	אורך	16 בתים
EDS	שם	מזהה תג ייחודי (UTI) מוצפן באמצעות מפתח משני
	פורמט	חתימה קריפטוגרפית חלופית (מוגדר בסעיף 2.1.1.8 להלן)
	אורך	16 בתים

2.1.1.6. חתימה קריפטוגרפית (TDS)

- 2.1.1.6.1. החתימה הקריפטוגרפית תכיל את מזהה התג הייחודי (UTI) המוצפן ותשמש לזיהוי הֶתְקָן זִיּהוּי במערכת העיבוד.
- 2.1.1.6.2. החתימה הקריפטוגרפית תהיה בנויה משלושה חלקים, תכלול 16 בתים ותהיה מוצפנת בעזרת אלגוריתם הצפנה AES128 עם מפתח הצפנה אוניברסלי, כפי שנקבע על ידי הרגולטור.
- 2.1.1.6.3. בזמן התקשורת בין הֶתְקָן הזִיּהוּי לקורא תפוענח החתימה הקריפטוגרפית ויתבצע אימות מזהה התג הייחודי (UTI).
- 2.1.1.6.4. החתימה תהיה מוצפנת ללא ריפוד (padding), כך שאורך החתימה המוצפנת יהיה 16 בתים.

2.1.1.6.5. סדר חישוב ההצפנה של החתימה יהיה לפי התיאור שלהלן, משמאל לימין.

USN[0]...USN[3], UIDC[0]... UIDC[7], CRC[0]...CRC[3]

2.1.1.7. מבנה מזהה התג הייחודי (UTI) מוגדר בטבלה 2 שלהלן.

טבלה 2 - מבנה מזהה התג הייחודי (UTI)

שדה נתונים		פירוט
USN	שם	מספר סידורי ייחודי של ה־תֶּקֶן זיהוי
	פורמט	8 ספרות (תווד המספרים שיוקצו ליצרן על ידי הרגולטור)
	אורך	4 בתים
UIDC	שם	מזהה תג ייחודי כפי שנצרב בתהליך ייצורו
	פורמט	בהתאם למוגדר בתקן הבין-לאומי ISO/IEC 15963. לפי הצורך, יש להוסיף קידומת של סיביות בעלות ערך 0 להשלמת אורך השדה.
	אורך	8 בתים
CRC	שם	CRC32
	פורמט	סיכום ביקורת CRC32 של שדות USN ו-UID
	אורך	4 בתים

2.1.1.7.1. סדר חישוב ה-CRC יהיה לפי התיאור שלהלן, משמאל לימין.

USN[0]...USN[3], UIDC[0]... UIDC[7]

2.1.1.8. חתימה קריפטוגרפית משנית (EDS)

2.1.1.8.1. החתימה הקריפטוגרפית המשנית תכיל את מזהה התג הייחודי (UTI) המוצפן באמצעות מפתח הצפנה משני ותשמש במצבים שיש בהם חשש כי מפתח ההצפנה האוניברסלי נחשף.

2.1.1.8.2. החתימה הקריפטוגרפית המשנית תהיה בנויה משלושה חלקים, תכלול 16 בתים ותהיה מוצפנת בעזרת אלגוריתם הצפנה AES128 עם מפתח הצפנה משני, כפי שנקבע על ידי הרגולטור.

2.1.1.8.3. כאשר המערכת פועלת באמצעות החתימה הקריפטוגרפית (TDS) החתימה הקריפטוגרפית המשנית (EDS) לא תועבר מה־תֶּקֶן הזיהוי לקורא. אם יש צורך בחתימה הקריפטוגרפית המשנית (EDS) היא תועבר מה־תֶּקֶן הזיהוי לקורא ולמערכת העיבוד.

2.1.1.8.4. המעבר לשימוש בחתימה משנית ייעשה לפי קביעת הרגולטור. המעבר ידרוש התערבות ידנית להפעלת קריאת החתימה בקורא ועדכון המפתח לאימות במערכת העיבוד. מטעמי אבטחת המידע התהליך לא יוכל להתבצע מרחוק.

2.1.1.8.5. עם הפעלת החתימה המשנית יתבצע תהליך קריאה, פיענוח ואימות מזהה התג הייחודי (UTI).

2.1.1.8.6. החתימה תהיה מוצפנת ללא ריפוד (padding), כך שאורך החתימה המוצפנת יהיה 16 בתים.

2.1.1.8.7. סדר חישוב ההצפנה של החתימה יהיה לפי התיאור שלהלן, משמאל לימין.

USN[0]...USN[3], UIDC[0]... UIDC[7], CRC[0]...CRC[3]

2.1.1.9. המידע האגור בה־תֶּקֶן הזיהוי יישמר ללא שינוי או שיבוש בכל תנאי הפעולה ותנאי הסביבה המוגדרים בסדרת התקנים הישראליים ת"י 6200 על חלקיה.

- 2.1.1.10. הֶתֶקֶן זיהוי יהיה לשימוש חד-פעמי. לאחר תכנות ושפעול הֶתֶקֶן לא יהיה ניתן למחוק או לשנות מידע הצרוב בו. לא יהיה ניתן להסירו ממקום התקנתו ולהפעילו בהצלחה במקום אחר.
- 2.1.1.11. מבנה הֶתֶקֶן זיהוי ופעולתו יתאימו לסביבה בעלת אטמוספירה נפיצה (של אדי דלק) ובעלת נגישות פיזית אל הֶתֶקֶן שיוצרת הפרעת חשמל סטטי.
- מבנה התקן זיהוי ופעולתו יבטיחו מניעה של הסיכון להתלקחות אש ושל שיבוש תפקודו התקין ויתאימו למוגדר בתקנים הישראליים ת"י 60079 חלקים 0, 11 ו-32 ובתקן הבין-לאומי IEC 61000-4-2.

2.1.2. תפקוד

- 2.1.2.1. התקשורת בין הֶתֶקֶן הזיהוי לבין הקורא תתקיים כאשר הקורא נמצא בטווח הפעולה המוגדר בסעיף 5.4. לא תתקיים תקשורת בטווח אי-הפעולה.
- 2.1.2.2. בקיום תקשורת כמוגדר בסעיף 2.1.2.1, לאחר אימות מוצלח כמוגדר בסעיף 4.3.3.7, יעבור המידע הייחודי האגור בהֶתֶקֶן הזיהוי לקורא.
- 2.1.2.3. זמן העברת מידע מהֶתֶקֶן הזיהוי לקורא לא יהיה יותר משנייה אחת.

2.2. משדר רכב

2.2.1. מבנה

- 2.2.1.1. מבנה משדר הרכב יתאים לדרישות הכלליות המוגדרות בתקן הישראלי ת"י 6200 חלק 2.
- 2.2.1.2. משדר הרכב יעמוד בדרישות החשמל המוגדרות בתקן הישראלי ת"י 6200 חלק 2 פרק ד סעיף 4.4.

2.2.2. תפקוד

- 2.2.2.1. משדר רכב היא יחידה המותקנת לפי דרישה בלבד והמערכת תפעל גם בלעדיה.
- 2.2.2.2. בקיום תקשורת תשדר היחידה את נתוני הנְסוּעָה לבקר התחנה באופן ישיר או באמצעות תחנת הממסר בתחנת התדלוק.
- 2.2.2.3. נתוני הנְסוּעָה בכלי הרכב שיועברו יהיו בדיוק שיוגדר על ידי יצרן משדר הרכב ויהיו זהים למד הנְסוּעָה בכלי הרכב או יהיו בסטייה של $\pm 5\%$ מקסימום מהמרחק שכלי הרכב נסע בפועל.
- 2.2.2.4. התקשורת בין משדר הרכב לבקר התחנה בתחנת התדלוק תבוצע באמצעות שידור אלחוטי לפי המוגדר בסעיף 4.2.1.

פרק ג – יחידה כללית המותקנת בתחנת תדלוק

3.1. קורא

3.1.1. מבנה

- 3.1.1.1. הקורא יכולל מנגנון לזיהוי של הסרה, פירוק וכדומה מאקדח התדלוק שיגרום לקורא להפסיק לפעול. התקנה והפעלה מחדש (שפעול) של הקורא תבצע אך ורק על ידי מי שהוסמך על ידי היצרן ובהתאם להוראות היצרן.

- 3.1.1.2. מבנה הקורא יתאים לדרישות הכלליות המוגדרות בתקן הישראלי ת"י 6200 חלק 2.

3.1.1.3. מבנה קורא ופעולתו יתאימו לסביבה בעלת אטמוספירה נפיצה של אדי דלק ובעלת נגישות פיזית אל הקורא שיוצרת הפרעת חשמל סטטי, מבנה קורא ופעולתו יבטיחו מניעה של הסיכון להתלקחות אש ושל שיבוש תפקודו התקין של הקורא ויתאימו למוגדר בתקנים הישראליים ת"י 60079 חלקים 0, 11 ו-32 ובתקן הבין-לאומי IEC 61000-4-2.

3.1.1.4. דרישות לסוללה יהיו לפי התקן הישראלי ת"י 6200 חלק 2 פרק ד סעיף 4.3.

3.1.2. תפקוד

3.1.2.1. הקורא יורכב על אקדח התדלוק וייצור קשר עם הֶתֶקֶן הזיהוי לצורך קבלת המידע הייחודי האגור בהֶתֶקֶן הזיהוי.

3.1.2.2. הקורא יידע לזהות ולקורא את התג של הֶתֶקֶן הזיהוי (ראו סעיף 2.1.1.3).

3.1.2.3. לשם התחלת תדלוק הקורא תתקבל "פקודת הפעלה" מבקר התחנה. הקורא יתקשר להֶתֶקֶן הזיהוי פעם אחת לפחות בכל 3 שניות עד לקבלת "פקודת הפסקה" מבקר התחנה. אם התקשורת הופרעה או הופסקה יתקבל חיווי על כך בבקר התחנה.

3.1.2.4. ברגע קליטת המידע הייחודי בקורא תיבדק תקינותו, ואם המידע תקין הוא יועבר אל בקר התחנה.

פרק ד – תקשורת

4.1. תקשורת בין הֶתֶקֶן זיהוי לקורא

4.1.1. התקשורת בין הֶתֶקֶן זיהוי לקורא תהיה באמצעות צימוד מגנטי לפי המוגדר בתקן הבין-לאומי ISO/IEC 18000-2:2004.

4.1.2. התקשורת בין הֶתֶקֶן זיהוי לקורא תהיה בתדר של 125 קילוהרץ.

4.1.3. הֶתֶקֶן הזיהוי והקורא יעמדו בדרישות הרלוונטיות של התקן האירופי ETSI EN 300 330-1.

4.1.4. שינוי בתדר ובעוצמת השידור, מכל סיבה שהיא לרבות התקנה של היחידות, לא יחרוג מהמוגדר בתקן האירופי ETSI EN 300 330-1 עבור תחום התדרים המוגדר בסעיף 4.1.2 שלעיל.

4.1.5. מרחקי התקשורת בין הקורא ובין הֶתֶקֶן זיהוי יהיו כמוגדר בסעיף 5.4 שלהלן.

4.2. תקשורת בין משדר רכב לבקר תחנה

4.2.1. התקשורת בין משדר רכב לבקר תחנה בתחנת התדלוק תהיה באמצעות שידור אלחוטי לפי המוגדר בתקן האמריקני IEEE 802.15.4.

4.2.2. מנשק התקשורת בין משדר רכב לבקר תחנה בתחנת התדלוק יהיה כמוגדר בנספח ג.

4.2.3. משדר רכב יעמוד בדרישות הרלוונטיות של התקן האירופי ETSI EN 300 330-1.

4.2.4. בזמן ההתקשורת יועבר המידע אוטומטית בשידור אלחוטי ממשדר הרכב אל בקר התחנה בתחנת תדלוק, כלומר ללא צורך בפעולה יזומה של הנהג או של עובדי תחנת התדלוק או של כל גורם אחר.

4.2.5. שידור המידע יימשך עד שיתקבל אישור מבקר התחנה במשדר רכב על תקינות המידע שהתקבל. לאחר קבלת האישור יופסק השידור.

- 4.2.6. שידור המידע יופסק אוטומטית אם לא תהיה תקשורת במקרים כגון חסימת התקשורת או שהמשדר נמצא מחוץ לטווח הקליטה.
- 4.2.7. נתוני הנסיעה יועברו במבנה Vehicle Distance High Resolution - VDHR, כמוגדר בתקן האמריקני SAE J1939-71.
- 4.2.8. בתים 1-4 של השדר האלחוטי בתקן האמריקני SAE J1939-71 המכילים את נתון הנסיעה הכולל הם שדות חובה. בתים 5-8 המכילים נתונים אחרים כגון נתוני מד מרחק (Trip) הם שדות רשות.

פרק ה – אבטחה

5.1 כללי

5.1.1. פירוק או הסרה של הֶתְקָן זיהוי ממקום התקנתו יגרום להשבתתו.

5.1.2. פירוק או הסרה של קורא ממקום התקנתו יגרום להפסקת פעולתו.

5.2 אבטחה פיזית

5.2.1. עיגון הֶתְקָן זיהוי לכלי הרכב יהיה חד-פעמי. הסרת התקן זיהוי, פירוקו, ניתוקו או כל פעולה אחרת תגרום לנטרולו המוחלט. לא יהיה אפשר לעשות שימוש חוזר או התקנה נוספת בהתקן זיהוי כזה.

5.2.2. לא תתאפשר צריבת מידע ייחודי חוזרת או נוספת על הֶתְקָן הזיהוי.

5.2.3. לא יהיה אפשר לשנות בקורא את המידע הייחודי שהתקבל מהֶתְקָן הזיהוי.

5.3 אבטחת מידע

הערה: דרישות אבטחת המידע שלהלן נוגעות ליחידות בלבד.

רמת אבטחת המידע של היחידות ודרישות אבטחת מידע לקשרים אחרים במערכת אינן מוגדרות בתקן זה.

5.3.1 תרחישי מתקפה (attack scenario)

המערכת תזהה את תרחישי המתקפה שלהלן ותגיב אליהם:

5.3.1.1. קריאה לא מורשית של הנתונים הצרובים בהֶתְקָן הזיהוי (Skimming) - הנתונים נקראים ישירות מתוך הֶתְקָן ללא ידיעת בעל הֶתְקָן.

5.3.1.2. יירוט תקשורת בין רכיבי המערכת (Eavesdropping) - מבוצע באמצעות השימוש בציוד רדיו במטרה לאסוף מידע תקשורתי גולמי לגילוי צורת התקשורת או/וגם אופן הצפנתה.

5.3.1.3. התחזות להֶתְקָן זיהוי (Spoofing) - מבוצע באמצעות הקלטת שידור נתוני הֶתְקָן זיהוי חוקי (לגיטימי - Legitimate) ושידור הקלטה זו לקורא.

5.3.1.4. שכפול הֶתְקָן זיהוי (Cloning) - העתקת הנתונים הצרובים בהֶתְקָן זיהוי קיים להֶתְקָן זיהוי נוסף.

5.3.1.5. שינוי נתונים (Data tampering) - שינוי או מחיקה של נתוני הֶתְקָן זיהוי.

5.3.2. **מנגנוני הגנה**

מנגנוני ההגנה של המערכת יכללו:

5.3.2.1. הגבלת המרחק המרבי לקליטה ולתקשורת בין ה־תֶּקֶן זיהוי לקורא – למניעת יירוט התקשורת בין ה־תֶּקֶן לקורא, לפי המוגדר בסעיף 5.4 שלהלן.

5.3.2.2. נעילת זיכרון ה־תֶּקֶן זיהוי לאחר ביצוע תכנות ושפעול.

5.3.2.3. הצפנת מזהה תג ייחודי (UTI) (יצירת חתימות קריפטוגרפיות, TDS ו-EDS) – יבוצע באמצעות השימוש בפרוטוקול הצפנה AES128 כמפורט בסעיפים 2.1.1.6-2.1.1.8.

5.3.2.4. אימות ה־תֶּקֶן זיהוי – יבוצע באמצעות אימות החתימה הקריפטוגרפית (TDS) בשלושה שלבים:

א. פיענוח החתימה הקריפטוגרפית (TDS) באמצעות מפתח ההצפנה האוניברסלי, חישוב סיכום ביקורת CRC32 עבור השדות UIDC ו-USN והשוואתו לערך השדה CRC.

ב. אימות המספר הסידורי הייחודי (USN), כפי שנרשם במהלך תכנות ושפעול ה־תֶּקֶן הזיהוי.

ג. אימות מזהה תג ייחודי (UID) – באמצעות השוואת ערך מזהה תג ייחודי, כפי שנצרב בתהליך ייצור התג, לערך השדה UIDC.

5.3.2.5. אם יש חשש לחשיפת מפתח ההצפנה האוניברסלי, באפשרות הרגולטור להחליט על מעבר לביצוע אימות ה־תֶּקֶן הזיהוי באמצעות אימות החתימה הקריפטוגרפית המשנית (EDS) כמפורט בסעיף 2.1.1.8. האימות ייערך באופן זהה לבדיקת החתימה הקריפטוגרפית (TDS), כמפורט בסעיף 5.3.3.4 שלעיל.

5.3.2.6. אישור ה־תֶּקֶן זיהוי יתבצע במערכת העיבוד (Back Office).

5.3.2.7. אימות בין ה־תֶּקֶן זיהוי לקורא – באמצעות מנגנון Challenge-Response המונע התחזות.

5.4. **מרחקי תקשורת בין ה־תֶּקֶן זיהוי וקורא**

5.4.1. טווח פעולה – ממרחק צמוד (אפס) ועד למרחק מרבי של 10 ס"מ.

5.4.2. טווח אי-פעולה – מרחק גדול יותר מ-12 ס"מ.

5.4.3. טווח אי-וודאות בפעולה – הטווח בין המרחק המרבי לפעולה (10 ס"מ) ועד המרחק המזערי לאי-פעולה (12 ס"מ) שבו יכולה להיות פעולה של העברת מידע.

פרק ו – בדיקות

6.1. **מידע והצהרות היצרן**

ליחידות הכלליות הנבדקות יצורפו מידע והצהרות היצרן הכוללים את המפורט להלן:

6.1.1. התייעוד הטכני המוגדר בתקן הישראלי ת"י 6200 חלק 2 סעיף 2.8.

6.1.2. תוצאות בדיקות המעידות שהיחידות עמדו בהצלחה בבדיקות תפקוד ואבטחת מידע.

6.1.3. הצהרת היצרן על שיטות ההגנה על המידע בה־תֶּקֶן הזיהוי (סעיף 2.1.1).

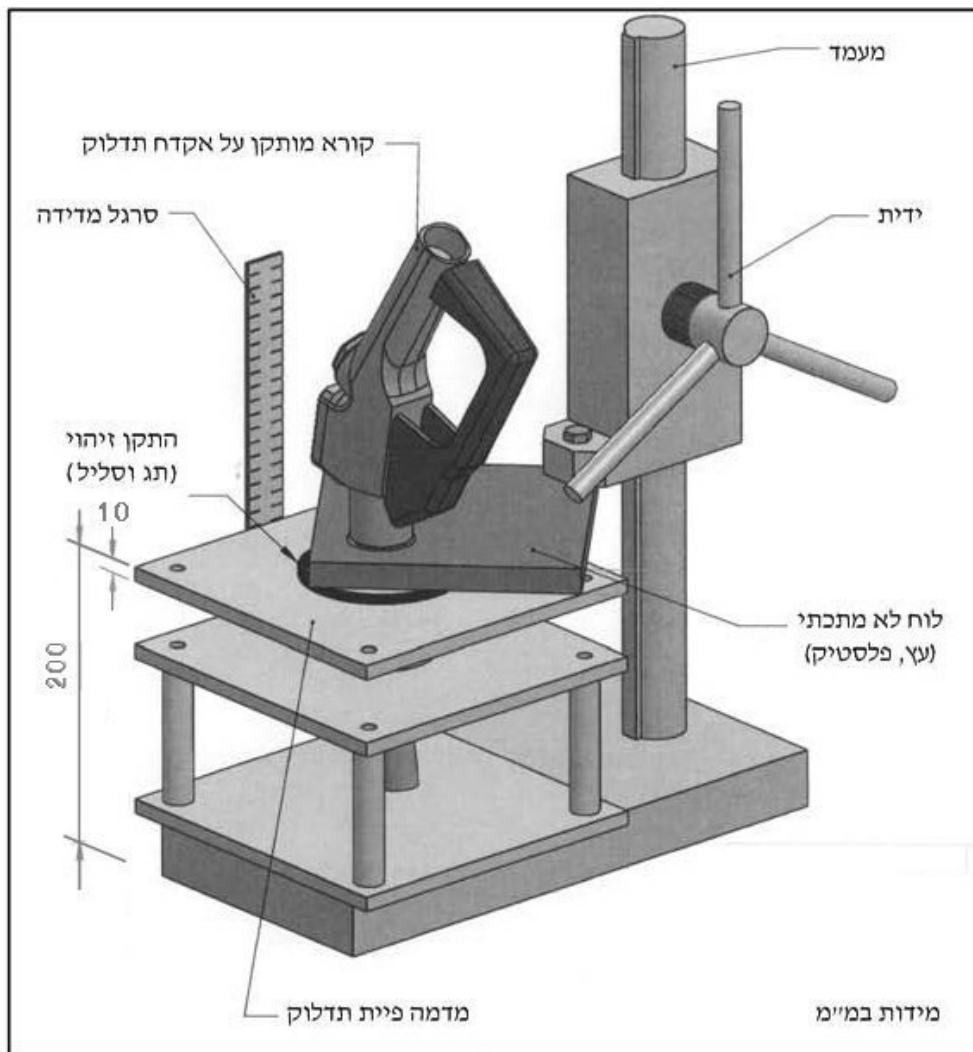
6.1.4. מידע והצהרת היצרן על עמידה בדרישות התקשורת בין ה־תֶּקֶן זיהוי לקורא (סעיף 4.1).

- 6.1.5 מידע על התקשורת בין קורא ומשדר רכב לבין בקר התחנה בתחנת התדלוק (סעיף 4.2).
- 6.1.6 הצהרת היצרן על עמידה בדרישות התקשורת בין משדר רכב לבקר התחנה בתחנת התדלוק (סעיף 4.2).
- 6.1.7 הצהרת יצרן על עמידת המערכת בדרישות אבטחה (פרק ה).
- 6.1.8 מידע על מימוש דרישות אבטחת המידע (סעיף 5.3).

6.2 ציוד בדיקה

ציוד הבדיקה יכלול את המפורט להלן:

- 6.2.1 מעמד לבדיקה של התקן זיהוי וקורא המותקנים בתנאי מעבדה, כמתואר בציור 2. התקן הזיהוי יותקן על המשטח של מדמה פיית התדלוק. מתקינים את הקורא על אקדח התדלוק (להלן: "ערכת תדלוק") במשטח העליון היכול לנוע על הציר האנכי.



ציור 2 – מעמד לבדיקת התקן זיהוי וערכת תדלוק

6.2.2. מכינים ערכות תדלוק מייצגות לפי סעיף 6.3.2 שלהלן עבור כל הדגמים של אקדחי התדלוק הקיימים בשוק.

6.2.3. הִתְקַנִּי זִיהוּי לִיחוס:

ערכה של 10 הִתְקַנִּי זִיהוּי לִיחוס. בחלק מהבדיקות נדרש להשתמש בהתקן זיהוי לייחוס יחיד המכוון לתדר התהודה T6, כמפורט בטבלה 3.

6.2.3.1. בונים ערכה של 10 הִתְקַנִּי זִיהוּי לִיחוס שכל אחד מהם מכוון לתדר תהודה אחר. ערכה זו מייצגת הִתְקַנִּי זִיהוּי המותקנים במגוון כלי הרכב (כלומר השפעות המתכת באזור ההתקנה בכלי הרכב על תדר התהודה).

6.2.3.2. **מבנה הִתְקַנִּי זִיהוּי לִיחוס:**

התקן הזיהוי יהיה מורכב מסליל כמפורט להלן:

- הסליל יורכב מחוט נחושת. עובי החוט יהיה 0.2 מ"מ עם בידוד.
- כמות הכריכות של החוט תהיה 143.
- השראות צפויה: $3.8 \pm 5\%$ מילי-הנרי.
- הקוטר הפנימי של הסליל יהיה 80 מ"מ.
- לסליל יחובר תג הכולל מידע ייחודי כמוגדר בסעיף 2.1 בחיבור מקבילי.
- לסליל יחובר קבל אחד או יותר בחיבור מקבילי, כך שתדר התהודה יהיה ברוחב 0.5 קילוהרץ ובמרווחים של 2.5 קילוהרץ כמפורט בטבלה 3 שלהלן:

טבלה 3 – תדרי ערכת הִתְקַנִּי זִיהוּי לִיחוס

מספר התג	תדר תהודה [הרץ - Hz]
T1	111,000 – 110,500
T2	113,500 – 113,000
T3	116,000 – 115,500
T4	118,500 – 118,000
T5	121,000 – 120,500
T6	123,500 – 123,000
T7	126,000 – 125,500
T8	128,500 – 128,000
T9	131,000 – 130,500
T10	133,500 – 133,000

6.2.4. יחידות נוספות וציוד בדיקה שיסופקו על ידי היצרן עבור בדיקות התפקוד:

6.2.4.1. משדר רכב לבדיקה.

6.2.4.2. יחידה מדמה המתחברת למשדר הרכב הנבדק שאפשר לשנות בה את נתוני הנְסוּעָה.

6.2.4.3. ציוד לתכנות ושפעול היחידות.

6.2.4.4. ציוד בדיקה המתחבר לקורא או מאפשר את הפעלת הקורא וקליטת התקשורת מהקורא לבקר התחנה לפיענוח ולהשוואה של המידע הייחודי שהועבר בתקשורת בין הִתְקַנִּי זִיהוּי לקורא.

6.2.4.5. ציוד בדיקה המדמה בקר תחנה ומאפשר תקשורת עם משדר הרכב לפיענוח ולהשוואה של נתוני הנסועה.

6.3. בדיקות במעבדה

6.3.1. כללי

6.3.1.1. עורכים את כל הבדיקות בטמפרטורה אופפת כמוגדר בתקן ישראלי ת"י 6200 חלק 2 סעיף 3.1, למעט בדיקות תנאי סביבה שבהן הטמפרטורה מוגדרת בכל בדיקה.

6.3.2. בדיקת תפקוד של ערכת התדלוק

6.3.2.1. הבדיקה תתבסס על ערכה של הֶתְקָנִי זיהוי לייחוס כמוגדר בסעיף 6.2.3 שיותקנו על מעמד כמוגדר בסעיף 6.2.1.

6.3.2.2. בודקים שערכת התדלוק קולטת ומעבדת את המידע הייחודי הצרוב בכל התגים של הֶתְקָנִי הזיהוי לייחוס בטווח הפעולה המוגדר בסעיף 5.4. חוזרים על הבדיקה כשהמרחק בין הֶתְקָנִי הזיהוי לקורא גדל במרווחים של 1.0 ס"מ מבדיקה לבדיקה עד לטווח אי-הפעולה.

6.3.2.3. בודקים שערכת התדלוק אינה קולטת את המידע הייחודי הצרוב בכל התגים של הֶתְקָנִי זיהוי לייחוס בטווח אי-הפעולה המוגדר בסעיף 5.4.

6.3.2.4. בודקים שזמן העברת המידע הייחודי מהֶתְקָנִי הזיהוי לייחוס לקורא עומד בדרישה שבסעיף 2.1.2.3.

6.3.2.5. בודקים שהקורא מבצע התקשרות להֶתְקָנִי הזיהוי לייחוס כמוגדר בסעיף 3.1.2.3.

6.3.2.6. ערכת תדלוק שעמדה בבדיקה תשמש כדגם של "ערכת תדלוק מייצגת" לבדיקות של הֶתְקָנִי זיהוי.

6.3.3. בדיקת פירוק, התקנה ושפעול מחדש של קורא

6.3.3.1. מתקינים קורא על אקדח תדלוק.

6.3.3.2. מפרקים את הקורא מאקדח התדלוק.

6.3.3.3. מתקינים התקן זיהוי לייחוס יחיד המכוון לתדר התהודה T6 על מעמד הבדיקה.

6.3.3.4. מקרבים את הקורא אל הֶתְקָנִי הזיהוי, ובודקים שאין תקשורת ביניהם ושהמידע הייחודי בהתקן הזיהוי אינו מועבר אל הקורא.

6.3.3.5. מתקינים את הקורא על אקדח התדלוק ומשפעלים אותו מחדש.

6.3.3.6. מקרבים את הקורא אל הֶתְקָנִי הזיהוי ובודקים שיש תקשורת ביניהם ושהמידע הייחודי בהתקן הזיהוי מועבר אל הקורא.

6.3.4. בדיקת תפקוד של הֶתְקָנִי זיהוי

6.3.4.1. מתקינים הֶתְקָנִי זיהוי לייחוס יחיד המכוון לתדר התהודה T6 על מעמד הבדיקה כמוגדר בסעיף 6.2.1.

6.3.4.2. מתקינים על המעמד ערכת תדלוק מייצגת ראשונה ובודקים כמפורט להלן:

- בודקים שערכת התדלוק המייצגת קולטת ומפענחת את המידע הייחודי הצרוב בתג של הֶתְקָנִי

הזיהוי בטווח הפעולה המוגדר בסעיף 5.4 במרווחים של 1.0 ס"מ.

- בודקים שערכת התדלוק המייצגת אינה קולטת את כל התגים בטווח אי-הפעולה המוגדר בסעיף 5.4.

- **בודקים שזמן העברת המידע הייחודי מהתקן הזיהוי לערכת התדלוק המייצגת עומד במוגדר בסעיף 2.1.2.3.**
- **בודקים שערכת התדלוק המייצגת מבצעת התקשרות להתקן הזיהוי בזמנים כמוגדר בסעיף 3.1.2.3.**
- 6.3.4.3 חוזרים על הפעולה שבסעיף 6.3.4.2 עם כל ערכות התדלוק המייצגות הנבדקות.
- 6.3.5 **בדיקת אי-יכולת לשנות מידע ייחודי הצרוב בהתקן זיהוי (לפי סעיף 2.1.1.10)**
- 6.3.5.1 בודקים התקן הזיהוי בבדיקה תפקוד לאחר תכנותו ושפעולו.
- 6.3.5.2 מתכנתים ומשפעלים את התקן הזיהוי פעם נוספת במידע ייחודי שונה.
- 6.3.5.3 בודקים בבדיקת תפקוד שהמידע הייחודי הצרוב בהתקן לא השתנה.
- 6.3.6 **בדיקת תקשורת ממשדר רכב**
- 6.3.6.1 מחברים את היחידה המדמה למשדר הרכב, מתקינים את ציוד הבדיקה המדמה בקר תחנה ומפעילים את כל הציוד.
- 6.3.6.2 קובעים נתון נסועה ביחידה המדמה ובודקים כמפורט להלן:
 - 6.3.6.2.1 **מקרבים את משדר הרכב לציוד הבדיקה המדמה בקר תחנה עד לקיום תקשורת ביניהם, ובודקים שנתון מד הנסועה מועבר ממשדר הרכב לציוד הבדיקה המדמה.**
 - 6.3.6.2.2 **בודקים שלאחר העברת אישור ממדמה בקר תחנה למשדר רכב על קבלת הנתון הופסקה התקשורת ממשדר הרכב.**
 - 6.3.6.2.3 **בודקים את נתון הנסועה שהתקבל ובודקים שהוא בתחום המוגדר בסעיף 2.2.2.3.**
 - 6.3.6.2.4 **חוזרים על הבדיקה ב- 10 ערכים שונים לפחות של נתון נסועה.**
 - 6.3.6.3 בודקים את הפסקת השידור ממשדר הרכב כמפורט להלן:
 - 6.3.6.3.1 **כאשר יש תקשורת בין משדר הרכב לציוד בדיקה המדמה בקר תחנה, מפסיקים (מכבים) את פעולת ציוד הבדיקה ובודקים כי משדר הרכב הפסיק אוטומטית לשדר.**
 - 6.3.6.3.2 **מפעילים מחדש את ציוד הבדיקה המדמה בקר תחנה, ובודקים שהתקשורת התחדשה אוטומטית.**
- 6.3.7 **בדיקות הורסות**
- עורכים את הבדיקות שלהלן לאחר שכל הבדיקות האחרות הסתיימו בהצלחה.
 - 6.3.7.1 **פירוק והסרה של התקן זיהוי (סעיף 2.1.1.10)**
 - 6.3.7.1.1 **מתקינים התקן זיהוי שנבדק לפי התקן הישראלי ת"י 6200 חלק 3 ולפי הנחיות היצרן על משטח מתכת.**
 - 6.3.7.1.2 **מפרקים ומסירים את התקן הזיהוי ממיקום התקנתו.**
 - 6.3.7.1.3 **מתקינים את התקן הזיהוי שוב לפי התקן הישראלי ת"י 6200 חלק 3 ולפי הנחיות היצרן במיקום אחר על משטח המתכת.**
 - 6.3.7.1.4 **מקרבים אל התקן הזיהוי קורא מייצג המורכב על אקדח תדלוק ובודקים שהתקן הזיהוי מנוטרל, שאין תקשורת בינו לקורא ושמידע ייחודי אינו מועבר אל הקורא.**
 - 6.3.7.2 **תכנות ושפעול חוזר של התקן זיהוי מנוטרל (סעיף 2.1.1.10)**

- 6.3.7.2.1 מתכנתים ומשפעלים מחדש הִתְקַן זיהוי שהוסר ממקומו ונוטרל.
- 6.3.7.2.2 מתקינים את הִתְקַן הזיהוי לפי התקן הישראלי ת"י 6200 חלק 3 ולפי הנחיות היצרן על משטח מתכת.
- 6.3.7.2.3 מקרבים קורא מייצג אל הִתְקַן הזיהוי ובדקים שאין תקשורת ביניהם ושמידע ייחודי אינו מועבר אל הקורא.

טיוטה לת"י 6200 חלק 1

נספח א – מבנה הנתונים של הֶתָקָן זיהוי על גבי תג HITAG S 2048
(נורמטיבי)

א-1. כללי

נספח זה מתאר את מבנה הנתונים של הֶתָקָן זיהוי על גבי תג בטכנולוגיית גלי רדיו (RFID) מסוג Phillips Semiconductors HITAG S 2048.

א-2. מיפוי הזיכרון

א-2.1. לתג HITAG S קיבולת אחסון של 2048 סיביות, המאורגנות ב-16 בלוקים. בכל בלוק 4 מילים בנות 4 בתים כל אחת (בכל מילה 32 סיביות).

א-2.2. טבלה א-1 להלן מתארת את מבנה הזיכרון של התג.

טבלה א-1 – מבנה זיכרון של תג HITAG S

הערות	תיאור	שם המילה	מספר מילה	
	מזהה ייחודי של התג כפי שנצרב בתהליך היצור	UID	0	נתונים ספציפיים לסוג התג
בלוק זה משמש לפעולת התג ואבטחתו, לפי המוגדר בסעיף 0	אוגרים (רגיסטרים) בשימוש התג	CON	1	
בלוק זה משמש מנגנון Challenge-Response של התג, לפי המוגדר בסעיף א-4	מפתחות ההזדהות	KEYH/L	3, 2	
לפי המוגדר בסעיף 2.2.1.5	מזהה יצרן המערכת	SID	4	נתונים תפעוליים ללא תלות בסוג התג
לפי המוגדר בסעיף 2.2.1.5	ערכים תפעוליים (שמור לשימוש היצרן)	OP	5	
חתימה קריפטוגרפית המשמשת לזיהוי התג, לפי המוגדר בסעיף 2.2.1.6	מזהה תג ייחודי (UTI) מוצפן באמצעות מפתח הצפנה אוניברסלי	TDS	9-6	
חתימה קריפטוגרפית משנית המשמשת לזיהוי התג במצבים שיש בהם חשש כי מפתח ההצפנה האוניברסלי נחשף, לפי המוגדר בסעיף 2.2.1.8	מזהה תג ייחודי (UTI) מוצפן באמצעות מפתח הצפנה משני	EDS	13-10	

א-3. מבנה האוגרים (רגיסטרים)

א-3.1. טבלה א-2 שלהלן מתארת את מבנה האוגרים (רגיסטרים) של התג. הסעיפים שלהלן מביאים את הערכים התקניים הדרושים לאתחול התג.

טבלה א-2 - מבנה אוגרים (רגיסטרים) של HITAG S

				מס' מילה
UID0	UID1	UID2	UID3	00
CON0	CON1	CON2	PWDH0	01
PWDL0	PWDL1	KEYH0	KEYH1	02
KEYL0	KEYL1	KEYL2	KEYL3	03

א-3.2. בתים UIDn

בתים UID0-UID3 (קריאה בלבד) - מזהה ייחודי של התג כפי שנצרב בתהליך הייצור.

א-3.3. בית CON0

בית CON0 (קריאה בלבד) מזהה את סוג התג (2,048 סיביות) במשפחת התגים. טבלה א-3 מתארת את הערכים התקניים לבית CON0.

טבלה א-3 - בית CON0

ערך	תיאור	סיביות
2	2048 סיביות	1-0
0	לא בשימוש	7-2

א-3.4. בית CON1

בית CON1 מגדיר פרמטרים פונקציונאליים של התג. טבלה א-4 מתארת את הערכים התקניים לבית CON1.

טבלה א-4 - בית CON1

הערות	ערך נדרש	תיאור	סיביות
Lock Key and Password. נועל את הבתים המכילים את המפתחות והסקמות הדרושים להזדהות התג (אינו מאפשר כתיבה)	1	LKP	0
נועל את הרגיסטר לשינויים	1	LCON	1
מצב עבודה: Transponder Talk First Mode	0	TTFM	3-2
TTFM Disabled = 0	1 (8kBit)	TTFRD	5-4
סיביות 6-4 מתייחסות למצב עבודה TTF ולכן אינן רלוונטיות	0	TTFC	6
התג דורש הזדהות לפני הקריאה	1	AUT	7

א-3.5. בית CON2

בית CON2 נועל את מילים 4-63 כדי למנוע צריבה מחדש של התג.
טבלה א-5 מתארת את הערכים התקניים לבית CON2.

טבלה א-5 - בית CON2

סיביות	תיאור	ערך נדרש	הערות
7-0	LCK0-7	1	נועל כל בית עם כתיבתו והופך אותו לקריאה בלבד

א-4. מפתח הזדהות (Challenge-Response)

א-4.1. מפתח ההזדהות משמש לזיהוי התג באמצעות הקורא. המפתח ייקבע על ידי הרגולטור בבלוק בעל 32 בתים ויימסר ליצרני המערכת לצורך הקידוד.

א-4.2. בעת צריבת התג HITAG-S, ייצרבו תשעת הבתים לפי מיקומם כפי שמפורט בטבלה א-2.

א-4.2.1. 6 בתים ראשונים המכילים את מפתחות ההזדהות של התג כמפורט להלן:
KEYH0, KEYH1, KEYL0, KEYL1, KEYL2, KEYL3

א-4.2.2. 3 בתים הבאים אחריהם המכילים את סקמות האימות (authentication) של התג כמפורט להלן:
PWDH0, PWDL0, PWDL1

נספח ב – מבנה הנתונים של הִתְקָן זיהוי על גבי תג Atmel ATA5580
(נורמטיבי)

ב-1. כללי

נספח זה מתאר את מבנה הנתונים של הִתְקָן זיהוי על גבי תג בטכנולוגיית גלי רדיו (RFID) מסוג Atmel ATA5580.

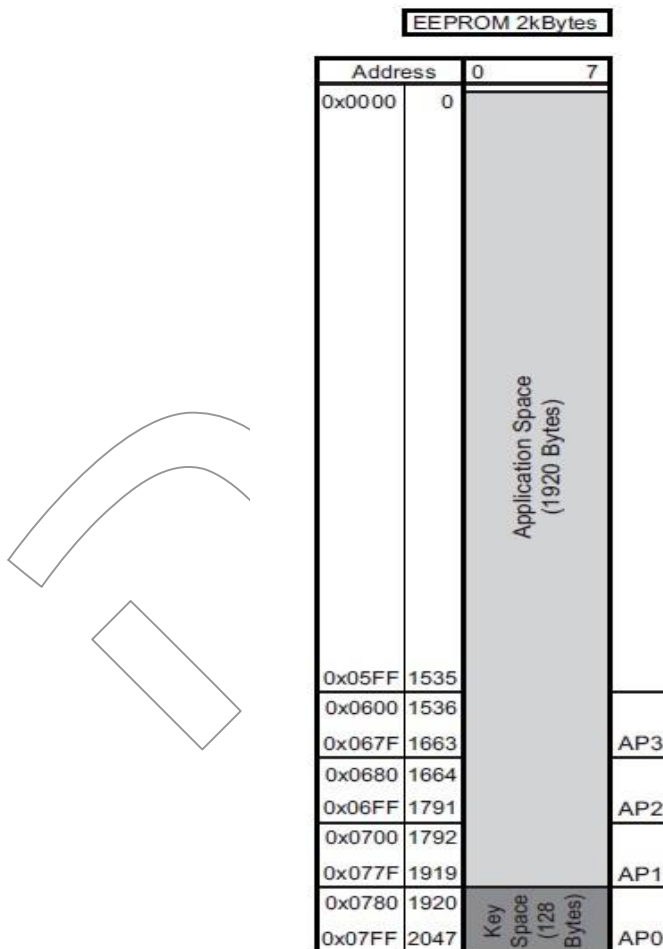
ב-2. מיפוי הזיכרון

ב-2.1. לתג ATA 5580 קיבולת אחסון של 2048 סיביות, המאורגנות ב-5 מקטעים.

ב-2.2. ציור ב-1 שלהלן מתאר את מבנה הזיכרון של התג.

- מרחב הזיכרון AP3, AP3, 0x600 עד 0x67F - משמש לאחסון נתוני הִתְקָן הזיהוי.
- מרחב הזיכרון AP0, AP0, 0x780 עד 0x7FF - מרחב מוגן המשמש לאחסון מפתחות ההזדהות.
- שאר מרחבי הזיכרון אינם בשימוש המערכת.

ציור ב-1 – מבנה זיכרון של תג ATA 5580



ב-2.3. טבלה ב-1 שלהלן מתארת את מבנה מרחב הזיכרון AP3 המשמש לאחסון נתוני ה־תֶקֶן הזיהוי. כתובת הבסיס של המרחב היא 0x0600.

טבלה ב-1 – מבנה AP3

הערות	תיאור	שם המילה	אורך (בתים)	נתונים תפעוליים ללא תלות בסוג התג
לפי המוגדר בסעיף 2.1.1.5	מזהה יצרן מערכת	SID	4	
לפי המוגדר בסעיף 2.1.1.5	ערכים תפעוליים (שמור לשימוש היצרן)	OP	4	
חתימה קריפטוגרפית המשמשת לזיהוי התג, לפי המוגדר בסעיף 2.1.1.6	מזהה תג ייחודי (UTI) מוצפן באמצעות מפתח הצפנה אוניברסלי	TDS	16	
חתימה קריפטוגרפית משנית המשמשת לזיהוי התג במצבים שיש בהם חשש כי מפתח ההצפנה האוניברסלי נחשף, לפי המוגדר בסעיף 2.1.1.8	מזהה תג ייחודי (UTI) מוצפן באמצעות מפתח הצפנה משני	EDS	16	

ב-2.4. טבלה ב-2 להלן מתארת את מבנה מרחב הזיכרון המשמש לאחסון החתימות הקריפטוגרפיות TDS ו-EDS⁽³⁾.

טבלה ב-2 – איחסון חתימות קריפטוגרפיות

Address	LSB			MSB
0x600	TDS[0]	TDS[1]
0x604				
0x608				
0x60C	TDS[0xE]	TDS[0xF]

Address	LSB			MSB
0x610	EDS[0]	EDS[1]
0x614				
0x618				
0x61C	EDS[0xE]	EDS[0xF]

(3) מזהה תג ייחודי כפי שנצרב בתהליך ייצור התג, המשמש לחישוב החתימות כמפורט בסעיף 2.1.1.6.5 שלעיל, כולל חמישה בתים בכתובת 0x800-0x804.

ב-3. מבנה האוגרים (רגיסטרים)

ב-3.1. טבלה ב-3 שלהלן מתארת את מבנה אוגרים (הרגיסטרים) של התג.

טבלה ב-3 – מבנה אוגרים (רגיסטרים) ATA 5580

Reg. Name	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	ADDR
Configuration	DCD	MOD	CM	DLP0	DLP1	KS	SKT	TDH	0x815
	1	0	1	0	0	0	1	1	

Reg. Name	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	ADDR
threshold	PLM0	PLM1	PLM2	PLM3	PLM4	PLM5	PLM6	PLM7	0x816
	0	0	1	0	0	1	0	0	

Reg. Name	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	ADDR
Baud setting*									0x817
T2 prescaler*									0x818

*TBD

Reg. Name	Bit 0	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	ADDR
Challenge length (80h)	0	0	0	0	0	0	0	1	0x819
Response length(50h)	0	0	0	0	1	0	1	0	0x81A

ב-4. מפתח הזדהות (Challenge-Response)

ב-4.1. מפתח ההזדהות משמש לזיהוי התג באמצעות הקורא. המפתח ייקבע על ידי הרגולטור בבלוק בעל 32 בתים וימסר ליצרני מערכת לצורכי הקידוד.

ב-4.2. בעת צריבת התג ATA 5580, ייצרבו 32 הבתים הבאים לפי מיקומם כפי שמפורט בטבלה ב-4 (כל אחד בשלושה עותקים):

Secret key 1 : data1..data 16 – 16 הבתים הראשונים

Secret key 2 : data1..data 16 – 16 הבתים הבאים

טבלה ב-4 – מיפוי מפתחות הזדהות עבור תג ATA 5580

Secret Key	Data 1	Data 2	Data 3	Data 4	Data 5	Data 6	Data 7	Data 8	Data 9	Data 10	Data 11	Data 12	Data 13	Data 14	Data 15	Data 16	Physical Address
2																	0780 - 078F
2 (Copy 1)																	0790 - 079F
2 (Copy 2)																	07A0 - 07AF
1																	07B0 - 07BF
1 (Copy 1)																	07C0 - 07CF
1 (Copy 2)																	07D0 - 07DF
																	07E0 - 07EF
																	07F0 - 07FF

128 bytes of Secret Key memory

AP0 128 Bytes

ב-5. הגנת הנתונים

ב-5.1. כדי להגן על נתוני המערכת, מרחב הזיכרון AP3 צריך להיות נעול ולקריאה בלבד.

ב-5.2. פעולה זו תבוצע בסיוע האיתחול של התג על ידי שליחת הפקודה Write Memory Access Protection כמפורט בטבלה ב-5 שלהלן:

טבלה ב-5 – מבנה פקודת Write Memory Access Protection

שדה	גודל	ערכים	תיאור
Command ID	4+4 בתים	0110b+1010 CRC	Write Memory Access Protection
Data Payload	1 בית	00110000	Protection scheme: locks AP3
CRC	1 בית	Calculate	

נספח ג – ממשק התקשורת בין משדר רכב לבקר תחנה בתחנת התדלוק

(נורמטיבי)

ג-1. מאפייני תקשורת אלחוטית

- ג-1.1. תקשורת אלחוטית בין משדר רכב (VDT) לבקר תחנה בתחנת התדלוק תבוצע באמצעות שידור אלחוטי לפי המוגדר בתקן האמריקני IEEE 802.15.4. התקשורת בין משדר הרכב לבקר התחנה תהיה ישירה או באמצעות תחנת ממסר אחת או יותר שיעבירו את השידורים של משדר הרכב אל בקר התחנה. מומלץ שהתקשורת תעבור דרך תחנת ממסר אחת לפחות.
- ג-1.2. לכל משדר רכב ולכל תחנת ממסר (Relay Station) כתובת MAC ייחודית בת שמונה בתים לפי המוגדר בתקן האמריקני IEEE 802.15.4.
- ג-1.3. לתחנת הממסר יוקצה תדר פנוי מתוך 16 התדרים המוגדרים ובמצב שידור היא תשלח הודעת הכרזת תחנת ממסר (RSAM) משודרת באופן מחזורי כדי לאפשר ליחידות משדר רכב הנכנסות לתחומה להתקשר עימה.

ג-2. מצבי עבודה של משדר הרכב

להלן מצבי התקשורת האלחוטית השונים ביחידת משדר הרכב:

- ג-2.1. **מצב נסיעה**

זהו מצב ההמתנה של היחידה. במצב זה היחידה סורקת את 16 התדרים המוגדרים לאיתור הודעת RSAM. ברגע שהיחידה מבחינה בהודעת RSAM, היא רושמת את נתוני תחנת הממסר ועוברת למצב התקשורת.
- ג-2.2. **מצב התקשורת**

במצב זה, היחידה שולחת הודעת נתוני רכב (VDDM) ומקבלת מתחנת הממסר הודעת אישור קבלת נתוני רכב (RSCM). כאשר הודעת האישור התקבלה, יחידת המשדר עוברת למצב תדלוק. אם הודעת ה-RSCM לא התקבלה במשדר הרכב גם לאחר שני ניסיונות נוספים, ההתקשורת תנותק ומשדר הרכב יעבור למצב נסיעה.
- ג-2.3. **מצב תדלוק**

מצב זה דומה למצב נסיעה, פרט לכך שמשדר הרכב אינו מבצע התקשורת לתחנות הממסר אשר הוא כבר מחובר אליהן. כאשר מתגלה יחידת ממסר חדשה, משדר הרכב יתקשר גם אליה. עם השלמת העברת המידע ממשדר הרכב היחידה תבטל את ההתקשורת אל תחנת הממסר. אם אין אף התקשורת פתוחה משדר הרכב יעבור למצב נסיעה.

ג-3. הודעות ממשק אלחוטי

ג-3.1. כללי

- הסעיפים שלהלן מתארים את בתי המידע (payloads) ומאפיינים נבחרים של הודעות בשימוש הממשק לפי התקן האמריקני IEEE 802.15.4. יתר מאפייני ההודעות מוגדרים במלואם בתקן האמריקני IEEE 802.15.4.
- לכל הודעה כותרת בת 5 בתים ואחריה רשימה של אלמנטים מסוג TLV (Tag-Length Value).

ג-3.2. מבנה כללי של הודעה: הוא מנדטורי, כפי שמפורט בתקן הבין-לאומי ISO/IEC 7816-4. כאשר הודעה מסומנת כמוצפנת, רק האלמנטים מסוג TLV יהיו מוצפנים. מילוי בתים (Padding)

טבלה ג-1 - מבנה ההודעות

שם השדה	אורך	תיאור
Net Command	1 בית	מזהה סוג הודעה
Msg ID	1 בית	מספר ההודעה. מספר בן 8 סיביות המוקצה לכל הודעה על ידי כל משדר (כולל יחידת הממסר). מספור ההודעה מתקדם באחד על כל הודעה נשלחת. הודעת ניסיון נוסף (Retry) אינה מקדמת את המספור.
Frame Control	1 בית	מזהה מצב הצפנה: לא מוצפן Bit 0 = 0 מוצפן Bit 0 = 1 Bit 1-7= Don't care
Data Len	2 בתים	ערך בינארי המזהה את אורך שדות בתי המידע (Payload). אם ההודעה מוצפנת הערך יכול להיות את מילוי הבתים המנדטורי.
Data Payload (TLV)	N בתים	כולל את נתוני כלי הרכב המועברים לתחנת הממסר.

ג-3.3. הודעת הכרזת תחנת ממסר (RSAM)

הודעה זו תישלח באופן שוטף כל 200-250ms מילישניות על ידי תחנת הממסר במצב שידור והיא לא תהיה מוצפנת.

טבלה ג-2 מתארת את הערכים התקניים להודעת RSAM.
טבלה ג-3 מתארת את המבנה התקני של שדות המידע.

טבלה ג-2 - הודעת RSAM

שדה	ערך	תיאור
Net Command	0x41	הודעת RSAM
Msg ID	xx	מספר הודעה
Frame Control	0x00	הודעה לא מוצפנת
Data Len	xxxx	בהתאם לבתי המידע

טבלה ג-3 - שדות המידע בהודעת RSAM

דרישה	תיאור	V(Value) ערך	L	T
Mandatory	מזהה מערכת	01h	01h	40h
Mandatory	גרסת מערכת		02h	42h
Mandatory	מזהה יצרן		01h	44h
Optional	נתונים ספציפיים של היצרן		02h	46h
Mandatory	מזהה תחנה (ייחודי)	בית 0-1 מספר תחנה בית 2 מספר חברה	03h	48h
Mandatory	מספר אקראי לצורכי הצפנת נתוני הודעת ה-VDDM		04h	4Ah

ג-3.4. הודעת נתוני רכב (VDDM)

הודעה זו תישלח על ידי משדר הרכב כאשר הוא במצב התקשרות. ההודעה תישלח במיעון ישיר אל תחנת הממסך ממנה התקבלה הודעת ה-RSAM והיא לא תהיה מוצפנת. אם הודעת אישור (ראו סעיף ג-3.5) אינה מתקבלת תוך 80 מילישניות, הודעת ה-VDDM תישלח שוב. אם לאחר עוד 80 מילישניות הודעת אישור אינה מתקבלת הודעת ה-VDDM תישלח שוב.
טבלה ג-4 מתארת את המבנה התקני של הודעת VDDM.
טבלה ג-5 מתארת את המבנה התקני של שדות המידע בהודעת VDDM.

טבלה ג-4 - הודעת VDDM

שדה	ערך	תיאור
Net Command	150x	הודעת VDDM
Msg ID	xx	מספר הודעה
Frame Control	0x00	הודעה לא מוצפנת
Data Len	xxxx	בהתאם לבתי המידע

טבלה ג-5 - שדות המידע בהודעת VDDM

דרישה	תיאור	V(Value)	L	T
Mandatory	מספר אקראי המועתק מה-RSAM		04h	4Ah
Mandatory	מזהה יצרן		01h	44h
Optional	גרסת VDT תוכנה		02h	2h5
Optional	גרסת VDT חומרה		02h	h54
Optional	נתונים ספציפיים של היצרן		02h	46h
Mandatory	מספר מקשר להִתְקָן הזיהוי המותקן בכלי רכב (UID)		h80	h56
Optional ⁽¹⁾	מספר מקשר להִתְקָן הזיהוי נוסף המותקן בכלי רכב (UID)		h80	h57
Mandatory	נתון מד הנְסוּעָה במבנה SAE-J1939-71	בית 0-1 (SPN) : 0x03 בית 2-5 ערך 0x095	03h	8h5
Optional ⁽¹⁾	נתון נוסף ממחשב כלי הרכב במבנה SAE-J1939-71	בית 0-1 (SPN) בית 2 - ערך xx	nn	h59

⁽¹⁾ מספר המופעים של שדה זה בהודעה: 0 או יותר.

ג-3.5. הודעת אישור קבלת נתוני רכב (RSCM)

הודעה זו תישלח על ידי תחנת הממסר לאחר קבלת הודעת ה-VDDM אך לא יאוחר מ-70 מילישניות לאחר קבלת ה-VDDM. ההודעה תישלח במיעון ישיר אל משדר הרכב ממנו התקבלה הודעת ה-VDDM והיא לא תהיה מוצפנת.

טבלה ג-6 מתארת את הערכים התקניים להודעת RSCM.
טבלה ג-7 מתארת את המבנה התקני של שדות המידע.

טבלה ג-6 - הודעת RSCM

שדה	ערך	תיאור
Net Command	0x61	הודעת RSCM
Msg ID	xx	מספר הודעה
Frame Control	0x00	הודעה לא מוצפנת
Data Len	xxxx	בהתאם לבתי המידע

טבלה ג-7 - שדות המידע בהודעת RSCM

דרישה	תיאור	V(Value) ערך	L	T
Mandatory	מזהה יצרן		01h	44h
Mandatory	מספר מקשר להִתְקֵן הזיהוי המותקן בכלי רכב (UID)		h80	6h5
Optional	נתונים ספציפיים ליצרן		02h	46h

נספח ד – דרישות מומלצות למערכת

(למידע בלבד)

ד-1. כללי

בנספח זה מובאות דרישות אשר מומלץ לשקול את יישומן ושילובן במערכת.

ד-2. מבנה ותפקוד הקורא

ד-2.1. מומלץ להתקין נורית מסוג דיודה פולטת אור (LED) על הקורא במקום בולט וברור לעין.

ד-2.2. מצב הנורית ייתן חיווי לקיום תקשורת בין הקורא להתקן הזיהוי:

ד-2.2.1. הארה מתמשכת של הנורית – תקשורת רציפה.

ד-2.2.2. הארה לסירוגין או הבהוב – התקשורת אינה רציפה.

ד-2.2.3. נורית כבויה - תקשורת מנותקת.

ד-2.3. צריכת האנרגיה של הנורית לא תפחית מאורך חיי הסוללה המוגדר בתקן הישראלי ת"י 6200 חלק 2.

ד-3. דיווח אירועים במערכת

דיווח וסיווג אירועים במערכת ישמש לאיתור תקלות ובעיות וישפר את ביצועיה ויכולותיה של המערכת. מומלץ שיהיה דיווח על אירועים למקרים כגון:

ד-3.1. זיהוי וניטור ניסיונות להוצאת אקדח התדלוק מפיית התדלוק בזמן התדלוק.

ד-3.2. הסרה או פירוק של קורא.

ד-3.3. תקלות תקשורת בין מרכיבי המערכת.

ד-3.4. קורא שלא שופעל.

ד-3.5. תקלות בקורא ובעיקר מצב הסוללה.