SI 5907

תקן ישראלי ת"י 5907

September 2014

תשרי התשע"ה - ספטמבר 2014

ICS CODE: 35.240.15

מדריך – מיפוי תקינה לכרטיסים חכמים

Guide – Standards mapping for smart cards

מכון התקנים הישראלי
The Standards Institution of Israel

רח' חיים לבנון 42, תל-אביב 69977, טל' 03-6465154, פקס' 03-6412762, www.sii.org.il

תקן זה הוכן על ידי ועדת המומחים 211409 – כרטיס חכם, בהרכב זה:
ויקטור איררה, אדי הררי, עופר ישי (יו"ר), יבגני ליברמן, יעקב מנדל

תקן זה אושר על ידי הוועדה הטכנית 2114 – אבטחת תקשוב, בהרכב זה:

איגוד האינטרנט הישראלי	-	איציק קוטלר
בנק ישראל – הפיקוח על הבנקים	-	רחל יעקובי
האיגוד הישראלי לביקורת ואבטחת מערכות מידע	-	משה שפר
המועצה הישראלית לצרכנות	-	ארי שסקין
הרשות למשפט, טכנולוגיה ומידע (רמו"ט)	-	עומר פרידמן
לשכת מנתחי מערכות מידע בישראל	-	נעמי אברמסון, אבנר בן אפרים, בועז דולב (יו"ר)
מכון התקנים הישראלי – אגף התעשייה	-	אילן כרמית
משרד האוצר – אגף התקשוב הממשלתי	-	גדעון קונפינו
משרד הביטחון	-	ניר סלינס
משרד ראש הממשלה – המטה הקיברנטי הלאומי	-	זיו סלומון
צבא ההגנה לישראל – אגף התקשוב	-	מיכאל לנגר
רשות ההסתדרות לצרכנות	-	עודד סלע

יניב גיאת ריכז את עבודת הכנת התקן.

מילות מפתח:
כרטיסים חכמים, כרטיסי זיהוי, חילוף מידע, קווים מנחים.

Descriptors:
smart cards, identity cards, information exchange, guidelines.

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 המסמך 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:

תוכן העניינים

מבוא

כרטיסים חכמים הם אמצעים נפוצים לזיהוי ולאימות של זהות, והם משמשים ביישומים שונים, כגון תעודות זהות, כרטיסי עובד, דרכונים, כרטיסים לתחבורה ציבורית. לפיכך ישנה חשיבות באסדרת יישומם של כרטיסים חכמים במדינת ישראל על סמך תקינה בין-לאומית ועל סמך תקינה לאומית.

מטרות תקן זה הן אלה:

- להפנות בצורה שיטתית לתקנים הקיימים;
- להגדיר את קשרי הגומלין ביניהם;
- כאשר הדבר נדרש, להדגיש היבטים מיוחדים הנוגעים ליישום הכרטיסים החכמים בישראל.

הערה:

תקן זה אינו מפנה לכל התקינה הקיימת בנושא ואינו מביא בהכרח רק תקינה בין-לאומית.

תקן זה מפנה אל התקנים הרלוונטיים לכרטיסים חכמים, לרבות:

- תקני אבטחת מידע בכרטיסים חכמים;
- תקנים הנוגעים להנגשת כרטיסים חכמים לאנשים עם מוגבלות;
- תקנים ליישומיים ייחודיים שבהם נעשה שימוש בכרטיסים חכמים, כגון: דרכון, תעודת זהות, תחבורה ציבורית, טלפונים סלולריים והתקנים ניידים.

כרטיסים חכמים הם חלק ממערכת שבה הם משתלבים כרכיב זיהוי, או/וגם כרכיב אבטחת מידע, או/וגם כאמצעי תשלום או/וגם לשימוש אחר.

חלקי מערכת כרטיס חכם הם אלה:

- הכרטיס החכם עצמו, על כל רכיביו;
- מתקן לקריאת הכרטיס או לכתיבה עליו;
- יישום הפועל הן על גבי הכרטיס החכם והן במתקן הקריאה/הכתיבה, או/וגם במערכת היעד, והכולל מנשקים[1] בין הכרטיס החכם לבין מתקן הקריאה/הכתיבה ומערכת היעד.

לכרטיסים חכמים יש מנשקים שונים, כגון:

- מנשק פיזי;
- מנשק העברת כוח חשמלי לתפעול הכרטיס;
- מנשק תקשורת להעברת מידע ומסרים;
- מנשק מערכת הפעלה הכולל הגדרת מבנה נתונים, מבנה פקודות ושירותים;
- מנשק יישומי הכולל גישה למבנה הנתונים שעל הכרטיס החכם לצורך ביצוע פעולות שונות.

מערכות ההפעלה בכרטיסים חכמים הן אלה:

- מערכת הפעלה "מולדת" (native);
- מערכת הפעלה מבוססת JAVA;
- מערכת הפעלה אחרת.

---

(1) לפי קביעת האקדמיה ללשון העברית: מנשק, מישק – interface. בלשון המקצוע מקובל לכנות מנשק או/וגם מישק בשם "ממשק".

1. חלות התקן

תקן זה מביא מידע הנוגע לתקנים החלים על כרטיסים חכמים.

2. תקנים החלים על כרטיסים חכמים

לידיעת המשתמש בתקן – התקנים הישראליים זהים לתקנים הבין-לאומיים המצוינים להלן בסוגריים.

2.1. כרטיסי זיהוי – כרטיסי מעגלים משולבים

ת"י 7816 חלק 1 – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – אופיינים פיזיים (ISO/IEC 7816-1)

ת"י 7816 חלק 2[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – מידות המגעים ומיקומם (ISO/IEC 7816-2)

ת"י 7816 חלק 3[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – מנשק חשמלי ופרוטוקולי תמסורת (ISO/IEC 7816-3)

ת"י 7816 חלק 4[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: ארגון, אבטחה ופקודות להחלפה (ISO/IEC 7816-4)

ת"י 7816 חלק 5[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: רישום ספקי יישומים (ISO/IEC 7816-5)

ת"י 7816 חלק 6[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: אלמנטי נתונים בתעשייה המיועדים להחלפה (ISO/IEC 7816-6)

ת"י 7816 חלק 7 – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – פקודות בין-ענפיות לשפת שאילתות כרטיס מובנות (SCQL) (ISO/IEC 7816-7)

ת"י 7816 חלק 8[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: פקודות לפעולות אבטחה (ISO/IEC 7816-8)

ת"י 7816 חלק 9[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: פקודות לניהול כרטיס (ISO/IEC 7816-9)

ISO/IEC 7816-10 – Identification cards – Integrated circuit(s) cards with contacts: Electronic signals and answer to reset for synchronous cards

ת"י 7816 חלק 11[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: אימות אישי בשיטות ביומטריות (ISO/IEC 7816-11)

ת"י 7816 חלק 12[2] – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – מנשק חשמלי מטיפוס USB ונוהלי תפעול (ISO/IEC 7816-12)

ISO/IEC 7816-13 – Identification cards – Integrated circuit cards: Commands for application management in a multi-application environment

ת"י 7816 חלק 15 – כרטיסי זיהוי – כרטיסי מעגלים משולבים: כרטיסים בעלי מגעים – יישום מידע הצפנה (ISO/IEC 7816-15)

---

[2] תקן זה זהה, בשינויים ובתוספות לאומיים, לתקן הבין-לאומי המצוין בסוגריים.

2.2. כרטיסים ללא מגע

2.2.1. כרטיסי קרבה (Proximity)

ת"י 14443 חלק 1 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: מאפיינים פיזיים (ISO/IEC 14443-1)

ת"י 14443 חלק 2 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: עוצמת תדר רדיו ומִנשק אותות (ISO/IEC 14443-2)

ת"י 14443 חלק 3 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: אתחול ומניעת התנגשויות (ISO/IEC 14443-3)

ת"י 14443 חלק 4 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: פרוטוקול שידור (ISO/IEC 14443-4)

2.2.2. כרטיסי קרבה (Vicinity)

ת"י 15693 חלק 1 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: מאפיינים פיזיקליים (ISO/IEC 15693-1)

ת"י 15693 חלק 2 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: מנשק שידור ואתחול (ISO/IEC 15693-2)

ת"י 15693 חלק 3 – כרטיסי זיהוי – כרטיסי מעגלים משולבים ללא מגע – כרטיסי קרבה: פרוטוקול שידור ומניעת התנגשויות (ISO/IEC 15693-3)

2.3. כרטיסים המשלבים מגע וללא מגע – כרטיס SIM (SIM card)

ETSI TS 100 977 V8.14.0 – Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface

ETSI TS 101 267 V.8.18.0 – Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit (SAT) for the subscriber Identity Module – Mobile Equipment (SIM-ME) interface

2.4. שיטות בדיקה

ת"י 10373 חלק 1 – כרטיסי זיהוי – שיטות בדיקה: מאפיינים כלליים (ISO/IEC 10373-1)

ISO/IEC 10373-2 – Identification cards – Test methods: Cards with magnetic stripes

ת"י 10373 חלק 3 – כרטיסי זיהוי – שיטות בדיקה: כרטיסי מעגלים משולבים בעלי מגעים ובעלי הֶתקני מנשקים קשורים (ISO/IEC 10373-3)

ISO/IEC 10373-5 – Identification cards – Test methods: Optical memory cards

ת"י 10373 חלק 6 – כרטיסי זיהוי – שיטות בדיקה: כרטיסי קרבה (ISO/IEC 10373-6)

ISO/IEC 10373-7 – Identification cards – Test methods: Vicinity cards

ISO/IEC 10373-8 – Identification cards – Test methods: USB-ICC

ISO/IEC 10373-9 – Identification cards – Test methods: Optical memory cards – Holographic recording method

2.5. כרטיסים ליישומים שונים

2.5.1. דרכונים

ת"י 7501 חלק 1 – כרטיסי זיהוי – תעודות מסע קריאות על ידי מחשב: דרכון קריא על ידי מחשב (ISO/IEC 7501-1[3])

ISO/IEC 7501-2[4] – Identification cards – Machine readable travel documents: Machine readable visa

ISO/IEC 7501-3[5] – Identification cards – Machine readable travel documents: Machine readable official travel documents

2.5.2. רישיונות נהיגה

ISO/IEC 18013-1 – Information technology – Personal identification – ISO-compliant driving license: Physical characteristics and basic data set

ISO/IEC 18013-2 – Information technology – Personal identification – ISO-compliant driving license: Machine-readable technologies

ISO/IEC 18013-3 – Information technology – Personal identification – ISO-compliant driving license: Access control, authentication and integrity validation – Scanning area identifier – Optional machine readable zone

ISO/IEC 18013-4 – Information technology – Personal identification – ISO-compliant driving license: Test methods

2.5.3. כרטיסים לתחבורה ציבורית

המפרטים הטכניים של "Calypso"[6]

2.5.4. כרטיסי אשראי

EMV Standard – November 2011 Ver.4.3

2.6. תקשורת שדה קרוב (Near Field Communication)

ISO/IEC 13157-1 – Information technology – Telecommunications and information exchange between systems – NFC Security: NFC-SEC NFCIP-1 security services and protocol

ISO/IEC 13157-2 – Information technology – Telecommunications and information exchange between systems – NFC Security: NFC-SEC cryptography standard using ECDH and AES

ISO/IEC 16353 – Information technology – Telecommunications and information exchange between systems – Front-end configuration command for NFC-WI (NFC-FEC)

---

(3) תקן זה זהה למסמך של הארגון הבין-לאומי לתעופה אזרחית ICAO 9303-1.

(4) תקן זה זהה למסמך של הארגון הבין-לאומי לתעופה אזרחית ICAO 9303-2.

(5) תקן זה זהה למסמך של הארגון הבין-לאומי לתעופה אזרחית ICAO 9303-3.

(6) מפרטים אלו נבחרו על ידי משרד התחבורה והבטיחות בדרכים ליישום בישראל.

ISO/IEC 18092 – Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

ISO/IEC 21481 – Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol -2 (NFCIP-2)

ISO/IEC 22536 – Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol (NFCIP-1) – RF interface test methods

ISO/IEC 23917 – Information technology – Telecommunications and information exchange between systems – NFCIP-1 – Protocol Test Methods

ISO/IEC 28361 – Information technology – Telecommunications and information exchange between systems – Near Field Communication Wired Interface (NFC-WI)

NFC Forum – NFC Data Exchange Format (NDEF) Technical Specification

NFC Forum – Type 1 Tag Operation Specification 1.1 –Technical Specification

NFC Forum – Type 2 Tag Operation Specification 1.1 – Technical Specification

NFC Forum – Type 3 Tag Operation Specification 1.1 – Technical Specification

NFC Forum – Type 4 Tag Operation Specification 2.0 – Technical Specification

NFC Forum – NFC Record Type Definition (RTD) – Technical Specification

NFC Forum – Text Record Type Definition – Technical Specification

NFC Forum – URI Record Type Definition – Technical Specification

NFC Forum – Smart Poster Record Type Definition – Technical Specification

NFC Forum – Generic Control Record Type Definition – Technical Specification

NFC Forum – Signature Record Type Definition – Technical Specification

NFC Forum – Connection Handover 1.2 – Technical Specification

NFC Forum – Personal Health Device Communication (PHDC) – Technical Specification

NFC Forum – Logical Link Control Protocol (LLCP 1.1) – Technical Specification

NFC Forum – NFC Digital Protocol – Technical Specification

NFC Forum – NFC Activity Specification – Technical Specification

NFC Forum – Simple NDEF Exchange Protocol (SNEP) – Technical Specification

NFC Forum – NFC Analog – Technical Specification

NFC Forum – NFC Controller Interface (NCI) Specification – Technical Specification

NFC Forum – LLCP to OBEX Protocol Binding – Candidate Technical Specification

NFC Forum – Bluetooth Secure Simple Pairing Using NFC – Application Document

2.7. אבטחת מידע[7]

ת"י 15408 חלק 1 – טכנולוגיית המידע – טכניקות אבטחה – קריטריונים להערכת אבטחה לטכנולוגיית המידע: הקדמה ומודל כללי (ISO/IEC 15408-1)

ת"י 15408 חלק 2 – טכנולוגיית המידע – טכניקות אבטחה – קריטריונים להערכת אבטחה לטכנולוגיית המידע: מרכיבי אבטחה תפקודיים (ISO/IEC 15408-2)

ת"י 15048 חלק 3 – טכנולוגיית המידע – טכניקות אבטחה – קריטריונים להערכת אבטחה לטכנולוגיית המידע: מרכיבי הבטחת אבטחה (ISO/IEC 15408-3)

ISO/IEC 19790[8] – Security techniques – Security requirements for cryptographic modules

2.8. נושאים נוספים

2.8.1. מִנשק אדם מכונה

EN 1332-1 – Identification card systems – Human-machine interface: Design principles for the user interface

EN 1332-2 – Identification card systems – Human-machine interface: Dimensions and location of a tactile identifier for ID-1cards

EN 1332-3 – Identification card systems – Human-machine interface: Keypads

EN 1332-4 – Identification card systems – Human-machine interface: Coding of user requirements for people with special needs

ISO/IEC 24787 – Information technology – Identification cards – On-card biometric comparison

2.8.2. השפה העברית

ת"י 4424 (1999) – כרטיסים הנושאים מעגלים משולבים – יישום השפה העברית

2.8.3. מִנשקים בין הכרטיס לבין יישומים חיצוניים

ISO/IEC 24727 – Identification cards – Integrated circuit card programming interfaces

---

(7) בפרק זה יש הפניה למספר תקני אבטחת מידע המשמשים להגדרת רמת אבטחת המידע בכרטיסים חכמים ובמערכות המשולבות בהן. יובהר, כי אין מדובר בהכרח בכל תקני אבטחת המידע הרלוונטיים ובאחריות כל מיישם מערכת לוודא את התאמתו לפרופיל אבטחת המידע הנדרש.

(8) תקן זה מבוסס על המסמך של המכון הלאומי לתקנים ולטכנולוגיה (NIST) FIPS 140-2.