

KONTAKTITTOMIEN ÄLYKORTTIEN STANDARDIN TILA JA SISÄLTÖ

Selvitys ISO 14443 standardin tilasta ja sisällöstä

29.07.2002

Suorittanut: Rabah Boussouira, DI, toimitusjohtaja, Advantec Oy
Tilannut: Liikenne- ja Viestintäministeriö, Yli-insinööri Seppo Öörni,

LOPPURAPORTTI

SISÄLLYSLUETTELO

SISÄLLYSLUETTELO	2
1. JOHDANTO	3
1.1. YLEISTÄ	3
1.2. KONTAKTITTOMIEN ÄLYKORTTIEN STANDARDEISTA	3
1.3. SELVITYKSEN KOHTEENA OLEVIA STANDARDIEN OSAT	3
2. STANDARDIEN TILA	4
2.1. ISO/IEC 14443-1	4
2.2. ISO/IEC 14443-2	4
2.3. ISO/IEC 14443-3	4
2.4. ISO/IEC 14443-4	4
2.5. ISO/IEC 10373-6	4
3. STANDARDIEN SISÄLTÖ	5
3.1. ISO/IEC 14443-1	5
3.2. ISO/IEC 14443-2	5
3.3. ISO/IEC 14443-3	7
3.4. ISO/IEC 14443-4	9
3.5. ISO/IEC 10373-6	10
4. MITÄ ON VIELÄ TEKEILLÄ	12
5. LUKIJALAITTEIDEN SOPIVUUDESTA – ELI MIHIN KANNATTAA KIINNITTÄÄ HUOMIOTA	13
5.1. YLEISTÄ	13
5.2. ESIMERKKEJÄ LUKIJALAITTEEN OMINAISUUKSISTA, JOIHIN KANNATTAA KIINNITTÄÄ ERITYISTÄ HUOMIOTA	13
6. LYHENTEET	14
7. VIITTEET	15
LIITE 1 – ISO/IEC 14443 STANDARDI JA PATENTITKYSYMYKSET	16

1. JOHDANTO

1.1. Yleistä

Liikenneministeriö on ottanut jo yli kymmenen vuoden ajan aktiivisesti osaa Suomessa tapahtuvaan älykorttitekniikan kehittämiseen ja tukenut älykorttijärjestelmien kehitystä erilaisilla toimenpiteillä. Merkittäviä toimenpiteitä ovat olleet mm. yhteisten julkisten määräysten ja suositusten laatiminen sekä yksittäisten hankkeiden taloudellinen avustaminen. Näillä toimenpiteillä ministeriö on pyrkinyt tukemaan järjestelmien yhteentoimivuutta ja edistämään yhtenäistä teknistä kehitystä.

Älykorttitekniikka (ts. sirukorttitekniikka) on laajassa käytössä useissa järjestelmissä Suomessa ja joukkoliikenteen osalta kontaktiton älykorttitekniikka on hyvää vauhtia yleistymässä. Käsitteet standardien tilasta ja sisällöstä eri osapuolten keskuudessa ovat varsin vaihtelevat ja näin ollen on katsottu tarpeelliseksi selvittää nämä asiat ja julkaista siitä raportti.

1.2. Kontaktittomien älykorttien standardeista

Kontaktittoman sirukorttitekniikan standardointi tapahtuu ISO:ssa (International Standards Organisation). Korttien ominaisuuksia koskevat standardit on ryhmitetty kontaktittoman rajapinnan kantaman mukaan:

- ISO/IEC 10536 määrittelee Close-coupled cards (CICC) eli lyhytkantaman korttien ominaisuudet
- ISO/IEC 14443 määrittelee Proximity cards (PICC) eli lähilukukorttien ominaisuudet
- ISO/IEC 15693 määrittelee Vicinity cards (VICC) eli etälukukorttien ominaisuudet

Lisäksi korttien testausmenettelyt on määritelty standardisarjassa:

- ISO/IEC 10373-6, joka määrittelee testausmenettelyt Proximity cards (PICC) eli lähilukukortteille
- ISO/IEC 10373-7, joka määrittelee testausmenettelyt Vicinity cards (VICC) eli etälukukortteille

Selvityksen kohteena ovat ISO/IEC 14443 standardin eri osat sekä ISO/IEC 19373-6 standardi. Ensimmäinen määrittelee lähilukukorttien fyysiset ominaisuudet, radiotaajuuden rajapinnan, alustamisen ja törmäysten hallinnan ja tiedonsiirtoprotokollat. Jälkimmäinen määrittelee testimenetelmät lähilukukortteille.

1.3. Selvityksen kohteena olevien standardien osat

ISO/IEC 14443:

ISO/IEC 14443-1 ID-kortit - Kontaktittomat sirukortit - Lähilukukortit
- Osa 1: Fyysiset ominaisuudet

ISO/IEC 14443-2 ID-kortit - Kontaktittomat sirukortit - Lähilukukortit - Osa 2: Radiotaajuinen teho- ja signaalirajapinta

ISO/IEC 14443-3 ID-kortit - Kontaktittomat sirukortit - Lähilukukortit - Osa 3: Alustaminen ja törmäysten hallinta

ISO/IEC 14443-4 ID-kortit - Kontaktittomat sirukortit - Lähilukukortit
- Osa 4: Tiedonsiirtoprotokollat

ISO/IEC 10373:

ISO/IEC 10373-6 ID-kortit – Testausmenetelmät - Osa 6: Lähilukukortit

2. STANDARDIEN TILA

Lähilukukortit

2.1. ISO/IEC 14443-1

Standardi on julkaistu kansainväliseksi standardiksi ja julkaisupäivämäärä on 2000-04-15

2.2. ISO/IEC 14443-2

Standardi on julkaistu kansainväliseksi standardiksi ja julkaisupäivämäärä on 2001-07-01

2.3. ISO/IEC 14443-3

Standardi on julkaistu kansainväliseksi standardiksi ja julkaisupäivämäärä on 2001-02-01

2.4. ISO/IEC 14443-4

Standardi on julkaistu kansainväliseksi standardiksi ja julkaisupäivämäärä on 2001-02-01

Testausmenettelyt

2.5. ISO/IEC 10373-6

Standardi on julkaistu kansainväliseksi standardiksi ja julkaisupäivämäärä on 2001-05-15

3. STANDARDIEN SISÄLTÖ

Standardi käyttää lähilukuteknologiaan perustuvista kontaktittomista korteista nimitystä PICC (Proximity IC cards), jossa IC on lyhenne sanoista Integrated Circuit(s)

3.1. ISO/IEC 14443-1

Tämä standardin osa määrittelee kortin fyysiset ominaisuudet:

- Mitat: samat kuin ISO/IEC 7810 mukaiset ID-1 kortit eli samat kuin kontaktikortit;
- Sietokyky ultraviolettivalolle;
- Sietokyky röntgensäteelle;
- Sietokyky dynaamiselle taivutusliikkeelle; (sietokyky taivutusrasitukselle)
- Sietokyky dynaamiselle kiertoliikkeelle; (sietokyky kiertorasitukselle)
- Sietokyky vuoroittaisille magneettisille kentille;
- Sietokyky vuoroittaisille sähköisille kentille;
- Sietokyky staattiselle sähkökentälle;
- Sietokyky staattiselle magneettiselle kentälle;
- Käyttölämpötila.

Lisäksi standardin informatiivisessa liitteessä on seuraavat maininnat ja suositukset:

- muistutus siitä, että standardi ei rajaa pois mahdollisuutta soveltaa muitakin olemassa olevia standardeja,
- rajoituksia saattaa esiintyä kortin pistotuksen osalta,
- mikäli on vaatimuksena jälkikäsitellä kortti valmistuksen jälkeen siten, että pinnalle tulostetaan aihiota (graafinen personointi), silloin näiden pintojen laadun on vastattava tulostimen tai tulostustekniikan asettamia vaatimuksia.

Tämä standardin osa on yhteinen A ja B tyypeille.

3.2. ISO/IEC 14443-2

Tämä standardin osa määrittelee kortin radiotaajuuden teho- ja signaalirajapinnan:

- **Alustava dialogi lukijalaitteen (PCD) ja kortin (PICC) välillä.** Alustava vuoropuhelu on sama molemmille korttityypeille: 1) kortti aktivoi ollessaan lukijalaitteen radiotaajuisessa kentässä, 2) kortti odottaa hiljaisena komentoa lukijalaitteelta, 3) lukijalaite lähettää komennon, 4) kortti lähettää vastauksen lukijalaitteelle.
- **Tehon siirto.** Tehon tuottaminen on lukijalaitteen tehtävä.
- **Taajuus.** Radiotaajuinen käyttökentän taajuus on $13,56 \text{ MHz} \pm 7 \text{ KHz}$ ja se on sama molemmille A ja B tyypeille.
- **Käyttökenttä.** Vähimmäis- ja enimmäisarvot lukijalaitteen tuottamalle käyttökentälle. Testausmenettelyt määritellään standardissa ISO/IEC 10373.
- **Signaalirajapinta.** Lukijalaitteen ollessa tyhjäkäynnillä sen tulee käyttää vuorotellen A ja B korttityypin modulointimenetelmää kunnes se havaitsee jommankumman korttityypin läsnäolon. Vain yksi (jompikumpi) korttityypin modulointimenetelmä voi olla käytössä yhden istunnon aikana, kunnes lukijalaite kytkee kentän pois päältä tai kortti otetaan pois.

- **A -tyypin kommunikaatiosignaalin rajapinta.** Standardissa määritellään yksityiskohtaisesti signaalin rajapinnan ominaisuudet molemmissa suunnissa (lukijalaitteesta kortille ja kortilta lukijalaitteeseen): bittitaso tiedonsiirtonopeus, modulaatio, bittiesitystapa ja koodaus.

Lukijalaitteesta korttiin:

- **Bittitasoinen tiedonsiirtonopeus.** Noin 106 kbit/s alustuksen ja törmäysten hallinnan aikana.
- **Modulaatio.** Lukijalaitteesta korttiin kommunikaatio perustuu RF-kentän ASK100% mukaiseen modulointiin eli lukijalaite vaientaa radiotaajuuden kentän lähes kokonaan tauon luomiseksi.
- **Bittiesitys ja koodaus.** Standardi määrittelee kolme erilaista sekvenssiä modulaatio/ei modulaatiota, jotka voivat esiintyä bitin keston aikana ja joiden avulla esitetään/koodataan bittien loogiset tilat, kommunikoinnin aloitus, lopetus ja informaation puute.

- Kortista lukijalaitteeseen:

- **Bittitasoinen tiedonsiirtonopeus.** Sama kuin toisessa suunnassa eli noin 106 kbit/s alustuksen ja yhteentörmäyksen aikana.
- **Kuormituksen modulaatio.** Kortin kommunikaatio lukijalaitteen kanssa perustuu alikantaaltoon joka syntyy kun kortti kytkee päälle ja pois sisäisen kuorman ja näin ollen muuttaa lukijalaitteen generoiman kentän kuormituksen. Alikantaallon taajuus on noin 847 kHz ja alustamisen ja törmäysten hallinnan ajaksi yhden bitin kesto on 8 alikantaallon jaksoa. Jokainen bitti alkaa määrättyssä suhteessa alikantaaltoon: bittijakso alkaa alikantaallon kuormitustilassa.
- **Bittiesitys ja koodaus.** Bitit koodataan Manchester koodauksen mukaisesti. Standardi määrittelee kolme erilaista sekvenssiä modulaatio/ei modulaatiota, jotka voivat esiintyä bitin keston aikana ja joiden avulla esitetään/koodataan bittien loogiset tilat, kommunikoinnin aloitus, lopetus ja informaation puute.

- **B -tyypin kommunikaatiosignaalin rajapinta.** Standardissa määritellään yksityiskohtaisesti signaalin rajapinnan ominaisuudet molemmissa suunnissa (lukijalaitteesta kortille ja kortilta lukijalaitteeseen): bittitaso tiedonsiirtonopeus, modulaatio, bittiesitystapa ja koodaus.

Lukijalaitteesta korttiin:

- **Bittitasoinen tiedonsiirtonopeus.** Noin 106 kbit/s alustuksen ja törmäysten hallinnan aikana (eli sama kuin A-tyypin).
- **Modulaatio.** Lukijalaitteesta korttiin kommunikaatio perustuu RF-kentän ASK10% mukaiseen modulointiin eli lukijalaite vaientaa radiotaajuuden kentän vain 10 prosentin verran tauon luomiseksi.
- **Bittiesitys ja koodaus.** NRZ-L koodaus jossa looginen "1" on sama kuin ei modulointia (kantaallon korkeataso) ja looginen "0" on sama kuin 10 % modulointi (kantaallon matalataso).

- Kortista lukijalaitteeseen:

- **Bittitasoinen tiedonsiirtonopeus.** Sama kuin toisessa suunnassa eli noin 106 kbit/s alustuksen ja yhteentörmäyksen aikana (eli sama kuin A-tyypin).
- **Kuormituksen modulaatio.** Sama periaate kuin A-tyypin. Kortin kommunikaatio lukijalaitteen kanssa perustuu alikantaaltoon, joka syntyy kun kortti kytkee päälle ja pois sisäisen kuorman ja näin ollen muuttaa lukijalaitteen generoiman kentän kuormituksen.

Alikantoaallon taajuus on noin 847 kHz ja alustamisen ja törmäysten hallinnan ajaksi yhden bitin kesto on 8 alikantoaallon jaksoa. Kortti generoi alikantoaallon vain kun se lähettää tietoa. Alikantoaalto on vaihemoduloitu ja vaiheen muutos tapahtuu vain määrättyssä paikoissa (nominal positions) suhteessa alikantoaaltoon.

- **Bittiesitys ja koodaus.** Bitit koodataan NRZ-L koodauksen mukaisesti. Standardi määrittelee eri tilat vaiheen muutoksina.

- **Kortin (PICC) vähimmäiskytkentäalue.** Kortin antennin muodon ja sijainnin on oltava sellaisia, että antenni ympäröi pienen alueen jonka keskipiste on ISO 7816-2 mukaisen kontaktien muodostaman keskipiste. Vaatimus on sama molemmille korttityypeille.

3.3. ISO/IEC 14443-3

Tämä standardin osa määrittelee alustuksen ja törmäysten hallinnan:

- **Pollaus.** Moduloimattomassa kentässä olevan kortin tulee kyetä hyväksymään pyyntö 5 ms sisällä. Jotta lukijalaite pystyisi havaitsemaan kenttään tulevia kortteja, sen tulee lähettää toistuvasti Request- eli pyyntö- komentoja ja odottaa ATQ vastausta. Request –komennot lähetetään molemmille korttityypeille (REQA ja REQB) missä hyvänsä järjestyksessä. Menettelyä kutsutaan pollaukseksi.

- **A-tyypin alustus ja törmäysten hallinta.** Standardissa määritellään yksityiskohtaisesti alustuksen ja törmäysten hallintaan liittyvät A-tyypin ominaisuudet:
 - **Tavu-, kehys- ja komentoformaatti ja ajastukset (timing).** Standardi määrittelee yksityiskohtaisesti kaikki tarvittavat formaatit ja ajastukset, mukaan lukien kehykset REQA ja WAKE-UP (Herätys) komennoille, joita käytetään kommunikoinnin aloittamiseen ja herättämiseen, ja vakiokehys normaaliin tiedon vaihtoon, ja kehys bittipohjaiselle törmäysten hallinnalle. Lisäksi standardi määrittelee tiedonvaihdossa käytettävän virheentunnistusmenetelmän (CRC_A).

 - **Kortin toimintatilat.** Standardi määrittelee kortin eri toimintatilat ja niiden väliset suhteet, eli miten siirrytään tilasta toiseen komentojen avulla. Kortin toimintatilat ovat:
 - **POWER-OFF** (Teho Pois). Tässä tilassa kortti ei saa energiaa;
 - **IDLE** (Tyhjäkäynti). Tässä tilassa kortti saa energiaa, kykenee demoduloimaan ja tunnistamaan korttilaitteen lähettämiä REQA ja WUPA -komentoja;
 - **READY** ja **READY*** (Valmis). Kortti siirtyy tähän tilaan heti saatuaan hyväksyttävän REQA tai WUPA –komennon. Kortti siirtyy pois tästä tilasta, kun se on tullut valituksi sen omalla tunnisteella (UID). Tässä tilassa sovelletaan törmäysten hallintamenettelyä;
 - **ACTIVE** ja **ACTIVE*** (Aktiivinen). Kortti siirtyy tähän tilaan, kun se on tullut valituksi sen omalla tunnisteella (UID);
 - **HALT** (Pysähtynyt). Kortti siirtyy tähän tilaan joko saatuaan HALT -komennon tai jonkin muun sovelluskohtaisen komennon, jota tämä standardi ei määrittele. Tässä tilassa kortti vastaa vain WUPA komentoon, joka saa kortin siirtymään READY tilaan.

 - **Komennot.** Standardi määrittelee komennot, joita lukijalaite käyttää hoitaakseen viestinnän useamman kortin kanssa:
 - **REQA** (A-Pyyntö) ja **WUPA** (Herätys). Lukijalaite lähettää nämä komennot selvittääkseen onko kentässä A-tyyppinen kortti tai A-tyyppisiä kortteja. Komennot

lähetetään lyhyessä kehyksessä. Lukijalaite lähettää WUPA komennon siirtääkseen HALT-tilassa olevat A-kortit takaisin READY*-tilaan, jotta ne osallistuisivat tuleviin törmäysten hallinta- ja valintamenettelyihin. Standardi määrittelee komentojen formaatin.

- **ANTICOLLISION** (Törmäysten hallinta) ja **SELECT** (Valinta). Näitä käytetään törmäysten hallinnan silmukassa, johon vaikutetaan komentojen sisältämällä parametreillä;
 - **HLTA** (Pysähdys).
- **Valintasekvenssi.** Standardi määrittelee yksityiskohtaisesti kortin valintaan liittyvät komennot ja vasteet, sekä törmäysten hallintaan liittyvät mekanismit.
- Lukijalaitteen lähettämän REQA eli A-Pyyntö komennon seurauksena kortit vastaavat samanaikaisesti ATQR:lla (Vastauksella A-Pyynnölle), joka koodaa sovellettavan törmäysten hallinnan tyyppin kahdessa tavussa. Jos useampi kortti vastaa, törmäyksiä saattaa esiintyä ja on lukijalaitteen vastuu selvittää törmäykset;
 - Bittikehykseen perustuvassa törmäysten hallinnassa käytettävä algoritmi (anticollision loop) ja lukijalaitteen ja korttien lähettämät tiedot on standardissa määritelty;
- **B-tyyppin alustus ja törmäysten hallinta.** Standardissa määritellään yksityiskohtaisesti alustuksen ja törmäysten hallintaan liittyvät B-tyyppin ominaisuudet:
- **Tavu-, kehys- ja komentoformaatti ja ajastukset (timing).** Standardi määrittelee yksityiskohtaisesti kaikki tarvittavat tavujen ja kehysten formaatit ja ajastukset. Lisäksi standardi määrittelee tiedonvaihdossa käytettävän virheetunnistusmenetelmän (CRC_B).
 - **Törmäysten hallintasekvenssi.** Törmäysten hallinta perustuu aika-aukkoihin (time slot) joiden puitteissa kortit saavat vastata minimitiedoilla. Käytävissä olevat komennot mahdollistavat eri törmäysten hallintastrategioiden toteuttamisen lukijalaitteen tasolla.
 - **Kortin toimintatilat.** Standardi määrittelee kortin eri toimintatilat ja niiden väliset suhteet, eli miten siirrytään tilasta toiseen komentojen avulla. Kortin toimintatilat ovat:
 - **POWER-OFF** (Teho pois). Tässä tilassa kortti ei saa energiaa;
 - **IDLE** (Tyhjäkäynti). Tässä tilassa kortti saa energiaa, kykenee demoduloimaan ja tunnistamaan korttilaitteen lähettämiä REQB tai WUPB -komentoja;
 - **READY-REQUESTED** (Valmis-pyydetty). Kortti saa energiaa ja on vastaanottanut hyväksyttävän REQB tai WUPB komennon kontrolliparametrillä N. Kortti laskee satunnaisluvun R, jota käytetään jälkeisen toiminnan kontrollissa;
 - **READY-DECLARED** (Valmis-Ilmoitettu). Kortti saa energiaa ja on lähettänyt ATQB vastauksensa viimeiselle hyväksyttävälle REQB/WUPB komennolle;
 - **ACTIVE** (Aktiivinen). Kortti siirtyy tähän tilaan, kun se on saanut korttinumeron (CID) hyväksyttävällä ATTRIB komennolla;
 - **HALT** (Pysähtynyt). Tässä tilassa kortti vastaa vain WUPB komentoon, joka saa sen siirtymään IDLE tilaan. Mikäli kortti ei saa enää energiaa, se siirtyy POWER-OFF – tilaan.
 - **Komennot.** Standardi määrittelee komennot, joita lukijalaite käyttää hoitaakseen viestinnän useamman kortin kanssa:

Jotta törmäysten hallinnan komennot erottuisivat sovelluskomennoista, kaikki törmäysten hallinnan komennot alkavat erityisellä sekvenssillä.

Standardi määrittelee seuraavat peruskomennot ja niiden parametrit kommunikointikanavien hallintaa varten:

- **REQB/WUPB** (B-Pyyntö/ B-Herätys). Lukijalaite lähettää tämän komennon selvittääkseen onko kentässä B-tyyppisiä kortteja. Lisäksi WUPB käytetään erityisesti herättämään HALT tilassa olevia kortteja. REQB sisältää CRC_B (virheentunnistusmenetelmän) kahden tavun lisäksi kolme parametriä, joilla voidaan mm. vaikuttaa tiettyä sovellusperhettä edustavan kortin valintaan ja törmäysten hallintaan;
- **Slot-MARKER**. REQB komennon jälkeen lukijalaite lähettää Slot-MARKER komentoja, joilla se merkitsee aika-aukkojen alkamiset;
- **ATQB** (vastaus B-pyynnölle). Tämä on kiinteäpitäinen (15 tavua) ja kestoltaan rajattu vastaus sekä REQB että Slot-Marker komennoille. ATQB sisältää erilaisia parametrejä kuten Näennäiskorttitunnus (jolla erotetaan kortit toisistaan törmäysten hallinnan aikana), Sovellustieto (jolla kortti kertoo lukijalaitteelle mitä sovelluksia se sisältää), ja Protokollainfo (joka kertoo sellaisista kortin tarjoamista ominaisuuksista kuten kommunikointinopeudesta, kehyksen enimmäiskoosta ja protokollatyypistä);

HUOM! Tämä standardin osa mahdollistaa erilaisia kortin ja lukijalaitteen välisiä kommunikointinopeuksia, 847 kbit/s asti.
--

- **ATTRIB**. Tämä komento sisältää kortin valinnan vaatimat tiedot: mm. Tunnus (PUPIN eli näennäiskorttitunnuksen arvo kortin lähettämässä ATQB –vastauksessa, eri ajastusten arvoja, lukijalaitteen tukema kehyksen enimmäiskoko ja kommunikointinopeudet;
- **Answer to ATTRIB**. Kortti on velvollinen vastaamaan ensimmäiselle hyväksyttävälle ATTRIB komennolle, joka sisältää sen tunnuksen. Oikein formatoitu vastaus ATTRIB komennolle on se keino, jolla lukijalaite tietää, että kortin valinta on onnistunut;
- **HLTB**. Lukijalaite lähettää tämän komennon siirtääkseen kortin Pysähdys-tilaan, josta se saa vastata ainoastaan WUPB komennolle. Kortti kuittaa komennon lähettämällä vastauksen;

Lisäksi lopussa on eri informatiivisissa liitteissä esimerkkejä kommunikoinnista lukijalaitteen ja A-korttityypin välillä, virheentunnistusmenetelmien toteutuksesta, aika-aukkoihin perustuvasta törmäysten hallinnasta, jota voi soveltaa A-korttityypeille ja yksityiskohtaisesta A-korttityypin tilakaaviosta.

3.4. ISO/IEC 14443-4

Tämä standardin osa määrittelee vuorosuuntaisen (half-duplex) lohkotiedonsiirtoprotokollan, joka huomioi kontaktittoman yhteyden erityistarpeet, sekä sekvenssin protokollan aktivoinnille ja deaktivoinnille.

- **Protokollan aktivointi A-korttityypille**. Standardissa määritellään yksityiskohtaisesti komennot ja vasteet, joilla protokolla aktivoidaan tilakaavioineen ja parametreineen. Kortin onnistuneen aktivointisekvenssin (Request, Anticollision loop ja Select) jälkeen, lukijalaite pyytää kortilta lisää tietoja RATS (Request for answer to select) komennolla, ja kortti voi vastata lähettämällä ATS (Answer to select) vastauksen. Mikäli kortti kertoo ATS - vastauksessa tukevansa muutettavia parametrejä lukijalaite voi lähettää PPS (Protocol and Parameter Selection) komennon muuttaakseen parametrit. Kortin ei tarvitse tukea PPS menettelyä, jos se ei sisällä muutettavia parametrejä.

- **RATS (Request for answer to select).** RATSin avulla korttilaite välittää tiedon siitä, mikä on sen tukema kehyksen enimmäiskoko sekä kortille myönnetty loogisen kanavan numero;
 - **ATS (Answer to Select).** ATS:ssä kortti välittää korttilaitteelle tietoa sen tukemista tiedonsiirtoprotokollan ominaisuuksista, kuten esim. tiedonsiirtonopeudet. Lisäksi ATS voi myös sisältää valinnaisia historiaavuja (sisältö määritelty ISO/IEC 7816-4 standardissa);
 - **PPS (Protocol and Parameter Selection).** PPS:ä käytetään muuttamaan tiedonsiirtoprotokollan ominaisuudet, lähinnä käytettävät tiedonsiirtonopeudet;
 - Lisäksi standardi määrittelee enimmäisajan, joka saa kulua ennen kuin kortti vastaa lukijalaitteelle, sekä virhehallinnan ja toipumismenettelyn.
- **Protokollan aktivointi B-korttityypille.** Aktivointi on määritelty ISO/IEC 14443-3 osassa.
 - **Vuorosuuntainen lohkotiedonsiirtoprotokolla.** Standardi määrittelee lohkojen rakenteen, kehyksen odotusajan (Frame waiting time), energiatason indikaattorin ja protokollan toimintaperiaatteet:
 - **Lohkorakenne (Block format).** Lohkorakenne koostuu 3 kentästä: Prologue, Information ja Epilogue. Ensimmäinen sisältää protokollan kontrolliin tarvittavan tiedon. Toinen sisältää välitettävän tiedon ja viimeinen sisältää virhehallinnan ja korjauksen tarkisteen;
 - **Kehyksen odotusaika (Frame waiting time).** Määrittelee maksimian, joka saa kulua ennen kuin kortti lähettää vastauksen lukijalaitteelle. Minimiarvo on noin 302 µs, maksimiarvo n. 4949 µs ja oletusarvo n. 4833 µs. Kehyksen odotusaika käytetään tiedonsiirtovirheen tai vastaamattoman kortin tunnistamiseksi;
 - **Energiatason indikaattori (Power level indicator).** Kaksi bittiä, joilla kortti voi kertoa havaitsemastaan energiatasosta;
 - **Protokollan toimintaperiaatteet (Protocol operation).** Protokolla on vuorosuuntainen ja lukijalaite hallitsee yhteyden. Protokolla mahdollistaa moniaktiivisuuden (jossa useampi kortti on samanaikaisesti ACTIVE tilassa), ketjutuksen (jolla siirretään tieto, joka ei mahdu yhteen lohkoon) ja virhehallinnan ja toipumisen. Lisäksi standardi määrittelee lohkojen numeroinnin periaatteet.
 - **Protokollan deaktivointi A- ja B-korttityypille.** Deaktivointi tapahtuu DESELECT komennolla. Standardi määrittelee myös Deaktivoinnille kehyksen odotusajan (n. 4833 µs) ja virhehallinnan ja toipumisen;

Lisäksi lopussa on eri informatiivisissa liitteissä esimerkkejä aktiivisuudesta, protokollaskenaarioista ja lohko- ja kehyskoodauksesta.

3.5. ISO/IEC 10373-6

Tämä standardin osa määrittelee testausmenetelmät lähilukukorteille (ISO/IEC 14443 mukaisille korteille).

Standardin määrittelemät testausmenetelmät käsittävät seuraavat alueet:

- **Oletusarvoiset olosuhteet testauksille.** Mm. arvot lämpötilalle, suhteelliselle kosteudelle ja toleransseille;
- **Staattinen sähkö.** Sovellettava testausmenettely, jolla selvitetään kortin käyttäytymistä staattisessa sähköisessä kentässä;
- **Testilaitteisto ja testipiirit.** Standardi määrittelee sellaiset asiat kuin kalibrointikään mitat ja ominaisuudet, testilukijalaitteen kokoonpanon ja rakenteen, referenssikortit, vaatimukset käytettävälle digitaaliselle oskilloskoopille;
- **Toiminnallinen testi kortille.** Standardi määrittelee sekä testimenettelyn että raportin kirjoitettavat asiat;

- **Toiminnallinen testi lukijalaitteelle.** Standardi määrittelee sekä testimenettelyn että raporttiin kirjoitettavat asiat. Testattavat asiat ovat: korttilaitteen kentän voimakkuus, energian siirto korttilaitteelta kortille, kuormamoduloinnin vastaanotto (ainoastaan informatiivinen);

Lisäksi lopussa on normatiivisissa liitteissä tarkka kuvaus käytettävästä lukijalaitteen testiantennista, ilmaisinkäämistä ja referenssikortista sekä eri informatiivisissa liitteissä kuvauksia lukijalaitteen testiantennin virittämismenettelystä ja referenssikortista kuormamoduloinnin testausta varten.

4. MITÄ ON VIELÄ TEKEILLÄ

Nykyisten lähilukukortteja koskevien standardien ISO/IEC 14443 ja ISO/IEC 10373-6 jatkokehitys tapahtuu seuraavilla alueilla:

ISO/IEC 14443

Suurempia tietomääriä käsittelevät nykyiset sovellukset vaativat myös nopeita käsittelytapahtumia. Standardin jatkotyössä määritellään parannuksia (amendments), joilla mahdollistetaan suurempia tiedonsiirtonopeuksia kortin ja lukijalaitteen välillä. 212 kbit/s - 848 kbit/s tiedonsiirtonopeuksille valintamekanismi on jo määritelty ISO/IEC 14443-3 ja 14443-4 standardiosissa. Vain signaalirajapinta (signal interface) jää tarkemmin määriteltäväksi ISO/IEC 14443-2 standardiosassa. 1,7 Mbit/s suuremmille tiedonsiirtonopeuksille on vielä määriteltävä sekä valintamekanismi että signaalirajapinta.

Ensimmäiset luonnokset (drafts) ja ehdotus uudelle työkohteelle on jo laadittu.

ISO/IEC 10373-6

Standardin jatkotyössä määritellään parannuksia (amendments), jotka kohdistuvat:

- 1) uusiin kortin testimenettelyihin (Additional PICC test methods - Draft ISO/IEC 10373-6/P-DAM1),
- 2) parannettuihin RF testimenettelyihin (Improved RF test methods - Draft CD 10373-6/AMD2),
- 3) uusiin lukijalaitteen testimenettelyihin (Additional PCD test methods - Draft ISO/IEC 10373-6/P-DAM3)

5. LUKIJALAITTEIDEN SOPIVUUDESTA – ELI MIHIN KANNATTA KIINNITTÄÄ HUOMIOTA

5.1. Yleistä

ISO/IEC 14443 standardisarja keskittyy määrittelemään lähilukuteknologiaan perustuvien korttien ominaisuudet. Osa ominaisuuksista on valinnaisia ja siten standardisarja mahdollistaa eri tasoisia korttitoteutuksia. Koska standardisarja ei määrittele korttilaitteelle asetettavia vaatimuksia, jotka kattaisivat korttien kaikki valinnaiset ominaisuudet on seurauksena näin ollen periaatteessa mahdollista toteuttaa standardin mukainen korttilaite, jonka ominaisuudet riittävät joidenkin korttien käsittelyyn, mutta osoittautuu sittenkin riittämättömäksi hyödyntämään seuraavien korttisukupolvien standardin mukaisia kehittyneitä ominaisuuksia.

5.2. Esimerkkejä lukijalaitteen ominaisuuksista, joihin kannattaa kiinnittää erityistä huomiota

Seuraavassa pari esimerkkiä lukijalaitteen ominaisuuksista, joihin kannattaa kiinnittää erityistä huomiota:

Type A:

Tuki Time slot detection protokollalle,
tuki 106Kbits/s suuremmille tiedonsiirtonopeuksille molempiin suuntiin.

Type B:

Tuki 106Kbits/s suuremmille tiedonsiirtonopeuksille (106Kbits/s ... 847 Kbit/s) molempiin suuntiin,
tuki eri maksimikokoisille kehyksille (16 bytes ... 256 bytes).

6. LYHENTEET

CICC	Closed-coupled cards
PICC	Proximity cards
VICC	Vicinity cards
PCD	Proximity Coupling Device - Lähilukulaite
ISO	International Standards Organisation
IEC	
RF	Radiotaajuinen (Radio frequency)
ASK	Amplitude shift keying
BPSK	Binary phase shift keying
NRZ-L	Non-return to zero, (L for Level)
ATQ	Answer To Request

7. VIITTEET

Close-coupled cards

- [1] ISO/IEC 10536-1 Identification cards – Contactless integrated circuit(s) cards – Close-coupled cards – Part 1: Physical characteristics
- [2] ISO/IEC 10536-2 Identification cards – Contactless integrated circuit(s) cards – Close-coupled cards – Part 2: Dimensions and location of coupling areas
- [3] ISO/IEC 10536-3 Identification cards – Contactless integrated circuit(s) cards – Close-coupled cards – Part 3: Electronic signals and reset procedures

Proximity cards

- [4] ISO/IEC 14443-1 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics
- [5] ISO/IEC 14443-2 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface
- [6] ISO/IEC 14443-3 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialisation and anticollision
- [7] ISO/IEC 14443-4 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

Vicinity cards

- [8] ISO/IEC 15693-1 Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 1: Physical characteristics
- [9] ISO/IEC 15693-2 Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 2: Air interface and initialisation
- [10] ISO/IEC 15693-3 Identification cards – Contactless integrated circuit(s) cards – Vicinity cards – Part 3: Anticollision and transmission protocol

Test methods

- [11] ISO/IEC 10373-6 Identification cards – Test methods – Part 6: Proximity cards
- [12] ISO/IEC 10373-7 Identification cards – Test methods – Part 7: Vicinity cards

LIITE 1 – ISO/IEC 14443 STANDARDI JA PATENTITKYSYMYKSET

ISO/IEC 14443 mukaisten korttien käyttämiin menetelmiin ja ratkaisuihin liittyy usein patenteja, niin A kuin B korttityyppien osalta. Standardin osat 2-4 sisältävät tietoa niihin liittyvistä patenteista.

Lisää informaatiota saa seuraavista osoitteista:

ISO/IEC 14443-2

- 1) Patentit, joiden haltijat ovat vakuuttaneet ISO ja IEC standardointijärjestöille, että heiltä löytyy halukkuutta neuvotella lisenssien myöntämisestä halukkaiden kanssa ympäri maailmaa ketään diskriminoimatta.

FRANCE TELECOM

Branch Développement
Centre National d'Etudes des Télécommunications
38-40 rue du Général Leclerc
92794 Issy-les-Moulineaux
Cedex 9
France

INNOVOTRON

Director of International Operations
Innovotrol
1 Rue Danton
75006 Paris
France

MOTOROLA

Motorola ESG
207 route de Ferney
P.O. Box 15
1218 Grand-Saconnex
Switzerland

OMRON

Intellectual Property Department
Law & Intellectual Property H.Q.
20, Igadera Shimokaiinji
Nagaokakyo City
Kyoto 617-8510
Japan

ON-TRACK INNOVATIONS

Z.H.R. Industrial Zone
P.O. Box 32
Rosh-Pina 12000
Israel

PHILIPS

Director
Koninklijke Philips Electronics N.V.

P O Box 32
5600 AE Eindhoven
The Netherlands

SONY CORPORATION

Intellectual Property Department
Communications Systems Solutions
Network Co.
6-7-37 Kitashinagawa
Shinagawa-ku
Tokyo, 141-0001
Japan

- 2) Seuraavat organisaatiot saattavat omistaa ISO/IEC 14443-2 liittyviä patenteja, mutta eivät ole antaneet tietoja eivätkä sitoutuneet myöntämään lisenssejä.

WAYNE S FOLETTA

4760 Castlewood Drive
San Jose, California CA 9512

JOHN W HALPERN

C/O Vincent M DeLuca
Rothwell, Figg, Ernst & Kurz, p.c.
555 Thirteenth Street, N.W.
Suite 701 East Tower
Washington, D.C. 20004

MAGELLAN CORPORATION

8717 Research Drive
Irvine
CA 92618
USA

- 3) Lisäksi standardin osassa on muistutus siitä, että on mahdollista, että standardiosaan liittyy muita patenteja kuin edellä mainitut.

ISO/IEC 14443-3

- 1) Patentit, joiden haltijat ovat vakuuttaneet ISO ja IEC standardointijärjestöille, että heiltä löytyy halukkuutta neuvotella lisenssien myöntämisestä halukkaiden kanssa ympäri maailmaa ketään diskriminoimatta.

CASIO

General Manager
Intellectual Property Centre
Casio Computer Co. Ltd
Hamura R & D Center
2-1 Sakae-cho 3Chome
Hamura-Shi
Tokyo 205-8555

Japan

FRANCE TELECOM
Branch Développement
Centre National d'Etudes des Télécommunications
38-40 rue du Général Leclerc
92794 Issy-les-Moulineaux
Cedex 9
France

INNOVOTRON
Philippe le Clech
Director of International Operations
Innovotrol
1 Rue Danton
75006 Paris
France

MOTOROLA
Motorola ESG
207 route de Ferney
P.O. Box 15
1218 Grand-Saconnex
Switzerland

ON-TRACK INNOVATIONS
Z.H.R. Industrial Zone
P.O. Box 32
Rosh-Pina 12000
Israel

PHILIPS
Director Philips Corporate Intellectual Property
Koninklijke Philips Electronics N.V.
P O Box 32
5600 AE Eindhoven
The Netherlands

2) Seuraavat organisaatiot saattavat omistaa ISO/IEC 14443-2 liittyviä patenteja, mutta eivät ole antaneet tietoja eivätkä sitoutuneet myöntämään lisenssejä.

WAYNE S FOLETTA
4760 Castlewood Drive
San Jose, California CA 9512
USA

JOHN W HALPERN
C/O Vincent M DeLuca
Rothwell, Figg, Ernst & Kurs, p.c.
555 Thirteenth Street, N.W.
Suite 701 East Tower
Washington, D.C. 20004

MAGELLAN CORPORATION

8717 Research Drive
Irvine
CA 92618
USA

- 3) Lisäksi standardin osassa on muistutus siitä, että on mahdollista, että standardiosaan liittyy muita patenteja kuin edellä mainitut.

ISO/IEC 14443-4

- 1) Patentit, joiden haltijat ovat vakuuttaneet ISO ja IEC standardointijärjestöille, että heiltä löytyy halukkuutta neuvotella lisenssien myöntämisestä halukkaiden kanssa ympäri maailmaa ketään diskriminoimatta.

FRANCE TELECOM

Branch Développement
Centre National d'Etudes des Télécommunications
38-40 rue du Général Leclerc
92794 Issy-les-Moulineaux
Cedex 9
France

MOTOROLA

Motorola ESG
207 route de Ferney
P.O. Box 15
1218 Grand-Saconnex
Switzerland

OMRON

Intellectual Property Department
Law & Intellectual Property H.Q.
20, Igadera Shimokaiinji
Nagaokakyo City
Kyoto 617-8510
Japan

ON-TRACK INNOVATIONS

Z.H.R. Industrial Zone
P.O. Box 32
Rosh-Pina 12000
Israel

- 2) Seuraavat organisaatiot saattavat omistaa ISO/IEC 14443-2 liittyviä patenteja, mutta eivät ole antaneet tietoja eivätkä sitoutuneet myöntämään lisenssejä.

WAYNE S FOLETTA

4760 Castlewood Drive
San Jose, California CA 9512

JOHN W HALPERN

C/O Vincent M DeLuca
Rothwell, Figg, Ernst & Kurz, p.c.
555 Thirteenth Street, N.W.
Suite 701 East Tower
Washington, D.C. 20004

MAGELLAN CORPORATION

8717 Research Drive
Irvine
CA 92618
USA

- 3) Lisäksi standardin osassa on muistutus siitä, että on mahdollista, että standardiosaan liittyy muita patenteja kuin edellä mainitut.