125 135 Khz buta tagek kivaltani a vonalkodok, mindent kiköp, egyedi chip azonosító, bárki leolvashatja.

13.5 Mhz Okos tagek, több funkció, security korlatozas, java nyelven is lehet programozni, amit futtat

e-útlevel 2004-2005 óta létezik. 13.5 Mhz-en működik, először csak személyes adatok, és arckép, ez ami stabdardizált, 2009 ápr. óta újlenyomat is.

RFIDI0T nevű csomag. mrpkey az alap program.

beirni utlevel szam, születesi datum (921127 formában).

EF\_COM: a chipen található fileok listája, nincs titkosítva

EG\_DG1: első adatcsoport, személyes adatok, nem unicode, csak angol betűk

EG\_DG2: második csoport fénykép

EF\_SOD: aláíró file

Passzív authentikáció, a DG1 és DG2 SHA1 hash-ét tárolja, amit a kiállító privát kulcsával írják alá. a publikus részét pedig mellé teszik.

3DES challange-response alapú protokoll. nincs brute-force elleni védelem. 3-4 karakter felett nem érdemes.

opcionális: active authentication, kiolvasni nem lehet, csak ellenőrizni, hogy létezik-e. ezzel lehet pl ellenőrizni, hogy tényleg útlevélhez van-e. kijátszható, mert a com file mondja meg, hogy van-e, igy átírható.

Extended Access Control: certificate alapú, de csak az ujlenyomatot, és iriszt nézi. com fileval lejátszható, ha azt mondom nincs ilyen file, akkor nem is keresi.

genpassport

PKD tartalmazza az országok publikus kulcsokat. nem használják az országok egyenlőre.