# U-PROX kaardilugejate ja DESFire kaartide seadistusjuhend

**DESFire kaartide kohta leiate allpool üksikasjaliku selgituse erinevate seadistuste kohta:**

1. **AID** autentimisvõtme number (AID auth key number): DESFire salvestab andmeid konkreetsete rakenduste (AID – **Application ID**) sees. Iga rakendus võib sisaldada kuni 14 erinevat krüptograafilist võtit (**nummerdatud 0 kuni 13**). Selle seadistusega määratakse, millist võtme indeksit kaardilugeja peab kasutama autentimiseks ja andmete lugemisõiguse saamiseks.

2. DESFire faili ID (**DESFire File ID**): DESFire rakenduses on andmed organiseeritud failidesse. See ID määrab, milline fail tuleb avada, et lugeda kasutajatunnuseid või läbipääsuandmeid.

3. Lugemine (aadressi järgi / kaardikoodi järgi) (Read – **By address / Card code**): See määrab, kuidas ligipääsuandmed failist välja loetakse. Võimalused on järgmised:

   „**By address**" (aadressi järgi): Kaardilugeja loeb failist kindlat piirkonda (baitide nihke alusel). Tuleb käsitsi määrata täpsed baidid, mida lugeda (näiteks baitidest 0 kuni 4). See annab täieliku kontrolli loetavate andmete üle.

   „**Card code**" (kaardikoodi järgi): Kaardilugeja eeldab, et failis olevad andmed on juba salvestatud standardses läbipääsusüsteemi formaadis (tavaliselt süsteemi enda tarkvara abil väljastatud kaartidel). Sellisel juhul leiab lugeja kaardi identifikaatori automaatselt.

4. Kasuta aadressi (**Use Address**) – aktiveerub, kui on valitud lugemine aadressi järgi. Sellega määratakse täpne baitide vahemik, mis failist välja loetakse.

5. Andmete järjekord sektoris (**The order of data in the sector**) – aktiveerub samuti aadressi järgi lugemise korral. Määrab baitide lugemise ja tõlgendamise järjekorra. See peab vastama kaardi kodeerimisel kasutatud järjekorrale, vastasel juhul loetakse kaardinumber valesti. Võimalused:
   **Big-endian** – kõige olulisem bait loetakse esimesena.
   **Little-endian** – kõige vähem oluline bait loetakse esimesena.

6. DESFire kommunikatsioonirežiim (**DESFire communication mode**): Määrab turvataseme kaardi ja lugeja vahelises andmesides pärast edukat autentimist. Võimalused:
   **Plain** – andmed edastatakse krüpteerimata kujul. Kuigi faili avamiseks kasutati turvavõtit, liiguvad loetavad andmed avatud kujul. Kiireim meetod, kuid haavatav pealtkuulamise suhtes.
   **MACed** (Message Authentication Code) – andmed edastatakse küll krüpteerimata kujul, kuid neile lisatakse krüptograafiline allkiri (MAC), mis tagab andmete tervikluse.
   **Fully Enciphered** (või **Enciphered**) – kõrgeim turvatase. Kogu andmeside on krüpteeritud, tagades nii andmete konfidentsiaalsuse kui ka tervikluse.

7. DESFire autentimisrežiim (**DESFire auth mode**):
   **EV1 Compatible** (Legacy) – kasutab vanemat autentimisprotokolli, mis võeti kasutusele DESFire EV1 kaartidega. Kuigi see kasutab AES krüpteerimist ja on endiselt turvaline, puuduvad uuemad kaitsemehhanismid. Seda tuleks kasutada ainult siis, kui kaardid on kodeeritud EV1 standardi järgi.
   **EV2 Secure Messaging** – uuem autentimisprotokoll, mis võeti kasutusele DESFire EV2 kaartidega ning mida toetavad täielikult ka EV3 kaardid. Pakub paremat kaitset näiteks releerünnakute vastu ning kasutab tugevamaid seansivõtmeid.

8. DESFire peavõti (**DESFire Master Key**): See on kogu füüsilise kaardi kõrgeima taseme administraatorivõti.
   Milleks seda kasutatakse?
   ▪ Kaardi vormindamine – kõigi rakenduste, failide ja andmete kustutamine.
   ▪ Rakenduste loomine või kustutamine – uue AID lisamine või olemasoleva eemaldamine.
   ▪ Peavõtme muutmine – et vältida volitamata vormindamist.
   Oluline teada:
   ▪ Tehaseseadistus – uutel tühjadel DESFire kaartidel on peavõti tavaliselt tehase vaikimisi väärtusega (sageli nullidest koosnev võti, näiteks 0000000000000000).
   ▪ Lukustatud kaardid – kui kaardid on eelnevalt kodeeritud mõne teise tootja või turvafirma poolt, on peavõti tõenäoliselt muudetud salajaseks väärtuseks. Kui seda võtit ei teata, ei ole võimalik kaarte vormindada ega uusi rakendusi lisada.

**MIFARE DESFire EV3 4K kaartide soovituslike parameetrite osas tuleb arvestada, et tegemist on väga paindliku ja keeruka identifitseerimistehnoloogiaga, mis sisaldab failisüsteemi ning suurel hulgal seadistatavaid parameetreid.**

**NÄIDE:**

**Kaardilugejas tuleb seadistada:**

AppID: XXXXXX

Master Key: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB

App Read Key: CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

(Märkus: AppID, Master Key ja App Read Key peavad olema samad, mida kasutati kaartide kodeerimisel.)

**Desktop Reader seadistused:**

Initial issue card code: 174578AB35

(Määrab esimese väljastatava kaardi numbri.)

**DESFire Settings:**

DESFire application name: XXXXXX

Key: YES

Key value: CCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

AID auth key number: 5

DESFire File ID: 1

Read: By address

Use address: 0–5

The order of data in the sector: Little-endian

DESFire communication mode: Enciphered

DESFire auth mode: EV2 Secure Messaging

DESFire master key: YES

Master Key value: BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB