SALTO / DESFire CLONING CHEAT SHEET

Kobe's Keys - Proxmark3 Reference Guide

PHASE 1: SCAN THE FOB

Step	Command	What It Does
1. Card Info	`hf mfdes info`	Shows UID, chip type, apps
2. List Apps	`hf mfdes lsapp`	Shows all AIDs on card

Write down the UID and AID - you need these for the next steps.

PHASE 2: FIND THE KEYS

Command	What It Does
`hf mfdes chk -f mfdes_default_keys --aid [AID]`	Try default keys (no diversification)
`hf mfdes chk -f mfdes_extended_keys.dic --aid [AID] --kdf 1 -i [UID]`	Try with AN10922 diversification
`hf mfdes chk -f mfdes_default_keys --aid [AID] --kdf 2 -i [UID]`	Try with Gallagher diversification

KDF: 0 = None, 1 = AN10922 (Salto common), 2 = Gallagher. If key found, save it!

PHASE 3: AUTHENTICATE & DUMP

Command	What It Does
`hf mfdes auth --aid [AID] -n 0 -t des -k [KEY]`	Auth with DES key
`hf mfdes auth --aid [AID] -n 0 -t aes -k [KEY]`	Auth with AES key
`hf mfdes auth --aid [AID] -n 0 -t aes -k [KEY] --kdf 1 -i [UID]`	Auth with diversified key
`hf mfdes dump --aid [AID] --no-auth`	Dump app data (if open access)
`hf mfdes dump --aid [AID] -t aes -k [KEY]`	Dump app data (with auth)

PHASE 4: WRITE TO BLANK CARD

Command	What It Does
`hf mfdes auth -n 0 -t des -k 0000000000000000`	Auth to blank card PICC
`hf mfdes createapp --aid [AID] --numkeys 1 --ks1 0F`	Create same app structure
`hf mfdes createfile --aid [AID] --fid 01 --size 000020 --rawrights EEEE --amode plain`	Create file in app
`hf mfdes write --aid [AID] --fid 01 --offset 000000 -d [DATA] --no-auth`	Write data to file

Replace [AID], [KEY], [UID], [DATA] with actual values from the original fob.

COMMON SALTO AIDs TO TRY

AID	Notes
`F4B1xx`	Common Salto format
`F5xxxx`	Salto format variant
`2xxxx`	Some Kantech systems

COMMON DEFAULT KEYS

Type	Key	Length
DES	`0000000000000000`	8 bytes
2TDEA	`00000000000000000000000000000000`	16 bytes
AES	`00000000000000000000000000000000`	16 bytes
3TDEA	`000000000000000000000000000000000000000000000000`	24 bytes

QUICK REFERENCE

Term	Meaning
AID	Application ID - 3 bytes identifying the app on card
FID	File ID - identifies files within an app
UID	Unique ID - card serial number (7 bytes for DESFire)
KDF	Key Derivation Function - calculates key from master + UID
AN10922	NXP standard KDF - common for Salto
PICC	Card level (whole card, not specific app)
SAM	Secure Access Module - holds master keys

Save every key you find! Build your database over time.