E-CTF

Visual Representations of
Main Ideas

Entities in our system

Host

host_privkey
host_pubkey
secrets
id →car_pubkey,
car_privkey

Car

host_pubkey
car_pubkey

Paired Fob

car_privkey
PIN

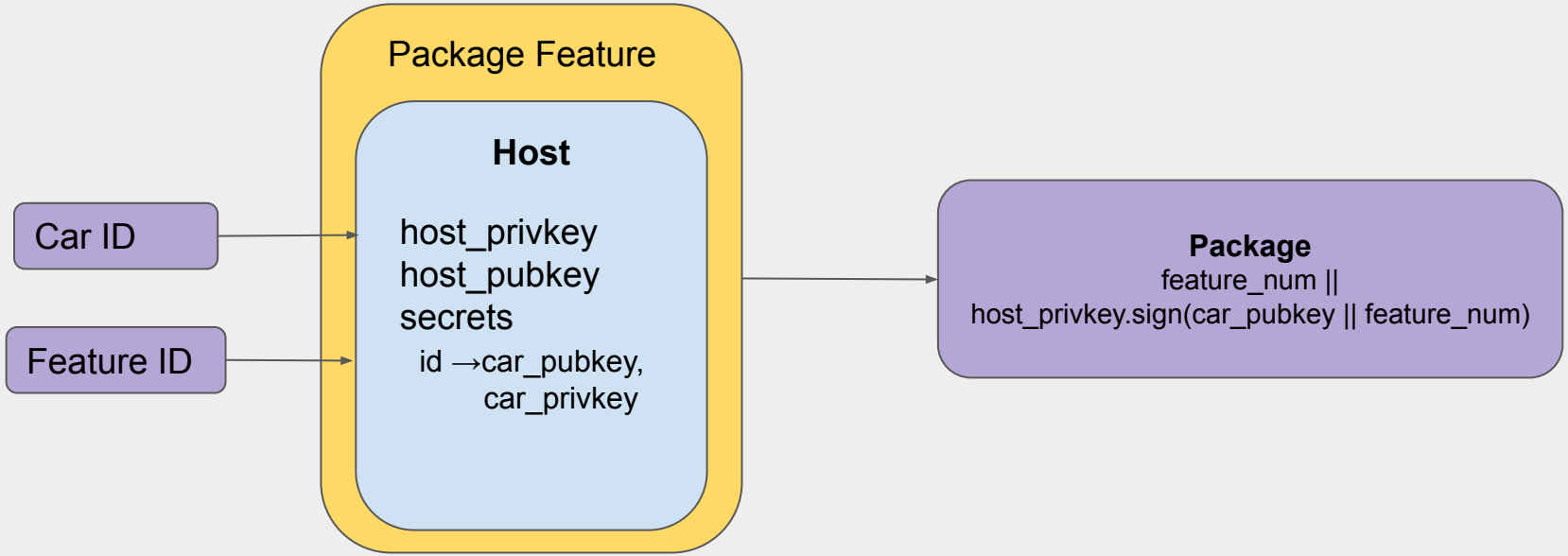
Package 1
Package 2
Package 3

Unpaired Fob

Package
feature_num ||
signature(car_pubkey || feature_num)

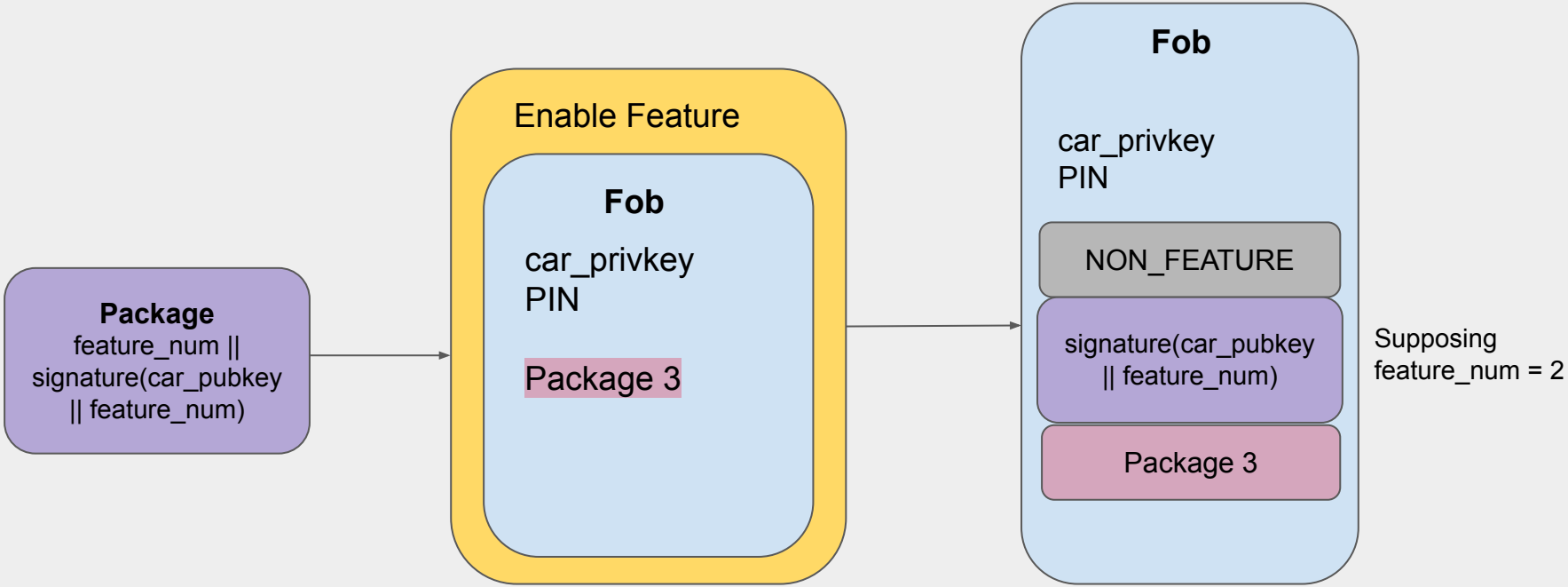
Package feature

Host generates a file containing the feature number followed by (Car Public Key + Feature ID) signed by the host public key.



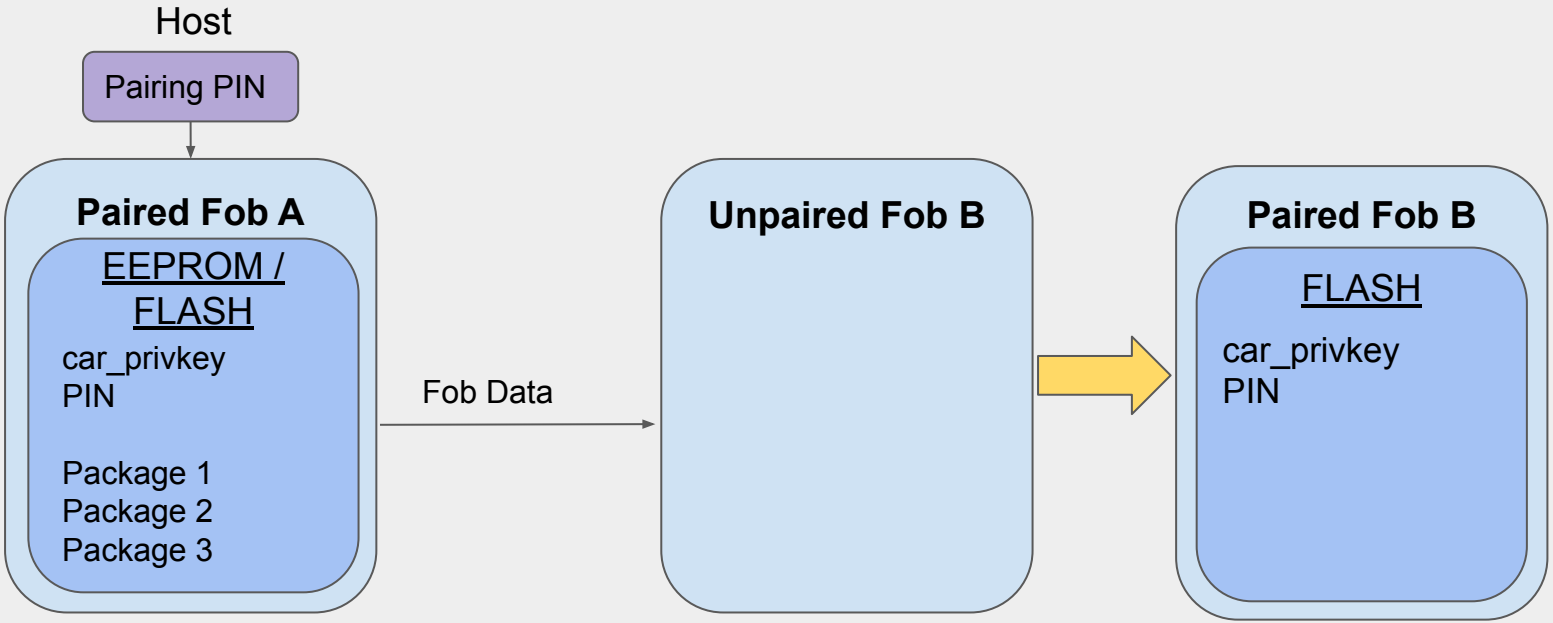
Enable Feature

Fob loads the package into its storage slot in FLASH according to feature number



Pair Fob

On receiving the correct pairing PIN, the paired fob sends its car private key and PIN to the unpaired fob, which stores it in FLASH.



Unlock and Start Car

Car sends Fob a random nonce as a challenge upon unlock request.
Fob signs challenge with car_privkey and sends it back to the car, along with the feature packages.
The car verifies the signature and packages, then prints the unlock and feature messages.