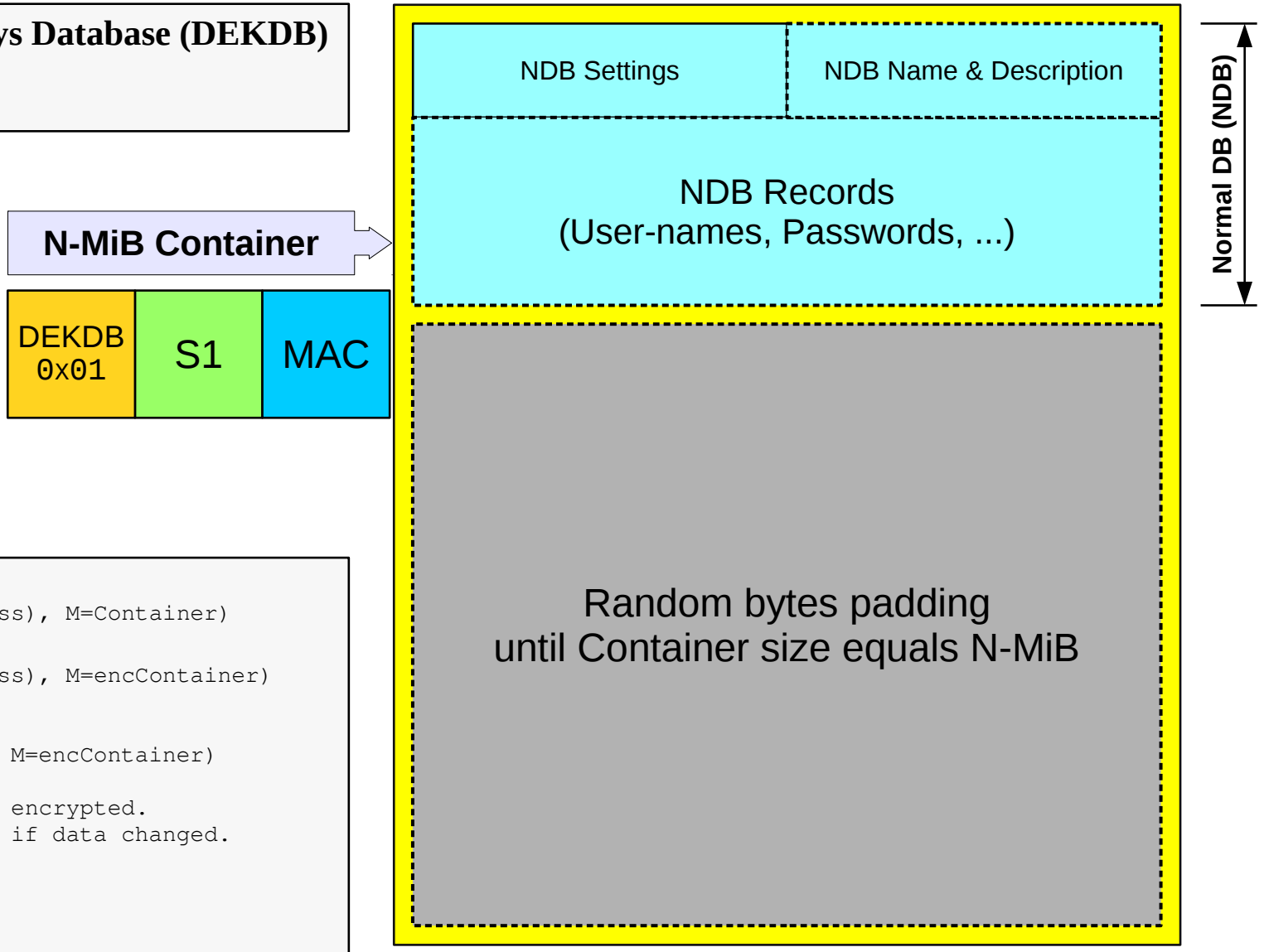
Deniable Encrypted Keys Database (DEKDB)

Normal DB only.

Version 1 – 2016/06



Container encrypt:

Enc(nonce=S1, K=**KDF**(S1,Pass), M=Container)

Container decrypt:

Dec(nonce=S1, K=**KDF**(S1,Pass), M=encContainer)

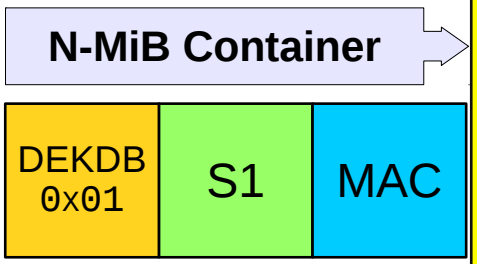
S1: Nonce.
MAC=**MAC256**(K=**KDF**(S1,Pass), M=encContainer)
Container=NDB|Pad
encContainer=The Container encrypted.
S1 and Pad get regenerated if data changed.

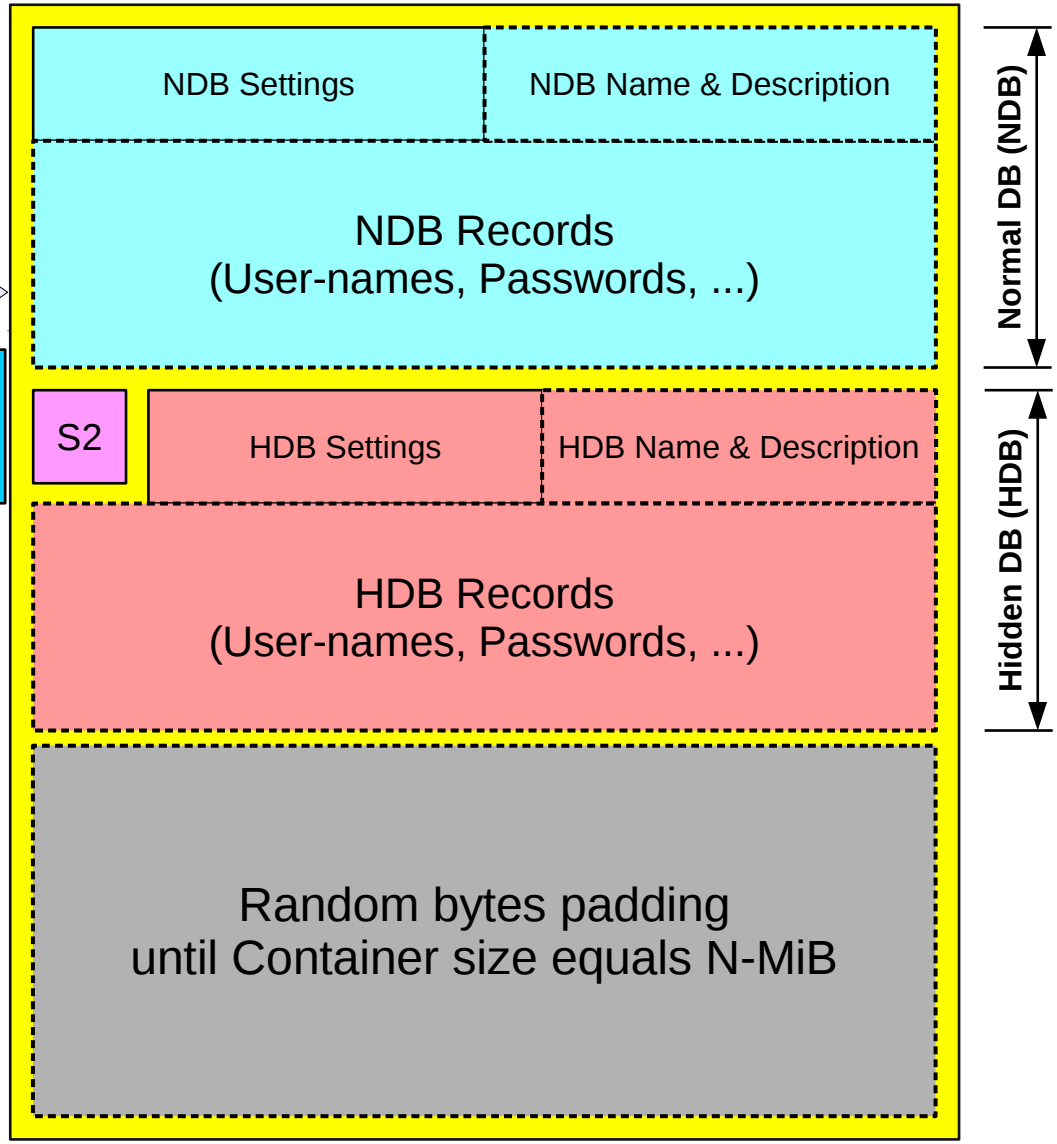
---- Flexible size.
———— Fixed size.

Deniable Encrypted Keys Database (DEKDB)

Normal DB and Hidden DB.

Version 1 – 2016/06





Container encrypt:
Enc(nonce=S1, K=**KDF**(S1,Pass_A), M=Container)

Container decrypt:
Dec(nonce=S1, K=**KDF**(S1,Pass_A), M=encContainer)

Hidden DB (HDB) encrypt:
Enc(nonce=S2, K=**KDF**(S2,Pass_B), M=HDB)

Hidden DB (HDB) decrypt:
Dec(nonce=S2, K=**KDF**(S2,Pass_B), M=encHDB)

S1, S2: Nonces.
MAC=**MAC256**(K=**KDF**(S1,Pass_A), M=encContainer)
Container=NDB|S2|encHDB|Pad
encContainer=The Container encrypted.
encHDB=The HDB encrypted.
S1, S2, and Pad get regenerated if data changed.

---- Flexible size.
———— Fixed size.