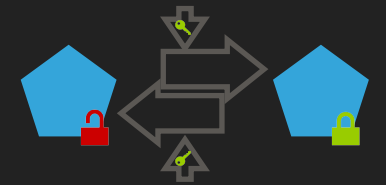


# SOLUTIONS FOR SECURING KEY(S)



## Master key in different storage

E.g. records in DB, master key on filesystem.

Baseline. Easy. Protects (only) against DB theft (e.g. SQL injection)

## Encrypt master key

Use baked in 'obfuscation key' to encrypt master key. Better: Store master key in OS keyring.

Easy. Some protection against FS access (e.g. remote file inclusion)

## Derive per-record key

Unique per record key derived from master key.  
*Bonus: Protect integrity. Bind to record.*

Mostly easy. Protects against some cipher text attacks. Use [AEAD](#)!

## Crypto Host

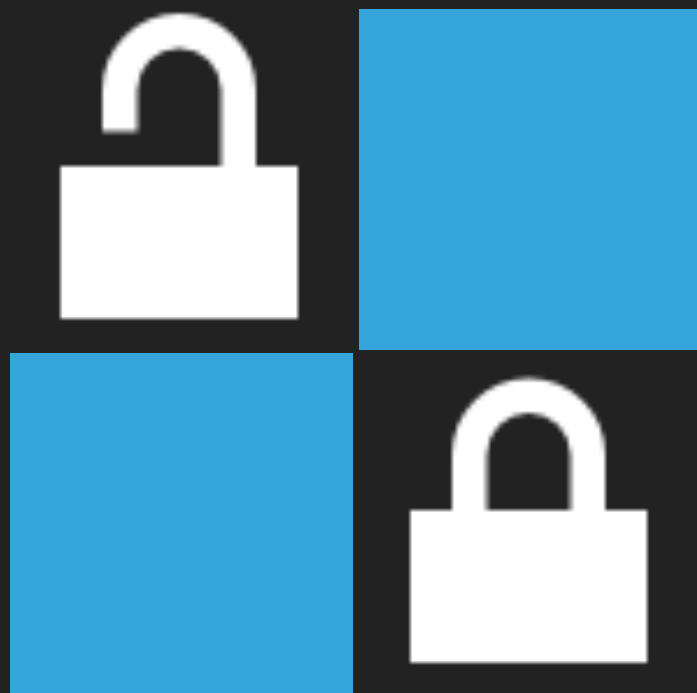
All crypto operations on a dedicated host. (Master)key never leaves Crypto Host.

Depends on architecture. Helps w. key distribution. Makes key theft difficult.

## HSM

Use Hardware Security Module as Crypto Host.

Expensive & difficult. "Crypto Host on steroids".



PATTERNS

---

**KEY DERIVATION 1:  
PASSWORD TO KEY**