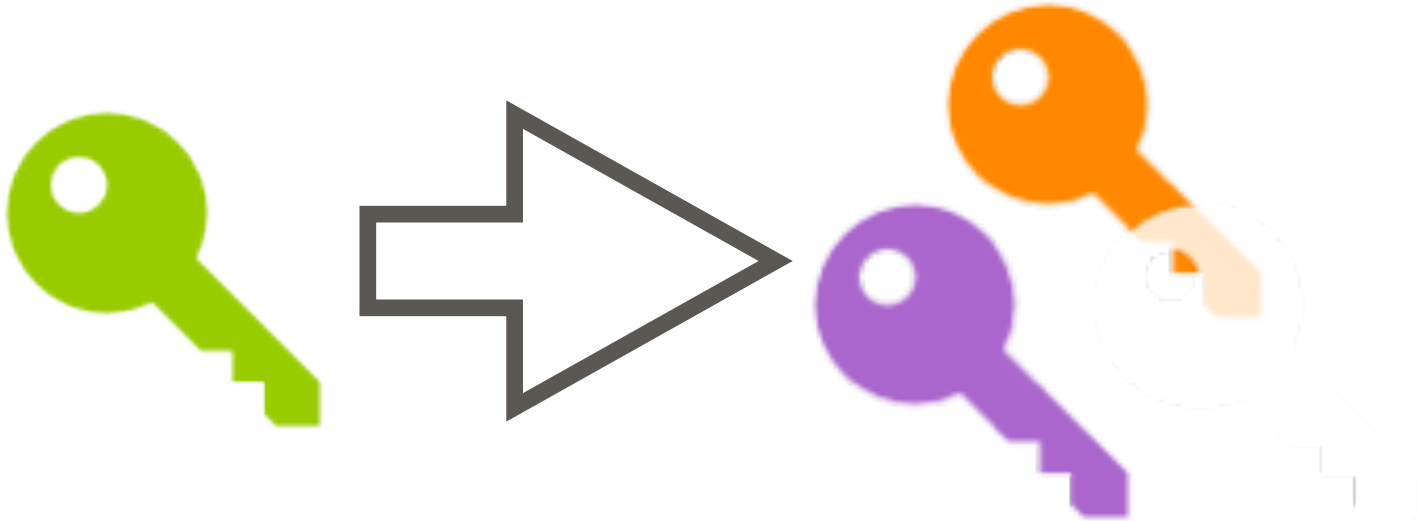
JENS NEUHALFEN

NEVER REUSE KEYS!

SLEEP BETTER WITH CONTENT ENCRYPTION

71

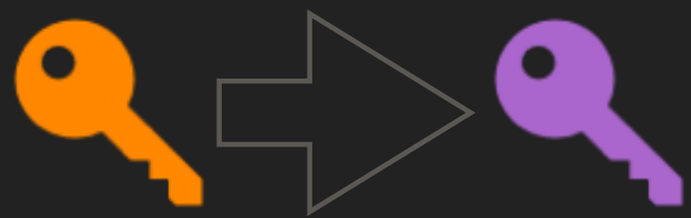
MAKE SURE THAT THE MASTER KEY HAS ENOUGH ENTROPY FOR DERIVED KEY AND DERIVED SALT



IMPORTANT: NEVER USE THE SAME KEY/IV TO ENCRYPT DIFFERENT DATA

- Encrypting different data with the same key and IV can lead to complete loss of confidentiality / integrity (*)
- **When updating encrypted records a new IV must be used** (better: a new key and IV)
- This can be achieved by incrementing a record-version on each encryption and using it in the key derivation.

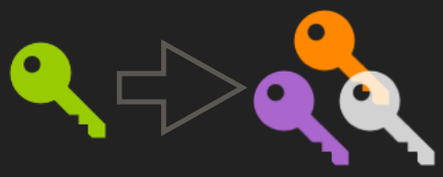
(*) This is because of the way CTR/GCM/CBC/… work. See e.g Appendix B of NIST Sp. Pub. 800-38A



PATTERNS

KEY REFRESH

NEVER REUSE KEYS!



- Encrypting different data with the same key and IV can lead to complete loss of confidentiality / integrity (*)
- **When updating encrypted records a new IV must be used** (better: a new key and IV)
- This can be achieved by incrementing a record-version on each encryption and using it in the key derivation.

(*) This is because of the way CTR/GCM/CBC/… work. See e.g Appendix B of NIST Sp. Pub. 800-38A

IMPORTANT: NEVER USE THE SAME KEY/IV TO ENCRYPT DIFFERENT DATA

MAKE SURE THAT THE MASTER KEY HAS ENOUGH ENTROPY FOR DERIVED KEY AND DERIVED SALT