Database of Long-Lived Symmetric Cryptographic Keys

draft-ietf-karp-crypto-key-table-06

Russell Housley , Tim Polk, Sam Hartman, Dacheng Zhang,

IETF 86, March. 2013, Orlando, USA

Updates since -04 (1)

- Change the name of several table fields

SendNotBefore	→	SendLifetimeStart
SendNotAfter	→	SendLifeTimeEnd
RcvNotBefore	→	AcceptLifeTimeStart
RcvNotAfter	→	AcceptLifeTimeEnd

Updates since -04 (2)

- 6. Operational Considerations

  When installing a series of keys to be used one after another (sometimes called a key chain), operators should configure the SendNotBefore field of the key to be several days after the RcvNotBefore field of the key to address the clock skew issue

  and guarantee there is some overlap. ⟶

  …operators should configure the SendLifetimeStart field of the key to be several hours after the AcceptLifeTimeStart field of the key to guarantee there is some overlap. This overlap is intended to address the clock skew issue and allow for basic operational considerations. Operators may choose to specify a longer overlap (e.g., several hours) to allow for exceptional circumstances.

Questions?