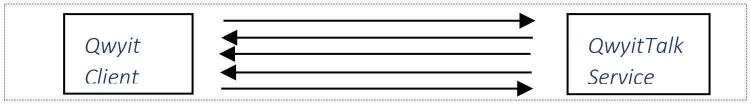
Let’s Break Qwyit

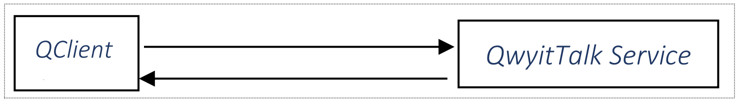
The following is a condensed display of the entire QwyitTalk™ process – with vulnerability discussion at each protocol step. There is no vulnerability in any QT™ primitive as a result of every use being underdetermined. This can be assured by simply doubling all key sizes, and performing an OWC prior to any use.

Verified Setup (VSU)



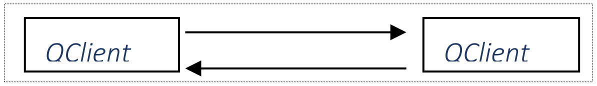
As noted in detail in papers, this multi-factor initial key distribution *can be made as strong as required; to include ultra-secure hand delivery*. Storage can also be made as strong as required, to include man-to-machine offsets, etc. Active listeners can be defeated using mandatory alerts – inactive listeners can be defeated using in-system additional keys. There are no breaks unaccounted for in the VSU.

Authentication Handshake (AH)



Each leg of the round trip are only numbers (CS, SSK) XORed with numbers (W). The 2nd set to the recipient client, is twice encrypted (W') so as not to leak any information to the sending client, who receives the bundle. Upon completion, QDS and Client independently without communication, PDAF update their DSKs to new versions. Versions are mathematically unique. Active use is alerted, inactive defeated using additional keys. There is no context for any break.

Messaging



C2C Start message includes bundled AH reply; no context. And MOD offset to create new SMK from AH SSK; QDS no longer has knowledge. Each message creates OTP msg key (W) for each new 256-bit PT, underdetermined, unconnected. SMK independently w/o communication PDAF updated at any interval. Any single broken W (known PT only available method) leaves underdetermined, unconnected next W; all W’s one-way gate protect SMK. No unaccounted for breaks in QT messaging.

NOTE: All transmission nuisance attacks defeated, if required, with MACs.