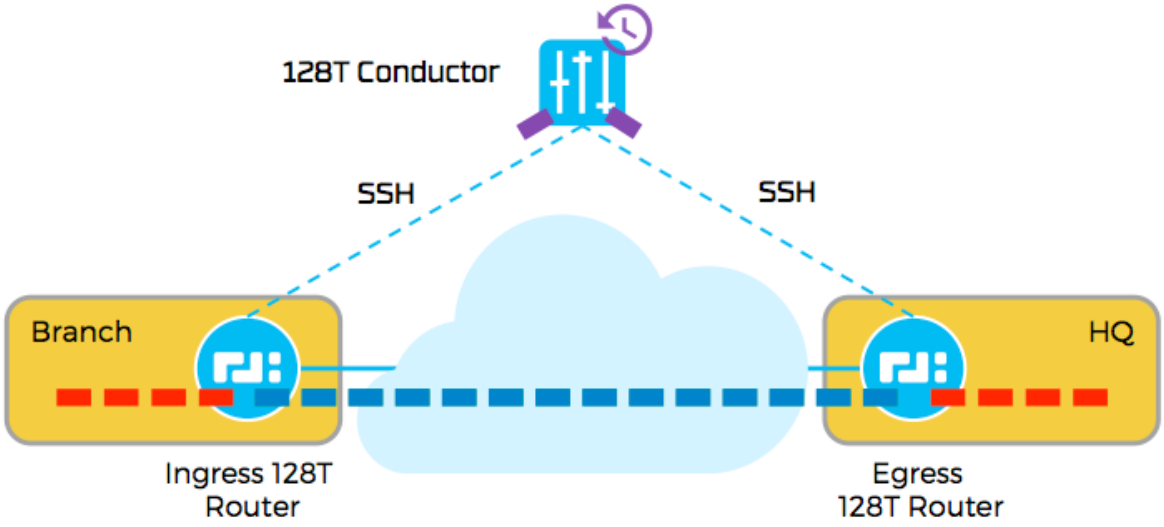
# 128T KEY GENERATION AND REKEYING




## KEY GENERATION AND REKEYING

All communication between 128T routers can be encrypted using AES128/AES256 and per packet authenticated using HMAC-SHA1/HMAC-SHA256. Configuration of the encryption and per packet authentication parameters are done at the tenant level. Any packet belonging to any service under the tenant with cryptography enabled will be automatically encrypted and per packet authenticated.

128T provides a centralized key management through 128T Conductor. Cryptogrphic keys used for encryption (AES128/AES256) and per packet authentication (HMAC-SHA128/HMAC-SHA256) are auto-generated by the Conductor in a FIPS 140-2 level 1 complaint way by using NIST 800-9A Deterministic Random Bit Generator (DRBG) mechanism. Conductor automatically generates these keys for all the tenants for which cryptography enabled. Conductor distributes these keys to all the 128T routers managed by the Conductor over an AES256/HMAC-SHA256 encrypted/authenticated SSH connection.

Cryptographic keys used for encryption/authentication can be centrally rekeyed through the Conductor. The mechanism followed for rekeying closely follows the procedure suggested in IKEv2 RFC 7296. Rekeying interval supported on the Conductor is in the range 1 hour – 720 hour (recommended rekeying interval is, rekey every 24 hours). Once the new keys are generated, Conductor will distribute these keys to all the 128T routers over the pre-

establish SSH connection. To avoid race condition, the routers will not use the new keys until it gets an explicit ACTIVATE request from the Conductor.

## PKI VS 128T KEY MANAGEMENT

128T key generation, key management and key distribution closely follows the procedure as suggested in the PKI standard RFC 3280. 128T Conductors generates and distributes keys in a FIPS 140-2 level 1 complaint manner. Generated keys are stored to comply with the PCI DSS 3.2 and HIPPA Security Compliance rules. 128T router closely follows all the procedures required to meet the ICSA Firewall Compliance. Thus, 128T provides a superior way of key generation and key life cycle management without the overhead and cost of maintaining a PKI infrastructure.