Process Flow

4. CA issues certificate with 1. CA transmits pre-certificate Log servers provide m proofs (SCTs) m of n proofs 3. CA confirms integrity of proofs to n logging servers Create pre-certificate Review next Remove CT poison Signed Certificate extension and Timestamp (SCT) Sign pre-certificate insert m of n SCTs (CT poison extension included) Yes Is m of n complete? Sign and issue Transmit pre-certificate certificate Have n logs to n logs been Yes exhausted? Fail





Session ID: ARCH-R01

Session Classification: Intermed.