

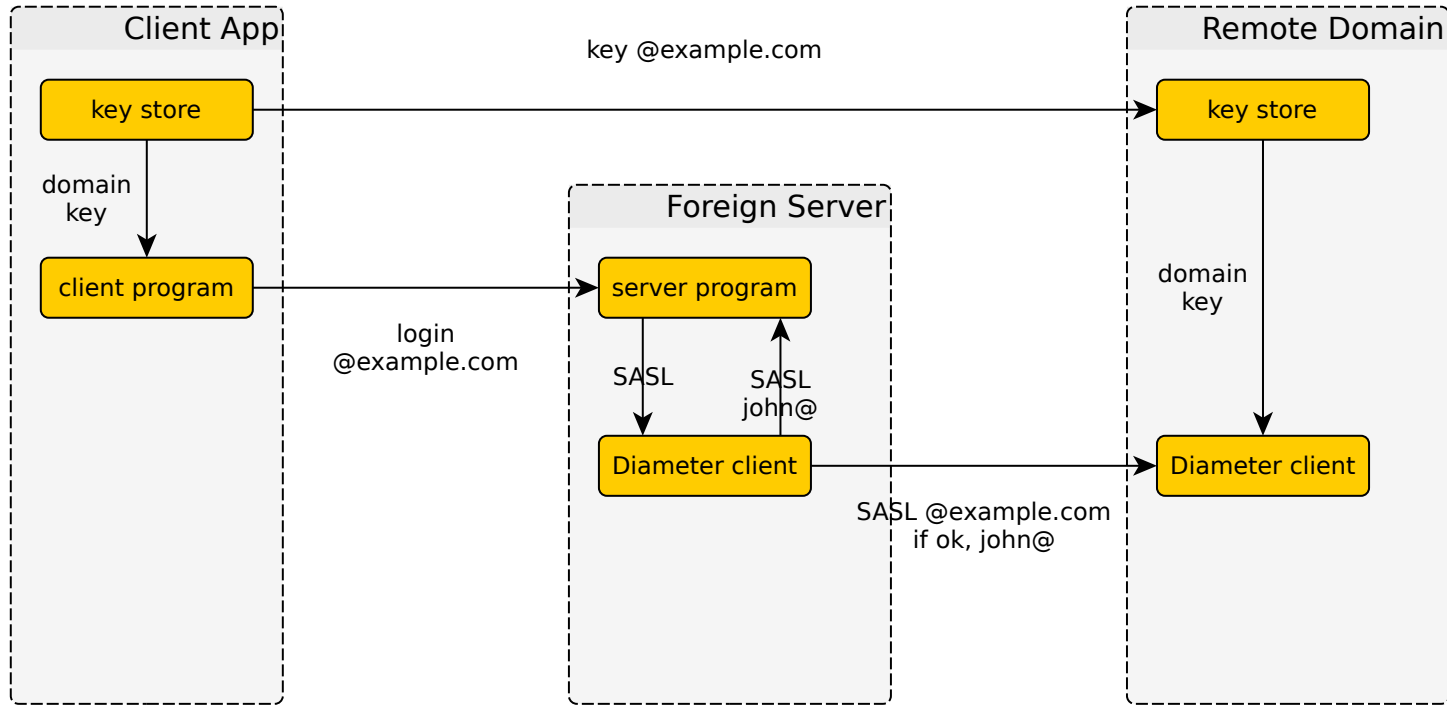
Key Derivation in SASL

- * **SASL often runs over TLS**
- * **TLS = pubkey auth on (EC)DHE encryption**
- * **(EC)DHE is a problem for Quantum Computing**

- * **SASL usually adds entropy**
- * **Mix that with TLS**

- * **Another example (VPN) follows**

Realm Crossover with SXOVER-PLUS



Realm Crossover for a VPN

