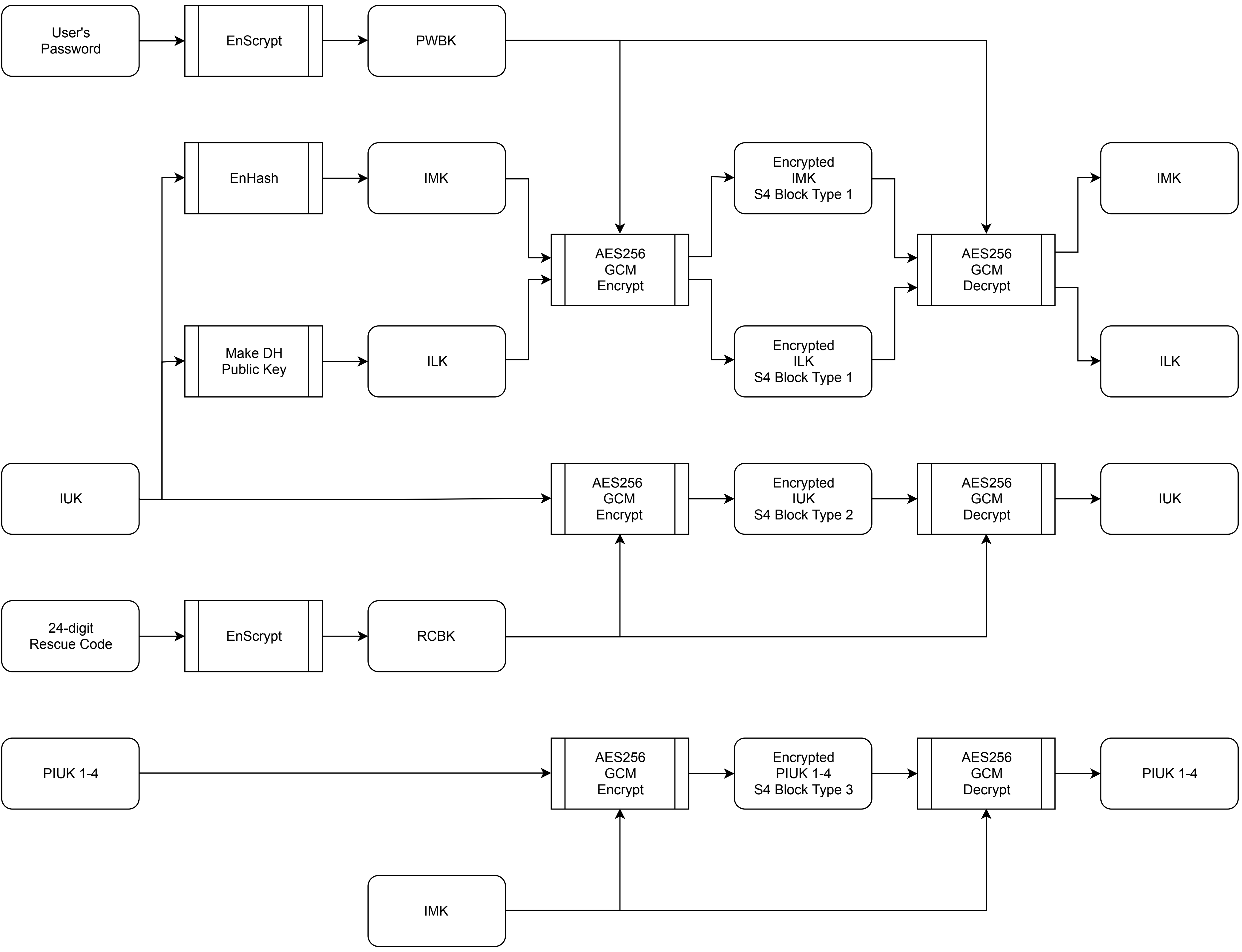
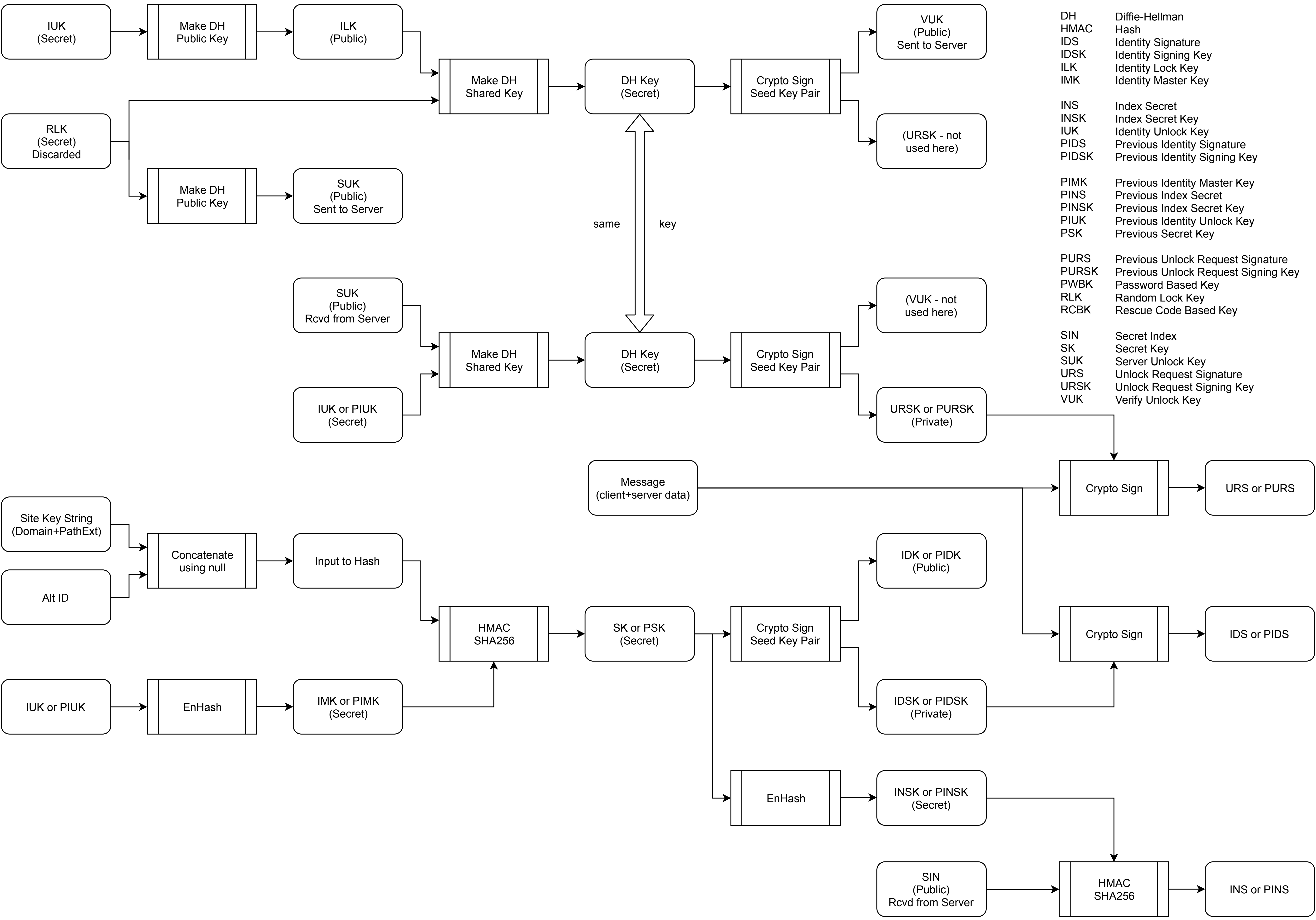
SQRL Client Crypto Diagram

Version 1.0 January 2020



AES	Advanced Encryption Standard
GCM	Galois Counter Mode
ILK	Identity Lock Key
IMK	Identity Master Key
IUK	Identity Unlock Key
PIUK	Previous Identity Unlock Key
PWBK	Password Based Key
RCBK	Rescue Code Based Key

S4 Blocks include Additional Data and Verification Tags



DH	Diffie-Hellman
HMAC	Hash
IDS	Identity Signature
IDSK	Identity Signing Key
ILK	Identity Lock Key
IMK	Identity Master Key
INS	Index Secret
INSK	Index Secret Key
IUK	Identity Unlock Key
PIDS	Previous Identity Signature
PIDSK	Previous Identity Signing Key
PIMK	Previous Identity Master Key
PINS	Previous Index Secret
PINSK	Previous Index Secret Key
PIUK	Previous Identity Unlock Key
PSK	Previous Secret Key
PURS	Previous Unlock Request Signature
PURSK	Previous Unlock Request Signing Key
PWBK	Password Based Key
RLK	Random Lock Key
RCBK	Rescue Code Based Key
SIN	Secret Index
SK	Secret Key
SUK	Server Unlock Key
URS	Unlock Request Signature
URSK	Unlock Request Signing Key
VUK	Verify Unlock Key