Efficient Asymmetric Cryptography for RFID Access Control

Progress Report

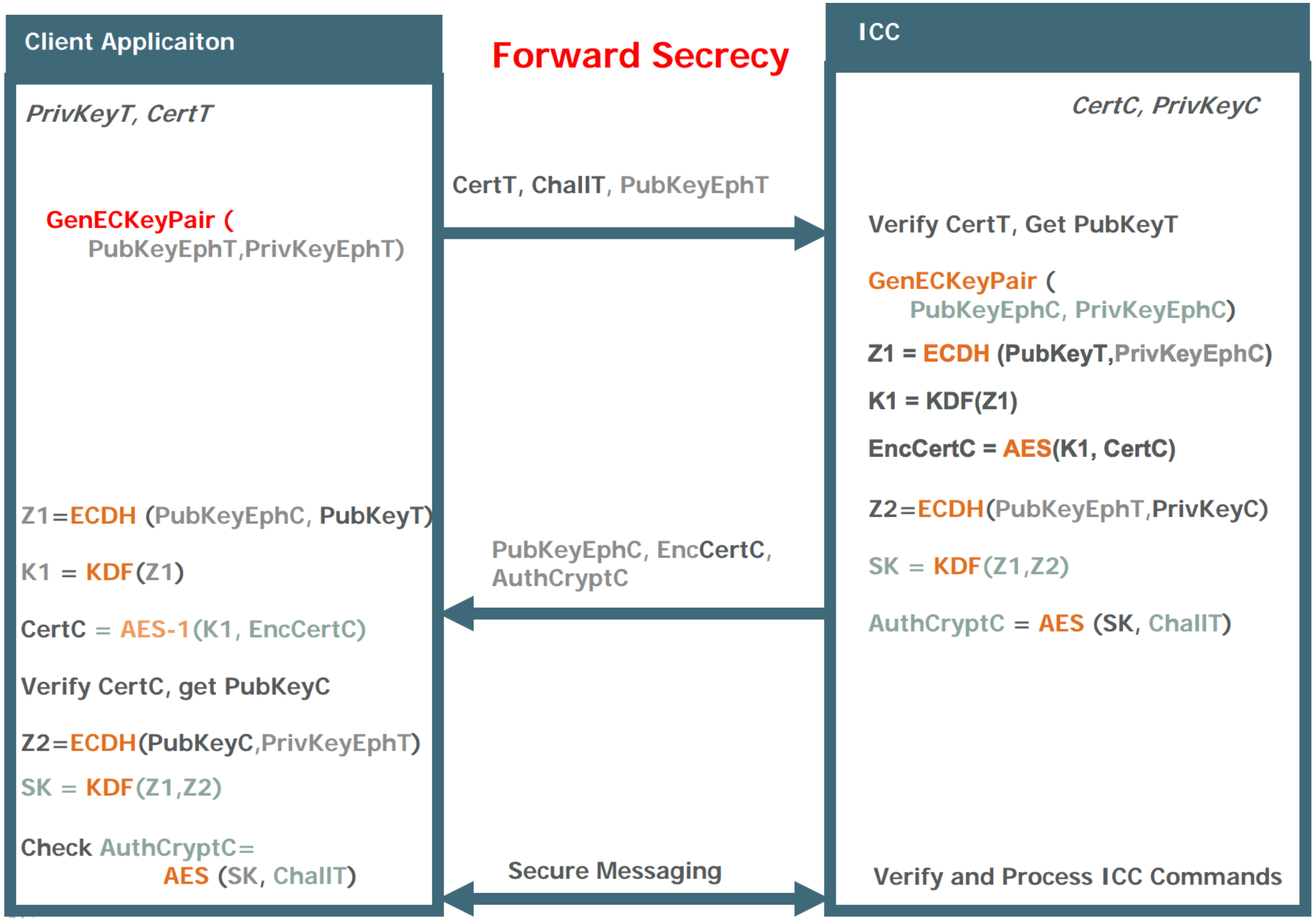
Benefits of OPACITY

The OPACITY-FS protocol provides:

- Mutual authentication
- User untraceability

These were listed as possible extensions in the proposal.

Open Protocol for Access Control Identification and Ticketing with privacY - OPACITY



Forward Secrecy

Client Applicaiton

PrivKeyT, CertT

GenECKeyPair (
PubKeyEphT,PrivKeyEphT)

Z1=ECDH (PubKeyEphC, PubKeyT)

K1 = KDF(Z1)

CertC = AES-1(K1, EncCertC)

Verify CertC, get PubKeyC

Z2=ECDH(PubKeyC,PrivKeyEphT)

SK = KDF(Z1,Z2)

Check AuthCryptC=
AES (SK, ChallT)

CertT, ChallT, PubKeyEphT

PubKeyEphC, EncCertC,
AuthCryptC

Secure Messaging

ICC

CertC, PrivKeyC

Verify CertT, Get PubKeyT

GenECKeyPair (
PubKeyEphC, PrivKeyEphC)

Z1 = ECDH (PubKeyT,PrivKeyEphC)

K1 = KDF(Z1)

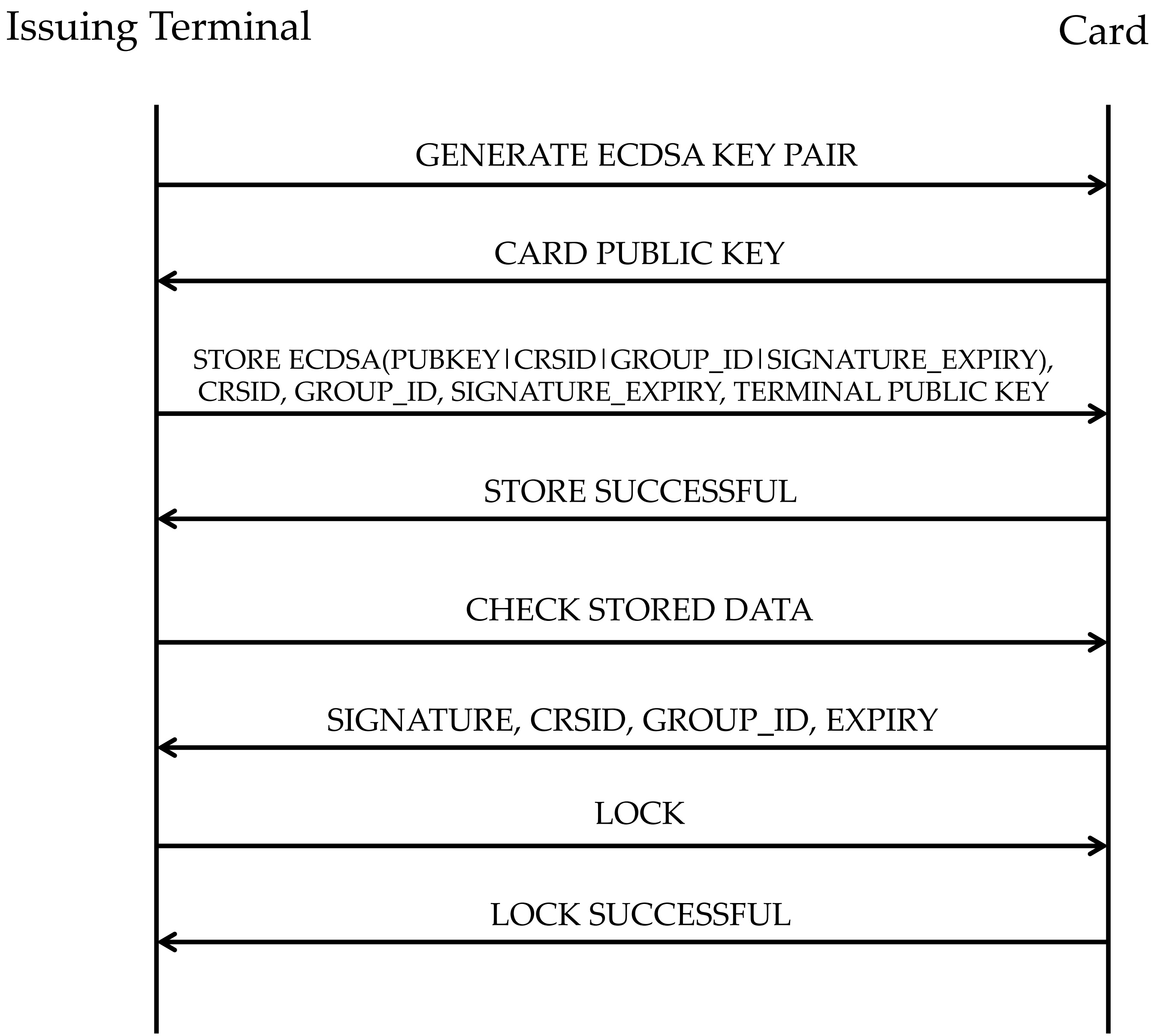
EncCertC = AES(K1, CertC)

Z2=ECDH(PubKeyEphT,PrivKeyC)

SK = KDF(Z1,Z2)

AuthCryptC = AES (SK, ChallT)

Verify and Process ICC Commands


Issuing Terminal
Card
GENERATE ECDSA KEY PAIR
CARD PUBLIC KEY
STORE ECDSA(PUBKEY|CRSID|GROUP_ID|SIGNATURE_EXPIRY),
CRSID, GROUP_ID, SIGNATURE_EXPIRY, TERMINAL PUBLIC KEY
STORE SUCCESSFUL
CHECK STORED DATA
SIGNATURE, CRSID, GROUP_ID, EXPIRY
LOCK
LOCK SUCCESSFUL

Schedule

- Provisioning application has been implemented and tested.
- Protocol not yet fully implemented.
  - Approx. 2 weeks behind schedule
  - However, last 6 weeks of Lent were allocated for bug fixes and implementing extensions.