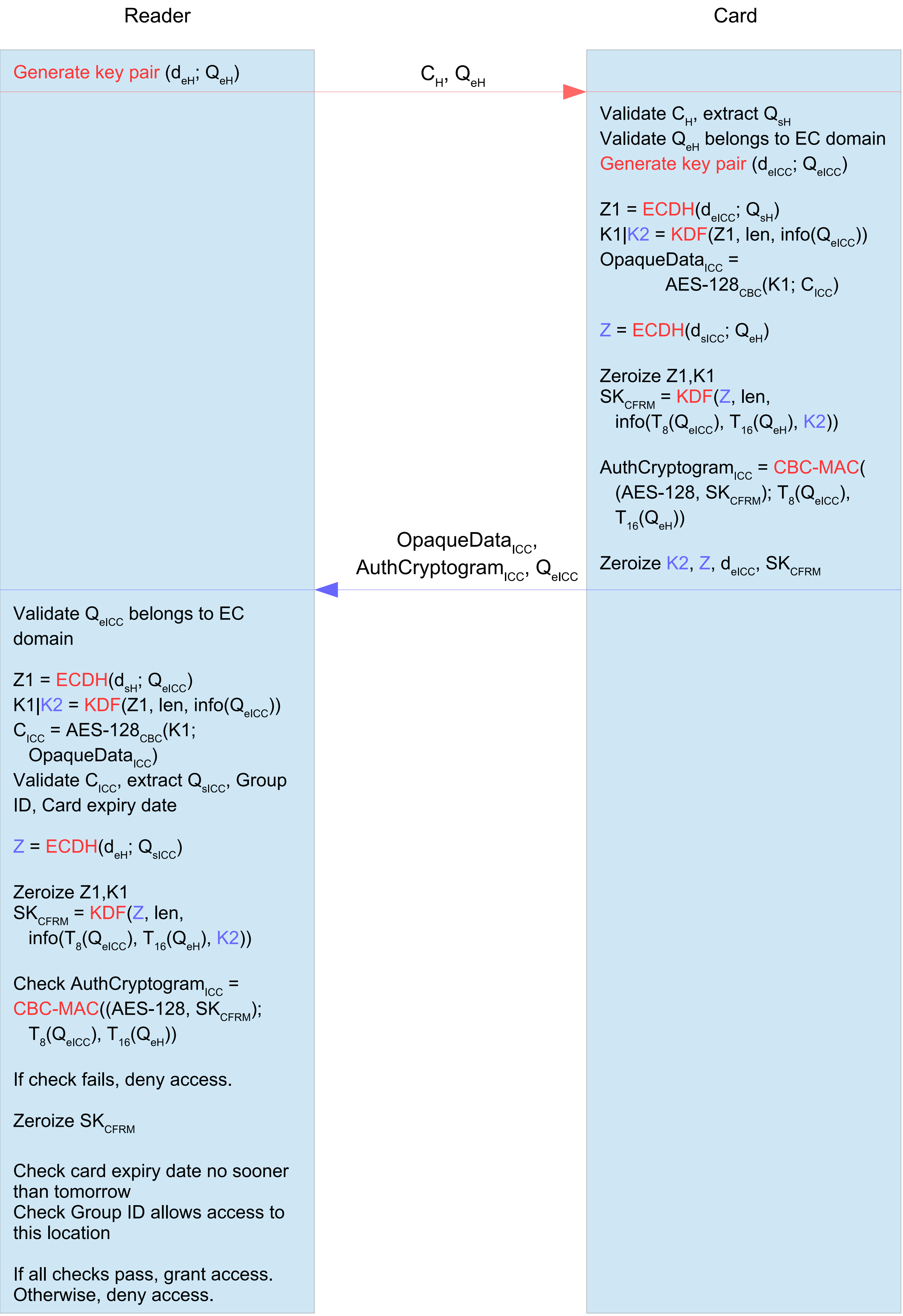

Reader

Card

Generate key pair (d_{eH}; Q_{eH})

C_H, Q_{eH}

Validate C_H, extract Q_{sH}
Validate Q_{eH} belongs to EC domain
Generate key pair (d_{eICC}; Q_{eICC})

Z1 = ECDH(d_{eICC}; Q_{sH})
K1|K2 = KDF(Z1, len, info(Q_{eICC}))
OpaqueData_{ICC} =
AES-128_{CBC}(K1; C_{ICC})

Z = ECDH(d_{sICC}; Q_{eH})

Zeroize Z1,K1
SK_{CFRM} = KDF(Z, len,
info(T_8(Q_{eICC}), T_{16}(Q_{eH}), K2))

$\text{AuthCryptogram}_{ICC}$ = CBC-MAC(
(AES-128, SK_{CFRM}); T_8(Q_{eICC}),
T_{16}(Q_{eH}))

Zeroize K2, Z, d_{eICC}, SK_{CFRM}

OpaqueData_{ICC},
$\text{AuthCryptogram}_{ICC}$, Q_{eICC}

Validate Q_{eICC} belongs to EC domain

Z1 = ECDH(d_{sH}; Q_{eICC})
K1|K2 = KDF(Z1, len, info(Q_{eICC}))
C_{ICC} = AES-128_{CBC}(K1;
OpaqueData_{ICC})
Validate C_{ICC}, extract Q_{sICC}, Group ID, Card expiry date

Z = ECDH(d_{eH}; Q_{sICC})

Zeroize Z1,K1
SK_{CFRM} = KDF(Z, len,
info(T_8(Q_{eICC}), T_{16}(Q_{eH}), K2))

Check $\text{AuthCryptogram}_{ICC}$ =
CBC-MAC((AES-128, SK_{CFRM});
T_8(Q_{eICC}), T_{16}(Q_{eH}))

If check fails, deny access.

Zeroize SK_{CFRM}

Check card expiry date no sooner than tomorrow
Check Group ID allows access to this location

If all checks pass, grant access.
Otherwise, deny access.