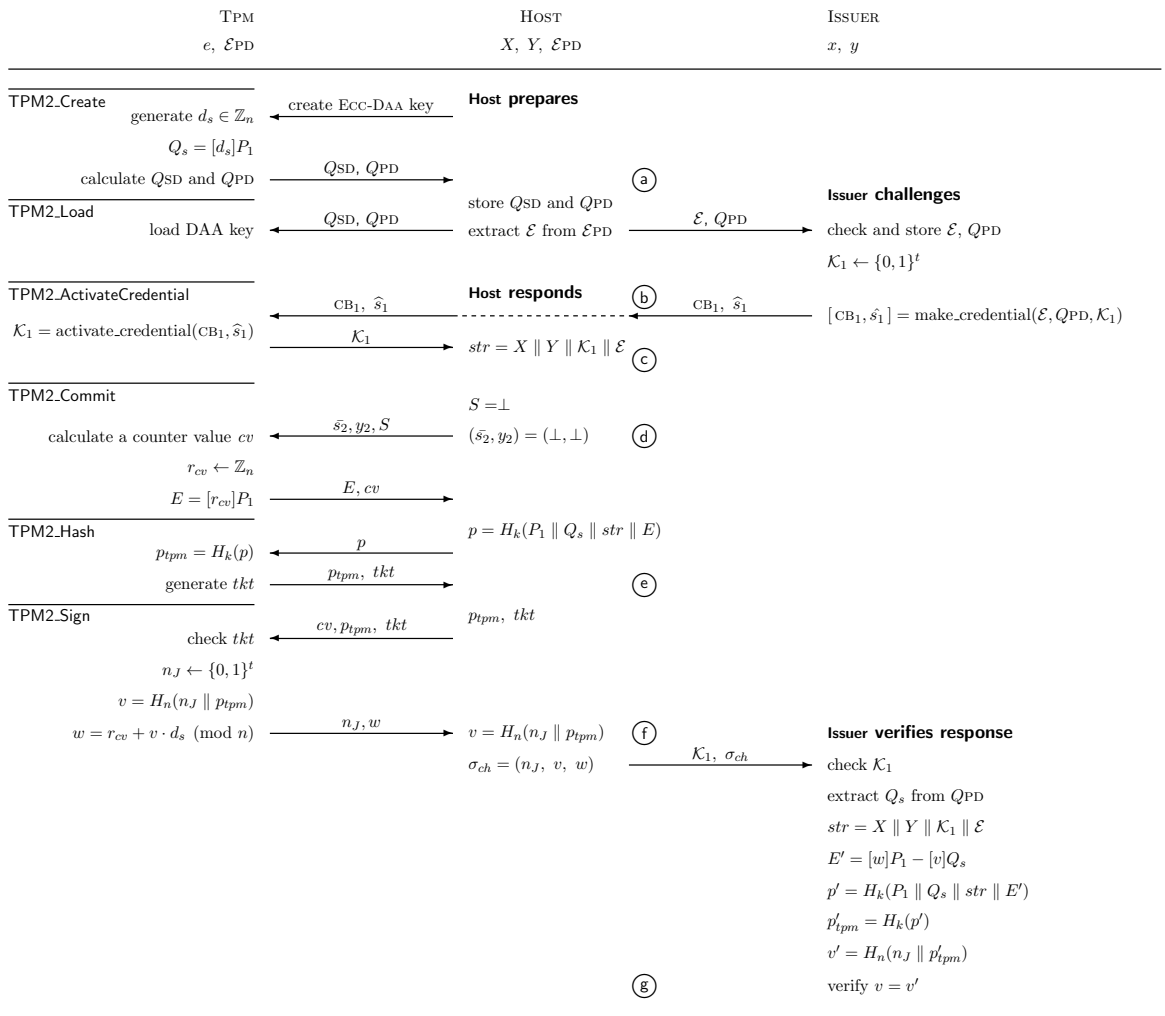

Figure 1: Initiating the join

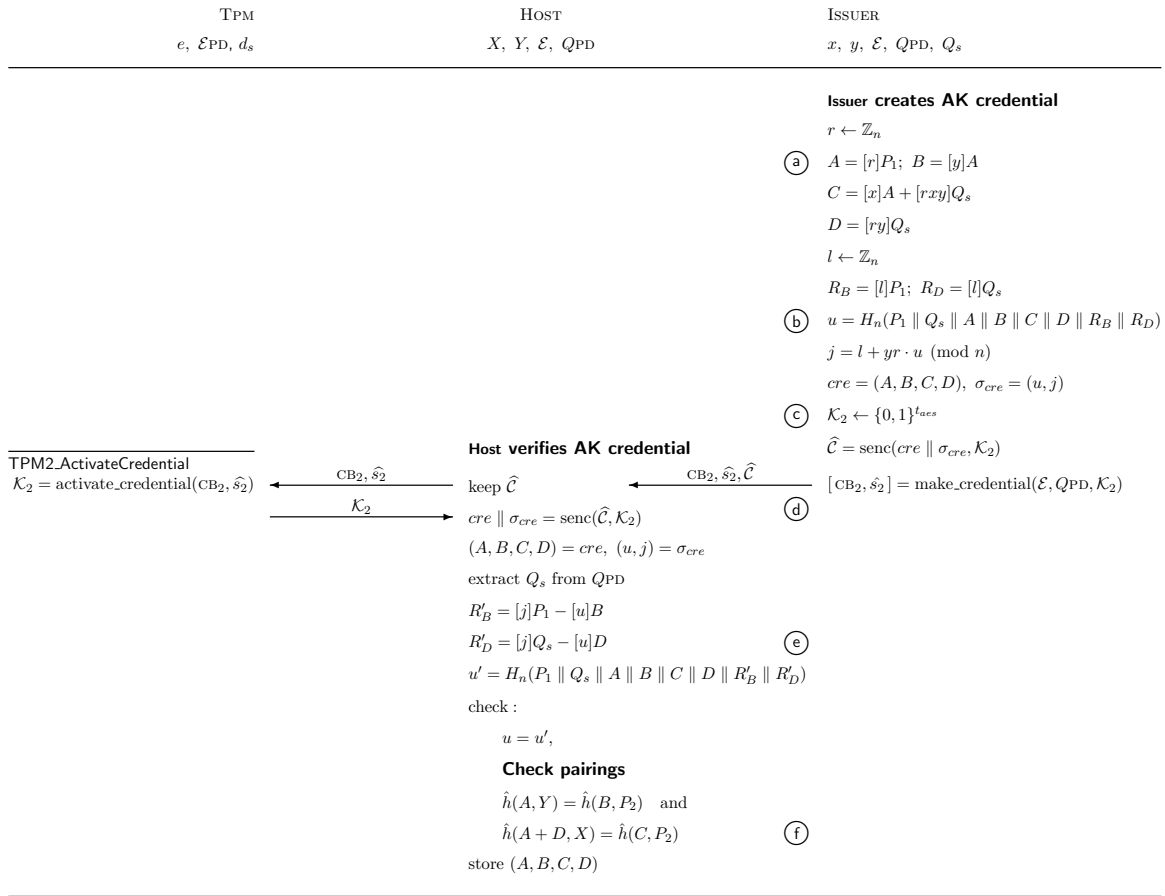

Figure 2: Completing the join

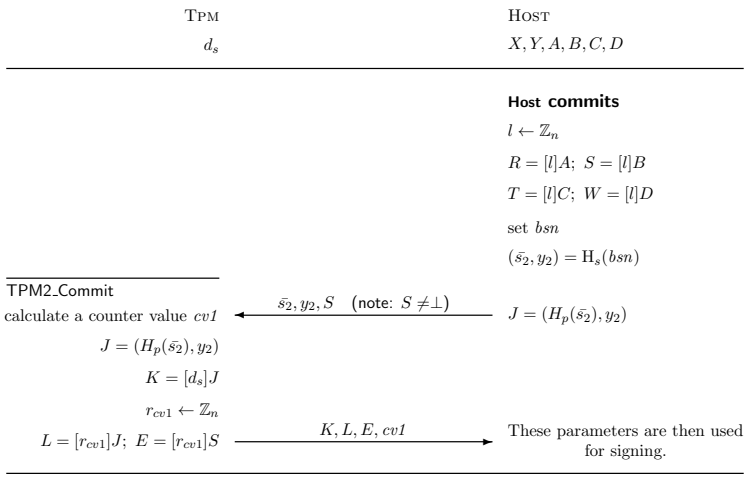

Figure 3: Preparing to use the DAA key

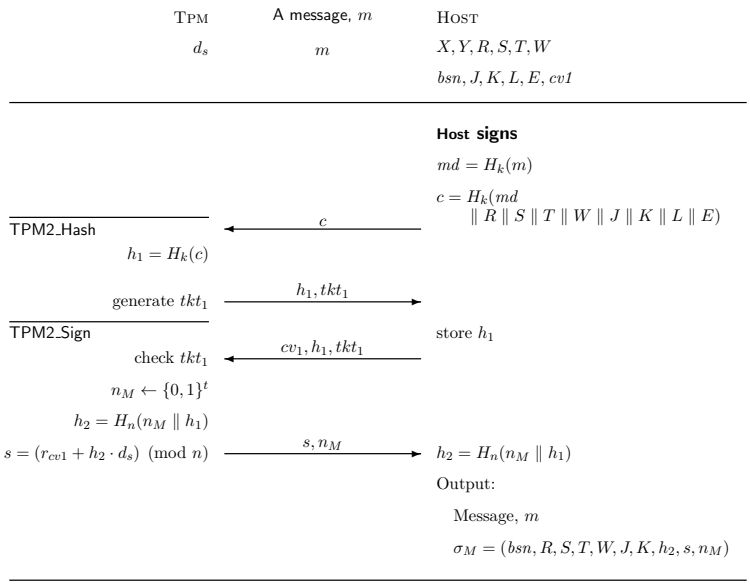

Figure 4: Signing a message using the DAA key

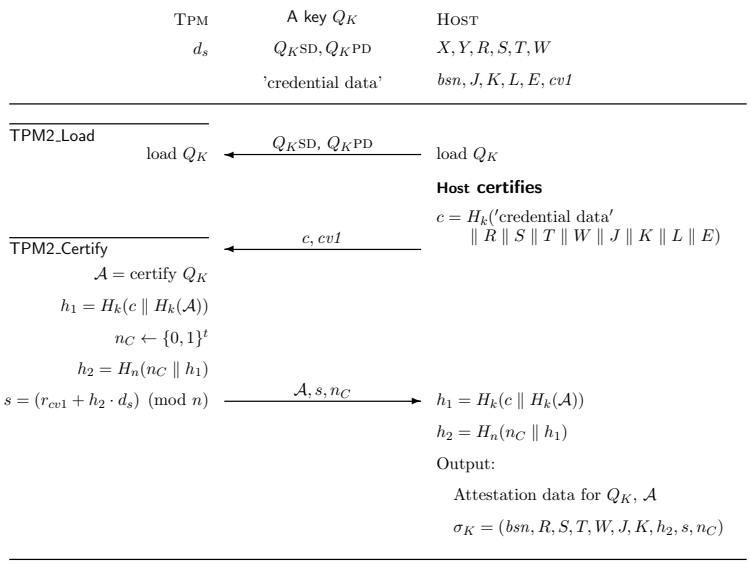

Figure 5: Certifying a key, Q_K, using the DAA key

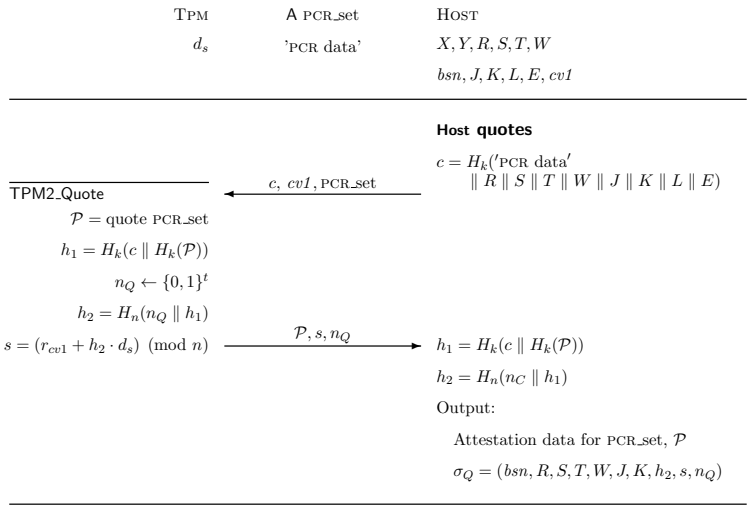

Figure 6: Quoting a set of PCR values using the DAA key

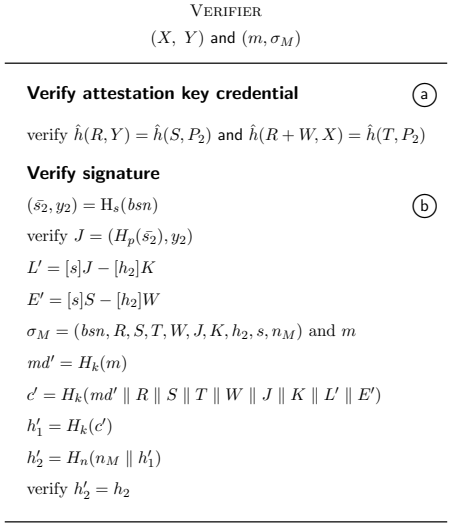

Figure 7: Verifying the DAA signature

VERIFIER

$(X,\ Y)$ and (m, σ_M) or $(Q_K\text{PD}, \mathcal{A}, \sigma_K)$ or $(\mathcal{P}, \sigma_Q)$

Verify attestation key credential

verify $\hat{h}(R, Y) = \hat{h}(S, P_2)$ and $\hat{h}(R + W, X) = \hat{h}(T, P_2)$

$(\bar{s_2}, y_2) = \text{F}(bsn)$

verify $J = (H_p(\bar{s_2}), y_2)$

$L' = [s]J - [h_2]K$

$E' = [s]S - [h_2]W$

Verify signature

$\sigma_M = (bsn, R, S, T, W, J, K, h_2, s, n_M)$ and m

$md' = H_k(m)$

$c' = H_k(md' \parallel R \parallel S \parallel T \parallel W \parallel J \parallel K \parallel L' \parallel E')$

$h'_1 = H_k(c')$

$h'_2 = H_n(n_M \parallel h'_1)$

verify $h'_2 = h_2$

Verify Q_K certificate

Calculate the key name, Q_N, from $Q_K\text{PD}$

Check the key name, Q_N, against that given in $\mathcal{A}$

$\sigma_K = (bsn, R, S, T, W, J, K, h_2, s, n_C)$ and 'credential data'

$c' = H_k(\text{'credential data'} \parallel R \parallel S \parallel T \parallel W \parallel J \parallel K \parallel L' \parallel E')$

$h'_1 = H_k(c' \parallel H_6(\mathcal{A}))$

$h'_2 = H_n(n_C \parallel h'_1)$

verify $h'_2 = h_2$

Verify PCR quote

Check the PCR value given in $\mathcal{P}$ against that expected

$\sigma_Q = (bsn, R, S, T, W, J, K, \mathcal{P}, h_2, s, n_Q)$ and 'PCR data'

$c' = H_k(\text{'PCR data'} \parallel R \parallel S \parallel T \parallel W \parallel J \parallel K \parallel L' \parallel E')$

$h'_1 = H_k(c' \parallel H_6(\mathcal{P}))$

$h'_2 = H_n(n_C \parallel h'_1)$

verify $h'_2 = h_2$

Figure 8: Verifying the attestation signatures

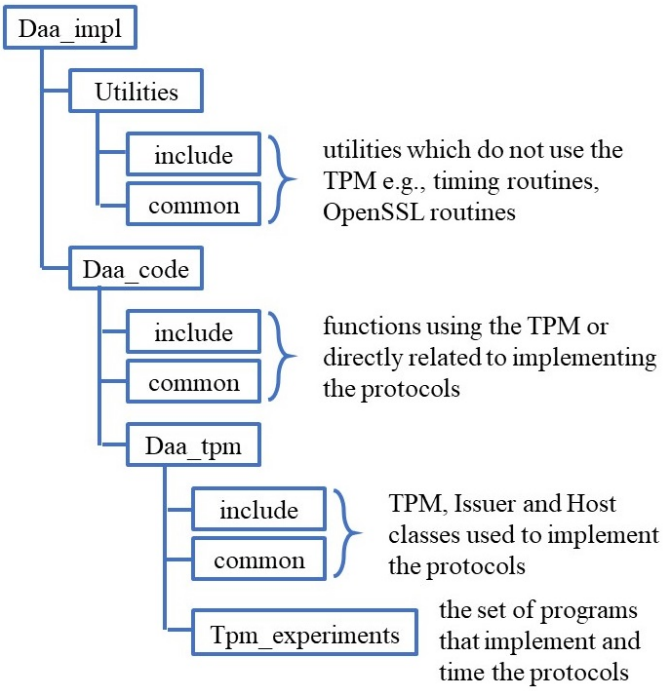

Figure 9: Structure of the C++ codebase