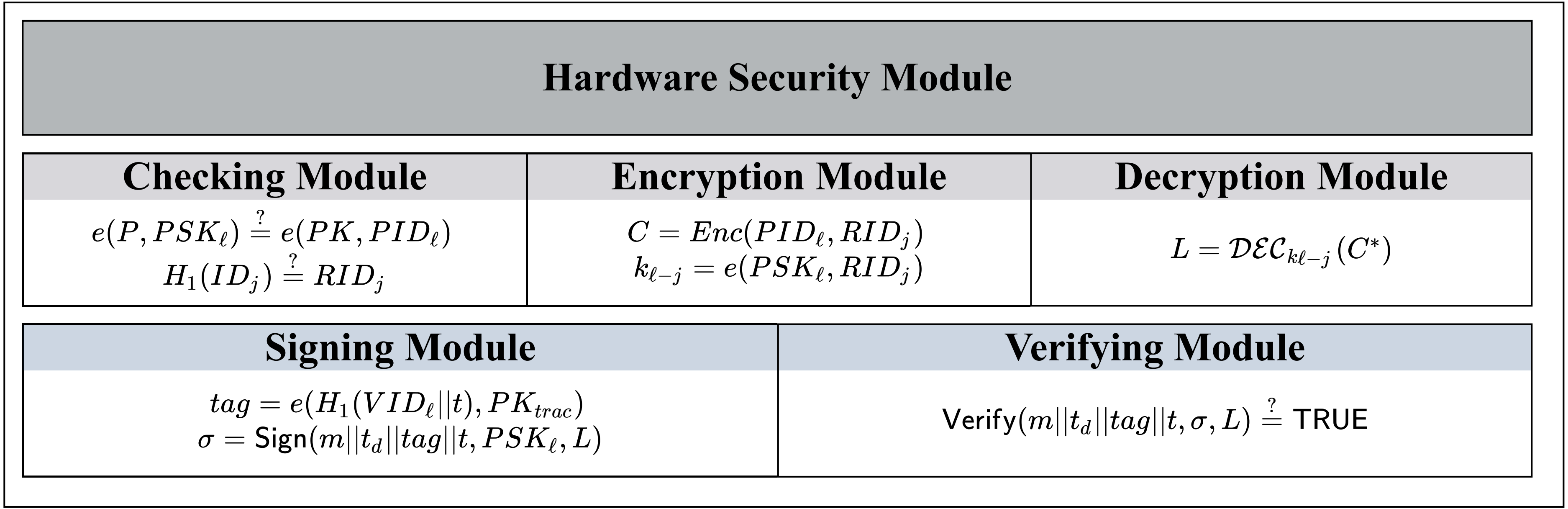

Hardware Security Module

Checking Module

$$e(P, PSK_\ell) \overset{?}{=} e(PK, PID_\ell)$$
$$H_1(ID_j) \overset{?}{=} RID_j$$

Encryption Module

$$C = Enc(PID_\ell, RID_j)$$
$$k_{\ell-j} = e(PSK_\ell, RID_j)$$

Decryption Module

$$L = \mathcal{DEC}_{k\ell-j}(C^*)$$

Signing Module

$$tag = e(H_1(VID_\ell||t), PK_{trac})$$
$$\sigma = \mathsf{Sign}(m||t_d||tag||t, PSK_\ell, L)$$

Verifying Module

$$\mathsf{Verify}(m||t_d||tag||t, \sigma, L) \overset{?}{=} \mathsf{TRUE}$$