Secure Convertible Authenticated Encryption Scheme Based on RSA

p, q: two large primes and $N = pq$;

ed: $\equiv 1 \pmod{\phi(N)}$;

$\{p_i, q_i, d_i\}$: U_i's private key;

$\{e_i, N_i\}$: U_i's public key;

$h(\cdot)$: a one-way hash function which generates a k-length output;

Authenticated ciphertext generation (ACG) (By the signer U_s)	Choose $c \in \{0, 1\}^k$; Compute $r = Mc^c \bmod N_v$; $t = c^{e_v} \bmod N_v$; $s = (h(M, c))^{d_s} \bmod N_s$; Send the authenticated ciphertext (s, r, t) to U_v.
Signature recovery and verification (SRV) (By the verifier U_v)	Compute $c = t^{d_v} \bmod N_v$; Recover $M = rc^{-c} \bmod N_v$; Verify $s^{e_s} = h(M, c) (\bmod N_s)$.
Signature conversion (SC) (By the verifier U_v)	U_v releases (M, s, c) ; Anyone can verify $s^{e_s} = h(M, c) (\bmod N_s)$.