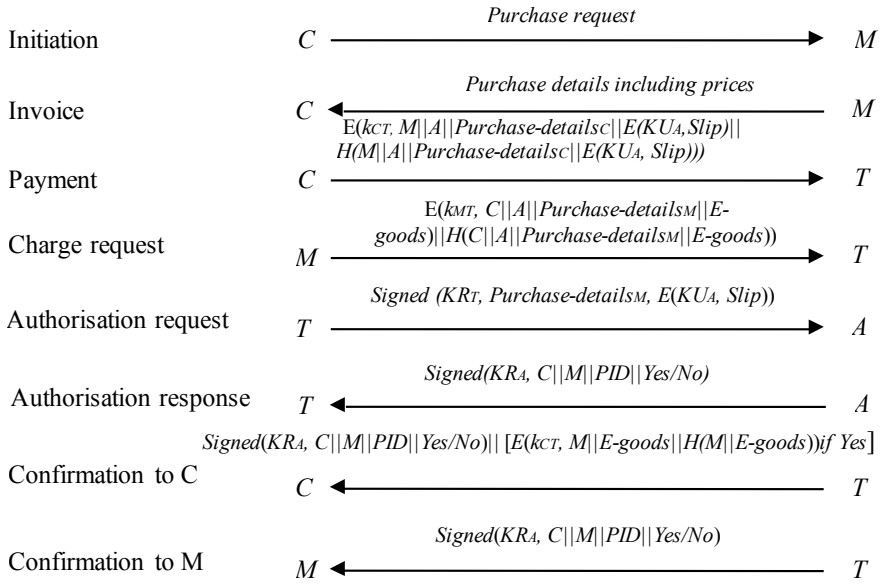
Model Answer to Q(C)

(c) Assume that there is a trusted third party *T* to assist in this fair trade. A protocol based on *T* is described below, where it is assumed that *T* shares a conventional (or symmetric) key k_{CT} with *C*, and k_{MT} with *M*. *Purchase-details*$_M$=*Purchase-details*$_C$ if all is authentic; C and M can negotiate and agree on *Purchase-details*. *Purchase-details* is like a purchase contract containing information such as the buyer ID (IDentity), the seller/merchant's ID, date/time of the purchase, description of the purchased item, the price to be paid. Signature verification keys are certified by a trusted CA and are valid.



Where *PID* (Identifier of this Purchase)=*H*(*Purchase-details*$_M$) (or *Purchase-details*$_M$), which is used to bind A's signature to this transaction. As *Purchase-details*$_M$=*Purchase-details*$_C$ if all is authentic, both C and M can verify these receipts (received in the Confirmations).

- In the step of Payment, *C* sends the Payment Request containing purchase details and encrypted *Slip to T* instead of to *M*; the Payment Request is encrypted with shared key k_{CT}; inside this encryption contained a hash value of the Request and this hash value serves as the checksum to ensure integrity of the Request by C to T.
- In the step of Charge Request, *M* sends the purchase details and electronic goods *E-goods*, encrypted with shared key k_{MT}, to *T* and the authenticity of the message is protected by the hash value inside the encryption.
- In the step of Authorisation Request, if the purchase details, which *T* has recovered by the decryption of the messages from *C* and *M*, match, and *E-goods* meet the purchase details, then *T* signs and forwards the received message including encrypted *Slip* to *A*. Otherwise, *T* terminates the protocol, and informs *C* and *M*.
- In the steps of Confirmation to *C* and *M*, *T* forwards *A*'s signature to both *C* and *M*. In addition, *T* sends *E-goods* encrypted with k_{CT} to *C* only if the payment has been confirmed by *A*.
- The above description shows that if *M* receives the payment, *C* can receive *E-goods*. This is because *T* would only forward *C*'s encrypted *Slip* to *A* after having received *E-goods* from *M* which meets *C*'s purchase details. Similarly, if *C* receives *E-goods*, *M* will receive the payment. If the protocol is terminated at the step of authorisation request, or *A* dis-approves the purchase, then neither of them can get anything from the other.