(a)

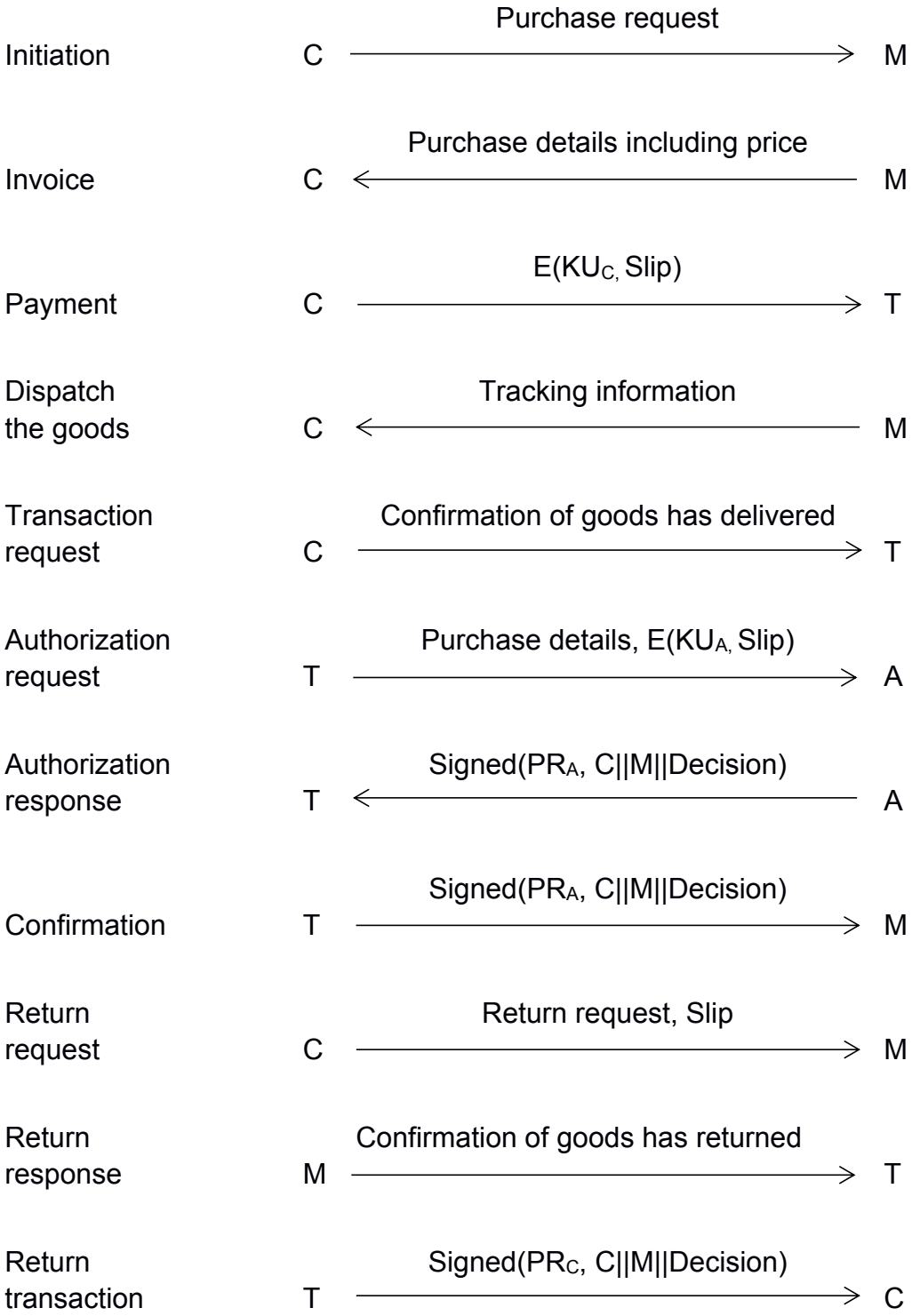
Generally speaking, three security threats are confidentiality, integrity and availability (CIA). To more specific, threats to confidentiality is disclosure, hackers may snooping or sniffing users' credit card details (e.g. card number, CVV number, and security questions) in data transactions; and they may access the system or other data in an unauthorized way (e.g. backdoor attack). Threats to integrity are deception, e-payment has a risk of fraud since once someone got users' password, he can steal the money; attackers may build up a fake website to steal our card information, then they can create verified accounts which will lead to payment fraud; they may modify the data before it sends to the intended place; repudiation attack is another attack that will happen so that the stored card data would be considered invalid. The threat to availability is disruption, users are likely to suffer denial-of-service attack (DoS attack) so that they are not able to access the data or system.

(b)

Confidentiality: Yes, because it will encrypt purchase information (Slip) with public keys, which can protect the confidentiality of the data.
Integrity: Yes. This protocol uses digital signature. It requires message-dependent in order to ensure content integrity, and it also requires signer-dependent so it also ensures origin authenticity, which helps to avoid repudiation. The signature will be invalid if there is any change made to it.
Availability: No, back up and redundancy can help ensure data availability is backup, but there is no kind of measure took in this protocol; while encryption and digital signature have nothing to do with maintaining availability.

(c)

In order to achieve fairness, we need a third-party online payment platform to temporarily keep the money. So after the customer purchases the goods, the money will be verified by the bank and will go to this third party platform instead of being transferred directly to the merchant, then after the goods dispatch, the merchant is asked to provide the tracking number of this goods to his customer so that both of them can know the current position of this parcel. After the parcel has been delivered, customer can check the quality of this goods if it is not as good as the merchant described, they can return the goods if this goods meets the return criteria, in this condition, customers will get their money back while merchant can get their goods back; or the customer can claim that he has received the goods and satisfied with it, then the third-party will transfer the money to merchant's bank account. In this way, merchants get the money only if their customers get the goods.



where, C, M, A and T represent a customer, a merchant, an acquirer (i.e. the merchant's bank) and a third-party online payment platform respectively. KU_A and PR_A are, respectively, A's public and private keys, E(K, x) denotes the encryption of x with key K, Signed(PR, x) denotes x signed with key PR (i.e. Signed(PR,x)=x||E(PR,H(x))), H(x) is cryptographic hash function, x||y is the concatenation of data items, x and y, and Slip = {the description of goods, prices to pay, C's credit card number}, Decision = yes or no.