

Security Requirements:

- *Regarding TTP:*

Off-line or Optimistic: “A TTP is involved in a protocol only in case of an incorrect behavior of a dishonest entity or in case of a network error”. (*Intensive Survey p6*),

Untrusted: The TTP must not be fully trusted, and must be ensured that it will be unable to derive any private information regarding the contract or the parties (their keys), also the TTP must have no interest in signing the contract or in any of the involved parties. (*p7-asokan, p:12*),

Stateless TTP: A stateless TTP, does keep no tracking of any information (DB or files) during of after the protocol execution, A stateless TTP has only one state during a given protocol instance. (check Wang p:414)

- *Regarding Network:*

Unreliable: we assume that TTP-X channel, $X = A|B$, is resilient (messages are not lost, delivered finally even after some time), while A-B channel is unreliable.

Asynchronous: In Asynchronous network, messages can be delayed and reordered differently (arbitrarily) from the way they were sent. (*pfitzmann, p 2*)

Dynamic timeout: This is the time which a party awaits for receiving a message, before issuing an abort or resolve request to the TTP, as a signal of party misbehavior or network error. I propose to use “dynamic timeout” in a way that each connection will have a different timeout derived by some means or history (e.g. ping, routing tables) by the protocol initiator and

recipient– [Discuss this idea](#)

- *Regarding Cryptosystem:*

A provably secure PKCS ({Private key, Public key}). that ensures the unforgeability of signatures – ([See Olga's first summary about digital signatures](#))

- *Regarding Protocol:*

- Non-repudiation

- NRO: An evidence that is generated by the protocol initiator (Alice), destined to the recipient (Bob), that can be presented to an adjudicator, who can unambiguously decide whether Alice is the author of a given message or not.”(p29-louridas, [Intensive Survey p4,](#))

- NRR: An evidence generated by the protocol message recipient, destined to Alice, that can be presented to an adjudicator, who can unambiguously decide whether Bob received a given message or not.” ([p29-louridas, Intensive Survey p4](#))

- Fairness: 1- [Intensive Survey p5](#), 2- [Maruyama p:80](#), 3- [Asokan, p:13](#), [wang-414](#))

- True Fairness is supported iff, it provides strong fairness (NRO+NRR or nothing), and if the exchange is successful, and the evidences produced during the protocol are independent of of how the protocol is executed.” (1)

- Strong fairness is supported, iff, at the end of the protocol, Alice has NRR and Bob has NRO of m and the message m , or neither of them got any useful information.(1)

- According to Maruyama et. al (2), an exchange between to parties is said to be fair, iff, both the parties receive each other's items or neither does, in particular neither party should gain any advantage by terminating the protocol in the middle”

- Timeliness: “a protocol is said to provide timeliness, iff, all the honest parties always have the ability to reach, in a finite time, a point in the protocol where they can stop the protocol while preserving fairness.” [Intensive Survey p 5](#)

- Abuse-free: According to Wang, this concept implies that, if the protocol is not executed successfully, any of the two parties cannot show the validity of the intermediate results generated by the other to an outsider. [Wang, p:414](#)

- Support for abort and arbitration: Abort (to ensure fairness) and Resolve (fairness after commitment) sub protocols ([me](#))

- Completeness (Correctness??): If the protocol is executed between two honest parties without any error or cheating events, then the protocol terminates normally and both parties get what was supposed to be received. ([me](#))

- Support verification: Show sub protocol, used for arbitration and dispute resolution instances, by TTP to verify a certain signed contract. ([pfitzmann p4](#))