Process for providing non repudiation of receipt (NRR) in an electronic transaction environment

A Non-Receipt Repudiation protocol between the emitter, the receiver and a Trusted Third Party (TTP) which is based on the transmission to the receiver of a first envelope which comprises an encrypted version of the message or document, a hash function of said message, and a Validation Certificate (VC) creating an unique link between said message M, said key K and said emitter. More specifically, the protocol involves the steps of transmitting a first envelope from the emitter to the receiver, said first envelope including a first, a second, a third, a fourth and a fifth element. The first element consists of an optional identifier (H1). The second element consists of an encrypted form of said document or message [M]K. The third element consists of the hashing of said message M. The fourth element is formed by [K, h(M)] encrypted with the public key of the TTP. A fifth element consists of a Validation Certificate (VC) consisting of a signature of said emitter which is used for creating an unambiguous link between the original message M and the key K chosen and used by the originator for encrypting this message before the latter is transmitted to the recipient.