SafeMessage System Description

A software development company intends to build a secure instant messaging product for use by bankers, brokers, lawyers, and other professionals with high communications confidentiality and integrity needs.

The *SafeMessage* system will allow individuals to communicate over the Internet with others using a peer-to-peer protocol at one of three security levels. Messages must be encrypted at every security level and the communication path between machines must be unspoofable. The three security levels are:

- *High*—At this level there must be an unspoofable communication path between users and message delivery must be non-repudiable.
- *Medium*—At this level there must be an unspoofable communication path between users, but no guarantee of delivery.
- *Low*—At this level there is neither an unspoofable path between users nor a delivery guarantee.

Thus, at the low security level, messages are sent securely from one machine to another with no guarantee of delivery, at the medium level they are sent from one user to another with no guarantee of delivery, and at the high level they are sent from one user to another with a guarantee of receipt.

Pairs of users must establish sessions with other another at a security level. All communication between the two users during the session then occurs at the established security level. Users may have concurrent sessions with many users at different security levels. Users may broadcast a message created in one session to other sessions provided the other sessions have a security level at least as high as the session in which the message is created.