Web based secure purchase order

Implement a secure purchase order system that allows the user to enter a purchase request and routes it (by secure email) to a supervisor for signature and then to the purchasing department.

- All user interactions will be web-based.
- All connections between parties will be preceded by public-key mutual authentication.
- The signatures of both the purchaser and the supervisor will be public key based, and will be performed on a hash of the purchase order. The signature of the purchaser will be sent to both the supervisor and the orders department along with a timestamp.
- If an order is approved by the supervisor, the orders department can cross-check the digest signed by the supervisor with the digest signed by the purchaser. The signature and time-stamping is obviously important in preventing repudiation.
- You can ignore the possibility that a user will “publish” his/her key to back up a repudiation. Ideally, the user’s key will not be easily accessible and, since the whole process takes place in one organization, the possible means of revealing a key are very limited.
- All messages will be encrypted using RSA public-key cryptography. Depending on performance (and time) this might be optimized by using RSA to only send a one-time secret key.

Note: Use cryptix at www.cryptix.org or security module provided by JAVA.