ABSTRACT

A worldwide Public Key Infrastructure (PKI) that supports international, government, and state policies/regulations will not be available until the turn of the century. In the meantime, corporations can utilize this security technology to satisfy current business needs. Corporate PKI addresses areas such as secure web application development and messaging. Many companies are choosing to manage their own Certificate Authority (CA) instead of outsourcing this function to a third party (i.e., Verisign, GTE CyberTrust). To benefit fully from the public key technology in a corporate environment, a thorough understanding of the current and future PKI technology and uses is required. The security requirements for each PKI component are detailed, as well as, their interaction with other components. In addition, a brief analysis of the PKI problem space is presented using a design framework graph.