

PUBLIC KEY INFRASTRUCTURE FEATURES: A CROSS-VENDOR COMPARISON

Kai S. Koong
University of Texas – Pan American
1201 West University Drive, Edinburg, TX 78539, USA
956-665-3353
koongk@utpa.edu

Lai C. Liu
University of Texas – Pan American
1201 West University Drive, Edinburg, TX 78539, USA
956-665-3353
liul@utpa.edu

Jun Sun
University of Texas – Pan American
1201 West University Drive, Edinburg, TX 78539, USA
956-665-3353
jsun@utpa.edu

ABSTRACT

Most companies use different combinations of technologies such as encryption, firewalls and passwords to help secure their systems. One relatively new technology in the realm of cryptography is known as Public Key Infrastructure (PKI). It enables computer establishments to authenticate transactions from one system to another with the use of paired public and private keys. Such an arrangement helps to minimize fraud and accidental access to protected resources of a company. It also helps companies to control which pieces of information can be accessed and by whom. However, there are many PKI vendors, the products of which have common as well as unique features. This study examines 28 selected PKI vendors and their products. Specifically this research attempts to identify the different features and essential components contained in PKI software. The results of this study show that there is a pyramid structure of the basic, mission-critical, essential, and optional features. Also, the distribution of such features varies significantly across different types of vendors (i.e. traditional, newcomer, and open-source). The findings provide insights on how to select PKI vendors and products for companies in a variety of fields, such as e-commerce, telecommunication, insurance, online banking and other financial services.