Public Key Infrastructure: managing the e-Business security

XUEJIA LAI

With the recent explosive growth of the Internet, more and more business are conducted over the open communication network. The increase of information transmitted electronically has lead to an increased need for security. Cryptographic techniques, especially the public-key cryptographic techniques are used to provide the necessary protection to ensure such business process. The widespread of public-key technology requires a reliable and trusted system to manage public keys. Public-key infrastructure provides such a system for manage the trust of the public keys.

In this presentation we shall consider the need for security in the open information network. Business conducted over the internet has two primary concerns for security in the applications: authenticity, which is to identify the user and control who can accesses information, and privacy, which is to ensure communication is private even when carried over open networks. The public-key cryptography appears to be best suited to fulfilling the requirements of the Internet. In order to establish the necessary trust on the public keys, the concept of Public-Key Infrastructure or PKI was introduced to manage such trust through the form of certificates issued by trusted parties.

As examples, we shall consider the different presently available solutions for the security requirements, form the use of simple password, the SSL contained in browsers, the use of single certificate (digital ID), and the need of dual certificates to achieve the data recovery and non-repudiation that are crucial in business environment.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35515-3_53](https://doi.org/10.1007/978-0-387-35515-3_53)