Advances in Natural Science **ISSN 1715-7862**
Vol. **3**, No. **1**, **2010**, pp. 44-50 **www.cscanada.net**
www.cscanada.org

PKI and Its Applications in E-Commerce in China

BAI Qing-hai[1]

Abstract: PKI system supports user authentication, message transmission, data integrity, message storage confidentiality, and the non-repudiation of operation. PKI can completely address e-commerce security requirements and PKI technology has been applied successfully in e-commerce as well. This article studies the system compositions of e-commerce, briefly analyzes e-commerce's applications in various countries, and highlights PKI and its applications in e-commerce in China.
Keywords: Public Key Infrastructure; E-commerce; application

1. INTRODUCTION

PKI is short for Public Key Infrastructure. It is a set of network security infrastructure (MA & WANG, 2008) to offer secured solutions with general adaptability to address the information security needs for open Internet by taking the advantages of the concept and technology of public keys. PKI system supports user authentication, message transmission, data integrity, message storage confidentiality, and the non-repudiation of operation.

PKI shares same characteristics with general infrastructure. Let's compare PKI with power infrastructure as an example: as power infrastructure, outlets on a wall can be used by various appliances. While PKI as well offers various application entities services, the difference is that what PKI provides is security services. PKI provides security architecture for overall application system and can be used by any entity with security requirements in the system. PKI's interface must thereby be uniform, only then it can make it as easy as appliance connects to outlet while entities use security services.

In addition, as an infrastructure, PKI is primarily used for providing support for application systems and is isolated from the application systems applying it. Since the design, development, and management can be conducted independently without concerning the particularity of applications. Just because of the characteristics of infrastructure that substantially improves the efficiency of PKI's system design and development. The entities PKI supports include both current applications and possible new applications in the future, for instance power infrastructure owns the feature of generality that can support the application of new halogen cooking pots which was unavailable at the starting stage of implementing power infrastructure.

Through PKI, application program developers then don't necessarily pay attention to complicated mathematical models and calculations. What they need to proceed is nothing but to follow standards and

[1] Male, Ph.D Candidate, College of Computer Science and Technology, Inner Mongolia University for the Nationalities, Tongliao 028000, China.
* Received 16 June 2009; accepted 5 January 2010

use uniform interfaces, just as users don't need to concern how power is being transmitted while using appliances.

PKI must meet following performance requirements: user-familiar and easy-to-use interface; predictable and valid PKI-provided secured services; and the feature that application objects don't need to know PKI provides secured services.

At present, PKI can completely address e-commerce security requirements and PKI technology has been applied successfully in e-commerce.

E-commerce belongs to something emerging and there is so far no fully unified definition since it is just available for a short time. Scholars and merchants, from different dimensions, have different definitions. Broadly speaking, business activities, as long as conducted through networks (fixed networks or wireless networks) can all be described as e-commerce. With the popularization and development of the Internet, people have gradually moved their focus to the Internet and Internet-associated applications are thereby even more and more widespread. People's understanding on e-commerce gradually exceeds previous category, i.e. extending network category from the Internet to all fixed networks and wireless ones. Therefore, as long as the business activities are performed via networks; they can then be called as e-commerce.

E-commerce was originally from Electronic Commerce or Electronic Business with EC or EB for short. Its contents include two aspects: one is electronic form and the other is business activities.

In November 1997, THE WORLD BUSINESS AGENDA FOR ELECTRONIC specifically defined e-commerce specifically: e-commerce refers to conducting electronization on overall business activity. Or e-commerce means buyer and seller conduct various business activities by using simple, swift, and low-cost electronic communications without seeing each other.

In general, e-commerce contains two levels: one is among businesses and the other is between businesses and consumers. Based on the definition from Market Intelligence & Consulting Institute (MCI), e-commerce among businesses (B2B EC) refers the business activities completed on automated trading platform via the Internet or LAN. The markets in B2B EC sector primarily include manufacturing sector and service sector. The e-commerce between businesses and consumers (B2C EC) refers to commodity or service fulfillment for consumers from businesses via the Internet. The markets in B2C EC sector include online shopping, network advertising, and network financial services, etc.

2. E-COMMERCE DEVELOPMENT IN VARIOUS COUNTRIES WORLDWIDE

Practice shows that e-commerce introduces human society revolutionary changes in economic, predicting the arrival of global digital economy. People from all over the world pay extra attention to the development of e-commerce and as well set it as the strategy to develop the economy in their own countries.

2.1 E-Commerce Development Overview in the United States

E-commerce in the modern sense emerged in the United States in the middle of 1990s of twenty century after the achievement of Internet commercialization.

After 1996, America's academic world formally presented the concept of e-commerce that has flourished in America ever since. E-commerce, once appeared as a new thing, has been highly valued in America. Both businesses and governments strongly support it and as well formulate plenty of e-commerce related regulations and policies to promote its growth (LIU, 2003).

In 1997 American government released "Global Electronic Commerce Outlines" and mentioned the

Internet in the same breath as Industrial Revolution happened 200 years ago. Clinton in 1998 delivered his famous speech of "Network Government", announcing tax exemption on e-commerce in order to promote network trading and U.S. Congress then passed "Internet Taxation Free Act" soon. In 1999, Utah firstly recognized the legal effect of e-signature through state legislation. And in 2000 the "Electronic Signature Act" was passed by the congress and turned into a federal law.

E-commerce was originally from America. Highly developed market economy system, advanced IT technology, and social market condition make e-commerce in America develop remarkably fast and maintain worldwide leading level currently.

In B2C sector, Amazon created the precedent of online retail, arousing e-commerce upsurge in America. Driven by Amazon, there appears plenty of online stores in America; many famous websites, such as Yahoo and AOL, etc, and access service provides as well established their own online stores to conduct online sales; Wal-Mart, the largest US retailer, and Sears Holdings, the second largest chain store, all launched online retail business in 1999.

In B2B sector, almost all US large enterprises are currently using e-commerce. In 2000, General Motor, Ford, and Daimler – Chrysler, the top three US auto makers, jointly established online purchasing market through which completes 300 billion parts and other goods purchasing annually. In addition to a 10% cost reduction, online purchasing also substantially scales down purchasing time and expedites auto making process as well.

2.2 E-Commerce Development Overview in Japan

E-commerce markets in Japan consistently grow in recent years, not only turning into an indispensable trading means among businesses, but also becoming the most convenient approach for individual consumers to obtain needed commodities. The status of e-commerce in Japan's economic activities is getting more and more important.

A couple of years ago, people using network to conduct e-commerce activities were almost all youngsters; at present more and more senior citizens are using network to conduct business activities. The statistics from Ministry of Internal Affairs of Japan indicated that 81% of aged families of over 60s once bought stocks, bonds, or commodities by using network in the past. Rakuten and Yahoo Japan are famous e-commerce companies in Japan and the online shopping malls from these two provide consumers with various services; and the prices for the goods they offer are generally 5%-10% lower than those from ordinary shopping malls for the same products.

2.3 E-Commerce Development Overview in United Kingdom

Until 2004, various indicators of e-commerce development in UK all have improved significantly, and turnover, in particular, even doubled. A survey conducted by British magazine Economist in April 2004 demonstrated that, in the top ten e-commerce counties worldwide UK ranked the second, Denmark the first, and US the sixth. The survey from British Interactive Media Retail Group (IMRG) also showed that there were 20 millions of British purchasing online. In 2003, online purchasing was accountable for 10% in overall retails in UK, and reached 80 billion pounds until 2009.

The widespread of the Internet is anther important driving power of e-commerce. Currently in UN, not also almost every single family has Internet access, but also businesses have largely equipped networking facilities. Based on existing dominance, a large number of traditional businesses, with a small amount of investment, rapidly open up networking services, among which financial and insurances, air transportation, computer, and retail sectors, etc, have grown into the leading industries in e-commerce world.

At present, with the trend that more and more enterprises use e-commerce to reconstruct traditional business activities, it is getting closer and closer to the goal of "Broadband China". E-commerce in UK still is still booming and British government hopes that UK's continuously leading status in e-commerce field could be more and more stable.

3. E-COMMERCE DEVELOPMENT OVERVIEW IN CHINA

The concept of e-commerce was firstly introduced in China in 1993 and the very first online transaction was conducted in China in 1996. The demo project of e-commerce among businesses aiming at promoting national economy informatization was launched in 1998. E-commerce has started its concept-to-practice transformation in China since 1999. From original B2C model to C2C online auction in 1999 as well as B2B model emerged in 1999, e-commerce has achieved sound development in China. NPC standing committee in April 2005 promulgated "China Electronic Signature Law", establishing legal protection on e-commerce activities in China.

China Development and Reform Commission and the State Council Information Office jointly promulgated the first "Eleventh Five-Year Plan on E-Commerce Development" in China that clearly defined the overall objective of China's e-commerce development during the eleventh five-year plan period: the pattern of e-commerce development environments, support systems, technical services, and application and coordination development will be basically established by the year of 2010. The plan stressed to put forth effort to perfect e-commerce supporting environment, including e-security authentication, online payment, modern logistics, credit service, and standard system.

3.1 Overview

China's B2B market turnover reached 650 billion RMB in 2005, accountable for 95% of total e-commerce transactions. B2C market enjoyed great development in 2006 and B2C currently has already formed a certain market size in China. DangDang.com and Joyo.com, etc take the lead in China's B2C e-commerce field, although C2C's market share is moderate in China market, it has been maintaining a rapidly growing trend in recent years. China's C2C market shows a tripod situation: veteran eBay suffers continuous market drop since it has continuously kept its chargeable service policy; the rising star taobao.com constantly scales up its market share with its free service policy; and paipai.com, under the banner of qq.com, has demonstrated a fast increasing posture with its free service policy as well as QQ's advantage of owning a tremendous number of users ever since its going online in September 2005.

3.2 The Principle to Develop E-Commerce in China

It mainly includes perfecting development environments, innovating development modes, improving application levels, and developing service industries, etc.

3.3 Primary Objectives

E-commerce service sector will grow into an importing emerging industry by the year of 2010, e-commerce application level in various fields such as national economy and social development will be improved substantially and achieved significantly.

(1) Networking production and operation mode will put in shape, business collaboration among enterprises will be substantially strengthened, and the proportions of online purchasing and sales turnout will be accountable for 25% and 10% respectively of total purchasing and sales amount.

(2) The development trend taking the third party e-commerce service as mainstream will put in shape, e-commerce businesses such network-based transaction services, service outsourcing, and IT outsourcing services, etc will take shape.

(3) Mode innovation, management innovation, and technical innovation competence will be improved substantially, the domestic market share of self-owned brand e-commerce key technical

equipments and software will be over 40%.

3.4 China's E-Commerce Development Trend

(1) The depth of e-commerce will be further expanded.

(2) China's e-Commerce will be facing severe challenges.

(3) There will be a merger and acquisition upsurge in e-commerce websites.

(4) Industry e-commerce will be the development mainstream of next generation e-commerce.

(5) The bottleneck of e-commerce will be the issue of online payment. The Chinese government needs to launch regulations to standardize e-payment market in e-commerce.

(6) The primary issue for both e-commerce website transactions and online payment of e-commerce transactions is security. E-commerce will not embrace sound development without the protection from corresponding security mechanism.

4. THE COMPONENTS OF E-COMMERCE

E-commerce is composed of four major parts: electronic trading platform, electronic payment platform, electronic security authentication center, and logistics and distribution center (YIN, 2010).

4.1 Electronic Trading Platform

Electronic trading platform is described as electronic trading center, and the one with larger scale is called electronic trading marketplace.

There are two driving forces in promoting e-commerce activities among businesses: "Buyer" and "Seller". Currently the service platforms in B2C EC transaction are also classified into buyer-led type and seller-led types, and most of them are dominated by large enterprises. In buyer-led type, it mainly collects suppliers' product data, offers enterprises automated purchasing process, and then improves efficiency and reduces purchasing costs, such as Marketplace.

As for seller-led type, it primarily targets large product suppliers and provides sales management channels including mechanisms such as customer relation management and services, etc to reduce sales costs. Dell computer network sales channel, for instance, is a typical successful story.

However, no matter buyer-led or seller-led type, it only has one party-biased function, and therefore can't integrate overall demands from buyers and sellers from markets. In seller-led Dell network sales channels, for example, since the channels only supply products from one maker, it is likely to lose market easily under severe market pressure from price competition; while in buyer-led type, it needs to expand business and extend it to SME-oriented buyer market since many vertical industries have no super-buyers that can dominate market yet. Both buyer-let and seller-led types will therefore develop towards eMarketplace.

4.2 Electronic Payment Platform

Among the four major components in e-commerce, electronic online payment platform is the cornerstone of them. Without online payment, e-commerce handling process would be incomplete. It would be unrealistic to always discuss and sign contracts online but make payment offline. At present, online payment has turned into the bottleneck in e-commerce development. In 2006, electronic payment platform embraced rapid grow. Based on incomplete statistics, non-independent and independent third party electronic payment platforms developed to as many as 50, and PayEase and YeePay typically stand for independent and non-independent third party electronic payment platforms respectively.

PayEase, started operation in March 1999, is the first online payment platform providing multiple bank cards online transactions cross banks and regions in China. It currently supports 23 banks nationwide and online payment of four major credit cards worldwide with a huge customer base including more than one thousand large and medium-sized enterprises and institutions, government agencies, and social groups.

PayEase's payment service platform includes various online payment services such as B2C, B2B, and G2C, etc, supports bankcards and electronic top-up billing systems to make payment in various terminals such as communities, the Internet, bank counters, information kiosks, cell phones, and desk phones, etc; and can also be broadly used in the application systems of transaction, payment, billing, liquidation, and membership managements in e-commerce and e-government fields.

The development of e-commerce is not the only issue of electronics or commerce; it meanwhile is rather the one of commercial credit. Based on its unique secondary settlement mode, PayEase, as the neutral third party in payment process, has turned into the essential component to establish e-commerce law and credit as well.

The secondary settlement mode that is defined upon ordinary payment services is PayEase's unique payment settlement mode. In the secondary settlement service process, PayEase doesn't simply functions as the channel connecting payment gateways in various banks; it, as the neutral third party institution instead, maintains valid transaction data from both merchants and consumers to provide effective protection on behalf of two parties' legitimate rights and interests.

4.3 Electronic Security Authentication Center

It needs PKI/CA infrastructure for security concern in the processes of electronic trading platform, online payment platform, and logistics and distribution center of e-commerce activities.

E-commerce, e-government, and online banking facts are based on the Internet with special security requirements. It must perform online authentication, keep online data flow and fund flow confidential, prohibit online data tampering, and conduct digital signature on transaction data, etc.

To achieve mentioned security requirements, it must introduce PKI mechanism (XIONG, May 2009) in the security design and implementation of online banks, e-commerce, and e-government, etc. At present, only PKI is the security cornerstone for online banks, e-commerce, and e-government.

4.4 Logistics and Distribution Center

Logistics and distribution center is one of the four major centers in e-commerce; it fulfills post-payment logistics and distribution. Distribution, as a minor system in logistics system, owns various elements in logistics and has certain parts consistent to large logistics activities. During operation, logistics and distribution center must put forth effort to discover cost-reduction ways for customers and seek minimum logistics costs. Distribution process optimization is not only required by enterprises to cut costs; it is also the key to develop overall logistics industry in China. As long as China-tailored distribution process optimization model machine method gets its breakthrough, it will introduce huge improving effect on overall logistics industry in China and generate important significance for the sound development of China's economy as well.

REFERENCES

LIU Bao-hui. (2003). E-Commerce Development Overview in the United States [J]. *Economic Forum*, *17*:31-32.

MA Chen-yun & WANG Yan. (July 2008). *Master PKI Network Security Authentication Technology and Programming Implementation [M]*. Beijing: Post and Telecom Press.

XIONG Ping. (May 2009). *Information Security Theory and Application [M]*. Beijing: Tsinghua University Press.

YIN Jie. (2010). The Issues and Solutions of E-Commerce Logistics and Distribution in China [J]. *Economy in Special Administration Region, (02):*277-278.