Research on key escrow technology Based on software

To cite this article: Zhengli Yu 2019 J. Phys.: Conf. Ser. 1168 032131

View the article online for updates and enhancements.
Research on key escrow technology Based on software

Zhengli Yu

1Department of Computer Science, University of Liverpool, L69 3BX Liverpool, United Kingdom

Abstract. With the rapid development of e-commerce, security issues have attracted more and more attention. In this paper, PKI-based electronic commerce security key escrow technology and protocol are studied, the role of PKI in e-commerce security and the application characteristics of PKI are explained, and the design scheme of a digital authentication system based on PKI is described.

1. Security issues related to e-commerce
The so-called electronic commerce refers to the operation and management activities conducted by using various information technologies. With the rapid development of Internet technology, e-commerce has to face a crucial issue -- security in e-commerce. So far, methods that can effectively guarantee the security of computer network, escrow security, access control wall, system vulnerability detection, hacker tracking and virus detection can be used. For the security of business transaction information, a relatively safe, reliable and convenient e-commerce application environment is established on the basis of computer network security to provide more perfect and reliable protection for information. PKI is a very effective tool that provides a trust foundation for exchanging data between Intranet, Extranet, and Internet network environments. This paper studies and discusses the application of PKI to secure key escrow technology and protocol in electronic commerce.

2. Concept of key escrow and related technologies

2.1 Key escrow
KeyRecovery, also known as KeyRecovery, is a technology that can obtain decryption information in an emergency. It is used to save users' private key backup, which can either help national judicial or security departments to obtain original plaintext information when necessary, or recover plaintext when users lose or damage their keys. Key escrow means that the user must divide his or her key into t pieces and hand them to a trusted custodian before applying for a data encryption certificate from the CA. No custodian can restore a complete user password with a portion of the user key stored on their own. Only the key stored by this t individual can be combined to get the user's complete key. Key escrow mainly has anti - repudiation, government surveillance, key recovery and other functions.

2.2 PKI
PKI technology is the most widely used and fundamental protocol in the system. In a broad sense, all systems providing public key encryption and digital signature services can be called PKI systems. A standard PKI domain must have the following main conditions : (I) CA (Certificate Authority) CA is the core executive body of PKI, which is the main component of PKI and is also the application registration, certificate issuance and management body of digital certificates. (2) Certificate and
certificate store certificate is the abbreviation of digital certificate or electronic certificate. It conforms to x.509 standard and is the proof of online entity identity. The certificate base is a public information base for CA to issue certificate and cancel certificate. (3) key backup and recovery to avoid key loss, PKI provides key backup and key recovery mechanism: when the user certificate is generated, the encryption key is stored by CA backup; When recovery is required, the user only needs to apply to the CA, and the CA will automatically resume for the user. (4) the update of keys and certificates is generally done automatically by the PKI system, without user intervention. Before the expiration date ends, FKI/CA will automatically initiate an update program to generate a new certificate to replace the old one. (5) the certificate history file records the entire key history of multiple 1-day certificates and at least one current new certificate. (6) client software client software is used to realize the functions of digital signature, encryption and data transmission, etc., and is responsible for querying the revocation information of certificates and related certificates, processing the certificate path, and making clear the stamp when providing specific documents during the authentication process. (7) there are basically two methods to realize cross certification: one is to bridge CA, which USES a third party CA as the bridge to connect multiple CA to become a trusted entity; Another -- multiple CA root CA (RCA) issues root certificates to each other, so that when end users in different PKI domains verify the roots along different authentication chains, mutual trust can be achieved.

3. Development status and existing problems of domestic PKI

3.1 The status quo
Compared with developed countries, the development of PKI technology in China is still in its infancy, and the government and relevant departments have attached great importance to the development of PKI industry in recent years. For example, the ministry of science and technology's 883 plan is specifically set up for PKI, and the national planning commission is also considering making new plans to support the development of PKI industry, and the construction of PKI system has been clearly proposed in the national electronic product administrative engineering. In 1998, Shanghai CA center (she-ca), the first entity in China, was established. Since then, dozens of different types of CA certification institutions have been established nationwide. The concept of CA certification has gradually permeated from e-commerce to e-government, finance, science and education and other fields.

3.2 Existing problems
At present, the main problems of PKI/CA certification in China are as follows: This lack of the same standard will inevitably lead to the coexistence of multiple technical standards, which is also a major reason why many CA centers in China are divided and difficult to communicate. (2) Authority issues some CA certification bodies are not rigorous enough in issuing and auditing certificates. In order to seize the market, it is difficult to guarantee the authority and impartiality of authentication without strict identification and verification. (3) in the distribution pattern of certification bodies, many CA certification bodies are obviously regional and industrial, which cannot meet the basic requirements of acting as a third-party authoritative certification body for the whole society. For the Internet, there should be no physical regional restrictions.

4. Application architecture of PKI
Specifically, the PKI includes CA, digital certificate store, key backup and restore system, certificate invalidation processing system and client certificate processing system. Certification center (CA) is the core link in the e-commerce system and the foundation of the trust in electronic trading. It can check and verify the user identity and relevant information of the certificate application through its own registration audit system, so that the objective authenticity of the user attributes of online transactions is consistent with the authenticity of the certificate. As an authoritative, reliable and impartial third party organization, certification center is especially responsible for issuing and
managing digital certificates required by all entities involved in online transactions. The certificate base is the central storage place for CA to issue and revoke certificates, and it can be used by users to make open queries to obtain other users’ certificates and public keys. The most widely used and fundamental protocol of PKI technology system is x.509 protocol of ITU, which aims to define a standard digital certificate format to provide a means of authentication for directory service based on x.509 protocol.

5. Application of PKI in e-business security key escrow

5.1 Structure of the secret system of key escrow
Key escrow encryption system mainly consists of three parts as shown in figure 1:

![Key escrow system diagram](image)

- **User security module** (USC: User Security Component): it is a hardware device or software program that uses the key to complete the encryption and decryption of data and appends to the encrypted data in the data recovery domain.
- **Key escrow module** (KEC: Key Escrow Component): controlled by the key escrow structure to manage the storage, transmission and use of data recovery keys, which can be an integral part of the key management foundation.
- **Data recovery module** (DRC: Data Recovery Component): composed of algorithms, protocols and devices, it is responsible for recovering the data encryption key from the private key information provided by the key escrow module and information contained in the data recovery domain, so as to unlock the cipher text.

5.2 Steps for security key escrow.
In order to prevent the key escrow agent from abusing its authority and the key to be leaked, the user's private key is decomposed into several parts and kept by different key escrow agents. The validity of the user's private key can only be restored by combining all the private key components. The steps for key escrow are as follows:

1. The user selects several key escrow agents and gives each agent a public key and a part of private key. The managed agent generates a corresponding managed certificate based on the key components obtained. The certificate contains the user's specific identifier (UID: UniqueIdentifier), the public and private keys that are managed, and the number of the managed certificate. The key escrow agent also encrypts the managed certificate with its signature public key, generates a digital signature, and attaches it to the managed certificate.
2. After receiving all the managed certificates, the user shall submit the certificate and complete public key to the certificate authority authentication center to apply for the encryption certificate.
3. The certificate authority certifies the authenticity of each managed certificate, that is, whether each managed agent keeps part of the valid private key component and confirms the user's identity. After all the validation work is completed, the certificate authority authentication center generates the encrypted certificate and sends it to the user.

5.3 Application of PKI in e-commerce security
In order to make online transactions safe and reliable, we must strengthen security measures to prevent
cheating. In June 1997, IBM, MasterCard, Microsoft and NetsCApe, GTE, Verisign, SAIC, Terisa common standards for the security of e-commerce (Secure Electronic Transactions, referred to as the SET), the purpose is to solve transmission on the public network the security of sensitive personal and financial information, prompting the development of global e-commerce. Adding key escrow technology to SET can help government and law departments to monitor and prevent criminal activities. The cardholder merchant payment gateway first applies to the CA to sign the public key certificate, then applies for the data exchange public key certificate and entrusts the data exchange private key (as shown in figure 2). Take cardholder A and merchant B as examples to illustrate the key escrow technology in SET: cardholder A sends message M to merchant B, and government or legal authorities wish to monitor this process compulsively. The client's public key signature certificate can be obtained from CA. After the client verifies its identity, it can send a private key fragment to the government or legal authorities. After combination, it can obtain the cardholder's private key and see the message.

5.4 generation of digital certificates
When two users need to establish secure communication, the first thing to do is to obtain a trusted digital certificate from the CA. If A wants to send encrypted web page information to B, it can send \((D^"E5+") + (\text{hash (des)}) + r, s(DaJa)\) to B. Where A generates session key uniformly adopted DES is one key at A time. We want to determine the security of DES, first hash the DES password, then encrypt it with A's public key, then encrypt the DES password and DES's signature with B's public key, and send the message to be sent with DES encryption. When B receives the data, it decrypts it with its private key and gets a DES password and an encrypted data. But the fact that this DES password is secure requires encrypting data to verify it. First, the public key of A is used to decrypt the Hash (DES). Since the Hash function is known by both parties, the inverse function is used to obtain another DES. The two DES compare with each other. If there is no error, the data is confirmed to be from trusted party A and is transmitted safely to B.

![Figure 2. Key escrow technology example](image)

6. Conclusion
E-commerce is a key project in the development of Internet application, and it will gradually become an important part of our economic life. The bottleneck of my e-commerce development is security, perfect and correct implementation of PKI system is the best way to comprehensively solve all network transactions and communication security problems. In order to truly popularize digital certificates and make network communication more secure, the system proposed in this paper will be extended to the application fields of power government and business.

References
[1] Choi W K, Moon A R, Han C, et al. A Study on Construction of escrow Garden based on the Growth Condition [J]. Horticulture Abstracts, 2016.
[2] Chen Y, Yun-Lin M A. On the escrow car application of gesture recognition technology based on vision [J]. Electronic Design Engineering, 2016.
[3] Gaylor T R. System and method for key recovery: U.S. Patent 7,831,833[P]. 2010-11-9.
[4] Liping H, Lei S. Research on trust model of pki[C]//Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on. IEEE, 2011, 1: 232-235.
[5] Han K, Yeun C Y, Shon T, et al. A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication [J]. International Journal of Communication Systems, 2011, 24(4): 461-472.